¡¡APRUEBE SU EXAMEN CON SCHAUM!!

Matemáticas discretas

Schaum

3ª EDICIÓN

Seymour Lipschutz • Marc Lipson

- 467 PROBLEMAS RESUELTOS PASO A PASO
- REVISIONES COMPLETAS DE ARITMÉTICA POR COMPUTADORA Y CRIPTOLOGÍA
- CUBRE TODOS LOS FUNDAMENTOS DEL CURSO: ES EL TEXTO IDEAL PARA EL AULA

Utilícelo para las siguientes asignaturas:

- ☑ INTRODUCCIÓN A LAS MATEMÁTICAS DISCRETAS
- ☑ MATEMÁTICAS DISCRETAS

Mc Graw Hill

MATEMÁTICAS DISCRETAS

MATEMÁTICAS DISCRETAS

Tercera edición

Seymour Lipschutz, Ph. D.
Temple University

Marc Lars Lipson, Ph. D.
University of Virginia

Revisión técnica

María de Lourdes Quezada Batalla
Departamento de Ciencias Básicas
Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Estado de México

MÉXICO • BOGOTÁ • BUENOS AIRES • CARACAS • GUATEMALA
LISBOA • MADRID • NUEVA YORK • SAN JUAN • SANTIAGO
AUCKLAND • LONDRES • MILÁN • MONTREAL • NUEVA DELHI
SAN FRANCISCO • SINGAPUR • SAN LUIS • SIDNEY • TORONTO

Director Higher Education: Miguel Ángel Toledo Castellanos
Director editorial: Ricardo A. del Bosque Alayón
Coordinadora editorial: Marcela I. Rocha Martínez
Editor sponsor: Pablo E. Roig Vázquez
Supervisor de producción: Zeferino García García

Traducción: Hugo Villagómez Velázquez

MATEMÁTICAS DISCRETAS
Tercera edición

ISBN 13: 978-970-10-7236-3

0123456789 08765432109

Impreso en México *Printed in Mexico*

ACERCA DE LOS AUTORES

SEYMOUR LIPSCHUTZ da clases en la Facultad de Matemáticas de la Universidad Temple y antes enseñó en el Instituto Politécnico de Brooklin. Se doctoró en 1960 en el Instituto Courant de Ciencias Matemáticas de la Universidad de Nueva York. Es uno de los más prolíficos autores de la serie Schaum's Outlines, y también es autor de *Probability*; *Finite Mathematics*, 2a. edición; *Linear Algebra*, 3a. edición; *Beginning Linear Algebra*; *Set Theory*; y *Essential Computer Mathematics*.

MARC LARS LIPSON da clases en la Universidad de Virginia y antes enseñó en la Facultad de la Universidad de Georgia. Se doctoró en finanzas en 1994 en la Universidad de Michigan. También es coautor de *Linear Algebra*, 3a. edición y *2000 Solved Problems in Discrete Mathematics* con Seymour Lipschutz.

PRÓLOGO

Las matemáticas discretas, el estudio de los sistemas finitos, han adquirido cada vez más importancia en la medida en que ha avanzado la era de las computadoras. Básicamente, la computadora digital es una estructura finita, y muchas de sus propiedades pueden comprenderse e interpretarse en el marco de referencia de los sistemas matemáticos finitos. Este libro, al presentar el material esencial, cumple los requisitos de un curso formal de matemáticas discretas, o como complemento de cualquier texto actual.

Los tres primeros capítulos cubren el material normal sobre conjuntos, relaciones y funciones y algoritmos. Luego, siguen capítulos sobre lógica, conteo y probabilidad. A continuación hay tres capítulos sobre teoría de gráficas, gráficas dirigidas y árboles binarios. Por último, hay capítulos individuales sobre propiedades de los enteros, lenguajes, máquinas, conjuntos ordenados y retículas, y álgebra booleana, así como apéndices sobre vectores y matrices, y sistemas algebraicos. El capítulo sobre funciones y algoritmos incluye un análisis de cardinalidad y conjuntos numerables, y complejidad. Los capítulos sobre teoría de gráficas incluyen análisis sobre planaridad, recorribilidad (*traversability*), rutas mínimas y los algoritmos de Warshall y Huffman. Se recalca que los capítulos han sido escritos de modo que sea posible modificar su orden sin dificultad ni pérdida de continuidad.

Cada capítulo empieza con un planteamiento claro de las definiciones, principios y teoremas pertinentes, con material ilustrativo y de otros materiales descriptivos. Después, se plantean conjuntos de problemas resueltos y complementarios. Los problemas resueltos sirven para ilustrar y ampliar el material, y también incluye demostraciones de teoremas. Los problemas complementarios proporcionan una revisión completa del material del capítulo. Se ha incluido más material, el cual puede cubrirse en la mayor parte de los primeros cursos. Lo anterior se ha hecho con la intención de que el libro sea más flexible, a fin de ofrecer un libro de referencia más útil, y para estimular un mayor interés en los temas presentados.

SEYMOUR LIPSCHUTZ
MARC LARS LIPSON

CONTENIDO

1 Teoría de conjuntos

CAPÍTULO

1.1 INTRODUCCIÓN

El concepto de *conjunto* aparece en todas las matemáticas. Por ello es que conviene iniciar este capítulo con la notación y la terminología básicas de la teoría de conjuntos, las cuales se utilizan en todo el texto; el capítulo termina con la definición formal, y ejemplos, de la inducción matemática.

1.2 CONJUNTOS, ELEMENTOS Y SUBCONJUNTOS

Un *conjunto* es una colección bien definida de objetos, que se denominan *elementos* o *miembros* del conjunto. Las letras mayúsculas $A, B, X, Y, \ldots$, denotan conjuntos y las minúsculas $a, b, x, y, \ldots$, denotan elementos de conjuntos. Algunos sinónimos de "conjunto" son "clase", "colección" y "familia".

La pertenencia a un conjunto se denota:

$a \in S$ denota que a pertenece al conjunto S.

$a, b \in S$ denota que a y b pertenecen al conjunto S.

Aquí $\in$ es el símbolo para indicar "es un elementos de" y $\notin$ significa "no es un elemento de".

Especificación de conjuntos

Hay dos formas para especificar un conjunto particular. Una forma, de ser posible, consiste en enumerar sus elementos separados por comas y escritos entre llaves { }. La segunda es escribir las propiedades que caracterizan a los elementos del conjunto. Dos ejemplos de lo anterior son:

$$A = \{1, 3, 5, 7, 9\} \quad \text{y} \quad B = \{x \mid x \text{ es un entero par}, x > 0\}$$

Es decir, A consta de los elementos 1, 3, 5, 7, 9. El segundo conjunto se lee:

$$B \text{ es el conjunto de } x \text{ tal que } x \text{ es un entero par y } x \text{ es mayor que } 0,$$

denota el conjunto B, cuyos elementos son los enteros pares positivos. Observe que para denotar un miembro del conjunto se usa una letra, casi siempre x; la recta vertical | se lee "tal que" y la coma "y".

EJEMPLO 1.1

a) El conjunto A anterior también se escribe como $A = \{x \mid x \text{ es un entero positivo impar}, x < 10\}$.

b) Aunque no es posible listar todos los elementos del conjunto B anterior, a este conjunto se le especifica como

$$B = \{2, 4, 6, \ldots\}$$

donde se supone que todo mundo lo entiende. Observe que $8 \in B$, pero $3 \notin B$.

c) Sean $E = \{x \mid x^2 - 3x + 2 = 0\}$, $F = \{2, 1\}$ y $G = \{1, 2, 2, 1\}$. Entonces $E = F = G$.

Aquí es preciso señalar que un conjunto no depende de la forma en que se muestren sus elementos. Un conjunto es el mismo aun si sus elementos se repiten o están en desorden.

Incluso si es posible enumerar los elementos de un conjunto, hacerlo tal vez no sea práctico. Es por esto que los elementos de un conjunto se enumeran sólo si son pocos; en caso contrario, un conjunto se describe con la indicación de la propiedad que caracteriza a sus elementos.

Subconjuntos

Suponga que todo elemento de un conjunto A también es un elemento de un conjunto B; es decir, si $a \in A$ implica que $a \in B$. Entonces se dice que A es un *subconjunto* de B. También se dice que A está *contenido* en B o que B *contiene* a A. Esta relación se escribe

$$A \subseteq B \quad \text{o} \quad B \supseteq A$$

Dos conjuntos son iguales si ambos tienen los mismos elementos o, equivalentemente, si cada uno está contenido en el otro. Es decir:

$$\boxed{A = B \text{ si y sólo si } A \subseteq B \text{ y } B \subseteq A}$$

Si A no es un subconjunto de B —porque al menos un elemento de A no pertenece a B— se escribe $A \nsubseteq B$.

EJEMPLO 1.2 Considere los conjuntos:

$$A = \{1, 3, 4, 7, 8, 9\}, \quad B = \{1, 2, 3, 4, 5\}, \quad C = \{1, 3\}.$$

Entonces $C \subseteq A$ y $C \subseteq B$, ya que 1 y 3, los elementos de C, también son miembros de A y B. Pero $B \nsubseteq A$, puesto que algunos elementos de B, por ejemplo, 2 y 5, no pertenecen a A. En forma semejante, $A \nsubseteq B$.

Propiedad 1: En matemáticas es una práctica común cruzar un símbolo con una línea vertical "|" o una diagonal "/" para indicar el significado opuesto o negativo del símbolo.

Propiedad 2: La declaración $A \subseteq B$ no excluye la posibilidad de que $A = B$. De hecho, para todo conjunto A se tiene $A \subseteq A$, ya que todo elemento de A pertenece a A. No obstante, si $A \subseteq B$ y $A \neq B$, entonces se dice que A es un subconjunto propio de B (lo que algunas veces se escribe $A \subset B$).

Propiedad 3: Suponga que todo elemento de un conjunto A pertenece a un conjunto B y que todo elemento de B pertenece a un conjunto C. Entonces resulta evidente que todo elemento de A también pertenece a C. En otras palabras, si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

Las propiedades anteriores llevan al siguiente teorema:

Teorema 1.1: Sean A, B y C tres conjuntos cualesquiera. Entonces:

i) $A \subseteq A$

ii) Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$

iii) Si $A \subseteq B$ y $A \subseteq B$, entonces $A \subseteq B$

Símbolos especiales

En el texto aparecen muy a menudo algunos conjuntos, para los que se usan símbolos especiales. Algunos de estos símbolos son:

$\mathbf{N}$ = conjunto de *números naturales* o enteros positivos: 1, 2, 3,...
$\mathbf{Z}$ = conjunto de todos los enteros: ..., −2, −1, 0, 1, 2,...
$\mathbf{Q}$ = conjunto de números racionales
$\mathbf{R}$ = conjunto de números reales
$\mathbf{C}$ = conjunto de números complejos

Observe que $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$.

Conjunto universo y conjunto vacío

Todos los conjuntos que se estudian en cualquier aplicación de la teoría de conjuntos pertenecen a un gran conjunto fijo denominado *universo*, que se denota por

$$\mathbf{U}$$

a menos que se establezca o implique otra cosa.

Dados un conjunto universo **U** y una propiedad P, en **U** puede no haber elementos que tengan la propiedad P. Por ejemplo, el siguiente conjunto no tiene elementos:

$$S = \{x \mid x \text{ es un entero positivo, } x^2 = 3\}$$

Un conjunto que no tiene elementos se denomina *conjunto vacío* o *conjunto nulo* y se denota por

$$\varnothing$$

Sólo hay un conjunto vacío. Es decir, si S y T son vacíos, entonces $S = T$, ya que tienen exactamente los mismos elementos, a saber, ninguno.

El conjunto vacío $\varnothing$ también se considera como un subconjunto de cualquier otro conjunto. Así, el planteamiento formal de este sencillo resultado es:

Teorema 1.2: Para cualquier conjunto A, se tiene $\varnothing \subseteq A \subseteq \mathbf{U}$.

Conjuntos ajenos o disjuntos

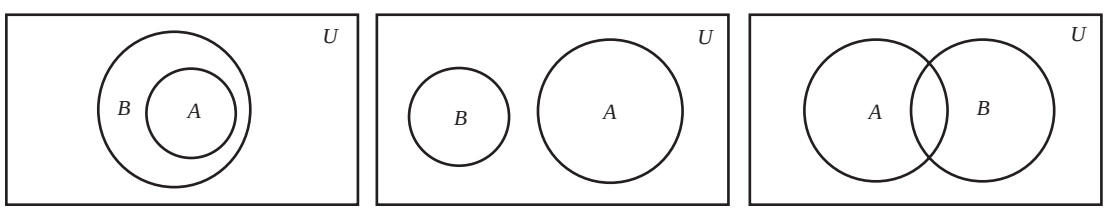
Dos conjuntos A y B son *ajenos* o *disjuntos*, si no tienen elementos en común. Por ejemplo, suponga

$$A = \{1, 2\}, \quad B = \{4, 5, 6\} \quad \text{y} \quad C = \{5, 6, 7, 8\}.$$

Entonces A y B son ajenos, y A y C son ajenos. Pero B y C no son ajenos porque B y C tienen elementos en común, 5 y 6. Observe que si A y B son ajenos, entonces ninguno es un subconjunto del otro (a menos que uno sea el conjunto vacío).

1.3 DIAGRAMAS DE VENN

Un diagrama de Venn es un gráfico donde los conjuntos se representan con regiones encerradas en un plano. Aquí el conjunto universo **U** es el interior de un rectángulo y los otros conjuntos se representan por círculos dentro del rectángulo. Si $A \subseteq B$, entonces el círculo que representa a A está dentro del círculo que representa a B, como se muestra en la figura 1-1*a*). Si A y B son ajenos, entonces el círculo que representa a A está separado del círculo que representa a B, como se muestra en la figura 1-1*b*).



a) $A \subseteq B$ *b*) A y B son ajenos *c*)

Figura 1-1

No obstante, si A y B son dos conjuntos arbitrarios, es posible que algunos elementos estén en A pero no en B, que otros estén en B pero no en A, que algunos estén tanto en A como en B, y que otros no estén ni en A ni en B; por tanto, en general A y B se representan como en la figura 1-1*c*).

Argumentos y diagramas de Venn

Muchas declaraciones verbales son, en esencia, sobre conjuntos y, en consecuencia, se les puede describir mediante diagramas de Venn; por tanto, éstos sirven para determinar si un argumento es válido o no.

EJEMPLO 1.3 Demuestre que el siguiente argumento (una adaptación de un libro de lógica de Lewis Carroll, autor de *Alicia en el país de las maravillas*) es válido:

S_1: Todos mis objetos de estaño son cazos.
S_2: Encuentro muy útiles todos tus regalos.
S_3: Ninguno de mis cazos es útil.

S : Tus regalos no son de estaño.

Las declaraciones S_1, S_2 y S_3, arriba de la línea horizontal, son los supuestos o las hipótesis y la declaración S, abajo de la línea horizontal, es la conclusión. El argumento es válido si la conclusión S se obtiene en forma lógica a partir de las hipótesis S_1, S_2 y S_3.

Si S_1 son todos los objetos de estaño que contiene el conjunto de los cazos, entonces S_3, el conjunto de los cazos, y el conjunto de los objetos útiles son ajenos. Además, por S_2, el conjunto de "tus regalos" es un subconjunto del conjunto de los objetos útiles. En consecuencia, es posible dibujar el diagrama de Venn que se muestra en la figura 1-2.

Resulta evidente que la conclusión es válida por el diagrama de Venn, porque el conjunto "tus regalos" es ajeno al conjunto de los objetos de estaño.

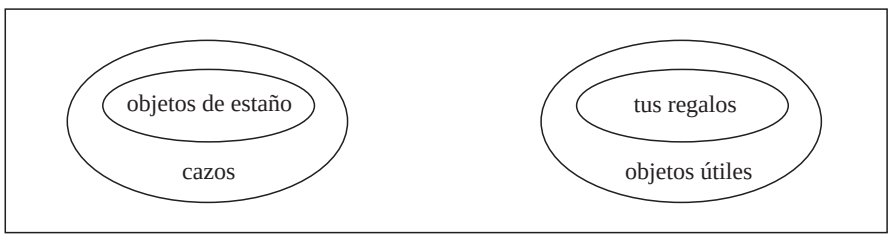


Figura 1-2

1.4 OPERACIONES CON CONJUNTOS

En esta sección se presentan varias operaciones con conjuntos, como son las operaciones básicas de unión, intersección y complemento.

Unión e intersección

La *unión* de dos conjuntos A y B, que se denota por $A \cup B$, es el conjunto de todos los elementos que pertenecen a A o a B; es decir,

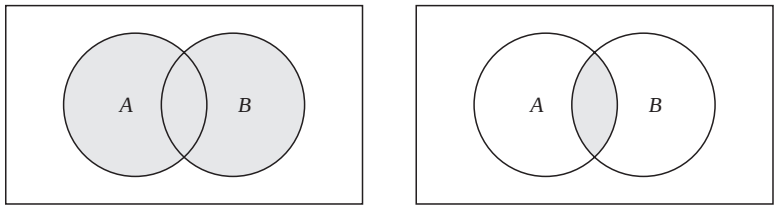
$$A \cup B = \{x \mid x \in A \text{ o } x \in B\}$$

Aquí "o" se usa en el sentido incluyente de y/o. La figura 1-3*a*) es un diagrama de Venn en el que $A \cup B$ está sombreada.

La *intersección* de dos conjuntos A y B, que se denota por $A \cap B$, es el conjunto de los elementos que pertenecen tanto a A como a B; es decir,

$$A \cap B = \{x \mid x \in A \text{ y } x \in B\}$$

La figura 1-3*b*) es un diagrama de Venn en el que $A \cap B$ está sombreada.



a) $A \cup B$ está sombreada *b*) $A \cap B$ está sombreada

Figura 1-3

Recuerde que los conjuntos A y B son *disjuntos* o *ajenos* si no tienen elementos en común o, al aplicar la definición de intersección, si $A \cap B = \varnothing$, el conjunto vacío. Suponga que

$$S = A \cup B \quad \text{y} \quad A \cap B = \varnothing$$

Entonces S se denomina *unión disjunta*, o *ajena*, de A y B.

EJEMPLO 1.4

a) Sean $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, $C = \{2, 3, 8, 9\}$. Entonces

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}, \quad A \cup C = \{1, 2, 3, 4, 8, 9\}, \quad B \cup C = \{2, 3, 4, 5, 6, 7, 8, 9\},$$
$$A \cap B = \{3, 4\}, \quad A \cap C = \{2, 3\}, \quad B \cap C = \{3\}.$$

b) Sean **U** el conjunto de estudiantes en una universidad, M el conjunto de estudiantes varones y F el conjunto de estudiantes mujeres. **U** es la unión disjunta de M y F; es decir,

$$\mathrm{U} = M \cup F \quad \text{y} \quad M \cap F = \varnothing$$

Esto se debe a que cualquier estudiante en **U** está en M o en F, y resulta evidente que ningún estudiante pertenece tanto a M como a F; es decir, M y F son disjuntos.

Es necesario observar las siguientes propiedades de la unión y la intersección.

Propiedad 1: Todo elemento x en $A \cap B$ pertenece tanto a A como a B; así, x pertenece a A y x pertenece a B. Entonces, $A \cap B$ es un subconjunto de A y de B; a saber,

$$A \cap B \subseteq A \quad \text{y} \quad A \cap B \subseteq B$$

Propiedad 2: Un elemento x pertenece a la unión $A \cup B$ si x pertenece a A o x pertenece a B; así, cualquier elemento en A pertenece a $A \cup B$, y cualquier elemento en B pertenece a $A \cup B$. Es decir,

$$A \subseteq A \cup B \quad \text{y} \quad B \subseteq A \cup B$$

El planteamiento formal de los resultados anteriores es:

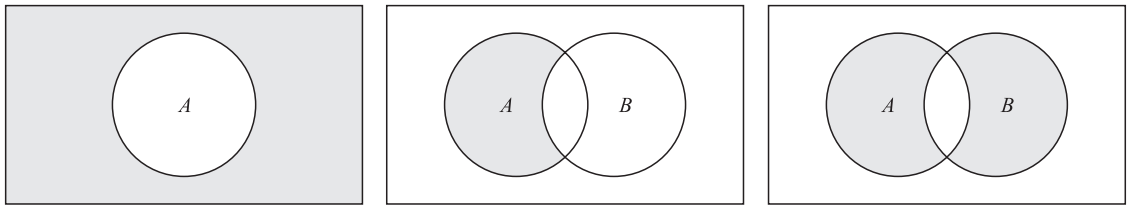
Teorema 1.3: Para dos conjuntos A y B arbitrarios, se tiene:

i) $A \cap B \subseteq A \subseteq A \cup B$ y
ii) $A \cap B \subseteq B \subseteq A \cup B$.

La operación de inclusión de conjuntos se relaciona estrechamente con las operaciones de unión e intersección, como se muestra en el siguiente teorema.

Teorema 1.4: Las siguientes expresiones son equivalentes: $A \subseteq B$, $A \cap B = A$, $A \cup B = B$.

Este teorema se demuestra en el problema 1.8. Otras condiciones equivalentes también se proporcionan en el problema 1.31.



a) A^{C} está sombreado *b*) $A\backslash B$ está sombreada *c*) $A \oplus B$ está sombreada

Figura 1.4

Complementos, diferencias y diferencias simétricas

Recuerde que todos los conjuntos a considerar en un momento particular son subconjuntos de un conjunto universo fijo **U**. El *complemento absoluto* o, simplemente, el *complemento* de un conjunto A, denotado por A^{C}, es el conjunto de elementos que pertenecen a **U**, pero que no pertenecen a A. Es decir,

$$A^{C} = \{x \mid x \in \mathbf{U}, x \notin A\}$$

En algunos textos el complemento de A se denota por A' o $\bar{A}$. La figura 1-4*a*) es un diagrama de Venn en el que A^{C} está sombreado.

El *complemento relativo* de un conjunto B respecto de un conjunto A o, simplemente, la *diferencia* de A y B, denotada por $A\backslash B$, es el conjunto de elementos que pertenecen a A pero que no pertenecen a B; es decir,

$$A\backslash B = \{x \mid x \in A, x \notin B\}$$

El conjunto $A\backslash B$ se lee "A menos B". En muchos textos la expresión $A\backslash B$ aparece como $A - B$ o como $A \sim B$. La figura 1-4*b*) es un diagrama de Venn en el que $A\backslash B$ está sombreada.

La *diferencia simétrica* de los conjuntos A y B, denotada por $A \oplus B$, consta de los elementos que pertenecen a A o a B pero no a ambos. Es decir,

$$A \oplus B = (A \cup B)\backslash(A \cap B) \quad \text{o} \quad A \oplus B = (A\backslash B) \cup (B\backslash A)$$

La figura 1-4*c*) es un diagrama de Venn en el que $A \oplus B$ está sombreada.

EJEMPLO 1.5 Suponga que $\mathbf{U} = \mathbf{N} = \{1, 2, 3, \ldots\}$ es el conjunto universo. Sean

$$A = \{1, 2, 3, 4\}, \quad B = \{3, 4, 5, 6, 7\}, \quad C = \{2, 3, 8, 9,\}, \quad E = \{2, 4, 6, \ldots\}$$

(Aquí E es el conjunto de enteros pares.) Entonces:

$$A^{C} = \{5, 6, 7, \ldots\}, \quad B^{C} = \{1, 2, 8, 9, 10, \ldots\}, \quad E^{C} = \{1, 3, 5, 7, \ldots\}$$

Es decir, E^{C} es el conjunto de enteros positivos impares. También:

$$\begin{array}{llll} A\backslash B = \{1, 2\}, & A\backslash C = \{1, 4\}, & B\backslash C = \{4, 5, 6, 7\}, & A\backslash E = \{1, 3\}, \\ B\backslash A = \{5, 6, 7\}, & C\backslash A = \{8, 9\}, & C\backslash B = \{2, 8, 9\}, & E\backslash A = \{6, 8, 10, 12, \ldots\}. \end{array}$$

Además:

$$\begin{array}{ll} A \oplus B = (A\backslash B) \cup (B\backslash A) = \{1, 2, 5, 6, 7\}, & B \oplus C = \{2, 4, 5, 6, 7, 8, 9\}, \\ A \oplus C = (A\backslash C) \cup (B\backslash C) = \{1, 4, 8, 9\}, & A \oplus E = \{1, 3, 6, 8, 10, \ldots\}. \end{array}$$

Productos fundamentales

Considere n conjuntos distintos $A_1, A_2, \ldots, A_n$. Un *producto fundamental* de los conjuntos es un conjunto de la forma

$$A_1^* \cap A_2^* \cap \ldots \cap A_n^* \quad \text{donde} \quad A_i^* = A \quad \text{o} \quad A_i^* = A^{C}$$

Observe lo siguiente:

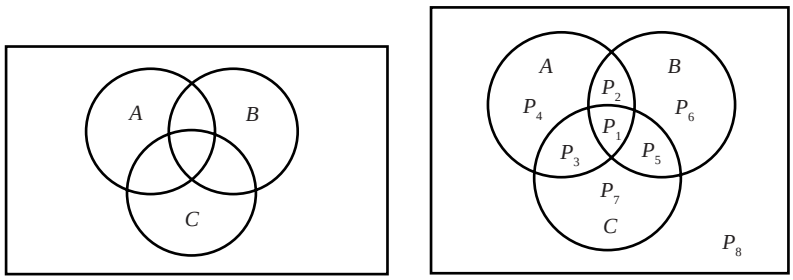
i) Hay $m = 2^n$ de estos productos fundamentales.
ii) Cualesquiera dos productos fundamentales arbitrarios son ajenos.
iii) El conjunto universo **U** es la unión de todos los productos fundamentales.

Así, **U** es la unión disjunta de los productos fundamentales (problema 1.60). Abajo se ilustra una descripción geométrica de estos conjuntos.

EJEMPLO 1.6 La figura 1-5*a*) es el diagrama de Venn de tres conjuntos *A*, *B*, *C*. A continuación se enumeran los $m = 2^3 = 8$ productos fundamentales de los conjuntos *A*, *B* y *C*:

$$P_1 = A \cap B \cap C, \quad P_3 = A \cap B^{\mathrm{C}} \cap C, \quad P_5 = A^{\mathrm{C}} \cap B \cap C, \quad P_7 = A^{\mathrm{C}} \cap B^{\mathrm{C}} \cap C,$$
$$P_2 = A \cap B \cap C^{\mathrm{C}}, \quad P_4 = A \cap B^{\mathrm{C}} \cap C^{\mathrm{C}}, \quad P_6 = A^{\mathrm{C}} \cap B \cap C^{\mathrm{C}}, \quad P_8 = A^{\mathrm{C}} \cap B^{\mathrm{C}} \cap C^{\mathrm{C}}.$$

Los ocho productos corresponden precisamente a las ocho regiones disjuntas en el diagrama de Venn de los conjuntos *A*, *B*, *C* como se indica con la identificación de las regiones en la figura 1-5*b*).



a) *b*)

Figura 1-5

1.5 ÁLGEBRA DE CONJUNTOS, DUALIDAD

Los conjuntos bajo las operaciones de unión, intersección y complemento satisfacen varias leyes (identidades) que se presentan en la tabla 1-1. El planteamiento formal es:

Teorema 1.5: Los conjuntos cumplen las leyes de la tabla 1-1.

Tabla 1-1 Leyes del álgebra de conjuntos

Leyes idempotentes:	(1a) $A \cup A = A$	(1b) $A \cap A = A$
Leyes asociativas:	(2a) $(A \cup B) \cup C = A \cup (B \cup C)$	(2b) $(A \cap B) \cap C = A \cap (B \cap C)$
Leyes conmutativas:	(3a) $A \cup B = B \cup A$	(3b) $A \cap B = B \cap A$
Leyes distributivas:	(4a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(4b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Leyes de identidad:	(5a) $A \cup \varnothing = A$	(5b) $A \cap \mathbf{U} = A$
	(6a) $A \cup \mathbf{U} = \mathbf{U}$	(6b) $A \cap \varnothing = \varnothing$
Leyes de involución:	(7a) $(A^{\mathrm{C}})^{\mathrm{C}} = A$	
Leyes de complementos:	(8a) $A \cup A^{\mathrm{C}} = \mathbf{U}$	(8b) $A \cap A^{\mathrm{C}} = \varnothing$
	(9a) $\mathbf{U}^{\mathrm{C}} = \varnothing$	(9b) $\varnothing^{\mathrm{C}} = \mathbf{U}$
Leyes de De Morgan:	(10a) $(A \cup B)^{\mathrm{C}} = A^{\mathrm{C}} \cap B^{\mathrm{C}}$	(10b) $(A \cap B)^{\mathrm{C}} = A^{\mathrm{C}} \cup B^{\mathrm{C}}$

Observación: Cada ley en la tabla 1-1 se deduce a partir de una ley lógica equivalente. Considere, por ejemplo, la demostración de la ley de De Morgan (10a):

$$(A \cup B)^{\mathrm{C}} = \{x \mid x \notin (A \text{ o } B)\} = \{x \mid x \notin A \text{ y } x \notin B\} = A^{\mathrm{C}} \cap \mathrm{B}^{\mathrm{C}}$$

Aquí se usa la ley lógica equivalente (de De Morgan):

$$\neg(p \vee q) = \neg p \wedge \neg q$$

donde $\neg$ significa "no", $\vee$ significa "o" y $\wedge$ significa "y". (Algunas veces se usan diagramas de Venn para ilustrar las leyes de la tabla 1-1, como en el problema 1.17.)

Dualidad

Las identidades en la tabla 1-1 están dispuestas por pares, por ejemplo (2a) y (2b). A continuación se abordará el principio que está detrás de esta disposición. Suponga que E es una ecuación de álgebra de conjuntos. El dual E^* de E es la ecuación que se obtiene al sustituir cada aparición de $\cup$, $\cap$, $\mathbf{U}$ y $\varnothing$ en E por $\cap$, $\cup$, $\varnothing$ y $\mathbf{U}$, respectivamente. Por ejemplo, el dual de

$$(\mathbf{U} \cap A) \cup (B \cap A) = A \quad \text{es} \quad (\varnothing \cup A) \cap (B \cup A) = A$$

Observe que los pares de leyes en la tabla 1-1 son duales entre sí. Se trata de un hecho del álgebra de conjuntos que se denomina *principio de dualidad*: si cualquier ecuación E es una identidad, entonces su dual E^* también es una identidad.

1.6 CONJUNTOS FINITOS Y PRINCIPIO DE CONTEO

Los conjuntos son finitos o infinitos. Se dice que un conjunto S es *finito* si S es vacío o contiene exactamente m elementos, donde m es un entero positivo; en caso contrario, S es *infinito*.

EJEMPLO 1.7

a) El conjunto A de las letras del alfabeto español y el conjunto D de los días de la semana son conjuntos finitos. En específico, A tiene 29 elementos y D tiene 7 elementos.

b) Sea E el conjunto de enteros positivos pares, y sea I el *intervalo unitario*; es decir,

$$E = \{2, 4, 6, \ldots\} \quad \text{e} \quad \mathbf{I} = [0, 1] = \{x \mid 0 \leq x \leq 1\}$$

Así, tanto E como $\mathbf{I}$ son infinitos.

Un conjunto $\boldsymbol{S}$ es *numerable* si $\boldsymbol{S}$ es finito o si es posible disponer los elementos de $\boldsymbol{S}$ como una sucesión, en cuyo caso se dice que $\boldsymbol{S}$ es *infinito numerable*; en caso contrario, se dice que $\boldsymbol{S}$ es *no numerable*. El conjunto E anterior de enteros positivos pares es infinito numerable, mientras es posible demostrar que el intervalo unitario $\mathbf{I} = [0, 1]$ es no numerable.

Conteo de elementos en conjuntos finitos

La notación $n(S)$ o $|S|$ denota el número de elementos en un conjunto S. (En algunos textos se usa $\#(S)$ o $\text{card}(S)$ en lugar de $n(S)$.) Así, $n(A) = 26$, donde A es el conjunto de letras del alfabeto español, y $n(D) = 7$, donde D es el conjunto de días de la semana. También, $n(\varnothing) = 0$, ya que el conjunto vacío no tiene elementos.

El siguiente lema es válido.

Lema 1.6: Suponga que A y B son conjuntos finitos ajenos. Entonces $A \cup B$ es finito y

$$n(A \cup B) = n(A) + n(B)$$

Este lema se replantea como:

Lema 1.6: Suponga que S es la unión disjunta de los conjuntos finitos A y B. Entonces S es finito y

$$n(S) = n(A) + n(B)$$

Demostración. Al contar los elementos de $A \cup B$, primero se cuentan los que están en A. De éstos hay $n(A)$. Los únicos elementos por contar de $A \cup B$ son los que están en B pero no en A. Pero como A y B son ajenos, ningún elemento de B está en A, de modo que hay $n(B)$ elementos que están en B pero no en A. En consecuencia, $n(A \cup B) = n(A) + n(B)$.

Para dos conjuntos arbitrarios A y B, el conjunto A es la unión disjunta de $A \backslash B$ y $A \cap B$. Así, el lema 1.6 proporciona el siguiente resultado útil.

Corolario 1.7: Sean A y B conjuntos finitos. Entonces

$$n(A \backslash B) = n(A) - n(A \cap B)$$

Por ejemplo, suponga que en un curso de arte A hay 25 estudiantes, de los cuales 10 llevan un curso B de biología. Entonces el número de estudiantes en el curso A que no están en el curso B es:

$$n(A \backslash B) = n(A) - n(A \cap B) = 25 - 10 = 15$$

Dado cualquier conjunto A, recuerde que el conjunto universo $\mathbf{U}$ es la unión disjunta de A y A^{C}. En consecuencia, el lema 1.6 también proporciona el siguiente resultado.

Corolario 1.8: Sea A un subconjunto de un conjunto universo $\mathbf{U}$. Entonces

$$n(A^{\mathrm{C}}) = n(\mathbf{U}) - n(A)$$

Por ejemplo, suponga que en un curso $\mathbf{U}$ con 30 estudiantes hay 18 estudiantes de tiempo completo. Entonces en el curso $\mathbf{U}$ hay $30 - 18 = 12$ estudiantes de tiempo parcial.

Principio de inclusión-exclusión

Hay una fórmula para $n(A \cup B)$ aun cuando A y B no son disjuntos, la cual se denomina principio de inclusión-exclusión. A saber:

Teorema (principio de inclusión-exclusión) 1.9: Suponga que A y B son conjuntos finitos. Entonces $A \cup B$ y $A \cap B$ son finitos y

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Es decir, el número de elementos en A o en B (o en ambos) se encuentra, primero, al sumar $n(A)$ y $n(B)$ (inclusión) y luego al restar $n(A \cap B)$ (exclusión), ya que sus elementos se contaron dos veces.

Este resultado se aplica con el fin de obtener una fórmula semejante para tres conjuntos:

Corolario 1.10: Suponga que A, B y C son conjuntos finitos. Entonces $A \cup B \cup C$ es finito y

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Para generalizar aún más este resultado a cualquier número de conjuntos finitos se aplica la inducción matemática (sección 1.8).

EJEMPLO 1.8 Suponga que una lista A contiene los 30 estudiantes de un curso de matemáticas, y otra lista B contiene los 35 estudiantes de un curso de inglés, y que en ambas listas hay 20 nombres. Encuentre el número de estudiantes *a*) sólo en la lista A (*es decir sólo toman clase de matemáticas*), *b*) sólo en la lista B (*es decir, sólo toman clase de inglés*), *c*) en la lista A o en la lista B (o en ambas), *d*) exactamente en una lista (es decir, sólo estudian matemáticas o sólo estudian inglés).

a) La lista A contiene 30 nombres, 20 de ellos están en la lista B; así, $30 - 20 = 10$ nombres están sólo en la lista A.

b) De manera semejante, $35 - 20 = 15$ nombres están sólo en la lista B.

c) Se busca $n(A \cup B)$. Por el principio de inclusión-exclusión,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) = 30 + 35 - 20 = 45.$$

En otras palabras, se combinan las dos listas y luego se eliminan los 20 nombres que aparecen dos veces.

d) Por los incisos *a*) y *b*), $10 + 15 = 25$ nombres están sólo en una lista; es decir, $n(A \oplus B) = 25$.

1.7 CLASES DE CONJUNTOS, CONJUNTOS POTENCIA Y PARTICIONES

Dado un conjunto S, quizá considere conveniente decir algo sobre algunos de sus subconjuntos. Entonces S sería un *conjunto de conjuntos*. Sin embargo, siempre que ocurra una situación así y para evitar confusión, se hablará de una *clase* de conjuntos o una *colección* de conjuntos, en lugar de un *conjunto* de conjuntos. Si se quiere considerar algunos de los conjuntos en una clase de conjuntos dada, entonces se habla de una *subclase* o *subcolección*.

EJEMPLO 1.9 Suponga que $S = \{1, 2, 3, 4\}$.

a) Sea A la clase de subconjuntos de S que contiene exactamente tres elementos de S. Entonces

$$A = [\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}]$$

Es decir, los elementos de A son los conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$ y $\{2, 3, 4\}$.

b) Sea B la clase de subconjuntos de S, donde cada uno contiene al 2 y a otros dos elementos de S. Entonces

$$B = [\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}]$$

Los elementos de B son los conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$ y $\{2, 3, 4\}$. Así, B es una subclase de A, ya que cada elemento de B también es un elemento de A. (Para evitar confusiones, algunas veces los conjuntos de una clase se escriben entre corchetes, en lugar de hacerlo entre llaves.)

Conjuntos potencia

Para un conjunto S dado, es posible hablar de la clase de todos los subconjuntos de S. Esta clase se denomina *conjunto potencia* de S y se denota $P(S)$. Si S es finito, entonces también $P(S)$ lo es. De hecho, el número de elementos en $P(S)$ es igual a 2 elevado a la potencia $n(S)$. Es decir,

$$n(P(S)) = 2^{n(S)}$$

(Debido a lo anterior, el conjunto potencia de S algunas veces se denota por 2^S.)

EJEMPLO 1.10 Suponga que $S = \{1, 2, 3\}$. Entonces

$$P(S) = [\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S]$$

Observe que el conjunto vacío $\varnothing$ pertenece a $P(S)$, ya que $\varnothing$ es un subconjunto de S. En forma semejante, S pertenece a $P(S)$. Como era de esperar, con base en la observación anterior, $P(S)$ tiene $2^3 = 8$ elementos.

Particiones

Sea S un conjunto no vacío. Una *partición* de S es una subdivisión de S en subconjuntos no vacíos que no se traslapan. Con más precisión, una *partición* de S es una colección $\{A_i\}$ de subconjuntos no vacíos de S tal que:

i) Cada a en S pertenece a uno de los A_i.
ii) Los conjuntos $\{A_i\}$ son mutuamente ajenos; es decir, si

$$A_j \neq A_k \quad \text{entonces} \quad A_j \cap A_k = \varnothing$$

En una partición los subconjuntos se denominan *celdas*. La figura 1-6 es un diagrama de Venn de una partición del conjunto rectangular S en cinco celdas, A_1, A_2, A_3, A_4, A_5.

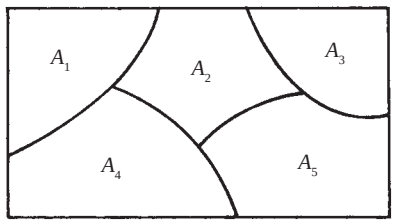


Figura 1-6

EJEMPLO 1.11 Considere las siguientes colecciones de subconjuntos de $S = \{1, 2, \ldots, 8, 9\}$:

i) [{1, 3, 5}, {2, 6}, {4, 8, 9}]
ii) [{1, 3, 5}, {2, 4, 6, 8}, {5, 7, 9}]
iii) [{1, 3, 5}, {2, 4, 6, 8}, {7, 9}]

Entonces *i*) no es una partición de *S* puesto que 7 está en *S* y no pertenece a ninguno de los subconjuntos. Además, *ii*) no es una partición de *S* puesto que {1, 3, 5} y {5, 7, 9} no son ajenos. Por otra parte, *iii*) es una partición de *S*.

Operaciones generalizadas con conjuntos

Las operaciones de unión e intersección de conjuntos ya se definieron para dos conjuntos. Estas operaciones se extienden a cualquier número de conjuntos, finitos o infinitos, como sigue.

Primero considere un número finito de conjuntos; por ejemplo, $A_1, A_2, \ldots, A_m$. La unión y la intersección de estos conjuntos se denotan y definen, respectivamente, por

$$A_1 \cup A_2 \cup \ldots \cup A_m = \bigcup_{i=1}^{m} A_i = \{x \mid x \in A_i \text{ para algún } A_i\}$$
$$A_1 \cap A_2 \cap \ldots \cap A_m = \bigcap_{i=1}^{m} A_i = \{x \mid x \in A_i \text{ para todo } A_i\}$$

Es decir, la unión consta de los elementos que pertenecen, por lo menos, a uno de los conjuntos, y la intersección consta de los elementos que pertenecen a todos los conjuntos.

Ahora, sea $\mathscr{A}$ cualquier colección de conjuntos. La unión y la intersección de los conjuntos en la colección A se denotan y definen, respectivamente, por

$$\bigcup (A \mid A \in \mathscr{A}) = \{x \mid x \in A_i \text{ para algún } A_i \in \mathscr{A}\}$$
$$\bigcap (A \mid A \in \mathscr{A}) = \{x \mid x \in A_i \text{ para todo } A_i \in \mathscr{A}\}$$

Es decir, la unión consta de los elementos que pertenecen por lo menos a uno de los conjuntos en la colección $\mathscr{A}$, y la intersección consta de los elementos que pertenecen a cada uno de los conjuntos en la colección $\mathscr{A}$.

EJEMPLO 1.12 Considere los conjuntos

$$A_1 = \{1, 2, 3, \ldots\} = \mathbf{N}, \quad A_2 = \{2, 3, 4, \ldots\}, \quad A_3 = \{3, 4, 5, \ldots\}, \quad A_n = \{n, n+1, n+2, \ldots\}.$$

Entonces la unión y la intersección de los conjuntos son:

$$\bigcup (A_k \mid k \in \mathbf{N}) = \mathbf{N} \quad \text{y} \quad \bigcap (A_k \mid k \in \mathbf{N}) = \varnothing$$

Las leyes de De Morgan también se cumplen para las operaciones generalizadas con los conjuntos anteriores. Es decir:

Teorema 1.11: Sea $\mathscr{A}$ una colección de conjuntos. Entonces:

i) $\left[\bigcup (A \mid A \in \mathscr{A})\right]^{\mathrm{C}} = \bigcap (A^{\mathrm{C}} \mid A \in \mathscr{A})$
ii) $\left[\bigcap (A \mid A \in \mathscr{A})\right]^{\mathrm{C}} = \bigcup (A^{\mathrm{C}} \mid A \in \mathscr{A})$

1.8 INDUCCIÓN MATEMÁTICA

A continuación se presenta una propiedad esencial del conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de enteros positivos:

Principio de inducción matemática I: Sea P una proposición definida acerca de los enteros positivos $\mathbf{N}$; es decir, $P(n)$ es verdadera o falsa para cualquier $n \in \mathbf{N}$. Suponga que P tiene las dos propiedades siguientes:

i) $P(1)$ es verdadera.
ii) $P(k + 1)$ es verdadera siempre que $P(k)$ es verdadera.

Entonces P es verdadera para todo entero positivo $n \in \mathbf{N}$.

Aquí no se demostrará este principio. De hecho, este principio suele aparecer como uno de los axiomas cuando $\mathbf{N}$ se desarrolla a partir de axiomas.

EJEMPLO 1.13 Sea P la proposición de que la suma de los n primeros números impares es igual a n^2; es decir,

$$P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(El k-ésimo número impar es $2k - 1$, y el siguiente número impar es $2k + 1$.) Observe que $P(n)$ es verdadera para $n = 1$; a saber,

$$P(1) = 1^2$$

Si se considera que $P(k)$ es verdadera, y se suma $2k + 1$ a ambos miembros de $P(k)$, se obtiene

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) - k^2 + (2k + 1) = (k + 1)^2$$

que es $P(k + 1)$. En otras palabras, $P(k + 1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción matemática, P es verdadera para todo n.

Hay una forma del principio de inducción matemática que es más conveniente utilizar algunas veces. Aunque parece diferente, en realidad es equivalente al principio de inducción anterior.

Principio de inducción matemática II: Sea P una proposición definida sobre los enteros positivos $\mathbf{N}$ tal que:

i) $P(1)$ es verdadera.
ii) $P(k)$ es verdadera siempre que $P(j)$ sea verdadera para todo $1 \leq j < k$.

Entonces P es verdadera para todo entero positivo $n \in \mathbf{N}$.

Observación: Algunas veces es necesario demostrar que una proposición P es verdadera para el conjunto de enteros

$$\{a, a + 1, a + 2, a + 3, \ldots\}$$

donde a es cualquier entero, incluso cero. En este caso se reemplaza 1 por a en cualquiera de los principios de inducción matemática anteriores.

PROBLEMAS RESUELTOS

CONJUNTOS Y SUBCONJUNTOS

1.1 ¿Cuáles de los siguientes conjuntos son iguales $\{x, y, z\}$, $\{z, y, z, x\}$, $\{y, x, y, z\}$, $\{y, z, x, y\}$?

Todos son iguales. El orden y la repetición de los elementos no modifican un conjunto.

1.2 Enumere los elementos de cada conjunto donde $\mathbf{N} = \{1, 2, 3, \ldots\}$.

a) $A = \{x \in \mathbf{N} \mid 3 < x < 9\}$

b) $B = \{x \in \mathbf{N} \mid x \text{ es par}, x < 11\}$

c) $C = \{x \in \mathbf{N} \mid 4 + x = 3\}$

a) A consta de los enteros positivos entre 3 y 9; por tanto, $A = \{4, 5, 6, 7, 8\}$.

b) B consta de los enteros positivos pares menores que 11; por tanto, $B = \{2, 4, 6, 8, 10\}$.

c) Ningún entero positivo satisface $4 + x = 3$; por tanto, $C = \varnothing$, el conjunto vacío.

1.3 Sea $A = \{2, 3, 4, 5\}$

a) Demuestre que A no es un subconjunto de $B = \{x \in \mathbf{N} \mid x \text{ es par}\}$.

b) Demuestre que A es un subconjunto propio de $C = \{1, 2, 3, \ldots, 8, 9\}$.

a) Es necesario demostrar que por lo menos un elemento en A no pertenece a B. Luego, $3 \in A$ y, puesto que B consta de los números pares, $3 \notin A$; por tanto, A no es un subconjunto de B.

b) Cada elemento de A pertenece a C, por lo que $A \subseteq C$. Por otra parte, $1 \in C$ pero $1 \notin A$. Así, $A \neq C$. En consecuencia, A es un subconjunto propio de C.

OPERACIONES CON CONJUNTOS

1.4 Sea $\mathbf{U} = \{1, 2, \ldots, 9\}$ el conjunto universo, y sea

$$A = \{1, 2, 3, 4, 5\}, \quad C = \{5, 6, 7, 8, 9\}, \quad E = \{2, 4, 6, 8\},$$
$$B = \{4, 5, 6, 7\}, \quad D = \{1, 3, 5, 7, 9\}, \quad F = \{1, 5, 9\}.$$

Encuentre: *a*) $A \cup B$ y $A \cap B$; *b*) $A \cup C$ y $A \cap C$; *c*) $D \cup F$ y $D \cap F$.

Recuerde que la unión $X \cup Y$ consta de los elementos que están en X o en Y (o en ambos), y que la intersección $X \cap Y$ consta de los elementos que están tanto en X como en Y.

a) $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ y $A \cap B = \{4, 5\}$

b) $A \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = \mathbf{U}$ y $A \cap C = \{5\}$

c) $D \cup F = \{1, 3, 5, 7, 9\} = D$ y $D \cap F = \{1, 5, 9\} = F$

Observe que $F \subseteq D$, de modo que por el teorema 1.4 debe tenerse $D \cup F = D$ y $D \cap F = F$.

1.5 Considere los conjuntos en el problema 1.4. Encuentre:

a) $A^{\mathrm{C}}, B^{\mathrm{C}}, D^{\mathrm{C}}, E^{\mathrm{C}}$; *b*) $A \backslash B, B \backslash A, D \backslash E$; *c*) $A \oplus B, C \oplus D, E \oplus F$.

Recuerde que:

1) Los complementos X^{C} constan de los elementos en $\mathbf{U}$ que no pertenecen a X.
2) La diferencia $X \backslash Y$ consta de los elementos en X que no pertenecen a Y.
3) La diferencia simétrica $X \oplus Y$ consta de los elementos que están en X o en Y pero no en ambos.

En consecuencia:

a) $A^{\mathrm{C}} = \{6, 7, 8, 9\}$; $B^{\mathrm{C}} = \{1, 2, 3, 8, 9\}$; $D^{\mathrm{C}} = \{2, 4, 6, 8\} = E$; $E^{\mathrm{C}} = \{1, 3, 5, 7, 9\} = D$.

b) $A \backslash B = \{1, 2, 3\}$; $B \backslash A = \{6, 7\}$; $D \backslash E = \{1, 3, 5, 7, 9\} = D$; $F \backslash D = \varnothing$.

c) $A \oplus B = \{1, 2, 3, 6, 7\}$; $C \oplus D = \{1, 3, 6, 8\}$; $E \oplus F = \{2, 4, 6, 8, 1, 5, 9\} = E \cup F$.

1.6 Demuestre que puede cumplirse: *a*) $A \cap B = A \cap C$ sin que $B = C$; *b*) $A \cup B = A \cup C$ sin que $B = C$.

a) Sea $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{2, 4\}$. Entonces $A \cap B = \{2\}$ y $A \cap C = \{2\}$; pero $B \neq C$.

b) Sea $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{2, 3\}$. Entonces $A \cup B = \{1, 2, 3\}$ y $A \cup C = \{1, 2, 3\}$; pero $B \neq C$.

1.7 Demuestre: $B \backslash A = B \cap A^{\mathrm{C}}$. Así, la operación de la diferencia en conjuntos se escribe en términos de las operaciones de intersección y complemento.

$$B \backslash A = \{x \mid x \in B,\ x \notin A\} = \{x \mid x \in B,\ x \in A^{\mathrm{C}}\} = B \cap A^{\mathrm{C}}.$$

1.8 Demuestre el teorema 1.4. Las siguientes expresiones son equivalentes: $A \subseteq B, A \cap B = A, A \cup B = B$.

Suponga que $A \subseteq B$ y sea $x \in A$. Entonces $x \in B$, por tanto $x \in A \cap B$ y $A \subseteq A \cap B$. Por el teorema 1.3, $(A \cap B) \subseteq A$; en consecuencia, $A \cap B = A$. Por otra parte, suponga $A \cap B = A$ y sea $x \in A$. Entonces $x \in (A \cap B)$, por tanto, $x \in A$ y $x \in B$. En consecuencia, $A \subseteq B$. Ambos resultados muestran que $A \subseteq B$ es equivalente a $A \cap B = A$.

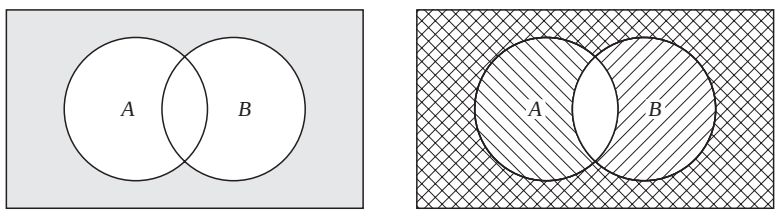
Suponga de nuevo que $A \subseteq B$. Sea $x \in (A \cup B)$. Entonces $x \in A$ o $x \in B$. Si $x \in A$, entonces $x \in B$, porque $A \subseteq B$. En cualquier caso, $x \in B$. Por consiguiente, $A \cup B \subseteq B$. Por el teorema 1.3, $B \subseteq A \cup B$. En consecuencia, $A \cup B = B$. Ahora suponga que $A \cup B = B$ y que $x \in A$. Entonces $x \in A \cup B$ por la definición de unión de conjuntos. Así, $x \in B = A \cup B$. Por consiguiente, $A \subseteq B$. Ambos resultados muestran que $A \subseteq B$ es equivalente a $A \cup B = B$.

Por tanto, $A \subseteq B$, $A \cup B = A$ y $A \cup B = B$ son equivalentes.

DIAGRAMAS DE VENN, ÁLGEBRA DE CONJUNTOS Y DUALIDAD

1.9 Ilustre la ley de De Morgan $(A \cup B)^C = A^C \cap B^C$ mediante diagramas de Venn.

En un diagrama de Venn de los conjuntos A a B se sombrea la región fuera de $A \cup B$. Esto se muestra en la figura 1-7*a*); por tanto, la región sombreada representa $(A \cup B)^C$. Luego, en un diagrama de Venn de A y B se sombrea la región fuera de A con líneas diagonales en un sentido (////) y luego se sombrea la región fuera de B con líneas diagonales en otro sentido (\\\\). Esto se muestra en la figura 1-7*b*); por tanto, la región sombreada como cuadrícula (región donde están presentes ambos tipos de líneas diagonales) representa $A^C \cap B^C$. Tanto $(A \cup B)^C$ como $A^C \cap B^C$ están representadas por la misma región; así, el diagrama de Venn indica $(A \cup B)^C = A^C \cap B^C$. (Cabe señalar que un diagrama de Venn no constituye una demostración formal, aunque indica relaciones entre conjuntos.)



a) *b*)

Figura 1-7

1.10 Demuestre la ley distributiva: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$\begin{aligned} A \cap (B \cup C) &= \{x \mid x \in A, x \in (B \cup C)\} \\ &= \{x \mid x \in A, x \in B \text{ o } x \in A, x \in C\} = (A \cap B) \cup (A \cap C) \end{aligned}$$

Aquí se usa la ley lógica análoga $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ donde $\wedge$ denota "y" y $\vee$ denota "o".

1.11 Escriba el dual de: *a*) $(\mathbf{U} \cap A) \cup (B \cap A) = A$; *b*) $(A \cap \mathbf{U}) \cap (\varnothing \cup A^C) = \varnothing$.

En cada ecuación de conjuntos se intercambian $\cup$ y $\cap$, así como $\mathbf{U}$ y $\varnothing$:

a) $(\varnothing \cup A) \cap (B \cup A) = A$; *b*) $(A \cup \varnothing) \cup (\mathbf{U} \cap A^C) = \mathbf{U}$.

1.12 Demuestre: $(A \cup B) \backslash (A \cap B) = (A \backslash B) \cup (B \backslash A)$. (Así, cualquiera puede usarse para definir $B \oplus A$.)

Al usar $X \backslash Y) = X \cap Y^C$ y las leyes en la tabla 1.1, junto con la ley de De Morgan, se obtiene

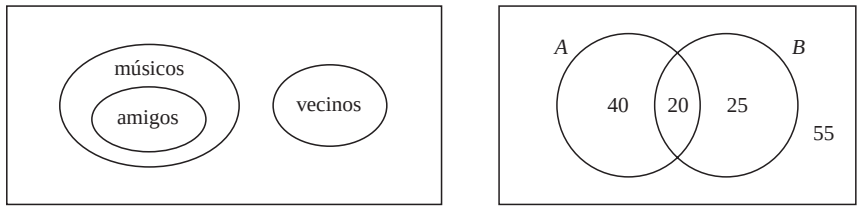
$$\begin{aligned} (A \cup B) \backslash (A \cap B) &= (A \cup B) \cap (A \cap B)^C = (A \cup B) \cap) A^C \cup B^C) \\ &= (A \cup A^C) \cup (A \cap B^C) \cup (B \cap A^C) \cup (B \cap B^C) \\ &= \varnothing \cup (A \cap B^C) \cup (B \cap A^C) \cup \varnothing \\ &= (A \cap B^C) \cup (B \cap A^C) = (A \backslash B) \cup (B \backslash A) \end{aligned}$$

1.13 Determine la validez del siguiente argumento:

S_1: Todos mis amigos son músicos.
S_2: Juan es mi amigo.
S_3: Ninguno de mis vecinos es músico.

S : Juan no es mi vecino.

Las premisas S_1 y S_3 conducen al diagrama de Venn en la figura 1-8*a*). Por S_2 Juan pertenece al conjunto de amigos que es ajeno del conjunto de vecinos. Por tanto, *S* es una conclusión válida y así el argumento es válido.



a) *b*)

Figura 1-8

CONJUNTOS FINITOS Y PRINCIPIO DEL CONTEO

1.14 En una universidad cada estudiante de humanidades debe acreditar un curso *A* de matemáticas y un curso *B* de ciencias. En una muestra de 140 estudiantes de segundo año se observó lo siguiente:

60 acreditaron *A*, 45 acreditaron *B*, 20 acreditaron tanto *A* como *B*.

Use un diagrama de Venn para determinar el número de estudiantes que acreditaron:

a) Por lo menos uno de *A* y *B*; *b*) exactamente uno de *A* o *B*; *c*) ni *A* ni *B*.

Al escribir los datos anteriores en notación de conjuntos se obtiene:

$$n(A) = 60,\ n(B) = 45,\ n(A \cap B) = 20,\ n(\mathbf{U}) = 140$$

Se dibuja un diagrama de Venn de los conjuntos *A* y *B* como en la figura 1-1*c*). Luego, como en la figura 1-8*b*), se asignan números a las cuatro regiones:

20 acreditaron tanto *A* como *B*, de modo que $n(A \cap B) = 20$.

$60 - 20 = 40$ acreditaron *A* pero no *B*, por lo que $n(A \backslash B) = 40$.

$45 - 20 = 25$ acreditaron *B* pero no *A*, por lo que $n(B \backslash A) = 25$.

$140 - 20 - 40 - 25 = 55$ no acreditaron *A* ni *B*.

Por el diagrama de Venn:

a) $20 + 40 + 25 = 85$ acreditaron *A* o *B*.Ahora, por el principio de inclusión-exclusión:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B) = 60 + 45 - 20 = 85$$

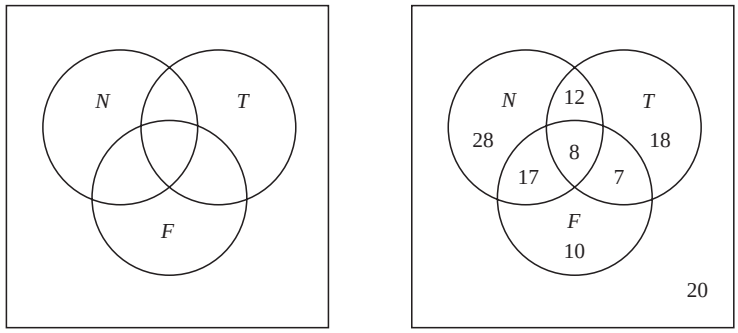
b) $40 + 25 = 65$ acreditaron exactamente uno de los cursos. Es decir, $n(A \oplus B) = 65$.

c) 55 no acreditaron ninguno de los cursos; es decir, $n(A^C \cap B^C) = n[(A \cup B)^C] = 140 - 85 = 55$.

1.15 En una encuesta aplicada a 120 personas se encontró que:

65 leen *Newsweek*, 20 leen tanto *Newsweek* como *Time*,
45 leen *Time*, 25 leen tanto *Newsweek* como *Fortune*,
42 leen *Fortune*, 15 leen tanto *Time* como *Fortune*.
8 leen las tres publicaciones.

a) Encuentre el número de personas que leen por lo menos una de las tres publicaciones.
b) En cada una de las ocho regiones del diagrama de Venn de la figura 1-9*a*) se escribe el número correcto de personas, donde *N*, *T* y *F* denotan el conjunto de personas que leen *Newsweek*, *Time* y *Fortune*, respectivamente.
c) Encuentre el número de personas que leen exactamente una publicación.



a) *b*)

Figura 1-9

a) Se quiere encontrar $n(N \cup T \cup F)$. Por el corolario 1.10 (principio de inclusión-exclusión),

$$\begin{aligned} n(N \cup T \cup F) &= n(N) + n(T) + n(F) - n(N \cap T) - n(N \cap F) - n(T \cap F) + n(N \cap T \cap F) \\ &= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100 \end{aligned}$$

b) El diagrama de Venn de la figura 1-9*b*) se obtiene como sigue:

8 leen las tres publicaciones,

$20 - 8 = 12$ leen *Newsweek* y *Time* pero no las tres publicaciones,

$25 - 8 = 17$ leen *Newsweek* y *Fortune* pero no las tres publicaciones,

$15 - 8 = 7$ leen *Time* y *Fortune* pero no las tres publicaciones,

$65 - 12 - 8 - 17 = 28$ sólo leen *Newsweek*,

$45 - 12 - 8 - 7 = 18$ sólo leen *Time*,

$42 - 17 - 8 - 7 = 10$ sólo leen *Fortune*,

$120 - 100 = 20$ no leen ninguna publicación.

c) $28 + 18 + 10 = 56$ leen exactamente una publicación.

1.16 Demuestre el teorema 1.9. Suponemos que A y B son conjuntos finitos. Entonces $A \cup B$ y $A \cap B$ son finitos y

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Si A y B son finitos, entonces resulta evidente que $A \cup B$ y $A \cap B$ son finitos.

Suponemos que primero se cuentan los elementos en A y después los elementos en B.

Entonces cualquier elemento en $A \cap B$ se contaría dos veces, una en A y otra en B. Así,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

CLASES DE CONJUNTOS

1.17 Sea $A = [\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8\}]$. *a*) Enumere los elementos de A; *b*) encuentre $n(A)$.

a) A tiene tres elementos; los conjuntos $\{1, 2, 3\}$, $\{4, 5\}$ y $\{6, 7, 8\}$.

b) $n(A) = 3$.

1.18 Determine el conjunto potencia $P(A)$ de $A = \{a, b, c, d\}$.

Los elementos de $P(A)$ son los subconjuntos de A. Así,

$$P(A) = [A, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a\}, \{b\}, \{c\}, \{d\}, \emptyset]$$

Como era de esperar, $P(A)$ tiene $2^4 = 16$ elementos.

1.19 Sea $S = \{a, b, c, d, e, f, g\}$. Determine cuáles de las siguientes particiones son de S:

a) $P_1 = [\{a, c, e\}, \{b\}, \{d, g\}]$, *c*) $P_3 = [\{a, b, e, g\}, \{c\}, \{d, f\}]$,

b) $P_2 = [\{a, e, g\}, \{c, d\}, \{b, e, f\}]$, *d*) $P_4 = [\{a, b, c, d, e, f, g\}]$.

a) P_1 no es una partición de S, puesto que $f \in S$ no pertenece a ninguna de las celdas.

b) P_2 no es una partición de S, puesto que $e \in S$ pertenece a dos de las celdas.

c) P_3 es una partición de S, puesto que cada elemento en S pertenece exactamente a una celda.

d) P_4 es una partición de S en una celda, S mismo.

1.20 Encuentre todas las particiones de $S = \{a, b, c, d\}$.

Primero observe que cada partición de S contiene 1, 2, 3 o 4 celdas distintas. Las particiones son como sigue:

1) $[\{a, b, c, d\}]$

2) $[\{a\}, \{b, c, d\}], [\{b\}, \{a, c, d\}], [\{c\}, \{a, b, d\}], [\{d\}, \{a, b, c\}],$
$[\{a, b\}, \{c, d\}], [\{a, c\}, \{b, d\}], [\{a, d\}, \{b, c\}]$

3) $[\{a\}, \{b\}, \{c, d\}], [\{a\}, \{c\}, \{b, d\}], [\{a\}, \{d\}, \{b, c\}],$
$[\{b\}, \{c\}, \{a, d\}], [\{b\}, \{d\}, \{a, c\}], [\{c\}, \{d\}, \{a, b\}]$

4) $[\{a\}, \{b\}, \{c\}, \{d\}]$

Hay 15 particiones distintas de S.

1.21 Sea $\mathbf{N} = \{1, 2, 3, \ldots\}$ y, para cada $n \in \mathbf{N}$. Sea $A_n = \{n, 2n, 3n, \ldots\}$. Encuentre:

a) $A_3 \cap A_5$; *b*) $A_4 \cap A_5$; *c*) $\bigcup_{i \in Q} A_i$ donde $Q = \{2, 3, 5, 7, 11, \ldots,\}$ es el conjunto de números primos.

a) Los números que son múltiplos tanto de 3 como de 5 son múltiplos de 15; por tanto, $A_3 \cap A_5 = A_{15}$.

b) Los elementos comunes a A_4 y A_6 son los múltiplos de 12; por tanto, $A_4 \cap A_6 = A_{12}$.

c) Todo entero positivo excepto 1 es múltiplo de por lo menos un número primo; por tanto,

$$\bigcup_{i \in Q} A_i = \{2, 3, 4, \ldots\} = \mathbf{N} \backslash \{1\}$$

1.22 Sea $\{A_i \mid i \in I\}$ una clase indexada de conjuntos y sea $i_0 \in I$. Demuestre

$$\bigcap_{i \in I} A_i \subseteq A_{i_0} \subseteq \bigcup_{i \in I} A_i .$$

Sea $x \in \bigcap_{i \in I} A_i$, entonces $x \in A_i$ para todo $i \in I$. En particular, $x \in A_{i_0}$. Por tanto, $\bigcap_{i \in l} A_i \subseteq A_{i_0}$. Ahora sea $y \in A_{i_0}$. Puesto que $i_0 \in I$, $y \in \bigcap_{i \in l} A_i$. Entonces $A_{i_0} \subseteq \bigcup_{i \in l} A_i$.

1.23 Demuestre (ley de De Morgan): Para cualquier clase indexada $\{A_i \mid i \in I\}$, se tiene $\left(\bigcup_i A_i\right)^{\mathrm{C}} = \bigcap_i A_i^{\mathrm{C}}$.

Al usar las definiciones de unión e intersección de clases indexadas de conjuntos:

$$\begin{aligned}\left(\bigcup_i A_i\right)^{\mathrm{C}} &= \{x \mid x \notin \bigcup_i A_i\} = \{x \mid x \notin A_i \text{ para toda } i\} \\ &= \{x \mid x \in A_i^{\mathrm{C}} \text{ para toda } i\} = \bigcap_i A_i^{\mathrm{C}}\end{aligned}$$

INDUCCIÓN MATEMÁTICA

1.24 Demuestre la proposición $P(n)$ de que la suma de los primeros n enteros positivos es igual a $\frac{1}{2}n(n+1)$, es decir

$$P(n) = 1 + 2 + 3 + \cdots + n = \tfrac{1}{2}n(n+1)$$

La proposición se cumple para $n = 1$, ya que:

$$P(1) : 1 = \tfrac{1}{2}(1)(1+1)$$

Si se acepta que $P(k)$ es verdadera, y se suma $k+1$ a ambos miembros de $P(k)$ se obtiene

$$\begin{aligned}1 + 2 + 3 + \cdots + k + (k+1) &= \tfrac{1}{2}k(k+1) + (k+1) \\ &= \tfrac{1}{2}[k(k+1) + 2(k+1)] \\ &= \tfrac{1}{2}[(k+1)(k+2)]\end{aligned}$$

que es $P(k+1)$. Es decir, $P(k+1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción, $P(n)$ es verdadera para toda n.

1.25 Demuestre la siguiente proposición (para $n \geq 0$):

$$P(n) : 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

$P(0)$ es verdadera porque $1 = 2^1 - 1$. Si se acepta que $P(k)$ es verdadera, y se suma 2^{k+1} a ambos miembros de $P(k)$ se obtiene

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2(2^{k+1}) - 1 = 2^{k+2} - 1$$

que es $P(k+1)$. Es decir, $P(k+1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción, $P(n)$ es verdadera para toda n.

PROBLEMAS SUPLEMENTARIOS

CONJUNTOS Y SUBCONJUNTOS

1.26 ¿Cuáles de los siguientes conjuntos son iguales?

$$\begin{array}{llll} A = \{x \mid x^2 - 4x + 3 = 0\}, & C = \{x \mid x \in \mathbf{N}, x < 3\}, & E = \{1, 2\}, & G = \{3, 1\}, \\ B = \{x \mid x^2 - 3x + 2 = 0\}, & D = \{x \mid x \in \mathbf{N}, x \text{ es impar}, x < 5\}, & F = \{1, 2, 1\}, & H = \{1, 1, 3\}. \end{array}$$

1.27 Enumere los elementos de los siguientes conjuntos si el conjunto universo es $\mathbf{U} = \{a, b, c, \ldots, y, z\}$
Además, identifique cuáles de los conjuntos, en caso de haber algunos, son iguales.

$A = \{x \mid x \text{ es una vocal}\}$, $C = \{x \mid x \text{ precede a } f \text{ en el alfabeto}\}$,
$B = \{x \mid x \text{ es una letra de la palabra "little"}\}$, $D = \{x \mid x \text{ es una letra de la palabra "title"}\}$.

1.28 Sea $A = \{1, 2, \ldots, 8, 9\}$, $B = \{2, 4, 6, 8\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{3, 4, 5\}$, $E = \{3, 5\}$.
¿Cuáles de esos conjuntos pueden ser iguales a X bajo cada una de las siguientes condiciones?

a) X y B son ajenos.
b) $X \subseteq D$ pero $X \not\subset B$.
c) $X \subseteq A$ pero $X \not\subset C$.
d) $X \subseteq C$ pero $X \not\subset A$.

OPERACIONES CON CONJUNTOS

1.29 Dados el conjunto universo $\mathbf{U} = \{1, 2, 3, \ldots, 8, 9\}$ y los conjuntos $A = \{1, 2, 5, 6\}$, $B = \{2, 5, 7\}$, $C = \{1, 3, 5, 7, 9\}$. Encuentre:

a) $A \cap B$ y $A \cap C$ *c*) A^{C} y C^{C} *e*) $A \oplus B$ y $A \oplus C$
b) $A \cup B$ y $B \cup C$ *d*) $A \backslash B$ y $A \backslash C$ *f*) $(A \cup C) \backslash B$ y $(B \oplus C) \backslash A$

1.30 Sean A y B conjuntos arbitrarios. Demuestre lo siguiente:

a) A es la unión disjunta de $A \backslash B$ y $A \cap B$.
b) $A \cup B$ es la unión disjunta de $A \backslash B$, $A \cap B$ y $B \backslash A$.

1.31 Demuestre lo siguiente:

a) $A \subseteq B$ si y sólo si $A \cap B^{\mathrm{C}} = \varnothing$ *c*) $A \subseteq B$ si y sólo si $B^{\mathrm{C}} \subseteq A^{\mathrm{C}}$
b) $A \subseteq B$ si y sólo si $A^{\mathrm{C}} \cup B = \mathbf{U}$ *d*) $A \subseteq B$ si y sólo si $A \backslash B = \varnothing$
(Compare los resultados con el teorema 1.4.)

1.32 Demuestre las leyes de absorción: *a*) $A \cup (A \cap B) = A$; *b*) $A \cap (A \cup B) = A$.

1.33 La fórmula $A \backslash B = A \cap B^{\mathrm{C}}$ define la operación diferencia en términos de las operaciones intersección y complemento. Encuentre una fórmula que defina la unión $A \cup B$ en términos de las operaciones intersección y complemento.

DIAGRAMAS DE VENN

1.34 En el diagrama de Venn de la figura 1-5*a*) se muestran los conjuntos A, B y C. Sombree los siguientes conjuntos:

a) $A \backslash (B \cup C)$; *b*) $A^{\mathrm{C}} \cap (B \cup C)$; *c*) $A^{\mathrm{C}} \cap (C \backslash B)$.

1.35 Use el diagrama de Venn de la figura 1-5*b*) para escribir cada conjunto como la unión (disjunta) de productos fundamentales:

a) $A \cap (B \cup C)$; *b*) $A^{\mathrm{C}} \cap (B \cup C)$; *c*) $A \cup (B \backslash C)$.

1.36 Considere las siguientes premisas:

S_1: Todos los diccionarios son útiles.
S_2: María sólo tiene novelas rosas.
S_3: Ninguna novela rosa es útil.

Use un diagrama de Venn para determinar la validez de cada una de las siguientes conclusiones:

a) Las novelas rosas no son diccionarios.
b) María no tiene ningún diccionario.
c) Todos los libros útiles son diccionarios.

ÁLGEBRA DE CONJUNTOS Y DUALIDAD

1.37 Escriba el dual de cada ecuación:

a) $A = (B^{\mathrm{C}} \cap A) \cup (A \cap B)$
b) $(A \cap B) \cup (A^{\mathrm{C}} \cap B) \cup (A \cap B^{\mathrm{C}}) \cup (A^{\mathrm{C}} \cap B^{\mathrm{C}}) = \mathbf{U}$

1.38 Use las leyes en la tabla 1-1 para demostrar cada identidad de conjuntos:

a) $(A \cap B) \cup (A \cap B^{\mathrm{C}}) = A$
b) $A \cup B = (A \cap B^{\mathrm{C}}) \cup (A^{\mathrm{C}} \cap B) \cup (A \cap B)$

CONJUNTOS FINITOS Y PRINCIPIO DEL CONTEO

1.39 Determine cuáles de los siguientes conjuntos son finitos:

a) Rectas paralelas al eje x. *c*) Enteros múltiplos de 5.

b) Letras del alfabeto español. *d*) Animales vivientes sobre la Tierra.

1.40 Use el teorema 1.9 para demostrar el corolario 1.10: Suponga que A, B y C son conjuntos finitos. Entonces $A \cup B \cup C$ es finito y

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

1.41 Se aplicó una encuesta acerca de 25 automóviles nuevos vendidos en una agencia para ver qué opciones de equipo: aire acondicionado (A), radio (R) y ventanillas eléctricas (W), ya estaban instaladas. Se encontró lo siguiente:

15 tenían aire acondicionado (A),	5 tenían A y P,	
12 tenían radio (R),	9 tenían A y R,	3 tenían las tres opciones.
11 tenían ventanillas eléctricas (W),	4 tenían R y W,	

Encuentre el número de automóviles que tenían: *a*) sólo W; *b*) sólo A; *c*) sólo R; *d*) R y W pero no A; *e*) A y R pero no W; *f*) sólo una de las opciones; *g*) por lo menos una opción; *h*) ninguna de las opciones.

CLASES DE CONJUNTOS

1.42 Encuentre el conjunto potencia $P(A)$ de $A = \{1, 2, 3, 4, 5\}$.

1.43 Dado $A = [\{a, b\}, \{c\}, \{d, e, f\}]$.

a) Enumere los elementos de A. *b*) Encuentre $n(A)$. *c*) Encuentre el conjunto potencia de A.

1.44 Suponga que A es finito y que $n(A) = m$. Demuestre que el conjunto potencia $P(A)$ tiene 2^m elementos.

PARTICIONES

1.45 Sea $S = \{1, 2, \ldots, 8, 9\}$. Determine si cada una de las siguientes expresiones es o no una partición de S:

a) $[\{1, 3, 6\}, \{2, 8\}, \{5, 7, 9\}]$ *c*) $[\{2, 4, 5, 8\}, \{1, 9\}, \{3, 6, 7\}]$

b) $[\{1, 5, 7\}, \{2, 4, 8, 9\}, \{3, 5, 6\}]$ *d*) $[\{1, 2, 7\}, \{3, 5\}, \{4, 6, 8, 9\}, \{3, 5\}]$

1.46 Sea $S = \{1, 2, 3, 4, 5, 6\}$. Determine si cada una de las siguientes expresiones es o no una partición de S:

a) $P_1 = [\{1, 2, 3\}, \{1, 4, 5, 6\}]$ *c*) $P_3 = [\{1, 3, 5\}, \{2, 4\}, \{6\}]$

b) $P_2 = [\{1, 2\}, \{3, 5, 6\}]$ *d*) $P_4 = [\{1, 3, 5\}, \{2, 4, 6, 7\}]$

1.47 Determine si cada una de las siguientes expresiones es o no una partición del conjunto **N** de enteros positivos:

a) $[\{n \mid n > 5\}, \{n \mid n < 5\}]$; *b*) $[\{n \mid n > 6\}, \{1, 3, 5\}, \{2, 4\}]$;

c) $[\{n \mid n^2 > 11\}, \{n \mid n^2 < 11\}]$.

1.48 Sean $[A_1, A_2, \ldots, A_m]$ y $[B_1, B_2, \ldots, B_n]$ particiones de un conjunto S.

Demuestre que la siguiente colección de conjuntos también es una partición (denominada *partición que se cruza*) de S:

$$P = [A_i \cap B_j | i = 1, \ldots, m,\ j = 1, \ldots, n] \backslash \varnothing$$

Se observa que se eliminó el conjunto vacío $\varnothing$.

1.49 Sea $S = \{1, 2, 3, \ldots, 8, 9\}$. Encontrar la partición que se cruza P de las siguientes particiones de S:

$$P_1 = [\{1, 3, 5, 7, 9\}, \{2, 4, 6, 8\}] \quad \text{y} \quad P_2 = [\{1, 2, 3, 4\}, \{5, 7\}, \{6, 8, 9\}]$$

INDUCCIÓN

1.50 Demuestre: $2 + 4 + 6 + \cdots + 2n = n(n + 1)$

1.51 Demuestre: $1 + 4 + 7 + \cdots + 3n - 2 = \frac{n(3n-1)}{2}$

1.52 Demuestre: $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

1.53 Demuestre: $\frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \frac{1}{5\cdot7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

1.54 Demuestre: $\frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \cdots + \frac{1}{(4n-3)(4n+1)} = \frac{n}{4n+1}$

1.55 Demuestre: $7^n - 2^n$ es divisible entre 5 para toda $n \in \mathbf{N}$

1.56 Demuestre: $n^3 - 4n + 6$ es divisible entre 3 para toda $n \in \mathbf{N}$

1.57 Use la identidad $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ para demostrar que:

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$$

PROBLEMAS DIVERSOS

1.58 Suponga que $\mathbf{N} = \{1, 2, 3, \ldots\}$ es el conjunto universo, y que

$$A = \{n \mid n \le 6\}, \quad B = \{n \mid 4 \le n \le 9\}, \quad C = \{1, 3, 5, 7, 9\}, \quad D = \{2, 3, 5, 7, 8\}.$$

Encuentre: *a*) $A \oplus B$; *b*) $B \oplus C$; *c*) $A \cap (B \oplus D)$; *d*) $(A \cap B) \oplus (A \cap D)$.

1.59 Demuestre las siguientes propiedades de la diferencia simétrica:

a) $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ (Ley asociativa).
b) $A \oplus B = B \oplus A$ (Ley conmutativa).
c) Si $A \oplus B = A \oplus C$, entonces $B = C$ (Ley de cancelación).
d) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ (Ley distributiva).

1.60 Considere m conjuntos no vacíos diferentes $A_1, A_2, \ldots, A_m$ en un conjunto universo **U**. Demuestre lo siguiente:

a) Hay 2^m productos fundamentales de los m conjuntos.
b) Dos productos fundamentales cualesquiera son ajenos.
c) **U** es la unión de todos los productos fundamentales.

Respuestas a los problemas suplementarios

1.26 $B = C = E = F, A = D = G = H$.

1.27 $A = \{a, e, i, o, u\}, B = D = \{l, i, t, e\}$, $C = \{a, b, c, d, e\}$.

1.28 *a*) C y E; *b*) D y E; *c*) A, B y D; *d*) ninguno.

1.29 *a*) $A \cap B = \{2, 5\}$, $A \cap C = \{1, 5\}$;
b) $A \cup B = \{1, 2, 5, 6, 7\}$, $B \cup C = \{1, 2, 3, 5, 7, 9\}$;
c) $A^{\mathrm{C}} = \{3, 4, 7, 8, 9\}$, $\mathrm{C}^{\mathrm{C}} = \{2, 4, 6, 8\}$;
d) $A \backslash B = \{1, 6\}$, $A \backslash C = \{2, 6\}$;
e) $A \oplus B = \{1, 6, 7\}$, $A \oplus C = \{2, 3, 6, 7, 9\}$;
f) $(A \cup C) \backslash B = \{1, 3, 6, 9\}$, $(B \oplus C) \backslash A = \{3, 9\}$.

1.33 $A \cup B = (A^{\mathrm{C}} \cap B^{\mathrm{C}})^{\mathrm{C}}$.

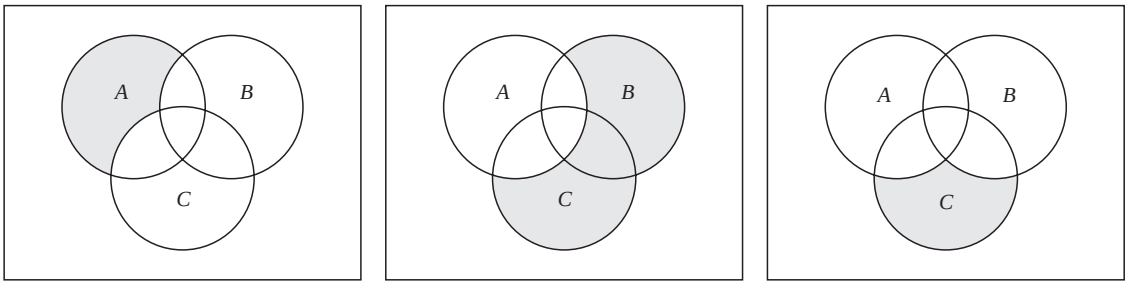
1.34 Vea la figura 1-10.

1.35 *a*) $(A \cap B \cap C) \cup (A \cap B \cap C^{\mathrm{C}}) \cup (A \cap B^{\mathrm{C}} \cap C)$
b) $(A^{\mathrm{C}} \cap B \cap C^{\mathrm{C}}) \cup (A^{\mathrm{C}} \cap B \cap C) \cup (A^{\mathrm{C}} \cap B^{\mathrm{C}} \cap C)$
c) $(A \cap B \cap C) \cup (A \cap B \cap C^{\mathrm{C}}) \cup (A \cap B^{\mathrm{C}} \cap C)$ $\cup (A^{\mathrm{C}} \cap B \cap C^{\mathrm{C}}) \cup (A \cap B^{\mathrm{C}} \cap C^{\mathrm{C}})$

1.36 Las tres premisas producen el diagrama de Venn en la figura 1-11*a*). *a*) y *b*) son válidas, pero *c*) no es válida.

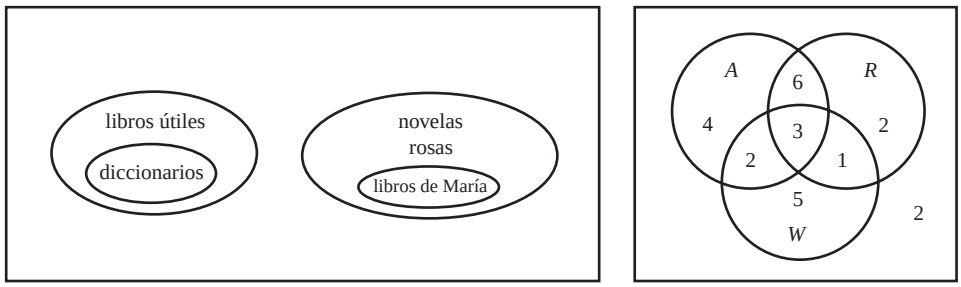
1.37 *a*) $A = (B^{\mathrm{C}} \cup A) \cap (A \cup B)$
b) $(A \cup B) \cap (A^{\mathrm{C}} \cup B) \cap (A \cup B^{\mathrm{C}}) \cap (A^{\mathrm{C}} \cup B^{\mathrm{C}}) = \varnothing$

1.39 *a*) Infinito; *b*) finito; *c*) infinito; *d*) finito.



a) *b*) *c*)

Figura 1-10



a) *b*)

Figura 1-11

1.41 Use los datos para sustituir lo que corresponda en la figura 1-11*b*). Entonces:

a) 5; *b*) 4; *c*) 2; *d*) 1; *e*) 6; *f*) 11; *g*) 23; *h*) 2.

1.42 $P(A)$ tiene $2^5 = 32$ elementos como sigue:

$[\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{3, 4, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 4, 5\}, \{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 4, 5\}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}, A]$

1.43 *a*) Tres elementos: $[a, b]$, (c), y $\{d, e, f\}$. *b*) 3. *c*) $P(A)$ tiene $2^3 = 8$ elementos como sigue:

$$P(A) = \{A, [\{a, b\}, \{c\}], [\{a, b\}, \{d, e, f\}],$$
$$[\{c\}, \{d, e, f\}], [\{a, b\}], [\{c\}], [\{d, e, f\}], \varnothing\}$$

1.44 Sea X un elemento en $P(A)$. Para cada $a \in A$ se tiene que $a \in X$ o $a \notin A$. Puesto que $n(A) = m$, hay 2^m conjuntos distintos X. Es decir, $|P(A)| = 2^m$.

1.45 *a*) No, *b*) no, *c*) sí, *d*) sí.

1.46 *a*) No, *b*) no, *c*) sí, *d*) no.

1.47 *a*) No, *b*) no, *c*) sí.

1.49 $[\{1, 3\}, \{2, 4\}, \{5, 7\}, \{9\}, \{6, 8\}]$

1.55 Sugerencia: $7^{k+1} - 2^{k+1} = 7^{k+1} - 7(2^k) + 7(2^k) - 2^{k+1}$
$= 7(7^k - 2^k) + (7 - 2)2^k$

1.58 *a*) $\{1, 2, 3, 7, 8, 9\}$; *b*) $\{1, 3, 4, 6, 8\}$; *c*) y *d*) $\{2, 3, 4, 6\}$.

2 Relaciones

CAPÍTULO

2.1 INTRODUCCIÓN

Puesto que el lector ya tiene familiaridad con muchas relaciones como "menor que", "es paralela a", "es un subconjunto de", etc., percibe que estas relaciones consideran la existencia o inexistencia de cierta conexión entre pares de objetos que se consideran en un orden definido. Formalmente, una relación se define en términos de estos "pares ordenados".

Un *par ordenado* de elementos a y b, donde a es el primer elemento y b es el segundo, se denota por (a, b). En particular,

$$(a, b) = (c, d)$$

si y sólo si $a = c$ y $b = d$. Así, $(a, b) \neq (b, a)$, a menos que $a = b$. Esto contrasta con los conjuntos donde el orden de los elementos es irrelevante; por ejemplo, $\{3, 5\} = \{5, 3\}$.

2.2 PRODUCTO DE CONJUNTOS

Considere dos conjuntos arbitrarios A y B. El conjunto de todos los pares ordenados (a, b), donde $a \in A$ y $b \in B$ se denomina *producto*, o *producto cartesiano*, de A y B. Una notación abreviada para indicar este producto es $A \times B$, que se lee "A cruz B". Por definición,

$$A \times B = \{(a, b)\} \mid a \in A \text{ y } b \in B\}$$

A menudo, en vez de $A \times A$ se escribe A^2.

EJEMPLO 2.1 $\mathbf{R}$ denota el conjunto de números reales, así que $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ es el conjunto de pares ordenados de números reales. El lector ya conoce la representación geométrica de $\mathbf{R}^2$ como puntos en el plano que se muestra en la figura 2-1. Aquí cada punto P representa un par ordenado (a, b) de números reales y viceversa; la recta vertical que pasa por P corta al eje x en a, y la recta horizontal que pasa por P corta al eje y en b. $\mathbf{R}^2$ a menudo se denomina *plano cartesiano*.

EJEMPLO 2.2 Sean $A = \{1, 2\}$ y $B = \{a, b, c\}$. Entonces

$$A \times B = \{(1, a),\ (1, b),\ (1, c),\ (2, a),\ (2, b),\ (2, c)\}$$
$$B \times A = \{(a, 1),\ (b, 1),\ (c, 1),\ (a, 2),\ (b, 2),\ (c, 2)\}$$

También, $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

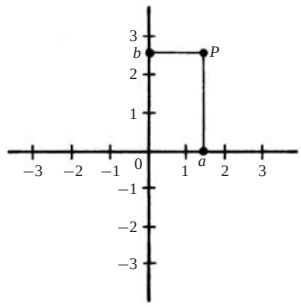


Figura 2-1

Hay dos cosas que vale la pena observar en los ejemplos presentados. En primer lugar, $A \times B \neq B \times A$. El producto cartesiano tiene que ver con pares ordenados, de modo que, naturalmente, el orden en que se consideran los conjuntos es importante. En segundo lugar, si $n(S)$ se usa para indicar el número de elementos que hay en un conjunto S, se tiene:

$$n(A \times B) = 6 = 2(3) = n(A)n(B)$$

De hecho, para conjuntos A y B finitos arbitrarios se tiene $n(A \times B) = n(A)n(B)$. Lo anterior es una consecuencia de la observación de que, para un par ordenado (a, b) en $A \times B$, para a hay $n(A)$ posibilidades, y para cada una de éstas hay $n(B)$ posibilidades para b.

La idea de producto de conjuntos se extiende a cualquier número finito de conjuntos. Para conjuntos cualesquiera $A_1, A_2, \ldots, A_n$, el conjunto de todas las n-adas ordenadas $(a_1, a_2, \ldots, a_n)$, donde $a_1 \in A_1$, $a_2 \in A_2, \ldots, a_n \in A_n$ se denomina *producto* de los conjuntos $A_1, \ldots, A_n$ y se denota por

$$A_1 \times A_2 \times \cdots \times A_n \quad \text{o} \quad \prod_{i=1}^{n} A_1$$

Así como en lugar de $A \times A$ se escribe A^2, también en lugar de $A \times A \times \cdots \times A$, donde hay n factores iguales a A, se escribe A^n. Por ejemplo, $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ denota el espacio tridimensional usual.

2.3 RELACIONES

Aquí conviene iniciar con una definición.

Definición 2.1: Sean A y B conjuntos. Una *relación binaria*, o simplemente una *relación* de A a B, es un subconjunto de $A \times B$.

Suponga que R es una *relación* de A a B. Entonces R es un conjunto de pares ordenados donde el primer elemento proviene de A y el segundo proviene de B. Es decir, para cada par $a \in A$ y $b \in B$, es verdadera exactamente una de las siguientes proposiciones:

i) $(a, b) \in R$; entonces se dice "a está relacionado con b", lo que se escribe aRb.
ii) $(a, b) \notin R$; entonces se dice "a no está relacionado con b", lo que se escribe $a \not R b$.

Si R es una relación del conjunto A en sí mismo; es decir, si R es un subconjunto de $A^2 = A \times A$, entonces se dice que R es una relación *sobre* A.

El *dominio* de una relación R es el conjunto de todos los primeros elementos de los pares ordenados que pertenecen a R, y el *rango* es el conjunto de los segundos elementos.

Aunque las relaciones n-arias, que implican n-adas ordenadas, se presentan en la sección 2.10, el término relación significará entonces relación binaria, a menos que se indique o implique otra cosa.

EJEMPLO 2.3

a) Sean $A = (1, 2, 3)$ y $B = \{x, y, z\}$, y sea $R = \{(1, y), (1, z), (3, y)\}$. Entonces R es una relación de A a B, puesto que R es un subconjunto de $A \times B$. Con respecto a esta relación,

$$1Ry, 1Rz, 3Ry, \quad \text{pero} \quad 1\not{R}x, 2\not{R}x, 2\not{R}y, 2\not{R}z, 3\not{R}x, 3\not{R}z$$

El dominio de R es $\{1, 3\}$ y el rango es $\{y, z\}$.

b) La inclusión de conjuntos $\subseteq$ es una relación sobre cualquier colección de conjuntos, ya que, dado cualquier par de conjuntos A y B, se tiene $A \subseteq B$ o $A \not\subseteq B$.

c) Una relación conocida sobre el conjunto $\mathbf{Z}$ de enteros es "m divide a n". Una notación común para indicar esto consiste en escribir $m \mid n$ cuando m divide a n. Así, $6 \mid 30$ pero $7 \nmid 25$.

d) Considere el conjunto de L líneas rectas en el plano. La perpendicularidad, que se escribe "$\perp$" es una relación sobre L. Es decir, dado cualquier par de líneas rectas a y b, se cumple $a \perp b$ o $a \not\perp b$. En forma semejante, la relación "es paralela a", que se escribe "$\parallel$", es una relación sobre L, ya que se cumple $a \parallel b$ o $a \nparallel b$.

e) Sea A cualquier conjunto. Una relación importante sobre A es la de *igualdad*,

$$\{(a, a) \mid a \in A\}$$

que suele denotarse por "=". Esta relación también se denomina relación *identidad* o *diagonal* sobre A y del mismo modo se denotará por Δ_A, o simplemente por Δ.

f) Sea A cualquier conjunto. Entonces $A \times A$ y $\varnothing$ son subconjuntos de $A \times A$ y son relaciones sobre A denominadas *relación universal* y *relación vacía*, respectivamente.

Relación inversa

Sea R cualquier relación de un conjunto A a un conjunto B. La *inversa* de R, denotada por R^{-1}, es la relación de B a A que consta de los pares ordenados que, cuando se invierten, pertenecen a R; es decir,

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

Por ejemplo, sean $A = \{1, 2, 3\}$ y $B = \{x, y, z\}$. Así, la inversa de

$$R = \{(1, y), (1, z), (3, y)\} \quad \text{es} \quad R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$$

Resulta evidente que si R es cualquier relación, entonces $(R^{-1})^{-1} = R$. También, el dominio y el rango de R^{-1} son iguales, respectivamente, al rango y al dominio de R. Además, si R es una relación sobre A, entonces R^{-1} también es una relación sobre A.

2.4 REPRESENTACIÓN GRÁFICA DE LAS RELACIONES

Hay varias formas de representar las relaciones.

Relaciones sobre R

Sea S una relación sobre el conjunto $\mathbf{R}$ de números reales; es decir, S es un subconjunto de $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$. A menudo, S consta de todos los pares ordenados de números reales que satisfacen alguna ecuación dada $E(x, y) = 0$ (como $x^2 + y^2 = 25$).

Puesto que R^2 puede representarse mediante el conjunto de puntos en el plano, S se representa recalcando los puntos en el plano que pertenecen a S. La representación gráfica de la relación algunas veces se denomina *gráfica* de la relación. Por ejemplo, la gráfica de la relación $x^2 + y^2 = 25$ es una circunferencia centrada en el origen con radio igual a 5. Vea la figura 2-2*a*).

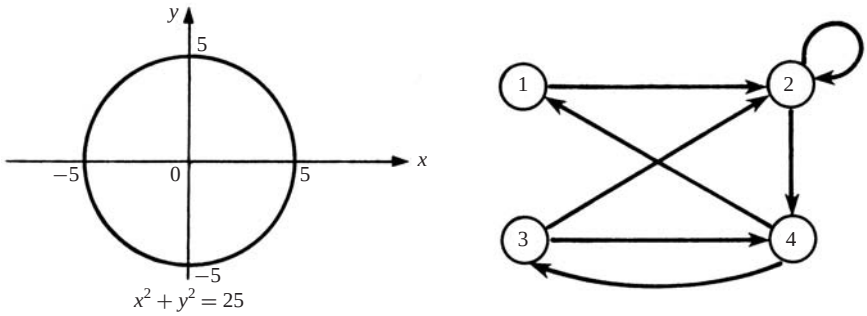


Figura 2-2

Gráficas dirigidas y relaciones sobre conjuntos

Hay una forma importante de representar una relación R sobre un conjunto finito. Primero se escriben los elementos del conjunto, y luego se traza una flecha desde cada elemento x hasta cada elemento y, siempre que x esté relacionado con y. Este diagrama se denomina *gráfica dirigida* de la relación. La figura 2-2*b*), por ejemplo, muestra la gráfica dirigida de la siguiente relación R sobre el conjunto $A = \{1, 2, 3, 4\}$:

$$R = \{(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)\}$$

Observe que hay una flecha que va de 2 a sí mismo, ya que 2 está relacionado con 2 bajo R.

Estas gráficas dirigidas se estudiarán en detalle como un tema por separado en el capítulo 8. Aquí se mencionan para tener una panorámica más completa.

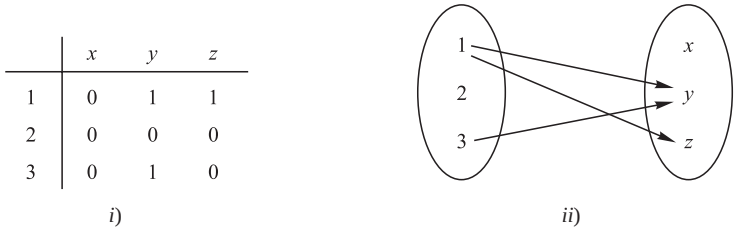
Representaciones de relaciones sobre conjuntos finitos

Suponga que A y B son conjuntos finitos. Hay dos formas de representar una relación R de A a B.

i) Se forma un arreglo rectangular (matriz) cuyos renglones se identifican mediante los elementos de A y cuyas columnas se identifican mediante los elementos de B. En cada posición del arreglo se escribe 1 o 0 según $a \in A$ esté o no relacionado con $b \in B$. Este arreglo se denomina *matriz de la relación*.

ii) Los elementos de A y de B se escriben en dos óvalos ajenos y luego se traza una flecha de $a \in A$ a $b \in B$ siempre que a esté relacionado con b. Esta representación se denomina *diagrama sagital* de la relación.

En la figura 2-3 se muestra, en las dos formas mencionadas, la relación R en el ejemplo 2.3*a*).



	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

i)

ii)

$R = \{(1, y),\ (1, z),\ (3, y)\}$

Figura 2-3

2.5 COMPOSICIÓN DE RELACIONES

Sean A, B y C conjuntos, R una relación de A a B y S una relación de B a C. Es decir, R es un subconjunto de $A \times B$ y S es un subconjunto de $B \times C$. Entonces R y S originan una relación de A a C denotada por $R \circ S$ y definida por:

$$a(R \circ S)c \text{ si para alguna } b \in B \text{ se tiene } aRb \text{ y } bSc.$$

Es decir,

$$R \circ S = \{(a, c) \mid \text{existe } b \in B \text{ para la cual } (a, b) \in R \text{ y } (b, c) \in S\}$$

La relación $R \circ S$ se denomina *composición* de R y S; algunas veces se denota simplemente por RS.

Suponga que R es una relación sobre un conjunto A; es decir, R es una relación de un conjunto A en sí mismo. Entonces $R \circ R$, la composición de R consigo mismo, siempre está definida. También, $R \circ R$ algunas veces se denota por R^2. En forma semejante, $R^3 = R^2 \circ R = R \circ R \circ R$, y así sucesivamente. Por tanto, R^n está definida para todo n positivo.

Advertencia: Muchos textos denotan la composición de las relaciones R y S con $S \circ R$, en lugar de $R \circ S$. Esto se hace así a fin de coincidir con el hábito de usar $g \circ f$ para denotar la composición de f y g, donde f y g son funciones. Así, el lector quizá deba ajustarse a esta notación cuando utilice este texto como complemento de otro texto. Sin embargo, cuando una relación R se compone consigo misma, entonces el significado de $R \circ R$ es inequívoco.

EJEMPLO 2.4 Sea $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$ y sea

$$R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\} \quad \text{y} \quad S = \{(b, x), (b, z), (c, y), (d, z)\}$$

Considere los diagramas sagitales de R y S como en la figura 2-4. Observe que hay una flecha de 2 a d seguida por una flecha de d a z. Estas dos flechas pueden considerarse como una "ruta" que "conecta" (o une) el elemento $2 \in A$ con el elemento $z \in C$. Así,

$$2(R \circ S)z \quad \text{puesto que} \quad 2Rd \text{ y } dSz$$

En forma semejante hay una ruta de 3 a x y una ruta de 3 a z. Entonces

$$3(R \circ S)x \quad \text{y} \quad 3(R \circ S)z$$

Ningún otro elemento de A está unido con un elemento de C. En consecuencia,

$$R \circ S = \{(2, z), (3, x), (3, z)\}$$

El primer teorema que se presenta establece que la composición de relaciones es asociativa.

Teorema 2.1: Sean A, B, C y D conjuntos. Suponga que R es una relación de A a B, S es una relación de B a C y T es una relación de C a D. Entonces

$$(R \circ S) \circ T = R \circ (S \circ T)$$

La demostración de este teorema se proporciona en el problema 2.8.

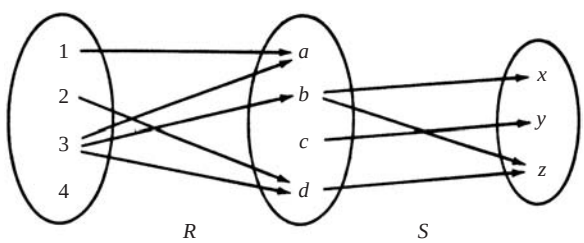


Figura 2-4

Composición de relaciones y matrices

Hay otra forma para encontrar $R \circ S$. Sean M_R y M_S que denotan, respectivamente, las representaciones matriciales de las relaciones R y S. Entonces

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{y} \quad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Al multiplicar M_R y M_S se obtiene la matriz

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

Los elementos diferentes de cero en esta matriz indican cuáles elementos están relacionados por $R \circ S$. Así, $M = M_R M_S$ y $M_{R \circ S}$ tienen los mismos elementos distintos de cero.

2.6 TIPOS DE RELACIONES

En esta sección se analizan varios tipos de relaciones importantes definidas sobre un conjunto A.

Relaciones reflexivas

Una relación R sobre un conjunto es *reflexiva* si aRa para toda $a \in A$; es decir, si $(a, a) \in R$ para toda $a \in A$. Por tanto, R no es reflexiva si existe $a \in A$ tal que $(a, a) \notin R$.

EJEMPLO 2.5 Considere las cinco relaciones siguientes sobre el conjunto $A = \{1, 2, 3, 4\}$:

$R_1 = \{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\}$
$R_2 = \{(1, 1)(1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$
$R_3 = \{(1, 3), (2, 1)\}$
$R_4 = \varnothing$, la relación vacía
$R_5 = A \times A$, la relación universal

Determine cuáles de las relaciones son reflexivas.

Puesto que A contiene los cuatro elementos 1, 2, 3 y 4, una relación sobre A es reflexiva si contiene los cuatro pares (1, 1), (2, 2), (3, 3) y (4, 4). Así, sólo R_2 y la relación universal $R_5 = A \times A$ son reflexivas. Observe que R_1, R_3 y R_4 no son reflexivas porque, por ejemplo, (2, 2) no pertenece a ninguna de ellas.

EJEMPLO 2.6 Considere las cinco relaciones siguientes:

1) Relación $\leq$ (menor que o igual a) sobre el conjunto $\mathbf{Z}$ de enteros.
2) Inclusión de conjuntos $\subseteq$ sobre una colección C de conjuntos.
3) Relación $\perp$ (es perpendicular a) sobre el conjunto L de líneas rectas en el plano.
4) Relación $\parallel$ (es paralela a) sobre el conjunto L de líneas rectas en el plano.
5) Relación $|$ de divisibilidad sobre el conjunto $\mathbf{N}$ de enteros positivos. (Recuerde que $x \mid y$ si existe z tal que $xz = y$.)

Determine cuáles de las relaciones son reflexivas.

La relación 3) no es reflexiva porque ninguna línea recta es perpendicular a sí misma. También la relación 4) no es reflexiva porque ninguna línea recta es paralela a sí misma. Las otras relaciones son reflexivas; es decir, $x \leq x$ para toda $x \in \mathbf{Z}$, $A \subseteq A$ para cualquier conjunto $A \subseteq C$, y $n \mid n$ para todo entero positivo $n \in \mathbf{N}$.

Relaciones simétricas y antisimétricas

Una relación R sobre un conjunto A es *simétrica* si siempre que aRb entonces bRa; es decir, siempre que $(a, b) \in R$ entonces $(b, a) \in R$. Por tanto, R no es simétrica si existen $a, b \in A$, tales que $(a, b) \in R$ pero $(b, a) \notin R$.

EJEMPLO 2.7

a) Determine cuáles de las relaciones en el ejemplo 2.5 son simétricas.

R_1 no es simétrica porque $(1, 2) \in R_1$ pero $(2, 1) \notin R_1$. R_3 no es simétrica porque $(1, 3) \in R_3$ pero $(3, 1) \notin R_3$. Las otras relaciones son simétricas.

b) Determine cuáles de las relaciones en el ejemplo 2.6 son simétricas.

La relación $\perp$ es simétrica porque si la línea recta a es perpendicular a la línea recta b, entonces b es perpendicular a a. También, $\parallel$ es simétrica porque si la línea recta a es paralela a la línea recta b, entonces b es paralela a la línea recta a. Las otras relaciones no son simétricas. Por ejemplo:

$$3 \leq 4 \text{ pero } 4 \not\leq 3; \quad \{1, 2\} \subseteq \{1, 2, 3\} \text{ pero } \{1, 2, 3\} \not\subseteq \{1, 2\} \quad \text{y} \quad 2 \mid 6 \text{ pero } 6 \not\mid 2.$$

Una relación R sobre un conjunto A es *antisimétrica* siempre que aRb y bRa entonces $a = b$; es decir, si $a \neq b$ y aRb, entonces $b \not R a$. Por tanto, R no es antisimétrica si existen elementos distintos a y b en A tales que aRb y bRa.

EJEMPLO 2.8

a) Determine cuáles de las relaciones en el ejemplo 2.5 son antisimétricas.

R_2 no es antisimétrica porque $(1, 2)$ y $(2, 1)$ pertenecen a R_2, pero $1 \neq 2$. En forma semejante, la relación universal R_3 no es antisimétrica. Todas las otras relaciones son antisimétricas.

b) Determine cuáles de las relaciones en el ejemplo 2.6 son antisimétricas.

La relación $\leq$ es antisimétrica porque siempre que $a \leq b$ y $b \leq a$ entonces $a = b$. La inclusión de conjuntos $\subseteq$ es antisimétrica siempre que $A \subseteq B$ y $B \subseteq A$ entonces $A = B$. También, la divisibilidad sobre $\mathbf{N}$ es antisimétrica porque siempre que $m \mid n$ y $n \mid m$, entonces $m = n$. (Observe que la divisibilidad sobre $\mathbf{Z}$ no es antisimétrica porque $3 \mid -3$ y $-3 \mid 3$ pero $3 \neq -3$.) Las relaciones $\perp$ y $\parallel$ no son antisimétricas.

Observación: Las propiedades de ser simétrica y ser antisimétrica no son negaciones entre sí. Por ejemplo, la relación $R = \{(1, 3), (3, 1), (2, 3)\}$ no es simétrica ni antisimétrica. Por otra parte, la relación $R' = \{(1, 1), (2, 2)\}$ es tanto simétrica como antisimétrica.

Relaciones transitivas

Una relación R sobre un conjunto A es *transitiva* si siempre que aRb y bRc entonces aRc; es decir, siempre que $(a, b), (b, c) \in R$ entonces $(a, c) \in R$. Por tanto, R no es transitiva si existe $a, b, c \in R$ tal que $(a, b), (b, c) \in R$ pero $(a, c) \notin R$.

EJEMPLO 2.9

a) Determine cuáles de las relaciones en el ejemplo 2.5 son transitivas.

La relación R_3 no es transitiva porque $(2, 1), (1, 3) \in R_3$ pero $(2, 3) \notin R_3$. Todas las otras relaciones son transitivas.

b) Determine cuáles de las relaciones en el ejemplo 2.6 son transitivas.

Las relaciones $\leq$, $\subseteq$ y $\mid$ son transitivas, aunque ciertamente $\perp$ no lo es. También, puesto que ninguna línea recta es paralela a sí misma, se tiene que $a \parallel b$ y $b \parallel a$, pero $a \parallel a$. Por tanto, $\parallel$ no es transitiva. (Se observa que la relación "es paralela o igual a" es una relación transitiva sobre el conjunto L de líneas rectas en el plano.)

La propiedad de transitividad también se expresa en términos de la composición de relaciones. Para una relación R sobre A se definió $R^2 = R \circ R$ y, de manera más general, $R^n = R^{n-1} \circ R$. Entonces se tiene el siguiente resultado:

Teorema 2.2: Una relación R es transitiva si y sólo si para toda $n \geq 1$, se tiene $R^n \subseteq R$.

2.7 PROPIEDADES DE CERRADURA

Considere un conjunto dado A y la colección de todas las relaciones sobre A. Sea P una propiedad de tales relaciones, como ser simétrica o transitiva. Una relación con la propiedad P se denomina P-relación. La P-cerradura de una relación arbitraria R sobre A, lo cual se escribe $P(R)$, es una P-relación tal que

$$R \subseteq P(R) \subseteq S$$

para toda P-relación S que contiene a R. Se escribe

$$(R)\text{reflexiva}, \quad (R)\text{simétrica} \quad \text{y} \quad (R)\text{transitiva}$$

para las cerraduras reflexiva, simétrica y transitiva de R.

En términos generales, no es necesario que $P(R)$ exista. Sin embargo, hay una situación general en la que $P(R)$ siempre existe. Suponga que P es una propiedad tal que por lo menos hay una P-relación que contiene a R y que la intersección de cualquier P-relaciones es nuevamente una P-relación. Entonces es posible demostrar (problema 2.16) que

$$P(R) = \cap (S \mid S \text{ es una } P\text{-relación y } R \subseteq S)$$

Por tanto, es posible obtener $P(R)$ a partir del enfoque descendente o "top-down"; es decir, como la intersección de relaciones. Sin embargo, por lo general $P(R)$ se quiere encontrar con el enfoque ascendente o "bottom-up"; es decir, adjuntando elementos a R a fin de obtener $P(R)$. Esto es lo que se hace a continuación.

Cerraduras reflexiva y simétrica

El siguiente teorema establece cómo obtener fácilmente las cerraduras reflexiva y simétrica de una relación. Aquí $\Delta_A = \{(a, a) \mid a \in A\}$ es la relación diagonal o de igualdad sobre A.

Teorema 2.3: Sea R una relación sobre un conjunto A. Entonces:

i) $R \cup \Delta_A$ es la cerradura reflexiva de R.

ii) $R \cup R^{-1}$ es la cerradura simétrica de R.

En otras palabras, (R)reflexiva se obtiene simplemente al agregar a R los elementos (a, a) en la diagonal que aún no pertenecen a R, y (R)simétrica se obtiene al añadir a R todos los pares (b, a) siempre que (a, b) pertenezca a R.

EJEMPLO 2.10 Considere la relación $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 3)\}$, sobre el conjunto $A = \{1, 2, 3, 4\}$. Entonces

$$(R)\text{reflexiva} = R \cup \{(2, 2), (4, 4)\} \quad \text{y} \quad (R)\text{simétrica} = R \cup \{(4, 2), (3, 4)\}$$

Cerradura transitiva

Sea R una relación sobre un conjunto A. Recuerde que $R^2 = R \circ R$ y $R^n = R^{n-1} \circ R$. Se define

$$R^* = \bigcup_{i=1}^{\infty} R^i$$

El siguiente teorema es válido:

Teorema 2.4: R^* es la cerradura transitiva de R.

Suponga que A es un conjunto finito con n elementos. En el capítulo 8 sobre gráficas se demuestra que

$$R^* = R \cup R^2 \cup \ldots \cup R^n$$

Esto proporciona el siguiente teorema:

Teorema 2.5: Sea R una relación sobre un conjunto A con n elementos. Entonces:

$$(R)\text{transitiva} = R \cup R^2 \cup \ldots \cup R^n$$

EJEMPLO 2.11 Considere la relación $R = \{(1, 2), (2, 3), (3, 3)\}$, sobre $A = \{(1, 2, 3)\}$. Entonces:

$$R^2 = R \circ R = \{(1, 3), (2, 3), (3, 3)\} \quad \text{y} \quad R^3 = R^2 \circ R = \{(1, 3), (2, 3), (3, 3)\}$$

En consecuencia,

$$(R)\text{transitiva} = (R) = \{(1, 2), (2, 3), (3, 3), (1, 3)\}$$

2.8 RELACIONES DE EQUIVALENCIA

Considere un conjunto S no vacío. Una relación R sobre S es una *relación de equivalencia* si R es reflexiva, simétrica y transitiva. Es decir, R es una relación de equivalencia sobre S si tiene las tres propiedades siguientes:

1) Para toda $a \in S$, aRa. 2) Si aRb, entonces bRa. 3) Si aRb y bRc, entonces aRc.

La idea general detrás de una relación de equivalencia es que es una clasificación de objetos que de alguna manera son "semejantes". De hecho, la relación "=" de igualdad sobre cualquier conjunto S es una relación de equivalencia; es decir,

1) $a = a$ para toda $a \in S$. 2) Si $a = b$, entonces $b = a$. 3) Si $a = b$, $b = c$, entonces $a = c$.

A continuación se presentan otras relaciones de equivalencia.

EJEMPLO 2.12

a) Sean L el conjunto de líneas rectas y T el conjunto de triángulos en el plano euclidiano.

   i) La relación "es paralela o idéntica a" es una relación de equivalencia sobre L.

   ii) Las relaciones de congruencia y semejanza son relaciones de equivalencia sobre T.

b) La relación $\subseteq$ de inclusión de conjuntos no es una relación de equivalencia. Es reflexiva y transitiva, pero no es simétrica, puesto que $A \subseteq B$ no implica $B \subseteq A$.

c) Sea m un entero positivo fijo. Se dice que dos enteros a y b son *congruentes módulo m*, lo cual se escribe

$$a \equiv b \text{ (mód } m\text{)}$$

si m divide a $a - b$. Por ejemplo, para el módulo $m = 4$ se tiene

$$11 \equiv 3 \text{ (mód 4)} \quad \text{y} \quad 22 \equiv 6 \text{ (mód 4)}$$

puesto que 4 divide a $11 - 3 = 8$ y 4 divide a $22 - 6 = 16$. Esta relación de congruencia módulo m es una relación de equivalencia importante.

Relaciones de equivalencia y particiones

En esta subsección se estudia la relación entre las relaciones de equivalencia y las particiones sobre un conjunto no vacío S. Primero recuerde que una partición P de S es una colección $\{A_i\}$ de subconjuntos no vacíos de S con las dos propiedades siguientes:

1) Cada $a \in S$ pertenece a algún A_i.
2) Si $A_i \neq A_j$ entonces $A_i \cap A_j = \varnothing$.

En otras palabras, una partición P de S es una subdivisión de S en conjuntos ajenos no vacíos. (Vea la sección 1.7.)

Suponga que R es una relación de equivalencia sobre un conjunto S. Para toda $a \in S$, sea $[a]$ el conjunto de elementos de S con los que a está relacionada bajo R; es decir,

$$[a] = \{x \mid (a, x) \in R\}$$

$[a]$ se denomina *clase de equivalencia* de a en S; cualquier $b \in [a]$ se denomina *representante* de la clase de equivalencia.

La colección de todas las clases de equivalencia de elementos de S bajo una relación de equivalencia R se denota con S/R; es decir,

$$S/R = \{[a] \mid a \in S\}$$

Se denomina *conjunto cociente* de S entre R. La propiedad fundamental de un conjunto cociente está contenida en el siguiente teorema.

Teorema 2.6: Sea R una relación de equivalencia sobre un conjunto S. Entonces S/R es una partición de S. En específico:

i) Para todo a en S, se tiene $a \in [a]$.
ii) $[a] = [b]$ si y sólo si $(a, b) \in R$.
iii) Si $[a] \neq [b]$, entonces $[a]$ y $[b]$ son ajenos.

A la inversa, dada una partición $\{A_i\}$ del conjunto S, hay una relación de equivalencia R sobre S tal que los conjuntos A_i son las clases de equivalencia.

Este importante teorema se demostrará en el problema 2.17.

EJEMPLO 2.13

a) Considere la relación $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ sobre $S = \{1, 2, 3\}$.

Es posible demostrar que R es reflexiva, simétrica y transitiva; es decir, que R es una relación de equivalencia. También:

$$[1] = \{1, 2\}, [2] = \{1, 2\}, [3] = \{3\}$$

Observe que $[1] = [2]$ y que $S/R = \{[1], [3]\}$ es una partición de S. Como un conjunto de representantes de las clases de equivalencia pueden elegirse $\{1, 3\}$ o $\{2, 3\}$.

b) Sea R_5 la relación de congruencia módulo 5 sobre el conjunto **Z** de enteros, denotada por

$$x \equiv y \text{ (mód 5)}$$

Esto significa que la diferencia $x - y$ es divisible entre 5. Entonces R_5 es una relación de equivalencia sobre **Z**. El conjunto cociente $\mathbf{Z}/R_5$ contiene las cinco clases de equivalencia siguientes:

$$\begin{aligned} A_0 &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\ A_1 &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\ A_2 &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ A_3 &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ A_4 &= \{\ldots, -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Cualquier entero x, expresado de manera única en la forma $x = 5q + r$, donde $0 \leq r < 5$, es un miembro de la clase de equivalencia A_r y r es el residuo. Como era de esperarse, **Z** es la unión disjunta de las clases de equivalencia A_1, A_2, A_3 y A_4. Como un conjunto de representantes de las clases de equivalencia suele elegirse {0, 1, 2, 3, 4} o {−2, −1, 0, 1, 2}.

2.9 RELACIONES DE ORDEN PARCIAL

Una relación R sobre un conjunto S se denomina *ordenamiento parcial* u *orden parcial* de S si R es reflexiva, antisimétrica y transitiva. Un conjunto S junto con un orden parcial R se denomina *conjunto parcialmente ordenado* o *conjunto PO*. Los conjuntos parcialmente ordenados se estudiarán con más detalle en el capítulo 14, por lo que aquí sólo se proporcionan algunos ejemplos.

EJEMPLO 2.14

a) La relación $\subseteq$ de inclusión de conjuntos es un ordenamiento parcial sobre cualquier colección de conjuntos, ya que la inclusión de conjuntos posee las tres propiedades deseadas. Es decir,

1) $A \subseteq A$ para cualquier conjunto A.
2) Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$.
3) Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

b) La relación $\leq$ sobre el conjunto **R** de números reales es reflexiva, antisimétrica y transitiva. Así, $\leq$ significa un orden parcial sobre **R**.

c) La relación "a divide a b", escrita $a \mid b$, es un ordenamiento parcial sobre el conjunto **N** de enteros positivos. Sin embargo, "a divide a b" no es un ordenamiento parcial sobre el conjunto **Z** de enteros, puesto que $a \mid b$ y $b \mid a$ no necesariamente implica $a = b$. Por ejemplo, $3 \mid -3$ y $-3 \mid 3$, pero $3 \neq -3$.

2.10 RELACIONES *n*-ARIAS

Todas las relaciones que se han analizado eran relaciones binarias. Por una *relación n-aria* se entiende un conjunto de eneadas ordenadas. Para cualquier conjunto S, un subconjunto del conjunto producto S^n se denomina relación n-aria sobre S. En particular, un subconjunto de S^3 se denomina *relación ternaria* sobre S.

EJEMPLO 2.15

a) Sea L una línea recta en el plano. Entonces "estar entre" es una relación ternaria R sobre los puntos de L; es decir, $(a, b, c) \in R$ si b está entre a y c sobre L.

b) La ecuación $x^2 + y^2 + z^2 = 1$ determina una relación ternaria T sobre el conjunto **R** de números reales. Es decir, una terna (x, y, z) pertenece a T si (x, y, z) satisface la ecuación, lo cual significa que (x, y, z) son las coordenadas de un punto en $\mathbf{R}^3$ sobre la esfera S de radio 1 y centro en el origen $O = (0, 0, 0)$.

PROBLEMAS RESUELTOS

PRODUCTO DE CONJUNTOS

2.1 Dados $A = \{1, 2\}$, $B = \{x, y, z\}$ y $C = \{3, 4\}$, encuentre: $A \times B \times C$.

$A \times B \times C$ consta de todas las ternas ordenadas (a, b, c) donde $a \in A$, $b \in B$, $c \in C$. Estos elementos de $A \times B \times C$ se pueden obtener en forma sistemática mediante un diagrama de árbol (figura 2-5). Los elementos de $A \times B \times C$ son precisamente las 12 ternas ordenadas a la derecha del diagrama de árbol.

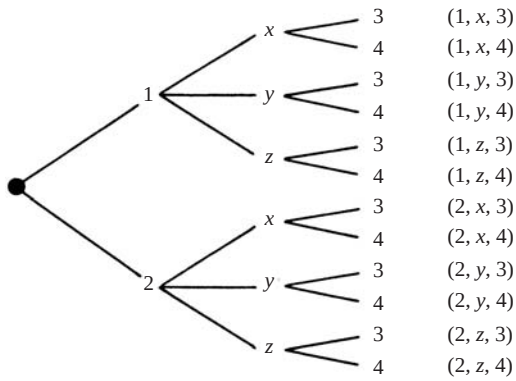


Figura 2-5

Observe que $n(A) = 2$, $n(B) = 3$ y $n(C) = 2$ y, como era de esperar,

$$n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$

2.2 Encuentre x y y dado $(2x, x + y) = (6, 2)$.

Dos pares ordenados son iguales si y sólo si las componentes correspondientes son iguales. Por tanto, se obtienen las ecuaciones

$$2x = 6 \quad \text{y} \quad x + y = 2$$

al resolver el sistema se obtienen las respuesta $x = 3$ y $y = 1$.

RELACIONES Y SUS GRÁFICAS

2.3 Encuentre el número de relaciones de $A = \{a, b, c\}$ a $B = \{1, 2\}$.

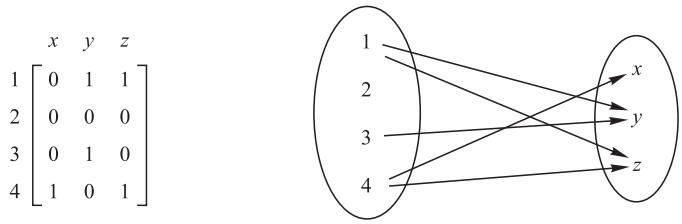
En $A \times B$ hay $3(2) = 6$ elementos, y entonces hay $m = 2^6 = 64$ subconjuntos de $A \times B$. Así, de A a B hay $m = 64$ relaciones.

2.4 Sean $A = \{1, 2, 3, 4\}$ y $B = \{x, y, z\}$. Sea R la siguiente relación de A a B:

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}$$

a) Determine la matriz de la relación.
b) Trace el diagrama sagital de R.
c) Encuentre la relación inversa R^{-1} de R.
d) Determine el dominio y el rango de R.

a) Vea la figura 2-6*a*). Observe que los renglones de la matriz están identificados por los elementos de A y las columnas, por los elementos de B. También observe en la matriz que el elemento correspondiente a $a \in A$ y $b \in B$ es 1 si a está relacionado con b y 0 en caso contrario.



a) *b*)

Figura 2-6

b) Vea la figura 2-6*b*). Observe que hay una flecha de $a \in A$ a $b \in B$ si y sólo si a está relacionada con b; es decir, si y sólo si $(a, b) \in R$.

c) Los pares ordenados de R se invierten para obtener R^{-1}:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3), (x, 4), (z, 4)\}$$

Observe que al invertir las flechas en la figura 2-6*b*) se obtiene el diagrama sagital de R^{-1}.

d) El dominio de R, Dom(R), consta de los primeros elementos de los pares ordenados de R, y el rango de R, Ran(R), consta de los segundos elementos. Así,

$$\text{Dom}(R) = \{1, 3, 4\} \quad \text{y} \quad \text{Ran}(R) = \{x, y, z\}$$

2.5 Sean $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ y $C = \{x, y, z\}$. Considere las siguientes relaciones R y S de A a B y de B a C, respectivamente.

$$A = \{(1, b), (2, a), (2, c)\} \quad \text{y} \quad S = \{(a, y), (b, x), (c, y), (c, z)\}$$

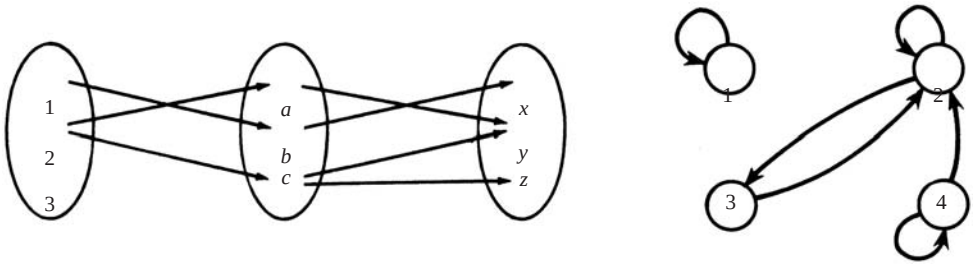
a) Encuentre la relación composición $R \circ S$.

b) Encuentre las matrices M_R, M_S y $M_{R \circ S}$ de las relaciones respectivas R, S y $R \circ S$, y comparar $M_{R \circ S}$ con el producto $M_R M_S$.

a) El diagrama sagital de las relaciones R y S se traza como en la figura 2-7*a*). Observe que 1 en A está "conectado" con x en C mediante la ruta $1 \to b \to x$; así, $(1, x)$ pertenece a $R \circ S$. En forma semejante, $(2, y)$ y $(2, z)$ pertenecen a $R \circ S$.

Se tiene

$$R \circ S = \{(1, x), (2, y), (2, z)\}$$



a) *b*)

Figura 2-7

b) Las matrices M_R, M_S y $M_{R\circ S}$ son las siguientes:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad M_S = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{array} \quad M_{R\circ S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

Al multiplicar M_R y M_S se obtiene

$$M_R M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Observe que $M_{R\circ S}$ y $M_R M_S$ tienen las mismas entradas cero.

2.6 Dada la relación $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (4, 2), (4, 4)\}$ sobre $A = \{1, 2, 3, 4\}$.

a) Trace su gráfica dirigida. *b*) Encuentre $R^2 = R \circ R$.

a) Para todo $(a, b) \in R$, se traza una flecha de *a* a *b* como en la figura 2-7*b*).

b) Para todo par $(a, b) \in R$, se encuentran todos los $(b, c) \in R$. Luego, $(a, c) \in R^2$. Así,

$$R^2 = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3), (4, 2), (4, 3), (4, 4)\}$$

2.7 Sean *R* y *S* las siguientes relaciones sobre $A = \{1, 2, 3\}$:

$$R = \{(1, 1), (1, 2), (2, 3), (3, 1), (3, 3)\}, \quad S = \{(1, 2), (1, 3), (2, 1), (3, 3)\}$$

Encuentre *a*) $R \cup S$, $R \cap S$, R^C; *b*) $R \circ S$; *c*) $S^2 = S \circ S$.

a) *R* y *S* se tratan simplemente como conjuntos, y se toman la unión e intersección de costumbre. Para R^C se utiliza el hecho de que $A \times A$ es la relación universal sobre *A*.

$$\begin{aligned} R \cap S &= \{(1, 2), (3, 3)\} \\ R \cup S &= \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\} \\ R^C &= \{(1, 3), (2, 1), (2, 2), (3, 2)\} \end{aligned}$$

b) Para todo par $(a, b) \in R$, se encuentran todos los pares $(b, c) \in S$. Entonces, $(a, c) \in R \circ S$. Por ejemplo, $(1, 1) \in R$ y $(1, 2), (1, 3) \in S$; por tanto, (1, 2) y (1, 3) pertenecen a $R \circ S$. Así,

$$R\circ S = \{(1, 2), (1, 3), (1, 1), (2, 3), (3, 2), (3, 3)\}$$

c) Al seguir el algoritmo en el inciso *b*), se obtiene

$$S^2 = S\circ S = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

2.8 Demuestre el teorema 2.1: Sean *A*, *B*, *C* y *D* conjuntos. Suponga que *R* es una relación de *A* a *B*, que *S* es una relación de *B* a *C* y que *T* es una relación de *C* a *D*. Entonces $(R \circ S) \circ T = R \circ (S \circ T)$.

Es necesario demostrar que cada par ordenado en $(R \circ S) \circ T$ pertenece a $R \circ (S \circ T)$ y viceversa.

Se supone que (a, d) pertenece a $(R \circ S) \circ T$. Entonces existe $c \in C$ tal que $(a, c) \in R \circ S$ y $(c, d) \in T$. Puesto que $(a, c) \in R \circ S$, existe $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Debido a que $(b, c) \in S$ y $(c, d) \in T$, se tiene $(b, d) \in S \circ T$; y puesto que $(a, b) \in R$ y $(b, d) \in S \circ T$, se tiene $(a, d) \in R \circ (S \circ T)$. En consecuencia, $(R \circ S) \circ T \subseteq R \circ (S \circ T)$. En forma semejante, $R \circ (S \circ T) \subseteq (R \circ S) \circ T$. Ambas relaciones de inclusión demuestran $(R \circ S) \circ T = R \circ (S \circ T)$.

TIPOS DE RELACIONES Y PROPIEDADES DE CERRADURA

2.9 Considere las cinco relaciones siguientes sobre el conjunto $A = \{1, 2, 3\}$:

$$R = \{(1, 1), (1, 2), (1, 3), (3, 3)\}, \qquad \varnothing = \text{relación vacía}$$
$$S = \{(1, 1)(1, 2), (2, 1)(2, 2), (3, 3)\}, \qquad A \times A = \text{relación universal}$$
$$T = \{(1, 1), (1, 2), (2, 2), (2, 3)\}$$

Determine si cada una de las relaciones indicadas sobre A es: *a*) reflexiva; *b*) simétrica; *c*) transitiva; *d*) antisimétrica.

a) R no es reflexiva puesto que $2 \in A$ pero $(2, 2) \notin R$. T no es reflexiva puesto que $(3, 3) \notin T$ y, en forma semejante, $\varnothing$ no es reflexiva. S y $A \times A$ son reflexivas.

b) R no es simétrica puesto que $(1, 2) \in R$ pero $(2, 1) \notin R$, y en forma semejante, T no es simétrica. S, $\varnothing$ y $A \times A$ son simétricas.

c) T no es transitiva puesto que $(1, 2)$ y $(2, 3)$ pertenecen a T, pero $(1, 3)$ no pertenece a T. Las otras cuatro relaciones son transitivas.

d) S no es antisimétrica porque $1 \neq 2$ y ambos $(1, 2)$ y $(2, 1)$ pertenecen a S. En forma semejante, $A \times A$ no es antisimétrica. Las otras tres relaciones son antisimétricas.

2.10 Proporcione un ejemplo de una relación R sobre $A = \{1, 2, 3\}$ tal que:

a) R sea tanto simétrica como antisimétrica.
b) R no sea simétrica ni antisimétrica.
c) R sea transitiva pero $R \cup R^{-1}$ no transitiva.

Hay muchos ejemplos así. A continuación se presenta un conjunto de ejemplos posibles:

a) $R = \{(1, 1), (2, 2)\}$; *b*) $R = \{(1, 2), (2, 3)\}$; *c*) $R = \{(1, 2)\}$.

2.11 Suponga que C es una colección de relaciones S sobre un conjunto A, y sea T la intersección de las relaciones S en C; es decir, $T = \cap (S \mid S \in C)$. Demostrar:

a) Si toda S es simétrica, entonces T es simétrica.
b) Si toda S es transitiva, entonces T es transitiva.

a) Suponga que $(a, b) \in T$. Entonces $(a, b) \in S$ para toda S. Puesto que toda S es simétrica, $(b, a) \in S$ para toda S. Así, $(b, a) \in T$ y T es simétrica.

b) Suponga que (a, b) y (b, c) pertenecen a T. Entonces (a, b) y (b, c) pertenecen a S para toda S. Puesto que toda S es transitiva, (a, c) pertenece a S para toda S. Por tanto, $(a, c) \in T$ y T es transitiva.

2.12 Sea R una relación sobre un conjunto A, y sea P una propiedad de las relaciones, como simetría y transitividad. Entonces P se denomina *R-cerrable* si P satisface las dos condiciones siguientes:

1) Existe una P-relación S que contiene a R.
2) La intersección de las P-relaciones es una P-relación.

a) Demuestre que la simetría y la transitividad son R-cerrables para cualquier relación R.
b) Suponga que P es R-cerrable. Entonces $P(R)$, la P-cerradura de R, es la intersección de todas las P-relaciones S que contienen a R; es decir,

$$P(R) = \cap (S \mid S \text{ es una } P\text{-relación y } R \subseteq S)$$

a) La relación universal $A \times A$ es simétrica y transitiva y $A \times A$ contiene cualquier relación R sobre A. Así, 1) se cumple. Por el problema 2.11, la simetría y la transitividad satisfacen 2). Entonces, la simetría y la transitividad son R-cerrables para cualquier relación R.

b) Sea $T = \cap (S \mid S$ es una P-relación y $R \subseteq S)$. Puesto que P es R-cerrable, T no es vacía por 1) y T es una P-relación por 2). Debido a que cada relación S contiene a R, la intersección T contiene a R. Así, T es una P-relación que contiene a R. Por definición, $P(R)$ es la P-relación más pequeña que contiene a R; por tanto, $P(R) \subseteq T$. Por otra parte, $P(R)$ es uno de los conjuntos S que definen a T; es decir, $P(R)$ es una P-relación y si $R \subseteq P(R)$. En consecuencia, $T \subseteq P(R)$. Por consiguiente, $P(R) = T$.

2.13 En la relación $R = \{(a, a), (a, b), (b, c), (c, c)\}$, sobre el conjunto $A = \{a, b, c\}$. Encuentre *a*) (R)reflexiva, *b*) (R)simétrica, *c*) (R)transitiva.

a) La cerradura reflexiva sobre R se obtiene al añadir a R todos los pares diagonales de $A \times A$ que aún no estén en R. Por tanto,

$$(R)\text{reflexiva} = R \cup \{(b, b)\} = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$$

b) La cerradura simétrica sobre R se obtiene al añadir a R todos los pares en R^{-1} que aún no estén en R. Por tanto,

$$(R)\text{simétrica} = R \cup \{(b, a), (c, b)\} = \{(a, a), (a, b), (b, a), (b, c), (c, b), (c, c)\}$$

c) Puesto que A tiene tres elementos, la cerradura transitiva sobre R se obtiene al tomar la unión de R con $R^2 = R \circ R$ y $R^3 = R \circ R \circ R$. Observe que

$$R^2 = R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

$$R^3 = R \circ R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Por tanto,

$$(R)\text{transitiva} = R \cup R^2 \cup R^3 = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

RELACIONES DE EQUIVALENCIA Y PARTICIONES

2.14 Dado el conjunto $\mathbf{Z}$ de enteros y un entero $m > 1$. Se dice que x es congruente con y módulo m, que se escribe

$$x \equiv y \ (\text{mód } m)$$

si $x - y$ es divisible entre m. Demuestre que esto define una relación de equivalencia sobre $\mathbf{Z}$.

Es necesario demostrar que la relación es reflexiva, simétrica y transitiva.

i) Para cualquier x en $\mathbf{Z}$ se tiene $x \equiv x$ (mód m) porque $x - x = 0$ es divisible entre m. Por tanto, la relación es reflexiva.

ii) Suponga que $x \equiv y$ (mód m), de modo que $x - y$ es divisible entre m. Entonces $-(x - y) = y - x$ también es divisible entre m, de modo que $y \equiv x$ (mód m). Por tanto, la relación es simétrica.

iii) Ahora suponga que $x \equiv y$ (mód m) y $y \equiv z$ (mód m), de modo que ambos $x - y$ y $y - z$ son divisibles entre m. Entonces la suma

$$(x - y) + (y - z) = x - z$$

también es divisible entre m; por tanto, la relación es transitiva.

En consecuencia, la relación de congruencia módulo m sobre $\mathbf{Z}$ es una relación de equivalencia.

2.15 Sea A un conjunto de enteros diferentes de cero y sea $\approx$ la relación sobre $A \times A$ definida por

$$(a, b) \approx (c, d) \text{ siempre que } ad = bc$$

Demuestre que $\approx$ es una relación de equivalencia.

Es necesario demostrar que $\approx$ es reflexiva, simétrica y transitiva.

i) *Reflexividad*: Se tiene $(a, b) \approx (a, b)$, puesto que $ab = ba$. Por tanto, $\approx$ es reflexiva.

ii) *Simetría*: Suponga que $(a, b) \approx (c, d)$. Entonces $ad = bc$. En consecuencia, $cb = da$ y así $(c, d) \approx (a, b)$. Por tanto, $\approx$ es simétrica.

iii) *Transitividad*: Suponga que $(a, b) \approx (c, d)$ y que $(c, d) \approx (e, f)$. Entonces, $ad = bc$ y $cf = de$. Al multiplicar los términos correspondientes de las ecuaciones se obtiene $(ad)(cf) = (bc)(de)$. Al cancelar $c \neq 0$ y $d \neq 0$ en ambos miembros de la ecuación se obtiene $af = be$, y entonces $(a, b) \approx (e, f)$. Por tanto, $\approx$ es transitiva. En consecuencia, $\approx$ es una relación de equivalencia.

2.16 Sea R la siguiente relación de equivalencia sobre el conjunto $A = \{1, 2, 3, 4, 5, 6\}$:

$$R = \{(1, 1), (1, 5), (2, 2), (2, 3), (2, 6), (3, 2), (3, 3), (3, 6), (4, 4), (5, 1), (5, 5), (6, 2), (6, 3), (6, 6)\}$$

Encontrar la partición de A inducida por R; es decir, encontrar las clases de equivalencia de R.

Los elementos relacionados con 1 son 1 y 5; así

$$[1] = \{1, 5\}$$

Se elige un elemento que no esté en [1]; por ejemplo, 2. Los elementos relacionados con 2 son 2, 3, y 6; así

$$[2] = \{2, 3, 6\}$$

El único elemento que no pertenece a [1] o a [2] es 4. El único elemento relacionado con 4 es 4. Así

$$[4] = \{4\}$$

En consecuencia, la partición de A inducida por R es:

$$[\{1, 5\}, \{2, 3, 6\}, \{4\}]$$

2.17 Demuestre el teorema 2.6: Sea R una relación de equivalencia en un conjunto A. Entonces el conjunto cociente A/R es una partición de A. Específicamente:

i) $a \in [a]$, para toda $a \in A$.
ii) $[a] = [b]$, si y sólo si $(a, b) \in R$.
iii) Si $[a] \neq [b]$, entonces $[a]$ y $[b]$ son ajenos.

a) *Demostración de i*): Puesto que R es reflexiva, $(a, a) \in R$ para toda $a \in A$ y, por consiguiente, $a \in [a]$.

b) *Demostración de ii*): Suponga que $(a, b) \in R$. Se quiere demostrar que $[a] = [b]$. Sea $x \in [b]$; entonces $(b, x) \in R$. Pero por hipótesis $(a, a) \in R$ y así, por transitividad, $(a, x) \in R$. En consecuencia, $x \in [a]$. Así, $[b] \subseteq [a]$. Para demostrar que $[a] \subseteq [b]$ se observa que $(a, b) \in R$ implica, por simetría, que $(b, a) \in R$. Entonces, por un razonamiento semejante, se obtiene $[a] \subseteq [b]$. En consecuencia, $[a] = [b]$.

Por otra parte, si $[a] = [b]$, entonces, por *i*), $b \in [b] = [a]$; por tanto, $(a, b) \in R$.

c) *Demostración de iii*): Se demuestra la proposición contrapositiva equivalente:

$$\text{Si } [a] \cap [b] \neq \varnothing \quad \text{entonces} \quad [a] = [b]$$

Si $[a] \cap [b] \neq \varnothing$, entonces existe un elemento $x \in A$ con $x \in [a] \cap [b]$. Así, $(a, x) \in R$ y $(b, x) \in R$. Por simetría, $(x, b) \in R$ y por transitividad, $(a, b) \in R$. En consecuencia, por *ii*), $[a] = [b]$.

ORDENAMIENTOS PARCIALES

2.18 Sea ℓ cualquier colección de conjuntos. La relación de inclusión de conjuntos $\subseteq$, ¿es de orden parcial sobre ℓ?

Sí, puesto que la inclusión de conjuntos es reflexiva, antisimétrica y transitiva. Es decir, para conjuntos arbitrarios A, B y C en ℓ se tiene: *i*) $A \subseteq A$; *ii*) si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$; *iii*) si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

2.19 Considere el conjunto $\mathbf{Z}$ de enteros. aRb se define como $b = a^r$ para algún entero positivo r. Demuestre que R es un orden parcial sobre $\mathbf{Z}$; es decir, que R es: *a*) reflexiva; *b*) antisimétrica; *c*) transitiva.

a) R es reflexiva puesto que $a = a^1$.

b) Suponga que aRb y bRa; por ejemplo, $b = a^r$ y $a = b^s$. Entonces $a = (a^r)^s = a^{rs}$. Hay tres posibilidades: *i*) $rs = 1$, *ii*) $a = 1$ y *iii*) $a = -1$. Si $rs = 1$, entonces $r = 1$ y $s = 1$ y así $a = b$. Si $a = 1$, entonces $b = 1^r = 1 = a$, y en forma semejante, si $b = 1$, entonces $a = 1$. Por último, si $a = -1$, entonces $b = -1$ (puesto que $b \neq 1$) y $a = b$. En los tres casos se tiene que $a = b$. Por tanto, R es antisimétrica.

c) Suponga que aRb y bRc; por ejemplo, $b = a^r$ y $c = b^s$. Entonces $c = (a^r)^s = a^{rs}$ y, por consiguiente, aRc. Por tanto, R es transitiva.

En consecuencia, R es un orden parcial sobre $\mathbf{Z}$.

PROBLEMAS SUPLEMENTARIOS

RELACIONES

2.20 Sean $S = \{a, b, c\}$, $T = \{b, c, d\}$ y $W = \{a, d\}$. Encuentre $S \times T \times W$.

2.21 Encuentre x y y, donde: *a*) $(x + 2, 4) = (5, 2x + y)$; *b*) $(y - 2, 2x + 1) = (x - 1, y + 2)$.

2.22 Demuestre: *a*) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; *b*) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2.23 Considere la relación: $R = \{(1, 3), (1, 4), (3, 2), (3, 3), (3, 4)\}$, sobre $A = \{1, 2, 3, 4\}$.

a) Encuentre la matriz M_R de R.
b) Encuentre el dominio y el rango de R.
c) Encuentre R^{-1}.
d) Trace la gráfica dirigida de R.
e) Encuentre la relación composición $R \circ R$.
f) Encuentre $R \circ R^{-1}$ y $R^{-1} \circ R$.

2.24 Sea $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{x, y, z\}$. Considere las relaciones R de A a B y S de B a C como sigue:

$$R = \{(1, b), (3, b), (3, b), (4, c)\} \quad \text{y} \quad S = \{(a, y), (c, x), (a, z)\}$$

a) Dibuje los diagramas de R y S.
b) Encuentre la matriz de cada relación R, S (composición) $R \circ S$.
c) Escriba R^{-1} y la composición $R \circ S$ como conjuntos de pares ordenados.

2.25 Sean R y S las siguientes relaciones sobre $B = \{a, b, c, d\}$:

$$R = \{(a, b), (a, c), (c, b), (c, d), (d, b)\} \quad \text{y} \quad S = \{(b, a), (c, c), (c, d), (d, a)\}$$

Encuentre las siguientes relaciones composición: *a*) $R \circ S$; *b*) $S \circ R$; *c*) $R \circ R$; *d*) $S \circ S$.

2.26 Sea R la relación sobre $\mathbf{N}$ definida por $x + 3y = 12$; es decir, $R = \{(x, y) \mid x + 3y = 12\}$

a) Escriba R como un conjunto de pares ordenados.
b) Encuentre el dominio y el rango de R.
c) Encuentre R^{-1}.
d) Encuentre la relación composición $R \circ R$.

PROPIEDADES DE LAS RELACIONES

2.27 En cada uno de los siguientes incisos se define una relación sobre los enteros positivos $\mathbf{N}$:

1) "x es mayor que y".
2) "xy es el cuadrado de un entero".
3) $x + y = 10$.
4) $x + 4y = 10$.

Determine cuáles de esas relaciones son: *a*) reflexivas; *b*) simétricas; *c*) antisimétricas; *d*) transitivas.

2.28 Sean R y S relaciones sobre un conjunto A. Suponga que A tiene tres elementos y mencione si cada una de las siguientes declaraciones es falsa o verdadera. Si es falsa, proporcione un contraejemplo sobre el conjunto $A = \{1, 2, 3\}$:

a) Si R y S son simétricas, entonces $R \cap S$ es simétrica.
b) Si R y S son simétricas, entonces $R \cup S$ es simétrica.
c) Si R y S son reflexivas, entonces $R \cap S$ es reflexiva.

d) Si R y S son reflexivas, entonces $R \cup S$ es reflexiva.

e) Si R y S son transitivas, entonces $R \cup S$ es transitiva.

f) Si R y S son antisimétricas, entonces $R \cup S$ es antisimétrica.

g) Si R es antisimétrica, entonces R^{-1} es antisimétrica.

h) Si R es reflexiva, entonces $R \cap R^{-1}$ no es vacía.

i) Si R es simétrica, entonces $R \cap R^{-1}$ no es vacía.

2.29 Suponga que R y S son relaciones sobre un conjunto A y que R es antisimétrica. Demuestre que $R \cap S$ es antisimétrica.

RELACIONES DE EQUIVALENCIA

2.30 Demuestre que si R es una relación de equivalencia sobre un conjunto A, entonces R^{-1} también es una relación de equivalencia sobre A.

2.31 Sea $S = \{1, 2, 3, \ldots, 18, 19\}$. Sea R la relación sobre S definida por "xy es un cuadrado". *a*) Demuestre que R es una relación de equivalencia. *b*) Encuentre la clase de equivalencia [1]. *c*) Enumere todas las clases de equivalencia con más de un elemento.

2.32 Sea $S = \{1, 2, 3, \ldots, 14, 15\}$. Sea R la relación de equivalencia sobre S definida por $x \equiv y$ (mód 5); es decir, $x - y$ es divisible entre 5. Encuentre la partición de S inducida por R; es decir, el conjunto cociente S/R.

2.33 Sea $S = \{1, 2, 3, \ldots, 9\}$ y sea $\sim$ la relación sobre $A \times A$ definida por

$$(a, b) \sim (c, d) \quad \text{siempre que} \quad a + d = b + c.$$

a) Demuestre que $\sim$ es una relación de equivalencia.

b) Encuentre [(2, 5)]; es decir, la clase de equivalencia de (2, 5).

Respuestas a los problemas suplementarios

2.20 $\{(a, b, a), (a, b, d), (a, c, a), (a, c, d), (a, d, a), (a, d, d), (b, b, a), (b, b, d), (b, c, a), (b, c, d), (b, d, a), (b, d, d), (c, b, a), (c, b, d), (c, c, a), (c, c, d), (c, d, a), (c, d, d)\}$

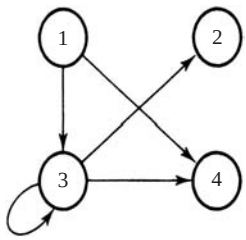
2.21 *a*) $x = 3, y = -2$; *b*) $x = 2, y = 3$.

2.23 *a*) $M_R = [0, 0, 1, 1; 0, 0, 0, 0; 0, 1, 1, 1; 0, 0, 0, 0]$;
b) Dominio $= \{1, 3\}$, rango $= \{2, 3, 4\}$;
c) $R^{-1} = \{(3, 1), (4, 1), (2, 3), (3, 3), (4, 3)\}$;
d) Vea la figura 2-8*a*);
e) $R \circ R = \{(1, 2), (1, 3), (1, 4), (3, 2), (3, 3), (3, 4)\}$.

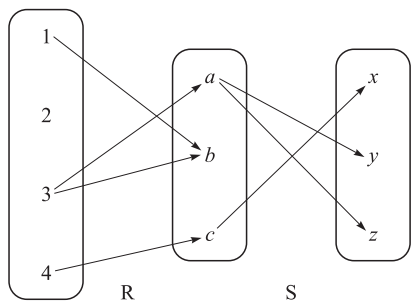
2.24 *a*) Vea la figura 2-8*b*);
b) $R = [0, 1, 0; 0, 0, 0; 1, 1, 0; 0, 0, 1]$,
$S = [0, 1, 1; 0, 0, 0; 1, 0, 0]$,
$R \circ S = [0, 0, 0; 0, 0, 0; 0, 1, 1; 1, 0, 0]$,
c) $\{(b, 1), (a, 3), (b, 3), (c, 4)\}$, $\{(3, y), (3, z), (4, x)\}$.

2.25 *a*) $R \circ S = \{(a, c), (a, d), (c, a), (d, a)\}$
b) $S \circ R = \{(b, a), (b, c), (c, b), (c, d), (d, a), (d, c)\}$
c) $R \circ R = \{(a, a), (a, b), (a, c), (a, d), (c, b)\}$
d) $S \circ S = \{(c, c), (c, a), (c, d)\}$

2.26 *a*) $\{(9, 1), (6, 2), (3, 3)\}$; *b*) *i*) $\{9, 6, 3)\}$; *ii*) $\{1, 2, 3)\}$; *iii*) $\{(1, 9), (2, 6), (3, 3)\}$; *c*) $\{(3, 3)\}$.



a)



b)

Figura 2-8

2.27 *a*) Ninguna; *b*)(2) y (3); *c*) (1) y (4); *d*) todas, excepto (3).

2.28 Todas son verdaderas excepto: *e*) $R = \{(1, 2)\}$, $S = \{(2, 3)\}$; *f*) $R = \{(1, 2)\}$, $S = \{(2, 1)\}$.

2.31 *b*) {1, 4, 9, 16}; *c*) {1, 4, 9, 16}, {2, 8, 18}, {3, 12}.

2.32 [{1, 6, 11}, {2, 7, 14}, {3, 8, 133}, {4, 9, 14}, {5, 10, 15}].

2.33 *b*) {(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 9)}.

3 Funciones y algoritmos

CAPÍTULO

3.1 INTRODUCCIÓN

Uno de los conceptos más importantes en matemáticas es el de función. Los términos "mapa", "mapeo", "transformación" y muchos otros significan lo mismo; la elección del término a usar en una situación dada depende de la tradición y del contexto matemático de quien lo utilice.

Al concepto de función se relaciona el de algoritmo. En este capítulo se incluyen la notación para representar un algoritmo y un análisis de su complejidad.

3.2 FUNCIONES

Suponga que a cada elemento de un conjunto A se asigna un único elemento de un conjunto B; la colección de estas asignaciones se denomina *función* de A en B. El conjunto A se denomina *dominio* de la función, y el conjunto B se denomina *conjunto objetivo* o *codominio*.

Las funciones suelen denotarse mediante símbolos. Por ejemplo, f denota una función de A en B. Entonces se escribe

$$f: A \to B$$

que se lee: "f es una función de A en B" o "f manda (o mapea, o transforma) A en B". Si $a \in A$, entonces $f(a)$ (que se lee "f de a") denota el elemento único de B que f asigna a a; se denomina *imagen* de a bajo f; o *valor* de f en a. El conjunto de todos los valores imagen se denomina *rango* o *imagen* de f. La imagen de $f: A \to B$ se denota por Ran(f), Im(f) o $f(A)$.

A menudo se expresa una función por medio de una fórmula matemática. Por ejemplo, considere la función que manda cada número real en su cuadrado. Esta función se describe como

$$f(x) = x^2 \quad \text{o} \quad x \mapsto x^2 \quad \text{o} \quad y = x^2$$

En la primera notación, x se denomina *variable* y la letra f denota la función. En la segunda notación, la flecha con barra $\mapsto$ se lee "va en ("se envía a x^2")". En la última notación x se denomina *variable independiente* y y *variable dependiente*, puesto que el valor de y depende del valor de x.

Observación: Siempre que una función se proporciona mediante una fórmula en términos de una variable x, se supone, a menos que se establezca otra cosa, que el dominio de la función es **R** (o el mayor subconjunto de **R** para el que la fórmula está definida) y que el codominio es **R**.

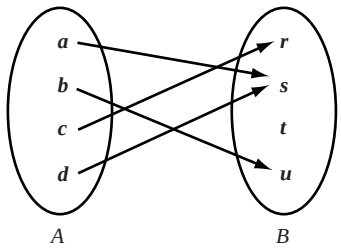


Figura 3-1

EJEMPLO 3.1

a) Considere la función $f(x) = x^3$; es decir, f asigna a cada número real a su cubo. Así, la imagen de 2 es 8, por lo que se escribe $f(2) = 8$.

b) En la figura 3-1 se define una función f de $A = \{a, b, c, d\}$ en $B = \{r, s, t, u\}$ en la forma evidente. Aquí

$$f(a) = s, \quad f(b) = u, \quad f(c) = r, \quad f(d) = s$$

La imagen de f es el conjunto de valores imagen $\{r, s, u\}$. Observe que t no pertenece a la imagen de f, porque no es imagen de algún elemento bajo f.

c) Sea A cualquier conjunto. La función de A en A que asigna cada elemento de A a sí mismo se denomina *función identidad* sobre A y suele denotarse por 1_A, o simplemente por 1. En otras palabras, para toda $a \in A$,

$$1_A(a) = a.$$

d) Suponga que S es un subconjunto de A; es decir, suponga $S \subseteq A$. La *transformación*, *mapeo*, o *inclusión* de S en A, denotado por i: $S \hookrightarrow A$ es una función tal que, para todo $x \in S$,

$$i(x) = x$$

La *restricción* de cualquier función $f : A \to B$, denotada por $f|_S$ es la función de S en B tal que, para cualquier $x \in S$,

$$f|_S(x) = f(x)$$

Funciones como relaciones

Hay otro punto de vista desde el cual se consideran las funciones. En primer lugar, toda función $f : A \to B$ origina una relación de A en B denominada *gráfica de f* y definida por

$$\text{Gráfica de } f = \{(a, b) \mid a \in A, b = f(a)\}$$

Dos funciones $f : A \to B$ y $g : A \to B$ se definen como *iguales*, lo que se escribe $f = g$, si $f(a) = g(a)$ para toda $a \in A$; es decir, si tienen la misma gráfica. En consecuencia, no se establece ninguna diferencia entre una función y su gráfica. Luego, este relación gráfica posee la propiedad de que cada a en A pertenece a un par ordenado único (a, b) en la relación. Por otra parte, cualquier relación f de A en B que tenga esta propiedad origina una función $f : A \to B$, donde $f(a) = b$ para todo (a, b) en f. En consecuencia, una forma equivalente de definir una función es:

Definición: Una función $f : A \to B$ es una relación de A en B (es decir, un subconjunto de $A \times B$) tal que cada $a \in A$ pertenece a un par ordenado único (a, b) en f.

Aunque no se establece ninguna diferencia entre una función y su gráfica se utilizará la terminología "gráfica de f" cuando se haga referencia a f como un conjunto de pares ordenados. Además, puesto que la gráfica de f es una relación, se representa como cualquier relación, y esta representación algunas veces se denomina gráfica de f. También, la condición definitoria de función, que cada $a \in A$ pertenece a un par único (a, b) en f, es equivalente a la condición geométrica de que cada línea recta vertical corta la gráfica exactamente en un punto.

EJEMPLO 3.2

a) Sea $f: A \to B$ la función definida en el ejemplo 3.1*b*). Entonces la gráfica de f es:

$$\{(a, s),\ (b, u),\ (c, r),\ (d, s)\}$$

b) Considere las tres relaciones siguientes sobre el conjunto $A = \{1, 2, 3\}$:

$$f = \{(1, 3),\ (2, 3),\ (3, 1)\}, \quad g = \{(1, 2),\ (3, 1)\}, \quad h = \{(1, 3),\ (2, 1),\ (1, 2),\ (3, 1)\}$$

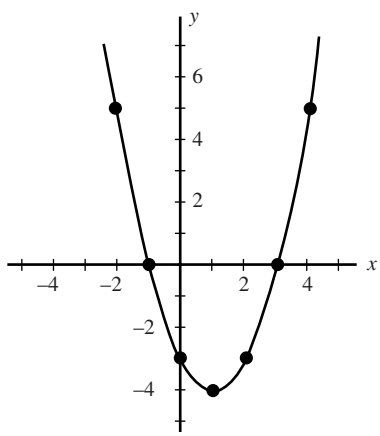
f es una función de A en A puesto que cada miembro de A aparece como primera coordenada exactamente en un único par ordenado en f; aquí $f(1) = 3$, $f(2) = 3$ y $f(3) = 1$. g no es una función de A en A puesto que $2 \in A$ no es la primera coordenada de algún par en g, de modo que g no asigna ninguna imagen a 2. Asimismo, h no es una función de A en A puesto que $1 \in A$ aparece como la primera coordenada de dos pares ordenados distintos en h: (1, 3) y (1, 2). Para que h sea una función, no debe asignar dos o más valores a un solo elemento, como en este caso 3 y 2 a $1 \in A$.

c) Por *función polinomial real* se entiende una función $f: \mathbf{R} \to \mathbf{R}$ de la forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde los a_i son números reales. Puesto que $\mathbf{R}$ es un conjunto infinito, sería imposible representar todos los puntos de la gráfica. No obstante, es posible aproximar la gráfica de esta función al dibujar algunos de sus puntos y luego se les une con una curva lisa. Los puntos se obtienen a partir de una tabla en la que se asignan varios valores a x y luego se calculan los valores correspondientes de $f(x)$. Esta técnica se ilustra en la figura 3-2 con la función $f(x) = x^2 - 2x - 3$.

x	$f(x)$
–2	5
–1	0
0	–3
1	–4
2	–3
3	0
4	5



Gráfica de $f(x) = x^2 - 2x - 3$

Figura 3-2

Composición de funciones

Considere las funciones $f: A \to B$ y $g: A \to B$; donde el codominio de f es el dominio de g. Entonces es posible definir una nueva función de A en C, la cual se denomina *composición* de f y g y se denota $g \circ f$:

$$(g \circ f)(a) \equiv g(f(a))$$

Es decir, se encuentra la imagen de a bajo f y luego se encuentra la imagen de $f(a)$ bajo g. Esta definición no es nueva. Si f y g se consideran relaciones, entonces es la misma función que en la composición de f y g como relaciones (vea la sección 2.6) excepto que aquí se usa la notación funcional $g \circ f$ para la composición de f y g en lugar de la notación $f \circ g$ que se usó para las relaciones.

Considere cualquier función $f: A \to B$. Entonces

$$f \circ 1_A = f \quad \text{y} \quad 1_B \circ f = f$$

donde 1_A y 1_B son las funciones identidad sobre A y B, respectivamente.

3.3 FUNCIONES UNO A UNO, SOBRE E INVERTIBLES

Se dice que una función $f: A \to B$ es *uno a uno* (que se escribe 1-1) si elementos diferentes en el dominio A tienen imágenes distintas. Otra forma de lo anterior es decir que f es *uno a uno* si $f(a) = f(a')$ implica $a = a'$.

Una función $f: A \to B$ se dice que es *sobre*, si cada elemento de B es la imagen de algún elemento de A. En otras palabras, $f: A \to B$ es sobre si la imagen de f es todo el codominio; es decir, si $f(A) = B$. En este caso se dice que f es una función de A sobre B, o que f mapea A sobre B.

Una función $f: A \to B$ es *invertible* si su relación inversa f^{-1} es una función de B a A. En general, la relación inversa f^{-1} puede no ser una función. El siguiente teorema proporciona ciertos criterios sencillos que indican cuándo ocurre lo anterior.

Teorema 3.1: Una función $f: A \to B$ es invertible si y sólo si f es uno a uno y sobre.

Si $f: A \to B$ es uno a uno y sobre, entonces f se denomina *correspondencia uno a uno* entre A y B. Esta terminología proviene del hecho de que a cada elemento de A le corresponde un único elemento de B y viceversa.

En algunos textos se usan los términos *inyectiva*, para indicar una función uno a uno, *suprayectiva*, para una función sobre, y *biyectiva*, para una correspondencia uno a uno.

EJEMPLO 3.3 Considere las funciones $f_1: A \to B$, $f_2: B \to C$, $f_3: C \to D$ y $f_4: D \to E$ definidas por el diagrama de la figura 3-3. Así, f_1 es uno a uno puesto que ningún elemento en B es la imagen de más de un elemento de A. En forma semejante, f_2 es uno a uno. Sin embargo, ni f_3 ni f_4 son uno a uno porque $f_3(r) = f_3(u)$ y $f_4(v) = f_4(w)$.

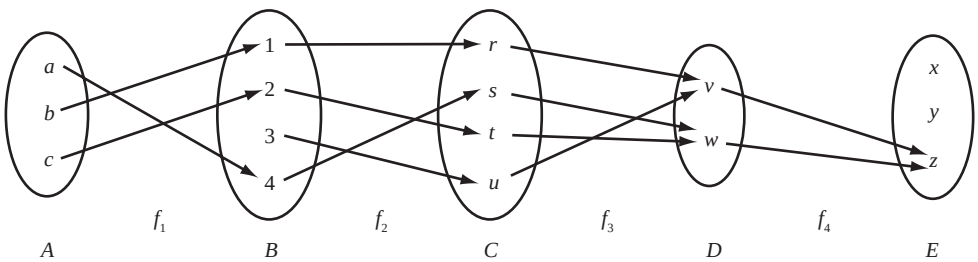


Figura 3-3

En relación con funciones sobre, las funciones f_2 y f_3 lo son, puesto que todo elemento de C es, bajo f_2, algún elemento de B, y todo elemento de D es, bajo f_3, algún elemento de C, $f_2(B) = C$ y $f_3(C) = D$. Por otra parte, f_1 no es sobre debido a que $3 \in B$ no es, bajo f_4, la imagen de algún elemento de A, y f_4 no es sobre, ya que $x \in E$ no es la imagen, bajo f_4, de algún elemento de D.

Así, f_1 es uno a uno pero no sobre; f_3 es sobre pero no uno a uno, y f_4 no es uno a uno ni sobre. Sin embargo, f_2 es tanto uno a uno como sobre, por lo que entre A y B hay una correspondencia uno a uno. Por tanto, f_2 es invertible y f_2^{-1} es una función de C en B.

Caracterización geométrica de funciones uno a uno y sobre

Ahora considere funciones de la forma $f: \mathbf{R} \to \mathbf{R}$. Puesto que las gráficas de tales funciones pueden trazarse en el plano cartesiano $\mathbf{R}^2$ y son funciones que se identifican con sus gráficas, surge la pregunta: ¿los conceptos uno a uno y sobre poseen algún significado geométrico? La respuesta es afirmativa. Sólo hay que especificar que:

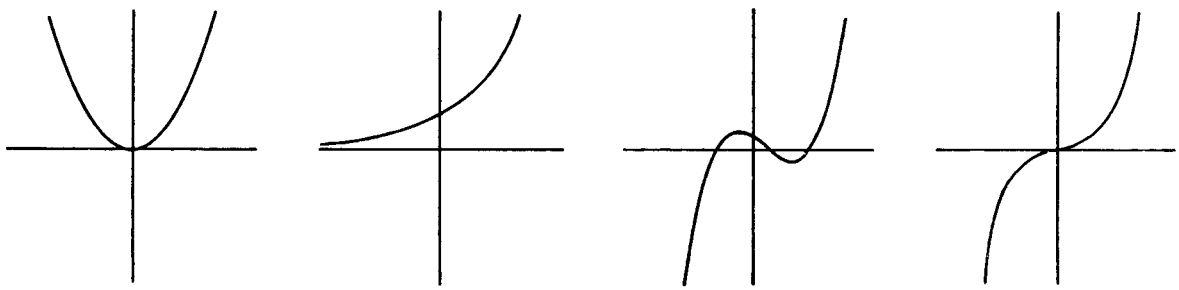
1) f: $\mathbf{R} \to \mathbf{R}$ es uno a uno, si cualquier línea horizontal corta la gráfica de f a lo más en un punto.
2) f: $\mathbf{R} \to \mathbf{R}$ es una función sobre, si cualquier línea horizontal corta la gráfica de f en uno o más puntos.

En consecuencia, si f es tanto uno a uno como sobre; es decir, invertible, entonces cualquier línea horizontal corta la gráfica de f exactamente en un punto.

EJEMPLO 3.4 Considere las cuatro siguientes funciones de **R** en **R**:

$$f_1(x) = x^2, \quad f_2(x) = 2^x, \quad f_3(x) = x^3 - 2x^2 - 5x + 6, \quad f_4(x) = x^3$$

Las gráficas de estas funciones se muestran en la figura 3-4. Observe que hay líneas horizontales que cortan dos veces la gráfica de f_1 y que hay líneas horizontales que no cortan la gráfica de f_1; por tanto, f_1 no es uno a uno ni sobre. En forma semejante, f_2 es uno a uno pero no sobre, f_3 es sobre pero no uno a uno y f_4 es tanto uno a uno como sobre. La inversa de f_4 es la función raíz cúbica; es decir, $f_4^{-1}(x) = \sqrt[3]{x}$.



$f_1(x) = x^2$ $f_2(x) = 2^x$ $f_3(x) = x^3 - 2x^2 - 5x + 6$ $f_4(x) = x^3$

Figura 3-4

Permutaciones

Una función invertible (biyectiva) σ: $X \to X$ se denomina *permutación* sobre X. La composición y las inversas de permutaciones sobre X y la función identidad sobre X también son permutaciones sobre X.

Suponga que $X = \{1, 2, \ldots, n\}$. Entonces una permutación σ sobre X se denota por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

donde $j_1 = \sigma(i)$. El conjunto de todas estas permutaciones se denota por S_n, y hay $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$ de ellas. Por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

son permutaciones en S_6, de las cuales hay $6! = 720$. Algunas veces sólo se escribe el segundo renglón de la permutación; es decir, las permutaciones antes mencionadas se denotan al escribir $\sigma = 462513$ y $\tau = 641325$.

3.4 FUNCIONES MATEMÁTICAS, FUNCIONES EXPONENCIAL Y LOGARÍTMICA

En esta sección se presentan varias funciones matemáticas que a menudo aparecen en el análisis de algoritmos y en computación, así como su notación. También se analizan las funciones exponencial y logarítmica, y su relación.

Funciones piso y techo

Sea x cualquier número real. Entonces x está entre dos enteros, uno piso y el otro techo de x. La simbología es

$\lfloor x \rfloor$, *piso* de x que denota el mayor entero que no excede a x.

$\lceil x \rceil$, *techo* de x que denota el menor entero que no es inferior a x.

Si x mismo es un entero, entonces $\lfloor x \rfloor = \lceil x \rceil$; en caso contrario, $\lfloor x \rfloor + 1 = \lceil x \rceil$. Por ejemplo,

$$\lfloor 3.14 \rfloor = 3, \quad \left\lfloor \sqrt{5} \right\rfloor = 2, \quad \lfloor -8.5 \rfloor = -9, \quad \lfloor 7 \rfloor = 7, \quad \lfloor -4 \rfloor = -4,$$

$$\lceil 3.14 \rceil = 4, \quad \left\lceil \sqrt{5} \right\rceil = 3, \quad \lceil -8.5 \rceil = -8, \quad \lceil 7 \rceil = 7, \quad \lceil -4 \rceil = -4$$

Funciones valor entero y valor absoluto

Sea x cualquier número real. El *valor entero* de x, escrito INT(x), convierte a x en un entero al eliminar (truncar) la parte fraccionaria del número. Así,

$$\text{INT}(3.14) = 3, \quad \text{INT}(\sqrt{5}) = 2, \quad \text{INT}(-8.5) = -8, \quad \text{INT}(7) = 7$$

Observe que INT(x) = $\lfloor x \rfloor$ o INT(x) = $\lceil x \rceil$, dependiendo de si x es positivo o negativo.

El *valor absoluto* del número real x, escrito ABS(x) o $|x|$, se define como el mayor de x o $-x$. Por tanto, ABS(0) = 0, y para $x \neq 0$, ABS(x) = x o ABS(x) = $-x$, dpendiendo de si x es positivo o negativo. Así

$$|-15| = 15, \quad |7| = 7, \quad |-3.33| = 3.33, \quad |4.44| = 4.44, \quad |-0.075| = 0.075$$

Observa que $|x| = |-x|$ y, para $x \neq 0$, $|x|$ es positivo.

Función residuo y aritmética modular

Sean k cualquier entero y M un entero positivo. Entonces

$$k \text{ (mód } M\text{)}$$

(que se lee: k módulo M) denota el residuo entero cuando M divide a k. Con mayor precisión, k (mód M) es el único entero r tal que

$$k = Mq + r \quad \text{donde} \quad 0 \leq r < M$$

Cuando k es positivo, para obtener el residuo r simplemente se divide k entre M. Así,

$$25 \text{ (mód } 7) = 4, \quad 25 \text{ (mód } 5) = 0, \quad 35 \text{ (mód } 11) = 2, \quad 3 \text{ (mód } 8) = 3$$

Si k es negativo, $|k|$ se divide entre M para obtener un residuo r'; entonces k (mód M) = $M - r'$ cuando $r' \neq 0$. Así,

$$-26 \text{ (mód } 7) = 7 - 5 = 2, \quad -371 \text{ (mód } 8) = 8 - 3 = 5, \quad -39 \text{ (mód } 3) = 0$$

El término "mód" también denota la relación matemática de congruencia, que se escribe y define:

$$a \equiv b \text{ (mód } M\text{)} \quad \text{si y sólo si} \quad M \text{ divide } b - a$$

M se denomina *módulo*, y $a \equiv b$ (mód M) se lee "a es congruente con b módulo M". Los siguientes aspectos de la relación de congruencia a menudo resultan útiles:

$$0 \equiv M \text{ (mód } M\text{)} \quad \text{y} \quad a \pm \text{M} \equiv a \text{ (mód } M\text{)}$$

La aritmética módulo M se refiere a las operaciones aritméticas de suma, multiplicación y sustracción donde el valor aritmético se sustituye por su valor equivalente en el conjunto

$$\{0, 1, 2, \ldots, M-1\} \quad \text{o en el conjunto} \quad \{1, 2, 3, \ldots, M\}$$

Por ejemplo, en aritmética módulo 12 o aritmética "del reloj", como algunas veces se le denomina,

$$6 + 9 \equiv 3, \quad 7 \times 5 \equiv 11, \quad 1 - 5 \equiv 8, \quad 2 + 10 \equiv 0 \equiv 12$$

(El uso de 0 o M depende de la aplicación.)

Funciones exponenciales

Recuerde las siguientes definiciones para exponentes enteros (donde m es un entero positivo):

$$a^m = a \cdot a \cdots a (m \text{ veces}), \quad a^0 = 1, \quad a^{-m} = \frac{1}{a^m}$$

Los exponentes se extienden para incluir todos los números racionales al definir, para cualquier número racional m/n,

$$a^{m/n} = \sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

Por ejemplo,

$$2^4 = 16, \quad 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \quad 125^{2/3} = 5^2 = 25$$

De hecho, los exponentes se extienden para incluir todos los números reales al definir, para cualquier número real x,

$$a^x = \lim_{r \to x} a^r, \quad \text{donde } r \text{ es un número racional}$$

En consecuencia, la función exponencial $f(x) = a^x$ está definida para todos los números reales.

Funciones logarítmicas

La relación de los logaritmos con los exponentes es como sigue. Sea b un número positivo. El logaritmo de cualquier número positivo x con base b se escribe

$$\log_b x$$

representa el exponente al que debe elevarse b para obtener x. Es decir,

$$y = \log_b x \quad \text{y} \quad b^y = x$$

son declaraciones equivalentes. Por consiguiente,

$$\begin{array}{llll} \log_2 8 = 3 & \text{puesto que} \quad 2^3 = 8; & \log_{10} 100 = 2 & \text{puesto que} \quad 10^2 = 100 \\ \log_2 64 = 6 & \text{puesto que} \quad 2^6 = 64; & \log_{10} 0.001 = -3 & \text{puesto que} \quad 10^{-3} = 0.001 \end{array}$$

Además, para cualquier base b, se tiene $b^0 = 1$ y $b^1 = b$, por tanto,

$$\log_b 1 = 0 \quad \text{y} \quad \log_b b = 1$$

El logaritmo de un número negativo y el logaritmo de 0 no están definidos.

A menudo los logaritmos se expresan con valores aproximados. Por ejemplo, si usa tablas o calculadora obtiene

$$\log_{10} 300 = 2.4771 \quad \text{y} \quad \log_e 40 = 3.6889$$

como respuestas aproximadas. (Aquí $e = 2.718281\ldots$)

Hay tres clases de logaritmos que revisten una importancia especial: los logaritmos base 10, *logaritmos comunes*; los logaritmos base *e*, *logaritmos naturales*; y los logaritmos base 2, *logaritmos binarios*. En algunos textos encontrará

$$\ln x \text{ para } \log_e x \quad \text{y} \quad \log x \text{ o } \log x \text{ para } \log_2 x$$

El término $\log x$ significa $\log_{10} x$, aunque en textos de matemáticas avanzadas también se usa para indicar $\log_e x$ y en textos de computación denota $\log_2 x$.

A menudo sólo requerirá el piso o el techo de un logaritmo binario. Lo que obtendrá al considerar las potencias de 2. Por ejemplo,

$$\lfloor \log_2 100 \rfloor = 6 \quad \text{puesto que} \quad 2^6 = 64 \quad \text{y} \quad 2^7 = 128$$
$$\lceil \log_2 1\,000 \rceil = 9 \quad \text{puesto que} \quad 2^8 = 512 \quad \text{y} \quad 2^9 = 1\,024$$

y así sucesivamente.

Relación entre las funciones exponencial y logarítmica

La relación básica entre las funciones exponencial y logarítmica

$$f(x) = b^x \quad \text{y} \quad g(x) = \log_b x$$

es que son inversas entre sí; por tanto, las gráficas de estas funciones tienen relación geométrica. Esta relación se ilustra en la figura 3-5, donde en el mismo sistema de ejes coordenados aparecen las gráficas de la función exponencial $f(x) = 2^x$, la función logarítmica $g(x) = \log_2 x$ y la función lineal $h(x) = x$. Puesto que $f(x) = 2^x$ y $g(x) = \log_2 x$ son funciones inversas, también son simétricas respecto a la función lineal $h(x) = x$ o, en otras palabras, la línea recta $y = x$.

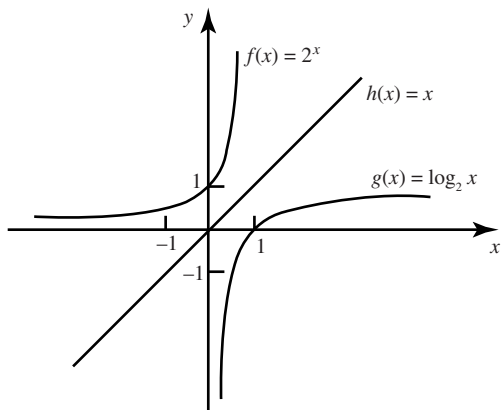


Figura 3-5

En la figura 3-5 también aparece otra propiedad importante de las funciones exponencial y logarítmica. En específico, para cualquier c positivo, se tiene

$$g(c) < h(c) < f(c), \quad \text{es decir,} \quad g(c) < c < f(c)$$

De hecho, a medida que aumenta el valor de c, también incrementa el valor de las distancias verticales $h(c) - g(c)$ y $f(c) - g(c)$. Además, la función logarítmica $g(x)$ tiene un crecimiento muy lento en comparación con la función lineal $h(x)$, y la función exponencial crece muy rápido en comparación con $h(x)$.

3.5 SUCESIONES, CLASES INDEXADAS DE CONJUNTOS

Las sucesiones y las clases indexadas de conjuntos son tipos de funciones especiales que tienen su propia notación. En esta sección se analizan estos objetos, así como la notación de sumatoria.

Sucesiones

Una *sucesión* es una función del conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de enteros positivos en un conjunto A. Para indicar la imagen del entero n se usa la notación a_n. Así, una sucesión suele denotarse por

$$a_1, a_2, a_3, \ldots \quad \text{o} \quad \{a_n : n \in \mathbf{N}\} \quad \text{o simplemente} \quad \{a_n\}$$

Algunas veces el dominio de una sucesión es el conjunto $\{0, 1, 2, \ldots\}$ de enteros no negativos, en lugar de $\mathbf{N}$. En este caso n empieza en 0 y no en 1.

Una *sucesión finita* sobre un conjunto A es una función de $\{1, 2, \ldots, m\}$ en A, y se denota con

$$a_1, a_2, \ldots, a_m$$

Algunas veces este tipo de sucesión finita se denomina *lista* o m-adas.

EJEMPLO 3.5

a) Las dos sucesiones siguientes son conocidas:

i) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ que puede definirse mediante $a_n = \frac{1}{n}$;

ii) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ que puede definirse mediante $b_n = 2^{-n}$

Observe que la primera sucesión empieza en $n = 1$ y que la segunda lo hace en $n = 0$.

b) La definición formal de la sucesión importante $1, -1, 1, -1, \ldots$, es

$$a_n = (-1)^{n+1} \quad \text{o, de manera equivalente, por} \quad b_n = (-1)^n$$

donde la primera sucesión empieza en $n = 1$ y la segunda lo hace en $n = 0$.

c) ***Cadenas*** Suponga que un conjunto A es finito y que A se considera como un conjunto de caracteres o un alfabeto. Entonces una sucesión finita sobre A se denomina *cadena* o *palabra*, la cual se escribe como $a_1a_2 \ldots a_m$, sin paréntesis. El número m de caracteres en la cadena se denomina su *longitud*. El conjunto con caracteres cero también es una cadena, que se denomina *cadena vacía* o *cadena nula*. Las cadenas sobre un alfabeto A y sus operaciones se analizarán con detalle en el capítulo 13.

Símbolo de sumatoria, sumas

Aquí se presenta el símbolo de sumatoria $\sum$ (la letra griega sigma). Considere una sucesión $a_1, a_2, a_3, \ldots$. Entonces se define lo siguiente:

$$\sum_{J=1}^{n} a_j = a_1 + a_2 + \cdots + a_n \quad \text{y} \quad \sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n$$

La letra j en las expresiones anteriores se denomina *índice mudo* o *variable ficticia*. Otras letras que suelen usarse como variables ficticias son i, k, s y t.

EJEMPLO 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

La última suma aparece muy a menudo. Su valor es $n(n + 1)/2$. Es decir,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \text{por ejemplo,} \quad 1 + 2 + \cdots + 50 = \frac{50(51)}{2} = 1\,275$$

Clases indexadas de conjuntos

Sea I cualquier conjunto no vacío, y sea S una colección de conjuntos. Una *función de indexación* de I a S es una función $f: I \to S$. Para cualquier $i \in I$, la imagen $f(i)$ se denota por A_i. Entonces, la función de indexación f suele denotarse por

$$\{A_i \mid i \in I\} \quad \text{o} \quad \{A_i\}_{i \in I} \quad \text{o simplemente} \quad \{A_i\}$$

El conjunto I se denomina *conjunto de indexación*, y los elementos de I se denominan *índices*. Si f es uno a uno y sobre, se dice que S está indexada por I.

Los conceptos de unión e intersección se definen para clases indexadas de conjuntos como sigue:

$$\cup_{i \in I} A_i = \{x \mid x \in A_i \text{ para alguna } i \in I\} \quad \text{y} \quad \cap_{i \in I} A_i = \{x \mid x \in A_i \text{ para toda } i \in I\}$$

Cuando I es un conjunto finito se tiene el mismo caso que en la definición previa de unión e intersección. Si I es $\mathbf{N}$, la unión e intersección se denotan, respectivamente, como sigue:

$$A_1 \cup A_2 \cup A_3 \cup \ldots \quad \text{y} \quad A_1 \cap A_2 \cap A_3 \cap \ldots$$

EJEMPLO 3.7 Sea I el conjunto $\mathbf{Z}$ de los enteros. Para cada $n \in \mathbf{Z}$ se asigna el siguiente intervalo infinito en $\mathbf{R}$:

$$A_n = \{x \mid x \leq n\} = (-\infty, n]$$

Para cualquier número real a, existen enteros n_1 y n_2 tales que $n_1 < a < n_2$; así, $a \in A_{n2}$ pero $a \notin A_{n1}$. Por tanto

$$a \in \cup_n A_n \quad \text{pero} \quad a \notin \cap_n A_n$$

En consecuencia,

$$\cup_n A_n = \mathbf{R} \quad \text{pero} \quad \cap_n A_n = \varnothing$$

3.6 FUNCIONES DEFINIDAS EN FORMA RECURSIVA

Se dice que una *función está definida en forma recursiva* si la definición de la función se refiere a sí misma. Para que la definición no sea circular, la definición de la función debe poseer las dos propiedades siguientes:

1) Debe haber ciertos argumentos, que se denominan *valores base*, en los que la función no se refiera a sí misma.
2) Cada vez que la función se refiere a sí misma, el argumento de la función debe estar más próximo a un valor base.

Se dice que una función recursiva con estas dos propiedades está *bien definida*.

Los ejemplos siguientes aclaran estas ideas.

Función factorial

El producto de los enteros positivos desde 1 hasta n, inclusive, se denomina "n factorial", y se denota con $n!$ Es decir,

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$$

También resulta conveniente definir $0! = 1$, de modo que la función esté definida para todos los enteros no negativos. Así:

$$0! = 1, \quad 1! = 1, \quad 2! = 2 \cdot 1 = 2, \quad 3! = 3 \cdot 2 \cdot 1 = 6, \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120, \quad 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

Y así sucesivamente. Observe que

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \quad \text{y} \quad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

Esto es cierto para todo entero positivo n; es decir,

$$n! = n \cdot (n - 1)!$$

En consecuencia, la función factorial también se define como:

Definición 3.1 (función factorial):

a) Si $n = 0$, entonces $n! = 1$.
b) Si $n > 0$, entonces $n! = n \cdot (n - 1)!$

Observe que la definición anterior de $n!$ es recursiva, ya que se refiere a sí misma cuando usa $(n - 1)!$ Sin embargo:

1) El valor de $n!$ se proporciona explícitamente cuando $n = 0$ (así, 0 es un valor base).
2) El valor de $n!$ para una n arbitraria está en términos de un valor menor que n, más próximo al valor base 0.

Por consiguiente, la definición no es circular o, en otras palabras, la función está bien definida.

EJEMPLO 3.8 En la figura 3-6 aparecen los nueve pasos para calcular 4! mediante la definición recursiva:

Paso 1. Aquí se define 4! en términos de 3!, de modo que es necesario retrasar la evaluación de 4! hasta que se evalúe 3! Este retraso se indica al sangrar el paso siguiente.

Paso 2. Aquí se define 3! en términos de 2!, de modo que es necesario retrasar la evaluación de 3! hasta que se evalúe 2!

Paso 3. Aquí se define 2! en términos de 1!

Paso 4. Aquí se define 1! en términos de 0!

Paso 5. En este paso es posible evaluar explícitamente 0!, ya que 0 es el valor base de la definición recursiva.

Pasos 6 a 9. Hay que retroceder, use 0! para encontrar 1!, use 1! para encontrar 2!, use 2! para encontrar 3! y, por último, use 3! para encontrar 4! Este procedimiento se indica con el sangrado "inverso".

Observe que este procedimiento se lleva a cabo en orden inverso a las evaluaciones originales que fueron retrasadas.

(1) $4! = 4 \cdot 3!$
(2) $3! = 3 \cdot 2!$
(3) $2! = 2 \cdot 1!$
(4) $1! = 1 \cdot 0!$
(5) $0! = 1$
(6) $1! = 1 \cdot 1 = 1$
(7) $2! = 2 \cdot 1 = 2$
(8) $3! = 3 \cdot 2 = 6$
(9) $4! = 4 \cdot 6 = 24$

Figura 3-6

Números de nivel

Sea P un procedimiento o una fórmula recursiva que se usa para evaluar $f(X)$, donde f es una función recursiva y X es la entrada. Con cada ejecución de P se asocia un *número de nivel*: a la ejecución inicial de P se asigna el nivel 1; y cada vez que se ejecuta P debido a una llamada recursiva, su nivel es una unidad mayor que el nivel de la ejecución que hizo la llamada recursiva. La *profundidad* de la recursión al evaluar $f(X)$ se refiere al máximo número de nivel de P durante su ejecución.

Así, considere la evaluación de 4! en el ejemplo 3.8, donde se usa la fórmula recursiva $n! = n(n-1)!$ El paso 1 pertenece al nivel 1 porque es la primera ejecución de la fórmula. Entonces,

El paso 2 pertenece al nivel 2; el paso 3 pertenece al nivel 3, ...; el paso 5 pertenece al nivel 5.

Por otra parte, el paso 6 pertenece al nivel 4 porque es resultado de un regreso desde el nivel 5. En otras palabras, el paso 6 y el paso 4 pertenecen al mismo nivel de ejecución. En forma semejante,

El paso 7 pertenece al nivel 3; el paso 8 al nivel 2; y el paso 9 al nivel 1.

En consecuencia, al evaluar 4!, la profundidad de la recursión es 5.

Sucesión de Fibonacci

La famosa sucesión de Fibonacci (que se denota con $F_0, F_1, F_2, \ldots$) es:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \quad \ldots$$

Es decir, $F_0 = 0$ y $F_1 = 1$ y cada término sucesivo es la suma de los dos términos precedentes. Por ejemplo, los dos términos siguientes de la sucesión son

$$34 + 55 = 89 \quad \text{y} \quad 55 + 89 = 144$$

A continuación se presenta una definición formal de esta función:

Definición 3.2 (sucesión de Fibonacci):

a) Si $n = 0$, o $n = 1$, entonces $F_n = n$.
b) Si $n > 0$, entonces $F_{n-2} + F_{n-1}$.

Es otro ejemplo de definición recursiva, ya que la definición se refiere a sí misma cuando usa F_{n-2} y F_{n-1}. No obstante:

1) Los valores base son 0 y 1.
2) El valor de F_n está en términos de valores menores que n, más próximos a los valores base.

En consecuencia, esta función está bien definida.

Función de Ackermann

Esta función cuenta con dos argumentos, a cada uno de los cuales es posible asignar cualquier entero no negativo; es decir, 0, 1, 2, ... Esta función se define como:

Definición 3.3 (función de Ackermann):

a) Si $m = 0$, entonces $A(m, n) = n + 1$.
b) Si $m \neq 0$ pero $n = 0$, entonces $A(m, n) = A(m - 1, 1)$.
c) Si $m \neq 0$ y $n \neq 0$, entonces $A(m, n) = A(m - 1, A(m, n - 1))$.

Una vez más, se trata de una definición recursiva, ya que se refiere a sí misma en los incisos *b*) y *c*). Observe que $A(m, n)$ sólo se proporciona de manera explícita cuando $m = 0$. Los valores base son los pares

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (0, 3), \quad \ldots, (0, n), \quad \ldots$$

Aunque no es evidente a partir de la definición, el valor de cualquier $A(m, n)$ se expresa al final en términos del valor de la función sobre uno o más de los pares base.

El valor de $A(1, 3)$ se calcula en el problema 3.21. Inclusive este simple caso requiere 15 pasos. En términos generales, la función de Ackermann es demasiado complicada de evaluar en cualquier ejemplo, excepto en uno trivial. La importancia de esta función proviene de su uso en lógica matemática, y se plantea aquí esencialmente para proporcionar otro ejemplo de una función recursiva clásica y mostrar que la parte recursiva de una definición puede ser complicada.

3.7 CARDINALIDAD

Se dice que dos conjuntos A y B son *equipotentes*, tienen el *mismo número de elementos* o *la misma cardinalidad*, que se escribe $A \simeq B$, si existe una correspondencia uno a uno $f: A \to B$. Un conjunto A es *finito* si A es vacío o si A tiene la misma cardinalidad que el conjunto $\{1, 2, \ldots, n\}$ para algún entero positivo n. Un conjunto es *infinito* si no es finito. Ejemplos familiares de conjuntos infinitos son los números naturales **N**, los enteros **Z**, los números racionales **Q** y los números reales **R**.

Ahora se presenta el concepto de "números cardinales". Son números que se considerarán como símbolos asignados a conjuntos de modo que a dos conjuntos se les asigna el mismo símbolo si y sólo si tienen la misma cardinalidad. El número cardinal de un conjunto A se denota por $|A|$, $n(A)$ o card(A). Aquí se usará $|A|$.

Para indicar la cardinalidad de conjuntos finitos se utilizan símbolos obvios. Es decir, al conjunto vacío $\varnothing$ se asigna 0, y al conjunto $\{1, 2, \ldots, n\}$ se asigna n. Así, $|A| = n$ si y sólo si A tiene n elementos. Por ejemplo,

$$|\{x, y, z\}| = 3 \quad \text{y} \quad |\{1, 3, 5, 7, 9\}| = 5$$

El número cardinal del conjunto infinito **N** de enteros positivos es $\aleph_0$ ("aleph-nada" o "aleph-cero"). Este símbolo fue introducido por Cantor. Así, $|A| = \aleph_0$ si y sólo si A tiene la misma cardinalidad que **N**.

EJEMPLO 3.9 Sea $E = \{2, 4, 6, \ldots\}$ el conjunto de enteros positivos pares. La función $f: \mathbf{N} \to E$ definida por $f(n) = 2n$ es una correspondencia uno a uno entre los enteros positivos N y E. Por tanto, E tiene la misma cardinalidad que **N**, de modo que es posible escribir

$$|E| = \aleph_0$$

Un conjunto con cardinalidad $\aleph_0$ es *enumerable* o *infinito numerable*. Un conjunto que es finito o enumerable es *numerable*. Puede demostrarse que el conjunto **Q** de números racionales es numerable. De hecho, se tiene el siguiente teorema (que se demuestra en el problema 3.13), que se usará ulteriormente.

Teorema 3.2: La unión numerable de conjuntos numerables es numerable.

Es decir, si cada conjunto $A_1, A_2, \ldots$ es numerable, entonces la siguiente unión es numerable:

$$A_1 \cup A_2 \cup A_3 \cup \ldots$$

Un ejemplo importante de un conjunto infinito que es innumerable, que no es numerable, lo proporciona el siguiente teorema, que se demuestra en el problema 3.14.

Teorema 3.3: El conjunto **I** de todos los números reales entre 0 y 1 es no numerable.

Desigualdades y números cardinales

A menudo es necesario comparar el tamaño de dos conjuntos. Esto se hace mediante una relación de desigualdad que para los números cardinales se define como: para dos conjuntos A y B arbitrarios, $|A| \leq |B|$ si existe una función $f: A \to B$ que es uno a uno. También se escribe

$$|A| < |B| \quad \text{si} \quad |A| \leq |B| \quad \text{pero} \quad |A| \neq |B|$$

Por ejemplo, $|\mathbf{N}| < |\mathbf{I}|$, donde $\mathbf{I} = \{x: 0 \leq x \leq 1\}$, ya que la función $f: \mathbf{N} \to \mathbf{I}$ definida por $f(n) = 1/n$ es uno a uno, pero $|\mathbf{N}| \neq |\mathbf{I}|$ por el teorema 3.3.

El teorema de Cantor, que se presenta a continuación y se demuestra en el problema 3.25, establece que los números cardinales no están acotados.

Teorema 3.4 (de Cantor): Para cualquier conjunto A, se tiene $|A| < |\text{Potencia}(A)|$ (donde Potencia(A) es el conjunto potencia de A, la colección de todos los subconjuntos de A).

El siguiente teorema establece que la relación de desigualdad para números cardinales es antisimétrica.

Teorema 3.5 (de Schroeder-Bernstein): Suponga que A y B son conjuntos tales que

$$|A| \leq |B| \quad \text{y} \quad |B| \leq |A|$$

Entonces $|A| = |B|$.

En el problema 3.26 se demuestra un planteamiento equivalente de este teorema.

3.8 ALGORITMOS Y FUNCIONES

Un algoritmo M es una lista paso a paso finita de instrucciones bien definidas para resolver un problema particular; por ejemplo, encontrar el resultado $f(X)$ para una función dada f con entrada X. (Aquí X puede ser una lista de valores.) Con frecuencia puede haber más de una forma de obtener $f(X)$, como ilustran los siguientes ejemplos. La elección particular del algoritmo M para obtener $f(X)$ puede depender de la "eficiencia" o "complejidad" del algoritmo; esta cuestión de la complejidad de un algoritmo M se analiza formalmente en la siguiente sección.

EJEMPLO 3.10 (Evaluación polinomial) Suponga, para un polinomio dado, $f(x)$ y un valor $x = a$, que se desea encontrar $f(a)$; por ejemplo,

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \quad \text{y} \quad a = 5$$

Esto puede hacerse en las dos formas siguientes.

a) **(*Método directo*):** Aquí, $a = 5$ se sustituye directamente en el polinomio para obtener

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe que hay 3 + 2 + 1 = 6 multiplicaciones y 3 adiciones. En general, la evaluación de un polinomio de grado n directamente requiere de manera aproximada

$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2} \text{ multiplicaciones y } n \text{ adiciones.}$$

b) **(*Método de Horner o división sintética*):** Aquí se vuelve a escribir el polinomio al factorizar sucesivamente x (a la derecha) como sigue:

$$f(x) = (2x^2 - 7x + 4)x - 15 = ((2x - 7)x + 4)x - 15$$

Entonces

$$f(5) = ((3)5 + 4)5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

Para quienes conocen la división sintética, los pasos aritméticos anteriores son equivalentes a la siguiente división sintética:

$$\begin{array}{r|cccccc} 5 & 2 & - & 7 & + & 4 & - & 15 \\ & & & 10 & + & 15 & + & 95 \\ \hline & 2 & + & 3 & + & 19 & + & 80 \end{array}$$

Observe que hay 3 multiplicaciones y 3 adiciones. En general, la evaluación de un polinomio de grado n con el método de Horner requiere aproximadamente

$$n \text{ multiplicaciones y } n \text{ adiciones}$$

Resulta evidente que el método de Horner *b*) es más eficiente que el método directo *a*).

EJEMPLO 3.11 (Máximo común divisor) Sean a y b enteros positivos tales que, por ejemplo, $b < a$; y suponga que desea encontrar $d = \text{MCD}(a, b)$, el máximo común divisor de a y b. Esto puede hacerse en las dos formas siguientes.

a) **(*Método directo*):** Aquí se encuentran todos los divisores de a; por ejemplo, se prueban todos los números desde 2 hasta $a/2$, así como todos los divisores de b. Luego se elige el máximo común divisor. Por ejemplo, suponga que $a = 258$ y $b = 60$. Los divisores de a y b son:

$a = 258$; divisores: 1, 2, 3, 6, 86, 129, 258
$a = 60$; divisores: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

En consecuencia, $d = \text{MCD}(258, 60) = 6$.

b) **(*Algoritmo euclidiano*):** Aquí se divide a entre b para obtener el residuo r_1. (Observe que $r_1 < b$.) Luego, b se divide entre el residuo r_1 para obtener un segundo residuo r_2. (Observe que $r_2 < r_1$.) Ahora, r_1 se divide entre r_2 para obtener un tercer residuo r_3. (Observe que $r_3 < r_2$.). Se continúa hasta dividir r_k entre r_{k+1} para obtener un residuo r_{k+2}. Puesto que

$$a > b > r_1 > r_2 > r_3 \ldots \qquad (*)$$

finalmente se obtiene el residuo $r_m = 0$. Entonces $r_{m-1} = \text{MCD}(a, b)$. Por ejemplo, suponga que $a = 258$ y $b = 60$. Entonces:

1) Al dividir $a = 258$ entre $b = 60$ se obtiene el residuo $r_1 = 18$.
2) Al dividir $b = 60$ entre $r_1 = 18$ se obtiene el residuo $r_2 = 6$.
3) Al dividir $r_1 = 18$ entre $r_2 = 6$ se obtiene el residuo $r_3 = 0$.

Así, $r_2 = 6 = \text{MCD}(258, 60)$.

El algoritmo euclidiano constituye una forma muy eficiente de encontrar el MCD de dos enteros positivos a y b. El hecho de que el algoritmo termina se concluye a partir de $(*)$. El hecho de que el algoritmo produce $d = \text{MCD}(a, b)$ no es evidente; este hecho se analizará en la sección 11.6.

3.9 COMPLEJIDAD DE LOS ALGORITMOS

El análisis de algoritmos constituye una tarea fundamental en computación, ya que para comparar algoritmos se requieren algunos criterios que midan su eficiencia. En esta sección se aborda este importante tema.

Suponga que M es un algoritmo y que n es el tamaño de los datos de entrada. El tiempo y el espacio que utiliza el algoritmo constituyen las dos medidas primordiales de la eficiencia de M. El tiempo se mide al contar el número de "operaciones clave"; por ejemplo:

a) Al ordenar y buscar se cuenta el número de comparaciones.

b) En aritmética, se cuentan las multiplicaciones y se omiten las adiciones.

Las operaciones clave se definen así cuando el tiempo para efectuar las otras operaciones es mucho menor que o es proporcional al tiempo para realizar las operaciones clave. El espacio se mide al contar el máximo de memoria necesaria para el algoritmo.

La *complejidad* de un algoritmo M es la función $f(n)$ que proporciona el requisito de tiempo de ejecución y/o espacio de almacenamiento del algoritmo en términos del tamaño n de los datos de entrada. A menudo, el espacio de almacenamiento requerido por el algoritmo es un simple múltiplo del tamaño de los datos. En consecuencia, a menos que se establezca o implique otra cosa, el término "complejidad" se refiere al tiempo de ejecución del algoritmo.

La función de complejidad $f(n)$, que se supone proporciona el tiempo de ejecución de un algoritmo, suele depender no sólo del tamaño n de los datos de entrada, sino también de los datos particulares. Por ejemplo, suponga que en un breve relato TEXT en inglés, se desea buscar la primera aparición de una palabra W de tres letras. Resulta evidente que si W es la palabra de tres letras "the", entonces es probable que W ocurra al principio de TEXT, de modo que $f(n)$ será pequeña. Por otra parte, si W es la palabra de tres letras "zoo", entonces tal vez W no aparezca en absoluto en TEXT, de modo que $f(n)$ será grande.

El análisis anterior origina el problema de encontrar la función de complejidad $f(n)$ para ciertos casos. Los dos casos que se suelen investigar en teoría de la complejidad son:

1) *Peor caso*: el valor máximo de $f(n)$ para cualquier entrada posible.
2) *Caso promedio*: el valor esperado de $f(n)$.

El análisis del caso promedio supone una cierta distribución probabilística para los datos de entrada; un supuesto posible podría ser que las permutaciones posibles de un conjunto de datos son equiprobables. El caso promedio también usa el siguiente concepto en teoría de probabilidad. Suponga que los números $n_1, n_2, \ldots, n_k$ ocurren con probabilidades respectivas $p_1, p_2, \ldots, p_k$. Entonces la *expectativa* (o *esperanza matemática*) o *valor medio E* está dado por

$$E = n_1 p_1 + n_2 p_2 + \cdots + n_k p_k$$

Estas ideas se ilustran a continuación.

Búsqueda lineal

Suponga que un arreglo lineal DATA contiene n elementos y que se proporciona un ITEM específico de información. Lo que se desea encontrar es la ubicación LOC de ITEM en el arreglo DATA, o enviar algún mensaje, como LOC = 0, para indicar que ITEM no aparece en DATA. El algoritmo de búsqueda lineal resuelve este problema al comparar ITEM, uno por uno, con cada elemento de DATA. Es decir, ITEM se compara con DATA[1], luego con DATA[2], y así sucesivamentese continúa, hasta que se encuentra LOC tal que ITEM = DATA[LOC].

La complejidad del algoritmo de búsqueda está dada por el número C de comparaciones entre ITEM y DATA[K]. Se busca $C(n)$ para el peor caso y para el caso promedio.

1) ***Peor caso*:** resulta evidente que el peor caso ocurre cuando ITEM es el último elemento en el arreglo DATA o no se encuentra ahí en absoluto. En cualquier situación se tiene

$$C(n) = n$$

En consecuencia, $C(n) = n$ es la complejidad del peor caso del algoritmo de búsqueda lineal.

2) ***Caso promedio*:** aquí se supone que ITEM aparece en DATA, y que tiene igual probabilidad de ocurrencia en cualquier posición del arreglo. Por consiguiente, el número de comparaciones puede ser cualquiera de los números 1, 2, 3, …, n, y cada número ocurre con probabilidad $p = 1/n$. Entonces

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

Esto coincide con la idea intuitiva de que el número medio de comparaciones necesarias para encontrar la ubicación de ITEM es aproximadamente igual a la mitad del número de elementos en la lista DATA.

Observación: El análisis de la complejidad del caso promedio de un algoritmo suele ser mucho más difícil que el del peor caso. Además, la distribución probabilística que se supone para el caso promedio tal vez no sea válida para situaciones reales. En consecuencia, a menos que se establezca o implique otra cosa, la complejidad de un algoritmo significará la función que proporciona el tiempo de ejecución del peor caso en términos del tamaño de los datos de entrada. Este supuesto no es demasiado sólido, ya que la complejidad del caso promedio para muchos algoritmos es proporcional a la complejidad del peor caso.

Tasa (o razón) de crecimiento: notación *O* grande

Suponga que M es un algoritmo y que n es el tamaño de los datos de entrada. Resulta evidente que la complejidad $f(n)$ de M crece cuando n aumenta; por lo que el análisis más común es la tasa o razón de crecimiento de $f(n)$, que se obtiene al comparar $f(n)$ con alguna función estándar, como

$$\log n, \quad n, \quad n \log n, \quad n^2, \quad n^3, \quad 2^n$$

Las razones de crecimiento para estas funciones estándar aparecen en la figura 3-7, que proporciona sus valores aproximados para ciertos valores de n. Observe que las funciones se presentan en orden ascendente de sus razones de crecimiento: la función logarítmica $\log_2 n$ crece más lentamente, la función exponencial 2^n crece más rápido, y las funciones polinomiales n^c crecen según el exponente c.

n \ $g(n)$	$\log n$	n	$n \log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1 000	10	10^3	10^4	10^6	10^9	10^{300}

Figura 3-7 Tasa de crecimiento de funciones estándar

La forma de comparar la función de complejidad $f(n)$ con una de las funciones estándar es mediante la notación funcional "*O* grande "; a continuación se da su definición formal:

Definición 3.4: Sean $f(x)$ y $g(x)$ funciones arbitrarias definidas sobre **R** o un subconjunto de **R**. Si "$f(x)$ es de orden $g(x)$", se escribe como

$$f(x) = O(g(x))$$

si existen un número real k y una constante positiva C tales que, para toda $x > k$, se tiene

$$|f(x)| \leq C|g(x)|$$

En otras palabras, $f(x) = O(g(x))$ si un múltiplo constante de $|g(x)|$ excede a $|f(x)|$ para toda x mayor que algún número real k.

También se escribe:

$$f(x) = h(x) + O(g(x)) \quad \text{cuando} \quad f(x) - h(x) = O(g(x))$$

(Lo anterior se denomina notación "*O* grande " puesto que el significado de $f(x) = o(g(x))$ es completamente diferente.)

Ahora considere un polinomio $P(x)$ de grado m. En el problema 3.24 se demuestra que $P(x) = O(x^m)$.

Así, por ejemplo,

$$7x^2 - 9x + 4 = O(x^2) \quad \text{y} \quad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

Complejidad de algoritmos bien conocidos

Si se supone que $f(n)$ y $g(n)$ son funciones definidas sobre los enteros positivos, entonces

$$f(n) = O(g(n))$$

significa que $f(n)$ está acotada para un múltiplo constante de $g(n)$ para casi toda n.

Para indicar la conveniencia de esta notación se proporciona la complejidad de ciertos algoritmos de búsqueda y ordenamiento bien conocidos en computación:

a) Búsqueda lineal: $O(n)$

b) Búsqueda binaria: $O(\log n)$

c) Ordenamiento burbuja: $O(n^2)$

d) Ordenamiento por mezcla: $O(n \log n)$

PROBLEMAS RESUELTOS

FUNCIONES

3.1 Sea $X = \{1, 2, 3, 4\}$. Determine si cada relación sobre X es una función de X en X.

a) $f = \{(2, 3), (1, 4), (2, 1), (3, 2), (4, 4)\}$
b) $g = \{(3, 1), (4, 2), (1, 1)\}$
c) $h = \{(2, 1), (3, 4), (1, 4), (2, 1), (4, 4)\}$

Recuerde que un subconjunto f de $X \times X$ es una función $f: X \to X$ si y sólo si cada $a \in X$ aparece como primera coordenada en exactamente un par ordenado en f.

a) No. Dos pares ordenados diferentes (2, 3) y (2, 1) en f tienen el mismo número, 2, como su primera coordenada.

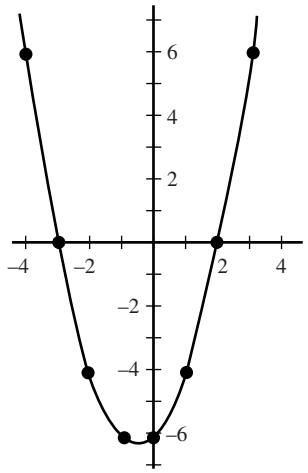
b) No. El elemento $2 \in X$ no aparece como la primera coordenada en ningún par ordenado en g.

c) Sí. Aunque $2 \in X$ aparece como la primera coordenada en dos pares ordenados en h, estos pares ordenados son iguales.

3.2 Dibuje la gráfica de: *a*) $f(x) = x^2 + x - 6$; *b*) $g(x) = x^3 - 3x^2 - x + 3$.

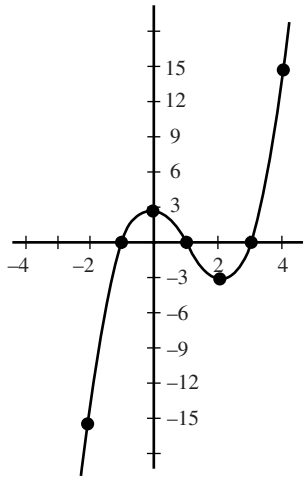
Se hace una tabla de valores para x y luego se encuentran los valores correspondientes de la función. Puesto que las funciones son polinomios, los puntos se trazan en un sistema de coordenadas y luego se dibuja una curva lisa continua que pase por los puntos. Vea la figura 3-8.

x	$f(x)$
–4	6
–3	0
–2	–4
–1	–6
0	–6
1	–4
2	0
3	6



Gráfica de $f = x^2 + x - 6$

x	$g(x)$
–2	–15
–1	0
0	3
1	0
2	–3
3	0
4	–15



Gráfica de $g = x^3 - 3x^2 - x + 3$

Figura 3-8

3.3. Sea $A = \{a, b, c\}$, $B = \{x, y, z\}$, $C = \{r, s, t\}$. Sean $f: A \to B$ y $g: B \to C$ definidas por:

$$f = \{(a, y)(b, x), (c, y)\} \quad \text{y} \quad g = \{(x, s), (y, t), (z, r)\}.$$

Encuentre: *a*) la composición de funciones $g \circ f: A \to C$; *b*) $\text{Im}(f)$, $\text{Im}(g)$, $\text{Im}(g \circ f)$.

a) Use la definición de composición de funciones para calcular:

$$(g \circ f)(a) = g(f(a)) = g(y) = t$$
$$(g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

Es decir $g \circ f = \{(a, t), (b, s), (c, t)\}$.

b) Obtenemos los puntos imagen (o segundas coordenadas):

$$\text{Im}(f) = \{x, y\}, \quad \text{Im}(g) = \{r, s, t\}, \quad \text{Im}(g \circ f) = \{s, t\}$$

3.4 Sean f: $\mathbf{R} \to \mathbf{R}$ y g: $\mathbf{R} \to \mathbf{R}$ definidas por $f(x) = 2x + 1$ y $g(x) = x^2 - 2$. Encuentre la fórmula para la composición de funciones $g \circ f$.

$g \circ f$ se calcula como sigue: $(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$.
Observe que se obtiene la misma respuesta al escribir

$$y = f(x) = 2x + 1 \quad \text{y} \quad z = g(y) = y^2 - 2$$

y luego se elimina y de ambas ecuaciones:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

FUNCIONES UNO A UNO, SOBRE E INVERTIBLES

3.5. Sean las funciones f: $A \to B$, g: $B \to C$, h: $C \to D$ definidas por la figura 3-9. Determine si cada función es: *a*) sobre, *b*) uno a uno, *c*) invertible.

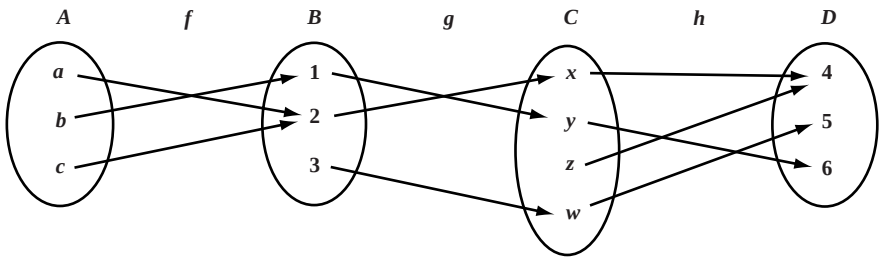


Figura 3-9

a) La función f: $A \to B$ no es sobre puesto que $3 \in B$ no es la imagen de ningún elemento en A.
La función g: $B \to C$ no es sobre puesto que $z \in C$ no es la imagen de ningún elemento en B.
La función h: $C \to D$ es sobre puesto que todo elemento en D es la imagen de algún elemento de C.

b) La función f: $A \to B$ no es uno a uno puesto que a y b tienen la misma imagen, 2.
La función g: $B \to C$ es uno a uno puesto que 1, 2 y 3 tienen imágenes distintas.
La función h: $C \to D$ no es uno a uno, ya que x y z tienen la misma imagen, 4.

c) Ninguna función es uno a uno ni sobre; por tanto, ninguna función es invertible.

3.6 Considere las permutaciones $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$ y $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$ en S_6.

Encuentre: *a*) la composición $\tau \circ \sigma$; *b*) σ^{-1}.

a) Observe que σ manda el 1 en el 3 y que τ manda el 3 en el 6. Así que la composición $\tau \circ \sigma$ manda 1 a 6. Es decir $(\tau \circ \sigma)(1) = 6$. Además, $\tau \circ \sigma$ manda el 2 en el 6 en el 1; es decir, $(\tau \circ \sigma)(2) = 1$. En forma semejante,

$$\text{m } (\tau \circ \sigma)(3) = 5, \quad (\tau \circ \sigma)(4) = 3, \quad (\tau \circ \sigma) = 2, \quad (\tau \circ \sigma)(6) = 4$$

Así,

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 2 & 4 \end{pmatrix}$$

b) El 1 se busca en el segundo renglón de σ. Observe que σ manda el 5 en el 1. Por tanto, $\sigma^{-1}(1) = 5$. El 2 se busca en el segundo renglón de σ. Observe que σ manda el 6 en el 2. Por tanto, $\sigma^{-1}(2) = 6$. En forma semejante, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$, $\sigma^{-1}(5) = 4$, $\sigma^{-1}(6) = 2$. Así,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}$$

3.7 Considere las funciones $f: A \to B$ y $g: B \to C$. Demuestre lo siguiente:

a) Si f y g son uno a uno, entonces la composición de funciones $g \circ f$ es uno a uno.
b) Si f y g son funciones sobre, entonces $g \circ f$ es una función sobre.

a) Suponga $(g \circ f)(x) = (g \circ f)(y)$ entonces $g(f(x)) = g(f(y))$. Así, $f(x) = f(y)$ porque g es uno a uno. Además, $x = y$ porque f es uno a uno. En consecuencia, $g \circ f$ es uno a uno.

b) Sea c cualquier elemento arbitrario de C. Puesto que g es sobre, existe una $b \in B$ tal que $g(b) = c$. Como f es sobre, existe una $a \in A$ tal que $f(a) = b$. Pero entonces

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Por tanto, todo $c \in C$ es la imagen de algún elemento $a \in A$. En consecuencia, $g \circ f$ es una función sobre.

3.8 Sea $f: \mathbf{R} \to \mathbf{R}$ definida por $f(x) = 2x - 3$. Ahora f es uno a uno y sobre; por tanto, f tiene una función inversa f^{-1}. Encuentre una formula para f^{-1}.

Sea y la imagen de x bajo la función f:

$$y = f(x) = 2x - 3$$

Por consiguiente, x es la imagen de y bajo la función inversa f^{-1}. Se despeja x en términos de y en la ecuación anterior:

$$x = (y + 3)/2$$

Entonces $f^{-1}(y) = (y + 3)/2$; y se sustituye por x para obtener

$$f^{-1}(x) = \frac{x + 3}{2}$$

que es la fórmula para f^{-1} con la variable independiente x de costumbre.

3.9 Demuestre la siguiente generalización de la ley de DeMorgan: Para cualquier clase de conjuntos $\{A_i\}$ se tiene

$$(\cup_i A_i)^c = \cap_i A_i^c$$

Se tiene:

$$x \in (\cup_i A_i)^c \quad \text{sii } x \notin \cup_i A_i, \quad \text{sii } \forall_i \in I, x \notin A_i, \quad \text{sii } \forall_i \in I, x \in A_i^c, \quad \text{sii } x \in \cap_i A_i^c$$

En consecuencia, $(\cup_i A_i)^c = \cap_i A_i^c$. (Aquí se han usado las notaciones lógicas sii por "si y sólo si" y $\forall$ por "para todo").

CARDINALIDAD

3.10 Encuentre el número cardinal de cada conjunto:

a) $A = \{a, b, c, \ldots, y, z\}$ *c*) $C = \{10, 20, 30, 40, \ldots\}$.
b) $B = \{x \mid x \in \mathbf{N}, x^2 = 5\}$, *d*) $D = \{6, 7, 8, 9, \ldots\}$.

a) $|A| = 29$, puesto que en el alfabeto español hay 29 letras.
b) $|B| = 0$ puesto que no existe ningún entero positivo cuyo cuadrado sea 5; es decir, B es vacío.
c) $|C| = \aleph_0$ porque $f: \mathbf{N} \to C$, definida por $f(n) = 10_n$, es una correspondencia uno a uno entre $\mathbf{N}$ y C.
d) $|D| = \aleph_0$ porque $g: \mathbf{N} \to D$, definida por $g(n), = n + 5$ es una correspondencia uno a uno entre $\mathbf{N}$ y D.

3.11 Demuestre que la cardinalidad del conjunto $\mathbf{Z}$ de enteros es $\aleph_0$.

El siguiente diagrama muestra una correspondencia uno a uno entre $\mathbf{N}$ y $\mathbf{Z}$:

$$\begin{array}{lccccccccc} \mathbf{N} = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ \mathbf{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \ldots \end{array}$$

Es decir, la siguiente función $f: \mathbf{N} \to \mathbf{Z}$ es uno a uno y sobre:

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ (1 - n)/2 & \text{si } n \text{ es impar} \end{cases}^{n/2}$$

En consecuencia, $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$.

3.12 Sean $A_1, A_2, \ldots,$ conjuntos finitos numerables. Demuestre que la unión $S = \cup_i A_i$ es numerable.

En esencia, se enumeran los elementos de A_1, luego se enumeran los elementos de A_2 que no pertenecen a A_1; después los elementos de A_3 que no pertenecen a A_1 o A_2; es decir, que no han sido enumerados, y así en lo sucesivo. Puesto que los A_i son finitos, siempre es posible enumerar los elementos de cada conjunto. Este proceso se efectúa formalmente como sigue.

Primero se definen los conjuntos $B_1, B_2, \ldots,$ donde B_i contiene los elementos de A_i que no pertenecen a los conjuntos precedentes; es decir, se define

$$B_1 = A_1 \quad \text{y} \quad B_k = A_k \backslash (A_1 \cup A_2 \cup \cdots \cup A_{k-1})$$

Entonces los B_i son ajenos y $S = \cup_i B_i$. Sean $b_{i1}, b_{i2}, \ldots, b_{im}$ los elementos de B_i. Entonces $S = \{b_{ij}\}$. Sea $f = S \to \mathbf{N}$ definida como sigue:

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j$$

Si S es finito, entonces S es numerable. Si S es infinito, entonces f es una correspondencia uno a uno entre S y $\mathbf{N}$. Por tanto, S es numerable.

3.13 Demuestre el teorema 3.2: una unión numerable de conjuntos numerables es numerable.

Suponga que $A_1, A_2, A_3, \ldots,$ es una colección de conjuntos numerables. En particular, suponga que $a_{i1}, a_{i2}, a_{i3}, \ldots$ son los elementos de A_i. Los conjuntos $B_2, B_3, B_4, \ldots,$ se definen como sigue:

$$B_k = \{a_{ij} \mid i + j = k\}$$

Por ejemplo, $B_6 = \{a_{15}, a_{24}, a_{33}, a_{12}, a_{51}\}$. Observe que cada B_k es finito y que

$$S = \cup_i A_i = \cup_k B_k$$

Por el problema precedente, $\cup_k B_k$ es numerable. Entonces $S = \cup_i A_i$ es numerable y se ha demostrado el teorema.

3.14 Demuestre el teorema 3.3: el conjunto **I** de todos los números reales entre 0 y 1 inclusive es no numerable.

Resulta evidente que **I** es infinito, ya que contiene a $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Suponga que **I** es enumerable. Entonces existe una correspondencia uno a uno f: $N \to \mathbf{I}$. Sea $f(1) = a_1, f(2) = a_2, \ldots$; es decir, $\mathbf{I} = \{a_1, a_2, a_3, \ldots\}$. Los elementos $a_1, a_2, \ldots$ se escriben en una columna y cada uno se expresa en su notación decimal:

$$\begin{aligned} a_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ a_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ a_3 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ a_4 &= 0.x_{41}x_{42}x_{43}x_{44}\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

donde $x_{ij} \in \{0, 1, 2, \ldots, 9\}$. (Cuando un número se expresa en dos notaciones decimales diferentes, por ejemplo $0.2000000 = 0.1999999$, se escoge el desarrollo que termina con nueves.)

Sea $b = 0.y_1y_2y_3y_4\ldots$ el número real obtenido como sigue:

$$y_i = \begin{cases} 1 & \text{si } x_{ii} \neq 1 \\ 2 & \text{si } x_{ii} = 1 \end{cases}$$

Luego, $b \in \mathbf{I}$. Pero

$$\begin{aligned} &b \neq a_1 \text{ porque } y_1 \neq x_{11} \\ &b \neq a_2 \text{ porque } y_2 \neq x_{22} \\ &b \neq a_3 \text{ porque } y_3 \neq x_{33} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

En consecuencia, b no pertenece a $\mathbf{I} = \{a_1, a_2, \ldots\}$. Esto contradice el hecho de que $b \in \mathbf{I}$. Por tanto, la hipótesis de que **I** es enumerable debe ser falsa, de modo que **I** es no numerable.

FUNCIONES MATEMÁTICAS ESPECIALES

3.15 Encuentre: *a*) $\lfloor 7.5 \rfloor, \lfloor -7.5 \rfloor, \lfloor -18 \rfloor$; *b*) $\lceil 7.5 \rceil, \lceil -7.5 \rceil, \lceil -18 \rceil$.

a) Por definición, $\lfloor x \rfloor$ denota el mayor entero que no excede a x, de modo que $\lfloor 7.5 \rfloor = 7$, $\lfloor -7.5 \rfloor = -8$.

b) Por definición, $\lceil x \rceil$ denota el menor entero que no es menor que x, de modo que $\lceil 7.5 \rceil = 8$, $\lceil -7.5 \rceil = -7$, $\lceil -18 \rceil = -18$.

3.16 Encuentre: *a*) 25 (mód 7); *b*) 25 (mód 5); *c*) -35 (mód 11); *d*) -3 (mód 8).

Cuando k es positivo, simplemente se divide k entre el módulo M para obtener el residuo r. Así, $r = k(\text{mód } M)$. Si k es negativo, $|k|$ se divide entre M para obtener el residuo r'. Entonces $k(\text{mód } M) = M - r'$ (cuando $r' \neq 0$). Así:

a) $25 \text{ (mód } 7) = 4$

b) $25 \text{ (mód } 5) = 0$

c) $-35 \text{ (mód } 11) = 11 - 2 = 9$

d) $-3 \text{ (mód } 8) = 8 - 3 = 5$

3.17 Evaluar módulo $M = 15$: *a*) $9 + 13$; *b*) $7 + 11$; *c*) $4 - 9$; *d*) $2 - 10$.

Use $a + M = a(\text{mód } M)$:

a) $9 + 13 = 22 = 22 - 15 = 7$

b) $7 + 11 = 18 = 18 - 15 = 3$

c) $4 - 9 = -5 = -5 + 15 = 10$

d) $2 - 10 = -8 = -8 + 15 = 7$

3.18 Simplifique: *a*) $\dfrac{n!}{(n-1)!}$; *b*) $\dfrac{(n+2)!}{n!}$.

a) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$ o, simplemente, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$

b) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n-1) = n^2 + 3n + 2$

3.19 Evalúe: *a*) $\log_2 8$; *b*) $\log_2 64$; *c*) $\log_{10} 100$; *d*) $\log_{10} 0.001$.

a) $\log_2 8 = 3$ puesto que $2^3 = 8$

b) $\log_2 64 = 6$ puesto que $2^6 = 64$

c) $\log_{10} 100 = 2$ puesto que $10^2 = 100$

d) $\log_{10} 0.001 = -3$ puesto que $10^{-3} = 0.001$

FUNCIONES RECURSIVAS

3.20 Sean a y b enteros positivos, y suponga que Q se define recursivamente como sigue:

$$Q(a, b) = \begin{cases} 0 & \text{si } a < b \\ Q(a-b, b) + 1 & \text{si } b \leq a \end{cases}$$

a) Encuentre: *i*) $Q(2, 5)$; *ii*) $Q(12, 5)$.

b) ¿Qué hace esta función Q? Encuentre $Q(5861, 7)$.

a) *i*) $Q(2, 5) = 0$ puesto que $2 < 5$.

ii) $Q(12, 5) = Q(7, 5) + 1$
$= [Q(2, 5) + 1] + 1 = Q(2, 5) + 2$
$= 0 + 2 = 2$

b) Cada vez que b se resta de a, el valor de Q aumenta 1. Por tanto, $Q(a, b)$ encuentra el cociente cuando a se divide entre b. Así, $Q(5861, 7) = 837$.

3.21 Use la definición de la función de Ackermann para encontrar $A(1, 3)$.

En la figura 3-10 se muestran los 15 pasos para evaluar $A(1, 3)$.

El sangrado hacia delante indica que se retrasa una evaluación y se vuelve a la definición, y el sangrado hacia atrás indica que se retrocede. Observe que el inciso *a*) de la definición se utiliza en los pasos 5, 8, 11 y 14; el inciso *b*), en el paso 4; y el inciso *c*), en los pasos 1, 2 y 3. En los otros pasos se retrocede con las sustituciones.

(1) $A(1, 3) = A(0, A(1, 2))$
(2) $A(1, 2) = A(0, A(1, 1))$
(3) $A(1, 1) = A(0, A(1, 0))$
(4) $A(1, 0) = A(0, 1)$
(5) $A(0, 1) = 1 + 1 = 2$
(6) $A(1, 0) = 2$
(7) $A(1, 1) = A(0, 2)$
(8) $A(0, 2) = 2 + 1 = 3$
(9) $A(1, 1) = 3$
(10) $A(1, 2) = A(0, 3)$
(11) $A(0, 3) = 3 + 1 = 4$
(12) $A(1, 2) = 4$
(13) $A(1, 3) = A(0, 4)$
(14) $A(0, 4) = 4 + 1 = 5$
(15) $A(1, 3) = 5$

Figura 3-10

PROBLEMAS DIVERSOS

3.22 Encuentre el dominio D de cada una de las siguientes funciones de evaluación real de variable real:

a) $f(x) = \frac{1}{x-2}$ *c*) $f(x) = \sqrt{25 - x^2}$
b) $f(x) = x^2 - 3x - 4$ *d*) x^2 donde $0 \le x \le 2$

Cuando una función de valuación real de una variable real está definida por una fórmula $f(x)$, entonces el dominio D consta del mayor subconjunto de $\mathbf{R}$ para el que cual $f(x)$ está definida y es real, a menos que se especifique otra cosa.

a) f no está definida para $x - 2 = 0$; es decir, cuando $x = 2$; por tanto $D = \mathbf{R}\backslash\{2\}$.

b) f está definida para todo número real; por tanto, $D = \mathbf{R}$.

c) f no está definida cuando $25 - x^2$ es negativo; por tanto $D = \{-5, 5\} = \{x \mid -5 \le x \le 5\}$.

d) Aquí, el dominio de f está dado explícitamente como $D = \{x \mid 0 \le x \le 2\}$.

3.23 Para cualquier $n \in \mathbf{N}$, sea $D_n = (0, 1/n)$ el intervalo abierto de 0 a $1/n$. Encuentre:

a) $D_3 \cup D_4$; *b*) $D_3 \cap D_{20}$; *c*) $D_s \cup D_t$; *d*) $D_s \cap D_t$.

a) Puesto que $(0, 1/3)$ es un superconjunto de $(0,1/7)$, $D_3 \cup D_4 = D_3$.

b) Puesto que $(0, 1/20)$ es un subconjunto de $(0,1/3)$, $D_3 \cap D_{20} = D_{20}$.

c) Sea $M = \text{mín}(s, t)$; es decir, el menor de los dos números s y t; entonces D_M es igual a D_s o D_t y contiene al otro como subconjunto. Por tanto, $D_s \cap D_t = D_M$.

d) Sea $M = \text{máx}(s, t)$; es decir, el mayor de los dos números s y t; entonces $D_s \cap D_t = D_M$.

3.24 Suponga que $P(n) = a_0 + a_1 n + a_2 n_2 + \cdots + a_m n^2$ tiene grado m. Demuestre que $P(n) = O(n^m)$.

Sea $b_0 = |a_0|,\ b_1 = |a_1|, \ldots,\ b_m = |a_m|$. Entonces para $n \ge 1$,

$$\begin{aligned} p(n) &\le b_0 + b_1 n + b_2 n^2 + \cdots + b_m n^m = \left(\tfrac{b_0}{n^m} + \tfrac{b_1}{n^{m-1}} + \cdots + b_m\right) n^m \\ &\le (b_0 + b_1 + \cdots + b_m) n^m = M n^m \end{aligned}$$

donde $M = |a_0| + |a_1| + \cdots + |a_m|$. Por tanto $P(n) = O(n^m)$.

Por ejemplo, $5x^3 + 3x = O(x^3)$ y $x^4 - 4000000x^2 = O(x^5)$.

3.25 Demuestre el teorema 3.4 (Cantor): $|A| < |\text{Potencia}(A)|$ (donde Potencia(A) es el conjunto potencia de A).

La función $g: A \to \text{Potencia}(A)$ definida por $g(a) = \{a\}$ es claramente uno a uno; por tanto, $|A| \le |\text{Potencia}(A)|$.

Si se demuestra que $|A| \ne |\text{Potencia}(A)|$, entonces se concluye el teorema. Se supone lo contrario; es decir, se supone que $|A| = |\text{Potencia}(A)|$ y que $f: A \to \text{Potencia}(A)$ es una función que es tanto uno a uno como sobre. Sea $a \in A$ que se denomina "mal" elemento si $a \notin f(a)$, y sea B el conjunto de los malos elementos. En otras palabras,

$$B = \{x : x \in A,\ x \notin f(x)\}$$

Así, B es un subconjunto de A. Puesto que $f: A \to \text{Potencia}(A)$ es sobre, existe $b \in A$ tal que $f(b) = B$; ¿b es un "mal" elemento o un "buen" elemento? Si $b \in B$, entonces por definición de B, $b \notin f(b) = B$, lo cual es imposible. En forma semejante, si $b \notin B$, entonces $b \in f(b) = B$, lo que también es imposible. Por tanto, la hipótesis original de que $|A| = |\text{Potencia}(A)|$ ha llevado a una contradicción. Entonces, la hipótesis es falsa, de modo que el teorema es verdadero.

3.26 Demuestre el siguiente planteamiento equivalente del teorema 3.5 de Schroeder-Bernstein:

Suponga que $X \supseteq Y \supseteq X_1$ y $X \simeq X_1$. Entonces $Y \simeq Y$.

Puesto que $X \simeq X_1$, existe una correspondencia uno a uno (biyección) $f: X \to X_1$. Puesto que $X \supseteq Y$, la restricción de f a Y, que también se denota por f, también es uno a uno. Sea $f(Y) = Y_1$. Entonces Y y Y_1 son equipotentes,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

y $f: Y \to Y_1$ es biyectiva. Pero ahora $Y \supseteq X_1 \supseteq Y_1$ y $Y \simeq Y_1$. Por razones semejantes, X_1 y $f(X_1) = X_2$ son equipotentes.

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

y $f: X_1 \to X_2$ es biyectiva. En consecuencia, existen conjuntos equipotentes $X, X_1, X_2, \ldots$, y conjuntos equipotentes $Y, Y_1, Y_2, \ldots$, tales que

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2 \supseteq Y_2 \supseteq X_3 \supseteq Y_3 \supseteq \cdots$$

y $f: X_k \to X_{k+1}$ y $f: Y_k \to Y_{k+1}$ son biyectivas.

Sea

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Entonces

$$X = (X \backslash Y) \cup (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup \cdots \cup B$$
$$Y = (Y \backslash X_1) \cup (X_1 \backslash Y_1) \cup (Y_1 \backslash X_2) \cup \cdots \cup B$$

Además, $X \backslash Y, X_1 \backslash Y_1, X_2 \backslash Y_2, \ldots$, son equipotentes. De hecho, la función

$$f: (X_k \backslash Y_k) \to (X_{k+1} \backslash Y_{k+1})$$

es uno a uno y sobre.

Considere la función $g: X \to Y$ definida por el diagrama en la figura 3-11. Es decir,

$$g(x) = \begin{cases} f(x) & \text{si } x \in X_k \backslash Y_k \text{ o } x \in X \backslash Y \\ x & \text{si } x \in Y_k \backslash X_k \text{ o } x \in B \end{cases}$$

Entonces g es uno a uno y sobre. En consecuencia, $X \simeq Y$.

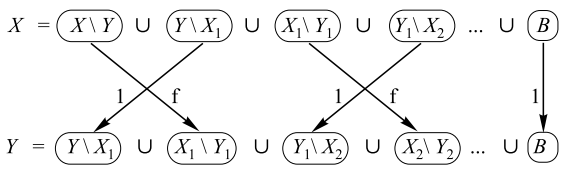


Figura 3-11

PROBLEMAS SUPLEMENTARIOS

FUNCIONES

3.27 Sea $W = \{a, b, c, d\}$. Decida si cada uno de los siguientes conjuntos de pares ordenados es una función de W en W.

a) $\{(b, a), (c, d), (d, a), (c, d) (a, d)\}$
b) $\{(d, d), (c, a), (a, b), (d, b)\}$
c) $\{(a, b), (b, b), (c, d), (d, b)\}$
d) $\{(a, a), (b, a), (a, b), (c, d)\}$

3.28 Sea $V = \{1, 2, 3, 4\}$. Para las siguientes funciones $f: V \to V$ y $g: V \to V$; encuentre:

a) $f \circ g$; *b*) $g \circ f$; *c*) $f \circ f$:

$$f = \{(1, 3), (2, 1), (3, 4), (4, 3)\} \quad \text{y} \quad g = \{(1, 2), (2, 3), (3, 1), (4, 1)\}$$

3.29 Encuentre la composición de funciones $h \circ g \circ f$ para las funciones en la figura 3-9.

FUNCIONES UNO A UNO, SOBRE E INVERTIBLES

3.30 Determine si cada función es uno a uno.

a) A cada persona en la Tierra se asigna el número que corresponde a su edad.
b) A cada país en el mundo se asignan la latitud y la longitud de su capital.
c) A cada libro escrito por un solo autor se asigna el autor.
d) A cada país en el mundo que tiene un primer ministro se asigna su primer ministro.

3.31 Sean las funciones f, g, h de $V = \{1, 2, 3, 4\}$ en V definidas por: $f(n) = 6 - n$, $g(n) = 3$, $h = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Decida cuáles funciones son:

a) uno a uno; *b*) sobre; *c*) ambas; *d*) ni uno a uno ni sobre.

3.32 Sean las funciones f, g, h de $\mathbf{N}$ en $\mathbf{N}$ definidas por $f(n) = n + 2$, *b*) $g(n) = 2^n$, $h(n) =$ número de divisores positivos de n. Decida cuáles funciones son:

a) uno a uno; *b*) sobre; *c*) ambas; *d*) ni uno a uno ni sobre; *e*) encuentre $h'(2) = \{x | h(x) = 2\}$.

3.33 Decida cuáles de las siguientes funciones son: *a*) uno a uno; *b*) sobre; *c*) ambas; *d*) ni uno a uno ni sobre.

1) f: $\mathbf{Z}^2 \to \mathbf{Z}$ donde $f(n, m) = n - m$; 3) h: $\mathbf{Z} \times (\mathbf{Z} \backslash 0) \to \mathbf{Q}$ donde $h(n, m) = n/m$;
2) g: $\mathbf{Z}^2 \to \mathbf{Z}^2$ donde $g(n, m) = (m, n)$; 4) k: $\mathbf{Z} \to \mathbf{Z}^2$ donde $k(n) = (n, n)$.

3.34 Sea f: $\mathbf{R} \to \mathbf{R}$ definida por $f(x) = 3x - 7$. Encuentre una fórmula para la función inversa f^{-1}: $\mathbf{R} \to \mathbf{R}$.

3.35 Considere las permutaciones $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix}$ y $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ en S_6.

Encuentre: *a*) $\tau \circ \sigma$; *b*) $\sigma \circ \tau$; *c*) σ^2; *d*) σ^{-1}; *e*) τ^{-1}

PROPIEDADES DE LAS FUNCIONES

3.36 Demuestre: suponga que f: $A \to B$ y g: $B \to A$ satisfacen $g \circ f = 1_A$. Entonces f es uno a uno y g es sobre.

3.37 Demuestre el teorema 3.1: una función f: $A \to B$ es invertible si y sólo si f es uno a uno y sobre.

3.38 Demuestre: suponga que f: $A \to B$ es invertible con función inversa f^{-1}: $B \to A$. Entonces $f^{-1} \circ f = 1_A$ y $f \circ f^{-1} = 1_B$.

3.39 Suponga que f: $A \to B$ es uno a uno y que g: $A \to B$ es sobre. Sea x un subconjunto de A.

a) Demuestre que $f1_x$, la restricción de f en x es uno a uno.
b) Demuestre que $g1_x$ no necesita ser sobre.

3.40 Para toda $n \in \mathbf{N}$, considere el intervalo abierto $A_n = (0, 1/n) = \{x \mid 0 < x < 1/n\}$. Encuentre:

a) $A_2 \cup A_8$; *c*) $\cup(A_i \mid i \in J)$; *e*) $\cup(A_i \mid i \in K)$;
b) $A_3 \cap A_7$; *d*) $\cap(A_i \mid i \in J)$; *f*) $\cap(A_i \mid i \in K)$.

donde J es un subconjunto finito de $\mathbf{N}$ y $\mathbf{K}$ es un subconjunto infinito de $\mathbf{N}$.

3.41 Para toda $n \in N$, sea $D_n = \{n, 2n, 3n, \ldots,\} = \{$múltiplos de $n\}$.

a) Encuentre: *i*) $D_2 \cap D_7$; *ii*) $D_6 \cap D_8$; *iii*) $D_3 \cap D_{12}$; *iv*) $D_3 \cup D_{12}$.
b) Demuestre que $\cap(D_i | i \in K) = \varnothing$ donde K es un subconjunto infinito de $\mathbf{N}$.

3.42 Considere una clase indexada de conjuntos $\{A_i \mid i \in I\}$, un conjunto $\mathbf{B}$ y un índice i_0 en I.

Demuestre: *a*) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$; *b*) $\cap (A_i \mid i \in I) \subseteq A_{i0} \subseteq \cup(A_i \mid i \in I)$.

NÚMEROS CARDINALES

3.43 Encuentre el número cardinal de cada conjunto: *a*) $\{x \mid x$ es una letra de "BASEBALL"$\}$; *b*) Conjunto potencia de $A = \{a, b, c, d, e\}$; *c*) $\{x \mid x^2 = 9, 2x = 8\}$.

3.44 Encuentre el número cardinal de:

a) Todas las funciones de $A = \{a, b, c, d\}$ en $B = \{1, 2, 3, 4, 5\}$;
b) Todas las funciones de P en Q, donde $|P| = r$ y $|Q| = s$;
c) Todas las relaciones sobre $A = \{a, b, c, d\}$;
d) Todas las relaciones sobre P donde $|P| = r$.

3.45 Demuestre:

a) Todo conjunto infinito A contiene un subconjunto enumerable D.
b) Cada subconjunto de un conjunto enumerable es finito o enumerable.
c) Si A y B son enumerables, entonces $A \times B$ es enumerable.
d) El conjunto **Q** de números racionales es enumerable.

3.46 Demuestre: *a*) $|A \times B| = |B \times A|$; *b*) si $A \subseteq B$ entonces $|A| \leq |B|$; *c*) si $|A| = |B|$ entonces $|P(A)| = |P(B)|$.

FUNCIONES ESPECIALES

3.47 Encuentre: *a*) $\lfloor 13.2 \rfloor$, $\lfloor -0.17 \rfloor$, $\lfloor 34 \rfloor$, *b*) $\lceil 13.2 \rceil$, $\lceil -0.17 \rceil$, $\lceil 34 \rceil$.

3.48 Encuentre:

a) 29 (mód 6);
b) 200 (mód 20);
c) 5 (mód 12);
d) -347 (mód 6);
e) -555 (mód 11).

3.49 Encuentre: *a*) $3! + 4!$; *b*) $3!\,(3! + 2!)$; *c*) $6!/5!$; *d*) $30!/28!$

3.50 Evalúe: *a*) $\log_2 16$; *b*) $\log_3 27$; *c*) $\log_{10} 0.01$.

PROBLEMAS DIVERSOS

3.51 Sea n un entero. Encuentre $L(25)$ y describa qué hace la función L, donde L está definida por:

$$L(n) = \begin{cases} 0 & \text{si } n = 1 \\ L(\lfloor n)2 \rfloor) + 1 & \text{si } n > 1 \end{cases}$$

3.52 Sean a y b enteros. Encuentre $Q(2, 7)$, $Q(5, 3)$ y $Q(15, 2)$, donde $Q(a, b)$ está definido por:

$$Q(a, b) = \begin{cases} 5 & \text{si } a < b \\ Q(a - b,\ b + 2) + a & \text{si } a \geq b \end{cases}$$

3.53 Demuestre: el conjunto P de todos los polinomios $p(x) = a_0 + a_1 x + \cdots + a_x^m$ con coeficientes enteros (es decir, donde a_0, $a_1, \ldots, a_m$ son enteros) es enumerable.

Respuestas a los problemas suplementarios

3.27 *a*) Sí; *b*) no; *c*) sí; *d*) no.

3.28 *a*) $\{(1, 1), (2, 4), (3, 3), (4, 3)\}$;
b) $\{(1, 1), (2, 2), (3, 1), (4, 1)\}$;
c) $\{(1, 4), (2, 3), (3, 3), (4, 4)\}$;

3.29 $\{(a, 4), (b, 6), (c, 4)\}$.

3.30 *a*) No; *b*) sí; *c*) no; *d*) sí.

3.31 *a*) f, h; *b*) f, h; *c*) f, h; *d*) g.

3.32 *a*) *f*, *g*; *b*) *h*; *c*) ninguna; *d*) ninguna; *e*) {todos los números primos}.

3.33 *a*) *g*, *k*; *b*) *f*, *g*, *h*; *c*) *g*; *d*) ninguna.

3.34 $f^{-1}(x) = (x + 7)/3$

3.35 *a*) 425631; *b*) 416253; *c*) 534261; *d*) 415623; *e*) 453261.

3.40 *a*) A_2; *b*) A_7; *c*) A_r, donde r es el menor entero en J; *d*) A_s, donde s es el mayor entero en J; *e*) A_r, donde r es el menor entero en K; *f*) $\varnothing$.

3.41 *i*) D_{14}; *ii*) D_{24}; *iii*) D_{12}; *iv*) D_3.

3.43 *a*) 5; *b*) $2^5 = 32$; *c*) 0.

3.44 *a*) $5^4 = 625$; *b*) s^r; *c*) $2^{16} = 65\,536$; *d*) 2.

3.47 *a*) 13, −1, 34; *b*) 14, 0, 34.

3.48 *a*) 5; *b*) 0; *c*) 2; *d*) $6 - 5 = 1$; *e*) $11 - 5 = 6$.

3.49 *a*) 30; *b*) 48; *c*) 6; *d*) 870.

3.50 *a*) 4; *b*) 3; *c*) −2.

3.51 $L(25) = 4$. Cada vez que n se divide entre 2, el valor de L aumenta 1. Así, L es el mayor entero tal que $2^L < N$. Entonces $L(n) = \lfloor \log_2 n \rfloor$.

3.52 $Q(2, 7) = 5$, $Q(5, 3) = 10$, $Q(15, 2) = 42$.

3.53 Sugerencia: Sea P_k el conjunto de polinomios $p(x)$ tal que $m \leq k$ y cada $|a_i| \leq k$. P_k es finito y $P = \cup_k P_k$.

4 Lógica y cálculo de proposiciones

CAPÍTULO

4.1 INTRODUCCIÓN

En muchos algoritmos y demostraciones se usan expresiones lógicas como:

"SI p ENTONCES" o "si p_1 Y p_2, ENTONCES q_1 O q_2"

Por consiguiente, es necesario conocer los casos en que estas expresiones son VERDADERAS o FALSAS; es decir, conocer el "valor de verdad" de tales expresiones. Estos temas se analizan en este capítulo.

También se investiga el valor de verdad de declaraciones cuantificadas, que son proposiciones en las que se usan los cuantificadores lógicos "para todo" y "existe".

4.2 PROPOSICIONES Y DECLARACIONES COMPUESTAS

Una *proposición* (o *declaración*) es una afirmación declarativa que es falsa o verdadera, pero no ambas. Considere, por ejemplo, las seis oraciones siguientes:

i) El hielo flota en el agua.
ii) China está en Europa.
iii) $2 + 2 = 4$.
iv) $2 + 2 = 5$.
v) ¿A dónde vas?
vi) Haz tu tarea.

Las cuatro primeras son proposiciones; las dos últimas, no. También, *i*) y *iii*) son verdaderas, pero *ii*) y *iv*) son falsas.

Proposiciones compuestas

Muchas proposiciones son *compuestas*; es decir, están compuestas de *subproposiciones* y varios conectivos que se analizarán dentro de poco. Estas proposiciones se denominan *proposiciones compuestas*. Se dice que una proposición es *primitiva* si no es posible separarla en proposiciones más simples; es decir, si no es compuesta.

Por ejemplo, las proposiciones anteriores *i*) a *iv*) son primitivas. Por otra parte, las dos siguientes proposiciones son compuestas:

"Las rosas son rojas y las violetas son azules" y "Juan es inteligente o estudia cada noche".

La propiedad fundamental de una proposición compuesta es que su valor de verdad lo determinan los valores de verdad de sus subproposiciones junto con la forma en que se conectan para formar las proposiciones compuestas. En la siguiente sección se estudian algunos de estos conectivos.

4.3 OPERACIONES LÓGICAS BÁSICAS

En esta sección se analizan las tres operaciones lógicas básicas de conjunción, disyunción y negación que corresponden, respectivamente, a las palabras "y", "o" y "no" en lenguaje coloquial.

Conjunción, $p \wedge q$

Dos proposiciones arbitrarias se combinan mediante la palabra "y" para formar una proposición compuesta que se denomina *conjunción* de las proposiciones originales. Se escribe así:

$$p \wedge q$$

que se lee "p y q", denota la conjunción de p y q. Puesto que $p \wedge q$ es una proposición, tiene un valor de verdad, que depende sólo de los valores de verdad de p y q. En específico:

Definición 4.1: Si p y q son verdaderas, entonces $p \wedge q$ es verdadera; en otro caso, $p \wedge q$ es falsa.

El valor de verdad de $p \wedge q$ tiene una forma equivalente de definición mediante la tabla 4-1*a*). Ahí, la primera línea es una forma abreviada de decir que si p es verdadera y q es verdadera, entonces $p \wedge q$ es verdadera. La segunda línea establece que si p es verdadera y q es falsa, entonces $p \wedge q$ es falsa. Y así en las sucesivas. Observe que hay cuatro líneas correspondientes a las cuatro combinaciones posibles de V y F para las dos subproposiciones p y q. También que $p \wedge q$ es verdadera sólo cuando ambas son verdaderas.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

a) "p y q"

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

b) "p o q"

p	$\neg p$
V	F
F	V

c) "no q"

Figura 4-1

EJEMPLO 4.1 Considere las cuatro proposiciones siguientes:

i) El hielo flota en el agua y $2 + 2 = 4$.
ii) El hielo flota en el agua y $2 + 2 = 5$.
iii) China está en Europa y $2 + 2 = 4$.
iv) China está en Europa y $2 + 2 = 5$.

Sólo la primera proposición es verdadera. Cada una de las otras es falsa puesto que por lo menos una de sus subproposiciones es falsa.

Disyunción, $p \vee q$

Dos proposiciones arbitrarias se combinan mediante el conectivo "o" para formar una proposición compuesta denominada *disyunción* de las proposiciones originales. Se escribe así,

$$p \vee q$$

que se lee "p o q", denota la disyunción de p y q. El valor de verdad de $p \vee q$ sólo depende de los valores de verdad de p y q como sigue.

Definición 4.2: Si p y q son falsas, entonces $p \vee q$ es falsa; en otro caso , $p \vee q$ es verdadera.

El valor de verdad de $p \vee q$ tiene una forma equivalente de definición por medio de la tabla 4-1*b*). Observe que $p \vee q$ es falsa sólo en el cuarto caso, cuando ambas p y q son falsas.

EJEMPLO 4.2 Considere las cuatro proposiciones siguientes:

i) El hielo flota en el agua o 2 + 2 = 4.
ii) El hielo flota en el agua o 2 + 2 = 5.
iii) China está en Europa o 2 + 2 = 4.
iv) China está en Europa o 2 + 2 = 5.

Sólo la proposición *iv*) es falsa. Cada una de las otras es verdadera puesto que por lo menos una de sus subproposiciones es verdadera.

Observación: La palabra "o" en español se usa en dos formas distintas. Algunas veces se utiliza en el sentido de "p o q o ambas" —es decir, por lo menos una de las dos alternativas ocurre, como acaba de observarse— y otras veces se utiliza en el sentido de "p o q pero no ambas"; es decir, ocurre exactamente una de las dos alternativas. Por ejemplo, en la oración "Él estudiará en Yale o en Harvard" la "o" se utiliza en el segundo sentido, denominado *disyunción exclusivo*. A menos que se establezca otra cosa, "o" se usará en el primer sentido. Esta argumentación indica la precisión que se adquiere a partir el lenguaje simbólico: $p \vee q$ se define mediante su tabla de verdad y *siempre* significa "p y/o q".

Negación, $\neg p$

Dada cualquier proposición p, es posible formar otra proposición, denominada *negación* de p, al escribir "no es verdad que…" o "Es falso que…" antes de p o, de ser posible, al insertar en p la palabra "no". El símbolo de la negación de p se lee "no p", se denota por

$$\neg p$$

El valor de verdad de $\neg p$ depende del valor de verdad de p como sigue:

Definición 4.3: Si p es verdadera, entonces $\neg p$ es falsa; y si p es falsa, entonces $\neg p$ es verdadera.

El valor de verdad de $\neg p$ tiene una forma equivalente de definición por medio de la tabla en la figura 4-1*c*). Así, el valor de verdad de la negación de p siempre es el opuesto al valor de verdad de p.

EJEMPLO 4.3 Considere las seis proposiciones siguientes:

a_1) El hielo flota en el agua. a_2) Es falso que el hielo flota en el agua. a_3) El hielo no flota en el agua.
b_1) $2 + 2 = 5$. b_2) Es falso que $2 + 2 = 5$. b_3) $2 + 2 \neq 5$.

Entonces a_2) y a_3) son, cada una, la negación de a_1); y b_2) y b_3) son, cada una, la negación de b_1). Puesto que a_1) es verdadera, a_2) y a_3) son falsas; y puesto que b_1) es falsa, b_2) y b_3) son verdaderas.

Observación: La notación lógica para los conectivos "y", "o" y "no" aún no está completamente estandarizada. Por ejemplo, en algunos textos se usa:

$$\begin{array}{ccc} p \,\&\, q,\ p \cdot q \text{ o } pq & \text{para} & p \wedge q \\ p + q & \text{para} & p \vee q \\ p',\ \bar{p} \text{ o } \sim p & \text{para} & \neg p \end{array}$$

4.4 PROPOSICIONES Y TABLAS DE VERDAD

Sea $P(p, q, \ldots)$ una expresión construida a partir de variables lógicas $p, q, \ldots$, que tienen el valor VERDADERO (V) o FALSO (F), y los conectivos lógicos $\wedge$, $\vee$ y $\neg$ (además de otros que se analizarán). Una expresión como $P(p, q, \ldots)$ se denomina *proposición*.

La propiedad más importante de una proposición $P(p, q, \ldots)$ es que su valor de verdad depende exclusivamente de los valores de verdad de sus variables; es decir, el valor de verdad de una proposición se conoce una vez que se conoce el valor de verdad de cada una de sus variables. Una forma concisa de mostrar esta relación es por medio de una *tabla de verdad*. A continuación se describe un método para obtener esta tabla de verdad.

Considere, por ejemplo, la proposición $\neg(p \wedge \neg q)$. En la figura 4-2*a*) se indica la forma en que se construye la tabla de verdad de $\neg(p \wedge \neg q)$. Observe que las primeras columnas de la tabla son para las variables $p, q, \ldots$, y que en la tabla hay suficientes renglones a fin de permitir todas las combinaciones posibles de *V* y *F* para estas *variables*. (Para 2 variables, como antes, se requieren 4 renglones; para 3 variables se necesitan 8 renglones; y, en general, para *n* variables se requieren 2^n renglones.) Entonces, hay una columna para cada etapa "elemental" de la construcción de la proposición, donde el valor de verdad en cada paso se determina a partir de las etapas previas por las definiciones de los conectivos $\wedge$, $\vee$, $\neg$. Por último, se obtiene el valor de verdad de la proposición, que aparece en la última columna.

La tabla de verdad real de la proposición $\neg(p \wedge \neg q)$ se muestra en la figura 4-2*b*). Consta precisamente de las columnas en la figura 4-2*a*) que aparecen bajo las variables y bajo la proposición; las otras columnas se usaron sólo para la construcción de la tabla de verdad.

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

a)

p	q	$\neg(p \wedge \neg q)$
V	V	V
V	F	F
F	V	V
F	F	V

b)

Figura 4-2

Observación: Para evitar una cantidad excesiva de paréntesis, algunas veces se adopta un orden de precedencia para los conectivos lógicos:

$\neg$ tiene precedencia sobre $\wedge$ que tiene precedencia sobre $\vee$

Por ejemplo, $\neg p \wedge q$ significa $(\neg p) \wedge q$ y no $\neg(p \wedge q)$.

Método alterno para construir una tabla de verdad

Otra forma de construir la tabla de verdad de $\neg(p \wedge \neg q)$ es la siguiente:

a) Primero se construye la tabla de verdad que se muestra en la figura 4-3. Es decir, primero se enumeran todas las variables y las combinaciones de sus valores de verdad. También hay un renglón final identificado por "Paso". Luego, se escribe la proposición en el renglón superior a la derecha de sus variables con espacio suficiente de modo que haya una columna bajo cada variable y bajo cada operación lógica en la proposición. Por último (paso 1), los valores de verdad de las variables se escriben en la tabla bajo las variables en la proposición.

b) Ahora se escriben valores de verdad adicionales en la tabla de verdad, columna por columna, bajo cada operación lógica, como se muestra en la figura 4-4. También se indica el paso en que se introducen los valores de verdad de cada columna.

La tabla de verdad de la proposición consta entonces de las columnas originales bajo las variables y el último paso; es decir, la última columna se escribe en la tabla.

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V			V
V	F		V			F
F	V		F			V
F	F		F			F
Paso						

Figura 4-3

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V		F	V
V	F		V		V	F
F	V		F		F	V
F	F		F		V	F
Paso			1		2	1

a)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V	F	F	V
V	F		V	V	V	F
F	V		F	F	F	V
F	F		F	F	V	F
Paso			1	3	2	1

b)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V	V	V	F	F	V
F	V	F	V	V	V	F
F	F	V	F	F	F	V
F	F	V	F	F	V	F
Paso		4	1	3	2	1

c)

Figura 4-4

4.5 TAUTOLOGÍAS Y CONTRADICCIONES

Algunas proposiciones $P(p, q, \ldots)$ sólo contienen V en la última columna de sus tablas de verdad o, en otras palabras, son verdaderas para cualesquiera valores de verdad de sus variables. Estas proposiciones se denominan *tautologías*. En forma semejante, una proposición $P(p, q, \ldots)$ se denomina *contradicción* si sólo contiene F en la última columna de su tabla de verdad o, en otras palabras, si es falsa para cualesquiera valores de verdad de sus variables. Por ejemplo, la proposición "p o no p", $p \vee \neg p$, es una tautología, y la proposición "p y no p", $p \wedge \neg p$, es una contradicción. Esto se comprueba al ver sus tablas de verdad en la figura 4-5. (Las tablas de verdad sólo tienen dos renglones puesto que cada proposición sólo tiene una variable: p.)

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

a) $p \vee \neg p$

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

b) $p \wedge \neg p$

Figura 4-5

Observe que la negación de una tautología es una contradicción, ya que siempre es falsa, y que la negación de una contradicción es una tautología, puesto que siempre es verdadera.

Ahora, sea $P(p, q, \ldots)$ una tautología, y sean $P_1(p, q, \ldots)$, $P_2(p, q, \ldots), \ldots$ proposiciones arbitrarias. Puesto que $P(p, q, \ldots)$ no depende de los valores de verdad particulares de sus variables $p, q, \ldots$, es posible sustituir P_1 por p, P_2 por $q, \ldots$, en la tautología $P(p, q, \ldots)$ y mantenerse una tautología. En otras palabras:

Teorema 4.1 (principio de sustitución): Si $P(p, q, \ldots)$ es una tautología, entonces $P(p_1, q_2, \ldots)$ es una tautología para proposiciones arbitrarias $P_1, P_2, \ldots$.

4.6 EQUIVALENCIA LÓGICA

Dos proposiciones $P(p, q, \ldots)$ y $Q(p, q, \ldots)$ son *lógicamente equivalentes*, *equivalentes* o *iguales*, lo cual se denota por

$$P(p, q, \ldots) \equiv Q(p, q, \ldots)$$

si tienen tablas de verdad idénticas. Considere, por ejemplo, las tablas de verdad de $\neg(p \wedge q)$ y $\neg p \vee \neg q$ que aparecen en la figura 4-6. Observe que ambas tablas de verdad son la misma; es decir, ambas proposiciones son falsas en el primer caso y verdaderas en los otros tres casos. En consecuencia, puede escribirse

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

En otras palabras, las proposiciones son lógicamente equivalentes.

Observación: Sean p "Las rosas son rojas" y q "Las violetas son azules". Sea S la proposición:

"No es verdad que las rosas son rojas y las violetas son azules."

Entonces S se escribe en la forma $\neg(p \wedge q)$. No obstante, como ya se observó, $\neg(p \wedge q) \equiv \neg p \vee \neg q$. En consecuencia, S tiene el mismo significado que la proposición:

"Las rosas no son rojas, o las violetas no son azules."

p	q	$p \wedge q$	$\neg(p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

a) $\neg(p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

b) $\neg p \vee \neg q$

Figura 4-6

4.7 ÁLGEBRA DE PROPOSICIONES

Las proposiciones satisfacen varias leyes que se listan en la tabla 4-1. (En esta tabla, *V* y *F* se restringen a los valores de verdad "Verdadera" y "Falsa".) El planteamiento formal de este resultado es:

Teorema 4.2: Las proposiciones satisfacen las leyes de la tabla 4-1.

(Observe la semejanza entre esta tabla 4-1 y la tabla 1-1 sobre conjuntos.)

Tabla 4-1 Leyes del álgebra de proposiciones

Leyes idempotentes:	(1a) $p \vee p \equiv p$	(1b) $p \wedge p \equiv p$
Leyes asociativas:	(2a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$	(2b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Leyes conmutativas:	(3a) $p \vee q \equiv q \vee p$	(3b) $p \wedge q \equiv q \wedge p$
Leyes distributivas:	(4a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	(4b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Leyes de identidad:	(5a) $p \vee F \equiv p$ (6a) $p \vee V \equiv V$	(5b) $p \wedge V \equiv p$ (6b) $p \wedge F \equiv F$
Leyes de doble negación:	(7a) $\neg\neg p \equiv p$	
Leyes de complementos:	(8a) $p \vee \neg p \equiv V$ (9a) $\neg V \equiv F$	(8b) $p \wedge \neg p \equiv V$ (9b) $\neg F \equiv V$
Leyes de DeMorgan:	(10a) $\neg(p \vee q) \equiv \neg p \wedge \neg q$	(10b) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

4.8 PROPOSICIONES CONDICIONALES Y BICONDICIONALES

Muchas proposiciones, en particular las que se hacen en matemáticas, son de la forma "Si p entonces q". Estas proposiciones se denominan *condicionales* y se denotan por

$$p \rightarrow q$$

La condicional $p \rightarrow q$ suele leerse "p implica q" o "p sólo si q".

Otra proposición común es de la forma "p si y sólo si q". Estas proposiciones se denominan *bicondicionales* y se denotan por

$$p \leftrightarrow q$$

Los valores de verdad de $p \rightarrow q$ y $p \leftrightarrow q$ están definidos por las tablas en la figura 4-7*a*) y *b*). Observe que:

a) La condicional $p \rightarrow q$ es falsa sólo cuando la primera parte, p, es verdadera y la segunda parte, q, es falsa. En consecuencia, cuando p es falsa, la condicional $p \rightarrow q$ es verdadera sin importar el valor de verdad de q.

b) La bicondicional $p \leftrightarrow q$ es verdadera siempre que p y q tienen los mismos valores de verdad; y es falsa en otro caso.

La tabla de verdad de $\neg p \wedge q$ se muestra en la figura 4-7*c*). Observe que las tablas de verdad de $\neg p \vee q$ y $p \rightarrow q$ son idénticas; es decir, ambas son falsas sólo en el segundo caso. Por consiguiente, $p \rightarrow q$ es lógicamente equivalente a $\neg p \vee q$; es decir,

$$p \rightarrow q \equiv \neg p \vee q$$

En otras palabras, la proposición condicional "Si p entonces q" es lógicamente equivalente a la proposición "No p o q" que sólo implica los conectivos $\vee$ y $\neg$, que ya formaba parte del lenguaje que se estableció antes, de modo que $p \rightarrow q$ se considera una abreviación de una proposición la cual se utiliza a menudo.

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

a) $p \rightarrow q$

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

b) $p \leftrightarrow q$

p	q	$\neg p$	$\neg p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

c) $\neg p \vee q$

Figura 4-7

4.9 ARGUMENTOS

Un *argumento* es una aseveración de que un conjunto dado de proposiciones $P_1, P_2, \ldots, P_n$, que se denominan *premisas*, conduce (tiene una consecuencia) a otra proposición Q, que se denomina *conclusión*. Un argumento se denota por

$$P_1, P_2, \ldots, P_n, \vdash Q$$

A continuación se formaliza el concepto de "argumento lógico" o "argumento válido":

Definición 4.4: Un argumento $P_1, P_2, \ldots, P_n, \vdash Q$ es *válido* si Q es verdadera siempre que todas las premisas $P_1, P_2, \ldots, P_n$ son verdaderas.

Un argumento que no es válido se denomina *falacia*.

EJEMPLO 4.4

a) El siguiente argumento es válido:

$$p, p \rightarrow q \vdash q \quad \textbf{(}\textbf{\textit{Ley de separación}}\textbf{)}$$

La demostración de esta regla se concluye a partir de la tabla de verdad de la figura 4-7*a*). En específico, p y $p \rightarrow q$ son verdaderas simultáneamente sólo en el caso (renglón) 1, y en este caso q es verdadera.

b) El siguiente argumento es una falacia:

$$p \rightarrow q, \; q \vdash p$$

Ya que ambas $p \rightarrow q$ y q son verdaderas en el caso (renglón) 3 en la tabla de verdad de la figura 4-7*a*), pero en este caso p es falsa.

Así, las proposiciones $P_1, P_2, \ldots, P_n$ son verdaderas simultáneamente si y sólo si la proposición $P_1 \wedge P_2 \wedge \ldots P_n$ es verdadera. Por tanto, el argumento $P_1, P_2, \ldots, P_n \vdash Q$ es válido si y sólo si Q es verdadera siempre que $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ es verdadero o, en forma equivalente, si la proposición $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \rightarrow Q$ es una tautología. Este resultado se plantea formalmente a continuación.

Teorema 4.3: El argumento $P_1, P_2, \ldots, P_n, \vdash Q$ es válido si y sólo si la proposición $(P_1 \wedge P_2 \ldots \wedge P_n) \rightarrow Q$ es una tautología.

Este teorema se aplica en el siguiente ejemplo.

EJEMPLO 4.5 Un principio fundamental del razonamiento lógico establece:

"Si p implica q y q implica r, entonces p implica r."

p	q	r	$[(p$	$\rightarrow$	$q)$	$\wedge$	$(q$	$\rightarrow$	$r)]$	$\rightarrow$	$(q$	$\rightarrow$	$r)$
V	V	V	V	V	V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	F	F	V	V	F	F
V	F	V	V	F	F	F	F	V	V	V	V	V	V
V	F	F	V	F	F	F	F	V	F	V	V	F	F
F	V	V	F	V	V	V	V	V	V	V	F	V	V
F	V	F	F	V	V	F	V	F	F	V	F	V	F
F	F	V	F	V	F	V	F	V	V	V	F	V	V
F	F	F	F	V	F	V	F	V	F	V	F	V	F
Paso			1	2	1	3	1	2	1	4	1	2	1

Figura 4-8

Es decir, el siguiente argumento es válido:

$$p \rightarrow q,\ q \rightarrow r \vdash p \rightarrow r \quad \textbf{(}\textbf{\textit{Ley del silogismo}}\textbf{)}$$

Este hecho se comprueba mediante la tabla de verdad en la figura 4-8, donde se muestra que la siguiente proposición es una tautología:

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$$

En forma equivalente, el argumento es válido puesto que las premisas $p \rightarrow q$ y $q \rightarrow r$ son verdaderas simultáneamente sólo en los casos (renglones) 1, 5, 7 y 8, y en estos casos la conclusión $p \rightarrow r$ también es verdadera. (Observe que la tabla de verdad requirió $2^3 = 8$ líneas porque hay tres variables: p, q y r.)

Ahora se aplica la teoría anterior a argumentos que implican proposiciones específicas. Se recalca que la validez de un argumento no depende de los valores de verdad ni del contenido de las proposiciones que aparecen en el argumento, sino de la forma particular del argumento. Esto se ilustra en el siguiente ejemplo.

EJEMPLO 4.6 Considere el siguiente argumento:

S_1: Si un hombre es un licenciado, es infeliz.
S_2: Si un hombre es infeliz, muere joven.

S : Los licenciados mueren jóvenes.

Aquí la proposición S bajo la línea es la conclusión del argumento, y las proposiciones S_1 y S_2 arriba de la línea son las premisas. Se afirma que el argumento $S_1, S_2 \vdash S$ es válido. Como el argumento es de la forma

$$p \rightarrow q,\ q \rightarrow r \vdash p \rightarrow r$$

donde p es "él es un licenciado", q es "él es infeliz y r es " él muere joven"; y por el ejemplo 4.5, este argumento (ley del silogismo) es válido.

4.10 FUNCIONES PROPOSICIONALES, CUANTIFICADORES

Sea A un conjunto dado. Una *función proposicional* (*oración* o *proposición abierta*) definida sobre A es una expresión

$$p(x)$$

que posee la propiedad de que $p(a)$ es verdadera o falsa para cada $a \in A$. Es decir, $p(x)$ se convierte en una proposición (con un valor de verdad) siempre que cualquier elemento $a \in A$ se sustituya por la variable x. El conjunto A se denomina *dominio* de $p(x)$, y el conjunto T_p de todos los elementos de A para los cuales $p(a)$ es verdadera se denomina *conjunto de verdad* de $p(x)$. En otras palabras,

$$T_p = \{x \mid x \in A,\ p(x) \text{ es verdadera}\} \quad \text{o} \quad T_p = \{x \mid p(x)\}$$

A menudo, cuando A es algún conjunto de números, la condición $p(x)$ tiene la forma de una ecuación o desigualdad que contiene la variable x.

EJEMPLO 4.7 Encuentre el conjunto de verdad para cada función proposicional $p(x)$ definida sobre el conjunto **N** de enteros positivos.

a) Sea $p(x)$ "$x + 2 > 7$". Su conjunto de verdad es $\{6, 7, 8, \ldots\}$, que consta de todos los enteros mayores que 5.

b) Sea $p(x)$ "$x + 5 < 3$". Su conjunto de verdad es el conjunto vacío $\varnothing$. Es decir, $p(x)$ no es verdadera para ningún entero en **N**.

c) Sea $p(x)$ "$x + 5 > 1$". Su conjunto de verdad es **N**. Es decir, $p(x)$ es verdadera para todo elemento en **N**.

Observación: El ejemplo anterior muestra que si $p(x)$ es una función proposicional definida sobre un conjunto A, entonces $p(x)$ puede ser verdadera para toda $x \in A$, para alguna $x \in A$ o para ninguna $x \in A$. En las dos subsecciones siguientes se analizan cuantificadores relacionados con tales funciones proposicionales.

Cuantificador universal

Sea $p(x)$ una función proposicional definida sobre un conjunto A. Considere la expresión

$$(\forall x \in A)p(x) \quad \text{o} \quad \forall x\, p(x) \tag{4.1}$$

que se lee "Para toda x en A, $p(x)$ es una proposición verdadera", o simplemente "Para toda x, $p(x)$". El símbolo

$$\forall$$

que se lee "para toda" o "para cada" se denomina *cuantificador universal*. La proposición (*4.1*) es equivalente a la proposición

$$T_p = \{x \mid x \in A,\ p(x)\} = A \tag{4.2}$$

es decir, que el conjunto de verdad de $p(x)$ es todo el conjunto A.

La expresión $p(x)$ es una oración o proposición abierta y en consecuencia carece de valor de verdad. Sin embargo, $\forall x\, p(x)$, que es $p(x)$ precedida por el cuantificador $\forall$ tiene un valor de verdad que se concluye a partir de la equivalencia de (*4.1*) y (*4.2*). En específico:

Q_1: Si $\{x \mid x \in A, p(x)\} = A$ entonces $\forall x\, p(x)$ es verdadera; en otro caso, $\forall x\, p(x)$ es falsa.

EJEMPLO 4.8

a) La proposición $(\forall n \in \mathbf{N})(n + 4 > 3)$ es verdadera puesto que $\{n \mid n + 4 > 3\} = \{1, 2, 3, \ldots\} = \mathbf{N}$.

b) La proposición $(\forall n \in \mathbf{N})(n + 2 > 8)$ es falsa puesto que $\{n \mid n + 2 > 8\} = \{7, 8, \ldots\} \neq \mathbf{N}$.

c) El símbolo $\forall$ define la intersección de una colección indexada $\{A_i \mid i \in I\}$ de conjuntos A_i como sigue:

$$\cap(A_i \mid i \in I) = \{x \mid \forall_i \in I,\ x \in A_i\}$$

Cuantificador existencial

Sea $p(x)$ una función proposicional definida sobre un conjunto A. Considere la expresión

$$(\exists x \in A)p(x) \quad \text{o} \quad \exists x,\, p(x) \tag{4.3}$$

que se lee "Existe una x en A tal que $p(x)$ es una proposición verdadera" o, simplemente, "Para alguna x, $p(x)$". El símbolo

$$\exists$$

que se lee "existe" o "para algún" o "al menos para un" se denomina *cuantificador existencial*. La proposición (*4.3*) es equivalente a la proposición

$$T_p = \{x \mid x \in A,\ p(x)\} \neq \varnothing \tag{4.4}$$

es decir, que el conjunto de verdad de $p(x)$ no es vacío. En consecuencia, $\exists x\, p(x)$; es decir, $p(x)$ precedida por el cuantificador $\exists$ tiene un valor de verdad. En específico:

Q_2: Si $\{x \mid p(x)\} \neq \varnothing$ entonces $\exists x\, p(x)$ es verdadera; en otro caso, $\exists x\, p(x)$ es falsa.

EJEMPLO 4.9

a) La proposición $(\exists n \in N)(n + 4 < 7)$ es verdadera puesto que $\{n \mid n + 4 < 7\} = \{1,\ 2\} \neq \varnothing$.

b) La proposición $(\exists n \in N)(n + 6 < 4)$ es falsa puesto que $\{n \mid n + 6 < 4\} = \varnothing$.

c) El símbolo $\exists$ define la unión de una colección indexada $\{A_i \mid i \in I\}$ de conjuntos A_i como sigue:

$$\cup(A_i \mid i \in I) = \{x \mid \exists\, i \in I,\ x \mid \in A_i\}$$

4.11 NEGACIÓN DE PROPOSICIONES CUANTIFICADAS

Considere la proposición: "Todos los especializados en matemáticas son varones". Su negación es:

> "No es cierto que todos los especializados en matemáticas son varones" o, en forma equivalente, "Existe por lo menos un especializado en matemáticas que es mujer (no varón)"

Con símbolos, si se usa M para denotar el conjunto de especializados en matemáticas lo anterior se escribe así

$$\neg(\forall x \in M)(x \text{ es varón}) \equiv (\exists\, x \in M)\ (x \text{ no es varón})$$

o, cuando $p(x)$ denota "x es varón",

$$\neg(\forall x \in M)\, p(x) \equiv (\exists\, x \in M) \neg p(x) \quad \text{o} \quad \neg \forall x p(x) \equiv \exists x \neg p(x)$$

Lo anterior es verdadero para cualquier proposición $p(x)$. Es decir:

Teorema 4.4 (de DeMorgan): $\neg(\forall x \in A)\, p(x) \equiv (\exists\, x \in A) \neg p(x)$.

En otras palabras, las dos proposiciones siguientes son equivalentes:

1) No es cierto que para toda $a \in A$, $p(a)$ es verdadera. 2) Existe una $a \in A$ tal que $p(a)$ es falsa.

Hay un teorema semejante para la negación de una proposición que contiene el cuantificador existencial.

Teorema 4.5 (de DeMorgan): $\neg(\exists x \in A)\, p(x) \equiv (\forall x \in A) \neg p(x)$.

Es decir, las dos proposiciones siguientes son equivalentes:

1) No es cierto que para alguna $a \in A$, $p(a)$ es verdadera. 2) Para toda $a \in A$, $p(a)$ es falsa.

EJEMPLO 4.10

a) Las siguientes proposiciones son negaciones mutuas:

"Para todos los enteros positivos n se cumple $n + 2 > 8$"
"Existe un entero positivo n tal que $n + 2 \not> 8$"

b) Las siguientes proposiciones también son negaciones mutuas:

"Existe una persona (viva) que tiene 150 años de edad"
"Toda persona viva no tiene 150 años de edad"

Observación: La expresión $\neg p(x)$ tiene el significado evidente:

"La proposición $\neg p(a)$ es verdadera cuando $p(a)$ es falsa, y viceversa"

Antes $\neg$ se usó como una operación sobre proposiciones; aquí $\neg$ se usa como una operación sobre funciones proposicionales. En forma semejante, $p(x) \wedge q(x)$ que se lee "$p(x)$ y $q(x)$", se define por:

"La proposición $p(a) \wedge q(a)$ es verdadera cuando $p(a)$ y $q(a)$ son verdaderas"

En forma semejante, $p(x) \vee q(x)$ que se lee "$p(x)$ o $q(x)$", se define por:

"La proposición $p(a) \vee q(a)$ es verdadera cuando $p(a)$ o $q(a)$ es verdadera"

Por tanto, en términos de conjuntos de verdad:

i) $\neg p(x)$ es el complemento de $p(x)$.
ii) $p(x) \wedge q(x)$ es la intersección de $p(x)$ y $q(x)$.
iii) $p(x) \vee q(x)$ es la unión de $p(x)$ y $q(x)$.

También es posible demostrar que las leyes para las proposiciones se cumplen para las funciones proposicionales. Por ejemplo, se tienen las leyes de DeMorgan:

$$\neg(p(x) \wedge q(x)) \equiv \neg p(x) \vee \neg q(x) \quad \text{y} \quad \neg(p(x) \vee q(x)) \equiv \neg p(x) \wedge \neg q(x)$$

Contraejemplo

El teorema 4.6 establece que demostrar que una proposición $\forall x$, $p(x)$ es falsa, es equivalente a demostrar que $\exists\, x \neg p(x)$ es verdadera o, en otras palabras, que existe un elemento x_0 con la propiedad de que $p(x_0)$ es falsa. Este elemento x_0 se denomina *contraejemplo* de la proposición $\forall x$, $p(x)$.

EJEMPLO 4.11

a) Considere la proposición $\forall x \in \mathbf{R}$, $|x| \neq 0$. La proposición es falsa puesto que 0 es un contraejemplo; es decir, $|0| \neq 0$ no es verdadera.

b) Considere la proposición $\forall x \in \mathbf{R}$, $x^2 \geq x$. La proposición no es verdadera puesto que, por ejemplo, $\frac{1}{2}$ es un contraejemplo. En específico, $(\frac{1}{2})^2 \geq \frac{1}{2}$ no es verdadera; es decir, $(\frac{1}{2})^2 < \frac{1}{2}$.

c) Considere la proposición $\forall x \in \mathbf{N}$, $x^2 \geq x$. Esta proposición es verdadera donde $\mathbf{N}$ es el conjunto de enteros positivos. En otras palabras, no existe ningún entero positivo n para el cual $n^2 < n$.

Funciones proposicionales con más de una variable

Una función proposicional (de n variables) definida sobre un conjunto producto $A = A_1 \times \cdots \times A_n$ expresiones se expresa con

$$p(x_1, x_2, \ldots, x_n)$$

con la propiedad de que $p(a_1, a_2, \ldots, a_n)$ es verdadera o falsa para cualquier n-eada $(a_1, \ldots, a_n)$ en A. Por ejemplo,

$$x + 2y + 3z < 18$$

es una función proposicional sobre $\mathbf{N}^3 = \mathbf{N} \times \mathbf{N} \times \mathbf{N}$. Tal función proposicional no tiene valor de verdad. Sin embargo, se hace lo siguiente:

Principio básico: Una función proposicional precedida por un cuantificador para cada variable, por ejemplo,

$$\forall x \exists y,\ p(x, y) \quad \text{o} \quad \exists x\, \forall y\, \exists z,\ p(x, y, z)$$

denota una proposición y tiene un valor de verdad.

EJEMPLO 4.12 Sea $B = \{1, 2, 3, \ldots, 9\}$ y sea $p(x, y)$ que denota "$x + y = 10$". Entonces $p(x, y)$ es una función proposicional sobre $A = B^2 = B \times B$.

a) La siguiente es una proposición puesto que para cada variable hay un cuantificador:

$$\forall x \exists y,\ p(x, y) \quad \text{es decir,} \quad \text{"Para toda } x \text{ existe una } y \text{ tal que } x + y = 10\text{"}$$

Esta proposición es verdadera. Por ejemplo, si $x = 1$, sea $y = 9$; si $x = 2$, sea $y = 8$ y así en lo sucesivo.

b) La siguiente también es una proposición:

$$\exists y \forall x,\ p(x, y), \quad \text{es decir,} \quad \text{"Existe una } y \text{ tal que, para toda } x, \text{ se tiene } x + y = 10\text{"}$$

No existe ninguna y así; por tanto, esta proposición es falsa.

Observe que la única diferencia entre *a*) y *b*) es el orden de los cuantificadores. Entonces, un orden distinto de los cuantificadores lleva a una proposición diferente. Se observa que al traducir estas proposiciones cuantificadas a lenguaje coloquial, la expresión "tal que" a menudo aparece a continuación de "existe".

Negación de proposiciones cuantificadas con más de una variable

La negación de las proposiciones cuantificadas con más de una variable se obtiene al aplicar los teoremas 4.5 y 4.6. Así, cada $\forall$ se cambia por $\exists$ y cada $\exists$ se cambia por $\forall$ a medida que el símbolo de negación $\neg$ recorre la proposición de izquierda a derecha. Por ejemplo

$$\begin{aligned} \neg[\forall x \exists y \exists z,\ p(x, y, z)] &\equiv \exists x \neg[\exists y \exists z,\ p(x, y, z)] \equiv \neg \exists z \forall y[\exists z,\ p(x, y, z) \\ &\equiv \exists x \forall y \forall z,\ \neg p(x, y, z) \end{aligned}$$

Por supuesto, al negar estas proposiciones cuantificadas no se escriben todos los pasos.

EJEMPLO 4.13

a) Considere la proposición cuantificada:

"Todo estudiante tiene por lo menos un curso en el cual el docente es un asistente del profesor titular".

Su negación es la proposición:

"Existe un estudiante tal que en todo curso el docente no es un asistente del profesor titular".

b) A continuación se proporciona la definición formal de que L es el límite de una sucesión $a_1, a_2, \ldots$:

$$\forall \in > 0, \exists\, n_0 \in \mathrm{N},\ \forall n > n_0 \text{ se tiene } |\, a_n - L| < \in$$

Entonces, L no es el límite de la sucesión $a_1, a_2, \ldots$, cuando:

$$\exists \in > 0, \forall n_0 \in \mathrm{N},\ \exists\, n > n_0 \text{ tal que } |\, a_n - L| \geq \in$$

PROBLEMAS RESUELTOS

PROPOSICIONES Y TABLAS DE VERDAD

4.1 Sean p "Hace frío" y q "Está lloviendo". Proporcionar una oración coloquial sencilla que describa cada una de las siguientes proposiciones: *a*) $\neg p$; *b*) $p \vee q$; *c*) $p \wedge q$; *d*) $q \vee \neg q$.

En cada caso, $\wedge$, $\vee$ y $\sim$ se traducen por "y", "o" y "es falso que" o "no", respectivamente, y luego se simplifica la oración en lenguaje coloquial.

a) No hace frío.
b) Hace frío y está lloviendo.
c) Hace frío o está lloviendo.
d) Está lloviendo o no hace frío.

4.2. Encontrar la tabla de verdad de $\neg p \wedge q$.

La tabla de verdad de $\neg p \wedge q$ se construye como en la figura 4-9*a*).

p	q	$\neg p$	$\neg p \wedge q$
V	V	F	F
V	F	F	F
F	V	V	V
F	F	V	F

a) $\neg p \wedge q$

p	q	$p \wedge q$	$\neg (p \wedge q)$	$p \vee \neg (p \wedge q)$
V	V	V	F	V
V	F	F	V	V
F	V	F	V	V
F	F	F	V	V

b) $p \vee \neg (p \wedge q)$

Figura 4-9

4.3 Compruebe que la proposición $p \vee \neg(p \wedge q)$ es una tautología.

La tabla de verdad de $p \vee \neg(p \wedge q)$ se construye como se muestra en la figura 4-9*b*). Puesto que el valor de verdad de $p \vee \neg(p \wedge q)$ es V para todos los valores de p y q, la proposición es una tautología.

4.4 Demuestre que las proposiciones $\neg(p \wedge q)$ y $\neg p \vee \neg q$ son lógicamente equivalentes.

Las tablas de verdad de $\neg(p \wedge q)$ y $\neg p \vee \neg q$ se construyen como en la figura 4-10. Puesto que las tablas de verdad son las mismas (ambas proposiciones son falsas en el primer caso y verdaderas en los otros tres), las proposiciones $\neg(p \wedge q)$ y $\neg p \vee \neg q$ son lógicamente equivalentes y puede escribirse

$$\neg(p \wedge q) \equiv \neg p \vee \neg q.$$

p	q	$p \wedge q$	$\neg (p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

a) $\neg (p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

b) $\neg p \vee \neg q$

Figura 4-10

4.5 Con las leyes de la tabla 4-1, demostrar que $\neg(p \wedge q) \vee (\neg q \wedge q) \equiv \neg q$.

	Proposición		**Razón**
1)	$\neg(p \vee q) \vee (\neg p \wedge q)$	$\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q)$	Ley de DeMorgan
2)		$\equiv \neg p \wedge (\neg q \vee q)$	Ley distributiva
3)		$\equiv \neg p \wedge T$	Ley de complementos
4)		$\equiv \neg p$	Ley de identidad

PROPOSICIONES CONDICIONALES

4.6 Reescriba las siguientes proposiciones sin usar el condicional:

a) Si hace frío, él lleva sombrero.
b) Si aumenta la productividad, entonces suben los salarios.

Recuerde que "Si p entonces q" es equivalente a "No p o q"; es decir, $p \rightarrow q \equiv \neg p \vee q$. Por tanto,

a) No hace frío o él lleva sombrero.
b) La productividad no aumenta o suben los salarios.

4.7 Considere la proposición condicional $p \rightarrow q$. Las proposiciones simples $q \rightarrow p$, $\neg p \rightarrow \neg q$ y $\neg q \rightarrow \neg p$ se denominan, respectivamente, *recíproca*, *inversa* y *contrapositiva* de la condicional $p \rightarrow q$. ¿Cuáles de estas proposiciones son lógicamente equivalentes a $p \rightarrow q$, en caso de haber alguna?

Sus tablas de verdad se construyen como en la figura 4-11. Sólo la contrapositiva $\neg q \rightarrow \neg p$ es lógicamente equivalente a la proposición condicional original $p \rightarrow q$.

p	q	$\neg p$	$\neg q$	Condicional $p \rightarrow q$	Recíproca $q \rightarrow p$	Inversa $\neg p \rightarrow \neg q$	Contrapositiva $\neg q \rightarrow \neg p$
V	V	F	F	V	V	V	V
V	F	F	V	F	V	V	F
F	V	V	F	V	F	F	V
F	F	V	V	V	V	V	V

Figura 4-11

4.8 Determine la contrapositiva de cada proposición:

a) Si Eric es poeta, entonces es pobre.
b) Sólo si Marcos estudia aprobará el examen.

a) La contrapositiva de $p \rightarrow q$ es $\neg q \rightarrow \neg p$. Por tanto, la contrapositiva es:

Si Eric no es pobre, entonces no es poeta.

b) La proposición es equivalente a: "Si Marcos aprueba el examen, entonces estudió." Por tanto, su contrapositiva es:

Si Marcos no estudia, entonces no aprobará el examen.

4.9 Escriba la negación de cada una de las siguientes proposiciones en la forma más sencilla posible:

a) Si ella trabaja, ganará dinero.
b) Él nada si y sólo si el agua está tibia.
c) Si nieva, entonces ellos no conducen el automóvil.

a) Observe que $\neg(p \rightarrow q) \equiv p \wedge \neg q$; por tanto, la negación de la proposición es:

Ella trabaja o no ganará dinero.

b) Observe que $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$; por tanto, la negación de la proposición es cualquiera de las siguientes:

Él nada si y sólo si el agua no está tibia.
Él no nada si y sólo si el agua está tibia.

c) Observe que $\neg(p \rightarrow \neg q) \equiv p \wedge \neg\neg q \equiv p \wedge q$; por tanto, la negación de la proposición es:

Nieva y ellos conducen el automóvil.

ARGUMENTOS

4.10 Demuestre que el siguiente argumento es una falacia: $p \rightarrow q, \neg p \vdash \neg q$.

La tabla de verdad de $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ se construye como en la figura 4-12. Puesto que la proposición $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ no es una tautología, el argumento es una falacia. En forma equivalente, el argumento es una falacia puesto que en la tercera línea de la tabla de verdad $p \rightarrow q$ y $\neg p$ son verdaderas pero $\neg q$ es falsa.

p	q	$p \rightarrow q$	$\neg p$	$(p \rightarrow q) \wedge \neg p$	$\neg q$	$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg p$
V	V	V	F	F	F	V
V	F	F	F	F	V	V
F	V	V	V	V	F	F
F	F	V	V	V	V	V

Figura 4-12

4.11 Determine la validez del siguiente argumento: $p \rightarrow q, \neg p \vdash \neg p$.

La tabla de verdad de $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ se construye como en la figura 4-13. Puesto que la proposición $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ es una tautología, el argumento es válido.

p	q	$[(p$	$\rightarrow$	$q)$	$\wedge$	$\neg$	$q]$	$\rightarrow$	$\neg$	p
V	V	V	V	V	F	F	V	V	F	V
V	F	V	F	F	F	V	F	V	F	V
F	V	F	V	V	F	F	V	V	V	F
F	F	F	V	F	V	V	F	V	V	F
Paso		1	2	1	3	2	1	4	2	1

Figura 4-13

4.12 Demuestre que el siguiente argumento es válido: $p \rightarrow \neg q, r \rightarrow q, r \vdash \neg p$.

La tabla de verdad de las premisas y conclusiones se muestran en la figura 4-14*a*). Luego, $p \rightarrow \neg q$, $r \rightarrow q$, y r son verdaderas simultáneamente sólo en el quinto renglón de la tabla, donde $\neg p$ también es verdadera. Por tanto, el argumento es válido.

	p	q	r	$p \rightarrow \neg q$	$r \rightarrow q$	$\neg q$
1	V	V	V	F	V	F
2	V	V	F	F	V	F
3	V	F	V	V	F	F
4	V	F	F	V	V	F
5	F	V	V	V	V	V
6	F	V	F	V	V	V
7	F	F	V	V	F	V
8	F	F	F	V	V	V

a)

p	q	$\neg q$	$p \rightarrow \neg q$	$\neg p$
V	V	F	F	F
V	F	V	V	F
F	V	F	V	V
F	F	V	V	V

b)

Figura 4-14

4.13 Determine la validez del siguiente argumento:

Si 7 es menor que 4, entonces 7 no es un número primo.
7 no es menor que 4.

---

7 es un número primo.

Primero debe traducir el argumento a su forma simbólica: sean p "7 es menor que 4" y q "7 es un número primo". Entonces el argumento es de la forma

$$p \to \neg q,\ \neg q \vdash q$$

Luego, se construye una tabla de verdad como se muestra en la figura 4-14*b*). Se demuestra que el argumento anterior es una falacia puesto que, en la cuarta línea de la tabla de verdad, las premisas $p \to \neg q$ y $\neg p$ son verdaderas, pero la conclusión q es falsa.

Observación: El que la conclusión del argumento sea una proposición verdadera es irrelevante respecto al hecho de que el argumento presentado es una falacia.

4.14 Pruebe la validez del siguiente argumento:

Si dos lados de un triángulo son iguales, entonces los ángulos opuestos son iguales.
Dos lados de un triángulo no son iguales.

Los ángulos opuestos de un triángulo no son iguales.

Primero se traduce el argumento a la forma simbólica $p \to q, \neg p \vdash \neg q$, donde p es "Dos lados de un triángulo son iguales" y q es "Los ángulos opuestos son iguales". De acuerdo con el problema 4.10, este argumento es una falacia.

Observación: Aunque la conclusión *es una* consecuencia de la segunda premisa y los axiomas de la geometría euclidiana, el argumento anterior no constituye tal demostración puesto que el argumento es una falacia.

CUANTIFICADORES Y FUNCIONES PROPOSICIONALES

4.15 Sea $A = \{1, 2, 3, 4, 5\}$. Determine el valor de verdad de cada una de las siguientes proposiciones:

a) $(\exists x \in A)(x + 3 = 10)$ *c*) $(\exists x \in A)(x + 3 < 5)$

b) $(\forall x \in A)(x + 3 < 10)$ *d*) $(\forall x \in A)(x + 3 \leq 7)$

a) Falsa, ya que ningún número en A es una solución de $x + 3 = 10$.

b) Verdadera, ya que todo número en A satisface $x + 3 < 10$.

c) Verdadera, ya que si $x_0 = 1$, entonces $x_0 + 3 < 5$; es decir, 1 es una solución.

d) Falsa, ya que si $x_0 = 5$, entonces $x_0 + 3$ no es menor o igual que 7. En otras palabras, 5 no es una solución de la condición dada.

4.16 Determine el valor de verdad de cada una de las siguientes proposiciones, donde $\mathbf{U} = \{1, 2, 3\}$ es el conjunto universo:

a) $\exists x \forall y,\ x^2 < y + 1$; *b*) $\forall x \exists y,\ x^2 + y^2 < 12$; *c*) $\forall x \forall y,\ x^2 + y^2 < 12$.

a) Verdadera, ya que si $x = 1$, entonces 1, 2 y 3 son soluciones de $1 < y + 1$.

b) Verdadera. Para todo x_0, sea $y = 1$; entonces $x_0^2 + 1 < 12$ es una proposición verdadera.

c) Falsa, ya que si $x_0 = 2$ y $y_0 = 3$, entonces $x_0^2 + y_0^2 < 12$ no es una proposición verdadera.

4.17 Niegue cada una de las siguientes proposiciones:

a) $\exists x\ \forall y,\ p(x, y)$; *b*) $\exists x\ \forall y,\ p(x, y)$; *c*) $\exists y\ \exists x\ \forall z,\ p(x, y, z)$.

Se usa $\neg \forall x\ p(x) \equiv \exists x \neg p(x)$ y $\neg \exists x\ p(x) \equiv \forall x \neg p(x)$:

a) $\neg(\exists x \forall y,\ p(x, y)) \equiv \forall x \exists y \neg p(x, y)$

b) $\neg(\forall x \forall y,\ p(x, y)) \equiv \exists x \exists y \neg p(x, y)$

c) $\neg(\exists y\ \exists x\ \forall z,\ p(x, y, z)) \equiv \forall y\ \forall x\ \exists z \neg p(x, y, z)$

4.18 Sea $p(x)$ la oración "$x + 2 > 5$". Concluya si $p(x)$ es o no una función proposicional sobre cada uno de los siguientes conjuntos: *a*) **N**, el conjunto de enteros positivos; *b*) $M = \{-1, -2, -3, \ldots\}$; *c*) C, el conjunto de números complejos.

a) Sí.

b) Aunque $p(x)$ es falsa para cualquier elemento en M, $p(x)$ sigue siendo una función proposicional sobre M.

c) No. Observe que $2i + 2 > 5$ no tiene ningún sentido. En otras palabras, las desigualdades no están definidas para los números complejos.

4.19 Niegue cada una de las siguientes proposiciones: *a*) Todos los estudiantes viven en los dormitorios. *b*) Todos los especializados en matemáticas son varones. *c*) Algunos estudiantes tienen 25 o más años de edad.

Se usa el teorema 4.4 para negar los cuantificadores.

a) Por lo menos un estudiante no vive en los dormitorios. (Algunos estudiantes no viven en los dormitorios.)

b) Por lo menos un especializado en matemáticas es mujer. (Algunas especializadas en matemáticas son mujeres.)

c) Ninguno de los estudiantes tiene 25 o más años de edad. (Todos los estudiantes son menores de 25 años de edad.)

PROBLEMAS SUPLEMENTARIOS

PROPOSICIONES Y TABLAS DE VERDAD

4.20 Sean p "Es rico" y q "Es feliz". Escriba cada proposición en forma simbólica, use p y q. Observe que "Es pobre" y "Es infeliz" son equivalentes a $\neg p$ y $\neg q$, respectivamente.

a) Si es rico, entonces es infeliz.

b) No es rico ni feliz.

c) Es necesario ser pobre para ser feliz.

d) Ser pobre es ser infeliz.

4.21 Encuentre las tablas de verdad para *a*) $p \vee \neg q$; *b*) $\neg p \wedge \neg q$.

4.22 Compruebe que la proposición $(p \wedge q) \wedge \neg(p \vee q)$ es una contradicción.

ARGUMENTOS

4.23 Pruebe la validez de cada argumento:

a) Si llueve, Eric se enfermará.
No llovió.

Eric no estaba enfermo.

b) Si llueve, Eric se enfermará.
Eric no estaba enfermo.

No llovió.

4.24 Probar la validez del siguiente argumento:

Si estudio, entonces no reprobaré matemáticas.
Si no juego basquetbol, entonces estudiaré.
Pero reprobé matemáticas.

Por tanto, debo haber jugado basquetbol.

CUANTIFICADORES

4.25 Sea $A = \{1, 2, \ldots, 9, 10\}$. Considere cada una de las siguientes oraciones. Si se trata de una proposición, determine su valor de verdad; si se trata de una función proposicional, determine su conjunto de verdad.

a) $(\forall x \in A)(\exists y \in A)(x + y < 14)$

b) $(\forall y \in A)(x + y < 14)$

c) $(\forall x \in A)(\forall y \in A)(x + y < 14)$

d) $(\exists y \in A)(x + y < 14)$

4.26 Niegue cada una de las siguientes proposiciones:

a) Si el profesor está ausente, entonces algunos estudiantes no terminan su tarea.
b) Todos los estudiantes terminaron su tarea y el profesor está presente.
c) Algunos de los estudiantes no terminaron su tarea o el profesor está ausente.

4.27 Niegue cada proposición en el problema 4.15.

4.28 Proporcione un contraejemplo para cada proposición, donde $\mathbf{U} = \{3, 5, 7, 9\}$ es el conjunto universo:

a) $\forall x, x + \geq 7$, *b*) $\forall x$, x es impar, *c*) $\forall x$, x es primo, *d*) $\forall x, |x| = x$

Respuestas a los problemas suplementarios

4.20 *a*) $p \rightarrow \neg q$; *b*) $\neg p \wedge \neg q$; *c*) $q \rightarrow \neg p$; *d*) $\neg p \rightarrow \neg q$.

4.21 *a*) V, V, F, V; *b*) F, F, F, V.

4.22 Se construye su tabla de verdad. Es una contradicción puesto que su tabla de verdad es falsa para todos los valores de p y q.

4.23 Primero se traducen los argumentos a su forma simbólica: p por "Llueve" y q por "Eric está enfermo":

a) $p \rightarrow q, \neg p \vdash \neg q$ *b*) $p \rightarrow q, \neg q \vdash \neg p$

Por el problema 4.10, *a*) es una falacia. Por el problema 4.11, *b*) es válida.

4.24 Sean p "Estudio", q "Reprobé matemáticas" y r "Juego basquetbol". El argumento tiene la forma:

$$p \rightarrow \neg q, \neg r \rightarrow p, q \vdash r$$

Se construyen las tablas de verdad como en la figura 4-15, donde las premisas $p \rightarrow \neg q$, $\neg r \rightarrow p$, y q son verdaderas simultáneamente sólo en la quinta línea de la tabla, y en ese caso la conclusión r también es verdadera. Por tanto, el argumento es válido.

p	q	r	$\neg q$	$p \rightarrow \neg q$	$\neg r$	$\neg r \rightarrow p$
V	V	V	F	F	F	V
V	V	F	F	F	V	V
V	F	V	V	V	F	V
V	F	F	V	V	V	V
F	V	V	F	V	F	V
F	V	F	F	V	V	F
F	F	V	V	V	F	V
F	F	F	V	V	V	F

Figura 4-15

4.25 *a*) La proposición abierta en dos variables está precedida por dos cuantificadores; por tanto, se trata de una proposición. Además, la proposición es verdadera.

b) La proposición abierta está precedida por un cuantificador; por tanto, se trata de una función proposicional de la otra variable. Observe que para todo $y \in A$, $x_0 + y < 14$ si y sólo si $x_0 = 1, 2$ o 3. Por tanto, el conjunto de verdad es $\{1, 2, 3\}$.

c) Se trata de una proposición y es falsa: si $x_0 = 8$ y $y_0 = 9$, entonces $x_0 + y_0 < 14$ no es verdadera.

d) Es una oración abierta en x. El conjunto de verdad es A en sí mismo.

4.26 *a*) El profesor está ausente y todos los estudiantes terminaron su tarea.

b) Algunos estudiantes no terminaron su tarea o el profesor está ausente.

c) Todos los estudiantes terminaron su tarea y el profesor está presente.

4.27 *a*) $(\forall x \in A)(x + 3 \neq 10)$ *c*) $(\forall x \in A)(x + 3 \geq 5)$
b) $(\exists x \in A)(x + 3 \geq 10)$ *d*) $(\exists x \in A)(x + 3 > 7)$

4.28 *a*) Aquí 3 es un contraejemplo.

b) La proposición es verdadera; por tanto, no existe ningún contraejemplo.

c) Aquí el único contraejemplo es 9.

d) La proposición es verdadera; por tanto, no existe ningún contraejemplo.

5 Técnicas de conteo

CAPÍTULO

5.1 INTRODUCCIÓN

En este capítulo se desarrollan algunas técnicas para determinar, sin enumeración directa, el número de resultados posibles de un evento particular o el número de elementos en un conjunto. Este conteo sofisticado, que algunas veces se denomina *análisis combinatorio*, incluye el estudio de permutaciones y combinaciones.

5.2 PRINCIPIOS BÁSICOS DE CONTEO

A lo largo de este capítulo se utilizan dos principios de conteo básicos. El primero implica la adición y el segundo, la multiplicación.

Principio de la regla de la suma:

Suponga que algún evento E puede ocurrir en m formas y que un segundo evento F puede ocurrir en n formas, pero ambos eventos no pueden ser simultáneos. Entonces E o F puede ocurrir en $m + n$ formas.

Principio de la regla del producto:

Suponga que un evento E ocurre en m formas e, independientemente de este evento, hay un segundo evento F que puede ocurrir en n formas. Entonces la combinación de E y F ocurre en mn formas.

Los principios indicados pueden extenderse a tres o más eventos. Es decir, suponga un evento E_1 que puede ocurrir en n_1 formas, un evento E_2 que puede ocurrir en n_2 formas, y a continuación de E_2, un tercer evento, E_3, puede ocurrir en n_3 formas y así en lo sucesivo. Entonces:

Regla de la suma: Si ningún par de eventos puede ocurrir al mismo tiempo, entonces uno de los eventos ocurre en:

$$n_1 + n_2 + n_3 + \cdots \text{ formas.}$$

Regla del producto: Si los eventos ocurren uno después del otro, entonces todos los eventos ocurren en el orden indicado en:

$$n_1 \cdot n_2 \cdot n_3 \cdot \ldots \text{ formas.}$$

EJEMPLO 5.1 Suponga que en una universidad se imparten 3 cursos diferentes de historia, 4 cursos diferentes de literatura y 2 cursos diferentes de sociología.

a) El número m de formas en que los estudiantes pueden escoger un curso de cada área es:

$$m = 3(4)(2) = 24$$

b) El número n de formas en que un estudiante puede escoger justo uno de los cursos es:

$$n = 3 + 4 + 2 = 9$$

Hay una interpretación teórica de estos dos principios. Con más precisión, suponga que $n(A)$ denota el número de elementos en un conjunto A. Entonces:

1) ***Principio de la regla de la suma*:** Suponga que A y B son conjuntos ajenos. Entonces

$$n(A \cup B) = n(A) + n(B)$$

2) ***Principio de la regla del producto*:** Sea $A \times B$ el producto cartesiano de los conjuntos A y B. Entonces

$$n(A \times B) = n(A) \cdot n(B)$$

5.3 FUNCIONES MATEMÁTICAS

A continuación se analizan dos funciones matemáticas importantes por su uso continuo en teoría combinatoria.

Función factorial

El producto de los enteros positivos desde 1 hasta n, incluso, se denota por $n!$ y se lee "n factorial". A saber,

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-2)(n-1)n = n(n-1)(n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

En consecuencia, $1! = 1$ y $n! = n(n - l)!$ También es conveniente definir $0! = 1$.

EJEMPLO 5.2

a) $3! = 3 \cdot 2 \cdot 1 = 6, \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24, \quad 5 = 5 \cdot 4! = 5(24) = 120.$

b) $\dfrac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} = \dfrac{12 \cdot 11 \cdot 10 \cdot 9!}{3 \cdot 2 \cdot 1 \cdot 9!} = \dfrac{12!}{3!\,9!}$ y, en forma más general,

$$\frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 3 \cdot 2 \cdot 1} = \frac{n(n-1)\cdots(n-r+1)(n-r)!}{r(r-1)\cdots 3 \cdot 2 \cdot 1 \cdot (n-r)!} = \frac{n!}{r!(n-r)!}$$

c) Para n grande, se aplica la aproximación de Stirling (donde $e = 2.7128\ldots$):

$$n! = \sqrt{2\pi n}\, n^n e^{-n}$$

Coeficientes binomiales

El símbolo $\binom{n}{r}$, que se lee "*nCr*" o "de *n* elementos se eligen *r*", donde *r* y *n* son enteros positivos con $r \leq n$, se define como sigue:

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r(r-1)\ldots 3\cdot 2\cdot 1} \quad \text{o, en forma equivalente} \quad \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Observe que $n-(n-r)=r$. Esto conduce a la siguiente relación importante.

Lema 5.1: $\binom{n}{n-r} = \binom{n}{r}$ o, en forma equivalente, $\binom{n}{a} = \binom{n}{b}$, donde $a+b=n$.

Con la motivación derivada del hecho de haber definido $0!=1$, se define:

$$\binom{n}{0} = \frac{n!}{0!n!} = 1 \quad \text{y} \quad \binom{0}{0} = \frac{0!}{0!\,0!} = 1$$

EJEMPLO 5.3

a) $\binom{8}{2} = \frac{8\cdot 7}{2\cdot 1} = 28$; $\binom{9}{4} = \frac{9\cdot 8\cdot 7\cdot 6}{4\cdot 3\cdot 2\cdot 1} = 126$; $\binom{12}{5} = \frac{12\cdot 11\cdot 10\cdot 9\cdot 8}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 792$.

Observe que $\binom{n}{r}$ tiene exactamente *r* factores tanto en el numerador como en el denominador.

b) Suponga que se desea calcular $\binom{10}{7}$. Hay 7 factores tanto en el numerador como en el denominador.

Sin embargo, 10 – 7 = 3. Así, se aplica el lema 5.1 para calcular:

$$\binom{10}{7} = \binom{10}{3} = \frac{10\cdot 9\cdot 8}{3\cdot 2\cdot 1} = 120$$

Coeficientes inomiales tri ngulo de P ascal

Los números $\binom{n}{r}$ se denominan *coeficientes binomiales*, ya que aparecen como los coeficientes en el desarrollo de $(a+b)^n$. Específicamente:

Teorema (del inomio) 5.2: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{r} a^{n-k}b^k$

Los coeficientes de las potencias consecutivas de $a+b$ pueden escribirse en un arreglo triangular de números, denominado triángulo de Pascal, como se muestra en la figura 5-1. Los números en el triángulo de Pascal poseen las siguientes propiedades interesantes:

i) En cada renglón, el primero y el último número es 1.

ii) Cualquier otro número se obtiene al sumar los dos números que aparecen arriba de él. Por ejemplo:

$$10 = 4+6, \quad 15 = 5+10, \quad 20 = 10+10$$

Puesto que estos números son coeficientes binomiales, a continuación se presenta el planteamiento formal de lo anterior.

$$
\begin{aligned}
(a+b)^0 &= 1 \\
(a+b)^1 &= a + b \\
(a+b)^2 &= a^2 + 2ab + b^2 \\
(a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\
(a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
(a+b)^5 &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\
(a+b)^6 &= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\
&\cdots\cdots\cdots\cdots
\end{aligned}
\qquad
\begin{array}{c}
1 \\
1\quad 1 \\
1\quad 2\quad 1 \\
1\quad 3\quad 3\quad 1 \\
1\quad 4\quad 6\quad 4\quad 1 \\
1\quad 5\quad 10\quad 10\quad 5\quad 1 \\
1\quad 6\quad 15\quad 20\quad 15\quad 6\quad 1 \\
\cdots\cdots\cdots
\end{array}
$$

Figura 5-1 Triángulo de Pascal

Teorema 5.3: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

5.4 PERMUTACIONES

Cualquier arreglo de un conjunto de n objetos en un orden dado se denomina *permutación* del objeto (tomando todos a la vez). Cualquier arreglo de cualesquiera $r \leq n$ de estos objetos en un orden dado se denomina "r-permutación" o "permutación de los n objetos tomando r a la vez". Considere, por ejemplo, el conjunto de letras A, B, C, D. Entonces

i) *BDCA*, *DCBA* y *ACDB* son permutaciones de las cuatro letras (tomando todas al mismo tiempo).

ii) *BAD*, *ACB* y *DBC* son permutaciones de las cuatro letras tomando tres a la vez.

iii) *AD*, *BC* y *CA* son permutaciones de las cuatro letras tomando dos a la vez.

Normalmente se tiene interés en el número de tales permutaciones sin enumerarlas.
El número de permutaciones de n objetos tomando r a la vez se denota por

$$P(n, r) \quad \text{(otros textos usan } {}_nP_r,\ P_{n,r},\ \text{o } (n)_r).$$

El siguiente teorema se aplica.

Teorema 5.4: $P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \dfrac{n!}{(n-r)!}$

Se recalca que en $n(n-1)(n-2)\cdots(n-r+1)$ hay r factores.

EJEMPLO 5.4 Encuentre el número m de permutaciones de seis objetos: A, B, C, D, E, F, tomando tres a la vez. En otras palabras, encuentre el número de "palabras de tres letras" que usen sólo las seis letras dadas sin repetición.

La palabra general de tres letras se representará con las tres siguientes posiciones:

$$\text{\_\_\_}, \quad \text{\_\_\_}, \quad \text{\_\_\_}$$

La primera letra puede elegirse en seis formas; luego, la segunda letra puede elegirse en 5 formas; y, por último, la tercera letra puede escogerse en 4 formas. Cada número se escribe en su posición correcta como sigue:

$$\underline{6}, \quad \underline{5}, \quad \underline{4}$$

Por la regla del producto, a partir de las seis letras hay $m = 6 \cdot 5 \cdot 4 = 120$ palabras posibles de tres letras sin repetición. A saber, hay 120 permutaciones de 6 objetos tomando 3 a la vez. Esto coincide con la fórmula en el teorema 5.4:

$$P(6, 3) = 6 \cdot 5 \cdot 4 = 120$$

De hecho, el teorema 5.4 se demuestra en la misma forma como se hizo para este caso particular.

Considere ahora el caso especial de $P(n, r)$ cuando $r = n$. Se obtiene el siguiente resultado.

Corolario 5.5: Hay $n!$ permutaciones de n objetos (tomando todos a la vez).

Por ejemplo, hay $3! = 6$ permutaciones de las letras *A*, *B*, *C*. Estas permutaciones son

$$ABC, \quad ACB, \quad BAC, \quad BCA, \quad CAB, \quad CBA.$$

Permutaciones con repeticiones

A menudo es necesario conocer el número de permutaciones en un multiconjunto; es decir, un conjunto de objetos de los cuales algunos son iguales. Entonces,

$$P(n;\ n_1,\ n_2,\ \ldots,\ n_r)$$

denota el número de permutaciones de n objetos, en donde hay n_1 iguales, n_2 iguales, $\ldots$, n_r iguales. A continuación se presenta la fórmula general:

Teorema 5.6: $P(n;\ n_1,\ n_2, \ldots,\ n_r) = \dfrac{n!}{n_1!\,n_2!\ldots n_r!}$

La demostración del teorema 5.6 se indica mediante un ejemplo particular. Suponga que desea formar todas las "palabras" posibles de cinco letras con las letras de la palabra "*BABBY*". Hay $5! = 120$ permutaciones de los objetos B_1, *A*, B_2, B_3, *Y*, donde se han identificado las tres letras *B*. Observe que las seis permutaciones siguientes

$$B_1B_2\,B_3AY, \quad B_2B_1\,B_3AY, \quad B_3B_1\,B_2AY, \quad B_1B_3\,B_2AY, \quad B_2B_3\,B_1AY, \quad B_3B_2\,B_1AY$$

producen la misma palabra cuando se suprimen los subíndices. El 6 proviene del hecho de que hay $3! = 3 \cdot 2 \cdot 1 = 6$ formas distintas de colocar las tres letras *B* en las tres primeras posiciones en la permutación. Esto es cierto para cada conjunto de tres posiciones en que pueden aparecer las letras *B*. En consecuencia, el número de palabras diferentes de cinco letras que pueden formarse con las letras de la palabra "*BABBY*" es:

$$P(5; 3) = \frac{5!}{3!} = 20$$

EJEMPLO 5.5 Encuentre el número m de palabras de siete letras que pueden formarse con las letras de la palabra "*BENZENE*".

Se busca el número de permutaciones de 7 objetos, de los cuales 3 son iguales (las tres letras *E*) y 2 son iguales (las dos letras *N*). Por el teorema 5.6,

$$m = P(7;\ 3,\ 2) = \frac{7!}{3!2!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 420$$

Muestras ordenadas

Muchos problemas tienen que ver con la elección de un elemento de un conjunto *S* con, por ejemplo, n elementos. Cuando un elemento se elige después de otro; por ejemplo r veces, la elección se denomina *muestra ordenada* de tamaño r. Se consideran dos casos.

1) Muestreo con reemplazo

Aquí el elemento se devuelve al conjunto *S* antes de elegir el siguiente elemento. Por tanto, cada vez hay n formas de elegir un elemento (se permiten las repeticiones). La regla del producto establece que el número de tales muestras es:

$$n \cdot n \cdot n \cdots n \cdot n(r \text{ factores}) = n^r$$

2) Muestreo sin reemplazo

Aquí el elemento no se regresa al conjunto S antes de elegir el siguiente elemento. Por tanto, en la muestra ordenada no hay repeticiones. Una muestra así es simplemente una r-permutación. Por tanto, el número de estas muestras es:

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

EJEMPLO 5.6 De una baraja con 52 naipes se eligen tres cartas, una después de la otra. Encuentre el número m de formas en que puede hacerse lo anterior: *a*) con reemplazo; *b*) sin reemplazo.

a) Cada carta puede elegirse en 52 formas. Así, $m = 52(52)(52) = 140\,608$.

b) Aquí no hay reemplazo. Por tanto, la primera carta puede escogerse en 52 formas; la segunda en 51 y la tercera en 50 formas. Por tanto:

$$m = (P52, 3) = 52(51)(50) = 132\,600$$

5.5 COMBINACIONES

Sea S un conjunto con n elementos. Una *combinación* de estos n elementos tomando r a la vez es cualquier selección de r de los elementos, donde el orden no importa. Esta selección se denomina r combinación; es simplemente un subconjunto de S con r elementos. El número de tales combinaciones se denotará por

$$C(n, r) \quad \text{(otros texto pueden usar } {}_nC_r,\ C_{n,r} \text{ o } C_r^n).$$

Antes de presentar la fórmula general para $C(n, r)$ se considerará un caso especial.

EJEMPLO 5.7 Encuentre el número de combinaciones de 4 objetos, A, B, C, D, tomando 3 a la vez. Cada combinación de tres objetos determina $3! = 6$ permutaciones de los objetos como sigue:

$$\begin{array}{lllllll} ABC: & ABC, & ACB, & BAC, & BCA, & CAB, & CBA \\ ABD: & ABD, & ADB, & BAD, & BDA, & DAB, & DBA \\ ACD: & ACD, & ADC, & CAD, & CDA, & DAC, & DCA \\ BCD: & BDC, & BDC, & CBD, & CDB, & DBC, & DCB \end{array}$$

Por tanto, al multiplicar el número de combinaciones por 3! se halla el número de permutaciones; es decir,

$$C(4, 3) \cdot 3! = P(4, 3) \quad \text{o} \quad C(4, 3) = \frac{P(4, 3)}{3!}$$

Pero $P(4, 3) = 4 \cdot 3 \cdot 2 = 24$ y $3! = 6$; por tanto $C(4, 3) = 4$ como se anotó antes.

Como ya se indicó, cualquier combinación de n objetos tomando r a la vez determina $r!$ permutaciones de los objetos en la combinación; es decir

$$P(n, r) = r!\, C(n, r)$$

En consecuencia, se obtiene la siguiente fórmula para $C(n, r)$, que tiene su expresión formal en el teorema.

Teorema 5.7: $C(n, r) = \dfrac{P(n, r)}{r!} = \dfrac{n!}{r!(n-r)!}$

Recuerde que el coeficiente binomial $\binom{n}{r}$ se definió como $\dfrac{n!}{r!(n-r)!}$; por tanto,

$$\boxed{C(r, n) = \binom{n}{r}}$$

Las expresiones $C(n, r)$ y $\binom{n}{r}$ se usan como sinónimos.

EJEMPLO 5.8 Un granjero compra 3 vacas, 2 cerdos y 4 gallinas a una persona que tiene 6 vacas, 5 cerdos y 8 gallinas. Encuentre el número m de opciones que tiene el granjero.

El granjero puede escoger las vacas en $C(6, 3)$ formas, los cerdos, en $C(5, 2)$ formas y las gallinas, en $C(8, 4)$ formas. Por tanto, el número m de opciones es:

$$m = \binom{6}{3}\binom{5}{2}\binom{8}{4} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} \cdot \frac{5 \cdot 4}{2 \cdot 1} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2 \cdot 1} = 20 \cdot 10 \cdot 70 = 14\,000$$

5.6 EL PRINCIPIO DEL PALOMAR

Muchos resultados de la teoría combinatoria provienen de la siguiente proposición casi evidente.

Principio del palomar: Si n casillas en el palomar las ocupan $n + 1$ palomas, entonces por lo menos una casilla está ocupada por más de una paloma.

Este principio se aplica a muchas situaciones en las que se busca demostrar que puede ocurrir una situación dada.

EJEMPLO 5.9

a) Suponga que en un área escolar hay 13 profesores y dos de ellos (palomas) nacieron el mismo mes (casillas).

b) Encuentre el número mínimo de elementos que es necesario tomar del conjunto $S = \{1, 2, 3, \ldots, 9\}$ para tener la certeza de que la suma de dos números es 10.
Aquí las casillas son los cinco conjuntos: {1, 9}, {2, 8}, {3, 7}, {4, 6}, {5}. Por tanto, cualquier elección de seis elementos (palomas) de S garantiza que la suma de dos números es 10.

El principio del palomar se generaliza como sigue.

Principio del palomar generalizado: Si n casillas están ocupadas por $kn + 1$ o más palomas, donde k es un entero positivo, entonces por lo menos una casilla está ocupada por $k + 1$ o más palomas.

EJEMPLO 5.10 Encuentre el número mínimo de estudiantes en un curso para asegurar que tres de ellos nacieron el mismo mes.

Aquí $n = 12$ meses son las casillas y $k + 1 = 3$, de modo que $k = 2$. Entonces, entre $kn + 1 = 25$ estudiantes (palomas) cualesquiera, tres de ellos nacieron el mismo mes.

5.7 EL PRINCIPIO DE INCLUSIÓN-EXCLUSIÓN

Sean A y B conjuntos finitos arbitrarios. Recuerde el teorema 1.9, que establece:

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

En otras palabras, para encontrar el número $n(A \cup B)$ de elementos en la unión de A y B, se suman $n(A)$ y $n(B)$ y luego se resta $n(A \cap B)$; es decir, se "incluyen" $n(A)$ y $n(B)$ y se "excluye" $n(A \cap B)$. Esto se debe a que cuando se suman $n(A)$ y $n(B)$, los elementos de $(A \cap B)$ se han contado dos veces.

El principio anterior es verdadero para cualquier número de conjuntos. Primero se plantea para tres conjuntos.

Teorema 5.8: Para tres conjuntos finitos arbitrarios, se tiene

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Es decir, se "incluyen" $n(A)$, $n(B)$, $n(C)$ y se "excluye" $n(A \cap B)$, $n(A \cap C)$, $n(B \cap C)$, y por último se "incluye" $n(A \cap B \cap C)$.

EJEMPLO 5.11 Encuentre el número de estudiantes de matemáticas en una universidad que cursan por lo menos uno de los siguientes idiomas: francés, alemán y ruso, tomando en consideración los datos siguientes:

65 estudian francés, 20 estudian francés y alemán.
45 estudian alemán, 25 estudian francés y ruso, 8 estudian los 3 idiomas.
42 estudian ruso, 15 estudian alemán y ruso.

Se quiere encontrar $n(F \cup G \cup R)$, donde F, G y R denotan los conjuntos de estudiantes que estudian francés, alemán y ruso, respectivamente.

Por el principio de inclusión-exclusión,

$$\begin{aligned} n(F \cup G \cup R) &= n(F) + n(G) + n(R) - n(F \cap G) - n(F \cap R) - n(G \cap R) + n(F \cap G \cap R) \\ &= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100 \end{aligned}$$

A saber, 100 estudiantes estudian por lo menos uno de los tres idiomas.

Ahora suponga que tiene cualquier número finito de conjuntos finitos; por ejemplo, $A_1, A_2, \ldots, A_m$. Sea S_k la suma de las cardinalidades

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_K})$$

de todas las intersecciones k-tuplas de los m conjuntos dados. Entonces se tiene el siguiente principio de inclusión-exclusión general.

Teorema 5.9: $n(A_1 \cup A_2 \cup \cdots \cup A_m) = s_1 - s_2 + s_3 - \cdots + (-1)^{m-1} s_m$.

5.8 DIAGRAMAS DE ÁRBOL

Un *diagrama de árbol* es un instrumento para enumerar todos los resultados posibles de una sucesión de eventos, donde cada evento puede ocurrir en una forma finita de formas. La construcción de los diagramas de árbol se ilustra en el siguiente ejemplo.

EJEMPLO 5.12

a) Encuentre el producto $A \times B \times C$, donde $A = \{1, 2\}$, $B = \{a, b, c\}$, $C = \{x, y\}$.

El diagrama de árbol para $A \times B \times C$ aparece en la figura 5-2*a*). Aquí el árbol se construye de izquierda a derecha, y el número de ramas en cada punto corresponde a los resultados posibles del siguiente evento. Cada punto terminal (hoja) del árbol se identifica mediante el elemento correspondiente de $A \times B \times C$. Como ya se observó, $A \times B \times C$ tiene $n = 2(3)(2) = 12$ elementos.

b) Marcos y Eric van a enfrentarse en un torneo de tenis. El ganador del torneo es el primero que gane dos partidos seguidos o quien gane tres juegos. Encuentre el número de formas en que puede ocurrir el torneo.

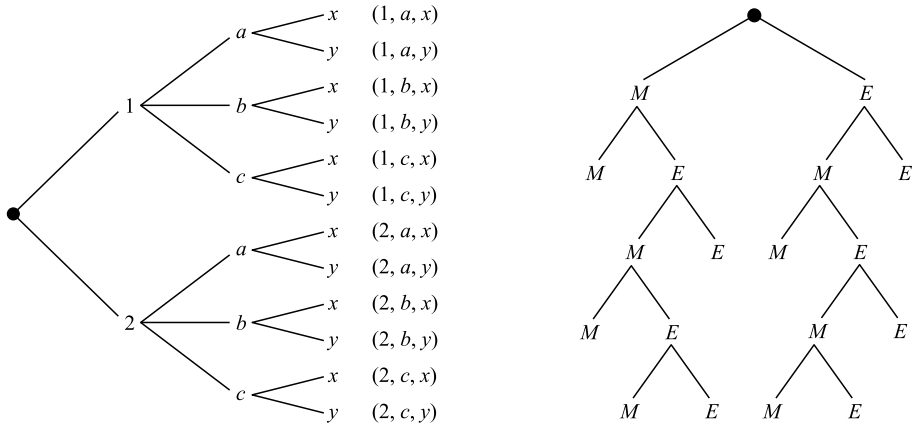


Figura 5-2

El diagrama de árbol que muestra los resultados posibles se muestra en la figura 5-2*b*). Aquí, el árbol se construye de arriba abajo, en lugar de izquierda a derecha. (Es decir, la "raíz" está en la parte superior del árbol.) Observe que hay 10 puntos terminales, que corresponden a las 10 formas como puede ocurrir el torneo:

MM, *MEMM*, *MEMEM*, *MEMEE*, *MEE*, *EMM*, *EMEMM*, *EMEME*, *EMEE*, *EE*

La ruta desde el inicio (parte superior) del árbol hasta el punto terminal describe quién ganó qué juego en el torneo.

PROBLEMAS RESUELTOS

NOTACIÓN FACTORIAL Y COEFICIENTES BINOMIALES

5.1 Calcule: *a*) 4!, 5! *b*) 6!, 7!, 8!, 9! *c*) 50!

a) $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24, \quad 5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5(24) = 120.$

b) Ahora se usa $(n + 1)! = (n + 1)n!$:

$$6! = 5(5!) = 6(120) = 720, \qquad 8! = 8(7!) = 8(5040) = 40\,320,$$
$$7! = 7(6!) = 7(720) = 5\,040, \quad 9! = 9(8!) = 9(40\,320) = 362\,880.$$

c) Puesto que n es muy grande, se usa la aproximación de Stirling: $n! = \sqrt{2\pi n}\, n^{\pi} e^{-n}$ donde $e \approx 2.718$. Por tanto,

$$50! \approx N = \sqrt{100\pi}\, 50^{50} e^{-50}$$

Al evaluar N con una calculadora, se obtiene $N = 3.04 \times 10^{64}$ (que tiene 65 dígitos).

5.2 Calcule: *a*) $\dfrac{13!}{11!}$; *b*) $\dfrac{7!}{10!}$.

a) $$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13 \cdot 12 = 156.$$

En forma alterna, lo anterior se resuelve así:

$$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11!}{11!} = 13 \cdot 12 = 156.$$

b) $$\frac{7!}{10!} = \frac{7!}{10 \cdot 9 \cdot 8 \cdot 7!} = \frac{1}{10 \cdot 9 \cdot 8} = \frac{1}{720}.$$

5.3 Simplificar: *a*) $\dfrac{n!}{(n-1)!}$; *b*) $\dfrac{(n+2)!}{n!}$.

a) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3\cdot 2\cdot 1}{(n-1)(n-2)\cdots 3\cdot 2\cdot 1} = n$; en forma alterna: $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$.

b) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2$.

5.4 Calcule: *a*) $\binom{16}{3}$; *b*) $\binom{12}{4}$; *c*) $\binom{8}{5}$.

Recuerde que en el numerador hay tantos factores como en el denominador.

a) $\binom{16}{3} = \dfrac{16\cdot 15\cdot 14}{3\cdot 2\cdot 1} = 560$; *b*) $\binom{12}{4} = \dfrac{12\cdot 11\cdot 10\cdot 9}{4\cdot 3\cdot 2\cdot 1} = 495$;

c) Puesto que $8 - 5 = 3$, se tiene $\binom{8}{5} = \binom{8}{3} = \dfrac{8\cdot 7.6}{3\cdot 2\cdot 1} = 56$.

5.5 Demuestre: $\binom{17}{6} = \binom{16}{5} + \binom{16}{6}$.

Ahora $\binom{16}{5} + \binom{16}{6} = \dfrac{16!}{5!11!} + \dfrac{16!}{6!10!}$. La primera fracción se multiplica por $\frac{6}{6}$ y la segunda por $\frac{11}{11}$ a fin de obtener el mismo denominador en ambas fracciones; luego se suma:

$$\begin{aligned}\binom{16}{5} + \binom{16}{6} &= \frac{6\cdot 16!}{6\cdot 5!\cdot 11!} + \frac{11\cdot 16!}{6!\cdot 11\cdot 10!} = \frac{6\cdot 16!}{6!\cdot 11!} + \frac{11\cdot 16!}{6!\cdot 11!} \\ &= \frac{6\cdot 16! + 11\cdot 16!}{6!\cdot 11!} = \frac{(6+11)\cdot 16!}{6!\cdot 11!} = \frac{17\cdot 16!}{6!\cdot 11!} = \frac{17!}{6!\cdot 11!} = \binom{17}{6}\end{aligned}$$

5.6 Demuestre el teorema 5.3: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

(La técnica aplicada en esta demostración es semejante a la del problema precedente.)

Ahora $\binom{n}{r-1} + \binom{n}{r} = \dfrac{n!}{(r-1)!\cdot(n-r+1)!} + \dfrac{n!}{r!\cdot(n-r)!}$.

Para obtener el mismo denominador en ambas fracciones, la primera fracción se multiplica por $\frac{r}{r}$ y la segunda, por $\dfrac{n-r+1}{n-r+1}$. Por tanto,

$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{r\cdot n!}{r\cdot(r-1)!\cdot(n-r+1)!} + \frac{(n-r+1)\cdot n!}{r!\cdot(n-r+1)\cdot(n-r)!} \\ &= \frac{r\cdot n!}{r!(n-r+1)!} + \frac{(n-r+1)\cdot n!}{r!(n-r+1)!} \\ &= \frac{r\cdot n! + (n-r+1)\cdot n!}{r!(n-r+1)!} = \frac{[r+(n-r+1)]\cdot n!}{r!(n-r+1)!} \\ &= \frac{(n+1)n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r}\end{aligned}$$

PRINCIPIOS DE CONTEO

5.7 Suponga que en un librero hay 5 textos de historia, 3 de sociología, 6 de antropología y 4 de psicología. Encuentre el número *n* de formas en que un estudiante puede escoger:

a) Uno de los libros; *b*) un libro de cada tema.

a) Aquí se aplica la regla de la suma; por tanto, $n = 5 + 3 + 6 + 4 = 18$.

b) Aquí se aplica la regla del producto; por tanto, $n = 5\cdot 3\cdot 6\cdot 4 = 360$.

5.8 En un curso de historia hay 8 estudiantes varones y 6 estudiantes mujeres. Encuentre las n formas en que es posible elegir: *a*) un representante del curso; *b*) dos representantes del curso: 1 varón y una mujer; *c*) 1 presidente y 1 vicepresidente.

a) Aquí se usa la regla de la suma; por tanto, $n = 8 + 6 = 14$.

b) Aquí se usa la regla del producto; por tanto, $n = 8 \cdot 6 = 48$.

c) Hay 14 formas para elegir un presidente, y así hay 13 formas para elegir al vicepresidente. Por tanto, $n = 14 \cdot 13 = 182$.

5.9 Entre A y B hay cuatro líneas de autobuses, y entre B y C hay tres líneas de autobuses. Encuentre el número m de formas en que una persona puede viajar en autobús: *a*) de A a C pasando por B; *b*) en viaje redondo de A a C pasando por B; *c*) en viaje redondo de A a C pasando por B pero sin usar una línea de autobús más de una vez.

a) Hay 4 formas de ir de A a B y 3 formas de ir de B a C; por tanto, $n = 4 \cdot 3 = 12$.

b) Hay 12 formas de ir de A a C pasando por B, y 12 formas para regresar. Por tanto, $n = 12 \cdot 12 = 144$.

c) La persona viajará de A a B a C a B a A. Estas letras se escriben con flechas vinculatorias:

$$A \to B \to C \to B \to A$$

La persona puede viajar en cuatro formas de A a B y en tres formas de B a C, pero sólo puede viajar en dos formas de C a B y en tres formas de B a A puesto que no desea viajar en la misma línea de autobús más de una vez. Estos números se escriben arriba de las flechas correspondientes como sigue:

$$A \xrightarrow{4} B \xrightarrow{3} C \xrightarrow{2} B \xrightarrow{3} A$$

Entonces, por la regla del producto, $n = 4 \cdot 3 \cdot 2 \cdot 3 = 72$.

PERMUTACIONES

5.10 Escriba la diferencia principal entre permutaciones y combinaciones, con ejemplos.

El orden importa en las permutaciones, como en las palabras, sentarse en fila y elegir un presidente, un vicepresidente y un tesorero. El orden no importa en las combinaciones, como en comités y equipos (sin contar las posiciones). La regla del producto suele usarse con permutaciones, puesto que la elección de cada una de las posiciones ordenadas se considera como una sucesión de eventos.

5.11 Encuentre: *a*) $P(7, 3)$; *b*) $P(14, 2)$.

Recuerde que $P(n, r)$ tiene r factores, empezando con n.

a) $P(7, 3) = 7 \cdot 6 \cdot 5 = 219$; *b*) $P(14, 2) = 14 \cdot 13 = 182$.

5.12 Encuentre las m formas en que 7 personas pueden sentarse:

a) En una fila de sillas; *b*) alrededor de una mesa redonda.

a) Aquí $m = P(7, 7) = 7!$ formas.

b) Una persona puede sentarse en cualquier sitio en la mesa. Las otras 6 personas pueden colocarse en 6! formas alrededor de la mesa; es decir, $m = 6!$

Éste es un ejemplo de *permutación circular*. En general, n objetos pueden colocarse en un círculo en $(n - 1)!$ formas.

5.13 Encuentre el número n de permutaciones distintas que pueden formarse con todas las letras de cada palabra:

a) *PATOS*; *b*) *PARADAS*; *c*) *SOCIOLÓGICAS*.

Éste es un problema de permutaciones con repeticiones.

a) $n = 5! = 120$, puesto que hay 5 letras sin repetición.

b) $n = \dfrac{7!}{3!} = 840$, ya que hay 7 letras, de las cuales 3 son A y no se repite ninguna otra letra.

c) $n = \dfrac{12!}{3!2!2!2!}$, ya que hay 12 letras, de las cuales 3 son *O*, 2 son *S*, 2 son *I* y 2 son *C*. (La respuesta se deja en términos factoriales, debido a que el número es muy grande.)

5.14 En un curso hay 8 estudiantes. Encuentre el número *n* de muestras de tamaño 3:

a) Con reemplazo; *b*) sin reemplazo .

a) A cada estudiante de la muestra ordenada se le puede escoger de 8 formas; por tanto, hay

$$n = 8 \cdot 8 \cdot 8 = 8^3 = 512 \text{ muestras de tamaño 3 con reemplazo.}$$

b) Hay 8 formas de escoger al primer estudiante; al segundo, 7 formas; y al último, 6 formas. Por tanto, hay $n = 8 \cdot 7 \cdot 6 = 336$ muestras de tamaño 3 sin reemplazo.

5.15 Encuentre *n* si $P(n, 2) = 72$.

$$P(n, 2) = n(n-1) = n^2 - n. \quad \text{Por tanto, se obtiene}$$

$$n^2 - n = 72 \quad \text{o} \quad n^2 - n - 72 = 0 \quad \text{o} \quad (n-9)(n+8) = 0$$

Debido a que *n* debe ser positiva, la única respuesta es $n = 9$.

COMBINACIONES

5.16 En un curso hay 10 estudiantes; 6 varones y 4 mujeres. Encuentre el número *n* de formas para:

a) Elegir un comité de 4 miembros.
b) Elegir un comité de 4 miembros con 2 varones y 2 mujeres.
c) Elegir un presidente, un vicepresidente y un tesorero.

a) Esta situación corresponde a combinaciones, no a permutaciones, ya que en un comité el orden no importa. Hay "10 en 4" comités así. Es decir,

$$n = C(10, 4) = \binom{10}{4} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2 \cdot 1} = 210$$

b) Los 2 varones pueden elegirse de los 6 varones en $C(6, 2)$ formas, y las 2 mujeres pueden elegirse de las 4 mujeres en $C(4, 2)$ formas. Entonces, por la regla del producto:

$$n = \binom{6}{2}\binom{4}{2} = \frac{6 \cdot 5}{2 \cdot 1} \cdot \frac{4 \cdot 3}{2 \cdot 1} = 15(6) = 90$$

c) Esta situación corresponde a permutaciones, no a combinaciones, ya que en un comité importa el orden. Así,

$$n = P(6, 3) = 6 \cdot 5 \cdot 4 = 120$$

5.17 Una caja contiene 8 calcetines azules y 6 calcetines rojos. Encuentre el número de formas en que es posible extraer dos calcetines de la caja si:

a) Pueden ser de cualquier color. *b*) Deben ser del mismo color.

a) Hay "14 en 2" formas de seleccionar 2 de los 14 calcetines. Por tanto,

$$n = C(14, 2) = \binom{14}{2} = \frac{14 \cdot 13}{2 \cdot 1} = 91$$

b) Hay $C(8, 2) = 28$ formas para escoger 2 de los 8 calcetines azules, y $C(6, 2) = 15$ formas para escoger 2 de los 6 calcetines rojos. Por la regla de la suma, $n = 28 + 15 = 43$.

5.18 Encuentre el número *m* de comités de 5 miembros con un director que es posible escoger entre un grupo de 12 personas.

Hay 12 formas de escoger al director, a los otros 4 miembros del comité se les puede escoger entre las 11 personas restantes en $C(11, 4)$ formas. Así, $m = 12 \cdot C(11, 4) = 12 \cdot 330 = 3\,960$.

PRINCIPIO DEL PALOMAR

5.19 Encuentre el número mínimo n de enteros a seleccionar de $S = \{1, 2, \ldots, 9\}$ de modo que: *a*) La suma de dos de los n enteros sea par. *b*) La diferencia de dos de los n enteros sea 5.

a) La suma de dos enteros pares o dos enteros impares es par. Considere que los subconjuntos {1, 3, 5, 7, 9} y {2, 4, 6, 8} de S son casillas. Por tanto, $n = 3$.

b) Considere que los cinco subconjuntos {1, 6}, {2, 7}, {3, 8}, {4, 9}, {5} de S son casillas. Por tanto, $n = 6$ garantiza que dos enteros pertenecen a uno de los subconjuntos y que su diferencia es 5.

5.20 Encuentre el número mínimo de estudiantes necesario para garantizar que cinco de ellos están en el mismo nivel (de primero, de segundo, de tercero o de último año).

Aquí los $n = 4$ niveles son las casillas y $k + 1 = 5$, de modo que $k = 4$. Por tanto, de entre cualesquiera $kn + 1 = 17$ estudiantes (las palomas), cinco de ellos están en el mismo nivel.

5.21 Sea L una lista (no necesariamente en orden alfabético) de las 26 letras del alfabeto inglés (que consta de cinco vocales: *A*, *E*, *I*, *O*, *U* y 21 consonantes).

a) Demuestre que L contiene una sublista que consta de cuatro o más consonantes consecutivas.
b) En el supuesto de que L empiece con una vocal; por ejemplo *A*, demuestre que L contiene una sublista que consta de cinco o más consonantes consecutivas.

a) Las cinco letras dividen a L en $n = 6$ sublistas (casillas) de consonantes consecutivas. Aquí $k + 1 = 4$ y así $k = 3$. Por tanto, $nk + 1 = 6(3) + 1 = 19 < 21$. Por tanto, alguna sublista tiene por lo menos cuatro consonantes consecutivas.

b) Puesto que L empieza con una vocal, el resto de las vocales dividen a L en $n = 5$ sublistas. Aquí $k + 1 = 5$ y entonces $k = 4$. Por tanto, $kn + 1 = 21$. Por consiguiente, alguna sublista tiene por lo menos cinco consonantes consecutivas.

PRINCIPIO DE INCLUSIÓN-EXCLUSIÓN

5.22 En un aula hay 22 estudiantes mujeres y 18 estudiantes varones. Encuentre el número total de t estudiantes.

Los conjuntos de estudiantes varones y mujeres son ajenos; así, $t = 22 + 18 = 40$.

5.23 Suponga que de 32 personas que separan papel o botellas (o ambos) para reciclar, hay 30 que separan papel y 14 que separan botellas. Encuentre el número m de personas que:

a) separan papel y botellas; *b*) sólo separan papel; *c*) sólo separan botellas.

Sean P y B los conjuntos de personas que separan papel y botellas, respectivamente. Entonces:

$$\begin{aligned} a)\quad & m = n(P \cap B) = n(P) + n(B) - n(P \cup B) = 30 + 14 - 32 = 12 \\ b)\quad & m = n(P \backslash B) = n(P) - n(P \cap B) = 30 - 12 = 18 \\ c)\quad & m = n(B \backslash P) = n(B) - n(P \cap B) = 14 - 12 = 2 \end{aligned}$$

5.24 Las letras *A*, *B*, *C* y *D* representan, respectivamente, cursos de arte, biología, química y teatro. Encuentre el número N de estudiantes en un dormitorio, dado lo siguiente:

12 cursan *A*,	5 cursan *A* y *B*,	4 cursan *B* y *D*,	2 cursan *B*, *C*, *D*,
20 cursan *B*,	7 cursan *A* y *C*,	3 cursan *C* y *D*,	3 cursan *A*, *C*, *D*,
20 cursan *C*,	4 cursan *A* y *D*,	3 cursan *A*, *B* y *C*,	2 cursan los cuatro,
8 cursan *D*,	16 cursan *B* y *C*,	2 cursan *A*, *B* y *D*,	71 no cursan ninguno.

Sea T el número de estudiantes que llevan por lo menos un curso. Por el principio de inclusión-exclusión, teorema 5.9, $T = s_1 - s_2 + s_3 - s_4$ donde:

$$\begin{aligned} s_1 &= 12 + 20 + 20 + 8 = 60, & s_2 &= 5 + 7 + 4 + 16 + 4 + 3 = 39, \\ s_3 &= 3 + 2 + 2 + 3 = 10, & s_4 &= 2. \end{aligned}$$

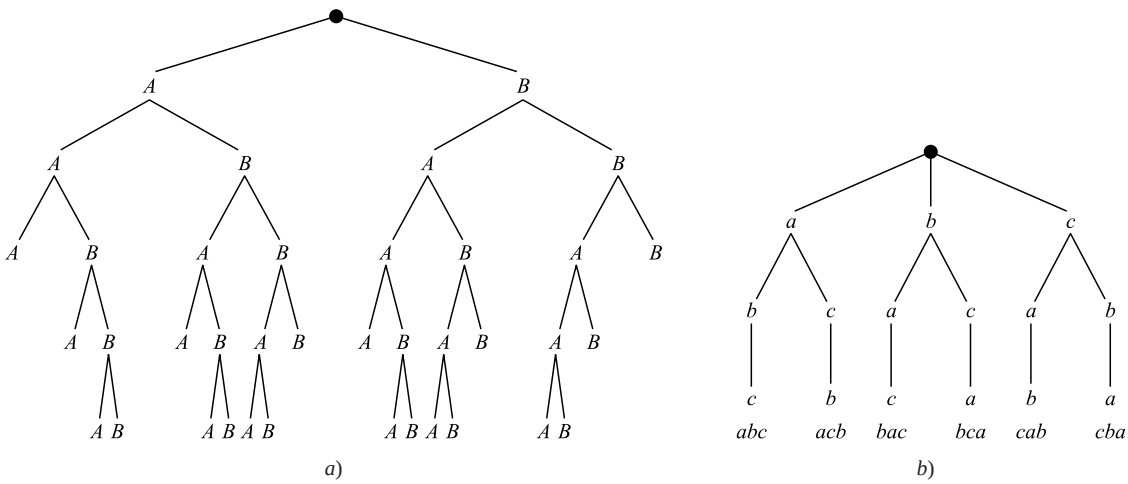
Así, $T = 29$ y $N = 71 + T = 100$.

DIAGRAMAS DE ÁRBOL

5.25 Los equipos A y B disputarán un torneo. El triunfador es el primer equipo que gane tres juegos. Encuentre el número n de formas en que es posible ganar el torneo.

En la figura 5-3*a*) aparece el diagrama de árbol idóneo. Los resultados del torneo pueden ocurrir en 20 formas:

AAA, *AABA*, *AABBA*, *AABBB*, *ABAA*, *ABABA*, *ABABB*, *ABBAA*, *ABBAB*, *ABBB*,
BBB, *BBAB*, *BBAAB*, *BBAAA*, *BABB*, *BABAB*, *BABAA*, *BAABB*, *BAABA*, *BAAA*



a) *b*)

Figura 5-3

5.26 Construya el diagrama de árbol que proporciona las permutaciones de $\{a, b, c\}$.

El diagrama de árbol se muestra en la figura 5-3*b*). Hay seis permutaciones, que se enumeran en la parte inferior del diagrama.

PROBLEMAS DIVERSOS

5.27 En un curso hay 12 estudiantes. Encuentre el número n de formas en que los 12 estudiantes pueden presentar 3 exámenes si 4 estudiantes deben presentar cada examen.

Hay $C(12, 4) = 495$ formas de escoger 4 de los 12 estudiantes para presentar el primer examen. Luego, hay $C(8, 4) = 70$ formas de escoger 4 de los 8 estudiantes restantes para presentar el segundo examen. Los estudiantes que quedan presentan el tercer examen. Así:

$$n = 70(495) = 34\,650$$

5.28 Demuestre el teorema (del binomio) 5.2: $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$.

El teorema se cumple para $n = 1$, puesto que

$$\sum_{r=0}^{1} \binom{1}{r} a^{1-r} b^r = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1$$

Se supone que el teorema es verdadero para $(a+b)^n$ y se tiene que es cierto para $(a+b)^{n+1}$.

$$(a+b)^{n+1} = (a+b)\,(a+b)^n$$

$$= (a+b)[a^n + \tbinom{n}{1} a^{n-1} b + \cdots + \tbinom{n}{r-1} a^{n-r+1} b^{r-1} + \tbinom{n}{r} a^{n-r} b^r + \cdots \tbinom{n}{1} a\, b^{n-1} + b^n]$$

Luego, el término en el producto que contiene b^r se obtiene a partir de

$$b[\binom{n}{r-1} a^{n-r+1} b^{r-1}] + a[\binom{n}{r} a^{n-r} b^r] = \binom{n}{r-1} a^{n-r+1} b^r + \binom{n}{r} a^{n-r+1} b^r$$
$$= [\binom{n}{r-1} + \binom{n}{r}] a^{n-r+1} b^r$$

Pero, por el teorema 5.3, $\binom{n}{r-1} = \binom{n}{r} = \binom{n+1}{r}$. Así, el término que contiene a b^r es:

$$\binom{n+1}{r} a^{n-r+1} b^r$$

Observe que $(a+b)(a+b)^n$ es un polinomio de grado $n+1$ en b. Por consiguiente:

$$(a+b)^{n+1} = (a+b)(a+b)^n = \sum_{r=0}^{n+1} \binom{n+1}{r} a^{n-r+1} b^r$$

lo que había que demostrar.

5.29 Sean n y $n_1, n_2, \ldots, n_r$ enteros no negativos tales que $n_1 + n_2 + \cdots + n_r = n$. Los *coeficientes multinomiales* se denotan y definen mediante:

$$\binom{n}{n_1,\ n_2, \ldots, n_r} = \frac{n!}{n_1! n_2! \ldots n_r!}$$

Calcular los siguientes coeficientes multinomiales:

a) $\binom{6}{3,\ 2,\ 1}$; *b*) $\binom{8}{4,\ 2,\ 2,\ 0}$; *c*) $\binom{10}{5,\ 3,\ 2,\ 2}$.

a) $\binom{6}{3,\ 2,\ 1} = \frac{6!}{3!\,2!\,1!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 1} = 60$

b) $\binom{8}{4,\ 2,\ 2,\ 0} = \frac{8!}{4!\,2!\,2!\,0!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 1} = 420$

c) $\binom{10}{5,\ 3,\ 2,\ 2}$ no tiene sentido, ya que $5 + 3 + 2 + 2 \neq 10$.

5.30 Un estudiante debe cursar cinco materias de tres áreas de estudio. En cada disciplina se ofrecen numerosos cursos, pero el estudiante no puede cursar más de dos materias de cualquier área.

a) Use el principio del palomar para demostrar que el estudiante debe cursar por lo menos dos materias de cada área.

b) Use el principio de inclusión-exclusión para demostrar que el estudiante debe cursar por lo menos una materia en cada área.

a) Las tres áreas son las casillas y el estudiante debe cursar cinco materias (las palomas). Por tanto, el estudiante debe cursar por lo menos dos materias en un área.

b) Cada una de las tres áreas de estudio se representan como tres conjuntos ajenos por las letras A, B y C. Puesto que los conjuntos son ajenos, $m(A \cup B \cup C) = 5 = n(A) + n(B) + n(C)$. Ya que el estudiante puede cursar sólo dos materias en cualquier área de estudio, la suma de las materias en dos conjuntos cualesquiera; por ejemplo, A y B, debe ser menor o igual que cuatro. Así, $5 - [n(A) + n(B)] = n(C) \geq 1$. Entonces, el estudiante debe cursar por lo menos una materia en cualquier área.

PROBLEMAS SUPLEMENTARIOS

NOTACIÓN FACTORIAL, COEFICIENTES BINOMIALES

5.31 Encuentre: *a*) 10!, 11!, 12!; *b*) 60! (Sugerencia: Use la aproximación de Sterling a $n!$)

5.32 Evalúe: *a*) 16!/14!, *b*) 14!/11!; *c*) 8!/10!, *d*) 10!/13!

5.33 Simplifique: *a*) $\dfrac{(n=1)!}{n!}$; *b*) $\dfrac{n!}{(n-2)!}$; *c*) $\dfrac{(n-1)!}{(n+2)!}$; *d*) $\dfrac{(n-r+1)!}{(n-r-1)!}$.

5.34 Encuentre: *a*) $\binom{5}{2}$; *b*) $\binom{7}{3}$; *c*) $\binom{14}{2}$; *d*) $\binom{6}{4}$; *e*) $\binom{20}{17}$; *f*) $\binom{18}{15}$.

5.35 Demuestre que: *a*) $\binom{n}{0} + \binom{n}{n} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n$

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + \binom{n}{n} = 0$

5.36 A partir del renglón ocho del triángulo de Pascal siguiente, encuentre: *a*) el noveno renglón; *b*) el décimo renglón.

1 8 28 56 70 56 28 8 1

5.37 Evalúe los siguientes coeficientes multinomiales (definidos en el problema 5.29):

a) $\begin{pmatrix} 6 \\ 2,\ 3,\ 1 \end{pmatrix}$; *b*) $\begin{pmatrix} 7 \\ 3,\ 2,\ 2,\ 0 \end{pmatrix}$; *c*) $\begin{pmatrix} 9 \\ 3,\ 5,\ 1 \end{pmatrix}$; *d*) $\begin{pmatrix} 8 \\ 4,\ 3,\ 2 \end{pmatrix}$.

PRINCIPIOS DE CONTEO

5.38 Una tienda vende ropa para hombre: tiene 3 estilos de chamarra, 7 estilos de playera y 5 estilos de pantalón. Encuentre el número de formas en que una persona puede comprar: *a*) uno de los artículos; *b*) un artículo de cada uno de los tres tipos de prenda.

5.39 En un grupo hay 10 estudiantes varones y 8 estudiantes mujeres. Encuentre el número de formas en que es posible elegir: *a*) un representante del grupo; *b*) dos representantes del grupo: un varón y una mujer; *c*) un presidente y un vicepresidente del grupo.

5.40 Suponga que un código consta de cinco caracteres: dos letras seguidas por tres dígitos. Encuentre el número de: *a*) códigos; *b*) códigos con letras distintas; *c*) códigos con las mismas letras.

PERMUTACIONES

5.41 Encuentre el número de placas de automóvil de modo que: *a*) cada placa contenga 2 letras distintas seguidas por 3 dígitos distintos; *b*) el primer dígito no sea 0.

5.42 Encuentre el número m de formas en que un juez puede otorgar el primer lugar, el segundo lugar y el tercer lugar en una justa con 18 competidores.

5.43 Encuentre el número de formas en que es posible colocar 5 libros grandes, 4 libros medianos y 3 libros pequeños en un librero de modo que: *a*) no haya restricciones; *b*) todos los libros del mismo tamaño estén juntos.

5.44 Un grupo de debate consta de tres muchachos y tres muchachas. Encuentre el número de formas en que pueden sentarse en una fila de modo que: *a*) no haya restricciones; *b*) los muchachos y las muchachas se sienten juntos; c) sólo las muchachas se sienten juntas.

5.45 Encuentre el número de formas en que 5 personas pueden sentarse juntas de modo que: *a*) no haya restricciones; *b*) dos personas insistan en sentarse juntas.

5.46 Repita el problema 5.45 si las personas se sientan en una mesa redonda.

5.47 Considere todos los enteros positivos con tres dígitos distintos. (Observe que el cero no puede ser el primer dígito.) Encuentre el número de los que son: *a*) mayores que 700; *b*) impares; *c*) divisibles entre 5.

5.48 Suponga que no se permiten repeticiones. *a*) Encuentre la cantidad de números de tres dígitos que es posible formar con los seis dígitos 2, 3, 5, 6, 7 y 9. *b*) ¿Cuántos de ellos son menores que 400? *c*) ¿Cuántos son pares?

5.49 Encuentre el número m de formas en que seis personas pueden subirse a un tobogán si uno de 3 de ellos debe ir adelante.

5.50 Encuentre n si: *a*) $P(n, 4) = 42P(n, 2)$; *b*) $2P(n, 2) + 50 = P(2n, 2)$.

PERMUTACIONES CON REPETICIÓN, MUESTRAS ORDENADAS

5.51 Encuentre el número de permutaciones que pueden formarse con todas las letras de cada palabra: *a*) QUEUE; *b*) COMMITTEE; *c*) PROPOSITION; *d*) BASEBALL.

5.52 Suponga que se tienen 4 banderas rojas idénticas, 2 banderas azules idénticas y 3 banderas verdes idénticas. Encuentre el número *m* de señales diferentes que es posible formar al colgar las 9 banderas en una línea vertical.

5.53 Una caja contiene 12 lámparas. Encuentre el número *n* de muestras ordenadas de tamaño 3: *a*) con reemplazo; *b*) sin reemplazo.

5.54 En un grupo hay 10 estudiantes. Encuentre el número *n* de muestras ordenadas de tamaño 4: *a*) con reemplazo; *b*) sin reemplazo.

COMBINACIONES

5.55 Un restorán ofrece 6 postres distintos. Encuentre el número de formas en que un cliente puede elegir:
a) un postre; *b*) 2 de los postres; *c*) 3 de los postres.

5.56 En un grupo que integran 9 hombres y 3 mujeres, encuentre el número de formas en que un maestro puede seleccionar un comité de 4 personas del grupo, de modo que:
a) no haya restricciones; *c*) haya exactamente una mujer;
b) haya 2 hombres y 2 mujeres; *d*) por lo menos una persona sea mujer.

5.57 Una mujer tiene 11 amigos cercanos. Encuentre el número de formas en que la mujer puede invitar a cenar a 5 de sus amigos, de modo que:
a) No haya restricciones.
b) Dos de las personas formen un matrimonio y no se sienten separadas.
c) Dos de los amigos no hablen entre sí y no se sienten separados.

5.58 En un curso hay 8 hombres y 6 mujeres y entre ellos sólo hay un matrimonio. Encuentre el número *m* de formas en que un maestro puede seleccionar un comité de 4 personas del curso donde el esposo o la esposa, pero no ambos, estén en el comité.

5.59 En una caja hay 6 calcetines azules y 4 calcetines blancos. Encuentre el número de formas en que es posible extraer dos calcetines de la caja de modo que:
a) No haya restricciones. *b*) Sean de distinto color. *c*) Sean del mismo color.

5.60 Una estudiante debe contestar 10 de 13 reactivos. Encuentre el número de sus opciones en que debe responder:
a) los dos primeros reactivos; *c*) exactamente 3 de los 5 primeros reactivos;
b) el primero o el segundo reactivo, pero no ambos; *d*) por lo menos 3 de los 5 primeros reactivos.

PRINCIPIO DE INCLUSIÓN-EXCLUSIÓN

5.61 Suponga que 32 estudiantes están en un curso de arte *A* y que 24 estudiantes están en un curso de biología *B*, y suponga que 10 estudiantes están en ambos cursos. Encuentre el número de estudiantes que están:
a) en el curso *A* o en el curso *B*; *b*) sólo en el curso *A*; *c*) sólo en el curso *B*.

5.62 Una encuesta aplicada a 80 propietarios de automóvil mostró que 24 poseen un automóvil extranjero y 60 poseen un automóvil nacional. Encuentre el número de propietarios que poseen:
a) tanto un automóvil extranjero como uno nacional;
b) sólo un automóvil extranjero;
c) sólo un automóvil nacional.

5.63 Considere todos los enteros desde 1 hasta 100. Encuentre el número de ellos que son:
a) impares o el cuadrado de un entero; *b*) pares o el cubo de un entero.

5.64 En un curso de 30 estudiantes, 10 obtuvieron *A* en el primer examen, 9 obtuvieron *A* en el segundo examen y 15 no obtuvieron *A* en ningún examen. Encuentre el número de estudiantes que obtuvieron:
a) *A* en ambos exámenes;
b) *A* en el primer examen pero no en el segundo;
c) *A* en el segundo examen pero no en el primero.

5.65 Considere todos los enteros desde 1 hasta 300. Encuentre el número de ellos que son divisibles entre:
a) por lo menos uno de 3, 5, 7; *c*) por 5, pero no por 3 ni por 7;
b) 3 y 5 pero no por 7; *d*) ninguno de los números 3, 5, 7.

5.66 En una escuela se imparten tres idiomas extranjeros: francés (F), español (S) y alemán (G). De 80 estudiantes:
i) 20 estudian F, 25 estudian S, 15 estudian G.
ii) 8 estudian F y S, 6 estudian S y G, 5 estudian F y G.
iii) 2 estudian los tres idiomas.
De los 80 estudiantes, encuentre el número de ellos que estudian:
a) ninguno de los idiomas;
b) sólo francés;
c) sólo un idioma;
d) sólo español y alemán;
e) exactamente dos de los idiomas.

5.67 Encuentre el número m de elementos en la unión de los conjuntos A, B, C y D, donde:
i) A, B, C y D tienen 50, 60, 70 y 80 elementos, respectivamente.
ii) Cada par de conjuntos tiene 20 elementos en común.
iii) Cada grupo de tres conjuntos tienen 10 elementos en común.
iv) Los cuatro conjuntos tienen 5 elementos en común.

PRINCIPIO DEL PALOMAR

5.68 Encuentre el número mínimo de estudiantes necesarios para garantizar que 4 de ellos nacieron: *a*) el mismo día de la semana; *b*) el mismo mes.

5.69 Encuentre el número mínimo de estudiantes necesarios para garantizar que 3 de ellos:
a) tienen apellidos que empiezan con la misma letra.
b) nacieron el mismo día de un mes (de 31 días).

5.70 Considere un torneo con n jugadores, donde cada jugador se enfrenta a cada uno de los demás jugadores. Suponga que cada jugador gana por lo menos una vez. Demuestre que por lo menos 2 de los jugadores tienen el mismo número de victorias.

5.71 Suponga que en el interior de un triángulo equilátero T que mide 2 pulgadas por lado se eligen al azar 5 puntos. Demuestre que la distancia entre dos de los puntos debe ser menor que una pulgada.

5.72 Considere el conjunto $X = \{x_1, x_2, \ldots, x_7\}$ de siete enteros distintos. Demuestre que existen $x, y \in X$ tales que $x + y$ o $x - y$ es divisible entre 10.

PROBLEMAS DIVERSOS

5.73 Encuentre el número m de formas en que es posible separar 10 estudiantes en tres equipos, donde un equipo tiene 4 estudiantes y los otros equipos tienen 3 estudiantes cada uno.

5.74 Si se considera que una celda puede estar vacía, encuentre el número n de formas en que un conjunto de 3 elementos puede colocarse en: *a*) 3 celdas ordenadas; *b*) 3 celdas desordenadas.

5.75 Si se supone que una celda puede estar vacía, encuentre el número n de formas en que un conjunto de 4 elementos puede acomodarse en: *a*) 3 celdas ordenadas; *b*) 3 celdas desordenadas.

5.76 El alfabeto inglés tiene 26 letras, de las cuales cinco son vocales. Considere sólo "palabras" de cinco letras integradas por tres consonantes distintas y dos vocales diferentes. Encuentre el número de palabras que:
a) no tengan restricciones; *c*) contienen las letras B y C;
b) contienen la letra B; *d*) empiezan con la letra B y contienen la letra C.

5.77 Los equipos A y B juegan la Serie Mundial de Béisbol, de modo que el primer equipo que gane cuatro juegos gana la serie. Suponga que A gana el primer juego y que el equipo que gana el segundo juego también gana el cuarto juego.
a) Encuentre y enliste el número n de formas en que puede ocurrir el desenlace de la serie.
b) Encuentre el número de formas en que B gana la serie.
c) Encuentre el número de formas en que la serie dura siete juegos.

5.78 Encuentre el número de formas en que puede lanzarse una moneda:
a) de modo que en una serie de 6 lanzamientos caigan exactamente 3 caras (H) y no se caigan dos caras (H) seguidas.
b) $2n$ veces de modo que en una serie caigan exactamente n caras y no caigan dos caras seguidas.

5.79 Encuentre el número de formas en que 3 elementos a, b, c pueden asignarse a 3 celdas, de modo que exactamente una celda quede vacía.

5.80 Encuentre el número de formas en que n elementos distintos pueden asignarse a n celdas, de modo que quede vacía exactamente una celda.

Respuestas a los problemas suplementarios

5.31 *a*) 3 628 800; 39 916 800; 479 001 600; *b*) log(60!) = 81.92, aquí $60! = 6.59 \times 10^{81}$.

5.32 *a*) 240; *b*) 2 184; *c*) 1/90; *d*) 1/1 716.

5.33 *a*) $n + 1$; (*b*) $n(n - 1)$; (*c*) $1/[n(n + 1)(n + 2)$; *d*) $(n - r)(n - r + 1)$.

5.34 *a*) 10; *b*) 35; *c*) 91; *d*) 15; *e*) 1 140; *f*) 816.

5.35 Sugerencias: *a*) Desarrolle $(1 + 1)^n$; *b*) Desarrolle $(1 - 1)^n$.

5.36 *a*) 1, 9, 36, 84, 126, 126, 84, 36, 9, 1; *b*) 1, 10, 45, 120, 210, 252, 210, 120, 45, 10, 1.

5.37 *a*) 60; *b*) 210; *c*) 504; *d*) no está definido.

5.38 *a*) 15; *b*) 105.

5.39 *a*)18; *b*) 80; *c*) 306.

5.40 *a*) $26^2 \cdot 10^3$; (*b*) $26 \cdot 25 \cdot 10^3$; *b*); *c*) $26 \cdot 10^3$.

5.41 *a*) $26 \cdot 25 \cdot 10 \cdot 9 \cdot 8 = 468\,000$; *b*) $26 \cdot 25 \cdot 9 \cdot 9 \cdot 8 = 421\,200$.

5.42 $m = 18 \cdot 17 \cdot 16 = 4\,896$.

5.43 *a*) 12!; *b*) 3!5!4!3! = 103 680.

5.44 *a*) 6! = 720; *b*) $2 \cdot 3! \cdot 3! \cdot = 72$; *c*) $4 \cdot 3! \cdot 3! = 144$.

5.45 *a*) 120; *b*) 48.

5.46 *a*) 24; *b*) 12.

5.47 *a*) $3 \cdot 9 \cdot 8$; *b*) $9 \cdot 8 \cdot 5$; *c*) $9 \cdot 8 \cdot 7/2$; *d*) $9 \cdot 8 \cdot 7/5$.

5.48 *a*) $P(6, 3) = 120$; *b*) $2 \cdot 5 \cdot 4 = 40$; *c*) $2 \cdot 5 \cdot 4 = 40$.

5.49 $m = 360$.

5.50 *a*) 9; *b*) 5.

5.51 *a*) 30; *b*) 9!/[2!2!2!] = 45 360; *c*) 11!/[2!3!2!] = 1 663 200; *d*) 8!/[2!2!2!] = 5 040.

5.52 $m = 9!/[4!2!3!] = 1\,260$.

5.53 *a*) $12^3 = 1\,728$; *b*) $P(12, 3) = 1\,320$.

5.54 *a*) $10^4 = 10\,000$; *b*) $P(10, 4) = 5\,040$.

5.55 *a*) 6; *b*) 15; *c*) 20.

5.56 *a*) $C(12, 4)$; *b*) $C(9, 2) \cdot C(3, 2) = 108$; *c*) $C(9, 3) \cdot 3 = 252$; *d*) $9 + 108 + 252 = 369$ o $C(12, 4) - C(9, 4) = 369$.

5.57 *a*) $C(11, 5) = 462$; *b*) $126 + 84 = 210$; *c*) $C(9, 5) + 2C(9, 4) = 378$.

5.58 $m = C(12, 4) + 2C(12, 3) = 935$.

5.59 *a*) $C(10, 2) = 45$; *b*) $6 \cdot 4 = 24$; *c*) $C(6, 2) + C(4, 2) = 21$ o $45 - 24 = 21$.

5.60 *a*) 165; *b*) 110; *c*) 80; *d*) 276.

5.61 *a*) 46; *b*) 22; *c*) 14.

5.62 *a*) 4; *b*) 20; *c*) 56.

5.63 *a*) 55; *b*) 52.

5.64 *a*) 4; *b*) 6; *c*) 5.

5.65 *a*) $100 + 60 + 42 - 20 - 14 - 8 + 2 = 162$; *b*) $20 - 2 = 18$; *c*) $60 - 20 - 8 + 2 = 34$; *d*) $300 - 162 = 138$.

5.66 *a*) 37; *b*) 9; *c*) 28; *d*) 4; *e*) 13.

5.67 $m = 175$

5.68. *a*) 22; *b*) 37.

5.69 *a*) 53; *b*) 63.

5.70 Cada jugador ganará cualquiera desde 1 hasta $n - 1$ juegos (casillas). Hay n jugadores (palomas).

5.71 Trace tres líneas entre los puntos medios de los lados de T. Esto divide a T en 4 triángulos equiláteros (casillas) donde la longitud de cada lado mide 1. Dos de los 5 puntos (palomas) deben estar en uno de los triángulos.

5.72 Sea r_i el residuo cuando x_i es divisible entre 10. Considere las seis casillas: $H_1 = \{x_i \mid r_i = 0\}$, $H_2 = \{x_i \mid r_i = 5\}$, $H_3 = \{x_i \mid r_i = 1 \text{ o } 9\}$, $H_4 = \{x_i \mid r_i = 2 \text{ u } 8\}$, $H_5 = \{x_i \mid r_i = 3 \text{ o } 7\}$, $H_6 = \{x_i \mid r_i = 4 \text{ o } 6\}$. Entonces alguna x y y pertenecen a alguna H_k.

5.73 $m = C(10, 4) \cdot C(6, 3) = 420$.

5.74 *a*) $n = 33 = 27$. (Cada elemento puede colocarse en cualquiera de las tres celdas.) *b*) El número de elementos en tres celdas puede distribuirse como sigue: [3, 0, 0], [2,1,0], o [1,1,1]. Por tanto $n = 1 + 3 + 1 = 5$.

5.75. *a*) $n = 3^4 = 81$. (Cada elemento puede colocarse en cualquiera de las tres celdas.). *b*) El número de elementos en tres celdas puede distribuirse como sigue: [4, 0, 0], [3, 1, 0], [2, 2, 0], o [2, 1, 1]. Por tanto $n = 1 + 4 + 3 + 6 = 14$.

5.76 *a*) $C(21, 3) \cdot C(5, 2) \cdot 5!$; *b*) $C(20, 2) \cdot C(5, 2) \cdot 5!$; *c*) $19 \cdot C(5, 2) \cdot 5!$; *d*) $19 \cdot C(5, 2) \cdot 4!$

5.77 Trace el diagrama de árbol T como en la figura 5-4. Observe que T empieza en A, el ganador del primer juego, y que sólo hay una opción en el cuarto juego, el ganador del segundo juego.
a) $n = 15$ como se enumera a continuación; *b*) 6; *c*) 8: *AAAA*, *AABAA*, *AABABA*, *AABABBA*, *AABABBB*, *ABABAA*, *ABABABA*, *ABABABB*, *ABABBAA*, *ABABBAB*, *ABABBB*, *ABBBAAA*, *ABBBAAB*, *ABBBAB*, *ABBBB*.

5.78 *a*) 4, *HTHTHT*, *HTTHTH*, *HTHTTH*, *THTHTH*; *b*) $n + 1$.

5.79 18.

5.80 $n!C(n, 2)$.

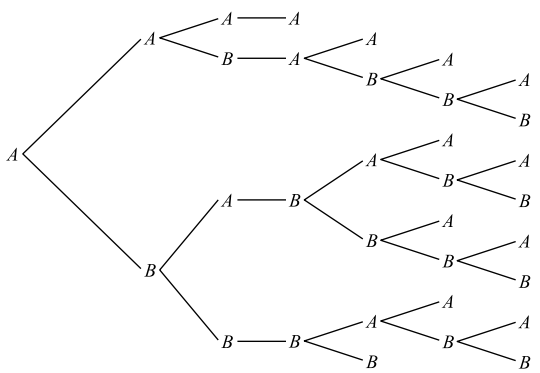


Figura 5-4

CAPÍTULO 6 Técnicas de conteo avanzadas, recurrencia

6.1 INTRODUCCIÓN

En este capítulo se presentan técnicas y problemas de conteo más elaborados como son combinaciones con repetición, particiones ordenadas y no ordenadas, el principio de inclusión-exclusión y el principio del palomar.

Aquí también se analiza la relación recursiva o de recurrencia.

6.2 COMBINACIONES CON REPETICIONES

Considere el siguiente problema. Una panadería elabora $M = 4$ tipos de galleta: *a*) manzana, *b*) plátano, *c*) zanahoria y *d*) dátil. Encuentre el número de formas en que una persona puede comprar $r = 8$ galletas.

Observe que el orden no cuenta y que se trata de un ejemplo de combinaciones con repetición. En este caso, cada combinación se enumera con letras *a*, primero, luego con las *b*, después con las *c* y finalmente con las *d*. A continuación se muestran cuatro de estas combinaciones.

$$r_1 = aa, bb, cc, dd; \quad r_2 = aaa, c, ddd; \quad r_3 = bbbb, c, ddd; \quad r_4 = aaaaa, ddd.$$

Contar el número *m* de tales combinaciones puede no ser fácil.

Suponga que quiere codificar las combinaciones anteriores con dos símbolos, por ejemplo 0 y 1. Entonces 0 denota una galleta y 1 denota el cambio de un tipo de galleta a otro. Así, cada combinación requiere $r = 8$ ceros, uno para cada galleta, y $M - 1 = 3$ unos, donde el primer uno denota el cambio de *a* a *b*; el segundo, el cambio de *b* a *c* y el tercero, un cambio de *c* a *d*. De modo que las cuatro combinaciones anteriores se codifican como sigue:

$$r_1 = 00100100100, \quad r_2 = 00001101000, \quad r_3 = 10000101000, \quad r_4 = 00000111000.$$

Contar el número *m* de estas "palabras código" es fácil. Cada una contiene $R + M - 1 = 11$ dígitos, donde $r = 8$ son ceros y, por tanto, $M - 1 = 3$ son unos. En consecuencia,

$$M = C(11, 8) = C(11, 3) = \frac{11 \cdot 10 \cdot 9}{3 \cdot 2 \cdot 1} = 165$$

Con un razonamiento semejante se obtiene el siguiente teorema.

Teorema 6.1: Suponga que hay M tipos de objetos. Entonces el número de combinaciones de r de estos objetos es $C(r + M - 1, r) = C(r + M - 1, M - 1)$.

EJEMPLO 6.1 Encuentre el número m de soluciones enteras no negativas de $x + y + z = 18$.

Cada solución, por ejemplo $x = 3$, $y = 7$, $z = 8$, se considera una combinación de $r = 18$ objetos que constan de 3 *aes*, 7 *bes* y 8 *ces*, donde hay $M = 3$ tipos de objetos: *aes*, *bes* y *ces*. Por el teorema 6.1,

$$m = C(r + M - 1, M - 1) = C(20, 2) = 190.$$

6.3 PARTICIONES ORDENADAS Y NO ORDENADAS

Suponga que un conjunto tiene 7 elementos y quiere encontrar el número m de particiones ordenadas de S en tres celdas: $[A_1, A_2, A_3]$ de modo que contengan 2, 3 y 2 elementos, respectivamente.

Puesto que S tiene 7 elementos, hay $C(7, 2)$ formas de escoger los dos primeros elementos para A_1. A continuación hay $C(5, 3)$ formas de escoger los 3 elementos para A_2. Por último, hay $C(2, 2)$ formas de escoger los 2 elementos para A_3 (o bien, los 2 últimos elementos forman la celda A_3). Así,

$$m = C(7, 2)C(5, 3)C(2, 2) = \binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7 \cdot 6}{2 \cdot 1} \cdot \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} \cdot \frac{2 \cdot 1}{2 \cdot 1} = 210$$

Observe que

$$m = \binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!5!} \cdot \frac{5!}{3!2!} \cdot \frac{2!}{2!0!} = \frac{7!}{2!3!2!}$$

puesto que cada numerador después del primero se cancela con un término en el denominador del factor previo.

Es posible demostrar que el análisis anterior es cierto en general. A saber:

Teorema 6.2: El número m de particiones ordenadas de un conjunto S con n elementos en r celdas $[A_1, A_2, \ldots, A_r]$ donde, para cada i, $n(A_i) = n_i$, es:

$$m = \frac{n!}{n_1!n_2! \ldots n_r!}$$

Particiones no ordenadas

A menudo es necesario partir un conjunto S en celdas $[A_1, A_2, \ldots, A_r]$, donde ahora las celdas no están ordenadas. El número m de tales particiones no ordenadas se obtiene a partir del número m' de particiones ordenadas al dividir m entre cada $k!$, donde k celdas tienen el mismo número de elementos.

EJEMPLO 6.2 Encuentre el número m de formas para repartir a 10 estudiantes en cuatro equipos $[A_1, A_2, A_3, A_4]$ de modo que en dos equipos haya 3 estudiantes y en dos equipos haya 2 estudiantes.

Por el teorema 6.2, hay $m' = 10!/(3!3!2!2!) = 25\,200$ de estas particiones ordenadas.

Debido a que los equipos forman una partición no ordenada, m' se divide entre 2! debido a las dos celdas con 3 elementos cada una y 2! debido a las dos celdas con 2 elementos cada una.

Así, $m = 25\,200/(2!2!) = 6\,300$.

6.4 OTRA APLICACIÓN DEL PRINCIPIO DE INCLUSIÓN-EXCLUSIÓN

Sean $A_1, A_2, \ldots, A_r$ subconjuntos de un conjunto universo U. Suponga que s_k denota la suma de las cardinalidades de las k intersecciones posibles de los conjuntos; es decir, la suma de todas las cardinalidades

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$$

Por ejemplo,

$$s_1 \sum_i n(A_i), \quad s_2 = \sum_{i<j} n(A_i \cap A_j), \quad s_3 = \sum_{i_1<i_2<i_3} n(A_{i_1} \cap A_{i_2} \cap A_{i_3})$$

El principio de inclusión-exclusión, que aparece en la sección 5.7, proporcionó una fórmula para el número de elementos en la unión de los conjuntos. Esto es, por el teorema 5.9

$$n(A_1 \cup A_2 \cup \cdots \cup A_r) = s_1 - s_2 + s_3 - \cdots + (-1)^{r-1} s_r$$

Si se aplica la ley de DeMorgan,

$$n(A_1^{\mathrm{C}} \cap A_2^{\mathrm{C}} \cap \ldots \cap A_r^{\mathrm{C}}) = n([A_1 \cup A_2 \cup \ldots \cup A_r]^{\mathrm{C}}) = |\mathbf{U}| - n(A_1 \cup A_2 \cup \ldots \cup A_r)$$

En consecuencia, resulta una forma alterna del teorema 5.9:

Teorema (principio de inclusión-exclusión) 6.3: Sean $A_1, A_2, \ldots, A_r$ subconjuntos de un conjunto universo **U**. Entonces el número m de elementos que no aparecen en ninguno de los subconjuntos $A_1, A_2, \ldots, A_r$ de **U** es:

$$m = n(A_1^{\mathrm{C}} \cap A_2^{\mathrm{C}} \cap \ldots \cap A_r^{\mathrm{C}}) = |\mathbf{U}| - s_1 + s_2 - s_3 + \cdots + (-1)^r s_r$$

EJEMPLO 6.3 Sea **U** el conjunto de enteros positivos menores o iguales que 1 000. Entonces $|U| = 1\,000$. Encuentre $|S|$, donde S es el conjunto de los enteros que no son divisibles entre 3, 5 o 7.

Sean A el subconjunto de enteros que son divisibles entre 3, B los divisibles entre 5 y C los divisibles entre 7. Entonces $S = A^C \cap B^C \cap C^C$ puesto que cada elemento de S no es divisible entre 3, 5 o 7. Por división entera,

$$|A| = 1\,000/3 = 333, \quad |B| = 1\,000/5 = 200, \quad |C| = 1\,000/7 = 142,$$
$$|A \cap B| = 1\,000/15 = 66, \quad |A \cap C| = 1\,000/21 = 47, \quad |B \cap C| = 1\,000/35 = 28,$$
$$|A \cap B \cap C| = 1\,000/105 = 9$$

Así, por el principio de inclusión-exclusión, teorema 6.3:

$$|S| = 1\,000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 1\,000 - 675 + 141 - 9 = 457$$

Número de funciones sobre

Sean A y B conjuntos tales que $|A| = 6$ y $|B| = 4$. Se quiere encontrar el número de funciones suprayectivas (sobre) de A sobre B.

Sean b_1, b_2, b_3, b_4 los cuatro elementos en B. Sea **U** el conjunto de todas las funciones de A en B. Además, sea F_1 el conjunto de funciones que no mandan ningún elemento de A en b_1; es decir, b_1 no está en el rango de ninguna función en F_1. En forma semejante, sean F_2, F_3 y F_4 los conjuntos de funciones que no mandan ningún elemento de A en b_2, b_3 y b_4, respectivamente.

Lo que se busca es el número de funciones en $S = F_1^C \cap F_2^C \cap F_3^C \cap F_4^C$, es decir, aquellas funciones que mandan por lo menos un elemento de A en b_1, por lo menos un elemento de A en b_2, y así en lo sucesivo. El principio de inclusión-exclusión, teorema 6.3, se aplica como sigue.

i) En cada función de **U**, hay 4 opciones para cada uno de los 6 elementos en A; por tanto, $|U| = 4^6 = 4\,096$.

ii) En F_i hay $C(4, 1) = 4$ funciones. En cada caso hay 3 opciones para cada uno de los 6 elementos en A; por tanto, $|F_i| = 3^6 = 729$.

iii) Hay $C(4, 2) = 6$ pares $F_i \cap F_j$. En cada caso hay 2 opciones para cada uno de los 6 elementos en A; por tanto, $|F_i \cap F_j| = 2^6 = 64$.

iv) Hay $C(4, 3) = 4$ tripletas $F_i \cap F_j \cap F_k$. En cada caso sólo hay una opción para cada uno de los 6 elementos en A; por tanto, $|F_i \cap F_j \cap F_k| = 1^6 = 1$.

v) $F_1 \cap F_2 \cap F_3 \cap F_4$ no tiene elementos; es decir, es vacío. Por tanto, $|F_1 \cap F_2 \cap F_3 \cap F_4| = 0$. Por el principio de inclusión-exclusión, teorema 6.3:

$$\begin{aligned}|S| &= |F_1^C \cap F_2^C \cap F_3^C \cap F_4^C| = 4^6 - C(4,1)3^6 + C(4,2)2^6 - C(4,3)1^7 \\ &= 4\,096 - 2\,916 + 384 - 1 = 795\end{aligned}$$

El resultado anterior es cierto en general. A saber,

Teorema 6.4: Suponga que $|A| = m$ y $|B| = n$, donde $m \geq n$. Entonces el número N de funciones suprayectivas (sobre) de A sobre B es:

$$N = n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \cdots + (-1)^{n-1}C(n,n-1)1^m$$

Desarreglos

Un *desarreglo* es una permutación de objetos en la que ningún objeto está en su posición original. Por ejemplo, 453162 no es un desarreglo de 123456, ya que 3 está en su posición correcta, pero 264531 es un desarreglo de 123456. (En forma alterna, una permutación de $\sigma = X \to X$ es un desarreglo si $\sigma(i) \neq i$ para toda $i \in X = \{1, 2, \ldots, n\}$.)

Sea D_n el número de desarreglos de n objetos. Por ejemplo, 231 y 312 son los únicos desarreglos de 123. Por tanto, $D_3 = 2$. El siguiente teorema, demostrado en el problema 6.6, se aplica.

Teorema 6.5: $D_n = n![1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}]$.

La probabilidad (capítulo 7) de que ocurra un desarreglo de n objetos es igual a D_n dividido entre $n!$, el número de permutaciones de los n objetos. Así, el teorema 6.5 produce el siguiente

Corolario 6.6: Sea p la probabilidad de un desarreglo de n objetos. Entonces

$$p = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}$$

EJEMPLO 6.4 (Problema de los sombreros) Suponga que $n = 5$ personas dejan sus sombreros en el guardarropa de un restorán, y que los sombreros les son devueltos al azar. Encuentre la probabilidad p de que ninguna persona reciba su sombrero.

Éste es un ejemplo de un desarreglo con $n = 5$. Por el corolario 6.6,

$$p = 1 - 1 + 1/2 - 1/6 + 1/24 - 1/120 = 44/120 = 11/30 \approx 0.367$$

Observe que los signos alternan y que los términos se hacen muy, muy pequeños en el corolario 6.6. En la figura 6-1 se proporcionan los valores de p para los primeros valores de n. Observe que, para $n > 4$, p está muy próximo del siguiente valor (donde $e = 2.718$):

$$e^{-1} = 1 - \tfrac{1}{1!} + \tfrac{1}{2!} - \tfrac{1}{3!} + \cdots + (-1)^n \tfrac{1}{n!} + \cdots \approx 0.368$$

n	1	2	3	4	5	6	7
$p = D_n/n!$	0.0000	0.5000	0.3333	0.3750	0.3667	0.3681	0.3679

Figura 6-1

6.5 OTRA APLICACIÓN DEL PRINCIPIO DEL PALOMAR

El principio del palomar (con su generalización) se planteó con ejemplos sencillos en la sección 5.6. Aquí se proporcionan ejemplos con aplicaciones más complicadas de este principio.

EJEMPLO 6.5 Considere a seis personas, de las que dos de ellas son conocidas o desconocidas. Demuestre que hay tres personas que se conocen o se desconocen entre sí.

Sea A una de las personas. Sean X el conjunto que consta de las personas que conoce A y Y el conjunto que consta de las que desconoce A. Por el principio del palomar, X o Y contiene por lo menos a tres personas. Suponga que X consta de tres personas. Si a dos de ellas las conoce, entonces las dos y A son tres personas que se conocen. En caso de no serlo, entonces X consta de tres personas desconocidas entre sí. En forma alterna, suponga que Y consta de tres personas. Si dos de ellas se desconocen, entonces las dos con A son tres personas que se desconocen. De no serlo, entonces X contiene tres personas que se conocen.

EJEMPLO 6.6 Considere cinco puntos *reticulares* $(x_1, y_1), \ldots, (x_5, y_5)$ en el plano; es decir, puntos con coordenadas enteras. Demuestre que el punto medio de cualquier par de los puntos también es un punto reticular.

El punto medio de los puntos $P(a, b)$ y $Q(c, d)$ es $([a + c]/2, ([b + d]/2)$. Observe que $(r + s)/2$ es un entero si r y s son enteros con la misma *paridad*; es decir, que ambos sean impares o ambos sean pares. Hay cuatro pares de paridades: (impar, impar), (impar, par), (par, impar) y (par, par). Hay cinco puntos. Por el principio del palomar, dos de los puntos tienen el mismo par de paridades. El punto medio de estos dos puntos tiene coordenadas enteras.

A continuación se presenta una aplicación importante del principio del palomar.

Teorema 6.7: Toda sucesión de $n^2 + 1$ números reales distintos contiene una subsucesión de longitud $n + 1$ que es estrictamente creciente o estrictamente decreciente.

Por ejemplo, considere la siguiente sucesión de $10 = 3^2 + 1$ números (donde $n = 3$): 2, 1, 8, 6, 7, 5, 9, 4, 12, 3. Hay muchas subsucesiones de longitud $n + 1 = 4$ que son estrictamente crecientes o estrictamente decrecientes; por ejemplo,

$$2, 6, 9, 12; \quad 1, 5, 9, 12; \quad 8, 6, 5, 4; \quad 7, 5, 4, 3.$$

Por otra parte, la siguiente sucesión de $9 = 3^2$ números no tiene ninguna subsucesión de longitud $n + 1 = 4$ que sea estrictamente creciente o estrictamente decreciente:

$$3, \quad 2, \quad 1, \quad 6, \quad 5, \quad 4, \quad 9, \quad 8, \quad 7.$$

La demostración del teorema 6.7 se presenta en el problema 6.10.

6.6 RELACIONES RECURSIVAS, O DE RECURRENCIA

Previamente analizó funciones definidas de manera recursiva como la

$$a) \text{ función factorial}, \quad b) \text{ sucesión de Fibonacci}, \quad c) \text{ función de Ackermann}.$$

Aquí analizará ciertos tipos de sucesiones $\{a_n\}$ definidas recursivamente y su solución. Lo primero es darse cuenta de que una *sucesión* es simplemente una función cuyo dominio es

$$\mathbf{N} = \{1, 2, 3, \ldots\} \quad \text{o} \quad \mathbf{N}_0 = \mathbf{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$$

Se empieza con algunos ejemplos.

EJEMPLO 6.7 Considere la siguiente sucesión que empieza con el número 3 y para la cual cada uno de los términos siguientes se encuentra al multiplicar por 2 el término previo:

$$3, \quad 6, \quad 12, \quad 24, \quad 48, \quad \ldots$$

Es posible definirla recursivamente por:

$$a_0 = 3, \quad a_k = 2a_{k-1} \text{ para } k \geq 1 \quad \text{o} \quad a_0 = 3, \quad a_{k+1} = 2a_k \quad \text{para } k \geq 0$$

La segunda definición se obtiene a partir de la primera al hacer $k = k + 1$. Resulta evidente que la fórmula $a_n = 3(2^n)$ proporciona el n-ésimo término de la sucesión sin necesidad de calcular ningún término previo.

A continuación se presentan las siguientes observaciones pertinentes sobre el ejemplo anterior.

1) La ecuación $a_k = 2a_{k-1}$ o, en forma equivalente, $a_{k+1} = 2a_k$, donde un elemento de la sucesión se define en función del término previo de la sucesión, se denomina *relación recursiva* o *de recurrencia*.
2) La ecuación $a_0 = 3$, que asigna un valor específico a uno de los términos, se denomina *condición inicial*.
3) La función $a_n = 3(2^n)$, que proporciona una fórmula para a_n como una función de n, no del término previo, se denomina *solución* de la relación de recurrencia.
4) Puede haber muchas sucesiones que satisfacen una relación de recurrencia. Por ejemplo, cada una de las siguientes expresiones es una solución de la relación recursiva $a_k = 2a_{k-1}$.

$$1, 2, 4, 8, 16, \ldots \quad \text{y} \quad 7, 14, 28, 56, 112, \ldots$$

Todas las soluciones constituyen la *solución general* de la relación de recurrencia.
5) Por otra parte, puede haber una solución única a una relación de recurrencia que también satisface condiciones iniciales dadas. Por ejemplo, la condición inicial $a_0 = 3$ únicamente produce la solución 3, 6, 12, 24, ... de la relación de recurrencia $a_k = 2a_{k-1}$.

En este capítulo se muestra cómo resolver algunas relaciones recursivas. Primero se proporcionan dos sucesiones importantes que quizá el lector ya ha estudiado.

EJEMPLO 6.8

a) *Progresión aritmética*

Una progresión aritmética es una sucesión de la forma

$$a, a + d, a + 2d, a + 3d, \ldots$$

Es decir, la sucesión empieza con el número a y cada término sucesivo se obtiene a partir del término previo al sumarle d (la diferencia común entre dos términos cualesquiera). Por ejemplo:

i) $a = 5, d = 3$: $5, 8, 9, 11, \ldots$
ii) $a = 2, d = 5$: $2, 7, 12, 17, \ldots$
iii) $a = 1, d = 0$: $1, 1, 1, 1, 1, \ldots$

Se observa que la progresión aritmética general puede definirse recursivamente por:

$$a_1 = a \quad \text{y} \quad a_{k+1} = a_k + d \quad \text{para } k \geq 1$$

donde la solución es $a_n = a + (n - 1)d$.

b) *Progresión geométrica*

Una progresión geométrica es una sucesión de la forma

$$a, ar, ar^2, ar^3, \ldots$$

Es decir, la sucesión empieza con el número a y cada término sucesivo se obtiene a partir del término previo al multiplicarlo por r (la razón común entre dos términos cualesquiera) por ejemplo:

i) $a = 1, r = 3$: $1, 3, 9, 27, 81, \ldots$
ii) $a = 5, r = 2$: $5, 10, 20, 40, \ldots$
iii) $a = 1, r = \frac{1}{2}$: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$

Se observa que la progresión geométrica general puede definirse recursivamente por:

$$a_1 = a \quad \text{y} \quad a_{k+1} = r\,a_k \quad \text{para } k \geq 1$$

donde la solución es $a_{n+1} = ar^n$.

6.7 RELACIONES RECURSIVAS, O DE RECURRENCIA, LINEALES CON COEFICIENTES CONSTANTES

Una *relación recursiva de orden k* es una función de la forma

$$a_n = \Phi(a_{n-1}, a_{n-2}, \ldots, a_{n-k}, n)$$

es decir, donde el n-ésimo término a_n de una sucesión es una función de los k términos precedentes $a_{n-1}, a_{n-2} \ldots, a_{n-k}$ (y posiblemente n). En particular, una *relación recursiva lineal de orden k con coeficientes constantes* es una relación recursiva de la forma

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k} + f(n)$$

donde $C_1, C_2, \ldots, C_k$ son constantes son $C_k \neq 0$ y $f(n)$ es una función de n. A continuación se proporciona el significado de los términos lineal y coeficientes constantes:

Lineal: No hay potencias o productos de los a_j.
Coeficientes constantes: Las $C_1, C_2, \ldots, C_k$ son constantes (no dependen de n).

Si $f(n) = 0$, entonces la relación es *homogénea*.

Resulta evidente que a_n se resuelve de manera única si se conocen los valores de $a_{n-1}, a_{n-2} \ldots, a_{n-k}$. En consecuencia, por inducción matemática, hay una sucesión única que satisface la relación de recurrencia si se proporcionan los *valores iniciales* de los k primeros términos de la sucesión.

EJEMPLO 6.9 Considere cada una de las siguientes relaciones de recurrencia.

a) $a_n = 5a_{n-1} - 4a_{n-2} + n^2$

Se trata de una relación de recurrencia de segundo orden con coeficientes constantes. Es no homogénea debido a la n^2. Suponga que se proporcionan las condiciones iniciales $a_1 = 1$, $a_2 = 2$. Entonces es posible encontrar secuencialmente los siguientes términos de la sucesión:

$$a_3 = 5(2) - 4(1) + 3^2 = 15, \quad a_4 = 5(15) - 4(2) + 4^2 = 83$$

b) $a_n = 2a_{n-1}a_{n-2} + n^2$

El producto $a_{n-1}a_{n-2}$ significa que la relación de recurrencia no es lineal. Dadas las condiciones iniciales $a_1 = 1$, $a_2 = 2$, aún es posible encontrar los siguientes elementos de la sucesión:

$$a_3 = 2(2)(1) + 3^2 = 13, \quad a_4 = 2(13)(2) + 4^2 = 68$$

c) $a_n = na_{n-1} + 3a_{n-2}$

Se trata de una relación de recurrencia lineal homogénea de segundo orden pero sin coeficientes constantes porque el coeficiente de a_{n-1} es n, no una constante. Dadas las condiciones iniciales $a_1 = 1$, $a_2 = 2$, los siguientes elementos de la sucesión son:

$$a_3 = 3(2) + 3(1) = 9, \quad a_4 = 4(9) + 3(2) = 42$$

d) $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$

Se trata de una relación de recurrencia lineal homogénea de tercer orden con coeficientes constantes. Así, se requieren tres, no dos, condiciones iniciales para obtener una solución única de la relación recursiva. Suponga que se proporcionan las condiciones iniciales $a_1 = 1$, $a_2 = 2$, $a_3 = 1$. Entonces, los siguientes elementos de la sucesión son:

$$a_4 = 2(1) + 5(2) - 6(1) = 6, \quad a_5 = 2(2) + 5(1) - 6(6) = -37$$
$$a_6 = 2(1) + 5(6) - 6(-37) = 254$$

En este capítulo se investigan las soluciones de relaciones de recurrencia lineales homogéneas con coeficientes constantes. La teoría de las relaciones de recurrencia no homogéneas y de las relaciones de recurrencia homogéneas sin coeficientes constantes rebasa el alcance de este texto.

Por conveniencia al realizar los cálculos, la mayor parte de las sucesiones que se estudian aquí empiezan con a_n en lugar de hacerlo con a_{n-1}. La teoría no se afecta en absoluto.

6.8 SOLUCIÓN DE RELACIONES DE RECURRENCIA LINEALES HOMOGÉNEAS DE SEGUNDO ORDEN

Considere una relación de recurrencia homogénea de segundo orden con coeficientes constantes que tiene la forma

$$a_n = sa_{n-1} + ta_{n-2} \quad \text{o} \quad a_n - sa_{n-1} - ta_{n-2} = 0$$

donde s y t son constantes con $t \neq 0$. El siguiente polinomio cuadrático se asocia a la relación de recurrencia anterior:

$$\Delta(x) = x^2 - sx - t$$

El polinomio $\Delta(x)$ se denomina *polinomio característico* de la relación de recurrencia, y las raíces de $\Delta(x)$ se denominan sus *raíces características*.

Teorema 6.8: Suponga que el polinomio característico $\Delta(x) = x^2 - sx - t$ de la relación de recurrencia

$$a_n = sa_{n-1} + ta_{n-2}$$

tiene raíces distintas r_1 y r_2. Entonces la solución general de la relación de recurrencia es la siguiente, donde c_1 y c_2 son constantes arbitrarias:

$$a_n = c_1 r_1^n + c_2 r_2^n$$

Conviene señalar que las constantes c_1 y c_2 pueden determinarse en forma única mediante condiciones iniciales; además, el teorema se cumple aun cuando las raíces no sean reales. Pero dichos casos rebasan el alcance de este texto.

EJEMPLO 6.10 Considere la siguiente relación de recurrencia homogénea:

$$a_n = 2a_{n-1} + 3a_{n-2}$$

La solución general se obtiene al encontrar, primero, su polinomio característico $\Delta(x)$ y sus raíces r_1 y r_2:

$$\Delta(x) = x^2 - 2x - 3 = (x - 3)(x + 1); \quad \text{raíces } r_1 = 3, r_2 = -1$$

Puesto que las raíces son distintas, se aplica el teorema 6.8 para encontrar la solución general:

$$a_n = c_1 3^n + c_2(-1)^n$$

Así, valores arbitrarios c_1 y c_2 proporcionan una solución de la relación de recurrencia.

Suponga que también se proporcionan las condiciones iniciales $a_0 = 1$, $a_1 = 2$. Mediante la relación de recurrencia es posible calcular los siguientes términos de la sucesión:

$$1, \quad 2, \quad 8, \quad 28, \quad 100, \quad 356, \quad 1\,268, \quad 3\,516, \quad \ldots$$

La solución única se obtiene al encontrar c_1 y c_2 mediante las condiciones iniciales:

$$\text{Para } n = 0 \text{ y } a_0 = 1, \text{ se obtiene:} \quad c_1 3^0 + c_2(-1)^0 = 1 \quad \text{o} \quad c_1 + c_2 = 1$$
$$\text{Para } n = 1 \text{ y } a_1 = 2, \text{ se obtiene:} \quad c_1 3^1 + c_2(-1)^1 = 2 \quad \text{o} \quad 3c_1 - c_2 = 2$$

Al resolver el sistema de dos ecuaciones en las incógnitas c_1 y c_2 se obtiene:

$$c_1 = \frac{3}{4} \quad \text{y} \quad c_2 = \frac{1}{4}$$

Por tanto, la solución única de la relación de recurrencia dada con las condiciones iniciales dadas $a_0 = 1$, $a_1 = 2$ es:

$$a_n = \frac{3}{4}3^n + \frac{1}{4}(-1)^n = \frac{3^{n+1} + (-1)^n}{4}$$

EJEMPLO 6.11 Considere la famosa sucesión de Fibonacci:

$$a_n = a_{n-1} + a_{n-2}, \quad \text{con} \quad a_0 = 0, a_1 = 1$$

Los 10 primeros términos de la sucesión son:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Algunas veces la sucesión de Fibonacci se define mediante las condiciones iniciales $a_0 = 1$, $a_1 = 1$ o las condiciones iniciales $a_1 = 1$, $a_2 = 2$. Por conveniencia al realizar los cálculos aquí se usa $a_0 = 1$, $a_1 = 1$. (Las tres condiciones iniciales producen la misma sucesión después del par de términos 1, 2.)

Observe que la sucesión de Fibonacci es una relación de recurrencia lineal homogénea de segundo orden, de modo que es posible resolverla con el teorema 6.8. Su polinomio característico es el siguiente:

$$\Delta(x) = x^2 - x - 1$$

Al aplicar la fórmula cuadrática se obtienen las raíces:

$$r_1 = \frac{1+\sqrt{5}}{2}, \quad r_2 = \frac{1-\sqrt{5}}{2}$$

Por el teorema 6.8 se obtiene la solución general:

$$a_n = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Las condiciones iniciales producen el siguiente sistema de dos ecuaciones lineales en c_1 y c_2:

$$\text{Para } n = 0 \text{ y } a_0 = 0, \text{ se obtiene:} \quad 0 = c_1 + c_2$$

$$\text{Para } n = 1 \text{ y } a_1 = 1, \text{ se obtiene:} \quad 1 = c_1 \left(\frac{1+\sqrt{5}}{2}\right) + c_2 \left(\frac{1-\sqrt{5}}{2}\right)$$

La solución del sistema es:

$$c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}}$$

En consecuencia, la solución de la relación de recurrencia de Fibonacci es:

$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Puede demostrarse que el valor absoluto del segundo término para a_n siempre es menor que ½. Por tanto, a_n también es el entero más próximo al número

$$\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \approx (0.4472)(1.6180)^n$$

Solución cuando las raíces del polinomio característico son iguales

Suponga que las raíces del polinomio característico no son distintas. Entonces se tiene el siguiente resultado.

Teorema 6.9: Suponga que el polinomio característico $\Delta(x) = x^2 - sx - t$ de la relación de recurrencia

$$a_n = sa_{n-1} + ta_{n-2}$$

sólo tiene una raíz r_0. Entonces se concluye que la solución general de la relación de recurrencia, donde c_1 y c_2 son constantes arbitrarias, es:

$$a_n = c_1 r_0^n + c_2 n r_0^n$$

Las constantes c_1 y c_2 se determinan en forma única mediante las condiciones iniciales.

EJEMPLO 6.12 Considere la siguiente relación de recurrencia homogénea:

$$a_n = 6a_{n-1} - 9a_{n-2}$$

El polinomio característico $\Delta(x)$ es el siguiente:

$$\Delta(x) = x^2 - 6x + 9 = (x-3)^2$$

Así, $\Delta(x)$ sólo tiene la raíz $r_0 = 3$. Luego se aplica el teorema 6.9 para obtener la siguiente solución general de la relación de recurrencia:

$$a_n = c_1 3^n + c_2 n 3^n$$

Por tanto, valores arbitrarios de c_1 y c_2 proporcionan una solución de la relación de recurrencia.

Suponga que también se proporcionan las condiciones iniciales $a_1 = 3$, $a_2 = 27$. La relación de recurrencia permite calcular los siguientes términos de la sucesión:

$$3, \quad 27, \quad 135, \quad 567, \quad 2\,187, \quad 8\,109, \quad \ldots$$

La solución única se obtiene al encontrar c_1 y c_2 mediante las condiciones iniciales:

$$\text{Para } n = 1 \text{ y } a_1 = 3, \text{ se obtiene:} \quad c_1 3^1 + c_2(1)(3)^1 = 3 \quad \text{o} \quad 3c_1 + 3c_2 = 3$$
$$\text{Para } n = 2 \text{ y } a_2 = 27, \text{ se obtiene:} \quad c_1 3^2 + c_2(2)(3)^2 = 27 \quad \text{o} \quad 9c_1 - 18c_2 = 27$$

Al resolver el sistema de ecuaciones con dos incógnitas c_1 y c_2 se obtiene:

$$c_1 = -1 \quad \text{y} \quad c_2 = 2$$

Por tanto, la única solución de la relación de recurrencia con las condiciones iniciales dadas es:

$$a_n = -3^n + 2n3^n = 3^n(2n-1)$$

6.9 SOLUCIÓN DE RELACIONES DE RECURRENCIA LINEALES HOMOGÉNEAS GENERALES

Ahora considere una relación general de recurrencia lineal homogénea de orden k con coeficientes constantes que tiene la forma

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + C_3 a_{n-3} + \cdots + C_k a_{n-k} = \sum_{i=1}^{k} C_i a_{n-1} \tag{6.1}$$

donde $C_1, C_2, \ldots, C_k$ son constantes con $C_k \neq 0$. El *polinomio característico* $\Delta(x)$ de la relación de recurrencia (*6.1*) es:

$$\Delta(x) = x^k - C_1 x^{k-1} - C_2 x^{k-2} - C_3 x^{k-3} - \cdots - C_k = x^k - \sum_{i=1}^{k} C_1 x^{k-1}$$

Las raíces de $\Delta(x)$ se denominan *raíces características* de la relación de recurrencia.

Las siguientes observaciones son pertinentes.

Observación 1: Si $p(n)$ y $q(n)$ son soluciones de (*6.1*), entonces cualquier combinación lineal

$$c_1 p(n) + c_2 q(n)$$

de $p(n)$ y $q(n)$ también es una solución. (Esto no es cierto si la relación de recurrencia es no homogénea.)

Observación 2: Si r es una raíz con multiplicidad m del polinomio característico $\Delta(x)$ de (*6.1*), entonces cada uno de los siguientes términos

$$r^n, nr^n, n^2r^n, \ldots, n^{n-1}r^n$$

es una solución de (*6.1*). Por tanto, cualquier combinación lineal

$$c_1r^n + c_2nr^n + c_3n^2r^n + \cdots + c_mn^{m-1}r^n = (c_1 + c_2n + c_3n^2 + \cdots + c_mn^{m-1})r^n$$

también es una solución.

EJEMPLO 6.13 Considere la siguiente relación de recurrencia homogénea de tercer orden:

$$a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$$

El polinomio característico $\Delta(x)$ de la relación de recurrencia es:

$$\Delta(x) = x^3 - 11x^2 + 39x - 45 = (x - 3)^2(x - 5)$$

Así, $\Delta(x)$ tiene dos raíces: $r_1 = 3$ con multiplicidad 2 y $r_2 = 5$ con multiplicidad 1. En consecuencia, por las observaciones anteriores, la solución general de la relación de recurrencia es la siguiente:

$$a_n = c_1(3^n) + c_2n(3^n) + c_3(5^n) = (c_1 + c_2n)(3^n) + c_3(5^n)$$

Por tanto, valores arbitrarios de c_1, c_2, c_3 proporcionan una solución de la relación de recurrencia.

Suponga que también se proporcionan las condiciones iniciales $a_0 = 5$, $a_1 = 11$, $a_3 = 25$. La relación de recurrencia permite calcular los siguientes términos de la sucesión:

$$5, \quad 11, \quad 25, \quad 71, \quad 301, \quad 1\,667, \quad \ldots$$

La solución única se encuentra al determinar c_1, c_2, c_3 mediante las condiciones iniciales:

$$\begin{array}{lll} \text{Para } n = 0 \text{ y } a_0 = 5, & \text{se obtiene:} & c_1 + c_3 = 5 \\ \text{Para } n = 1 \text{ y } a_1 = 11, & \text{se obtiene:} & 3c_1 + 3c_2 + 5c_3 = 11 \\ \text{Para } n = 2 \text{ y } a_2 = 25, & \text{se obtiene:} & 9c_1 + 18c_2 + 25c_3 = 25 \end{array}$$

Al resolver el sistema de tres ecuaciones en las incógnitas c_1, c_2, c_3 se obtiene:

$$c_1 = 4, \quad c_2 = -2, \quad c_3 = 1$$

En consecuencia, la solución única de la relación de recurrencia con las condiciones iniciales dadas es la siguiente:

$$a_n = (4 - 2n)(3^n) + 5^n$$

Observación: La determinación de las raíces del polinomio característico $\Delta(x)$ es un paso importante al resolver relaciones de recurrencia, pero, en términos generales, es difícil cuando el grado de $\Delta(x)$ es mayor que 2. (En el ejemplo B.16 se muestra una forma de encontrar las raíces de algunos polinomios de grado mayor o igual que 3.)

PROBLEMAS RESUELTOS

TÉCNICAS AVANZADAS DE CONTEO, INCLUSIÓN-EXCLUSIÓN

6.1 Una tienda de bagels vende $M = 5$ tipos de bagels. Encuentre el número m de formas en que un cliente puede comprar: *a*) 8 bagels; *b*) una docena de bagels.

Se aplica $m = C(r + M - 1, r) = C(r + M - 1, M - 1)$; es decir, el teorema 6.1, puesto que este problema corresponde a combinaciones con repeticiones.

a) Aquí $r = 8$, de modo que $m = C(8 + 4, 4) = C(12, 4) = 494$.

b) Aquí $r = 12$, de modo que $m = C(12 + 4, 4) = C(16, 4) = 1\,820$.

6.2 Encuentre el número m de soluciones no negativas de $x + y + z = 18$ con las condiciones $x \geq 3$, $y \geq 2$, $z \geq 1$.

Sean $x' = x - 3$, $y' = y - 2$ y $z' = z - 1$. Entonces m también es el número de soluciones no negativas de $x' + y' + z' = 12$. Así como en el ejemplo 6.1, este segundo problema corresponde a combinaciones con repeticiones con $M = 3$ y $r = 12$. Por tanto,

$$m = C(12 + 2, 2) = C(14, 2) = 91.$$

6.3 Sea E la ecuación $x + y + z = 18$. Encuentre el número m de soluciones no negativas de E con las condiciones de que $x < 7$, $y < 8$, $z < 9$.

Sea S el conjunto de todas las soluciones no negativas de E. Sean A el conjunto de soluciones para las cuales $x \geq 7$, B el conjunto de soluciones para las cuales $y \geq 8$ y C el conjunto de soluciones para las cuales $z \geq 9$. Entonces

$$m = |A^C \cap B^C \cap C^C|$$

Como en el problema 6.2, se obtiene

$$\begin{aligned} |A| &= C(11 + 2, 2) = 78, \quad & |A \cap B| &= C(3 + 2, 2) = 10 \\ |B| &= C(10 + 2, 2) = 66, \quad & |A \cap C| &= C(2 + 2, 2) = 6 \\ |C| &= C(9 + 2, 2) = 55, \quad & |B \cap C| &= C(1 + 2, 2) = 3 \end{aligned}$$

También, $|S| = C(18 + 2, 2) = 190$ y $|A \cap B \cap C| = 0$. Por el principio de inclusión-exclusión,

$$m = 190 - (78 + 66 + 55) + (10 + 6 + 3) - 0 = 10$$

6.4 En un grupo hay 9 estudiantes. Encuentre el número m de formas: *a*) en que los 9 estudiantes pueden presentar 3 exámenes distintos si 3 estudiantes deben presentar todos los exámenes; *b*) los 9 estudiantes pueden repartirse en 3 equipos A, B, C, de modo que en cada equipo haya 3 estudiantes.

a) Método 1: Se busca el número m de particiones de los 9 estudiantes en celdas que contengan 3 estudiantes. Por el teorema 6.2, $m = 9!/(3!3!3!) = 5\,040$.

Método 2: Hay $C(9, 3)$ formas de escoger tres estudiantes para que presenten el primer examen, luego, hay $C(6, 3)$ formas de escoger 3 estudiantes para que presenten el segundo examen; y los estudiantes restantes presentan el tercer examen. Por tanto, $m = C(9, 3)C(6, 3) = 5\,040$.

b) Cada partición $\{A, B, C\}$ de los estudiantes puede ordenarse en $3! = 6$ formas como una partición ordenada. Por *a*), hay 5 040 de estas particiones ordenadas. Por tanto, $m = 5\,040/6 = 840$.

6.5 Encuentre el número N de formas en que una empresa puede asignar 7 proyectos a 4 personas de modo que cada persona obtenga por lo menos un proyecto.

Se quiere encontrar el número N de funciones sobre de un conjunto con $m = 7$ elementos sobre un conjunto con $n = 4$ elementos. Se aplica el teorema 6.4:

$$\begin{aligned} N &= 4^2 - C(4, 1)(3^7) + C(4, 2)(2^7) - C(4, 3)(1^7) \\ &= 4^7 - 4(3^7) + 6(2^7) - 4(1^7) = 16\,384 - 8\,748 + 768 - 4 = 8\,400 \end{aligned}$$

6.6 Demuestre el teorema 6.5: $D_n = n![1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}]$

Conviene recordar por la sección 3.3, que S_n denota el conjunto de permutaciones sobre $X = \{1, 2, \ldots, n\}$ y $|S_n| = n!$ Para $i = 1, \ldots, n$, representa F_i todas las permutaciones en S_n que "fijan i"; es decir, $F_i = \{\sigma \in S_n \mid \sigma(i) = i\}$. Entonces, para subíndices distintos,

$$|F_r| = (n-1)!, \quad |F_i \cap F_i| = (n-2)!, \ldots |F_{i_1} \cap F_{i_2} \cap \ldots \cap F_{i_r}| = (n-r)!$$

Sea Y el conjunto de todos los desarreglos en S_n; entonces

$$D_n = |Y| = |F_1^C \cap F_2^C \cap \cdots \cap F_n^C|$$

Por el principio de inclusión-exclusión,

$$D_n = |S_n| - s_1 + s_2 - s_3 + \cdots + (-1)^n s_n$$

donde

$$s_r = \sum_{i_1 < i_2 < \ldots < i_n} |F_{i_1} \cap F_{i_2} \cap \ldots \cap F_{i_r}| = C(n, r)\,(n-r)! = \frac{n!}{r!}$$

Al hacer $|S_n| = n!$ y $s_r = n!/r!$ en la fórmula para D_n se obtiene el teorema.

PRINCIPIO DEL PALOMAR

6.7 Si se escogen cinco puntos del interior de un cuadrado S que mide dos pulgadas por lado, demuestre que la distancia entre dos de los puntos debe ser menor que $\sqrt{2}$ pulgadas.

Se trazan dos líneas entre los lados opuestos de S, con lo cual S se separa en cuatro subcuadrados, cada uno de los cuales mide una pulgada por lado. Por el principio del palomar, dos de los puntos están en uno de los subcuadrados. La diagonal de cada subcuadrado mide $\sqrt{2}$ pulgadas, de modo que la distancia entre los dos puntos es menor que $\sqrt{2}$ pulgadas.

6.8 Sean p y q enteros positivos. Se dice que un número r satisface la propiedad (p, q) de Ramsey si un conjunto de r personas contiene un subconjunto p de personas conocidas o un subconjunto q de personas desconocidas. El número de Ramsey $R(p, q)$ es el menor entero r. Demuestre que $R(3, 3) = 6$.

Por el ejemplo 6.5, $R(3, 3) \geq 6$. Lo que demuestra $R(3, 3) > 5$. Si cinco personas están sentadas alrededor de una mesa redonda y cada persona sólo es amiga de la persona que está a su lado, no puede haber tres personas desconocidas mutuamente porque dos de las tres personas deben estar sentadas una al lado de la otra. Asimismo, no puede haber tres personas amigas entre sí, ya que no pueden sentarse una al lado de la otra. Por tanto, $R(3, 3) > 5$. En consecuencia, $R(3, 3) = 6$.

6.9 Un equipo X sostiene 18 encuentros en un periodo de dos semanas —14 días— y sostiene por lo menos un encuentro diario. Demostrar que hay un periodo de días en el que se juegan exactamente 9 encuentros.

Sea $S = \{s_1, s_2, \ldots, s_{14}\}$, donde s_i es el número de encuentros sostenidos por X desde el primer día hasta el i-ésimo día. Entonces $s_{14} = 18$ y todas las s_i son distintas. Sea $T = \{t_1, t_2, \ldots, t_{14}\}$, donde $t_i = s_i + 9$. Entonces $t_{14} = 18 + 9 = 27$, y las t_i son distintas. Juntos, S y T tienen $14 + 14 = 28$ números, que están entre 1 y 27. Por el principio del palomar, dos de los números deben ser iguales. No obstante, los elementos en S y los elementos en T son distintos. Por tanto, hay $s_j \in S$ y $t_n \in T$ tales que $s_j = t_k = s_k + 9$. En consecuencia,

$$9 = s_j - s_n = \text{número de encuentros jugados en los días } k+1, k+2, \ldots, j-1, j$$

6.10 Demuestre el teorema 6.7: cualquier sucesión de $n^2 + 1$ números reales distintos contiene una subsucesión de longitud $n + 1$ que es estrictamente creciente o estrictamente decreciente.

Sea $a_1, a_2, \ldots, a_{n^2+i}$ una sucesión de $n^2 + 1$ números reales distintos. A cada a_i se asocia el par (i_t, d_t) donde: 1) i_t es la subsucesión creciente más larga que empieza en a_t y 2) d_t es la subsucesión decreciente más larga que empieza en a_t. Por tanto, hay $n^2 + 1$ pares ordenados así: uno por cada número en la sucesión.

Luego se supone que ninguna subsucesión es más larga que n. Entonces i_t y d_t no pueden exceder a n. Por tanto, hay cuando mucho n^2 pares distintos (i_t, d_t). Por el principio del palomar, dos de los pares $n^2 + 1$ son iguales; es decir, hay dos puntos distintos a_r y a_s tales que $(i_r, d_r) = (i_s, d_s)$. Se puede suponer que $r < s$. Entonces a_r aparece antes que a_s en la sucesión [vea la figura 6-2*a*)]. Luego, a_r seguido por la subsucesión creciente de i_s números empezando en a_s constituye una subsucesión de longitud $i_s + 1 = i_r + 1$ empezando en a_r [vea la figura 6-2*b*)]. Esto contradice la definición de i_r. En forma

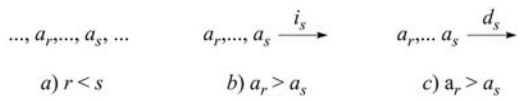


Figura 6-2

semejante, se supone que $a_r > a_s$. Luego, a_n seguido por la subsucesión decreciente de d_s números empezando en a_s constituye una subsucesión de longitud $d_r + 1 = d_s + 1$ empezando en a_r, lo cual contradice la definición de d_r [vea la figura 6-2*c*)]. En cada caso se llega a una contradicción. Así, la hipótesis de que ninguna subsucesión excede a n no es verdadera, por lo que se ha demostrado el teorema.

RECURSIÓN

6.11 Considere la relación de recurrencia homogénea de segundo orden $a_n = a_{n-1} + 2a_{n-2}$ con condiciones iniciales $a_0 = 2$, $a_1 = 7$.

a) Encuentre los tres términos siguientes de la sucesión.
b) Encuentre la solución general.
c) Encuentre la solución única con las condiciones iniciales dadas.

a) Cada término es la suma del término precedente más dos veces su segundo término precedente. Así:

$$a_2 = 7 + 2(2) = 11, \quad a_3 = 11 + 2(7) = 25, \quad a_4 = 25 + 2(11) = 46$$

b) Primero se debe encontrar el polinomio característico $\Delta(x)$ y sus raíces:

$$\Delta(x) = x^2 - x - 2 = (x - 2)(x + 1); \quad \text{raíces } r_1 = 2, r_2 = -1$$

Puesto que las raíces son distintas, para obtener la solución general se aplica el teorema 6.8:

$$a_n = c_1(2^n) + c_2(-1)^n$$

c) La solución única se obtiene al determinar c_1 y c_2 mediante las condiciones iniciales:

$$\text{Para } n = 0,\ a_0 = 2, \text{ se obtiene: } c_1(2^0) + c_2(-1)^0 = 2 \quad \text{o} \quad c_1 + c_2 = 2$$
$$\text{Para } n = 0,\ a_1 = 7, \text{ se obtiene: } c_1(2^1) + c_2(-1)^1 = 7 \quad \text{o} \quad 2c_1 - c_2 = 7$$

Al resolver las dos ecuaciones para c_1 y c_2 se obtiene $c_1 = 3$ y $c_2 = 1$. La solución única es la siguiente:

$$a_n = 3(2^n) - (-1)^n$$

6.12 En la relación de recurrencia homogénea de tercer orden $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$

a) Encuentre la solución general.
b) Encuentre la solución con condiciones iniciales $a_0 = 3$, $a_1 = 4$, $a_2 = 12$.

a) Primero se debe encontrar el polinomio característico

$$\Delta(x) = x^3 - 6x^2 + 12x - 8 = (x - 2)^3$$

Entonces $\Delta(x)$ sólo tiene una raíz: $r_0 = 2$, de multiplicidad 3. Así, la solución general de la relación de recurrencia es:

$$a_n = c_1(2^n) + c_2n(2^n) + c_3n^2(2^n) = (c_1 + c_2n + c_3n^2)(2^n)$$

b) Para encontrar los valores de c_1, c_2 y c_3 se procede así:

$$\text{Para } n = 0,\ a_0 = 3 \quad \text{se obtiene:} \quad c_1 = 3$$
$$\text{Para } n = 1,\ a_1 = 4 \quad \text{se obtiene:} \quad 2c_1 + 2c_2 + 2c_3 = 4$$
$$\text{Para } n = 2,\ a_2 = 12 \quad \text{se obtiene:} \quad 4c_1 + 8c_2 + 16c_3 = 12$$

Al resolver el sistema de tres ecuaciones en c_1, c_2 y c_3 se obtiene la solución

$$c_1 = 3, \quad c_2 = -2, \quad c_3 = 1$$

Por tanto, la solución única de la relación de recurrencia es:

$$a_n = (3 - 2n + n^2)(2^n)$$

PROBLEMAS SUPLEMENTARIOS

TÉCNICAS AVANZADAS DE CONTEO, INCLUSIÓN-EXCLUSIÓN

6.13 Una tienda vende $M = 4$ tipos de galleta. Encuentre el número de formas en que un cliente puede comprar:
a) 10 galletas; *b*) 15 galletas.

6.14 Encuentre el número m de soluciones no negativas de $x + y + z = 20$ con las condiciones de que $x \geq 5$, $y \geq 3$ y $z \geq 1$.

6.15 Sea E la ecuación $x + y + z = 20$. Encuentre el número m de soluciones no negativas de E con las condiciones de que $x < 8$, $y < 9$, $z < 10$.

6.16 Encuentre el número m de enteros positivos que no exceden a 1 000 y no son divisibles entre 3, 7 ni 11.

6.17 Encuentre el número de formas en que es posible repartir 14 personas en 6 comités de modo que en 2 comités haya 3 personas y en los otros comités haya 2 personas.

6.18 Suponga que una celda puede estar vacía. Encuentre el número m de formas en que un conjunto:
a) Con 3 personas puede separarse en *i*) tres celdas ordenadas; *ii*) tres celdas no ordenadas.
b) Con 4 personas puede separarse en *i*) tres celdas ordenadas; *ii*) tres celdas no ordenadas.

6.19 Encuentre el número N de funciones suprayectivas (sobre) de un conjunto A a un conjunto B donde:
a) $|A| = 8, |B| = 3$; *b*) $|A| = 6, |B| = 4$; *c*) $|A| = 5, |B| = 5$; *d*) $|A| = 5, |B| = 7$.

6.20 Encuentre el número de desarreglos de $X = \{1, 2, 3, \ldots, 2m\}$ tales que los m primeros elementos de cada desarreglo sean:
a) Los m primeros elementos de X; *b*) los m últimos elementos de X.

PRINCIPIO DEL PALOMAR

6.21 Encuentre el número mínimo de estudiantes que es posible admitir en una universidad, de modo que haya por lo menos 15 estudiantes de cada uno de los 50 estados de la Unión Americana.

6.22 Considere nueve puntos reticulares en el espacio. Demuestre que el punto medio de dos de los puntos también es un punto reticular.

6.23 Encuentre una subsucesión creciente de longitud máxima y una subsucesión decreciente de longitud máxima en la sucesión: 14, 2, 8, 3, 25, 15, 10, 20, 9, 4.

6.24 Considere una fila de 50 personas de estaturas distintas. Muestre una subfila de 8 personas que sea creciente o decreciente.

6.25 Proporcione un ejemplo de una sucesión de 25 enteros distintos que no tenga una subsucesión de 6 enteros que sea creciente o decreciente.

6.26 Suponga que un equipo X sostiene 19 encuentros en un periodo de dos semanas de 14 días y que sostiene por lo menos un encuentro por día. Demuestre que hay un periodo de días consecutivos en que X sostiene exactamente 8 encuentros.

6.27 Suponga que se escogen 10 puntos al azar en el interior de un triángulo equilátero T que mide 3 pulgadas por lado. Demuestre que la distancia entre dos de los puntos debe ser menor que 1 pulgada.

6.28 Sea $X = \{x_i\}$ un conjunto de n enteros positivos. Demuestre que la suma de los enteros de un subconjunto de X es divisible entre n.

6.29 Considere un grupo de 10 personas (donde cada par son conocidas o desconocidas). Demuestre que hay un subgrupo de 4 que se conocen o un subgrupo de 3 que se desconocen.

6.30 Para los números de Ramsey $R(p, q)$, demuestre que: *a*) $R(p, q) = R(q, p)$; *b*) $R(p, 1) = 1$; *c*) $R(p, 2) = p$.

RECURSIÓN

6.31 Para cada relación de recurrencia y condiciones iniciales, encuentre: *i*) la solución general; *ii*) la solución única con las condiciones iniciales dadas:

a) $a_n = 3a_{n-1} + 10a_{n-2}$; $a_0 = 5, a_1 = 11$
b) $a_n = 4a_{n-1} + 21a_{n-2}$; $a_0 = 9, a_1 = 13$
c) $a_n = 3a_{n-1} - 2a_{n-2}$; $a_0 = 5, a_1 = 8$
d) $a_n = 5a_{n-1} - 6a_{n-2}$; $a_0 = 2, a_1 = 8$
e) $a_n = 3a_{n-1} - a_{n-2}$; $a_0 = 0, a_1 = 1$
f) $a_n = 5a_{n-1} - 3a_{n-2}$; $a_0 = 0, a_1 = 1$

6.32 Repita el problema 6.31 para las siguientes relaciones de recurrencia y condiciones iniciales:

a) $a_n = 6a_{n-1}$; $a_0 = 5$ *c*) $a_n = 4a_{n-1} - 4a_{n-2}$; $a_0 = 1, a_1 = 8$
b) $a_n = 7a_{n-1}$; $a_0 = 5$ *d*) $a_n = 10a_{n-1} - 25a_{n-2}$; $a_0 = 2, a_1 = 15$

6.33 Encuentre la solución única de cada relación de recurrencia con las condiciones iniciales dadas:

a) $a_n = 10a_{n-1} - 32a_{n-2} + 32a_{n-3}$ con $a_0 = 5, a_1 = 18, a_2 = 76$
b) $a_n = 9a_{n-1} - 27a_{n-2} + 27a_{n-3}$ con $a_0 = 5, a_1 = 24, a_2 = 117$

6.34 Considere la siguiente relación de recurrencia de segundo orden y su polinomio característico $\Delta(x)$:

$$a_n = sa_{n-1} + ta_{n-2} \quad \text{y} \quad \Delta(x) = x^2 - sx - t \qquad (*)$$

a) Suponga que $p(n)$ y $q(n)$ son soluciones de $(*)$. Demuestre que, para constantes arbitrarias c_1 y c_2, $c_1 p(n) + c_2 q(n)$ también es una solución de $(*)$.
b) Suponga que r es una raíz de $\Delta(x)$. Demuestre que $a_n = r^n$ es una solución de $(*)$.
c) Suponga que r es una raíz doble de $\Delta(x)$. Demuestre que: *i*) $s = 2r$ y $t = -r^2$; *ii*) $a_n = nr^n$ también es una raíz de $(*)$.

6.35 Repita el problema 6.34*a*) y *b*) para cualquier relación de recurrencia lineal homogénea de orden k con coeficientes constantes y su polinomio característico $\Delta(x)$ que tiene la forma:

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \cdots + C_k a_{n-k} = \sum_{i=1}^{k} C_1 a_{n-1} \quad \text{y} \quad \Delta(x) = x^k - \sum_{i=1}^{k} C_1 x^{k-i}$$

Respuestas a los problemas suplementarios

6.13 *a*) 286; *b*) 646.
6.14 78.
6.15 15.
6.16 520.
6.17 $(14!)/[(3!3!2!2!2!2!)(2!4!)] = 3\,153\,150$.
6.18 *a*) *i*) $3^3 = 27$; *ii*) Pueden distribuirse como: [3, 0, 0], [2, 1, 0], o [1, 1, 1]. Por tanto $m = 1 + 3 + 1 = 5$. *b*) *i*) $3^4 = 81$; *ii*) Pueden distribuirse como: [4, 0, 0], [3, 1, 0], [2, 2, 0] o [2, 1, 1]. Por tanto, $m = 1 + 4 + 3 + 6 = 14$.
6.19 *a*) 5 796; *b*) 1 560; *c*) $5! = 120$; *d*) 0.
6.20 *a*) $(D_m)^2$; *b*) $(m!)^2$.
6.21 701.
6.22 Hay ocho tripletas de paridades: (impar, impar, impar), (impar, impar, par), ... Así, 2 de los 9 puntos tienen la misma tripleta de paridades.
6.23 2, 3, 10, 20; 25, 15, 10, 8, 4.
6.24 Use el teorema 6.7 con $n = 9$.
6.25 5, 4, 3, 2, 1, 10, 9, 8, 7, 6, . . ., 25, 24, 23, 22, 21.
6.26 (Sugerencia: vea el problema 6.9.)
6.27 (Sugerencia: separe T en 9 triángulos equiláteros que midan 1 pulgada por lado.)
6.28 Sea $s_i = x_1 + \cdots + x_i$. El resultado es verdadero si n divide alguna s_i. En caso contrario, sea r' el residuo cuando s_i se divide entre n. Dos de los rs deben ser iguales. Por ejemplo $r_p = r_q$, donde $p < q$. Entonces n divide a $s_q - s_p = x_{p+1} + \cdots + x_q$.
6.31 *a*) $a_n = c_1(5^n) + c_2(-2)^n$; $c_1 = 3, c_2 = 2$
b) $a_n = c_1(7^n) + c_2(-3)^n$; $c_1 = 4, c_2 = 5$
c) $a_n = c_1 + c_2(2^n)$; $c_1 = 2, c_2 = 3$
d) $a_n = c_1(2^n) + c_2(3^n)$; $c_1 = -2, c_2 = 4$
e) $a_n = c_1[(3 + t)/2]^n + c_2[(3 - t)/2]^n$; $c_1 = 1/t$, $c_2 = -1/t$ donde $t = \sqrt{5}$
f) $a_n = c_1[(5+s)/2]^n + c_2[(5 - s)/2]^n$; $c_1 = 1/s$, $c_2 = -1/s$ donde $= \sqrt{13}$
6.32 *a*) $a_n = c_1(6^n)$, $c_1 = 5$
b) $a_n = c_1(7^n)$, $c_1 = 5$
c) $a_n = c_1(2^n) + c_2 n(2^n)$, $c_1 = 1, c_2 = 3$
d) $a_n = c_1(5^n) + c2n(5^n)$, $c_1 = 2, c_2 = 1$
6.33 *a*) $a_n = 2(4^n) + n(4^n) + 3(2^n)$; *b*) $a_n = 5(3^n) + 2n(3^n) + n^2(3^n) = (5 + 2n + n^2)3^n$.
6.34 *b*) r es una raíz de $\Delta(x)$ de modo que $r^2 - sr - t = 0$ o $r^2 = sr+t$. Sea $a_n = r^n$. Entonces $sa_{n-1} + ta_{n-2} = sr^{n-1} + tr^{n-2} = (sr + t)r^{n-2} = r^2(r^{n-2}) = r^n = a_n$
c) *i*) r es una raíz doble de $\Delta(x)$; por tanto $\Delta(x) = (x - r)^2 = x^2 - 2rx + r^2 = x^2 - sx - t$. Así $s = 2r$ y $t = -r2$. *ii*) Sea $a_n\, nr_n$. Entonces $sa_{n-1} + ta_{n-2} = nr^n = an$.

7 Probabilidad

CAPÍTULO

7.1 INTRODUCCIÓN

La teoría de la probabilidad es un modelo matemático para analizar el fenómeno del azar o la aleatoriedad. Por ejemplo, si se lanza una moneda en forma aleatoria, el resultado puede ser cara (H) o cruz (T), pero es difícil saber cuál será el resultado en el siguiente lanzamiento. No obstante, suponga que s es el número de veces que aparece cara cuando la moneda se lanza n veces. A medida que n crece, la razón $f = s/n$, denominada *frecuencia relativa* del resultado, se vuelve más estable. Si la moneda está perfectamente balanceada, entonces se espera que el resultado sea cara aproximadamente 50% de las veces o, en otras palabras, la frecuencia relativa tiende a $\frac{1}{2}$. En forma alterna, si la moneda está perfectamente balanceada, es posible obtener al valor $\frac{1}{2}$ en forma deductiva. Es decir, cualquier lado de la moneda tiene la misma probabilidad de ocurrir que el otro; por tanto, la posibilidad de obtener una cara es 1 de 2, lo cual significa que la probabilidad de obtener cara es $\frac{1}{2}$. Aunque se desconoce el resultado específico de un lanzamiento, el comportamiento a largo plazo es determinado. Este comportamiento estable a largo plazo de los fenómenos aleatorios constituye la base de la teoría de la probabilidad.

Un modelo matemático probabilístico de fenómenos aleatorios se define al asignar "probabilidades" a todos los resultados posibles de un experimento. La confiabilidad del modelo matemático de un experimento depende de la proximidad que tengan las probabilidades asignadas con las frecuencias relativas limitantes reales. Esto origina problemas de pruebas y confiabilidad, que constituyen el tema de estudio de la estadística y que rebasan el alcance de este libro.

7.2 ESPACIO MUESTRAL Y EVENTOS

El conjunto S de todos los resultados posibles de un experimento dado se denomina *espacio muestral*. Un resultado particular, un elemento en S, se denomina *punto muestral*. Un *evento* A es un conjunto de resultados o, en otras palabras, un subconjunto del espacio muestral S. En particular, el conjunto $\{a\}$ que consta de un punto muestral $a \in S$ se denomina *evento elemental*. Además, el conjunto vacío $\varnothing$ y S mismo son subconjuntos de S y entonces $\varnothing$ y S también son eventos; algunas veces se denomina *evento imposible* o *evento nulo* a $\varnothing$.

Puesto que un evento es un conjunto, es posible combinar eventos para formar nuevos eventos al usar las diversas operaciones con conjuntos:

i) $A \cup B$ es el evento que ocurre sii A ocurre o B ocurre (o ambos).

ii) $A \cap B$ es el evento que ocurre sii A ocurre y B ocurre.

iii) A^c, el complemento de A, también se escribe $\overline{A}$ es el evento que ocurre sii no ocurre A.

Dos eventos A y B se denominan *mutuamente excluyentes* si son ajenos; es decir, si $A \cap B = \varnothing$. En otras palabras, A y B son mutuamente excluyentes sii no pueden ocurrir simultáneamente. Tres o más eventos son mutuamente excluyentes si dos de ellos son mutuamente excluyentes.

EJEMPLO 7.1

a) ***Experimento*:** Lance una moneda tres veces y observe la sucesión de caras (*H*) y cruces (*T*) que se obtiene.
El espacio muestral consta de los ocho elementos siguientes:

$$S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, T\,T\,T\}$$

Sean *A* el evento de obtener dos o más caras consecutivas y *B* el evento que todos los resultados sean iguales:

$$A = \{HHH, HHT, THH\} \quad \text{y} \quad B = \{HHH, T\,T\,T\}$$

Entonces $A \cap B = \{HHH\}$ es el evento elemental en que sólo se obtienen caras. El evento de obtener cinco caras es el conjunto vacío $\varnothing$.

b) ***Experimento*:** Lance un dado (de seis caras), mostrado en la figura 7-1*a*), y observe el número (de puntos) que aparece en la cara superior.
El espacio muestral *S* consta de los seis números posibles; es decir, $S = \{1, 2, 3, 4, 5, 6\}$. Sea *A* el evento en el que se observa un número par, *B* el evento en el que se observa un número impar y *C* el evento en el que se observa un número primo. Es decir, sea

$$A = \{2, 4, 6\}, \quad B = \{1, 3, 5\}, \quad C = \{2, 3, 5\}$$

Entonces

$A \cup C = \{2, 3, 4, 5, 6\}$ es el evento en que ocurre un número par o un número primo.
$B \cap C = \{3, 5\}$ es el evento en que ocurre un número primo impar.
$C^c = \{1, 4, 6\}$ es el evento en que no ocurre un número primo.

Observe que *A* y *B* son mutuamente excluyentes: $A \cap B = \varnothing$. En otras palabras, el que ocurran un número par y un número impar no puede ocurrir simultáneamente.

c) ***Experimento*:** Lance una moneda hasta que aparezca una cara y cuente el número de veces que se lanzó la moneda.
El espacio muestral *S* de este experimento es $S = \{1, 2, 3, \ldots\}$. Debido a que todo entero positivo es un elemento de *S*, el espacio muestral es infinito.

Observación: El espacio muestral *S* en el ejemplo 7.1*c*), como se observó, no es finito. La teoría que relaciona a dichos espacios muestrales rebasa el alcance de este texto. Por tanto, a menos que se establezca otra cosa, todos los espacios muestrales *S* que se presentan en este texto son finitos.

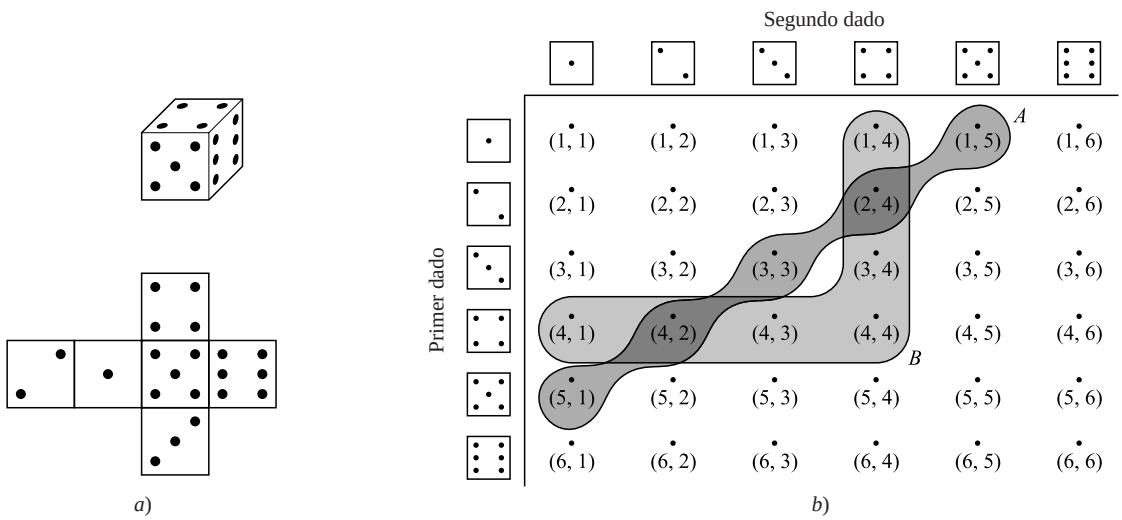


Figura 7-1

EJEMPLO 7.2 (Par de dados) Lance un par de dados y anote los números de las caras superiores.

En cada dado hay seis números posibles: 1, 2, . . . , 6. Por tanto, S consta de los pares de números de 1 a 6, de modo que $n(S) = 36$. En la figura 7-1*b*) se muestran estos 36 pares de números dispuestos de modo que los renglones corresponden al primer dado y las columnas, al segundo.

Sean A el evento cuando la suma de los dos números es 6 y B el evento cuando el mayor de los dos números sea 4. Es decir, sea

$$A = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}, \quad B = \{(1, 4), (2, 4), (3, 4), (4, 4), (4, 3), (4, 2), (4, 1)\}$$

Entonces el evento "A y B" consta de los pares de enteros cuya suma es 6 y el número más grande es 4 o, en otras palabras, la intersección de A y B. Así,

$$A \cap B = \{(2, 4), (4, 2)\}$$

En forma semejante, "A o B", que la suma sea 6 o el número más grande sea 4, la parte sombreada en la figura 7-1*b*), es la unión $A \cup B$.

EJEMPLO 7.3 (Mazo de cartas) De una baraja normal de 52 naipes, mostrada en la figura 7-2*a*) se extrae una carta.

El espacio muestral S consta de cuatro *palos*: tréboles (T), diamantes (D), corazones (C) y picas (P), y cada palo tiene 13 cartas numeradas del 2 al 10, así como una sota (J), una reina (Q), un rey (K) y un as (A). Los corazones (C) y los diamantes (D) son naipes rojos, y los picas (P) y los tréboles (T) son naipes negros. En la figura 7-2*b*) se muestran 52 puntos que representan el mazo S de la baraja en la forma evidente. Sea E el evento de una *carta con figura*; es decir, una sota (J), una reina (Q) o un rey (K), y sea F el evento de un corazón. Entonces $E \cap F = \{JH, QH, KH\}$, como aparece en el sombreado de la figura 7-2*b*).

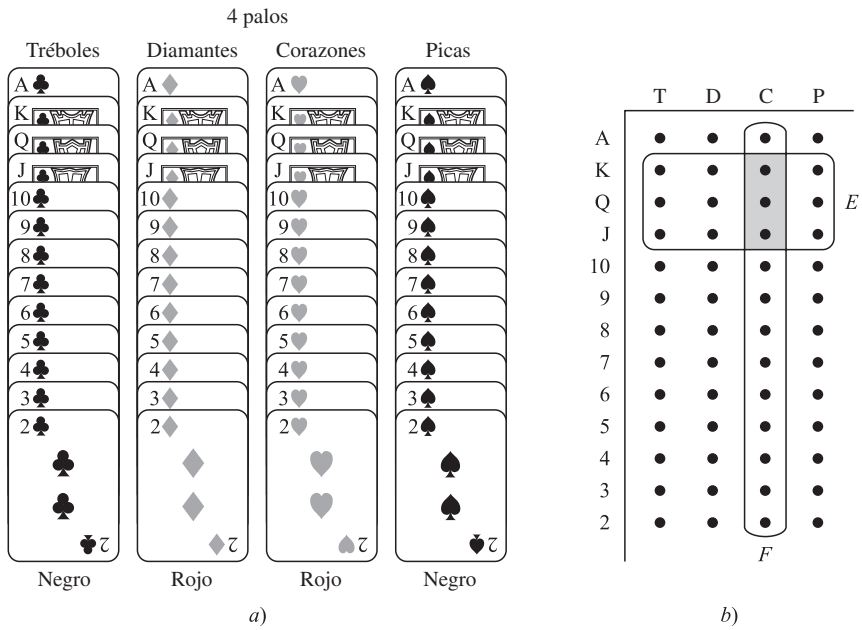


Figura 7-2

7.3 ESPACIOS DE PROBABILIDAD FINITOS

Se aplica la siguiente definición.

Definición 7.1: Sea S un espacio muestral finito; por ejemplo $S = \{a_1, a_2, \ldots, a_n\}$. Un *espacio de probabilidad finito*, o *modelo de probabilidad*, se obtiene al asignar a cada punto a_i en S un número real p_i, denominado *probabilidad* de a_i que cumple las siguientes propiedades:

i) Todo p_i es no negativo; es decir, $p_i \geq 0$.

ii) La suma de los p_i es 1; es decir, $p_1 + p_2 + \cdots + p_n = 1$.

La *probabilidad* de un evento A, escrito $P(A)$, se define entonces como la suma de las probabilidades de los puntos en A.

El conjunto unitario $\{a_i\}$ se denomina evento *elemental* y, por conveniencia en la notación, se escribe $P(a_i)$ en lugar de $P(\{a_i\})$.

EJEMPLO 7.4 (Experimento) Suponga que se lanzan tres monedas y que se registra el número de caras. [Compare este experimento con el ejemplo 7.1*a*)].

El espacio muestral es $S = \{0, 1, 2, 3\}$. Las siguientes asignaciones sobre los elementos de S definen un espacio de probabilidad:

$$P(0) = \tfrac{1}{8}, \quad P(1) = \tfrac{3}{8}, \quad P(2) = \tfrac{3}{8}, \quad P(3) = \tfrac{1}{8}$$

Es decir, cada probabilidad es no negativa y la suma de las probabilidades es 1. Sea A el evento de obtener por lo menos una cara y sea B el evento de obtener sólo caras o sólo cruces; es decir, sean $A = \{1, 2, 3\}$ y $B = \{0, 3\}$. Entonces, por definición,

$$P(A) = P(1) + P(2) + P(3) = \tfrac{3}{8} + \tfrac{3}{8} + \tfrac{1}{8} = \tfrac{7}{8} \quad \text{y} \quad P(B) = P(0) + P(3) = \tfrac{1}{8} + \tfrac{1}{8} = \tfrac{1}{4}$$

Espacios equiprobables

A menudo las características físicas de un experimento sugieren la asignación de probabilidades iguales a los diversos resultados del espacio muestral. De modo que un espacio de probabilidad finito S, donde cada punto muestral tiene la misma probabilidad, se denomina *espacio equiprobable*. En particular, si S contiene n puntos, entonces la probabilidad de cada punto es $1/n$. Además, si un evento A contiene r puntos, entonces su probabilidad es $r(1/n) = r/n$. En otras palabras, donde $n(A)$ denota el número de elementos en un conjunto A,

$$P(A) = \frac{\text{número de elementos en } A}{\text{número de elementos en } S} = \frac{n(A)}{n(S)} \quad \text{o} \quad P(A) = \frac{\text{número de resultados favorables a } A}{\text{número total de resultados posibles}}$$

Conviene señalar que la fórmula anterior para $P(A)$ sólo se aplica para a un espacio equiprobable, no es posible utilizarla en general.

La expresión *al azar* sólo se usará para un espacio equiprobable; la declaración "escoger al azar un punto de un conjunto S" significará que cualquier punto muestral en S tiene la misma probabilidad de ser escogido.

EJEMPLO 7.5 De una baraja normal de 52 naipes se selecciona una carta. Sean

$$A = \{\text{la carta es una pica}\} \quad \text{y} \quad B = \{\text{la carta es una figura}\}.$$

Se calculan P(A), P(B) y $P(A \cap B)$. Puesto que se tiene un espacio equiprobable,

$$P(A) = \frac{\text{número de picas}}{\text{número de cartas}} = \frac{13}{52} = \frac{1}{4}, \quad P(B) = \frac{\text{número de cartas con figura}}{\text{número de cartas}} = \frac{12}{52} = \frac{3}{13}$$

$$P(A \cap B) = \frac{\text{número de cartas de picas con figura}}{\text{número de cartas}} = \frac{3}{52}$$

Teoremas sobre espacios de probabilidad finitos

El siguiente teorema se concluye directamente a partir que la probabilidad de un evento es la suma de las probabilidades de sus puntos:

Teorema 7.1: La función de probabilidad P definida sobre la clase de todos los eventos en un espacio de probabilidad finito tiene las siguientes propiedades:

$[\mathbf{P}_1]$ Para todo evento A, $0 \leq P(A) \leq 1$.

$[\mathbf{P}_2]$ $P(S) = 1$.

$[\mathbf{P}_3]$ Si los eventos A y B son mutuamente excluyentes, entonces $P(A \cup B) = P(A) + P(B)$.

El siguiente teorema formaliza la intuición que si p es la probabilidad que ocurra un evento E, entonces $1 - p$ es la probabilidad que E no ocurra. (Es decir, si se acierta en el blanco $1/3$ de las veces, entonces se falla $1 - p = 2/3$ de las veces.)

Teorema 7.2: Sea A cualquier evento. Entonces $P(A^c) = 1 - P(A)$.

El siguiente teorema (que se demuestra en el problema 7.13) se concluye directamente a partir del teorema 7.1.

Teorema 7.3: Considere el conjunto vacío $\varnothing$ y dos eventos arbitrarios A y B. Entonces:

i) $P(\varnothing) = 0$.

ii) $P(A \backslash B) = P(A) - P(A \cap B)$.

iii) Si $A \subseteq B$, entonces $P(A) \leq P(B)$.

Observe que la propiedad $[\mathbf{P}_3]$ en el teorema 7.1 proporciona la probabilidad de la unión de eventos cuando los eventos son ajenos. La fórmula general (demostrada en el problema 7.14) se denomina principio de adición. Específicamente:

Teorema 7.4 (Principio de adición): Para dos eventos arbitrarios A y B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

EJEMPLO 7.6 Suponga que un estudiante es elegido al azar entre 100 estudiantes, de los cuales 30 cursan matemáticas, 20 cursan química y 10 cursan matemáticas y química. Encuentre la probabilidad p que curse matemáticas o química.

Sean $M = \{\text{estudiantes que cursan matemáticas}\}$ y $C = \{\text{estudiantes que cursan química}\}$. Puesto que el espacio es equiprobable,

$$P(M) = \frac{30}{100} = \frac{3}{10}, \quad P(C) = \frac{20}{100} = \frac{1}{5}, \quad P(M \text{ y } C) = P(M \cap C) = \frac{10}{100} = \frac{1}{10}$$

Entonces, por el principio de adición (teorema 7.4),

$$p = P(M \text{ o } C) = P(M \cup C) = P(M) + P(C) - P(M \cap C) = \frac{3}{10} + \frac{1}{5} - \frac{1}{10} = \frac{2}{5}$$

7.4 PROBABILIDAD CONDICIONAL

Suponga que E es un evento en un espacio muestral S con $P(E) > 0$. La probabilidad de que un evento A ocurra una vez que ha ocurrido E o, específicamente, *la probabilidad condicional de A dado E*, que se escribe $P(A|E)$ se define como sigue:

$$P(A|E) = \frac{P(A \cap E)}{P(E)}$$

Como se muestra en el diagrama de Venn en la figura 7-3, $P(A|E)$ mide, en cierto sentido, la probabilidad relativa de A con respecto al espacio reducido E.

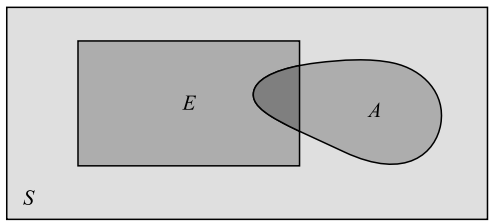


Figura 7-3

Suponga que S es un espacio equiprobable, y que $n(A)$ denota el número de elementos en A. Entonces:

$$P(A \cap E) = \frac{n(A \cap E)}{n(S)}, \quad P(E) = \frac{n(E)}{n(S)}, \quad \text{y así} \quad P(A|E) = \frac{P(A \cap E)}{P(E)} = \frac{n(A \cap E)}{n(E)}$$

Este resultado se plantea formalmente.

Teorema 7.5: Suponga que S es un espacio equiprobable y que A y E son eventos. Entonces

$$P(A|E) = \frac{\text{número de elementos en } A \cap E}{\text{número de elementos en } E} = \frac{n(A \cap E)}{n(E)}$$

EJEMPLO 7.7

a) Se lanza un par de dados normales. El espacio muestral S consta de los 36 pares ordenados (a, b), donde a y b pueden ser cualquiera de los enteros del 1 al 6. (Vea el ejemplo 7.2.). Por tanto, la probabilidad de cualquier punto es $\frac{1}{36}$. Encuentre la probabilidad de que uno de los dados sea 2 si la suma es 6. Es decir, encuentre $P(A|E)$ donde:

$$E = \{\text{la suma es 6}\} \quad \text{y} \quad A = \{\text{el 2 aparece por lo menos en un dado}\}$$

Así, E consta de 5 elementos y $A \cap E$ consta de dos elementos; a saber,

$$E = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\} \quad \text{y} \quad A \cap \text{E} = \{(2, 4), (4, 2)\}$$

Por el teorema 7.5, $P(A|E) = 2/5$.

Por otra parte, A en sí consta de 11 elementos; es decir,

$$A = \{(2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (1, 2), (3, 2), (4, 2), (5, 2), (6, 2)\}$$

Puesto que S consta de 36 elementos, $P(A) = 11/36$.

b) Una pareja tiene dos hijos; el espacio muestral es $S = \{vv, vn, nv, nn\}$ ($v =$ varón; $n =$ niña) con probabilidad $\frac{1}{4}$ para cada punto. Encuentre la probabilidad p que ambos hijos sean varones si se sabe que: *i*) por lo menos uno de los hijos es varón; *ii*) que el hijo mayor es varón.

i) Aquí el espacio reducido consta de tres elementos: $\{vv, vn, nv\}$; entonces, $p = \frac{1}{3}$.

ii) Aquí el espacio reducido consta sólo de dos elementos: $\{vv, vn\}$; entonces, $p = \frac{1}{2}$.

Teorema de la multiplicación para la probabilidad condicional

Suponga que A y B son eventos en un espacio muestral S con $P(A) > 0$. Por definición de probabilidad condicional,

$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

Al multiplicar ambos miembros por $P(A)$ se obtiene el siguiente resultado útil:

Teorema 7.6 (Teorema de la multiplicación para la probabilidad condicional):

$$P(A \cap B) = P(A)P(B|A)$$

Este teorema proporciona una fórmula para encontrar la probabilidad de ocurrencia de ambos eventos A y B. Resulta fácil extenderlo a tres o más eventos $A_1, A_2, \ldots A_m$; es decir,

$$P(A_1 \cap A_2 \cap \cdots A_m) = P(A_1) \cdot P(A_2|A_1) \cdots P(A_m|A_1 \cap A_2 \cap \cdots \cap A_{m-1})$$

EJEMPLO 7.8 Un lote contiene 12 artículos, de los cuales 4 son defectuosos. Del lote se extraen al azar tres artículos, uno después del otro. Encuentre la probabilidad p de que los tres artículos no sean defectuosos.

La probabilidad de que el primer artículo no sea defectuoso es $\frac{8}{12}$, puesto que 8 de los 12 artículos no son defectuosos. Si el primer artículo no es defectuoso, entonces la probabilidad de que el siguiente artículo no sea defectuoso es $\frac{7}{11}$, ya que sólo 7 de los 11 artículos restantes no son defectuosos. Si los dos primeros artículos no son defectuosos, entonces la probabilidad que el último artículo no sea defectuoso es $\frac{6}{10}$, ya que ahora sólo 6 de los 10 artículos restantes no son defectuosos. Así, por el teorema de la multiplicación,

$$p = \frac{8}{12} \cdot \frac{7}{11} \cdot \frac{6}{10} = \frac{14}{55} \approx 0.25$$

7.5 EVENTOS INDEPENDIENTES

Se dice que los eventos A y B en un espacio de probabilidad S son *independientes* si la ocurrencia de uno de ellos no afecta la ocurrencia del otro. De forma más precisa, B es independiente de A si $P(B)$ es igual a $P(B|A)$. Luego, al sustituir $P(B)$ por $P(B|A)$ en el teorema de la multiplicación $P(A \cap B) = P(A)P(B|A)$ se obtiene

$$P(A \cap B) = P(A)P(B).$$

Las ecuaciones anteriores se utilizan formalmente como la definición de independencia.

Definición 7.2: Los eventos A y B son *independientes* si $P(A \cap B) = P(A)P(B)$; en caso contrario, son *dependientes*.

Conviene señalar que la independencia es una relación simétrica. En particular, la ecuación

$$P(A \cap B) = P(A)P(B) \quad \text{implica ambos} \quad P(B|A) = P(B) \quad \text{y} \quad P(A|B) = P(A)$$

EJEMPLO 7.9 Una moneda normal se lanza tres veces, lo que da el espacio equiprobable

$$S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}$$

Considere los eventos:

$$A = \{\text{el primer lanzamiento es cara}\} = \{HHH, HHT, HTH, HTT\}$$
$$B = \{\text{el segundo lanzamiento es cara}\} = \{HHH, HHT, THH, THT\}$$
$$C = \{\text{se obtienen exactamente dos caras consecutivas}\} = \{HHT, THH\}$$

Resulta evidente que A y B son eventos independientes: este hecho se comprueba a continuación. Por otra parte, la relación entre A y C y entre B y C no es evidente. Se afirma que A y B son eventos independientes, en cambio B y C son dependientes. Se tiene:

$$P(A) = \tfrac{4}{8} = \tfrac{1}{2}, \quad P(B) = \tfrac{4}{8} = \tfrac{1}{2}, \quad P(C) = \tfrac{2}{8} = \tfrac{1}{4}$$

También,

$$P(A \cap B) = P(\{HHH, HHT\}) = \tfrac{1}{4}, \quad P(A \cap C) = P(\{HHT\}) = \tfrac{1}{8}, \quad P(B \cap C) = P(\{HHT, THH\}) = \tfrac{1}{4}$$

En consecuencia,

$$\begin{aligned} P(A)P(B) &= \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4} = P(A \cap B), \quad \text{y así } A \text{ y } B \text{ son independientes} \\ P(A)P(C) &= \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} = P(A \cap C), \quad \text{y así } A \text{ y } C \text{ son independientes} \\ P(B)P(C) &= \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} \neq P(B \cap C), \quad \text{y así } B \text{ y } C \text{ son dependientes} \end{aligned}$$

A menudo, se postulará que dos eventos son independientes, o el experimento en sí implicará que dos eventos son independientes.

EJEMPLO 7.10 La probabilidad que A acierte en un blanco es $\frac{1}{4}$, y la probabilidad que B acierte en el blanco es $\frac{2}{5}$. Ambos disparan al blanco. Encuentre la probabilidad que por lo menos uno de ellos acierte en el blanco; es decir, que A o B (o ambos) den en el blanco.

Se cuenta con que $P(A) = \frac{1}{2}$ y $P(B) = \frac{2}{5}$, y se busca $P(A \cup B)$. Además, la probabilidad que A o B dé en el blanco no afecta que el otro lo haga; es decir, el evento que A acierte en el blanco es independiente del evento que B dé en el blanco; es decir, $P(A \cap B) = P(A)\,P(B)$. Así,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A)P(B) = \tfrac{1}{4} + \tfrac{2}{5} - \left(\tfrac{1}{4}\right)\left(\tfrac{2}{5}\right) = \tfrac{11}{20}$$

7.6 ENSAYOS INDEPENDIENTES REPETIDOS, DISTRIBUCIÓN BINOMIAL

Previamente se han analizado espacios de probabilidad asociados con un experimento repetido un número finito de veces, como lanzar tres veces una moneda. Este concepto de repetición se formaliza como sigue:

Definición 7.3: Sea S un espacio de probabilidad finito. Por el espacio de *n ensayos independientes repetidos* se entiende el espacio de probabilidad S_n que consta de las *n-adas* ordenadas de elementos de S, con la probabilidad de una *n-ada* definida como el producto de las probabilidades de sus componentes:

$$P((s_1, s_2, \ldots, s_n)) = P(s_1)P(s_2)\ldots P(s_n)$$

EJEMPLO 7.11 Siempre que tres caballos a, b y c corren juntos, sus probabilidades respectivas de ganar son $\frac{1}{2}$, $\frac{1}{3}$ y $\frac{1}{6}$. En otras palabras, $S = \{a, b, c\}$ con $P(a) = \frac{1}{2}$, $P(b) = \frac{1}{3}$ y $P(c) = \frac{1}{6}$. Si los caballos corren dos veces, entonces el espacio muestral de los dos ensayos repetidos es

$$S_2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$$

Por conveniencia en la notación, se ha escrito ac en lugar del par ordenado (a, c). La probabilidad de cada punto en S_2 es

$$\begin{aligned} P(aa) = P(a)P(a) &= \tfrac{1}{2}\left(\tfrac{1}{2}\right) = \tfrac{1}{4}, \quad P(ba) = \tfrac{1}{6}, \quad P(ca) = \tfrac{1}{12} \\ P(ab) = P(a)P(b) &= \tfrac{1}{2}\left(\tfrac{1}{3}\right) = \tfrac{1}{6}, \quad P(bb) = \tfrac{1}{9}, \quad P(cb) = \tfrac{1}{18} \\ P(ac) = P(a)P(c) &= \tfrac{1}{2}\left(\tfrac{1}{6}\right) = \tfrac{1}{12}, \quad P(bc) = \tfrac{1}{18}, \quad P(cc) = \tfrac{1}{36} \end{aligned}$$

Por tanto, la probabilidad que c gane la primera carrera y que a gane la segunda carrera es $P(ca) = \frac{1}{12}$.

Ensayos repetidos con dos resultados, ensayos de Bernoulli, experimento binomial

Ahora se considerará un experimento con sólo dos resultados. Ensayos repetidos independientes de tal experimento se denominan ensayos de Bernoulli, en honor del matemático suizo Jacob Bernoulli (1654-1705). La expresión ensayos independientes significa que el resultado de cualquier ensayo no depende de los resultados previos (como lanzar una moneda). Uno de los resultados se denomina *éxito* y el otro, *fracaso*.

Sea p la probabilidad de éxito en un ensayo de Bernoulli, de modo que $q = 1 - p$ es la probabilidad de fracaso. Un *experimento binomial* consta de un número fijo de ensayos de Bernoulli. Un experimento binomial con n ensayos y probabilidad p de éxito se denota por

$$B(n, p)$$

A menudo se tiene interés en el número de éxitos en un experimento binomial y no en el orden en que ocurren. Entonces se aplica el siguiente teorema (que se demuestra en el problema 7.27). Observe que en el teorema se usa el siguiente coeficiente binomial, que se analizó con detalle en el capítulo 5:

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)(k-2)\dots 3\cdot 2\cdot 1} = \frac{n!}{k!(n-k)!}$$

Teorema 7.7: La probabilidad de obtener exactamente k éxitos en un experimento binomial $B(n, p)$ está dada por

$$P(k) = P(k \text{ éxitos}) = \binom{n}{k} p^k q^{n-k}$$

La probabilidad de uno o más éxitos es $1 - q^n$.

EJEMPLO 7.12 Una moneda normal se lanza 6 veces; un éxito se denomina cara. Por tanto, éste es un experimento binomial con $n = 6$ y $p = q = \frac{1}{2}$.

a) La probabilidad de obtener exactamente dos caras (es decir, $k = 2$) es

$$P(2) = \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{15}{64} \approx 0.23$$

b) La probabilidad de obtener por lo menos cuatro caras (es decir, $k = 4$, 5 o 6) es

$$\begin{aligned} P(4) + P(5) + P(6) &= \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{6}\left(\frac{1}{2}\right)^6 \\ &= \frac{15}{64} + \frac{6}{64} + \frac{1}{64} = \frac{11}{32} \approx 0.34 \end{aligned}$$

c) La probabilidad de no obtener caras (es decir, de obtener sólo fracasos) es $q^6 = \left(\frac{1}{2}\right)^6 = \frac{1}{64}$, de modo que la probabilidad de obtener una o más caras es $1 - q^n = 1 - \frac{1}{64} = \frac{63}{64} \approx 0.94$.

Observación: La función $P(k)$ para $k = 0, 1, 2, \dots, n$, para un experimento binomial $B(n, p)$ se denomina *distribución binomial* porque corresponde a los términos sucesivos del desarrollo del binomio:

$$(q + p)^n = q^n + \binom{n}{1} q^{n-1}p + \binom{n}{2} q^{n-2}p^2 + \cdots + p^n$$

El uso del término *distribución* se explicará después en este capítulo.

7.7 VARIABLES ALEATORIAS

Sea S un espacio muestral de un experimento. Como ya se observó, el resultado del experimento, o los puntos en S, no necesariamente son números. Por ejemplo, al lanzar una moneda los resultados son H (cara) o T (cruz), y al lanzar un par de dados los resultados son pares de enteros positivos. Sin embargo, a menudo es necesario asignar un número específico a cada resultado del experimento. Por ejemplo, al lanzar una moneda, puede ser conveniente asignar 1 a H y 0 a T; o al lanzar un par de dados, asignar la suma de los dos enteros al resultado. Una asignación así de valores numéricos se denomina *variable aleatoria*. En forma más general, se tiene la siguiente definición.

Definición 7.4: Una *variable aleatoria* X es una regla que asigna un valor numérico a cada resultado en un espacio muestral S.

R_X denota el conjunto de números asignados por una variable aleatoria X, y R_X se denomina *espacio rango*.

Observación: En términos más formales, X es una función de S en los números reales $\mathbf{R}$, y R_X es el rango de X. También, para algunos espacios muestrales infinitos S, no todas las funciones de S en $\mathbf{R}$ se consideran variables aleatorias. Sin embargo, los espacios muestrales en este texto son finitos, y toda función real definida sobre un espacio muestral finito es una variable aleatoria.

EJEMPLO 7.13 Se lanzan un par de dados normales. (Vea el ejemplo 7.2.). El espacio muestral S consta de los 36 pares ordenados (a, b), donde a y b pueden ser cualquiera de los enteros del 1 al 6.

Sea X la suma de los números en cada punto en S; entonces X es una variable aleatoria con espacio rango

$$R_X = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

Sea Y el máximo de los dos números en cada punto en S; entonces Y es una variable aleatoria con espacio rango

$$R_Y = \{1, 2, 3, 4, 5, 6\}$$

Sumas y productos de variables aleatorias: notación

Suponga que X y Y son variables aleatorias sobre el mismo espacio muestral S. Entonces $X + Y$, kX y XY son funciones sobre S definidas como sigue (donde $s \in S$):

$$(X + Y)(s) = X(s) + Y(s), \quad (kX)(s) = kX(s), \quad (XY)(s) = X(s)Y(s)$$

En forma más general, para cualquier función polinomial o exponencial $h(x, y, \ldots, z)$, $h(X, Y, \ldots, Z)$ se define como la función sobre S dada por

$$[h(X, Y, \ldots, Z)](s) = h[X(s), Y(s), \ldots, Z(s)]$$

Puede demostrarse que éstas también son variables aleatorias. (Esto es trivial cuando todo subconjunto de S es un evento).

La notación abreviada $P(X = a)$ y $P(a \leq X \leq b)$ se usarán, respectivamente, para indicar la probabilidad que "X mapea sobre a" y "X mapea sobre el intervalo $[a, b]$". Es decir, para $s \in S$:

$$P(X = a) \equiv P(\{s \mid X(s) = a\}) \quad \text{y} \quad P(a \leq X \leq b) \equiv P(\{s \mid a \leq X(s) \leq b\})$$

Significados semejantes se asignan a $P(X \leq a)$, $P(X = a, Y = b)$, $P(a \leq X \leq b, c \leq Y \leq d)$, y así sucesivamente.

Distribución de probabilidad de una variable aleatoria

Sea X una variable aleatoria sobre un espacio muestral finito S con espacio rango $Rx = \{x_1, x_2, \ldots, x_t\}$. Entonces, X induce una función f que asigna probabilidades p_k a los puntos x_k en R_x como sigue:

$$f(x_k) = p_k = P(X = x_k) = \text{suma de probabilidades de los puntos en } S \text{ cuya imagen es } x_k.$$

El conjunto de pares ordenados $(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))$ se denomina *distribución* de la variable aleatoria X; suele proporcionarse mediante una tabla como en la figura 7-4. Esta función f posee las dos propiedades siguientes:

$$i)\ f(x_k) \geq 0 \quad \text{y} \quad ii)\ \sum_k f(x_k) = 1$$

Por tanto, R_X con las asignaciones de probabilidades anteriores es un espacio de probabilidad. (Algunas veces, para denotar la distribución de X, se usará la notación de pares $[x_k, p_k]$ en lugar de la notación funcional $[x, f(x)]$.)

Resultado x	x_1	x_2	x_3	$\cdots$	x_t
Probabilidad f(x)	$f(x_1)$	$f(x_2)$	$f(x_3)$	$\cdots$	$f(x_t)$

Figura 7-4 Distribución *f* de una variable aleatoria *X*.

Cuando S es un espacio equiprobable, resulta fácil obtener la distribución de una variable aleatoria a partir del siguiente resultado.

Teorema 7.8: Sea S un espacio equiprobable, y sea f la distribución de una variable aleatoria X sobre S con el espacio rango $R_X = \{x_1, x_2, \ldots, x_t\}$. Entonces

$$p_i = f(x_i) = \frac{\text{número de puntos en } S \text{ cuya imagen es } x_i}{\text{número de puntos en } S}$$

EJEMPLO 7.14 Sea X la variable aleatoria del ejemplo 7.13 que asigna la suma al resultado del lanzamiento de un par de dados. Observe que $n(S) = 36$ y que $R_x = \{2, 3, \ldots, 12\}$. Al aplicar el teorema 7.8, se obtiene la distribución f de X:

$f(2) = 1/36$, ya que hay un resultado (1, 1) cuya suma es 2.
$f(3) = 2/36$, ya que hay dos resultados (1, 2) y (2, 1) cuya suma es 3.
$f(4) = 3/36$, ya que hay tres resultados (1, 3), (2, 2) y (3, 1) cuya suma es 4.

En forma semejante, $f(5) = 4/36$, $f(6) = 5/36, \ldots, f(12) = 1/36$. Así, se tiene como distribución de X:

x	2	3	4	5	6	7	8	9	10	11	12
$f(x)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Esperanza de una variable aleatoria

Sea X una variable aleatoria sobre un espacio de probabilidad $S = \{s_1, s_2, \ldots, s_m\}$. Entonces la *media* o *esperanza* de X se denota y define como:

$$\mu = E(X) = X(s_1)P(s_1) + X(s_2)P(sa_2) + \cdots + X(s_m)P(s_m) = \sum X(s_k)P(s_k)$$

En particular, si X está dada por la distribución f en la figura 7-4, entonces la esperanza de X es:

$$\mu = E(X) = x_1 f(x_1) + x_2 f(x_2) + \cdots + x_t f(x_t) = \sum x_k f(x_k)$$

De manera alterna, cuando se usa la notación $[x_k, p_k]$ en lugar de $[x_k, f(x_k)]$,

$$\mu = E(X) = x_1 p_1 + x_2 p_2 + \cdots + x_t p_t = \sum x_i p_i$$

(Por conveniencia en la notación, se han omitido los límites en el símbolo de sumatoria Σ.)

EJEMPLO 7.15

a) Suponga que una moneda normal se lanza seis veces. El número de veces que puede ocurrir cara, con sus probabilidades respectivas es:

x_i	0	1	2	3	4	5	6
p_1	1/64	6/64	15/64	20/64	15/64	6/64	1/64

Entonces la media o esperanza (o número esperado de caras) es:

$$\mu = E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{6}{64}\right) + 2\left(\tfrac{15}{64}\right) + 3\left(\tfrac{20}{64}\right) + 4\left(\tfrac{15}{64}\right) + 5\left(\tfrac{6}{64}\right) + 6\left(\tfrac{1}{64}\right) = 3$$

(Esto coincide con la intuición de que la mitad de los resultados será cara.)

b) Tres caballos *a*, *b* y *c* compiten en una carrera; suponga que sus probabilidades de triunfo respectivas son $\frac{1}{2}$, $\frac{1}{3}$ y $\frac{1}{6}$. Sea *X* la función de rendimiento para el caballo triunfador, y suponga que *X* paga \$2, \$6 o \$9, según sea *a*, *b* o *c* el ganador de la carrera. El rendimiento esperado para la carrera es

$$\begin{aligned} E(X) &= X(a)P(a) + X(b)P(b) + X(c)P(c) \\ &= 2\left(\tfrac{1}{2}\right) + 6\left(\tfrac{1}{3}\right) + 9\left(\tfrac{1}{6}\right) = 4.5 \end{aligned}$$

Varianza y desviación estándar de una variable aleatoria

Sea *X* una variable aleatoria con media μ y distribución *f* como en la figura 7-4. Entonces la *varianza* de *X*, denotada por *Var*(*X*), se define como:

$$Var(X) = (x_1 - \mu)^2 f(x_1) + (x_2 - \mu)^2 f(x_2) + \cdots + (x_t - \mu)^2 f(x_t) = \Sigma(x_k - \mu)^2 f(x_k) = E((X - \mu)^2)$$

De manera alterna, cuando se usa la notación $[x_k, p_k]$ en lugar de $[x_k, f(x_k)]$,

$$Var(X) = (x_1 - \mu)^2 p_1 + (x_2 - \mu)^2 p_2 + \cdots + (x_t - \mu)^2 p_t = \Sigma(x_k - \mu)^2 p_k = E((X - \mu)^2)$$

La *desviación estándar* de *X*, que se denota σ_x o simplemente σ, es la raíz cuadrada no negativa de *Var*(*X*):

$$\sigma_x = \sqrt{Var(X)}$$

En consecuencia, $Var(X) = {\sigma_x}^2$. Tanto *Var*(*X*) como ${\sigma_x}^2$ o simplemente σ^2 se usan para denotar la varianza de *X*.

Las fórmulas siguientes suelen ser más convenientes para calcular *Var*(*X*):

$$Var(X) = {x_1}^2 f(x_1) + {x_2}^2 f(x_2) + \cdots + {x_t}^2 f(x_t) - \mu^2 = \left[\sum {x_k}^2 f(x_k)\right] - \mu^2 = E(X^2) - \mu^2$$

o

$$Var(X) = {x_1}^2 p_1 + {x_2}^2 p_2 + \cdots + {x_t}^2 p_t - \mu^2 = \left[\sum x_k^2 p_k\right] - \mu^2 = E(X^2) - \mu^2$$

EJEMPLO 7.16 Sea *X* el número de veces que ocurre cara cuando una moneda normal se lanza seis veces. La distribución de *X* aparece en el ejemplo 7.15*a*), donde se calculó su media $\mu = 3$. La varianza de *X* se calcula como sigue:

$$Var(X) = (0-3)^2\tfrac{1}{64} + (1-3)^2\tfrac{6}{64} + (2-3)^2\tfrac{15}{64} + \cdots + (6-3)\tfrac{1}{64} = 1.5$$

De manera alterna:

$$Var(X) = 0^2\tfrac{1}{64} + 1^2\tfrac{6}{64} + 2^2\tfrac{15}{64} + 3^2\tfrac{20}{64} + 4^2\tfrac{15}{64} + 5^2\tfrac{6}{64} + 6^2\tfrac{1}{64} - 3^2 = 1.5$$

Por tanto, la desviación estándar es $\sigma = \sqrt{1.5} \approx 1.225$ (caras).

Distribución binomial

Considere un experimento binomial $B(n, p)$. Es decir, $B(n, p)$ consta de n ensayos independientes repetidos con dos resultados: éxito o fracaso, y p es la probabilidad de éxito (y $q = (1 - p)$ es la probabilidad de fracaso). El número X de k éxitos es una variable aleatoria cuya distribución se muestra en la figura 7-5.

Número de éxitos k	0	1	2	…	n
Probabilidad $P(k)$	q^n	$\binom{n}{1}q^{n-1}p$	$\binom{n}{2}q^{n-1}p^2$	…	p^n

Figura 7-5

Se aplica el siguiente teorema.

Teorema 7.9: Sonsidere la distribución binomial $B(n, p)$. Entonces:

i) Valor esperado $E(X) = \mu = np$.
ii) Varianza $Var(X) = \sigma^2 = npq$.
iii) Desviación estándar $\sigma = \sqrt{npq}$.

EJEMPLO 7.17

a) La probabilidad de que una persona acierte en el blanco es $p = 1/5$. La persona dispara 100 veces. Encuentre el número esperado μ de veces que la persona acertará en el blanco, así como la desviación estándar σ.

Aquí $p = \frac{1}{5}$, así que $q = \frac{4}{5}$. Por tanto,

$$\mu = np = 100 \cdot \frac{1}{5} = 20 \quad \text{y} \quad \sigma = \sqrt{npq} = \sqrt{100 \cdot \frac{1}{5} \cdot \frac{4}{5}} = 4$$

b) Encuentre el número esperado $E(X)$ de respuestas correctas que se obtienen al adivinar en una prueba de cinco reactivos falso-verdadero. Aquí $p = \frac{1}{2}$. Por tanto, $E(X) = np = 5 \cdot \frac{1}{2} = 2.5$.

7.8 DESIGUALDAD DE CHEBYSHEV, LEY DE LOS GRANDES NÚMEROS

La desviación estándar σ de una variable aleatoria X mide la dispersión ponderada de los valores de X con respecto a la media μ. Así, para σ más pequeña, es de esperar que X esté más próxima a μ. Un planteamiento más preciso de esta esperanza está dado por la siguiente desigualdad, denominada de Chebyshev en honor del matemático ruso P.L. Chebyshev (1821-1894).

Teorema 7.10 (Desigualdad de Chebyshev): Sea X una variable aleatoria con media μ y desviación estándar σ. Entonces para cualquier número positivo arbitrario k, la probabilidad que un valor de X esté en el intervalo $[\mu - k\sigma, \mu + k\sigma]$ es al menos $1 - 1/k^2$. Es decir,

$$P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \frac{1}{k^2}$$

EJEMPLO 7.18 Suponga que X es una variable aleatoria con media $\mu = 75$ y desviación estándar $\sigma = 5$. ¿Qué conclusión acerca de X puede obtenerse a partir de la desigualdad de Chebyshev para $k = 2$ y $k = 3$?

Al hacer $k = 2$, se obtiene:

$$\mu - k\sigma = 75 - 2(5) = 65 \quad \text{y} \quad \mu + k\sigma = 75 + 2(5) = 85$$

Así, puede concluirse que la probabilidad que un valor de X esté entre 65 y 85 es al menos $1 - (1/2)^2 = 3/4$; es decir:

$$P(65 \leq X \leq 85) \geq 3/4$$

En forma semejante, al hacer $k = 3$ puede concluirse que la probabilidad que un valor de X esté entre 60 y 90 es al menos $1 - (1/3)^2 = 8/9$.

Media muestral y ley de los grandes números

Considere un número finito de variables aleatorias $X, Y, \ldots, Z$ sobre un espacio muestral S. Estas variables son *independientes* si, para valores arbitrarios $x_i, y_j, \ldots, z_k$,

$$P(X = x_i, Y = y_j, \ldots, Z = z_k) \equiv P(X = x_i)P(Y = y_j) \ldots P(Z = z_k)$$

En particular, X y Y son independientes si

$$P(X = x_i, Y = y_j) \equiv P(X = x_i)P(Y = y_j)$$

Ahora, sea X una variable aleatoria con media μ. Es posible considerar el resultado numérico de cada uno de n ensayos independientes como una variable aleatoria con la misma distribución que X. La variable aleatoria correspondiente al i-ésimo resultado se denotará por X_i ($i = 1, 2, \ldots, n$). (Se observa que las X_i son independientes con la misma distribución que X.) El valor promedio de todos los n resultados también es una variable aleatoria que se denota por $\overline{X_n}$ y se denomina *media muestral*. Es decir:

$$\overline{X_n} = \frac{X_1 + X_2 + \cdots + X_n}{n}$$

La ley de los grandes números establece que conforme n crece, el valor de la media muestral $\overline{X_n}$ tiende al valor de la media μ. A saber:

Teorema 7.11 (Ley de los grandes números): para cualquier número positivo α, no importa cuán pequeño sea, la probabilidad que la media muestral $\overline{X_n}$ tenga un valor en el intervalo $[\mu - \alpha, \mu + \alpha]$ se aproxima a 1 cuando n tiende a infinito. Es decir:

$$P([\mu - \alpha \leq X \leq \mu + \alpha]) \to 1 \quad \text{cuando} \quad n \to \infty.$$

EJEMPLO 7.19 Suponga que un dado se lanza cinco veces, con los siguientes resultados:

$$x_1 = 3, \quad x_2 = 4, \quad x_3 = 6, \quad x_4 = 1, \quad x_5 = 4$$

Entonces el valor correspondiente $\bar{x}$ de la media muestral $\overline{X_5}$ es:

$$\bar{x} = \frac{3 + 4 + 6 + 1 + 4}{5} = 3.6$$

Para un dado normal, la media $\mu = 3.5$. La ley de los grandes números indica que, a medida que n crece, hay una mayor probabilidad que $\overline{X_n}$ esté más próxima a 3.5.

PROBLEMAS RESUELTOS

ESPACIOS MUESTRALES Y EVENTOS

7.1 Se lanzan simultáneamente un dado y una moneda. Sea S el espacio muestral que consta de los 12 elementos:

$$S = \{H1, H2, H3, H4, H5, H6, T1, T2, T3, T4, T5, T6\}$$

a) Exprese explícitamente los siguientes eventos:

$A = \{\text{cara y un número par}\}$, $B = \{\text{un número primo}\}$, $C = \{\text{cruz y un número impar}\}$

b) Exprese explícitamente los eventos: *i*) ocurre A o B; *ii*) ocurren B y C; *iii*) sólo ocurre B.

c) ¿Qué par de eventos, A, B y C son mutuamente excluyentes?

a) Los elementos de A son los elementos de S que constan de una H (cara) y un número par:

$$A = \{H2, H4, H6\}$$

Los elementos de B son los puntos en S cuya segunda componente es un número primo (2, 3 o 5):

$$B = \{H2, H3, H5, T2, T3, T5\}$$

Los elementos de C son los puntos en S que constan de una T (cruz) y un número impar: $C = \{T1, T3, T5\}$.

b) *i*) $A \cup B = \{H2, H4, H6, H3, H5, T2, T3, T5\}$

ii) $B \cap C = \{T3, T5\}$

iii) $B \cap A^c \cap C^c = \{H3, H5, T2\}$

c) A y C son mutuamente excluyentes, puesto que $A \cap C = \varnothing$.

7.2 Se lanza un par de dados. (Vea el ejemplo 7.2). Encuentre el número de elementos en cada evento:

a) $A = \{\text{dos números son iguales}\}$

b) $B = \{\text{la suma es 10 o mayor}\}$

c) $C = \{5 \text{ aparece en el primer dado}\}$

d) $D = \{5 \text{ aparece por lo menos en un dado}\}$

Usar la figura 7-1*b*) como ayuda para contar el número de elementos en el evento.

a) $A = \{(1, 1), (2, 2), \ldots, (6, 6)\}$, de modo que $n(A) = 6$.

b) $B = \{(6, 4), (5, 5), (4, 6), (6, 5), (5, 6), (6, 6)\}$, de modo que $n(B) = 6$.

c) $C = \{(5, 1), (5, 2), \ldots, (5, 6)\}$, de modo que $n(C) = 6$.

d) Hay seis pares con 5 como primer elemento, y seis pares con 5 como segundo elemento. No obstante, (5, 5) aparece en ambos sitios. Por tanto

$$n(D) = 6 + 6 - 1 = 11$$

De manera alterna, se cuentan los pares en la figura 7-1*b*) que están en D para obtener $n(D) = 11$.

ESPACIOS EQUIPROBABLES FINITOS

7.3 Determine la probabilidad p de cada evento:

a) Al lanzar una vez un dado normal, obtener un número par;

b) Al lanzar una vez tres monedas al mismo tiempo, obtener una o más caras;

c) Obtener una canica roja al extraer al azar una canica de una caja que contiene cuatro canicas blancas, tres canicas rojas y cinco canicas azules.

Cada espacio muestral S es un espacio equiprobable. Así, para cada evento S, se usa:

$$P(E) = \frac{\text{número de elementos en } E}{\text{número de elementos en } S} = \frac{n(E)}{n(S)}$$

a) El evento puede ocurrir en tres formas (2, 4 o 6) de los 6 casos; por tanto, $p = \frac{3}{6} = \frac{1}{2}$.

b) Hay 8 casos:

$$HHH, HHT, HTH, HTT, THH, THT, TTH, TTT$$

Sólo el último caso no es favorable; así, $p = 7/8$.

c) Hay $4 + 3 + 5 = 12$ canicas, de las cuales tres son rojas; por tanto, $p = \frac{3}{12} = \frac{1}{4}$.

7.4 De una baraja normal con 52 naipes se extrae una carta. (Vea la figura 7-2.) Encuentre la probabilidad p que la carta sea:

a) una carta con figura (sota, reina o rey);
b) un corazón;
c) una carta con figura y un corazón;
d) una carta con figura o un corazón.

Aquí, $n(S) = 52$.

a) Hay $4(3) = 12$ cartas con figura; por tanto, $p = \dfrac{12}{52} = \dfrac{3}{13}$.

b) Hay 13 corazones; así, $p = \dfrac{13}{52} = \dfrac{1}{4}$.

c) Hay 3 cartas con figura que son corazones; por tanto, $p = \dfrac{3}{52}$.

d) Si se hace $F = \{\text{cartas con figura}\}$ y $H = \{\text{corazones}\}$, se tiene

$$n(F \cup H) = n(F) + n(H) - n(F \cap H) = 12 + 13 - 3 = 22$$

Por tanto, $p = \frac{22}{52} = \frac{11}{26}$.

7.5 De una baraja normal con 52 naipes se extraen al azar dos cartas. Encuentre la probabilidad p de que:

a) ambas cartas sean picas;
b) una carta sea pica y la otra sea un corazón;

Hay $\binom{52}{2} = 1\,326$ formas de extraer 2 cartas de una baraja con 52 naipes.

a) Hay $\binom{13}{2} = 78$ formas de extraer 2 picas de un palo con 13 picas; por tanto,

$$p = \frac{\text{número de formas en que es posible extraer 2 picas}}{\text{número de formas en que es posible extraer 2 cartas}} = \frac{78}{1326} = \frac{3}{51}$$

b) Hay 13 picas y 13 corazones, de modo que hay $13 \cdot 13 = 169$ formas de extraer una pica y un corazón. Por tanto, $p = \frac{169}{1326} = \frac{13}{102}$.

7.6 Considere el espacio muestral en el problema 7.1. Suponga que la moneda y el dado son normales; entonces S es un espacio equiprobable. Encontrar:

a) $P(A)$, $P(B)$, $P(C)$
b) $P(A \cup B)$, $P(B \cap C)$, $P(B \cap A^{C} \cap C^{C})$

Puesto que S es un espacio equiprobable, se usa $P(E) = n(E)/n(S)$. Aquí $n(S) = 12$. Por tanto, sólo es necesario contar el número de elementos en el conjunto dado.

a) $P(A) = \frac{3}{12}$, $P(B) = \frac{6}{12}$, $P(C) = \frac{3}{12}$

b) $P(A \cup B) = \frac{8}{12}$, $P(B \cap C) = \frac{2}{12}$, $P(B \cap A^{C} \cap C^{C}) = \frac{3}{12}$

7.7 Una caja contiene dos calcetines blancos y dos calcetines azules. Se extraen al azar dos calcetines. Encuentre la probabilidad p de que coincidan (que ambos sean del mismo color).

Hay $\binom{4}{2} = 6$ formas de extraer dos de los calcetines. Sólo dos pares coinciden. Por tanto, $p = \frac{2}{6} = \frac{1}{3}$.

7.8 Cinco caballos compiten en una carrera. Audrey escoge al azar dos de los caballos y apuesta por ellos. Encuentre la probabilidad p que Audrey haya escogido al ganador.

Hay $\binom{5}{2} = 10$ formas de escoger 2 de los caballos. Cuatro de los pares contienen al ganador. Por tanto, $p = \frac{4}{10} = \frac{2}{5}$.

ESPACIOS DE PROBABILIDAD FINITOS

7.9 Un espacio muestral S consta de cuatro elementos; es decir, $S = \{a_1, a_2, a_3, a_4\}$. ¿Bajo cuál(es) de la(s) siguiente(s) función(es) S se convierte en un espacio de probabilidad?

a) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{3}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = \frac{1}{5}$

b) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = -\frac{1}{4}$ $P(a_4) = \frac{1}{2}$

c) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{8}$ $P(a_4) = \frac{1}{8}$

d) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = 0$

a) Puesto que la suma de los valores sobre los puntos muestrales es mayor que uno, la función no define a S como un espacio de probabilidad.

b) Puesto que $P(a_3)$ es negativo, la función no define a S como un espacio de probabilidad.

c) Puesto que cada valor es no negativo y la suma de los valores es uno, la función define a S como un espacio de probabilidad.

d) Los valores son no negativos y su suma es uno; por tanto, la función define a S como un espacio de probabilidad.

7.10 Una moneda está "cargada", de modo que la probabilidad de obtener cara (H) es dos veces la probabilidad de obtener cruz (T). Encontrar $P(T)$ y $P(H)$.

Sea $P(T) = p$; entonces $P(H) = 2p$. Luego, la suma de las probabilidades se iguala a uno; es decir, se hace $p + 2p = 1$. Entonces $p = \frac{1}{3}$. Por tanto, $P(H) = \frac{1}{3}$ y $P(T) = \frac{2}{3}$.

7.11 Suponga que A y B son eventos con $P(A) = 0.6$, $P(B) = 0.3$, y $P(A \cap B) = 0.2$. Encontrar la probabilidad de que:

a) no ocurra A; *b*) no ocurra B; *c*) ocurra A o B; *d*) no ocurra ni A ni B.

a) $P(\text{no } A) = P(A^{\text{C}}) = 1 - P(A) = 0.4$.

b) $P(\text{no } B) = P(B^{\text{C}}) = 1 - P(B) = 0.7$.

c) Por el principio de adición,

$$\begin{aligned} P(A \text{ o } B) &= P(A \cup B) = P(A) + P(B) - P(A \cap B) \\ &= 0.6 + 0.3 - 0.2 = 0.7 \end{aligned}$$

d) Recuerde (ley de De Morgan) que ni A ni B es el complemento de $A \cup B$. Por tanto,

$$P(\text{ni } A \text{ ni } B) = P((A \cup B)^{\text{C}}) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$$

7.12 Demuestre el teorema 7.2: $P(A^{\text{c}}) = 1 - P(A)$.

$S = A \cup A^{\text{c}}$, donde A y A^{c} son ajenos. El resultado se obtiene a partir de lo siguiente:

$$1 = P(S) = P(A \cup A^{\text{c}}) = P(A) + P(A^{\text{c}})$$

7.13 Demuestre el teorema 7.3: *i*) $P(\varnothing) = 0$; *ii*) $P(A \backslash B) = P(A) - P(A \cap B)$; *iii*) Si $A \subseteq B$, entonces $P(A) \leq P(B)$.

i) $\varnothing = S^{\text{c}}$ y $P(S) = 1$. Por tanto $P(\varnothing) = 1 - 1 = 0$.

ii) Como se indica en la figura 7-6*a*), $A = (A \backslash B) \cup (A \cap B)$ donde $A \backslash B$ y $A \cap B$ son ajenos. Por tanto

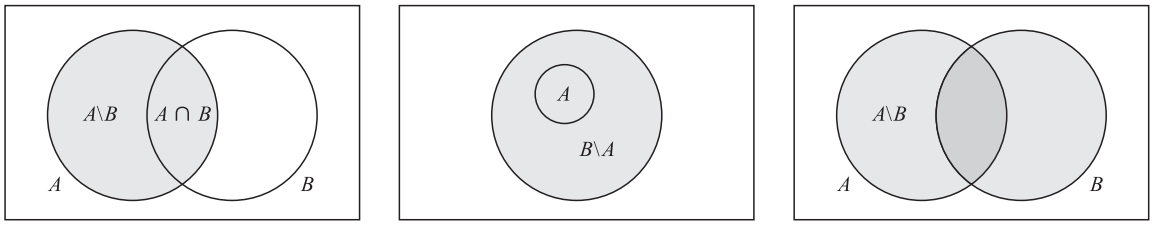
$$P(A) = P(A \backslash B) + P(A \cap B)$$

De donde se obtuvo el resultado.

iii) Si $A \subseteq B$ entonces, según se indica en la figura 7-6*b*), $B = A \cup (B \backslash A)$ donde A y $B \backslash A$ son ajenos. Por tanto,

$$P(B) = P(A) + P(B \backslash A)$$

Puesto que $P(B \backslash A) \geq 0$, se tiene $P(A) \leq P(B)$.



a) *A* está sombreado *b*) *B* está sombreado *c*) $A \cup B$ está sombreado

Figura 7-6

7.14 Demuestre el teorema 7.4 (principio de adición): para eventos arbitrarios *A* y *B*,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Según se indica en la figura 7-6*c*), $(A \cup B) = (A \backslash B) \cup B$, donde $A \backslash B$ y *B* son conjuntos ajenos. Por tanto, al aplicar el teorema 7.3*ii*),

$$\begin{aligned} P(A \cup B) &= P(A \backslash B) + P(B) = P(A) - P(A \cap B) + P(B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

PROBABILIDAD CONDICIONAL

7.15 Se lanza un par de dados normales. (Vea la figura 7-1*b*).) Encuentre la probabilidad que la suma sea 10 o más si:

a) En el primer dado aparece 5; *b*) aparece 5 por lo menos en un dado.

a) Si en el primer dado aparece 5, entonces el espacio muestral reducido es

$$A = \{(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6)\}$$

La suma es 10 o más en dos de los seis resultados: (5, 5) y (5, 6). Por tanto, $p = \frac{2}{6} = \frac{1}{3}$.

b) Si aparece 5 por lo menos en un dado, entonces el espacio muestral reducido tiene once elementos.

$$B = \{(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6), (1, 5), (2, 5), (3, 5), (4, 5), (6, 5)\}$$

La suma es 10 o mayor en tres de los once resultados: (5, 5), (5, 6), (6, 5). Por tanto, $p = \frac{3}{11}$.

7.16 En una universidad, 25% de los estudiantes reprobaron matemáticas (*M*), 15% reprobaron química (*C*) y 10% reprobaron tanto matemáticas como química. Se escoge un estudiante al azar.

a) Si reprobó química, encontrar la probabilidad de que también reprobó matemáticas.
b) Si reprobó matemáticas, encontrar la probabilidad de que también reprobó química.
c) Encontrar la probabilidad de que haya reprobado matemáticas o química.
d) Encontrar la probabilidad de que no haya reprobado ni matemáticas ni química.

a) La probabilidad de que un estudiante haya reprobado matemáticas, dado que reprobó química, es

$$P(M|C) = \frac{P(M \cap C)}{P(C)} = \frac{0.10}{0.15} = \frac{2}{3}$$

b) La probabilidad de que un estudiante haya reprobado química, dado que reprobó matemáticas, es

$$P(C|M) = \frac{P(C \cap M)}{P(M)} = \frac{0.10}{0.25} = \frac{2}{5}$$

c) Por el principio de adición (teorema 7.4),

$$P(M \cup C) = P(M) + P(C) - P(M \cap C) = 0.25 + 0.15 - 0.10 = 0.30$$

d) Los estudiantes que no reprobaron ni matemáticas ni química forman el complemento del conjunto $M \cup C$; es decir, constituyen el conjunto $(M \cup C)^{C}$. Por tanto,

$$P((M \cup C)^{C}) = 1 - P(M \cup C) = 1 - 0.30 = 0.70$$

7.17 Un par de dados normales se lanza una vez. Dado que los dos números en la cara superior son diferentes, encontrar la probabilidad p de que: *a*) la suma sea 6; *b*) aparezca un uno; *c*) la suma sea menor o igual que 4.

Hay 36 resultados posibles al lanzar un par de dados, y seis de ellos, (1, 1), (2, 2),..., (6, 6), tienen los mismos números. Por tanto, el espacio muestral reducido consta de $36 - 6 = 30$ elementos.

a) La suma 6 puede aparecer en cuatro formas: (1, 5), (2, 4), (4, 2), (5, 1). (No es posible incluir (3, 3) puesto que los números son iguales.) Por tanto, $p = \frac{4}{30} = \frac{2}{15}$.

b) Un uno puede aparecer en 10 formas: (1, 2), (1, 3),..., (1, 6) y (2, 1), (3, 1),..., (6, 1). En consecuencia, $p = \frac{10}{30} = \frac{1}{3}$.

c) Que la suma sea 4 o menor puede aparecer en cuatro formas: (3, 1), (1, 3), (2, 1), (1, 2). Así que, $p = \frac{4}{30} = \frac{2}{15}$.

7.18 En un grupo hay 12 varones y 4 mujeres y se seleccionan al azar tres estudiantes. Encontrar la probabilidad p que todos sean varones.

La probabilidad de que el primer estudiante seleccionado sea un varón es $12/16$, puesto que de los 16 estudiantes, 12 son varones. Si el primer estudiante es un varón, entonces la probabilidad de que el segundo estudiante sea un varón es $11/15$, ya que 11 de los 15 estudiantes restantes son varones. Por último, si los dos primeros estudiantes seleccionados son varones, entonces la probabilidad de que el tercer estudiante sea un varón es $10/14$, ya que 10 de los 14 estudiantes restantes son varones. Así, por el teorema de la multiplicación, la probabilidad de que los tres estudiantes seleccionados sean varones es

$$p = \frac{12}{16} \cdot \frac{11}{15} \cdot \frac{10}{14} = \frac{11}{28}$$

Otro método

Hay $C(16, 3) = 560$ formas de seleccionar tres varones de un grupo de 16 estudiantes, y $C(12, 3) = 220$ formas de seleccionar tres varones de un grupo de 12 varones; por tanto,

$$p = \frac{220}{560} = \frac{11}{28}$$

Otro método

Si los estudiantes se seleccionan uno después del otro, entonces hay $16 \cdot 15 \cdot 14$ formas de seleccionar tres estudiantes, y $12 \cdot 11 \cdot 10$ formas de seleccionar tres varones; por tanto,

$$p = \frac{12 \cdot 11 \cdot 10}{16 \cdot 15 \cdot 14} = \frac{11}{28}$$

INDEPENDENCIA

7.19 La probabilidad de que A acierte en el blanco es $\frac{1}{3}$ y la probabilidad de que B acierte en el blanco es $\frac{1}{5}$. Ambos disparan al blanco. Encuentre la probabilidad de que:

a) A no acierte en el blanco;
b) ambos acierten en el blanco;
c) uno de ellos acierte en el blanco;
d) ninguno acierte en el blanco.

Se proporciona $P(A) = \frac{1}{3}$ y $P(B) = \frac{1}{5}$ (y se supone que los eventos son independientes).

a) $(P \text{ no } A) = P(A^{C}) = 1 - P(A) = 1 - \frac{1}{3} = \frac{2}{3}$.

b) Puesto que los eventos son independientes,

$$P(A \text{ y } B) = P(A \cap B) = P(A) \cdot P(B) = \tfrac{1}{3} \cdot \tfrac{1}{5} = \tfrac{1}{15}$$

c) Por el principio de adición (teorema 7.4),

$$P(A \text{ o } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) = \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{15} = \tfrac{7}{15}$$

d) Se tiene

$$P(\text{ni } A \text{ ni } B) = P((A \cup B)^{\text{C}}) = 1 - P(A \cup B) = 1 - \tfrac{7}{15} = \tfrac{8}{15}$$

7.20 Considere los siguientes eventos para una familia con hijos:

$$A = \{\text{hijos de ambos sexos}\},\ B = \{\text{ a lo más un varón}\}$$

a) Demostrar que A y B son eventos independientes si una familia tiene tres hijos.
b) Demuestre que A y B son eventos dependientes si una familia sólo tiene dos hijos.

a) Se tiene el espacio equiprobable $S = \{vvv, vvn, vnv, vnn, nvv, nvn, nnv, nnn\}$ (v = varón; n = niña). Aquí

$$\begin{array}{lll} A = \{vvn, vnv, vnn, nvv, nvn, nnv\} & \text{y así} & P(A) = \frac{6}{8} = \frac{3}{4} \\ B = \{vnn, nvn, nnv, nnn\} & \text{y así} & P(B) = \frac{4}{8} = \frac{1}{2} \\ A \cap B = \{vnn, nvn, nnv\} & \text{y así} & P(A \cap B) = \frac{3}{8} \end{array}$$

Puesto que $P(A)P(B) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8} = P(A \cap B)$, A y B son independientes.

b) Se tiene el espacio equiprobable $S = \{vv, vn, nv, nn\}$. Aquí

$$\begin{array}{lll} A = \{vn, nv\} & \text{y así} & P(A) = \frac{1}{2} \\ B = \{vn, nv, nn\} & \text{y así} & P(B) = \frac{3}{4} \\ A \cap B = \{vn, nv\} & \text{y así} & P(A \cap B) = \frac{1}{2} \end{array}$$

Puesto que $P(A)P(B) \neq P(A \cap B)$, A y B son dependientes.

7.21 La caja A contiene cinco canicas rojas y tres canicas azules, y la caja B contiene tres canicas rojas y dos canicas azules. De cada caja se extrae al azar una canica.

a) Encuentre la probabilidad p de que ambas canicas sean rojas.
b) Encuentre la probabilidad p de que una canica sea roja y la otra sea azul.

a) La probabilidad de escoger una canica roja de A es $\frac{5}{8}$ y de B es $\frac{3}{5}$. Puesto que los eventos son independientes, $P = \frac{5}{8} \cdot \frac{3}{5} = \frac{3}{8}$.

b) La probabilidad p_1 de escoger una canica roja de A y una canica azul de B es $\frac{5}{8} \cdot \frac{2}{5} = \frac{1}{4}$. La probabilidad p_2 de escoger una canica azul de A y una canica roja de B es $\frac{3}{8} \cdot \frac{3}{5} = \frac{9}{40}$. Por tanto, $p = p_1 + p_2 = \frac{1}{4} + \frac{9}{40} = \frac{19}{40}$.

7.22 Demuestre: si A y B son eventos independientes, entonces A^{c} y B^{c} son eventos independientes.

Sean $P(A) = x$ y $P(B) = y$. Entonces $P(A^{\text{c}}) = 1 - x$ y $P(B^{\text{c}}) = 1 - y$. Puesto que A y B son independientes, $P(A \cap B) = P(A)P(B) = xy$. Además,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = x + y - xy$$

Por la ley de De Morgan, $(A \cup B)^{\text{c}} = A^{\text{c}} \cap B^{\text{c}}$; por tanto,

$$P(A^{\text{c}} \cap B^{\text{c}}) = P((\text{A} \cup B)^{\text{c}}) = 1 - P(A \cup B) = 1 - x - y + xy$$

Por otra parte,

$$P(A^{\text{c}})P(B^{\text{c}}) = (1 - x)(1 - \text{y}) = 1 - x - y + xy$$

Por tanto, $P(A^{\text{c}} \cap B^{\text{c}}) = P(A^{\text{c}})P(B^{\text{c}})$, y así A^{c} y B^{c} son independientes.

En forma semejante, puede demostrarse que A y B^{c}, así como A^{c} y B, son independientes.

ENSAYOS REPETIDOS, DISTRIBUCIÓN BINOMIAL

7.23 Suponga que, siempre que los caballos *a*, *b*, *c*, *d* corren juntos, sus probabilidades respectivas de ganar son 0.2, 0.5, 0.1, 0.2. Es decir, $S = \{a, b, c, d\}$, donde $P(a) = 0.2$, $P(b) = 0.5$, $P(c) = 0.1$, $P(d) = 0.2$. Corren tres veces.

a) Describa y encuentre el número de elementos en el espacio de probabilidad producto S_3.
b) Encuentre la probabilidad de que el mismo caballo gane las tres carreras.
c) Encuentre la probabilidad de que el ganador de cada carrera sea *a*, *b* y *c*.

Por conveniencia en la notación, se escribe *xyz* en lugar de (x, y, z).

a) Por definición, $S_3 = S \times S \times S = \{xyz \mid x, y, z \in S\}$ y $P(xyz) = P(x)P(y)P(z)$.
Por tanto, en particular, S_3 contiene $4^3 = 64$ elementos.

b) Se busca la probabilidad del evento $A = \{aaa, bbb, ccc, ddd\}$. Por definición,

$$P(aaa) = (0.2)^3 = 0.008, \quad P(ccc) = (0.1)^3 = 0.001$$
$$P(bbb) = (0.5)^3 = 0.125, \quad P(ddd) = (0.2)^3 = 0.008$$

Por tanto, $P(A) = 0.0008 + 0.125 + 0.001 + 0.008 = 0.142$.

c) Se busca la probabilidad del evento $B = \{abc, acb, bac, bca, cab, cba\}$. Cualquier elemento en *B* tiene la misma probabilidad, el producto $(0.2)(0.5)(0.1) = 0.01$. Por tanto, $P(B) = 6(0.01) = 0.06$.

7.24 La probabilidad de que Juan acierte en un blanco es $p = \frac{1}{4}$. Dispara $n = 6$ veces. Encuentre la probabilidad de que acierte en el blanco: *a*) exactamente dos veces; *b*) más de cuatro veces; *c*) por lo menos una vez.

Se trata de un experimento binomial con $n = 6$, $p = \frac{1}{4}$ y $q = 1 - p = \frac{3}{4}$; es decir, $B(6, \frac{1}{4})$. En consecuencia, se aplica el teorema 7.7.

a) $P(2) = \binom{6}{2}\left(\frac{1}{4}\right)^2\left(\frac{3}{4}\right)^4 = 15(3^4)/(4^6) = \frac{1\,215}{4\,096} \approx 0.297.$

b) $P(5) + P(6) = \binom{6}{5}\left(\frac{1}{4}\right)^5\left(\frac{3}{4}\right)^1 + \left(\frac{1}{4}\right)^6 = \frac{18}{4}^6 + \frac{1}{4}^6 = \frac{19}{4}^6 = \frac{19}{4\,096} \approx 0.0046.$

c) $P(0) = \left(\frac{3}{4}\right)^6 = \frac{729}{4\,096}$, de donde $P(X > 0) = 1 - \frac{729}{4\,096} = \frac{3\,367}{4\,096} \approx 0.82.$

7.25 Una familia tiene seis descendientes. Encuentre la probabilidad *p* que haya: *a*) tres varones y tres niñas; *b*) menos varones que niñas. Suponga que la probabilidad que cualquier descendiente sea varón es $\frac{1}{2}$.

Aquí $n = 6$ y $p = q = \frac{1}{2}$.

a) $p = P(3\text{ varones}) = \binom{6}{3}\left(\frac{1}{2}\right)^3\left(\frac{1}{2}\right)^2 = \frac{20}{64} = \frac{5}{16}.$

b) Hay menos varones que niñas si hay cero, uno o dos varones. Por tanto,

$$p = P(0\text{ varones}) + P(1\text{ varón}) + P(2\text{ varones}) = \left(\frac{1}{2}\right)^6 + \binom{6}{1}\left(\frac{1}{2}\right)^5 + \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{11}{32} = 0.34$$

7.26 Un persona dispara hacia un blanco $n = 6$ veces y acierta $k = 2$ veces. *a*) Enumerar las distintas formas en que puede ocurrir esto. *b*) ¿Cuántas formas hay?

a) Se enumeran todas las sucesiones con dos éxitos (*E*) y cuatro fracasos (*F*):

EEFFFF, *EFEFFF*, *EFFEFF*, *EFFFEF*, *EFFFFE*, *FEEFFF*, *FEFEFF*, *FEFFEF*, *FEFFFE*, *FFEEFF*, *FFEFEF*, *FFEFFE*, *FFFEEF*, *FFFEFE*, *FFFFEE*.

b) Como se indica en la lista, hay 15 formas distintas. Observe que lo anterior es igual a $\binom{6}{2}$ puesto que se están distribuyendo $k = 2$ letras *E* entre $n = 6$ posiciones en la sucesión.

7.27 Demuestre el teorema 7.7: La probabilidad de obtener exactamente k éxitos en un experimento binomial $B(n, p)$ está dada por

$$P(k) = p(k \text{ éxitos}) = \binom{n}{k} p^k q^{n-k}$$

La probabilidad de uno o más éxitos es $1 - q^n$.

El espacio muestral de los n ensayos repetidos consta de todas las n-adas (es decir, sucesiones con n elementos) cuyas componentes son E (éxito) o F (fracaso). Sea A el evento de obtener exactamente k éxitos. Entonces A consta de todas las n-adas de las cuales k componentes son E y $n - k$ componentes son F. El número de tales n-adas en el evento A es igual al número de formas en que k letras E pueden repartirse entre las n componentes de una n-ada; por tanto, A consta de $C(n, k) = \binom{n}{k}$ puntos muestrales. La probabilidad de cada punto en A es $p^k q^{n-k}$; por tanto

$$P(A) = \binom{n}{k} p^k q^{n-k}$$

En particular, la probabilidad de obtener cero éxitos es

$$P(0) = \binom{n}{0} p^0 q^n = q^n$$

Por tanto, la probabilidad de obtener uno o más éxitos es $1 - q^n$.

VARIABLES ALEATORIAS, ESPERANZA

7.28 Un jugador lanza dos monedas normales. Gana \$2 si ocurren dos caras (H), y \$1 si ocurre una cara. Por otra parte, pierde \$3 si no ocurre cara. Encontrar el valor esperado E del juego. El juego, ¿es justo? (El juego es justo, favorable o desfavorable para el jugador según si $E = 0$, $E > 0$ o $E < 0$.)

El espacio muestral $S = \{HH, HT, TH, TT\}$, y cada punto muestral tiene la probabilidad ¼. Para que gane el jugador, se tiene

$$X(HH) = \$2, \quad X(HT) = X(TH) = \$1, \quad X(TT) = -\$3$$

Por tanto, se concluye que la distribución de X es:

x_i	2	1	−3
p_i	1/4	2/4	1/4

Así, $E = E(X) = 2(1/4) + 1(2/4) - 3(1/4) = \$0.25$. Puesto que $E(X) > 0$, el juego es favorable para el jugador.

7.29 Una persona ha ganado una competencia. El premio consiste en seleccionar uno de tres sobres y guardar su contenido. Dos sobres contienen un cheque por \$30 cada uno, pero el tercer sobre contiene un cheque por \$3 000. Encuentre la esperanza E de los triunfos (como una distribución de probabilidad).

X denota los triunfos. Entonces $X = 30$ o 3 000, y $P(30) = \frac{2}{3}$ y $P(3\,000) = \frac{1}{3}$. Por tanto

$$E = E(X) = 30 \cdot \tfrac{2}{3} + 3\,000 \cdot \tfrac{1}{3} = 20 + 1\,000 = 1\,020$$

7.30 Del conjunto {1, 2, 3} se extrae con reemplazamiento una muestra aleatoria de tamaño $n = 2$, de modo que se obtiene el siguiente espacio muestral equiprobable con 9 elementos:

$$S = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

a) Sea X la suma de los dos números. Encuentre la distribución f de X, así como el valor esperado $E(X)$.
b) Sea Y el menor de los dos números. Encuentre la distribución g de Y, así como el valor esperado $E(Y)$.

a) La variable aleatoria X tiene los valores 2, 3, 4, 5, 6. Se calcula la distribución f de X:

i) Un punto (1, 1) tiene suma 2; por tanto, $f(2) = \frac{1}{9}$.

ii) Dos puntos (1, 2), (2, 1) tienen suma 3; por tanto, $f(3) = \frac{2}{9}$.

iii) Tres puntos (1, 3), (2, 2), (1, 3) tienen suma 4; por tanto, $f(4) = \frac{3}{9}$.

iv) Dos puntos (2, 3), (3, 2) tienen suma 5; por tanto, $f(5) = \frac{2}{9}$.

v) Un punto (3, 3) tiene suma 6; por tanto, $f(6) = \frac{1}{9}$.

Así, la distribución f de X es:

x	2	3	4	5	6
$f(x)$	1/9	2/9	3/9	2/9	1/9

El valor esperado $E(X)$ de X se obtiene al multiplicar cada valor de x por su probabilidad $f(x)$ y tomar la suma. Por tanto,

$$E(X) = 2\left(\frac{1}{9}\right) + 3\left(\frac{2}{9}\right) + 4\left(\frac{3}{9}\right) + 5\left(\frac{2}{9}\right) + 6\left(\frac{1}{9}\right) = 4$$

b) La variable aleatoria Y sólo tiene los valores 1, 2, 3. Se calcula la distribución g de Y:

i) Cinco puntos, (1, 1), (1, 2), (1, 3), (2, 1) y (3, 1), tienen a 1 como el menor número; por tanto, $g(1) = \frac{5}{9}$.

ii) Tres puntos, (2, 2), (2, 3), (3, 2) tienen a 2 como el menor número; por tanto, $g(2) = \frac{3}{9}$.

iii) Un punto (3, 3) tiene a 3 como el menor número; por tanto, $g(3) = \frac{1}{9}$.

Así, la distribución g de Y es:

y	1	2	3
$g(y)$	5/9	3/9	1/9

El valor esperado $E(Y)$ de Y es:

$$E(Y) = 1\left(\frac{5}{9}\right) + 2\left(\frac{3}{9}\right) + 3\left(\frac{1}{9}\right) = \frac{12}{9} \approx 1.33$$

7.31 Un arreglo lineal PALANCAS consta de n elementos. Suponga que SUMA aparece al azar en el arreglo, y que se realiza una búsqueda lineal para encontrar la ubicación K de SUMA; es decir, para encontrar K tal que PALANCAS[K] = SUMA. Sea $f(n)$ el número que denota las comparaciones en la búsqueda lineal.

a) Encuentre el valor esperado de $f(n)$.
b) Encuentre el valor máximo (peor caso) de $f(n)$.

a) Sea X el número que denota las comparaciones. Puesto que SUMA puede aparecer en cualquier posición en el arreglo con la misma probabilidad de $1/n$, se tiene $X = 1, 2, 3, \ldots, n$, cada uno con probabilidad $1/n$. Por tanto,

$$\begin{aligned} f(n) = E(X) &= 1 \cdot \tfrac{1}{n} + 2 \cdot \tfrac{1}{n} + 3 \cdot \tfrac{1}{n} + \cdots + n \cdot \tfrac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \tfrac{1}{n} = \tfrac{n(n+1)}{2} \cdot \tfrac{1}{n} = \tfrac{n+1}{2} \end{aligned}$$

b) Si SUMA aparece al final del arreglo, entonces $f(n) = n$.

MEDIA, VARIANZA, DESVIACIÓN ESTÁNDAR

7.32 Encuentre la media $\mu = E(X)$, la varianza $\sigma^2 = Var(X)$ y la desviación estándar $\sigma = \sigma_x$ de cada distribución:

a)

x_i	2	3	11
p_i	1/3	1/2	1/6

b)

x_i	1	3	4	5
p_i	0.4	0.1	0.2	0.3

Se usan las fórmulas:

$$\mu = E(X) = x_1 p_1 + x_2 p_2 + \cdots + x_m p_m = \Sigma x_i p_i, \quad \sigma^2 = Var\,(X) = E(X^2) - \mu^2$$

$$E(X^2) = x_1^2 p_1 + x_2^2 p_2 + \cdots + x_m^2 p_m = \Sigma x_i^2 p_i, \qquad \sigma = \sigma_x = \sqrt{Var\,(X)}$$

a) $\mu = \Sigma x_i p_i = 2\left(\frac{1}{3}\right) + 3\left(\frac{1}{2}\right) + 11\left(\frac{1}{6}\right) = 4$
$E(X^2) = \Sigma x_i^2 p_i = 2^2\left(\frac{1}{3}\right) + 3^2\left(\frac{1}{2}\right) + 11^2\left(\frac{1}{6}\right) = 26$
$\sigma^2 = Var(X) = E(X^2) - \mu^2 = 26 - 4^2 = 10$
$\sigma = \sqrt{Var(X)} = \sqrt{10} = 3.2$

b) $\mu = \Sigma x_i p_i = 1(0.4) + 3(0.1) + 4(0.2) + 5(0.3) = 3$
$E(X^2) = \Sigma x_i^2 p_i = 1(0.4) + 9(0.1) + 16(0.2) + 25(0.3) = 12$
$\sigma^2 = Var(X) = E(X^2) - \mu^2 = 12 - 9 = 3$
$\sigma = \sqrt{Var(X)} = \sqrt{3} = 1.7$

7.33 El lanzamiento de un dado normal da el espacio muestral equiprobable $S = \{1, 2, 3, 4, 5, 6\}$, donde $n(S) = 6$ y cada punto tiene probabilidad $1/6$.

a) Sea X una variable aleatoria que denota el doble del número que ocurre. Encuentre la distribución f de X y su esperanza $E(X)$.

b) Sea Y la variable aleatoria que asigna 1 o 3 según ocurre un número impar o par. Encuentre la distribución g de Y y su esperanza $E(Y)$.

a) Aquí el espacio rango $R_X = \{2, 4, 6, 8, 10, 12\}$ puesto que

$$X(1) = 2, \quad X(2) = 4, \quad X(3) = 6, \quad X(4) = 8, \quad X(5) = 10, \quad X(6) = 12$$

También, cada número ocurre con probabilidad $1/6$. Por tanto, se concluye que la distribución f de X es:

x	2	4	6	8	10	12
$f(x)$	1/6	1/6	1/6	1/6	1/6	1/6

Así,

$$E(X) = \sum xf(x) = \frac{2}{6} + \frac{4}{6} + \frac{6}{6} + \frac{8}{6} + \frac{10}{6} + \frac{12}{6} = 7$$

b) Aquí el espacio rango $R_Y = \{1, 3\}$, ya que

$$Y(1) = 1, \quad Y(2) = 3, \quad Y(3) = 1, \quad Y(4) = 3, \quad Y(5) = 1, \quad Y(6) = 3$$

La distribución g de Y se calcula con $n(S) = 6$:

i) Tres puntos, 1, 3, 5 son impares y su imagen es 1; por tanto, $g(1) = 3/6$.

ii) Tres puntos, 2, 4, 6 son pares y su imagen es 3; por tanto, $g(3) = 3/6$.

Por tanto, la distribución g de Y es:

y	1	3
$g(y)$	3/6	3/6

Así,

$$E(Y) = \sum yg(y) = \frac{3}{6} + \frac{9}{6} = 2$$

7.34 Sea $Z = X + Y$, donde X y Y son las variables aleatorias del problema 7.33. Encontrar la distribución h de Z, así como $E(Z)$. Comprobar que $E(X + Y) = E(X) + E(Y)$.

El espacio muestral aún es $S = \{1, 2, 3, 4, 5, 6\}$ y cada punto sigue con la probabilidad de $1/6$. Se obtiene con $Z(s) = (X + Y)(s) = X(s) + Y(s)$.

$$Z(1) = X(1) + Y(1) = 2 + 1 = 3; \quad Z(4) = X(4) + Y(4) = 8 + 3 = 11,$$
$$Z(2) = X(2) + Y(2) = 4 + 3 = 7; \quad Z(5) = X(5) + Y(5) = 10 + 1 = 11,$$
$$Z(3) = X(3) + Y(3) = 6 + 1 = 7; \quad Z(6) = X(6) + Y(6) = 12 + 3 = 15.$$

Por tanto, el espacio rango es $R_z = \{3, 7, 11, 15\}$. La distribución h de Z se obtiene al usar el hecho que $n(S) = 6$:

i) Un punto tiene imagen 3, de modo que $h(3) = 1/6$;
ii) Dos puntos tienen imagen 7, de modo que $h(7) = 2/6$;
iii) Dos puntos tienen imagen 11, de modo que $h(11) = 2/6$;
iv) Un punto tiene imagen 15, de modo que $h(15) = 1/6$.

Por tanto, se tiene como distribución h de Z:

z	3	7	11	15
$h(z)$	1/6	2/6	2/6	1/6

Así,

$$E(Z) = \sum zh(z) = \frac{3}{6} + \frac{14}{6} + \frac{22}{6} + \frac{15}{6} = 9$$

En consecuencia,

$$E(X + Y) = E(Z) = 9 = 7 + 2 = E(X) + E(Y).$$

DISTRIBUCIÓN BINOMIAL

7.35 La probabilidad que una persona acierte en un blanco es $p = 0.1$. La persona dispara $n = 100$ veces. Encontrar el número esperado μ de veces que la persona acierta en el blanco, así como la desviación estándar σ.

Se trata de un experimento binomial $B(n, p)$, donde $n = 100$, $p = 0.1$ y $q = 1 - p = 0.9$. En consecuencia, se aplica el teorema 7.9 para obtener

$$\mu = np = 100(0.1) = 10 \quad \text{y} \quad \sigma = \sqrt{npq} = \sqrt{100(0.1)(0.9)} = 3$$

7.36 Un estudiante presenta un examen de opción múltiple de 18 reactivos, con cuatro opciones por reactivo. Suponga que una de las opciones es incorrecta en forma evidente, y que el estudiante hace una elección "deducida" de las opciones restantes. Encuentre el número esperado $E(X)$ de respuestas correctas, así como la desviación estándar σ.

Se trata de un experimento binomial $B(n, p)$, donde $n = 18$, $p = \frac{1}{3}$ y $q = 1 - p = \frac{2}{3}$. Así,

$$E(X) = np = 18 \cdot \tfrac{1}{3} = 6 \quad \text{y} \quad \sigma = \sqrt{npq} = \sqrt{18 \cdot \tfrac{1}{3} \cdot \tfrac{2}{3}} = 2$$

7.37 Puede demostrarse que la función esperanza $E(X)$ sobre el espacio de variables aleatorias sobre un espacio muestral S es *lineal*; es decir,

$$E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$$

Usar esta propiedad para demostrar que $\mu = np$ para un experimento binomial $B(n, p)$.

Sobre el espacio muestral de n ensayos de Bernoulli, sea X_i (para $i = 1, 2, \ldots, n$) la variable aleatoria que tiene el valor 1 o 0 si el i-ésimo ensayo es un éxito o un fracaso. Entonces, cada X_i tiene la distribución

x	0	1
$p(x)$	q	p

Por tanto, $E(X_i) = 0(q) + 1(p) = p$. El número total de éxitos en n ensayos es

$$X = X_1 + X_2 + \cdots + X_n$$

Al aplicar la propiedad de linealidad de E, se obtiene

$$\begin{aligned} E(X) &= E(X_1 + X_2 + \cdots + X_n) \\ &= E(X_1) + E(X_2) + \cdots + E(X_n) \\ &= p + p + \cdots + p = np \end{aligned}$$

PROBLEMAS DIVERSOS

7.38 Suponga que X es una variable aleatoria con media $\mu = 75$ y desviación estándar $\sigma = 5$.

Calcule la probabilidad que X esté entre $75 - 20 = 55$ y $75 + 20 = 95$.

La desigualdad de Chebyshev establece lo siguiente:

$$P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \frac{1}{k^2}$$

Aquí $k\sigma = 20$. Puesto que $\sigma = 5$, se obtiene $k = 4$. Entonces, por la desigualdad de Chebyshev,

$$P(55 \leq X \geq 95) = 1 - \frac{1}{4^2} = \frac{15}{16} \approx 0.94$$

7.39 Sea X una variable aleatoria con media $\mu = 40$ y desviación estándar $\sigma = 2$. Usar la desigualdad de Chebyshev a fin de encontrar una b para la cual $P(40 - b \leq X \leq 40 + b) \geq 0.95$.

Primero de $1 - 1/k^2 = 0.95$ se resuelve para k como sigue:

$$0.05 = \frac{1}{k^2} \quad \text{o} \quad k^2 = \frac{1}{0.05} = 20 \quad \text{o} \quad k = \sqrt{20} = 2\sqrt{5}$$

Entonces, por la desigualdad de Chebyshev, $b = k\sigma = 10\sqrt{5} \approx 23.4$. Por tanto, $[P(16.6 \leq X \leq 63.60) \geq 0.95]$.

7.40 Sea x una variable aleatoria con distribución f. El r-ésimo *momento* M_r de X se define como

$$M_r = E(X^r) = \sum x_i^r f(x_i)$$

Encuentre los cuatro primeros momentos de X si X tiene la distribución:

x	-2	1	3
$f(x)$	1/2	1/4	1/4

Observe que M_1 es la media de X, y que M_2 se usa para calcular la desviación estándar de X.

Se usa la fórmula para M_r a fin de obtener:

$$M_1 = \sum x_i f(x_i) = -2\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 3\left(\tfrac{1}{4}\right) = 0$$
$$M_2 = \sum x_i^2 f(x_i) = 4\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 9\left(\tfrac{1}{4}\right) = 4.5$$
$$M_3 = \sum x_i^3 f(x_i) = -8\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 27\left(\tfrac{1}{4}\right) = 3$$
$$M_4 = \sum x_i^4 f(x_i) = 16\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{4}\right) + 81\left(\tfrac{1}{4}\right) = 28.5$$

7.41 Demuestre el teorema 7.10 (desigualdad de Chebyshev): Para $k > 0$,

$$P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \tfrac{1}{k^2}$$

Por definición,

$$\sigma^2 = Var(X) = \sum (x_i - \mu)^2 p_i$$

De la sumatoria se eliminan todos los términos x_i que están en el intervalo $[\mu - k\sigma, \mu + k\sigma]$; es decir, se borran todos los términos para los cuales $|x_i - \mu| \leq k\sigma$. La sumatoria de los términos restantes se denota por $\sum^* (x_i - \mu)^2 pi$. Entonces

$$\left[\sigma^2 \geq \sum{}^* (x_i - \mu)^2 p_i \geq \sum{}^* k^2\sigma^2 p_i = k^2\sigma^2 \sum{}^* p_i = k^2\sigma^2 P(|X - \mu| > k\sigma)\right]$$
$$= k^2\sigma^2[1 - P(|X - \mu| \leq k\sigma)] = k^2\sigma^2[1 - P(\mu - k\sigma \leq X \leq \mu + k\sigma)]$$

Si $\sigma > 0$, entonces al dividir entre $k^2\sigma^2$ se obtiene

$$\tfrac{1}{k^2} \geq 1 - P(\mu - k\sigma \leq X \leq \mu = k\sigma) \quad \text{o} \quad P(\mu - k\sigma \leq X \leq \mu + k\sigma) \geq 1 - \tfrac{1}{k^2}$$

lo cual demuestra la desigualdad de Chebyshev para $\sigma > 0$. Si $\sigma = 0$, entonces $x_i = \mu$ para toda $p_i > 0$, y

$$P(\mu - k \cdot 0 \leq X \leq \mu + k \cdot 0) = P(X = \mu) = 1 > 1 - \tfrac{1}{k^2}$$

con lo que se completa la demostración.

PROBLEMAS SUPLEMENTARIOS

ESPACIOS MUESTRALES Y EVENTOS

7.42 Sean A, B y C eventos. Con notación de conjuntos vuelva a escribir cada uno de los siguientes eventos:

a) Ocurren A y B pero no ocurre C;
b) Ocurren A o C pero no ocurre B;
c) Ninguno de los eventos ocurre;
d) Ocurren al menos dos de los eventos.

7.43 Se lanzan dos monedas de distintas denominaciones y un dado.

a) Describa un espacio muestral idóneo S, y encuentre $n(S)$.
b) Exprese explícitamente los siguientes eventos:
$A = \{$dos caras y un número par$\}$
$B = \{$aparece 2$\}$
$C = \{$exactamente una cara y un número impar$\}$
c) Exprese explícitamente los siguientes eventos: *i*) A y B; *ii*) sólo B; *iii*) B y C.

ESPACIOS EQUIPROBABLES FINITOS

7.44 Determine la probabilidad de cada evento:

a) El resultado al lanzar un dado normal es un número impar.
b) En el lanzamiento de cuatro monedas normales se obtienen una o más caras.
c) En el resultado al lanzar dos dados normales, uno o ambos números exceden a 4.

7.45 De 50 tarjetas numeradas del 1 al 50 se escoge una al azar. Encuentre la probabilidad de que el número de la tarjeta sea:

a) mayor que 10;
b) divisible entre 5;
c) mayor que 10 y divisible entre 5;
d) mayor que 10 o divisible entre 5.

7.46 De 10 muchachas en un grupo, tres tienen ojos azules. Se escogen al azar dos del grupo. Encuentre la probabilidad de que:

a) ambas tengan ojos azules;
b) ninguna tenga ojos azules;
c) por lo menos una tenga ojos azules;
d) exactamente una tenga ojos azules.

7.47. En un grupo hay 10 estudiantes, $A, B, \ldots$. Para representar al grupo es necesario elegir al azar un comité integrado por tres estudiantes. Encuentre la probabilidad de que:

a) A pertenezca al comité;
b) B pertenezca al comité;
c) A y B pertenezcan al comité;
d) A o B pertenezcan al comité.

7.48 En una caja hay tres tornillos y tres tuercas. Se escogen dos piezas al azar. Encuentre la probabilidad que una sea un tornillo y la otra sea una tuerca.

7.49 En una caja hay dos calcetines blancos, dos calcetines azules y dos calcetines rojos. Se extraen al azar dos calcetines. Encuentre la probabilidad que coincidan (que sean del mismo color).

7.50 De 120 estudiantes, 60 estudian francés, 50 estudian español y 20 estudian francés y español. Se escoge un estudiante al azar, encuentre la probabilidad p que él estudie *a*) francés o español; *b*) ni francés ni español; *c*) sólo francés; *d*) exactamente uno de los dos idiomas.

ESPACIOS DE PROBABILIDAD FINITOS

7.51 Decida cuáles de las siguientes funciones definen un espacio de probabilidad sobre $S = \{a_1, a_2, a_3\}$:

a) $P(a_1) = \frac{1}{4}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$
b) $P(a_1) = \frac{2}{3}, P(a_2) = -\frac{1}{3}, P(a_3) = \frac{2}{3}$
c) $P(a_1) = \frac{1}{6}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$
d) $P(a_1) = 0, P(a_2) = \frac{1}{3}, P(a_3) = \frac{2}{3}$

7.52 Una moneda está "cargada" de modo que la ocurrencia de caras (H) es tres veces más probable que la ocurrencia de cruces (T). Encuentre $P(H)$ y $P(T)$.

7.53 Tres estudiantes A, B y C compiten en una carrera de natación. A y B tienen la misma probabilidad de ganar y cada uno tiene el doble de probabilidad de ganar que C. Encuentre la probabilidad de que: *a*) gane B; *b*) gane C; *c*) gane B o C.

7.54 Considere la siguiente distribución de probabilidad:

Resultado x	1	2	3	4	5
Probabilidad $P(x)$	0.2	0.4	0.1	0.1	0.2

Considere los eventos $A = \{\text{número par}\}$, $B = \{2, 3, 4, 5\}$, $C = \{1, 2\}$. Encuentre:

a) $P(A)$, $P(B)$, $P(C)$; *b*) $P(A \cap B)$, $P(A \cap C)$, $P(B \cap C)$.

7.55 Suponga que A y B son eventos con $P(A) = 0.7$, $P(B) = 0.5$ y $P(A \cap B) = 0.4$. Encuentre la probabilidad de que:

a) A no ocurra; *c*) ocurra A pero no ocurra B;
b) ocurra A o B; *d*) no ocurra ni A ni B.

PROBABILIDAD CONDICIONAL, INDEPENDENCIA

7.56 Se lanza un dado normal. Considere los eventos $A = \{2, 4, 6\}$, $B = \{1, 2\}$, $C = \{1, 2, 3, 4\}$. Encuentre:

a) $P(A \text{ y } B)$ y $P(A \text{ o } C)$, *c*) $P(A|C)$ y $P(C|A)$
b) $P(A|B)$ y $P(B|A)$ *d*) $P(B|C)$ y $P(C|B)$

Decida si los siguientes eventos son independientes: *i*) A y B; *ii*) A y C; *iii*) B y C.

7.57 Se lanza un par de dados normales. Si los números que se obtienen son diferentes, encuentre la probabilidad de que: *a*) la suma sea par; *b*) la suma exceda a nueve.

7.58 Sean A y B eventos con $P(A) = 0.6$, $P(B) = 0.3$ y $P(A \cap B) = 0.2$ Encuentre:

a) $P(A \cup B)$; *b*) $P(A|B)$; *c*) $P(B|A)$

7.59 Sean A y B eventos con $P(A) = 1/3$, $P(B) = \frac{1}{4}$ y $P(A \cup B) = \frac{1}{2}$.

a) Encuentre $P(A|B)$ y $P(B|A)$. *b*) A y B ¿son independientes?

7.60 Sean A y B eventos con $P(A) = 0.3$, $P(A \cup B) = 0.5$ y $P(B) = p$. Encuentre p si:

a) A y B son ajenos; *b*) A y B son independientes; *c*) A es un subconjunto de B.

7.61 Sean A y B eventos independientes con $P(A) = 0.3$ y $P(B) = 0.4$. Encuentre:

a) $P(A \cap B)$ y $P(A \cup B)$; *b*) $P(A|B)$ y $P(B|A)$.

7.62 En un club campestre, 60% de las mujeres juegan tenis; 40% juegan golf y 20% juegan tanto tenis como golf. Se escoge una mujer al azar.

a) Encuentre la probabilidad de que no juegue tenis ni golf.
b) Si juega tenis, encuentre la probabilidad de que juegue golf.
c) Si juega golf, encuentre la probabilidad de que juegue tenis.

7.63 En la caja A hay seis canicas rojas y dos canicas azules, y en la caja B hay dos rojas y cuatro azules. De cada caja se extrae al azar una canica.

a) Encuentre la probabilidad p de que ambas canicas sean rojas.
b) Encuentre la probabilidad p de que una canica sea roja y la otra sea azul.

7.64 La probabilidad de que A acierte en un blanco es $\frac{1}{4}$ y la probabilidad de que B acierte en el blanco es $\frac{1}{3}$.

a) Si cada uno dispara dos veces, ¿cuál es la probabilidad de que se acierte en el blanco por lo menos una vez?
b) Si cada uno dispara una vez y sólo hay un acierto en el blanco, ¿cuál es la probabilidad de que A dé en el blanco?

7.65 Se lanzan tres monedas normales. Considere los eventos:

$A = \{\text{todas cara o todas cruz}\}$, $B = \{\text{por lo menos dos caras}\}$, $C = \{\text{a lo más dos caras}\}$.

De los pares (A, B), (A, C) y (B, C), ¿cuáles son independientes? ¿Cuáles son dependientes?

7.66 Encuentre $P(B|A)$ si *a*) A es un subconjunto de B; *b*) A y B son mutuamente excluyentes. (Suponga que $P(A) > 0$.)

ENSAYOS REPETIDOS, DISTRIBUCIÓN BINOMIAL

7.67 Siempre que los caballos *a*, *b* y *c* corren juntos, sus probabilidades de ganar son 0.3, 0.5 y 0.2 respectivamente. Corren tres veces.

a) Encuentre la probabilidad de que el mismo caballo gane las tres carreras.
b) Encuentre la probabilidad de que cada uno gane una carrera.

7.68 El porcentaje de bateo de un beisbolista es 0.300. Tiene cuatro turnos al bat. Encuentre la probabilidad de que el jugador conecte: *a*) exactamente dos sencillos; *b*) al menos un sencillo.

7.69 La probabilidad de que Tom anote una canasta de tres puntos es $p = 0.4$. Dispara $n = 5$ veces. Encuentre la probabilidad de que anote *a*) exactamente dos veces; *b*) al menos una vez.

7.70 Cierto tipo de misil acierta en el blanco con probabilidad $P = \frac{1}{3}$.

a) Si se disparan tres misiles, encuentre la probabilidad de que se acierte en el blanco por lo menos una vez.
b) Encuentre el número de misiles que es necesario disparar de modo que haya por lo menos una probabilidad de 90% de dar en el blanco.

VARIABLES ALEATORIAS

7.71 Se lanza un par de dados. X denota el mínimo de los dos números que ocurren. Encuentre las distribuciones y la esperanza de X.

7.72 Una moneda normal se lanza cuatro veces. X denota la secuencia más larga de caras. Encuentre la distribución y la esperanza de X.

7.73 Una moneda normal se lanza hasta que se obtiene una cara o cinco cruces. Encuentre el número esperado E de lanzamientos de la moneda.

7.74 Una moneda está "cargada" de modo que $P(H) = \frac{3}{4}$ y $P(T) = \frac{1}{4}$. La moneda se lanza tres veces. X es el número de caras que se obtienen.

a) Encuentre la distribución f de X. *b*) Encuentre la esperanza $E(X)$.

7.75 La probabilidad de que el equipo A gane cualquier juego es $\frac{1}{2}$. Suponga que A juega contra B en un torneo. El primer equipo que gane dos juegos seguidos o tres juegos gana el torneo. Encuentre el número esperado de juegos en el torneo.

7.76 Una caja contiene 10 transistores, dos de ellos son defectuosos. De la caja se elige un transistor y se prueba hasta que se escoge uno no defectuoso. Encuentre el número esperado de transistores a escoger.

7.77 Una lotería con 500 boletos otorga un premio de \$100, tres premios de \$50 cada uno y cinco premios de \$25 cada uno.

a) Encuentre el número esperado de triunfos de un boleto.
b) Si un boleto cuesta \$1, ¿cuál es el valor esperado del juego?

7.78 Un jugador lanza tres monedas normales. Gana \$5 si se obtienen tres caras, \$3 si se obtienen dos caras y \$1 si sólo se obtiene una cara. Por otra parte, pierde \$15 si se obtienen tres cruces. Encuentre el valor del juego para el jugador.

MEDIA, VARIANZA Y DESVIACIÓN ESTÁNDAR

7.79 Encuentre la media μ, la varianza σ^2 y la desviación estándar σ de cada distribución:

a)

x	2	3	8
$f(x)$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

b)

y	-1	0	1	2	3
$g(y)$	0.3	0.1	0.1	0.3	0.2

7.80 Encuentre la media μ, la varianza σ^2 y la desviación estándar σ de la siguiente distribución de dos puntos, donde $p + q = 1$:

x	a	b
$f(x)$	p	q

7.81 Sea $W = XY$, donde X y Y son las variables aleatorias en el problema 7.33. (Recuerde que $W(s) = (XY)(s) = X(s)Y(s)$.)

a) Encuentre la distribución h de W; *b*) Encuentre $E(W)$.
¿$E(W) = E(X)E(Y)$?

7.82 Sea X una variable aleatoria con la distribución:

x	-1	1	2
$f(x)$	0.2	0.5	0.3

a) Encuentre la media, la varianza y la desviación estándar de X.
b) Encuentre la distribución, la media, la varianza y la desviación estándar de Y, donde *i*) $Y = X^4$; *ii*) $Y = 3^X$.

DISTRIBUCIÓN BINOMIAL

7.83 La probabilidad de que una mujer acierte en un blanco es $p = 1/3$, cuando dispara 50 veces. Encuentre el número esperado μ de veces que acierta en el blanco y la desviación estándar σ.

7.84 El equipo A tiene la probabilidad $p = 0.8$ de ganar cada vez que juega. Sea X el número de veces que A ganará en $n = 100$ juegos. Encuentre la media μ, la varianza σ^2 y la desviación estándar σ de X.

7.85 Un estudiante que no se preparó contesta al azar un examen de cinco reactivos falso-verdadero. Encuentre la probabilidad de que el estudiante apruebe el examen si para aprobar debe contestar correctamente por lo menos cuatro reactivos.

7.86 Sea X una variable aleatoria $B(n, p)$ distribuida binomialmente con $E(X) = 2$ y $Var(X) = \frac{4}{3}$. Encuentre n y p.

DESIGUALDAD DE CHEBYSHEV

7.87 Sea X una variable aleatoria con media μ y desviación estándar σ.
Use la desigualdad de Chebyshev para calcular $P(\mu - 3\sigma \leq X \leq \mu + 3\sigma)$.

7.88 Sea Z la variable aleatoria normal con media $\mu = 0$ y desviación estándar $\sigma = 1$.
Use la desigualdad de Chebyshev a fin de encontrar un valor b para el cual $P(-b \leq Z \leq b) = 0.9$.

7.89 Sea X una variable aleatoria con media $\mu = 0$ y desviación estándar $\sigma = 1.5$.
Use la desigualdad de Chebyshev para calcular $P(-3 \leq X \leq 3)$.

7.90 Sea X una variable aleatoria con media $\mu = 70$.
¿Para qué valor de σ la desigualdad de Chebyshev proporciona $P(65 \leq X \leq 75) \geq 0.95$?

Respuestas a los problemas suplementarios

Se usará la notación $[x_1, \ldots, x_n; f(x_1), \ldots, f(x_n)]$ para la distribución $f = \{(x_i, f(X_i)\}$.

7.42 *a*) $A \cap B \cap C^C$; *c*) $(A \cup B \cup B)^C = A^C \cap B^C C^C$;
b) $(A \cup C) \cap B^C$; *d*) $(A \cap B) \cup (A \cap C) \cup (B \cap C)$.

7.43 *a*) $n(S) = 24$; $S = \{H, T\} \times \{H, T\} \times \{1, 2, \ldots, 6\}$
b) $A = \{HH2, HH4, HH6\}$; $B = \{HH2, HT2, TH2, TT2\}$; $C = \{HT1, HT3, HT5, TH1, TH3, TH5\}$
c) *i*) $HH2$; *ii*) $HT2$, TH2, $TT2$; *iii*) $\varnothing$.

7.44 *a*) 3/6; *b*) 15/16; *c*) 20/36.

7.45 *a*) 40/50; *b*) 10/50; *c*) 8/50; *d*) 42/50.

7.46 *a*) 1/15; *b*) 7/15; *c*) 8/15; *d*) 7/15.

7.47 *a*) 3/10; *b*) 3/10; *c*) 1/15; *d*) 8/15.

7.48 3/5.

7.49 1/5.

7.50 *a*) 3/4; *b*) 1/4; *c*) 1/3; *d*) 7/12.

7.51 *c*) y *d*).

7.52 $P(H) = 3/4$; $P(T) = 1/4$.

7.53 *a*) 2/5; *b*) 1/5; *c*) 3/5.

7.54 *a*) 0.6, 0.8, 0.5; *b*) 0.5, 0.7, 0.4.

7.55 *a*) 0.3; *b*) 0.8; *c*) 0.3; *d*) 0.2.

7.56 *a*) 1/6, 5/6; *b*) 1/2, 1/3; *c*) 1/2, 2/3; *d*) 1/2,
i) Sí; *ii*) sí; *iii*) no.

7.57 *a*) 12/30; *b*) 4/30.

7.58 *a*) 0.7; *b*) 2/3; *c*) 1/3.

7.59 *a*) 1/3, 1/4; *b*) sí.

7.60 *a*) 0.2; *b*) 2/7; *c*) 0.5.

7.61 *a*) 0.12, 0.58; *b*) 3/10, 4/10.

7.62 *a*) 20%; *b*) 1/3; *c*) 1/2.

7.63 *a*) 1/4; *b*) 7/12.

7.64 *a*) 3/4; *b*) 1/3.

7.65 Sólo (A, B) son independientes.

7.66 *a*) l, *b*) 0.

7.67 *a*) 0.16; *b*) 0.18.

7.68 *a*) $6(0.3)^2(0.7)^2 = 0.2646$; *b*) $1 - (0.7)^4 = 0.7599$.

7.69 *a*) $10(0.4)^2(0.6)^3$; *b*) $1 - (0.6)^5$.

7.70 *a*) $1 - (2/3)^5 = 211/243$; *b*) Seis veces.

7.71 [1, 2, 3, 4, 5, 6; 11/36, 9/36, 7/36, 5/36, 3/36, 1/36]; $E(X) = 91/36 \approx 2.5$.

7.72 [0, 1, 2, 3, 4; 1/16, 7/16, 5/16, 2/16, 1/16]; $E(X) = 27/16 \approx 1.7$.

7.73 $E = 1.9$.

7.74 *a*) [0, 1, 2, 3; 1/64, 9/64, 27/64, 27/64]; *b*) $E(X) = 2.25$.

7.75 $23/8 \approx 2.9$.

7.76 $11/9 \approx 1.2$.

7.77 *a*) 0.75; *b*) -0.25.

7.78 0.25.

7.79 *a*) $\mu = 4$, $\sigma^2 = 5.5$, $\sigma = 2.3$; *b*) $\mu = 1$, $\sigma^2 = 2.4$, $\sigma = 1.5$.

7.80 $\mu = ap + bq$; $\sigma^2 = pq(a - b)^2$; $\sigma = |a - b|\sqrt{pq}$

7.81 *a*) [2, 6, 10, 12, 24, 36; 1/6, . . . , 1/6]; *b*) $E(W) = 15$. No.

7.82 *a*) 0.9, 1.09, 1.04; *b*) *i*) [1, 1, 16; 0.2, 0.5, 0.3], 5.5, 47.25, 6.87; *ii*) [1/3, 3, 9; 0.2, 0.5, 0.3], 4.67, 5.21, 3.26.

7.83 $\mu = 50/3 = 16.67$; $\sigma = 10/3 = 3.33$

7.84 $\mu = 80$; $\sigma^2 = 16$; $\sigma = 4$

7.85 6/32.

7.86 $n = 6$, $p = 1/3$

7.87 $P \geq 1 - 1/8 \approx 8.75$

7.88 $B = \sqrt{10} \approx 3.16$

7.89 $P \geq 0.75$

7.90 $\sigma = 5/\sqrt{20} \approx 1.12$

8 Teoría de grafos

CAPÍTULO

8.1 INTRODUCCIÓN, ESTRUCTURA DE DATOS

Grafos, grafos dirigidos, árboles y árboles binarios se utilizan en muchas áreas de las matemáticas y de la computación. Dichos temas se cubrirán en este capítulo y en los dos próximos. No obstante, con el fin de comprender cómo se almacenan estos objetos en la memoria y entender sus algoritmos, es necesario conocer ciertas estructuras de datos. Aquí se supondrá que el lector comprende los arreglos lineales y bidimensionales; por tanto, a continuación sólo se estudiarán listas ligadas y apuntadores, así como pilas y colas.

Listas ligadas y apuntadores

Las listas ligadas y los apuntadores se presentarán por medio de un ejemplo. Suponga que una empresa de correduría mantiene un archivo en el que cada registro contiene el nombre de un cliente y el de un vendedor; por ejemplo, el archivo contiene los datos siguientes:

Cliente	Adams	Brown	Clark	Drew	Evans	Farmer	Geller	Hiller	Infeld
Vendedor	Smith	Ray	Ray	Jones	Smith	Jones	Ray	Smith	Ray

Hay dos operaciones básicas que a veces es necesario efectuar con los datos:

Operación A: dado el nombre de un cliente, encontrar su vendedor.

Operación B: dado el nombre de un vendedor, encontrar la lista de sus clientes.

Enseguida se analizan varias formas para almacenar los datos en una computadora, así como la facilidad con que es posible realizar las operaciones *A* y *B* con los datos.

Resulta evidente que el archivo se puede almacenar en la computadora por medio de un arreglo con dos renglones (o columnas) de nueve nombres. Puesto que los nombres de los clientes están en orden alfabético, es fácil efectuar la operación *A*. No obstante, para efectuar la operación *B* es necesario buscar a través de todo el arreglo.

Es fácil almacenar los datos en la memoria si usa un arreglo bidimensional en el que, por ejemplo, los renglones correspondan a una lista en orden alfabético de los nombres de los clientes y las columnas correspondan a una lista en orden alfabético de los nombres de los vendedores, y en cuya matriz haya un 1 que indica el vendedor de un cliente y haya ceros en el resto de la matriz. La desventaja más importante de esta representación es que se desperdicia bastante memoria debido a que en la matriz puede haber muchos ceros. Por ejemplo, si la firma tiene 1 000 clientes y 20 vendedores, podría ser necesario contar con 20 000 localizaciones de memoria para los datos, aunque sólo 1 000 de ellas serían útiles.

A continuación se analiza una forma para almacenar los datos en la memoria, en la cual se utilizan listas ligadas y apuntadores. Una *lista ligada* es una colección lineal de elementos de datos, denominados *nodos*, en la que el orden lineal se proporciona por medio de un campo de apuntadores. La figura 8-1 es un esquema de una lista ligada con seis nodos. Cada nodo está dividido en dos partes: la primera contiene la información del elemento (por ejemplo, NAME, ADDRESS, . . .) y la segunda parte, denominada *campo liga* (*link field*) o *campo apuntador al siguiente elemento*

(*nextpointer field*), contiene la dirección del siguiente nodo en la lista. Este campo apuntador se indica con una flecha trazada de un nodo al siguiente nodo en la lista. En la figura 8-1 también hay un apuntador variable, denominado START, que proporciona la dirección del primer nodo en la lista. Además, el campo apuntador del último nodo contiene una dirección no válida, denominada *apuntador nulo*, que indica el fin de la lista.

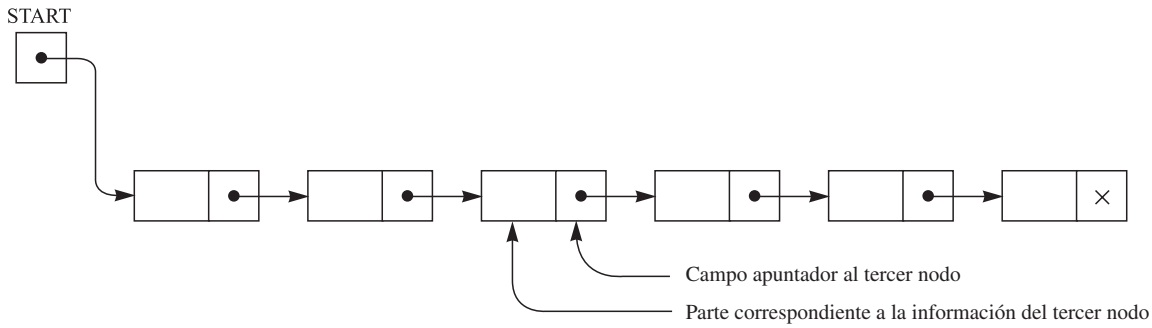


Figura 8-1 Lista ligada con seis nodos

Una forma primordial para almacenar los datos originales representados en la figura 8-2 utiliza listas ligadas. Observe que hay arreglos por separado (en orden alfabético) para los nombres de clientes y de los vendedores. También hay un arreglo apuntador SLSM paralelo a CUSTOMER que proporciona la ubicación del vendedor de un cliente, de modo que la operación *A* puede efectuarse muy rápida y fácilmente. Además, la lista de clientes de cada vendedor es una lista ligada, como ya se analizó. En efecto, hay un arreglo apuntador START paralelo a SALESMAN que indica al primer cliente de un vendedor, y hay un arreglo NEXT que indica la ubicación del siguiente cliente en la lista del vendedor (o contiene un 0 para indicar el fin de la lista). Este proceso se indica mediante las flechas en la figura 8-2 para el vendedor Ray.

	Cliente	SLSM	NEXT
1	Adams	3	5
2	Brown	2	3
3	Clark	2	7
4	Drew	1	6
5	Evans	3	8
6	Farmer	1	0
7	Geller	2	9
8	Hill	3	0
9	Infeld	2	0

Vendedor	START	
Jones	4	1
Ray	2	2
Smith	1	3

Figura 8-2

Ahora la operación *B* puede efectuarse fácil y rápidamente; no es necesario buscar en la lista de todos los clientes para obtener la lista de clientes de un vendedor dado. En la figura 8-3 se proporciona un algoritmo así (que está escrito en pseudocódigo).

Pilas, colas y colas prioritarias

Además de los arreglos y las listas ligadas hay otras estructuras de datos que aparecen en los algoritmos de grafos. Estas estructuras, pilas, colas y colas prioritarias se describen brevemente a continuación.

a) **Pila:** también denominada sistema *último en entrar, primero en salir* (LIFO: *last-in, first-out*), es una lista lineal tal que las inserciones y las eliminaciones pueden llevarse a cabo sólo en un extremo, denominado "parte superior" de la lista. Esta estructura es semejante en su operación a una pila de platos montada en un sistema de resorte, como se muestra en la figura 8-4*a*). Observe que los nuevos platos se insertan sólo en la parte superior de la pila y que los platos pueden retirarse sólo de la parte superior de la pila.

Algoritmo 8.1 Se lee el nombre de un vendedor y se imprime la lista de sus clientes.

Paso 1. Leer XXX.

Paso 2. Encontrar *K* tal que SALESMAN[K] = XXX. [Usar búsqueda binaria].

Paso 3. Sea PTR: START[K]. [Inicializa el apuntador PTR].

Paso 4. Repetir while PTR ≠ NULL.

a) Print CUSTOMER[PTR].

b) Set PTR := NEXT[PTR]. [Actualiza PTR].

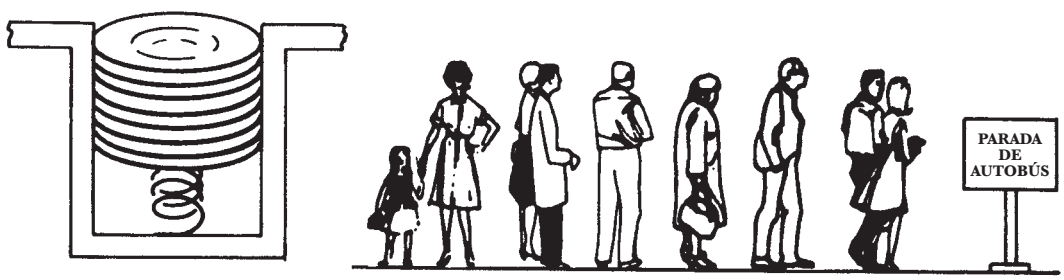
[Fin del ciclo].

Paso 5. Salir.

Figura 8-3

b) **Cola:** también denominada sistema *primero en entrar, primero en salir* (FIFO: *first-in first-out*), es una lista lineal tal que las eliminaciones pueden llevarse a cabo sólo en un extremo de la lista, denominado "frente" de la lista, y las inserciones pueden llevarse a cabo sólo en el otro extremo de la lista, denominado "parte trasera" de la lista. La estructura opera de forma bastante parecida a una cola de personas que esperan en una parada de autobús, como se muestra en la figura 8-4*b*). Es decir, la primera persona en la cola es la primera que aborda el autobús, y una persona recién llegada se coloca al final de la cola.

c) **Cola prioritaria:** sea *S* un conjunto de elementos en el que pueden insertarse periódicamente nuevos elementos, aunque siempre se elimina el mayor elemento actual (el elemento con la "prioridad más alta"). Entonces *S* se denomina *cola prioritaria.* Las reglas "mujeres y niños primero" y "la edad antes que la belleza" son ejemplos de cola prioritaria. Las pilas y las colas normales son tipos especiales de cola prioritaria. En efecto, el elemento con la prioridad más alta en una pila es el último elemento insertado, pero el elemento con la prioridad más alta en una cola es el primer elemento insertado.



a) Pila de platos *b*) Cola en espera del autobús

Figura 8-4

8.2 GRAFOS Y MULTIGRAFOS

Un *grafo G* consta de dos partes:

i) Un conjunto $V = V(G)$ cuyos elementos se denominan *vértices*, *puntos* o *nodos* de *G*.

ii) Un conjunto $E = E(G)$ de pares no ordenados de vértices distintos denominados *aristas* de *G*.

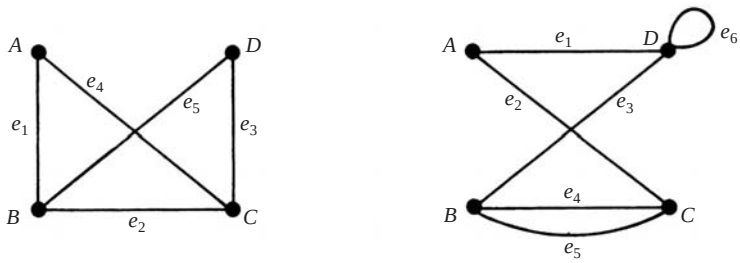
Cuando se desea recalcar las dos partes de un grafo *G*, grafo se denota $G(V, E)$.

Los vértices u y v son *adyacentes* o *vecinos* si hay una arista $e = \{u, v\}$. En este caso, u y v se denominan *extremos* de e, y se dice que e *conecta* o *une* u y v, o también que la arista e es *incidente* (o que incide) en cada uno de sus extremos u y v. Los grafos se representan mediante diagramas en el plano de forma natural. Específicamente, cada vértice v en V se representa por un punto (o un círculo pequeño), y cada arista $e = \{v_1, v_2\}$ se representa por una curva que une sus puntos extremos v_1 y v_2. Por ejemplo, la figura 8-5*a*) representa el grafo $G(V, E)$, donde:

i) V consta de los vértices A, B, C, D.

ii) E consta de las aristas $e_1 = \{A, B\}$, $e_2 = \{B, C\}$, $e_3 = \{C, D\}$, $e_4 = \{A, C\}$, $e_5 = \{B, D\}$.

De hecho, un grafo suele denotarse al trazar su diagrama en lugar de enumerar explícitamente sus vértices y aristas.



a) Grafo *b*) Multigrafo

Figura 8-5

Multigrafos

Considere el diagrama en la figura 8-5*b*). Las aristas e_4 y e_5 se denominan *aristas múltiples* puesto que unen los mismos puntos extremos, y la arista e_6 se denomina lazo porque sus extremos tienen el mismo vértice. Este diagrama se denomina *multigrafo*; la definición formal de grafo no permite aristas múltiples ni lazos. Por tanto, un grafo se define como un multigrafo sin aristas múltiples ni lazos.

Observación: En algunos textos el término *grafo* se usa para incluir multigrafos y el término *grafo simple* para indicar un grafo sin aristas múltiples ni lazos.

Grado de un vértice

El *grado* de un vértice v en un grafo G, se escribe $\text{grd}(v)$, es igual al número de aristas en G que contienen a v; es decir, que inciden sobre v. Puesto que cada arista se cuenta dos veces al contar los grados de los vértices de G, se tiene el siguiente resultado sencillo pero importante.

Teorema 8.1: La suma de los grados de los vértices de un grafo G es igual al doble del número de aristas en G.

Considere, por ejemplo, el grafo de la figura 8-5*a*). Se tiene

$$\text{grd}(A) = 2, \quad \text{grd}(B) = 3, \quad \text{grd}(C) = 3, \quad \text{grd}(D) = 2.$$

La suma de los grados es igual a 10 que, como era de esperar, es el doble del número de aristas. Un vértice es *par* o *impar* si su grado es un número par o impar. Por tanto, A y D son vértices pares, mientras B y C son vértices impares.

El teorema 8.1 también se cumple para multigrafos en las que un lazo se cuenta dos veces para el grado de ese vértice. Por ejemplo, en la figura 8-5*b*) se tiene $\text{grd}(D) = 4$, puesto que la arista e_6 se cuenta dos veces; por tanto, D es un vértice par.

Un vértice de grado cero se denomina vértice *aislado*.

Grafos finitos, grafos triviales

Un multigrafo se dice que es *finito* si tiene un número finito de vértices y de aristas. Observe como una consecuencia que un grafo con un número finito de vértices y aristas tiene que ser finito. Un grafo con un SÓLO vértice sin ninguna arista, un punto, se llama *grafo trivial*. A menos que se especifique otra cosa, en este libro los multigrafos son finitos.

8.3 SUBGRAFOS, GRAFOS ISOMORFOS Y HOMEOMORFOS

En esta sección se analizan relaciones importantes entre grafos.

Subgrafos

Considere un grafo $G = G(V, E)$. Un grafo $H = H(V', E')$ se denomina *subgrafo* de G si los vértices y las aristas de H están contenidas en los vértices y en las aristas de G; es decir, si $V' \subseteq V$ y $E' \subseteq E$. En particular:

i) Un subgrafo $H(V', E')$ de $G(V, E)$ se denomina subgrafo *inducido* por sus vértices V' si su conjunto de aristas E' contiene todas las aristas en G cuyos puntos extremos pertenecen a los vértices en H.

ii) Si v es un vértice en G, entonces $G - v$ es el subgrafo de G obtenida al eliminar v *de* G y al eliminar todas las aristas en G que contienen a v.

iii) Si e es una arista en G, entonces $G - e$ es el subgrafo de G obtenido al eliminar la arista e *de* G. Grafos isomorfos

Grafos isomorfos

Se dice que los grafos $G(V, E)$ y $G^*(V^*, E^*)$ son *isomorfos* si existe una correspondencia uno a uno f; $V \rightarrow V^*$ tal que $\{u, v\}$ es una arista de G si y sólo si $\{f(u), f(v)\}$ es una arista de G^*. Normalmente no se establece ninguna diferencia entre grafos isomorfos (aun cuando sus diagramas puedan "parecer diferentes"). En la figura 8-6 se proporcionan 10 grafos representados como letras; puede observar que A y R son grafos isomorfos, también lo son F y T, K y X son grafos isomorfos y M, S, V y Z también lo son.

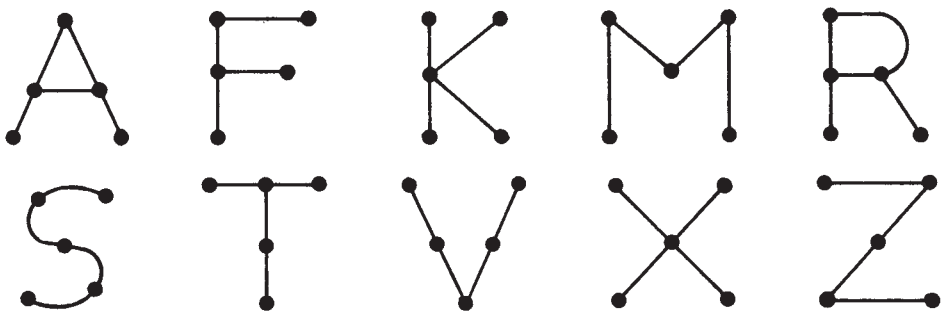
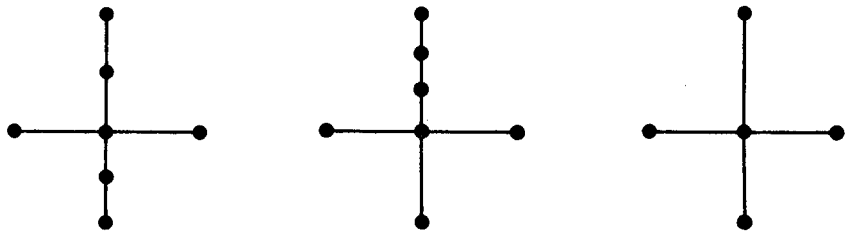


Figura 8-6

Grafos homeomorfos

Dado cualquier grafo G, es posible obtener un nuevo grafo al dividir una arista de G con vértices adicionales. Dos grafos G y G^* son *homeomorfos*, si es posible obtenerlos a partir del mismo grafo o grafos isomorfos al aplicar este método. Los grafos *a*) y *b*) en la figura 8-7 no son isomorfos, aunque son homoeomorfos puesto que pueden obtenerse a partir del grafo *c*) al agregar vértices apropiados.



a) *b*) *c*)

Figura 8-7

8.4 CAMINOS Y CONECTIVIDAD

Un *camino* en un multigrafo G consta de una secuencia alternada de vértices y aristas de la forma

$$v_0, \quad e_1, \quad v_1, \quad e_2, \quad v_2, \quad \ldots, \quad e_{n-1}, \quad v_{n-1}, \quad e_n, \quad v_n$$

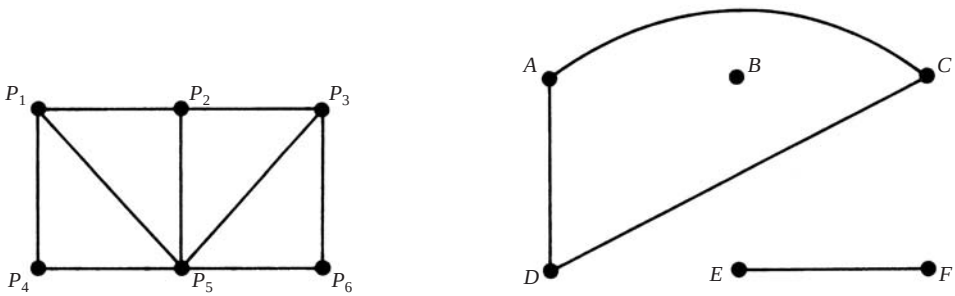
donde cada arista e_i contiene a los vértices v_{i-1} y v_i (que aparecen a los lados de e_i en la secuencia). El número n de aristas se denomina *longitud* del camino. Cuando no hay ambigüedad, un camino se denota por su secuencia de vértices $(v_0, v_1, \ldots, v_n)$. Se dice que el camino es *cerrado* si $v_0 = v_n$. En caso contrario, se dice que el camino es de v_0 a v_n o *entre* v_0 y v_n, o que *une* v_0 y v_n.

Un *camino simple* es un camino en el que todos los vértices son distintos. (Un camino en que todas las aristas son diferentes se denomina *recorrido.*) Un *ciclo* es un camino cerrado de longitud 3 o más donde todos los vértices son distintos excepto $v_0 = v_n$. Un ciclo de longitud k se denomina *k-ciclo*.

EJEMPLO 8.1 Considere el grafo G en la figura 8-8*a*). Considere las siguientes secuencias:

$$\alpha = (P_4, P_1, P_2, P_5, P_1, P_2, P_3, P_6), \quad \beta = (P_4, P_1, P_5, P_2, P_6),$$
$$\gamma = (P_4, P_1, P_5, P_2, P_3, P_5, P_6), \quad \delta = (P_4, P_1, P_5, P_3, P_6).$$

La secuencia α es un camino de P_4 a P_6; pero no es un recorrido porque la arista $\{P_1, P_2\}$ se usa dos veces. La secuencia β no es un camino porque no hay arista $\{P_2, P_6\}$. La secuencia γ es un recorrido porque ninguna arista se usa dos veces; pero no es un camino simple porque el vértice P_5 se usa dos veces. La secuencia δ es un camino simple de P_4 a P_6; pero no es el camino más corto (con respecto a la longitud) de P_4 a P_6. El camino más corto de P_4 a P_6 es el camino simple (P_4, P_5, P_6), cuya longitud es 2.



a) *b*)

Figura 8-8

Al eliminar aristas innecesarias, no es difícil ver que cualquier camino desde un vértice u hasta un vértice v puede sustituirse por un camino simple de u a v. Este resultado se plantea formalmente a continuación.

Teorema 8.2: Hay un camino de un vértice u a un vértice v si y sólo si existe un camino simple de u a v.

Conectividad, componentes conexos

Un grafo G es *conexo* si existe un camino entre dos de sus vértices. El grafo en la figura 8-8*a*) es conexo, pero el grafo en la figura 8-8*b*) no es conexo ya que, por ejemplo, entre los vértices D y E no hay ningún camino.

Suponga que G es un grafo. Un subgrafo conexo H de G se denomina *componente conexo* de G si H no está contenido en ningún subgrafo conexo más grande de G. Resulta intuitivamente claro que cualquier grafo G puede partirse en sus componentes conexos. Por ejemplo, el grafo G en la figura 8-8*b*) tiene tres componentes conexos, los subgrafos inducidos por los conjuntos de vértices $\{A, C, D\}$, $\{E, F\}$ y $\{B\}$.

El vértice B en la figura 8-8*b*) se denomina *vértice aislado* porque B no pertenece a ninguna arista o, en otras palabras, $\text{grd}(B) = 0$. En consecuencia, como se observó, B mismo forma un componente conexo del grafo.

Observación: En términos formales, en el supuesto de que cualquier vértice u esté unido consigo mismo, la relación "u está unido con v" es una relación de equivalencia sobre el conjunto de vértices de un grafo G y las clases de equivalencia de la relación constituyen los componentes conexos de G.

Distancia y diámetro

Considere un grafo conexo G. La *distancia* entre los vértices u y v en G, que se escribe $d(u, v)$, es la longitud de la ruta más corta entre u y v. El *diámetro* de G, lo cual se escribe $\text{diám}(G)$, es la distancia máxima entre dos puntos cualesquiera en G. Por ejemplo, en la figura 8-9*a*), $d(A, F) = 2$ y $\text{diám}(G) = 3$, mientras que en la figura 8-9*b*), $d(A, F) = 3$ y $\text{diám}(G) = 4$.

Puntos de corte y puentes

Sea G un grafo conexo. Un vértice v en G se denomina *punto de corte* si $G - v$ es disconexo. (Recuerde que $G - v$ es el grafo obtenido a partir de G al eliminar v y todos las aristas que contienen a v.) Una arista e de G se denomina *puente* si $G - e$ es disconexo . (Recuerde que $G - e$ es el grafo obtenido a partir de G al eliminar la arista e.) En la figura 8-9*a*), el vértice D es un punto de corte y no hay puentes. En la figura 8-9*b*), la arista $\{D, F\}$ es un puente. (Sus puntos extremos D y F son necesariamente puntos de corte.)

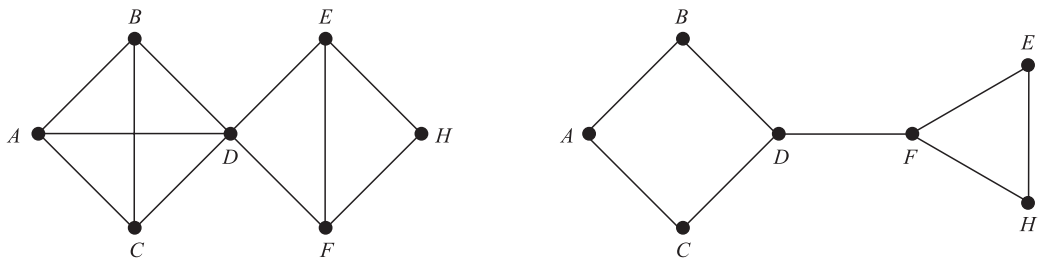
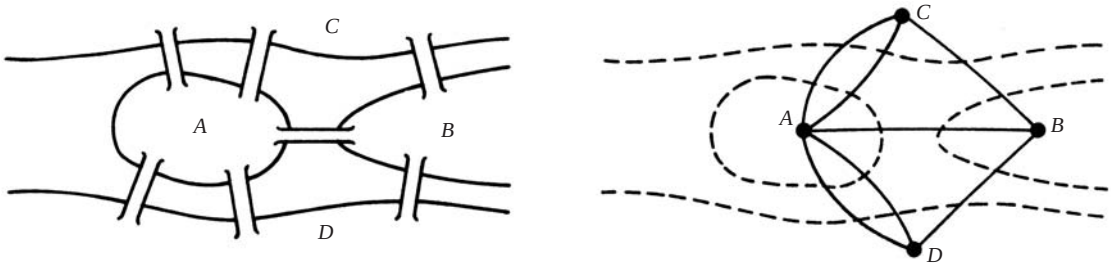


Figura 8-9

8.5 RECORRIDOS Y GRAFOS EULERIANOS, LOS PUENTES DE KÖNIGSBERG

En el siglo XVIII el oriental pueblo prusiano de Königsberg incluía dos islas y siete puentes, como se muestra en la figura 8-10*a*). Pregunta: si una persona empieza en cualquier punto y termina en cualquier punto, ¿es posible que recorra el pueblo de modo que cruce los siete puentes sin cruzar ninguno dos veces? Los ciudadanos de Königsberg escribieron al célebre matemático suizo L. Euler sobre esta cuestión. Euler demostró en 1736 que tal recorrido es imposible; sustituyó las islas y las dos orillas del río por puntos y los puentes por curvas, con lo que obtuvo la figura 8-10*b*).

Observe que la figura 8-10*b*) es un multigrafo. Se dice que un multigrafo es *recorrible* si "la curva puede trazarse sin interrupciones y sin que pase dos veces por cualquiera de las aristas"; es decir, si existe un camino que incluya todos los vértices y use cada arista exactamente una vez. Tal camino debe ser un recorrido (puesto que ninguna arista se usa dos veces), y se denomina *recorrido atravesable* o *recorrible*. Resulta evidente que un multigrafo recorrible debe ser finito y conexo.



a) Königsberg en 1736 *b*) Representación gráfica de Euler

Figura 8-10

A continuación se mostrará cómo Euler probó que el multigrafo en la figura 8-10*b*) no es recorrible y, por tanto, que el recorrido a pie de Königsberg es imposible. Primero recuerde que un vértice es par o impar si su grado es un número par o impar. Suponga que un multigrafo es recorrible y que un recorrido atravesable no empieza o termina en un vértice *P*. Se afirma que *P* es un vértice par. Ya que siempre que el recorrido atravesable entra a *P* por una arista, siempre debe haber una arista no usada previamente por el cual el recorrido puede abandonar *P*. En consecuencia, las aristas del recorrido incidente con *P* deben aparecer por pares, de modo que *P* es un vértice par. Por consiguiente, si un vértice *Q* es impar, entonces el recorrido atravesable debe empezar o terminar en *Q*. En consecuencia, un multigrafo con más de dos vértices impares no puede ser recorrible. Observe que el multigrafo correspondiente al problema de los puentes de Königsberg tiene cuatro vértices impares. Por tanto, no es posible recorrer Königsberg de modo que cada puente se cruce exactamente una vez.

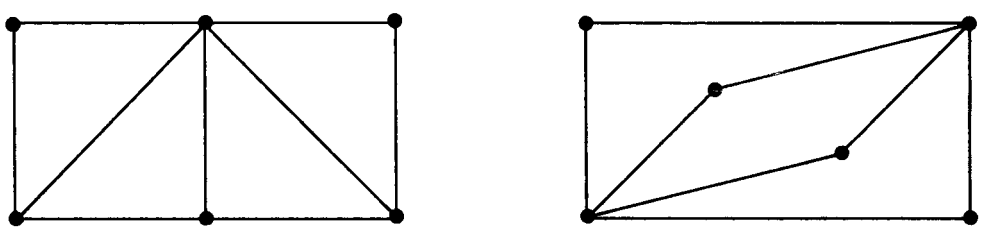
Euler realmente demostró lo contrario del planteamiento anterior, que está contenido en los siguientes teorema y corolario. (El teorema se demuestra en el problema 8.9.). Un grafo *G* se denomina grafo *euleriano* si existe un recorrido atravesable cerrado, denominado *recorrido euleriano*.

Teorema 8.3 (de Euler): Un grafo conexo finito es euleriano si y sólo si cualquier vértice tiene grado par.

Corolario 8.4: Cualquier grafo conexo finito con dos vértices impares es recorrible. Un recorrido atravesable puede empezar en cualquier vértice impar y terminar en el otro vértice impar.

Grafos hamiltonianos

En el análisis anterior sobre los grafos Eulerianos se recalcaron las aristas recorridas; aquí la atención se centra en la visita de vértices. Un *circuito hamiltoniano* en un grafo *G*, así denominado en honor del matemático irlandés del siglo XIX William Hamilton (1803-1865) es un camino cerrado que visita todos los vértices en *G* exactamente una vez. (Este camino cerrado debe ser un ciclo.) Si *G* admite un circuito hamiltoniano, entonces *G* se denomina *grafo hamiltoniano.* Observe que un circuito de Euler recorre cada arista exactamente una vez, aunque puede repetir vértices, mientras que un circuito hamiltoniano visita cada vértice exactamente una vez aunque puede repetir aristas. En la figura 8-11 se proporciona un ejemplo de uno que es hamiltoniano pero no euleriano y viceversa.



a) Hamiltoniano pero no euleriano *b*) Euleriano pero no hamiltoniano

Figura 8-11

Aunque resulta evidente que sólo los grafos conexos pueden ser hamiltonianos, no hay ningún criterio simple para decidir si un grafo es o no hamiltoniano, como sí lo hay para el caso de los grafos eulerianos. Se cuenta con la siguiente condición suficiente, que se debe a G. A. Dirac.

Teorema 8.5: Sea G un grafo conexo con n vértices. Entonces G es hamiltoniano si $n \geq 3$ y $n \leq \text{grd}(v)$ para cada vértice v en G.

8.6 GRAFOS ETIQUETADOS Y PONDERADOS

Un grafo G se denomina *grafo etiquetado* si sus aristas y/o vértices son datos asignados de un tipo o del otro. En particular, G se denomina *grafo ponderado* si a cada arista e de G se asigna un número no negativo $w(e)$ denominado *peso* o *longitud* de v. En la figura 8-12 se muestra un grafo ponderado, en el que el peso de cada arista se proporciona en forma evidente. El *peso* (o la *longitud*) de un camino en tal grafo ponderado G se define como la suma de los pesos de las aristas en el camino. Un problema importante en teoría de grafos es encontrar *el camino más corto*; es decir, un camino de peso (longitud) mínimo(a), entre dos vértices arbitrarios dados. La longitud de un camino más corto entre P y Q en la figura 8-12 es 14; un camino es

$$(P, A_1, A_2, A_5, A_3, A_6, Q)$$

El lector puede tratar de encontrar otro camino más corto.

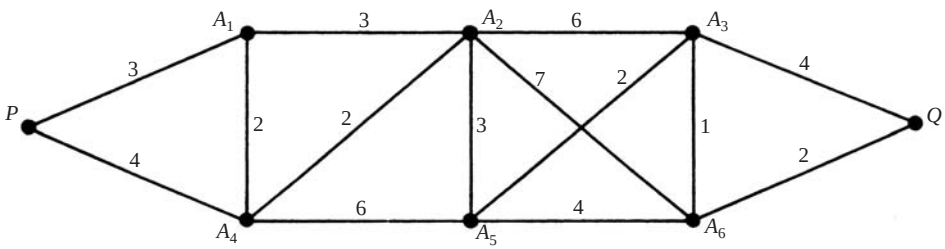


Figura 8-12

8.7 GRAFOS COMPLETOS, REGULARES Y BIPARTIDOS

Hay muchos tipos distintos de grafos. En esta sección se consideran tres: grafos completos, regulares y bipartidos.

Grafos completos

Un grafo G es *completo* si cualquier vértice en G está unido a todos los demás vértices en G. Por tanto, un grafo completo G debe ser conexo. El grafo completo con n vértices se denomina K_n. En la figura 8-13 se muestran los grafos K_1 a K_6.

Grafos regulares

Un grafo G es *regular de grado k* o *k-regular* si sus vértices tienen grado k, si todos los vértices tienen el mismo grado.

Los grafos regulares conexos de grados 0, 1 o 2 se describen con facilidad. El grafo conexo 0-regular es el grafo trivial con un vértice y sin ninguna arista. El grafo conexo 1-regular es el grafo con dos vértices y una arista que los une. El grafo conexo 2-regular con n vértices es el grafo que consta de un solo n-ciclo. Vea la figura 8-14.

Los grafos 3-regular deben tener un número par de vértices, ya que la suma de los grados de los vértices es un número par (teorema 8.1). En la figura 8-15 se muestran dos grafos 3-regular conexos con seis vértices. En general,

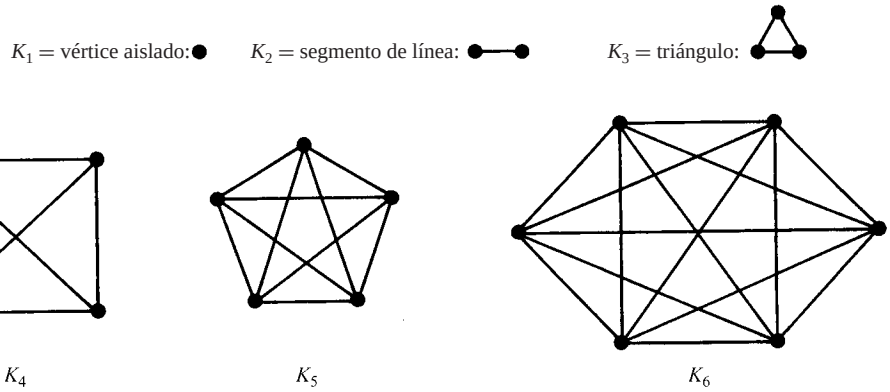


Figura 8-13

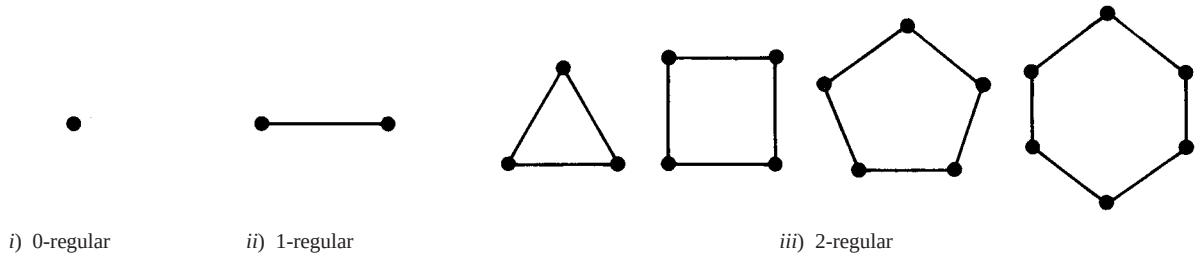


Figura 8-14

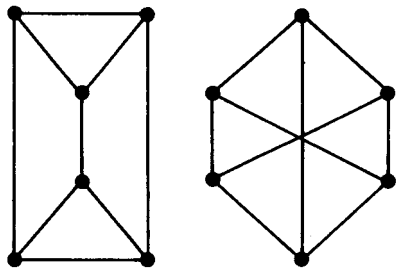


Figura 8-15

los grafos regulares pueden ser bastante complicados. Por ejemplo, hay 19 grafos 3-regular con 10 vértices. Observe que la gráfica completa con n vértices K_n es regular de grado $n - 1$.

Grafos bipartidos

Un grafo G es *bipartido* si sus vértices V pueden partirse en dos subconjuntos M y N tales que cada arista de G une un vértice de M con un vértice de N. Por un grafo bipartido completo se entiende que cada vértice de M está unido a cada vértice de N; este grafo se denota por $K_{m,n}$, donde m es el número de vértices en M y n es el número de vértices en N y, por razones de estandarización, se supone $m \leq n$. En la figura 8-16 se muestran los grafos $K_{2,3}$, $K_{3,3}$ y $K_{2,4}$. Resulta evidente que el grafo $K_{m,n}$ tiene mn aristas.

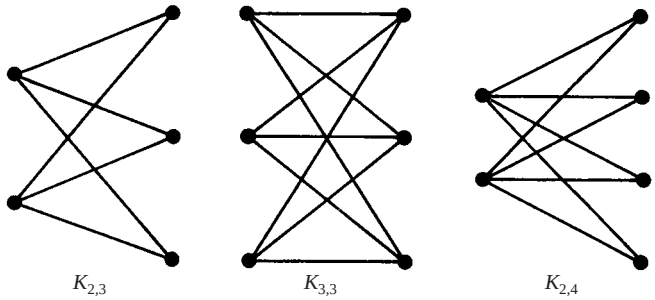


Figura 8-16

8.8 ÁRBOLES

Un grafo T se denomina *árbol* si T es conexo y T no tiene ciclos. En la figura 8-17 se muestran ejemplos de árboles. Un *bosque* G es un grafo sin ciclos; por tanto, los componentes conexos de un bosque G son árboles. Un grafo sin ciclos es *libre de ciclos*. El árbol que consta de un solo vértice sin aristas se denomina *árbol degenerado*.

Considere un árbol T. Resulta evidente que sólo hay un camino simple entre dos vértices de T; en caso contrario, los dos caminos formarían un ciclo. También:

a) Suponga que en T no hay ninguna arista $\{u, v\}$ y que a T se agrega la arista $e = \{u, v\}$. Entonces el camino simple de u a v en T y e forma un ciclo; por tanto, T ya no es un árbol.

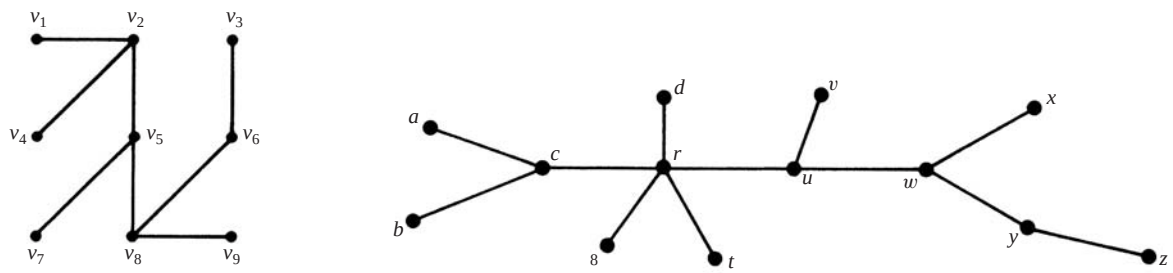
b) Por otra parte, suponga que en T hay una arista $e = \{u, v\}$, y que de T se elimina e. Entonces T ya no es conexo (puesto que no puede haber ningún camino de u a v); así, T ya no es un árbol.

El siguiente teorema (demostrado en el problema 8.14) es válido cuando los grafos son finitos.

Teorema 8.6: Sea G un grafo con $n > 1$ vértices. Entonces las siguientes afirmaciones son equivalentes:

i) G es un árbol.
ii) G es libre de ciclos y tiene $n - 1$ aristas.
iii) G es conexo y tiene $n - 1$ aristas.

Este teorema también indica que un árbol finito con n vértices debe tener $n - 1$ aristas. Por ejemplo, el árbol en la figura 8-17*a*) tiene 9 vértices y 8 aristas, y el árbol en la figura 8-17*b*) tiene 13 vértices y 12 aristas.



a) *b*)

Figura 8-17

Árboles de expansión

Un subgrafo T de un grafo conexo G se denomina *árbol de expansión* de G si T es un árbol y T incluye a todos los vértices de G. En la figura 8-18 se muestra un grafo conexo G y árboles de expansión T_1, T_2 y T_3 de G.

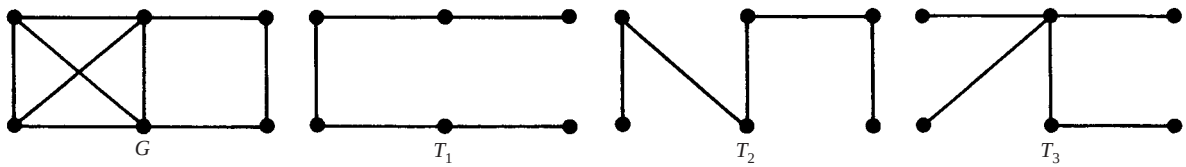


Figura 8-18

Árboles de expansión mínima

Suponga que G es un grafo ponderado conexo. Es decir, a cada arista de G se asigna un número no negativo denominado *peso* de la arista. Entonces a cualquier árbol de expansión T de G se asigna un peso total que resulta de sumar los pesos de las aristas en T. Un *árbol de expansión mínima* de G es un árbol de expansión cuyo peso total es el más pequeño posible.

Los algoritmos 8.2 y 8.3, que aparecen en la figura 8-19, permiten encontrar un árbol de expansión mínima T de un grafo ponderado conexo G, donde G tiene n vértices. (En cuyo caso T debe tener $n - 1$ aristas.)

Algoritmo 8.2: La entrada es un grafo ponderado conexo G con n vértices.

Paso 1. Las aristas de G se disponen en orden decreciente de peso.

Paso 2. Se procede secuencialmente para eliminar cada arista que no haga inconexo al grafo, hasta que queden $n - 1$ aristas.

Paso 3. Salir.

Algoritmo 8.3 (de Kruskal): La entrada es un grafo ponderado conexo G con n vértices.

Paso 1. Las aristas de G se disponen en orden creciente de peso.

Paso 2. Se empieza sólo con los vértices de G y en forma secuencial se agrega cada arista que no origine un ciclo hasta que se hayan agregado $n - 1$ aristas.

Paso 3. Salir.

Figura 8-19

El peso de un árbol de expansión mínima es único, aunque el árbol de expansión mínima en sí no lo es. Cuando dos o más aristas tienen el mismo peso pueden ocurrir distintos árboles de expansión mínima. En este caso, la disposición de las aristas en el paso 1 de los algoritmos 8.2 u 8.3 no es única, y así resultan árboles de expansión mínima distintos, como se ilustra en el siguiente ejemplo.

EJEMPLO 8.2 Encontrar un árbol de expansión mínima del grafo ponderado Q en la figura 8-20*a*). Observe que Q tiene seis vértices, de modo que un árbol de expansión mínima tiene cinco aristas.

a) Aquí se aplica el algoritmo 8.2.

Primero se ordenan las aristas en orden decreciente de peso y luego en forma consecutiva se eliminan las aristas sin hacer inconexo a Q hasta que queden cinco aristas. Así se obtienen los datos siguientes:

Aristas	BC	AF	AC	BE	CE	BF	AE	DF	BD
Peso	8	7	7	7	6	5	4	4	3
Eliminar	Sí	Sí	Sí	No	No	Sí			

Así, el árbol de expansión mínima de Q que se obtiene contiene las aristas

$$BE,\quad CE,\quad AE,\quad DF,\quad BD$$

El peso del árbol de expansión es 24 y se muestra en la figura 8-20*b*).

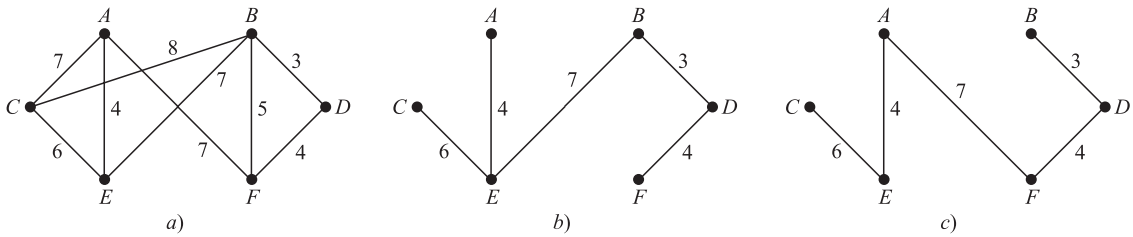


Figura 8-20

b) Aquí se aplica el algoritmo 8.3.

Primero se ordenan las aristas en orden creciente de peso y enseguida se agregan las aristas sin formar ningún ciclo hasta que se incluyen cinco aristas. Así se obtienen los datos siguientes:

Aristas	BD	AE	DF	BF	CE	AC	AF	BE	BC
Peso	3	4	4	5	6	7	7	7	8
¿Agregar?	Sí	Sí	Sí	No	Sí	No	Sí		

Así, el árbol de expansión mínima de Q contiene las aristas

$$BD,\quad AE,\quad DF,\quad CE,\quad AF$$

El árbol de expansión se muestra en la figura 8-20c). Observe que este árbol de expansión no es el mismo que se obtuvo al usar el algoritmo 8.2 y que, como era de esperar, su peso también es 24.

Observación: Los algoritmos anteriores se ejecutan fácilmente cuando el grafo G es relativamente pequeño, como en la figura 8-20*a*). Suponga que G tiene docenas de vértices y centenas de aristas que, por ejemplo, se proporcionan mediante una lista de pares de vértices. Entonces decidir si G es conexo no es evidente; puede ser necesario algún tipo de algoritmo de búsqueda en profundidad en grafos (DFS: Deep-first search) o de búsqueda en anchura (BFS: Breadth-first search) en grafos. En secciones ulteriores y en el siguiente capítulo se analizan formas para representar grafos G en la memoria y se abordarán varios algoritmos para grafos.

8.9 GRAFOS PLANOS

Un grafo o un multigrafo es *plano* cuando puede trazarse en el plano de modo que sus aristas no se crucen. Aunque grafo completo K_4 con cuatro vértices suele representarse con aristas cruzadas como en la figura 8-21*a*), también puede trazarse de modo que sus aristas no se crucen, como en la figura 8-21*b*); por tanto, K_4 es plano. Los árboles constituyen una clase importante de grafos planos. En esta sección se presentan estos grafos importantes.

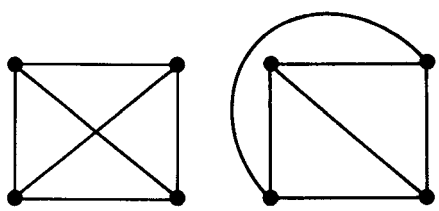


Figura 8-21

Mapas y regiones

Una representación plana particular de un multigrafo plano finito se denomina *mapa*. Se dice que el mapa es *conexo* si el multigrafo subyacente es conexo. Un mapa dado divide el plano en varias regiones. Por ejemplo, el mapa en la figura 8-22 con seis vértices y nueve aristas divide el plano en cinco regiones. Observe que cuatro de las regiones están acotadas y que la quinta región, fuera del diagrama, no está acotada. Así, no hay pérdida de generalidad al contar el número de regiones, si se supone que el mapa está contenido en algún gran rectángulo, en lugar de estarlo en todo el plano.

Observe que la frontera de cada región de un mapa consta de aristas. Algunas veces las aristas forman un ciclo, pero algunas veces no es así. Por ejemplo, en la figura 8-22 las fronteras de todas las regiones son ciclos excepto para r_3. No obstante, si se realiza un movimiento en el sentido contrario al movimiento de las manecillas del reloj alrededor de r_3 empezando, por ejemplo, en el vértice C, entonces se obtiene el camino cerrado

$$(C, D, E, F, E, C)$$

donde la arista $\{E, F\}$ ocurre dos veces. Por el *grado* de una región r, que se escribe grd(r), se entiende la longitud del ciclo o camino cerrado que rodea r. Observe que cada arista delimita dos regiones o está contenida en una región y ocurre dos veces en cualquier recorrido a lo largo de la frontera de la región. Por tanto, se tiene un teorema para regiones que es semejante al teorema 8.1 para vértices.

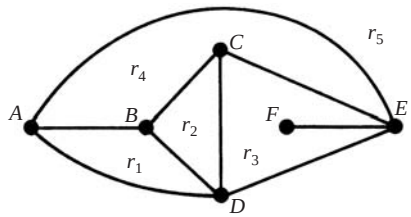


Figura 8-22

Teorema 8.7: La suma de los grados de las regiones de un mapa es igual al doble del número de aristas.

Los grados de las regiones en la figura 8-22 son:

$$\text{grd}(r_1) = 3, \quad \text{grd}(r_2) = 3, \quad \text{grd}(r_3) = 5, \quad \text{grd}(r_4) = 4, \quad \text{grd}(r_5) = 3$$

La suma de los grados es 18 y, como era de esperar, es el doble del número de aristas.

Por conveniencia en la notación, los vértices de un mapa se representan como puntos o círculos pequeños, o se supondrá que cualquier intersección de líneas o curvas en el plano es un vértice.

Fórmula de Euler

Euler proporcionó una fórmula que relaciona el número V de vértices, el número E de aristas y el número R de regiones de cualquier mapa conexo. Específicamente:

Teorema 8.8 (de Euler): $V - E + R = 2$.

(La demostración del teorema 8.8 se proporciona en el problema 8.18.)

Observe que en la figura 8-22, $V = 6$, $E = 9$ y $R = 5$, y, como era de esperar por la fórmula de Euler,

$$V - E + R = 6 - 9 + 5 = 2$$

Se recalca que el grafo subyacente de un mapa debe ser conexo para que se cumpla la fórmula de Euler.

Sea G un multigrafo plano conexo con tres o más vértices, de modo que G no es K_1 ni K_2. Sea M una representación plana de G. No resulta difícil ver que 1) una región de M puede tener grado 1 sólo si su frontera es un lazo, y 2) una región de M puede tener grado 2 sólo si su frontera consta de dos aristas múltiples. En consecuencia, si G es un grafo, no un multigrafo, entonces toda región de M debe tener grado 3 o mayor. Este comentario y la fórmula de Euler se usan para demostrar el siguiente resultado sobre grafos planos.

Teorema 8.9: Sea G un grafo plano conexo con p vértices y q aristas, donde $p \geq 3$. Entonces $q \geq 3p - 6$.

Observe que el teorema no se cumple para K_1, donde $p = 1$ y $q = 0$, y no es verdadero para K_2 donde $p = 2$ y $q = 1$.

Demostración: Sea r el número de regiones en una representación plana de G. Por la fórmula de Euler, $p - q + r = 2$.

Luego, la suma de los grados de las regiones es igual a $2q$ por el teorema 8.7. Pero cada región tiene 3 grados o más; por tanto, $2q \geq 3r$. Así, $r \geq 2q/3$. Al sustituir esto en la fórmula de Euler se obtiene

$$2 = p - q + r \leq p - q + \frac{2q}{3} \quad \text{o} \quad 2 \leq p - \frac{q}{3}$$

Al multiplicar la desigualdad por 3 se obtiene $6 \leq 3p - q$, con lo cual se llega al resultado. □

Grafos no planos, teorema de Kuratowski

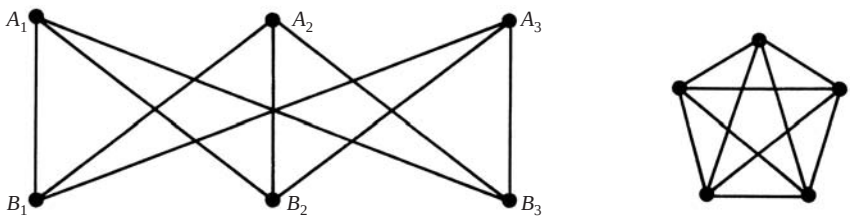
Se proporcionan dos ejemplos de grafos no planos. Primero considere el *grafo de servicios*; es decir, a tres casas A_1, A_2, A_3 deben conectarse las tomas de agua, gas y electricidad B_1, B_2, B_3 como se muestra en la figura 8-23*a*). Observe que se trata del grafo $K_{3,3}$ y que tiene $p = 6$ vértices y $q = 9$ aristas. Suponga que el grafo es plano. Por la fórmula de Euler, una representación plana tiene $r = 5$ regiones. Observe que no hay tres vértices que estén unidos entre sí; por tanto, el grado de cada región debe ser 4 o mayor y así la suma de los grados de las regiones debe ser 20 o mayor. Por el teorema 8.7, el grafo debe tener 10 o más aristas. Esto contradice que el grafo tiene $q = 9$ aristas. Por tanto, el grafo de servicios $K_{3,3}$ no es plano.

Considere el *grafo estrella* en la figura 8-23*b*). Es el grafo completo K_5 sobre $p = 5$ vértices y tiene $q = 10$ aristas. Si el grafo es plano, entonces por el teorema 8.9,

$$10 = q \leq 3p - 6 = 15 - 6 = 9$$

lo cual es imposible. Por tanto, K_5 no es plano.

Durante muchos años los matemáticos intentaron caracterizar los grafos planos y los grafos no planos. Este problema fue resuelto finalmente en 1930 por el matemático polaco K. Kuratowski. La demostración de este resultado, que se plantea a continuación, rebasa el alcance de este texto.



a) $K_{3,3}$ *b*) K_5

Figura 8-23

Teorema 8.10 (de Kuratowski): Un grafo es no plano si y sólo si contiene una subgrafo homeomorfo a $K_{3,3}$ o a K_5.

8.10 COLOREADOS DE GRAFOS

Considere un grafo G. Un *coloreado de vértices*, o simplemente *coloreado de G*, es una asignación de colores a los vértices de G de modo que vértices adyacentes tengan diferentes colores. Se dice que G es n-coloreable si existe un coloreado de G en el que se usan n colores. (Puesto que el término "color" se usa como sustantivo, se intentará evitar

su uso como verbo al decir, por ejemplo, "pintura" G en lugar de "color" G cuando se asignen colores a los vértices de G.) El número mínimo de colores necesarios para pintar a G se denomina *número cromático* de G y se denota por $\chi(G)$.

En la figura 8-24 se proporciona un algoritmo propuesto por Welch y Powell para el coloreado de un grafo G. Se recalca que este algoritmo no siempre produce un coloreado mínimo de G.

Algoritmo 8.4 (de Welch y Powell): La entrada es un grafo G.

Paso 1. Los vértices de G se ordenan en orden decreciente de grado.

Paso 2. El primer color C_1 se asigna al primer vértice y después, en orden secuencial, C_1 se asigna a cada vértice que no sea adyacente al vértice previo al que se asignó C_1.

Paso 3. El paso 2 se repite con un segundo color C_2 y la subsecuencia de vértices no coloreados.

Paso 4. El paso 3 se repite con un tercer color C_3, y luego con un cuarto color C_4, hasta que todos los vértices estén coloreados.

Paso 5. Salir.

Figura 8-24

EJEMPLO 8.3

a) Considere el grafo G en la figura 8-25. Se aplica el algoritmo 8.4, de Welch y Powell, para obtener un coloreado de G. Cuando los vértices se escriben en orden decreciente de grado se obtiene la siguiente secuencia:

$$A_5,\quad A_3,\quad A_7,\quad A_1,\quad A_2,\quad A_4,\quad A_6,\quad A_8$$

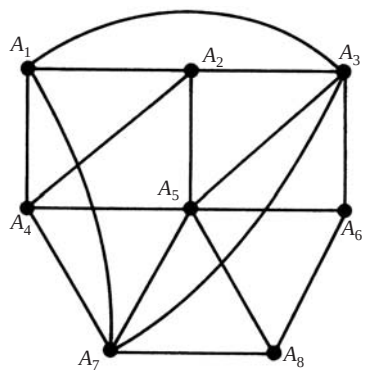


Figura 8-25

El primer color se asigna a los vértices A_5 y A_1. El segundo color se asigna a los vértices A_3, A_4 y A_8. El tercer color se asigna a los vértices A_7, A_2 y A_6. A todos los vértices se ha asignado un color, de modo que G es 3-coloreable. Observe que G no es 2-coloreable puesto que a los vértices A_1, A_2 y A_3, que están unidos entre sí, deben asignarse colores diferentes. En consecuencia, $\chi(G) = 3$.

b) Considere el grafo completo K_n con n vértices. Puesto que cada vértice es adyacente a cualquier otro vértice, K_n requiere n colores en cualquier coloreado. Por tanto, $\chi(K_n) = n$.

No hay ninguna forma sencilla para determinar realmente si un grafo arbitrario es n-coloreable. Sin embargo, el siguiente teorema (que se demuestra en el problema 8.19) proporciona una caracterización simple de grafos 2-coloreables.

Teorema 8.11: Las siguientes afirmaciones son equivalentes para un grafo G:

i) G es 2-coloreable.
ii) G es bipartido.
iii) Todo ciclo de G tiene longitud par.

No hay límite sobre el número de colores que pueden requerirse para colorear un grafo arbitrario puesto que, por ejemplo, el grafo completo K_n requiere n colores. No obstante, si el estudio se restringe a grafos planos, sin importar el número de vértices, bastan cinco colores. Específicamente, en el problema 8.20 se demuestra el siguiente:

Teorema 8.12: Cualquier grafo plano es 5-coloreable.

En realidad, desde el año de 1850 los matemáticos han conjeturado que los grafos planos son 4-coloreables, puesto que todo grafo plano conocido es 4-coloreable. En 1976 Kenneth Appel y Wolfgang Haken demostraron finalmente que esta conjetura es cierta. Es decir:

Teorema de los cuatro colores (Appel y Haken): Cualquier grafo plano es 4-coloreable.

Este teorema se analiza en la siguiente subsección.

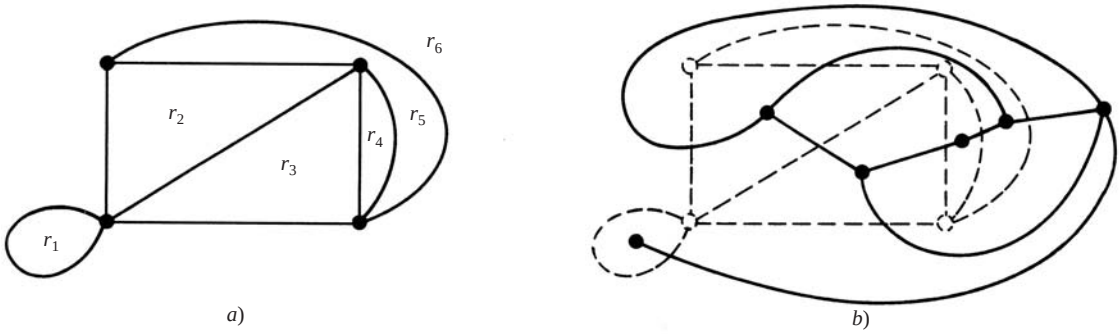
Mapas duales y el teorema de los cuatro colores

Considere un mapa M; por ejemplo, el mapa M en la figura 8-26*a*). En otras palabras, M es una representación plana de un multigrafo plano. Dos regiones de M son *adyacentes* si tienen una arista en común. Así, las regiones r_2 y r_5 en la figura 8-26*a*) son adyacentes, pero las regiones r_3 y r_5 no lo son. Por un *coloreado* de M se entiende la asignación de un color a cada región de M, de modo que regiones adyacentes tengan colores distintos. Un mapa es *n-coloreable* si existe un coloreado de M en el que se usen n colores. Por tanto, el mapa en la figura 8-26*a*) es 3-coloreable, ya que a las regiones pueden asignarse los siguientes colores:

$$r_1 \text{ rojo}, \quad r_2 \text{ blanco}, \quad r_3 \text{ rojo}, \quad r_4 \text{ blanco}, \quad r_5 \text{ rojo}, \quad r_6 \text{ azul}$$

Observe la semejanza entre este análisis sobre coloreado de mapas y el análisis previo sobre coloreado de grafos. De hecho, al usar el concepto de mapa dual definido a continuación, puede demostrarse que el coloreado de un mapa es equivalente al coloreado de vértices de un grafo plano.

Considere un mapa M. En cada región de M se escoge un punto, y si dos regiones tienen una arista en común, entonces se unen los puntos correspondientes con una curva que pasa por la arista común. Estas curvas pueden trazarse de modo que no se crucen. Así se obtiene un nuevo mapa M^* denominado *dual* de M, tal que cada vértice de M^* corresponde exactamente a una región de M. En la figura 8-26*b*) se muestra el dual del mapa de la figura 8-26*a*). Puede demostrarse que cada región de M^* contiene exactamente un vértice de M y que cada arista de M^* corta exactamente una arista de M y viceversa. Por tanto, M es el dual del mapa M^*.



a) *b*)

Figura 8-26

Observe que cualquier coloreado de las regiones de un mapa M corresponde a un coloreado de los vértices del mapa dual M^*. Por tanto, M es n-coloreable si y sólo si el grafo plano del mapa dual M^* de vértices es n-coloreable. Así, el teorema anterior puede volver a plantearse como sigue:

Teorema de los cuatro colores (de Appel y Haken): Si las regiones de cualquier mapa M se colorean de modo que regiones adyacentes tengan colores distintos, entonces no se requieren más de cuatro colores.

Para demostrar el teorema anterior se usan computadoras; puesto que Appel y Haken demostraron por primera vez que si el teorema de los cuatro colores es falso, entonces debe haber un contraejemplo entre aproximadamente 2 000 tipos distintos de grafos planos. Entonces demostraron, usando una computadora, que ninguno de estos tipos de grafos posee tal contraejemplo. El análisis de cada tipo de grafo diferente parece estar más allá del alcance del ser humano sin el uso de una computadora. Por tanto la demostración, a diferencia de la mayor parte de las demostraciones en matemáticas, depende de la tecnología; es decir, depende del desarrollo de computadoras de alta velocidad.

8.11 REPRESENTACIÓN DE GRAFOS EN LA MEMORIA DE LA COMPUTADORA

Hay dos formas normales para mantener un grafo G en la memoria de una computadora. Una forma, denominada *representación secuencial* de G, es por medio de su matriz de adyacencia A. La otra forma, denominada *representación enlazada* o *estructura de adyacencia* de G, usa listas ligadas de vecinos. Las matrices se usan cuando el grafo G es denso, y las listas ligadas suelen usarse cuando G es disperso. (Se dice que un grafo G con m vértices y n aristas es *denso* cuando $m = O(n^2)$ y *disperso*, cuando $m = O(n)$ o inclusive $O(n \log n)$.)

Sin importar la forma en que se mantenga un grafo G en la memoria, el grafo G normalmente se introduce en la computadora mediante su definición formal; es decir, como una colección de vértices y una colección de pares de vértices (aristas).

Matriz de adyacencia

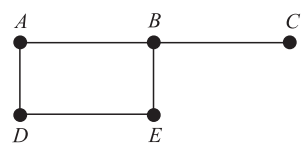
Suponga que G es un grafo con m vértices, y suponga que los vértices se han ordenado; por ejemplo, $v_1, v_2, \ldots, v_m$. Entonces la *matriz de adyacencia* $A = [a_{ij}]$ del grafo G es la matriz de $m \times m$ definida por

$$a_{ij} = \begin{cases} 1 & \text{si } v_i \text{ es adyacente a } v_j \\ 0 & \text{en otro caso} \end{cases}$$

La figura 8-27*b*) contiene la matriz de adyacencia del grafo G en la figura 8-27*a*), donde el orden de los vértices es A, B, C, D, E. Observe que cada arista $\{v_i, v_j\}$ de G está representado dos veces, por $a_{ij} = 1$ y $a_{ji} = 1$. Así, en particular, la matriz de adyacencia es simétrica.

La matriz de adyacencia A de un grafo G depende del orden de los vértices de G; es decir, un orden diferente de los vértices produce una matriz de adyacencia diferente. Sin embargo, dos matrices de adyacencia arbitrarias están estrechamente relacionadas en el sentido de que una puede obtenerse a partir de la otra al intercambiar simplemente renglones y columnas. Por otra parte, la matriz de adyacencia no depende del orden en que las aristas (pares de vértices) se introducen en la computadora.

Hay variantes de la representación anterior. Si G es un multigrafo, entonces usualmente se deja que a_{ij} denote el número de aristas $\{v_i, v_j\}$. Además, si G es un multigrafo ponderado, entonces puede dejarse que a_{ij} denote el peso de la arista $\{v_i, v_j\}$.



a)

	A	*B*	*C*	*D*	*E*
A	0	1	0	1	0
B	1	0	1	0	1
C	0	1	0	0	0
D	1	0	0	0	1
E	0	1	0	1	0

b)

Figura 8-27

Representación enlazada de un grafo *G*

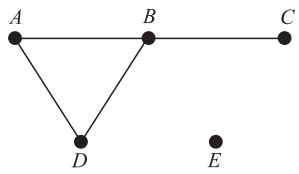
Sea *G* un grafo con *m* vértices. La representación de *G* en la memoria por medio de su matriz de adyacencia *A* presenta varias desventajas fundamentales. En primer lugar, puede ser difícil insertar o eliminar vértices en *G*. La razón es que puede ser necesario modificar el tamaño de *A* y reordenar los vértices, de modo que en la matriz *A* puede haber muchos, muchos cambios. Además, suponga que el número de aristas es $O(m)$ o inclusive $O(m \log m)$; es decir, suponga que *G* es disperso. Entonces la matriz *A* contiene muchos ceros; por tanto, se desperdicia bastante espacio de la memoria. En consecuencia, cuando *G* es disperso, *G* suele representarse en la memoria por medio de algún tipo de *representación enlazada*, también denominada *estructura de adyacencia*, que se describe a continuación mediante un ejemplo.

Considere el grafo *G* en la figura 8-28*a*). Observe que *G* puede definirse en forma equivalente por la tabla en la figura 8-28*b*), que muestra cada vértice en *G* seguido por su *lista de adyacencia*; es decir, su lista de vértices adyacentes (*vecinos*). Aquí el símbolo $\varnothing$ denota una lista vacía. Esta tabla también se representa en forma más breve como

$$G = [A{:}B, D; \quad B{:}A, C, D; \quad C{:}B; \quad D{:}A, B; \quad E{:}\varnothing]$$

donde dos puntos ":" separan un vértice de su lista de vecinos; y un punto y coma ";" separa las distintas listas.

Observación: Cada arista de un grafo *G* se representa dos veces en una estructura de adyacencia; es decir, cualquier arista , por ejemplo $\{A, B\}$, se representa por *B* en la lista de adyacencia de *A*, y también por *A* en la lista de adyacencia de *B*. El grafo *G* en la figura 8-28*a*) tiene cuatro aristas, de modo que en las listas de adyacencia debe haber 8 vértices. Por otra parte, cada vértice en una lista de adyacencia corresponde a una arista única en el grafo *G*.



a)

Vértice	Lista de adyacencia
A	*B*, *D*
B	*A*, *C*, *D*
C	*B*
D	*A*, *B*
E	$\varnothing$

b)

Figura 8-28

La *representación enlazada* de un grafo *G*, que mantiene a *G* en la memoria al usar sus listas de adyacencia, normalmente contiene dos archivos (o conjuntos de registros), uno denominado Vertex File y el otro denominado Edge File, como sigue.

a) ***Vertex File***: este archivo contiene la lista de vértices del grafo *G* que suelen mantenerse por medio de un arreglo o una lista ligada. Cada registro de este archivo tiene la forma

VERTEX	NEXT-V	PTR	

Aquí VERTEX es el nombre del vértice, NEXT-V apunta hacia el siguiente vértice en la lista de vértices en el Vertex File cuando los vértices se mantienen por medio de una lista ligada, y PTR apunta al primer elemento en la lista de adyacencia del vértice que aparece en el Edge File. El área sombreada indica que puede haber otra información en el registro correspondiente al vértice.

b) ***Edge File***: este archivo contiene las aristas del grafo *G*. Específicamente, el Edge File contiene todas las listas de adyacencia de *G*, donde cada lista se mantiene en la memoria por medio de una lista ligada. Cada registro del Edge File corresponde a un vértice en una lista de adyacencia y, entonces, indirectamente, a una arista en *G*. El registro suele tener la forma

EDGE	ADJ	NEXT	

Aquí:

1) EDGE es el nombre de la arista (en caso de tener una).
2) ADJ apunta a la ubicación del vértice en el Vertex File.
3) NEXT apunta a la ubicación del siguiente vértice en la lista de adyacencia.

Se recalca que cada arista está representada dos veces en el Edge File, pero cada registro del archivo corresponde a una arista única. El área sombreada indica que puede haber otra información en el registro correspondiente a la arista.

La figura 8-29 muestra cómo el grafo *G* en la figura 8-28*a*) puede aparecer en la memoria. Aquí los vértices de *G* se mantienen en la memoria por medio de una lista ligada que usa la variable START para apuntar hacia el primer vértice. (Una forma alterna para la lista de vértices es usar un arreglo lineal, y así NEXT-V no sería necesario.) Observe que el campo EDGE no es necesario aquí porque las aristas carecen de nombre. La figura 8-29 también muestra, con las flechas, la lista de adyacencia [*D*, *C*, *A*] del vértice *B*.

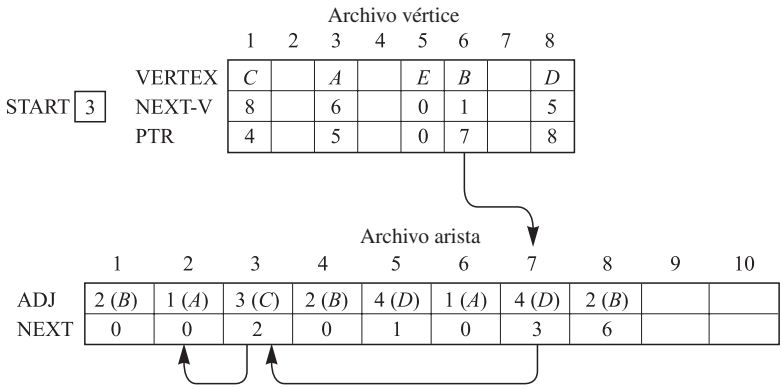
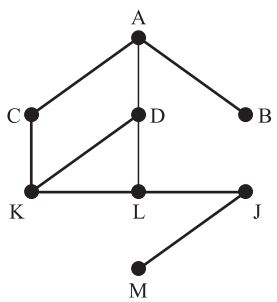


Figura 8-29

8.12 ALGORITMOS DE GRÁFICAS

En esa sección se analizan dos importantes algoritmos de grafos que examinan de manera sistemática los vértices y las aristas de un grafo *G*. Uno se denomina *búsqueda en profundidad* (DFS: depth-first search) y el otro, *búsqueda en anchura* (BFS: breadth-first search). Otros algoritmos de grafos se analizarán en el siguiente capítulo en relación con grafos dirigidos. Cualquier algoritmo de grafos particular puede depender de la forma en que *G* se mantiene en la memoria. Aquí se supone que *G* se mantiene en la memoria por medio de su lista de adyacencia. El grafo de prueba *G* con su estructura de adyacencia se muestra en la figura 8-30, donde se supone que los vértices están ordenados alfabéticamente.



a)

Vértice	Lista de adyacencia
A	B, C, D
B	A
C	A, K
D	A, K, L
J	L, M
K	C, D, L
L	D, J, K
M	J

b)

Figura 8-30

Durante la ejecución de los algoritmos, cada vértice (nodo) N de G se encuentra en uno de tres estados, denominados *status* de N, como sigue:

STATUS = 1: (Estado Ready) El estado inicial del vértice N.

STATUS = 2: (Estado Waiting) El vértice N está en una lista (de espera), en espera de ser procesado.

STATUS = 3: (Estado Processed) El vértice N ha sido procesado.

La lista de espera para la búsqueda en profundidad (DFS) será una STACK —modificada— (que se escribe horizontalmente con la parte superior de STACK a la izquierda) mientras que la lista de espera para la búsqueda en anchura (BFS) será una QUEUE.

Búsqueda en profundidad

La idea general detrás de una búsqueda en profundidad que empieza en un vértice inicial A es la siguiente: primero se procesa el vértice inicial A. Luego se procesa cada vértice N a lo largo de un camino P que empieza en A; es decir, se procesa un vecino de A, luego un vecino de A y así sucesivamente. Después de llegar a un "punto muerto"; es decir, a un vértice sin vecino no procesado, se retrocede en el camino P hasta que es posible continuar a lo largo de otro camino P'. Y así en lo sucesivo. El retroceso se logra usando una STACK para mantener los vértices iniciales de posibles caminos futuros. También se requiere un campo STATUS que indique el estado actual de cualquier vértice, de modo que ningún vértice sea procesado más de una vez.

El algoritmo de la búsqueda en profundidad (DFS) se muestra en la figura 8-31. El algoritmo procesa sólo aquellos vértices que están unidos al vértice inicial A; es decir, el componente conexo que incluye a A. Suponga que se desea procesar todos los vértices del grado G. Entonces es necesario modificar el algoritmo de modo que empiece de nuevo con otro vértice (que se denomina B) que aún se encuentre en el estado ready (STATE = 1). Este vértice B se obtiene al recorrer la lista de vértices.

Observación: La estructura STACK en el algoritmo anterior no es técnicamente una pila puesto que, en el paso 5*b*), se permite la eliminación de un vértice J que después se inserta enfrente de la pila. (Aunque se trata del mismo vértice J, suele representar una arista diferente en la estructura de adyacencia.) Si J no se elimina en el paso 5*b*), entonces se obtiene una forma alterna de la búsqueda en profundidad.

Algoritmo 8.5 (Búsqueda en profundidad): Este algoritmo ejecuta una búsqueda en profundidad sobre un grafo G; la búsqueda empieza con un vértice inicial A.

Paso 1. Todos los vértices se inicializan en el estado ready (STATUS = 1).

Paso 2. El vértice inicial se introduce sobre STACK y se cambia el estado de A al estado waiting (STATUS = 2).

Paso 3. Se repiten los pasos 4 y 5 hasta que STACK esté vacía.

Paso 4. Se saca el vértice superior N de STACK. Se procesa N y se hace STATUS (N) = 3, el estado processed.

Paso 5. Se analiza cada vecino J de N.

a) Si STATUS (J) = 1 (estado ready), J se introduce en STACK y se restablece STATUS (J) = 2 (estado waiting).

b) Si STATUS (J) = 2 (estado waiting), el J previo se elimina de STACK y el J actual se introduce en STACK.

c) Si STATUS (J) = 3 (estado processed), se ignora el vértice J.

[Fin del ciclo del paso 3].

Paso 6. Salir.

Figura 8-31

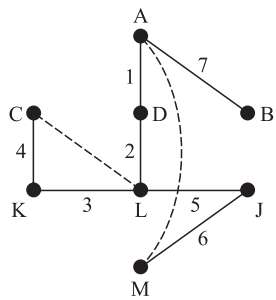
EJEMPLO 8.4 Suponga que el algoritmo 8.5 de búsqueda en profundidad en la figura 8-31 se aplica al grafo en la figura 8-30. Los vértices se procesan en el siguiente orden:

$$A, \quad D, \quad L, \quad K, \quad C, \quad J, \quad M, \quad B$$

En la figura 8-32*a*) se muestra la secuencia de los vértices que están en proceso y la secuencia de las listas de espera en STACK. (Observe que después que se procesa el vértice *A*, sus vecinos *B*, *C* y *D* se añaden a STACK en el orden primero *B*, luego *C* y por último *D*; por tanto, *D* está en la parte superior de STACK y *D* es el siguiente vértice que será procesado.) Cada vértice, excluyendo a *A*, proviene de una lista de adyacencia y entonces corresponde a una arista del grafo. Estas aristas constituyen un árbol de expansión de *G* que se muestra en la figura 8-32*b*). Los números indican el orden en que las aristas se agregan al árbol de expansión, y las líneas discontinuas indican retroceso.

STACK	Vértice
A	A
D, C, B	D
L, K, C, B	L
K, J, ~~K~~, C, B	K
C, J, ~~C~~, B	C
J, B	J
M, B	M
B	B
∅	

a)



b)

Figura 8-32

Búsqueda en anchura

La idea general detrás de una búsqueda en anchura que empieza en un vértice inicial *A* es la siguiente: primero se procesa el vértice inicial *A*. Luego se procesan todos los vecinos de *A*. Enseguida se procesan todos los vecinos de los vecinos de *A*. Lo natural es seguir la pista de los vecinos de un vértice, y es necesario garantizar que ningún vértice sea procesado dos veces. Esto se logra mediante el uso de una QUEUE para mantener los vértices que están en espera de ser procesados, y por un campo STATUS que indica el estado actual de un vértice.

El algoritmo de búsqueda en anchura (BFS) se muestra en la figura 8-33. De nuevo, el algoritmo sólo procesa los vértices que están unidos al vértice inicial *A*; es decir, el componente conexo incluyendo a *A*. Suponga que desea procesar todos los vértices en el grafo *G*. Entonces es necesario modificar el algoritmo de modo que empiece de nuevo con otro vértice (que se denomina *B*) que aún se encuentre en el estado ready (STATUS = 1). Este vértice *B* puede obtenerse recorriendo la lista de vértices.

EJEMPLO 8.5 Suponga que el algoritmo 8.6 de búsqueda en anchura (BFS) en la figura 8-33 se aplica al grafo en la figura 8-30. Los vértices se procesan en el siguiente orden:

$$A, \quad B, \quad C, \quad D, \quad K, \quad L, \quad J, \quad M$$

En la figura 8-34*a*) se muestra la secuencia de las listas de espera en QUEUE y la secuencia de los vértices que están siendo procesados. (Observe que después de procesar el vértice *A*, sus vecinos *B*, *C* y *D* se añaden a QUEUE en el orden primero *B*, luego *C* y por último *D*; por tanto, *B* está al frente de la QUEUE y así *B* es el siguiente vértice que será procesado.) De nuevo, cada vértice, excluyendo a *A*, proviene de una lista de adyacencia y, por tanto, corresponde a una arista del grafo. Estas aristas forman un árbol de expansión de *G* que se muestra en la figura 8-34*b*). Una vez más, los números indican el orden en que las aristas se agregan al árbol de expansión. Observe que este árbol de expansión es diferente al de la figura 8-32*b*), que proviene de una búsqueda en profundidad.

Algoritmo 8.6 (Búsqueda en anchura): Al empezar en un vértice inicial *A*, este algoritmo ejecuta una búsqueda en anchura sobre un grafo *G*.

Paso 1. Todos los vértices se inicializan en el estado ready (STATUS = 1).

Paso 2. El vértice inicial *A* se coloca en QUEUE y el estado de *A* se cambia al estado waiting (STATUS = 2).

Paso 3. Se repiten los pasos 4 y 5 hasta que QUEUE esté vacía.

Paso 4. Se elimina el vértice frontal *N* en QUEUE. Se procesa *N* y se hace STATUS (*N*) = 3, el estado processed.

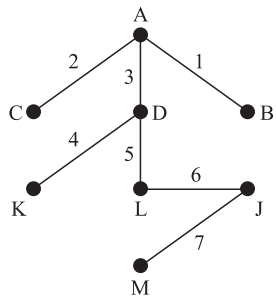
Paso 5. Se analiza cada vecino *J* de *N*.
a) Si STATUS (*J*) = 1 (estado ready), *J* se agrega a la parte trasera de QUEUE y se restablece STATUS (*J*) = 2 (estado waiting).
b) Si STATUS (*J*) = 2 (estado waiting) o STATUS(*J*) = 3 (estado processed), se ignora el vértice *J*.
[Fin del ciclo del paso 3].

Paso 6. Salir.

Figura 8-33

QUEUE	Vértice
A	A
D, C, B	B
D, C	C
D	D
L, K	K
L	L
J	J
M	M
∅	

a)



b)

Figura 8-34

8.13 EL PROBLEMA DEL AGENTE VIAJERO

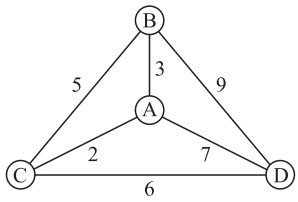
Sea *G* un grafo ponderado completo. (Los vértices de *G* se consideran ciudades y las aristas ponderadas de *G* las distancias entre las ciudades.) El "problema del agente viajero" busca encontrar un circuito hamiltoniano de peso mínimo para *G*.

Primero se observa el siguiente teorema, demostrado en el problema 8.33:

Teorema 8.13: El grafo completo K_n con $n \geq 3$ vértices tiene $H = (n-1)!/2$ circuitos hamiltonianos (donde no se distingue entre un circuito y su opuesto).

Considere el grafo ponderado completo *G* en la figura 8-35*a*). Tiene cuatro vértices, *A*, *B*, *C*, *D*. Por el teorema 8.13, tiene $H = 3!/2 = 3$ circuitos hamiltonianos. En el supuesto de que los circuitos empiezan en el vértice *A*, a continuación se muestran los tres circuitos y sus pesos:

$$\begin{aligned} |ABCDA| &= 3+5+6+7 = 21 \\ |ACDBA| &= 2+6+9+3 = 20 \\ |ACBDA| &= 2+5+9+7 = 23 \end{aligned}$$



a)

	P	Q	R	S	T
P		18	22	15	20
Q	18		11	12	22
R	22	11		16	10
S	15	12	16		13
T	20	22	10	13	

b)

Figura 8-35

Por tanto, *ACDBA* con peso 20 es el circuito hamiltoniano de peso mínimo.

El "problema del agente viajero" se resolvió para el grafo completo ponderado *G* en la figura 8-35*a*) al enumerar y determinar los pesos de sus tres posibles circuitos hamiltonianos. No obstante, para un grafo con muchos vértices, hacer lo anterior puede ser impráctico o incluso imposible. Por ejemplo, un grafo completo con 15 vértices tiene más de 40 millones de circuitos hamiltonianos. En consecuencia, para circuitos con muchos vértices, se requiere una estrategia para resolver o encontrar una solución aproximada al problema del agente viajero. A continuación se analiza uno de los algoritmos más simples.

Algoritmo del vecino más próximo

Este algoritmo, que empieza en un vértice dado, escoge la arista con peso mínimo hacia el siguiente vértice posible; es decir, al vértice "más próximo". Esta estrategia continúa en cada vértice sucesivo hasta que se completa un circuito hamiltoniano.

EJEMPLO 8.6 Sea *G* el grafo ponderado de la tabla en la figura 8-35*b*). Es decir, *G* tiene los vértices *P*, *Q*, . . . , *T*, y la distancia de *P* a *Q* es 18; la de *P* a *R* es 22 y así hasta que la distancia de *T* a *S* es 13. El algoritmo del vecino más próximo se aplica a *G* en *a*) *P*, *b*) *Q*.

a) Al empezar en *P*, el primer renglón de la tabla muestra que el vértice más próximo a *P* es *S* con distancia 15. El cuarto renglón muestra que el vértice más próximo a *S* es *Q* con distancia 12. El vértice más próximo a *Q* es *R* con distancia 11. Desde *R*, no hay ninguna opción más que dirigirse a *T* con distancia 10. Por último, desde *T*, no hay ninguna opción más que regresar a *P* con distancia 20. En consecuencia, el algoritmo del vecino más próximo empezando en *P* produce el siguiente circuito hamiltoniano ponderado:

$$|PSQRTP| = 15 + 12 + 11 + 10 + 20 = 68$$

b) Al empezar en *Q*, el vértice más próximo es *R* con distancia 11; desde *R*, el vértice más próximo es *T* con distancia 10; y desde *T* el vértice más próximo es *S* con distancia 13. Desde *S* es necesario ir hasta *P* con distancia 15 y, por último, desde *P* es necesario regresar a *Q* con distancia 18. En consecuencia, el algoritmo del vecino más próximo empezando en *Q* produce el siguiente circuito hamiltoniano ponderado:

$$|QRTSPQ| = 11 + 10 + 13 + 15 + 18 = 67$$

La idea detrás del algoritmo del vecino más próximo es minimizar el peso total al minimizar el peso en cada paso. Aunque esto puede parecer razonable, el ejemplo 8.6 muestra que no es posible obtener ningún circuito hamiltoniano de peso mínimo; es decir, puede no ser ambos 68 y 67. Sólo mediante la comprobación de todos los $H = (n - 1)!/2 = 12$ circuitos hamiltonianos de *G* es realmente posible saber cuál es el de peso mínimo. De hecho, el algoritmo del vecino más próximo empezando en *A* en la figura 8-35*a*) produce el circuito *ACBDA* que tiene el peso máximo. Sin embargo, el algoritmo del vecino más próximo suele proporcionar un circuito hamiltoniano relativamente próximo al de peso mínimo.

PROBLEMAS RESUELTOS

TERMINOLOGÍA DE GRAFOS

8.1 Considere el grafo G en la figura 8-36*a*).

a) Describir G formalmente; es decir, encontrar el conjunto $V(G)$ de vértices de G y el conjunto $E(G)$ de aristas de G.

b) Encontrar el grado de cada vértice y comprobar el teorema 8.1 para este grafo.

a) Hay cinco vértices, de modo que $V(G) = \{A, B, C, D, E\}$. Hay siete pares $\{x, y\}$ de vértices donde el vértice x está unido al vértice y; así

$$E(G) = [\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, E\}, \{C, D\}, \{C, E\}]$$

b) El grado de un vértice es igual al número de aristas a las que pertenece; por ejemplo, $\text{grd}(A) = 3$ puesto que A pertenece a las tres aristas $\{A, B\}$, $\{A, C\}$, $\{A, D\}$. En forma semejante,

$$\text{grd}(B) = 3, \quad \text{grd}(C) = 4, \quad \text{grd}(D) = 2, \quad \text{grd}(E) = 2$$

La suma de los grados es $3 + 3 + 4 + 2 + 2 = 14$, que es igual a dos veces el número de aristas.

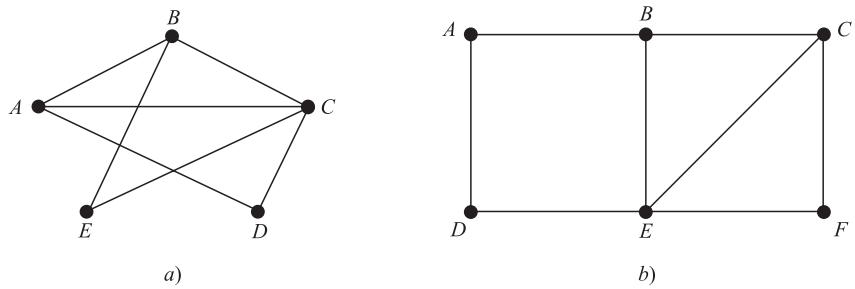


Figura 8-36

8.2 Considerar el grafo G en la figura 8-36*b*). Encontrar:

a) todos los caminos simples de A a F;
b) todos los recorridos de A a F;
c) $d(A, F)$, la distancia de A a F;
d) diám(G), el diámetro de G;
e) todos los ciclos que incluyen al vértice A;
f) todos los ciclos en G.

a) Un camino simple de A a F es una en la cual ningún vértice, y por tanto ninguna arista, se repite. Hay siete rutas así, cuatro que empiezan con las aristas $\{A, B\}$ y tres que empiezan con las aristas $\{A, D\}$:

$$(A, B, C, F), \quad (A, B, C, E, F), \quad (A, B, E, F), \quad (A, B, E, C, F),$$
$$(A, D, E, F), \quad (A, D, E, B, C, F), \quad (A, D, E, C, F).$$

b) Un recorrido de A a F es un camino tal que ninguna arista se repite. Hay nueve Recorridos así, los siete caminos simples de *a*) junto con

$$(A, D, E, B, C, E, F) \quad \text{y} \quad (A, D, E, C, B, E, F).$$

c) Hay un camino; por ejemplo, (A, B, C, F), de A a F de longitud 3 y ningún otro camino más corto de A a F; por tanto, $d(A, F) = 3$.

d) La distancia entre dos vértices cualesquiera no es mayor que 3, y la distancia de A a F es 3; por tanto, diám(G) = 3.

e) Un ciclo es un camino cerrado en la que no se repite ningún vértice (excepto el primero y el último). Hay tres ciclos que incluyen el vértice A:

$$(A, B, E, D, A), \quad (A, B, C, E, D, A), \quad (A, B, C, F, E, D, A).$$

f) En G hay seis ciclos; los tres en *e*) y

$$(B, C, E, B), \quad (C, F, E, C), \quad (B, C, F, E, B).$$

8.3 Considerar los multigrafos en la figura 8-37.

a) ¿Cuáles son conexos? Si un grafo no es conexo, encuentre sus componentes conexos.
b) ¿Cuáles son libres de ciclos (sin ciclos)?
c) ¿Cuáles son libres de lazos (sin lazos)?
d) ¿Cuáles son grafos (simples)?

a) Sólo 1) y 3) son conexos, 2) es inconexo; sus componentes conexos son $\{A, D, E\}$ y $\{B, C\}$; 4) es inconexo; sus componentes conexos son $\{A, B, E\}$ y $\{C, D\}$.

b) Sólo 1) y 4) son libres de ciclos. 2) tiene el ciclo (A, D, E, A), y 3) tiene el ciclo (A, B, E, A).

c) Sólo 4) tiene un lazo, que es $\{B, B\}$.

d) Sólo 1) y 2) son grafos. El multigrafo 3) tiene las aristas múltiples $\{A, E\}$ y $\{A, E\}$; y 4) tiene tanto las aristas múltiples $\{C, D\}$ y $\{C, D\}$ como un lazo $\{B, B\}$.

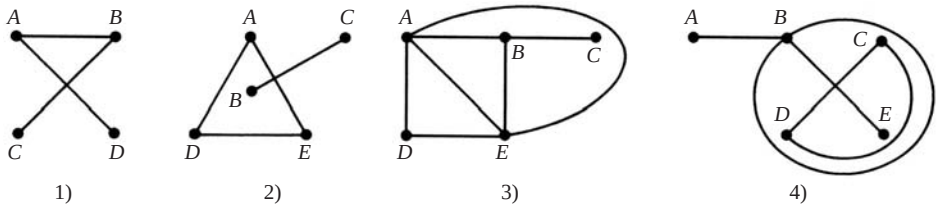


Figura 8-37

8.4 Sea G el grafo en la figura 8-38*a*). Encontrar:

a) todos los caminos simples de A a C;
b) todos los ciclos;
c) el subgrafo H generado por $V' = \{B, C, X, Y\}$;
d) $G - Y$;
e) todos los puntos de corte;
f) todos los puentes.

a) Hay dos caminos simples de A a C: (A, X, Y, C) y (A, X, B, Y, C).

b) Hay sólo un ciclo: (B, X, Y, B).

c) Como se muestra en la figura 8-38*b*), H consta de los vértices V' y el conjunto E' de todas las aristas cuyos puntos extremos pertenecen a V'; es decir, $E' = [\{B, X\}, \{X, Y\}, \{B, Y\}, \{C, Y\}]$.

d) Se eliminan el vértice Y de G y todas las aristas que contienen a Y para obtener el grafo $G - Y$ en la figura 8-38*c*). (Observe que Y es un punto de corte dado que $G - Y$ es inconexo.)

e) Los vértices A, X y Y son puntos de corte.

f) Una arista e es un puente si $G - e$ es inconexo. Así, hay tres puentes: $\{A, Z\}$, $\{A, X\}$ y $\{C, Y\}$.

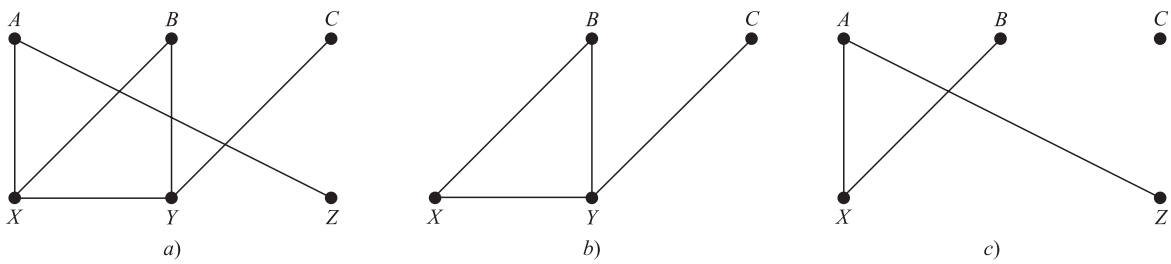


Figura 8-38

8.5 Considerar el grafo G en la figura 8-36*b*). Encontrar el subgrafo que resulta de eliminar cada vértice. ¿G tiene puntos de corte?

Cuando se elimina un vértice de G, también se eliminan todas las aristas que contienen al vértice. Los seis grafos obtenidos al eliminar cada uno de los vértices de G se muestran en la figura 8-39. Todos los seis grafos son conexos; así, ningún vértice es un punto de corte.

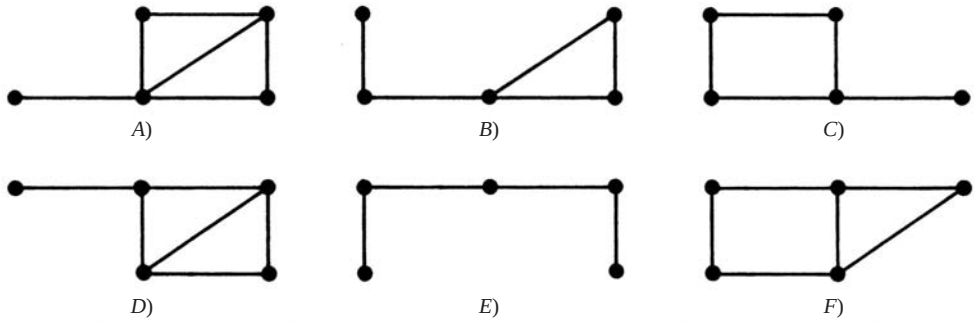


Figura 8-39

8.6 Demostrar que los seis grafos obtenidos en el problema 8.5 son distintos; es decir, que ningún par de ellos son isomorfos. Demostrar también que *B*) y *C*) son homeomorfos.

Los grados de los cinco vértices de cualquier grafo no pueden parearse con los grados de ningún otro grafo, excepto *B*) y *C*). Así, ninguno de los grafos es isomorfo, excepto quizá *B*) y *C*).

No obstante, si se elimina el vértice de grado 3 en *B*) y *C*), se obtienen subgrafos distintos. Por tanto, *B*) y *C*) tampoco son no isomorfos; en consecuencia, todos los seis grafos son distintos. Sin embargo, *B*) y *C*) son homeomorfos, puesto que es posible obtenerlos a partir de grafos isomorfos al agregar vértices idóneos.

GRÁFICAS RECORRIBLES, CIRCUITOS EULERIANOS Y HAMILTONIANOS

8.7 Considerar cada grafo en la figura 8-40. ¿Cuáles son recorribles; es decir, que tienen caminos eulerianos?

¿Cuáles son eulerianos; es decir, que tienen un circuito euleriano? Los que no sean eulerianos, explicar por qué.

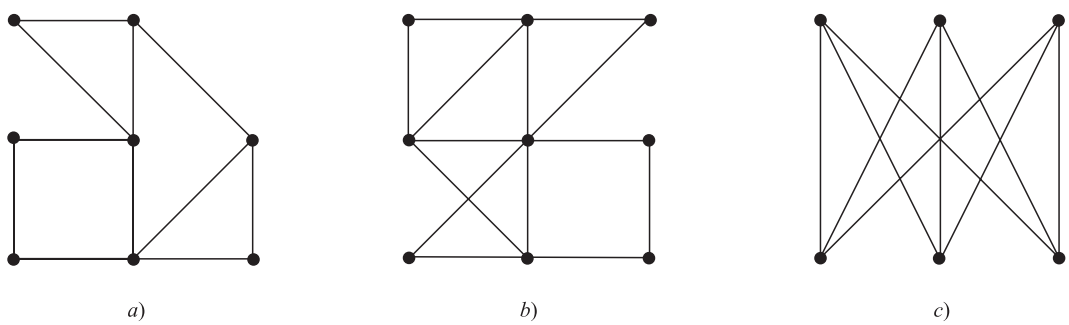


Figura 8-40

G es recorrible (tiene un camino euleriano) si sólo 0 o 2 vértices tienen grado impar, y G es euleriano (tiene un circuito euleriano) si todos los vértices son de grado par (teorema 8.3).

a) Es recorrible, puesto que hay dos vértices impares. El camino recorrible debe empezar en uno de los vértices impares y terminar en el otro;

b) Es recorrible, puesto que todos los vértices son pares. Por tanto, G tiene un circuito euleriano.

c) Debido a que los seis vértices son de grado impar, G no es recorrible.

8.8 ¿Cuáles de los grafos en la figura 8-40 tienen algún circuito hamiltoniano? En caso de no tenerlo, ¿por qué?

Los grafos *a*) y *c*) tienen circuitos hamiltonianos. (El lector debe poder encontrarlos fácilmente.) Sin embargo, el grafo *b*) no tiene ningún circuito hamiltoniano. Si α es un circuito hamiltoniano, entonces α debe unir el vértice de enmedio con el vértice inferior derecho, luego proceder a lo largo del renglón inferior hacia el vértice inferior derecho, luego verticalmente hacia el vértice derecho de enmedio, donde es obligado a retroceder hacia el vértice central antes de visitar los vértices restantes.

8.9 Demostrar el teorema 8.3 (de Euler). Un grafo conexo finito G es euleriano si y solo si todo vértice tiene grado par.

El supuesto es que G es Euleriano y que T es un recorrido cerrado de Euler. Para cualquier vértice v de G, el recorrido T entra y sale de v el mismo número de veces sin repetir ninguna arista. Así, el grado de v es par.

A la inversa, cada vértice de G tiene grado par. Se construye un recorrido euleriano. Se empieza un recorrido T_1 en cualquier arista e. T_1 se extiende al agregar una arista después de otra. Si T_1 no está cerrado en ningún paso, por ejemplo, T_1 empieza en u pero termina en $v \neq u$, entonces sólo un número impar de las aristas que inciden sobre v aparecen en T_1; por tanto, T_1 puede extenderse por medio de otra arista que incida en v. Así es posible continuar extendiendo T_1 hasta que T_1 regresa a su vértice inicial u; es decir, hasta que T_1 esté cerrado. Si T_1 incluye a todas las aristas de G, entonces T_1 es el recorrido euleriano buscado.

Ahora se considera que T_1 no incluye a todas las aristas de G; es el caso del grafo H que se obtiene al eliminar en G todas las aristas de T_1. Es posible que H no sea conexo, aunque cada vértice de H es de grado par, ya que T_1 contiene un número par de las aristas que inciden sobre cualquier vértice. Debido a que G es conexo, existe una arista e' de H que tiene un punto extremo u' en T_1. Se construye un recorrido T_2 en H que empiece en u' y que use e'. Puesto que todos los vértices en H son de grado par, es posible continuar extendiendo a T_2 en H hasta que T_2 regresa a u' como se muestra en la figura 8-41. Resulta evidente que T_1 y T_2 se colocan juntos para formar un recorrido cerrado más largo en G. Este proceso continúa hasta que se usan todas las aristas de G. Finalmente se obtiene un recorrido euleriano, de modo que G es euleriano.

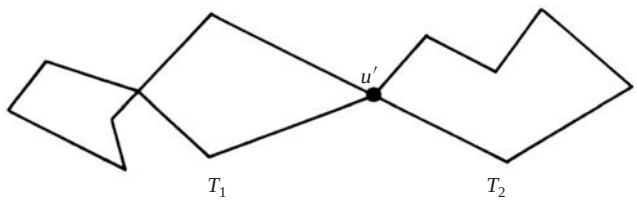


Figura 8-41

ÁRBOLES, ÁRBOLES DE EXPANSIÓN

8.10 Trazar todos los árboles que hay con exactamente seis vértices.

En la figura 8-42 hay seis árboles. El primero tiene un diámetro de 5, los dos siguientes un diámetro de 4, los dos siguientes de 3 y el último un diámetro de 2. Cualquier otro árbol con 6 nodos es isomorfo a alguno de estos árboles.

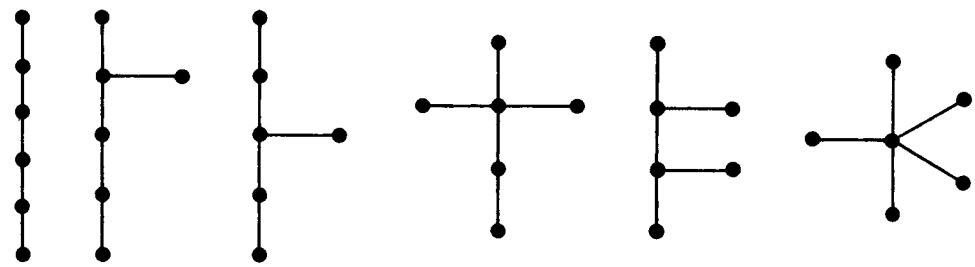
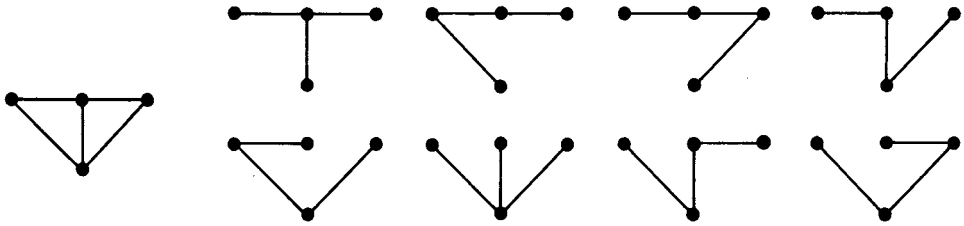


Figura 8-42

8.11 Encontrar todos los árboles de expansión del grafo G mostrada en la figura 8-43*a*).

Hay ocho árboles de expansión, como se muestra en la figura 8-43*b*). Cada árbol de expansión debe tener $4 - 1 = 3$ aristas, ya que G tiene cuatro vértices. Así, cada árbol puede obtenerse al eliminar dos de las cinco aristas de G. Esto puede hacerse



a) Grafo G *b*) Árboles de expansión

Figura 8-43

en 10 formas, excepto que dos de las formas producen grafos inconexos. Por tanto, los ocho árboles de expansión anteriores son todos los árboles de expansión de G.

8.12 Encontrar un árbol de expansión mínima T para el grafo ponderado G en la figura 8-44*a*).

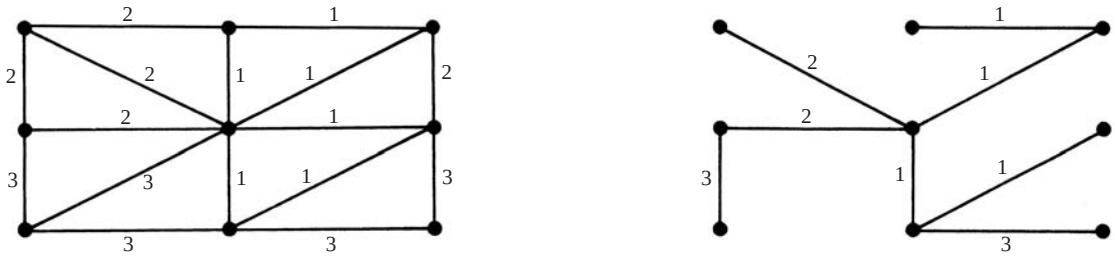


Figura 8-44

Puesto que G tiene $n = 9$ vértices, T debe tener $n - 1 = 8$ aristas. Se aplica el algoritmo 8.2; es decir, se eliminan las aristas con longitud máxima y sin desconectar el grafo hasta que sólo queden $n - 1 = 8$ aristas. En forma alterna, se aplica el algoritmo 8.3; es decir, empezando con los nueve vértices, se agregan aristas de longitud mínima y sin formar ningún ciclo hasta que se han agregado $n - 1 = 8$ aristas. Con ambos métodos se obtiene un árbol de expansión mínima como el que se muestra en la figura 8-44*b*).

8.13 Sea G un grafo con más de un vértice. Demostrar que las siguientes afirmaciones son equivalentes.

i) G es un árbol.
ii) Cada par de vértices está unido por exactamente un camino simple.
iii) G es conexo; pero $G - e$ es inconexo para cualquier arista e de G.
iv) G es libre de ciclos, pero si a G se agrega cualquier arista, entonces el grafo resultante tiene exactamente un ciclo.

i) *implica ii*). Sean u y v dos vértices en G. Puesto que G es un árbol, G es conexo, de modo que hay por lo menos un camino entre u y v. Por el problema 8.37, entre u y v sólo puede haber un camino simple; en caso contrario, G contiene un ciclo.

ii) *implica iii*). Si se elimina una arista $e = \{u, v\}$ de G, e es un camino de u a v. Entonces, si el grafo resultante $G - e$ tiene un camino P de u a v. Por tanto, P y e son dos caminos distintos de u a v, lo que contradice la hipótesis. Por consiguiente, en $G - e$ no puede haber ningún camino entre u y v, de modo que $G - e$ es inconexo.

iii) *implica iv*). Si en G hay un ciclo C que contiene una arista $e = \{u, v\}$; por hipótesis, G es conexo pero $G' = G - e$ es inconexo, donde u y v pertenecen a componentes distintos de G' (problema 8.41). Esto contradice que u y v son conexos por el camino $P = C - e$ que está en G'. Por tanto, G es libre de ciclos. Luego, sean x y y los vértices de G y sea H el grafo que se obtiene al adjuntar la arista $e = \{x, y\}$ a G. Debido a que G es conexo, en G hay una ruta P de x a y; por tanto, $C = Pe$ forma un ciclo en H. Ahora, si H contiene otro ciclo C', puesto que G es libre de ciclos, C' debe contener la arista e; por ejemplo, $C' = P'e$. Entonces P y P' son dos caminos simples en G de x a y. (Vea la figura 8-45.) Por el problema 8.37, G contiene un ciclo, lo que contradice que G es libre de ciclos. Por consiguiente, H sólo contiene un ciclo.

iv) *implica i*). Puesto que al agregar cualquier arista $e = \{x, y\}$ a G se obtiene un ciclo, los vértices x y y ya deben estar unidos en G. Así, G es conexo y por hipótesis G es libre de ciclos; es decir, G es un árbol.

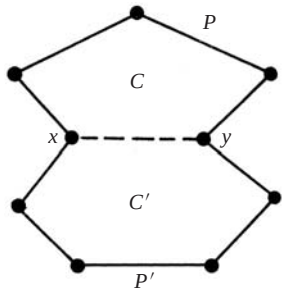


Figura 8-45

8.14 Demostrar el teorema 8.6: Sea G un grafo finito con $n \geq 1$ vértices. Entonces las afirmaciones siguientes son equivalentes. *i*) G es un árbol, *ii*) G es libre de ciclos y tiene $n - 1$ aristas, *iii*) G es conexo y tiene $n - 1$ aristas.

La demostración es por inducción sobre n. Ciertamente, el teorema es verdadero para el grafo con un solo vértice y que entonces no tiene aristas. Es decir, el teorema se cumple para $n = 1$. Ahora se supone que $n > 1$ y que el teorema es verdadero para grafos con menos de n vértices.

i) *implica ii*). Si G es un árbol, entonces G es libre de ciclos, de modo que sólo es necesario demostrar que G tiene $n - 1$ aristas. Por el problema 8.38, G tiene un vértice de grado 1. Al eliminar este vértice y su arista se obtiene un árbol T que tiene $n - 1$ vértices. El teorema se cumple para T, de modo que T tiene $n - 2$ aristas. Así, G tiene $n - 1$ aristas.

ii) *implica iii*). Si G es libre de ciclos y tiene $n - 1$ aristas. Sólo es necesario demostrar que G es conexo. Entonces, si G es inconexo y tiene k componentes, $T_1, \ldots, T_k$ que son árboles puesto que cada uno es conexo y libre de ciclos. Por ejemplo, T_i tiene n_i vértices donde $n_i < n$. Por tanto, el teorema se cumple para T_i, de modo que T_i tiene $n_i - 1$ aristas. Así,

$$n = n_1 + n_2 + \cdots + n_k$$

y

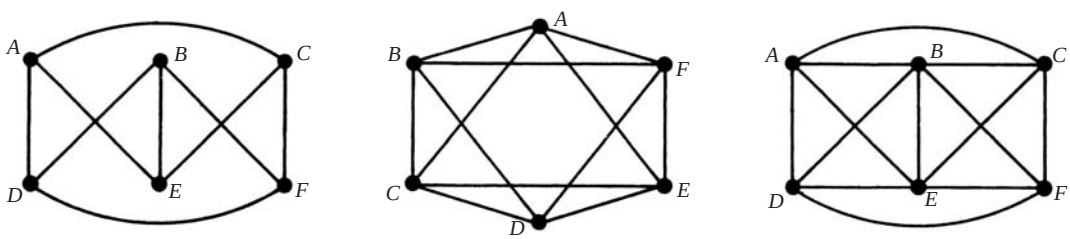
$$n - 1 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - k = n - k$$

Por consiguiente, $k = 1$. Pero esto contradice la hipótesis que G es inconexo y que tiene $k > 1$ componentes. En consecuencia, G es conexo.

iii) *implica i*). Si G es conexo y tiene $n - 1$ aristas, sólo es necesario demostrar que G es libre de ciclos. Al suponer que en G hay un ciclo que contiene una arista e. Al eliminar e se obtiene el grafo $H = G - e$ que también es conexo. Sin embargo, H tiene n vértices y $n - 2$ aristas, lo cual contradice el problema 8.39. En consecuencia, G es libre de ciclos y, por tanto, es un árbol.

GRAFOS PLANOS

8.15 Dibujar una representación plana, en caso de ser posible, de los grafos *a*), *b*) y *c*) de la figura 8-46.



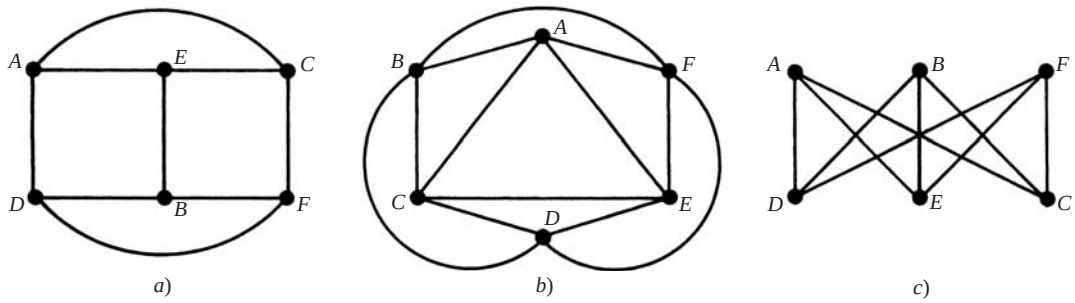
a) *b*) *c*)

Figura 8-46

a) Al volver a dibujar las posiciones de *B* y *E* se obtiene una representación plana del grafo como en la figura 8-47*a*).

b) No es el grafo estrella K_5. Éste tiene una representación plana del grafo como en la figura 8-47*b*).

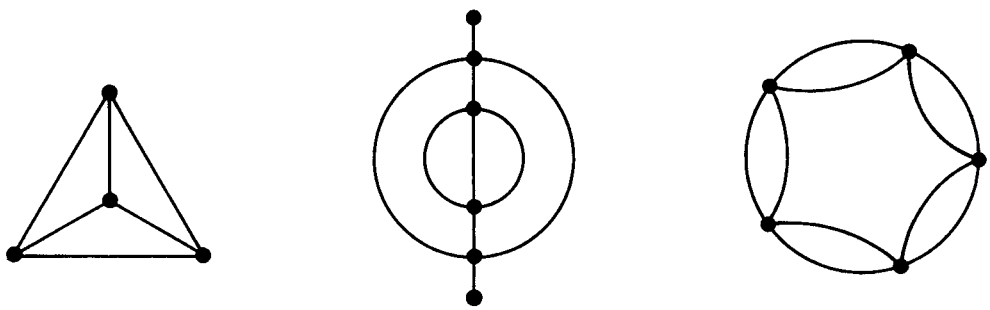
c) Este grafo no es plano. El grafo de servicios $K_{3,3}$ es un subgrafo como se muestra en la figura 8-47*c*), donde se han vuelto a dibujar las posiciones de *C* y *F*.



a) *b*) *c*)

Figura 8-47

8.16 Contar el número *V* de vértices, el número *E* de aristas y el número *R* de regiones de cada mapa en la figura 8-48, y comprobar la fórmula de Euler. También, encontrar el grado *d* de la región exterior.



a) *b*) *c*)

Figura 8-48

a) $V = 4$, $E = 6$, $R = 4$. Por tanto $V - E + R = 4 - 6 + 4 = 2$. También $d = 3$.

b) $V = 6$, $E = 9$, $R = 5$, de modo que $V - E + R = 6 - 9 + 5 = 2$. Aquí $d = 6$ puesto que dos aristas se contaron dos veces.

c) $V = 4$, $E = 10$, $R = 7$. Por tanto $V - E + R = 5 - 10 + 7 = 2$. Aquí $d = 5$.

8.17 Encontrar el número mínimo *n* de colores necesarios para pintar cada mapa en la figura 8-48.

a) $n = 4$; *b*) $n = 3$; *c*) $n = 2$.

8.18 Demostrar el teorema 8.8 (de Euler): $V - E + R = 2$.

Si el mapa conexo *M* consta de un solo vértice *P* como en la figura 8-49*a*), entonces $V = 1$, $E = 0$ y $R = 1$. Así, $V - E + R = 2$. En caso contrario, *M* puede establecerse a partir de un solo vértice por medio de las dos construcciones siguientes:

1) Se agrega un nuevo vértice Q_2, que se une a un vértice existente Q_1 por medio de una arista que no cruce ninguna arista existente como en la figura 8-49*b*).
2) Unir dos vértices existentes Q_1 y Q_2 mediante un arista *e* que no cruce ninguna arista existente como en la figura 8-49*c*).

Ninguna de estas operaciones modifica el valor de $V - E + R$. Por tanto, *M* tiene el mismo valor de $V - E + R$ que el mapa que consta de un solo vértice; es decir, $V - E + R = 2$. Por consiguiente, ya se demostró el teorema.

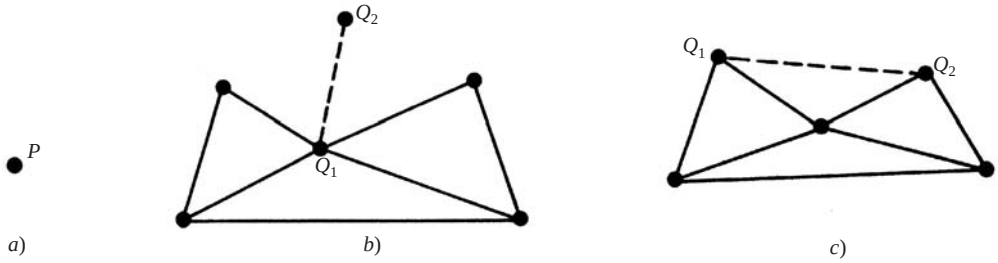


Figura 8-49

8.19 Demostrar el teorema 8.11: las afirmaciones siguientes son equivalentes para un grafo G: *i*) G es 2-coloreable. *ii*) G es bipartido. *iii*) Todo ciclo de G tiene longitud par.

i) *implica ii*). Si G es 2-coloreable, sea M el conjunto de vértices pintados con el primer color y N el conjunto de vértices pintados con el segundo color. Entonces M y N forman una partición bipartida de los vértices de G puesto que ninguno de los vértices de M y ninguno de los vértices de N pueden ser adyacentes entre sí porque son del mismo color.

ii) *implica iii*). Si G es bipartido y M y N forman una partición bipartida de los vértices de G, y si un ciclo empieza en un vértice u de, por ejemplo M, entonces irá a un vértice de N, y luego a un vértice de M, luego a uno de N y así continuará. En consecuencia, cuando el ciclo regresa a u debe ser de longitud par. Es decir, todo ciclo de G es de longitud par.

iii) *implica i*). Por último, si cualquier ciclo de G es de longitud par, se escoge un vértice en cada componente conexo y se pinta con el primer color, por ejemplo rojo. Luego, se pintan todos los vértices como sigue: si un vértice está pintado de rojo, entonces cualquier vértice adyacente se pinta con el segundo color, por ejemplo azul. Si un vértice está pintado de azul, entonces cualquier vértice adyacente a él se pinta de rojo. Debido a que todo ciclo es de longitud par, ningún vértice adyacente se pinta del mismo color. Por consiguiente, G es 2-coloreable y se ha demostrado el teorema.

8.20 Demostrar el teorema 8.12: un grafo plano G es 5-coloreable.

La demostración es por inducción sobre el número p de vértices de G. Si $p \leq 5$, entonces resulta evidente que el teorema se cumple. Ahora bien, si $p > 5$ y el teorema es verdadero para grafos con menos de p vértices; por el problema precedente, G tiene un vértice v tal que $\text{grd}(v) \leq 5$. Por inducción, el subgrafo $G - v$ es 5-coloreable. Ahora hay que suponer uno de tales coloreados: si los vértices adyacentes a v usan menos de los cinco colores, entonces simplemente v se pinta con uno de los colores restantes y se obtiene un 5-coloreado de G. Queda aún pendiente el caso en que v es adyacente a cinco vértices que están pintados con diferentes colores. Por ejemplo, los vértices, en sentido contrario al movimiento de las manecillas del reloj, adyacentes a v son $v_1, \ldots, v_5$ y están pintados con los colores $c_1, \ldots, c_5$. (Vea la figura 8-50*a*).)

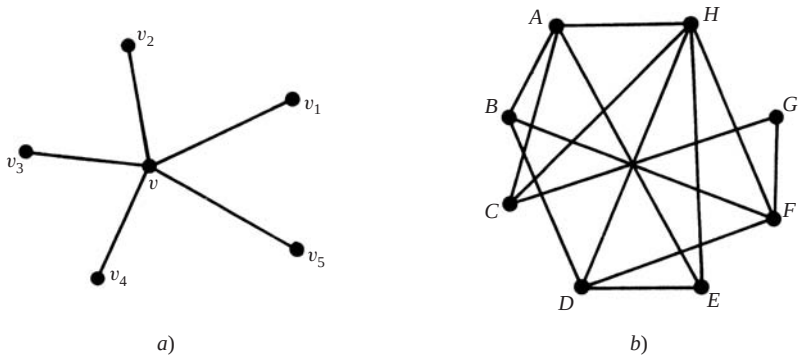


Figura 8-50

Luego se considera el subgrafo H de G generada por los vértices pintados con los colores c_1 y c_3, donde H incluye a v_1 y v_3. Si v_1 y v_3 pertenecen a componentes distintos de H, entonces es posible intercambiar los colores c_1 y c_3 en el componente que contiene a v_1 sin destruir el coloreado de $G - v$. Luego, v_1 y v_3 están pintados con c_3 y puede elegirse c_1 para pintar a v, y así se tiene un 5-coloreado de G. Por otra parte, si v_1 y v_3 pertenecen al mismo componente de H, entonces hay una ruta P de v_1 a v_3 cuyos vértices están pintados con c_1 o con c_3. La ruta P junto con las aristas $\{v, v_1\}$ y $\{v, v_3\}$ forman

un ciclo C que abarca ya sea a v_2 o a v_4. Luego se considera el subgrafo K generado por los vértices pintados con los colores c_3 o c_4. Debido a que C incluye a v_2 o a v_4, pero no a ambos, los vértices v_2 y v_4 pertenecen a componentes distintos de K. Por tanto, es posible intercambiar los colores c_2 y c_4 en el componente que contiene a v_2 sin destruir el coloreado de $G - v$. Entonces, v_2 y v_4 están pintados con el color c_4 y es posible escoger c_2 para pintar v y obtener un 5-coloreado de G. En consecuencia, G es 5-coloreable y se ha demostrado el teorema.

8.21 Aplicar el algoritmo 8.4, de Welch y Powell (figura 8-24), para pintar el grafo en la figura 8-50*b*).

Primero, los vértices se ordenan en orden decreciente de grado para obtener la secuencia

$$H, \quad A, \quad D, \quad F, \quad B, \quad C, \quad E, \quad G$$

Al proceder en secuencia, el primer color se usa para pintar los vértices H, B y luego G. (No es posible pintar A, D o F con el primer color porque cada uno está unido a H, y no es posible pintar C o E con el primer color porque cada uno está unido a H o a B.) Al continuar en secuencia con los vértices sin pintar, el segundo color se usa para pintar los vértices A y D. Los vértices restantes F, C y E pueden pintarse con el tercer color. Así, el número cromático n no puede ser mayor que 3. Sin embargo, en cualquier coloreado, H, D y E deben pintarse con colores diferentes, ya que están unidos entre sí. Por tanto, $n = 3$.

8.22 Sea G un grafo plano conexo finito con por lo menos tres vértices. Demostrar que G tiene por lo menos un vértice de grado 5 o menos.

Sean p el número de vértices y q el número de aristas de G, y se supone que $\text{grd}(u) \geq 6$ para cada vértice u de G. Sin embargo, $2q$ es igual a la suma de los grados de los vértices de G (teorema 8.1); así, $2q \geq 6p$. En consecuencia,

$$q \geq 3p > 3p - 6$$

Esto contradice el teorema 8.9. Por consiguiente, algún vértice de G tiene grado 5 o menos.

REPRESENTACIÓN SECUENCIAL DE GRAFOS

8.23 Encontrar la matriz de adyacencia $A = [a_{ij}]$ de cada grafo G en la figura 8-51.

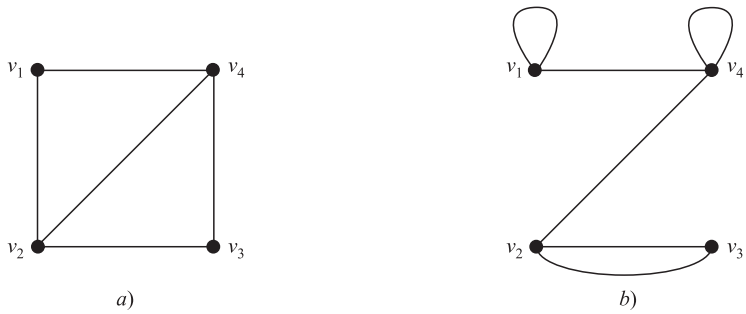


Figura 8-51

Sean $a_{ij} = n$ si hay n aristas $\{v_i, v_j\}$ y $a_{ij} = 0$ en caso contrario. Entonces:

$$a)\ A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \quad b)\ A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

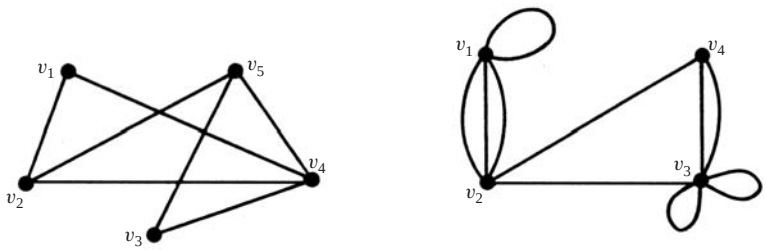
(Puesto que *a*) no tiene arista múltiples ni lazos, las entradas de A son 0 o 1, y son 0 en la diagonal).

8.24 Dibujar el grafo G correspondiente a cada matriz de adyacencia:

$$a)\ A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}; \quad b)\ A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

a) Puesto que A es una matriz cuadrada de 5×5, G tiene cinco vértices v_1, $v_2 \ldots$, v_5. Cuando $a_{ij} = 1$, se traza una arista de v_i a v_j. El grafo se muestra en la figura 8-52*a*).

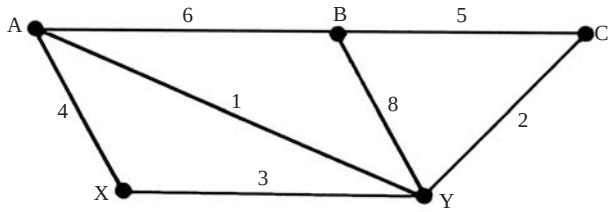
b) Puesto que A es una matriz cuadrada de 4×4, G tiene cuatro vértices $v_1, \ldots, v_4$. Cuando $a_{ij} = n$, se trazan n aristas de v_i a v_j. También, cuando $a_i = n$ se trazan n lazos en v_i. El grafo se muestra en la figura 8-52*b*).



a) *b*)

Figura 8-52

8.25 Encontrar la matriz de pesos $W = [w_{ij}]$ del grafo ponderado G en la figura 8-53*a*), donde los vértices están almacenados en el arreglo DATA como sigue: DATA: *A*, *B*, *C*, *X*, *Y*.



a)

$$W = \begin{bmatrix} 0 & 6 & 0 & 4 & 1 \\ 6 & 0 & 5 & 0 & 8 \\ 0 & 5 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 3 \\ 1 & 8 & 2 & 3 & 0 \end{bmatrix}$$

b)

Figura 8-53

Los vértices se numeran según la forma en que se almacenan en el arreglo DATA; así, $v_1 = A$, $v_2 = B, \ldots, v_5 = Y$. Luego se hace $W_{ij} = w$, donde w es el peso de la arista que va de v_i a v_j. Así se obtiene la matriz W en la figura 8-53*b*).

REPRESENTACIÓN ENLAZADA DE GRAFOS

8.26 Un grafo G con vértices $A, B, \ldots, F$ se almacena en la memoria mediante una representación enlazada con un archivo vértice y un archivo arista como en la figura 8-54.

a) Enumerar los vértices en el orden en que aparecen en la memoria.

b) Enumerar la lista de adyacencia ady(v) de cada vértice v de G.

a) Puesto que START = 4, la lista empieza con el vértice *D*. El NEXT-V indica dirigirse a 1(*B*), luego a 3(*F*), a 5(*A*), a 8(*E*) y a 7(*C*); es decir,

D, *B*, *F*, *A*, *E*, *C*

b) Aquí ady(D) = [5(A), 1(B), 8(E)]. Específicamente, PTR[4(D)] = 7 y ADJ[7] = 5(A) indican que ady(D) empieza con A. Luego, NEXT[7] = 3 y ADJ[3] = 1(B) indican que B es el siguiente vértice en ady(D). Luego, NEXT[3] = 10 y ADJ[10] = 8(E) indican que E es el siguiente vértice en ady(D). Sin embargo, NEXT[10] = 0 indica que ya no hay más vecinos de D. En forma semejante,

$$\text{ady}(B) = [A, D], \quad \text{ady}(F) = [E], \quad \text{ady}(A) = [B, D], \quad \text{ady}(E) = [C, D, F], \quad \text{ady}(C) = [E]$$

En otras palabras, la estructura de adyacencia de G es la siguiente:

$$G = [A{:}B, D; \quad B{:}A, D; \quad C{:}E; \quad D{:}A, B, E; \quad E{:}C, D, F; \quad F{:}E]$$

Archivo vértice

		1	2	3	4	5	6	7	8
	VERTEX	*B*		*F*	*D*	*A*		*C*	*E*
START 4	NEXT-V	3		5	1	8		0	7
	PTR	9		4	7	6		5	12

Archivo arista

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ADJ	4	4	1	8	8	1	5	3	5	8	4	7		
NEXT	8	0	10	0	0	2	3	0	11	0	0	1		

Figura 8-54

8.27 Dibujar el diagrama del grafo G cuya representación enlazada se muestra en la figura 8-54.

Para dibujar el grafo G en la figura 8-55 se usan la lista de vértices obtenida en el problema 8.26*a*) y las listas de adyacencia obtenidas en el problema 8.26*b*).

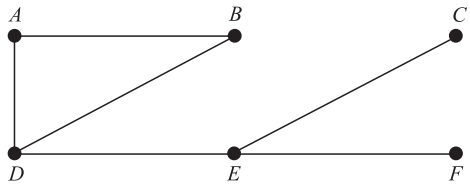


Figura 8-55

8.28 Mostrar la estructura de adyacencia (EA) del grafo G en la: *a*) figura 8-56*a*), *b*) figura 8-56*b*).

La estructura de adyacencia de un grafo G consta de las listas de adyacencia de los vértices, donde se usan dos puntos ":" para separar un vértice de su lista de adyacencia, y punto y coma ";" para separar las diversas listas. Así:

a) $G = [A{:}B, C, D; \quad B{:}A, C, E; \quad C{:}A, B, D, E; \quad D{:}A, C; \quad E{:}B, C]$

b) $G = [A{:}B, D; \quad B{:}A, C, E; \quad C{:}B, E, F; \quad D{:}A, E; \quad E{:}B, C, D, F; \quad F{:}C, E]$

ALGORITMOS DE GRAFOS

8.29 Considere el grafo G en la figura 8-56*a*) (donde los vértices están ordenados alfabéticamente).

a) Encontrar la estructura de adyacencia de G.

b) Encontrar el orden en que se procesan los vértices de G mediante un algoritmo DFS (búsqueda en profundidad) empezando en el vértice A.

a) Los vecinos de cada vértice se enumeran como sigue:

$$G = [A{:}B, C, D; \quad B{:}A, J; \quad C{:}A; \quad D{:}A, K; \quad J{:}B, K, M; \quad K{:}D, J, L; \quad L{:}K, M; \quad M{:}J, L]$$

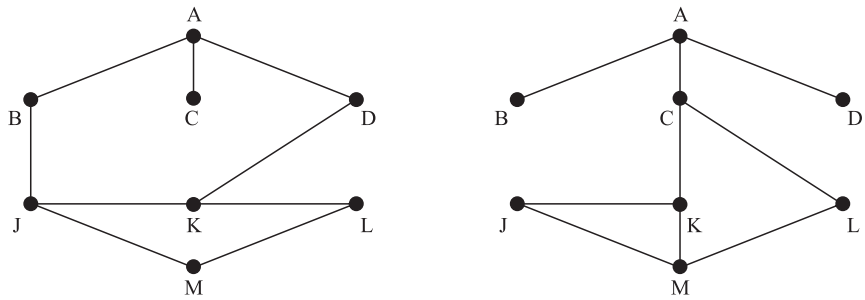


Figura 8-56

b) Durante el algoritmo de búsqueda en profundidad, se procesa el primer vértice *N* en STACK y los vecinos de *N* (que no se han procesado antes) se colocan sobre STACK. Al principio, el vértice inicial *A* se coloca sobre STACK. A continuación se muestra la secuencia de las listas de espera en STACK y los vértices que están en proceso:

STACK	*A*	*DCB*	*KCB*	*LJCB*	*MJCB*	*JCB*	*CB*	*B*	$\varnothing$
Vértice	*A*	*D*	*K*	*L*	*M*	*J*	*C*	*B*	

En otras palabras, los vértices se procesan en el orden: *A, D, K, L, M, J, C, B.*

8.30 Repetir el problema 8.29 para el grafo *G* en la figura 8-56*b*).

a) Los vecinos de cada vértice se enumeran como sigue:

$$G = [A{:}B, C, D; \quad B{:}A; \quad C{:}A, K, L; \quad D{:}A; \quad J{:}K, M; \quad K{:}C, J, M; \quad L{:}C, M; \quad M{:}J, K, L]$$

b) A continuación se muestra la secuencia de las listas de espera en STACK y los vértices que están en proceso:

STACK	*A*	*DCB*	*CB*	*LKB*	*MKB*	*KJB*	*JB*	*B*	$\varnothing$
Vértice	*A*	*D*	*C*	*L*	*M*	*K*	*J*	*B*	

En otras palabras, los vértices se procesan en el orden: *A, D, C, L, M, K, J, B.*

8.31 Si se empieza en el vértice *A* y se usa un algoritmo de búsqueda en anchura, encontrar el orden en que se procesan los vértices para el grafo *G* en la: *a*) figura 8-56*a*), *b*) figura 8-56*b*).

a) La estructura de adyacencia de *G* se muestra en el problema 8-29. Durante la ejecución del algoritmo de búsqueda en profundidad, se procesa el primer vértice *N* en QUEUE y luego a QUEUE se agregan los vecinos de *N* (que no habían aparecido antes). Al principio, el vértice inicial *A* se asigna a QUEUE. A continuación se muestra la secuencia de las listas de espera en QUEUE y los vértices que están en proceso:

QUEUE	*A*	*DCB*	*JDC*	*JD*	*KJ*	*MK*	*LM*	*L*	$\varnothing$
Vértice	*A*	*B*	*C*	*D*	*J*	*K*	*M*	*L*	

En otras palabras, los vértices se procesan en el orden: *A, B, C, D, J, K, M, L.*

b) La estructura de adyacencia de *G* aparece en el problema 8.30. A continuación se muestra la secuencia de las listas de espera en QUEUE y los vértices que están en proceso:

QUEUE	*A*	*DCB*	*DC*	*LKD*	*LK*	*MJL*	*MJ*	*M*	$\varnothing$
Vértice	*A*	*B*	*C*	*D*	*K*	*L*	*J*	*M*	

En otras palabras, los vértices se procesan en el orden: *A, B, C, D, K, L, J, M*.

EL PROBLEMA DEL AGENTE VIAJERO

8.32 Aplicar el algoritmo del vecino más próximo al grafo ponderado completo *G* en la figura 8-57, empezando en el: *a*) vértice *A*; *b*) vértice *B*.

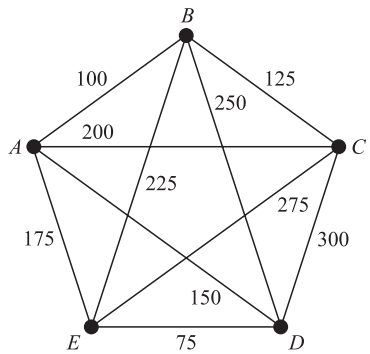


Figura 8-57

a) Al empezar en *A* el vértice más próximo es *B*, con distancia 100; desde *B* el más próximo es *C*, con distancia 125; y desde *C* el más próximo es *E*, con distancia 275. Desde *E* es necesario ir a *D* con distancia 75 y, finalmente, desde *D* es necesario retroceder hacia *A* con distancia 150. En consecuencia, el algoritmo del vecino más próximo al empezar en *A*, produce el siguiente circuito hamiltoniano ponderado:

$$|ABCEDA| = 100 + 125 + 275 + 75 + 150 = 725$$

b) Al empezar en *D*, es necesario ir hacia *E*, luego hacia *A*, de ahí hacia *B*, luego hacia *C* y finalmente de regreso a *D*. En consecuencia, el algoritmo del vecino más próximo al empezar en *D*, produce el siguiente circuito hamiltoniano ponderado:

$$|DEABCD| = 75 + 175 + 100 + 125 + 300 = 775$$

8.33 Demostrar el teorema 8.13. El grafo completo K_n con $n \geq 3$ vértices tiene $H = (n-1)!/2$ circuitos hamiltonianos.

La convención para el conteo de circuitos hamiltonianos permite designar cualquier vértice en un circuito como el punto inicial. A partir del punto inicial es posible ir a cualquiera de los $n-1$ vértices, y de ahí a cualquiera de los $n-2$ vértices y así hasta que se llega al último vértice y luego se regresa al punto inicial. Por el principio de conteo básico, hay un total de $(n-1)(n-2)\cdots 2\cdot 1 = (n-1)!$ circuitos que pueden formarse a partir de un punto inicial. Para $n \geq 3$, cualquier circuito puede parearse con uno en la dirección opuesta que determine el mismo circuito hamiltoniano. En consecuencia, hay un total de $H = (n-1)!/2$ circuitos hamiltonianos.

PROBLEMAS SUPLEMENTARIOS

TERMINOLOGÍA DE GRAFOS

8.34 Considere el grafo G en la figura 8-58. Encuentre:

a) el grado de cada vértice (y compruebe el teorema 8.1);
b) todos los caminos simples de A a L;
c) todos los recorridos (aristas distintas) de B a C;
d) $d(A, C)$, la distancia de A a C;
e) diám(G), el diámetro de G.

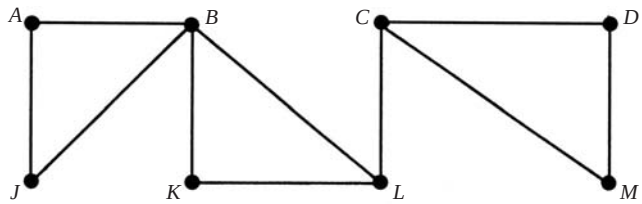


Figura 8-58

8.35 Considere el grafo en la figura 8-58. Encuentre (en caso de haberlos): *a*) todos los ciclos; *b*) todos los puntos de corte; *c*) todos los puentes.

8.36 Considere el grafo en la figura 8-58. Encuentre el subgrafo $H = H(V', E')$ de G, donde V' es igual a:

a) $\{B, C, D, J, K\}$ *b*) $\{A, C, J, L, M\}$ *c*) $\{B, D, J, M\}$ *d*) $\{C, K, L, M\}$

¿Cuáles son isomorfos y cuáles son homeomorfos?

8.37 Suponga que un grafo G contiene dos caminos distintos de un vértice u a un vértice v. Demuestre que G tiene un ciclo.

8.38 Suponga que G es un grafo finito libre de ciclos con por lo menos una arista. Demuestre que G tiene por lo menos dos vértices de grado 1.

8.39 Demuestre que un grafo conexo G con n vértices debe tener por lo menos $n - 1$ aristas.

8.40 Encuentre el número de grafos conexos que hay con cuatro vértices. (Dibújelos.)

8.41 Sea G un grafo conexo. Demuestre:

a) Si en G hay un ciclo C que contiene una arista e, entonces $G - e$ sigue siendo conexo.
b) Si $e = \{u, v\}$ es una arista tal que $G - e$ es inconexo, entonces u y v pertenecen a componentes distintos de $G - e$.

8.42 Suponga que G tiene V vértices y E aristas. Sean M y m que denotan, respectivamente, el máximo y el mínimo de los grados de los vértices en G. Demuestre que $m \leq 2E/V \leq M$.

8.43 Considere los dos pasos siguientes en un grafo G: 1) Eliminar una arista. 2) Eliminar un vértice y todas las aristas que contienen a ese vértice. Demostrar que todo subgrafo H de un grafo finito G puede obtenerse mediante una secuencia que consta de estos dos pasos.

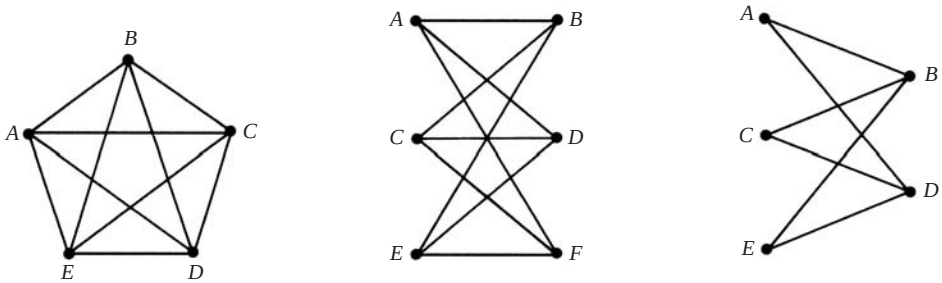
GRAFOS RECORRIBLES, CIRCUITOS EULERIANOS Y HAMILTONIANOS

8.44 Considere las grafos K_5, $K_{3,3}$ y $K_{2,3}$ en la figura 8-59. Encuentre un camino euleriano (recorrible) o un circuito euleriano de cada grafo, si existe. En caso de no existir, explique por qué.

8.45 Considere cada grafo en la figura 8-59. Encuentre un camino o un circuito hamiltoniano, si existe. En caso de no existir, explique por qué.

8.46 Demuestre que K_n tiene $H = (n - 1)!/2$ circuitos hamiltonianos. En particular, encuentre el número de circuitos hamiltonianos para el grafo K_5 en la figura 8-59*a*).

8.47 Suponga que G y G^* son grafos homeomorfos. Demuestre que G es recorrible (euleriano) si y sólo si G^* es recorrible (euleriano).



a) *b*) *c*)

Figura 8-59

GRAFOS ESPECIALES

8.48 Dibuje dos grafos 3-regular con *a*) ocho vértices; *b*) nueve vértices.

8.49 Considere el grafo completo K_n.

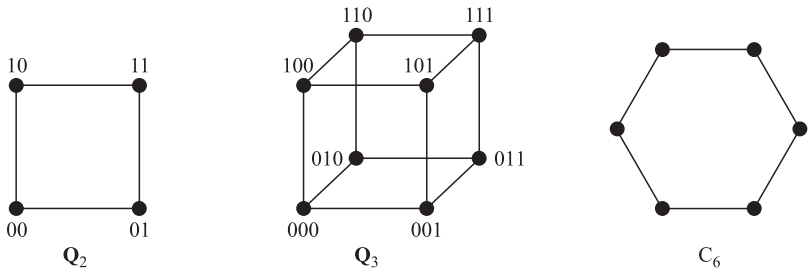
a) Encuentre el diámetro de K_n.
b) Encuentre el número m de aristas en K_n.
c) Encuentre el grado de cada vértice en K_n.
d) Encuentre los valores de n para los que K_n es: *i*) recorrible; *ii*) regular.

8.50 Considere el grafo completo $K_{m,n}$.

a) Encuentre el diámetro de $K_{m,n}$.
b) Encuentre el número E de aristas en $K_{m,n}$.
c) Encuentre los $K_{m,n}$ que son recorribles.
d) ¿Cuáles de los grafos $K_{m,n}$ son isomorfos y cuáles son homeomorfos?

8.51 El *n-cubo*, denotado por $\mathbf{Q}_n$, es el grafo cuyos vértices son las 2^n cadenas de bits de longitud n, y donde dos vértices son adyacentes si sólo difieren por una posición. En las figuras 8-60*a*) y *b*) se muestran los n-cubos $\mathbf{Q}_2$ y $\mathbf{Q}_3$.

a) Encuentre el diámetro de $\mathbf{Q}_n$.
b) Encuentre el número m de aristas en $\mathbf{Q}_n$.
c) Encuentre el grado de cada vértice en $\mathbf{Q}_n$.
d) Encuentre los valores de n para los que $\mathbf{Q}_n$ es recorrible.
e) Encuentre un circuito hamiltoniano (denominado *código Gray*) para *i*) $\mathbf{Q}_3$; *ii*) $\mathbf{Q}_4$.



a) *b*) *c*)

Figura 8-60

8.52 El *n-ciclo*, denotado por C_n, es el grafo que consta de un solo ciclo de longitud n. En la figura 8-60*c*) se muestra el 6-ciclo C_6. *a*) Encuentre el número de vértices y aristas en C_n. *b*) Encuentre el diámetro de C_n.

8.53 Describa los grafos conexos que son bipartidos y regulares.

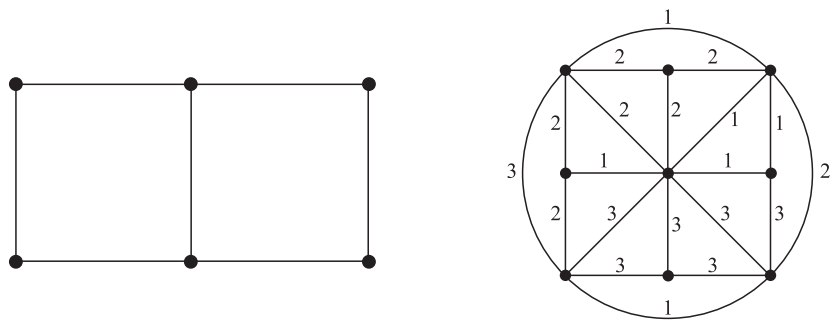
ÁRBOLES

8.54 Dibuje todos los árboles con cinco vértices o menos.

8.55 Encuentre el número de árboles con siete vértices.

8.56 Encuentre el número de árboles de expansión en la figura 8-61*a*).

8.57 Encuentre el peso de un árbol de expansión mínima en la figura 8-61*b*).



a) *b*)

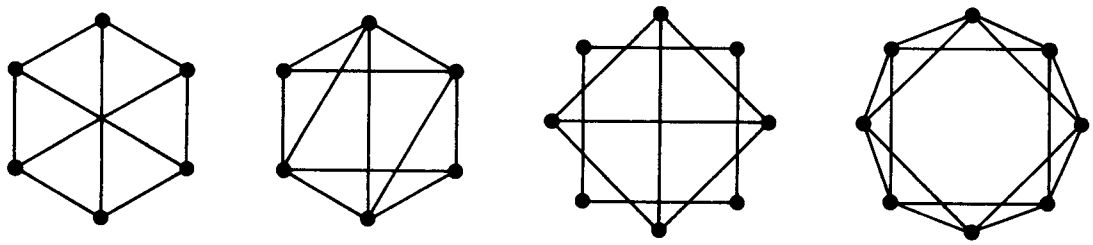
Figura 8-61

8.58 Demuestre que cualquier árbol es un grafo bipartido.

8.59 ¿Cuáles grafos bipartidos completos $K_{m,n}$ son árboles?

GRAFOS PLANAS, MAPAS, COLOREADOS

8.60 De ser posible dibuje una representación plana de cada grafo G en la figura 8-62; en caso contrario, demuestre que tiene un subgrafo homeomorfo a K_5 o a $K_{3,3}$.



a) *b*) *c*) *d*)

Figura 8-62

8.61 Demuestre que el 3-cubo Q_3 [figura 8-60*b*)] es plano.

8.62 Para el mapa en la figura 8-63, encuentre el grado de cada región y compruebe que la suma de los grados de las regiones es igual al doble del número de aristas.

8.63 Cuente el número V de vértices, el número E de aristas y el número R de regiones de cada uno de los mapas en la figura 8-64, y compruebe la fórmula de Euler.

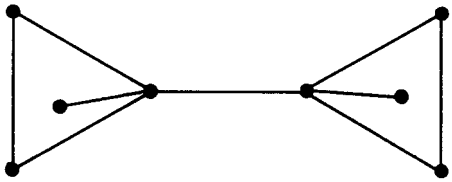
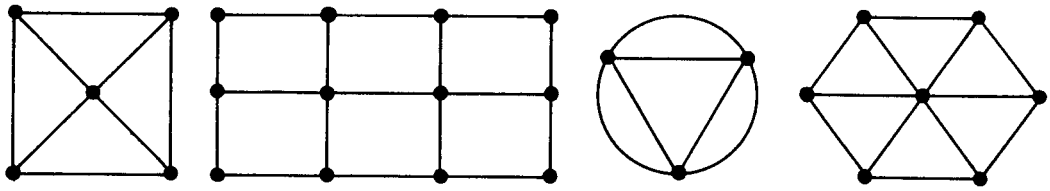


Figura 8-63



a) *b*) *c*) *d*)

Figura 8-64

8.64 Encuentre el número mínimo de colores necesarios para pintar las regiones de cada mapa en la figura 8-64.

8.65 Dibuje el mapa dual a cada mapa en la figura 8-64.

8.66 Aplique el algoritmo de Welch y Powell para pintar cada grafo en la figura 8-65. Encuentre el número cromático *n* del grafo.

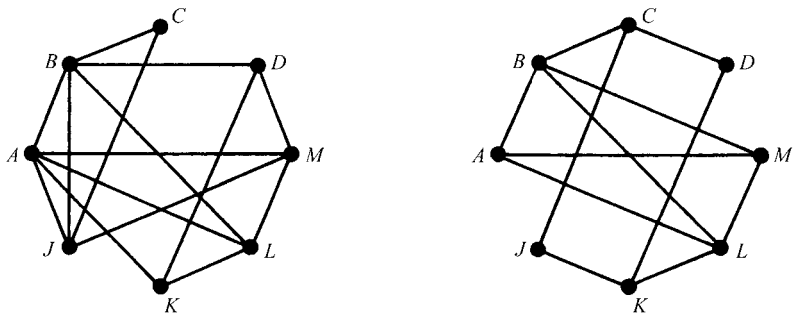


Figura 8-65

REPRESENTACIÓN SECUENCIAL DE GRAFOS

8.67 Encuentre la matriz de adyacencia *A* de cada multigrafo en la figura 8-66.

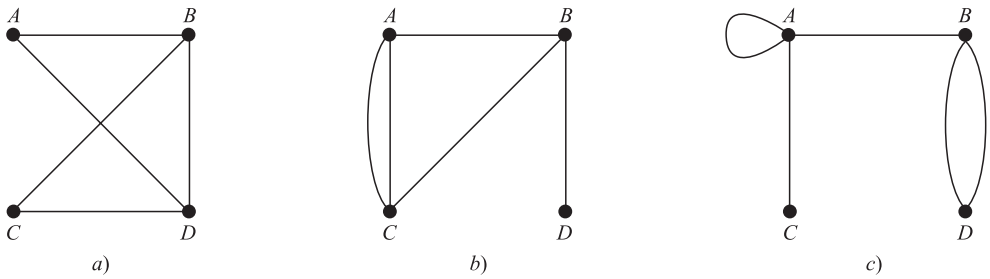


Figura 8-66

8.68 Dibuje el multigrafo G correspondiente a cada una de las siguientes matrices de adyacencia:

$$a)\ A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \quad b)\ A = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 2 \end{bmatrix}$$

8.69 Suponga que un grafo G es bipartido. Demuestre que es posible ordenar los vértices de G de modo que su matriz de adyacencia A tenga la forma: $A = \begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$

REPRESENTACIÓN ENLAZADA DE GRAFOS

8.70 Suponga que un grafo G se almacena en la memoria como en la figura 8-67.

Archivo vértice

		1	2	3	4	5	6	7	8
START 7	VERTEX	*C*		*F*	*E*	*A*		*B*	*D*
	NEXT-V	0		5	1	8		3	4
	PTR	2		11	6	12		4	1

Archivo arista

	1	2	3	4	5	6	7	8	9	10	11	12
ADJ	7	7	4	5		7	1		8	3	1	7
NEXT	0	10	0	7		0	9		3	0	0	0

Figura 8-67

a) Enumere los vértices en el orden en que aparecen en la memoria.

b) Encuentre la estructura de adyacencia de G; es decir, encuentre la lista de adyacencia ady(v) de cada vértice v de G.

8.71 Muestre la estructura de adyacencia (*EA*) para cada grafo G en la figura 8-59.

8.72 En la figura 8.68*a*) se muestra un grafo G que representa seis ciudades $A, B, \ldots, F$ unidas por siete autopistas numeradas 22, 33, …, 88. Muestre la forma en que G puede mantenerse en la memoria mediante una presentación ligada con arreglos ordenados para las ciudades y las autopistas numeradas. (Observe que VERTEX es un arreglo ordenado, de modo que el campo NEXT-V no es necesario).

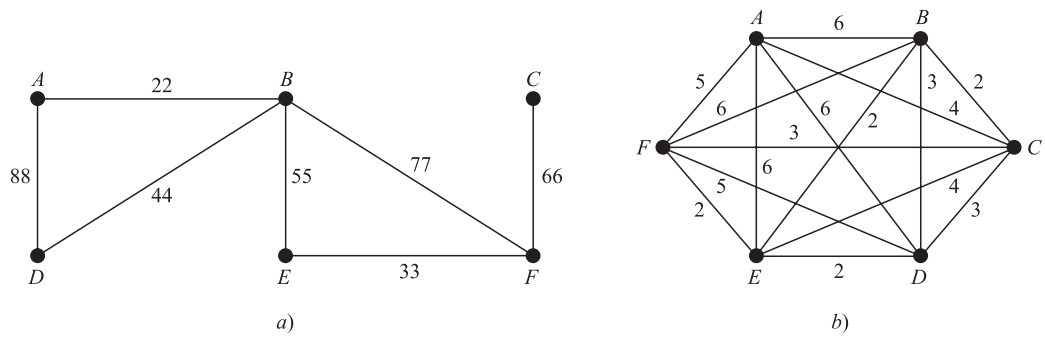


Figura 8-68

PROBLEMA DEL AGENTE VIAJERO

8.73 Aplique el algoritmo del vecino más próximo al grafo ponderado completo G en la figura 8-68*b*) empiece en: *a*) el vértice A; *b*) el vértice$B$.

8.74 Considere el graf ponderado completo G en la figura 8-57 con 5 vértices.

a) Empiece en el vértice A y enumere los $H = (n-1)!/2 = 12$ circuitos hamiltonianos de G, y encuentre el peso de cada uno.

b) Encuentre un circuito hamiltoniano de peso mínimo.

ALGORITMOS DE GRAFS

8.75 Considere el grafo G en la figura 8-57 (donde los vértices están ordenados alfabéticamente).

a) Encuentre la estructura de adyacencia (EA) de G.

b) Use el algoritmo de búsqueda en profundidad 8.5 sobre G, empiece en el vértice C, encuentre la secuencia STACK y el orden en que se procesan los vértices.

c) Repita el inciso *b*); ahora empiece en el vértice K.

8.76 Use el algoritmo de búsqueda en anchura 8.6 sobre el grafo G en la figura 8-57 para encontrar la secuencia QUEUE y el orden en que se procesan los vértices, empiece en: *a*) vértice C; *b*) vértice K.

8.77 Repita el problema 8.75 para el grafo G en la figura 8-65*a*).

8.78 Repita el problema 8.76 para el grafo G en la figura 8-65*a*).

8.79 Repita el problema 8.75 para el grafo G en la figura 8-65*b*).

8.80 Repita el problema 8.76 para el grafo G en la figura 8-65*b*).

Respuestas a los problemas suplementarios

8.34 *a*) 2, 4, 3, 2, 2, 2, 3, 2; *b*) $ABL, ABKL, AJBL, AJBKL$; *c*) $BLC, BKLC, BAJBLC, BAJBKLC$; *d*) 3; *e*) 4.

8.35 *a*) $AJBA, BKLB, CDMC$; *b*) B, C, L; *c*) sólo $\{C, L\}$.

8.36 *a*) $E' = \{BJ, BK, CD\}$; *b*) $E' = \{AJ, CM, LC\}$; *c*) $E' = \{BJ, DM\}$; *d*) $E' = \{KL, LC, CM\}$. También, *a*) y *b*) son isomorfos, y *a*), *b*) y *c*) son homeomorfos.

8.38 *Sugerencia*: Considere un camino simple máximo α, y demuestre que sus puntos extremos tienen grado 1.

8.40 Hay cinco de ellos, como se muestra en la figura 8-69.

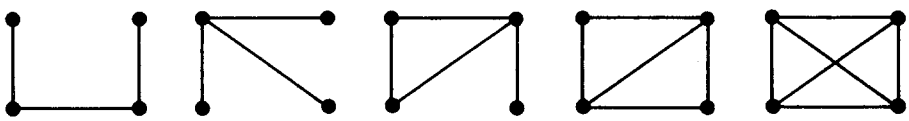


Figura 8-69

8.42 *Sugerencia*: Use el teorema 8.1.

8.43 Primero elimine todas las aristas en G que no están en H; luego, elimine todos los vértices en G que no están en H.

8.44 *a*) euleriano, puesto que todos los vértices son pares: $ABCDEACEBDA$. *b*) Ninguno, puesto que cuatro vértices son impares. *c*) Camino euleriano que empieza en B y termina en D (o viceversa): $BADCBED$.

8.45 *a*) $ABCDEA$; *b*) $ABCDEFA$; *c*) ninguno, puesto que B o D deben visitarse dos veces en cualquier camino cerrado que incluya todos los vértices.

8.46 $(5-1)!/2 = 12$.

8.47 *Sugerencia*: Agregar un vértice al dividir una arista no modifica el grado de los vértices originales y simplemente agrega un vértice de grado par.

8.48 *a*) Los dos grafos 3-regular en la figura 8-70 no son isomorfos; *b*) tiene un 5-ciclo, pero *a*) no. *b*) No hay ninguno. La suma de los grados de un grafo r-regular con s vértices es igual a rs, y rs debe ser par.

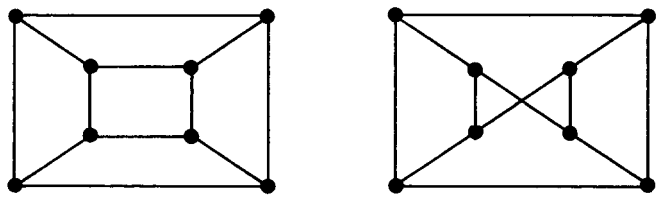


Figura 8-70

8.49 *a*) diám$(K_1) = 0$; todas las demás tienen diámetro 1; *b*) $m = C(n, 2) = n(n-1)/2$; *c*) $n-1$; *d*) *i*) $n = 2$ y n impar; *ii*) toda n.

8.50 *a*) diám$(K_{1,1}) = 1$; todas las demás tienen diámetro 2; *b*) $E = mn$; *c*) $K_{1,1}$ y $K_{1,2}$, y todo $K_{m,n}$ donde m y n sean pares; *d*) ninguno es isomorfo; sólo $K_{1,1}$ y $K_{1,2}$ son homeomorfos.

8.51 *a*) n; *b*) $n2^{n-1}$; *c*) n; *d*) $n = 1$, par, *e*) considere la matriz de 4×16:

$$M = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

que muestra la forma en que $\mathbf{Q}_4$ (las columnas de M) se obtiene a partir de $\mathbf{Q}_3$. Es decir, la submatriz superior izquierda de 3×8 de M es $\mathbf{Q}_3$, la submatriz superior derecha de 3×8 de M es $\mathbf{Q}_3$ escrita al revés, y el último renglón consta de ocho ceros seguidos de ocho unos.

8.52 *a*) n y n; *b*) $n/2$ cuando n es par, $(n+1)/2$ cuando n es impar.

8.53 $K_{m,m}$ es bipartido y m-regular. También, al empezar con $K_{m,m}$, se eliminan m aristas ajenas para obtener un grafo bipartido que es $(m-1)$-regular, se eliminan otros m aristas ajenas para obtener un grafo bipartido que es $(m-2)$-regular y así sucesivamente. Estos grafos pueden ser inconexos, pero sus componentes conexos poseen las propiedades deseadas.

8.54 Hay ocho árboles así, como se muestra en la figura 8-71. El grafo con un vértice y ninguna arista se denomina *árbol trivial*.

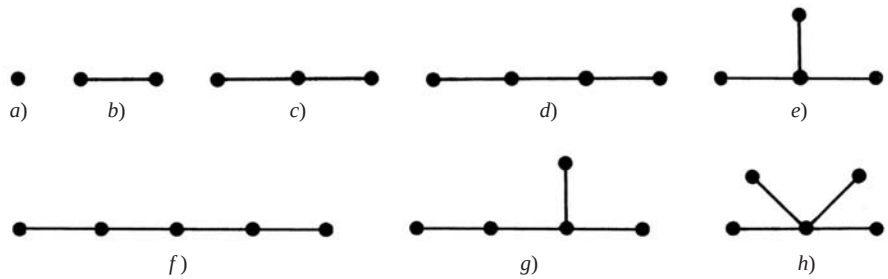


Figura 8-71

8.55 10

8.56 15

8.57 $1 + 1 + 1 + 1 + 1 + 2 + 2 + 3 = 12$.

8.59 $m = 1$.

8.60 Sólo *a*) no es plano, y $K_{3,3}$ es un subgrafo.

8.61 La figura 8-70*a*) es una representación plana de Q_3.

8.62 La región exterior tiene grado 8, y las otras dos regiones tienen grado 5.

8.63 *a*) 5, 8, 5; *b*) 12, 17, 7; *c*) 3, 6, 5; *d*) 7, 12, 7.

8.64 *a*) 3; *b*) 3; *c*) 2; *d*) 3.

8.65 Vea la figura 8-72.

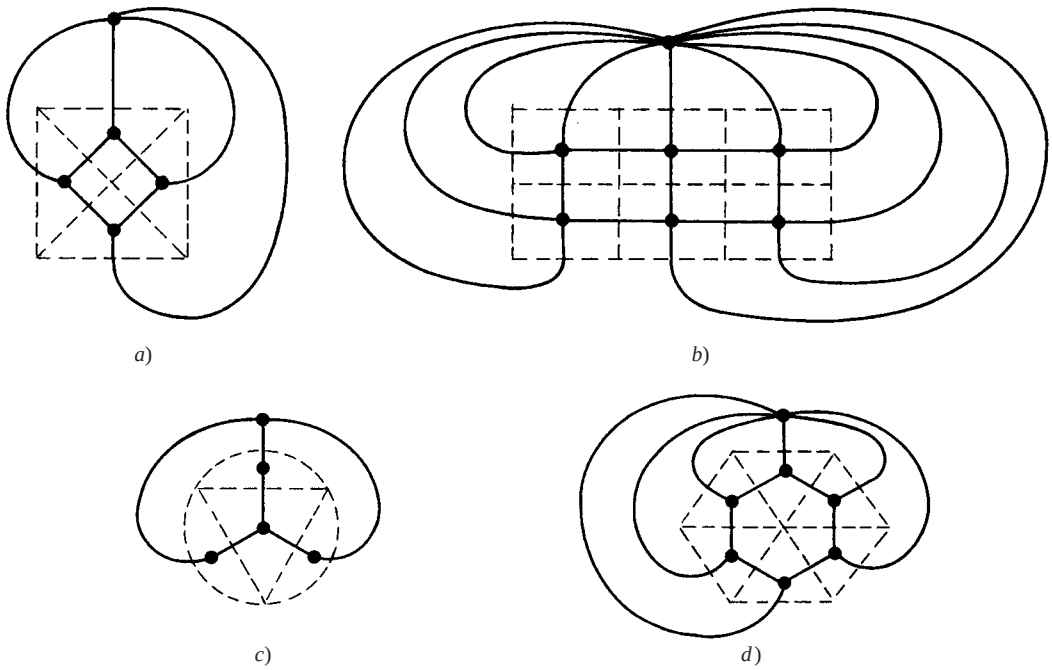


Figura 8-72

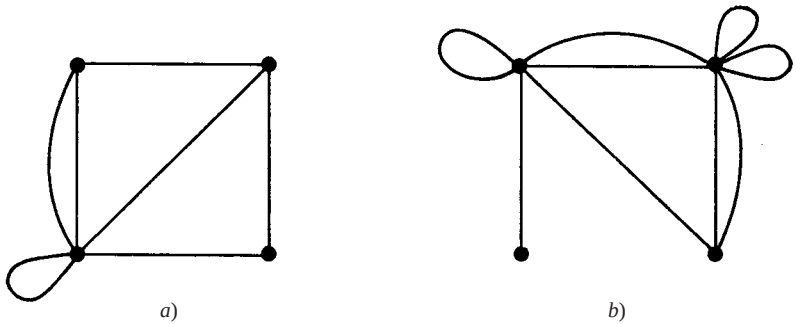
8.66 *a*) $n = 3$; *a*) $n = 4$.

8.67 *a*) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$; *b*) $\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$; *c*) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix}$

8.68 Vea la figura 8-73.

8.69 Sean M y N los dos conjuntos ajenos de vértices que determinan el grafo bipartido G. Primero se ordenan los vértices en M y luego se ordenan los vértices en N.

8.70 *a*) *B*, *F*, *A*, *D*, *E*, *C*.
b) $G = [A{:}B;\ B{:}A,\ C,\ D,\ E;\ C{:}F;\ D{:}B;\ E{:}B;\ F{:}C]$.



a) *b*)

Figura 8-73

8.71 *a*) Cada vértice es adyacente a los otros cuatro vértices.
b) $G = [A{:}B, D, F; B{:}A, C, E; C{:}B, D, F; D{:}A, C, E; E{:}B, D, F; F{:}A, C, E]$.
c) $G = [A{:}B, D; B{:}A, C, E; C{:}B, D; D{:}A, C, E; E{:}B, D]$.

8.72. Vea la figura 8-74.

Archivo vértice

	1	2	3	4	5	6	7	8
VERTEX	*A*	*B*	*C*	*D*	*E*	*F*		
PTR	1	2	9	14	8	12		

Archivo arista

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NUMBER	22	22	33	33	44	44	55	55	66	66	77	77	88	88	
ADJ	2	1	6	5	4	2	5	2	6	3	6	2	4	1	
NEXT	13	5	0	0	7	0	11	3	0	4	0	10	0	6	

Figura 8-74

8.73 *a*) $|ACBEDFA| = 20$ o $|A\,CBEFDA| = 21$; *B*) $|BCFEDAB| = 21$ o $|BCDEFAB| = 20$

8.74 *a*) $|ABCDEA| = 775$, $|ABCEDA| = 725$, $|ABDCEA| = 1\,100$, $|ABDECA| = 900$, $|ABECDA| = 1\,050$, $|ABEDCA| = 900$, $|ACBDEA| = 825$, $|ACBEDA| = 775$, $|ACDBEA| = 1\,150$, $|ACEBDA| = 1\,100$, $|ADBCEA| = 975$;
b) $|ABCEDA| = 725$

8.75 *a*) $G = [A{:}BJ; B{:}AJKL; C{:}DLM; D{:}CM; J{:}AB; K{:}BL; L{:}BCK; M{:}CD]$
b) [STACK : *C*, *MLD*, *DL*, *L*, *KB*, *B*, *J*, *A*],$CMDLKBJA$
c) [STACK : *K*, *LB*, *CB*, *MDB*, *DB*, *B*, *JA*, *A*], $KLCMDBJA$

8.76 *a*) [QUEUE : *C*, *MLD*, *ML*, *L*, *KB*, *JAK*, *JA*, *J*], $CDMLBKAJ$
b) [QUEUE : *K*, *LB*, *JAL*, *CJA*, *CJ*, *C*, *MD*, *M*], $KBLAJCDM$

8.77 *a*) $G = [A{:}BMJKL; B{:}ACDJL; C{:}BJ; D{:}BKM;\ J{:}ABCM; K{:}ADL; L{:}ABKM; M{:}ADJL]$
b) [STACK : *C*, *JB*, *MBA*, *LDAB*, *KBAD*, *DAB*, *AB*, *B*], $CJMLKDAB$
c) [STACK : *K*, *LDA*, *MBAD*, *JDAB*, *CBAD*, *BAD*, *AD*, *D*], $KLMJCBAD$

8.78 *a*) [QUEUE : *C*, *JB*, *LDAJ*, *MLDA*, *KMLD*, *KML*, *KM*, *K*], $CBJADLMK$
b) [QUEUE : *K*, *LDA*, *JMBLD*, *JMBL*, *CJMB*, *CJM*, *CJ*, *C*], $KADLBMJC$

8.79 *a*) $G = [A{:}BLM; B{:}ACLM; C{:}BDJ; D{:}CK; J{:}CK; K{:}DJL; L{:}ABKM; M{:}ABL]$

b) [STACK : $C, JDB, KDB, LDB, MBAD, BAD, AD, D$], $CJKLMBAD$

c) [STACK : $K, LJD, MBAJD, BAJD, CAJD, JDA, DA, A$], $KLMBCJDA$

8.80 *a*) [QUEUE : $C, JDB, MLAJD, KMLAJ, KMLA, KML, KM, K$], $CBDJALMK$

b) [QUEUE : $K, LJD, CLJ, CL, MBAC, MBA, MB, M$], $KDJLCABM$

9 Grafos dirigidos

CAPÍTULO

9.1 INTRODUCCIÓN

Los *grafos dirigidos* son grafos con aristas orientadas en una dirección. Dichos grafos son útiles en sistemas dinámicos como computadoras digitales o sistemas de flujo y es esta característica agregada lo que hace más difícil la determinación de ciertas propiedades de los grafos. Es decir, el procesamiento de estos grafos puede ser semejante a recorrer una ciudad con muchas calles de un solo sentido.

En este capítulo se proporcionan las definiciones y propiedades básicas de los grafos dirigidos. Muchas de las definiciones son semejantes a las del capítulo precedente sobre grafos (no dirigidos). Sin embargo, por razones pedagógicas, este capítulo es esencialmente independiente del capítulo precedente.

9.2 GRAFOS DIRIGIDOS

Un *grafo dirigido G*, o *digrafo* (o simplemente *grafo*), consta de dos partes:

i) Un conjunto V cuyos elementos ordenados se denominan *vértices*, *nodos* o *puntos*.

ii) Un conjunto E de pares *ordenados* (u, v) de vértices que se denominan *arcos*, *aristas dirigidas*, o simplemente *aristas*.

Cuando se desea recalcar las dos partes de G, se escribe $G(V, E)$. También se escribe $V(G)$ y $E(G)$ para denotar, respectivamente, el conjunto de vértices y el conjunto de aristas de un grafo G. (En caso de que no se plantee explícitamente, el contexto suele determinar si un grafo es o no un grafo dirigido.)

Suponga que $e = (u, v)$ es una arista en un grafo dirigido G. Entonces se usa la siguiente terminología:

a) *e empieza* en u y *termina* en v.

b) u es el *origen* o *punto inicial* de e, y v es el *destino* o *punto terminal* de e.

c) v es un *sucesor* de u.

d) *u es adyacente a v*, y *v es adyacente a u*.

Si $u = v$, entonces e se denomina *lazo*.

El conjunto de todos los sucesores de un vértice u es importante; se denota y define formalmente por

$$\text{suc}(u) = \{v \in V | \text{ existe una arista } (u, v) \in E\}$$

Se denomina *lista de sucesores* o *lista de adyacencia* de u.

Una *ilustración* de un grafo dirigido G es una representación de G en el plano. Es decir, cada vértice u de G se representa por un punto (o un círculo pequeño) y cada arista (dirigida) $e = (u, v)$ se representa por una flecha o una curva dirigida desde el punto inicial u de e hasta el punto terminal v. Un grafo dirigido G suele representarse por su ilustración, más que mediante la enumeración explícita de sus vértices y aristas.

Si las aristas y/o los vértices de un grafo dirigido G se etiquetan con algún tipo de datos, entonces G se denomina *grafo dirigido etiquetado*.

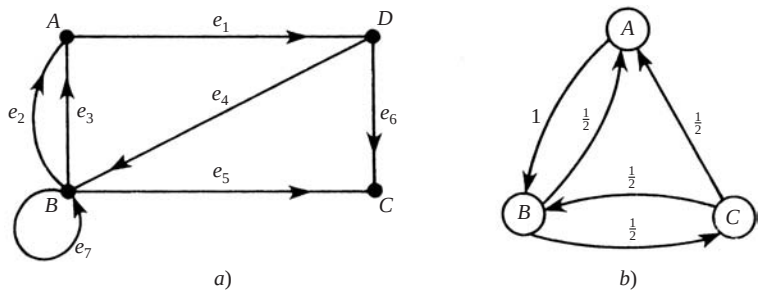
Se dice que un grafo dirigido $\{V, E\}$ es *finito* si su conjunto V de vértices y su conjunto E de aristas son finitos.

EJEMPLO 9.1

a) Considere el grafo dirigido G que se muestra en la figura 9-1*a*). Consta de cuatro vértices A, B, C, D, es decir, $V(G) = \{A, B, C, D\}$ y las siete aristas siguientes:

$$E(G) = \{e_1, e_2, \ldots, e_7\} = \{(A, D), (B, A), (B, A), (D, B), (B, C), (D, C), (B, B)\}$$

Se dice que las aristas e_2 y e_3 son *paralelas*, puesto que ambas empiezan en B y terminan en A. La arista e_7 es un *lazo*, ya que empieza y termina en B.



a) *b*)

Figura 9-1

b) Suponga que tres muchachos A, B, C, se lanzan una pelota entre sí de modo que A siempre la lanza a B, pero B y C tienen la misma probabilidad de lanzar la pelota a A, así como uno al otro. Este sistema dinámico se representa en la figura 9-1*b*), donde las aristas están etiquetadas con las probabilidades respectivas; es decir, A lanza la pelota a B con probabilidad 1, B la lanza a A y a C con probabilidad igual a $1/2$ para cada uno, y C la lanza a A y a B con probabilidad igual a $1/2$ para cada uno.

Subgrafos

Sea $G = G(V, E)$ un grafo dirigido, y sea V' un subconjunto del conjunto V de vértices de G. Suponga que E' es un subconjunto de E tal que los puntos terminales de las aristas de E' pertenecen a V'. Entonces $H(V', E')$ es un grafo dirigido, y se denomina un *subgrafo* de G. En particular, si E' contiene todas las aristas en E cuyos puntos terminales pertenecen a V', entonces $H(V', E')$ se denomina subgrafo de G *generado* o *determinado* por V'. Por ejemplo, para el grafo $G = G(V, E)$ en la figura 9-1*a*), $H(V', E')$ es el subgrafo de G determinado por el conjunto de vértices V', donde

$$V' = \{B, C, D\} \quad \text{y} \quad E' = \{e_4, e_5, e_6, e_7 = \{(D, B), (B, C), (D, C), (B, B)\}$$

9.3 DEFINICIONES BÁSICAS

En esta sección se analizan las cuestiones de grados de los vértices, caminos y conectividad en un grafo dirigido.

Grados

Suponga que G es un grafo dirigido. El *grado de salida (outdegree)* de un vértice v de G, que se escribe outdeg(v), es el número de aristas que empiezan en v, y el *grado de entrada* (*indegree*) de v, que se escribe indeg(v), es el número de aristas que terminan en v. Puesto que cada arista empieza y termina en un vértice, de inmediato se obtiene el siguiente teorema.

Teorema 9.1: La suma de los grados de salida de los vértices de un grafo dirigido G es igual a la suma de los grados de entrada de los vértices, que es igual al número de aristas en G.

Un vértice v con grado de entrada cero se denomina *fuente*, y un vértice con grado de salida cero se denomina *sumidero*.

EJEMPLO 9.2 Considere el grafo G en la figura 9-1*a*). Se tiene

$$\text{outdeg}\,(A) = 1, \quad \text{outdeg}\,(B) = 4, \quad \text{outdeg}\,(C) = 0, \quad \text{outdeg}\,(D) = 2,$$
$$\text{indeg}\,(A) = 2, \quad \text{indeg}\,(B) = 2, \quad \text{indeg}\,(C) = 2, \quad \text{indeg}\,(D) = 1.$$

Como era de esperar, la suma de los grados de salida es igual a la suma de los grados de entrada, que es igual al número 7 de aristas. El vértice C es un sumidero, puesto que ninguna arista empieza en C. El grafo no tiene fuentes.

Caminos

Sea G un grafo dirigido. Los conceptos de camino, camino simple, recorridos y ciclo válidos para grafos no dirigidos se aplican a los grafos dirigidos G, excepto que las direcciones de las aristas deben coincidir con la dirección del camino. Con más precisión:

i) Un *camino* (*dirigido*) P en G es una secuencia alterna de vértices y aristas dirigidas; Por ejemplo,

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$$

tal que la arista e_i empieza en v_{i-1} y termina en v_i. Si no hay ambigüedad, P se denota por su secuencia de vértices o su secuencia de aristas.

ii) La *longitud* del camino P es n, su número de aristas.

iii) Un *camino simple* es un camino con vértices distintos. Un *recorrido* es un camino con aristas distintas.

iv) Un *camino cerrado* tiene los mismos vértices inicial y final.

v) Un *camino de expansión* contiene todos los vértices de G.

vi) Un *ciclo* (o *circuito*) es un camino cerrado con vértices distintos (excepto el primero y el último).

vii) Un *semicamino* es lo mismo que un camino, excepto que la arista e_i puede empezar en v_{i-1} o en v_i y terminar en el otro vértice. Los *semirecorridos* y los *caminos semisimples* se definen en forma análoga.

Un vértice v es *alcanzable* desde un vértice u si hay una camino de u a v. Si v es alcanzable desde u, entonces (al eliminar las aristas redundantes) debe haber un camino simple de u a v.

EJEMPLO 9.3 Considere el grafo G en la figura 9-1*a*).

a) La secuencia $P_1 = (D, C, B, A)$ es un semicamino, no un camino, puesto que (C, B) no es una arista; es decir, la dirección de $e_5 = (C, B)$ no coincide con la dirección de P_1.

b) La secuencia $P_2 = (D, B, A)$ es un camino de D a A puesto que (D, B) y (B, A) son aristas. Por tanto, A es alcanzable desde D.

Conectividad

En un grafo dirigido G hay tres tipos de conectividad:

i) G es *fuertemente conexo* o *fuerte* si para cualquier par de vértices u y v en G, hay un camino de u a v y un camino de v a u; es decir, cada uno es alcanzable desde el otro.

ii) G es *unilateralmente conexo* o *unilateral* si para cualquier par de vértices u y v en G, hay un camino de u a v o un camino de v a u; es decir, uno de ellos es alcanzable desde el otro.

iii) G es *débilmente conexo* o *débil* si entre cualquier par de vértices u y v en G hay un semicamino.

Sea G' el grafo (no dirigido) que se obtiene a partir de un grafo dirigido G al dejar que todas las aristas de G sean no dirigidas. Resulta evidente que G es débilmente conexo si y sólo si el grafo G' es conexo.

Observe que fuertemente conexo implica unilateralmente conexo, lo cual implica débilmente conexo. Se dice que G es *estrictamente unilateral* si es unilateral pero no fuerte, y se dice que G es *estrictamente débil* si es débil pero no unilateral.

La conectividad puede caracterizarse en términos de los caminos de expansión como sigue:

Teorema 9.2: Sea G un grafo dirigido finito. Entonces:

i) G es fuerte si y sólo si G tiene un camino de expansión cerrado.

ii) G es unilateral si y sólo si G tiene un camino de expansión.

iii) G es débil si y sólo si G tiene un semicamino de expansión.

EJEMPLO 9.4 Considere el grafo G en la figura 9-1*a*). Es débilmente conexo puesto que el grafo no dirigido subyacente es conexo. No hay ningún camino desde C hasta cualquier otro vértice; es decir, C es un sumidero, de modo que G no es fuertemente conexo. Sin embargo, $P = (B, A, D, C)$ es un camino de expansión, de modo que G es unilateralmente conexo.

Los grafos con fuentes y sumideros aparecen en muchas aplicaciones (como diagramas de flujo y redes). Una condición suficiente para que tales vértices existan es la siguiente.

Teorema 9.3: Suponga que un grafo dirigido finito G es libre de ciclos; es decir, que no contiene ciclos (dirigidos). Entonces G contiene una fuente y un sumidero.

Demostración: Sea $P = (v_0, v_1, \ldots, v_n)$ un camino simple de longitud máxima, que existe porque G es finito. Entonces el último vértice v_n es un sumidero; en caso contrario, una arista (v_n, u) extiende a P o forma un ciclo si $u = v_i$ para alguna i. En forma semejante, el primer vértice v_0 es una fuente.

9.4 ÁRBOLES CON RAÍZ

Recuerde que un grafo de un árbol es un grafo conexo libre de ciclos; es decir, un grafo conexo sin ningún ciclo. Un *árbol T con raíz* es un grafo de un árbol con un vértice designado r al que se le denomina *raíz* del árbol. Puesto que existe un camino simple único de la raíz r a cualquier otro vértice v en T, esto determina una dirección hacia las aristas de T. Por tanto, T puede considerarse como un grafo dirigido. Observe que cualquier árbol puede hacerse un árbol con raíz con la simple elección de uno de los vértices como la raíz.

Considere un árbol T con raíz cuya raíz es r. La longitud del camino de la raíz r a cualquier vértice v se denomina *nivel* (o *profundidad*) de v, y el máximo nivel de vértice se denomina *profundidad* del árbol. Los vértices con grado 1, que no sean la raíz r, se denominan *hojas* de T, y un camino dirigido de un vértice a una hoja se denomina *rama*.

Por lo general, un árbol T con raíz se ilustra con la raíz en la parte superior del árbol. En la figura 9-2*a*) se muestra un árbol T con raíz r y 10 vértices más. El árbol tiene cinco hojas d, f, h, i y j. Observe que $nivel(a) = 1$, $nivel(f) = 2$, $nivel\ (j) = 3$. Además, la profundidad del árbol es 3.

El hecho de que un árbol T con raíz proporcione una dirección a las aristas significa que es posible asignar una relación de precedencia entre los vértices. De manera más precisa, se dice que un vértice u *precede* a un vértice v o que v *sigue a* u si hay un camino (dirigido) de v a u. En particular, se dice que v *sigue inmediatamente a* u si (u, v) es

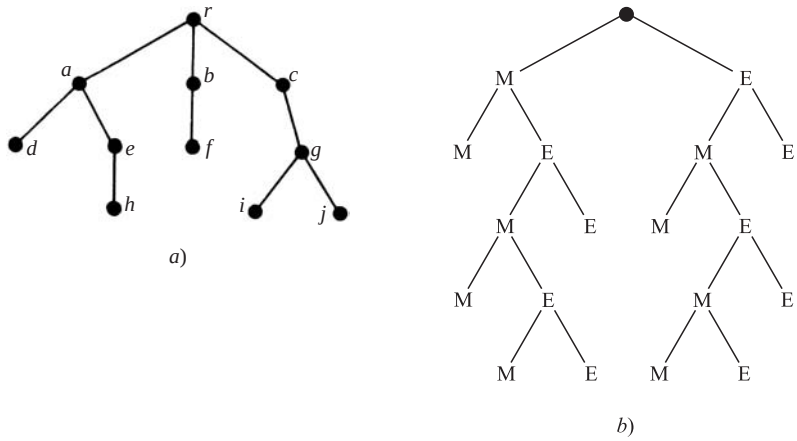


Figura 9-2

una arista; es decir, si v sigue a u y v es adyacente a u. Observe que cualquier vértice v, que no sea la raíz, sigue inmediatamente a un vértice único, aunque v puede ser seguido inmediatamente por más de un vértice. Por ejemplo, en la figura 9-2*a*), el vértice j sigue a c aunque inmediatamente sigue a g. Ambos vértices i y j siguen inmediatamente a g.

Un árbol T con raíz también es un dispositivo útil para enumerar todas las posibilidades lógicas de una secuencia de eventos donde cada evento puede ocurrir en una forma finita de formas. Este hecho se ilustra con el siguiente ejemplo.

EJEMPLO 9.5 Suponga que Marcos y Eric juegan en un torneo de tenis de modo que la primera persona en ganar dos juegos seguidos o quien gane un total de tres juegos gana el torneo. Encuentre el número de formas en que puede desarrollarse el torneo.

El árbol con raíz en la figura 9-2*b*) muestra las diferentes formas en que puede desarrollarse el torneo. Hay 10 hojas que corresponden a las 10 formas en que puede ocurrir el torneo:

MM, **MEMM**, **MEMEM**, **MEMEE**, **MEE**, **EMM**, **EMEMM**, **EMEME**, **EMEE**, **EE**

Específicamente, el camino de la raíz a la hoja describe quién ganó cuáles juegos en el torneo.

Árboles con raíz ordenados

Considere un árbol T con raíz en el que las aristas que salen de cada vértice están ordenadas. Entonces se tiene el concepto de *árbol con raíz ordenado*. Los vértices de un árbol así pueden etiquetarse (o *direccionarse*) en forma sistemática como: primero se asigna 0 a la raíz r. Luego se asigna 1, 2, 3,…, a los vértices que siguen de inmediato a r según la forma en que se ordenaron las aristas. Enseguida se etiquetan los vértices restantes: si a es la etiqueta de un vértice v, entonces $a.1$, $a.2$,… se asignan a los vértices que siguen de inmediato a v según la forma en que se ordenaron las aristas. Este sistema de direcciones se ilustra en la figura 9-3*a*), donde las aristas se representan de izquierda a derecha según su orden. Observe que el número de puntos decimales en cualquier etiqueta es uno menos que el nivel del vértice. Este sistema de identificación se denomina *sistema universal de direcciones* para un árbol con raíz ordenado.

El sistema universal de direcciones constituye una forma importante para describir (o almacenar) linealmente un árbol con raíz ordenado. De manera más concisa, dadas las direcciones a y b, se hace $a < b$ si $b = a.c$ (es decir, a es un *segmento inicial* de b), o si hay enteros positivos m y n con $m < n$ tales que

$$a = \text{r.m.s} \quad \text{y} \quad b = \text{r.n.t}$$

Este orden se denomina *orden lexicográfico* puesto que es semejante a la forma en que las palabras están dispuestas en un diccionario. Por ejemplo, las direcciones en la figura 9-3*a*) están ordenadas linealmente según se representa en la figura 9-3*b*). Ese orden lexicográfico es idéntico al orden que se obtiene al moverse hacia abajo a partir de la rama

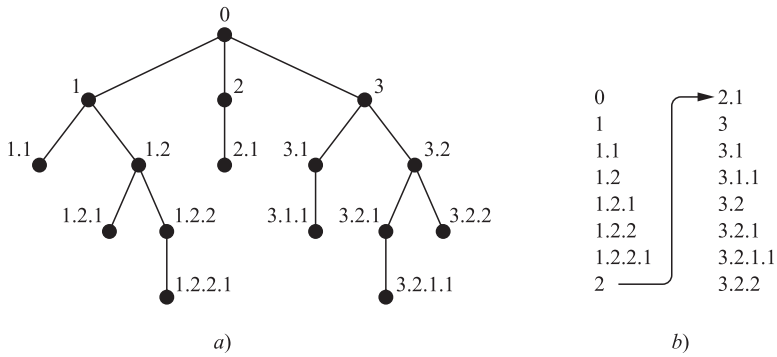


Figura 9-3

más a la izquierda del árbol, en seguida hacia la siguiente rama a la derecha, luego la segunda rama a la derecha y así sucesivamente.

9.5 REPRESENTACIÓN SECUENCIAL DE GRAFOS DIRIGIDOS

Hay dos formas fundamentales para mantener un grafo dirigido G en la memoria de una computadora. Una forma, denominada *representación secuencial* de G, es por medio de su matriz de adyacencia A. La otra forma, denominada *representación enlazada* de G, es por medio de listas ligadas de vecinos. En esta sección se estudia la primera representación. La representación enlazada se analizará en la sección 9.7.

Suponga que un grafo G tiene m vértices (nodos) y n aristas. Se dice que G es *denso* si $m = O(n^2)$ y *disperso* si $m = O(n)$ o inclusive si $m = O(n \log n)$. Cuando G es denso suele usarse la representación matricial de G, y cuando G es disperso suelen usarse las listas ligadas. Sin importar la forma en que un grafo G se mantiene en la memoria, el grafo G suele introducirse en la computadora por medio de su definición formal; es decir, como una colección de vértices y una colección de aristas (pares de vértices).

Observación: Para evitar casos especiales de los resultados se supone, a menos que se especifique otra cosa, que $m > 1$, donde m es el número de vértices en el grafo G. En consecuencia, G no es conexo si G no tiene aristas.

Diagramas y relaciones, matriz de adyacencia

Sea $G(V, E)$ un grafo dirigido *simple*; es decir, un grafo sin aristas paralelas. Entonces E es simplemente un subconjunto de $V \times V$, y entonces E es una relación sobre V. A la inversa, si R es una relación sobre un conjunto V, entonces $G(V, R)$ es un grafo dirigido simple. Por tanto, los conceptos de relaciones sobre un conjunto y de grafos dirigidos simples son uno y el mismo. De hecho, en el capítulo 2, ya se presentó el grafo dirigido correspondiente a una relación sobre un conjunto.

Suponga que G es un grafo dirigido simple con m vértices y que los vértices de G se han ordenado y que se denominan $v_1, v_2, \ldots, v_m$. Entonces la *matriz de adyacencia* $A = [a_{ij}]$ de G es la matriz de $m \times m$ definida como sigue:

$$a_{ij} = \begin{cases} 1 & \text{si existe una arista } (v_i, v_j) \\ 0 & \text{en otro caso} \end{cases}$$

Esta matriz A, que sólo contienen entradas 0 o 1, se denomina *matriz de bits* o *matriz booleana*. (Aunque la matriz de adyacencia de un grafo no dirigido es simétrica, esto no es cierto aquí para un grafo dirigido.)

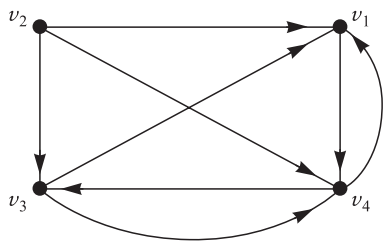
La matriz de adyacencia A del grafo G depende del ordenamiento de los vértices de G. Sin embargo, las matrices resultantes de dos ordenamientos distintos están estrechamente relacionadas en el sentido de que una puede obtenerse a partir de la otra al intercambiar simplemente renglones y columnas. A menos que se establezca otra cosa, se supone que los vértices de la matriz tienen un ordenamiento fijo.

Observación: La matriz de adyacencia $A = [a_{ij}]$ puede extenderse a grafos dirigidos con aristas paralelas al hacer:

$$a_{ij} = \text{número de aristas que empiezan en } v_i \text{ y terminan en } v_j$$

Así, las entradas de A son enteros no negativos. A la inversa, toda matriz A $m \times m$ con entradas enteras no negativas define de manera única un grafo dirigido con m vértices.

EJEMPLO 9.6 Sea G el grafo dirigido en la figura 9-4*a*) con vértices v_1, v_2, v_3, v_4. Entonces la matriz de adyacencia A de G se muestra en la figura 9-4*b*). Observe que el número de unos en A es igual al número (ocho) de aristas.



a)

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

b)

Figura 9-4

Considere las potencias A, A^2, $A^3, \ldots$, de la matriz de adyacencia $A = [a_{ij}]$ de un grafo G. Sea

$$a_K(i, j) = \text{la entrada } ij \text{ en la matriz } A^K$$

Observe que $a_1(i, j) = a_{ij}$ proporciona el número de caminos de longitud 1 del vértice v_i al vértice v_j. Puede demostrarse que $a_2(i, j)$ proporciona el número de caminos de longitud 2 de v_i a v_j. De hecho, en el problema 9.17 se demuestra el siguiente resultado general.

Proposición 9.4: Sea A la matriz de adyacencia de un grafo G. Entonces $a_K(i, j)$, la entrada ij en la matriz A^K, proporciona el número de caminos de longitud K de v_i a v_j.

EJEMPLO 9.7 Considere de nuevo el grafo G y su matriz de adyacencia A que se muestran en la figura 9-4. A continuación se proporcionan las potencias A^2, A^3 y A^4:

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 2 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 3 & 0 & 2 & 3 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 2 & 0 & 2 & 1 \\ 5 & 0 & 3 & 5 \\ 3 & 0 & 2 & 3 \\ 3 & 0 & 1 & 4 \end{bmatrix}$$

Observe que $a_2(4, 1) = 1$, de modo que hay un camino de longitud 2 de v_4 a v_1. También, $a_3(2, 3) = 2$, de modo que hay dos caminos de longitud 3 de v_2 a v_3; y $a_4(2, 4) = 5$, de modo que hay cinco caminos de longitud 4 de v_2 a v_4.

Observación: Sea A la matriz de adyacencia de un grafo G, y sea B_r la matriz definida por:

$$B_r = A + A^2 + A^3 + \cdots + A^r$$

Entonces la entrada ij de la matriz B_r proporciona el número de caminos de longitud r o menos del vértice v_i al vértice v_j.

Matriz de caminos

Sea $G = G(V, E)$ un grafo dirigido simple con m vértices $v_1, v_2, \ldots, v_m$. La *matriz de caminos* o *matriz de alcanzabilidad* de G es la matriz cuadrada $P = [p_{ij}]$ definida como:

$$p_{ij} = \begin{cases} 1 & \text{si hay un camino de } v_i \text{ a } v_j \\ 0 & \text{en otro caso} \end{cases}$$

(La matriz de caminos puede considerarse como la cerradura transitiva de la relación E sobre V.)

Ahora suponga que en un grafo G con m vértices hay un camino del vértice v_i al vértice v_j. Entonces debe haber un camino simple de v_i a v_j cuando $v_i \neq v_j$, o debe haber un ciclo de v_i a v_j cuando $v_i = v_j$. Puesto que G tiene m vértices, este camino simple debe tener longitud $m - 1$ o menor, o tal ciclo debe tener longitud m o menor. Esto significa que en la matriz B_m (definida antes) hay una entrada ij distinta de cero, donde A es la matriz de adyacencia de G. En consecuencia, la matriz de caminos P y B_m tienen las mismas entradas diferentes de cero. Este resultado se plantea formalmente como sigue.

Proposición 9.5: Sea A la matriz de adyacencia de un grafo G con m vértices. Entonces la matriz de caminos P y B_m tienen las mismas entradas diferentes de cero, donde

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Recuerde que un grafo dirigido G es *fuertemente conexo* si, para cualquier par de vértices u y v en G, hay un camino de u a v y de v a u. Por consiguiente, G es fuertemente conexo si y sólo si la matriz de caminos P de G no tiene entradas cero. Este hecho junto con la proposición 9.5 proporciona el siguiente resultado.

Proposición 9.6: Sea A la matriz de adyacencia de un grafo G con m vértices. Entonces G es fuertemente conexo si y sólo si B_m no tiene entradas cero, donde

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

EJEMPLO 9.8 Considere el grafo G y su matriz de adyacencia A, que se muestran en la figura 9-4. Aquí G tiene $m = 4$ vértices. Al sumar la matriz A y las matrices A^2, A^3, A^4 en el ejemplo 9.7 se obtiene la siguiente matriz B_4 y también una matriz de caminos (de alcanzabilidad) P al sustituir las entradas diferentes de cero en B_4 por 1:

$$B_4 = \begin{bmatrix} 4 & 0 & 3 & 4 \\ 11 & 0 & 7 & 11 \\ 7 & 0 & 4 & 7 \\ 7 & 0 & 4 & 7 \end{bmatrix} \quad \text{y} \quad P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Al analizar la matriz B_4 o P, se observan entradas iguales a cero; por tanto, G no es fuertemente conexo. En este caso se observa que el vértice v_2 no es alcanzable desde ninguno de los otros vértices.

Observación: La matriz de adyacencia A y la matriz de camino P de un grafo G se consideran matrices lógicas (booleanas) cuando 0 representa "falso" y 1 representa "verdadero". Así, las operaciones lógicas de $\wedge$ (AND) y $\vee$ (OR) pueden aplicarse a las entradas de A y P donde estas operaciones, usadas en la siguiente sección, se definen en la figura 9-5.

$\wedge$	0	1
0	0	0
1	0	1

a) AND.

$\vee$	0	1
0	0	1
1	1	1

b) OR.

Figura 9-5

Cerradura transitiva y la matriz de caminos

Sea R una relación sobre un conjunto finito V con m elementos. Como ya se observó, la relación R puede identificarse con el grafo dirigido simple $G = G(V, R)$. Se observa que la relación composición $R^2 = R \times R$ consta de todos los pares (u, v) tales que hay un camino de longitud 2 de u a v. En forma semejante:

$$R^K = \{(u, v) \mid \text{hay un camino de longitud } K \text{ de } u \text{ a } v\}.$$

La cerradura transitiva R^* de la relación R sobre V ahora puede considerarse como un conjunto de pares ordenados (u, v) tales que hay en el grafo G un camino de u a v. Además, por el análisis anterior, sólo es necesario buscar caminos simples de longitud $m - 1$ o menor y ciclos de longitud m o menor. En consecuencia, se tiene el siguiente resultado, que caracteriza la cerradura transitiva R^* de R.

Teorema 9.7: Sea R una relación sobre un conjunto V con m elementos. Entonces:

i) $R^* = R \cup R^2 \cup \ldots \cup R^m$ es la cerradura transitiva de R.

ii) La matriz de caminos P de $G(V, \mathrm{R})$ es la matriz de adyacencia de $G'(V, R^*)$.

9.6 ALGORITMO DE WARSHALL, CAMINOS MÁS CORTOS

Sea G un grafo dirigido con m vértices $v_1, v_2, \ldots, v_m$. Suponga que desea encontrar la matriz de caminos P del grafo G. Warshall proporcionó un algoritmo mucho más eficiente que calcular las potencias de la matriz de adyacencia A. Tal algoritmo se define en esta sección, y un algoritmo semejante se utiliza para encontrar los caminos más cortos en G cuando G es ponderado.

Algoritmo de Warshall

Primero se definen las matrices booleanas cuadradas $m \times m$ $P_0, P_1, \ldots, P_m$, donde $P_k[i, j]$ denota la entrada ij de la matriz P_k:

$$P_k[i, j] = \begin{cases} 1 & \text{si hay un camino simple de } v_i \text{ a } v_j \text{ que no use ningún otro vértice,} \\ & \quad \text{excepto quizá } v_1, v_2, \ldots, v_k. \\ 0 & \text{en otro caso.} \end{cases}$$

Por ejemplo,

$$P_k[i, j] = 1 \quad \text{si hay un camino simple de } v_i \text{ a } v_j \text{ que no use ningún otro vértice, excepto quizá } v_1, v_2, v_3.$$

Observe que la primera matriz $P_0 = A$ es la matriz de adyacencia de G. Además, puesto que G sólo tiene m vértices, la última matriz $P_m = P$ es la matriz de caminos de G.

Warshall observó que $P_k[i, j] = 1$ puede pasar sólo si ocurre uno de los dos casos siguientes:

1) Hay un camino simple de v_i a v_j que no usa ningún otro vértice, excepto quizá $v_1, v_2, \ldots, v_{k-1}$; por tanto,

$$P_{k-1}[i, j] = 1$$

2) Hay un camino simple de v_i a v_k y un camino simple de v_k a v_j donde cada camino simple no usa ningún otro vértice, excepto quizá $v_1, v_2, \ldots, v_{k-1}$; por tanto,

$$P_{k-1}[i, k] = 1 \quad \text{y} \quad P_{k-1}[k, j] = 1$$

Estos dos casos se representan como sigue:

$$1)\ v_i \to \cdots \to v_j; \qquad 2)\ v_i \to \cdots \to v_k \to \cdots v_j$$

donde $\to \cdots \to$ denota parte de un camino simple que no usa ningún otro vértice, excepto quizá $v_1, v_2, \ldots, v_{k-1}$. En consecuencia, los elementos de P_k pueden obtenerse como sigue:

$$P_k[i, j] = P_{k-1}[i, j] \ \vee \ (P_{k-1}[i, k] \ \wedge \ P_{k-1}[k, j])$$

donde se usan las operaciones lógicas de $\wedge$ (AND) y $\vee$ (OR). En otras palabras, cada entrada en la matriz P_k puede obtenerse buscando sólo tres entradas en la matriz P_{k-1}. El algoritmo de Warshall se muestra en la figura 9-6.

Algoritmo 9.1 (de Warshall): Un grafo dirigido G con M vértices se mantiene en la memoria por medio de su matriz de adyacencia A. Este algoritmo encuentra la matriz de caminos (booleana) P del grafo de G.

Paso 1. Repetir para $I, J = 1, 2, \ldots, M$; [Inicializa P].
Si $A[I, J] = 0$, entonces: Establecer $P[I, J]: = 0$;
O bien: Establecer $P[I, J]: = 1$.
[Fin del ciclo].

Paso 2. Repetir los pasos 3 y 4 para $K = 1, 2, \ldots, M$: [Actualiza P].

Paso 3. Repetir el paso 4 para $I = 1, 2, \ldots, M$:

Paso 4. Repetir para $J = 1, 2, \ldots, M$:
Establecer $P[I, J]:= P[I, J] \vee P[I, K] \wedge P[K, J]$).
[Fin del ciclo].
[Fin del ciclo del paso 3].
[Fin del ciclo del paso 2].

Paso 5. Salir.

Figura 9-6

Algoritmo del camino más corto

Sea G un grafo dirigido simple con m vértices, $v_1, v_2, \ldots, v_m$. Suponga que G es ponderado; es decir, suponga que a cada arista e de G se asigna un número no negativo $w(e)$ denominado *peso* o *longitud* de e. Entonces G puede mantenerse en la memoria por medio de su matriz de pesos $W = [w_{ij}]$ definida como sigue:

$$w_{ij} = \begin{cases} w(e) & \text{si hay una arista } e \text{ de } v_i \text{ a } v_j \\ 0 & \text{si no hay una arista de } v_i \text{ a } v_j \end{cases}$$

La matriz de caminos P indica si entre los vértices hay o no caminos. Ahora se desea encontrar una matriz Q que indique las longitudes de los caminos más cortas entre los vértices o, más exactamente, una matriz $Q = [q_{ij}]$ donde

$$[q_{ij}] = \text{longitud del camino más corto de } v_i \text{ a } v_j$$

A continuación se describe una modificación del algoritmo de Warshall que encuentra de manera eficiente la matriz Q.

Aquí se define una secuencia de matrices $Q_0, Q_1, \ldots, Q_m$ (semejante a las matrices anteriores $P_0, P_1, \ldots, P_m$) donde $Q_k[i, j]$, la entrada ij de Q_k, se define como sigue:

$Q_k[i, j]$ = la menor longitud del camino precedente de v_i a v_j o la suma de las longitudes de los caminos precedentes de v_i a v_k y de v_k a v_j.

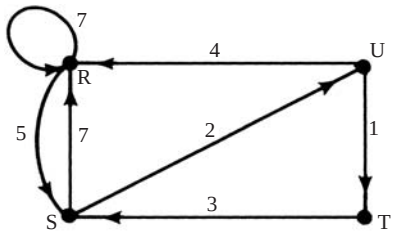
Más exactamente,

$$Q_k[i, j] = \text{MIN}(Q_{k-1}[i, j],\ Q_{k-1}[i, k] + Q_{k-1}[k, j])$$

La matriz inicial Q_0 es la misma que la matriz de pesos W, excepto que cada 0 en w se sustituye por ∞ (o por un número muy, muy grande). La matriz final Q_m es la matriz buscada Q.

EJEMPLO 9.9 En la figura 9-7 se muestran un grafo ponderado G y su matriz de pesos W, donde se supone que $v_1 = R$, $v_2 = S$, $v_3 = T$, $v_4 = U$.

Suponga que el modelo modificado del algoritmo de Warshall se aplica al grafo ponderado G en la figura 9-7. Se obtienen las matrices Q_0, Q_1, Q_3 y Q_4 en la figura 9-8. (A la derecha de cada matriz Q_k en la figura 9-8 se muestra la matriz de caminos que



$$W = \begin{bmatrix} 7 & 5 & 0 & 0 \\ 7 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{bmatrix}$$

Figura 9-7

corresponde a las longitudes en la matriz Q_k.) Las entradas en la matriz Q_0 son las mismas que en la matriz de pesos W, excepto que cada 0 en W se sustituye por ∞ (un número muy, muy grande). A continuación se indica cómo se obtuvieron las entradas encerradas en un círculo:

$$Q_1[4, 2] = \text{MÍN}\,(Q_0[4, 2], \quad Q_0[4, 1] + Q_0[1, 2]) = \text{MÍN}(\infty, 4 + 5) = 9$$
$$Q_2[1, 3] = \text{MÍN}\,(Q_1[1, 3], \quad Q_1[1, 2] + Q_1[2, 3]) = \text{MÍN}(\infty, 5 + \infty) = \infty$$
$$Q_3[4, 2] = \text{MÍN}\,(Q_2[4, 2], \quad Q_2[4, 3] + Q_2[3, 2]) = \text{MÍN}(9, 3 + 1) = 4$$
$$Q_4[3, 1] = \text{MÍN}\,(Q_3[3, 1], \quad Q_3[3, 4] + Q_3[4, 1]) = \text{MÍN}(10, 5 + 4) = 9$$

La última matriz $Q_4 = Q$, la matriz buscada con el camino más corto.

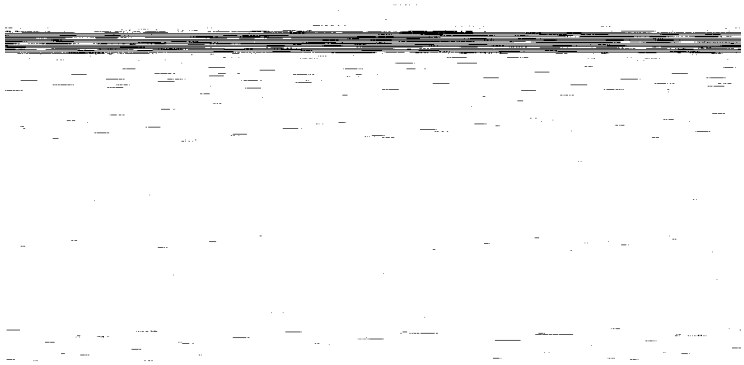
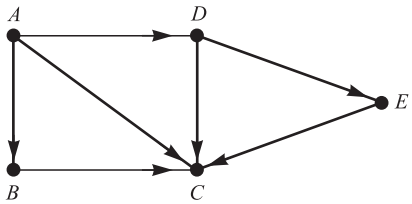


Figura 9-8

9.7 REPRESENTACIÓN LIGADA DE GRAFOS DIRIGIDOS

Sea G un grafo dirigido con m vértices. Suponga que el número de aristas de G es $O(m)$, o incluso $O(m \log m)$; es decir, suponga que G es disperso. Entonces la matriz de adyacencia A de G contiene muchos ceros; por tanto, se desperdicia

bastante espacio de memoria. En consecuencia, cuando G es disperso, G suele representarse en la memoria por medio de algún tipo de *representación enlazada*, también denominada *estructura de adyacencia*, que se describe a continuación con un ejemplo.



a) Grafo G

Vértice	Lista de adyacencia
A	B, C, D
B	C
C	$\varnothing$
D	C, E
E	C

b) Listas de adyacencia de G

Figura 9-9

Considere el grafo dirigido G en la figura 9-9*a*). Observe que G puede definirse en forma equivalente por la tabla en la figura 9-9*b*), donde se muestra cada vértice en G seguido por su *lista de adyacencia*, también denominada de sus *sucesores* o *vecinos*. Aquí el símbolo $\varnothing$ denota una lista vacía. Observe que cada arista de G corresponde a un vértice único en una lista de adyacencia y viceversa. Aquí, G tiene siete aristas y en las listas de adyacencia hay siete vértices. Esta tabla también puede presentarse en la siguiente forma abreviada, donde dos puntos ":" separan un vértice de su lista de vecinos y un punto y coma ";" separa las diversas listas:

$$G = [A : B, C, D; \quad B : C; \quad C : \varnothing; \quad D : C, E; \quad E : C]$$

La *representación ligada* de un grafo dirigido G mantiene a G en la memoria mediante el uso de listas ligadas para sus listas de adyacencia. Con más brevedad, la representación enlazada normalmente contiene dos archivos (conjuntos de registros), uno denominado Vertex File y el otro Edge File, como sigue.

a) ***Vertex File***: Este archivo contiene la lista de vértices del grafo G usualmente mantenida por medio de un arreglo o por una lista ligada. Cada registro del archivo tiene la forma

VERTEX	NEXT-V	PTR	

Aquí VERTEX es el nombre del vértice, NEXT-V apunta al siguiente vértice en la lista de vértices en el Vertex File, y PTR apunta al primer elemento en la lista de adyacencia del vértice que aparece en el Edge File. El área sombreada indica que en el registro correspondiente al vértice puede haber otra información.

b) ***Edge File***: Este archivo contiene las aristas de G y todas las listas de adyacencia de G, donde cada lista se mantiene en la memoria por medio de una lista ligada. Cada registro del Edge File representa una arista única en G y, por tanto, corresponde a un vértice único en una lista de adyacencia. Normalmente, el registro tiene la forma

EDGE	BEG-V	END-V	NEXT-E	

Aquí:

1) EDGE es el nombre de la arista (en caso de tener una).
2) BEG-V apunta a la ubicación del Vertex File del vértice inicial de la arista.
3) END-V apunta a la ubicación del Vertex File del vértice terminal de la arista. Las listas de adyacencia aparecen en este campo.
4) NEXT-E apunta a la ubicación en el Edge File del siguiente vértice en la lista de adyacencia.

Recuerde que las listas de adyacencia constan de vértices terminales, por lo que se mantienen mediante el campo END-V. El área sombreada indica que en el registro correspondiente a la arista puede haber otra información. Se observa que el orden de los vértices en una lista de adyacencia no depende del orden en que las aristas (pares de vértices) aparecen en los datos de entrada.

En la figura 9-10 se muestra la forma en que el grafo *G* en la figura 9-9*a*) puede aparecer en la memoria. Aquí los vértices de *G* se mantienen en la memoria por medio de una lista ligada usando la variable START para apuntar al primer vértice. (En forma alterna, podría usarse un arreglo lineal para la lista de vértices, y así no sería necesario NEXT-V.) La elección de ocho ubicaciones para el Vertex File y 10 localizaciones para el Edge File es arbitraria. El espacio adicional en los archivos se usa en caso de que en el grafo se inserten vértices o aristas adicionales. En la figura 9-10 también se muestra, con flechas, la lista de adyacencia [*B, C, D*] del vértice *A*.

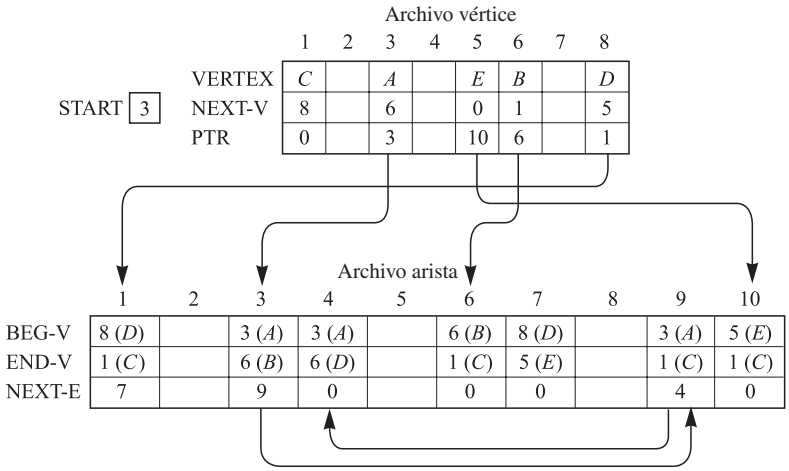


Figura 9-10

9.8 ALGORITMOS DE GRAFOS: BÚSQUEDAS EN PROFUNDIDAD Y EN ANCHURA

En esta sección se analizan dos importantes algoritmos de grafos para un grafo dado *G*. Cualquier algoritmo de grafos particular puede depender de la forma en que *G* se mantiene en la memoria. Aquí se supone que *G* se mantiene en la memoria por medio de su estructura de adyacencia. El grafo de prueba *G* con su estructura de adyacencia se muestran en la figura 9-11.

Muchas aplicaciones de grafos requieren el examen sistemático de los vértices y las aristas de un grafo *G*. Hay dos formas normales para hacer lo anterior. Una forma se denomina *búsqueda en profundidad* (DFS: depth-first search) y la otra, *búsqueda en anchura* (BFS: breadth-first search). (Estos algoritmos son esencialmente idénticos a los correspondientes para grafos no dirigidos del capítulo 8.)

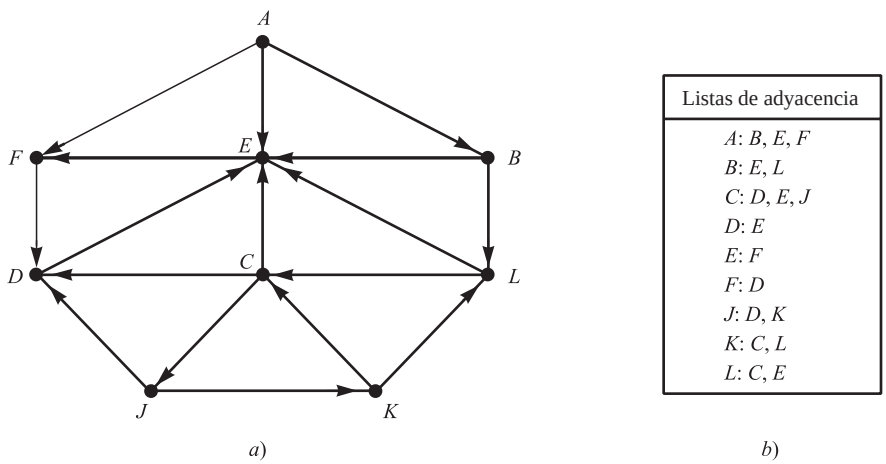


Figura 9-11

Durante la ejecución de los algoritmos, cada vértice (nodo) N de G se encuentra en uno de tres estados, denominados *status* de N, como sigue:

STATUS = 1: (Estado Ready) El estado inicial del vértice N.

STATUS = 2: (Estado Waiting) El vértice N está en una lista (de espera), en espera de ser procesado.

STATUS = 3: (Estado Processed) El vértice N ha sido procesado.

La lista de espera para la búsqueda en profundidad es una STACK —modificada— (que se escribe horizontalmente con la parte superior de STACK a la izquierda), mientras la lista de espera para la búsqueda en anchura es una QUEUE.

a) **Búsqueda en profundidad:** La idea general detrás de una búsqueda en profundidad que empieza en un vértice inicial A es: primero se procesa el vértice inicial A. Luego se procesa cada vértice N a lo largo de un camino P que empiece en A; es decir, se procesa un vecino de A, luego un vecino de un vecino de A y así en lo sucesivo. Después de llegar a un "punto muerto"; es decir, a un vértice sin vecino no procesado, se retrocede sobre el camino P hasta que es posible continuar a lo largo de otro camino P'. Y se continúa del mismo modo. El retroceso se logra usando una STACK para mantener los vértices iniciales de futuros caminos posibles. También se requiere un campo STATUS que indica el estado actual de cualquier vértice, de modo que ningún vértice sea procesado más de una vez. El algoritmo se muestra en la figura 9-12.

Algoritmo 9.2 (De búsqueda en profundidad): Este algoritmo ejecuta una búsqueda en profundidad sobre un grafo dirigido G, empezando en un vértice inicial A.

Paso 1. Todos los vértices se inicializan en el estado ready (STATUS = 1).

Paso 2. El vértice inicial A se introduce en STACK y el status de A cambia al estado waiting (STATUS = 2).

Paso 3. Repetir los pasos 4 y 5 hasta que STACK esté vacía.

Paso 4. El vértice superior N se saca de STACK. Se procesa N, y se establece STATUS (N) = 3, el estado processed.

Paso 5. Examinar cada vecino J de N.

a) Si STATUS (J) = 1 (estado ready), J se coloca sobre STACK y se restablece STATUS (J) = 2 (estado waiting).
b) Si STATUS (J) = 2 (estado waiting), el J previo se elimina de STACK y el J actual se coloca sobre STACK.
c) Si STATUS (J) = 3 (estado processed), se ignora el vértice J.
[Fin del ciclo del paso 3.]

Paso 6. Salir.

Figura 9-12

El algoritmo 9.2 procesa sólo aquellos vértices que son alcanzables desde un vértice inicial A. Suponga que se desea procesar todos los vértices en el grafo G. Así, el algoritmo debe modificarse de modo que vuelva a empezar con otro vértice que aún se encuentre en el estado ready (STATE = 1). Este nuevo vértice, por ejemplo B, puede obtenerse al recorrer la lista de vértices.

Observación: Técnicamente, la estructura STACK en el algoritmo 9.2 no es una pila ya que, en el paso 5*b*), se permite la eliminación de un vértice J y luego su inserción en el frente de la pila. (Aunque se trata del mismo vértice J, representa una arista distinta.) Si el J previo no se elimina en el paso 5*b*), entonces se obtiene un algoritmo de recorrido alterno.

EJEMPLO 9.10 Considere el grafo de prueba *G* en la figura 9-11. Suponga que desea encontrar e imprimir todos los vértices alcanzables desde el vértice *J* (incluso a *J*). Una forma de hacerlo es aplicar un algoritmo en profundidad de *G* empezando en el vértice *J*.

Al aplicar el algoritmo 9.2, los vértices se procesan e imprimen en el orden siguiente:

$$J, \quad K, \quad L, \quad E, \quad F, \quad D, \quad C$$

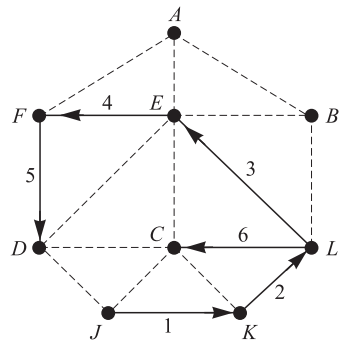
En la figura 9-13*a*) se muestra la secuencia de las listas de espera en STACK y los vértices que están en proceso. (La línea diagonal / indica que un vértice se elimina de la lista de espera.) Recuerde que cada vértice, excepto *J*, proviene de una lista de adyacencia, y por tanto, es el vértice terminal de una arista única del grafo. La arista se ha indicado al etiquetar el vértice terminal con el vértice inicial de la arista como un subíndice. Por ejemplo,

$$D_j$$

significa que *D* está en la lista de adyacencia de *J*, y entonces que *D* es el vértice terminal de una arista que empieza en *J*. Estas aristas constituyen un árbol *T* con raíz cuya raíz es *J*, lo cual se muestra en la figura 9-13*b*). (Los números indican el orden en que las aristas se agregan al árbol.) Este árbol *T* genera el subgrafo G' de *G* que consta de los vértices alcanzables desde *J*.

STACK	Vértice
J	J
K_J, D_J	K_J
L_K, C_K, D_J	L_K
$E_L, C_L, \not{C}_K, D_J$	E_L
F_E, C_L, D_J	F_E
$D_F, C_L, \not{D}_J$	D_F
C_L	C_L
∅	

a)



b)

Figura 9-13

b) **Búsqueda en anchura:** La idea general detrás de una búsqueda en anchura que empieza en un vértice inicial *A* es: primero se procesa el vértice inicial *A*. Luego se procesan todos los vecinos de *A* y enseguida se procesan todos los vecinos de los vecinos de *A*. Y así se continúa. Resulta evidente que es necesario mantener la pista de los vecinos de un vértice, así como garantizar que ningún vértice sea procesado dos veces. Esto se logra usando una QUEUE para mantener los vértices que están en espera de ser procesados; y mediante un campo STATUS que indica el estado actual de un vértice. El algoritmo se muestra en la figura 9-14.

El algoritmo 9.3 sólo procesa aquellos vértices que son alcanzables desde un vértice inicial *A*. Suponga que se desea procesar todos los vértices en un grafo *G*. Entonces es necesario modificar el algoritmo de modo que nuevamente empiece con otro vértice que aún se encuentre en el estado ready (STATE = 1). Este nuevo vértice *B*, por ejemplo, puede obtenerse al recorrer la lista de vértices.

EJEMPLO 9.11 Considere el grafo de prueba *G* en la figura 9-11. Suponga que *G* representa los vuelos diarios entre ciudades y que desea volar de la ciudad *A* a la ciudad *J* con el menor número de escalas. Es decir, se quiere encontrar un camino más corto *P* de *A* a *J* (donde cada arista tiene un peso de 1). Una forma de hacer lo anterior es usar una búsqueda en anchura de *G* empezando en el vértice *A*, y detenerse tan pronto como se encuentre *J*.

En la figura 9-15*a*) se muestra la secuencia de las listas de espera en QUEUE y los vértices que se están procesando hasta el momento en que se encuentra el vértice *J*. Luego se trabaja hacia atrás a partir de *J* para obtener el siguiente camino deseado que se muestra en la figura 9-15*b*):

$$J_C \leftarrow C_L \leftarrow L_B \leftarrow B_A \leftarrow A \quad \text{o} \quad A \rightarrow B \rightarrow L \rightarrow C \rightarrow J$$

Así, un vuelo de la ciudad *A* a la ciudad *J* hará tres escalas intermedias en *B*, *L* y *C*. Observe que el camino no incluye todos los vértices procesados por el algoritmo.

Algoritmo 9.3 (de búsqueda en anchura): Este algoritmo ejecuta una búsqueda en anchura sobre un grafo dirigido G, empezando en un vértice inicial A.

Paso 1. Todos los vértices se inicializan en el estado ready (STATUS = 1).

Paso 2. El vértice inicial A se introduce en QUEUE y el status de A se cambia al estado waiting (STATUS = 2).

Paso 3. Repetir los pasos 4 y 5 hasta que QUEUE esté vacía.

Paso 4. Sacar el primer vértice N de QUEUE. Se procesa N, y se establece STATUS (N) = 3, el estado processed.

Paso 5. Se examina cada vecino J de N.
a) Si STATUS (J) = 1 (estado ready), J se coloca en la parte trasera de QUEUE y se restablece STATUS (J) = 2 (estado waiting).
b) Si STATUS (J) = 2 (estado waiting) o STATUS(J) = 3 (estado processed), se ignora el vértice J.

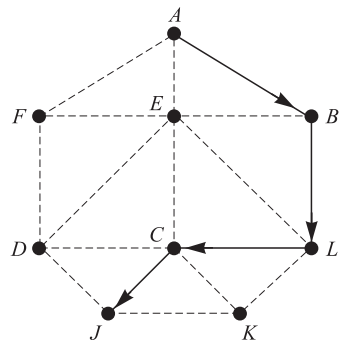
[Fin del ciclo del paso 3.]

Paso 6. Salir.

Figura 9-14

QUEUE	Vértice
A	A
F_A, E_A, B_A	B_A
L_B, F_A, E_A	E_A
L_B, F_A	F_A
D_F, L_B	L_B
C_L, D_F	D_F
C_L	C_L
J_C	J_C

a)



b)

Figura 9-15

9.9 GRAFOS DIRIGIDOS LIBRES DE CICLOS, ORDENACIÓN TOPOLÓGICA

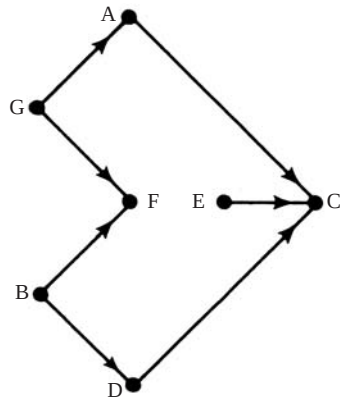
Sea S un grafo dirigido con las dos propiedades siguientes:

1) Cada vértice v_i de S representa una tarea.
2) Cada arista (dirigida) (u, v) de S significa que la tarea u debe completarse antes de empezar la tarea v.

Se observa que un grafo S así no puede contener ningún ciclo, como $P = (u, v, w, u)$, puesto que, en caso contrario, sería necesario completar u antes de empezar v, completar v antes de empezar w y completar w antes de empezar u. Es decir, no es posible comenzar ninguna de las tres tareas del ciclo.

Se dice que un grafo S así, que representa tareas y una relación prerrequisito y que no puede tener ningún ciclo, es *libre de ciclos* o *acíclico*. La forma abreviada de denominar a un grafo acíclico dirigido (libre de ciclos) es *gad*. En la figura 9-16 se muestra un ejemplo de un grafo así.

Una operación fundamental sobre un gad S consiste en procesar los vértices uno después de otro de modo que el vértice u siempre sea procesado antes que el vértice v siempre que (u, v) sea una arista. Un ordenamiento lineal T así de los vértices de S, que puede no ser único, se denomina *ordenamiento topológico*.



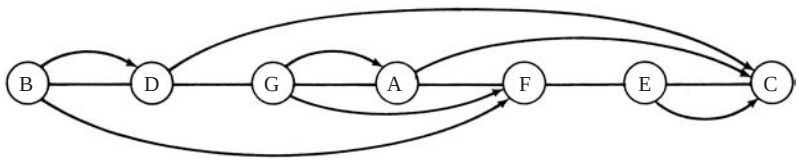
a)

Listas de adyacencia		
A:	C	
B:	D,	F
C:		
D:	C	
E:	C	
F:		
G:	A,	F

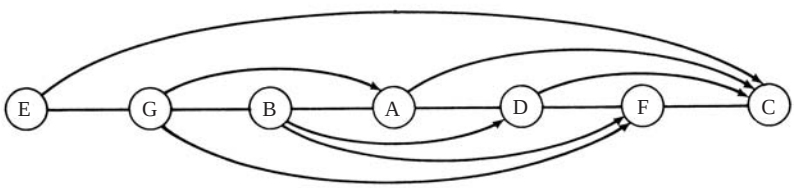
b)

Figura 9-16

En la figura 9-17 se muestran dos ordenamientos topológicos del grafo *S* en la figura 9-16. En la figura 9-17 se han incluido las aristas de *S* para mostrar que coinciden con la dirección del ordenamiento lineal.



a)



b)

Figura 9-17 Dos ordenamientos topológicos

A continuación se presenta el resultado teórico más importante de esta sección.

Teorema 9.8: Sea *S* un grafo libre de ciclos dirigido finito. Entonces existe un ordenamiento topológico *T* del grafo *S*.

Observe que el teorema sólo establece que existe un ordenamiento topológico. A continuación se proporciona un algoritmo que encuentra un ordenamiento topológico. La idea más importante del algoritmo es que cualquier vértice (nodo) *N* con grado de entrada cero puede escogerse como el primer elemento en el ordenamiento *T*. En esencia el algoritmo repite los dos pasos siguientes hasta que *S* está vacía:

1) Encontrar un vértice *N* con grado de entrada cero.
2) Eliminar *N* y sus aristas del grafo *S*.

Se usa una QUEUE auxiliar para mantener temporalmente todos los vértices con grado cero. El algoritmo se muestra en la figura 9-18.

Algoritmo 9.4: El algoritmo encuentra un ordenamiento topológico T de un grafo libre de ciclos dirigido S.

Paso 1. Encontrar el grado de entrada INDEG(N) de cada vértice N de S.

Paso 2. Insertar en QUEUE todos los vértices con grado cero.

Paso 3. Repetir los pasos 4 y 5 hasta que QUEUE esté vacía.

Paso 4. Eliminar y procesar el vértice frontal N de QUEUE.

Paso 5. Repetir para cada vecino M del vértice N.
a) Establecer INDEG(M) : = INDEG(M) – 1.
[Así se elimina la arista de N a M.]
b) Si INDEG(M) = 0, agregar M a QUEUE.
[Fin del ciclo.]
[Fin del ciclo del paso 3.]

Paso 6. Salir.

Figura 9-18

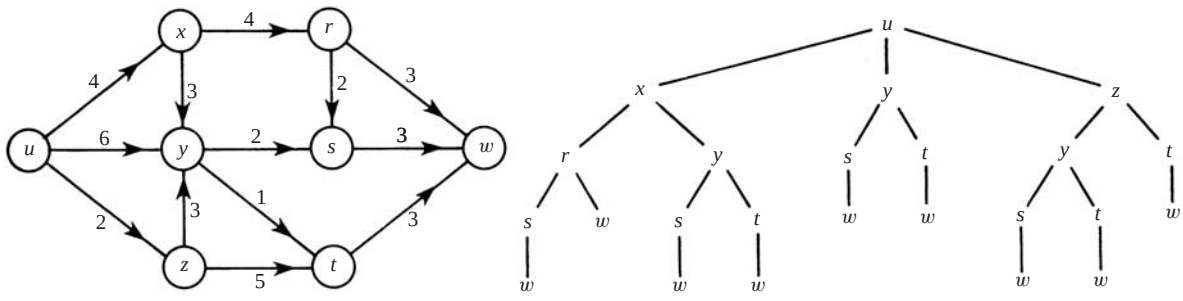
EJEMPLO 9.12 Suponga que el algoritmo 9.4 se aplica al grafo S en la figura 9-16. Se obtiene la siguiente secuencia de los elementos de QUEUE y la secuencia de los vértices que están en proceso:

QUEUE	*GEB*	*DGE*	*DG*	*FAD*	*FA*	*CF*	*C*	∅
Vértice	*B*	*E*	*G*	*D*	*A*	*F*	*C*	

Así, los vértices se procesan en el orden: *B, E, G, D, A, F*.

9.10 ALGORITMO DE PODA PARA EL CAMINO MÁS CORTO

Si G es un grafo libre de ciclos dirigido ponderado, se busca el camino más corto entre dos vértices, por ejemplo, u y w. Se supone que G es finito, de modo que en cada paso hay un número finito de movimientos. Puesto que G es libre de ciclos, todos los caminos entre u y w se proporcionan mediante un árbol con raíz cuya raíz sea u. En la figura 9-19b) se enumeran todos los caminos entre u y w en el grafo en la figura 9-19a).



a) *b*)

Figura 9-19

Una forma de encontrar el camino más corto entre u y w es calcular las longitudes de todos los caminos que corresponden a las raíces del árbol. Por otra parte, suponga que dos caminos parciales conducen a un vértice intermedio v. A partir de entonces, sólo es necesario considerar el camino parcial más corto; es decir, el árbol se poda en el vértice correspondiente al camino parcial más largo. El algoritmo de poda se describe a continuación.

Algoritmo de poda

Este algoritmo encuentra el camino más corto entre un vértice u y un vértice w en un grafo G dirigido libre de ciclos. El algoritmo posee las siguientes propiedades:

a) Durante el algoritmo a cada vértice v' de G se le asignan:

1) Un número $\ell(v')$ que denota la longitud mínima actual de un camino de u a v'.
2) Un camino $p(v')$ de u a v' de longitud $\ell(v')$.

b) Al inicio se hace $\ell(u) = 0$ y $p(u) = u$. A cualquier otro vértice v al inicio se le asigna $\ell(v) = \infty$ y $p(v) = \varnothing$.

c) En cada paso el algoritmo examina una arista $e = (v', v)$ de v' a v con, por ejemplo, longitud k. Se calcula $\ell(v') + k$.

1) Suponga que $\ell(v') + k < \ell(v)$. Entonces se ha encontrado un camino más corto de u a v. Así, se actualiza:

$$\ell(v) = \ell(v') + k \quad \text{y} \quad p(v) = p(v')v$$

(Esto siempre es cierto cuando $\ell(v) = \infty$; es decir, cuando el vértice v se introduce por primera vez.)

2) En caso contrario, no se modifican $\ell(v)$ ni $p(v)$.

Si ninguna otra arista no examinada entra en v, se dice que se ha determinado $p(v)$.

d) El algoritmo termina cuando se ha determinado $p(w)$.

Observación: La arista $e = (v', v)$ en el inciso *c*) sólo puede escogerse si v' ha sido visitado previamente; es decir, si $p(v')$ no está vacío. Además, suele ser mejor examinar una arista que empieza en un vértice v' cuyo camino $p(v')$ ha sido determinado.

EJEMPLO 9.13 El algoritmo de poda se aplica al grafo G en la figura 9-19*a*).

Desde *u*: los vértices sucesivos son x, y y z, que se introducen por primera vez. Así:

1) se hace $\ell(x) = 4$, $p(x) = ux$.
2) se hace $\ell(y) = 6$, $p(y) = uy$.
3) se hace $\ell(z) = 2$, $p(z) = uz$.

Observe que se han determinado $p(x)$ y $p(z)$.

Desde *x*: los vértices sucesivos son r, introducido por primera vez, y y. Así:

1) Se hace $\ell(r) = 4 + 4 = 8$ y $p(r) = p(x)r = uxr$.
2) Se calcula:

$$\ell(x) + k = 4 + 3 = 7 \quad \text{que no es menor que} \quad \ell(y) = 6.$$

Por tanto, $\ell(y)$ y $p(y)$ se dejan solos.

Observe que se ha determinado $p(r)$.

Desde *z*: los vértices sucesivos son t, introducido por primera vez, y y. Así:

1) Se hace $\ell(t) = \ell(z) + k = 2 + 5 = 7$ y $p(t) = p(z)t = urt$.
2) Se calcula:

$$\ell(z) + k = 2 + 3 = 5 \quad \text{que es menor que} \quad \ell(y) = 6.$$

Se ha encontrado un camino más corto hacia y, de modo que se actualizan $\ell(y)$ y $p(y)$; se hace

$$\ell(y) = \ell(z) + k = 5 \quad \text{y} \quad p(y) = p(z)y = uzy$$

Ahora se ha determinado $p(y)$.

Desde *y*: los vértices sucesivos son *s*, introducido por primera vez, y *t*. Así:

1) Se hace $\ell(s) = \ell(y) + k = 5 + 2 = 7$ y $p(s) = p(y)s = uzys$.

2) Se calcula:

$$\ell(y) + k = 5 + 1 = 6 \quad \text{que es menor que} \quad \ell(t) = 7.$$

Por tanto, se cambian $\ell(t)$ y $p(t)$ para leer:

$$\ell(t) = \ell(y) + 1 = 6 \quad \text{y} \quad p(t) = p(y)t = uzyt.$$

Ahora se ha determinado $p(t)$.

Desde *r*: los vértices sucesivos son w, introducido por primera vez, y s. Así:

1) Sea $\ell(w) = \ell(r) + 3 = 11$ y $p(w) = p(r)w = uxrw$.

2) Se calcula:

$$\ell(r) + k = 8 + 2 = 10 \quad \text{que es menor que} \quad \ell(s) = 7.$$

Por tanto, $\ell(s)$ y $p(s)$ se dejan solos.

Observe que se ha determinado $p(s)$.

Desde *s*: el vértice sucesivo es w. Se calcula:

$$\ell(s) + k = 7 + 3 = 10 \quad \text{que es menor que} \quad \ell(w) = 11.$$

Por tanto, se cambian $\ell(w)$ y $p(w)$ para leer:

$$\ell(w) = \ell(s) + 3 = 10 \quad \text{y} \quad p(w) = p(s)w = uzysw.$$

Desde *t*: el vértice sucesivo es w. Se calcula:

$$\ell(t) + k = 6 + 3 = 9 \quad \text{que es menor que} \quad \ell(w) = 10.$$

Por tanto, se actualizan $\ell(w)$ y $p(w)$ como sigue:

$$\ell(w) = \ell(t) + 3 = 9 \quad \text{y} \quad p(w) = p(t) = uzytw$$

Ahora se ha determinado $p(w)$.

El algoritmo ha terminado puesto que se ha determinado $p(w)$. Por tanto, $p(w) = uzytw$ es el camino más corto de u a w y $\ell(w) = 9$.

Las aristas que se analizaron en el ejemplo precedente constituyen el árbol con raíz en la figura 9-20. Es el árbol de la figura 9-19*b*) que ha sido podado en los vértices que pertenecen a caminos parciales más largos. Observe que sólo fue necesario examinar 13 de las 23 aristas originales del árbol.

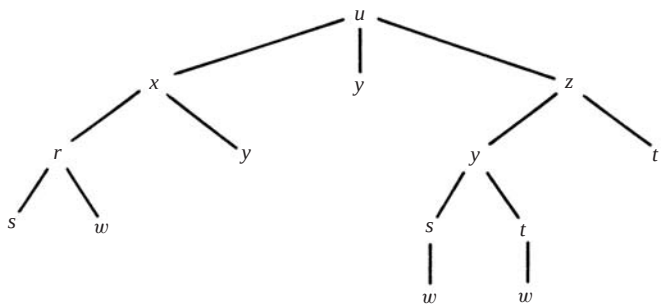


Figura 9-20

PROBLEMAS RESUELTOS

TERMINOLOGÍA DE GRAFOS

9.1 Sea G el grafo dirigido en la figura 9-21*a*).

a) Describa formalmente a G.
b) Encuentre todos los caminos simples de X a Z.
c) Encuentre todos los caminos simples de Y a Z.
d) Encuentre todos los ciclos en G.
e) ¿G es unilateralmente conexo?
f) ¿G es fuertemente conexo?

a) El conjunto de vértices V tiene cuatro vértices y el conjunto de aristas E tiene siete aristas (dirigidas) como sigue:

$$V = \{X, Y, Z, W\} \quad \text{y} \quad E = \{(X, Y), (X, Z), (X, W), (Y, W), (Z, Y), (Z, W), (W, Z)\}$$

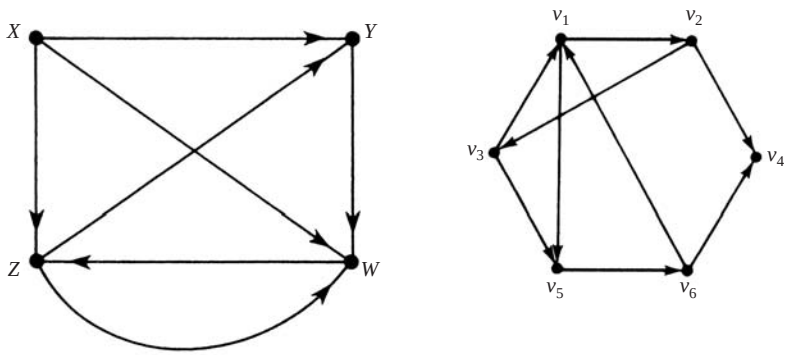
b) Hay tres caminos simples de X a Z, que son (X, Z), (X, W, Z) y (X, Y, W, Z).

c) De Y a Z sólo hay un camino simple, que es (Y, W, Z).

d) En G sólo hay un ciclo, que es (Y, W, Z, Y).

e) G es unilateralmente conexo, ya que (X, Y, W, Z) es un camino de expansión.

f) G no es fuertemente conexo porque no hay ningún camino de expansión.



a) *b*)

Figura 9-21

9.2 Sea G el grafo dirigido en la figura 9-21*a*).

a) Encuentre el grado de entrada y el grado de salida de cada vértice de G.
b) Encuentre la lista de sucesores de cada vértice de G.
c) ¿Hay alguna fuente o algún sumidero?
d) Encuentre el subgrafo H de G determinado por el conjunto de vértices $V' = X, Y, Z$.

a) Se cuenta el número de aristas que empiezan y terminan en un vértice v para obtener, respectivamente, indeg(v) y outdeg(v). Lo anterior produce los datos siguientes:

$$\text{indeg}(X) = 0, \quad \text{indeg}(Y) = 2, \quad \text{indeg}(Z) = 2, \quad \text{indeg}(W) = 3,$$
$$\text{outdeg}(X) = 3, \quad \text{outdeg}(Y) = 1, \quad \text{outdeg}(Z) = 2, \quad \text{outdeg}(W) = 1,$$

(Como era de esperar, la suma de los grados de entrada y la suma de los grados de salida es igual —cada una— a 7, el número de aristas).

b) El vértice v se agrega a la lista de sucesores (u) para cada arista (u, v) en G. Así se obtiene:

$$\text{suc}(X) = [Y, Z, W], \quad \text{suc}(Y) = [W], \quad \text{suc}(Z) = [Y, W], \quad \text{suc}(W) = [Z]$$

c) X es una fuente a la que no entra ninguna arista; es decir, indeg(X) = 0. No hay sumideros, ya que cada vértice es el punto inicial de una arista; es decir, tiene grado de salida distinto de cero.

d) Sea E' que consta de todas las aristas de G cuyos puntos terminales están en V'. Así se obtiene $E' = \{(X, Y), (X, Z), (Z, Y)\}$. Entonces $H = H(V', E')$.

9.3 Sea G el grafo dirigido en la figura 9-21*b*).

a) Encuentre dos caminos simples de v_1 a v_6. ¿Es $\alpha = (v_1, v_2, v_4, v_6)$ un camino simple?
b) Encuentre todos los ciclos en G que incluyen a v_3.
c) ¿G es unilateralmente conexo? ¿Fuertemente conexo?
d) Encuentre la lista de sucesores de cada vértice de G.
e) ¿Hay alguna fuente en G? ¿Algún sumidero?

a) En un camino simple todos los vértices son distintos. Así, (v_1, v_5, v_6) y $(v_1, v_2, v_3, v_5, v_6)$ son dos caminos simples de v_1 a v_6. La secuencia ni siquiera es un camino puesto que la arista que une v_4 a v_6 no empieza en v_4.

b) Hay dos ciclos así: (v_3, v_1, v_2, v_3) y $(v_3, v_5, v_6, v_1, v_2, v_3)$.

c) G es unilateralmente conexo puesto que $(v_1, v_2, v_3, v_5, v_6, v_4)$ es un camino de expansión. G no es fuertemente conexo, porque no hay ningún camino de expansión cerrado.

d) El vértice v se agrega a la lista de sucesores suc(u) para cada arista (u, v) en G. Así se obtiene:

$$\text{suc}(v_1) = [v_2, v_5], \quad \text{suc}(v_2) = [v_3, v_4], \quad \text{suc}(v_3) = [v_1, v_5]$$
$$\text{suc}(v_4) = \varnothing, \quad \text{suc}(v_5) = [v_6], \quad \text{suc}(v_6) = [v_1, v_4]$$

(Como era de esperar, el número de sucesores es igual a 9, que es el número de aristas).

e) No hay fuentes, ya que todo vértice es el punto terminal de alguna arista. Sólo v_4 es un sumidero puesto que ninguna arista empieza en v_4; es decir, suc(v_4) = $\varnothing$, el conjunto vacío.

9.4 Sea G el grafo dirigido con conjunto de vértices $V(G) = (a, b, c, d, e, f, g)$ y conjunto de aristas:

$$E(G) = \{(a, a), (b, e), (a, e), (e, b), (g, c), (a, e), (d, f), (d, b), (g, g)\}$$

a) Identifique cualquier lazo o aristas paralelas.
b) ¿Hay alguna fuente en G?
c) ¿Hay algún sumidero en G?
d) Encuentre el subgrafo H de G determinado por el conjunto de vértices $V' = \{a, b, c, d\}$.

a) Un lazo es una arista cuyos puntos inicial y terminal son los mismos; por tanto, (a, a) y (g, g) son lazos. Dos aristas son paralelos si sus puntos inicial y terminal son los mismos. Así, (a, e) y (a, e) son aristas paralelas.

b) El vértice d es una fuente, ya que ninguna arista termina en d; es decir, d no aparece como el segundo elemento en ninguna arista. No hay otras fuentes.

c) Tanto c como f son sumideros, ya que ninguna arista empieza en c o en f; es decir, ni c ni f aparecen como el primer elemento en ninguna arista. No hay otros sumideros.

d) Sea E' que consta de todas las aristas de G cuyos puntos terminales están en $V' = \{a, b, c, d\}$. Así se obtiene $E' = \{(a, a), (d, b)\}$. Entonces, $H = H(V', E')$.

ÁRBOLES CON RAÍZ, ÁRBOLES CON RAÍZ ORDENADOS

9.5 Sea T el árbol con raíz en la figura 9-22.

a) Identifique el camino α de la raíz R a cada uno de los vértices siguientes, y encuentre el número de nivel n del vértice: *i*) H; *ii*) F; *iii*) M.
b) Encuentre los hermanos de E.
c) Encuentre las hojas de T.

a) Los vértices del árbol se enumeran procediendo a partir de *R* hacia el vértice. El número de vértices, que no sean *R*, es el número de nivel:

$$i)\ \alpha = (R, A, C, H),\ n = 3; \quad ii)\ \alpha = (R, B, F),\ n = 2; \quad iii)\ \alpha = (R, B, G, L, M),\ n = 4.$$

b) Los hermanos de *E* son *F* y *G*, puesto que tienen el mismo padre.

c) Las hojas son los vértices sin hijos; es decir, *H, D, I, J, K, M, N*

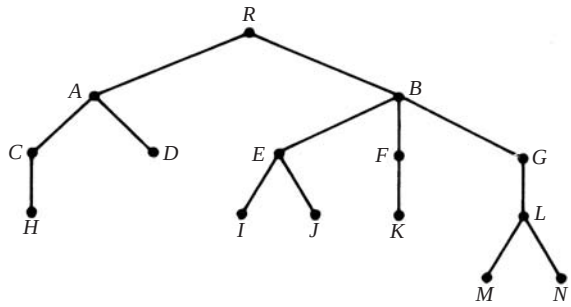


Figura 9-22

9.6 Sea *T* el árbol con raíz ordenado en la figura 9-23 cuyos vértices se han etiquetado mediante el sistema universal de direcciones. Encuentre el orden lexicográfico de las direcciones del árbol *T*.

Un árbol *T* con raíz ordenado suele trazarse de modo que las aristas estén ordenadas de izquierda a derecha como en la figura 9-23. El orden lexicográfico se obtiene al leer la rama que está más a la izquierda, luego la segunda rama a la izquierda y así en lo sucesivo.

Al leer la rama que está más a la izquierda de *T* se obtiene:

0, 1, 1.1, 1.1.1

La rama siguiente es 1.2, 1.2.1, 1.2.1.1, de modo que esto se agrega a la lista para obtener

0, 1, 1.1, 1.1.1 1.2 1.2.1, 1.2.1.1

Al proceder se esta manera, finalmente se obtiene

0, 1, 1.1, 1.1.1 1.2 1.2.1, 1.2.1.1, 1.2.2 1.3, 2, 2.1, 2.2.1

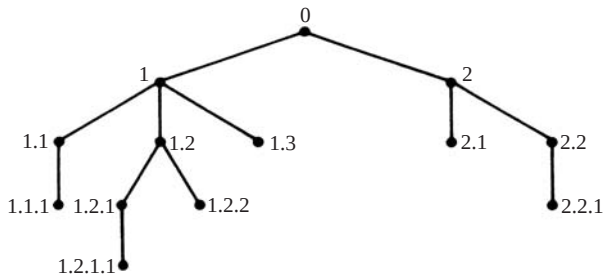


Figura 9-23

REPRESENTACIÓN SECUENCIAL DE GRAFOS

9.7 Considere el grafo *G* en la figura 9-21*a*), y suponga que los vértices están almacenados en la memoria en el arreglo:

DATA: *X, Y, Z, W*

a) Encuentre la matriz de adyacencia A del grafo G y las potencias A^2, A^3, A^4.
b) Encuentre la matriz de caminos P de G con las potencias de A. ¿G es fuertemente conexo?

a) Los vértices suelen ordenarse según la forma en que aparecen en la memoria; es decir, se supone $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. La matriz de adyacencia $A = [a_{ij}]$ se obtiene al hacer $a_{ij} = 1$ si hay una arista de v_i a v_j; y 0 en caso contrario. A continuación se muestran la matriz A y sus potencias:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A^2 = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 0 & 2 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

b) Puesto que G tiene 4 vértices, sólo es necesario encontrar la matriz $B_4 = A + A^2 + A^3 + A^4$ y luego la matriz de caminos $P = [p_{ij}]$ se obtiene al hacer $p_{ij} = 1$ siempre que en la matriz B_4 haya una entrada diferente de cero, y 0 en caso contrario. A continuación se muestran las matrices B_4 y P:

$$B_4 = \begin{bmatrix} 0 & 5 & 6 & 8 \\ 0 & 1 & 2 & 3 \\ 0 & 3 & 3 & 5 \\ 0 & 2 & 3 & 5 \end{bmatrix} \quad \text{y} \quad P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

La matriz de caminos P indica que no hay caminos desde ningún nodo hacia v_1. Por tanto, G no es fuertemente conexo.

9.8 Considere la matriz de adyacencia A del grafo G en la figura 9-19*a*) obtenida en el problema 9.7. Encuentre la matriz de caminos P de G con el algoritmo de Warshall en lugar de las potencias de A.

Al inicio se hace $P_0 = A$. Luego, P_1, P_2, P_3, P_4 se obtienen recursivamente al hacer

$$P_k[i, j] = P_{k-1}[i, j] \vee (P_{k-1}[i, k] \wedge P_{k-1}[k, j])$$

donde $P_k[i, j]$ denota el ij-ésimo elemento de la matriz P_k. Es decir, al hacer

$$P_k[i, j] = 1 \quad \text{si} \quad P_{k-1}[i, j] = 1 \quad \text{o si ambas} \quad P_{k-1}[i, k] = 1 \quad \text{y} \quad P_{k-1}[k, j] = 1$$

Las matrices P_1, P_2, P_3, P_4 son las siguientes:

$$P_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad P_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Observe que $P_1 = P_2 = A$. Los cambios en P_3 ocurren por las razones siguientes:

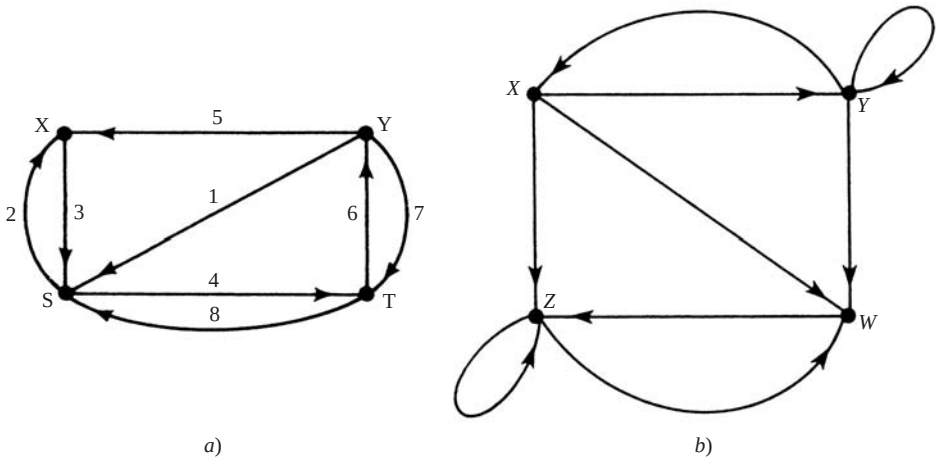
$$P_3[4, 2] = 1 \quad \text{porque} \quad P_2[4, 3] = 1 \text{ y } P_2[3, 2] = 1$$
$$P_3[4, 4] = 1 \quad \text{porque} \quad P_2[4, 3] = 1 \text{ y } P_2[3, 4] = 1$$

9.9 Dibuje una representación del grafo ponderado G que se mantiene en la memoria mediante el siguiente arreglo de vértices DATA y la matriz de pesos W:

$$\text{DATA: } X, Y, S, T; \quad W = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 5 & 0 & 1 & 7 \\ 2 & 0 & 0 & 4 \\ 0 & 6 & 8 & 0 \end{bmatrix}$$

La representación se muestra en la figura 9-24*a*). Los vértices se etiquetaron con las entradas en DATA.

Si se supone que $v_1 = X$, $v_2 = Y$, $v_3 = S$, $v_4 = T$, el orden de los vértices aparece en el arreglo DATA, se traza una arista de v_i a v_j con peso w_{ij} cuando $w_{ij} \neq 0$.



a) *b*)

Figura 9-24

REPRESENTACIÓN LIGADA DE GRAFOS

9.10 Sea G el grafo presentado por medio de la tabla siguiente:

$$G = [X : Y, Z, W; \quad Y : X, Y, W; \quad Z : Z,W; \quad W : Z]$$

a) Encuentre el número de vértices y aristas en G.
b) Trace el grafo de G.
c) ¿Hay alguna fuente o algún sumidero?

a) La tabla indica que hay cuatro vértices, X, Y, Z, W. Los grados de salida de los vértices son 3, 3, 2, 1, respectivamente. Por tanto, hay $3 + 3 + 2 + 1 = 9$ aristas.

b) Con las listas de adyacencia en la figura 9-24*b*) se traza el grafo.

c) Ningún vértice tiene grado de salida cero, por lo que no hay sumideros. Asimismo, ningún vértice tiene grado de entrada cero; es decir, cada vértice es un sucesor y no hay fuentes.

9.11 Un grafo ponderado G con seis vértices, $A, B, \ldots, F$, se almacena en la memoria mediante una representación ligada con un archivo de vértices y un archivo de aristas como en la figura 9-25*a*).

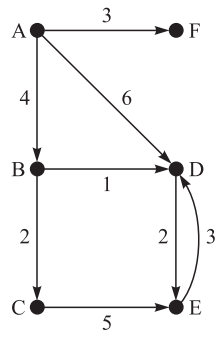
Archivo vértice

		1	2	3	4	5	6	7	8
	VERTEX	*D*		*B*	*F*	*A*		*C*	*E*
START 3	NEXT-V	7		1	5	0		8	4
	PTR	9		3	0	6		10	1

Archivo arista

	1	2	3	4	5	6	7	8	9	10
BEG-V	8	5	3		5	5	3		1	7
END-V	1	4	7		3	1	1		8	8
NEXT-E	0	5	7		0	2	0		0	0
WEIGHT	3	4	2		6	3	1		2	5

a)



b)

Figura 9-25

a) Enumere los vértices en el orden en que aparecen en la memoria.
b) Encuentre la lista de sucesores suc(v) de cada vértice v.
c) Trace el grafo de G.

a) Puesto que START = 3, la lista empieza con el vértice *B*. Luego, NEXT-V indica ir hacia 1(*D*), enseguida a 7(*C*), a 8(*E*), a 4(*F*) y luego a 5(*A*); es decir,

$$B,\quad D,\quad C,\quad E,\quad F,\quad A$$

b) Aquí suc(*A*) = [1(*D*), 4(*F*), 3(*B*)] = [*D*, *F*, *B*]. Específicamente, PTR[5(*A*)] = 6 y END-V[6] = 1(*D*) indican que suc(*A*) empieza con *D*. Luego, NEXT-E[6] = 2 y END-V[2] = 4(*F*) indican que *F* es el siguiente vértice en suc(*A*). Luego, NEXT-E[2] = 5 y END-V[5] = 3(*B*) indican que *B* es el siguiente vértice en suc(*A*). Sin embargo, NEXT-E[5] = 0 indica que ya no hay más sucesores de *A*. En forma semejante,

$$\text{suc}(B) = [C, D],\quad \text{suc}(C) = [E],\quad \text{suc}(D) = [E],\quad \text{suc}(E) = [D]$$

Además, suc(*F*) = ∅, puesto que PTR[4(*F*)] = 0. En otras palabras,

$$G = [A\!:\!D, F, B;\quad B\!:\!C, D;\quad C\!:\!E;\quad D\!:\!E;\quad E\!:\!D;\quad F\!:\!\varnothing]$$

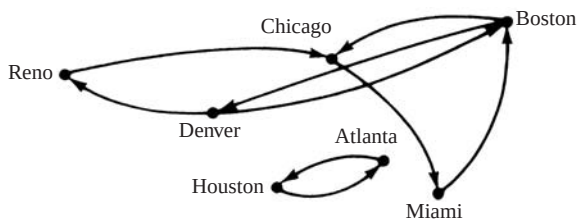
c) Utilice la lista de sucesores obtenida en el inciso *b*) y los pesos de las aristas en el archivo de aristas en la figura 9-25*a*) para trazar el grafo en la figura 9-25*b*).

9.12 Suponga que una aerolínea tiene nueve vuelos diarios como sigue:

103	Atlanta a Houston	203	Boston a Denver	305	Chicago a Miami
106	Houston a Atlanta	204	Denver a Boston	308	Miami a Boston
201	Boston a Chicago	301	Denver a Reno	401	Reno a Chicago

Describa los datos por medio de un grafo dirigido etiquetado *G*.

Los datos se describen mediante el grafo en la figura 9-26*a*) (donde los números de vuelo se han omitido por conveniencia en la notación).



a)

Archivo vértice

	1	2	3	4	5	6	7	8
CITY	*A*	*B*	*C*	*D*	*H*	*M*	*R*	
PTR	1	3	7	5	2	8	9	

Archivo arista

	1	2	3	4	5	6	7	8	9	10
NUMBER	103	106	201	203	204	301	305	308	402	
ORIG	1	5	2	2	4	4	3	6	7	
DEST	5	1	3	4	2	7	6	2	3	
NEXT-E	0	0	4	0	6	0	0	0	0	

b)

Figura 9-26

9.13 Describa cómo el grafo en el problema 9.12 puede aparecer en la memoria mediante una representación ligada donde las ciudades y los vuelos aparezcan en arreglos lineales ordenados.

Vea la figura 9-26*b*) (donde *A*, *B*, . . . , denotan, respectivamente, Atlanta, Boston, . . .). No hay necesidad de una variable START, puesto que las ciudades constituyen un arreglo, no una lista ligada. También se usa ORIG (origen) y DEST (destino) en lugar de BEG-V y END-V.

9.14 Resulta evidente que los datos del problema 9.12 pueden almacenarse de manera eficiente en un archivo en el que cada registro contiene sólo tres campos:

Número de vuelo, Ciudad de origen, Ciudad de destino

Sin embargo, cuando hay demasiados vuelos, esta representación no contesta fácilmente las siguientes preguntas naturales:

i) ¿Hay un vuelo directo de la ciudad *X* a la ciudad *Y*?
ii) ¿Es posible volar de la ciudad *X* a la ciudad *Y*?
iii) ¿Cuál es el camino más directo (número mínimo de escalas) de la ciudad *X* a la ciudad *Y*?

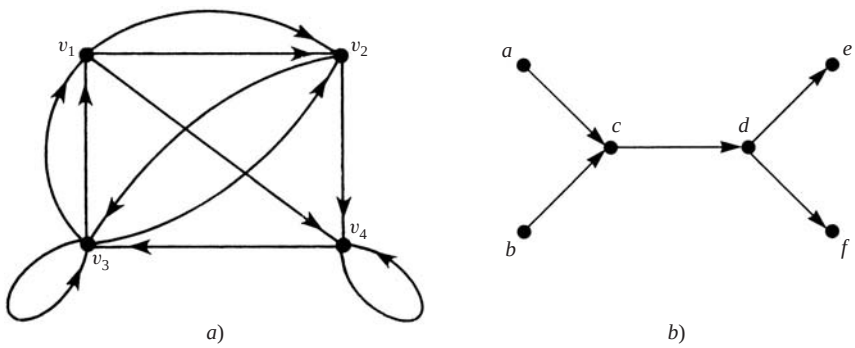
Muestre cómo la respuesta, por ejemplo en el inciso *ii*), puede obtenerse más fácilmente si los datos se almacenan en la memoria con la representación ligada en el grafo de la figura 9-26*b*).

Una forma de contestar al inciso *ii*) es usar un algoritmo de búsqueda en anchura o en profundidad para decidir si la ciudad *Y* es alcanzable desde la ciudad *X*. Estos algoritmos requieren las listas de adyacencia, que pueden obtenerse fácilmente a partir de la representación ligada de un grafo, pero no a partir de la representación anterior, que sólo usa tres campos.

PROBLEMAS DIVERSOS

9.15 Sea $A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ la matriz de adyacencia de un multigrafo *G*. Dibuje una representación de *G*.

Puesto que *A* es una matriz de 4×4, *G* tiene cuatro vértices v_1, v_2, v_3, v_4. Para cada entrada a_{ij} en *A*, se trazan a_{ij} arcos (aristas dirigidas) del vértice v_i al vértice v_j para obtener el grafo de la figura 9-27*a*).



a) *b*)

Figura 9-27

9.16 Sea *S* el grafo libre de ciclos en la figura 9-27*b*). Encuentre todos los ordenamientos topológicos posibles de *S*.

Hay cuatro ordenamientos topológicos posibles de *S*: cada ordenamiento *T* debe empezar con *a* o con *b*, debe terminar con *e* o con *f* y *c* y *d* deben ser los elementos tercero y cuarto, respectivamente. Los cuatro ordenamientos son los siguientes:

$$T_1 = [a, b, c, d, e, f], \qquad T_2 = [b, a, c, d, e, f]$$
$$T_3 = [a, b, c, d, f, e], \qquad T_4 = [b, a, c, d, f, e]$$

9.17 Demuestre la proposición 9.4: sea *A* la matriz de adyacencia de un grafo *G*. Entonces $a_K[i, j]$, la *ij*-ésima entrada en la matriz A^K, proporciona el número de caminos de longitud *K* de v_i a v_j.

La demostración es por inducción sobre *K*. Un camino de longitud 1 de v_i a v_j es precisamente una arista (v_i, v_j). Por definición de la matriz de adyacencia *A*, $a_1[i, j] = a_{ij}$ proporciona el número de aristas de v_i a v_j. Así, la proposición es verdadera para $K = 1$.

Se supone $K > 1$. (Es decir, que *G* tiene *m* nodos). Puesto que $A^K = A^{K-1}A$,

$$a_K[i, j] = \sum_{s=1}^{m} a_{K-1}[i, s]\, a_1[s, j]$$

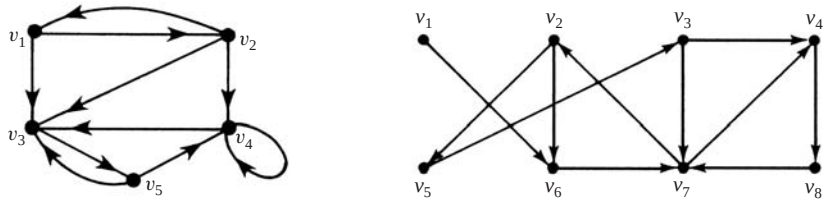
Por inducción, $a_{K-1}[i, s]$ proporciona el número de caminos de longitud $K - 1$ de v_i a v_s y $a_1[s, j]$ proporciona el número de caminos de longitud 1 de v_s a v_j. Por tanto, $a_{K-1}[i, s]a_1[s, j]$ proporciona el número de caminos de longitud *K* de v_i a v_j donde v_s es el penúltimo vértice. Por lo que, todos los caminos de longitud *K* de v_i a v_j pueden obtenerse al sumar el producto $a_{K-1}[i, s]a_1[s, j]$ para toda *s*. En consecuencia, $a_K[i, j]$ es el número de caminos de longitud *K* de v_i a v_j. Así, se ha demostrado la proposición.

PROBLEMAS SUPLEMENTARIOS

TERMINOLOGÍA DE GRAFOS

9.18 Considere el grafo G en la figura 9-28*a*).

a) Encuentre el grado de entrada y el grado de salida de cada vértice.
b) ¿Hay alguna fuente o algún sumidero?
c) Encuentre todos los caminos simples de v_1 a v_4.
d) Encuentre todos los ciclos en G.
e) Encuentre todos los caminos de longitud 3 o menores de v_1 a v_3.
f) ¿G es unilateral o fuertemente conexo?



a) *b*)

Figura 9-28

9.19 Considere el grafo G en la figura 9-28*b*).

a) ¿Hay alguna fuente o algún sumidero?
b) Encuentre todas los caminos simples de v_1 a v_4.
c) Encuentre un camino no simple de v_1 a v_4.
d) Encuentre todos los ciclos en G que incluyen a v_4.

9.20 Considere el grafo G en la figura 9-28*b*).

a) Encuentre: suc(v_1), suc(v_3), suc(v_5), suc(v_7).
b) Encuentre el subgrafo H de G generado por *i*) $\{v_1, v_3, v_5, v_6\}$; *ii*) $\{v_2, v_3, v_6, v_7\}$.

9.21 Sea G el grafo con conjunto de vértices $V(G) = \{A, B, C, D, E\}$ y conjunto de aristas

$$E(G) = \{(A, D), \quad (B, C), \quad (C, E), \quad (D, B), \quad (D, D), \quad (D, E), \quad (E, A)\}$$

a) Exprese G mediante su tabla de adyacencia.
b) ¿G tiene lazos o aristas paralelas?
c) Encuentre todos los caminos simples de D a E.
d) Encuentre todos los ciclos en G.
e) ¿G es unilateral o fuertemente conexo?
f) Encuentre el número de subgrafos de G con vértices C, D, E.
g) Encuentre el subgrafo H de G generado por C, D, E.

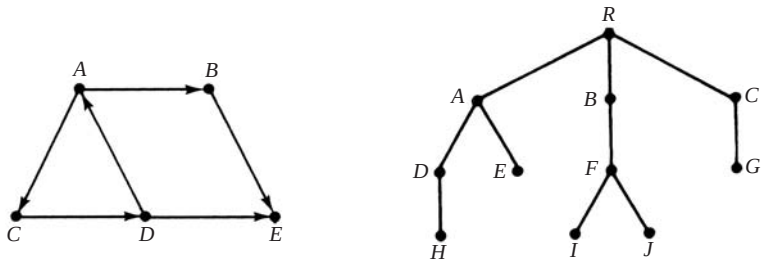
9.22 Sea G el grafo con conjunto de vértices $V(G) = \{a, b, c, d, e\}$ y las siguientes listas de sucesores:

$$\text{suc}(a) = [b, c] \quad \text{suc}(b) = \varnothing \quad \text{suc}(c) = [d, e] \quad \text{suc}(d) = [a, b, e] \quad \text{suc}(e) = \varnothing$$

a) Enumere las aristas de G. *b*) ¿G es débil, unilateral o fuertemente conexo?

9.23 Sea G el grafo en la figura 9-29*a*).

a) Exprese G mediante su tabla de adyacencia.
b) ¿G tiene fuentes o sumideros?
c) Encuentre todos los caminos simples de A a E.
d) Encuentre todos los ciclos en G.
e) Encuentre un camino de expansión en G.
f) ¿G es fuertemente conexo?



a) *b*)

Figura 9-29

ÁRBOLES CON RAÍZ, ÁRBOLES CON RAÍZ ORDENADOS

9.24 Sea T el árbol con raíz en la figura 9-29*b*).

a) Identifique el camino α de la raíz R a cada uno de los siguientes vértices, y encuentre el número de nivel del vértice: *i*) D; *ii*) J; *iii*) G.

b) Encuentre las hojas de T.

c) Suponga que T es un árbol con raíz ordenado y encuentre la dirección universal de cada hoja de T.

9.25 Las siguientes direcciones están en orden aleatorio:

2.1.1, 3.1, 2.1. 1, 2.2.1.2, 0, 3.2, 2.2, 1.1, 2, 3.1.1, 2.2.1, 3, 2.2.1.1

a) Escriba las direcciones en orden lexicográfico.

b) Dibuje el árbol con raíz correspondiente.

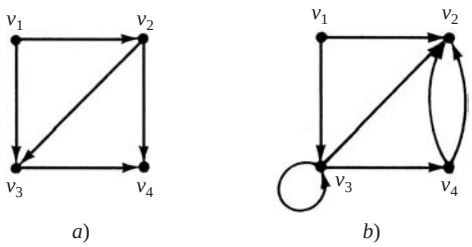
REPRESENTACIÓN SECUENCIAL DE GRAFOS

9.26 Sea G el grafo en la figura 9-30*a*).

a) Encuentre la matriz de adyacencia A y la matriz de caminos P para G.

b) Para toda $k > 0$, encuentre n_k, donde n_k denota el número de caminos de longitud k de v_1 a v_4.

c) ¿G es débil, unilateral o fuertemente conexo?



a) *b*)

Figura 9-30

9.27 Repita el problema 9.26 para el grafo G en la figura 9-30*b*).

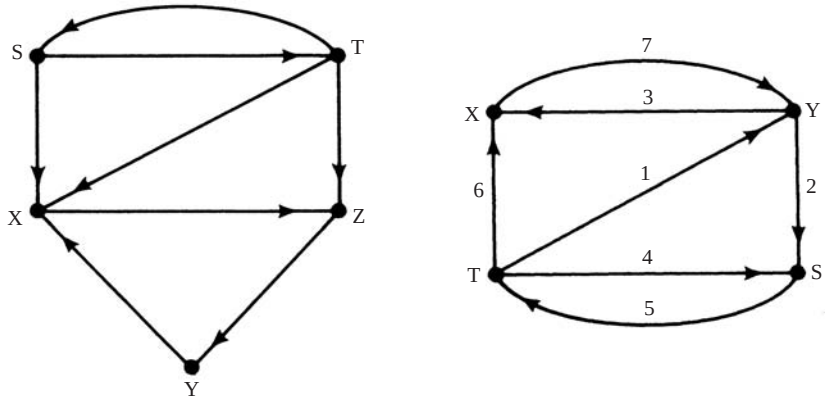
9.28 Sea P la matriz de caminos de un grafo G. Describa P cuando G es: *a*) fuertemente conexo; *b*) unilateralmente conexo.

9.29 Sea G el grafo en la figura 9-31*a*), donde los vértices se mantienen en la memoria mediante el arreglo DATA: X, Y, Z, S, T. *a*) Encuentre la matriz de adyacencia A y la matriz de caminos P de G. *b*) Encuentre todos los ciclos en G. *c*) ¿G es unilateralmente conexo? ¿Fuertemente conexo?

9.30 Sea G el grafo ponderado en la figura 9-31*b*), donde los vértices se mantienen en la memoria mediante el arreglo DATA: X, Y, S, T.

a) Encuentre la matriz ponderada W de G.

b) Use el algoritmo de Warshall para encontrar la matriz Q de los caminos más cortos.



a) *b*)

Figura 9-31

REPRESENTACIÓN LIGADA DE GRAFOS

9.31 El grafo ponderado G con seis vértices $A, B, \ldots, F$ se almacena en la memoria mediante una representación ligada con un archivo de vértices y un archivo de aristas como en la figura 9-32.

a) Enumere los vértices en el orden en que aparecen en la memoria.

b) Encuentre la lista de sucesores suc(v) de cada vértice v en G.

c) Dibuje una representación de G.

Archivo vértice

START 7

	1	2	3	4	5	6	7	8
VERTEX	*D*		*B*	*F*	*A*		*C*	*E*
NEXT-V	3		8	1	0		4	5
PTR	7		5	9	2		3	0

Archivo arista

	1	2	3	4	5	6	7	8	9	10	11	12
BEG-V	5	5	7		3	7	1		4	1	4	7
END-V	8	7	5		1	1	5		8	4	3	8
NEXT-E	0	1	12		0	0	10		11	0	0	6
WEIGHT	5	2	1		3	2	4		1	3	4	1

Figura 9-32

9.32 Sea G el grafo presentado por la tabla: $G = [A: B, C;\quad B: C, D;\quad C: C;\quad D: B;\quad E: \varnothing]$.

a) Encuentre el número de vértices y aristas en G.

b) Dibuje una representación de G.

c) ¿Hay alguna fuente o algún sumidero?

d) ¿G es débil, unilateral o fuertemente conexo?

9.33 Repita el problema 9.32 para la tabla: $G = [A: D;\quad B: C;\quad C: E;\quad D: B, D, E;\quad E: A]$.

9.34 Repita el problema 9.32 para la tabla: $G = [A: B, C, D, K;\quad B: J;\quad C: \varnothing;\quad D: \varnothing;\quad J: B, D, L;\quad K: D, L;\quad L: D]$.

9.35 Suponga que una aerolínea tiene ocho vuelos diarios que sirven a las ciudades Atlanta, Boston, Chicago, Denver, Houston, Filadelfia y Washington. Suponga que los datos sobre los vuelos se almacenan en la memoria como en la figura 9-33; es decir, que se usa una representación ligada donde las ciudades y los vuelos aparecen en arreglos ordenados linealmente. Dibuje un grafo dirigido etiquetado G que describa los datos.

Archivo vértice

	1	2	3	4	5	6	7	8
CITY	*A*	*B*	*C*	*D*	*H*	*P*	*W*	
PTR	1	2	3	8	9	5	7	

Archivo arista

	1	2	3	4	5	6	7	8	9	10
NUMBER	101	102	201	202	203	301	302	401	402	
ORIG	1	2	3	1	6	6	7	4	5	
DEST	2	3	6	7	3	1	6	5	4	
NEXT-E	4	0	0	0	6	0	0	0	0	

Figura 9-33

9.36 Use los datos en la figura 9-33 para escribir un procedimiento con entrada CITY *X* y CITY *Y* que encuentre el número de un vuelo directo de la ciudad *X* a la ciudad *Y*, en caso de existir. Use lo siguiente para probar el procedimiento:

a) $X =$ Atlanta, $Y =$ Filadelfia; *c*) $X =$ Houston, $Y =$ Chicago;
b) $X =$ Filadelfia, $Y =$ Atlanta; *d*) $X =$ Washington, $Y =$ Chicago.

9.37 Use los datos en la figura 9-33 para escribir un procedimiento con entrada CITY *X* y CITY *Y* que encuentre el camino más directo (número mínimo de escalas) de la ciudad *X* a la ciudad *Y*, en caso de existir. Pruebe el procedimiento con los datos de entrada del problema 9.36.

PROBLEMAS DIVERSOS

9.38 Use el algoritmo de poda para encontrar el camino más corto de *s* a *t* en la figura 9-34.

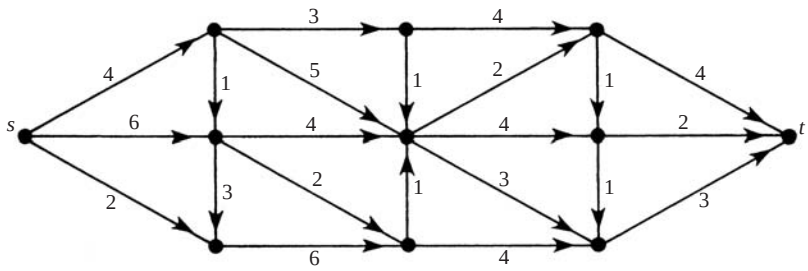


Figura 9-34

9.39 Encuentre un ordenamiento topológico *T* de cada uno de los siguientes grafos:

a) $G = [A:Z;\ B:T;\ C:B;\ D:\varnothing;\ X:D;\ Y:X;\ Z:B, X;\ S:C, Z;\ T:\varnothing]$
b) $G = [A:X, Z;\ B:A;\ C:S, T;\ D:Y;\ X:S, T;\ Y:B;\ Z:\varnothing;\ S:Y;\ T:\varnothing]$
c) $G = [A:C, S;\ B:T, Z;\ C:\varnothing;\ D:Z;\ X:A;\ Y:A;\ Z:X, Y;\ S:\varnothing;\ T:Y]$

9.40 Dibuje un grafo etiquetado *G* que represente la siguiente situación. Tres hermanas, Bárbara, Rosa y Susana, llaman por teléfono, cada una, en forma regular a su madre, Gertrudis, aunque Gertrudis sólo llama a Rosa. Susana no llama a Rosa, aunque Rosa continúa llamando a Susana. Bárbara y Susana se llaman mutuamente, y Bárbara y Rosa se llaman entre sí.

9.41 Sea *R* la relación (grafo dirigido) sobre $V = \{2, 3, 4, 9, 15\}$ definido por "*x* es menor que y primo relativo de *y*". *a*) Dibuje el diagrama del grafo *R*. *b*) ¿*R* es débilmente conexo? ¿Unilateralmente conexo? ¿Fuertemente conexo?

9.42 Un grafo dirigido *G* es *completo* si, para cada par de vértices distintos *u* y *v*, se cumple que (u, v) es un arco o que (v, u) es un arco. Demuestre que un grafo dirigido completo finito *G* tiene un camino que incluye todos los vértices. (Resulta evidente que esto se cumple para grafos completos no dirigidos.) Por tanto, *G* es unilateralmente conexo.

9.43 Suponga que un grafo G se introduce por medio de un entero M, que representa los vértices 1, 2,..., M y una lista de N pares ordenados de enteros que representan las aristas de G. Escriba un procedimiento que efectúe lo siguiente:

a) Encuentre la matriz de adyacencia A $M \times M$ del grafo G.

b) Utilice A y el algoritmo de Warshall para encontrar la matriz de caminos P de G.

Use los datos siguientes para probar el procedimiento:

i) $M = 5$; $N = 8$; (3, 4), (5, 3), (2, 4), (1, 5), (3, 2), (4, 2), (3, 1), (5, 1)

ii) $M = 6$; $N = 10$; (1, 6), (2, 1), (2, 3), (3, 5), (4, 5), (4, 2), (2, 6), (5, 3), (4, 3), (6, 4)

9.44 Suponga que un grafo G se introduce por medio de un entero M, que representa los vértices 1, 2,..., M y una lista de N tripletas ordenadas (a_i, b_i, w_i) de enteros tales que (a_i, b_i) es una arista de G y w_i es su peso. Escriba un procedimiento que efectúe lo siguiente:

a) Encuentre la matriz de pesos W de $M \times M$ del grafo G.

b) Utilice W y el algoritmo de Warshall para encontrar la matriz Q de caminos más cortos entre los vértices de G.

Use los datos siguientes para probar el procedimiento:

i) $M = 4$; $N = 7$; (1, 2, 5), (2, 4, 2), (3, 2, 3), (1, 1, 7), (4, 1, 4), (4, 3, 1)

ii) $M = 5$; $N = 8$; (3, 5, 3), (4, 1, 2), (5, 2, 2), (1, 5, 5), (1, 3, 1), (2, 4, 1), (3, 4, 4), (5, 4, 4)

9.45 Considere el grafo G en la figura 9-11. Muestre la secuencia de listas de espera en STACK y la secuencia de vértices procesados mientras se lleva a cabo una búsqueda en profundidad (DFS) de G que empiece en el vértice: *a*) B; *b*) E; *c*) K.

9.46 Considere el grafo G en la figura 9-11. Como se hizo en el ejemplo 9.11, use una búsqueda en anchura de G para encontrar el camino más corto de K a F. En particular, muestre la secuencia de listas de espera en QUEUE durante la búsqueda.

Respuestas a los problemas suplementarios

Notación: $M = [R_1; R_2; \ldots; R_n]$ denota una matriz con renglones $R_1, R_2, \ldots, R_n$.

9.18 *a*) Grados de entrada: 1, 1, 4, 3, 1; grados de salida: 2, 3, 1, 2, 2.
b) Ninguno.
c) (v_1, v_2, v_4), (v_1, v_3, v_5, v_4), $(v_1, v_2, v_3, v_5, v_4)$
d) (v_3, v_5, v_4, v_3)
e) (v_1, v_3), (v_1, v_2, v_3), (v_1, v_2, v_4, v_3), (v_1, v_2, v_1, v_3), (v_1, v_3, v_5, v_7)
f) unilateralmente conexo, pero no fuertemente conexo.

9.19 *a*) Fuentes: v_1
b) (v_1, v_6, v_7, v_4), $(v_1, v_6, v_7, v_2, v_5, v_3, v_4)$
c) $(v_1, v_6, v_7, v_2, v_6, v_7, v_4)$
d) (v_4, v_8, v_7, v_4), $(v_4, v_8, v_7, v_2, v_5, v_3, v_4)$

9.20 *a*) (suc1) = [6], (suc3) = [4, 7], (suc5) = [3], (suc7) = [2, 4].
b) *i*) (1, 6), (5, 3); *ii*) (2, 6), (6, 7), (7, 2), (3, 7).

9.21 *a*) G = [$A : D$; $B : C$; $C : E$; $D : B, D, E$; $E : A$]
b) Lazo: D, D)
c) (D, E), (D, B, C, E)
d) (A, D, E, A), (A, D, B, C, E, A)
e) Unilateral y fuertemente conexo.
f) y *g*) H tiene tres aristas: (C, E), (D, E), (D, D). Hay $8 = 2^3$ formas de escoger alguno de las tres aristas; y con cada elección se obtiene un subgrafo.

9.22 *a*) (a, b), (a, c), (c, d), (c, e), (d, a), (d, b), (d, e)
b) Puesto que b y e son sumideros, de b a e o de e a b no hay ningún camino, de modo que G no es unilateral ni fuertemente conexo. G es débilmente conexo, ya que cc, a, b, d, e es un semicamino de expansión.

9.23 *a*) $G = [A : B, C : B : E; C : D; E : \varnothing]$; *b*) Sumidero: E; *c*) (A, B, E), (A, C, D, E); *d*) (A, C, D, A); *e*) (C, D, A, B, E); *f*) No.

9.24 *a*) *i*) (R, A, D), 2; *ii*) (R, B, F, J), 3; *iii*) $R, C, G)$, 2.
b) H, E, I, J, G
c) H : 1.1.1, E : 1.2, I : 2.1.1, J : 2.1.2, G : 3.1

9.25 *a*) 0, 1, 1.1, 2, 2.1, 2.1.1, 2.2, 2.2.1, 2.2.1.1, 2.2.1.2, 3, 3.1, 3.1.1, 3.2. *b*) Fig. 9-35*a*).

9.26 *a*) $A = [0, 1, 1, 0; 0, 0, 1, 1; 0, 0, 0, 1; 0, 0, 0, 0]$;
$P = [0, 1, 1, 1; 0, 0, 1, 1; 0, 0, 0, 1; 0, 0, 0, 0]$;
b) 0, 2, 1, 0, 0,...; c) Débil y unilateralmente conexo.

9.27 *a*) $A = [0, 1, 1, 0; 0, 0, 0, 0; 0, 1, 1, 1; 0, 2, 0, 0]$;
$P = [0, 1, 1, 1; 0, 0, 0, 0; 0, 1, 1, 1; 0, 1, 0, 0]$;
b) 0, 1, 1, 1,...; c) Débil y unilateralmente conexo.

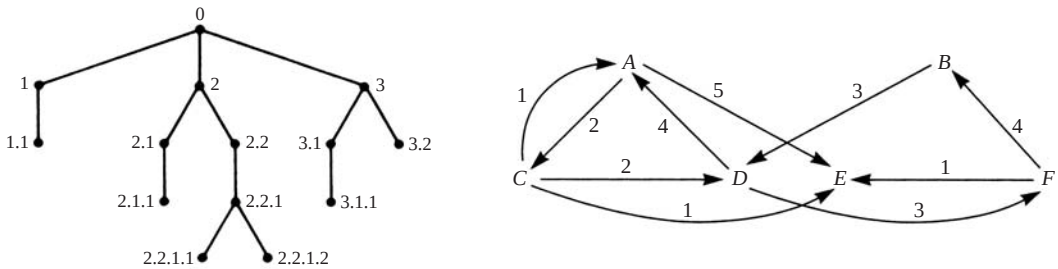
9.28 Sea $P = [p_{ij}]$. Para $i \neq j$: *a*) $p_{ij} \neq 0$; *b*) cualquiera $p_{ij} \neq 0$ o $p_{ji} \neq 0$.

9.29 *a*) $A = [0, 0, 1, 0, 0; 1, 0, 0, 0, 0; 0, 1, 0, 0, 0; 1, 0, 0, 0, 1; 1, 0, 1, 1, 0]$;
$P = [1, 1, 1, 0, 0; 1, 1, 1, 0, 0; 1, 1, 1, 0, 0; 1, 1, 1, 1, 1; 1, 1, 1, 1, 1; 1, 1, 1, 1, 1]$
b) (X, Z, Y, X); (S, T, S) *c*) Unilateralmente.

9.30 *a*) $A = [0, 7, 0, 0; 3, 0, 2, 0; 0, 0, 0, 5; 6, 1, 4, 0]$
b) $Q = [XYX, XY, XYS, XYST; YX, YSTY, YS, YST; STYX, STY, STYS, ST; TX, TY, TYS, TYST]$

9.31 *a*) C, F, D, B, E, A; *b*) $[A : C, E; B : D; C : D, E, A; D : A, F; E : \varnothing; F : B, E]$; *c*) Vea la figura 9-35*b*).

9.32 *a*) 5, 6; *b*) fuente: A; *c*) Vea la figura 9-36*a*); ninguno.

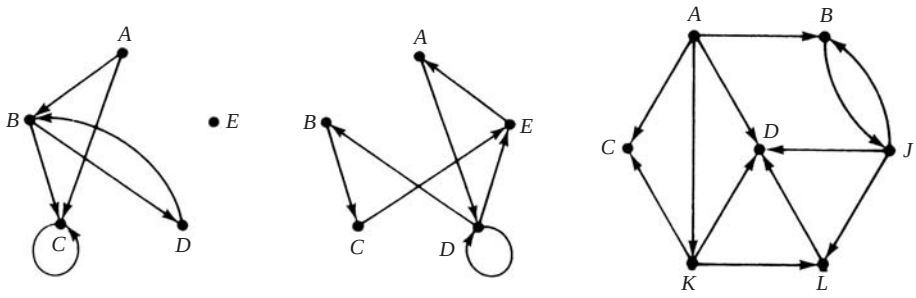


a) *b*)

Figura 9-35

9.33 *a*) 5, 1; *b*) ninguno: *A*; *c*) Vea la figura 9-36*b*); *d*) los tres.

9.34 *a*) 7, 11; *b*) fuente: *A*; sumideros: *C*, *D*; *c*) Vea la figura 9-36*c*); *d*) sólo débilmente.



a) *b*) *c*)

Figura 9-36

9.35 Vea la figura 9-37.

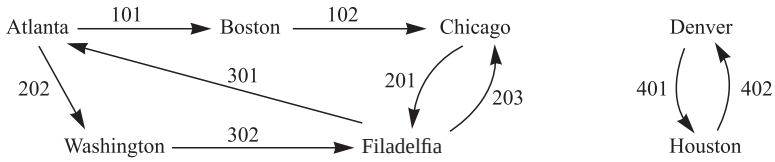
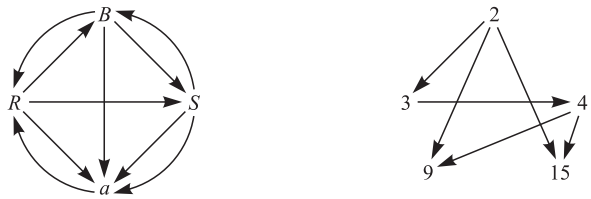


Figura 9-37

9.36 *a*) No; *b*) sí; *c*) no; *d*) no.
9.37 *a*) *AWP*; *b*) *PA*; *c*) ninguno; *d*) *WPC*.
9.38 (*s*, 4, 1, 2, 1, 2, 1, 2, *t*)
9.39 ***Sugerencia*:** Primero trace el grafo. *a*) *ASYCZBXTD*; *b*) ninguno, el grafo no es libre de ciclos; por ejemplo, *YBAXSY* es un ciclo; *c*) *BTYXACSDZ*.
9.40 Vea la figura 9-38*a*).
9.41 *a*) Vea la figura 9-38*b*). *b*) Sólo débilmente conexo.

9.42 ***Sugerencia*:** Suponga que $(\alpha = v_1, \ldots, v_m)$ es un camino más largo en G y que no incluye al vértice u. Si (u_1, v_1) es un arco, entonces $\beta = (u, \alpha)$ extiende a α. Por tanto, (v_1, u) es un arco. Si (u, v_2) también es un arco, entonces $\beta = (v_1, u, v_2, \ldots, v_m)$ extiende a α; por tanto, (v_2, u) es un arco. En forma semejante, $(v_3, u), \ldots, (v_m, u)$ son arcos. Por tanto, $\beta = (\alpha, u)$ extiende a α. Esto contradice la maximalidad de α.



a) *b*)

Figura 9-38

9.43 *i*) $A = [0, 0, 0, 0, 0; 0, 0, 0, 1, 0; 1, 1, 0, 1, 0; 0, 1, 0, 0, 0; 1, 0, 1, 0, 0]$
$P = [1, 1, 1, 1, 1; 0, 1, 0, 1, 0; 1, 1, 1, 1, 1; 0, 1, 0, 1, 0; 1, 1, 1, 1, 1]$
ii) $A = [0, 0, 0, 0, 0, 1; 1, 0, 1, 0, 0, 1; 0, 0, 0, 0, 1, 0; 0, 1, 1, 0, 1, 0; 0, 0, 1, 0, 0, 0; 0, 0, 0, 1, 0, 0]$
$P = [1, 1, 1, 1, 1, 1; 1, 1, 1, 1, 1, 1; 0, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1, 1; 0, 0, 1, 0, 1, 0; 1, 1, 1, 1, 1, 1]$

9.44 *i*) $W = [7, 5, 0, 0; 0, 0, 0, 2; 0, 3, 0, 0; 4, 0, 1, 0]$;
$Q = [AA, AB, ABCD, ABD; BDA, BDCB, BDC, BD; CBDA, CB, CBDC, CBD; DA, DCB, DC, DCBD]$, donde A, B, C, D son los vértices.
ii) $W = [0, 0, 1, 0, 5; 0, 0, 0, 1, 0; 0, 0, 0, 4, 3; 2, 0, 0, 0, 0; 0, 2, 0, 4, 0]$;
$Q = [ACDA, ACEB, AC, ACD, ACE; BDA, BDACEB, BDAC, BD, BDACE; CDA, CEB, CDAC, CD, CE; DA, DACEB, DAC, DACD, DACEB; EDA, EB, EDAC, ED, EDACE]$ donde A, B, C, D, E son los vértices.

9.45 *a*) STACK: $B, L_B\, E_B, E_L\, C_L\, E_B, F_E\, C_L, D_F\, C_L, C_L, J_C, K_J, \varnothing$; Vértice: $B, L_B, E_L, F_E, D_F, C_L, J_C, K_J$
b) STACK: $E, F_E, D_F, \varnothing$; Vértice: E, F_E, D_F
c) STACK: $K, L_K C_K, E_L C_L, C_K, C_L, D_F C_L, C_L J_C, \varnothing$; Vértice: $K, L_K, E_L, F_E, D_F, C_L, J_C$

9.46 QUEUE: $K, L_K C_K, J_C E_C D_C L_K, J_C E_C D_C, J_C E_C, F_E$; Vértice: $K, C_K, L_K, D_C, E_C, J_C, F_E$; Camino mínimo: $F_E \leftarrow E_C \leftarrow C_K \leftarrow$ o $K \rightarrow C_K \rightarrow E_C \rightarrow F_E$.

10 Árboles binarios

CAPÍTULO

10.1 INTRODUCCIÓN

El árbol binario es una estructura fundamental en matemáticas y computación y también se le aplican algunos de los términos de los árboles con raíz como arista, camino, rama, hoja, profundidad y número de nivel. No obstante, en los árboles binarios se usará el término nodo, en lugar de vértice. Debe tener en cuenta que un árbol binario no es un caso especial de un árbol con raíz; son entes matemáticos diferentes.

10.2 ÁRBOLES BINARIOS

Un *árbol binario T* es un conjunto finito de elementos que se denominan *nodos*, tales que:

1) *T* es vacío (*árbol nulo* o *árbol vacío*), o
2) *T* contiene un nodo distintivo *R*, denominado *raíz de T*, y los nodos restantes de *T* forman un par ordenado de árboles binarios ajenos T_1 y T_2.

Si *T* contiene una raíz *R*, entonces los árboles T_1 y T_2 se denominan, respectivamente, subárbol izquierdo y subárbol derecho de *R*. Si T_1 no es vacío, entonces su raíz se denomina *sucesor izquierdo* de *R*; en forma semejante, si T_2 no es vacío, entonces su raíz se denomina *sucesor derecho* de *R*.

La definición anterior de un árbol binario *T* es recursiva, ya que *T* se define en términos de los subárboles binarios T_1 y T_2. Esto significa, en particular, que cualquier nodo *N* de *T* contiene un subárbol izquierdo y un subárbol derecho, y que cada subárbol o ambos pueden ser vacíos. Así, cualquier nodo *N* en *T* tiene 0, 1 o 2 sucesores. Un nodo sin sucesores se denomina nodo *terminal*. Por tanto, los dos subárboles de un nodo terminal son vacíos.

Representación de un árbol binario

Un árbol binario *T* suele presentarse por medio de un diagrama en el plano, denominado *ilustración* de *T*. En específico, el diagrama de la figura 10-1*a*) representa un árbol binario ya que:

i) *T* consta de 11 nodos, que se representan con las letras *A* a *L*, excepto la *I*.
ii) La raíz de *T* es el nodo *A* en la parte superior del diagrama.
iii) Una línea inclinada hacia la izquierda en un nodo *T* indica un sucesor izquierdo de *N*; y una línea inclinada hacia la derecha en *T* indica un sucesor derecho de *N*.

Por consiguiente, en la figura 10-1*a*):

a) *B* es un sucesor izquierdo y *C* es un sucesor derecho de la raíz *A*.

b) El subárbol izquierdo de la raíz *A* consta de los nodos *B*, *D*, *E* y *F*, y el subárbol derecho consta de los nodos *C*, *G*, *H*, *J*, *K* y *L*.

c) Los nodos *A*, *B*, *C* y *H* tienen dos sucesores; los nodos *E* y *J* tienen sólo un sucesor, y los nodos *D*, *F*, *G*, *L* y *K* no tienen sucesores; es decir, son nodos terminales.

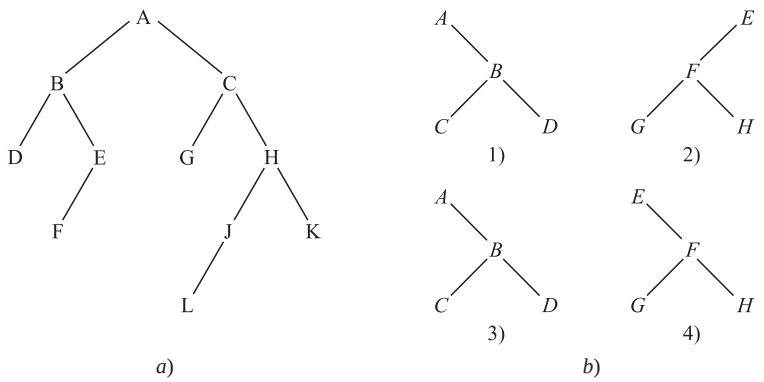


Figura 10-1

Árboles binarios semejantes

Se dice que los árboles binarios T y T' son *semejantes* si tienen la misma estructura o, en otras palabras, si tienen la misma forma. Se dice que son *copias* si son semejantes y si tienen el mismo contenido en nodos correspondientes.

EJEMPLO 10.1 Considere los cuatro árboles binarios en la figura 10-1*b*). Los tres árboles 1), 3) y 4) son semejantes. En particular, los árboles 1) y 3) son copias, puesto que también tienen los mismos datos en los nodos correspondientes. El árbol 2) no es semejante ni copia del árbol 4) porque, en un árbol binario, se distingue entre un sucesor izquierdo y un sucesor derecho incluso cuando sólo hay un sucesor.

Terminología

Para describir relaciones entre los nodos de un árbol T a menudo se usa la terminología que describe relaciones familiares: suponga que N es un nodo en T con sucesor izquierdo S_1 y sucesor derecho S_2. Entonces N se denomina *padre* (o *progenitor*) de S_1 y S_2. En forma semejante, S_1 se denomina *hijo izquierdo* (o *descendiente izquierdo*) de N, y S_2 se denomina *hijo derecho* (o *descendiente derecho*) de N. Además, se dice que S_1 y S_2 son *hermanos* (o *consanguíneos*). Todo nodo N en un árbol binario T, excepto la raíz, tiene un padre único, denominado *predecesor* de N.

Los términos descendiente y ancestro tienen su significado de costumbre. Es decir, un nodo L se denomina *descendiente* de un nodo N (y N se denomina *ancestro* de L) si existe una sucesión de hijos de N a L; y se especifica si L es *descendiente izquierdo* o *derecho* de N según si L pertenece al subárbol izquierdo o derecho de N.

La terminología de la teoría de grafos y de la horticultura también se usa con un árbol binario T. Para mayor claridad, la línea que se traza desde un nodo N de T hasta un sucesor se denomina *arista*, y una secuencia de aristas consecutivas se denomina *camino*. Un nodo terminal se denomina *hoja*, y un camino que termina en una hoja se denomina *rama*.

A cada nodo en un árbol binario T se le asigna un *número de nivel* en el orden siguiente: a la raíz R del árbol T se le asigna el número de nivel 0, y a los demás nodos se les asigna un número de nivel que es 1 más que el número de nivel de su padre. Además, se dice que los nodos con el mismo número de nivel pertenecen a la misma *generación*.

La *profundidad* (o *altura*) de un árbol T es el número máximo de nodos en una rama de T. Resulta que ésta es una unidad mayor que el número de nivel de T. El árbol T en la figura 10-1*a*) tiene profundidad 5.

10.3 ÁRBOLES BINARIOS COMPLETOS Y EXTENDIDOS

En esta sección se consideran dos tipos especiales de árboles binarios.

Árboles binarios completos

Considere cualquier árbol binario T. Cada nodo de T puede tener cuando mucho dos hijos. En consecuencia, es posible demostrar que el nivel r de T puede tener cuando mucho 2^r nodos. Se dice que el árbol T es *completo* si todos sus niveles, excepto posiblemente el último, tienen el número máximo de nodos posibles, y si todos los nodos en el último nivel se encuentran lo más a la izquierda posible. Por tanto, hay un único árbol completo T_n con exactamente n nodos (donde se ignora el contenido de los nodos). El árbol completo T_{26} con 26 nodos se muestra en la figura 10-2.

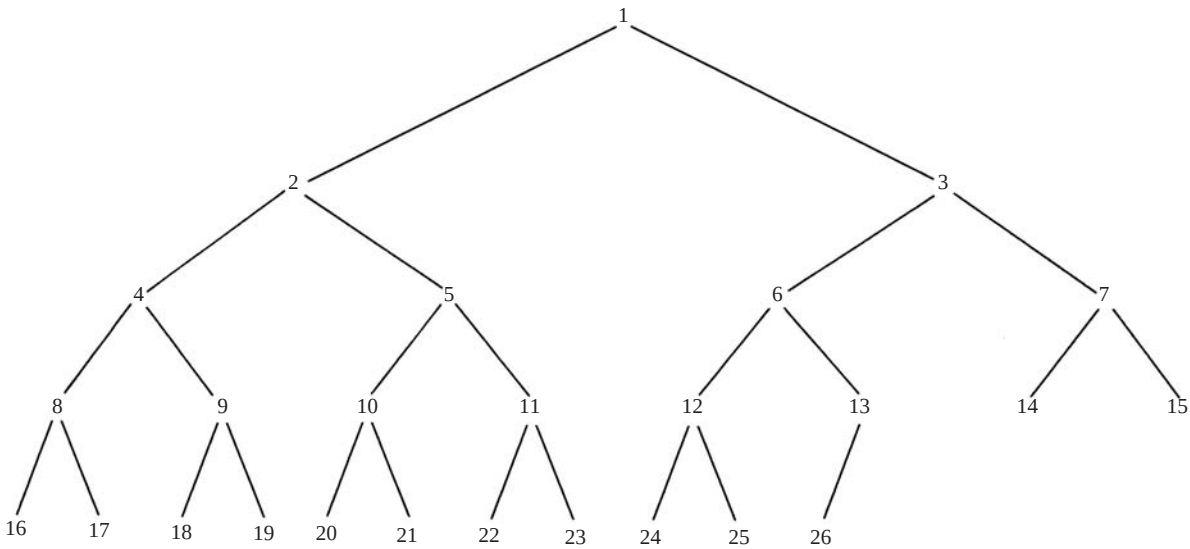


Figura 10-2 Árbol completo T_{26}

Los nodos del árbol binario completo T_{26} en la figura 10-2 se han etiquetado a propósito con los enteros 1, 2,…, 26, de izquierda a derecha, generación por generación. Dicho etiquetado facilita determinar los hijos y los padres de cualquier nodo K en cualquier árbol completo T_n. De modo que los hijos izquierdo y derecho del nodo K son $2^* K$ y $2^* K + 1$, y el padre de K es el nodo $[K/2]$. Por ejemplo, los hijos del nodo 9 son los nodos 18 y 19, y su padre es el nodo $[9/2] = 4$. La profundidad d_n del árbol completo T_n con n nodos está dada por

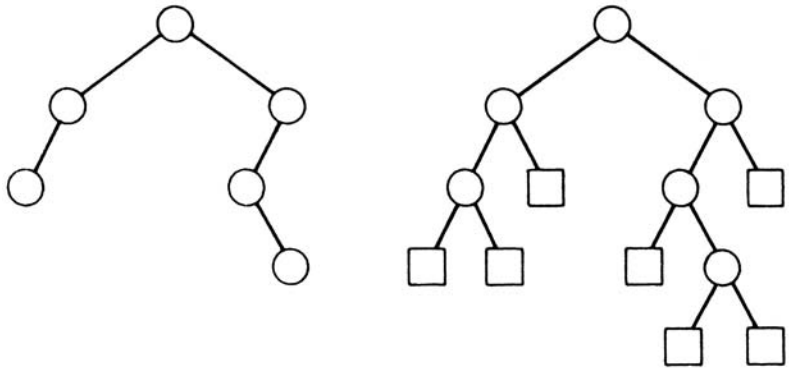
$$d_n = \lfloor \log_2 n + 1 \rfloor$$

Éste es un número relativamente pequeño. Por ejemplo, si el árbol completo T_n tiene $n = 1\,000\,000$ nodos, entonces su profundidad $d_n = 21$.

Árboles binarios extendidos: 2-árboles

Se dice que un árbol binario T es un *2-árbol* o un *árbol binario extendido* si cada nodo N tiene 0 o 2 hijos. En tal caso, los nodos con dos hijos se denominan *nodos internos*, y los nodos con 0 hijos se denominan *nodos externos*. Algunas veces los nodos se distinguen en diagramas por medio de círculos para los nodos internos y cuadrados para los nodos externos.

La expresión "árbol binario extendido" proviene de la siguiente operación. Considere un árbol binario T, como el árbol en la figura 10-3*a*). Entonces, T puede "convertirse" en un 2-árbol al sustituir cada subárbol vacío por un nuevo nodo, como se muestra en la figura 10-3*b*). Observe que el nuevo árbol es, en efecto, un 2-árbol. Además, los nodos en el árbol original T ahora son los nodos internos en el árbol extendido, y los nuevos nodos son los nodos externos en el árbol extendido. Se observa que si un 2-árbol tiene n nodos internos, entonces tiene $n + 1$ nodos externos.



a) Árbol binario *T* *b*) 2-árbol extendido

Figura 10-3 Conversión de un árbol binario *T* en un 2-árbol

Expresiones algebraicas y notación polaca

Sea *E* cualquier expresión algebraica en la que sólo se usan operaciones binarias, como

$$E = (a - b)/((c \times d) + e)$$

Entonces *E* puede representarse por medio de un 2-árbol como en la figura 10-4*a*), donde las variables en *E* aparecen como los nodos externos y las operaciones en *E* aparecen como nodos internos.

El matemático polaco Lukasiewics observó que al escribir el símbolo para operaciones binarias antes de sus argumentos, por ejemplo,

$$+ab \text{ en lugar de } a + b \quad \text{y} \quad /cd \text{ en lugar de } c/d$$

no es necesario usar ningún paréntesis. Esta notación se denomina *notación polaca en forma de prefijo*. (De manera semejante, el símbolo puede escribirse después de sus argumentos, lo que se denomina *notación polaca en notación de posfijo*.) Cuando *E* vuelve a escribirse en forma de prefijo se obtiene:

$$E = / - a\ b + \times c\ d\ e$$

Observe que éste es precisamente el orden lexicográfico de los vértices en su 2-árbol que se obtiene al examinar el árbol como en la figura 10-4*b*).

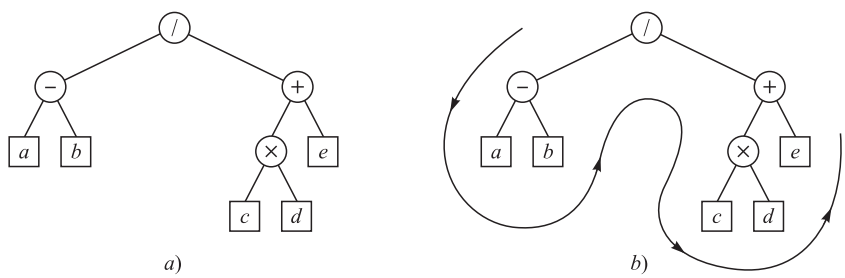


Figura 10-4

10.4 REPRESENTACIÓN DE ÁRBOLES BINARIOS EN LA MEMORIA

Sea *T* un árbol binario. En esta sección se analizan dos formas de representar *T* en la memoria. La primera forma, que es la de costumbre, se denomina *representación ligada de T* y es semejante a la forma en que las listas ligadas se representan en la memoria. La segunda forma, en la que se usa un solo arreglo, se denomina *representación secuencial de T*. El requisito principal de cualquier representación de *T* es tener acceso directo a la raíz *R* de *T* y, dado cualquier nodo *N* de *T*, debe tenerse acceso directo a los hijos de *N*.

Representación ligada de árboles binarios

Considere un árbol binario *T*. A menos que se establezca o implique otra cosa, *T* se mantiene en la memoria por medio de una representación ligada en la que se usan tres arreglos paralelos, INFO, LEFT y RIGHT, así como un apuntador variable ROOT como sigue. En primer lugar, cada nodo *N* de *T* corresponde a una ubicación *K* tal que:

1) INFO[*K*] contiene los datos en el nodo *N*.
2) LEFT[*K*] contiene la ubicación del hijo izquierdo del nodo *N*.
3) RIGHT[*K*] contiene la ubicación del hijo derecho del nodo *N*.

Además, ROOT contiene la ubicación de la raíz *R* de *T*. Si cualquier subárbol es vacío, entonces el apuntador correspondiente contiene el valor nulo; si el árbol *T* mismo es vacío, entonces ROOT contiene el valor nulo.

Observación 1: En la mayor parte de los ejemplos presentados se muestra un solo dato de información en cada nodo *N* de un árbol binario *T*. En la práctica real un registro entero puede almacenarse en el nodo *N*. En otras palabras, INFO puede realmente ser un arreglo lineal de registros o una colección de arreglos paralelos.

Observación 2: Para el apuntador nulo denotado por NULL puede escogerse cualquier dirección inválida. En la práctica real, para NULL se usa 0 o un número negativo.

EJEMPLO 10.2 Considere el árbol binario en la figura 10-1*a*). La representación ligada de *T* aparece en la figura 10-5, donde por conveniencia en la notación los arreglos lineales se han escrito en forma vertical en lugar de horizontal. Observe que ROOT = 5 apunta a INFO[5] = *A* puesto que *A* es la raíz de *T*, también que LEFT[5] = 10 apunta a INFO[10] = *B* puesto que *B* es el hijo izquierdo de *A*, y que RIGHT[5] = 2 apunta a INFO[2] = *C* puesto que *C* es el hijo derecho de *A*. Y así en lo sucesivo. La elección de 18 elementos para el arreglo es arbitraria.

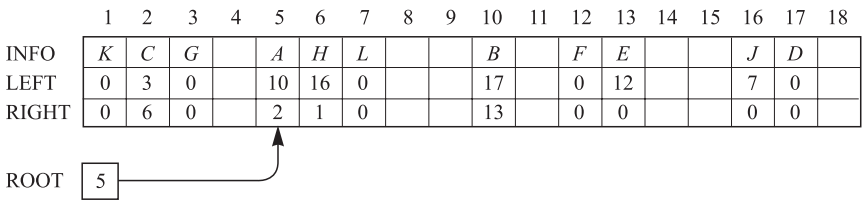


Figura 10-5

Representación secuencial de árboles binarios

Suponga que *T* es un árbol binario que es completo o casi completo. Entonces hay una forma eficiente de mantener *T* en la memoria, denominada *representación secuencial* de *T*. Esta representación usa sólo un arreglo lineal TREE junto con un apuntador variable END como sigue:

1) La raíz *R* de *T* se almacena en TREE[1].
2) Si un nodo *N* ocupa TREE[*K*], entonces su hijo izquierdo se almacena en TREE[2**K*] y su hijo derecho se almacena en TREE[2**K* + 1].
3) END contiene la ubicación del último nodo de *T*.

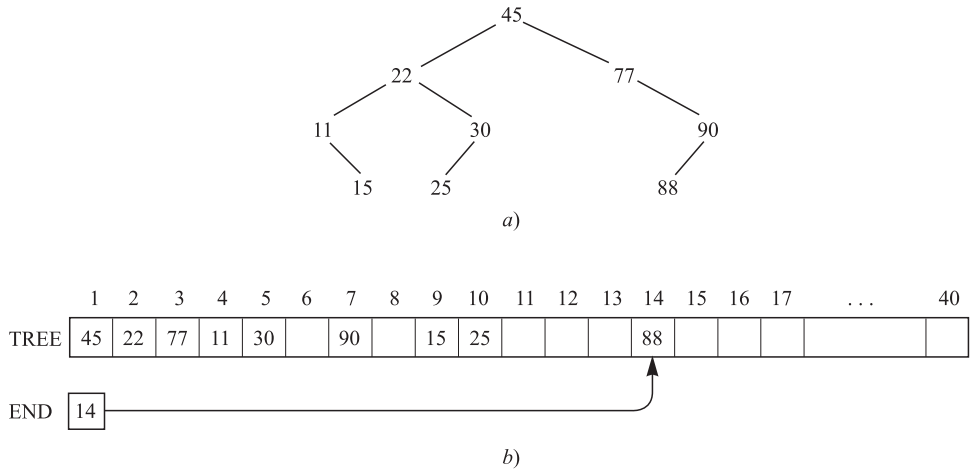


Figura 10-6

Además, el nodo *N* en TREE[*K*] contiene un subárbol izquierdo vacío o un subárbol derecho vacío según si 2^*K o $2^*K + 1$ excede END o según si TREE[2^*K] o TREE[$2^*K + 1$] contiene el valor NULL.

La representación secuencial del árbol binario *T* en la figura 10-6*a*) aparece en la figura 10-6*b*). Observe que se requieren 14 ubicaciones en el arreglo TREE aun cuando *T* sólo tiene 9 nodos. En términos generales, la representación secuencial de un árbol con profundidad *d* requiere un arreglo con aproximadamente 2^d elementos. En consecuencia, esta representación secuencial suele ser ineficiente, a menos que, como ya se afirmó, el árbol binario *T* sea completo o casi completo. Por ejemplo, el árbol *T* en la figura 10-1*a*) tiene 11 nodos y profundidad 5, es decir que requiere un arreglo con aproximadamente $2^5 = 32$ elementos.

10.5 RECORRIDO DE ÁRBOLES BINARIOS

Hay tres formas normales para recorrer un árbol binario *T* con raíz *R*. Estos tres algoritmos, que se denominan *preorden*, *inorden* y *postorden*, tienen la función de:

Preorden: 1) Procesa la raíz *R*.
2) Recorre el subárbol izquierdo de *R* en preorden.
3) Recorre el subárbol derecho de *R* en preorden.

Inorden: 1) Recorre el subárbol izquierdo de *R* en inorden.
2) Procesa la raíz *R*.
3) Recorre el subárbol derecho de *R* en inorden.

Postorden: 1) Recorre el subárbol izquierdo de *R* en postorden.
2) Recorre el subárbol derecho de *R* en postorden.
3) Procesa la raíz *R*.

Observe que cada algoritmo consta de los mismos tres pasos y que el subárbol izquierdo de *R* siempre se recorre antes que el subárbol derecho. La diferencia entre los algoritmos es el momento en que se procesa la raíz. Específicamente, en el algoritmo "pre" la raíz *R* se procesa antes de que se recorran los subárboles; en el algoritmo "in", la raíz *R* se procesa entre el recorrido de los subárboles; en el algoritmo "post", la raíz *R* se procesa después que se recorren los subárboles.

Algunas veces los tres algoritmos se denominan, respectivamente, recorrido del nodo-izquierdo-derecho (NLR: node-left-right), recorrido del izquierdo-nodo-derecho (left-node-right, LNR), y recorrido izquierdo-derecho-nodo (LRN: left-right-node).

EJEMPLO 10.3 Considere el árbol binario T en la figura 10-7*a*). Observe que A es la raíz de T, que el subárbol izquierdo L_T de T consta de los nodos B, D y E, y el subárbol derecho R_T de T consta de los nodos C y F.

a) El recorrido en preorden de T procesa A, recorre L_T y recorre R_T. Sin embargo, el recorrido en preorden de L_T procesa la raíz B y luego D y E; y el recorrido en preorden de R_T procesa la raíz C y luego F. Así, *ABDECF* es el recorrido en preorden de T.

b) El recorrido en inorden de T recorre L_T, procesa A y recorre R_T. Sin embargo, el recorrido en inorden de L_T procesa D, B y luego E; y el recorrido inorden de R_T procesa C y luego F. Así, *DBEACF* es el recorrido en inorden de T.

c) El recorrido en postorden de T recorre L_T, recorre R_T y procesa A. Sin embargo, el recorrido en postorden de L_T procesa D, E y luego B, y el recorrido en postorden de R_T procesa F y luego C. En consecuencia, *DEBFCA* es el recorrido en postorden de T.

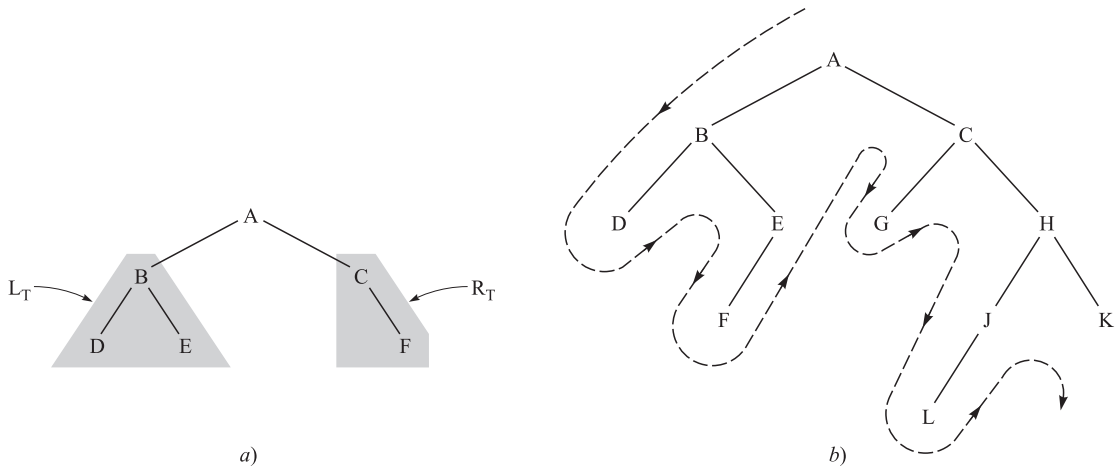


Figura 10-7

EJEMPLO 10.4 Sea T el árbol binario en la figura 10-7*b*). El recorrido en preorden es como sigue:

(Preorden) *A B D E F C G H J L K*

Este orden es el mismo que resulta al analizar el árbol desde la izquierda como se indica con el camino en la figura 10-7*b*). Es decir, se hace un "desplazamiento" por la rama más a la izquierda hasta que se encuentra un nodo terminal; luego se retrocede hacia la rama siguiente y así sucesivamente. En el recorrido en preorden, el nodo terminal más a la derecha, el nodo K, es el último nodo que se analiza. Observe que el subárbol izquierdo de la raíz A se recorre antes que el subárbol derecho; y que ambos se recorren después de A. Lo mismo es cierto para cualquier otro nodo que tenga subárboles, que es la propiedad subyacente de un recorrido en preorden.

El lector puede comprobar por inspección que las otras dos formas de recorrer el árbol T en la figura 10-7*b*) son como sigue:

(Inorden) *D B F E A G C L J H K*
(Postorden) *D F E B G L J K H C A*

Observación: Los nodos terminales D, F, G, L y K del árbol binario en la figura 10-7*b*) se recorren en el mismo orden, de izquierda a derecha, en los tres recorridos, lo que es verdad para cualquier árbol binario T.

10.6 ÁRBOLES BINARIOS DE BÚSQUEDA

En esta sección se analiza una de las estructuras de datos más importantes en computación: un árbol binario de búsqueda. Dicha estructura permite buscar y encontrar un elemento con un tiempo medio de ejecución $f(n) = O(\log_2 n)$, donde n es el número de datos. También permite insertar y eliminar elementos fácilmente. Esta estructura contrasta con las siguientes estructuras:

a) *Arreglo lineal ordenado*: permite buscar y encontrar un elemento con tiempo de ejecución $f(n) = O(\log_2 n)$. Sin embargo, insertar y eliminar elementos es costoso puesto que, en promedio, implica el movimiento de $O(n)$ elementos.

b) *Lista ligada*: permite insertar y eliminar elementos fácilmente. No obstante, resulta costoso buscar y encontrar un elemento, ya que es necesario usar una búsqueda lineal con tiempo de ejecución $f(n) = O(n)$.

Aunque cada nodo en un árbol binario de búsqueda puede contener un registro completo de datos, la definición del árbol depende de un campo dado cuyos valores son distintos y pueden ordenarse.

Definición: Suponga que T es un árbol binario. Entonces T se denomina *árbol binario de búsqueda* si cada nodo N de T tiene la siguiente propiedad:

> El valor de N es mayor que cualquier valor en el subárbol izquierdo de N y es menor que cualquier valor en el subárbol derecho de N.

No es difícil ver que la propiedad enunciada garantiza que el recorrido en inorden de T produce un listado ordenado de los elementos de T.

Observación: La definición anterior de un árbol binario de búsqueda supone que todos los valores de los nodos son distintos. Hay una definición semejante de un árbol binario de búsqueda T que admite duplicados; es decir, donde cada nodo N tiene las siguientes propiedades:

a) $N > M$ para cualquier nodo M en un subárbol izquierdo de N.

b) $N \leq M$ para cualquier nodo M en un subárbol derecho de N.

La aplicación de esta definición modifica las operaciones siguientes, según el caso.

EJEMPLO 10.5 El árbol binario T en la figura 10-8*a*) es un árbol binario de búsqueda. Es decir, todo nodo N en T excede a todo número en su subárbol izquierdo y es menor que cualquier número en su subárbol derecho. Suponga que el 23 se sustituye por 35 y T aún es un árbol binario de búsqueda. Por otra parte, suponga que el 23 se sustituye por 40. Entonces T no sería un árbol binario de búsqueda, puesto que 40 estaría en el subárbol izquierdo de 38 pero $40 > 38$.

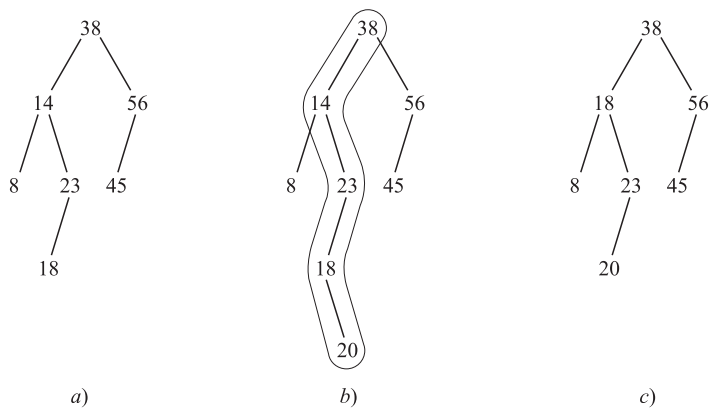


Figura 10-8

Búsqueda e inserción en un árbol binario de búsqueda

En la figura 10-9 se muestra un algoritmo de búsqueda e inserción en un árbol binario de búsqueda T.

Algoritmo 10.1: Se proporcionan un árbol binario de búsqueda T y un ITEM de información. El algoritmo encuentra la ubicación de ITEM en T, o inserta ITEM como un nuevo nodo en el árbol.

Paso 1. ITEM se compara con la raíz N del árbol.
- *a*) Si ITEM $< N$ se procede al hijo izquierdo de N.
- *b*) Si ITEM $> N$ se procede al hijo derecho de N.

Paso 2. Se repite el paso 1 hasta que ocurre una de las siguientes situaciones:
- *a*) Se encuentra un nodo N tal que ITEM $= N$. En este caso, la búsqueda ha sido exitosa.
- *b*) Se encuentra un subárbol vacío, indicación de que la búsqueda ha sido infructuosa. ITEM se inserta en lugar del subárbol vacío.

Paso 3. Salir.

Figura 10-9

EJEMPLO 10.6 Considere el árbol binario de búsqueda T en la figura 10-8*a*). Suponga que se proporciona ITEM $= 20$, y que se desea encontrar o insertar ITEM en T. Al simular el algoritmo 10-1 se obtienen los pasos siguientes:

1) ITEM $= 20$ se compara con la raíz $R = 38$. Puesto que $20 < 38$, se procede al hijo izquierdo de 38, que es 14.
2) ITEM $= 20$ se compara con 14. Puesto que $20 > 14$, se procede al hijo derecho de 14, que es 23.
3) ITEM $= 20$ se compara con 23. Puesto que $20 < 23$, se procede al hijo izquierdo de 23, que es 18.
4) ITEM $= 20$ se compara con 18. Puesto que $20 > 18$ y 18 no tiene hijo derecho, 20 se inserta como el hijo derecho de 18.

En la figura 10-11*b*) se muestra el nuevo árbol con ITEM $= 20$ insertado. Se destaca el camino bajo el árbol durante el algoritmo.

Eliminación en un árbol binario de búsqueda

En la figura 10-10 se muestra un algoritmo que elimina un ITEM dado de un árbol binario de búsqueda T. Se usa el algoritmo 10-1 en la figura 10-9 para encontrar la ubicación de ITEM en T.

Observación: El caso *iii*) en el paso 2*c*) es más complicado que en los dos primeros casos. El sucesor inorden $S(N)$ de N se encuentra como sigue. A partir del nodo N se realiza un desplazamiento a la derecha hacia al hijo derecho de N y luego se hacen desplazamientos sucesivos hacia la izquierda hasta que se encuentra un nodo M sin hijo izquierdo. El nodo M es el sucesor inorden $S(N)$ de N.

EJEMPLO 10.7 Considere el árbol binario T en la figura 10-8*b*). Suponga que se desea eliminar ITEM $= 14$ de T. Primero se encuentra el nodo N tal que $N = 14$. Observe que $N = 14$ tiene dos hijos. Al realizar un movimiento hacia la derecha y luego a la izquierda, se encuentra el sucesor inorden $S(N) = 18$ de N. $S(N) = 18$ se elimina al sustituirlo por su hijo único 20, y luego $N = 14$ se sustituye por $S(N) = 18$. Así se obtiene el árbol en la figura 10-8*c*).

Complejidad de los algoritmos de los árboles binarios de búsqueda

Sea T un árbol binario con n nodos y profundidad d, y sea $f(n)$ que denota el tiempo de ejecución de cualquiera de los algoritmos anteriores. El algoritmo 10.1 indica proceder a partir de la raíz R y recorrer el árbol T hasta encontrar ITEM en T o insertar ITEM como un nodo terminal. El algoritmo 10.2 indica proceder a partir de la raíz R y recorrer el árbol T para encontrar ITEM y luego continuar el recorrido por el árbol para encontrar el sucesor inorden de ITEM. En

Algoritmo 10.2: Se proporcionan un árbol binario de búsqueda T y un ITEM de información. $P(N)$ denota el padre de un nodo N, y $S(N)$ denota el sucesor inorden de N. El algoritmo elimina ITEM de T.

Paso 1. El algoritmo 10.1 se usa para encontrar la ubicación del nodo N que contiene a ITEM y mantiene el rastro de la ubicación del nodo padre $P(N)$. (Si ITEM no está en T, entonces STOP y salir.)

Paso 2. Se determina el número de hijos de N. Hay tres casos:

a) N no tiene hijos. N se elimina de T al sustituir simplemente la ubicación de N en el nodo padre $P(N)$ por el apuntador NULL.

b) N tiene exactamente un hijo M. N se elimina de T al sustituir la ubicación de N en el nodo padre $P(N)$ por la ubicación de M. (Esto sustituye N por M.)

c) N tiene dos hijos.

i) Se encuentra el sucesor inorden $S(N)$ de N. (Entonces $S(N)$ no tiene hijo izquierdo.)

ii) $S(N)$ se elimina de T usando *a*) o *b*).

iii) N se sustituye por $S(N)$ en T.

Paso 3. Salir.

Figura 10-10

cualquier caso, el número de movimientos no puede exceder la profundidad d del árbol. Por tanto, el tiempo de ejecución $f(n)$ de cualquier algoritmo depende de la profundidad d del árbol T.

Ahora suponga que T tiene la propiedad de que, para cualquier nodo N de T, las profundidades de los subárboles de N difieren cuando mucho por 1. Entonces se dice que el árbol T está balanceado y $d \approx \log_2 n$. En consecuencia, el tiempo de ejecución $f(n)$ de cualquier algoritmo en un árbol balanceado es muy rápido; específicamente, $f(n) = O(\log_2 n)$. Por otra parte, a medida que se agregan datos en un árbol binario de búsqueda T, no hay garantía de que T permanezca balanceado. Incluso puede ocurrir que $d \approx n$. En este caso, $f(n)$ puede ser relativamente lento; específicamente, $f(n) = O(n)$. Por fortuna, hay técnicas para volver a balancear un árbol binario de búsqueda T a medida que se le agregan elementos. Sin embargo, tales técnicas rebasan el alcance de este texto.

10.7 COLAS PRIORITARIAS, MONTÍCULOS

Sea S una cola de prioridad. Es decir, S es un conjunto donde es posible insertar o eliminar elementos periódicamente, pero donde siempre se elimina el mayor elemento actual (el elemento con prioridad más alta). Para mantener a S en la memoria hay que hacer un:

a) Arreglo lineal: aquí resulta fácil insertar un elemento al agregarlo simplemente al final del arreglo. Sin embargo, resulta costoso buscar y encontrar el elemento más grande, ya que es necesario usar una búsqueda lineal con tiempo de ejecución $f(n) = O(n)$.

b) Arreglo lineal ordenado: aquí el elemento más grande es el primero o el último, de modo que es fácil eliminarlo. No obstante, insertar y eliminar elementos resulta costoso porque, en promedio, implica mover $O(n)$ elementos.

En esta sección se presenta una estructura discreta que puede implementar en forma eficiente una cola de prioridad S.

Montículos

Suponga que H es un árbol binario completo con n elementos. Se supone que H se mantiene en la memoria mediante su representación secuencial, no una representación ligada. (Vea la sección 10.4.)

Definición 10.1: Suponga que H es un árbol binario completo. Entonces H se denomina *montículo* (*heap*) o *máxheap*, si cada nodo N tiene la siguiente propiedad.

El valor de N es mayor que o igual al valor de cada uno de los hijos de N.

Por consiguiente, en un montículo, el valor de N excede el valor de cada uno de sus descendientes. En particular, la raíz de H es un valor más grande de H.

Un *mínheap* se define en forma semejante: el valor de N es menor que o igual al valor de cada uno de sus hijos.

EJEMPLO 10.8 Considere el árbol binario completo H en la figura 10-11*a*). Observe que H es un montículo. Esto significa, en este caso, que el elemento más grande de H aparece en la "parte superior" del montículo. En la figura 10-11*b*) se muestra la representación secuencial de H mediante el arreglo TREE y la variable END. En consecuencia:

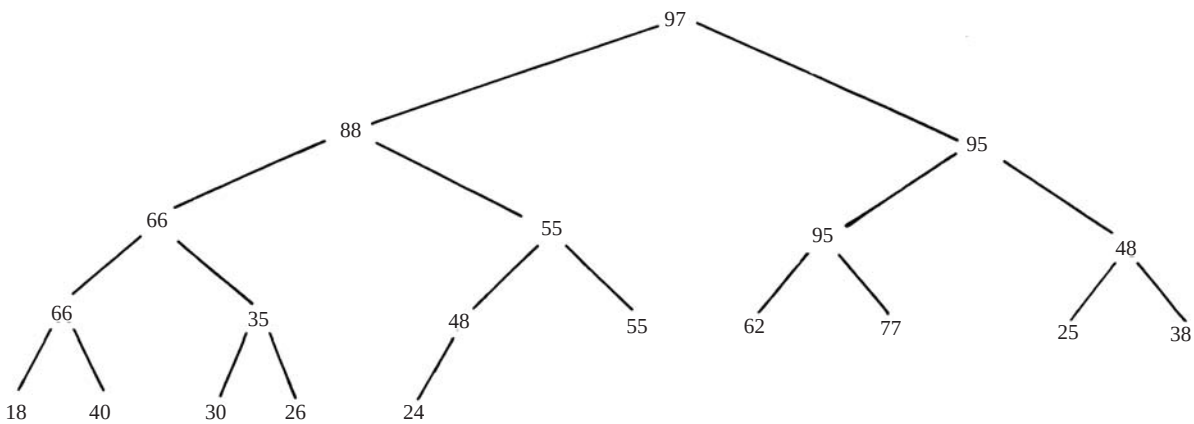
a) TREE[1] es la raíz R de H.

b) TREE[2K] y TREE[2K + 1] son los hijos izquierdo y derecho de TREE[K].

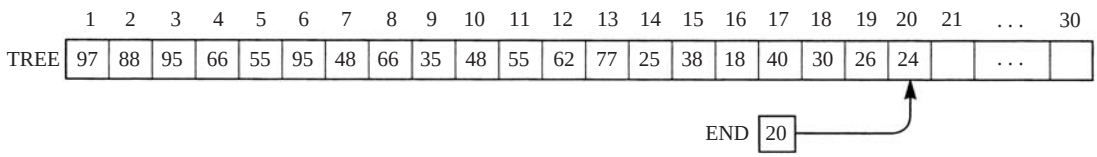
c) La variable END = 20 apunta al último elemento en H.

d) El padre de cualquier nodo TREE(J) distinto de la raíz es el nodo TREE[$J \div 2$] (donde $J \div 2$ significa división entera).

Observe que los nodos de H en el mismo nivel aparecen uno después del otro en el arreglo TREE. La elección de 30 ubicaciones para TREE es arbitraria.



a) Montículo



b) Representación secuencial

Figura 10-11

Inserción en un montículo

En la figura 10-12 se proporciona un algoritmo que inserta un ITEM de datos dado en un montículo H.

Observación: Es necesario comprobar que el algoritmo 10.3 produce un montículo como el árbol final. No es difícil ver esto y la verificación se deja al lector.

EJEMPLO 10.9 Considere el montículo H en la figura 10-11. Suponga que se desea insertar ITEM = 70 en H. Al simular el algoritmo 10.3, primero se adjunta ITEM como el último elemento del árbol completo; es decir, como el hijo derecho de 48.

Algoritmo 10.3: Se proporcionan un montículo H y un nuevo ITEM. El algoritmo inserta ITEM en H.

Paso 1. ITEM se adjunta al final de H, de modo que H aún es un árbol completo, pero no necesariamente un montículo.

Paso 2. (Reheap) Se deja que ITEM suba a su "sitio apropiado" en H, de modo que H es un montículo. Es decir:

a) ITEM se compara con su padre P(ITEM). Si ITEM $>$ P(ITEM), entonces se intercambian ITEM y P(ITEM).

b) Se repite *a*) hasta que ITEM $\leq$ P(ITEM).

Paso 3. Salir

Figura 10-12

En otras palabras, se hace TREE[21] $=$ 70 y END $=$ 21. Luego se aplica la operación *reheap*; es decir, se deja que ITEM suba a su sitio apropiado como sigue:

a) ITEM $=$ 70 se compara con su padre 48. Puesto que 70 $>$ 48, se intercambian 70 y 48.

b) ITEM $=$ 70 se compara con su nuevo padre 55. Puesto que 70 $>$ 55, se intercambian 70 y 55.

c) ITEM $=$ 70 se compara con su padre 88. Puesto que 70 $<$ 88, ITEM $=$ 70 ha subido a su sitio apropiado en el montículo H.

En la figura 10-13 se muestra el árbol final H con la inserción de ITEM $=$ 70. En el árbol se destaca el camino hecho por ITEM.

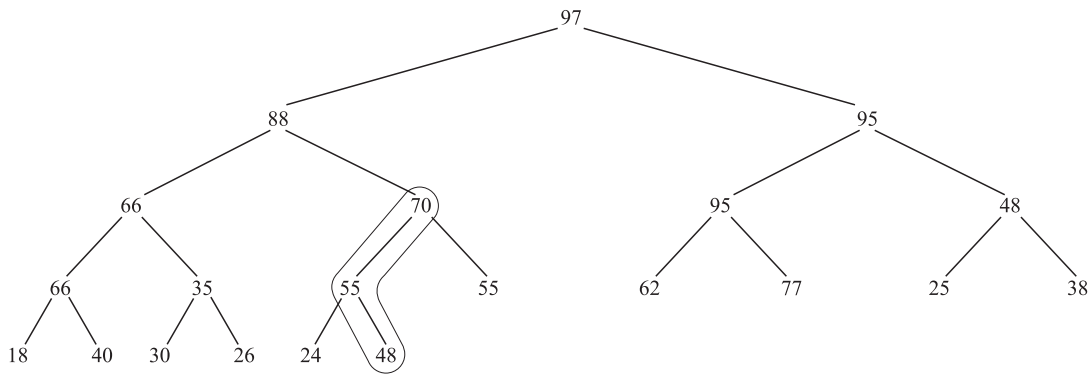


Figura 10-13 ITEM = 70 se ha insertado

Eliminación de la raíz de un montículo

En la figura 10-14 se proporciona un algoritmo que elimina la raíz R de un montículo H.

Observación: Tal como ocurre en la inserción en un montículo es necesario comprobar que el algoritmo 10.4 siempre produce un montículo como árbol final. De nuevo, esta verificación se deja al lector. Se le recuerda que el paso 3 termina hasta que el nodo L llega a la parte inferior del árbol; es decir, hasta que L no tiene hijos.

EJEMPLO 10.10 Considere el montículo H en la figura 10-15*a*), donde R $=$ 95 es la raíz y L $=$ 22 es el último nodo de H. Suponga que quiere eliminar R $=$ 95 del montículo H. Al simular el algoritmo 10.4, primero se "elimina" R $=$ 95 al asignar ITEM $=$ 95, y luego se sustituye R $=$ 95 por L $=$ 22. Así se obtiene el árbol completo en la figura 10-15*b*) que no es un montículo.

Algoritmo 10.4: El algoritmo elimina la raíz *R* de un montículo *H* dado.

Paso 1. La raíz *R* se asigna a algún ITEM variable.

Paso 2. La raíz eliminada *R* se sustituye por el último nodo de *L* de *H*, de modo que *H* aún es un árbol binario completo, aunque no necesariamente un montículo. [Es decir, se hace TREE[1] := TREE[END] y luego se hace END := END – 1.]

Paso 3. (*Reheap*) Se hace que *L* asuma su "sitio apropiado" en *H* de modo que *H* es un montículo. Es decir:
a) Se encuentra el mayor hijo LARGE(*L*) de *L*. Si $L <$ LARGE(*L*), entonces se intercambian *L* y LARGE(*L*).
b) Se repite *a*) hasta que $L \geq$ LARGE(*L*).

Paso 4. Salir.

Figura 10-14

(Observe que ambos subárboles de 22 aún son montículos.) Luego se efectúa una operación *reheap*; es decir, se deja que $L = 22$ asuma su sitio apropiado como sigue:

a) Los hijos de $L = 22$ son 85 y 70. El mayor es 85. Puesto que $22 < 85$, se intercambian 22 y 85. Así se obtiene el árbol en la figura 10-15*c*).

b) Ahora los hijos de $L = 22$ son 33 y 55. El mayor es 55. Puesto que $22 < 55$, se intercambian 22 y 55. Así se obtiene el árbol en la figura 10-15*d*).

c) Ahora los hijos de $L = 22$ son 15 y 11. El mayor es 55. Puesto que $22 > 15$, el nodo $L = 22$ ha asumido su sitio apropiado en el montículo.

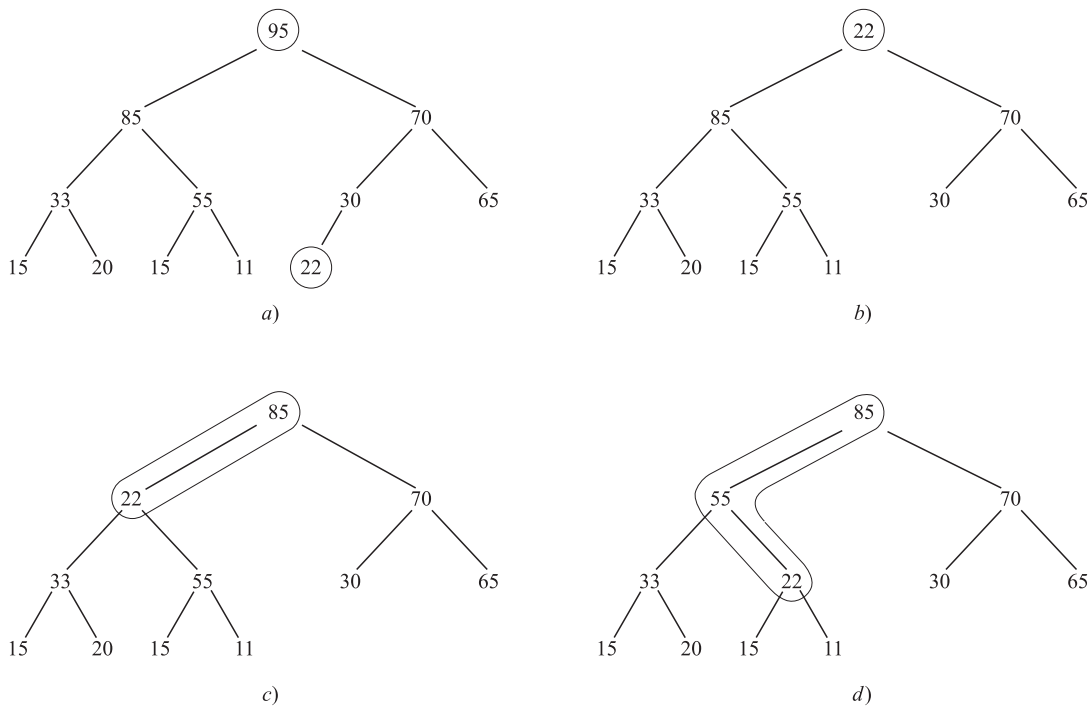


Figura 10-15

Así, la figura 10-15*d*) es el montículo requerido H sin su raíz original $R = 95$. Observe que se han encerrado los caminos a medida que $L = 22$ recorre el árbol.

Complejidad de los algoritmos de montículos

Sea H un montículo con n nodos. Puesto que H es un árbol completo, $d \approx \log_2 n$, donde d es la profundidad de H. El algoritmo 10.3 indica dejar que el nuevo ITEM recorra el árbol, de nivel en nivel, hasta que encuentre su sitio apropiado en H. El algoritmo 10.4 indica dejar que el último nodo original L recorra el árbol, de nivel en nivel, hasta que encuentre su sitio apropiado en H. En cualquier caso, el número de movimientos no puede exceder la profundidad d de H. Así, el tiempo de ejecución $f(n)$ de cualquier algoritmo es muy rápido; específicamente, $f(n) = O(\log_2 n)$. En consecuencia, el montículo constituye una forma mucho más eficiente de implementar una cola de prioridad S que el arreglo lineal o el arreglo lineal ordenado mencionado al principio de la sección.

10.8 LONGITUDES DE CAMINOS, ALGORITMO DE HUFFMAN

Sea T un árbol binario extendido o un 2-árbol (sección 10.3). Recuerde que si T tiene n nodos externos, entonces T tiene $n - 1$ nodos internos. En la figura 10-3*b*) se muestra un 2-árbol con siete nodos externos y entonces $7 - 1 = 6$ nodos internos.

Longitudes de caminos ponderados

Suponga que T es un 2-árbol con n nodos externos, y que a cada nodo externo se asigna un peso (no negativo). La longitud del camino ponderado (o simplemente la longitud del camino) P del árbol T se define como la suma

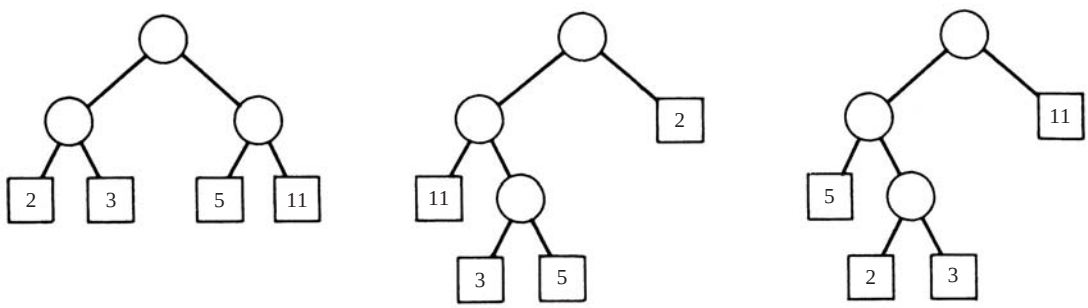
$$P = W_1L_1 + W_2L_2 + \cdots + W_nL_n$$

donde W_1 es el peso en un nodo externo N_i y L_i es la longitud del camino desde la raíz R hasta el nodo L_i. (La longitud del camino existe inclusive para 2-árboles no ponderados, donde simplemente se supone el peso 1 en cada nodo externo.)

EJEMPLO 10.11 En la figura 10-16 se muestran tres árboles binarios, T_1, T_2, T_3, donde cada uno tiene nodos externos con los mismos pesos 2, 3, 5 y 11. Las longitudes de caminos ponderados de los tres árboles son:

$$P_1 = 2(2) + 3(2) + 5(2) + 11(2) = 42$$
$$P_2 = 2(1) + 3(3) + 5(3) + 11(2) = 48$$
$$P_3 = 2(3) + 3(3) + 5(2) + 11(1) = 36$$

Las cantidades P_1 y P_3 indican que el árbol completo no necesariamente proporciona un camino mínimo, y que las cantidades P_2 y P_3 indican que árboles semejantes no necesariamente proporcionan la misma longitud del camino.



a) T_1 *b*) T_2 *c*) T_3

Figura 10-16

Algoritmo de Huffman

El problema general que se quiere resolver es el siguiente. Suponga que se proporciona una lista de n pesos:

$$W_1, W_2, \ldots, W_n$$

De entre todos los árboles binarios con n nodos externos y con los n pesos dados, se debe encontrar un árbol con longitud del camino ponderado mínimo. (Un árbol así rara vez es único.) Huffman proporcionó un algoritmo para encontrar un árbol T así.

El algoritmo de Huffman, que se muestra en la figura 10-17, se define recursivamente en términos del número n de pesos. En la práctica se usa una forma iterada equivalente del algoritmo de Huffman que construye el árbol T buscado a partir de la parte inferior, en lugar de hacerlo desde la parte superior.

Algoritmo 10.5 (de Huffman): El algoritmo encuentra recursivamente un árbol binario ponderado T con n pesos dados $w_1, w_2, \ldots, w_n$ que tiene una longitud del camino ponderado mínimo.

Paso 1. Suponga $n = 1$. Sea T el árbol con un nodo N con peso w_1, y luego Salir.

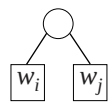
Paso 2. Suponga $n > 1$.

a) Se encuentran dos pesos mínimos, por ejemplo, w_i y w_j, de entre los n pesos dados.

b) w_i y w_j se sustituyen en la lista por $w_i + w_j$, de modo que la lista tenga $n - 1$ pesos.

c) Se encuentra un árbol T' que proporcione una longitud del camino ponderado mínimo para los $n - 1$ pesos.

d) En el árbol T' se sustituye el nodo externo

$\boxed{w_i + w_j}$ por el subárbol 

e) Salir.

Figura 10-17

EJEMPLO 10.12 Sean A, B, C, D, E, F, G, H ocho datos con los siguientes pesos asignados:

Dato:	A	B	C	D	E	F	G	H
Peso:	22	5	11	19	2	11	25	5

Construir un árbol binario T con una longitud del camino ponderado mínimo P que tenga los datos anteriores como nodos externos.

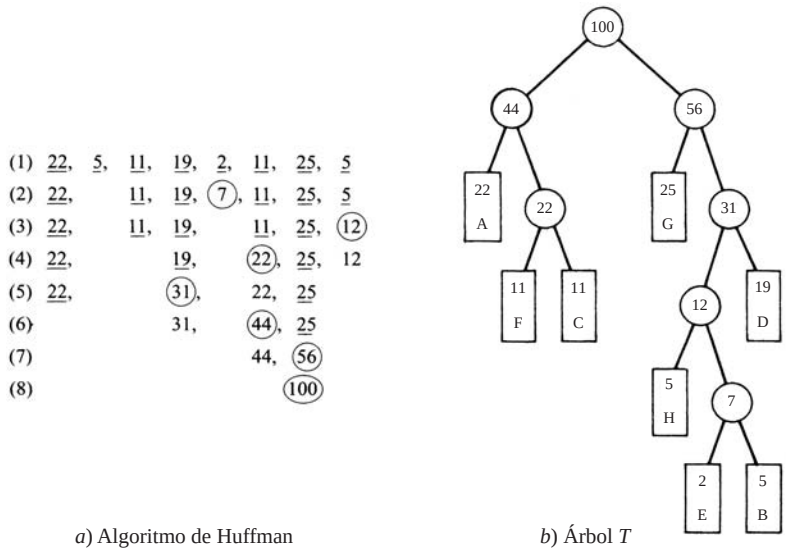
Se aplica el algoritmo de Huffman. Es decir, los dos subárboles con pesos mínimos se combinan repetidamente en un solo árbol como se muestra en la figura 10-18*a*). Por razones de claridad los pesos originales se han subrayado y un número en un círculo indica la raíz de un nuevo subárbol. El árbol T se traza a partir del paso 8) hacia atrás, con lo que se obtiene la figura 10-18*b*). (Cuando un nodo se separa en dos partes, el menor se indica a la izquierda.) A continuación se proporciona la longitud del camino P:

$$P = 22(2) + 11(3) + 11(3) + 25(2) + 5(4) + 2(5) + 5(5) + 19(3) = 280$$

Implementación en computadora del algoritmo de Huffman

Considere de nuevo los datos en el ejemplo 10.12. Suponga que se desea implementar el algoritmo con la computadora. Puesto que algunos de los nodos en el árbol binario están ponderados, el árbol puede mantenerse por medio de cuatro arreglos paralelos: INFO, WT, LEFT y RIGHT. En las ocho primeras columnas de la figura 10-19 se muestra la forma en que los datos pueden almacenarse inicialmente en la computadora.

Cada paso del algoritmo de Huffman asigna valores a WT, LEFT y RIGHT en las columnas de la 9 a la 15, que corresponden, respectivamente, a los pasos del 2) al 8) en la figura 10-18: cada paso encuentra los dos pesos mínimos actuales y sus ubicaciones, y luego introduce la suma en WT y sus ubicaciones en LEFT y RIGHT. Por ejemplo, los pesos mínimos actuales después de asignar valores a la columna 11, que corresponde al paso 4), son 12 y 19, que aparecen en WT[10] y WT[4]. Por consiguiente, se asigna WT[12] = 12 + 19 = 31 y LEFT[12] = 10 y RIGHT[12] = 4.



a) Algoritmo de Huffman *b*) Árbol *T*

Figura 10-18

El último paso indica que ROOT = 15, o se usa el hecho de que ROOT = $2n - 1$, donde $n = 8$ es el número de nodos externos. Así, toda la figura 10-19 proporciona el árbol *T* requerido.

	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16
INFO	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*									
WT	22	5	11	19	2	11	25	5		7	12	22	31	44	56	100	
LEFT	0	0	0	0	0	0	0	0		5	8	6	10	1	7	13	
RIGHT	0	0	0	0	0	0	0	0		2	9	3	4	11	12	14	
										(2)	(3)	(4)	(5)	(6)	(7)	(8)	

ROOT 15

Figura 10-19

Observación: Durante la ejecución del algoritmo de Huffman es necesario seguir la pista de los pesos actuales y encontrar dos de los pesos mínimos. Esto puede lograrse en forma satisfactoria al mantener un minheap auxiliar, donde cada nodo contenga un peso y su ubicación en el árbol. Se usa un minheap en lugar de un maxheap porque se quiere que el nodo con el peso mínimo esté en la parte superior del montículo.

Aplicación a la codificación

Suponga que una colección de *n* datos $A_1, A_2, \ldots, A_n$ va a codificarse por medio de cadenas de bits. Además, suponga que los datos no ocurren con la misma probabilidad. Entonces es posible conservar espacio y tiempo de memoria al utilizar cadenas de longitud variable, donde a los datos que ocurren frecuentemente se les asignan cadenas más cortas y a los datos que ocurren con menor frecuencia se les asignan cadenas más largas. Por ejemplo, este principio se aplica en los códigos telefónicos de países. El código de país para Estados Unidos es simplemente 1; para Francia 33 y para Finlandia 358. En esta sección se analiza una codificación que utiliza longitud variable que está basada en al *árbol T de Huffman* para datos ponderados; es decir, un árbol binario *T* con longitud del camino mínimo *P*.

Código de Huffman: Sea *T* el árbol de Huffman para los *n* datos ponderados $A_1, A_2, \ldots, A_n$. A cada arista en *T* se asigna 0 o 1 según si la arista apunta a un hijo izquierdo o a un hijo derecho. El código de Huffman asigna a cada nodo

externo A_i la secuencia de bits desde la raíz R del árbol T hasta el nodo A. El código de Huffman mencionado posee la propiedad de los "prefijos"; es decir, el código de cualquier dato no es una subcadena inicial del código de ningún otro dato. Esto significa que no puede haber ninguna ambigüedad al decodificar cualquier mensaje que use un código de Huffman.

EJEMPLO 10.13 Considere nuevamente los ocho datos *A*, *B*, *C*, *D*, *E*, *F*, *G*, *H* del ejemplo 10.12. Suponga que los pesos representan las probabilidades porcentuales de ocurrencia de los datos. Al asignar, como antes, etiquetas de bits a las aristas en el árbol de Huffman en la figura 10-18*b*), es decir, al asignar 0 o 1 según si la arista apunta hacia un hijo izquierdo o un hijo derecho, se obtiene el siguiente código para los datos:

$$A: 00, \quad B: 11011, \quad C: 011, \quad D: 111,$$
$$E: 11010, \quad F: 010, \quad G: 10, \quad H: 1100.$$

Por ejemplo, para llegar a *E* desde la raíz, el camino consta de una arista derecha, arista derecha, arista izquierda, arista derecha y arista izquierda, con lo que se obtiene el código 11010 para *E*.

10.9 ÁRBOLES GENERALES (CON RAÍZ ORDENADOS), REPASO

Sea T un árbol con raíz ordenado (sección 9.4), que también se denomina *árbol general*. T se define formalmente como un conjunto no vacío de elementos, denominados nodos, tal que

1) T contiene un elemento distintivo R, denominado *raíz* de T.
2) Los elementos restantes de T constituyen una colección ordenada de cero o más árboles ajenos, $T_1, T_2, \ldots, T_n$.

Los árboles $T_1, T_2, \ldots, T_n$ se denominan *subárboles* de la raíz R, y las raíces de $T_1, T_2, \ldots, T_n$ se denominan *sucesores* de R.

La terminología de relaciones familiares, teoría de grafos y de horticultura se usa para árboles generales de la misma forma en que se hace para árboles binarios. En particular, si N es un nodo con sucesores $S_1, S_2, \ldots, S_n$, entonces N se denomina *padre* de los S_i, los S_i se denominan hijos de N y los S_i se denominan hermanos entre sí.

EJEMPLO 10.14 La figura 10-20*a*) es una ilustración de un árbol general T con 13 nodos,

$$A, B, C, D, E, F, G, H, J, K, L, M, N$$

A menos que se establezca otra cosa, la raíz de un árbol T es el nodo en la parte superior del diagrama y los hijos de un nodo se ordenan de izquierda a derecha. En consecuencia, *A* es la raíz de *T*, y *A* tiene tres hijos: el primer hijo *B*, el segundo hijo *C* y el tercer hijo *D*. Observe que:

a) *C* tiene tres hijos.
b) Cada uno de *B* y *K* tiene dos hijos.
c) Cada uno de *D* y *H* tiene sólo un hijo.
d) Ninguno de *E*, *F*, *G*, *L*, *J*, *M* tiene hijos.

El último grupo de nodos, los que no tienen hijos, se denominan *nodos terminales*.

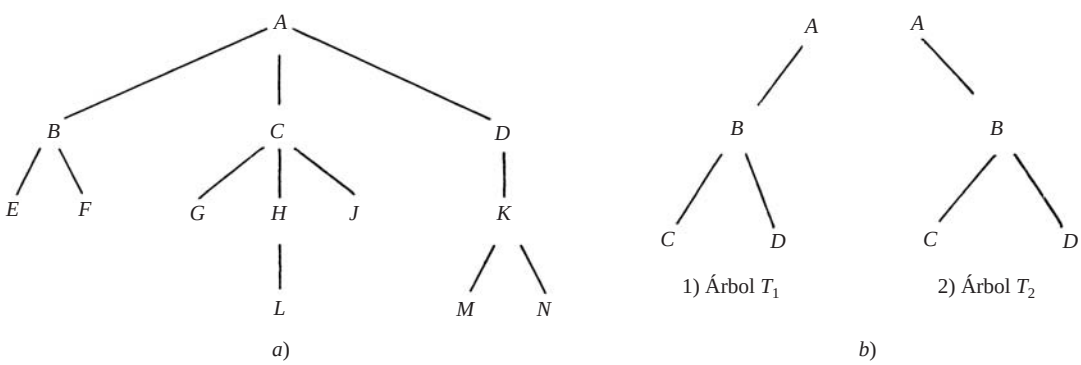


Figura 10-20

Observación: Un árbol binario T no es un caso especial de un árbol general T. Son dos objetos distintos. A continuación se presentan sus dos diferencias básicas:

1) Un árbol binario T' puede estar vacío, pero un árbol general T no está vacío.
2) Suponga que un nodo N tiene sólo un hijo. Entonces en un árbol binario T' el hijo se identifica como hijo izquierdo o hijo derecho, pero en un árbol general T no existe esta distinción.

La segunda diferencia se ilustra mediante los árboles T_1 y T_2 en la figura 10-20*b*). En cuanto a árboles binarios, T_1 y T_2 son árboles distintos, ya que B es el hijo izquierdo de A en el árbol T_1, pero B es el hijo derecho de A en el árbol T_2. Por otra parte, como árboles generales, entre T_1 y T_2 no hay ninguna diferencia.

Bosque

Un *bosque* F se define como una colección ordenada de cero o más árboles generales distintos. Resulta evidente que si se elimina la raíz R de un árbol general T, entonces se obtiene el bosque F que consta de los subárboles de R (que pueden estar vacíos). A la inversa, si F es un bosque, entonces es posible adjuntar un nodo R a F para formar un árbol general T, donde R es la raíz de T y los subárboles de R constan de los árboles originales en F.

Árboles generales y árboles binarios

Suponga que T es un árbol general. Entonces es posible asignar un único árbol binario T' a T como sigue. En primer lugar, los nodos del árbol binario T' son los mismos que los nodos del árbol general T, y la raíz de T' es la raíz de T. Sea N un nodo arbitrario del árbol binario T'. Entonces, el hijo izquierdo de N en T' es el primer hijo del nodo N en el árbol general T y el hijo derecho de N en T' es el siguiente hermano de N en el árbol general T. Esta correspondencia se ilustra en el problema 10.16.

PROBLEMAS RESUELTOS

ÁRBOLES BINARIOS

10.1 Si T es el árbol binario almacenado en la memoria, como en la figura 10-21, dibuje el diagrama de T.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
INFO	20	30	40	50	60	70	80	90			35	45	55	95
LEFT	0	1	0	0	2	0	0	7			0	3	11	0
RIGHT	0	13	0	0	6	8	0	14			12	4	0	0

ROOT 5

Figura 10-21

El árbol T se dibuja desde su raíz R hacia abajo como sigue:

a) La raíz R se obtiene a partir del valor del apuntador ROOT. Observe que ROOT = 5. Por tanto, INFO[5] = 60 es la raíz R de T.

b) El hijo izquierdo de R se obtiene a partir del campo del apuntador izquierdo de R. Observe que LEFT[5] = 2. Por tanto, INFO[2] = 30 es el hijo izquierdo de R.

c) El hijo derecho de R se obtiene a partir del campo del apuntador derecho de R. Observe que RIGHT[5] = 6. Por tanto, INFO[6] = 70 es el hijo derecho de R.

Ahora ya es posible trazar la parte superior del árbol y luego, al repetir el proceso con cada nodo nuevo, al final se obtiene todo el árbol T de la figura 10-22*a*).

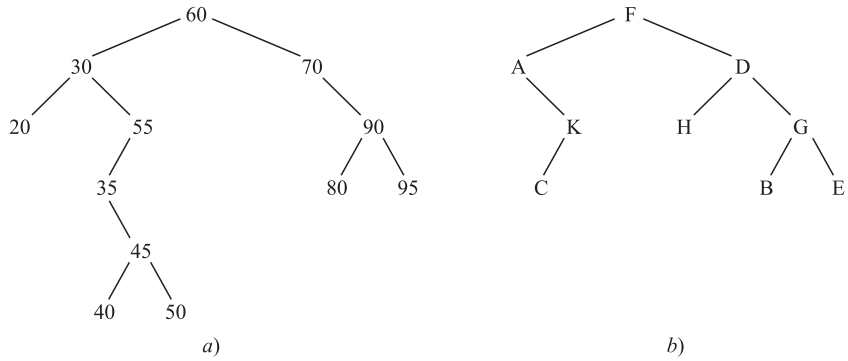


Figura 10-22

10.2 Considere el árbol binario T en la figura 10-22*b*).

a) Encuentre la profundidad d de T.
b) Recorra T con el algoritmo en preorden.
c) Recorra T con el algoritmo en inorden.
d) Recorra T con el algoritmo en postorden.
e) Encuentre los nodos terminales de T, así como el orden en que son recorridos en los incisos *b*), *c*) y *d*).

a) La profundidad d es el número de nodos en una rama más larga de T; por tanto, $d = 4$.

b) El recorrido en preorden de T es un algoritmo NLR recursivo; es decir, primero procesa un nodo N, luego su subárbol izquierdo L y, por último, su subárbol derecho R. Al hacer que $[A_1, \ldots, A_k]$ denote un subárbol con nodos $A_1, \ldots, A_k$, el árbol T se recorre como sigue:

$$F - [A, K, C][D, H, G, B, E] \quad \text{o} \quad F - A - [K, C] - D - [H][G, B, E]$$

o finalmente,

$$F - A - K - C - D - H - G - B - E$$

c) El recorrido en inorden de T es un algoritmo LNR recursivo; es decir, primero procesa un subárbol izquierdo L, luego su nodo N y, por último, su subárbol derecho R. Por tanto, T se recorre como sigue:

$$[A, K, C] - F - [D, H, G, B, E] \quad \text{o} \quad A - [K, C] - F - [H] - D - [G, B, E]$$

o finalmente,

$$A - K - C - F - H - D - B - G - E$$

d) El recorrido en postorden de T es un algoritmo LRN recursivo; es decir, primero procesa un subárbol izquierdo L, luego su subárbol derecho R y, por último, su nodo N. Por tanto, T se recorre como sigue:

$$[A, K, C][D, H, G, B, E] - F \quad \text{o} \quad [K, C] - A - [H][G, B, E] - D - F$$

o finalmente,

$$C - K - A - H - B - E - G - D - F$$

e) Los nodos terminales son los nodos sin hijos. Se recorren en el mismo orden en los tres algoritmos de recorrido: C, H, B, E.

10.3 Sea T el árbol binario en la figura 10-22*b*). Encuentre la representación secuencial de T en la memoria.

La representación secuencial de T usa un simple arreglo TREE y un apuntador variable END.

a) La raíz R de T se almacena en TREE[1]; por tanto, $R = \text{TREE}[1] = F$.

b) Si el nodo N ocupa TREE[K], entonces sus hijos izquierdo y derecho se almacenan en TREE[2^*K] y TREE[$2^*K + 1$], respectivamente. Así, TREE[2] $= A$ y TREE[3] $= D$ puesto que A y D son los hijos izquierdo y derecho de F. Y así sucesivamente. La figura 10-23 contiene la representación secuencial de T. Observe que TREE[10] $= C$, ya que C es el hijo izquierdo de K, que se almacena en TREE[5]. También, TREE[14] $= B$ y TREE[15] $= E$, ya que B y E son los hijos izquierdo y derecho de G, que se almacenan en TREE[7].

c) END apunta hacia la ubicación del último nodo de *T*; así, END = 15.

Por último, en la figura 10-23 se obtiene la representación secuencial de *T*.

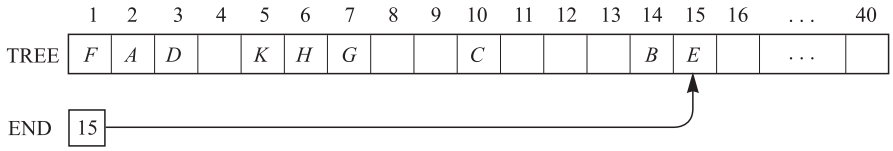


Figura 10-23

10.4 Considere los árboles T_1, T_2, T_3 en la figura 10-24 e identifique los que representen el mismo árbol:

a) con raíz; *b*) con raíz ordenado; *c*) binario.

a) Los tres representan el mismo árbol con raíz; es decir, *A* es la raíz con hijos (sucesores inmediatos) *B* y *C*, y *C* tiene el hijo único *D*.

b) Aquí T_1 y T_2 son el mismo árbol con raíz ordenado, pero T_3 es diferente: *B* es el primer hijo de *A* en T_1 y T_2, pero es el segundo hijo de *A* en T_3.

c) Todos representan árboles binarios distintos: específicamente, T_1 y T_2 son diferentes ya que es posible distinguir entre sucesores izquierdos y derechos aun cuando sólo haya un sucesor (lo que no es cierto para árboles con raíz ordenados). Es decir, *D* es un sucesor izquierdo de *C* en T_1 pero es un sucesor derecho de *C* en T_2.

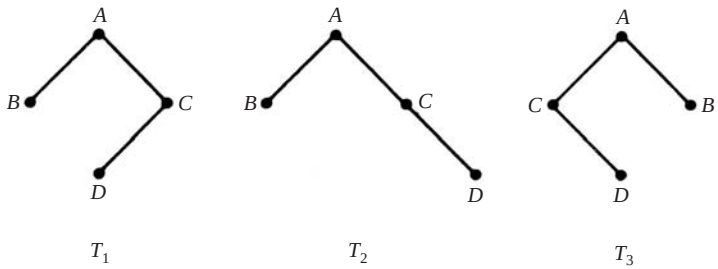


Figura 10-24

10.5 Un árbol binario *T* tiene nueve nodos. Representar *T* si los recorridos en preorden y en inorden de *T* producen las siguientes secuencias de nodos:

Preorden:	*G*	*B*	*Q*	*A*	*C*	*P*	*D*	*E*	*R*
Inorden:	*Q*	*B*	*C*	*A*	*G*	*P*	*E*	*D*	*R*

El árbol *T* se dibuja a partir de su raíz *R* hacia abajo como sigue:

a) La raíz de *T* se obtiene al escoger el primer nodo en su preorden. Así, la raíz del árbol *T* es *G*.

b) El hijo izquierdo del nodo *G* se obtiene como sigue: primero se usa el inorden de *T* para encontrar los nodos en el subárbol izquierdo T_1 de *G*. Por tanto, T_1 consta de los nodos *Q*, *B*, *C*, *A* que están a la izquierda de *G* en el inorden de *T*. Luego, el hijo izquierdo de *G* se obtiene al escoger el primer nodo (raíz) en el preorden de T_1 que aparece en el preorden de *T*. Por tanto, *B* es el hijo izquierdo de *G*.

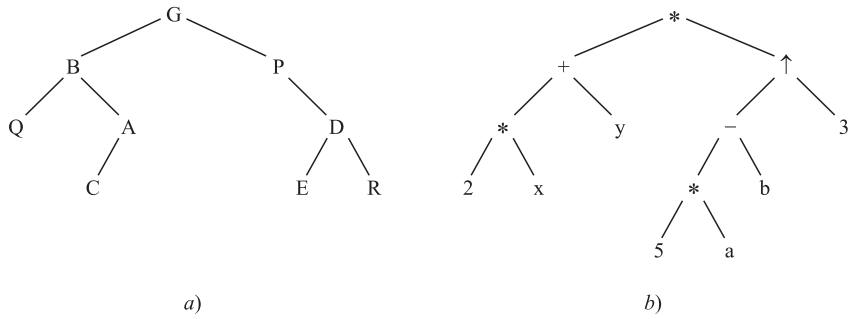
c) En forma semejante, el subárbol derecho T_2 de *G* consta de los nodos *P*, *E*, *D*, *R* y *P* es la raíz de T_2; es decir, *P* es el hijo derecho de *G*.

Al repetir el proceso anterior con cada nodo nuevo, el árbol requerido *T* se obtiene finalmente en la figura 10-25*a*).

10.6 Considere la expresión algebraica $E = (2x + y)(5a - b)^3$.

a) Trace el 2-árbol correspondiente. *b*) Use *T* para escribir *E* en forma de prefijo polaco.

a) A fin de obtener el árbol en la figura 10-25*b*) se usa una flecha (↑) para exponenciación, un asterisco (*) para multiplicación y una línea inclinada (/) para división.



a) *b*)

Figura 10-25

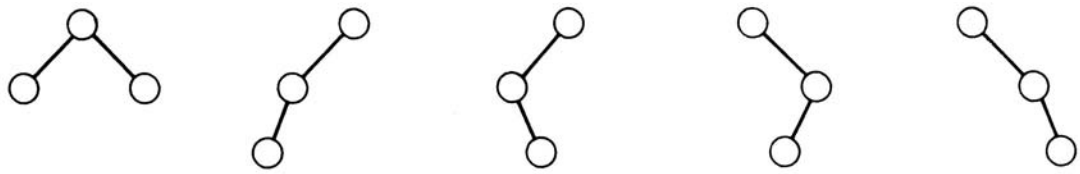
b) El árbol se examina desde la izquierda como en la figura 10-4*b*), para obtener

$$* + * 2\ x\ y \uparrow - * 5\ a\ b\ 3$$

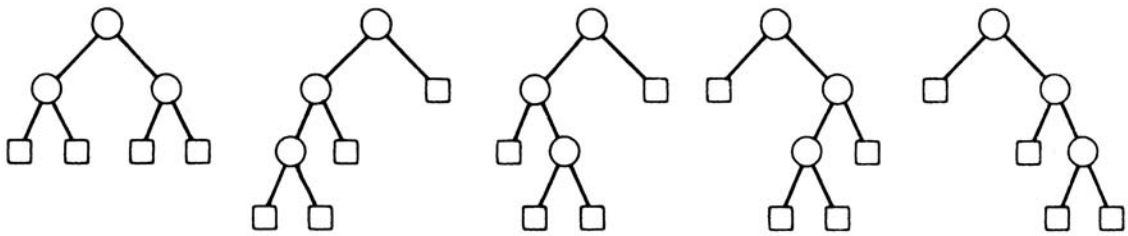
10.7 Trace todos los posibles *a*) árboles binarios T no semejantes con tres nodos; *b*) árboles binarios T' no semejantes con cuatro nodos externos.

a) Hay cinco árboles T así, que se muestran en la figura 10-26*a*).

b) Cada 2-árbol T' con cuatro nodos externos se determina por un árbol binario T con tres nodos; es decir, por un árbol T del inciso *a*. Por tanto, hay cinco árboles 2-binarios T', se muestran en la figura 10-26*b*).



a) Árboles binarios con 3 nodos



b) Árboles binarios extendidos con 4 nodos externos

Figura 10-26

ÁRBOLES BINARIOS DE BÚSQUEDA, MONTÍCULOS

10.8 Considere el árbol binario T en la figura 10-22*a*).

a) ¿Por qué T es un árbol binario de búsqueda?

b) Si al árbol se agrega ITEM = 33, encuentre el nuevo árbol T.

a) T es un árbol binario de búsqueda, puesto que cada nodo N es mayor que los valores en su subárbol izquierdo y menores que los valores en su subárbol derecho.

b) ITEM = 33 se compara con la raíz 60. Puesto que 33 < 60, el desplazamiento es hacia el hijo izquierdo, 30. Puesto que 33 > 30, el desplazamiento es hacia el hijo derecho, 55. Puesto que 33 < 55, el desplazamiento es hacia el hijo izquierdo, 35. Ahora, 33 < 35, pero 35 no tiene hijo izquierdo.

Por tanto, ITEM = 33 se agrega como un hijo izquierdo del nodo 35 para obtener el árbol en la figura 10-27*a*). Las aristas sombreadas indican el camino en el árbol durante la inserción.

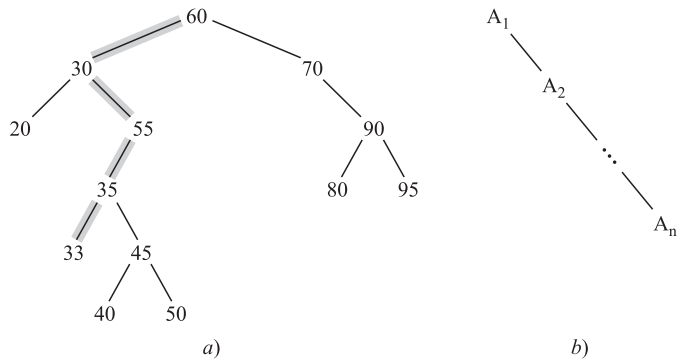


Figura 10-27

10.9 Suponga que n datos $A_1, A_2, \ldots, A_N$ ya están ordenados; es decir, $A_1 < A_2 < \cdots < A_N$.

a) Si los datos se insertan en orden en un árbol binario vacío T, describir el árbol final T.
b) ¿Cuál es la profundidad d del árbol final T?
c) Compare d con la profundidad media d^* de un árbol binario con n nodos para *i*) $n = 50$; *ii*) $n = 100$; *iii*) $n = 500$.

a) El árbol T consta de una rama que se extiende hacia la derecha, como se muestra en la figura 10-27*b*).

b) La rama de T tiene n nodos; así, $d = n$.

c) Se sabe que $d^* = c \log_2 n$, donde $c \approx 1.4$. Por tanto, *i*) $d(50) = 50$, $d^*(50) \approx 9$; *ii*) $d(100) = 100$, $d^*(100) \approx 10$; *iii*) $d(500) = 500$, $d^*(500) \approx 12$.

10.10 Suponga que la siguiente lista de letras se inserta en un árbol binario de búsqueda vacío:

$$J, \quad R, \quad D, \quad G, \quad W, \quad E, \quad M, \quad H, \quad P, \quad A, \quad F, \quad Q$$

a) Encuentre el árbol final T. *b*) Encuentre el recorrido inorden de T.

a) Los nodos se insertan uno después del otro para obtener el árbol T en la figura 10-28*a*).

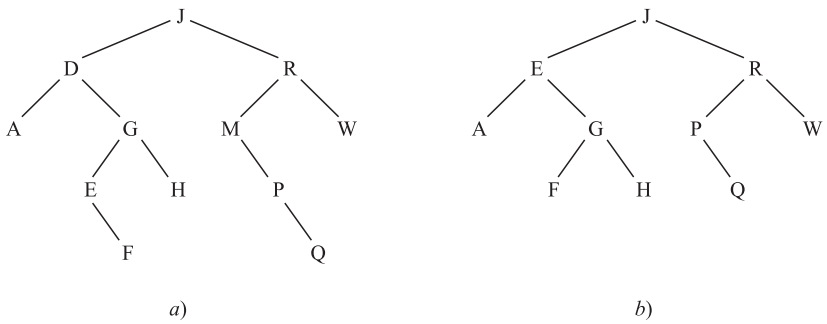


Figura 10-28

b) A continuación se muestra el recorrido inorden de *T*:

$$A, \quad D, \quad E, \quad F, \quad G, \quad H, \quad J, \quad M, \quad P, \quad Q, \quad R, \quad W$$

Es el listado alfabético de las letras. (El recorrido inorden de cualquier árbol binario *T* de búsqueda produce una lista ordenada de los nodos.)

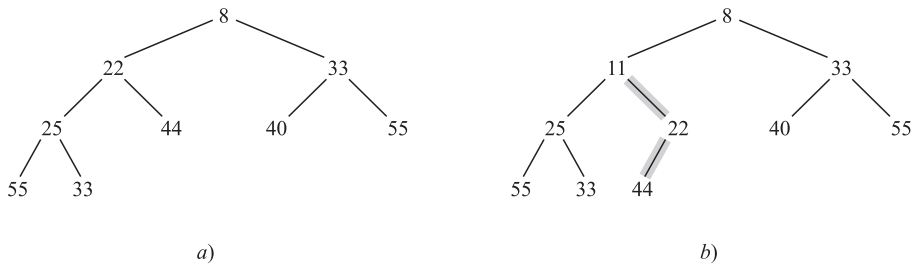
10.11 Considere el árbol binario *T* de la figura 10-28*a*), describa el árbol *T* después que se han eliminado *a*) el nodo *M* y *b*) el nodo *D*.

a) El nodo *M* tiene sólo un hijo, *P*. Por tanto, se elimina *M* y se deja que *P* se vuelva el hijo izquierdo de *R* en lugar de *M*.

b) El nodo *D* tiene dos hijos. Se encuentra el sucesor inorden de *D*, que es el nodo *E*. Primero se elimina *E* del árbol y luego *D* se sustituye por el nodo *E*.

En la figura 10-28*b*) se muestra el árbol *T* actualizado.

10.12 Sea *H* el minheap en la figura 10-29*a*). (*H* es un *minheap* puesto que los elementos más pequeños están en la parte superior del montículo, en lugar de los elementos más grandes.) Describa el montículo después que se ha insertado ITEM = 11 en *H*.



a) *b*)

Figura 10-29

Primero se inserta ITEM como el nodo siguiente en el árbol completo; es decir, como el hijo izquierdo del nodo 44. Luego, se compara ITEM con su PARENT y se intercambian ITEM y PARENT hasta que ITEM < PARENT. Puesto que $11 < 44$, se intercambian 11 y 44. Puesto que $11 < 22$ se intercambian 11 y 22. Debido a que $11 > 8$, ITEM = 11 ha encontrado su sitio apropiado en el montículo *H*. En la figura 10-29*b*) se muestra el montículo final *H*. Las aristas sombreadas indican el camino de ITEM a medida que se desplaza por el árbol.

LONGITUDES DE CAMINOS, ALGORITMO DE HUFFMAN

10.13 Sea *T* el árbol binario ponderado en la figura 10-30*a*). Encuentre la longitud del camino ponderado *P* del árbol *T*.

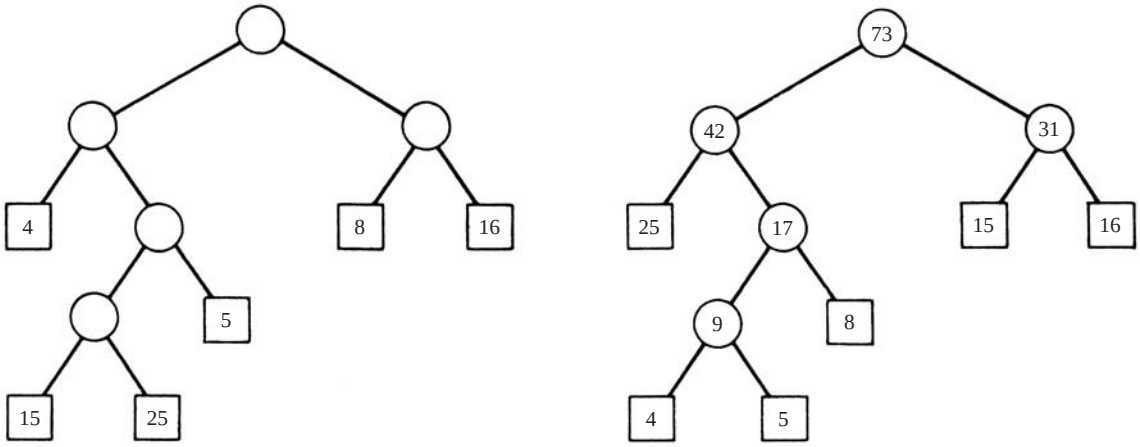
Cada peso W_i se multiplica por la longitud L_i del camino que va de la raíz de *T* al nodo que contiene el peso, y luego todos estos productos se suman para obtener *P*. Así:

$$\begin{aligned} P &= 4(2) + 15(4) + 25(4) + 5(3) + 8(2) + 16(2) \\ &= 8 + 60 + 100 + 15 + 16 + 32 \\ &= 231 \end{aligned}$$

10.14 Con los seis pesos 4, 15, 25, 5, 8, 16, encuentre un árbol binario *T* con los pesos dados y con una longitud del camino mínimo *P*. (Compare *T* con el árbol en la figura 10-30*a*).)

Se usa el algoritmo de Huffman. Es decir, se combinan en forma repetida los dos subárboles con pesos mínimos en un simple subárbol como sigue:

a) 4, 15, 25, 5, 8, 16;
b) 15, 25, (9,) 8, 16;
c) 15, 25, (17,) 16;
d) 25, 17, (31;)
e) (42,) 31;
f) (73.)



a) *b*)

Figura 10-30

(El número encerrado en un círculo indica la raíz del nuevo subárbol en el paso.) El árbol *T* se traza a partir del paso *f*) hacia atrás, con lo que se obtiene la figura 10-30*b*). La longitud del camino de *T* es la siguiente:

$$\begin{aligned} P &= 25(2) + 4(4) + 5(4) + 8(3) + 15(2) + 16(2) \\ &= 50 + 60 + 20 + 24 + 30 + 32 \\ &= 172 \end{aligned}$$

(La longitud del camino del árbol en la figura 10-30*a*) es 231.)

10.15 Si los datos *A*, *B*, *C*, *D*, *E*, *F*, *G* ocurren con la siguiente distribución de probabilidad:

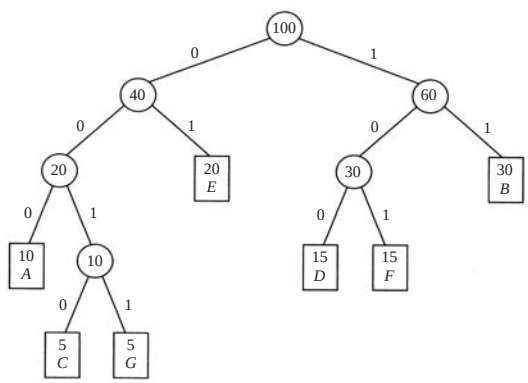
Dato:	*A*	*B*	*C*	*D*	*E*	*F*	*G*
Probabilidad:	10	30	5	15	20	15	5

Encuentre un código Huffman para los datos.

Así como en la figura 10-31*a*), el algoritmo de Huffman se aplica para encontrar un árbol binario con una longitud del camino ponderado mínimo *P*. (De nuevo, el número encerrado en un círculo indica la raíz del nuevo subárbol en el paso.) El árbol *T* se traza a partir del paso *g*) hacia atrás, con lo que se obtiene la figura 10-31*b*). Se asignan etiquetas de bits a las aristas del árbol *T*, 0 a una arista izquierda y 1 a una arista derecha, como en la figura 10-31*b*). El árbol *T* produce el siguiente código de Huffman:

$$A: 000; \quad B: 11; \quad C: 0010; \quad D: 100; \quad E: 01; \quad F: 101; \quad G: 0011$$

a) 10, 30, 5, 15, 20, 15, 5
b) 10, 30, (10,) 15, 20, 15,
c) (20,) 30, 15, 20, 15
d) 20, 30, (30,) 20
e) (40,) 30, 30
f) 40 (60,)
g) (100)



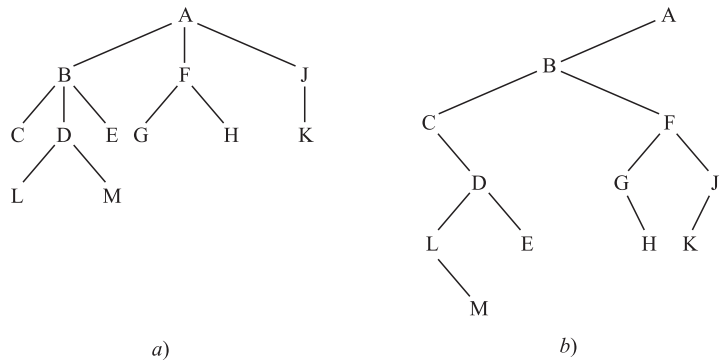
a) *b*)

Figura 10-31

ÁRBOLES GENERALES

10.16 Sea T el árbol general en la figura 10-32*a*). Encuentre el árbol binario T' correspondiente.

Los nodos de T' son los mismos que los nodos del árbol general T. En particular, la raíz de T' es la misma que la raíz de T. Además, si N es un nodo en el árbol binario T', entonces su hijo izquierdo es el primer hijo de N en T y su hijo derecho es el siguiente hermano de N en T. Al construir T' a partir de la raíz se obtiene el árbol en la figura 10-32*b*).



a) *b*)

Figura 10-32

PROBLEMAS SUPLEMENTARIOS

10.17 Considere el árbol binario T en la figura 10-33*a*).

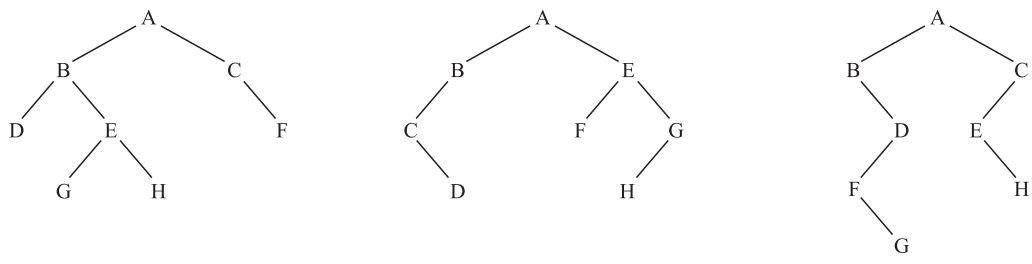
a) Encuentre: *i*) la profundidad d de T; *ii*) los descendientes de B.

b) Recorra T en *i*) preorden; *ii*) inorden; *iii*) postorden.

c) Encuentre los nodos terminales de T y los órdenes en que se recorren en el inciso *b*).

10.18 Repita el problema 10.17 para el árbol binario T en la figura 10-33*b*).

10.19 Repita el problema 10.17 para el árbol binario T en la figura 10-33*c*).



a) *b*) *c*)

Figura 10-33

10.20 Sea T el árbol binario almacenado en la memoria como en la figura 10-34, donde ROOT = 14.

a) Dibuje el diagrama de T.

b) Recorra T en *i*) preorden; *ii*) inorden; *iii*) postorden.

c) Encuentre la profundidad d de T.

d) Encuentre el número mínimo de ubicaciones requeridas para un arreglo lineal TREE si T se almacena secuencialmente en TREE.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	*H*	*R*		*P*	*B*		*E*		*C*	*F*	*Q*	*S*		*A*	*K*	*L*		*D*
LEFT	4	0		0	18		1		0	15	0	0		5	2	0		0
RIGHT	11	0		0	7		0		10	16	12	0		9	0	0		0

Figura 10-34

10.21 Suponga que los recorridos en preorden y en inorden de un árbol binario *T* producen las siguientes secuencias de nodos:

Preorden: *G, B, Q, A, C, K, F, P, D, E, R, H*
Inorden: *Q, B, K, C, F, A, G, P, E, D H, R*

a) Dibuje el diagrama de *T*.

b) Encuentre: *i*) la profundidad *d* de *T*; *ii*) los descendientes de *B*.

c) Enumere los nodos terminales de *T*.

10.22 Considere la expresión algebraica $E = (x + 3y)^4(a - 2b)$. *a*) Dibuje el árbol binario correspondiente. *b*) Escriba *E* en forma de prefijo polaco.

ÁRBOLES BINARIOS DE BÚSQUEDA, MONTÍCULOS

10.23 Encuentre el árbol final *T* si los números siguientes se insertan en un árbol binario de búsqueda vacío *T*:

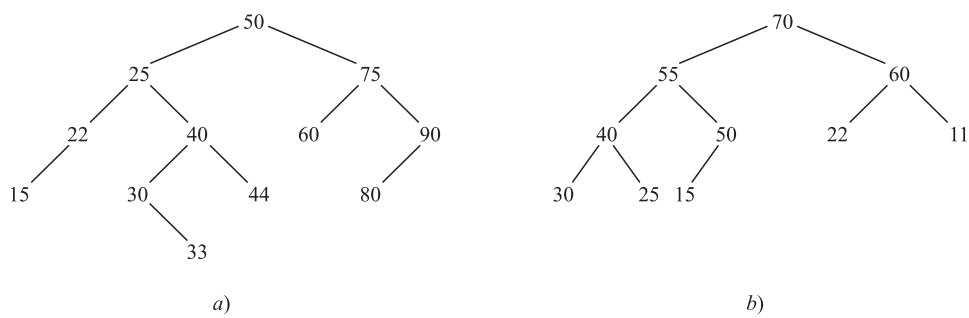
50, 33, 44, 22, 77, 35, 60, 40

10.24 Encuentre el montículo final *H* si los números en el problema 10.23 se insertan en un maxheap vacío *H*.

10.25 Encuentre el montículo final *H* si los números en el problema 10.23 se insertan en un minheap vacío *H*.

10.26 Sea *T* el árbol binario de búsqueda en la figura 10-35*a*). Suponga que los nodos 20, 55, 88 se insertan uno después del otro en *T*. Encuentre el árbol final *T*.

10.27 Sea *T* el árbol binario de búsqueda en la figura 10-35*a*). Suponga que los nodos 22, 25, 75 se eliminan uno después del otro en *T*. Encuentre el árbol final *T*.



a) *b*)

Figura 10-35

10.28 Sea *H* el montículo en la figura 10-35*b*). Encuentre el montículo final *H* si los números 65, 44 y 75 se insertan uno después del otro en *H*.

10.29 Sea *H* el montículo en la figura 10-35*b*). Encuentre el montículo final *H* si de *H* se eliminan la raíz y luego la siguiente raíz.

ALGORITMO DE HUFFMAN, ÁRBOLES GENERALES

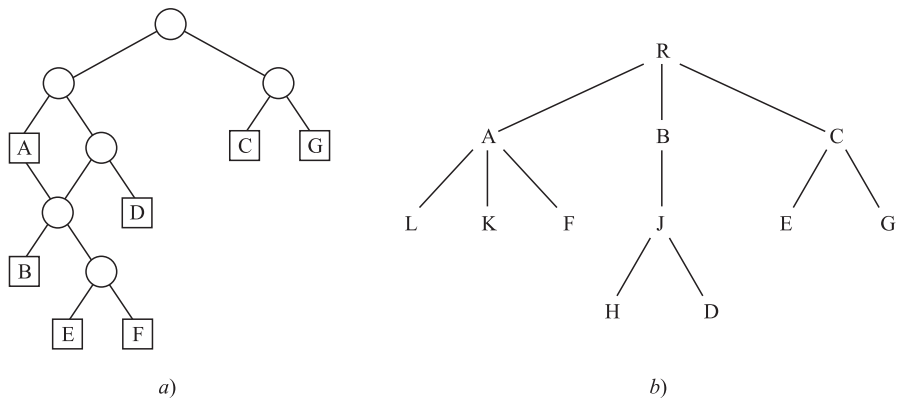
10.30 Considere el árbol binario T en la figura 10-36*a*), que contiene las letras A, B, C, D, E, F, G como nodos externos. Encuentre la codificación de Huffman de las letras determinada por el árbol T.

10.31 Encuentre la longitud del camino ponderado P del árbol en la figura 10-36*a*) si a los datos $A, B, \ldots, G$ se asignan los pesos siguientes:

$$(A, 13), \quad (B, 2), \quad (C, 19), \quad (D, 23), \quad (E, 29), \quad (F, 5), \quad (G, 9)$$

10.32 Use los datos del problema 10.31 a fin de encontrar una codificación de Huffman para las siete letras usando un árbol binario con una longitud del camino mínimo P, y encuentre P.

10.33 Sea T el árbol general en la figura 10-36*b*). Encuentre el árbol binario T' correspondiente.



a) *b*)

Figura 10-36

PROBLEMAS EN COMPUTADORA

Los problemas del 10.34 al 10.40 se refieren a la figura 10-37, que es una lista de registros de empleados almacenada en la memoria. Se trata de un árbol binario de búsqueda con respecto a la llave NAME. Usa un apuntador HEAD donde el número de empleados está en SSN[HEAD], el salario total está en SALARY[HEAD], y la raíz del árbol está en LEFT[HEAD]. También, a fin de permitir inserciones, las ubicaciones disponibles (vacías) forman una lista ligada donde AVAIL apunta hacia el primer elemento en la lista y el enlace se mantiene por medio del arreglo LEFT.

HEAD 5

AVAIL 8

	NAME	SSN	SEX	SALARY	LEFT	RIGHT
1					0	
2	Davis	192-38-7282	Female	22 800	0	12
3	Kelly	165-64-3351	Male	19 000	0	0
4	Green	175-56-2251	Male	27 200	2	0
5		0009		191 600	14	0
6	Brown	178-52-1065	Female	14 700	0	0
7	Lewis	181-58-9939	Female	16 400	3	10
8					11	
9	Cohen	177-44-4557	Male	19 000	6	4
10	Rubin	135-46-6262	Female	15 500	0	0
11					13	
12	Evans	168-56-8113	Male	34 200	0	0
13					1	
14	Harris	208-56-1654	Female	22 800	9	7

Figura 10-37

10.34 Dibuje un diagrama del árbol binario de búsqueda NAME.

10.35 Escriba un programa que imprima la lista de registros de los empleados en orden alfabético. (*Sugerencia*: imprima los registros en inorden.)

10.36 Escriba un programa que lea el nombre *NNN* de un empleado e imprima el registro del empleado. Pruebe el programa usando *a*) Evans, *b*) Smith y *c*) Lewis.

10.37 Escriba un programa que lea el número de seguridad social *SSS* de un empleado e imprima el registro del empleado. Pruebe el programa usando *a*) 165-64-3351, *b*) 135-46-626 y *c*) 177-44-5555.

10.38 Escriba un programa que lea un entero K e imprima el nombre de cada empleado varón cuando $K = 1$ o el nombre de cada empleada cuando $K = 2$. Pruebe el programa usando *a*) $K = 2$; *b*) $K = 5$, y *c*) $K = 1$.

10.39 Escriba un programa que lea el nombre *NNN* de un empleado y elimine de la estructura el registro del empleado. Pruebe el programa usando *a*) Davis; *b*) Jones, y *c*) Rubin.

10.40 Escriba un programa que lea el registro de un nuevo empleado e inserte el registro en el archivo. Pruebe el programa usando:

a) Fletcher; 168-52-3388; Mujer; 21 000;

b) Nelson; 175-32-2468; Hombre; 19 000

Respuestas a los problemas suplementarios

10.17 *a*) 4; *D*, *E*, *G*, *H*; *b*) *ABDEGHCF*, *DBGEHACF*, *DGHEBFCA*; *c*) Los tres: *D*, *G*, *H*, *F*.

10.18 *a*) 4; *C*, *D*; *b*) *ABCDEFGH*, *CDBAFEHG*, *DCBFHGEA*; *c*) Los tres: *D*, *F*, *H*.

10.19 *a*) 5; *D*, *F*, *G*; *b*) *ABDFGCEH*, *BFGDAEHC*, *GFDBHECA*; *c*) Los tres: *G*, *H*.

10.20 *a*) Vea la figura 10-38*a*); *b*) *ABDEHPQSCFKRL*, *DBPHQSEACRKFL*, *DPSQHEBRKLFCA*; *c*) $d = 6$; por tanto $32 \leq \text{END} = 64$; aquí END = 43.

10.21 *a*) Vea la figura 10-38*b*); *b*) 5; *QACKF*; *c*) *Q*, *K*, *F*, *E*, *H*.

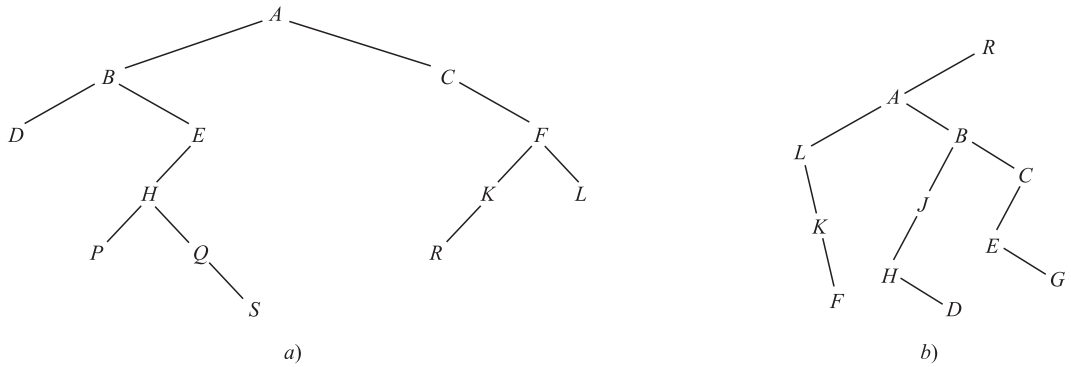


Figura 10-38

10.22 *a*) Vea la figura 10-39*a*); *b*) $* \uparrow + x * 3y4 - a * 2b$

10.23 Vea la figura 10-39*b*).

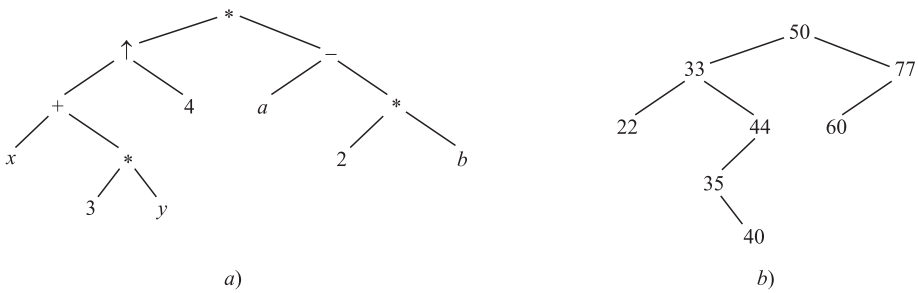


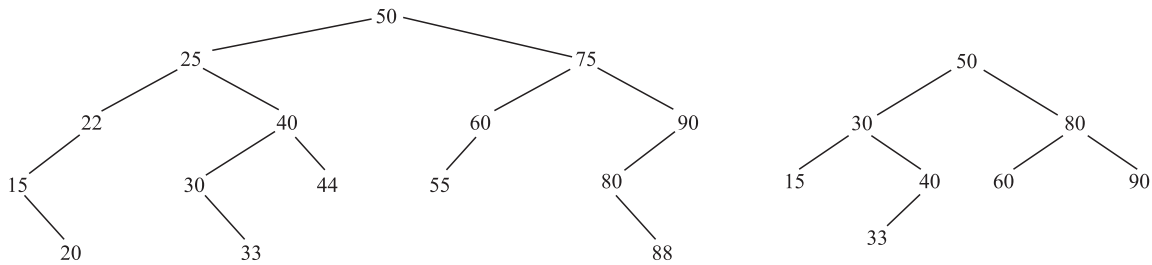
Figura 10-39

10.24 Nivel por nivel: 77, 50, 60, 40, 33, 35, 44, 22.

10.25 Nivel por nivel: 22, 33, 35, 40, 77, 44, 60, 50.

10.26 Vea la figura 10-40*a*).

10.27 Vea la figura 10-40*b*).



a) *b*)

Figura 10-40

10.28 Nivel por nivel: 75, 65, 70, 40, 55, 60, 11, 30, 25, 15, 50, 22, 44.

10.29 Nivel por nivel: 55, 50, 22, 40, 25, 15, 11, 30.

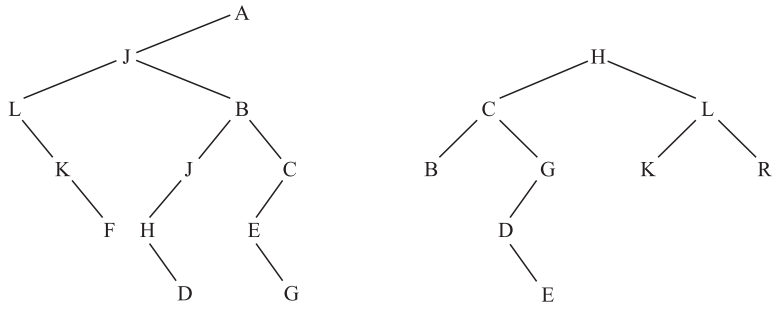
10.30 *A*: 00; *B*: 0100; *C*: 10; *D*: 011; *E*: 01010; *F*: 01011; *G*: 11.

10.31 $P = 329$.

10.32 *A*: 000; *B*: 00101; *C*: 10; *D*: 11; *E*: 01; *F*: 00100; *G*: 0011; $P = 257$.

10.33 Vea la figura 10-41*a*).

10.34 Vea la figura 10-41*b*), donde sólo se usa la primera letra de cada nombre.



a) *b*)

Figura 10-41

11 Propiedades de los enteros

CAPÍTULO

11.1 INTRODUCCIÓN

En este capítulo se investigan algunas propiedades fundamentales de los *números naturales* (o *enteros positivos*); es decir, el conjunto

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

y sus "primos", los enteros; es decir, el conjunto

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

(La letra **Z** proviene de la palabra "Zahlen", que significa "números" en alemán.)

Se parte de las siguientes reglas simples de suma y multiplicación de estos números (donde a, b, c son enteros arbitrarios):

a) Ley asociativa de la multiplicación y la adición:

$$(a + b) + c = a + (b + c) \quad \text{y} \quad (ab)c = a(bc)$$

b) Ley conmutativa de la multiplicación y la adición:

$$a + b = b + a \quad \text{y} \quad ab = ba$$

c) Ley distributiva:

$$a(b + c) = ab + ac$$

d) Identidad aditiva 0 e identidad multiplicativa 1:

$$a + 0 = 0 + a = a \quad \text{y} \quad a \cdot 1 = 1 \cdot a = a$$

e) Inverso aditivo $-a$ para cualquier entero a:

$$a + (-a) = (-a) + a = 0$$

En el apéndice B se muestra que otras estructuras matemáticas poseen las propiedades anteriores. Una propiedad fundamental que distingue a los enteros **Z** de otras estructuras es el principio de inducción matemática (sección 1.8) que vuelve a analizarse aquí. También se plantea y demuestra (problema 11.30) el siguiente teorema.

Teorema fundamental de la aritmética: La única forma de escribir cualquier entero positivo $n > 1$ es como un producto de números primos.

Este teorema ya aparece en los *Elementos* de Euclides. Aquí también se desarrollan los conceptos y métodos que se usan para demostrar este importante teorema.

11.2 ORDEN Y DESIGUALDADES, VALOR ABSOLUTO

En esta sección se estudian las propiedades elementales de orden y valor absoluto.

Orden

Observe que en **Z** el orden se define en términos de los enteros positivos **N**. Todas las propiedades usuales de esta relación de orden son una consecuencia de las dos siguientes propiedades de **N**:

[$\mathbf{P_1}$] Si a y b pertenecen a **N**, entonces $a + b$ y ab pertenecen a **N**.

[$\mathbf{P_2}$] Para cualquier entero a, ningún $a \in \mathbf{N}$, $a = 0$ o $-a \in \mathbf{N}$.

También se usa la siguiente notación:

$a > b$ significa $b < a$;	se lee a es mayor que b.
$a \leq b$ significa $a < b$ o $a = b$;	se lee a es menor o igual que b.
$a \geq b$ significa $a > b$ o $a = b$;	se lee a es mayor o igual que b.

Las relaciones $<$, $>$, $\leq$ y $\geq$ se denominan *desigualdades* a fin de distinguirlas de la relación $=$ de igualdad. El lector ya está familiarizado con la representación de los enteros como puntos sobre una línea recta, que se denomina *recta numérica* **R**, como se muestra en la figura 11-1.

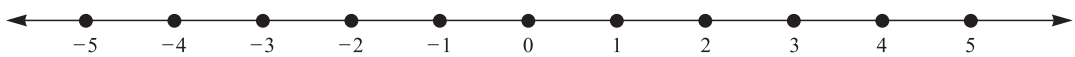


Figura 11-1

Se observa que $a < b$ si y sólo si a está a la izquierda de b en la recta numérica **R** en la figura 11-1. Por ejemplo,

$$2 < 5; \qquad -6 < -3; \qquad 4 \leq 4; \qquad 5 > -8; \qquad 6 \geq 0; \qquad -7 \leq 0$$

También se observa que a es positivo ssi $a > 0$ y a es negativo si y sólo si $a < 0$. (Recuerde que "ssi" significa "si y sólo si".) A continuación se presentan algunas propiedades básicas de las relaciones de desigualdad:

Proposición 11.1: La relación $\geq$ en **Z** tiene las siguientes propiedades:

i) $a \leq a$ para cualquier entero a.
ii) Si $a \leq b$ y $b \leq a$, entonces $a = b$.
iii) Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Proposición 11.2 (Ley de tricotomía): Para enteros a y b cualesquiera, se cumple sólo una de las siguientes relaciones:

$$a < b, \quad a = b \quad \text{o} \quad a > b$$

Proposición 11.3: Suponga $a \leq b$ y sea c cualquier entero. Entonces:

i) $a + c \leq b + c$.
ii) $ac \leq bc$ cuando $c > 0$; pero $ac \geq bc$ cuando $c < 0$.

(En el problema 11.5 se demuestra la proposición 11.3.)

Valor absoluto

El *valor absoluto* de un entero a, que se escribe $|a|$, se define formalmente como

$$|a| = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases}$$

En consecuencia, $|a| > 0$, excepto cuando $a = 0$. En términos geométricos, $|a|$ puede considerarse como la distancia entre los puntos a y 0 en la recta numérica $\mathbf{R}$. También, $|a - b| = |b - a|$ puede considerarse como la distancia entre los puntos a y b. Por ejemplo:

$$a)\ |-3| = 3; \quad |7| = 7; \quad |-13| = 13; \qquad b)\ |2 - 7| = |-5| = 5; \quad |7 - 2| = |5| = 5$$

A continuación se presentan algunas propiedades de la función valor absoluto. [En los problemas 11.6 y 11.7 se demuestran los incisos *iii*) y *iv*).]

Proposición 11.4: Sean a y b enteros cualesquiera. Entonces:

i)	$\|a\| \geq 0$, y $\|a\| = 0$ ssi $a = 0$	*iv*)	$\|a \pm b\| \leq \|a\| + \|b\|$
ii)	$-\|a\| \leq a \leq \|a\|$	*v*)	$\|\|a\| - \|b\|\| \leq \|a \pm b\|$
iii)	$\|ab\| = \|a\|\|b\|$		

11.3 INDUCCIÓN MATEMÁTICA

El principio de inducción matemática, que se plantea a continuación, establece que los enteros positivos $\mathbf{N}$ empiezan con el número 1 y que los siguientes se obtienen al sumar 1 sucesivamente. Es decir, se empieza con 1, luego $2 = 1 + 1$, luego $3 = 2 + 1$, luego $4 = 3 + 1$ y así se continúa. El principio hace precisa la vaga expresión "y así sucesivamente".

Principio de inducción matemática: Sea S un conjunto de enteros positivos con las dos propiedades siguientes:

i) 1 pertenece a S.

ii) Si k pertenece a S, entonces $k + 1$ pertenece a S.

En consecuencia, S es el conjunto de todos los enteros positivos.

No se demostrará este principio. Por el contrario, cuando el conjunto $\mathbf{N}$ de los enteros positivos (números naturales) se desarrolla axiomáticamente, este principio se proporciona como uno de los axiomas.

Hay una forma equivalente del principio enunciado que suele usarse al demostrar teoremas:

Principio de inducción matemática: Sea P una proposición definida sobre los enteros $n \geq 1$ tal que:

i) $P(1)$ es verdadera.

ii) $P(k + 1)$ es verdadera siempre que $P(k)$ es verdadera.

Entonces P es verdadera para todo entero $k \geq 1$.

EJEMPLO 11.1

a) Sea P la proposición de que la suma de los n primeros números impares es n^2; es decir:

$$P(n)\text{: } 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(El n-ésimo número impar es $2n - 1$ y el siguiente número impar es $2n + 1$.)

Resulta evidente que $P(n)$ es verdadera para $n = 1$; es decir:

$$P(1)\text{: } 1 = 1^2$$

Suponga que $P(k)$ es verdadera. (Ésta es la hipótesis de inducción.) Al sumar $2k + 1$ a ambos miembros de $P(k)$ se obtiene

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1)$$
$$= (2k + 1)^2$$

que es $P(k + 1)$. Se demuestra que $P(k + 1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción matemática, P es verdadera para todos los enteros positivos n.

b) El símbolo $n!$ (que se lee n factorial) se define como el producto de los n primeros enteros positivos; es decir:

$$1! = 1, \quad 2! = 2 \cdot 1 = 2, \quad 3! = 3 \cdot 2 \cdot 1 = 6, \qquad \text{y así en lo sucesivo.}$$

La definición formal es:

$$1! = 1 \quad \text{y} \quad (n + 1)! = (n + 1)(n!), \quad \text{para } n > 1$$

Observe que si S es el conjunto de enteros positivos para los que está definido !, entonces S satisface las dos propiedades de la inducción matemática. Por consiguiente, la definición anterior define ! para todo entero positivo.

Hay otra forma del principio de inducción matemática (que se demuestra en el problema 11.13) que algunas veces es más conveniente de usar. A saber:

Teorema 11.5 (Inducción: segunda forma): Sea P una proposición definida sobre los enteros $n \geq 1$ tal que:

i) $P(1)$ es verdadera.

ii) $P(k)$ es verdadera siempre que $P(j)$ es verdadera para todo $1 \leq j < k$.

Entonces P es verdadera para cualquier entero $n \geq 1$.

Observación: El teorema anterior es verdadero si se sustituye 1 por 0 o por cualquier otro entero a.

Principio del buen orden

Una propiedad de los enteros positivos equivalente al principio de inducción, aunque en apariencia es muy distinta, es el principio del buen orden (que se demuestra en el problema 11.12). A saber:

Teorema 11.6 (Principio del buen orden): Sea S un conjunto no vacío de enteros positivos. Entonces S contiene un *elemento mínimo*; es decir, S contiene un elemento a tal que $a \leq s$ para todo s en S.

En términos generales, se dice que un conjunto ordenado S está *bien ordenado* si cualquier subconjunto de S contiene un primer elemento. Así, el teorema 11.6 establece que **N** está bien ordenado.

Se dice que un conjunto S de enteros está *acotado por abajo* si todo elemento de S es mayor que algún entero m (que puede ser negativo). (El número m se denomina *cota inferior* de S.) A continuación se presenta un simple corolario del teorema anterior:

Corolario 11.7: Sea S un conjunto no vacío de enteros acotado por abajo. Entonces S contiene un elemento mínimo.

11.4 ALGORITMO DE LA DIVISIÓN

La siguiente propiedad fundamental de la aritmética (que se demuestra en los problemas 11.17 y 11.18) es un replanteamiento del resultado de la división larga.

Teorema 11.8 (Algoritmo de la división): Sean a y b enteros con $b \neq 0$. Entonces existen enteros q y r tales que

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|$$

También los enteros q y r son únicos.

El número q en el teorema precedente se denomina *cociente* y r se denomina *residuo*. Se recalca el hecho de que r debe ser no negativo. El teorema también establece que

$$r = a - bq$$

Esta ecuación se usará más adelante.

Si a y b son positivos, entonces q es no negativo. Si b es positivo, entonces la figura 11-2 proporciona una interpretación geométrica de este teorema. Es decir, los múltiplos positivos y negativos de b se distribuyen de modo uniforme a lo largo de la recta numérica **R**, y a se encuentra entre algunos múltiplos qb y $(q + 1)b$. Entonces, la distancia entre qb y a es el residuo r.

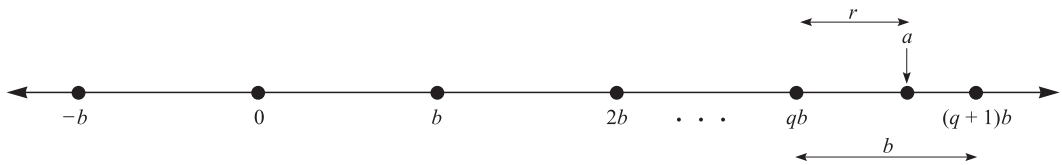


Figura 11-2

Algoritmo de la división con calculadora

Suponga que a y b son positivos. Entonces el cociente q y el residuo r pueden encontrarse con una calculadora:

Paso 1. Dividir a entre b, usando una calculadora; es decir, encontrar a/b.

Paso 2. Sea q la parte entera de a/b, es decir, sea $q = INT(a/b)$.

Paso 3. Sea r la diferencia entre a y bq; es decir, sea $r = a - bq$.

EJEMPLO 11.2

a) Sean $a = 4\,461$ y $b = 16$. El cociente $q = 278$ y el residuo $r = 13$ pueden encontrarse mediante la división larga. En forma alterna, con una calculadora, q y r se obtienen como sigue:

$$a/b = 278.8125\ldots, \quad q = 278, \quad r = 4\,461 - 16(278) = 13$$

Como era de esperar, $a = bq + r$; a saber,

$$4\,461 = 16(278) + 13$$

b) Sean $a = -262$ y $b = 3$. Primero se divide $|a| = 262$ entre $b = 3$. Esto produce el cociente $q' = 87$ y un residuo $r' = 1$. Por tanto,

$$262 = 3(87) + 1$$

Se requiere $a = -262$, de modo que se multiplica por -1 para obtener

$$-262 = 3(-87) - 1$$

Sin embargo, -1 es negativo y por tanto no puede ser r. Este hecho se corrige al sumar y restar el valor de b (que es 3) como sigue:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

En consecuencia, $q = -88$ y $r = 2$.

c) Sea $b = 2$. Entonces cualquier entero a puede expresarse en la forma

$$a = 2q + r \quad \text{donde} \quad 0 \leq r < 2$$

Así, r sólo puede ser 0 o 1. Por tanto, todo entero es de la forma $2k$ o $2k + 1$. Los enteros de la forma $2k$ se denominan enteros *pares*, mientras que los de la forma $2k + 1$ se denominan enteros *impares*. (Lo usual es definir un entero par como un entero divisible entre 2 y cualquier otro entero es impar. Así, el algoritmo de la división demuestra que todo entero impar tiene la forma $2k + 1$.)

11.5 DIVISIBILIDAD, PRIMOS

Sean a y b enteros con $a \neq 0$. Suponga $ac = b$ para algún entero c. Entonces se dice que a divide a b o que b es divisible entre a, y este hecho se denota como

$$a|b$$

También se dice que b es un múltiplo de a o que a es un *factor* o un *divisor* de b. Si a no divide a b se escribe $a \nmid b$.

EJEMPLO 11.3

a) Resulta evidente que $3|6$ puesto que $3 \cdot 2 = 6$ y $-4|28$ puesto que $(-4)(-7) = 28$.

b) Los divisores de 4 son ± 1, ± 2, ± 4 y los divisores de 9 son ± 1, ± 3, ± 9.

c) Si $a \neq 0$, entonces $a|0$ puesto que $a \cdot 0 = 0$.

d) Todo entero a es divisible entre ± 1 y $\pm a$. Éstos a menudo se denominan *divisores triviales* de a. Las propiedades básicas de la divisibilidad se plantean en el siguiente teorema (que se demuestra en el problema 11.24).

Teorema 11.9: Suponga que a, b, c son enteros.

i) Si $a|b$ y $b|c$, entonces $a|c$.

ii) Si $a|b$ entonces, para cualquier entero x, $a|bx$.

iii) Si $a|b$ y $a|c$, entonces $a|(b + c)$ y $a|(b - c)$.

iv) Si $a|b$ y $b \neq 0$, entonces $a = \pm b$ o $|a| < |b|$.

v) Si $a|b$ y $b|a$, entonces $|a| = |b|$, es decir, $a = \pm b$.

vi) Si $a|1$, entonces $a = \pm 1$.

Al escribir *i*) y *ii*) juntos se obtiene el siguiente resultado importante.

Corolario 11.10: Suponga $a|b$ y $a|c$. Entonces, para cualesquiera enteros x y y, $a|(bx + cy)$. La expresión $bx + cy$ se denomina *combinación lineal* de b y c.

Primos

Un entero positivo $p > 1$ es un *número primo* o *primo* si sólo sus divisores son ± 1 y $\pm p$, si p sólo tiene divisores triviales. Si $n > 1$ no es primo, entonces n es *compuesto*. Observe que (problema 11.13) si $n > 1$ es compuesto entonces $n = ab$ donde $1 < a, b < n$.

EJEMPLO 11.4

a) Los enteros 2 y 7 son primos, mientras que $6 = 2 \cdot 3$ y $15 = 3 \cdot 5$ son compuestos.

b) Los primos menores que 50 son:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \quad 41, \quad 43, \quad 47$$

c) Aunque 21, 24 y 1 729 no son primos, cada uno puede escribirse como un producto de primos:

$$21 = 3 \cdot 7; \qquad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3; \qquad 1\,729 = 7 \cdot 13 \cdot 19$$

El teorema fundamental de la aritmética establece que todo entero $n > 1$ puede escribirse como un producto de primos esencialmente de una forma: se trata de un teorema profundo y algo difícil de demostrar. Sin embargo, mediante inducción, en este momento resulta fácil demostrar que tal producto existe. A saber:

Teorema 11.11: Cualquier entero $n > 1$ puede escribirse como un producto de primos.

Observe que un producto puede consistir de un solo factor, de modo que un primo p es en sí un producto de primos. A continuación se demuestra el teorema 11.11, ya que su demostración es relativamente sencilla.

Demostración: La demostración es por inducción. Sea $n = 2$. Puesto que 2 es primo, n es un producto de primos. Suponga que $n > 2$ y el teorema se cumple para enteros positivos menores que n. Si n es primo, entonces n es un producto de primos. Si n es compuesto, entonces $n = ab$, donde $a, b < n$. Por inducción, a y b son productos de primos; por tanto, $n = ab$ también es un producto de primos.

Euclides, quien demostró el teorema fundamental de la aritmética, también se preguntó si había o no un primo máximo. Contestó esta pregunta así:

Teorema 11.12: No hay primo máximo; es decir, existe una infinidad de primos.

Demostración: Suponga que hay un número finito de primos, por ejemplo, $p_1, p_2, \ldots, p_m$. Considere el entero

$$n = p_1 p_2 \cdots p_m + 1$$

Puesto que n es un producto de primos (teorema 11.11) es divisible entre uno de los primos; por ejemplo, p_k. Observe que p_k también divide al producto $p_1 p_2 \ldots p_m$. En consecuencia, p_k divide a

$$n - p_1 p_2 \ldots p_m = 1$$

Esto es imposible, y así n es divisible por algún otro primo. Esto contradice la hipótesis de que $p_1, p_2, \ldots, p_m$ son sólo primos. Por tanto, el número de primos es infinito y esto demuestra el teorema.

11.6 MÁXIMO COMÚN DIVISOR, ALGORITMO EUCLIDIANO

Suponga que a y b son enteros, no ambos cero. Un entero d es un *divisor común* de a y b si d divide tanto a a como a b; es decir, si $d|a$ y $d|b$. Observe que 1 es un divisor común positivo de a y b, y que cualquier divisor común de a y b no puede ser mayor que $|a|$ o $|b|$. Por tanto, existe un común divisor máximo de a y b; se denota por

$$\text{mcd}(a, b)$$

y se denomina *máximo común divisor* de a y b.

EJEMPLO 11.5

a) Los divisores comunes de 12 y 18 son $\pm 1, \pm 2, \pm 3, \pm 6$. Por tanto, $\text{mcd}(12, 18) = 6$; en forma semejante:

$$\text{mcd}(12, -18) = 16, \qquad \text{mcd}(12, -16) = 4, \qquad \text{mcd}(29, 15) = 1, \qquad \text{mcd}(14, 49) = 7$$

b) Para cualquier entero a, se tiene $\text{mcd}(1, a) = 1$.

c) Para cualquier primo p, se tiene $\text{mcd}(p, a) = p$ o $\text{mcd}(p, a) = 1$ según sea el caso si p divide o no a a.

d) Suponga que a es positivo. Entonces $a|b$ si y sólo si $\text{mcd}(a, b) = a$.

El siguiente teorema (que se demuestra en el problema 11.26) proporciona una caracterización alterna del máximo común divisor.

Teorema 11.13: Sea d el menor entero positivo de la forma $ax + by$. Entonces

$$d = \text{mcd}(a, b).$$

Corolario 11.14: Suponga $d = \text{mcd}(a, b)$. Entonces existen enteros x y y tales que $d = ax + by$.

Otra forma de caracterizar el máximo común divisor, sin usar la relación de desigualdad es la siguiente:

Teorema 11.15: Un entero positivo $d = \text{mcd}(a, b)$ si y sólo si d tiene las siguientes propiedades:

1) d divide tanto a a como a b.
2) Si c divide tanto a a como a b, entonces $c|d$.

A continuación se presentan algunas propiedades simples del máximo común divisor:

a) $\text{mcd}(a, b) = \text{mcd}(b, a)$.
b) Si $x > 0$, entonces $\text{mcd}(ax, bx) = x \cdot \text{mcd}(a, b)$.
c) Si $d = \text{mcd}(a, b)$, entonces $\text{mcd}(a/d, b/d) = 1$.
d) Para cualquier entero x, $\text{mcd}(a, b) = \text{mcd}(a, b + ax)$.

Algoritmo euclidiano

Sean a y b enteros y $d = \text{mcd}(a, b)$. d se encuentra siempre al enumerar todos los divisores de a y luego todos los divisores de b y entonces se escoge al máximo común divisor. La complejidad de un algoritmo así es $f(n) = 0(\sqrt{n})$, donde $n = |a| + |b|$. Asimismo, no se ha proporcionado ningún método para encontrar los enteros x y y tales que $d = ax + by$.

Esta subsección da un algoritmo muy eficiente, el algoritmo euclidiano, con una complejidad $f(n) = O(\log n)$, para encontrar $d = \text{mcd}(a, b)$ al aplicar el algoritmo de división a a y b a cada cociente y residuo hasta obtener el residuo diferente a cero. El último residuo diferente de cero es $d = \text{mcd}(a, b)$.

Entonces, se tiene un algoritmo para "desenredar", que regresa por los pasos del algoritmo euclidiano para encontrar los enteros x y y tales que $d = xa + yb$.

El algoritmo se ilustra con un ejemplo.

EJEMPLO 11.6 Sean $a = 540$ y $b = 168$. Se aplica el algoritmo euclidiano a a y b. Estos pasos, que en forma repetida aplican el algoritmo de la división a cada cociente y residuo hasta que se obtiene un residuo cero, se representan en la figura 11-3*a*) mediante la división larga y también en la figura 11-3*b*), donde las flechas indican el cociente y el residuo en el paso siguiente. El último residuo diferente de cero es 12. Así,

$$12 = \text{mcd}(540, 168)$$

Esto se concluye por el hecho de que

$$\text{mcd}(540, 168) = \text{mcd}(168, 36) = \text{mcd}(36, 24) = \text{mcd}(24, 12) = 12$$

Luego se encuentran x y y tales que $12 = 540x + 168y$ al "desenredar" los pasos anteriores en el algoritmo euclidiano. Con más precisión, los tres primeros cocientes en la figura 11-3 producen las siguientes ecuaciones:

$$1)\ 36 = 540 - 3(168), \qquad 2)\ 24 = 168 - 4(36), \qquad 3)\ 12 = 36 - 1(24)$$

La ecuación 3) establece que $d = \text{mcd}(a, b) = 12$ es una combinación lineal de 36 y 24. Ahora se usan las ecuaciones precedentes en orden inverso para eliminar los otros residuos. Es decir, primero se usa la ecuación 2) para sustituir 24 en la ecuación 3) para poder escribir 12 como una combinación lineal de 168 y 36:

$$4)\ 12 = 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) = 5(36) - 1(168)$$

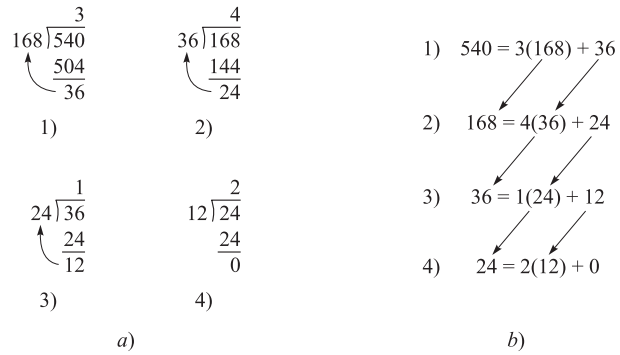


Figura 11-3

Luego se usa la ecuación 1) para sustituir 36 en 4) para poder escribir 12 como una combinación lineal de 168 y 540 como sigue:

$$12 = 5[540 - 3(168)] - 1(168) = 5(54) - 15(168) - 1(168) = 5(540) - 16(168)$$

Ésta es la combinación lineal buscada. En otras palabras, $x = 5$ y $y = -16$.

Mínimo común múltiplo

Suponga que a y b son enteros distintos de cero. Observe que $|ab|$ es un múltiplo común positivo de a y b. Por tanto, existe un múltiplo común positivo mínimo de a y b; se denota por

$$\text{mcm}(a, b)$$

y se denomina *mínimo común múltiplo* de a y b.

EJEMPLO 11.7

a) $\text{mcm}(2, 3) = 6$; $\text{mcm}(4, 6) = 12$; $\text{mcm}(9, 10) = 90$.

b) Para cualquier entero positivo a se tiene $\text{mcm}(1, a) = a$.

c) Para cualquier primo p y cualquier entero positivo a,

$$\text{mcm}(p, a) = a \quad \text{o} \quad \text{mcm}(p, a) = ap$$

según sea el caso si p divide o no a a.

d) Suponga que a y b son enteros positivos. Entonces $a \mid b$ si y sólo si $\text{mcm}(a, b) = b$.

El siguiente teorema proporciona una relación importante entre el máximo común divisor y el mínimo común múltiplo.

Teorema 11.16: Suponga que a y b son enteros diferentes de cero. Entonces

$$\text{mcm}(a, b) = \frac{|ab|}{\text{mcd}(a, b)}$$

11.7 TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

En esta sección se analiza el teorema fundamental de la aritmética. Primero se definen los enteros primos relativos.

Enteros primos relativos

Dos enteros a y b son primos relativos o *coprimos* si $\text{mcd}(a, b) = 1$. En consecuencia, si a y b son primos relativos, entonces existen enteros x y y tales que

$$ax + by = 1$$

A la inversa, si $ax + by = 1$, entonces a y b son primos relativos.

EJEMPLO 11.8

a) Observe que: $\text{mcd}(12, 35) = 1$, $\text{mcd}(49, 18) = 1$, $\text{mcd}(21, 64) = 1$, $\text{mcd}(-28, 45) = 1$

b) Si p y q son primos distintos, entonces $\text{mcd}(p, q) = 1$.

c) Para cualquier entero a, se tiene $\text{mcd}(a, a + 1) = 1$, puesto que cualquier factor común de a y $a + 1$ debe dividir a su diferencia $(a + 1) - a = 1$.

La relación de ser primos relativos es de particular importancia debido a los resultados siguientes. El primer teorema se demuestra en el problema 11.27 y el segundo teorema se demostrará aquí.

Teorema 11.17: Suponga $\text{mcd}(a, b) = 1$ y que tanto a como b dividen a c. Entonces ab divide a c.

Teorema 11.18: Suponga $a|bc$ y $\text{mcd}(a, b) = 1$. Entonces $a|c$.

Demostración: Puesto que $\text{mcd}(a, b) = 1$, existen x y y tales que $ax + by = 1$. Al multiplicar ambos miembros por c se obtiene:

$$acx + bcy = c$$

Se tiene $a|acx$. También, $a|bcy$, puesto que, por hipótesis, $a|bc$. Por tanto, a divide a la suma $acx + bcy = c$.

Corolario 11.19: Suponga que a, un primo p divide al producto ab. Entonces $p|a$ o $p|b$.

Este corolario (que se demuestra en el problema 11.28) se remonta a Euclides; constituye la base de su demostración del teorema fundamental de la aritmética.

Teorema fundamental de la aritmética

El teorema 11.11 establece que todo entero positivo es un producto de primos. ¿Es posible que diferentes productos de primos produzcan el mismo número? Resulta evidente que es posible reagrupar el orden de los factores primos, por ejemplo,

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

El teorema fundamental de la aritmética (que se demuestra en el problema 11.30) establece que la siguiente es la única forma en que dos productos "diferentes" pueden proporcionar el mismo número. A saber,

Teorema 11.20 (Teorema fundamental de la aritmética): Cualquier entero $n > 1$ puede expresarse en forma única (salvo por el orden) como un producto de primos.

Los primos en la factorización de n no necesitan ser distintos. A menudo es de utilidad reunir juntos a todos los primos iguales. Entonces, n puede expresarse en forma única como

$$n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$$

donde los m_i son positivos y $p_1 < p_2 < \dots < p_r$. Esto se denomina *factorización canónica* de n.

EJEMPLO 11.9 Dados $a = 2^4 \cdot 3^3 \cdot 7 \cdot 13$ y $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Encontrar $d = \text{mcd}(a, b)$ y $m = \text{mcm}(a, b)$.

a) Primero se encuentra $d = \text{mcd}(a, b)$. Los primos p que aparecen tanto en a como en b, 2, 3 y 11, también aparecen en d, y el exponente de p en d será el menor de sus exponentes en a y b. Así,

$$d = \text{mcd}(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

b) Luego se encuentra $m = \text{mcm}(a, b)$. Los primos p que aparecen ya sea en a o en b, 2, 3, 5, 7, 11, 13 y 17, también aparecen en m, y el exponente de p en m será el mayor de sus exponentes en a y b. Así,

$$m = \text{mcm}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

Ya es tan arraigada la costumbre de usar números, como si el teorema fundamental de la aritmética fuese verdadero, que parece innecesario demostrarlo. Es un tributo a Euclides, el primero que demostró el teorema y quien reconoció que es necesario demostrarlo. Se recalca la no trivialidad del teorema con un ejemplo de un sistema de números que no satisface este teorema.

EJEMPLO 11.10 Sea F el conjunto de enteros positivos de la forma $3x + 1$. Así, F consta de los números:

$$1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22, \ldots$$

Observe que el producto de dos números en F de nuevo está en F, puesto que:

$$(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

La definición de primos tiene perfecto sentido en F. Aunque $4 = 2 \cdot 2$, el número 2 no está en F. Por tanto, 4 es primo en F puesto que 4 no tiene factores, excepto 1 y 4. En forma semejante 10, 22, 25, ..., son primos en F. A continuación se enumeran los primeros primos en F:

$$4,\ 7,\ 10,\ 13,\ 19,\ 22,\ 25, \ldots$$

Observe que $100 = 3(33) + 1$ pertenece a F. Sin embargo, 100 tiene esencialmente dos factorizaciones diferentes en primos en F; a saber,

$$100 = 4 \cdot 25 \quad \text{y} \quad 100 = 10 \cdot 10$$

Por tanto, no existe factorización única en primos en F.

11.8 RELACIÓN DE CONGRUENCIA

Sea m un entero positivo. Se dice que a es *congruente* con b *módulo* m, lo que se escribe

$$a \equiv b \ (\text{módulo } m) \qquad \text{o simplemente} \qquad a \equiv b \ (\text{mód } m)$$

si m divide a la diferencia $a - b$. El entero m se denomina *módulo*. La negación de $a \equiv b$ (mód m) se escribe $a \not\equiv b$ (mód m). Por ejemplo:

i) $87 \equiv 23$ (mód 4) puesto que 4 divide a $87 - 23 = 64$.

ii) $67 \equiv 1$ (mód 6) puesto que 6 divide a $67 - 1 = 66$.

iii) $72 \equiv -5$ (mód 7) puesto que 7 divide a $72 - (-5) = 77$.

iv) $27 \not\equiv 8$ (mód 9) puesto que 9 no divide a $27 - 8 = 19$.

El primer teorema (que se demuestra en el problema 11.34) establece que la relación de congruencia módulo m es una relación de equivalencia.

Teorema 11.21: Sea m un entero positivo. Entonces:

i) Para cualquier entero a se tiene $a \equiv a$ (mód m).

ii) Si $a \equiv b$ (mód m), entonces $b \equiv a$ (mód m).

iii) Si $a \equiv b$ (mód m) y $b \equiv c$ (mód m), entonces $a \equiv c$ (mód m).

Observación: Suponga que m es positivo y que a es cualquier entero. Por el algoritmo de la división, existen enteros q y r con $0 = r \leq m$ tal que $a = mq + r$. Por tanto,

$$mq = a - r \quad \text{o} \quad m|(a - r) \quad \text{o} \quad a \equiv r \ (\text{mód } m)$$

En consecuencia:

1) Cualquier entero a es congruente con módulo m con un entero único en el conjunto

$$\{0, 1, 2, \ldots, m - 1\}$$

La unicidad proviene del hecho de que m no puede dividir a la diferencia de dos enteros así.

2) Dos enteros cualesquiera a y b son congruentes con módulo m si y sólo si tienen el mismo residuo cuando se dividen entre m.

Clases de residuos

Puesto que la congruencia módulo m es una relación de equivalencia, separa el conjunto $\mathbf{Z}$ de los enteros en clases de equivalencia ajenas que se denominan *clases de residuos módulo m*. Por las observaciones anteriores, una clase de residuos consta de todos los enteros con el mismo residuo cuando se dividen entre m. En consecuencia, hay m de estas clases de residuos y cada clase de residuos contiene exactamente uno de los enteros en el conjunto de residuos posibles; es decir,

$$\{0, 1, 2, \ldots, m - 1\}$$

En términos generales, se dice que un conjunto de m enteros $\{a_1, a_2, \ldots, a_m\}$ es un *sistema de residuos completo módulo m* si cada a_i proviene de una clase de residuos distinta. (En tal caso, cada a_i se denomina *representante* de su clase de equivalencia.)

Por tanto, los enteros desde 0 hasta $m - 1$ constituyen un sistema de residuos completo. De hecho, cualesquiera m enteros consecutivos forman un sistema de residuos completo módulo m.

La notación $[x]_m$, o simplemente $[x]$ se usa para indicar la clase de residuos (módulo m) que contiene a un entero x; es decir, los enteros que son congruentes con x. En términos matemáticos,

$$[x] = \{a \in \mathbf{Z} \mid a \equiv x \ (\text{mód } m)\}$$

En consecuencia, las clases de residuos pueden denotarse por

$$[0], [1], [2], \ldots, [m - 1]$$

o con cualquier otra elección de enteros en un sistema de residuos completo.

EJEMPLO 11.11 Las clases de residuos módulo 6 son las siguientes:

$$[0] = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}, \quad |3| = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}$$
$$[1] = \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\}, \quad |4| = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}$$
$$[2] = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}, \quad |5| = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\}$$

Observe que $\{-2, -1, 0, 1, 2, 3\}$ es también un sistema de residuos completo módulo $m = 6$, y estos representantes tienen valores absolutos mínimos.

Aritmética de congruencia

El siguiente teorema (que se demuestra en el problema 11.35) establece que, bajo la suma y la multiplicación, la relación de congruencia se comporta en forma muy semejante a la relación de igualdad. A saber:

Teorema 11.22: Suponga $a \equiv c \ (\text{mód } m)$ y $b \equiv d \ (\text{mód } m)$. Entonces:

$$i)\ a + b \equiv c + d \ (\text{mód } m); \quad ii)\ a \cdot b \equiv c \cdot d \ (\text{mód } m)$$

Observación: Suponga que $p(x)$ es un polinomio con coeficientes enteros. Si $s \equiv t \ (\text{mód } m)$, entonces al usar repetidas veces el teorema 11.22 puede demostrarse que $p(s) \equiv p(t) (\text{mód } m)$.

EJEMPLO 11.12 Observe que $2 \equiv 8 (\text{mód } 6)$ y $5 \equiv 41 (\text{mód } 6)$. Entonces:

a) $2 + 5 \equiv 8 + 41 \ (\text{mód } 6)$ o $7 \equiv 49 \ (\text{mód } 6)$

b) $2 \cdot 5 \equiv 8 \cdot 41 \ (\text{mód } 6)$ o $10 \equiv 328 \ (\text{mód } 6)$

c) Suponga $p(x) = 3x^2 - 7x + 5$. Entonces

$$p(2) = 12 - 14 + 5 = 3 \qquad \text{y} \qquad p(8) = 192 - 56 + 5 = 141$$

Por tanto, $3 \equiv 141 (\text{mód } 6)$.

Aritmética de clases de residuos

La suma y la multiplicación para las clases de residuos módulo m se definen como:

$$[a] + [b] = [a + b] \qquad \text{y} \qquad [a] \cdot [b] = [ab]$$

Por ejemplo, considere las clases de residuos módulo $m = 6$; es decir,

$$[0], [1], [2], [3], [4], [5]$$

Entonces

$$[2] + [3] = [5], \quad [4] + [5] = [9] = [3], \quad [2]\cdot[2] = [4], \quad [2]\cdot[5] = [10] = [4]$$

El contenido del teorema 11.22 establece que las definiciones anteriores están bien definidas; es decir, que la suma y el producto de las clases de residuos no dependen de la elección del representante de la clase de residuos.

Sólo hay un número finito m de clases de residuos módulo m. Así, cuando m es pequeño es fácil escribir explícitamente sus tablas de suma y multiplicación. En la figura 11-4 se muestran las tablas de suma y multiplicación para las clases de residuos módulo $m = 6$. Por conveniencia en la notación se omitieron los corchetes y las clases de residuos se denotan simplemente por los números 0, 1, 2, 3, 4, 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Figura 11-4

Enteros módulo *m*, $\mathbf{Z_m}$

Los *enteros módulo m*, que se denotan $\mathbf{Z_m}$, se refieren al conjunto

$$\mathbf{Z_m} = \{0, 1, 2, 3, \ldots, m - 1\}$$

donde la adición y la multiplicación se definen por la aritmética módulo m o, en otras palabras, las operaciones correspondientes para las clases de residuos. Por ejemplo, la figura 11-4 también puede considerarse como las tablas de la adición y la multiplicación para $\mathbf{Z_6}$. Esto significa:

> No hay diferencia esencial entre $\mathbf{Z_m}$ y la aritmética de las clases de residuos módulo m, de modo que se utilizan como sinónimos.

Leyes de cancelación para congruencias

Recuerde que los enteros satisfacen lo siguiente:

Ley de cancelación: si $ab = ac$ y $a \neq 0$, entonces $b = c$.

La diferencia fundamental entre la aritmética normal y la aritmética módulo m es que la ley de cancelación anterior no es verdadera para congruencias. Por ejemplo:

$$3 \cdot 1 \equiv 3 \cdot 5 \text{ (mód 6)} \quad \text{pero} \quad 1 \not\equiv 5 \text{ (mód 6)}$$

Es decir, no es posible cancelar 3 incluso si $1 \not\equiv 3$ (mód 6). No obstante, se cuenta con la siguiente *ley de cancelación modificada* para las relaciones de congruencia.

Teorema 11.23 (Ley de cancelación modificada): Suponga $ab \equiv ac$ (mód m) y mcd(a, m) = 1.

Entonces $b \equiv c$ (mód m).

El teorema precedente es una consecuencia del siguiente resultado más general (que se demuestra en el problema 11.37).

Teorema 11.24: Suponga $ab \equiv ac$ (mód m) y d = mcd(a, m). Entonces $b \equiv c$ (mód m/d).

EJEMPLO 11.13 Considere la siguiente congruencia:

$$6 \equiv 36 \text{ (mód 10)} \tag{11.1}$$

Puesto que mcd(3, 10) = 1 pero mcd(6, 10) $\neq$ 1, es posible dividir ambos miembros de (11.1) entre 3 pero no entre 6. Es decir,

$$2 \equiv 12 \text{ (mód 10)} \quad \text{pero} \quad 1 \not\equiv 6 \text{ (mód 10)}$$

Sin embargo, por el teorema 11.24, ambos miembros de (11.1) son divisibles entre 6 si el módulo también se divide entre 2, que es igual a mcd(6, 10). Es decir,

$$1 \equiv 6 \text{ (mód 5)}$$

Observación: Suponga que p es primo. Entonces los enteros desde 1 hasta $p - 1$ son primos relativos con p. Por tanto, la ley de cancelación de costumbre se cumple cuando el módulo es un primo p. Es decir:

Si $ab \equiv ac$(mód p) y $a \neq 0$ (mód p), entonces $b \equiv c$(mód p).

Por tanto, $\mathbf{Z_p}$, los enteros módulo un primo p, juegan un papel bastante especial en teoría de números.

Sistemas de residuos reducidos, función fi de Euler

La ley de cancelación modificada, teorema 11.23, indica el papel especial que juegan los enteros que son primos relativos (coprimos) con el módulo m. Se observa que a es coprimo de m si y sólo si cada elemento en la clase de residuos [a] es coprimo de m. Así, puede hablarse de una clase de residuos que es coprima de m.

El número de clases de residuos que son primos relativos con m o, en forma equivalente, el número de enteros entre 1 y m (inclusive) que son primos relativos de m se denotan con

$$\phi(m)$$

La función $\phi(m)$ se denomina *función fi de Euler*. La lista de números entre 1 y m que son coprimos de m o, de modo más general, cualquier lista de $\phi(m)$ enteros incongruentes que son coprimos de m, se denomina *sistema de residuos reducido módulo m*.

EJEMPLO 11.14

a) Considere el módulo $m = 15$. Hay ocho enteros entre 1 y 15 que son coprimos de 15:

$$1, \quad 2, \quad 4, \quad 7, \quad 8, \quad 11, \quad 13, \quad 14$$

Así, $\phi(15) = 8$ y los ocho enteros anteriores constituyen un sistema de residuos reducido módulo 15.

b) Considere cualquier primo p. Todos los números $1, 2, \ldots, p-1$ son coprimos de p; por tanto $\phi(p) = p - 1$.

Se dice que una función f cuyo dominio es el conjunto de enteros positivos $\boldsymbol{N}$ es *multiplicativa*, siempre que a y b sean primos relativos,

$$f(ab) = f(a)\, f(b)$$

El siguiente teorema (que se demuestra en el problema 11.44) es válido.

Teorema 11.25: La función fi de Euler es multiplicativa. Es decir, si a y b son primos relativos, entonces

$$\phi(ab) = \phi(a)\phi(b)$$

11.9 ECUACIONES DE CONGRUENCIA

Una *ecuación polinomial de congruencia* o, simplemente, una *ecuación de congruencia* (en una incógnita x) es una ecuación de la forma

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m} \tag{11.2}$$

Se dice que una ecuación así es de *grado n* si $a \not\equiv 0 \pmod{m}$.

Suponga $s \equiv t \pmod{m}$. Entonces s es una solución de (11.2) si y sólo si t es una solución de (11.2). Por tanto, el *número de soluciones* de (11.2) se define como el número de soluciones incongruentes o, en forma equivalente, el número de soluciones en el conjunto

$$\{0, 1, 2, \ldots, m-1\}$$

Por supuesto, estas soluciones siempre pueden encontrarse con el método de prueba; es decir, al sustituir cada uno de los m números en (11.2) para ver si, en efecto, satisface la ecuación.

El *conjunto completo de soluciones* de (11.2) es un conjunto máximo de soluciones incongruentes, mientras que la *solución general* de (11.2) es el conjunto de todas las soluciones enteras de (11.2). La solución general de (11.2) resulta al sumar todos los múltiplos del módulo m a cualquier conjunto completo de soluciones.

EJEMPLO 11.15 Considere las ecuaciones:

a) $x^2 + x + 1 \equiv 0 \pmod{4}$

b) $x^2 + 3 \equiv 0 \pmod{6}$

c) $x^2 - 1 \equiv 0 \pmod{8}$

Aquí, las soluciones se encontraron con el método de prueba.

a) No hay soluciones puesto que 0, 1, 2 y 3 no satisfacen la ecuación.

b) Sólo hay una solución entre 0, 1,…, 5, que es 3. Así, la solución general consta de los enteros $3 + 6k$, donde $k \in \mathbf{Z}$.

c) Hay cuatro soluciones: 1, 3, 5 y 7. Esto muestra que una ecuación de congruencia de grado n puede tener más de n soluciones.

Hay que señalar que el interés por estudiar ecuaciones de congruencia no sólo consiste en encontrar sus soluciones, ya que siempre se determinan mediante una comprobación. El interés esencial es el desarrollo de técnicas que ayuden a encontrar tales soluciones, así como una teoría que indique las condiciones en que existen las soluciones, así como el número de éstas. Una teoría así se cumple para ecuaciones de congruencia lineales que se investigan a continuación. También se analizará el teorema chino del residuo, que en esencia es un sistema de ecuaciones de congruencia lineales.

Observación 1: Los coeficientes de una ecuación de congruencia siempre pueden reducirse a módulo m, puesto que debe obtenerse una ecuación *equivalente*; es decir, una ecuación con las mismas soluciones. Por ejemplo, las siguientes ecuaciones son equivalentes porque los coeficientes son congruentes módulo $m = 6$:

$$15x^2 + 28x + 14 \equiv 0 \text{ (mód 6)}, \quad 3x^2 + 4x + 2 \equiv 0 \text{ (mód 6)}, \quad 3x^2 - 2x + 2 \equiv 0 \text{ (mód 6)}.$$

Por lo general, se escogen coeficientes entre 0 y $m - 1$ o entre $-m/2$ y $m/2$.

Observación 2: Puesto que en realidad se buscan las soluciones de (11.2) entre las clases de residuos módulo m, en lugar de hacerlo entre los enteros, (11.2) puede considerarse una ecuación sobre los enteros módulo m, más que una ecuación sobre $\mathbf{Z}$, los enteros. En este contexto, el número de soluciones de (11.2) es simplemente el número de soluciones en $\mathbf{Z_m}$.

Ecuación de congruencia lineal: $ax \equiv 1$ (mód m)

Primero se considera la ecuación de congruencia lineal especial

$$ax \equiv 1 \text{ (mód } m) \tag{11.3}$$

donde $a \not\equiv 0$ (mód m). La historia completa de esta ecuación se proporciona en el siguiente teorema (que se demuestra en el problema 11.57).

Teorema 11.26: Si a y m son primos relativos, entonces $ax \equiv 1$ (mód m) tiene una solución única; en otro caso, no tiene solución.

EJEMPLO 11.16

a) Considere la ecuación de congruencia $6x \equiv 1$ (mód 33). Puesto que mcd(6, 33) = 3, esta ecuación no tiene solución.

b) Considere la ecuación de congruencia $7x \equiv 1$ (mód 9). Puesto que mcd(7, 9) = 1, esta ecuación tiene solución única. Al probar los números 0, 1,…, 8 se encuentra que

$$7(4) = 28 \equiv 1 \text{ (mód 9)}$$

Así, $x = 4$ es la solución única. (La solución general es $4 + 9k$ para $k \in \mathbf{Z}$.)

Suponga que la solución de (11.3) existe; es decir, suponga que mcd(a, m) = 1. Además, que el módulo m es grande. Entonces es posible usar el algoritmo de Euclides para encontrar una solución de (11.3); en este caso se usa para encontrar x_0 y y_0 tales que

$$ax_0 + my_0 = 1$$

A partir de esto se concluye que $ax_0 \equiv 1$ (mód m); es decir, x_0 es una solución de (11.3).

EJEMPLO 11.17 Considere la siguiente ecuación de congruencia:

$$81 \equiv 1 \text{ (mód } 256)$$

Por observación o al aplicar el algoritmo de Euclides a 81 y a 256, se encuentra que mcd(81, 256) = 1. Por tanto, la ecuación tiene una solución única. Aplicar un método de prueba quizá no sea una forma eficiente para encontrar esta solución, ya que el módulo $m = 256$ es relativamente grande. Así, el algoritmo de Euclides se aplica a $a = 81$ y a $m = 256$. En este caso, como en el ejemplo 11.6, se encuentran $x_0 = -25$ y $y_0 = 7$ tales que

$$81x_0 + 256y_0 = 1$$

Esto significa que $x_0 = -25$ es una solución de la ecuación de congruencia dada. Al sumar $m = 256$ a -25 se obtiene la siguiente solución única entre 0 y 256:

$$x = 231$$

Ecuación lineal de congruencia: $ax \equiv b$ (mód m)

Ahora se considera la ecuación lineal de congruencia más general

$$ax \equiv b \text{ (mód } m) \tag{11.4}$$

donde $a \not\equiv 0$ (mód m). Primero se considera el caso (que se demuestra en el problema 11.58) en que a y m son coprimos.

Teorema 11.27: Suponga que a y m son primos relativos. Entonces $ax \equiv b$ (mód m) tiene solución única. Además, si s es la única solución de $ax \equiv 1$ (mód m), entonces la solución única de $ax \equiv b$ (mód m) es $x = bs$.

EJEMPLO 11.18

a) Considere la ecuación de congruencia $3x \equiv 5$ (mód 8). Puesto que 3 y 8 son coprimos, la ecuación tiene una solución única. Al probar los enteros 0, 1, . . . , 7 se encuentra que

$$3(7) = 21 \equiv 5 \text{ (mód } 8)$$

Por tanto, $x = 7$ es la única solución de la ecuación.

b) Considere la ecuación lineal de congruencia

$$33x \equiv 38 \text{ (mód } 280) \tag{11.5}$$

Puesto que mcd(33, 280) = 1, la ecuación tiene una solución única. Aplicar un método de prueba quizá no sea una forma eficiente para encontrar esta solución, ya que el módulo $m = 280$ es relativamente grande. Así, primero se aplica el algoritmo de Euclides para encontrar una solución de

$$33x \equiv 1 \text{ (mód } 280) \tag{11.6}$$

Es decir, como en el ejemplo 11.6, se encuentra que $x_0 = 17$ y $y_0 = 2$ son una solución de

$$33x_0 + 280y_0 = 1$$

Esto significa que $s = 17$ es una solución de (11.6). Así,

$$sb = 17(38) = 646$$

es una solución de (11.5). Al dividir 646 entre $m = 280$ se obtiene el residuo

$$x = 86$$

que es la única solución 11.5 entre 0 y 280. (La solución general es $86 + 280k$, con $k \in \mathbf{Z}$.)

La historia completa del caso general de (11.4) la contiene el siguiente teorema (que se demuestra en el problema 11.59).

Teorema 11.28: Considere la ecuación $ax \equiv b \pmod{m}$, donde $d = \text{mcd}(a, m)$.

i) Suponga que d no divide a b. Entonces $ax \equiv b \pmod{m}$ no tiene solución.

ii) Suponga que d divide a b. Entonces $ax \equiv b \pmod{m}$ tiene d soluciones, todas congruentes módulo M con la solución única de

$$Ax \equiv B \pmod{M} \quad \text{donde} \quad A = a/d, \quad B = b/d, M = m/d.$$

Se recalca que el teorema 11.27 es válido para la ecuación $Ax \equiv B \pmod{M}$ en el teorema 11.28, ya que $\text{mcd}(A, M) = 1$.

EJEMPLO 11.19 Resuelva cada ecuación de congruencia: *a*) $4x \equiv 9 \pmod{14}$; *b*) $8x \equiv 12 \pmod{28}$.

a) Observe que $\text{mcd}(4, 14) = 2$. Sin embargo, 2 no divide a 9. Por tanto, la ecuación no tiene solución.

b) Observe que $d = \text{mcd}(8, 28) = 4$ y $d = 4$ divide a 12. Por tanto, la ecuación tiene $d = 4$ soluciones. Al dividir cada término en la ecuación entre $d = 4$ se obtiene la ecuación de congruencia (11.7), que tiene una solución única.

$$2x \equiv 3 \pmod{7} \tag{11.7}$$

Al probar los enteros $0, 1, \ldots, 6$ se encuentra que 5 es la solución única de (11.7). Luego se suman $d - 1 = 3$ múltiplos de 7 a la solución 5 de (11.7) para obtener:

$$5 + 7 = 12, \quad 5 + 2(7) = 19, \quad 5 + 3(7) = 26$$

En consecuencia, 5, 12, 19, 26 son las $d = 4$ soluciones requeridas de la ecuación original $8x \equiv 12 \pmod{28}$.

Observación: La solución de la ecuación (11.7) en el ejemplo 11.19 se obtuvo por inspección. Sin embargo, en caso de que el módulo m sea grande, siempre es posible usar el algoritmo de Euclides para encontrar su solución única como en el ejemplo 11.17.

Teorema chino del residuo

Un antiguo acertijo chino plantea la siguiente cuestión.

> ¿Hay algún entero positivo x tal que cuando x se divide entre 3 se obtiene un residuo igual a 2, cuando x se divide entre 5 se obtiene un residuo igual a 4 y cuando x se divide entre 7 se obtiene un residuo igual a 6?

En otras palabras, se busca una solución común a las tres siguientes relaciones de congruencia:

$$x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 6 \pmod{7}$$

Observe que los módulos 3, 5 y 7 son primos relativos por pares. Por tanto, es válido el siguiente teorema (que se demuestra en el problema 11.60); establece que hay una solución única módulo $M = 3 \cdot 5 \cdot 7 = 105$.

Teorema 11.29 (Teorema chino del residuo): Considere el sistema

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \cdots, \quad x \equiv r_k \pmod{m_k} \tag{11.8}$$

donde los m_i son primos relativos por pares. Entonces el sistema tiene una solución única módulo $M = m_1 m_2 \cdots m_k$.

En realidad, el teorema 11.29 proporciona una fórmula explícita para la solución del sistema (11.8), que se plantea como proposición.

Proposición 11.30: Considere el sistema (11.8) de relaciones de congruencia. Sean $M = m_1 m_2 \dots m_k$, y

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \ \dots, \quad M_k = \frac{M}{m_k}$$

(Entonces, cada par M_i y m_i son coprimos.) Sea $s_1, s_2, \dots, s_k$ las soluciones, respectivamente, de las ecuaciones de congruencia

$$M_1 x \equiv 1 \ (\text{mód } m_1), \quad M_2 x \equiv 1 \ (\text{mód } m_2), \dots, \quad M_k x \equiv 1 \ (\text{mód } m_k)$$

Entonces, la siguiente es una solución del sistema (11.8):

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \tag{11.9}$$

Ahora es posible resolver el acertijo original de dos formas:

Método 1: Primero se aplica el teorema chino del residuo (TCR) a las dos primeras ecuaciones,

$$a)\ x \equiv 2 \ (\text{mód } 3) \quad \text{y} \quad b)\ x \equiv 4 \ (\text{mód } 5)$$

El TCR indica que hay una solución única módulo $M = 3 \cdot 5 = 15$. Al sumar múltiplos del módulo $m = 5$ a la solución dada $x = 4$ de la segunda ecuación b), se obtienen las tres soluciones siguientes de b) que son menores que 15:

$$4, \quad 9, \quad 14$$

Al probar cada una de estas soluciones en la ecuación a) se encuentra que la única solución de ambas ecuaciones es 14. Ahora se aplica el mismo proceso a las dos ecuaciones

$$c)\ x \equiv 14 \ (\text{mód } 15) \quad \text{y} \quad d)\ x \equiv 6 \ (\text{mód } 7)$$

El TCR establece que hay una solución única módulo $M = 15 \cdot 7 = 105$. Al sumar múltiplos del módulo $m = 15$ a la solución dada $x = 14$ de la primera ecuación c) se obtienen las siete soluciones siguientes de b) que son menores que 105:

$$14, \quad 29, \quad 44, \quad 59, \quad 74, \quad 89, \quad 104$$

Al probar cada una de estas soluciones de c) en la segunda ecuación d) se encuentra que la única solución de ambas ecuaciones es 104. Por tanto, el menor entero positivo que satisface las tres ecuaciones es

$$x = 104$$

Ésta es la solución del acertijo.

Método 2: Al usar la notación anterior, se obtiene

$$M = 3 \cdot 5 \cdot 7 = 105, \quad M_1 = 105/3 = 35, \quad M_2 = 105/5 = 21, \quad M_3 = 105/7 = 15$$

Ahora se buscan las soluciones de las ecuaciones

$$35x \equiv 1 \ (\text{mód } 3), \quad 21x \equiv 1 \ (\text{mód } 5), \quad 15x \equiv 1 \ (\text{mód } 7)$$

Al reducir 35 módulo 3, reducir 21 módulo 5 y reducir 15 módulo 7 se obtiene el sistema

$$2x \equiv 1 \ (\text{mód } 3), \quad x \equiv 1 \ (\text{mód } 5), \quad x \equiv 1 \ (\text{mód } 7)$$

Las soluciones de estas tres ecuaciones son, respectivamente,

$$s_1 = 2, \quad s_2 = 1, \quad s_3 = 1$$

Ahora se sustituye en la fórmula (11.9) para obtener la siguiente solución del sistema original:

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$$

Al dividir esta solución entre el módulo $M = 105$ se obtiene el residuo

$$x = 104$$

que es la solución única del acertijo entre 0 y 105.

Observación: Las soluciones anteriores $s_1 = 2$, $s_2 = 1$, $s_3 = 1$ se obtuvieron por inspección. Si los módulos son grandes, siempre es posible usar el algoritmo de Euclides para encontrar estas soluciones como en el ejemplo 11.17.

PROBLEMAS RESUELTOS

DESIGUALDADES, VALOR ABSOLUTO

11.1 Inserte el símbolo correcto, $<$, $>$ o $=$, entre cada par de enteros.

a) $4 \_\_\_\_ -7$; *b*) $-2 \_\_\_\_ -9$; *c*) $(-3)^2 \_\_\_\_ 9$; *d*) $8 \_\_\_\_ 3$,

Para cada par de enteros, por ejemplo a y b, determine sus posiciones relativas en la recta numérica R; o, en forma alterna, calcule $b - a$ y escriba $a < b$, $a > b$ o $a = b$, según $b - a$ sea positivo, negativo o cero. Por tanto:

a) $4 > -7$; *b*) $-2 > -9$; *c*) $(-3)^2 = 9$; *d*) $-8 < 3$.

11.2 Evalúe *a*) $|2 - 5|, |-2 + 5|, |-2 - 5|$; *b*) $|5 - 8| + |2 - 4|, |4 - 3| - |3 - 9|$.

Primero evalúe dentro del signo de valor absoluto:

a) $|2 - 5| = |-3| = 3, |-2 + 5| = |3| = 3, |-2 - 5| = |-7| = 7$

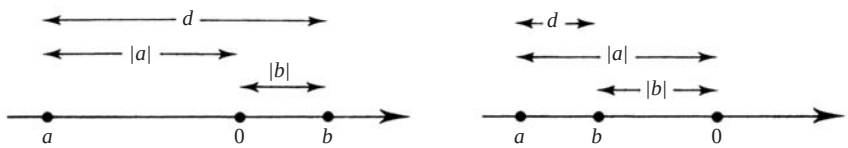
b) $|5 - 8| + |2 - 4| = |-3| + |-2| = 3 + 2 = 5; |4 - 3| - |3 - 9| = |1| - |-6| = 1 - 6 = -5$

11.3 Encuentre la distancia d entre cada par de enteros:

a) 3 y -7; *b*) -4 y 2; *c*) 1 y 9; *d*) -8 y -3; *e*) -5 y -8.

La distancia d entre a y b está dada por $d = |a - b| = |b - a|$. En forma alterna, como se indica en la figura 11-5, $d = |a| + |b|$ cuando a y b tienen signos distintos, y $d = |a| - |b|$ cuando a y b tienen el mismo signo y $d = |a| > |b|$.

Por tanto, *a*) $d = 3 + 7 = 10$; *b*) $d = 4 + 2 = 6$; *c*) $d = 9 - 1 = 8$; *d*) $d = 8 - 3 = 5$; *e*) $d = 8 - 5 = 3$.



i) $d = |a| + |b|$ *ii*) $d = |a| + |b|$

Figura 11-5

11.4 Encuentre todos los enteros n tales que *a*) $1 < 2n - 6 < 14$; *b*) $2 < 8 - 3n < 18$.

a) A los "tres miembros" se suma 6 para obtener $7 < 2n < 20$. Luego, todos los miembros se dividen entre 2 (o se multiplican por $1/2$) para obtener $3.5 < n < 10$. Por tanto, $n = 4, 5, 6, 7, 8, 9$.

b) A los "tres miembros" se suma -8 para obtener $-6 < -3n < 10$. Luego, se divide entre -3 (o se multiplican por $-1/3$) y, como -3 es negativo, el sentido de la desigualdad cambia para obtener

$$2 > n > -3.3 \quad \text{o} \quad -3.3 < n < 2$$

Por tanto, $n = -3, -2, -1, 0, 1$.

11.5 Demuestre la proposición 11.3: suponga $a \leq b$ y que c es cualquier entero. Entonces: *i*) $a + c \leq b + c$, *ii*) $ac = bc$ cuando $c > 0$; pero $ac = bc$ cuando $c < 0$.

Ciertamente, la proposición es verdadera cuando $a = b$. Por tanto, sólo es necesario considerar el caso en que $a < b$; es decir, cuando $b - a$ es positivo.

i) La siguiente diferencia es positiva: $(b + c) - (a + c) = b - a$. Así, $a + c < b + c$.

ii) Se supone que c es positivo. Por la propiedad $[\mathbf{P_1}]$ de los enteros positivos $\mathbf{N}$, el producto $c(b - a)$ también es positivo. Así, $ac < bc$.

Luego se supone que c es negativo. Entonces $-c$ es positivo y el producto $(-c)(b - a) = ac - bc$ también es positivo. En consecuencia, $bc < ac$, de modo que $ac > bc$.

11.6 Demuestre la proposición 11.4 *iii*): $|ab| = |a||b|$.

La demostración consiste en el análisis de los cinco casos siguientes: *a*) $a = 0$ o $b = 0$; *b*) $a > 0$ y $b > 0$; *c*) $a > 0$ y $b < 0$; *d*) $ba < 0$ y $b > 0$; *e*) $ba < 0$ y $b < 0$. Aquí sólo se prueba el tercer caso. *c*) Puesto que $a > 0$ y $b < 0$, $|a| = a$ y $|b| = -b$. También, $ab < 0$. Por tanto, $|ab| = -(ab) = a(-b) = |a||b|$.

11.7 Demostrar la proposición 11.4 *iv*): $|a \pm b| \leq |a| + |b|$.

Ahora $ab \leq |ab| = |a||b|$, y así $2ab \leq 2|a||b|$. Por tanto

$$(a + b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$$

Pero $\sqrt{(a + b)^2} = |a + b|$. Por tanto, la raíz cuadrada de lo anterior produce $|a + b| \leq |a| + |b|$. También,

$$|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$$

INDUCCIÓN MATEMÁTICA, PRINCIPIO DEL BUEN ORDEN

11.8 Demuestre la proposición de que la suma de los n primeros enteros positivos es $n(n + 1)/2$; es decir:

$$P(n): \quad 1 + 2 + \cdots + n = \frac{1}{2}n(n + 1)$$

$P(1)$ es verdadera puesto que $1 = \frac{1}{2}(1)(1 + 1)$. Se supone que $P(k)$ es verdadera y a ambos miembros de $P(k)$ se suma $k + 1$, con lo que se obtiene

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k + 1) &= \frac{1}{2}k(k + 1) + (k + 1) = \frac{1}{2}[k(k + 1) + 2(k + 1)] \\ &= \frac{1}{2}[(k + 1)(k + 2)] \end{aligned}$$

Esto es $P(k + 1)$. En consecuencia, $P(k+ 1)$ es verdadera siempre que $P(k)$ sea verdadera. Por el principio de inducción matemática, P es verdadera para $n \in \mathbf{N}$.

11.9 Si $a \neq 1$, demuestre que P es verdadera para toda $n \geq 1$, donde P se define como:

$$P(n): \quad 1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

$P(1)$ es verdadera puesto que

$$1 + a = \frac{a^2 - 1}{a - 1}$$

Se supone que $P(k)$ es verdadera y se suma a^{k+1} a ambos miembros de $P(k)$, con lo que se obtiene

$$\begin{aligned} 1 + a + a^2 + \ldots + a^k + a^{k+1} &= \frac{a^{k+1} - 1}{a - 1} + a^{k+1} = \frac{a^{k+1} - 1 + (a - 1)a^{k+1}}{a - 1} \\ &= \frac{a^{k+2} - 1}{a - 1} \end{aligned}$$

Esto es $P(k + 1)$. En consecuencia, $P(k+ 1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción matemática, P es verdadera para $n \in \mathbf{N}$.

11.10 Si n es un entero positivo. Demuestre $n \geq 1$. (Esto no es cierto para los números racionales $\mathbf{Q}$.) En otras palabras, si $P(n)$ es la declaración de que $n \geq 1$, entonces $P(n)$ es verdadera para cualquier $n \in \mathbf{N}$.

$P(n)$ se cumple para $n = 1$ puesto que $1 \geq 1$. Se supone que $P(k)$ es verdadera; es decir, $k \geq 1$ y se suma 1 a ambos miembros para obtener

$$k + 1 \geq 1 + 1 = 2 > 1$$

Esto es $P(k + 1)$. En consecuencia, $P(k+ 1)$ es verdadera siempre que $P(k)$ es verdadera. Por el principio de inducción matemática, P es verdadera para $n \in \mathbf{N}$.

11.11 Suponga que a y b son enteros positivos. Demuestre que:

a) Si $b \neq 1$, entonces $a < ab$.
b) Si $ab = 1$, entonces $a = 1$ y $b = 1$.
c) Si n es compuesto, entonces $n = ab$, donde $1 < a, b < n$.

a) Por el problema 11.10, $b > 1$. Por tanto, $b - 1 > 0$; es decir, $b - 1$ es positivo. Por la propiedad $[P_1]$ de los enteros positivos $\mathbf{N}$, el siguiente producto también es positivo:

$$a(b - 1) = ab - a$$

Por tanto, $a < ab$, como se requería.

b) Si $b \neq 1$. Por el inciso *a*), $a < ab = 1$. Esto contradice el problema 11.10; por tanto, $b = 1$. Entonces se concluye que $a = 1$.

c) Si n no es primo, entonces n tiene un divisor positivo a tal que $a \neq 1$ y $a \neq n$. Entonces $n = ab$, donde $b \neq 1$ y $b \neq n$. Así, por el problema 11.10 y por el inciso *a*), $1 < a, b < ab = n$.

11.12 Demuestre el teorema 11.6 (principio del buen orden): sea S un conjunto no vacío de enteros positivos. Entonces S contiene un elemento mínimo.

Suponga que S no contiene un elemento mínimo. Si M consta de todos aquellos enteros positivos que son menores que cualquier elemento de S, entonces $1 \in M$; de otra manera, $1 \in S$ y 1 deberá ser el elemento mínimo de S. Suponga que $k \in M$. Entonces k es menor que cualquier elemento de S. Por tanto, $k + 1 \in M$; de otra manera $k + 1$ sería el elemento mínimo de S.

Por el principio de inducción matemática, M contiene a todo entero positivo. Así, S es vacío, lo que contradice la hipótesis de que S no es vacío. En consecuencia, la hipótesis original de que S no tiene un elemento mínimo no puede ser verdadera. Por tanto, el teorema es verdadero.

11.13 Demuestre el teorema 11.5 (inducción: segunda forma): sea P una proposición definida sobre los enteros $n \geq 1$ tales que: *i*) $P(1)$ es verdadera. *ii*) $P(k)$ es verdadera siempre que $P(j)$ sea verdadera para todo $1 \leq j < k$.

Entonces P es verdadera para toda $n \geq 1$.

Sea A el conjunto de los enteros $n \geq 1$ para los que P no es verdadera. Se supone que A no es vacío. Por el principio del buen orden, A contiene un elemento mínimo a_0. Por el inciso *i*), $a_0 \neq 1$.

Debido a que a_0 es el elemento mínimo de A, P es verdadera para todo entero j donde $1 \leq j < a_0$. Por el inciso *ii*), P es verdadera para a_0. Esto contradice el hecho de que $a_0 \in A$. Por tanto, A es vacío, de modo que P debe ser verdadera para todo entero $n > 1$.

ALGORITMO DE LA DIVISIÓN

11.14 Para cada par de enteros a y b, encuentre enteros q y r tales que $a = bq + r$ y $0 < r < |b|$;

a) $a = 258$ y $b = 12$; *b*) $a = 573$ y $b = -16$.

a) Aquí a y b son positivos. Simplemente se divide a entre b; es decir, 258 entre 12, por ejemplo, con la división larga, para obtener el cociente $q = 21$ y el residuo $r = 6$. En forma alterna, con una calculadora, se obtiene

$$258/12 = 21.5, \quad q = INT(a/b) = 21, \quad r = a - bq = 258 - 12(21) = 6$$

b) Aquí a es positivo pero b es negativo. a se divide entre $|b|$, es decir, 573 entre 12; con una calculadora se obtiene

$$a/|b| = 573/16 = 35.8125, \quad q' = \text{INT}(a/|b|) = 35, \quad r' = 573 - 16(35) = 13$$

Entonces

$$573 = (16)(35) + 13 \quad \text{y} \quad 573 = (-16)(-35) + 13$$

Por tanto, $q = 35$ y $r = 13$.

11.15 Para cada par de enteros a y b, encuentre enteros q y r tales que $a = bq + r$ y $0 < r < |b|$:

a) $a = -381$ y $b = 14$; *b*) $a = -433$ y $b = -17$.

Aquí a es negativo en cada caso; por tanto, es necesario hacer algunos ajustes para asegurar que $0 < r < |b|$.

a) Se divide $|a| = 381$ entre $b = 14$; con una calculadora se obtiene el cociente $q' = 27$ y el residuo $r' = 3$. Así,

$$381 = (14)(27) + 3 \quad \text{y así sucesivamente} \quad -381 = (14)(-27) - 3$$

Pero -3 es negativo y no puede ser el residuo r; entonces, $b = 14$ se suma y resta como sigue:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Así, $q = -28$ y $r = 11$.

b) Se divide $|a| = 433$ entre $|b| = 17$; por ejemplo, con una calculadora, para obtener el cociente $q' = 25$ y el residuo $r' = 8$. Así:

$$433 = (17)(25) + 8 \quad \text{y así sucesivamente} \quad -433 = (-17)(25) - 8$$

Pero -8 es negativo y no puede ser el residuo r; esto se corrige al sumar y restar $|b| = 17$ como sigue:

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9$$

Así, $q = 26$ y $r = 9$.

11.16 Demuestre que $\sqrt{2}$ no es racional; es decir, que $\sqrt{2} \neq a/b$ donde a y b son enteros.

Suponga que $\sqrt{2}$ es racional y $\sqrt{2} = a/b$, donde a y b son enteros escritos en su mínima expresión; es decir, mcd$(a, b) = 1$. Al elevar al cuadrado ambos miembros se obtiene

$$2 = \frac{a^2}{b^2} \quad \text{o} \quad a^2 = 2b^2$$

Así, 2 divide a a^2. Puesto que 2 es primo, 2 también divide a a. Por ejemplo, $a = 2c$. Entonces

$$2b^2 = a^2 = 4c^2 \quad \text{o} \quad b^2 = 2c^2$$

Entonces, 2 divide a b^2. Puesto que 2 es primo, también divide a b. Por consiguiente, 2 divide a a y a b. Esto contradice el supuesto de que mcd$(a, b) = 1$. Por tanto, $\sqrt{2}$ no es racional.

11.17 Demuestre el teorema 11.8 (algoritmo de la división) para el caso de los enteros positivos. Es decir, si se supone que a y b son enteros positivos, demostrar que existen enteros no negativos q y r tales que

$$a = bq + r \quad \text{y} \quad 0 \leq r < b \tag{11.10}$$

Si $a < b$, se escogen $q = 0$ y $r = a$. Si $a = b$, se escogen $q = 1$ y $r = 0$. En cualquier caso, q y r satisfacen (11.10).

La demostración es por inducción sobre a. Si $a = 1$, entonces $a < b$ o $a = b$; por tanto, el teorema se cumple cuando $a = 1$. Se supone que $a > b$. Entonces $a - b$ es positivo y $a - b < a$. Por inducción, el teorema se cumple para $a - b$. Por tanto, existen q' y r' tales que

$$a - b = bq' + r \quad \text{y} \quad 0 \leq r' < b$$

Entonces

$$a = bq' + b + r \; = b(q' + 1) + r'$$

Se escogen $q = q' + 1$ y $r = r'$. Entonces, q y r son enteros no negativos y satisfacen (11.10). Así, se demuestra el teorema.

11.18 Demostrar el teorema 11.8 (algoritmo de la división). Sean a y b enteros con $b \neq 0$. Entonces existen enteros q y r tales que $a = bq + r$ y $0 \leq r' < |b|$. También, los enteros q y r son únicos.

Sea M el conjunto de los enteros no negativos de la forma $a - xb$ para algún entero x. Si $x = -|a|b$, entonces $a - xb$ es no negativo; por tanto, M no es vacío. Por el principio de buen orden, M tiene un elemento mínimo; por ejemplo, r. Puesto que $r \in M$ se tiene

$$r \geq 0 \quad \text{y} \quad r = a - qb$$

para algún entero q. Sólo es necesario demostrar que $r < |b|$. Se supone que $r \geq |b|$. Sea $r' = r - |b|$.

Entonces $r' \geq 0$ y también $r' < r$ porque $b \neq 0$. Además,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{si } b < 0 \\ a - (q-1)b, & \text{si } b > 0 \end{cases}$$

En cualquier caso, r' pertenece a M. Esto contradice el hecho de que r es el elemento mínimo de M. En consecuencia, $r < |b|$. Así, se demuestra la existencia de q y r.

Luego se demuestra que q y r son únicos. Si existen enteros q y r y q' y r' tales que

$$a = bq + r \quad \text{y} \quad a = bq' + r' \quad \text{donde} \quad 0 < r, r' < |b|$$

Entonces $bq + r = bq' + r'$; por tanto

$$b(q - q') = r' - r$$

Así, b divide a $r' - r$. Pero $|r' - r| < |b$ puesto que $0 < r, r' < |b|$. En consecuencia, $r' - r = 0$. Debido a que $b \neq 0$, esto implica que $q - q' = 0$. Por consiguiente, $r' = r$ y $q' = q$; es decir, q y r están determinados en forma única por a y b.

DIVISIBILIDAD, PRIMOS, MÁXIMO COMÚN DIVISOR

11.19 Encuentre todos los divisores positivos de *a*) 18; *b*) $256 = 2^8$; *c*) $392 = 2^3 \cdot 7^2$.

a) Puesto que 18 es relativamente pequeño, se escriben todos los enteros positivos (≤ 18) que dividen a 18. Éstos son:

$$1, \quad 2, \quad 3, \quad 6, \quad 9, \quad 18$$

b) Puesto que 2 es primo, los divisores positivos de $256 = 2^8$ son simplemente las potencias menores que 2; es decir,

$$2^0, \quad 2^1, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad 2^7, \quad 2^8$$

En otras palabras, los divisores positivos de 256 son:

$$1, \quad 2, \quad 4, \quad 8, \quad 16, \quad 32, \quad 64, \quad 128, \quad 256$$

c) Puesto que 2 y 7 son primos, los divisores positivos de $392 = 2^3 \cdot 7^2$ son productos de potencias menores que 2 por potencias menores que 7; es decir,

$$2^0 \cdot 7^0, \quad 2^1 \cdot 7^0, \quad 2^2 \cdot 7^0, \quad 2^3 \cdot 7^0, \quad 2^0 \cdot 7^1, \quad 2^1 \cdot 7^1, \quad 2^2 \cdot 7^1, \quad 23 \cdot 7^1,$$
$$2^0 \cdot 7^2, \quad 2^1 \cdot 7^2, \quad 2^2 \cdot 7^2, \quad 2^3 \cdot 7^2$$

En otras palabras, las potencias positivas de 392 son:

$$1, \quad 2, \quad 4, \quad 8, \quad 7, \quad 14, \quad 28, \quad 56, \quad 49, \quad 98, \quad 196, \quad 392.$$

(Se usó la convención de que $n^0 = 1$ para cualquier número n distinto de cero.)

11.20 Enumere todos los primos entre 50 y 100.

Simplemente se escriben los números entre 50 y 100 que no pueden escribirse como un producto de dos enteros positivos, excepto a 1 y a p. Así se obtiene:

$$51, \quad 53, \quad 57, \quad 59, \quad 61, \quad 67, \quad 71, \quad 73, \quad 79, \quad 83, \quad 87, \quad 89, \quad 91, \quad 93, \quad 97$$

11.21 Sean $a = 8\,316$ y $b = 10\,920$.

a) Encuentre $d = \text{mcd}(a, b)$, el máximo común divisor de a y b.
b) Encuentre enteros m y n tales que $d = ma + nb$.
c) Encuentre $\text{mcm}(a, b)$, el mínimo común múltiplo de a y b.

a) El algoritmo de Euclides se aplica a a y b. Es decir, el algoritmo de la división se aplica a a y b y luego, en forma repetida, el algoritmo de la división se aplica a cada cociente y residuo hasta que se obtiene un residuo igual a cero. Estos pasos se muestran en la figura 11-6*a*) mediante la división larga y también en la figura 11-6*b*), donde las flechas indican el cociente y el residuo en el paso siguiente. El último residuo diferente de cero es 84. Así, $84 = \text{mcd}(8\,316, 10\,920)$.

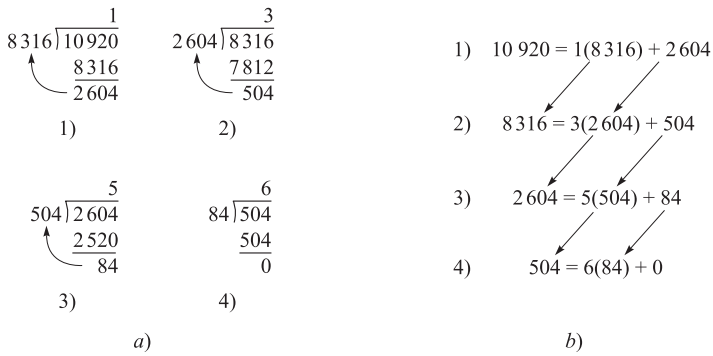


Figura 11-6

b) Luego, se encuentran m y n tales que $84 = 8\,316m + 1\,092n$ al "desenredar" los pasos anteriores en el algoritmo de Euclides. En específico, los tres primeros cocientes en la figura 11-6 conducen a la ecuación:

$$1)\ 2\,604 = 10\,920 - 1(8\,316); \quad 2)\ 504 = 8\,316 - 3(2\,604); \quad 3)\ 84 = 2\,604 - 5(504).$$

La ecuación 3) indica que $d = 84$ es una combinación lineal de 2 604 y 504. Se usa 2) para sustituir 5 044 en 3), de modo que 84 pueda escribirse como una combinación lineal de 2 604 y 8 316 como sigue:

$$\begin{aligned} 5)\ 84 &= 2\,604 - 5[8\,316 - 3(2\,604)] = 2\,604 - 5(8\,316) + 15(2\,604) \\ &= 16(2\,604) - 5(8\,316) \end{aligned}$$

Luego se usa 1) para sustituir 2 604 en 5), de modo que 84 pueda escribirse como una combinación lineal de 8 316 y 10 290 como sigue:

$$\begin{aligned} 6)\ 84 &= 16[10\,920 - 1(8\,316)] - 5(8\,316) = 16(10\,920) - 16(8\,316) - 5(8\,316) \\ &= -21(8\,316) + 16(10\,920) \end{aligned}$$

Ésta es la combinación lineal que se busca. En otras palabras, $m = -21$ y $n = 16$.

c) Por el teorema 11.16,

$$\text{mcm}(a, b) = \frac{|ab|}{\text{mcd}(a, b)} = \frac{(8\,316)(10\,920)}{84} = 1\,081\,080$$

11.22 Encuentre la factorización única de cada número: *a*) 135; *b*) 1 330; *c*) 3 105; *d*) 211.

a) $135 = 5 \cdot 27 = 5 \cdot 3 \cdot 3 \cdot 3$ o $135 = 3^3 \cdot 5$.
b) $1\,330 = 2 \cdot 665 = 2 \cdot 5 \cdot 133 = 2 \cdot 5 \cdot 7 \cdot 19$.
c) $3\,105 = 5 \cdot 621 = 5 \cdot 3 \cdot 207 = 5 \cdot 3 \cdot 3 \cdot 69 = 5 \cdot 3 \cdot 3 \cdot 3 \cdot 23$, o $3\,105 = 3^3 \cdot 5 \cdot 23$.
d) Ninguno de los primos 2, 3, 5, 7, 11, 13 divide a 211; por tanto, 211 no puede factorizarse; es decir, 211 es primo.

(**Observación:** sólo se prueban los primos menores que $\sqrt{211}$.)

11.23 Sean $a = 2^3 \cdot 3^5 \cdot 5^4 \cdot 11^6 \cdot 17^3$ y $b = 2^5 \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^2$. Encuentre mcd($a$, b) y mcm(a, b).

Los primos p_i que aparecen tanto en a como en b también aparecen en mcd(a, b). Además, el exponente de p_i en mcd(a, b) es el menor de los exponentes en a y b. Entonces,

$$\text{mcd}(a, b) = 2^3 \cdot 5^3 \cdot 11^4$$

Los primos p_i que aparecen en a o en b también aparecen en mcm(a, b). También, el exponente de p_i en mcm(a, b) es el mayor de sus exponentes en a y b. Entonces,

$$\text{mcm}(a, b) = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^2 \cdot 17^3$$

11.24 Demuestre el teorema 11.9: Suponga que a, b, c son enteros.

i) Si $a|b$ y $b|c$, entonces $a|c$.
ii) Si $a|b$, entonces, para cualquier entero x, $a|bx$.
iii) Si $a|b$ y $a|c$, entonces $a|(b + c)$ y $a|(b - c)$.
iv) Si $a|b$ y $b \neq 0$, entonces $a = \pm b$ o $|a| < |b|$.
v) Si $a|b$ y $b|a$, entonces $|a| = |b|$, es decir, $a = \pm b$.
vi) Si $a|1$, entonces $a = \pm 1$.

i) Si $a|b$ y $b|c$, entonces existen enteros x y y tales que $ax = b$ y $by = c$. Al sustituir b por ax se obtiene $axy = c$. Por tanto, $a|c$.

ii) Si $a|b$, entonces existe un entero c tal que $ac = b$. Al multiplicar la ecuación por x se obtiene $acx = bx$. Por tanto, $a|bx$.

iii) Si $a|b$ y $a|c$, entonces existen enteros x y y tales que $ax = b$ y $ay = c$. Al sumar las igualdades se obtiene

$$ax + ay = b + c \quad \text{y así} \quad a(x + y) = b + c$$

Por tanto, $a|(b + c)$. Al restar las igualdades $ay = b$ y $by = c$ se obtiene

$$ax - ay = b - c \quad \text{y así} \quad a(x - y) = b - c.$$

Por tanto, $a|(b - c)$.

iv) Si $a|b$, entonces existe c tal que $ac = b$. Entonces

$$|b| = |ac| = |a||c|$$

Por tanto, se cumple una de dos $|c| = 1$ o $|a| < |a||c| = |b|$. Si $|c| = 1$, entonces $c = \pm 1$; donde $a = \pm b$, como se requería.

v) Si $a \mid b$, entonces $a = \pm b$ o $|a| < |b|$. Si $|a| < |b|$ entonces $b \mid a$. Por tanto $a = \pm b$.

vi) Si $a \mid 1$, entonces $a = \pm 1$ o $|a| < |1| = 1$. Por el problema 11.11, $|a| \geq 1$. Por tanto, $a = \pm 1$.

11.25 Un subconjunto no vacío J de $\mathbf{Z}$ se denomina *ideal* si J tiene las dos propiedades siguientes:

1) Si $a, b \in J$, entonces $a + b \in J$. 2) Si $a \in J$ y $n \in \mathbf{Z}$, entones $na \in J$.

Sea d el menor entero positivo en un ideal $J \neq \{0\}$. Demuestre que d divide a todo elemento de J.

Puesto que $J \neq \{0\}$, existe $a \in J$ con $a \neq 0$. Entonces $-a = (-1)a \in J$. Por tanto, J contiene elementos positivos. Por el principio del buen orden, J contiene un entero positivo mínimo, de modo que d existe. Ahora, sea $b \in J$. Al dividir b entre d, el algoritmo de la división indica que existen q y r tales que

$$b = qd + r \quad \text{y} \quad 0 \leq r < d$$

Ahora, $d \in J$ y J en un ideal; por tanto, $b + (-q)d = r$ también pertenece a J. Por la propiedad de que d es mínimo, debe tenerse $r = 0$. Por tanto, $d|b$, como se requería.

11.26 Demuestre el teorema 11.13. Sea d el menor entero positivo de la forma $ax + by$. Entonces $d = \text{mcm}(a, b)$.

Considere el conjunto $J = \{ax + yb \mid x, y \in \mathbf{Z}\}$. Entonces

$$a = 1(a) + 0(b) \in J \quad \text{y} \quad b = 0(a) + 1(b) \in J$$

También suponga que $s, t \in J$, por ejemplo, $s = x_1a + y_1b$ y $t = x_2a + y_2b$. Entonces, para cualquier $n \in \mathbf{Z}$, lo siguiente pertenece a J:

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \quad \text{y} \quad ns = (nx_1)a + (ny_1)b$$

Por tanto, J es un ideal. Sea d el elemento positivo mínimo en J. Se afirma que $d = \text{mcd}(a, b)$.

Por el problema 11.25, d divide a todos los elementos de J. Así, en particular, d divide a a y a b. Ahora se supone que h divide tanto a a como a b. Entonces h divide a $xa + yb$ para cualquier x y y; es decir, h divide a todos los elementos de J. Por tanto, h divide a d, y así $h \leq d$. En consecuencia, $d = \text{mcd}(a, b)$.

11.27 Demuestre el teorema 11.17: si $\text{mcd}(a, b) = 1$, y a y b dividen a c. Entonces ab divide a c.

Puesto que $\text{mcd}(a, b) = 1$, existen x y y únicos tales que $ax + by = 1$. Debido a que $a|c$ y $b|c$, entonces existen m y n tales que $c = ma$ y $c = nb$. Al multiplicar $ax + by = 1$ por c se obtiene

$$acx + bcy = c \quad \text{o} \quad a(nb)x + b(ma)y = c \quad \text{o} \quad ab(nx + my) = c$$

Por tanto, ab divide a c.

11.28 Demuestre el corolario 11.19: si un primo p divide a un producto ab. Entonces $p \mid a$ y $p|b$.

Suponga que p no divide a a. Entonces $\text{mcd}(p, a) = 1$, puesto que los únicos divisores de p son ± 1 y $\pm p$. Así, existen enteros m y n tales que $1 = mp + nq$. Al multiplicar por b se obtiene $b = mpb + nab$. Por hipótesis, $p|ab$; por ejemplo, $ab = cp$. Entonces

$$b = mpb + nab = mpb + ncp = p(mb + nc).$$

En consecuencia, $p|b$, como se requería.

11.29 Demuestre: *a*) Si $p \mid q$, donde p y q son primos. Entonces $p = q$. *b*) Si $p \mid q_1q_2 \cdots q_r$, donde p y los q son primos. Entonces p es igual a uno de los q.

a) Los únicos divisores de q son ± 1 y $\pm q$. Puesto que $p > 1$, $p = q$.

b) Si $r = 1$, entonces $p = q_1$ por *a*). Si $r > 1$. Por el problema 11.28 (corolario 11.19), $p|q_1$ o $p \mid (q_2 \cdots q_r)$.
Si $p \mid q_1$, entonces $p = q_1$ por *a*). De no ser así, entonces $p \mid (q_2 \cdots q_r)$. Se repite el argumento. Es decir, se obtiene $p = p_2$ o $p \mid (q_3 \cdots q_r)$. Finalmente (o por inducción), p debe ser igual a uno de los q.

11.30 Demuestre el teorema fundamental de la aritmética (teorema 11.20): cualquier entero $n > 1$ se expresa en forma única (salvo por el orden) como un producto de primos.

En el teorema 11.11 ya se demostró que este producto de primos existe. Así, sólo es necesario demostrar que el producto es único (salvo por el orden). Si

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_r$$

donde los p y los q son primos. Observe que $p_1 \mid (q_1q_2 \cdots q_r)$. Por el problema precedente 11.29, p_1 es igual a uno de los q. Los q se reordenan de modo que $p_1 = q_1$. Entonces

$$p_1p_2 \cdots p_k = p_1q_2 \cdots p_r \quad \text{y así sucesivamente} \quad p_2 \cdots p_k = q_2 \cdots p_r$$

Por el mismo argumento, los q restantes se reordenan de modo que $p_2 = q_2$. Y así sucesivamente. Por tanto, n puede expresarse de manera única como un producto de primos (salvo por el orden).

CONGRUENCIAS

11.31 ¿Cuál de las siguientes declaraciones es verdadera?

a) $446 \equiv 278 \pmod 7$, *c*) $269 \equiv 413 \pmod{12}$, *e*) $445 \equiv 536 \pmod{18}$
b) $793 \equiv 682 \pmod 9$, *d*) $473 \equiv 369 \pmod{26}$, *f*) $383 \equiv 126 \pmod{15}$

Recuerde que $a \equiv b \pmod m$ si y sólo si m divide a $a - b$.

a) Encuentre la diferencia 446 – 278 = 168. Divida la diferencia 168 entre el módulo $m = 7$. El residuo es 0; por tanto, la declaración es verdadera.

b) Divida la diferencia 739 – 682 = 111 entre el módulo $m = 9$. El residuo no es 0; por tanto, la declaración es falsa.

c) Verdadera, ya que 12 divide a 269 – 413 = −144.

d) Verdadera, ya que 26 divide a 472 – 359 = 104.

e) Falsa, ya que 18 no divide a 445 – 536 = −91.

f) Falsa, ya que 15 no divide a 383 – 126 = 157.

11.32 Encuentre el menor entero en valor absoluto que es congruente módulo $m = 7$ con cada uno de los números siguientes: *a*) 386; *b*) 257; *c*) −192; *d*) −466.

El entero debe estar en el conjunto $\{-3, -2, -1, 0, 1, 2, 3\}$.

a) Al dividir 386 entre $m = 7$ se obtiene un residuo de 1; por tanto, $386 \equiv 1$ (mód 7).

b) Al dividir 257 entre $m = 7$ se obtiene un residuo de 5; por tanto, $257 \equiv 5 \equiv -2$ (mód 7). (Se obtiene −2 al restar el módulo $m = 7$ de 5.)

c) Al dividir 192 entre $m = 7$ se obtiene un residuo de 3; por tanto, $-192 \equiv -3$ (mód 7).

d) Al dividir 466 entre $m = 7$ se obtiene un residuo de 4; por tanto, $-466 \equiv -4 \equiv 3$ (mód 7). (Se obtiene 3 al sumar el módulo $m = 7$ a −4.)

11.33 Encuentre todos los números entre −50 y 50 que son congruentes con 21 módulo $m = 12$; es decir, encuentre todos los x tales que $-50 \leq x \leq 50$ y $x \equiv 21$ (mód 12).

Al número dado 21 se suman y restan múltiplos del módulo $m = 12$ para obtener:

$$21 + 0 = 21, \quad 21 + 12 = 33, \quad 33 + 12 = 46, \quad 21 - 12 = 9$$
$$9 - 12 = -3, \quad -3 - 12 = -15, \quad -15 - 12 = -27, \quad -27 - 12 = -39$$

Es decir: −39, −27, −15, −3, 9, 21, 33, 46

11.34 Demuestre el teorema 11.21: sea m un entero positivo. Entonces:

i) Para todo entero a se tiene $a \equiv a$ (mód m).
ii) Si $a \equiv b$ (mód m), entonces $b \equiv a$ (mód m).
iii) Si $a \equiv b$ (mód m) y $b \equiv c$ (mód m), entonces $a \equiv c$ (mód m).

i) La diferencia $a - a = 0$ es divisible entre m; por tanto, $a \equiv a$ (mód m).

ii) Si $a \equiv b$ (mód m), entonces $m|(a - b)$. Por tanto, m divide a $-(a - b) = b - a$. En consecuencia, $b \equiv a$ (mód m).

iii) Se tiene $m|(a - b)$ y $m|(b - c)$. Así, m divide a la suma $(a - b) + (b - c) = a - c$. En consecuencia, $a \equiv c$ (mód m).

11.35 Demuestre el teorema 11.22: sean $a \equiv c$ (mód m) y $b \equiv d$ (mód m). Entonces:

i) $a + b \equiv c + d$ (mód m). *ii*) $a \cdot b \equiv c \cdot d$ (mód m).

Se tiene que $m|(a - c)$ y $m|(b - d)$.

i) Entonces m divide a la suma $(a - c) + (b - d) = (a + b) - (c + d)$. Por tanto $a + b \equiv c + d$ (mód m).

ii) Entonces m divide a $b(a - c) = ab - bc$ y m divide $c(b - d) = bc - cd$. Entonces m divide a la suma $(ab - bc) + (bc - cd) = ab - cd$. Por tanto $ab \equiv cd$ (mód m).

11.36 Sea $d = \text{mcd}(a, b)$. Demuestre que a/d y b/d son primos relativos.

Existe x y y tales que $d = xa + yb$. Al dividir la ecuación entre d se obtiene $1 = x(a/d) + y(b/d)$. Por tanto, a/d y b/d son primos relativos.

11.37 Demuestre el teorema 11.24: sean $ab \equiv ac$(mód m) y $d = \text{mcd}(a, m)$. Entonces $b \equiv c$ (mód m/d).

Por hipótesis, m divide a $ab - ac = a(b - c)$. Por tanto, existe un entero x tal que $a(b - c) = mx$. Al dividir entre d se obtiene $(a/d)(b - c) = (m/d)x$. Por tanto, m/d divide a $(a/d)(b - c)$. Puesto que m/d y a/d son primos relativos, m/d divide a $b - c$. Es decir, $b \equiv c$(mód m/d), como se requería.

SISTEMAS DE RESIDUOS, FUNCIÓN FI DE EULER, ϕ

11.38 Para cada módulo m, demuestre dos sistemas de residuos completos, uno que conste de los enteros no negativos más pequeños y el otro que conste de los enteros con valor absoluto más pequeño: *a*) $m = 9$; *b*) $m = 12$.

En el primer caso se escoge $\{0, 1, 2, \ldots, m-1\}$, y en el segundo caso se escoge

$$\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\} \quad \text{o} \quad \{-(m-2)/2, \ldots, -1, 0, 1, \ldots, m/2\}$$

según sea el caso si m es par o impar:

a) $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ y $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

b) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ y $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

11.39 Encuentre un sistema reducido de residuos módulo m y ϕ donde *a*) $m = 9$; *b*) $m = 16$; *c*) $m = 7$.

Se escogen aquellos números positivos menores que m y primos relativos con m. La cantidad de tales números es $\phi(m)$.

a) $\{1, 2, 4, 5, 7, 8\}$; por tanto $\phi(9) = 6$.

b) $\{1, 3, 5, 7, 9, 11, 13, 15\}$; por tanto $\phi(16) = 8$.

c) $\{1, 2, 3, 4, 5, 6\}$; por tanto $\phi(7) = 6$. (Esto es de esperar, puesto que $\phi(p) = p - 1$ para cualquier primo p.)

11.40 Recuerde que $S_m = 0, 1, 2, \ldots, m-1$ es un sistema completo de residuos módulo m. Demuestre:

a) Cualesquiera enteros m consecutivos es un sistema completo de residuos módulo m.

b) Si $\text{mcd}(a, m) = 1$, entonces $aS_m = \{0, a, 2a, 3a, \ldots, (m-1)a\}$ es un sistema completo de residuos módulo m.

a) Hay que considerar cualquier otra sucesión de m enteros; por ejemplo, $\{a, a+1, a+2, \ldots, a+(m-1)\}$. El valor absoluto de la diferencia s de dos enteros cualesquiera es menor que m. Por tanto, m no divide a s, de modo que los números son incongruentes módulo m.

b) Si $ax \equiv ay \pmod m$, donde $x, y \in S_m$. Puesto que $\text{mcd}(a, m) = 1$, el teorema 11.24 de la ley de cancelación modificada establece que $x \equiv y \pmod m$. Puesto que $x, y \in S_m$ debe tenerse $x = y$. Es decir, aS_m es un sistema completo de residuos módulo m.

11.41 Muestre un sistema completo de residuos módulo $m = 8$ que conste sólo de múltiplos de 3.

Por el problema 11.40*b*), $3S_8 = \{0, 3, 6, 9, 12, 15, 18, 21\}$ es un sistema de residuos completo módulo $m = 8$.

11.42 Demuestre que si p es primo, entonces $\phi(p^n) = p^n - \text{p}^{n-1} = \text{p}^{n-1}(p-1)$.

Resulta evidente que $\text{mcd}(a, p^n) \neq 1$ si y sólo si p divide a a. Por tanto, los únicos números entre 1 y p^n que no son primos relativos con p^n son los múltiplos de p; es decir, $p, 2p, 3p, \ldots, p^{n-1}(p)$. Hay p^{n-1} múltiplos así de p. Todos los otros números entre 1 y p^n son primos relativos con p^n. Por tanto, como se afirmó:

$$\phi(p^n) = pn - p^{n-1} = p^{n-1}(p-1).$$

11.43 Encuentre *a*) $\phi(81)$, $\phi(7^6)$; *b*) $\phi(72)$, $\phi(3\,000)$.

a) Por el problema 11.42,

$$\phi(81) = \phi(3^4) = 3^3(3-1) = 27(2) = 54 \quad \text{y} \quad \phi(7^6) = 7^5(7-1) = 6(7^5)$$

b) Se usa el teorema 11.14 de que ϕ es multiplicativo:

$$\phi(72) = \phi(3^2 \cdot 2^3) = \phi(3^2)\phi(2^3) = 3(3-1) \cdot 2^2(2-1) = 24$$
$$\phi(3\,000) = \phi(3 \cdot 2^2 \cdot 5^3) = \phi(3)\phi(2^2)\phi(5^3) = 2 \cdot 2 \cdot 5^2(5-1) = 400$$

11.44 Demuestre el teorema 11.25: si a y b son primos relativos, entonces $\phi(ab) = \phi(a)\phi(b)$.

Sean a y b enteros positivos coprimos (primos relativos), y sea S el conjunto de números desde 1 hasta ab dispuestos en un arreglo como en la figura 11-7. Es decir, el primer renglón de S es la lista de números desde 1 hasta a, el segundo renglón es la lista desde $a + 1$ hasta $2a$ y así sucesivamente. Puesto que a y b son coprimos, cualquier entero x es coprimo de ab si y sólo si es coprimo tanto de a como de b. En el arreglo S se encuentra ese número de enteros x.

Puesto que $na + k \equiv k$ (mód a), cada columna en S pertenece a la misma clase de residuos módulo a. En consecuencia, cualquier entero x en S es coprimo de a si y sólo si x pertenece a una columna encabezada por algún entero k que es coprimo de a. Por otra parte, hay $\phi(a)$ columnas así, puesto que el primer renglón es un sistema de residuos módulo a.

1	2	3	...	k	...	a
$a+1$	$a+2$	$a+3$	...	$a+k$	...	$2a$
$2a+1$	$2a+2$	$2a+3$	...	$2a+k$	...	$3a$
.....						
$(b-1)a+1$	.....			$(b-1)a+k$	...	ba

Figura 11-7

Ahora se considera una columna arbitraria en el arreglo S, que consta de los números:

$$k, \quad a + k, \quad 2a + k, \quad 3a + k, \ldots, (b - 1)a + k \tag{11.11}$$

Por el problema 11.10, estos b enteros constituyen un sistema de residuos módulo b; es decir, ningún par de enteros son congruentes módulo b. En consecuencia, (11.11) contiene exactamente $\phi(b)$ enteros que son coprimos de b. Así se demuestra que el arreglo S contiene $\phi(a)$ columnas que constan de los enteros que son coprimos de a, y que cada columna contiene $\phi(b)$ enteros que son coprimos de b. Por tanto, hay $\phi(a)\ \phi(b)$ enteros en el arreglo S que son coprimos tanto de a como de b y que entonces son coprimos de ab. En consecuencia, como se requería

$$\phi(ab) = \phi(a)\phi(b)$$

ARITMÉTICA MÓDULO m, $\mathbf{Z_M}$

11.45 Escriba las tablas de suma y multiplicación para: *a*) $\mathbf{Z}_4$; *b*) $\mathbf{Z}_7$

a) Ver la figura 11-8. *b*) Ver la figura 11-9.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figura 11-8

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Figura 11-9

11.46 En $\mathbf{Z}_{11}$, encuentre: *a*) $-2, -5, -9, -10$; *b*) $2/7, 3/7, 5/7, 8/7, 10/7, 1/7$.

a) Observe que $-a = m - a$ puesto que $(m - a) + a = 0$. En consecuencia:

$$-2 = 11 - 2 = 9, \quad -5 = 11 - 5 = 6, \quad -9 = 11 - 9 = 2, \quad -10 = 11 - 10 = 1$$

b) Por definición, a/b es el entero c tal que $bc = a$. Puesto que se divide entre 7, primero se calcula la tabla de multiplicación para 7 en $\mathbf{Z}_{11}$ como en la figura 11-10. Luego se encuentra el número dentro de la tabla y la respuesta está arriba de este número. Así,

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

Figura 11-10

$$2/7 = 5, \quad 3/7 = 2, \quad 5/7 = 7, \quad 8/7 = 9, \quad 10/7 = 3, \quad 1/7 = 8$$

Observe que $7^{-1} = 8$ puesto que $7(8) = 8(7) = 1$.

11.47 Considere $\mathbf{Z_p}$, donde p es primo. Demuestre:

a) Si $ab = ac$ y $a \neq 0$, entonces $b = c$;
b) Si $ab = 0$, entonces $a = 0$ o $b = 0$.

a) Si $ab = ac$ en $\mathbf{Z_p}$, entonces $ab \equiv ac \pmod{m}$. Puesto que $a \neq 0$, $\text{mcd}(a, p) = 1$. Por el teorema 11.23, es posible cancelar las a para obtener $b \equiv c \pmod{p}$. En consecuencia, $b = c$ en $\mathbf{Z_p}$.

b) Si $ab = 0$ en $\mathbf{Z_p}$, entonces $ab \equiv 0 \pmod{p}$. En consecuencia, p divide al producto ab. Puesto que p es primo, $p|a$ y $p|b$; es decir, $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$. Por tanto, $a = 0$ o $b = 0$ en $\mathbf{Z_p}$.

11.48 Considere $a \neq 0$ en $\mathbf{Z}_m$, donde $\text{mcd}(a, m) = 1$. Demuestre que a tiene inverso multiplicativo en $\mathbf{Z}_m$.

Puesto que $a \neq 0$ y $\text{mcd}(a, m) = 1$, existen enteros x y y tales que $ax + my = 1$ o $ax - 1 = my$. Así, m divide a $ax - 1$ y por tanto $ax \equiv 1 \pmod{m}$. Luego, un elemento x' en $\mathbf{Z}_m$ se reduce a x módulo m. Entonces $ax' = 1$ en $\mathbf{Z}_m$.

11.49 Encuentre a^{-1} en $\mathbf{Z}_m$ donde: *a*) $a = 37$ y $m = 249$; *b*) $a = 15$ y $m = 234$.

a) Primero se encuentra $d = \text{mcd}(37, 249)$, con lo que se obtiene $d = 1$. Luego, como en el ejemplo 11.6, se encuentran x y y tales que $ax + my = 1$. Así se obtiene $x = -74$ y $y = 14$; es decir,

$$-74(37) + 11(249) = 1 \quad \text{de modo que} \quad -74(37) \equiv 1 \pmod{249}$$

$m = 249$ se suma a -74 para obtener $-74 + 249 = 175$. Así, $(175)(37) \equiv 1 \pmod{249}$.
En consecuencia, $a^{-1} = 175$ en $\mathbf{Z}_{249}$.

b) Primero se encuentra $d = \text{mcd}(15, 234)$, con lo que se obtiene $d = 3$. Así, $d \neq 1$ y entonces 15 no tiene inverso multiplicativo en $\mathbf{Z}_{234}$.

11.50 Para los siguientes polinomios sobre $\mathbf{Z}_7$, encuentre *a*) $f(x) + g(x)$ y *b*) $f(x)h(x)$.

$$f(x) = 6x^3 - 5x^2 + 2x - 4, \quad g(x) = 5x^3 + 2x^2 + 6x - 1, \quad h(x) = 3x^2 - 2x - 5$$

Efectuar las operaciones como si los polinomios fuesen sobre los enteros $\mathbf{Z}$, y luego reducir los coeficientes módulo 7.

a) Se obtiene: $f(x) + g(x) = 11x^3 - 3x^2 + 8x - 5 = 4x^3 - 3x^2 + x - 5 = 4x^3 + 4x^2 + x + 2$

b) Primero se encuentra el producto $f(x)h(x)$ como en la figura 11-11. Luego, al reducir módulo 7, se obtiene: *g*)

$$f(x)h(x) = 4x^5 - 6x^4 + 2x^2 - 2x + 6 = 4x^5 + x^4 + 2x^2 + 5x + 6$$

$$
\begin{array}{r}
6x^3 - 5x^2 + 2x - 4 \\
3x^2 - 2x - 5 \\
\hline
18x^5 - 15x^4 + 6x^3 - 12x^2 \\
\quad -12x^4 + 10x^3 - 4x^2 + 8x \\
\quad\quad -30x^2 + 25x^2 - 10x + 20 \\
\hline
18x^5 - 27x^4 + 14x^3 + 9x^2 - 2x + 20
\end{array}
$$

Figura 11-11

ECUACIONES DE CONGRUENCIA

11.51 Resuelva la ecuación de congruencia $f(x) = 4x^4 - 3x^3 + 2x^2 + 5x - 4 \equiv 0 \pmod 6$.

Puesto que la ecuación no es lineal, la ecuación se resuelve al probar los números en un sistema completo de residuos módulo 6; por ejemplo, $\{0, 1, 2, 3, 4, 5\}$. Se tiene:

$f(0) = 4 \not\equiv 0 \pmod 6$, $f(2) = 54 \not\equiv 0 \pmod 6$, $f(4) = 880 \equiv 4 \not\equiv 0 \pmod 6$
$f(1) = 4 \not\equiv 0 \pmod 6$, $f(3) = 272 \equiv 2 \not\equiv 0 \pmod 6$, $f(5) = 2\,196 \equiv 0 \pmod 6$

Por tanto, 2 y 5 son las únicas raíces de $f(x)$ módulo 6. Es decir, $\{2, 5\}$ es un conjunto de soluciones completo.

11.52 Resuelva la ecuación de congruencia $f(x) = 26x^4 - 31x^3 + 46x^2 - 76x + 57 \equiv 0 \pmod 8$.

Primero se reducen los coeficientes de $f(x)$ módulo 8 para obtener la siguiente ecuación de congruencia equivalente.

$$g(x) = 2x^4 - 7x^3 + 6x^2 - 4x + 1 \equiv 0 \pmod 8$$

Puesto que $7 \equiv -1 \pmod 8$ y $6 \equiv -2 \pmod 8$, la ecuación original puede simplificarse aún más para obtener la ecuación de congruencia

$$h(x) = 2x^4 + x^3 - 2x^2 - 4x + 1 \equiv 0 \pmod 8$$

Los números se prueban en un sistema completo de residuos módulo 8 y, a fin de preservar las operaciones aritméticas lo más simples posible, se escoge $\{-3, -2, -1, 0, 1, 2, 3, 4\}$. (Es decir, se escogen aquellos números cuyo valor absoluto es mínimo.) Al sustituir estos números en $h(x)$ se obtiene

$h(-3) = 130 \equiv 2 \pmod 8$, $h(0) = 1 \equiv 1 \pmod 8$, $h(3) = 160 \equiv 0 \pmod 8$,
$h(-2) = 9 \equiv 1 \pmod 8$, $h(1) = -2 \equiv 6 \pmod 8$, $h(4) = 529 \equiv 1 \pmod 8$.
$h(-1) = 4 \equiv 4 \pmod 8$, $h(2) = 25 \equiv 1 \pmod 8$,

Por tanto, 3 es la única raíz de $f(x) \pmod 8$.

11.53 Resuelva la ecuación lineal de congruencia:

a) $3x \equiv 2 \pmod 8$; *b*) $6x \equiv 5 \pmod 9$; *c*) $4x \equiv 6 \pmod{10}$

Debido a que los módulos son relativamente pequeños, mediante prueba se encuentran todas las soluciones. Se debe recordar que $ax \equiv b \pmod m$ tiene exactamente la solución $d = \text{mcd}(a, m)$, en el supuesto de que d divida a b.

a) Aquí, $\text{mcd}(3, 8) = 1$, de modo que la ecuación tiene una solución única. Al probar $0, 1, 2, \ldots, 7$ se encuentra que $3(6) = 18 \equiv 2 \pmod 8$. Por tanto, 6 es la solución única.

b) Aquí, $\text{mcd}(6, 9) = 3$, pero 3 no divide a 5. Por tanto el sistema no tiene solución.

c) Aquí, $\text{mcd}(4, 10) = 2$ y 2 divide a 6; por tanto, el sistema tiene dos soluciones. Al probar $0, 1, 2, 3, \ldots, 9$ se encuentra que

$$4(4) = 16 \equiv 6 \pmod{10} \quad \text{y} \quad 4(9) = 36 \equiv 6 \pmod{10}$$

Por tanto, 4 y 9 son las dos soluciones buscadas.

11.54 Resuelva la ecuación de congruencia $1\,092x \equiv 213 \pmod{2\,295}$.

El método de prueba no es una forma eficiente para resolver esta ecuación puesto que el módulo $m = 2\,295$ es grande. Primero se aplica el algoritmo de Euclides para encontrar $d = \text{mcd}(1\,092, 2\,295) = 3$. Al dividir 213 entre $d = 3$ se obtiene un residuo igual a 0; es decir, 3 divide a 213. Por tanto, la ecuación tiene tres soluciones (incongruentes).

La ecuación y el módulo $m = 2\,295$ se dividen entre $d = 3$ para obtener la ecuación de congruencia

$$364x \equiv 71 \text{ (mód } 765) \tag{11.12}$$

Se sabe que 364 y 796 son primos relativos puesto que se dividió entre $d = \text{mcd}(1\,092, 2\,295) = 3$; por tanto, la ecuación (11.12) tiene una solución única módulo 765. La ecuación (11.12) se resuelve al encontrar primero la solución de la ecuación

$$364x \equiv 1 \text{ (mód } 765) \tag{11.13}$$

Esta solución se obtiene al encontrar s y t tales que

$$364s + 765t = 1$$

Al usar el algoritmo de Euclides y "desenredar" como se hizo en el ejemplo 11.6 y en el problema 11.21 se obtiene $s = 124$ y $t = -59$.

En consecuencia, $s = 124$ es la única solución de (11.13). Al multiplicar esta solución $s = 124$ por 71 y reducir módulo 765 se obtiene

$$124(71) = 8\,804 \equiv 389 \text{ (mód } 765)$$

Ésta es la única solución de (11.12).

Por último, el nuevo módulo $m = 765$ se suma a la solución $x_1 = 389$ dos veces para obtener las otras dos soluciones de la ecuación dada:

$$x_2 = 389 + 765 = 1\,154, \qquad x_3 = 1\,154 + 765 = 1\,919$$

En otras palabras, $x_1 = 389$, $x_2 = 1\,154$, $x_3 = 1\,919$ constituyen un conjunto completo de soluciones de la ecuación de congruencia dada $1\,092x \equiv 213$(mód 2 295).

11.55 Resuelva la ecuación de congruencia $455x \equiv 204$(mód 469).

Primero se usa el algoritmo de Euclides para encontrar $d = \text{mcd}(455, 469) = 7$. Al dividir 204 entre $d = 7$ se obtiene un residuo igual a 1; es decir, 7 no divide a 204. Por tanto, la ecuación no tiene solución.

11.56 Encuentre el menor entero positivo x tal que cuando x se divide entre 3 se obtiene un residuo igual a 2, cuando x se divide entre 7 se obtiene un residuo igual a 4 y cuando x se divide entre 10 se obtiene un residuo igual a 6.

Se busca la menor solución positiva común de las tres siguientes ecuaciones de congruencia:

$$a)\ x \equiv 2(\text{mód } 3); \quad b)\ x \equiv 4 \text{ (mód } 7); \quad c)\ x \equiv 6 \text{ (mód } 10)$$

Observe que los módulos 3, 7 y 10 son primos relativos por pares. El teorema chino del residuo (TCR), teorema 11.29, establece que hay una solución única módulo del producto $m = 3(7)(10) = 210$. Este problema se resuelve de dos formas.

Método 1: Primero se aplica el TCR a las dos primeras ecuaciones,

$$a)\ x \equiv 2 \text{ (mód } 3) \quad \text{y} \quad b)\ x \equiv 4 \text{ (mód } 7)$$

Se sabe que hay una solución única módulo $M = 3 \cdot 7 = 21$. Al sumar múltiplos del módulo $m = 7$ a la solución dada $x = 4$ de la segunda ecuación b), se obtienen las tres siguientes soluciones de b) que son menores que 21:

$$4, 11, 18$$

Al probar cada una de estas soluciones de b) en la primera ecuación a) se encuentra que 11 es la única solución de ambas ecuaciones.

Luego, el mismo proceso se aplica a las dos ecuaciones

$$c)\ x \equiv 6 \text{ (mód } 10) \quad \text{y} \quad d)\ x \equiv 11 \text{ (mód } 21)$$

El TCR indica que hay una solución única módulo $M = 21 \cdot 10 = 210$. Al sumar múltiplos del módulo $m = 21$ a la solución dada $x = 11$ de la ecuación *d*), se obtienen las 10 soluciones siguientes de *d*), que son menores que 210:

$$11, 32, 53, 74, 95, 116, 137, 158, 179, 210$$

Al probar cada una de estas soluciones de *d*) en la ecuación *c*) se encuentra que $x = 116$ es la única solución de la ecuación *c*). En consecuencia, $x = 116$ es el menor entero positivo que satisface las tres ecuaciones dadas *a*), *b*) y *c*).

Método 2: al usar la notación de la proposición 11.30 se obtiene

$$M = 3 \cdot 7 \cdot 10 = 210, \quad M_1 = 210/3 = 70, \quad M_2 = 210/7 = 30, \quad M_3 = 210/10 = 21$$

Ahora se buscan soluciones de las ecuaciones

$$70x \equiv 1 \text{ (mód 3)}, \quad 30x \equiv 1 \text{ (mód 7)}, \quad 21x \equiv 1 \text{ (mód 10)}$$

Al reducir 70 módulo 3, reducir 30 módulo 7 y reducir 21 módulo 10, se obtiene el sistema equivalente

$$x \equiv 1 \text{ (mód 3)}, \quad 2x \equiv 1 \text{ (mód 7)}, \quad x \equiv 1 \text{ (mód 10)}$$

Las soluciones de estas tres ecuaciones son, respectivamente,

$$s_1 = 1, \quad s_2 = 4, \quad s_3 = 1$$

Al sustituir en la fórmula

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

se obtiene la siguiente solución del sistema original:

$$x_0 = 70 \cdot 1 \cdot 2 + 30 \cdot 4 \cdot 4 + 21 \cdot 1 \cdot 6 = 746$$

Al dividir esta solución entre el módulo $M = 210$ se obtiene el residuo $x = 116$, que es la única solución del sistema original entre 0 y 210.

11.57 Demuestre el teorema 11.26: si *a* y *m* son primos relativos, entonces $ax \equiv 1$ (mód *m*) tiene una solución única; en caso contrario, no tiene solución.

Si x_0 es una solución, entonces *m* divide a $ax_0 - 1$ y, por tanto, existe y_0 tal que $my_0 = ax_0 - 1$. En consecuencia,

$$ax_0 + my_0 = 1 \tag{11.14}$$

y *a* y *m* son coprimos (primos relativos). A la inversa, si *a* y *m* son coprimos, entonces existen x_0 y y_0 que satisfacen (11.14), en cuyo caso x_0 es una solución de $ax \equiv 1$ (mód m).

Queda por demostrar que x_0 es una solución única módulo *m*. Suponga que x_1 es otra solución. Entonces

$$ax_0 \equiv 1 \equiv ax_1 \text{(mód } m\text{)}$$

Puesto que *a* y *m* son coprimos, aquí se cumple la ley de cancelación modificada, de modo que

$$x_0 \equiv x_1 \text{ (mód } m\text{)}$$

Por tanto, esto demuestra el teorema.

11.58 Demuestre el teorema 11.27. Si *a* y *m* son primos relativos, entonces $ax \equiv b$ (mód *m*) tiene una solución única. Además, si *s* es la solución única de $ax \equiv 1$(mód *m*), entonces $x = bs$ es la única solución de $ax \equiv b$ (mód *m*).

Por el teorema 11.26 (que se demuestra en el problema 11.57), existe una solución única de $ax \equiv 1$(mód *m*). Por tanto, $as \equiv 1$(mód *m*) y así

$$a(bs) = (as)b \equiv 1 \cdot b = b \text{ (mód } m\text{)}$$

Es decir, $x = bs$ es una solución de $ax \equiv b$ (mód *m*). Si x_0 y x_1 son dos de estas soluciones, entonces

$$ax_0 \equiv b \equiv ax_1 \text{ (mód } m\text{)}$$

Puesto que *a* y *m* son coprimos, la ley de cancelación modificada establece que $x_0 \equiv x_1$(mód *m*). Es decir, $ax \equiv b$ (mód *m*) tiene una solución única módulo *m*.

11.59 Demuestre el teorema 11.28: considere la siguiente ecuación, donde $d = \text{mcd}(a, m)$:

$$ax \equiv b \pmod{m} \tag{11.15}$$

i) Si d no divide a b, entonces (11.15) no tiene solución.

ii) Si d divide a b, entonces (11.15) tiene d soluciones, todas congruentes módulo M con la solución única de la siguiente ecuación, donde $A = a/d, B = b/d, M = m/d$:

$$Ax \equiv B \pmod{M} \tag{11.16}$$

i) Si x_0 es una solución de (11.15). Entonces $ax_0 \equiv b \pmod{m}$, y entonces m divide a $ax_0 - b$. Por tanto, existe un entero y_0 tal que $my_0 = ax_0 - b$ o $my_0 + ax_0 = b$. Pero $d = \text{mcd}(a, m)$, y así d divide a $my_0 + ax_0$. Es decir, d divide a b. En consecuencia, si d no divide a b, entonces no existe solución.

ii) Si x_0 es una solución de (11.15). Entonces, como antes,

$$my_0 + ax_0 = b$$

Al dividir entre d se obtiene (11.16). Por tanto, M divide a $Ax_0 - B$ y entonces x_0 es una solución de (11.16). A la inversa, suponga que x_1 es una solución de (11.16). Entonces, como antes, existe un entero y_1 tal que

$$My_1 + Ax_1 = B$$

Al multiplicar por d se obtiene

$$dMy_1 + dAx_1 = dB \quad \text{o} \quad my_1 + ax_1 = b$$

Por consiguiente, m divide a $ax_1 - b$, por lo cual x_1 es una solución de (11.15). Así, (11.16) tiene la misma solución entera. Sean x_0 las menores soluciones posibles de (11.16). Puesto que $d = dM$,

$$x_0, \quad x_0 + M, \quad x_0 + 2M, \quad x_0 + 3M, \quad \ldots, \quad x_0 + (d-1)M$$

son precisamente las soluciones de (11.16) y (11.15) entre 0 y m. Por tanto, (11.15) tiene d soluciones módulo m, y todas son congruentes con x_0 módulo M.

11.60 Demuestre el teorema chino del residuo (teorema 11.29). Dado el sistema:

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \ldots, \quad x \equiv r_k \pmod{m_k} \tag{11.17}$$

donde los m_i son primos relativos por pares. Entonces el sistema tiene una solución única módulo $M = m_1 m_2 \cdots m_k$.

Considere el entero

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

donde $M_i = M/m_i$ y s_i es la solución única de $M_i x \equiv 1 \pmod{m_i}$. Se da j.

Para $i \neq j$ se tiene $m_j \mid M_i$ y entonces

$$M_i \, s_i \, r_i \equiv 0 \pmod{m_j}$$

Por otra parte, $M_j \, S_j \equiv 1 \pmod{m_j}$; y entonces

$$M_j \, s_j \, r_j \equiv r_j \pmod{m_j}$$

En consecuencia,

$$x_0 \equiv 0 + \cdots + 0 + r_j + 0 + \cdots + 0 \equiv r_j \pmod{mj}$$

En otras palabras, x_0 es una solución de cada una de las ecuaciones en (11.17).

Queda por demostrar que x_0 es la solución única del sistema (11.17) módulo M.

Si x_1 es otra solución de todas las ecuaciones en (11.17). Entonces:

$$x_0 \equiv x_1 \pmod{m_1}, \quad x_0 \equiv x_1 \pmod{m_2}, \quad \cdots, \quad x_0 \equiv x_1 \pmod{m_k}$$

Por tanto, $m_i \mid (x_0 - x_1)$ para cada i. Puesto que los m_i son primos relativos, $M = \text{mcm}\,(m_1, m_2, \ldots, m_k)$ y así $M \mid (x_0 - x_1)$. Es decir, $x_0 \equiv x_1 \pmod{M}$. Así se demuestra el teorema.

PROBLEMAS SUPLEMENTARIOS

ORDEN Y DESIGUALDADES, VALOR ABSOLUTO

11.61 Inserte el símbolo correcto, $<$, $>$ o $=$, entre cada par de enteros:

a) $2 \_\_\_ -6$; *c*) $-7 \_\_\_ 3$; *e*) $2^3 \_\_\_ 11$; *g*) $-2 \_\_\_ -7$;
b) $-3 \_\_\_ -5$; *d*) $-8 \_\_\_ -1$, *f*) $2^3 \_\_\_ -9$; *h*) $4 \_\_\_ -9$.

11.62 Evalúe: *a*) $|3-7|, |-3+7|, |-3-7|$; *b*) $|2-5|+|3+7|, |1-4|-|2-9|$; *c*) $|5-9|+|2-3|, |-6-2|-|2-6|$.

11.63 Encuentre la distancia d entre cada par de enteros: *a*) 2 y -5; *b*) -6 y 3; *c*) 2 y 8; *d*) -7 y -1; *e*) 3 y -3; *f*) -7 y -9.

11.64 Encuentre todos los enteros n tales que: *a*) $3 < 2n-4 < 10$; *b*) $1 < 6-3n < 13$.

11.65 Demuestre la proposición 11.1: *i*) $a \le a$, para cualquier entero; *ii*) Si $a \le b$ y $b \le a$, entonces $a = b$.

11.66 Demuestre la proposición 11.2: para enteros cualesquiera a y b se cumple exactamente una de las siguientes proposiciones: $a < b$, $a = b$ o $a > b$.

11.67 Demuestre que: *a*) $2ab \le a^2 + b^2$; *b*) $ab + ac + bc \le a^2 + b^2 + c^2$.

11.68 Proposición 11.4: *i*) $|a| \ge 0$, y $|a| = 0$ ssi $a = 0$; *ii*) $-|a| \le a \le |a|$; *iii*) $||a| - |b|| \le |a \pm b|$.

11.69 Demuestre que $a - xb \ge 0$, si $b \ne 0$ y $x = -|a|b$.

INDUCCIÓN MATEMÁTICA, PRINCIPIO DEL BUEN ORDEN

11.70 Demuestre la proposición de que la suma de los n primeros enteros pares positivos es $n(n+1)$; es decir,

$$P(n) : 2 + 4 + 6 + \cdots + 2n - = n(n+1)$$

11.71 Demuestre que la suma de los n primeros cubos es igual al cuadrado de la suma de los n primeros enteros positivos:

$$P(n) : 1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

11.72 Demuestre: $1 + 4 + 7 + \cdots + (3n-2) = n(3n-1)/2$

11.73 Demuestre: *a*) $a^n\, a^m = a^{n+m}$; *b*) $(a^n)^m = a^{nm}$; *c*) $(ab)^n = a^n b^n$

11.74 Demuestre: $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} = \frac{1}{3\cdot 4} = \cdots = \frac{1}{n(n+1)} = \frac{n}{n+1}$

11.75 Demuestre: $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} = \frac{1}{5\cdot 7} = \cdots = \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

11.76 Demuestre: $\frac{1^2}{1\cdot 3} + \frac{2^2}{3\cdot 5} = \frac{3^2}{5\cdot 7} = \cdots = \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}$

11.77 Demuestre: $x^{n+1} - y^{n+1} = (x-y)(x^n + x^{n-1}y + x^{n-2}y^2 + \cdots + y^n)$

11.78 Demuestre: $|P(A)| = 2^n$ donde $|A| = n$. Aquí $P(A)$ es el conjunto potencia A con n elementos

ALGORITMO DE LA DIVISIÓN

11.79 Para cada par de enteros a y b, encuentre enteros q y r tales que $a = bq + r$ y $0 \le r < |b|$:

a) $a = 608$ y $b = -17$; *b*) $a = -278$ y $b = 12$; *c*) $a = -417$ y $b = -8$.

11.80 Demuestre cada una de las siguientes proposiciones:

a) Cualquier entero a es de la forma $5k$, $5k+1$, $5k+2$, $5k+3$, o $5k+4$.
b) Uno de cinco enteros consecutivos es un múltiplo de 5.

11.81 Demuestre cada una de las siguientes proposiciones:

a) El producto de tres enteros consecutivos cualesquiera es divisible entre 6.
b) El producto de cuatro enteros consecutivos cualesquiera es divisible entre 24.

11.82 Demuestre que cada uno de los números siguientes no es racional: *a*) $\sqrt{3}$; *b*) $\sqrt[3]{2}$.

11.83 Demuestre que $\sqrt{p}$ no es racional, donde p es cualquier número primo.

DIVISIBILIDAD, MÁXIMOS COMUNES DIVISORES, PRIMOS

11.84 Encuentre todos los divisores posibles de: *a*) 24; *b*) $19\,683 = 3^9$; *c*) $432 = 2^4 \cdot 3^3$.

11.85 Escriba todos los números primos entre 100 y 150.

11.86 Exprese lo siguiente como un producto de números primos: *a*) 2 940; *b*) 1 485; *c*) 8 712; *d*) 319 410.

11.87 Para cada par de enteros a y b, encuentre $d = \text{mcd}(a, b)$ y encuentre m y n tales que $d = ma + nb$:

a) $a = 356$, $b = 48$; *b*) $a = 1\,287$, $b = 165$; *c*) $a = 2\,310$, $b = 168$; *d*) $a = 195$, $b = 968$; *e*) $a = 249$, $b = 37$.

11.88 Encuentre: *a*) mcm(5, 7); *b*) mcm(3, 33); *c*) mcm(12, 28).

11.89 Suponga $a = 5\,880$ y $b = 8\,316$. *a*) Exprese a y b como un producto de primos. *b*) Encuentre mcd(a, b) y mcm(a, b). c) Compruebe que $\text{mcd}(a, b) = |ab|/\text{mcd}(a, b)$.

11.90 Demuestre: *a*) Si $a|b$, entonces *i*) $a| - b$, *ii*) $-a|b$, *iii*) $-a| - b$; *b*) Si $ac|bc$, entonces $b|c$.

11.91 Demuestre: *a*) Si $n > 1$ es compuesto, entonces n tiene un divisor positivo d tal que $d \leq \sqrt{n}$. *b*) Si $n > 1$ no es divisible entre un primo $p \leq \sqrt{n}$, entonces n es primo.

11.92 Demuestre: *a*) Si $am + bn = 1$, entonces mcd $(a, b) = 1$; *b*) Si $a = bq + r$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

11.93 Demuestre: *a*) $\text{mcd}(a, a + k)$ divide a k; *b*) $\text{mcd}(a, a + 2)$ es igual a 1 o a 2.

11.94 Demuestre: *a*) Si $a > 2$ y $k > 1$, entonces $a^k - 1$ es compuesto. *b*) Si $n > 0$ y $2^n - 1$ es primo, entonces n es primo.

11.95 Sea n un entero positivo. Demuestre:

a) 3 divide a n si y sólo si 3 divide a la suma de los dígitos de n.

b) 9 divide a n si y sólo si 9 divide a la suma de los dígitos de n.

c) 8 divide a n si y sólo si 8 divide al entero formado por los tres últimos dígitos de n.

11.96 Extienda la definición de mcd y mcm a cualquier conjunto finito de enteros; es decir, para enteros $a_1, a_2, \ldots, a_k$ defina:

a) $\text{mcd}(a_1, a_2, \ldots, a_k)$; *b*) $\text{mcm}(a_1, a_2, \ldots, a_k)$.

11.97 Demuestre: si $a_1|n, a_2|n, \ldots, a_k|n$, entonces $m|n$, donde $m = \text{mcm}(a_1, a_2, \ldots, a_k)$.

11.98 Demuestre: entre los números primos hay huecos arbitrariamente grandes; es decir, para cualquier entero positivo k, existen k enteros compuestos (no primos) consecutivos.

CONGRUENCIAS

11.99 ¿Cuáles de las siguientes proposiciones son verdaderas?

a) $224 \equiv 762$ (mód 8); *b*) $582 \equiv 263$ (mód 11); *c*) $156 \equiv 369$ (mód 7); *d*) $-238 \equiv 483$ (mód 13).

11.100 Encuentre el menor entero no negativo que es congruente módulo $m = 9$ con cada uno de los siguientes números: *a*) 457; *b*) 1 578; *c*) -366; *d*) $-3\,288$. (El entero debe estar en el conjunto $\{0, 1, 2, \ldots, 7, 8\}$.)

11.101 Encuentre el menor entero en valor absoluto que es congruente módulo $m = 9$ con cada uno de los siguientes números: *a*) 511; *b*) 1 329; *c*) -625; *d*) $-2\,717$. (El entero debe estar en el conjunto $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.)

11.102 Encuentre todos los números entre 1 y 100 que son congruentes con 4 módulo $m = 11$.

11.103 Encuentre todos los números entre -50 y 50 que son congruentes con 12 módulo $m = 9$.

SISTEMAS DE RESIDUOS, FUNCIÓN FI DE EULER, ϕ

11.104 Para cada módulo m, muestre dos sistemas completos de residuos, uno que conste de los menores enteros no negativos y el otro que conste de los enteros con menores valores absolutos: (*a*) $m = 11$; (*b*) $m = 14$.

11.105 Escriba un sistema reducido de residuos módulo m y encuentre $\phi(m)$, donde *a*) $m = 4$; *b*) $m = 11$; *c*) $m = 14$; *d*) $m = 15$.

11.106 Escriba un sistema completo de residuos módulo $m = 8$ que conste completamente de *a*) múltiplos de 5; *b*) potencias de 3.

11.107 Demuestre que $\{1^2, 2^2, 3^2, \ldots, m^2\}$ no es un sistema completo de residuos módulo m para $m > 2$.

11.108. Encuentre: *a*) $\phi(10)$; *b*) $\phi(12)$; *c*) $\phi(15)$; *d*) $\phi(3^7)$; *e*) $\phi(5^6)$; *f*) $\phi(2^4 \cdot 7^6 \cdot 13^3)$.

11.109 Encuentre el número de enteros positivos menores que 3 200 que son coprimos con 8 000.

11.110 Considere una columna arbitraria en el arreglo S en la figura 11-7, que consiste de los números:

$$k, a + k, 2a + k, 3a + k, \ldots, (b - 1)a + k$$

Demuestre que estos b enteros constituyen un sistema de residuos completo módulo b.

ARITMÉTICA MÓDULO m, $\mathbf{Z}_m$

11.111 Escriba las tablas de suma y multiplicación para: *a*) $\mathbf{Z}_2$; *b*) $\mathbf{Z}_8$.

11.112 En $\mathbf{Z}_{12}$, encuentre: *a*) $-2, -3, -5, -9, -10, -11$; *b*) $2/9, 4/9, 5/9, 7/9, 8/9$.

11.113 En $\mathbf{Z}_{17}$, encuentre: *a*) $-3, -5, -6, -8, -13, -15, -16$; *b*) $3/8, 5/8, 7/8, 13/8, 15/8$.

11.114 Encuentre a^{-1} en $\mathbf{Z}_m$, donde (*a*) $a = 15$, $m = 127$; *b*) $a = 61$, $m = 124$; *c*) $a = 12$, $m = 111$.

11.115 Encuentre el producto $f(x)g(x)$ para los siguientes polinomios sobre $\mathbf{Z}_5$:

$$f(x) = 4x^3 - 2x^2 + 3x - 1,\ g(x) = 3x^2 - x - 4$$

ECUACIONES DE CONGRUENCIA

11.116 Resuelva cada una de las siguientes ecuaciones de congruencia:

a) $f(x) = 2x^3 - x^2 + 3x + 1 \equiv 0$ (mód 5)
b) $g(x) = 3x^4 - 2x^3 + 5x^2 + x + 2 \equiv 0$ (mód 7)
c) $h(x) = 45x^3 - 37x^2 + 26x + 312 \equiv 0$ (mód 6)

11.117 Resuelva cada una de las siguientes ecuaciones lineales de congruencia:

a) $7x \equiv 3$ (mód 9); *b*) $4x \equiv 6$ (mód 14); *c*) $6x \equiv 4$ (mód 9).

11.118 Resuelva cada una de las siguientes ecuaciones lineales de congruencia:

a) $5x \equiv 3$ (mód 8); *b*) $6x \equiv 9$ (mód 16); *c*) $9x \equiv 12$ (mód 21).

11.119 Resuelva cada una de las siguientes ecuaciones lineales de congruencia: *a*) $37x \equiv 1$ (mód 249); *b*) $195x \equiv 23$ (mód 968).

11.120 Resuelva cada una de las siguientes ecuaciones lineales de congruencia: *a*) $132x \equiv 169$ (mód 735); *b*) $48x \equiv 284$ (mód 356)

11.121 El aforo de un teatro de marionetas es de sólo 60 butacas. La admisión al teatro es de \$2.25 por adulto y \$1.00 por niño. Suponga que de entradas se reunieron \$117.25. Encuentre el número de adultos y de niños que asistieron a la función.

11.122 Un muchacho vende manzanas a 12 centavos cada una y peras a 7 centavos cada una. Suponga que el muchacho reunió \$3.21. Encuentre el número de manzanas y peras que vendió.

11.123 Encuentre la menor solución posible de cada sistema de ecuaciones de congruencia:

a) $x \equiv 2$ (mód 3), $x \equiv 3$ (mód 5), $x \equiv 4$ (mód 11)
b) $x \equiv 3$ (mód 5), $x \equiv 4$ (mód 7), $x \equiv 6$ (mód 9)
c) $x \equiv 5$ (mód 45), $x \equiv 6$ (mód 49), $x \equiv 7$ (mód 52)

Respuestas a los problemas suplementarios

11.61 *a*) $2 > -6$; *b*) $-3 > -5$; *c*) $-7 < 3$; *d*) $-8 < -1$; *e*) $23 < 11$; *f*) $23 > -9$; *g*) $-2 > -7$; *h*) $4 > -9$

11.62 *a*) 4, 4, 10; *b*) $3 + 10 = 13$, $3 - 7 = -4$; *c*) $4 + 1 = 5$, $8 - 4 = 4$.

11.63 *a*) 7; *b*) 9; *c*) 6; *d*) 6; *e*) 6; *f*) 2.

11.64 *a*) 4, 5, 6; *b*) $-2, -1, 0, 1$.

11.79 *a*) $q = -15$, $r = 13$; *b*) $q = -24$, $r = 10$. *c*) $q = 53$, $r = 7$.

11.81 *a*) Uno es divisible entre 2 y el otro es divisible entre 3. *b*) Uno es divisible entre 4, otro es divisible entre 2 y uno es divisible entre 3.

11.84 *a*) 1, 2, 3, 4, 6, 8, 12, 24; *b*) 3^n para $n = 0$ a 9; *c*) 2^r3^s para $r = 0$ a 4 y $s = 0$ a 3.

11.85 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

11.86 *a*) $2\,940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; *b*) $1\,485 = 3^3 \cdot 5 \cdot 11$; *c*) $8\,712 = 2^3 \cdot 3^2 \cdot 11^2$; *d*) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$.

11.87 *a*) $d = 4 = 5(356) - 37(48)$; *b*) $d = 33 = 8(165) - 1(1287)$; *c*) $d = 42 = 14(168) - 1(2310)$; *d*) $d = 1 = 139(195) - 28(968)$; *e*) $11(249) - 74(37)$.

11.88 *a*) 35; *b*) 33; *c*) 84.

11.89 *a*) $a = 2^3 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$; *b*) $\text{mcd}(a, b) = 2^2 \cdot 3 \cdot 7$, $\text{mcm}(a, b) = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 = 1, 164, 240$.

11.94 Sugerencia: $a^k - 1 = (a-1)(1 + a + a2 + \cdots + a^k - 1)$; *b*) Sugerencia: $n = ab$, entonces $2^{n-1} = (2^a)^b - 1$.

11.98 $(k + 1)! + 2$, $(k + 1)! + 3$, $(k + 1)! + 4, \ldots, (k+ 1)! + (k + 1)$ son divisibles entre 2, 3, $4, \ldots, k + 1$, respectivamente.

11.99 *a*) Falsa; *b*) verdadera; *c*) falsa; *d*) falsa.

11.100 *a*) 7; *b*) 3; *c*) 3; *d*) 6.

11.l01 *a*) -2; *b*) -3; *c*) -4; *d*) 1.

11.102 4, 15, 26, 37, 48, 59, 70, 81, 92.

11.103 $-42, -33, -24, -15, -6$, 3, 12, 21, 30, 39, 48.

11.104 *a*) $\{0, 1, \ldots, 10\}$ y $\{-5, -4, \ldots, -1, 0, 1, \ldots, 4, 5)$. *b*) $\{0, 1, \ldots, 13\}$ y $\{-6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$.

11.105 *a*) {1, 3}; *b*) $\{1, 2, \ldots, 10\}$; *c*) {1, 3, 5, 9, 11,13}; *d*) {1, 2, 4, 7, 8, 11, 13, 14}.

11.106 *a*) {5, l0, 15, 20, 25, 30, 35, 40}; (*b*) {3, 9, 27, 81, 243, 729, 2 187, 6 561}.

11.107 $m - 1 \equiv -1 \pmod{m}$ y así $(m - 1)2 \equiv 1 \pmod{m}$.

11.108 *a*) 4; *b*) 4; *c*) = 8; *d*) 2(36); *e*) 4(55); *f*) $(2^3)(6 \cdot 7^5)(12 \cdot 13^2)$.

11.109 $\phi(8\ 000) = \phi(2^5 \cdot 5^2) = 2^4 \cdot 4 \cdot 5 = 320$. Por tanto $s = 4(320) = 1\ 280$.

11.112 *a*) 11, 10, 8, 4, 3, 2; *b*) 6, 12, 2, 8, 11.

11.113 *a*) 14, 12, 11, 9, 4, 2; *b*) 11, 7, 3, 8, 4.

11.114 *a*) 17; *b*) 61; *c*) a^{-1} no existe.

11.115 $2x^5 + 2x^2 - x + 4$.

11.116 *a*) 1, 3, 4; *b*) 2, -2; *c*) 0, 2, 3, -1.

11.117 *a*) 3; *b*) 5, 12; *c*) no hay solución.

11.118 *a*) 7; *b*) no hay solución; *c*) 6, 13, 20.

11.119 *a*) 175; *b*) 293.

11.120 *a*) no hay solución; *b*) 43, 132, 221, 310.

11.121 49 adultos, 7 niños.

11.122 25 manzanas, 3 peras; 18 manzanas, 15 peras; 11 manzanas, 27 peras; o 4 manzanas, 39 peras.

11.123 *a*) 158; *b*) 1(123); *c*) 3l 415.

12 CAPÍTULO Lenguajes, autómatas, gramáticas

12.1 INTRODUCCIÓN

En este capítulo se estudian tres temas que tienen una estrecha relación entre sí: *lenguajes*, *autómatas* y *gramáticas*. En los lenguajes que se usan aquí se utilizan las letras $a, b, \ldots$ para codificar los datos, a diferencia de los dígitos 0 y 1 que se usan en otros textos.

12.2 ALFABETO, PALABRAS, SEMIGRUPO LIBRE

Considere un conjunto A de símbolos no vacío, en el que una *palabra* o *cadena* w sobre el conjunto A es una secuencia finita de sus elementos. Por ejemplo, suponga $A = \{a, b, c\}$. Entonces las siguientes secuencias son palabras sobre A:

$$u = ababb \quad \text{y} \quad v = accbaaa$$

Cuando se analizan palabras sobre A, a menudo A se denomina *alfabeto* y sus elementos, *letras*. También se abrevia la notación y se escribe a^2 por aa, a^3 por aaa, etc.; de modo que la secuencia anterior de palabras queda como $u = abab^2$ y $v = ac^2ba^3$.

La secuencia vacía de letras, que se denota con λ (letra griega lambda) o con ϵ (letra griega épsilon) o 1, también se considera una palabra sobre A, que se denomina *palabra vacía*. El conjunto de todas las palabras sobre A se denota por A^* (que se lee: "A estrella").

La *longitud* de una palabra u, que se escribe $|u|$ o $l(u)$, es el número de elementos en su secuencia de letras. Para las palabras anteriores u y v, se tiene $l(u) = 5$ y $l(v) = 7$. También, $l(\lambda) = 0$, donde λ es la palabra vacía.

Observación: A menos que se establezca otra cosa, el alfabeto A es finito, los símbolos u, v, w se reservan para palabras sobre A y los elementos de A provienen de las letras a, b, c.

Concatenación

Considere dos palabras u y v sobre el alfabeto A. La *concatenación* de u y v, que se escribe uv, es la palabra que se obtiene al escribir las letras de u seguidas de las letras de v. Por ejemplo, para las palabras anteriores u y v, se tiene

$$uv = ababbaccbaaa = abab^2\, ac^2\, ba^3$$

Así como ocurre con las letras, para cualquier palabra u se define $u^2 = uu$, $u^3 = uuu$, y, en general, $u^{n+1} = uu^n$.

Resulta evidente que para palabras arbitrarias u, v, w, las palabras $(uv)w$ y $u(vw)$ son idénticas, ya que consta sólo de las letras u, v y w escritas una después de la otra. También, al adjuntar la palabra vacía antes o después de una palabra u no se modifica la palabra u. Es decir:

Teorema 12.1: La operación concatenación para palabras sobre un alfabeto A es asociativa. La palabra vacía λ es un elemento identidad para la operación.

(En términos generales, la operación no es conmutativa; por ejemplo, $uv \neq vu$ para las palabras anteriores u y v.)

Subpalabras, segmentos iniciales

Considere cualquier palabra $u = a_1a_2\ldots a_n$ sobre un alfabeto A. Cualquier secuencia $w = a_j\, a_{j+1}\ldots a_k$ se denomina *subpalabra* de u. En particular, la subpalabra $w = a_1a_2\ldots a_k$ que empieza con la primera letra de u, se denomina *segmento inicial* de u. En otras palabras, w es una subpalabra de u si $u = v_1wv_2$ y w es un segmento inicial de u si $u = wv$. Observe que ambas λ y u son subpalabras de uv puesto que $u = \lambda u$.

Considere la palabra $u = abca$. Las subpalabras y los segmentos iniciales de u son los siguientes:

1) Subpalabras: λ, a, b, c, ab, bc, ca, abc, bca, $abca = u$
2) Segmentos iniciales: λ, a, ab, abc, $abca = u$

Observe que la subpalabra $w = a$ aparece en dos sitios en u. La palabra ac no es una subpalabra de u, aun cuando todas sus letras pertenecen a u.

Semigrupo libre, monoide libre

Sea F el conjunto de todas las palabras no vacías de un alfabeto A con la operación de concatenación. Como ya se observó, la operación es asociativa. Por tanto, F es un semigrupo; se denomina *semigrupo libre sobre A*, o *semigrupo libre generado por A*. Resulta fácil demostrar que F satisface las leyes de cancelación por la izquierda y por la derecha. Sin embargo, F no es conmutativa cuando A tiene más de un elemento. Cuando se desea especificar el conjunto A, para el semigrupo libre sobre A se escribe F_A.

Ahora, sea $M = A^*$ el conjunto de todas las palabras de A incluso la palabra vacía λ. Puesto que λ es un elemento identidad para la operación de concatenación, M es un monoide, denominado *monoide libre* sobre A.

12.3 LENGUAJES

Un *lenguaje* L sobre un alfabeto A es una colección de palabras sobre A. Recuerde que A^* denota el conjunto de todas las palabras sobre A. Así, un lenguaje L es simplemente un subconjunto de A^*.

EJEMPLO 12.1 Sea $A = \{a, b\}$. Algunos lenguajes sobre A son los siguientes.

$$a)\ L_1 = \{a, ab, ab^2, \ldots\} \qquad c)\ L_3 = \{a^mb^m \mid m > 0\}$$
$$b)\ L_2 = \{a^mb^n \mid m > 0, n > 0\} \qquad d)\ L_4 = b^mab^n \mid m \geq 0, n \geq 0\}$$

La descripción verbal de estos lenguajes es:

a) L_1 consta de todas las palabras que empiezan con una a seguida de cero o más b.

b) L_2 consta de todas las palabras que empiezan con una o más a seguidas de una o más b.

c) L_3 consta de todas las palabras que empiezan con una o más a seguidas por el mismo número de b.

d) L_4 consta de todas las palabras que tienen exactamente una a.

Operaciones sobre los lenguajes

Suponga que L y M son lenguajes sobre un alfabeto A. Entonces la "concatenación" de L y M, que se denota por LM, es el lenguaje definido como sigue:

$$LM = \{uv \mid u \in L, v \in V\}$$

Es decir, LM denota el conjunto de todas las palabras que provienen de la concatenación de una palabra de L con una de M. Por ejemplo, suponga que

$$L_1 = \{a, b^2\}, \quad L_2 = \{a^2, ab, b^3\}, \quad L_3 = \{a^2, a^4, a^6, \ldots\}$$

Entonces:

$$L_1L_1 = \{a^2, ab^2, b^2a, b^4\}, \quad L_1L_2 = \{a^3, a^2b, ab^3, b^2a^2, b^2ab, b^5\}$$
$$L_1L_3 = \{a^3, a^5, a^7, \ldots, b^2a^2, b^2a^4, b^2a^6, \ldots\}$$

Resulta evidente que la concatenación de lenguajes es asociativa, ya que la concatenación de palabras es asociativa.

Las *potencias* de un lenguaje L se definen como sigue:

$$L^0 = \{\lambda\}, \quad L^1 = L, \quad L^2 = LL, \quad L^{m+1} = L^mL \quad \text{para} \quad m > 1$$

La operación unaria L^* (que se lee "L estrella") de un lenguaje L, que se denomina *cerradura de Kleene* de L porque Kleene demostró el teorema 12.2, que se define como la unión infinita:

$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots = \bigcup_{k=0}^{\infty} L^k$$

La definición de L^* coincide con la notación A^*, que consta de todas las palabras sobre A. Algunos textos definen L^+ como la unión de $L^1, L^2, \ldots$ es decir, L^+ es lo mismo que L^*, aunque sin la palabra vacía λ.

12.4 EXPRESIONES REGULARES, LENGUAJES REGULARES

Sea A un alfabeto (no vacío). En esta sección se definen una expresión regular r sobre A y un lenguaje $L(r)$ sobre A en asociación con la expresión regular r. La expresión r y su lenguaje correspondiente $L(r)$ se definen inductivamente como sigue.

Definición 12.1: Cada una de las siguientes expresiones es regular sobre un alfabeto A.

1) El símbolo "λ" (palabra vacía) y el par "()" (expresión vacía) son expresiones regulares.
2) Cada letra a en A es una expresión regular.
3) Si r es una expresión regular, entonces (r^*) es una expresión regular.
4) Si r_1 y r_2 son expresiones regulares, entonces $(r_1 \vee r_2)$ es una expresión regular.
5) Si r_1 y r_2 son expresiones regulares, entonces (r_1r_2) es una expresión regular.

Todas las expresiones regulares se forman de esta manera.

Observe que una expresión regular r es un tipo especial de palabra (cadena) que usa las letras de A y los cinco símbolos:

$$(\quad) \quad * \quad \vee \quad \lambda$$

Se recalca que ningún otro símbolo se usa para las expresiones regulares.

Definición 12.2: El lenguaje $L(r)$ sobre A que define una expresión regular r sobre A es:

1) $L(\lambda) = \{\lambda\}$ y $L((\,)) = \varnothing$, el conjunto vacío.
2) $L(a) = \{a\}$. donde a es una letra en A.

3) $L(r^*) = (L(r))^*$ (la cerradura de Kleene de $L(r)$).

4) $L(r_1 \vee r_2) = L(r_1) \cup L(r_2)$ (la unión de los lenguajes).

5) $L(r_1 r_2) = L(r_1)L(r_2)$ (la concatenación de los lenguajes).

Observación: Cuando es posible, en las expresiones regulares se omiten los paréntesis. Puesto que la concatenación de lenguajes y la unión de lenguajes son asociativas, es posible omitir muchos de los paréntesis. También, al adoptar la convención de que "*" tiene precedencia sobre la concatenación y ésta a su vez tiene precedencia sobre "$\vee$," es posible omitir otros paréntesis.

Definición 12.3: Sea L un lenguaje sobre A. Entonces L se denomina *lenguaje regular* sobre A si existe una expresión regular r sobre A tal que $L = L(r)$.

EJEMPLO 12.2 Sea $A = \{a, b\}$. Cada una de las siguientes es una expresión r y su lenguaje correspondiente es $L(r)$:

a) Sea $r = a^*$. Entonces $L(r)$ consta de todas las potencias de a incluso la palabra vacía λ.

b) Sea $r = aa^*$. Entonces $L(r)$ consta de todas las potencias positivas de a excepto la palabra vacía λ.

c) Sea $r = a \vee b^*$. Entonces $L(r)$ consta de a o de cualquier palabra en b; es decir, $L(r) = \{a, \lambda, b, b^2, \cdots\}$.

d) Sea $r = (a \vee b)^*$. Observe que $L(a \vee b) = \{a\} \cup \{b\} = A$; por tanto, $L(r) = A^*$, todas las palabras sobre A.

e) Sea $r = (a \vee b)^*bb$. Entonces $L(r)$ consta de la concatenación de cualquier palabra en A con bb; es decir, todas las palabras que terminan en b^2.

f) Sea $r = a \wedge b^*$. $L(r)$ no existe puesto que r no es una expresión regular. (En este caso $\wedge$ no es uno de los símbolos que se usan para expresiones regulares.)

EJEMPLO 12.3 Considere los siguientes lenguajes sobre $A = \{a, b\}$.

a) $L_1 = \{a^m b^n \mid m > 0, n > 0\}$; *b*) $L_2 = \{b^m a b^n \mid m > 0, n > 0\}$; *c*) $L_3 = \{a^m b^m \mid m > 0\}$.

Encontrar una expresión regular r sobre $A = \{a, b\}$ tal que $L_i = L(r)$ para $i = 1, 2, 3$.

a) L_1 consta de aquellas palabras que empiezan con una o más a seguidas por una o más b. Por tanto, $r = aa^*bb^*$. Observe que r no es única; por ejemplo, $r = a^*abb^*$ es otra solución.

b) L_2 consta de todas las palabras que empiezan con una o más b seguidas por una sola a que luego es seguida por una o más b; es decir, todas las palabras que contienen exactamente una a que no es la primera o la última letra. Por tanto, $r = bb^*abb^*$ es una solución.

c) L_3 consta de todas las palabras que empiezan con una o más a seguidas por el mismo número de b. No existe ninguna expresión regular r tal que $L_3 = L(r)$; es decir, L_3 no es un lenguaje regular. La demostración de este hecho se proporciona en el ejemplo 12.8.

12.5 AUTÓMATAS DE ESTADO FINITO

Un *autómata de estado finito* (*finite state automaton*, FSA) o, simplemente, un *autómata M*, consta de cinco partes:

1) Un conjunto finito (alfabeto) A de datos de entrada.

2) Un conjunto finito S de estados (internos).

3) Un subconjunto Y de S (que se denominan estados de aceptación o estados "sí").

4) Un estado inicial s_0 en S.

5) Una función F de estado siguiente de $S \times A$ en S.

Un autómata M así se denota por $M = (A, S, Y, s_0, F)$ cuando se quieren indicar sus cinco partes.

En algunos textos la función de estado siguiente se define $F : S \times A \to S$ en (5) por medio de una colección de funciones $f_a : S \to S$, una para cada $a \in A$. Al hacer $F(s, a) = f_a(s)$ se demuestra que ambas definiciones son equivalentes.

EJEMPLO 12.4 A continuación se define un autómata M con dos símbolos de entrada y tres estados:

1) $A = \{a, b\}$, símbolos de entrada.

2) $S = \{s_0, s_1, s_2\}$, estados internos.

3) $Y = \{s_0, s_1\}$, estados "sí".

4) s_0, estado inicial.

5) La función de estado siguiente $F : S \times A \to S$ que se define explícitamente en la figura 12-1*a*) o en la tabla de la figura 12-1*b*).

$$F(s_0, a) = s_0,\ F(s_1, a) = s_0,\ F(s_2, a) = s_2$$
$$F(s_0, b) = s_1,\ F(s_1, b) = s_2,\ F(s_2, b) = s_2$$

a)

F	a	b
s_0	s_0	s_1
s_1	s_0	s_2
s_2	s_2	s_2

b)

Figura 12-1

Diagrama de estado de un autómata *M*

A un autómata M se le define por su diagrama de estado $D = D(M)$, en lugar de enumerar sus cinco partes. El diagrama de estado $D = D(M)$ es una gráfica dirigida etiquetada como sigue.

1) Los vértices de $D(M)$ son los estados en S y un estado de aceptación se denota por medio de un círculo doble.

2) Hay una flecha (arista dirigida) en $D(M)$ del estado s_j al estado s_k identificada por una entrada a si $F(s_j, a) = s_k$ o, en forma equivalente, si $f_a(s_j) = s_k$.

3) El estado inicial s_0 se indica por medio de una flecha especial que termina en s_0 pero que, en cambio, no tiene vértice inicial.

Para cada vértice s_j y cada letra a en el alfabeto A, hay una flecha identificada por a que sale de s_j; por tanto, el grado de salida de cada vértice es igual al número de elementos en A. Por conveniencia en la notación, una sola flecha identifica todas las entradas que ocasionan el mismo cambio de estado, en lugar de tener una flecha para cada una de tales entradas.

El diagrama de estado $D = D(M)$ del autómata M en el ejemplo 12.4 se muestra en la figura 12-2. Observe que tanto a como b identifican la flecha que va de s_2 a s_2 puesto que $F(s_2, a) = s_2$ y $F(s_2, b) = s_2$; también que el grado de salida de cada vértice es 2, el número de elementos en A.

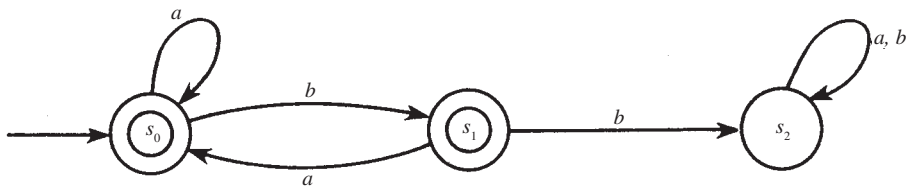


Figura 12-2

El autómata *M* determina el lenguaje *L*(*M*)

Cada autómata M con alfabeto de entrada A define un lenguaje sobre A, que se denota con $L(M)$, como sigue.

Sea $w = a_1a_2 \cdots a_m$ una palabra sobre A. Entonces, w determina la siguiente ruta en la gráfica del diagrama de estado $D(M)$, donde s_0 es el estado inicial y $F(s_{i-1}, a_i) = s_i$ para $i \geq 1$:

$$P = (s_0, a_1, s_1, a_2, s_2, \cdots, a_m, s_m)$$

Se dice que M *reconoce* la palabra w si el estado final s_m es un estado de aceptación en Y. El lenguaje $L(M)$ de M es la colección de todas las palabras de A que M acepta.

EJEMPLO 12.5 Determine si el autómata M en la figura 12-2 acepta o no las palabras:

$$w_1 = ababba; \quad w_2 = baab; \quad w_3 = \lambda \text{ la palabra vacía.}$$

Para obtener los siguientes caminos respectivos se usan la figura 12-2 y las palabras w_1 y w_2:

$$P_1 = s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{b} s_2 \xrightarrow{a} s_2 \quad \text{y} \quad P_2 = s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1$$

El estado final en P_1 es s_2, que no está en Y; por tanto, w_1 no es aceptada por M. Por otra parte, el estado final en P_2 es s_1, que está en Y; por tanto, w_2 es aceptada por M. El estado final determinado por w_3 es el estado inicial s_0, puesto que $w_3 = \lambda$ es la palabra vacía. Así, w_3 es aceptada por M puesto que $s_0 \in Y$.

EJEMPLO 12.6 El lenguaje $L(M)$ del autómata M se describe en la figura 12-2.

$L(M)$ consta de todas las palabras w sobre A que no tienen dos b consecutivas. Esto se debe a los hechos siguientes:

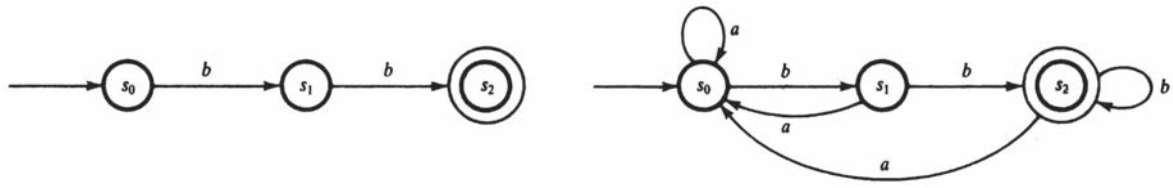
1) El estado s_2 se introduce si y sólo si hay dos b consecutivas.
2) Nunca es posible dejar s_2.
3) El estado s_2 es el único estado de rechazo (no aceptación).

La relación fundamental entre los lenguajes regulares y los autómatas aparece en el siguiente teorema (cuya demostración rebasa el alcance de este texto).

Teorema 12.2 (de Kleene): Un lenguaje L sobre un alfabeto A es regular si y sólo si existe un autómata de estado finito M tal que $L = L(M)$.

La operación estrella L^* sobre un lenguaje L a veces se denomina cerradura de Kleene de L, ya que Kleene fue el primero en demostrar el resultado fundamental anterior.

EJEMPLO 12.7 Sea $A = \{a, b\}$. Construya un autómata M que acepte precisamente las palabras de A que terminan en dos b.



a) *b*)

Figura 12-3

Puesto que b^2 es aceptada, pero no λ o b, se requieren tres estados: s_0, el estado inicial, y s_1 y s_2 con una flecha identificada por b que va de s_0 a s_1 y una de s_1 a s_2. Además s_2 tiene un estado de aceptación, pero s_0 no, tampoco s_1. Así se obtiene la gráfica en la figura 12-3*a*). Por otra parte, si hay una a, entonces es recomendable retroceder a s_0, y si se está en s_2 y hay una b, entonces es recomendable permanecer en s_2. Estas condiciones adicionales proporcionan el autómata requerido M, que se muestra en la figura 12-3*b*).

Lema de bombeo

Sea M un autómata sobre A con k estados. Suponga que $w = a_1a_2 \cdots a_n$ es una palabra sobre A aceptada por M y suponga que $|w| = n > k$, el número de estados. Sea

$$P = (s_0, s_1, \ldots, s_n)$$

la secuencia correspondiente de los estados que determina la palabra w. Puesto que $n > k$, deben ser iguales dos de los estados en P, por ejemplo, $s_i = s_j$ donde $i < j$. Sean x, y, z las subpalabras en que se dividió w:

$$x = a_1a_2 \cdots a_i, \quad y = a_{i+1} \cdots a_j, \quad z = a_{j+1} \cdots a_n$$

Como se muestra en la figura 12-4, xy termina en $s_i = s_j$; por tanto, xy^m también termina en s_i. Así, para cualquier m, $w_m = xy^mz$ termina en s_n, que es un estado de aceptación.

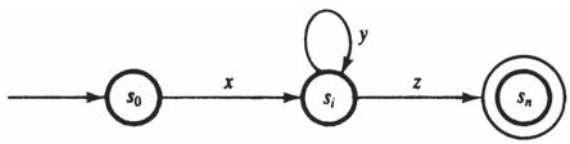


Figura 12-4

El análisis anterior demuestra el siguiente resultado importante.

Teorema 12.3 (lema de bombeo): Suponga que M es un autómata M sobre A tal que:
i) M tiene k estados. *ii*) M acepta una palabra w de A donde $|w| >$ k. Entonces $w = xyz$, donde, para cualquier m positivo, m, $w_m = xy^mz$ lo acepta M.

El siguiente ejemplo constituye una aplicación del lema de bombeo.

EJEMPLO 12.8 Demuestre que el lenguaje $L = \{a^mb^m \mid m \text{ es positivo}\}$ no es regular.

Se supone que L es regular. Entonces, por el teorema 12.2, existe un autómata de estado finito M que acepta a L. Se supone que M tiene k estados. Sea $w = a^kb^k$. Entonces $|w| > k$. Por el lema de bombeo (teorema 12.3), $w = xyz$, donde y no es vacía y $w_2 = xy^2z$ también es aceptada por M. Si y consta sólo de a o sólo de b, entonces w^2 no tiene el mismo número de a que de b. Si y consta tanto de a como de b, entonces w_2 tendrá a después de las b. En cualquier caso, w_2 no pertenece a L, lo que es una contradicción. Por tanto, L no es regular.

12.6 GRAMÁTICAS

En la figura 12-5 se muestra la construcción gramatical de una oración específica. Observe que hay:

1) varias variables; por ejemplo (oración), (frase nominal),…;
2) varias palabras terminales; por ejemplo, "El", "muchacho",…;
3) una variable inicial (oración);
4) varias sustituciones o producciones; por ejemplo,

$$\begin{aligned} \langle \textit{oración} \rangle &\rightarrow \langle \textit{ frase nominal} \rangle \langle \textit{verbo frase} \rangle \\ \langle \textit{ frase objetual} \rangle &\rightarrow \langle \textit{artículo} \rangle \langle \textit{sustantivo} \rangle \\ \langle \textit{sustantivo} \rangle &\rightarrow \langle \textit{manzana} \rangle \end{aligned}$$

La oración final sólo contiene terminales, aunque aparecen tanto variables como terminales en su construcción por las producciones. La descripción intuitiva se proporciona a fin de motivar la siguiente definición de una gramática y el lenguaje que genera.

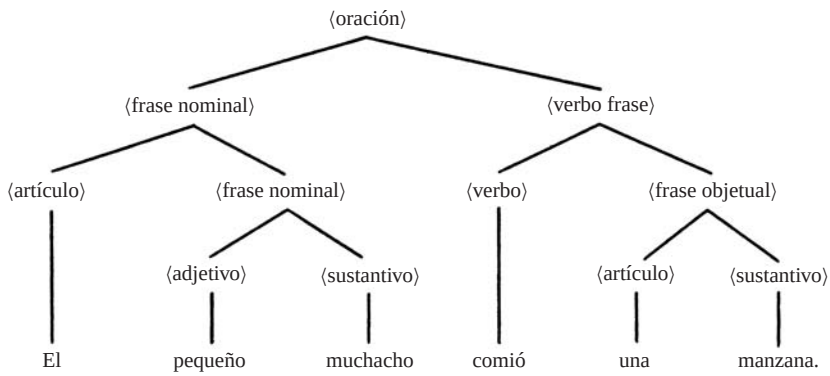


Figura 12-5

Definición 12.4: Una *gramática de estructura de frases* o, simplemente, una *gramática G*, consta de cuatro partes:

1) Un conjunto finito (vocabulario) V.
2) Un subconjunto T de V cuyos elementos se denominan *terminales*; los elementos de $N = V \setminus T$ se denominan *no terminales* o *variables*.
3) Un símbolo no terminal S se denomina símbolo *inicial*.
4) Un conjunto finito P de producciones. (Una producción es un par ordenado (α, β), que suele escribirse $\alpha \rightarrow \beta$, donde α y β son palabras en V, y la producción debe contener por lo menos una α no terminal en su miembro izquierdo.)

Una gramática G así se denota por $G = G(V, T, S, P)$ cuando se quieren indicar sus cuatro partes.

La siguiente notación, a menos que se establezca o implique otra cosa, se usa para las gramáticas en este texto. Los terminales se indican con minúsculas cursivas $a, b, c, \cdots$, y los no terminales se indican con mayúsculas cursivas $A, B, C, \cdots$, con S como símbolo inicial. También, las letras griegas $\alpha, \beta, \cdots$, denotan palabras en V; es decir, palabras en terminales y no terminales. Además, se escribe

$$\alpha \rightarrow (\beta_1, \beta_2, \cdots, \beta_k) \quad \text{en lugar de} \quad \alpha \rightarrow \beta_1, \alpha \rightarrow \beta_2, \cdots, \alpha \rightarrow \beta_k$$

Observación: A menudo una gramática G se define al proporcionar sólo sus producciones, se supone que S es el símbolo inicial y que los terminales y no terminales de G son sólo los que aparecen en las producciones.

EJEMPLO 12.9 A continuación se define una gramática G con S como símbolo inicial:

$$V = \{A, B, S, a, b\}, \quad T = \{a, b\}, \quad P = \{S \xrightarrow{1} AB,\ A \xrightarrow{2} Aa,\ B \xrightarrow{3} Bb,\ A \xrightarrow{4} a,\ B \xrightarrow{5} b\}$$

Las producciones pueden abreviarse como sigue: $S \to AB, A \to (Aa, a), B \to (Bb, b)$.

Lenguaje $L(G)$ de una gramática G

Suponga que w y w' son palabras sobre el conjunto vocabulario V de una gramática G. Se escribe

$$w \Rightarrow w'$$

si w' puede obtenerse a partir de w mediante el uso de una de las producciones; es decir, si existen palabras u y v tales que $w = u\alpha v$ y $w' = u\beta v$ y hay una producción $\alpha \to \beta$. Además, se escribe

$$w \Rightarrow\Rightarrow w' \quad \text{o} \quad w \overset{*}{\Rightarrow} w'$$

si w' puede obtenerse a partir de w con un número finito de producciones.

Ahora, sea G una gramática con conjunto terminal T. El lenguaje de G, denotado por $L(G)$, consta de todas las palabras en T que pueden obtenerse a partir del símbolo inicial S mediante el proceso anterior; es decir,

$$L(G) = \{w \in T^* \mid S \Rightarrow\Rightarrow w\}$$

EJEMPLO 12.10 Considere la gramática G en el ejemplo 12.9. Observe que $w = a^2b^4$ puede obtenerse a partir del símbolo inicial S como sigue:

$$S \Rightarrow AB \Rightarrow AaB \Rightarrow aaB \Rightarrow aaBb \Rightarrow aaBbb \Rightarrow aaBbbb \Rightarrow aabbbb = a^2b^4$$

Aquí se han usado las producciones 1, 2, 4, 3, 3, 3, 5, respectivamente. Por tanto, es posible escribir $S \Rightarrow\Rightarrow a^2b^4$. Entonces, $w = a^2b^4$ pertenece a $L(G)$. En términos más generales, la secuencia de producciones:

$$1, 2\ (r \text{ veces}), 4, 3\ (s \text{ veces}), 5$$

produce la palabra $w = a^rab^sb$, donde r y s son enteros no negativos. Por otra parte, ninguna secuencia de producciones puede producir una a después de una b. En consecuencia,

$$L(G) = \{a^mb^n \mid m \text{ y } n \text{ son enteros positivos}\}$$

Es decir, el lenguaje $L(G)$ de la gramática G consta de todas las palabras que empiezan con una o más letras a seguidas por una o más b.

EJEMPLO 12.11 Encuentre el lenguaje $L(G)$ sobre $\{a, b, c\}$ generado por la gramática G:

$$S \to aSb, \quad aS \to Aa, \quad Aab \to c$$

Primero es necesario aplicar la primera producción una o más veces para obtener la palabra $w = a^nSb^n$, donde $n > 0$. Para eliminar S es necesario aplicar la segunda producción para obtener la palabra $w' = a^mAabb^m$, donde $m = n - 1 \geq 0$. Ahora sólo hay que aplicar la tercera producción para obtener finalmente la palabra $w' = a^mcb^m$, donde $m \geq 0$. En consecuencia,

$$L(G) = \{a^mcb^m \mid m \text{ es no negativo}\}$$

Es decir, $L(G)$ consta de todas las palabras con el mismo número no negativo de letras a y b separadas por a c.

Tipos de gramáticas

Las gramáticas se clasifican según los tipos de producción que se les permiten. La siguiente clasificación de gramáticas se debe a Noam Chomsky.

Una gramática tipo 0 no tiene restricciones en sus producciones. Los tipos 1, 2 y 3 se definen como sigue:

1) Una gramática G es de tipo 1 si cualquier producción es de la forma $\alpha \to \beta$, donde $|\alpha| \leq |\beta|$, o de la forma $\alpha \to \lambda$.

2) Una gramática G es de tipo 2 si cualquier producción es de la forma $A \to \beta$, donde el miembro izquierdo A es un no terminal.

3) Una gramática G es de tipo 3 si cualquier producción es de la forma $A \to a$ o $A \to aB$; es decir, donde el miembro izquierdo A es un no terminal simple y el miembro derecho es un terminal simple o un terminal seguido por un no terminal, o de la forma $S \to \lambda$.

Observe que las gramáticas constituyen una jerarquía; es decir, toda gramática tipo 3 es una gramática tipo 2, toda gramática tipo 2 es una gramática tipo 1 y toda gramática tipo 1 es una gramática tipo 0.

Las gramáticas también se clasifican en términos de sensibles al contexto, libres del contexto y regulares como sigue.

a) Una gramática es *sensible al contexto* si las producciones son de la forma

$$\alpha A \alpha' \to \alpha \beta \alpha'$$

La expresión "sensible al contexto" proviene del hecho de que es posible sustituir la variable A por β en una palabra sólo cuando A está entre α y α'.

b) Una gramática es *libre del contexto* si las producciones son de la forma

$$A \to \beta$$

La expresión "libre del contexto" proviene del hecho de que ahora es posible sustituir la variable A por β sin tomar en cuenta dónde aparece A.

c) Una gramática es *regular* si las producciones son de la forma

$$A \to a, \quad A \to aB, \quad S \to \lambda$$

Observe que una gramática libre del contexto es lo mismo que una gramática tipo 2, y que una gramática regular es lo mismo que una gramática tipo 3.

A continuación se presenta una relación fundamental entre gramáticas regulares y autómatas finitos.

Teorema 12.4: Una gramática tipo 3 (regular) puede generar un lenguaje L si y sólo si existe un autómata finito M que acepta a L.

Por tanto, un lenguaje L es regular ssi $L = L(r)$, donde r es una expresión regular ssi $L = L(M)$, donde M es un autómata finito ssi $L = L(G)$, donde G es una gramática regular. (Recuerde que "ssi" es una abreviatura de si y sólo si).

EJEMPLO 12.12 Considere el lenguaje $L = \{a^n b^n \mid n > 0\}$.

a) Encuentre una gramática G libre del contexto que genere a L.

Resulta evidente que la gramática G con las siguientes producciones genera a L:

$$S \to ab, \quad S \to aSb$$

Observe que G es libre del contexto.

b) Encuentre una gramática G regular que genere a L.

Por el ejemplo 12.8, L no es un lenguaje regular. Por tanto, L no puede ser generado por una gramática regular.

Árboles de derivación de gramáticas libres del contexto

Considere una gramática G libre del contexto (tipo 2). Cualquier derivación de una palabra w en $L(G)$ puede representarse gráficamente por medio de un árbol T con raíz ordenado, denominado *árbol de derivación* o *árbol de análisis sintáctico*. A continuación se ilustra un árbol de derivación de estas características.

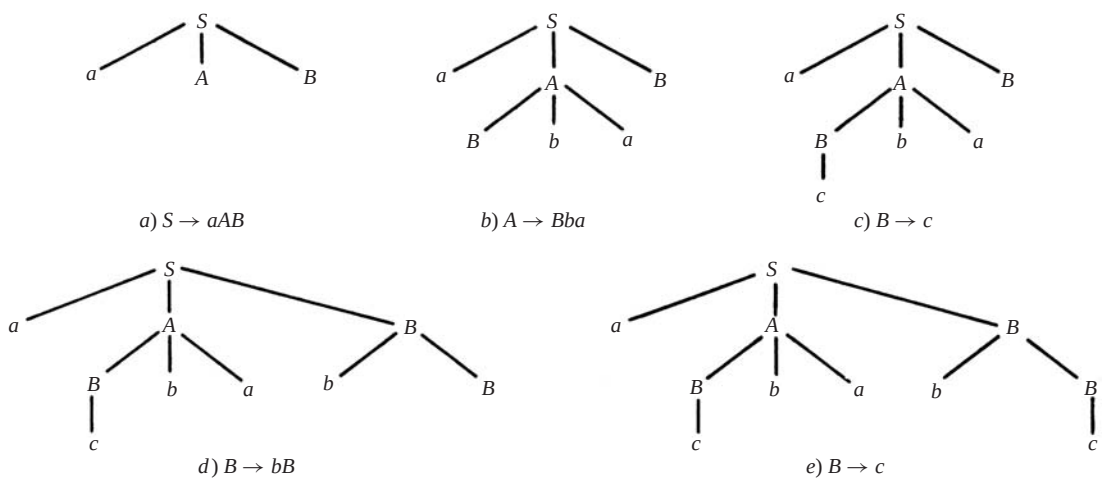
Sea G una gramática libre del contexto con las siguientes producciones:

$$S \to aAB \quad A \to Bba, \quad B \to bB, \quad B \to c$$

La palabra $w = acbabc$ puede derivarse a partir de S como sigue:

$$S \Rightarrow aAB \Rightarrow a(Bba)B \Rightarrow acbaB \Rightarrow acba(bB) \Rightarrow acbabc$$

El árbol de derivación T de la palabra w puede dibujarse como se indica en la figura 12-6. Se empieza con S como la raíz y luego se agregan ramas al árbol según la producción utilizada en la derivación de w. Así se obtiene el árbol T completo que se muestra en la figura 12-6*e*). La secuencia de hojas de izquierda a derecha en T es la palabra derivada w. También, cualquier no hoja en T es una variable; por ejemplo, A, y los sucesores inmediatos (hijos) de A forman una palabra α donde $A \to \alpha$ es la producción de G usada en la derivación de w.



a) $S \to aAB$ *b*) $A \to Bba$ *c*) $B \to c$

d) $B \to bB$ *e*) $B \to c$

Figura 12-6

Forma de Backus-Naur

Hay otra notación, que se denomina forma de Backus-Naur, que algunas veces se usa para describir las producciones de una gramática libre del contexto (tipo 2). Específicamente:

i) "::=" se usa en lugar de "$\to$".

ii) Cualquier no terminal se escribe entre corchetes $\langle\ \rangle$.

iii) Todas las producciones con el mismo miembro izquierdo no terminal se combinan en una proposición con todos los miembros derechos enumerados a la derecha de ::= separados por barras verticales.

Por ejemplo, las producciones $A \to aB, A \to b, A \to BC$ se combinan en una declaración:

$$\langle A \rangle ::= a\ \langle B \rangle\ |b|\ \langle B \rangle\ \langle C \rangle$$

Máquinas y gramáticas

El teorema 12.4 establece que los lenguajes regulares corresponden a los autómatas de estado finito (FSA). También hay máquinas, más poderosas que tales autómatas, que corresponden a las otras gramáticas.

a) **Autómatas con pila:** Un autómata con pila P es semejante a un autómata de estado finito, excepto que P tiene una pila auxiliar que proporciona una cantidad ilimitada de memoria para P. Un autómata con pila P reconoce un lenguaje L si y sólo si L es libre del contexto.

b) **Autómatas delimitados linealmente:** Un autómata B delimitado linealmente es más poderoso que un autómata con pila. Un autómata B así usa una cinta que está limitada linealmente por la longitud de la palabra de entrada w. Un autómata B delimitado linealmente reconoce un lenguaje L si y sólo si L es sensible al contexto.

c) **Máquina de Turing:** Una máquina M de Turing, denominada así en honor del matemático británico Alan Turing, usa una cinta infinita; es capaz de reconocer cualquier lenguaje L que pueda ser generado por cualquier gramática G con estructura de frase. De hecho, una máquina M de Turing es una de varias formas equivalentes de definir la idea de función "calculable".

El análisis de los autómatas con pila y los autómatas delimitados linealmente rebasa este texto. La máquina M de Turing se analizará en el capítulo 13.

PROBLEMAS RESUELTOS

PALABRAS

12.1 Considere las palabras $u = a^2ba^3b^2$ y $v = bab^2$. Encuentre: *a*) uv; $|uv|$; *b*) vu, $|vu|$; *c*) v^2, $|v^2|$.

Se escriben las letras de la primera palabra seguidas de las letras de la segunda palabra y, luego, se cuenta el número de letras en la palabra resultante.

a) $uv = (a^2ba^3b^2)(bab^2) = a^2ba^3b^3ab^2$; $|uv| = 12$

b) $vu = (bab^2)(a^2ba^3b^2) = bab^2a^2ba^3b^2$; $|vu| = 12$

c) $v^2 = vv = (bab^2)(bab^2) = bab^3ab^2$; $|v^2| = 8$

12.2 Suponga $u = a^2b$ y $v = b^3ab$. Encuentre *a*) uvu; *b*) λu, $u\lambda$, $u\lambda v$.

a) Se escriben las letras en u, luego en v y finalmente en u para obtener $uvu = a^2b^4aba^2b$.

b) Puesto que λ es la palabra vacía, $\lambda u = u\lambda = u = a^2b$ y $u\lambda v = uv = a^2b^4ab$.

12.3 Sea $w = abcd$. *a*) Encuentre todas las subpalabras de w. *b*) ¿Cuáles de ellas son segmentos iniciales?

a) Las subpalabras son λ, *a*, *b*, *c*, *d*, *ab*, *bc*, *cd*, *abc*, *bcd*, $w = abcd$. (Se recalca que $v = acd$ no es una subpalabra de w, aunque todas sus letras pertenecen a w.)

b) Los segmentos iniciales son λ, *a*, *ab*, *abc*, $w = abcd$.

12.4 Para palabras u y v arbitrarias, demuestre que: *a*) $|uv| = |u| + |v|$; *b*) $|uv| = |vu|$.

a) Suponga $|u| = r$ y $|v| = s$. Entonces uv consta de las r letras de u seguidas por las s letras de v; así $|uv| = r + s = |u| + |v|$.

b) Al usar *a*) se obtiene $|uv| = |u| + |v| = |v| + |u| = |vu|$.

12.5 Escribir la diferencia entre el semigrupo libre sobre un alfabeto A y el monoide libre sobre A.

El semigrupo libre sobre un A es el conjunto de todas las palabras en A bajo la operación de concatenación; no incluye la palabra vacía λ. Por otra parte, el monoide libre sobre A incluye la palabra vacía λ.

LENGUAJES

12.6 Sea $A = \{a, b\}$. Describa verbalmente los siguientes lenguajes sobre A (que son subconjuntos de A^*):

$a)$ $L_1 = \{(ab)^m \mid m > 0\}$; $b)$ $L_2 = \{a^r b a^s b a^t \mid r, s, t \geq 0\}$; $c)$ $L_3 = \{a^2 b^m a^3 \mid m > 0\}$.

$a)$ L_1 consta de las palabras $w = ababab \cdots ab$, es decir, que empiezan con a, alternan con b y terminan con b.

$b)$ L_2 consta de todas las palabras que contienen exactamente dos b.

$c)$ L_3 consta de todas las palabras que empiezan con a^2 y terminan con a^3 con una o más b entre ellas.

12.7 Sean $K = \{a, ab, a^2\}$ y $L = \{b^2, aba\}$ lenguajes sobre $A = \{a, b\}$. Encuentre $a)$ KL; $b)$ LL.

$a)$ Las palabras en K se concatenan con las palabras en L para obtener $KL = \{ab^2, a^2ba, ab^3, ababa, a^2b^2, a^3ba\}$.

$b)$ Las palabras en L se concatenan con las palabras en L para obtener $LL = \{b^4, b^2aba, abab^2, aba^2ba\}$.

12.8 Considere el lenguaje $L = \{ab, c\}$ sobre $A = \{a, b, c\}$. Encuentre: $a)$ L^0; $b)$ L^3; $c)$ L^{-2}

$a)$ $L^0 = \{\lambda\}$, por definición

$b)$ Se forman todas las secuencias de tres palabras de L para obtener:

$$L^3 = \{ababab, ababc, abcab, abc^2, cabab, cabc, c^2ab, c^3\}$$

$c)$ La potencia negativa de un lenguaje no está definida.

12.9 Sea $A = \{a, b, c\}$. Encuentre L^*, donde $a)$ $L = \{b^2\}$; $b)$ $L = \{a, b\}$; $c)$ $L = \{a, b, c^3\}$.

$a)$ L^* consta de todas las palabras b^n, donde n es par (incluso la palabra vacía λ).

$b)$ L^* consta de palabras con a y b.

$c)$ L^* consta de todas las palabras de A con la propiedad de que la longitud de cada palabra máxima compuesta completamente de c es divisible entre 3.

12.10 Considere un alfabeto numerable $A = \{a_1, a_2, \ldots\}$. Sea L_k el lenguaje sobre A que consta de las palabras w tales que la suma de los subíndices de las letras en w es igual a k. (Por ejemplo, $w = a_2a_3a_3a_6a_4$ pertenece a L_{18}.) $a)$ Encuentre L_4. $b)$ Demuestre que L_k es finito. $c)$ Demuestre que A^* es numerable. $d)$ Demuestre que cualquier lenguaje sobre A es numerable.

$a)$ Ninguna palabra en L_4 puede tener más de cuatro letras y no puede usarse ninguna letra a_n con $n > 4$.
Por tanto, se obtiene la siguiente lista:

$$a_1a_1a_1a_1, \quad a_1a_1a_2, \quad a_1a_2a_1, \quad a_2a_1a_1, \quad a_1a_3, \quad a_3a_1, \quad a_2a_2, \quad a_4$$

$b)$ En L_k sólo es posible usar un número finito de las a; es decir, $a_1, a_2, \ldots, a_k$ y ninguna palabra en L_k puede tener más de k letras. Por tanto, L_k es finito.

$c)$ A^* es la unión numerable de los conjuntos finitos L_k; por tanto, A^* es numerable.

$d)$ L es un subconjunto del conjunto numerable A^*; por tanto, L también es numerable.

EXPRESIONES REGULARES, LENGUAJES REGULARES

12.11 Sea $A = \{a, b\}$. Describa el lenguaje $L(r)$ donde:

$a)$ $r = abb^*a$; $b)$ $r = b^*ab^*ab^*$; $c)$ $r = a^* \vee b^*$; $d)$ $r = ab^* \wedge a^*$.

$a)$ $L(r)$ consta de todas las palabras que empiezan y terminan en a y contienen una o más b.

$b)$ $L(r)$ consta de todas las palabras que contienen exactamente dos a.

$c)$ $L(r)$ consta de todas las palabras que sólo contienen a o b; es decir, $L(r) = \{\lambda, a, a^2, \cdots, b, b^2, \cdots\}$.

$d)$ Aquí r no es una expresión regular puesto que $\wedge$ no es uno de los símbolos usados para formar expresiones regulares.

12.12 Sea $A = \{a, b, c\}$ y sea $w = abc$. Establezca si w pertenece o no a $L(r)$, donde:

a) $r = a^* \vee (b \vee c)^*$; *b*) $r = a^*(b \vee c)^*$.

a) No. Aquí $L(r)$ consta de palabras con a o palabras con b y c.

b) Sí, puesto que $a \in L(a)^*$ y $bc \in (b \vee c)^*$.

12.13 Sea $A = \{a, b\}$. Encuentre una expresión regular r tal que $L(r)$ conste de todas las palabras w donde:

a) w empiece con a^2 y termine con b^2; *b*) w contenga un número par de a.

a) Sea $r = a^2(a \vee b)^*b^2$. (Observe que $(a \vee b)^*$ consta de todas las palabras sobre A.)

b) Observe que $s = b^*ab^*ab^*$ consta de todas las palabras que contienen exactamente dos letras a. Entonces sea $r = s^* = (b^*ab^*ab^*)^*$.

AUTÓMATAS FINITOS

12.14 Sea M un autómata con el siguiente conjunto de entrada A, conjunto de estados S con estado inicial s_0 y conjunto de estados de aceptación ("sí") Y:

$$A = \{a, b\}, \qquad S = \{s_0, s_1, s_2\}, \qquad Y = \{s_2\}$$

Suponga que la función de estado siguiente F de M está dada por la tabla de la figura 12-7*a*).

a) Dibuje el diagrama de estado $D = D(M)$ de M.

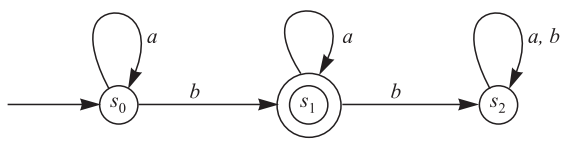
b) Describa el lenguaje $L = L(M)$ aceptado por M.

a) El diagrama de estado D aparece en la figura 12-7*b*). Los vértices de D son los estados y un círculo doble indica un estado de aceptación. Si $F(s_j, x) = s_k$, entonces hay una arista dirigida de s_j a s_k identificada por el símbolo de entrada x. También hay una flecha especial que termina en el estado inicial s_0.

b) $L(M)$ consta de todas las palabras w que contienen exactamente una b. En específico, si una palabra de entrada w no contiene b, entonces termina en s_0 y si w contiene una o más b, entonces termina en s_2. En caso contrario, w termina en s_1, que es el único estado de aceptación.

F	a	b
s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_2

a)



b)

Figura 12-7

12.15 Sea $A = \{a, b\}$. Construya un autómata M que acepte precisamente las palabras de A que contienen un número par de a. Por ejemplo, *aababbab*, *aa*, *bbb*, *ababaa* serán aceptadas por M, pero *ababa*, *aaa*, *bbabb* serán rechazadas por M.

Sólo se requieren dos estados, s_0 y s_1. Se supone que M está en el estado s_0 o s_1 según sea el caso si el número de a hasta el paso dado es par o impar. (Por tanto, s_0 es un estado de aceptación, pero s_1 es un estado de rechazo.) Entonces, sólo a modifica el estado. Asimismo, s_0 es el estado inicial. El diagrama de estado se muestra en la figura 12-8*a*).

12.16 Sea $A = \{a, b\}$. Construya un autómata M que acepte precisamente aquellas palabras de A que empiecen con una a seguida por (cero o más) b.

El autómata se muestra en la figura 12-8*b*).

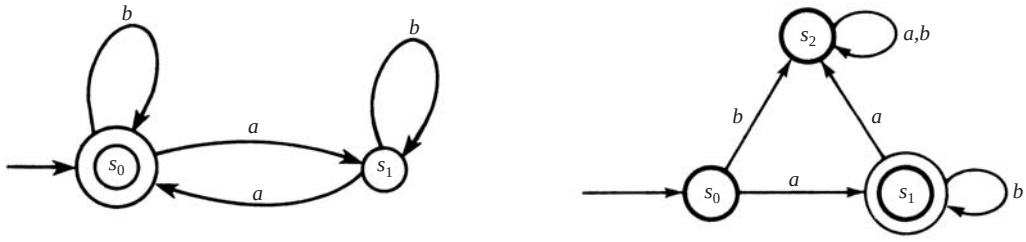


Figura 12-8

12.17 Describa las palabras w en el lenguaje L aceptadas por el autómata en la figura 12-9*a*).

El sistema puede alcanzar el estado de aceptación s_2 sólo cuando existe una a en w que sigue a una b.

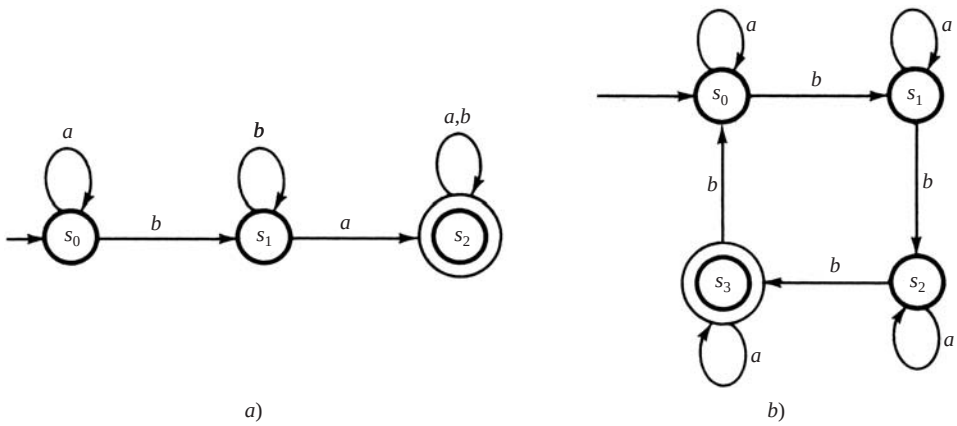


Figura 12-9

12.18 Describa las palabras w en el lenguaje L aceptadas por el autómata en la figura 12-9*b*).

Ninguna a en w cambia el estado del sistema, mientras que cada b en w cambia el estado de R_i a s_{i+1} (módulo 4). Así, w es aceptada por M si el número n de b en w es congruente con 3 módulo 4; es decir, donde $n = 3, 7, 11, \cdots$.

12.19 Suponga que L es un lenguaje sobre A que es aceptado por el autómata $M = (A, S, Y, s_0, F)$. Encuentre un autómata N que acepte L^C; es decir, aquellas palabras de A que no pertenecen a L.

Simplemente se intercambian los estados de aceptación y rechazo en M para obtener N. Luego, w será aceptada en la nueva máquina N si y sólo si w es rechazada en M, es decir, si y sólo si w pertenece a L^C. Formalmente, $N = (A, S, S \backslash Y, s_0, F)$.

12.20 Sean $M = (A, S, Y, s_0, F)$ y $M' = (A, S', Y', S'_0, F')$ autómatas sobre el mismo alfabeto A que acepta, respectivamente, los lenguajes $L(M)$ y $L(M')$ sobre A. Construya un autómata N sobre A que acepte precisamente $L(M) \cap L(M')$.

Sea $S \times S'$ el conjunto de estados de N. Sea (s, s') un estado de aceptación de N si tanto s como s' son estados de aceptación en M y M', respectivamente. Sea (s_0, s'_0) el estado inicial de N. Sea la función de estado siguiente de N, $G : (S \times S') \times A \to (S \times S')$ que se define por:

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Entonces N aceptará precisamente las palabras en $L(M) \cap L(M')$.

12.21 Repita el problema 12.20, excepto que ahora se deja que N acepte precisamente $L(M) \cup L(M')$.

De nuevo, sea $S \times S'$ el conjunto de estados de N y sea (s_0, s_0) el estado inicial de N. Luego, sean $(S \times Y') \cup (Y \times S')$ los estados de aceptación en N. La función de estado siguiente G vuelve a definirse por

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Entonces N aceptará precisamente las palabras en $L(M) \cup L(M')$.

GRAMÁTICAS

12.22 Defina: *a*) gramática libre del contexto; *b*) gramática regular.

a) Una gramática libre del contexto es lo mismo que una gramática tipo 2; es decir, toda producción es de la forma $A \to \beta$, es decir, el miembro izquierdo es una variable simple y el miembro derecho, una palabra con uno o más símbolos.

b) Una gramática regular es lo mismo que una gramática tipo 3; es decir, toda producción es de la forma $A \to a$, o de la forma $A \to aB$, es decir, el miembro izquierdo es una variable simple y el miembro derecho es un terminal simple o un terminal seguido por una variable.

12.23 Encuentre el lenguaje $L(G)$ generado por la gramática G con variables S, A, B, terminales a, b y producciones $S \to aB$, $B \to b$, $B \to bA$, $A \to aB$.

Observe que la primera producción sólo puede usarse una vez, puesto que el símbolo inicial S no aparece en ninguna otra parte. Asimismo, sólo puede obtenerse una palabra terminal al finalmente utilizar la segunda producción. En caso contrario, en forma alterna se agregan a y b usando la tercera y cuarta producciones. En consecuencia,

$$L(G) = \{(ab)^n = ababab \cdots ab \mid n \in N\}$$

12.24 Sea L el lenguaje sobre $A = \{a, b\}$ que consta de todas las palabras w que contienen exactamente una b; es decir,

$$L = \{b, a^r b, ba^s, a^r ba^s \mid r > 0, s > 0\}$$

a) Encuentre una expresión regular r tal que $L = L(r)$.
b) Encuentre una gramática regular G que genere el lenguaje L.

a) Sea $r = a^*ba^*$. Entonces $L(r) = L$.

b) La gramática regular G con las siguientes producciones genera L:

$$S \to (b, aA), \quad A \to (b, aA, bB), \quad B \to (a, aB)$$

Es decir, la letra b sólo puede aparecer una vez en cualquier palabra derivada a partir de S. G es regular puesto que tiene la forma requerida.

12.25 Sea G la gramática regular con producciones $S \to aA$, $A \to aB$, $B \to bB$, $B \to A$.

a) Encuentre el árbol de derivación de la palabra $w = aaba$.
b) Describa todas las palabras w en el lenguaje L generadas por G.

a) Primero observe que w puede derivarse a partir de S como sigue:

$$S \Rightarrow aA \Rightarrow a(aB) \Rightarrow aa(bB) \Rightarrow aaba$$

En la figura 12.10*a*) se muestra el árbol de derivación correspondiente.

b) Al usar la producción 1, luego 2, luego 3, r veces, y al final 4, se deriva la palabra $w = aab^r$, donde $r \geq 0$. A partir de S no es posible derivar ninguna otra palabra.

12.26 La figura 12.10*b*) es el árbol de derivación de una palabra w en el lenguaje L de una gramática G libre del contexto. *a*) Encuentre w. *b*) ¿Cuáles terminales, variables y producciones deben estar en G?

a) La secuencia de hojas de izquierda a derecha produce la palabra $w = ababbbba$.

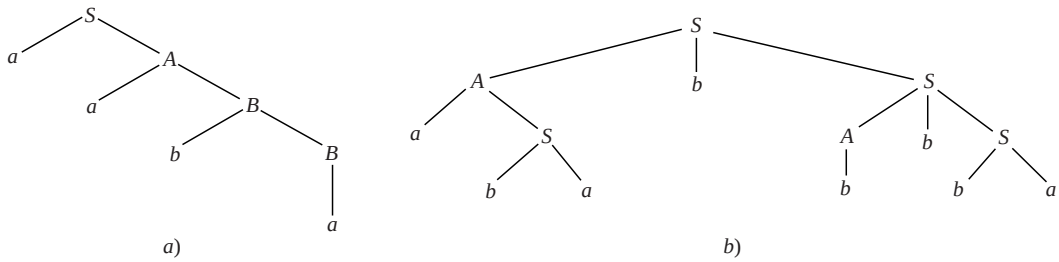


Figura 12-10

b) Las hojas muestran que *a* y *b* deben ser terminales, y los vértices internos muestran que *S* y *A* deben ser variables con *S* como la variable inicial. Los hijos de cada variable muestran que $S \to AbS$, $A \to aS$, $S \to ba$ y $A \to b$ deben ser producciones.

12.27 ¿Existe un árbol de derivación para cualquier palabra w derivada a partir del símbolo inicial S en una gramática G?

No. Los árboles de derivación sólo existen para las gramáticas tipos 2 y 3; es decir, para gramáticas libres del contexto y gramáticas regulares.

12.28 Determine el tipo de gramática G que consiste de las siguientes producciones:

a) $S \to aA, A \to aAB, B \to b, A \to a$
b) $S \to aAB, AB \to bB, B \to b, A \to aB$
c) $S \to aAB, AB \to a, A \to b, B \to AB$
d) $S \to aB, B \to bA, B \to b, B \to a, A \to aB, A \to a$

a) Cada producción es de la forma $A \to \alpha$; por tanto, G es una gramática libre del contexto o una gramática tipo 2.

b) La longitud del miembro izquierdo de cada producción no excede la longitud del miembro derecho; por tanto, G es una gramática tipo 1.

c) La producción $AB \to a$ significa que G es una gramática tipo 0.

d) G es una gramática regular o tipo 3 puesto que cada producción es de la forma $A \to a$ o $A \to aB$.

12.29 Reescriba cada gramática del problema 12.28 en forma de Backus-Naur.

La forma de Backus-Naur sólo es válida para gramáticas libres del contexto (que incluyen a las gramáticas regulares). Por tanto, sólo *a*) y *d*) pueden escribirse en forma de Backus-Naur. La forma se obtiene como sigue:

i) $\to$ se sustituye por $::=$.

ii) Las no terminales se escriben entre corchetes $\langle\ \rangle$.

iii) Todas las producciones con el mismo miembro izquierdo se combinan en una declaración con todos los miembros derechos enumerados a la derecha de $::=$ separados por barras verticales.

En consecuencia:

a) $\langle S\rangle ::= a\ \langle A\rangle,\quad \langle A\rangle ::= a\ \langle A\rangle\ \langle B\rangle \mid a,\quad \langle B\rangle ::= b$

b) $\langle S\rangle ::= a\ \langle B\rangle,\quad \langle B\rangle ::= b\ \langle A\rangle \mid b \mid a,\quad \langle A\rangle ::= a\ \langle B\rangle \mid a$

PROBLEMAS SUPLEMENTARIOS

PALABRAS

12.30 Considere las palabras $u = ab^2a^3$ y $v = aba^2b^2$. Encuentre *a*) uv; *b*) vu; *c*) u^2; *d*) λu; *e*) $v\lambda v$.

12.31 Para las palabras $u = ab^2a^3$ y $v = aba^2b^2$, encuentre $|u|$, $|v|$, $|uv|$, $|vu|$ y $|v^2|$.

12.32 Sea $w = abcde$. *a*) Encuentre todas las subpalabras de w. *b*) ¿Cuáles son segmentos iniciales?

12.33 Suponga $u = a_1a_2 \cdots a_r$, donde las a_k son distintas. Encuentre el número n de subpalabras de u.

LENGUAJES

12.34 Sea $L = \{a^2, ab\}$ y $K = \{a, ab, b^2\}$. Encuentre: *a*) LK; *b*) KL; *c*) $L \vee K$; *d*) $K \wedge L$.

12.35 Sea $L = \{a^2, ab\}$. Encuentre: (*a*) L^0; (*b*) L^2; (*c*) L^3.

12.36 Sea $A = \{a, b, c\}$. Describa L^*: *a*) $L = \{a^2\}$; *b*) $L = \{a, b^2\}$; *c*) $L = \{a, b^2, c^3\}$.

12.37 ¿Es cierto que $(L^2)^* = (L^*)^2$? De no ser cierto, ¿cómo están relacionados?

12.38 Considere un alfabeto numerable $A = \{a_1, a_2, \cdots\}$. Sea L_k el lenguaje sobre A que consta de las palabras w tales que la suma de los subíndices de las letras en w es igual a k. (Vea el problema 12.10.) Encuentre: *a*) L_3; *b*) L_5.

EXPRESIONES REGULARES, LENGUAJES REGULARES

12.39 Sea $A = \{a, b, c\}$. Describa el lenguaje $L(r)$ para cada una de las siguientes expresiones regulares:

a) $r = ab^*c$; *b*) $r = (ab \vee c)^*$; *c*) $r = ab \vee c^*$.

12.40 Sea $A = \{a, b\}$. Encuentre una expresión regular r tal que $L(r)$ conste de todas las palabras w donde:

a) w contiene exactamente tres a.

b) El número de letras a es divisible entre 3.

12.41 Sea $A = \{a, b, c\}$ y sea $w = ac$. Decida si w pertenece o no a $L(r)$, donde:

a) $r = a^*bc^*$; *b*) $r = a^*b^*c$; *c*) $r = (ab \vee c)^*$

12.42 Sea $A = \{a, b, c\}$ y sea $w = abc$. Decida si w pertenece o no a $L(r)$, donde:

a) $r = ab^*(bc)^*$; *b*) $r = a^* \vee (b \vee c)^*$; *c*) $r = a^*b(bc \vee c^2)^*$.

AUTÓMATAS FINITOS

12.43 Sea $A = \{a, b\}$. Construya un autómata M tal que $L(M)$ consta de las palabras w donde:

a) El número de b es divisible entre 3. *b*) w empieza en a y termina en b.

12.44 Sea $A = \{a, b\}$. Construya un autómata M que acepte el lenguaje:

a) $L(M) = \{b^r a b^s \mid r > 0, s > 0\}$; *b*) $L(M) = \{a^r b^s \mid r > 0, s > 0\}$.

12.45 Sea $A = \{a, b\}$. Construya un autómata M tal que $L(M)$ consta de las palabras donde el número de a es divisible entre 2 y el número de b es divisible entre 3.

(*Sugerencia*: use los problemas 12.15, 12.43*a*) y 12.20.)

12.46 Encuentre el lenguaje $L(M)$ aceptado por el autómata M en la figura 12.11.

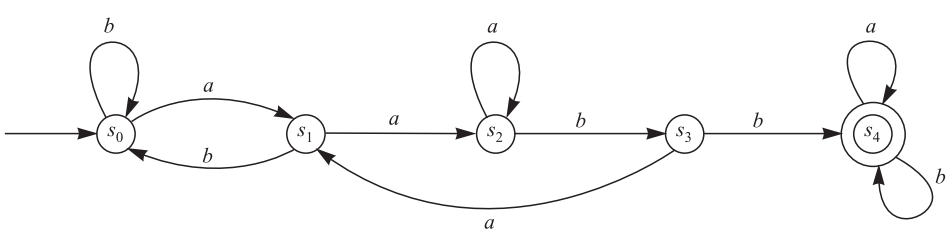


Figura 12-11

GRAMÁTICAS

12.47 Determine el tipo de gramática G que consta de las producciones:

a) $S \to aAB;\quad S \to AB;\quad A \to a;\quad B \to b$

b) $S \to aB;\quad B \to AB;\quad aA \to b;\quad A \to a;\quad B \to b$

c) $S \to aB;\quad B \to bB;\quad B \to bA;\quad A \to a;\quad B \to b$

12.48 Encuentre una gramática regular G que genere el lenguaje L que consta de todas las palabras con a y b tales que no hay dos a consecutivas.

12.49 Encuentre una gramática G libre del contexto que genere el lenguaje L que consta de todas las palabras con a y b tales que el número de a es dos veces el número de b.

12.50 Encuentre una gramática G que genere el lenguaje L que consta de todas las palabras con a y b tales que el número de a es par.

12.51 Encuentre una gramática G que genere el lenguaje L que consta de todas las palabras de la forma $a^n b a^n$ con $n \geq 0$.

12.52 Demuestre que el lenguaje L en el problema 12.51 no es regular. (*Sugerencia*: use el lema de bombeo.)

12.53 Describa el lenguaje $L = L(G)$ donde G tiene las producciones $S \to aA$, $A \to bbA$, $A \to c$.

12.54 Describa el lenguaje $L = L(G)$ donde G tiene las producciones $S \to aSb$, $Sb \to bA$, $abA \to c$.

12.55 Escriba cada gramática G en el problema 12.47 en forma Backus-Naur.

12.56 Sea G la gramática libre del contexto con producciones $S \to (a, aAS)$ y $A \to bS$.

a) Escriba G en forma Backus-Naur. *b*) Encuentre el árbol de derivación de la palabra $w = abaa$.

12.57 La figura 12-12 es el árbol de derivación de una palabra w en un lenguaje L de una gramática G libre del contexto.

a) Encuentre w. *b*) ¿Qué terminales, variables y producciones deben pertenecer a G?

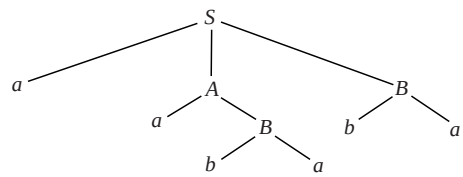


Figura 12-12

Respuestas a los problemas suplementarios

12.30 *a*) $uv = ab^2a^4ba^2b^2$; *b*) $vu = aba^2b^2ab^2a^3$;
c) $u^2 = ab^2a^4b^2a^3$; *d*) $\lambda u = u$;
e) $v\lambda v = v^2 = aba^2b^2aba^2b^2$.

12.31 6, 6, 12, 12, 12.

12.32 *a*) λ, a, b, c, d, e, ab, bc, cd, de, abc, bcd, cde, $abcd$, $bcde$, $w = abcde$.
b) λ, a, ab, abc, $abcd$, $w = abcde$.

12.33 Si $\mathbf{u} = \lambda$ entonces $n = 1$; en caso contrario, $n = 1 + [r + (r - 1) + \cdots + 2 + 1] = 1 + r(r + 1)/2$.

12.34 *a*) $LK = \{a^3, a^3b, a^2b^2, aba, abab, ab^3\}$;
b) $KL = \{a^3, a^2b, aba^2, abab, b^2a^2, b^2ab\}$;
c) $L \vee K = \{a^2, ab, a, b^2\}$; *d*) $K \wedge L$ no está definido.

12.35 *a*) $L^0 = \{\lambda\}$; (*b*) $L^2 = \{a^4, a^3b, aba^2, abab\}$;
c) $L^3 = \{a^6, a^5b, a^3ba^2, a^3bab, aba^4, aba^3b, ababa^2, ababab\}$

12.36 *a*) $L^* = \{a^n \mid n \text{ es par}\}$. *b*) Todas las palabras w con a y b que sólo tienen potencias pares de b.
c) Todas las palabras con a, b, c donde cada potencia de b es par y cada potencia de c es un múltiplo de 3.

12.37 No. $(L^2)^* \subseteq (L^*)^2$.

12.38 *a*) $a_1a_1a_1$, a_1a_2, $a_2a_1a_3$ *b*) $a_1a_1a_1a_1a_1$, $a_1a_1a_1a_2$, $a_1a_1a_2a_1$, $a_1a_2a_1a_1$, $a_2a_1a_1a_1$, $a_1a_1a_3$, $a_1a_3a_1$, $a_3a_1a_1$, a_2a_3, a_3a_2, a_1a_4, a_4a_1, a_5.

12.39 *a*) $L(r) = \{ab^nc \mid n \geq 0\}$. *b*) Todas las palabras con x y c donde $x = ab$. *c*) $L(r) = ab \cup \{c^n \mid n \geq 0\}$.

12.40 *a*) $r = b^*ab^*ab^*ab^*$; *b*) $r = (b^*ab^*ab^*ab^*)^*$.

12.41 *a*) No; *b*) sí; *c*) no.

12.42 *a*) Sí; *b*) no; *c*) no.

12.43 Vea la: *a*) Fig. 12-13*a*); *b*) Fig. 12-13*b*).

12.44 Vea la: *a*) Fig. 12-14; *b*) Fig. 12-15*a*).

12.45 Vea la: Fig. 12-15*b*).

12.46 $L(M)$ consta de todas las palabras w que contienen a $aabb$ como subpalabra.

12.47 *a*) Tipo 2; *b*) Tipo 0; *c*) Tipo 3.

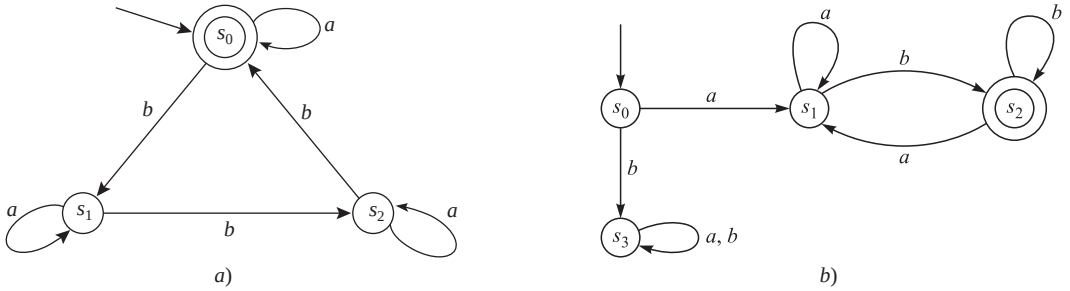


Figura 12-13

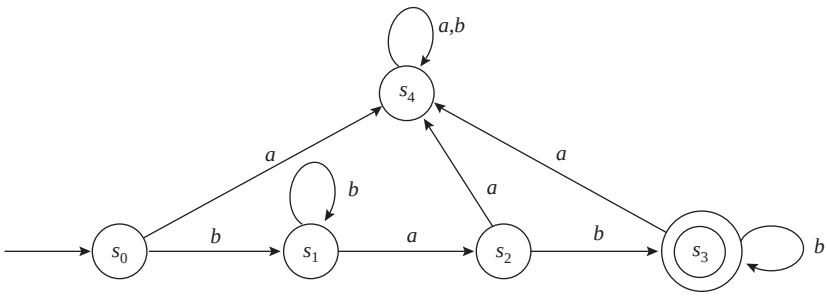


Figura 12-14

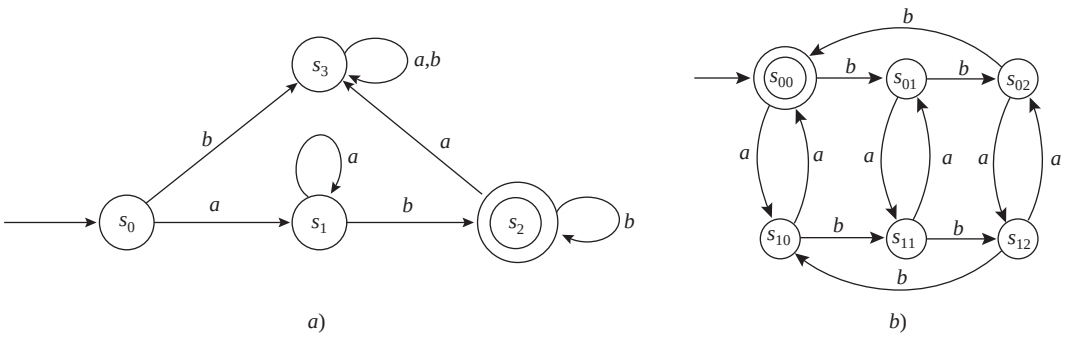


Figura 12-15

12.48 $S \rightarrow (a, b, aB, bA)$, $A \rightarrow (bA, ab, a, b)$, $B \rightarrow (b, bA)$.

12.49 $S \rightarrow (AAB, ABA, BAA)$, $A \rightarrow (a, BAAA, ABAA, AABA, AAAB)$,
$B \rightarrow (b, BBAA, BABA, aBAAB, ABAB, AABB)$.

12.50 $S \rightarrow (aA, bB)$, $A \rightarrow (aB, bA, a)$, $B \rightarrow (bB, aA, b)$

12.51 $S \rightarrow (aSa, b)$.

12.53 $L = \{ab^{2n}c \mid n \geq 0\}$

12.54 $L = \{a^n cb^n \mid n > 0\}$

12.55 *a*) $\langle S\rangle ::= a\,\langle A\rangle\langle B\rangle | \langle A\rangle\langle B\rangle$, $\langle A\rangle ::= a$, $\langle B\rangle ::= b$
b) No está definido para un lenguaje tipo 0.
c) $\langle S\rangle ::= a\langle B\rangle$, $\langle B\rangle ::= b\langle B\rangle | \; b\,\langle A\rangle$, $\langle A\rangle ::= a \mid b$

12.56 $\langle S\rangle ::= a|a\,\langle A\rangle\langle S\rangle$, $\langle A\rangle ::= b\langle S\rangle$; *b*) Vea la figura 12-16.

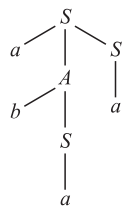


Figura 12-16

12.57 *a*) $w = aababa$; *b*) $S \rightarrow aAB, A \rightarrow aB, B \rightarrow ba$.

13 CAPÍTULO Máquinas de estados finitos y máquinas de Turing

13.1 INTRODUCCIÓN

En este capítulo se estudian dos tipos de "máquinas". La primera es una máquina de estados finitos (FSM, *finite state machine*), que es semejante a un autómata de estados finitos (FSA, *finite state automaton*) excepto que la primera al "imprimir" una salida usa un alfabeto de salida que puede ser distinto al alfabeto de entrada. La segunda es la célebre máquina de Turing, que puede usarse para definir funciones computables.

13.2 MÁQUINAS DE ESTADOS FINITOS

Una máquina de estados finitos (o máquina secuencial completa) M consta de seis partes:

1) Un conjunto finito A de símbolos de entrada.
2) Un conjunto finito S de estados "internos".
3) Un conjunto finito Z de símbolos de salida.
4) Un estado inicial s_0 en S.
5) Una función f de estado siguiente de $S \times A$ en S.
6) Una función g de salida de $S \times A$ en Z.

Cuando se indican las seis partes de una máquina M se denota por $M = M(A, S, Z, s_0, f, g)$.

EJEMPLO 13.1 A continuación se define una máquina de estados finitos M con dos símbolos de entrada, tres estados internos y tres símbolos de salida:

1) $A = \{a, b\}$, 2) $S = \{s_0, s_1, s_2\}$, 3) $Z = \{x, y, z\}$, 4) Estado inicial s_0,

5) Función de estado siguiente $f : S \times A \to S$ que se define con:

$$f(s_0, a) = s_1, \quad f(s_1, a) = s_2, \quad f(s_2, a) = s_0$$
$$f(s_0, b) = s_2, \quad f(s_1, b) = s_1, \quad f(s_2, b) = s_1$$

6) Función de salida $g : S \times A \to S$ que se define con:

$$g(s_0, a) = x, \quad g(s_1, a) = x, \quad g(s_2, a) = z$$
$$g(s_0, b) = y, \quad g(s_1, b) = z, \quad g(s_2, b) = y$$

Tabla de estado y diagrama de estado de una máquina de estados finitos

Hay dos formas de representar una máquina de estados finitos M en forma breve. Una es mediante la *tabla de estado* de la máquina M, y la otra es por medio de una gráfica dirigida etiquetada que se denomina *diagrama de estado* de la máquina M.

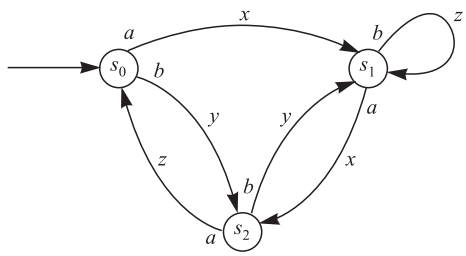
La tabla de estado combina la función f de estado siguiente y la función g de salida en una sola tabla que representa la función $F : S \times A \to S \times Z$, la que se define:

$$F(s_i, a_j) = [f(s_i, a_j), g(s_i, a_j)]$$

Por ejemplo, la tabla de estado de la máquina M del ejemplo 13.1 se muestra en la figura 13-1*a*). Los estados se enumeraron a la izquierda de la tabla con el estado inicial primero y los símbolos de salida se muestran en la parte superior de la tabla. Una entrada en la tabla es un par (s_k, z_r) donde $s_k = f(s_i, a_j)$ es el siguiente estado y $z_r = g(s_i, a_j)$ es el símbolo de salida. Se supone que no hay símbolos de salida distintos a los que aparecen en la tabla.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_2, x	s_1, y
s_2	s_0, x	s_1, y

a)



b)

Figura 13-1

El diagrama de estado $D = D(M)$ de una máquina de estados finitos $M = M(A, S, Z, s_0, f, g)$ es una gráfica dirigida etiquetada. Los vértices de D son los estados de M. Además, si

$$F(s_i, a_j) = (s_k, z_r), \quad \text{o, en forma equivalente,} \quad f(s_i, a_j) = s_k \text{ y } g(s_i, a_j) = z_r$$

entonces hay un arco (flecha) de s_i a s_k que se identifica por el par a_j, z_r. Suele acostumbrarse escribir el símbolo de entrada a_i cerca de la base de la flecha (cerca de s_i) y el símbolo de salida z_r, cerca del centro de la flecha. El estado inicial s_0 también se identifica al trazar una flecha adicional hacia s_0. Por ejemplo, el diagrama de estado de la máquina M en el ejemplo 13.1 se muestra en la figura 13-1*b*).

Cintas de entrada y de salida

El análisis anterior de una máquina de estados finitos M no muestra la calidad dinámica de M. Suponga que M es una cadena (palabra) de símbolos de entrada; por ejemplo,

$$u = a_1 a_2 \ldots a_m$$

Estos símbolos se visualizan como una "cinta de entrada". La máquina M "lee" estos símbolos de entrada uno por uno y, en forma simultánea, cambia a través de una secuencia de estados

$$v = s_0 s_1 s_2 \ldots s_m$$

donde s_0 es el estado inicial, mientras imprime una cadena (palabra) de símbolos de salida

$$w = z_1 z_2 \dots z_m$$

en una "cinta de salida". En términos formales, el estado inicial s_0 y la cadena de entrada u determinan las cadenas v y w como sigue, donde $i = 1, 2, \dots, m$:

$$s_i = f(s_{i-1}, a_i) \quad \text{y} \quad z_i = g(s_{i-1}, a_i)$$

EJEMPLO 13.2 Considere la máquina M en la figura 13-1; es decir, el ejemplo 13.1. Suponga que la entrada es la palabra

$$u = abaab$$

La secuencia v de estados y la palabra w de salida se calculan a partir del diagrama de estado: se empieza en el estado inicial s_0 y se siguen las flechas que están identificadas por los símbolos de entrada como sigue:

$$s_0 \xrightarrow{a,x} s_1 \xrightarrow{b,z} s_1 \xrightarrow{a,x} s_2 \xrightarrow{a,z} s_0 \xrightarrow{b,y} s_2$$

Así se obtienen la siguiente secuencia v de estados y la palabra w de salida:

$$v = s_0 s_1 s_1 s_2 s_0 s_2 \quad \text{y} \quad w = xzxzy$$

Adición binaria

En esta subsección se describe una máquina de estados finitos M capaz de efectuar una suma binaria. Al agregar ceros (0) al inicio de los números, puede suponerse que éstos tienen la misma cantidad de dígitos. Si a la máquina se introduce la entrada

$$\begin{array}{r} 1101011 \\ +0111011 \\ \hline \end{array}$$

entonces se desea que la salida sea la suma binaria 10100110. En este caso, la entrada es la cadena de pares de dígitos a sumar:

$$11, \quad 11, \quad 00, \quad 11, \quad 01, \quad 11, \quad 10, \quad b$$

donde b denota espacios en blanco y la salida debe ser la cadena:

$$0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 0, \quad 1$$

También se desea introducir a la máquina un estado denominado "alto" (stop) cuando la máquina termine la adición.

Los símbolos de entrada y salida son, respectivamente:

$$A = \{00, 01, 10, 11, b\} \quad \text{y} \quad Z = \{0, 1, b\}$$

La máquina M que se "construye" tiene tres estados:

$$S = \{\text{llevar } (c), \text{ no llevar } (n), \text{ alto } (s)\}$$

Aquí el estado inicial es n. La máquina se observa en la figura 13-2.

A fin de mostrar las limitaciones de estas máquinas se plantea el siguiente teorema.

Teorema 13.1: No hay máquina de estados finitos M capaz de efectuar una multiplicación binaria.

Si se limita el tamaño de los números que se multiplican, entonces estas máquinas existen. Las computadoras constituyen ejemplos importantes de máquinas de estados finitos que multiplican números, aunque éstos estén limitados en cuanto a su tamaño.

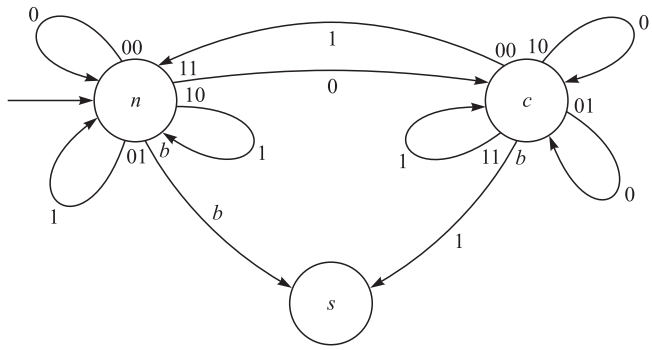


Figura 13-2

13.3 NÚMEROS DE GÖDEL

Recuerde (sección 11.5) que un entero positivo $p > 1$ se denomina número primo si sus únicos divisores positivos son 1 y p. Se hace que $p_1, p_2, p_3, \ldots$ denote los números primos consecutivos. Así,

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \ldots$$

(Por el teorema 11.12, existe una infinidad de números primos.) El teorema fundamental de la aritmética (teorema 11.20) establece que cualquier entero positivo $n > 1$ puede escribirse en forma única (salvo por el orden) como un producto de números primos. Kurt Gödel, alemán especialista en lógica, usó este resultado para codificar secuencias finitas de números y también para codificar palabras sobre un alfabeto finito o numerable. A cada secuencia o palabra se le asigna un entero positivo, *número de Gödel*, como sigue.

El número de Gödel de la secuencia $s = (n_1, n_2, \ldots, n_k)$ de enteros no negativos es el entero positivo $c(s)$, donde n_i es el exponente de p_i en la descomposición en primos de $c(s)$; es decir,

$$c(s) = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Por ejemplo,

$$s = (3, 1, 2, 0, 2) \quad \text{se codifica como} \quad c(s) = 2^3 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^2 = 72\,600$$

El número de Gödel de una palabra w sobre un alfabeto $\{a_0, a_1, a_2, a_3, \ldots\}$ es el entero positivo $c(w)$ donde el subíndice de la i-ésima letra de w es el exponente de p_i en la descomposición en primos de $c(w)$. Por ejemplo,

$$w = a_4a_1a_3a_2a_2 \quad \text{se codifica como} \quad c(w) = 2^4 \cdot 3 \cdot 5^3 \cdot 7^2 \cdot 11^2$$

(Observe que ambos códigos son esencialmente lo mismo, puesto que una palabra w se considera como la secuencia de los subíndices de sus letras.)

La codificación anterior constituye la demostración del resultado más importante de esta sección.

Teorema 13.2: Suponga que un alfabeto A es numerable. Entonces cualquier lenguaje L sobre A también es numerable.

Demostración: El código de Gödel es una transformación uno a uno c: $L \to N$. Por tanto, L es numerable.

13.4 MÁQUINAS DE TURING

Hay varias formas equivalentes de definir formalmente una función "computable". Esto se hace mediante una máquina de Turing M. En esta sección se define con formalidad una máquina de Turing M, y en la siguiente se define lo que es una función computable.

En la definición de máquina de Turing en este texto se usan una cinta infinita de dos posiciones, quíntuplas y tres estados de detención, interrupción o alto. En otras definiciones se usan una cinta infinita de una posición y/o cuádruplas y un estado de detención, interrupción o alto. Sin embargo, todas las definiciones son equivalentes.

Definiciones básicas

Una *máquina de Turing M* implica tres conjuntos no vacíos ajenos:

1) Un conjunto finito de *cinta* donde $B = a_0$ es el símbolo en "blanco":

$$A = \{a_1, a_2, \ldots, a_m\} \cup \{B\}$$

2) Un conjunto finito *de estados* donde a_0 es el *estado inicial*:

$$S = \{s_1, s_2, \ldots, s_n\} \cup \{s_0\} \cup \{s_H, s_Y, s_N\}$$

Aquí s_H (HALT) es el estado de detención, interrupción o alto, s_Y (YES) es el estado de aceptación y S_N (NO) es el estado de no aceptación o rechazo.

3) Una conjunto de *direcciones*, donde L denota "izquierda" y R denota "derecha".

$$d = \{L, R\}$$

Definición 13.1: Una *expresión* es una secuencia finita (tal vez vacía) de elementos de $A \cup S \cup d$.

En otras palabras, una expresión es una palabra cuyas letras (símbolos) provienen de los conjuntos A, S y d.

Definición 13.2: Una *expresión en una cinta* es en la que sólo se usan elementos del conjunto A en la cinta.

La máquina de Turing M puede considerarse como una cabeza de lectura/escritura en una cinta, que se mueve de un lado a otro a lo largo de una cinta infinita. La cinta tiene divisiones a lo largo en cuadrados (celdas) y cada cuadrado puede estar en blanco o contener un símbolo de la cinta. En cada paso temporal, la máquina de Turing M se encuentra en algún estado interno s_i, en el que *escanea* (examina) uno de los símbolos a_j de la cinta. Se supone que en la cinta sólo aparece un número finito de símbolos que no están en blanco.

La figura 13-3*a*) es una ilustración de una máquina de Turing M en el estado s_2, que escanea el segundo símbolo donde $a_1a_3Ba_1a_1$ está impreso en la cinta. (Observe de nuevo que B es el símbolo en blanco.) Esta ilustración se representa mediante la expresión $\alpha = a_1s_2a_3Ba_1a_1$, donde el estado s_2 de M se escribe antes del símbolo a_3 en la cinta que escanea M. Observe que α es una expresión que sólo usa el alfabeto A en la cinta, excepto por el símbolo del estado s_2 que no está al final de la expresión, puesto que aparece antes del símbolo a_3 en la cinta que M escanea. En la figura 13-3 aparecen otras dos ilustraciones informales y sus expresiones correspondientes.

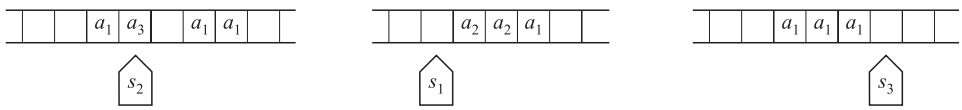


Figura 13-2

A continuación se proporcionan definiciones formales.

Definición 13.3: Una *ilustración* α es una expresión como la siguiente, donde P y Q son expresiones en la cinta (quizá vacías):

$$\alpha = Ps_ia_kQ$$

Definición 13.4: Sea $\alpha = Ps_ia_kQ$ una ilustración. Se dice que la máquina de Turing M *se encuentra en el estado* s_i *escaneando la letra* a_k y que la *expresión en la cinta* es la expresión Pa_kQ; es decir, sin su símbolo de estado s_i.

Como ya se mencionó, en cada paso temporal la máquina de Turing M se encuentra en algún estado s_i, y está escaneando un símbolo a_k en la cinta. La máquina de Turing M es capaz de realizar en forma simultánea las tres actividades siguientes:

i) borrar el símbolo escaneado a_k y en su lugar escribir un símbolo en la cinta a_l (donde se permite $a_l = a_k$);
ii) cambiar sus estados internos s_i a un estado s_j (donde se permite $s_i = s_j$);
iii) moverse un cuadro a la izquierda o un cuadro a la derecha.

Cada una de las acciones anteriores que realiza M se describe mediante una expresión con cinco letras denominada *quíntupla* que se define a continuación.

Definición 13.5: Una quíntupla q es una expresión con cinco letras de la forma:

$$q = \left(s_i, a_k, a_l, s_j, \begin{Bmatrix} L \\ R \end{Bmatrix}\right)$$

Es decir, la primera letra de q es un símbolo de estado; la segunda, uno de cinta; la tercera, uno de cinta; la tercera, uno de cinta; la cuarta, uno de estado, y la última, uno de dirección, L o R.

A continuación se proporciona una definición formal de una máquina de Turing M.

Definición 13.6: Una máquina de Turing M es un conjunto finito de quíntuplas tal que:

i) Ninguna quíntupla empieza con las dos mismas letras.

ii) Ninguna quíntupla empieza con s_H, s_Y o s_N.

La condición *i*) en la definición asegura que la máquina M no puede hacer más de una cosa en cualquier paso dado, y la condición *ii*) garantiza que M se detiene en el estado s_H, s_Y o s_N.

A continuación se proporciona una definición equivalente alterna.

Definición 13.6′: Una máquina de Turing M es una función parcial de

$$S\backslash\{s_H, s_Y \text{ o } s_N\} \times A \quad \text{en} \quad A \times S \times d$$

La expresión función parcial simplemente significa que el dominio de M es un subconjunto de $S\backslash\{s_H, s_Y \text{ o } s_N\} \times A$.

Ahora es posible dar una definición formal de la acción de la máquina de Turing recién descrita.

Definición 13.7: Sean α y β ilustraciones. Lo que se escribe

$$\alpha \to \beta$$

si se cumple una de las siguientes condiciones, donde a, b y c son letras en la cinta y P y Q son expresiones en la cinta (posiblemente vacías):

i) $\alpha = Ps_i acQ$, $\beta = Pbs_j cQ$ y M contiene la quíntupla $q = s_i abs_j R$.

ii) $\alpha = Pcs_i aQ$, $\beta = Ps_j cbQ$ y M contiene la quíntupla $q = s_i abs_j L$.

iii) $\alpha = Ps_i a$, $\beta = Pbs_j B$ y M contiene la quíntupla $q = s_i abs_j R$.

iv) $\alpha = s_i aQ$, $\beta = s_j BbQ$ y M contiene la quíntupla $q = s_i abs_j L$.

Observe que, en los cuatro casos, M sustituye a a en la cinta por b (donde se permite $b = a$), y M cambia su estado de s_i a s_j (donde se permite $s_j = s_i$). Además:

i) Aquí M se mueve a la derecha.

ii) Aquí M se mueve a la izquierda.

iii) Aquí M se mueve a la derecha; no obstante, puesto que M se encuentra escaneando la letra que está más a la derecha, debe agregar el símbolo en blanco B a la derecha.

iv) Aquí M se mueve a la izquierda; no obstante, puesto que M se encuentra escaneando la letra que está más a la izquierda, debe agregar el símbolo en blanco B a la izquierda.

Definición 13.8: Se dice que una ilustración α es *terminal* si no hay ninguna ilustración β tal que $\alpha \to \beta$.

En particular, cualquier ilustración α en uno de los tres estados de detención debe ser terminal puesto que ninguna quíntupla empieza con s_H, s_Y o s_N.

Cálculos con una máquina de Turing

Lo que se ha presentado recientemente es una descripción estática (de un paso) de una máquina de Turing M. A continuación se analiza su dinámica.

Definición 13.9: Un *cálculo* o *cómputo* de una máquina de Turing M es una secuencia de ilustraciones $\alpha_1, \alpha_2, \ldots, \alpha_m$ tal que $\alpha_{i-1} \rightarrow \alpha_i$, para $i = 1, 2, \ldots, m$, y α_m es una ilustración terminal.

En otras palabras, un cálculo es una secuencia

$$\alpha_0 \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \ldots \rightarrow \alpha_m$$

que no puede extenderse porque α_m es terminal. Se deja que term(α) denote la ilustración final de un cómputo que empieza con α. Por tanto, term(α_0) $= \alpha_m$ en el cálculo anterior.

Máquinas de Turing con entrada

La siguiente definición es válida.

Definición 13.10: Una *entrada* para una máquina de Turing M es una expresión W en la cinta. La *ilustración inicial* para una entrada W es $\alpha(W)$, donde $\alpha(W) = s_0(W)$.

Observe que la ilustración inicial $\alpha(W)$ de la entrada W se obtiene al colocar el estado inicial s_0 antes que la expresión W en la cinta. En otras palabras, la máquina de Turing M empieza en su estado inicial s_0 y escanea la primera letra de W.

Definición 13.11: Sea M una máquina de Turing y sea W una entrada. Se dice que M se detiene en W si hay un cómputo que empieza con la ilustración inicial $\alpha(W)$.

Es decir, dada una entrada W, es posible formar la ilustración inicial $\alpha(W) = s_0(W)$ y aplicar M para obtener la secuencia

$$\alpha(W) \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \ldots$$

Pueden ocurrir dos cosas:

1) ***M* se detiene en *W*.** Es decir, la secuencia termina con alguna ilustración terminal α_r.
2) ***M* no se detiene en *W*.** Es decir, la secuencia no termina nunca.

Gramáticas y máquinas de Turing

Las máquinas de Turing sirven para reconocer lenguajes. En específico, suponga que M es una máquina de Turing con conjunto de cinta A. Sea L el conjunto W de palabras en A tal que M se detiene en el estado de aceptación s_Y cuando la entrada es W. Entonces se escribe $L = L(M)$, y se dice que M reconoce el lenguaje L. Por tanto, una entrada W no pertenece a $L(M)$ si M no se detiene en W o si M se detiene en W pero no en el estado de aceptación s_Y.

El siguiente teorema es el resultado más importante de esta subsección; su demostración rebasa el alcance de este texto.

Teorema 13.3: Un lenguaje L es reconocible por una máquina de Turing si y sólo si L es un lenguaje tipo 0.

Observación: La razón por la cual hay tres estados de detención es que s_Y y s_N se usan para reconocer lenguajes, mientras que s_H se usa para cómputos que se analizan en la siguiente sección.

EJEMPLO 13.3 Suponga que una máquina de Turing M con conjunto de cinta $A = \{a, b, c\}$ contiene las siguientes quíntuplas:

$$q_1 = s_0aas_0R, \quad q_2 = s_0bbs_0R, \quad q_3 = s_0BBs_NR, \quad q_4 = s_0ccs_YR$$

a) Suponga que $W = W(a, b, c)$ es una entrada sin ninguna c.

Por las quíntuplas q_1 y q_2, M permanece en el estado s_0 y se mueve a la derecha hasta que encuentra un símbolo B en blanco. Luego, M cambia su estado al estado s_N de no aceptación y se detiene.

b) Suponga que $W = W(a, b, c)$ es una entrada con por lo menos un símbolo c.
Por la quíntupla q_4, cuando M inicialmente encuentra la primera c en W, cambia al estado s_Y de aceptación y se detiene.

Así, M reconoce el lenguaje L de todas las palabras W en a, b, c que contienen por lo menos una letra c. Es decir, $L = L(M)$.

13.5 FUNCIONES COMPUTABLES

Estas funciones se definen sobre el conjunto de enteros no negativos. En algunos textos este conjunto se denota por **N**. Aquí, **N** se usa para denotar el conjunto de enteros positivos, de modo que se usará la notación

$$\mathbf{N}_0 = \{0, 1, 2, 3, \ldots\}$$

En toda esta sección, los términos número, entero y entero no negativo son sinónimos. En la sección precedente se describió la forma en que una máquina de Turing M trata y reconoce caracteres de datos. Aquí se mostrará la forma en que M maneja datos numéricos. Primero, no obstante, es necesario poder representar los números mediante el conjunto de cinta A. Se escribe 1 para el símbolo de cinta a_1 y 1^n para 111… 1, donde 1 ocurre n veces.

Definición 13.12: Cada número n se representa mediante la expresión de cinta $\langle n \rangle$ donde $\langle n \rangle = 1^{n+1}$. Así:

$$\langle 4 \rangle = 11111 = 1^5, \quad \langle 0 \rangle = 1, \quad \langle 2 \rangle = 111 = 1^3.$$

Definición 13.13: Sea E una expresión. Entonces $[E]$ denota el número de veces que 1 ocurre en E. Entonces

$$[11Bs_2a_3111\mathrm{B}a_4] = 5, \quad [a_4s_2Ba_2] = 0, \quad [\langle n \rangle] = n + 1.$$

Definición 13.14: Una función f: $\mathbf{N_0} \to \mathbf{N_0}$ es computable si existe una máquina de Turing M tal que, para cualquier entero n, M se detiene en $\langle n \rangle$ y

$$f(n) = [\text{térm}(\alpha(\langle n \rangle))]$$

Entonces se dice que M calcula a f.

Es decir, dados una función f y un entero n, se introduce $\langle n \rangle$ y se aplica M. Si M siempre se detiene en $\langle n \rangle$ y el número de unos en la ilustración final es igual a $f(n)$, entonces f es una función computable y se dice que M calcula a f.

EJEMPLO 13.4 La función $f(n) = n + 3$ es computable. La entrada es $W = 1^{n+1}$. Entonces, sólo es necesario agregar dos unos a la entrada. A continuación se describe una máquina de Turing M que calcula a f:

$$M = \{q_1, q_2, q_3\} = \{s_01s_0L, s_0B1s_1L, s_1B1s_HL\}$$

Observe que:

1) q_1 mueve la máquina M a la izquierda.
2) q_2 escribe 1 en el cuadrado en blanco B y mueve M a la izquierda.
3) q_3 escribe 1 en el cuadrado en blanco B y detiene a M.

En consecuencia, para cualquier entero positivo n,

$$s_01^{n+1} \to s_0B1^{n+1} \to s_1B1^{n+2} \to s_HB1^{n+3}$$

Entonces, M calcula a $f(n) = n + 3$. Resulta evidente que, para cualquier entero positivo k, la función $f(n) = n + k$ es computable.

Se aplica el siguiente teorema.

Teorema 13.4: Suponga que $f : \mathbf{N_0} \to \mathbf{N_0}$ y $g : \mathbf{N_0} \to \mathbf{N_0}$ son computables. Entonces la composición de funciones $h = g \circ f$ es computable.

Ahora siga la demostración de este teorema. Suponga que M_f y M_g son las máquinas de Turing que computan f y g, respectivamente. Dada la entrada $\langle n \rangle$, M_f se aplica a $\langle n \rangle$ para finalmente obtener una expresión E con $[E] = f(n)$. Luego se procede de forma que $E = s_01^{f(n)}$. A continuación se agrega 1 a E para obtener $E' = s_011^{f(n)}$ y M_g se aplica a E'. Así se obtiene E'', donde $[E''] = g(f(n)) = (g \circ f)(n)$, como se deseaba.

Funciones de varias variables

En esta subsección se define una función computable $f(n_1, n_2, \ldots, n_k)$ de k variables. Primero es necesario representar la lista $m = (n_1, n_2, \ldots, n_k)$ en el alfabeto A.

Definición 13.15: Cada lista $m = (n_1, n_2, \ldots, n_k)$ de k enteros está representada por la expresión de cinta

$$\langle m \rangle = \langle n_1 \rangle B \langle n_2 \rangle B \cdots B \langle n_k \rangle$$

Por ejemplo, $\langle (2, 0, 4) \rangle = 111B1B11111 = 1^3B1^1B1^5$.

Definición 13.16: Una función $f(n_1, n_2, \ldots, n_k)$ de k variables es computable si existe una máquina de Turing M tal que, para cualquier lista $m = (n_1, n_2, \ldots, n_k)$ M se detiene en $\langle m \rangle$ y

$$f(m) = [\text{térm}(\alpha(\langle m \rangle))]$$

Entonces se dice que M calcula a f.

La definición es semejante a la definición 13.14 para una variable.

EJEMPLO 13.5 La función adición $f(m, n) = m + n$ es computable. La entrada es $W = 1^{m+1}B1^{n+1}$. Entonces, sólo es necesario borrar dos de los unos. A continuación se muestra una máquina de Turing M que calcula a f:

$$M = \{q_1, q_2, q_3, q_4\} = \{s_0 1 B s_1 R,\ s_1 1 B s_H R,\ s_1 B B s_2 R,\ s_2 1 B s_H R\}$$

Observe que:

1) q_1 borra el primer 1 y mueve a M a la derecha.
2) Si $m \neq 0$, entonces q_2 borra el segundo 1 y detiene a M.
3) Si $m = 0$, q_3 mueve M a la derecha más allá del espacio en blanco B.
4) q_4 borra el 1 y detiene a M.

En consecuencia, si $m \neq 0$, se tiene:

$$s_0 1^{m+1} B 1^{n+1} \rightarrow s_1 1^m B 1^{n+1} \rightarrow s_H\, 1^{m-1} B 1^{n+1}$$

pero si $m = 0$ y $m + n = n$, se tiene

$$s_0 1 B 1^{n+1} \rightarrow s_1 B 1^{n+1} \rightarrow s_H\, 1^{n+1} \rightarrow s^{\text{H}} 1^n$$

Entonces M computa $f(m, n) = m + n$.

PROBLEMAS RESUELTOS

13.1 Sea M la máquina de estados finitos con la tabla de estado que se muestra en la figura 13-4*a*).

a) Encuentre el conjunto de entrada A, el conjunto de estados S, el conjunto de salida Z y el estado inicial.
b) Dibuje el diagrama de estado $D = D(M)$ de M.
c) Suponga que $w = aababaabbbab$ es una palabra (cadena) de entrada y encuentre la palabra de salida v correspondiente.

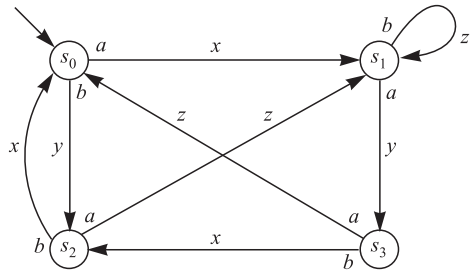
a) Los símbolos de entrada están en la parte superior de la tabla, los estados están enumerados a la izquierda y los símbolos de salida aparecen en la tabla. Así:

$$A = \{a, b\}, \quad S = \{s_0, s_1, s_2, s_3\}, \quad Z = \{x, y, z\}$$

El estado s_0 es el estado inicial, puesto que es el primer estado enumerado en la tabla.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_3, y	s_1, z
s_2	s_1, z	s_0, x
s_3	s_0, z	s_2, x

a)



b)

Figura 13-4

b) El diagrama de estado $D = D(M)$ se muestra en la figura 13-4*b*). Observe que los vértices de D son los estados de M. Suponga que $F(s_i, a_j) = (s_k, z_r)$. (Es decir, $f(s_i, a_j) = s_k$ y $g(s_i, a_j) = z_r$.)

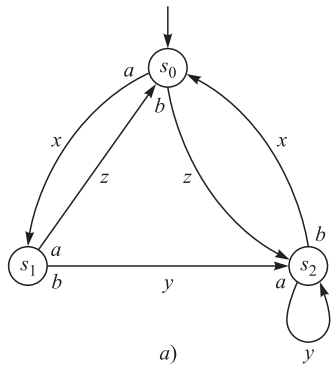
Entonces hay una arista dirigida de s_i a s_k identificado por el par a_j a z_r. Suele acostumbrarse colocar el símbolo de entrada a_j cerca de la base de la flecha (próximo a s_i) y colocar el signo de salida z_r cerca del centro de la flecha.

d) Se empieza en el estado inicial s_0 y se realiza un desplazamiento de estado a estado mediante las flechas que están identificadas, respectivamente, por los símbolos de entrada dados como sigue:

$$s_0 \xrightarrow{a} s_1 \xrightarrow{a} s_3 \xrightarrow{b} s_2 \xrightarrow{a} s_1 \xrightarrow{b} s_1 \xrightarrow{a} s_3 \xrightarrow{a} s_0 \xrightarrow{b} s_2 \xrightarrow{b} s_0 \xrightarrow{a} s_1 \xrightarrow{b} s_1$$

Los símbolos de salida sobre las flechas anteriores producen la palabra de salida $v = xyxzzyzxxz$ requerida.

13.2 Sea M la máquina de estados finitos con conjunto de entrada $A = \{a, b\}$, conjunto de salida $Z = \{x, y, z\}$, y diagrama de estado $D = D(M)$ que se muestra en la figura 13-5*a*).



a)

F	a	b
s_0	s_1, x	s_2, z
s_1	s_0, z	s_2, y
s_2	s_2, y	s_0, x

b)

Figura 13-5

a) Construya la tabla de estado de M.

b) Encuentre la palabra v de salida si la entrada es la palabra: *i*) $w = a^2b^2abab$; *ii*) $w = abab^3a^2$.

a) La tabla de estado se muestra en la figura 13-5*b*). Puesto que s_0 es el estado inicial, se escribe primero.

También, $F(s_i, a_j) = (s_k, z_r)$ si hay una arista dirigida de s_i a s_k identificado por el par a_j, z_r.

b) El desplazamiento se realiza de estado a estado por las flechas que están identificadas, respectivamente, por los símbolos de entrada dados a fin de obtener la siguiente salida: *i*) $v = xz^2x^2y^2x$; *ii*) $v = xy^2xzxx^2z$.

MÁQUINAS DE TURING

13.3 Sea M una máquina de Turing. Determine la ilustración α correspondiente a cada situación:

a) M se encuentra en el estado s_3 y escanea a la tercera letra de la expresión de cinta $w = aabca$.

b) M se encuentra en el estado s_2 y escanea a la tercera letra de la expresión de cinta $w = abca$.
c) La entrada es la expresión de cinta $w = 1^4B1^2$.

La ilustración α se obtiene al colocar el símbolo de estado antes de escanear la letra de cinta. Al inicio M se encuentra en el estado s_0 escaneando la primera letra de una entrada. Así,

a) $\alpha = aas_3bca$; *b*) $\alpha = abcs_2a$; *c*) $\alpha = s_0 1111B11$.

13.4 Suponga que $\alpha = aas_2bca$ es una ilustración. Encuentre β tal que $\alpha \rightarrow \beta$ si la máquina de Turing M tiene la quíntupla q donde *a*) $q = s_2bas_1L$; *b*) $q = s_2bbs_3R$; *c*) $q = s_2bas_2R$; *d*) $q = s_3abs_1L$.

a) Aquí M borra b y escribe a, cambia su estado a s_1 y se mueve a la izquierda. Así, $\beta = as_1aaa$.
b) Aquí M no cambia la letra escaneada b, cambia su estado a s_3 y se mueve a la derecha. Así, $\beta = aabs_3a$.
c) Aquí M borra b y escribe a, mantiene su estado s_2 y se mueve a la derecha. Así, $\beta = aaas_2a$.
d) Aquí q no tiene ningún efecto sobre α puesto que q no empieza con s_2b.

13.5 Sea $A = \{a, b\}$ y sea $L = \{a^r b^s \mid r > 0, s > 0\}$; es decir, L consiste de todas las palabras W que empiezan con una o más a seguidas por una o más b. Encuentre una máquina de Turing M que reconozca a L.

La estrategia es que se quiere que M haga lo siguiente: 1) se mueva a la derecha sobre todas las a, 2) se mueva a la derecha sobre todas las b y 3) se detenga en el estado de aceptación s_Y cuando encuentre el símbolo en blanco B. Esto lo realizan las siguientes quíntuplas:

$$q_1 = s_0aas_1R, \quad q_2 = s_1aas_1R, \quad q_3 = s_1bbs_2R, \quad q_4 = s_2bbs_2R, \quad q_5 = s_2BBs_YR.$$

En específico, q_1 y q_2 hacen 1); q_3 y q_4 hacen 2); y q_5 hace 3).

Sin embargo, también se quiere que M no acepte una palabra de entrada W que no pertenezca a L. Por tanto, también se requieren las siguientes quíntuplas:

$$q_6 = s_0BBs_NR, \quad q_7 = s_0bbs_NR, \quad q_8 = s_1BBs_NR, \quad q_9 = s_2aas_NR.$$

Aquí q_6 se usa si la entrada $W = \lambda = B$, es la palabra vacía; q_7 se usa si la entrada W es una expresión que empieza con b; q_8 se usa si la entrada W sólo contiene letras a, y q_9 se usa si la entrada W contiene la letra a a continuación de una letra b.

FUNCIONES COMPUTABLES

13.6 Encuentre $\langle m \rangle$ si: *a*) $m = 5$; *b*) $m = (4, 0, 3)$; *c*) $m = (3, -2, 5)$.

Recuerde que $\langle n \rangle = 1^{n+1} = 11^n$ y $\langle (n_1, n_2, \ldots n_r) \rangle = \langle n_1 \rangle B \langle n_2 \rangle B \cdots B \langle n_r \rangle$. Por tanto,

a) $\langle m \rangle = 1^6 = 111111$
b) $\langle m \rangle = 1^5B1^1B1^4 = 11111B1B1111$.
c) $\langle m \rangle$ no está definido para enteros negativos.

13.7 Encuentre $[E]$ para las expresiones:

a) $E = a\text{l}\,\text{ls}_2Bb11111$; *c*) $E = \langle m \rangle$ donde $m = (4, 1, 2)$;
b) $E = aas_3bb$; *d*) $E = \langle m \rangle$ donde $m = (n_1, n_2, \ldots, n_r)$.

Recuerde que $[E]$ cuenta el número de unos en E. Así:

a) $[E] = 5$; *b*) $[E] = 0$; *c*) $[E] = 10$ puesto que $E = 1^5B1^2B1^3$;
d) $[E] = n_1 + n_2 + \cdots + n_r + r$ puesto que el número de números 1 con los que contribuye cada n_k a E es $n_k + 1$.

13.8 Sea f la función $f(n) = n - 1$ cuando $n > 0$ y $f(0) = 0$. Demuestre que f es computable.

Es necesario encontrar una máquina de Turing M que compute f. En este caso se quiere que M borre dos de los unos en la entrada $\langle n \rangle$ cuando $n > 0$, pero sólo uno cuando $n = 0$. Esto se logra con las siguientes quíntuplas:

$$q_1 = s_0 1Bs_1R, \quad q_2 = s_1BBs_HR, \quad q_3 = s_1 1Bs_HR$$

Aquí q_1 borra el primer 1 y mueve a M a la derecha. Si sólo hay un 1, entonces M ahora está escaneando un símbolo en blanco B y q_2 indica a la computadora que se detenga. En caso contrario, q_3 borra el segundo 1 y detiene a M.

13.9 Sea f la función $f(x, y) = y$. Demuestre que f es computable.

Es necesario encontrar una máquina de Turing M que calcule a f. En específico, se quiere que M borre todos los números 1 de $\langle x \rangle$ y uno de los 1 de $\langle y \rangle$. Esto se logra con las siguientes quíntuplas:

$$q_1 = s_0 1 B s_1 R, \quad q_2 = s_0 B B s_1 R, \quad q_3 = s_1 1 B s_H R$$

Aquí q_1 borra todos los 1 en $\langle x \rangle$ mientras mueve a M a la derecha. Cuando M escanea el espacio en blanco divisorio B, q_2 cambia el estado de M de s_0 a s_1 y mueve a M a la derecha. Luego q_3 borra el primer 1 en $\langle y \rangle$ y detiene a M.

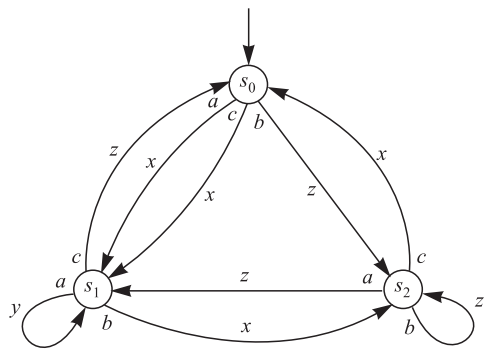
PROBLEMAS SUPLEMENTARIOS

MÁQUINAS DE ESTADOS FINITOS

13.10 Sea M la máquina de estados finitos cuya tabla de estado se muestra en la figura 13-6*a*).

F	a	b
s_0	s_2, y	s_1, z
s_1	s_2, x	s_3, y
s_2	s_2, y	s_1, z
s_3	s_3, z	s_0, x

a)



b)

Figura 13-6

a) Encuentre el conjunto de entrada A, el conjunto de estados S, el conjunto de salida Z y el estado inicial de M.

b) Dibuje el diagrama de estado $D = D(M)$ de M.

c) Encuentre la palabra v de salida si la entrada es la palabra: *i*) $w = ab^3a^2ba^3b$; *ii*) $w = a^2b^2ab^2a^2b$.

13.11 Sea M la máquina de estados finitos con conjunto de entrada $A = \{a, b, c\}$, conjunto de salida $Z = \{x, y, z\}$ y diagrama de estado $D = D(M)$ que se muestran en la figura 13-6*b*).

a) Construya la tabla de estado de M.

b) Encuentre la palabra v de salida si la entrada es la palabra: *i*) $w = a^2c^2b^2cab^3$; *ii*) $w = ca^2b^2ac^2ab$.

13.12 Sea M la máquina de estados finitos con conjunto de entrada $A = \{a, b\}$, conjunto de salida $Z = \{x, y, z\}$ y diagrama de estado $D = D(M)$ que se muestran en la figura 13-7*a*). Encuentre la palabra v de salida si la entrada es la palabra:

a) $w = ab^3a^2ba^3b$; *b*) $w = aba^2b^2ab^2a^2ba^2$.

13.13 Repita el problema 13.12 para el diagrama de estado $D = D(M)$ que se muestra en la figura 13-7*b*).

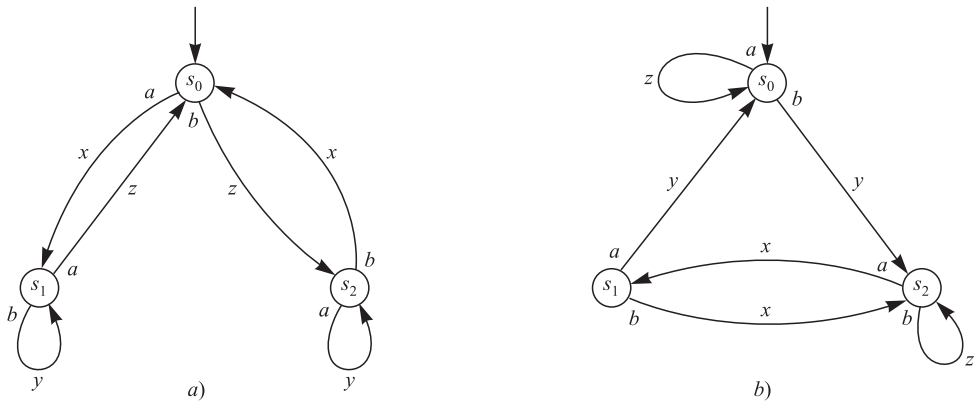


Figura 13-7

MÁQUINAS DE TURING

13.14 Sea M una máquina de Turing. Determine la ilustración α correspondiente a cada situación:

a) M se encuentra en el estado s_2, escaneando la tercera letra de la expresión de cinta $w = abbaa$.
b) M se encuentra en el estado s_3, escaneando la última letra de la expresión de cinta $w = aabb$.
c) La entrada es la palabra $W = a^3b^3$.
d) La entrada es la expresión de cinta $W = \langle(3, 2)\rangle$.

13.15 Suponga que $\alpha = abs^2aa$ es una ilustración. Encuentre β tal que $\alpha \rightarrow \beta$ si la máquina de Turing M tiene la quíntupla q donde:

a) $q = s_2abs_1R$; *b*) $q = s_2aas_3L$; *c*) $q = s_2abs_2R$;
d) $q = s_2abs_3L$; *e*) $q = s_3abs_2R$; *f*) $q = s_2aas_2L$.

13.16 Repita el problema 13.15 para la ilustración $\alpha = s_2aBab$.

13.17 Encuentre ilustraciones distintas α_1, α_2, α_3, α_4 y una máquina de Turing M tales que la siguiente secuencia no termine:

$$\alpha_1 \rightarrow \alpha_2 \rightarrow \alpha_3 \rightarrow \alpha_4 \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \cdots$$

13.18 Suponga que $\alpha \rightarrow \beta_1$ y $\alpha \rightarrow \beta_2$. ¿Debe cumplirse $\beta_1 \rightarrow \beta_2$?

13.19 Suponga que $\alpha = \alpha(W)$ para alguna entrada W, y suponga que $\alpha \rightarrow \beta \rightarrow \alpha$. ¿$M$ puede reconocer a W?

13.20 Sea $A = \{a, b\}$. Encuentre una máquina de Turing M que reconozca el lenguaje $L = \{ab^n \mid n > 0\}$; es decir, donde L consta de todas las palabras W que empiezan con una a y están seguidas por una o más b.

13.21 Sea $A = \{a, b\}$. Encuentre una máquina de Turing M que reconozca el lenguaje finito $L = \{a, a^2\}$; es decir, donde L consta de las dos primeras potencias de a distintas de cero.

FUNCIONES COMPUTABLES

13.22 Encuentre $\langle m\rangle$ si: *a*) $m = 6$; *b*) $m = (5, 0, 3, 1)$; *c*) $m = (0, 0, 0)$; *d*) $m = (2, 3, -1)$

13.23 Encuentre $[E]$ para las expresiones: *a*) $E = 111s_2aa1B111$; *b*) $E = a11bs_1Bb$; *c*) $E = \langle m\rangle$ donde $m = (2, 5, 4)$.

13.24 Sea f la función $f(n) = n - 2$ cuando $n > 1$ y $f(n) = 0$ cuando $n = 0$ o 1. Demuestre que f es computable.

13.25 Sea f la función $f(x, y) = x$. Demuestre que f es computable.

Respuestas a los problemas suplementarios

13.10 *a*) $A = (a, b)$, $S = \{s_0, s_1, s_2\}$, $Z = \{x, y, z\}$ y s_0 es el estado inicial. *b*) Vea la figura 13-8*a*).
c) $v = y^2zyzxzxyz$.

13.11 *a*) Vea la figura 13-8*b*) *i*) $v = xyz^2x^2zx^3z^2$,
ii) $v = xy^2xz^3xyx$.

13.12 *a*) $xy^3zxyzxz^2$; *b*) $xyzxy^2z^2x^2z^2y^2$.

13.13 *a*) zyz^2xy^2xyzy; *b*) $zyxy^2zx^2zxy^2xy$.

13.14 *a*) $\alpha = abs_2baa$; *b*) $\alpha = aabs_3b$; *c*) $\alpha = s_0aaabbb$;
d) $\alpha = s_01111B111$.

13.15 *a*) $\beta = abbs_3a$; *b*) $\beta = as_3baa$; *c*) $\beta = abbs_2a$;
d) $\beta = as_3bba$;
e) α no es modificada por q;
f) $\beta = as_2baa$.

13.16 *a*) $\beta = bs_1Bab$; *b*) $\beta = s_3BaBab$; *c*) $\beta = bs_2Bab$;
d) $\beta = s_3BbBab$
e) α no es modificada por q;
f) $\beta = s_2BaBab$.

13.17 $\alpha_1 = s_0ab$, $\alpha_2 = bs_1b$, $\alpha_3 = s_2bb$, $\alpha_4 = as_3b$;
$q_1 = s_0abs_1R$, $q_2 = s_1bbs_2L$, $q_3 = s_2bas_3R$,
$q_4 = s_3bbs_0L$.

13.18 Sí.

13.19 No, puesto que $\alpha \rightarrow \beta \rightarrow \alpha \rightarrow \beta \rightarrow \alpha \rightarrow \beta \rightarrow \cdots$ no termina nunca.

13.20 $q_1 = s_0BBs_NR$ *(NO)*; $q_2 = s_0bbs_NR$ (NO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_NR$ (NO); $q_5 = s_1aas_NR$ (NO); $q_6 = s_1bbs_NR$; $q_7 = s_2bbs_2R$; $q_8 = s_2aas_NR$ (NO); $q_9 = s_2BBs_YR$ (YES).

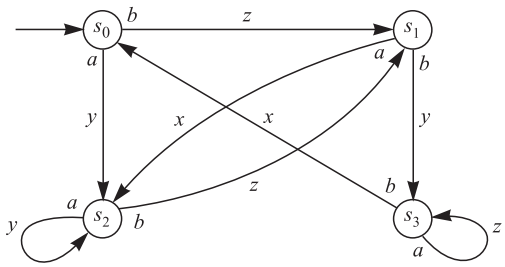
13.21 $q_1 = s_0BBs_NR$ (NO); $q_2 = s_0bbs_NR$ (NO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_YR$ (YES);
$q_5 = s_1bbs_NR$ (NO); $q_6 = s_1aas_2R$; $q_7 = s_2BBs_YR$ (YES); $q_8 = s_2aas_NR$ (NO); $q_9 = s_2bbs_NR$ (NO).

13.22 *a*) $\langle 6 \rangle = 1^7$; *b*) $\langle m \rangle = 1^6B1B1^4B1^2$;
c) $\langle m \rangle = 1B1B1$; *d*) no está definido.

13.23 *a*) $[E] = 7$; *b*) $[E] = 2$; *c*) $[E] = 14$.

13.24 Estrategia: borrar los tres primeros 1
$q_1 = S_01Bs_1R$; $q_2 = s_1BBs_HR$ (HALT); $q3 = s_11Bs_2R$; $q_4 = s_2BBs_HR$ (HALT); $q_5 = s_2BBs_HR$ (HALT).

13.25 Estrategia: borrar el primer 1 y luego todos los 1 después de *B*.
$q_1 = s_01Bs_1R$; $q_2 = s_111s_1R$; $q^3 = s_1BBs_2R$;
$q_4 = s_21Bs_3R$; $q_5 = s_31Bs_3R$; $q_6 = s_3BBs_HR$ (HALT).



a)

F	a	b	c
s_0	s_1, x	s_2, z	s_1, x
s_1	s_1, y	s_2, z	s_0, z
s_0	s_1, z	s_2, x	s_0, x

b)

Figura 13-8

14 Conjuntos ordenados y retículos

CAPÍTULO

14.1 INTRODUCCIÓN

Las relaciones de orden y precedencia aparecen en muchas partes de las matemáticas y computación. En este capítulo se precisan estas nociones. También se define al retículo, que es un tipo especial de conjunto ordenado.

14.2 CONJUNTOS ORDENADOS

Suponga que R es una relación sobre un conjunto S, que satisface las tres propiedades siguientes:

[$\mathbf{O}_1$] (Reflexiva) Para $a \in S$ arbitrario, se tiene aRa.

[$\mathbf{O}_2$] (Antisimétrica) Si aRb y bRa, entonces $a = b$.

[$\mathbf{O}_3$] (Transitiva) Si aRb y bRc, entonces aRc.

Entonces R se denomina *orden parcial* o, simplemente, una relación de *orden*, y se dice que R define un *orden* (u *ordenamiento*) *parcial* de S. El conjunto S con el orden parcial se denomina *conjunto parcialmente ordenado* o, simplemente, *conjunto ordenado*, o *conjunto PO*. Se escribe (S, R) cuando se desea especificar la relación R.

La relación de orden más conocida, que se denomina *orden usual*, es la relación $\leq$ (que se lee "menor o igual que") sobre los enteros positivos **N** o, en forma más general, sobre cualquier subconjunto de los números reales **R**. Debido a esto, una relación de orden parcial suele denotarse por $\preceq$; y

$$a \preceq b$$

se lee "a precede a b". En este caso también se escribe:

$a \prec b$ significa $a \preceq b$ y $a \neq b$; que se lee "a precede estrictamente a b".
$b \succeq a$ significa $a \preceq b$; que se lee "b sucede a a".
$b \succ a$ significa $a \prec b$; que se lee "b sucede estrictamente a a".
$\not\preceq$, $\not\prec$, $\not\succeq$ y $\not\succ$ son evidentes.

Cuando no hay ambigüedad, suelen usarse a menudo los símbolos $\leq$, $<$, $>$ y $\geq$ en lugar de $\preceq$, $\prec$, $\succ$ y $\succeq$, respectivamente.

EJEMPLO 14.1

a) Sea S cualquier colección de conjuntos. La relación $\subseteq$ de inclusión de conjuntos es un orden parcial de S. Específicamente, $A \subseteq A$ para cualquier conjunto A; si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$; y si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

b) Considere el conjunto $\mathbf{N}$ de enteros positivos. Se dice que "a divide a b", lo que se escribe $a|b$, si existe un entero c tal que $ac = b$. Por ejemplo, $2|4$, $3|12$, $7|21$ y así sucesivamente. Esta relación de divisibilidad es un orden parcial de $\mathbf{N}$.

c) La relación "|" de divisibilidad no es un orden del conjunto $\mathbf{Z}$ de enteros. Con más precisión, la relación no es antisimétrica. Por ejemplo, $2|-2$ y $-2|2$, pero $2 \neq -2$.

d) Considere el conjunto $\mathbf{Z}$ de enteros. aRb se define si hay un entero positivo r tal que $b = a^r$. Por ejemplo, $2\ R\ 8$, puesto que $8 = 2^3$. Así, R es un ordenamiento parcial de $\mathbf{Z}$.

Orden dual

Sea $\precsim$ cualquier orden parcial de un conjunto S. La relación $\succsim$; es decir, a sucede a b, también es un orden parcial de S; se denomina *orden dual*. Observe que $a \precsim b$ si y sólo si $b \succsim a$; por tanto, el orden dual $\succsim$ es la inversa de la relación $\precsim$; es decir, $\succsim = \precsim^{-1}$.

Subconjuntos ordenados

Sea A un subconjunto de un conjunto ordenado S, y suponga que $a, b \in A$. $a \precsim b$ se define como elementos de A siempre que $a \precsim b$ sean elementos de S. Esto define un orden parcial de A que se denomina *orden inducido* sobre A. El subconjunto A con el orden inducido se denomina *subconjunto ordenado* de S. A menos que se establezca o implique otra cosa, cualquier subconjunto de un conjunto ordenado S se trata como un subconjunto ordenado de S.

Cuasiorden

Suponga que $\prec$ es una relación sobre un conjunto S que satisface las dos propiedades siguientes:

$[\mathbf{Q}_1]$ (Irreflexiva) Para cualquier $a \in A$, se tiene $a \not\prec a$.

$[\mathbf{Q}_2]$ (Transitiva) Si $a \prec b$ y $b \prec c$, entonces $a \prec c$.

Entonces $\prec$ se denomina *cuasiorden* sobre S.

Hay una relación bastante estrecha entre los órdenes parciales y los cuasiórdenes. En este caso, si $\precsim$ es un orden parcial sobre un conjunto S y se define $a \prec b$, para indicar $a \precsim b$ pero $a \neq b$, entonces $\prec$ es un cuasiorden sobre S. A la inversa, si $\prec$ es un cuasiorden sobre un conjunto S y se define $a \precsim b$ para indicar $a \prec b$ o $a = b$, entonces $\precsim$ es un orden parcial sobre S. Esto permite elegir entre un orden parcial y sus cuasiórdenes correspondientes, depende de cuál sea más conveniente.

Comparabilidad, conjuntos linealmente ordenados

Suponga que a y b son elementos en un conjunto S parcialmente ordenado. Se dice que a y b son *comparables* si

$$a \precsim b \quad \text{o} \quad b \precsim a$$

es decir, si uno precede al otro. Por tanto, a y b no son comparables, lo que se escribe

$$a \parallel b$$

si ni $a \precsim b$ ni $b \precsim a$.

La palabra "parcial" se usa para definir un conjunto S parcialmente ordenado, puesto que algunos de los elementos de S no requieren ser comparables. Suponga, por otra parte, que todo par de elementos de S son comparables. Entonces se dice que S está *totalmente ordenado* o *linealmente ordenado*, y entonces S se denomina *cadena*. Aunque un conjunto ordenado S puede no estar linealmente ordenado, es posible que un subconjunto A de S esté linealmente ordenado. Resulta evidente que cualquier subconjunto de un conjunto S linealmente ordenado también debe estar linealmente ordenado.

EJEMPLO 14.2

a) Considere el conjunto **N** de enteros positivos ordenados por divisibilidad. Entonces 21 y 7 son comparables puesto que 7|21. Por otra parte, 3 y 5 no son comparables porque ni 3|5 ni 5|3. Así, **N** no está linealmente ordenado por divisibilidad. Observe que $A = \{2, 6, 12, 36\}$ es un subconjunto linealmente ordenado de **N** puesto que 2|6, 6|12 y 12|36.

b) El conjunto **N** de enteros positivos con el orden usual $\leq$ (menor o igual que) está linealmente ordenado y entonces todo subconjunto ordenado de **N** también está linealmente ordenado.

c) El conjunto potencia $P(A)$ de un conjunto A con dos o más elementos no está linealmente ordenado por inclusión de conjuntos. Por ejemplo, suponga que a y b pertenecen a A. Entonces $\{a\}$ y $\{b\}$ no son comparables. Observe que el conjunto vacío $\varnothing$, $\{a\}$ y A constituyen un subconjunto linealmente ordenado de $P(A)$, puesto que $\varnothing \subseteq \{a\} \subseteq A$. En forma semejante, $\varnothing$, $\{b\}$ y A constituyen un subconjunto linealmente ordenado de $P(A)$.

Conjuntos producto y orden

Hay muchas formas de definir una relación de orden sobre el producto cartesiano de conjuntos ordenados dados. A continuación se muestran dos de ellas:

a) ***Orden producto*:** Suponga que S y T son conjuntos ordenados. Entonces la siguiente relación es de orden sobre el conjunto producto $S \times T$, que se denomina *orden producto*:

$$(a, b) \precsim (a', b') \quad \text{si} \quad a \leq a' \text{ y } b \leq b'$$

b) ***Orden lexicográfico*:** Suponga que S y T son conjuntos linealmente ordenados. Entonces la siguiente relación es de orden sobre el conjunto producto $S \times T$, que se denomina *orden lexicográfico* u *orden del diccionario*:

$$(a, b) < (a', b') \quad \text{si} \quad a < b \quad \text{o si} \quad a = a' \text{ y } b < b'$$

Este orden se puede extender a $S_1 \times S_2 \times \cdots \times S_n$ como sigue:

$$(a_1, a_2, \ldots, a_n) \prec (a'_1, a'_2, \ldots, a'_n) \quad \text{si} \quad a_i = a'_i \text{ para } i = 1, 2, \ldots, k-1 \text{ y } a_k < a'_k$$

Observe que el orden lexicográfico también es lineal.

Cerradura de Kleene y orden

Sea A un alfabeto linealmente ordenado (no vacío). Recuerde que A^*, denominada cerradura de Kleene de A, consta de todas las palabras w sobre A y que $|w|$ denota la longitud de w. Así, las siguientes son dos relaciones de orden sobre A^*.

a) ***Orden alfabético (lexicográfico)*:** Sin duda, el lector ya conoce el orden alfabético de A^*. Es decir:

i) $\lambda \prec w$, donde λ es la palabra vacía y w es cualquier palabra no vacía.

ii) Suponga que $u = au'$ y $v = bv'$ son palabras no vacías distintas, donde $a, b \in A$ y $u', v' \in A^*$. Entonces

$$u \prec v \quad \text{si } a < b \quad \text{o} \quad \text{si } a = b \text{ pero } u' \prec v'$$

b) ***Orden Short-lex*:** Aquí A^* está ordenado primero por longitud y luego alfabéticamente. Es decir, para palabras distintas u, v en A^*,

$$u \prec v \quad \text{si } |u| < |v| \quad \text{o} \quad \text{si } |u| = |v| \text{ pero } u \text{ precede a } v \text{ alfabéticamente}$$

Por ejemplo, "ya" precede a "mas", ya que $|\text{ya}| = 2$ pero $|\text{mas}| = 3$. Sin embargo, "si" precede a "ya" puesto que tienen la misma longitud, pero "si" precede a "ya" alfabéticamente. Este orden también se denomina *orden de semigrupo libre*.

14.3 DIAGRAMAS DE HASSE DE CONJUNTOS PARCIALMENTE ORDENADOS

Sea S un conjunto parcialmente ordenado y suponga que a, b pertenecen a S. Se dice que a es un *predecesor inmediato* de b, o que b es un *sucesor inmediato* de a, o que b es una *cubierta* de a, lo que se escribe

$$a \ll b$$

si $a < b$ pero ningún elemento de S está entre a y b; es decir, en S no hay ningún elemento c tal que $a < c < b$.

Suponga que S es un conjunto finito parcialmente ordenado. Entonces el orden en S se conoce por completo una vez que se conocen todos los pares a, b en S tales que $a \ll b$; es decir, una vez que se conoce la relación $\ll$ sobre S. Esto se concluye del hecho de que $x < y$ si y sólo si $x \ll y$ o si existen elementos $a_1, a_2, \ldots,$ en S tales que

$$x \ll a_1 \ll a_2 \ll \cdots \ll a_m \ll y$$

El *diagrama de Hasse* de un conjunto finito parcialmente ordenado es el grafo dirigido cuyas aristas son los elementos de S y hay una arista dirigida de a a b siempre que $a \ll b$ en S. (En lugar de trazar una flecha de a a b, algunas veces b se coloca más alto que a y se traza una línea entre ellas. Así, se sobrentiende que el movimiento hacia arriba indica sucesión.) En el diagrama así creado, hay una arista dirigida del vértice x al vértice y si y sólo si $x \ll y$. También, en el diagrama de S no puede haber ciclos (dirigidos) puesto que la relación de orden es antisimétrica.

El diagrama de Hasse en un conjunto PO S es una ilustración de S; por tanto, resulta muy útil para describir tipos de elementos en S. Algunas veces un conjunto parcialmente ordenado se define al presentar simplemente su diagrama de Hasse. Se observa que el diagrama de Hasse de un conjunto PO S no necesita ser conexo.

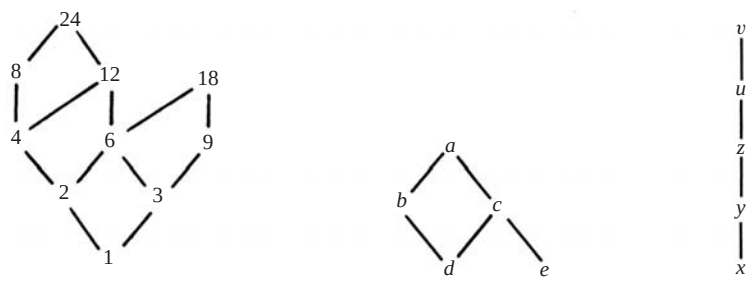
Observación: Resulta que el diagrama de Hasse de un conjunto PO finito S es un grafo dirigido libre de ciclos, que se estudió en la sección 9.9. La investigación aquí es independiente de la investigación previa. Aquí principalmente el orden se considera en términos de "menor que" o "mayor que", en lugar de hacerlo en términos de relaciones de adyacencia dirigidas. En consecuencia, los contenidos a veces se traslapan.

EJEMPLO 14.3

a) Sea $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ ordenado por la relación "x divide a y". El diagrama de A se muestra en la figura 14-1*a*). (A diferencia de los árboles con raíz, la dirección de una línea en el diagrama de un conjunto parcialmente ordenado siempre es hacia arriba.)

b) Sea $B = \{a, b, c, d, e\}$. El diagrama en la figura 14-1*b*) define un orden parcial sobre B en la forma natural. Es decir, $d \leq b$, $d \leq a$, $e \leq c$ y así sucesivamente.

c) El diagrama de un conjunto ordenado linealmente finito; es decir, una cadena finita, consiste simplemente de un camino. Por ejemplo, en la figura 14-1*c*) se muestra al diagrama de una cadena con cinco elementos.



a) *b*) *c*)

Figura 14-1

EJEMPLO 14.4 Una *partición* de un entero positivo m es un conjunto de enteros positivos cuya suma es m. Por ejemplo, hay siete particiones de $m = 5$ como sigue:

$$5, \quad 3-2, \quad 2-2-1, \quad 1-1-1-1-1, \quad 4-1, \quad 3-1-1, \quad 2-1-1-1$$

Las particiones de un entero m tienen el siguiente orden. Una partición P_1 precede a una partición P_2 si los enteros en P_1 pueden sumarse para obtener los enteros de P_2 o, en forma equivalente, si los enteros en P_2 pueden subdividirse aún más para obtener los enteros de P_1. Por ejemplo,

$$2-2-1 \quad \text{precede a} \quad 3-2$$

puesto que $2 + 1 = 3$. Por otra parte, $3 - 1 - 1$ y $2 - 2 - 1$ no son comparables.

En la figura 14-2 se proporciona el diagrama de Hasse para las particiones de $m = 5$.

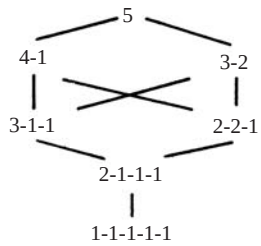


Figura 14-2

Elementos minimal, maximal, primero y último

Sea S un conjunto parcialmente ordenado. Un elemento a en S se denomina elemento *minimal* si ningún otro elemento de S precede estrictamente a (es menor que) a. En forma semejante, un elemento b en S se denomina elemento *maximal* si ningún otro elemento de S sucede estrictamente a (es mayor que) b. En términos geométricos, a es un elemento minimal si ninguna arista entra a a (desde abajo), y b es un elemento maximal si ninguna arista sale de b (en dirección hacia arriba). Se observa que S puede tener más de un elemento minimal y más de un elemento maximal.

Si S es infinito, entonces puede no tener elemento minimal ni elemento maximal. Por ejemplo, el conjunto $\mathbf{Z}$ de los enteros con el orden usual $\leq$ no tiene elemento minimal ni elemento maximal. Por otra parte, si S es finito, entonces S debe tener por lo menos un elemento minimal y por lo menos un elemento maximal.

Un elemento a en S se denomina *primer* elemento si para todo elemento x en S se tiene

$$a \preceq x$$

es decir, si a precede a cualquier otro elemento en S. En forma semejante, un elemento b en S se denomina *último* elemento si para cualquier elemento y en S se cumple

$$y \preceq b$$

es decir, si b sucede a cualquier otro elemento en S. Se observa que S puede tener cuando mucho un primer elemento, que debe ser el elemento minimal, y que S puede tener cuando mucho un último elemento, que debe ser el elemento maximal. En términos generales, S puede no tener ni un primer ni un último elemento, incluso cuando S es finito.

EJEMPLO 14.5

a) Considere los tres conjuntos parcialmente ordenados en el ejemplo 14.3, cuyos diagramas de Hasse se muestran en la figura 14-1.

- *i*) A tiene dos elementos maximales: 18 y 24 y ninguno es un último elemento. A sólo tiene un elemento minimal, 1, que también es un primer elemento.
- *ii*) B tiene dos elementos minimal: d y e y ninguno es un primer elemento. B sólo tiene un elemento maximal, a, que también es un último elemento.
- *iii*) La cadena tiene un elemento minimal, x, que es un primer elemento, y un elemento maximal, v, que es un último elemento.

b) Sea A cualquier conjunto no vacío y sea $P(A)$ el conjunto potencia de A ordenado por la inclusión de conjuntos. Entonces el conjunto vacío $\varnothing$ es un primer elemento de $P(A)$ puesto que, para cualquier conjunto X, se tiene $\varnothing \subseteq X$. Además, A es un último elemento de $P(A)$, ya que todo elemento Y de $P(A)$ es, por definición, un subconjunto de A; es decir, $Y \subseteq A$.

14.4 ENUMERACIÓN CONSISTENTE

Suponga que S es un conjunto finito ordenado parcialmente. A menudo es necesario asignar enteros positivos a los elementos de S de modo que se preserve el orden. Es decir, se busca una función $f: S \to \mathbf{N}$ de forma que si $a \prec b$, entonces $f(a) < f(b)$. Una función así se denomina *enumeración consistente* de S. El hecho de que esto siempre puede hacerse es el contenido del siguiente teorema.

Teorema 14.1: Existe una enumeración consistente para cualquier conjunto finito parcialmente ordenado A.

Este teorema se demuestra en el problema 14.18. De hecho, se demuestra que si S tiene n elementos, entonces existe una enumeración consistente $f: S \to \{1, 2, \ldots, n\}$.

Se recalca que tal enumeración no necesariamente tiene que ser única. Por ejemplo, a continuación se proporcionan dos enumeraciones así del conjunto parcialmente ordenado en la figura 14-1*b*):

i) $f(d) = 1, f(e) = 2, f(b) = 3, f(c) = 4, f(a) = 5.$

ii) $g(e) = 1, g(d) = 2, g(c) = 3, g(b) = 4, g(a) = 5.$

Sin embargo, la cadena en la figura 14-1*c*) sólo admite una enumeración consistente si el conjunto se transforma en $\{1, 2, 3, 4, 5\}$. Específicamente, es necesario asignar:

$$h(x) = 1, \quad h(y) = 2, \quad h(z) = 3, \quad h(u) = 4, \quad h(v) = 5$$

14.5 SUPREMO E ÍNFIMO

Sea A un subconjunto de un conjunto parcialmente ordenado S. Un elemento M en S se denomina *cota superior* de A si M sucede a cualquier elemento de A; es decir, si, para toda x en A, se tiene

$$x \precsim M$$

Si una cota superior de A precede a cualquier cota superior de A, entonces se denomina *supremo* (*supremum*) de A y se denota por

$$\sup(A)$$

También se escribe $\sup(a_1, \ldots, a_n)$ en lugar de $\sup(A)$ si A consiste de los elementos $a_1, \ldots, a_n$. Se recalca que cuando mucho puede haber un $\sup(A)$; sin embargo, $\sup(A)$ puede no existir.

En forma semejante, un elemento m en un conjunto parcialmente ordenado S se denomina *cota inferior* de un subconjunto A de S si m precede a cualquier elemento de A; es decir, si, para cualquier y en A, se tiene

$$m \precsim y$$

Si una cota inferior de A sucede a cualquier otro elemento de A, entonces se denomina *ínfimo* de A y se denota por

$$\text{ínf}(A) \quad \text{o} \quad \text{ínf}(a_1, \ldots, a_n)$$

si A consta de los elementos $a_1, \ldots, a_n$. Puede haber cuando mucho un $\text{ínf}(A)$, aunque $\text{ínf}(A)$ puede no existir.

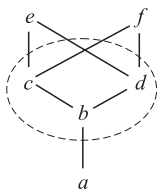
En algunos textos se usa la expresión *mínima cota superior* en lugar de supremo y entonces se escribe mcs(A) en vez de $\sup(A)$, y se usa el término *máxima cota inferior* en lugar de ínfimo y se escribe $\text{mci}(A)$ en vez de $\text{ínf}(A)$.

Si A tiene una cota superior, se dice que A está *acotado por arriba*, y si A tiene una cota inferior, se dice que A está *acotado por abajo*. En particular, A está acotado si A tiene una cota superior y una cota inferior.

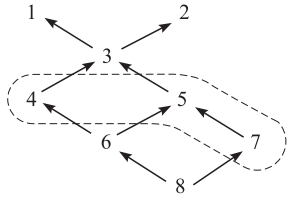
EJEMPLO 14.6

a) Sea $S = \{a, b, c, d, e, f\}$ ordenado como se muestra en la figura 14-3*a*), y sea $A = \{b, c, d\}$. Las cotas superiores de A son e y f puesto que sólo e y f suceden a todo elemento en A. Las cotas inferiores de A son a y b puesto que sólo a y b preceden a todo elemento en A. Observe que e y f no son comparables; por tanto, sup(A) no existe. Sin embargo, b también sucede a a, de modo que ínf(A) $= b$.

b) Sea $S = \{1, 2, 3, \ldots, 8\}$ ordenado como se muestra en la figura 14-3*b*), y sea $A = \{4, 5, 7\}$. Las cotas superiores de A son 1, 2 y 3, y la única cota inferior es 8. Observe que 7 no es una cota inferior puesto que 7 no precede a 4. Aquí sup(A) $= 3$, ya que 3 precede a las otras cotas superiores 1 y 2. Observe que ínf(A) $= 8$ porque 8 es la única cota inferior.



a)



b)

Figura 14-3

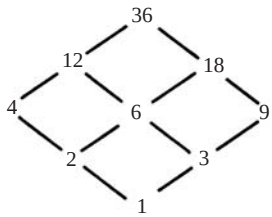


Figura 14-4

En términos generales, sup(a, b) e ínf(a, b) no necesariamente existen para todo par de elementos a y b en un conjunto parcialmente ordenado S. A continuación se proporcionan dos ejemplos de conjuntos parcialmente ordenados donde sup(a, b) e ínf(a, b) existen para todo a, b en el conjunto.

EJEMPLO 14.7

a) Sea **N** el conjunto de enteros positivos ordenados por divisibilidad. El *máximo común divisor* de a y b en **N** se denota con

$$\text{mcd}(a, b)$$

es el entero más grande que divide a a y a b. El *mínimo común múltiplo* de a y b se denota con

$$\text{mcm}(a, b)$$

es el entero más pequeño que es divisible entre a y b.

Un teorema importante en teoría de números establece que todo divisor común de a y b divide a mcd(a, b). También puede demostrarse que mcm(a, b) divide a todo múltiplo de a y b. Así,

$$\text{mcd}(a, b) = \text{ínf}(a, b) \text{ y } \text{mcm}(a, b) = \text{sup}(a, b)$$

En otras palabras, ínf(a, b) y sup(a, b) existen para cualquier par de elementos de **N** ordenado por divisibilidad.

b) Para todo entero positivo, sea $\mathbf{D}_m$ el conjunto de los divisores de m ordenados por divisibilidad. El diagrama de Hasse de

$$\mathbf{D}_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

se muestra en la figura 14-4. De nuevo, ínf(a, b) $=$ mcd(a, b) y sup(a, b) $=$ mcm(a, b) existen para cualquier par a, b en $\mathbf{D}_m$.

14.6 CONJUNTOS ORDENADOS (SEMEJANTES) ISOMORFOS

Suponga que X y Y son conjuntos parcialmente ordenados. Una función uno a uno (inyectiva) $f: X \to Y$ se denomina *transformación de semejanza* de X en Y si f preserva la relación de orden; es decir, si las dos condiciones siguientes se cumplen para cualquier par a y a' en X:

1) Si $a \precsim a'$ entonces $f(a) \precsim f(a')$.
2) Si $a \parallel a'$ (no comparables), entonces $f(a) \parallel f(a')$.

En consecuencia, si A y B están linealmente ordenados, entonces sólo 1) se requiere para que f sea una transformación de semejanza.

Se dice que dos conjuntos ordenados X y Y son *isomorfos* o *semejantes*, lo cual se escribe

$$X \simeq Y$$

si existe una correspondencia uno a uno (mapeo biyectivo) $f: X \to Y$ que preserva el orden de las relaciones; es decir, que es un mapeo de semejanza.

EJEMPLO 14.8 Suponga que $X = \{1, 2, 6, 8, 12\}$ está ordenado por divisibilidad y suponga que $Y = \{a, b, c, d, e\}$ es isomorfo a X; por ejemplo, la siguiente función f es una transformación de semejanza de X sobre Y:

$$f = \{(1, e), (2, d), (6, b), (8, c), (12, a)\}$$

Trazar el diagrama de Hasse de Y.

La transformación de semejanza preserva el orden del conjunto inicial X y es uno a uno y sobre. Por tanto, la transformación se considera simplemente como una retiquetación de los vértices en el diagrama de Hasse del conjunto inicial X. Los diagramas de Hasse tanto para X como para Y se muestran en la figura 14-5.

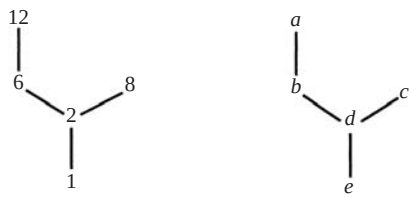


Figura 14-5

14.7 CONJUNTOS BIEN ORDENADOS

Se empieza con una definición.

Definición 14.1: Se dice que un conjunto ordenado está *bien ordenado* si todo subconjunto de S tiene un primer elemento.

El ejemplo clásico de un conjunto bien ordenado es el conjunto $\mathbf{N}$ de enteros positivos con el orden usual $\leq$. Los siguientes hechos se concluyen a partir de la definición.

1) Un conjunto bien ordenado está linealmente ordenado. Ya que si $a, b, \in S$, entonces $\{a, b\}$ tiene un primer elemento; por tanto, a y b son comparables.
2) Todo subconjunto de un conjunto bien ordenado está bien ordenado.
3) Si X está bien ordenado y Y es isomorfo a X, entonces Y está bien ordenado.
4) Todos los conjuntos finitos bien ordenados con el mismo número n de elementos están bien ordenados y todos son isomorfos entre sí. De hecho, todos son isomorfos a $\{1, 2, \ldots, n\}$ con el orden usual $\leq$.

5) Cualquier elemento $a \in S$ que no sea el último elemento, tiene un sucesor inmediato. Sea $M(a)$ el conjunto de elementos que suceden estrictamente a a. Entonces el primer elemento de $M(a)$ es el sucesor inmediato de a.

EJEMPLO 14.9

a) El conjunto **Z** de enteros con el orden usual $\leq$ está linealmente ordenado y todo elemento tiene un sucesor inmediato y un predecesor inmediato, pero **Z** no está bien ordenado. Por ejemplo, **Z** no tiene primer elemento. Sin embargo, cualquier subconjunto de **Z** que esté acotado por abajo está bien ordenado.

b) El conjunto **Q** de números racionales con el orden usual $\leq$ está linealmente ordenado, pero ningún elemento en **Q** tiene un sucesor inmediato o un predecesor inmediato. Sea $a, b \in Q$; por ejemplo, $a < b$, entonces $(a + b)/2 \in \mathbf{Q}$ y

$$a < \frac{a+b}{2} < b$$

c) Considere los conjuntos ordenados ajenos

$$A = \{1, 3, 5, \ldots,\} \quad \text{y} \quad B = \{2, 4, 6, \ldots\}$$

Entonces el siguiente conjunto ordenado

$$S = \{A; B\} = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

Está bien ordenado. Observe que, aparte del primer elemento 1, el elemento 2 no tiene un predecesor inmediato.

Notación: A partir de ahora y en adelante, si $A, B, \ldots,$ son conjuntos ordenados ajenos, entonces $\{A; B; \ldots\}$ significa el conjunto $A \cup B \cup \ldots$ ordenado por posiciones de izquierda a derecha; es decir, los elementos en el mismo conjunto preservan su orden, y cualquier elemento en un conjunto a la izquierda precede a cualquier elemento en un conjunto a la derecha. Así, todo elemento en A precede a todo elemento en B.

Inducción transfinita

Primero vuelve a plantearse el principio de inducción matemática. (Vea las secciones 1.8 y 11.3.)

Principio de inducción matemática: Sea A un subconjunto del conjunto **N** de enteros positivos con las dos propiedades siguientes:

i) $1 \in A$.
ii) Si $k \in A$, entonces $k + 1 \in A$.

Entonces $A = \mathbf{N}$.

El principio anterior es uno de los axiomas de Peano para los números naturales (enteros positivos) **N**. Hay otra forma que algunas veces es más conveniente usar. A saber:

Principio de inducción matemática (segunda forma): Sea A un subconjunto de **N** con las dos propiedades siguientes:

i) $1 \in A$.
ii) Si j pertenece a A para entonces $1 \leq j < k$, entonces $k \in A$.

Entonces $A = \mathbf{N}$.

La segunda forma de inducción es equivalente al hecho de que **N** está bien ordenado (teorema 11.6). De hecho, hay una proposición algo parecida que es verdadera para todo conjunto bien ordenado.

Principio de inducción transfinita: Sea A un subconjunto de un conjunto bien ordenado S con las siguientes propiedades:

i) $a_0 \in A$.
ii) Si $s(a) \subseteq A$, entonces $a \in A$.

Entonces $A = S$.

Aquí a_0 es el primer elemento de S y $s(a)$ es el *segmento inicial* de a que se define por ser el conjunto de todos los elementos de S que preceden estrictamente a a.

Axioma de elección y axioma del buen orden

Sea $\{A_i \mid i \in I\}$ una colección de conjuntos ajenos no vacíos. Se supone que todo $A_i \subseteq X$. Una función f: $\{A_i\} \to X$ se denomina *función elección* si $f(A_i) = a_i \in A_i$. En otras palabras, f "elige" un punto $a_i \in A_i$ para todo conjunto A_i.

El axioma de elección constituye una piedra angular de las matemáticas y, en particular, de la teoría de conjuntos. Este axioma "aparentemente inocente", que se presenta a continuación, tiene como consecuencia algunos de los resultados más importantes y poderosos.

Axioma de elección: Existe una función elección para cualquier colección no vacía de conjuntos ajenos no vacíos.

Una de las consecuencias del axioma de elección es el siguiente teorema, que se atribuye a Zermelo.

Teorema del buen orden: Cualquier conjunto S puede estar bien ordenado.

La demostración de este teorema rebasa el alcance de este texto. Además, puesto que las estructuras aquí presentadas son finitas o numerables, este teorema no es necesario. Basta la inducción matemática normal.

14.8 RETÍCULOS

Hay dos formas para definir un retículo (o latiz) L. Una es definirla en términos de un conjunto parcialmente ordenado. En específico, una retícula L puede definirse como un conjunto parcialmente ordenado en el cual ínf(a, b) y sup(a, b) existen para cualquier par de elementos $a, b \in L$. Otra forma es definir a L axiomáticamente. Esto se hace a continuación.

Axiomas que definen un retículo

Sea L un conjunto no vacío cerrado bajo dos operaciones binarias denominadas *encontrar* y *unir*, denotadas cada una por $\wedge$ y $\vee$. Entonces L se denomina *retícula* si se cumplen los siguientes axiomas, donde a, b y c son elementos de L:

[$\mathbf{L}_1$] Ley conmutativa:
$1a)$ $a \wedge b = b \wedge a$ $\qquad$ $1b)$ $a \vee b = b \vee a$

[$\mathbf{L}_2$] Ley asociativa:
$2a)$ $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ $\qquad$ $2b)$ $(a \vee b) \vee c = a \vee (b \vee c)$

[$\mathbf{L}_3$] Ley de absorción:
$3a)$ $a \wedge (a \vee b) = a$ $\qquad$ $3b)$ $a \vee (a \wedge b) = a$

Algunas veces el retículo se denota por $(L, \wedge, \vee)$ cuando se desea mostrar las operaciones relacionadas.

Dualidad y la ley idempotente

El *dual* de cualquier proposición en un retículo $(L, \wedge, \vee)$ se define por ser la proposición que se obtiene por el intercambio de $\wedge$ y $\vee$. Por ejemplo, el dual de

$$a \wedge (b \vee a) = a \vee a \text{ es } a \vee (b \wedge a) = a \wedge a$$

Observe que el dual de cada axioma de un retículo también es un axioma. En consecuencia, se cumple el principio de dualidad; es decir,

Teorema 14.2 (principio de dualidad): El dual de cualquier teorema sobre un retículo también es un teorema.

Esto se concluye a partir del hecho de que el teorema dual puede demostrarse mediante el dual de cada paso de la demostración del teorema original.

Una propiedad importante de los retículos se concluye a partir de la ley de absorción.

Teorema 14.3 (ley idempotente): *i*) $a \wedge a = a$; *ii*) $a \vee a = a$.

La demostración del inciso *i*) sólo requiere dos líneas:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge b)) && \text{(al usar (3}b\text{))} \\ &= a && \text{(al usar (3}a\text{))} \end{aligned}$$

La demostración del inciso *ii*) se sigue del principio de dualidad enunciado antes (o puede demostrarse en forma semejante).

Retículos y orden

Dada un retículo L, un orden parcial sobre L puede definirse como sigue:

$$a \precsim b \quad \text{si} \quad a \wedge b = a$$

En forma semejante, es posible definir

$$a \precsim b \quad \text{si} \quad a \vee b = b$$

Estos resultados se plantean como un teorema.

Teorema 14.4: Sea L un retículo. Entonces

i) $a \wedge b = a$ si y sólo si $a \vee b = b$.

ii) La relación $a \precsim b$ (definida por $a \wedge b = a$ o $a \vee b = b$) es un orden parcial sobre L.

Ahora que se tiene un orden parcial sobre cualquier retículo L, ésta puede representarse mediante un diagrama, como se hizo para conjuntos parcialmente ordenados en general.

EJEMPLO 14.10 Sea C una colección de conjuntos cerrados bajo la intersección y la unión. Entonces $(C, \cap, \cup)$ es un retículo. En este retículo la relación de orden parcial es la misma que la inclusión de conjuntos. En la figura 14-6 se muestra el diagrama del retículo L de todos los subconjuntos de (a, b, c).

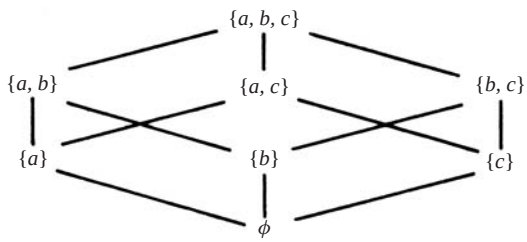


Figura 14-6

Se ha mostrado cómo definir un orden parcial sobre un retículo L. El siguiente teorema establece cuándo es posible definir un retículo sobre un conjunto parcialmente ordenado P de modo que el retículo devuelve el orden original sobre P.

Teorema 14.5: Sea P un conjunto parcialmente ordenado tal que ínf(a, b) y sup(a, b) existen para todo a, b en P. Al hacer

$$a \wedge b = \text{ínf}(a, b) \quad \text{y} \quad a \vee b = \sup(a, b)$$

se tiene que $(P, \wedge, \vee)$ es un retículo. Además, el orden parcial sobre P inducido por el retículo es el mismo que el orden parcial original sobre P.

La conversa del teorema anterior también es verdadera. Es decir, sea L un retículo y sea $\preceq$ el orden parcial inducido sobre L. Entonces ínf(a, b) y sup(a, b) existen para todo par a, b en L y el retículo obtenido a partir del conjunto parcialmente ordenado $(L, \preceq)$ es el retículo original. Entonces:

Definición alterna: Un retículo es un conjunto parcialmente ordenado en el cual

$$a \wedge b = \text{ínf}(a, b) \quad \text{y} \quad a \vee b = \sup(a, b)$$

existen para todo par de elementos a, b.

Primero se observa que cualquier conjunto parcialmente ordenado es un retículo, puesto que ínf$(a, b) = a$ y sup$(a, b) = b$ siempre que $a \preceq b$. Por el ejemplo 14.7, los enteros positivos $\mathbf{N}$ y el conjunto $\mathbf{D}_m$ de divisores de m son retículos bajo la relación de divisibilidad.

Subretículos, retículos isomorfos

Suponga que M es un subconjunto no vacío de un retículo L. Se dice que M es un *subretículo* de L si M mismo es un retículo (con respecto a las operaciones de L). Se observa que M es un subretículo de L si y sólo si M es cerrado bajo las operaciones de $\wedge$ y $\vee$ de L. Por ejemplo, el conjunto $\mathbf{D}_m$ de divisores de m es un subretículo de los enteros positivos $\mathbf{N}$ bajo divisibilidad. Se dice que dos retículos L y L' son *isomorfos* si existe una correspondencia uno a uno $f: L \to L'$ tal que

$$f(a \wedge b) = f(a) \wedge f(b) \quad \text{y} \quad f(a \vee b) = f(a) \vee f(b)$$

para elementos arbitrarios a y b en L.

14.9 RETÍCULOS ACOTADOS

Un retículo L tiene una *cota inferior* 0 si para cualquier elemento x en L se tiene $0 \preceq x$. En forma semejante, se dice que un retículo L tiene una *cota superior* I si para cualquier x en L se tiene $x \preceq I$. Se dice que L *está acotado* si L tiene tanto una cota inferior 0 como una cota superior I. Para este tipo de retículos se tienen las siguientes identidades

$$a \vee I = I, \quad a \wedge I = a, \quad a \vee 0 = a, \quad a \wedge 0 = 0$$

para cualquier elemento a en L.

Los enteros no negativos con el orden usual,

$$0 < 1 < 2 < 3 < 4 < \cdots$$

tienen a 0 como cota inferior pero no tienen cota superior. Por otra parte, el retículo $P(U)$ de todos los subconjuntos de cualquier conjunto universo $\mathbf{U}$ es un retículo acotado con $\mathbf{U}$ como una cota superior y el conjunto vacío $\varnothing$ como una cota inferior.

Suponga que $L = \{a_1, a_2, \ldots, a_n\}$ es un retículo infinito. Entonces

$$a_1 \vee a_2 \vee \cdots \vee an \quad \text{y} \quad a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

son cotas superior e inferior de L, respectivamente. Así, se tiene el siguiente

Teorema 14.6: Todo retículo finito L es acotado.

14.10 RETÍCULOS DISTRIBUTIVOS

Un retículo L es *distributivo* si para elementos arbitrarios a, b, c en L se tiene lo siguiente:
[$\mathbf{L}_4$] Ley distributiva:

$$4a)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad 4b)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

En caso contrario, se dice que L *no es distributivo*. Por el principio de dualidad se observa que la condición 4a) se cumple si y sólo si se cumple la condición 4b).

La figura 14-7a) es un retículo que no es distributivo puesto que

$$a \vee (b \wedge c) = a \vee 0 = a \quad \text{pero} \quad (a \vee b) \wedge (a \vee c) = I \wedge c = c$$

La figura 14-7b) también es un retículo que no es distributivo. De hecho, se tiene la siguiente caracterización de tales retículos.

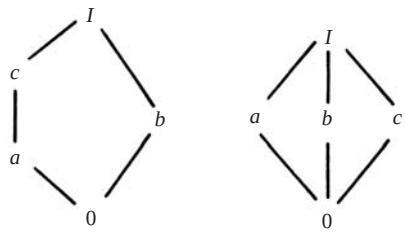


Figura 14-7

Teorema 14.7: Un retículo L no es distributivo si y sólo si contiene un retículo isomorfo a la figura 14-7a) o a la figura 14-7b).

La demostración del teorema rebasa el alcance de este texto.

Elementos irreducibles, átomos

Sea L un retículo con una cota inferior 0. Se dice que un elemento a en L es *irreducible* si $a = x \vee y$ implica $a = x$ o $a = y$. (Los números primos bajo la multiplicación poseen esta propiedad; es decir, si $p = ab$ entonces $p = a$ o $p = b$, donde p es primo). Resulta evidente que 0 es irreducible. Si a tiene por lo menos dos predecesores inmediatos, por ejemplo b_1 y b_2 como en la figura 14-8a), entonces $a = b_1 \vee b_2$ y así a no es irreducible. Por otra parte, si a tiene un predecesor inmediato único c, entonces $a \neq \sup(b_1, b_2) = b_1 \vee b_2$ para cualesquiera otros elementos b_1 y b_2 porque c podría estar entre las b y las a en la figura 14-8b). En otras palabras, $a \neq 0$ es irreducible si y sólo si a tiene un predecesor inmediato único. Estos elementos que suceden inmediatamente a 0, denominados *átomos*, son irreducibles. Sin embargo, los retículos pueden tener otros elementos irreducibles. Por ejemplo, el elemento c en la figura 14-7a) no es un átomo aunque es irreducible puesto que a es su único predecesor inmediato.

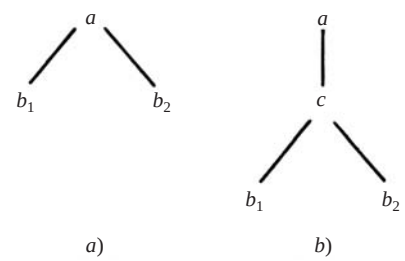


Figura 14-8

Si un elemento a en un retículo finito L no es irreducible, entonces es posible escribir $a = b_1 \vee b_2$. Luego, b_1 y b_2 pueden escribirse como los elementos unidos de otros elementos en caso de no ser irreducibles y así sucesivamente. Puesto que L es finita se tiene, por último,

$$a = d_1 \vee d_2 \vee \cdots \vee d_n$$

donde las d son irreducibles. Si d_i precede a d_j, entonces $d_i \vee d_j = d_j$; de modo que d_i puede eliminarse de la expresión. En otras palabras, se asume que las d son *irredundantes*; es decir, que ninguna d precede a ninguna otra d. Se recalca que una expresión así no necesariamente es única; por ejemplo, $I = a \vee b$ y $I = b \vee c$ en ambos retículos en la figura 14-7. Ahora se establece el principal teorema de esta sección (que se prueba en el problema 14-28).

Teorema 14.8: Sea L un retículo distributivo finito. Entonces toda a en L se escribe en forma única (salvo por el orden) como la unión de elementos irreducibles.

En realidad, este teorema se generaliza a retículos de *longitud finita*; es decir, donde todos los subconjuntos linealmente ordenados son finitos. (En el problema 14.30 se proporciona un retículo finito de longitud finita.)

14.11 COMPLEMENTOS, RETÍCULOS COMPLEMENTADOS

Sea L un retículo acotado con cota inferior 0 y cota superior I. Sea a un elemento de L. Un elemento x en L se denomina *complemento* de a si

$$a \vee x = I \quad \text{y} \quad a \wedge x = 0$$

Los complementos no necesariamente existen y no requieren ser únicos. Por ejemplo, los elementos a y c son complementos de b en la figura 14-7*a*). También, los elementos y, z y u en la cadena en la figura 14-1 no tienen complementos. Se presenta el siguiente resultado.

Teorema 14.9: Sea L un retículo distributivo acotado. Entonces, en caso de existir, los complementos son únicos.

Demostración: Suponga que x y y son complementos de todo elemento a en L. Entonces

$$a \vee x = I, \quad a \vee y = I, \quad a \wedge x = 0, \quad a \wedge y = 0$$

Mediante la distributividad,

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) = x \vee y$$

En forma semejante,

$$y = y \vee 0 = y \vee (a \wedge x) = (y \vee a) \wedge (y \vee x) = I \wedge (y \vee x) = y \vee x$$

Entonces

$$x = x \vee y = y \vee x = y$$

y se ha demostrado el teorema.

Retículos complementarios

Un retículo está *complementado* si L está acotado y todo elemento en L tiene un complemento. En la figura 14-7*b*) se muestra un retículo complementado donde los complementos no son únicos. Por otra parte, el retículo $P(\mathbf{U})$ de todos los subconjuntos de un conjunto universo $\mathbf{U}$ está complementado, y todo subconjunto A de $\mathbf{U}$ tiene un complemento único $A^c = \mathbf{U} \backslash A$.

Teorema 14.10: Sea L un retículo complementado con complementos únicos. Entonces los elementos irreducibles de L, distintos de 0, son sus átomos.

Al combinar este teorema y los teoremas 14.8 y 14.9 se obtiene un resultado importante.

Teorema 14.11: Sea L un retículo distributivo complementado finito. Entonces todo elemento a en L es la unión de un conjunto único de átomos.

Observación: En algunos textos un retículo L se define como complementado si todo elemento a en L tiene un complemento único. En ese caso, el teorema 14.10 se plantea de otra forma.

PROBLEMAS RESUELTOS

CONJUNTOS ORDENADOS Y RETÍCULOS

14.1 Sea $\mathbf{N} = \{1, 2, 3, \ldots\}$ ordenado por divisibilidad. Indique cuáles de los siguientes subconjuntos de $\mathbf{N}$ están linealmente ordenados.

a) $\{24, 2, 6\}$; *c*) $\mathbf{N} = \{1, 2, 3\ldots\}$; *e*) $\{7\}$;
b) $\{3, 15, 5\}$; *d*) $\{2, 8, 32, 4\}$; *f*) $\{15, 5, 30\}$.

a) Puesto que 2 divide a 6 que divide a 24, el conjunto está linealmente ordenado.

b) Puesto que 3 y 5 no son comparables, el conjunto no está linealmente ordenado.

c) Puesto que 2 y 3 no son comparables, el conjunto no está linealmente ordenado.

d) El conjunto está linealmente ordenado porque $2 \prec 4 \prec 8 \prec 32$.

e) Cualquier conjunto que consta de un elemento está linealmente ordenado.

f) Puesto que 5 divide a 15 que divide a 30, el conjunto está linealmente ordenado.

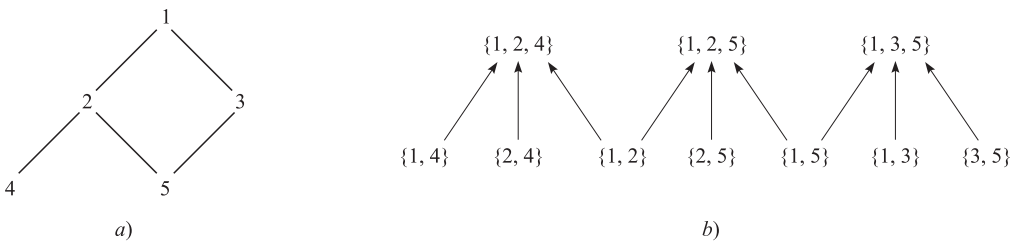
14.2 Sea $A = \{1, 2, 3, 4, 5\}$ ordenado por el diagrama de Hasse en la figura 14-9*a*).

a) Inserte el símbolo correcto $\prec$, $\succ$ o $\|$ (no comparable), entre cada par de elementos:
i) 1 ___ 5; *ii*) 2 ___ 3; *iii*) 4 ___ 1; *iv*) 3 ___ 4.

b) Encuentre todos los elementos minimales y maximales de A.

c) ¿A tiene un primer elemento o un último elemento?

d) Sea $L(A)$ la colección de todos los subconjuntos linealmente ordenados de A con 2 o más elementos, y sea $L(A)$ ordenado por inclusión de conjuntos. Dibuje el diagrama de Hasse de $L(A)$.



a) *b*)

Figura 14-9

a) *i*) Puesto que hay un "camino" (arista hacia arriba) de 5 a 3 a 1, 5 precede a 1; por tanto, $1 \succ 5$.
ii) De 2 a 3 no hay camino o viceversa; por tanto, $2 \| 3$.
iii) Hay un camino de 4 a 2 a 1; por tanto, $4 \prec 1$.
iv) Ni $3 \prec 4$ ni $4 \prec 3$; por tanto, $3 \| 4$.

b) Ningún elemento precede estrictamente a 4 o a 5, así que 4 y 5 son elementos minimales de A. Ningún elemento sucede a 1 de modo que 1 es un elemento maximal de A.

c) A no tiene primer elemento. Aunque 4 y 5 son elementos minimales de A, ninguno precede al otro. Sin embargo, 1 es un último elemento de A puesto que 1 sucede a todo elemento de A.

d) Los elementos de $L(A)$ son como sigue:

$$\{1, 2, 4\}, \quad \{1, 2, 5\}, \quad \{1, 3, 5\}, \quad \{1, 2\}, \quad \{1, 4\}, \quad \{1, 3), \quad \{1, 5\}, \quad \{2, 4\}, \quad \{2, 5\}, \quad \{3, 5\}$$

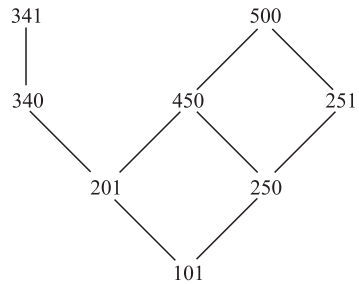
(Observe que $\{2, 5\}$ y $\{3, 4\}$ no están linealmente ordenados). El diagrama de $L(A)$ se muestra en la figura 14-9*b*).

14.3 Un prerrequisito en la universidad es un ordenamiento parcial conocido de cursos disponibles. Se escribe $A \prec B$ si el curso A es un prerrequisito para el curso B. Sea C el conjunto ordenado que consta de los cursos de matemáticas y sus prerrequisitos, que se muestran en la figura 14.10*a*).

a) Trace el diagrama de Hasse para el orden parcial C de estos cursos.
b) Encuentre todos los elementos minimales y maximales de C.
c) ¿C tiene un primer elemento o un último elemento?

Curso	**Prerrequisitos**
Mat 101	Ninguno
Mat 201	Mat 101
Mat 250	Mat 101
Mat 251	Mat 250
Mat 340	Mat 201
Mat 341	Mat 340
Mat 450	Mat 201, Mat 250
Mat 500	Mat 450, Mat 251

a)



b)

Figura 14-10

a) Mat 101 debe estar en la parte inferior del diagrama, puesto que es el único curso sin prerrequisitos. Debido a que Mat 201 y Mat 250 sólo requieren Mat 101, se tiene Mat 101 $\ll$ Mat 201 y Mat 101 $\ll$ Mat 201 y Mat 101 $\ll$ Mat 250; por tanto, se traza una línea hacia arriba desde Mat 101 hasta Mat 201 y otra desde Mat 101 hasta Mat 250. Al continuar este proceso, se obtiene el diagrama de Hasse en la figura 14-10*b*).

b) Ningún elemento precede estrictamente a Mat 101, de modo que Mat 101 es un elemento minimal de C. Ningún elemento precede estrictamente a Mat 341 o a Mat 500, de modo que cada uno es un elemento maximal de C.

c) Mat 101 es un primer elemento de C, puesto que precede a cualquier otro elemento de C. Sin embargo, C no tiene último elemento. Aunque Mat 341 y Mat 500 son elementos maximales, ninguno es el último elemento puesto que ninguno precede al otro.

CONJUNTOS PRODUCTO Y ORDEN

14.4 Suponga que a $\mathbf{N^2} = \mathbf{N} \times \mathbf{N}$ asigna el orden del producto (sección 14.2) donde $\mathbf{N}$ tiene el orden usual $\leq$.

Inserte el símbolo correcto $\prec$, $\succ$ o $\|$ (no comparable), entre cada uno de los siguientes pares de elementos de $\mathbf{N} \times \mathbf{N}$:

a) (5, 7) ___ (7, 1); *c*) (5, 5) ___ (4, 8); *e*) (7, 9) ___ (4, 1);
b) (4, 6) ___ (4, 2); *d*) (1, 3) ___ (1, 7); *f*) (7, 9) ___ (8, 2).

Aquí $(a, b) \prec (a', b')$ si $a < a'$ y $b \leq b'$ o si $a \leq a'$ y $b < b'$. Así,

a) $\|$ puesto que $5 < 7$ pero $7 > 1$. *c*) $\|$ puesto que $5 > 4$ y $5 < 8$. *e*) $\succ$ puesto que $7 > 4$ y $9 > 1$.
b) $\succ$ puesto que $4 = 4$ y $6 > 2$. *d*) $\prec$ puesto que $1 = 1$ y $3 < 7$. *f*) $\|$ puesto que $7 < 8$ y $9 > 1$.

14.5 Repita el problema 14.4, pero ahora aplique el orden lexicográfico de $\mathbf{N^2} = \mathbf{N} \times \mathbf{N}$.

Aquí $(a, b) \prec (a', b')$ si $a < a'$ o si $a = a'$ pero $b < b'$. Así,

a) $\prec$ puesto que $5 < 7$. *c*) $\succ$ puesto que $5 > 4$. *e*) $\succ$ puesto que $7 > 4$.
b) $\succ$ puesto que $4 = 4$ y $6 > 2$. *d*) $\prec$ puesto que $1 = 1$ pero $3 < 7$. *f*) $\prec$ puesto que $7 < 8$.

14.6 Considere el alfabeto inglés $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ con el orden alfabético (usual). (Recuerde que $\mathbf{A}^*$ consta de todas las palabras en $\mathbf{A}$). Considere la siguiente lista de palabras en $\mathbf{A}^*$:

went, forget, to, medicine, me, toast, melt, for, we, arm

a) Ordene la lista de palabras según el orden short-lex (semigrupo libre).

b) Ordene la lista de palabras según el orden alfabético (usual) de **A***.

a) Primero, los elementos se ordenan por longitud y luego lexicográficamente (alfabéticamente):

me, to, we, arm, for, melt, went, toast, forget, medicine

b) El orden lexicográfico (alfabético) produce:

arm, for, forget, me, medicine, melt, to, toast, we, went

ENUMERACIONES CONSISTENTES

14.7 Suponga que una estudiante desea llevar todos los cursos del problema 14.3, aunque sólo uno por semestre.

a) ¿Qué opción u opciones debe hacer para el primer semestre y para el último semestre (octavo)?

b) Suponga que la estudiante desea llevar Mat 250 en su primer año (primero o segundo semestres) y Mat 340 en su cuarto año (séptimo u octavo semestres). Encuentre todas las formas en que la estudiante puede llevar los ocho cursos.

a) Por la figura 14-10, Mat 101 es el único elemento minimal y así debe llevarse en el primer semestre, y Mat 341 y 500 son los elementos maximales, de modo que es necesario llevar uno en el último semestre.

b) Mat 250 no es un elemento minimal, por lo que es necesario cursarlo en el segundo semestre, y Mat 340 no es un elemento maximal, de modo que debe cursarse en el séptimo semestre y Mat 341 en el octavo semestre. Asimismo, Mat 500 debe cursarse en el sexto semestre. A continuación se proporcionan las tres formas posibles de llevar los ocho cursos:

101, 250, 251, 201, 450, 500, 340, 341, 101, 250, 201, 251, 450, 500, 340, 341,
101, 250, 201, 450, 251, 500, 340, 341

14.8 Demuestre el teorema 14.1: Suponga que S es un conjunto ordenado finito con n elementos. Entonces existe una enumeración consistente $f: S \to \{1, 2, \ldots, n\}$.

La demostración es por inducción sobre el número n de elementos en S. Se supone que $n = 1$; por ejemplo, $S = \{s\}$. Entonces $f(s) = 1$ es una enumeración consistente de S. Luego se supone que $n > 1$ y el teorema se cumple para conjuntos parcialmente ordenados con menos de n elementos. Sea $a \in S$ un elemento mínimo. (Este elemento a existe porque S es finito). Sea $T = S \backslash \{a\}$. Entonces T es un conjunto parcialmente ordenado con $n - 1$ elementos y así, por inducción, T admite una enumeración consistente; por ejemplo, $g: T \to \{1, 2, \ldots, n-1\}$. Se define $f: S \to \{1, 2, \ldots, n\}$ por:

$$f(x) = \begin{cases} 1, & \text{si } x = a \\ g(x) + 1 & \text{si } x \neq a \end{cases}$$

Entonces f es la enumeración consistente requerida.

COTAS SUPERIOR E INFERIOR, SUPREMO E ÍNFIMO

14.9 Sea $S = \{a, b, c, d, e, f, g\}$ ordenado como en la figura 14.11*a*), y sea $X = \{c, d, e\}$.

a) Encuentre las cotas superior e inferior de X.

b) Identifique sup(X), el supremo de X, e ínf(X), el ínfimo de X, en caso de existir.

a) Los elementos e, f y g suceden a cualquier otro elemento de X; por tanto, e, f y g son las cotas superiores de X. El elemento a precede a cualquier elemento de X; por tanto, a es la cota inferior de X. Observe que b no es una cota inferior puesto que b no precede a c; de hecho, b y c no son comparables.

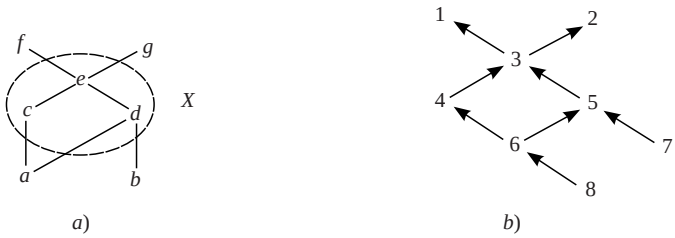
b) Puesto que e precede tanto a f como a g, se tiene $e = \sup(X)$. En forma semejante, ya que a precede (trivialmente) a toda cota inferior de X, se tiene $a = \text{ínf}(X)$. Observe que sup(X) pertenece a X pero ínf(X) no pertenece a X.

14.10 Sea $S = \{1, 2, 3, \ldots, 8\}$ ordenado como en la figura 14.11*b*), y sea $A = \{2, 3, 6\}$.

a) Encuentre las cotas superior e inferior de X. *b*) Identifique sup(A) e ínf(A), en caso de existir.

a) La cota superior es 2, y las cotas inferiores son 6 y 8.

b) Aquí $\sup(A) = 2$ e $\text{ínf}(A) = 6$.



a) *b*)

Figura 14-11

14.11 Repita el problema 14.10 para el subconjunto $B = \{1, 2, 5\}$.

a) No hay cota superior para B puesto que ningún elemento sucede tanto a 1 como a 2. Las cotas inferiores son 6, 7, 8.

b) Trivialmente, sup(A) no existe puesto que no hay cotas superiores. Aunque A tiene tres cotas inferiores, ínf(A) no existe puesto que ninguna cota inferior sucede tanto a 6 como a 7.

14.12 Considere el conjunto $\mathbf{Q}$ de números racionales con el orden usual $\leq$. Considere el subconjunto D de $\mathbf{Q}$ definido por

$$D = \{x \mid x \in \mathbf{Q} \text{ y } 8 < x^3 < 15\}$$

a) ¿D está acotado por arriba o por abajo? *b*) ¿Existen sup(D) o ínf(D)?

a) El subconjunto D está acotado por arriba y por abajo. Por ejemplo, 1 es la cota inferior y 100 la cota superior.

b) Se afirma que sup(D) no existe. Suponga, por el contrario, que sup(D) $= x$. Puesto que $\sqrt[3]{15}$ es irracional, $x > \sqrt[3]{15}$. Sin embargo, existe un número racional y tal que $\sqrt[3]{15} < y < x$. Por tanto, y también es una cota superior de D. Esto contradice la hipótesis de que $x =$ sup(D). Por otra parte, ínf(D) existe. Precisamente, ínf(D) $= 2$.

CONJUNTOS (SEMEJANTES) ISOMORFOS, TRANSFORMACIONES DE SEMEJANZA

14.13 Suponga que un conjunto parcialmente ordenado A es isomorfo (semejante) a un conjunto parcialmente ordenado B y que $f: A \to B$ es un transformación de semejanza. Las siguientes proposiciones, ¿son verdaderas o falsas?

a) Un elemento $a \in A$ es un primer (último, minimal o maximal) elemento de A si y sólo si $f(a)$ es un primer (último, minimal o maximal) de B.

b) Un elemento $a \in A$ precede inmediatamente a un elemento $a' \in A$; es decir $a \ll a'$ si y sólo si $f(a) \ll f(a')$.

c) Un elemento $a \in A$ tiene r sucesores inmediatos en A si y sólo si $f(a)$ tiene r sucesores inmediatos en B.

Todas las proposiciones son verdaderas; la estructura de orden de A es la misma que la estructura de orden de B.

14.14 Sea $S = \{a, b, c, d, e\}$ el conjunto ordenado en la figura 14-12*a*). Suponga que $A = \{1, 2, 3, 4, 5\}$ es isomorfo a S. Dibuje el diagrama de Hasse de A si el siguiente mapeo de una transformación de semejanza de S en A:

$$f = \{(a, 1), (b, 3), (c, 5), (d, 2), (e, 4)\}$$

La transformación de semejanza f preserva la estructura de orden de S y por tanto f puede considerarse simplemente como una retiquetación de los vértices en el diagrama de S. Así, la figura 14-12*b*) muestra el diagrama de Hasse de A.

14.15 Sea $A = \{1, 2, 3, 4, 5\}$ ordenado como en la figura 14-12*b*). Encuentre el número n de transformaciones de semejanza $f: A \to A$.

Puesto que el único elemento minimal de A es 1 y el único elemento maximal es 4, debe tenerse $f(1) = 1$ y $f(4) = 4$. Asimismo, $f(3) = 3$ es el único sucesor inmediato de 1. Por otra parte, hay dos posibilidades para $f(2)$ y $f(5)$; es decir, puede tenerse $f(2) = 2$ y $f(5) = 5$, o $f(2) = 5$ y $f(5) = 2$. En consecuencia, $n = 2$.

14.16 Proporcione un ejemplo de un conjunto finito no linealmente ordenado $X = (A, R)$ que sea isomorfo a $Y = (A, R^{-1})$, el conjunto A con el orden inverso.

Sea R el ordenamiento parcial de $A = \{a, b, c, d, e\}$ que se muestra en la figura 14-13*a*).

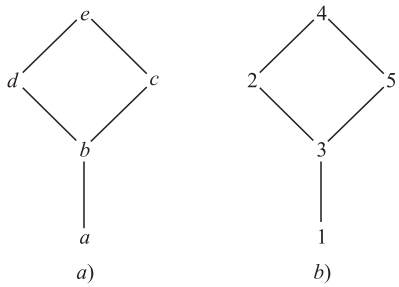


Figura 14-12

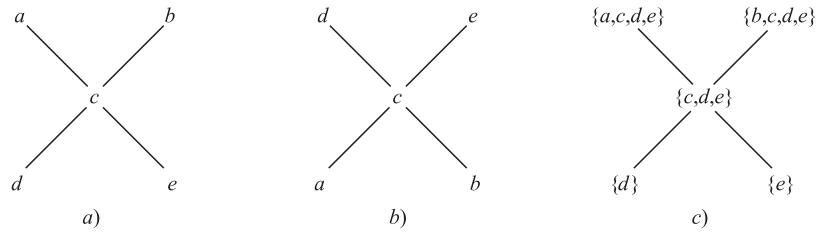


Figura 14-13

Así, en la figura 14-13*b*) se muestra *A* con el orden inverso *R*. (El diagrama de *R* simplemente se ha puesto de cabeza a fin de obtener R^{-1}.) Observe que los dos diagramas son idénticos, excepto por la etiquetación. Por tanto, *X* es isomorfo a *Y*.

14.17 Sea *A* un conjunto ordenado y, para todo $a \in A$, sea $p(a)$ el conjunto de predecesores de *a*:

$$p(a) = \{x \mid x \precsim a\}$$

(denominado *conjunto de predecesores* de *a*). Sea $p(A)$ la colección de todos los conjuntos de predecesores de los elementos en *A* ordenados por inclusión de conjuntos.

a) Demuestre que *A* y $p(A)$ son isomorfos al demostrar que la función $f: A \to p(A)$, definida por $f(a) = p(a)$ es una transformación de semejanza de *A* sobre $p(A)$.

b) Encuentre el diagrama de Hasse de $p(A)$ para el conjunto *A* en la figura 14-13*a*).

a) Primero se demuestra que *f* preserva la relación de orden de *A*. Se supone que $a \precsim b$. Sea $x \in p(a)$. Entonces $x \precsim a$ y entonces $a \precsim b$; de modo que $x \in p(b)$. Así, $p(a) \subseteq p(b)$. Se supone que $a \parallel b$ (no comparables). Entonces $a \in p(a)$ pero $a \notin p(b)$; por tanto, $p(a) \not\subseteq p(b)$. En forma semejante, $b \in p(b)$ pero $b \notin p(a)$; así, $p(b) \not\subseteq p(a)$. En consecuencia, $p(a) \parallel p(b)$. Así, *f* preserva el orden.

Sólo es necesario demostrar que *f* es uno a uno y sobre. Suponga que $y \in p(A)$, entonces $y = p(a)$ para alguna $a \in A$. Así, $f(a) = p(a) = y$ y entonces *f* es sobre $p(A)$. Se supone que $a \neq b$. Entonces $a \prec b$, $b \prec a$ o $a \| b$. En los casos primero y tercero, $b \in p(b)$ pero $b \notin p(a)$ y en el segundo caso $a \in p(a)$ pero $a \notin p(b)$. En consecuencia, en los tres casos, se tiene $p(a) \neq p(b)$. Así, *f* es uno a uno.

Por consiguiente, *f* es una transformación de semejanza de *A* sobre $p(A)$ y así $A \simeq p(A)$.

b) Los elementos de $p(A)$ son los siguientes:

$$p(a) = \{a, c, d, e\}, \quad p(b) = \{b, c, d, e\}, \quad p(c) = \{c, d, e\}, \quad p(d) = \{d\}, \quad p(e) = \{e\}$$

En la figura 14-13*c*) se muestra el diagrama de $p(A)$ ordenado por inclusión de conjuntos. Observe que los diagramas en la figura 14-13*a*) y *c*) son idénticos, excepto por la identificación de los vértices.

CONJUNTOS BIEN ORDENADOS

14.18 Demuestre el principio de inducción transfinita. Sea *A* un subconjunto de un conjunto *S* bien ordenado con las dos propiedades siguientes: *i*) $a_0 \in A$. *ii*) Si $s(a) \subseteq A$ entonces $a \in A$. Así que $A = S$.

(Aquí a_0 es el primer elemento de *A*, y $s(a)$ es el segmento inicial de a; es decir, el conjunto de todos los elementos que preceden estrictamente a *a*.) Suponga que $A \neq S$. Sea $B = S \backslash A$. Entonces $B \neq \varnothing$. Puesto que *S* está bien ordenado, *B* tiene un primer elemento b_0. Cada elemento $x \in s(b_0)$ precede a b_0 y entonces no pertenece a *B*. Así, todo $x \in s(b_0)$ pertenece a

A; de modo que $s(b_0) \subseteq A$. Por *ii*), $b_0 \in A$. Esto contradice la hipótesis de que $b_0 \in S \backslash A$. Por tanto, la hipótesis original de que $A \neq S$ no es verdadera. En consecuencia, $A = S$.

14.19 Sea S un conjunto bien ordenado con el primer elemento a_0. Defina un *elemento límite* de S.

Un elemento $b \in S$ es un elemento límite de S si $b \neq a_0$ y b no tiene predecesor inmediato.

14.20 Considere el conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de enteros positivos. Todo número en $\mathbf{N}$ puede escribirse de manera única como un producto de una potencia no negativa de 2 multiplicada por un número impar. Suponga que a, $a' \in \mathbf{N}$ y

$$a = 2^r (2s + 1) \quad \text{y} \quad a' = 2^{r'} (2s' + 1)$$

donde r, r' y s, s' son enteros no negativos. Se define:

$$a \prec a' \quad \text{si } r < r' \quad \text{o} \quad \text{si } r = r' \text{ pero } s < s'$$

a) Inserte el símbolo correcto $\prec$ o $\succ$ entre cada par de números:

$$i)\ 5 \_\_\_ 14; \quad ii)\ 6 \_\_\_ 9; \quad iii)\ 3 \_\_\_ 20; \quad iv)\ 14 \_\_\_ 21$$

b) Sea $S = (\mathbf{N}, \prec)$. Demuestre que S está bien ordenado.

c) ¿S tiene algún elemento finito?

a) Los elementos de $\mathbf{N}$ pueden enumerarse como en la figura 14-14. El primer renglón consta de los números impares; el segundo, de 2 veces los números impares; el tercero, de $2^2 = 4$ veces los números impares y así en lo sucesivo. Entonces $a \prec a'$ si a está en un renglón superior, entonces a' o si a y a' están en el mismo renglón pero a aparece antes que a' en el renglón. En consecuencia:

$$i)\ 5 \prec 14; \quad ii)\ 6 \succ 9; \quad iii)\ 3 \succ 20; \quad iv)\ 14 \succ 20.$$

r \ s	0	1	2	3	4	5	6	7	
0	1	3	5	7	9	11	13	15	...
1	2	6	10	14	18	22	26	30	...
2	4	12	20	28	36	44	52	60	...
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Figura 14-14

b) Sea A un subconjunto de S. Los renglones están bien ordenados. Sea r_0 el mínimo renglón de elementos en A. En r_0 puede haber muchos elementos de A. Las columnas están bien ordenadas, de modo que sea s_0 la columna mínima de los elementos de A en el renglón r_0. Entonces, $x = (r_0, s_0)$ es el primer elemento de A. Así S está bien ordenado.

c) Como se indica en la figura 14-14, toda potencia de 2; es decir, 1, 2, 4, 8, ... no tiene predecesor inmediato. Así, todo elemento distinto de 1 es un elemento límite de S.

14.21 Sea S un conjunto bien ordenado. Sea f: $S \to S$ una transformación de semejanza de S en S. Demuestre que, para toda $a \in S$ se tiene $a \precsim f(a)$.

Sea $D = \{x | f(x) \prec x\}$. Si D es vacío, entonces la proposición es verdadera. Suponga que $D \neq \varnothing$. Puesto que D está bien ordenado, D tiene un primer elemento; por ejemplo, d_0. Debido a que $d_0 \in D$, se tiene $f(d_0) \prec d_0$. Puesto que f es una transformación de semejanza:

$$f(d_0) \prec d_0 \quad \text{implica} \quad f(f(d_0)) \prec f(d_0)$$

Así, $f(d_0)$ también pertenece a D. Pero $f(d_0) \prec d_0$ y $f(d_0) \in D$ contradicen el hecho de que d_0 es el primer elemento de D. Por tanto, la hipótesis original de que $D \neq \varnothing$ lleva a una contradicción. En consecuencia, D es vacío y la proposición es verdadera.

14.22 Sea A un conjunto bien ordenado. Sea $s(A)$ la colección de todos los segmentos iniciales $s(a)$ de elementos $a \in A$ ordenados por inclusión de conjuntos. Demuestre que A es isomorfo a $s(A)$ al demostrar que la función $f: A \to s(A)$, definido por $f(a) = s(a)$ es una transformación de semejanza de A sobre $s(A)$. (Compare con el problema 14.17.)

Primero se demuestra que f es uno a uno y sobre. Suponga que $y \in s(A)$. Entonces $y = s(a)$ para alguna $a \in A$. Por tanto, $f(a) = s(a) = y$, así que f es sobre $s(A)$. Suponga que $x \neq y$. Entonces uno precede al otro; por ejemplo, $x \prec y$. Entonces $x \in s(y)$. Pero $x \notin s(x)$. Así, $s(x) \neq s(y)$. En consecuencia, f es uno a uno.

Sólo es necesario demostrar que f preserva el orden; es decir,

$$x \precsim y \quad \text{si y sólo si} \quad s(x) \subseteq s(y)$$

Suponga que $x \precsim y$. Si $a \in s(x)$, entonces $a \prec x$ y por tanto $a \prec y$; así, $a \in s(y)$. Entonces $s(x) \subseteq s(y)$. Por otra parte, suponga que $x \not\precsim y$, es decir, $x \succ y$. Entonces $y \in s(x)$. Pero $y \notin s(y)$; así, $s(x) \not\subseteq s(y)$. En otras palabras, $x \precsim y$ si y sólo si $s(x) \subseteq s(y)$. En consecuencia, f es una transformación de semejanza de A sobre $s(A)$, y así $A \cong s(A)$.

RETÍCULOS

14.23 Escriba el dual de cada proposición:

$a)$ $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$; $\quad b)$ $(a \wedge b) \vee a = a \wedge (b \vee a)$.

$\vee$ se sustituye por $\wedge$ y $\wedge$ se sustituye por $\vee$ en cada proposición a fin de obtener la proposición dual:

$a)$ $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$; $\quad b)$ $(a \vee b) \wedge a = a \vee (b \wedge a)$

14.24 Demuestre el teorema 14.4: sea L un retículo. Entonces:

i) $a \wedge b = a$ si y sólo si $a \vee b = b$.
ii) La relación $a \precsim b$ (definida por $a \wedge b = a$ o $a \vee b = b$) es un orden parcial sobre L.

i) Se supone que $a \wedge b = a$. Al usar la ley de absorción en el primer paso se tiene:

$$b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$$

Ahora se supone que $a \vee b = b$. Al usar de nuevo la ley de absorción en el primer paso se tiene:

$$a = a \wedge (a \vee b) = a \wedge b$$

Por tanto $a \wedge b = a$ si y sólo si $a \vee b = b$.

ii) Para cualquier a en L, se tiene $a \wedge a = a$ por idempotencia. Así $a \precsim a$, y así $\precsim$ es reflexiva.

Se supone que $a \precsim b$ y $b \precsim a$. Entonces $a \wedge b = a$ y $b \wedge a = b$. En consecuencia, $a = a \wedge b = b \wedge a = b$, y así $\precsim$ es antisimétrica.

Por último, se supone que $a \precsim b$ y $b \precsim c$. Entonces $a \wedge b = a$ y $b \wedge c = b$. Así

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$$

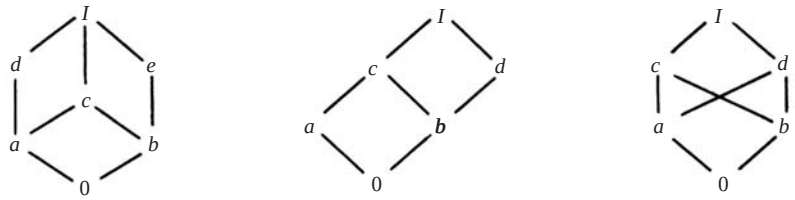
En consecuencia, $a \precsim c$, y así $\precsim$ es transitiva. En consecuencia, $\precsim$ es un orden parcial sobre L.

14.25 ¿Cuál(cuales) de los conjuntos parcialmente ordenados en la figura 14-15 es (son) retículo(s)?

Un conjunto parcialmente ordenado es un retículo si y sólo si sup(x, y) e ínf(x, y) existen para cada par x, y en el conjunto. Sólo c) no es retículo puesto que (a, b) tiene tres cotas superiores: c, d e I, y ninguna precede a las otras dos; es decir, sup(a, b) no existe.

14.26 Considere el retículo en la figura 14-15a).

a) ¿Cuáles elementos distintos de cero son irreducibles?
b) ¿Cuáles elementos son átomos?



a) *b*) *c*)

Figura 14-15

c) ¿Cuáles de los siguientes son subretículos de L?:

$$L_1 = \{0, a, b, I\}, \quad L_2 = \{0, a, e, I\}, \quad L_3 = \{a, c, d, I\}, \quad L_4 = \{0, c, d, I\}$$

d) ¿L es distributiva?
e) Encuentre los complementos, en caso de existir, de los elementos a, b y c.
f) ¿L es un retículo complementado?

a) Los elementos diferentes de cero con un predecesor inmediato son irreducibles. Por tanto, a, b, d y e son irreducibles.

b) Los elementos que suceden inmediatamente a 0 son átomos, de modo que a y b son los átomos.

c) Un subconjunto L' es un subretículo si es cerrado bajo $\wedge$ y $\vee$. L_1 no es un subretículo puesto que $a \vee b = c$, que no pertenece a L_1. El conjunto L_4 no es un subretículo puesto que $c \wedge d = a$ no pertenece a L_4. Los otros dos conjuntos L_2 y L_3, son subretículos.

d) L no es distributiva puesto que $M = \{0, a, d, e, I\}$ es un subretículo isomorfo al subretículo no distributivo la figura 14-7*a*).

e) Se tiene $a \wedge e = 0$ y $a \vee e = I$, de modo que a y e son complementos. En forma semejante, b y d son complementos. Sin embargo, c no tiene complemento.

f) L no es un retículo complementado ya que c no tiene complemento.

14.27 Considere el retículo en la figura 14-15*b*).

a) Encuentre los elementos irreducibles distintos de cero y los átomos de M.
b) ¿M es *i*) distributiva? *ii*) ¿complementada?

a) Los elementos distintos de cero con un predecesor único son a, b y d, y de estos tres sólo a y b son átomos puesto que su único predecesor es 0.

b) *i*) M es distributiva puesto que M no tiene un subretículo isomorfo a un de los retículos en la figura 14-7. *ii*) M no es complementada porque b no tiene complemento. Observe que a es la única solución de $b \wedge x = 0$ pero $b \wedge a = c \neq I$.

14.28 Demuestre el teorema 14.8: sea L un retículo distributivo finito. Entonces todo $a \in L$ puede escribirse de manera única (salvo por el orden) como la unión de elementos irreducibles irredundantes.

Puesto que L es finito, a puede escribirse como la unión de elementos irreducibles irredundantes, que se analizaron en la sección 14.9. Por tanto, se requiere demostrar la unicidad. Se supone lo siguiente:

$$a = b_1 \vee b_2 \vee \cdots \vee b_r = c_1 \vee c_2 \vee \cdots \vee c_s$$

donde las b son irredundantes e irreducibles. Para cualquier i dada se tiene

$$b_i \precsim (b_1 \vee b_2 \vee \cdots \vee b_r) = (c_1 \vee c_2 \vee \cdots \vee c_s)$$

Por tanto

$$b_i = b_i \wedge (c_1 \vee c_2 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee (b_i \wedge c_2) \vee \cdots \vee (b_i \wedge c_s)$$

Puesto que b_1 es irreducible, existe una j tal que $b_i = b_i \wedge c_j$ y $b_i \precsim c_j$. Con un argumento semejante, para c_j existe una b_k tal que $c_j \precsim b_k$. En consecuencia,

$$b_i \precsim c_j \precsim b_k$$

con lo cual se obtiene $b_i = c_j = b_k$, ya que las b son irredundantes. En consecuencia, las b y las c pueden parearse. Entonces, la representación de a es única salvo por el orden.

14.29 Demuestre el teorema 14.10: sea L un retículo complementado con complementos únicos. Entonces los elementos irreducibles de L, distintos de 0, son sus átomos.

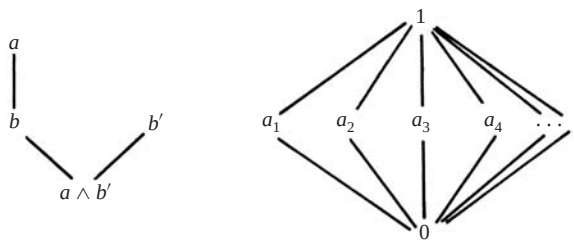
Se supone que a es irreducible y que a no es un átomo. Entonces a tiene un predecesor inmediato único $b \neq 0$. Sea b' el complemento de b. Puesto que $b \neq 0$, se tiene $b' \neq 1$. Si a precede a b', entonces $b \precsim a \precsim b$ y así $b \wedge b' = b'$, lo que es imposible ya que $b \wedge b' = I$. Entonces, a no precede a b', y así $a \wedge b'$ debe preceder estrictamente a a. Debido a que b es el único predecesor inmediato de a, también se tiene que $a \wedge b'$ precede a b, como en la figura 14-16a). Pero $a \wedge b'$ precede a b'. Así,

$$a \wedge b' \precsim \text{ínf}(b, b') = b \wedge b' = 0$$

Por tanto, $a \wedge b' = 0$. Debido a que $a \vee b = a$, también se tiene que

$$a \vee b' = (a \vee b) \vee b' = a \vee (b \vee b') = a \vee I = I$$

En consecuencia, b' es un complemento de a. Debido a que los complementos son únicos, $a = b$. Esto contradice la hipótesis de que b es un predecesor inmediato de a. Por tanto, los únicos elementos irreducibles de L son sus átomos.



a) *b*)

Figura 14-16

14.30 Dé un ejemplo de un retículo infinito L de longitud finita.

Sea $L = \{0, 1, a_1, a_2, a_3, \ldots\}$ y sea L un retículo ordenado como en la figura 14-16b). En consecuencia, para cada $n \in \mathbf{N}$, se tiene $0 < a_n < 1$. Así, L es de longitud finita puesto que no contiene ningún subconjunto linealmente ordenado.

PROBLEMAS SUPLEMENTARIOS

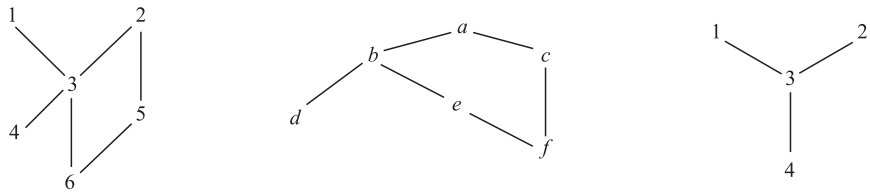
CONJUNTOS Y SUBCONJUNTOS ORDENADOS

14.31 Sea $A = \{1, 2, 3, 4, 5, 6\}$ ordenado como en la figura 14-17*a*).

a) Encuentre todos los elementos mínimales y máximales de *A*.

b) ¿*A* tiene un primer elemento o un último elemento?

c) Encuentre todos los subconjuntos linealmente ordenados de *A*, cada uno de los cuales contiene por lo menos tres elementos.



a) *b*) *c*)

Figura 14-17

14.32 Sea $B = \{a, b, c, d, e, f\}$ ordenado como en la figura 14-17*b*).

a) Encuentre todos los elementos minimales y maximales de *B*.

b) ¿*B* tiene un primer elemento o un último elemento?

c) Enliste y encuentre el número de enumeraciones consistentes de *B* en el conjunto $\{1, 2, 3, 4, 5, 6\}$.

14.33 Sea $C = \{1, 2, 3, 4\}$ ordenado como en la figura 14-17*c*). Sea $L(C)$ la colección de todos los subconjuntos no vacíos linealmente ordenados de *C* ordenados por inclusión de conjuntos. Dibuje un diagrama de $L(C)$.

14.34 Trace los diagramas de las particiones de *m* (vea el ejemplo 14.4) donde: *a*) $m = 4$; *b*) $m = 6$.

14.35 Si $\mathbf{D}_m$ denota los divisores positivos de *m* ordenados por divisibilidad, trace los diagramas de Hasse de:

a) $\mathbf{D}_{12}$; *b*) $\mathbf{D}_{15}$; *c*) $\mathbf{D}_{16}$; *d*) $\mathbf{D}_{17}$.

14.36 Sea $S = \{a, b, c, d, e, f\}$ un conjunto parcialmente ordenado. Suponga que hay exactamente seis pares de elementos donde el primero precede inmediatamente al segundo como sigue:

$$f \ll a, \quad f \ll d, \quad e \ll b, \quad c \ll f, \quad e \ll c, \quad b \ll f$$

a) Encuentre todos los elementos minimales y maximales de *S*.

b) ¿*S* tiene algún primer elemento o algún último elemento?

c) Encuentre todos los pares de elementos, en caso de haber alguno, que no son comparables.

14.37 Indique si cada una de las siguientes proposiciones es falsa o verdadera y, si es falsa, dé un contraejemplo.

a) Si un conjunto parcialmente ordenado *S* tiene sólo un elemento maximal *a*, entonces *a* es el último elemento.

b) Si un conjunto finito parcialmente ordenado *S* tiene sólo un elemento maximal *a*, entonces *a* es el último elemento.

c) Si un conjunto *S* linealmente ordenado sólo tiene un elemento maximal *a*, entonces *a* es el último elemento.

14.38 Sea $S = \{a, b, c, d, e\}$ ordenado como en la figura 14-18*a*).

a) Encuentre todos los elementos minimales y maximales de *S*.

b) ¿*S* tiene algún primer elemento o algún último elemento?

c) Encuentre todos los subconjuntos de *S* donde *c* es un elemento minimal.

d) Encuentre todos los subconjuntos de *S* donde *c* es un primer elemento.

e) Enumere todos los subconjuntos linealmente ordenados con tres o más elementos.

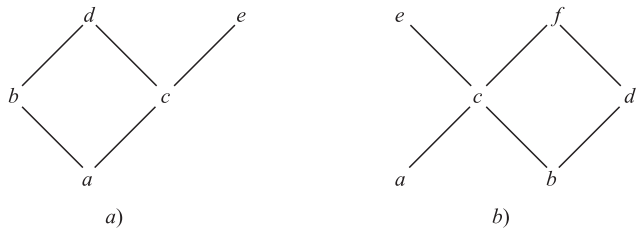


Figura 14-18

14.39 Sea $S = \{a, b, c, d, e, f\}$ ordenado como en la figura 14-18*b*).

a) Encuentre todos los elementos minimales y maximales de S.

b) ¿S tiene algún primer elemento o algún último elemento?

c) Enliste todos los subconjuntos linealmente ordenados con tres o más elementos.

14.40 Sea $S = \{a, b, c, d, e, f, g\}$ ordenado como en la figura 14-11*a*). Encuentre el número n de subconjuntos linealmente ordenados de S con: *a*) cuatro elementos; *b*) cinco elementos.

14.41 Sea $S = \{1, 2, \ldots, 7, 8\}$ ordenado como en la figura 14-11*b*). Encuentre el número n de subconjuntos linealmente ordenados de S con: *a*) cinco elementos; *b*) seis elementos.

ENUMERACIONES CONSISTENTES

14.42 Sea $S = \{a, b, c, d, e\}$ ordenado como en la figura 14-18*a*). Enliste todas las enumeraciones consistentes de S en {1, 2, 3, 4, 5}.

14.43 Sea $S = \{a, b, c, d, e, f\}$ ordenado como en la figura 14-18*b*). Encuentre el número n de las enumeraciones consistentes de S en {1, 2, 3, 4, 5, 6}.

14.44 Suponga que las tres siguientes enumeraciones son consistentes de un conjunto ordenado $A = \{a, b, c, d\}$.

$$[(a, 1), (b, 2), (c, 3), (d, 4)], \quad [(a, 1), (b, 3), (c, 2), (d, 4)], \quad [(a, 1), (b, 4), (c, 2), (d, 3)]$$

En el supuesto de que los diagramas de Hasse D de A sean conexos, dibujar D.

ORDEN Y CONJUNTOS PRODUCTO

14.45 Sean $M = \{2, 3, 4, \ldots\}$ y $M^2 = M \times M$ ordenados como sigue:

$$(a, b) \prec (c, d) \quad \text{si} \quad a \mid c \text{ y } b < d$$

Encuentre todos los elementos minimales y maximales de $M \times M$.

14.46 Considere el alfabeto inglés $A = \{a, b, c, \ldots, y, z\}$ con el orden usual (alfabético). Recuerde que A^* consiste de todas las palabras en A. Sea L la siguiente lista de palabras en A^*:

gone, or, arm, go, an, about, gate, one, at, occur

a) Ordene L según el orden short-lex; es decir, primero por longitud y luego alfabéticamente.

b) Ordene L alfabéticamente.

14.47 Considere los conjuntos ordenados A y B que se muestran en la figura 14-17*a*) y *b*), respectivamente. Se supone que $S = A \times B$ esté definido por el orden del producto. Inserte el símbolo correcto $\prec$, $\succ$ o $\|$ entre cada par de elementos de S:

a) $(4, b)\_\_\_(2, e)$; *b*) $(3, a)\_\_\_(6, f)$; *c*) $(5, d)\_\_\_(1, a)$; *d*) $(6, e)\_\_\_(2, b)$.

14.48 Suponga que a $\mathbf{N} = \{1, 2, 3, \ldots\}$ y $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ se les asignan los órdenes usuales y que $S = \mathbf{N} \times \mathbf{A}$ se ordena lexicográficamente. Ordene los siguientes elementos de S:

$$(2, z), \quad (1, c), \quad (2, c), \quad (1, y), \quad (4, b), \quad (4, z), \quad (3, b), \quad (2, a)$$

COTAS SUPERIOR E INFERIOR, SUPREMO E ÍNFIMO

14.49 Sea $S = \{a, b, c, d, e, f, g\}$ ordenado como en la figura 14-11*a*). Sea $A = \{a, c, d\}$.

a) Encuentre el conjunto de cotas superiores de A. *c*) ¿Existe sup(A)?

b) Encuentre el conjunto de cotas inferiores de A. *d*) ¿Existe ínf(A)?

14.50 Repita el problema 14.49 para el subconjunto $B = \{b, c, e\}$ de S.

14.51 Sea $S = \{1, 2, \ldots, 7, 8\}$ ordenado como en la figura 14-11*b*). Considere el subconjunto $A = \{3, 6, 7\}$ de S.

a) Encuentre el conjunto de cotas superiores de A. *c*) ¿Existe sup(A)?

b) Encuentre el conjunto de cotas inferiores de A. *d*) ¿Existe ínf(A)?

14.52 Repita el problema 14.51 para el subconjunto $B = \{1, 2, 4, 7\}$ de S.

14.53 Considere los números racionales $\mathbf{Q}$ con el orden usual $\leq$. Sea $A = \{x \mid x \in \mathbf{Q} \text{ y } 5 < x^3 < 27\}$.

a) ¿A está acotado por arriba o por abajo? *b*) ¿Existen sup(A) o ínf(A)?

14.54 Considere los números reales $\mathbf{R}$ con el orden usual $\leq$. Sea $A = \{x \mid x \in \mathbf{Q} \text{ y } 5 < x^3 < 27\}$.

a) ¿A está acotado por arriba o por abajo? *b*) ¿Existen sup(A) o ínf(A)?

CONJUNTOS ISOMÓRFOS (SEMEJANTES), TRANSFORMACIONES DE SEMEJANZA

14.55 Encuentre el número de conjuntos parcialmente ordenados no isomorfos con tres elementos a, b, c, y dibuje sus diagramas.

14.56 Encuentre el número de conjuntos parcialmente ordenados no isomorfos conexos con cuatro elementos a, b, c, d y dibuje sus diagramas.

14.57 Encuentre el número de transformaciones de semejanza $f: S \to S$ donde S es el conjunto ordenado en la:

a) Fig. 14-17*a*); *b*) Fig. 14-17*b*); *c*) Fig. 14-17*c*).

14.58 Demuestre que la relación isomorfa $A \cong B$ para conjuntos ordenados es una relación de equivalencia; es decir:

a) $A \cong A$ para cualquier conjunto ordenado A. *b*) Si $A \cong B$, entonces $B \cong A$. *c*) Si $A \cong B$ y $B \cong C$, entonces $A \cong C$.

CONJUNTOS BIEN ORDENADOS

14.59 Sea la unión S de conjuntos bien ordenados $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$, $C = \{c_1, c_2, c_3, \ldots\}$ ordenados por:

$$S = \{A; B; C\} = \{a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots\}$$

a) Demuestre que S está bien ordenado.

b) Encuentre todos los elementos límite de S.

c) Demuestre que S no es isomorfo a $\mathbf{N} = \{1, 2, \ldots\}$ con el orden usual $\leq$.

14.60 Sea $A = \{a, b, c\}$ linealmente ordenado por $a < b < c$, y sea $\mathbf{N}$ con el orden usual $\leq$.

a) Demuestre que $S = \{A; \mathbf{N}\}$ es isomorfo con $\mathbf{N}$.

b) Demuestre que $S' = \{\mathbf{N}; A\}$ no es isomorfo con $\mathbf{N}$.

14.61 Suponga que A es un conjunto bien ordenado bajo la relación $\precsim$ y suponga que A también está bien ordenado bajo la relación inversa $\succsim$. Describa A.

14.62 Suponga que A y B son conjuntos isomorfos bien ordenados. Demuestre que sólo hay una transformación de semejanza $f: A \to B$.

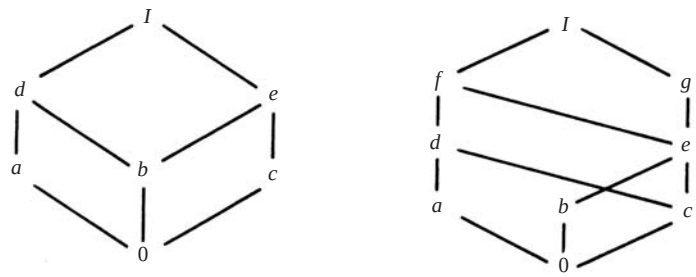
14.63 Sea S un conjunto bien ordenado. Para cualquier $a \in S$, el conjunto $s(a) = \{x \mid x \prec a\}$ se denomina *segmento inicial* de a. Demuestre que S no puede ser isomorfo a uno de sus *segmentos iniciales*. (*Sugerencia:* use el problema 14.21).

14.64 Suponga que $s(a)$ y $s(b)$ son segmentos iniciales distintos de un conjunto S bien ordenado. Demuestre que $s(a)$ y $s(b)$ no pueden ser isomorfos. (*Sugerencia:* use el problema 14.63).

RETÍCULOS

14.65 Considere el retículo L en la figura 14-19*a*).

a) Encuentre todos los subretículos con cinco elementos.
b) Encuentre todos los elementos irreducibles y los átomos.
c) Encuentre los complementos de a y b, en caso de existir.
d) ¿L es distributivo? ¿Complementado?



a) *b*)

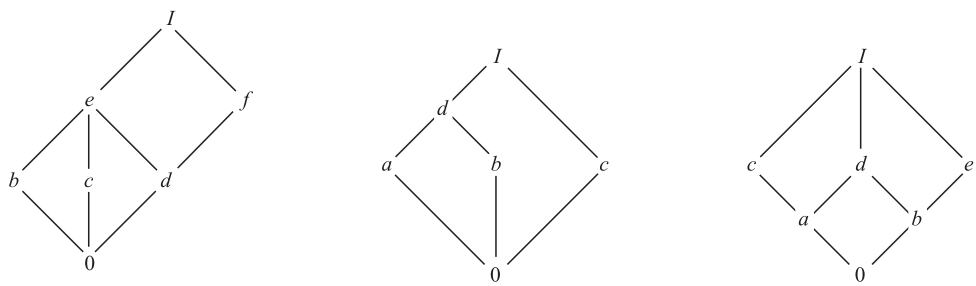
Figura 14-19

14.66 Considere el retículo M en la figura 14-19*b*).

a) Encuentre todos los elementos irreducibles.
b) Encuentre los átomos.
c) Encuentre los complementos de a y b, en caso de existir.
d) Exprese cada x en M como la unión de elementos irreducibles irredundantes.
e) ¿M es distributivo? ¿Complementado?

14.67 Considere el retículo acotado L en la figura 14-20*a*).

a) Encuentre los complementos, en caso de existir, de e y f.
b) Exprese I como una descomposición irredundante de irreducibles en la mayor cantidad de formas posible.
c) ¿L es distributiva?
d) Describa los isomorfismos de L consigo misma.



a) *b*) *c*)

Figura 14-20

14.68 Considere el retículo acotado L en la figura 14-20*b*).

a) Encuentre los complementos, en caso de existir, de a y b.
b) Exprese I como una descomposición irredundante de irreducibles en la mayor cantidad de formas posible.
c) ¿L es distributivo?
d) Describa los isomorfismos de L consigo mismo.

14.69 Considere el retículo acotado L en la figura 14-20*c*).

a) Encuentre los complementos, en caso de existir, de a y c.

b) Exprese I como una descomposición irredundante de irreducibles en la mayor cantidad de formas posible.

c) ¿L es distributivo?

d) Describa los isomorfismos de L consigo mismo.

14.70 Considere el retículo $\mathbf{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, los divisores de 60 ordenados por divisibilidad.

a) Haga el diagrama de $\mathbf{D}_{60}$.

b) ¿Cuáles elementos son irreducibles y cuáles son átomos?

c) Encuentre los complementos de 2 y 10, en caso de existir.

d) Exprese cada número x como la unión de un número mínimo de elementos irreducibles irredundantes.

14.71 Considere el retículo **N** de enteros positivos ordenados por divisibilidad.

a) ¿Cuáles elementos son irreducibles?

b) ¿Cuáles elementos son átomos?

14.72 Demuestre que las siguientes leyes distributivas "débiles" se cumplen para cualquier retículo L:

a) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$;

b) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

14.73 Sea $S = \{1, 2, 3, 4\}$. Se usa la notación $[12, 3, 4] \equiv [\{1, 2\}, \{3\}, \{4\}]$. A continuación se muestran tres particiones de S:

$$P_1 = [12, 3, 4], \quad P_2 = [12, 34], \quad P_3 = [13, 2, 4]$$

a) Encuentre las otras doce particiones de S.

b) Sea L la colección de las 12 particiones de S ordenadas por *refinamiento*; es decir, $P_i \prec P_j$ si cada celda de P_i es un subconjunto de una celda de P_j. Por ejemplo, $P_1 \prec P_2$ pero P_2 y P_3 no son comparables. Demuestre que L es un retículo acotado y trace su diagrama.

14.74 Se dice que un elemento a en un retículo es irreducible si $a = x \wedge y$ implica $a = x$ o $a = y$. Encuentre todos los elementos irreducibles en: *a*) Fig. 14-19*a*); *b*) Fig. 14-19*b*); *c*) $\mathbf{D}_{60}$ (vea el problema 14.70)

14.75 Se dice que un retículo es *modular* si siempre que $a \leq c$ se tiene la ley

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

a) Demuestre que todo retículo distributivo es modular.

b) Compruebe que el retículo no distributivo en la figura 14-7*b*) es modular; por tanto, la conversa de *a*) no es verdadera.

c) Demuestre que el retículo no distributivo en la figura 14-7*a*) no es modular. (De hecho, puede demostrarse que todo retículo no modular contiene un subretículo isomorfo a la figura 14-7*a*.)

14.76 Sea R un anillo. Sea L la colección de todos los ideales de R. Demuestre que L es un retículo acotado donde, para ideales arbitrarios J y K de R se define: $J \vee K = J + K$ y $J \wedge K = J \cap K$.

Respuestas a los problemas suplementarios

14.31 *a*) Minimales 4 y 6; maximales, 1 y 2. *b*) Primero, ninguno, último, ninguno, *c*) {1, 3, 4}, {1, 3, 6}, {2, 3, 4}, {2, 3, 6}, {2, 5, 6}.

14.32 *a*) Minimales, *d* y *f*; maximal, *a*. *b*) Primero, ninguno; último, *a*. *c*) Hay once: *dfebca*, *dfecba*, *dfceba*, *fdebca*, *fdecba*, *fdceba*, *fedbca*, *fedcba*, *fcdeba*, *fecdba*, *fcedba*.

14.33 Vea la figura 14-21.

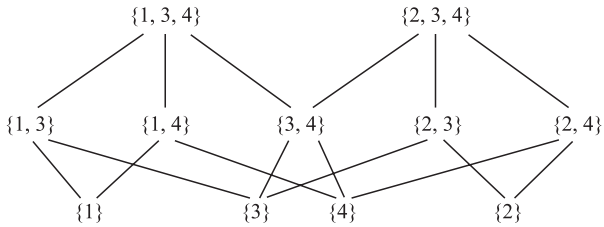
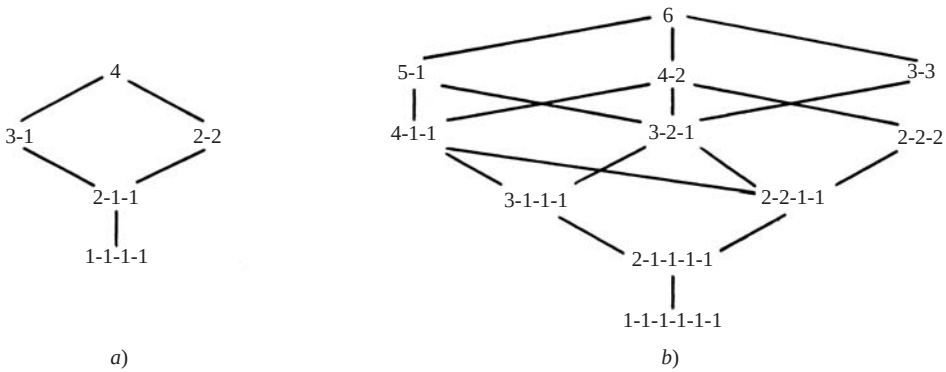


Figura 14-21

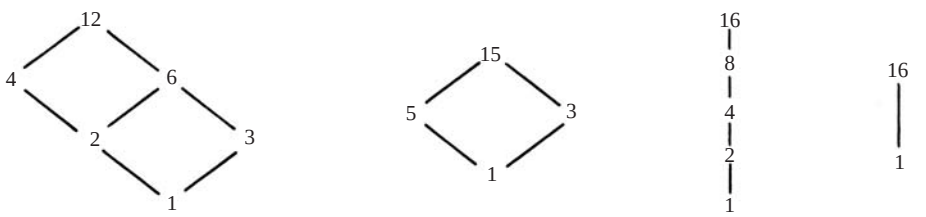
14.34 Vea la figura 14-22.



a) *b*)

Figura 14-22

14.35 Vea la figura 14-23.



a) *b*) *c*) *d*)

Figura 14-23

14.36 *Sugerencia:* Dibuje el diagrama de S.
a) Minimal, e; maximal, a, d.
b) Primero, e; último: ninguno.
c) $\{a, d\}$, $\{b, c\}$.

14.37 *a*) Falsa. Ejemplo: $\mathbf{N} \cup \{a\}$ donde $1 \ll a$ y $\mathbf{N}$ ordenado por $\leq$. *b*) Verdadera. *c*) Verdadera.

14.38 *a*) Minimal, a; máximal, d y e. *b*) Primero, a; último, ninguno. *c*) Cualquier subconjunto que contenga a c y omita a a; es decir, c, cb, cd, ce, cbd, cbe, cde, $cbde$. *d*) c, cd, ce, cde. *e*) abd, acd, ace.

14.39 *a*) Minimal a y b; maximal, e y f. *b*) Primero, ninguno; último, ninguno. *c*) ace, acf, bce, bcf, bdf.

14.40 *a*) Cuatro; *b*) Ninguno.

14.41 *a*) Seis; *b*) Ninguno.

14.42 $abcde$, $abced$, $acbde$, $acbed$, $acebd$.

14.43 Once.

14.44 $a \ll b$, $a \ll c$, $c \ll d$.

14.45 Minimal, $(p, 2)$, donde p es primo. Maximal, ninguno.

14.46 *a*) an, at, go, or, arm, one, gate, gone, about, occur.
b) an, about, arm, at, gate, go, gone, occur, one, or.

14.47 *a*) $\|$; *b*) $>$; *c*) $\|$; *d*) $<$.

14.48 1c, 1y, 2a, 2c, 2z, 3b, 4b, 4z.

14.49 *a*) e, f, g; *b*) a; *c*) $\sup(A) = e$; *d*) $\text{ínf}(A) = a$.

14.50 *a*) e, f, g; *b*) ninguno; *c*) $\sup(B) = e$; *d*) ninguno.

14.51 *a*) 1, 2, 3; *b*) 8; *c*) $\sup(A) = 3$; *d*) $\text{ínf}(A) = 8$.
14.52 *a*) Ninguno; *b*) 8; *c*) ninguno; *d*) $\text{ínf}(B) = 8$.
14.53 *a*) Ambos; *b*) $\sup(A) = 3$; c) $\text{ínf}(A)$ no existe.
14.54 *a*) Ambos; *b*) $\sup(A) = 3$; $\text{ínf(A)} = \sqrt[3]{5}$
14.55 Cuatro: 1) *a*, *b*, *c*; 2) *a*, $b \ll c$; 3) $a \ll b$, $a \ll c$. 4) $a \ll b \ll c$.
14.56 Cuatro: vea la figura 14-24.

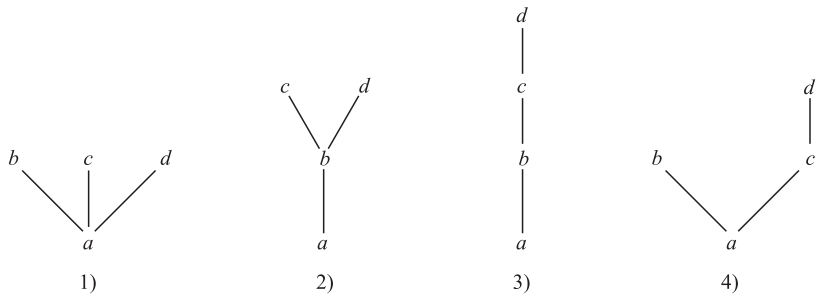


Figura 14-24

14.57 *a*) Uno: transformación identidad; b) uno; c) dos.
14.59 *b*) b_1, c_1; *c*) **N** no tiene puntos límite.
14.60 *a*) Se define $f: S \to \mathbf{N}$ por $f(a) = 1$, $f(b) = 2$, $f(3) = 3$, $f(n) = n + 3$.
b) El elemento *a* es un punto límite de S', pero **N** no tiene puntos límite.
14.61 *A* es un conjunto finito linealmente ordenado.
14.65 *a*) Seis: 0*abdI*, 0*acdI*, 0*adeI*, 0*bceI*, 0*aceI*, 0*cdeI*; *b*) *i*) *a*, *b*, *c*, 0; *ii*) *a*, *b*, *c*. *c*) *c* y *e* son complementos de *a*; *b* no tiene complemento. *d*) No. No.
14.66 *a*) *a*, *b*, *c*, *g*, 0. *b*) *a*, *b*, *c*. *c*) *a* tiene a *g*; *b* no tiene ninguno. *d*) $I = a \vee g$, $f = a \vee b$, $e = b \vee c$, $d = a \vee c$. Otros elementos son irreducibles. *e*) No. No.
14.67 *a*) *a* no tiene ninguno; *f* tiene a *b* y a *c*. *b*) $I = c \vee f = b \vee f = b \vee d \vee f$. *c*) No, puesto que las descomposiciones no son únicas. *d*) Dos: 0, *d*, *e*, *f*, *I* deben transformarse en sí mismos. Entonces $F = 1_L$, la transformación identidad sobre *L*, o $F = \{(b, c), (c, b)\}$.
14.68 *a*) *a* tiene a *c*; *c* tiene a *a* y *b*. *b*) $I = a \vee c = b \vee c$. c) No. *d*) Dos: 0, *c*, *d*, *I* deben transformarse en sí mismos. Entonces, $f = 1_L$ o $f = \{(a, b), (b, a)\}$.
14.69 *a*) *a* tiene a *e*; *c* tiene a *b* y *e*. *b*) $I = a \vee e = b \vee c = c \vee e$. *c*) No. *d*) Dos: 0, *d*, *I* deben transformarse en sí mismos. Entonces, $f = 1_L$ o $f = \{(a, b), (b, a), (c, d), (d, c)\}$.
14.70 *a*) Vea la figura 14-25. *b*) 1, 2, 3, 4, 5. Los átomos son 2, 3 y 5. *c*) 2 no tiene ninguno, 10 no tiene ninguno. *d*) $60 = 4 \vee 3 \vee 5$; $30 = 2 \vee 3 \vee 5$; $20 = 4 \vee 5$; $15 = 3 \vee 5$; $12 = 3 \vee 4$; $10 = 2 \vee 5$; $6 = 2 \vee 3$.

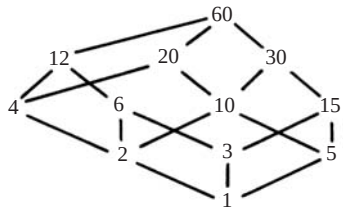


Figura 14-25

14.73 *a*) [1, 2, 3, 4], [14, 2, 3], [13, 24], [14, 23], [123, 4], [124, 3], [134, 2], [234, 1], [1234], [23, 1, 4] [24, 1, 3], [34, 1, 2]. *b*) Vea la Fig. 14-26.

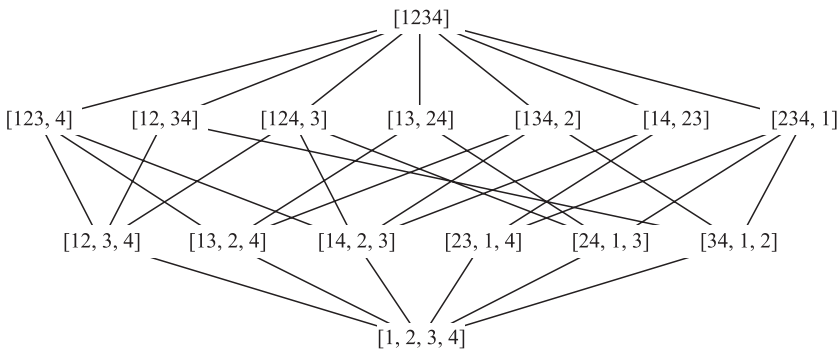


Figura 14-26

14.74 Geométricamente, un elemento $a \neq I$ es irreducible si y sólo si a tiene sólo un sucesor inmediato. *a*) a, c, d, e, I; *b*) a, b, d, f, g, I; *c*) 4, 6, 12, 15, 60.

14.75 *a*) Si $a \leq c$ entonces $a \vee c = c$. Por tanto $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$; *b*) Aquí $a \leq c$. Pero $a \vee (b \wedge c) = a \vee 0 = a$ y $(a \vee b) \wedge c = I \wedge c = c$; por tanto $a \vee (b \wedge c) = (a \vee b) \wedge c$.

15 Álgebra booleana

CAPÍTULO

15.1 INTRODUCCIÓN

Los conjuntos y las proposiciones satisfacen leyes semejantes, que se enumeran en las tablas 1-1 y 4-1 (en los capítulos 1 y 4). Estas leyes sirven para definir una estructura matemática abstracta denominada *álgebra booleana*, en honor del matemático George Boole (1815-1864).

15.2 DEFINICIONES BÁSICAS

Sea B un conjunto no vacío con dos operaciones binarias: $+$ y $*$, una operación unaria: $'$, y dos elementos distintos: 0 y 1. Entonces B se denomina *álgebra booleana* si los siguientes axiomas se cumplen, donde a, b, c son elementos arbitrarios en B:

[$\mathbf{B_1}$] Leyes conmutativas:
$1a)$ $a + b = b + a$ $\qquad$ $1b)$ $a * b = b * a$

[$\mathbf{B_2}$] Leyes distributivas:
$2a)$ $a + (b * c) = (a + b) * (a + c)$ $\qquad$ $2b)$ $a * (b + c) = (a * b) + (a * c)$

[$\mathbf{B_3}$] Leyes de identidad:
$3a)$ $a + 0 = a$ $\qquad$ $3b)$ $a * 1 = a$

[$\mathbf{B_4}$] Leyes del complemento:
$4a)$ $a + a' = 1$ $\qquad$ $4b)$ $a * a' = 0$

Algunas veces, un álgebra booleana se designa por $\langle B, +, *, ', 0, 1\rangle$ cuando se quiere resaltar sus seis partes. Se dice que 0 es el elemento *cero*; 1, el elemento *unidad* y a' el *complemento* de a. El símbolo * no suele usarse y en su lugar se usa la yuxtaposición. Así $(2b)$, se escribe $a(b + c) = ab + ac$, que es la conocida identidad algebraica de anillos y campos. Sin embargo $(2a)$, se convierte en $a + bc = (a + b)(a + c)$, que ciertamente no es una identidad usual en álgebra.

Las operaciones $+$, $*$ y $'$ se denominan, respectivamente, suma, producto y complemento. Se adopta la convención de costumbre de que, a menos que haya paréntesis, $'$ tiene precedencia sobre $*$ y $*$ tiene precedencia sobre $+$. Por ejemplo,

$$a + b * c \text{ significa } a + (b * c) \text{ y no } (a + b) * c; \quad a * b' \text{ significa } a * (b') \text{ y no } (a * b)'$$

Por supuesto, cuando $a + b * c$ se escribe $a + bc$, entonces el significado es evidente.

EJEMPLO 15.1

a) Sea $\mathbf{B} = \{0, 1\}$ el conjunto de *bits* (dígitos binarios), con las operaciones binarias de $+$ y $*$ y la operación unaria $'$ definida por la figura 15-1. Entonces **B** es un álgebra booleana. (Observe que $'$ simplemente cambia el bit; es decir, $1' = 0$ y $0' = 1$).

$+$	1	0
1	1	1
0	1	0

$*$	1	0
1	1	0
0	0	0

$'$	1	0
	0	1

Figura 15-1

b) Sea $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \cdots \times \mathbf{B}$ (n factores) donde las operaciones de $+$, $*$ y $'$ están definidas por componentes al usar la figura 15-1. Por conveniencia en la notación, los elementos de $\mathbf{B}^n$ se escriben como secuencias de n-bits sin comas; por ejemplo, $x =$ 110011 y $y = 111000$ pertenecen a $\mathbf{B}^n$. Por tanto,

$$x + y = 111011, \quad x * y = 110000, \quad x' = 001100$$

Entonces $\mathbf{B}^n$ es un álgebra booleana. Aquí, $0 = 000 \cdots 0$ es el elemento cero, y $1 = 111 \cdots 1$ es el elemento unidad. Se observa que $\mathbf{B}^n$ tiene 2^n elementos.

c) Sea $\mathbf{D}_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$, los divisores de 70. $+$, * y $'$ se definen sobre $\mathbf{D_{70}}$ como

$$a + b = \text{mcm}(a, b), \quad a * b = \text{mcd}(a, b), \quad a' = \frac{70}{a}$$

Entonces $\mathbf{D}_{70}$ es un algebra booleana con 1 como elemento cero y 70 como elemento unidad.

d) Sea C una colección de conjuntos cerrados bajo las operaciones de conjuntos unión, intersección y complemento. Entonces C es un álgebra booleana con el conjunto vacío $\varnothing$ como elemento cero y el conjunto universo $\mathbf{U}$ como elemento unidad.

Subálgebras, álgebras booleanas isomorfas

Suponga que C es un subconjunto no vacío de un álgebra booleana B. Se dice que C es un *subálgebra* de B si C mismo es un álgebra booleana (con respecto a las operaciones de B). Observe que C es una subálgebra de B si y sólo si C es cerrado bajo las tres operaciones de B; es decir, $+$, $*$ y $'$. Por ejemplo $\{1, 2, 35, 70\}$, es un subálgebra de $\mathbf{D}_{70}$ en el ejemplo 15.1*c*).

Dos álgebras booleanas B y B' son *isomorfas* si existe una correspondencia uno a uno f: B $\rightarrow B'$ que preserva las tres operaciones; es decir, tal que para elementos arbitrarios a, b en B,

$$f(a + b) = f(a) + f(b), \quad f(a * b) = f(a) * f(b) \quad \text{y} \quad f(a') = f(a)'$$

15.3 DUALIDAD

El *dual* de cualquier proposición en un álgebra booleana B es la proposición que se obtiene al intercambiar las operaciones $+$ y $*$, e intercambiar sus elementos identidad 0 y 1 en la proposición original. Por ejemplo, el dual de

$$(1 + a) * (b + 0) = b \quad \text{es} \quad (0 * a) + (b * 1) = b$$

Observe la simetría en los axiomas de un álgebra booleana B. Es decir, el dual del conjunto de axiomas de B es el mismo que el conjunto original de axiomas. En consecuencia, el importante principio de dualidad se cumple en B. A saber,

Teorema 15.1 (Principio de dualidad): El dual de cualquier teorema en un álgebra booleana también es un teorema.

En otras palabras, si cualquier proposición es una consecuencia de los axiomas de un álgebra booleana, entonces el dual también es una consecuencia de estos axiomas, puesto que la proposición dual se demuestra al aplicar el dual de cada paso en la demostración de la proposición original.

15.4 TEOREMAS BÁSICOS

El siguiente teorema se demuestra (problema 15.5) mediante los axiomas **[$\mathbf{B_1}$]** a [$\mathbf{B_4}$]:

Teorema 15.2: Sean a, b, c elementos arbitrarios en un álgebra booleana B.

i) Leyes de idempotencia:
5*a*) $a + a = a$ 5*b*) $a * a = a$
ii) Leyes de acotamiento:
6*a*) $a + 1 = 1$ 6*b*) $a * 0 = 0$
iii) Leyes de absorción:
7*a*) $a + (a * b) = a$ 7*b*) $a * (a + b) = a$
iv) Leyes asociativas:
8*a*) $(a + b) + c = a + (b + c)$ 8*b*) $(a * b) * c = a * (b * c)$

El teorema 15.2 y los axiomas contienen todas las propiedades de conjuntos enumeradas en la tabla 1-1. Los dos teoremas siguientes proporcionan las propiedades restantes.

Teorema 15.3: Sea a cualquier elemento de un álgebra booleana B.

i) (Unicidad del complemento) Si $a + x = 1$ y $a * x = 0$, entonces $x = a'$.
ii) (Ley de involución) $(a')' = a$.
iii) 9*a*) $0' = 1$. 9*b*) $1' = 0$.

Teorema 15.4 (Leyes de DeMorgan): 10*a*) $(a + b)' = a' * b'$. 10*b*) $(a * b)' = a' + b'$.

Estos teoremas se demuestran en los problemas 15.6 y 15.7.

15.5 ÁLGEBRAS BOOLEANAS COMO RETÍCULOS

Por el teorema 15.2 y el axioma [$\mathbf{B_1}$], toda álgebra booleana B satisface las leyes asociativa, conmutativa y de absorción, de modo que se trata de un retículo donde $+$ y $*$ son las operaciones unir y encontrar, respectivamente. Con respecto a este retículo, $a + 1 = 1$ implica $a \leq 1$ y $a * 0 = 0$ implica $0 \leq a$, para cualquier elemento $a \in B$. Así, B es un retículo acotado. Además, los axiomas [$\mathbf{B_2}$] y [$\mathbf{B_4}$] muestran que B también es distributivo y complementado. A la inversa, todo retículo L acotado, distributivo y complementado satisface los axiomas [$\mathbf{B_1}$] a [$\mathbf{B_4}$]. En consecuencia, se tiene la siguiente

Definición alterna: Un álgebra booleana B es un retículo acotado, distributivo y complementado.

Puesto que un álgebra booleana B es un retículo, tiene un orden parcial natural (y entonces es posible trazar su diagrama). Recuerde (capítulo 14) que $a \leq b$ se define cuando se cumplen las condiciones equivalentes $a + b = b$ y $a * b = a$. Puesto que se está en un álgebra booleana B, en realidad puede decirse mucho más.

Teorema 15.5: Las siguientes expresiones son equivalentes en un álgebra booleana:

1) $a + b = b$, *2*) $a * b = a$, *3*) $a' + b = 1$, *4*) $a * b' = 0$

Por tanto, en un álgebra booleana puede escribirse $a \leq b$ siempre que se sepa que cualquiera de las condiciones anteriores es verdadera.

EJEMPLO 15.2

a) Considere un álgebra booleana de conjuntos. Entonces el conjunto A precede al conjunto B si A es un subconjunto de B. El teorema 15.4 establece que si $A \subseteq B$, entonces se cumplen las siguientes condiciones:

1) $A \cup B = B$ 2) $A \cap B = A$ 3) $A^c \cup B = \mathbf{U}$ 4) $A \cap B^c = \varnothing$

b) Considere el álgebra booleana $\mathbf{D}_{70}$. Entonces a precede a b si a divide a b. En este caso, mcm(a, b) = b y mcd(a, b) = a. Por ejemplo, sean $a = 2$ y $b = 14$. Entonces las siguientes condiciones se cumplen:

1) mcm(2, 14) = 14.
2) mcd(2, 14) = 2.
3) mcm(2′, 14) = mcm(35, 14) = 70.
4) mcd(2, 14′) = mcd(2, 5) = 1.

15.6 TEOREMA DE REPRESENTACIÓN

Sea B un álgebra booleana finita. Recuerde (sección 14.10) que un elemento a en B es un átomo de a si a sucede inmediatamente a 0; es decir, si $0 \ll a$. Sea A el conjunto de átomos de B y sea $P(A)$ el álgebra booleana de todos los subconjuntos del conjunto A de átomos. Por el teorema 14.8, cada $x \neq 0$ en B puede expresarse de manera única (salvo por el orden) como la suma (unión) de átomos; es decir, elementos de A. Por ejemplo,

$$x = a_1 + a_2 + \cdots + a_r$$

es una representación así. Considere la función $f: B \to P(A)$ definida por

$$f(x) = \{a_1, a_2, \ldots, a_r\}$$

La transformación está bien definida puesto que la representación es única.

Teorema 15.6: La transformación $f: B \to P(A)$ anterior es un isomorfismo.

Por tanto, se observa la estrecha relación entre teoría de conjuntos y álgebras booleanas abstractas en el sentido de que toda álgebra booleana finita es estructuralmente lo mismo que un álgebra booleana de conjuntos.

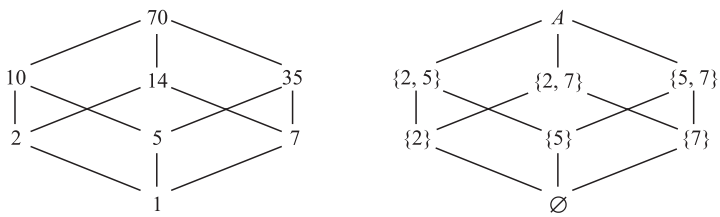
Si un conjunto A tiene n elementos, entonces su conjunto potencia $P(A)$ tiene 2^n elementos. Así, el teorema anterior proporciona el siguiente resultado.

Corolario 15.7: Un álgebra booleana finita tiene 2^n elementos para algún entero positivo n.

EJEMPLO 15.3 Considere el álgebra booleana $\mathbf{D}_{70} = \{1, 2, 5, \ldots, 70\}$, cuyo diagrama se muestra en la figura 15-2*a*). Observe que $A = \{2, 5, 7\}$ es el conjunto de átomos de $\mathbf{D}_{70}$. A continuación se presenta la única representación de cada no átomo mediante átomos:

$$10 = 2 \vee 5, \quad 14 = 2 \vee 7, \quad 35 = 5 \vee 7, \quad 70 = 2 \vee 5 \vee 7$$

En la figura 15-2*b*) se proporciona el diagrama del álgebra booleana del conjunto potencia $P(A)$ del conjunto A de átomos. Observe que ambos diagramas son estructuralmente lo mismo.



a) $\mathbf{D}_{70}$ *b*) $P(A)$

Figura 15-2

15.7 REPRESENTACIÓN DE CONJUNTOS EN FORMA DE SUMA DE PRODUCTOS

Esta sección motiva el concepto de suma de productos en álgebra booleana mediante un ejemplo de teoría de conjuntos. Considere el diagrama de Venn en la figura 15-3 de tres conjuntos A, B y C. Observe que estos conjuntos parten el rectángulo (conjunto universo) en ocho conjuntos numerados que pueden representarse como sigue:

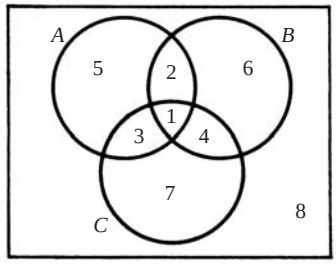


Figura 15-3

1) $A \cap B \cap C$ 3) $A \cap B^c \cap C$ 5) $A \cap Bc \cap C^c$ 7) $A^c \cap B^c \cap C$
2) $A \cap B \cap C^c$ 4) $A^c \cap B \cap C$ 6) $A^c \cap B \cap C^c$ 8) $A^c \cap B^c \cap C^c$

Cada uno de estos ocho conjuntos es de la forma $A^* \cap B^* \cap C^*$, donde:

$$A^* = A \text{ o } A^c, \quad B^* = B \text{ o } B^c, \quad C^* = C \text{ o } C^c$$

Considere cualquier expresión de conjuntos no vacía E que implique los conjuntos A, B y C, por ejemplo,

$$E = [(A \cap B^c)^c \cup (A^c \cap C^c)] \cap [(B^c \cup C)^c \cap (A \cup C^c)]$$

Entonces E representa algún área en la figura 15-3 y, por tanto, es igual en forma única a la unión de uno o más de los ocho conjuntos.

Suponga que ahora se interpreta una unión como una suma y una intersección como un producto. Entonces los ocho conjuntos anteriores son productos y la única representación de E es una suma (unión) de productos. Esta representación única de E es lo misma que el desarrollo completo como suma de productos en álgebras booleanas que se analiza a continuación.

15.8 REPRESENTACIÓN DE ÁLGEBRAS BOOLEANAS EN FORMA DE SUMA DE PRODUCTOS

Considere un conjunto de variables (o letras o símbolos); por ejemplo, $x_1, x_2, \ldots, x_n$. Una *expresión booleana* E en estas variables, lo cual algunas veces se escribe $E(x_1, \ldots, x_n)$, es cualquier variable o cualquier expresión que se obtiene a partir de las variables mediante las operaciones booleanas $+$, $*$ y $'$. (Por supuesto, la expresión E debe estar *bien formada*; es decir, donde $+$ y $*$ se usan como operaciones binarias, y $'$ se usa como operación unaria.) Por ejemplo,

$$E_1 = (x + y'z)' + (xyz' + x'y)' \quad \text{y} \quad E_2 = ((xy'z' + y)' + x'z)'$$

son expresiones booleanas en x, y y z.

Una *literal* es una variable o una variable complementada, como x, x', y, y', y así en lo sucesivo. Un *producto fundamental* es una literal o un producto de dos o más literales donde ningún par de literales implican la misma variable. Así,

$$xz', \quad xy'z, \quad x, \quad y', \quad x'yz$$

son productos fundamentales, pero $xyx'z$ y $xyzy$ no lo son. Observe que cualquier producto de literales puede reducirse a 0 o a un producto fundamental; por ejemplo, $xyx'z = 0$, puesto que $xx' = 0$ (ley de complemento), y $xyzy = xyz$ porque $yy = y$ (ley de idempotencia).

Un producto fundamental P_1 está *contenido en* (o *incluido en*) otro producto fundamental P_2 si las literales de P_1 también son las literales de P_2. Por ejemplo, $x'z$ está contenido en $x'yz$, pero $x'z$ no está contenido en $xy'z$ porque x' no es una literal de $xy'z$. Observe que si P_1 está contenido en P_2, por ejemplo, $P_2 = P_1 * Q$, entonces, por la ley de absorción,

$$P_1 + P_2 = P_1 + P_1 * Q = P_1$$

Así, por ejemplo, $x'z + x'yz = x'z$.

Definición 15.1: Una expresión booleana E se denomina expresión de *suma de productos* si E es un producto fundamental o la suma de dos o más productos fundamentales, ninguno de los cuales está contenido en el otro.

Definición 15.2: Sea E una expresión booleana arbitraria. Una forma de *suma de productos* de E es una expresión de suma de productos booleana equivalente.

EJEMPLO 15.4 Considere las expresiones

$$E_1 = xz' + y'z + xyz' \quad \text{y} \quad E_2 = xz' + x'yz + xy'z$$

Aunque la primera expresión E_1 es una suma de productos, no es una expresión de suma de productos. En específico, el producto xz' está contenido en el producto xyz'. Sin embargo, por la ley de absorción, E_1 se expresa como

$$E_1 = xz' + y'z + xyz' = xz' + xyz' + y'z = xz' + y'z$$

Esto lleva a una forma de suma de productos para E_1. La segunda expresión E_2 ya es una expresión de suma de productos.

Algoritmo para encontrar formas de suma de productos

En la figura 15-4 se proporciona un algoritmo de cuatro pasos que aplica leyes del álgebra booleana para transformar cualquier expresión booleana en una expresión de suma de productos equivalente.

Algoritmo 15.1: La entrada es una expresión booleana E. El resultado es una expresión de suma de productos equivalente a E.

Paso 1. Se usan las leyes de DeMorgan y de involución para mover la operación complemento en cualquier paréntesis hasta que la operación complemento sólo se aplica a variables. Entonces, E sólo consistirá de sumas y productos de literales.

Paso 2. Se usa la operación distributiva para transformar a continuación E en una suma de productos.

Paso 3. Se usan las leyes conmutativa, de idempotencia y de complemento para transformar cada producto en E en 0 o en un producto fundamental.

Paso 4. Se usan las leyes de absorción e identidad para transformar finalmente E en una expresión de suma de productos

Figura 15-4

EJEMPLO 15.5 Suponga que el algoritmo 15.1 se aplica a la siguiente expresión booleana:

$$E = ((xy)'z)'((x' + z)(y' + z))'$$

Paso 1. Al usar las leyes de DeMorgan y de involución se obtiene.

$$E = (xy'' + z')((x' + z)' + (y' + z')') = (xy + z')(xz' + yz)$$

Ahora E consiste sólo de sumas y productos de literales.

Paso 2. Al usar las leyes distributivas, se obtiene

$$E = xyxz' + xyyz + xz'z' + yzz'$$

Ahora E es una suma de productos.

Paso 3. Al usar las leyes conmutativa, de idempotencia y de complemento, se obtiene

$$E = xyz' + xyz + xz' + 0$$

Cada término en E es un producto fundamental o 0.

Paso 4. El producto xz' está contenido en xyz'; así, por la ley de absorción,

$$xz' + (xz'y) = xz'$$

Entonces, es posible borrar xyz' de la suma. También, por la ley identidad para 0, es posible eliminar 0 de la suma. En consecuencia,

$$E = xyz + xz'$$

Ahora, E está representada por una expresión de suma de productos.

Formas completas de suma de productos

Se dice que una expresión booleana $E = E(x_1, x_2, \ldots, x_n)$ es una expresión *completa de suma de productos* si E es una expresión de suma de productos donde cada producto P implica a todas las n variables. Cualquier producto fundamental P que utiliza a todas las variables se denomina *minterm* y hay un máximo de 2^n productos así para n variables. El siguiente teorema es válido.

Teorema 15.8: Cualquier expresión booleana diferente de cero $E = E(x_1, x_2, \ldots, x_n)$ es equivalente a una expresión completa de suma de productos y esta representación es única.

La representación única anterior de E se denomina *forma completa de suma de productos* de E. El algoritmo 15.1 en la figura 15-4 indica cómo transformar E en una forma de suma de productos. La figura 15-5 contiene un algoritmo que transforma una forma de suma de productos en una forma completa de suma de productos.

Algoritmo 15.2: La entrada es una expresión booleana E de suma de productos $E = E(x_1, x_2, \ldots, x_n)$. El resultado es una expresión completa de suma de productos equivalente a E.

Paso 1. Se encuentra un producto P en E que no implique a la variable x_i y luego P se multiplica por $x_1 + x_i'$, eliminando todos los productos repetidos. (Esto es posible puesto que $x_i + x_i' = 1$ y $P + P = P$.)

Paso 2. Se repite el paso 1 hasta que todo producto en E es un minterm; es decir, que todo producto P implica a todas las variables.

Figura 15-5

EJEMPLO 15.6 Exprese $E(x, y, z) = x(y'z)'$ en su forma completa de suma de productos.

a) El algoritmo 15.1 se aplica a E, de modo que E quede representada como una expresión de suma de productos:

$$E = x(y'z)' = x(y + z') = xy + xz'$$

b) Luego se aplica el algoritmo 15.1 para obtener:

$$\begin{aligned} E &= xy(z + z') + xz'(y + y') = xyz + xyz' + xyz' + xy'z' \\ &= xyz + xyz' + xy'z' \end{aligned}$$

Ahora, E está representada en su forma completa de suma de productos.

***Advertencia*:** La terminología en esta sección no se ha estandarizado. La forma de suma de productos para una expresión booleana E también se denomina *forma normal disyuntiva* o FND de E. La forma completa de suma de productos para E también se denomina *forma normal disyuntiva completa*, o *forma canónica disyuntiva*, o *forma canónica minterm de E*.

15.9 EXPRESIONES BOOLEANAS MINIMALES, IMPLICANTES PRIMOS

Hay muchas formas de representar la misma expresión booleana E. Aquí se define e investiga una forma de suma de productos minimal para E. También es necesario definir e investigar implicantes primos de E puesto que la suma de productos minimal supone tales implicantes. Hay otras formas minimales, pero su investigación rebasa el alcance de este texto.

Suma de productos minimal

Considere una expresión booleana de suma de productos E. Sea E_L el número de literales en E (contadas según multiplicidad), y sea E_S el número de sumandos en E. Por ejemplo, suponga

$$E = xyz' + x'y't + xy'z't + x'yzt$$

Entonces $E_L = 3 + 3 + 4 + 4 = 14$ y $E_S = 4$.

Suponga que E y F son expresiones booleanas de suma de productos equivalentes. Se dice que E es más *simple* que F si:

$$i)\ E_L < F_L \text{ y } E_S \leq F_L, \quad \text{o} \quad ii)\ E_L \leq F_L \text{ y } E_S < F_L$$

Se dice que E es *minimal* si no hay ninguna expresión de suma de productos más simple que E. Observe que puede haber más de una expresión minimal de suma de productos equivalente.

Implicantes primos

Un producto fundamental P se denomina *implicante primo* de una expresión booleana E si

$$P + E = E$$

pero ningún otro producto fundamental contenido en P tiene esta propiedad. Por ejemplo, suponga que

$$E = xy' + xyz' + x'yz'$$

Puede demostrarse (problema 15.5) que:

$$xz' + E = E \quad \text{pero} \quad x + E \neq E \quad \text{y} \quad z' + E \neq E$$

Así, xz' es un implicante primo de E.

El siguiente teorema es válido.

Teorema 15.9: Una forma de suma de productos minimal de una expresión booleana E es una suma de implicantes primos de E.

En las siguientes subsecciones se proporciona un método para encontrar los implicantes primos de E con base en el concepto del consenso de productos fundamentales. Así, este método puede usarse para encontrar una forma de suma de productos minimal para E. En la sección 15.2 se proporciona un método geométrico para encontrar estos implicantes primos.

Consenso de productos fundamentales

Sean P_1 y P_2 productos fundamentales con exactamente una variable, por ejemplo x_k, que aparece sin complementar ya sea en P_1 o P_2 y aparece complementada en la otra. Entonces el *consenso* de P_1 y P_2 es el producto (sin repeticiones) de las literales de P_1 y las literales de P_2 después que se han eliminado x_k y x_k'. (No se define este consenso de $P_1 = x$ y $P_2 = x'$.)

El lema siguiente (que se demuestra en el problema 15.19, es válido).

Lema 15.10: Suponga que Q es el consenso de P_1 y P_2. Entonces $P_1 + P_2 + Q = P_1 + P_2$.

EJEMPLO 15.7 Encuentre el consenso Q de P_1 y P_2, donde

a) $P_1 = xyz's$ y $P_2 = xy't$.

Se eliminan y y y' y luego se multiplican las literales de P_1 y P_2 (sin repetición) para obtener $Q = xz'st$.

b) $P_1 = xy'$ y $P_2 = y$.

Al eliminar y y y' queda $Q = x$.

c) $P_1 = x'yz$ y $P_2 = x'yt$

Ninguna variable aparece sin complementar en uno de los productos y complementada en el otro. Por tanto, P_1 y P_2 no tienen consenso.

d) $P_1 = x'yz$ y $P_2 = xyz'$.

Cada una de x y z aparecen complementadas en uno de los productos e incomplementadas en el otro. Por tanto, P_1 y P_2 no tienen consenso.

Método del consenso para encontrar implicantes primos

La figura 15-6 muestra un algoritmo, que se denomina *método de consenso*, que se usa para encontrar los implicantes primos de una expresión booleana E. El siguiente teorema proporciona la propiedad fundamental de este algoritmo.

Teorema 15.11: Cuando el método de consenso finaliza, E es la suma de sus implicantes primos.

Algoritmo 15.3 (método de consenso): La entrada es una expresión booleana $E = P_1 + P_2 + \cdots + P_m$ donde las P son productos fundamentales. El resultado expresa E como una suma de sus implicantes primos (teorema 15.11).

Paso 1. Se eliminan todos los productos fundamentales P_i que incluyen a cualquier otro producto fundamental P_j (permisible por la ley de absorción).

Paso 2. Se suma el consenso de cualquier P_i y P_j en el supuesto de que Q no incluye a ninguna de las P (permisible por el lema 15.10).

Paso 3. Se repite el paso 1 y/o el paso 2 hasta que no es posible aplicar ninguno.

Figura 15-6

EJEMPLO 15.8 Sea $E = xyz + x'z' + xyz' + x'y'z + x'yz'$. Entonces:

$$\begin{aligned}
E &= xyz + x'z' + xyz' + x'y'z && (x'yz' \text{ incluye } x'z') \\
&= xyz + x'y' + xyz' + x'y'z + xy && (\text{consenso de } xyz \text{ y } xyz') \\
&= x'z' + x'y'z + xy && (xyz \text{ y } xyz' \text{ incluye } xy) \\
&= x'z + x'y'z + xy + x'y' && (\text{consenso de } x'z' \text{ y } x'y'z) \\
&= x'z' + xy + x'y' && (x'y'z \text{ incluye } x'y') \\
&= x'z' + xy + x'y' + yz' && (\text{consenso de } x'z' \text{ y } xy)
\end{aligned}$$

Así, ningún paso en el método de consenso modifica a E. Por tanto, E es la suma de sus implicantes primos, que aparecen en la última línea; es decir, $x'z'$, xy, $x'y'$ y yz'.

Determinación de una forma de suma de productos minimal

El método de consenso (algoritmo 15.3) se usa para escribir expresiones booleanas E como una suma de todos sus implicantes primos. En la figura 15-7 se presenta un algoritmo que usa tal suma para determinar una forma de suma de productos mínima para E.

Algoritmo 15.4: La entrada es una expresión booleana $E = P_1 + P_2 + \cdots + P_m$ donde todas las P son los implicantes primos de E. El resultado expresa a E como forma de suma de productos minimal.

Paso 1. Cada implicante primo se expresa como una suma de productos completa.

Paso 2. Se eliminan uno por uno los implicantes primos cuyos sumandos aparecen entre los sumandos de los implicantes primos restantes.

Figura 15-7

EJEMPLO 15.9 El algoritmo 15.4 se aplica a la siguiente expresión E que (por el ejemplo 15.8) ahora expresa la suma de todos sus implicantes primos:

$$E = x'z' + xy + x'y' + yz'$$

Paso 1. Cada implicante primo de E se expresa como una suma de productos completa para obtener:

$$\begin{aligned} x'z' &= x'z'(y + y') = x'yz' + x'y'z' \\ xy &= xy(z + z') = xyz + xyz' \\ x'y' &= x'y'(z + z') = x'y'z + x'y'z' \\ yz' &= yz'(x + x') = xyz' + x'yz' \end{aligned}$$

Paso 2. Los sumandos de $x'z'$ son $x'yz$ y $x'y'z'$, que aparecen entre los otros sumandos. Por tanto, se elimina $x'z'$ para obtener

$$E = xy + x'y' + yz'$$

Los sumandos de ningún otro implicante primo aparecen entre los sumandos de los implicantes primos restantes, de modo que se trata de una forma de suma de productos minimal para E. En otras palabras, ninguno de los implicantes primos restantes es *superfluo*; es decir, no es posible eliminar ninguno sin modificar a E.

15.10 COMPUERTAS Y CIRCUITOS LÓGICOS

Los *circuitos lógicos* (que también se denominan *redes lógicas*) son estructuras elaboradas a partir de ciertos circuitos elementales denominados *compuertas lógicas*. Cualquier circuito lógico se considera como una máquina L que contiene uno o más dispositivos de entrada y exactamente un dispositivo de salida. Cada dispositivo de entrada en L envía una señal, específicamente, un *bit* (*binary digit*: dígito binario),

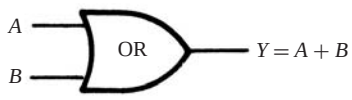
$$0 \quad \text{o} \quad 1$$

al circuito L, y L procesa el conjunto de bits para producir un bit de salida. En consecuencia, una secuencia de n bits puede asignarse a cada dispositivo de entrada, y L procesa las secuencias de entrada bit por bit para producir una secuencia de salida de n bits. Primero se definen las compuertas lógicas y luego se investigan los circuitos lógicos.

Compuertas lógicas

Hay tres compuertas lógicas básicas que se describen a continuación. Se adopta la convención de que las líneas que entran al símbolo de la compuerta por la izquierda son las líneas de entrada y que la línea a la derecha es la línea de salida.

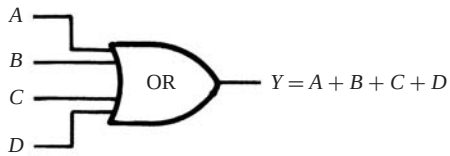
a) ***Compuerta OR:*** En la figura 15-8*a*) se muestra una compuerta OR con entradas A y B y salida $Y = A + B$, donde "adición" se define mediante la "tabla de verdad" en la figura 15-8*b*). Por tanto, la salida es $Y = 0$ sólo cuando se introducen $A = 0$ y $B = 0$. Esta compuerta OR puede tener más de dos entradas. En la figura 15-8*c*) se muestra una compuerta OR con cuatro entradas, A, B, C, D, y una salida $Y = A + B + C + D$. La salida es $Y = 0$ si y solo si todas las entradas son 0.



a) Compuerta OR

A	B	$A + B$
1	1	1
1	0	1
0	1	1
0	0	0

b)



c)

Figura 15-8

Suponga, por ejemplo, que los datos de entrada para la compuerta OR en la figura 15-15*c*) son las siguientes secuencias de 8 bits:

$$A = 10000101, \quad B = 10100001, \quad C = 00100100, \quad 10010101$$

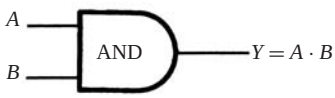
La compuerta OR sólo produce 0 cuando todos los bits de entrada son 0. Esto sólo ocurre en las posiciones segunda, quinta y séptima (de izquierda a derecha). Por tanto, la salida es la secuencia $Y = 10110101$.

b) ***Compuerta AND:*** En la figura 15-9*a*) se muestra una compuerta AND con entradas A y B y salida $Y = A \cdot B$ (o simplemente $Y = AB$) donde "multiplicación" se define mediante la "tabla de verdad" en la figura 15-9*b*). Por tanto, la salida $Y = 1$ cuando se introducen $A = 1$ y $B = 1$; en caso contrario, $Y = 0$. Una compuerta AND así puede tener más de dos entradas. En la figura 15-9*c*) se muestra una compuerta AND con cuatro entradas A, B, C, D y salida $Y = A \cdot B \cdot C \cdot D$. La salida es $Y = 1$ si y solo si todas las entradas son 1.

Suponga, por ejemplo, que los datos de entrada para la compuerta AND en la figura 15-9*c*) son las siguientes secuencias de 8 bits:

$$A = 11100111, \quad B = 01111011, \quad C = 01110011, \quad D = 11101110$$

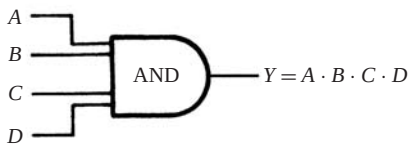
La compuerta AND sólo produce 1 cuando todos los bits de entrada son 1. Esto sólo ocurre en las posiciones segunda, tercera y séptima. Por tanto, la salida es la secuencia $Y = 01100010$.



a) Compuerta AND

A	B	$A \cdot B$
1	1	1
1	0	0
0	1	0
0	0	0

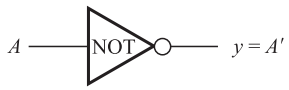
b)



c)

Figura 15-9

c) ***Compuerta NOT:*** En la figura 15-10*a*) se muestra una compuerta NOT, también denominada *invertidor*, con entrada A y salida $Y = A'$ donde "inversión", denotada por la prima, se define mediante la "tabla de verdad" en la figura 15-10*b*). Por tanto, el valor de la salida $Y = A'$ es lo opuesto de la entrada A; es decir, $A' = 1$ cuando $A = 0$ y $A' = 0$ cuando $A = 1$. Se recalca que una compuerta NOT sólo puede tener una entrada, en tanto que las compuertas OR y AND pueden tener dos o más entradas.



a) Compuerta NOT

A	A'
1	0
0	1

b)

Figura 15-10

Suponga, por ejemplo, que a una compuerta NOT se le indica procesar las tres secuencias siguientes:

$$A_1 = 110001, \quad A_2 = 10001111, \quad A_3 = 101100111000$$

La compuerta NOT cambia 0 a 1 y 1 a 0. Así,

$$A_1' = 001110, \quad A_2' = 01110000, \quad A_3' = 010011000111$$

son las tres salidas correspondientes.

Circuitos lógicos

Un circuito lógico L es una estructura L bien formada cuyos componentes elementales son las compuertas OR, AND y NOT recién mencionadas. La figura 15-11 es un ejemplo de un circuito lógico con entradas A, B, C y salida Y. Un punto indica un sitio en donde la línea de entrada se separa de modo que su señal de bits se envía en más de una dirección. (A menudo, por conveniencia en la notación, se omite la palabra en el interior del símbolo de la compuerta.) Al trabajar de izquierda a derecha, Y se expresa en términos de las entradas A, B, C como sigue: la salida de la compuerta AND es $A \cdot B$, que luego se niega para obtener $(A \cdot B)'$. La salida de la compuerta OR inferior es $A' + C$, que luego se niega para llegar a $(A' + C)'$. La salida de la compuerta OR a la derecha, con entradas $(A \cdot B)'$ y $(A' + C)'$, proporciona la representación deseada; es decir,

$$Y = (A \cdot B)' + (A' + C)'$$

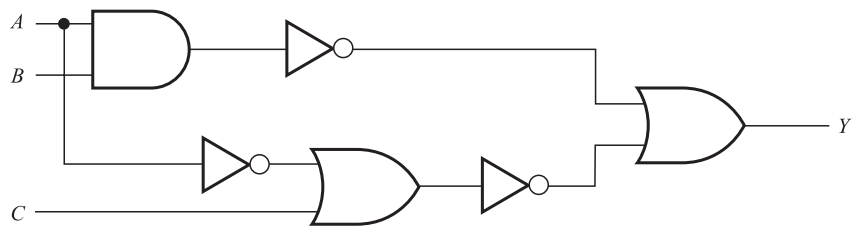


Figura 15-11

Circuitos lógicos como álgebras booleanas

Observe que las tablas de verdad de las compuertas OR, AND y NOT son idénticas respectivamente a las tablas de verdad de las proposiciones $p \vee q$ (disyunción, "p o q"), $p \wedge q$ (conjunción, "p y q"), y $\neg p$ (negación, "no p"), que aparecen en la sección 4.3. La única diferencia es que se usan 0 y 1 en vez de T y F. Así, los circuitos lógicos cumplen las mismas leyes que las proposiciones y entonces constituyen un álgebra booleana. Este resultado se plantea formalmente a continuación.

Teorema 15.12: Los circuitos lógicos constituyen un álgebra booleana.

En consecuencia, todos los términos usados con álgebras booleanas, como complementos, literales, productos fundamentales, minterms, suma de productos y suma de productos completa, también pueden usarse con los circuitos lógicos.

Circuitos AND-OR

El circuito lógico L, que corresponde a una expresión booleana de suma de productos, se denomina circuito AND-OR. Un circuito L así tiene varias entradas, donde:

1) Algunas entradas o sus complementos se introducen en cada compuerta AND.
2) Las salidas de todas las compuertas AND se introducen en una sola compuerta OR.
3) La salida de la compuerta OR es la salida del circuito L.

A continuación se ilustra este tipo de circuito lógico.

EJEMPLO 15.10: La figura 15-12 es un circuito típico AND-OR con tres entradas *A*, *B*, *C* y una salida *Y*. Resulta fácil escribir Y como una expresión booleana en las entradas *A*, *B*, *C* como sigue: primero se encuentra la salida de cada compuerta AND:

a) Las entradas de la primera compuerta AND son *A*, *B*, *C*, de modo que la salida es $A \cdot B \cdot C$.

b) Las entradas de la segunda compuerta AND son *A*, B', *C*, de modo que la salida es $A \cdot B' \cdot C$.

c) Las entradas de la tercera compuerta AND son A' y *B*, de modo que la salida es $A' \cdot B$.

Así, la suma de las salidas de las compuertas AND es la salida de la compuerta OR, que es la salida *Y* del circuito. Por tanto,

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

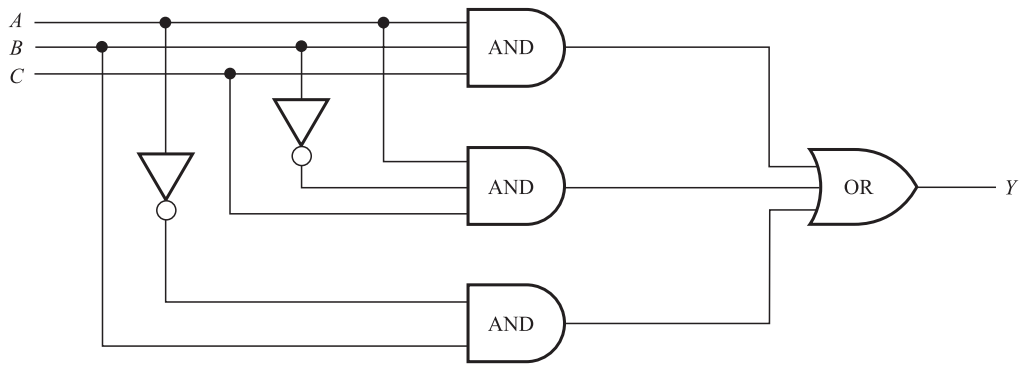


Figura 15-12

Compuertas NAND y NOR

Hay dos compuertas adicionales que son equivalentes a combinaciones de las compuertas básicas recién descritas.

a) Una compuerta NAND, representada en la figura 15-13*a*), es equivalente a una compuerta AND seguida por una compuerta NOT.

b) Una compuerta NOR, representada en la figura 15-13*b*), es equivalente a una compuerta OR seguida por una compuerta NOT.

Las tablas de verdad de estas compuertas (con dos entradas *A* y *B*) se muestran en la figura 15-13*c*). Las compuertas NAND y NOR en realidad pueden tener dos o más entradas, así como las compuertas correspondientes AND y OR. Además, la salida de una compuerta NAND es 0 si y solo si todas las entradas son 1, y la salida de una compuerta NOR es 1 si y solo si todas las entradas son 0.

a) Compuerta NAND

b) Compuerta NOR

A	*B*	NAND	NOR
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

c)

Figura 15-13

Observe que la única diferencia entre las compuertas AND y NAND y entre las compuertas OR y NOR es que las compuertas NAND y NOR están seguidas cada una por un círculo. En algunos textos también se usa un círculo pequeño para indicar un complemento antes de una compuerta. Por ejemplo, las expresiones booleanas correspondientes a dos circuitos lógicos en la figura 15-14 son como sigue:

$$a) \quad Y = (A'B)', \quad b) \quad Y = (A' + B' + C)'$$

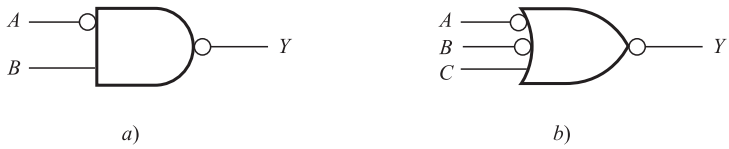


Figura 15-14

15.11 TABLAS DE VERDAD, FUNCIONES BOOLEANAS

Considere el circuito lógico L con $n = 3$ dispositivos de entrada A, B, C y salida Y, por ejemplo

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

Cada asignación de un conjunto de tres bits a las entradas A, B, C produce un bit de salida para Y. En total, hay $2^n = 2^3 = 8$ formas posibles de asignar los bits a las entradas como sigue:

$$000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111$$

La hipótesis es que la secuencia de los primeros bits se asigna a A, la secuencia de los segundos bits se asigna a B y la secuencia de los terceros bits se asigna a C. Por tanto, el conjunto anterior de entradas puede volver a escribirse en la forma

$$A = 00001111, \quad B = 00110011, \quad C = 01010101$$

Se recalca que estas tres secuencias de $2^n = 8$ bits contienen las ocho combinaciones posibles de los bits de entrada.

La *tabla de verdad* $T = T(L)$ del circuito L anterior consta de la secuencia de salida Y que corresponde a las secuencias de entrada A, B, C. Esta tabla de verdad T se expresa mediante notación fraccionaria o relacional; es decir, T puede escribirse en la forma

$$T(A, B, C) = Y \quad \text{o} \quad T(L) = [A, B, C; Y]$$

Esta forma para la tabla de verdad de L es esencialmente la misma que la tabla de verdad de una proposición analizada en la sección 4.4. La única diferencia es que aquí los valores para A, B, C y Y se escriben horizontalmente, mientras que en la sección 4.4 se escriben verticalmente.

Considere un circuito lógico L con n dispositivos de entrada. Hay muchas maneras para formar n secuencias de entrada $A_1, A_2, \ldots, A_n$ de modo que contengan las 2^n combinaciones posibles de los bits de entrada. (Observe que cada secuencia debe contener 2^n bits.) Un esquema de asignación es el siguiente:

A_1: Asignar 2^{n-1} bits que son ceros seguidos por 2^{n-1} bits que son unos.

A_2: Asignar repetidamente 2^{n-2} bits que son ceros seguidos por 2^{n-2} bits que son unos.

A_3: Asignar 2^{n-3} bits que son ceros seguidos por 2^{n-3} bits que son unos.

Y así sucesivamente. Las secuencias obtenidas de esta manera se denominan *secuencias especiales*. Al sustituir 0 por 1 y 1 por 0 en las secuencias especiales se obtienen los complementos de las secuencias especiales.

Observación: En el supuesto de que en la entrada están las secuencias especiales, a menudo no es necesario distinguir entre la tabla de verdad

$$T(L) = [A_1, A_2, \ldots, A_n; Y]$$

y la salida Y en sí.

EJEMPLO 15.11

a) Suponga que un circuito lógico L tiene $n = 4$ dispositivos de entrada A, B, C, D. Las $2^n = 2^4 =$ secuencias especiales de 16 bits A, B, C, D son las siguientes:

$$A = 0000000011111111, \quad C = 0011001100110011$$
$$B = 0000111100001111, \quad D = 0101010101010101$$

Es decir:

1) A empieza con ocho ceros seguidos por ocho unos. (Aquí $2^{n-1} = 2^3 = 8$.)

2) B empieza con cuatro ceros seguidos por cuatro unos y así continúa. (Aquí $2^{n-2} = 2^2 = 4$.)

3) C empieza con dos ceros seguidos por dos unos y así en lo sucesivo. (Aquí $2^{n-3} = 2^1 = 2$.)

4) D empieza con un cero seguido por un uno y así en lo sucesivo. (Aquí $2^{n-4} = 2^0 = 1$.)

b) Suponga que un circuito lógico L tiene $n = 3$ dispositivos de entrada A, B, C. Las $2^n = 2^3 =$ secuencias especiales de 8 bits para A, B, C y sus complementos A', B', C' son las siguientes:

$$A = 00001111, \quad B = 00110011, \quad C = 01010101$$
$$A' = 11110000, \quad B' = 11001100, \quad C' = 10101010$$

La figura 15-15 contiene un algoritmo de tres pasos para encontrar la tabla de verdad de un circuito lógico L donde la salida Y está dada por una expresión booleana de suma de productos en las entradas.

Algoritmo 15.5: La entrada es una expresión booleana de suma de productos $Y = Y(A_1, A_2, \ldots)$.

Paso 1. Se escriben las secuencias especiales para las entradas $A_1, A_2, \ldots$ y sus complementos.

Paso 2. Se encuentra cada producto que aparece en Y. (Recuerde que un producto $X_1 \cdot X_2, \cdots = 1$ está en una posición si y sólo si todas las $X_1, X_2, \ldots$ tienen 1 en la posición.)

Paso 3. Se encuentra la suma Y de los productos. (Recuerde que una suma $X_1 + X_2 + \cdots = 0$ está en una posición si y sólo si todas las $X_1, X_2, \ldots$ tienen 0 en la posición.)

Figura 15-15

EJEMPLO 15.12 El algoritmo 15.5 se usa para encontrar la tabla de verdad $T = T(L)$ del circuito lógico L en la figura 15-12 o, en forma equivalente, de la expresión booleana de suma de productos anterior

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

1) Las secuencias especiales y sus complementos aparecen en el ejemplo 15.14*b*).

2) Los productos son los siguientes:

$$A \cdot B \cdot C = 00000001, \quad A \cdot B' \cdot C = 00000100, \quad A' \cdot B = 00110000$$

3) La suma es $Y = 00110101$.

En consecuencia,

$$T\,(00001111, 00110011, 01010101) = 00110101$$

o simplemente $T(L) = 00110101$, donde se supone que la entrada consta de las secuencias especiales.

Funciones booleanas

Sea E una expresión booleana con n variables $x_1, x_2, \ldots, x_n$. Todo el análisis anterior también puede aplicarse a E, donde ahora las secuencias especiales se asignan a las variables $x_1, x_2, \ldots, x_n$ en vez de a los dispositivos de entrada $A_1, A_2, \ldots, A_n$. La tabla de verdad $T = T(E)$ de E se define de la misma forma que la tabla de verdad $T = T(L)$ para un circuito lógico L. Por ejemplo, la expresión booleana

$$E = xyz + xy'z + x'y$$

que es semejante al circuito lógico L en el ejemplo 15.12 produce la tabla de verdad

$$T\,(00001111, 00110011, 01010101) = 00110101$$

o simplemente $T(E) = 00110101$, donde se supone que la entrada consta de las secuencias especiales.

Observación: La tabla de verdad de una expresión booleana $E = E(x_1, x_2, \ldots, x_n)$ con n variables también puede considerarse como una función "booleana" de $\mathbf{B}^n$ en $\mathbf{B}$. (Las álgebras booleanas $\mathbf{B}^n$ y $\mathbf{B} = \{0, 1\}$ se definen en el ejemplo 15.1.) Es decir, cada elemento en $\mathbf{B}^n$ es una lista de n bits que al ser asignada a la lista de variables en E produce un elemento en $\mathbf{B}$. La tabla de verdad $T(E)$ de E es simplemente la gráfica de la función.

EJEMPLO 15.13

a) Considere las expresiones booleanas $E = E(x, y, z)$ con tres variables. Los ocho minterms (productos fundamentales que implican a las tres variables) son los siguientes:

$$xyz, \quad xyz', \quad xy'z, \quad x'yz, \quad xy'z', \quad x'yz', \quad x'y'z'$$

Las tablas de verdad de estos minterms (con las secuencias especiales para x, y, z) son las siguientes:

$$xyz = 00000001, \quad xyz' = 00000010, \quad xy'z = 00000100, \quad x'yz = 00001000$$
$$xy'z' = 00010000, \quad x'yz' = 00100000, \quad x'y'z = 01000000, \quad x'y'z' = 10000000$$

Observe que cada minterm tiene el valor 1 en sólo una de las ocho posiciones.

b) Considere la expresión booleana $E = xyz' + x'yz + x'y'z$. Observe que E es una expresión completa de suma de productos que contiene tres minterms. En consecuencia, la tabla de verdad $T = T(E)$ de E, con las secuencias especiales para x, y, z puede obtenerse fácilmente a partir de las secuencias del inciso *a*). En específico, la tabla de verdad $T(E)$ contiene exactamente tres unos en las mismas posiciones que los unos en los tres minterms en E. Así,

$$T\,(00001111, 00110011, 01010101) = 01001010$$

o simplemente $T(E) = 01001010$.

15.12 MAPAS DE KARNAUGH

Los mapas de Karnaugh, donde los minterms que implican las mismas variables se representan con cuadrados, son dispositivos gráficos que se usan para encontrar implicantes primos y formas minimales para expresiones booleanas con un máximo de seis variables. Aquí sólo se abordan los casos de dos, tres y cuatro variables. En el contexto de los mapas de Karnaugh, algunas veces los términos "cuadrado" y "minterm" se usan como sinónimos. Recuerde que un minterm es un producto fundamental que implica a todas las variables, y que una expresión completa de suma de productos es una suma de minterms.

Primero es necesario definir el concepto de productos adyacentes. Se dice que dos productos fundamentales P_1 y P_2 son *adyacentes* si P_1 y P_2 tienen las mismas variables y si difieren exactamente en una literal. Por tanto, debe haber una variable no complementada en un producto y una variable complementada en el otro. En particular, la suma de estos dos productos adyacentes es un producto fundamental con una literal menos.

EJEMPLO 15.14 Encuentre la suma de productos adyacentes P_1 y P_2 donde:

a) $P = xyz'$ y $P_2 = xy'z'$.

$$P_1 + P_2 = xyz' + xy'z' = xz'(y + y') = xz'(1) = xz'$$

b) $P_1 = x'yzt$ y $P_2 = x'yz't$.

$$P_1 + P_2 = x'yzt + x'yz't = x'yt(z + z') = x'yt(1) = x'yt$$

c) $P_1 = x'yzt$ y $P_2 = xyz't$.

Aquí P_1 y P_2 no son adyacentes, puesto que difieren en dos literales. En particular,

$$P_1 + P_2 = x'yzt + xyz't = (x' + x)y(z + z')t = (1)y(1)t = yt$$

d) $P_1 = xyz'$ y $P_2 = xyzt$.

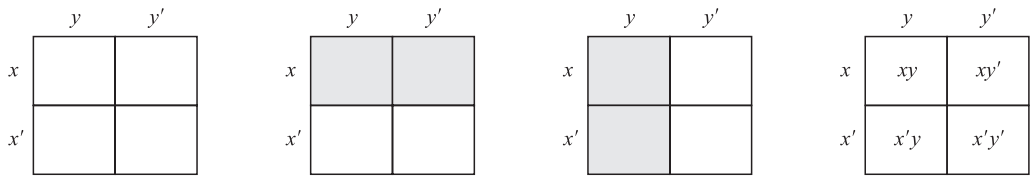
Aquí P_1 y P_2 no son adyacentes, puesto que tienen variables diferentes. Así, en particular, no aparecen como cuadrados en el mismo mapa de Karnaugh.

Caso de dos variables

El mapa de Karnaugh correspondiente a las expresiones booleanas $E = E(x, y)$ con dos variables x y y aparece en la figura 15-16*a*). El mapa de Karnaugh puede considerarse como un diagrama de Venn donde los puntos en la parte superior del mapa representan a x, sombreado en la figura 15-16*b*), y los puntos en la parte izquierda del mapa representan a y, sombreado en la figura 15-16*c*). Así, x' se representa con los puntos en la parte inferior del mapa, y y' con los puntos en la parte derecha del mapa. En consecuencia, los cuatro minterms posibles con dos literales

$$xy, \quad xy', \quad x'y, \quad x'y'$$

están representados por los cuatro cuadrados del mapa, como se observa en la figura 15-16*d*). Observe que dos de estos cuadrados son adyacentes, como se acaba de definir, si y solo si los cuadrados son geométricamente adyacentes (tienen un lado en común).



a) *b*) Sombreado x *c*) Sombreado y *d*)

Figura 15-16

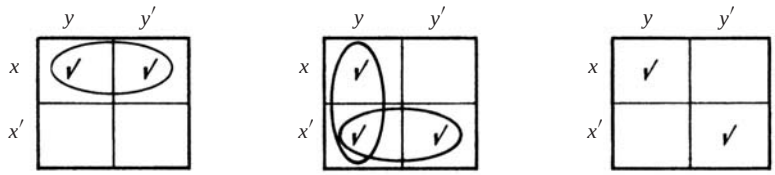
Cualquier expresión booleana completa de suma de productos $E(x, y)$ es una suma de minterms y, por tanto, se representa en el mapa de Karnaugh mediante la colocación de controles en los cuadrados apropiados. Un implicante primo de $E(x, y)$ es un par de cuadrados adyacentes en E o un *cuadrado aislado*; es decir, un cuadrado que no es adyacente a ningún otro cuadrado de $E(x, y)$. Una forma de suma de productos minimal para $E(x, y)$ consiste de un número mínimo de implicantes primos que cubren a todos los cuadrados de $E(x, y)$, como se ilustra en el siguiente ejemplo.

EJEMPLO 15.15 Encuentre los implicantes primos y una forma de suma de productos minimal para cada una de las siguientes expresiones booleanas completas de suma de productos:

$$a) \quad E_1 = xy + xy'; \quad b) \quad E_2 = xy + x'y + x'y'; \quad c) \quad E_3 = xy + x'y'$$

Esto puede resolverse mediante mapas de Karnaugh como sigue:

a) Se comprueban los cuadrados correspondientes a xy y xy' como se muestra en la figura 15-17*a*). Observe que E_1 consiste de un implicante primo, los dos cuadrados adyacentes designados por el "óvalo" en la figura 15-17*a*). Este par de cuadrados adyacentes representa la variable x, de modo que x es el único implicante primo de E_1. En consecuencia, $E_1 = x$ es una suma minimal.



a) E_1 *b*) E_2 *c*) E_3

Figura 15-17

b) Se comprueban los cuadrados correspondientes a xy, $x'y$ y $x'y'$ como se muestra en la figura 15-17*b*). Observe que E_2 contiene dos pares de cuadrados adyacentes (designados por los dos óvalos) que incluyen a todos los cuadrados de E_2. El par vertical representa a y y el par horizontal representa a x'; por tanto, y y x' son los implicantes primos de E_2. Así, $E_2 = x' + y$ es su suma minimal.

c) Se comprueban los cuadrados correspondientes a xy y $x'y'$ como se muestra en la figura 15-17*c*). Observe que E_2 consiste de dos cuadrados aislados que representan a xy y $x'y'$; por tanto, xy y $x'y'$ son los implicantes primos de E_3 y $E_3 = xy + x'y'$ es su suma minimal.

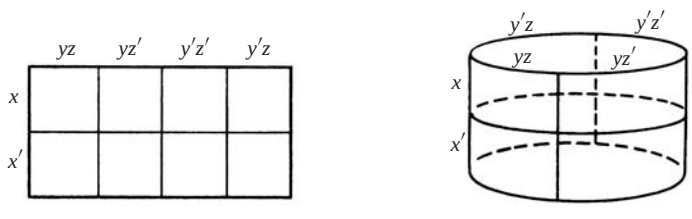
Caso de tres variables

El mapa de Karnaugh correspondiente a las expresiones booleanas $E = E(x, y, z)$ con tres variables x, y, z se muestra en la figura 15-18*a*). Recuerde que hay exactamente ocho minterms con tres variables:

$$xyz, \quad xyz', \quad xy'z', \quad xy'z, \quad x'yz, \quad x'yz', \quad x'y'z', \quad x'y'z$$

Estos minterms se enumeran de modo que correspondan a los ocho cuadrados en el mapa de Karnaugh.

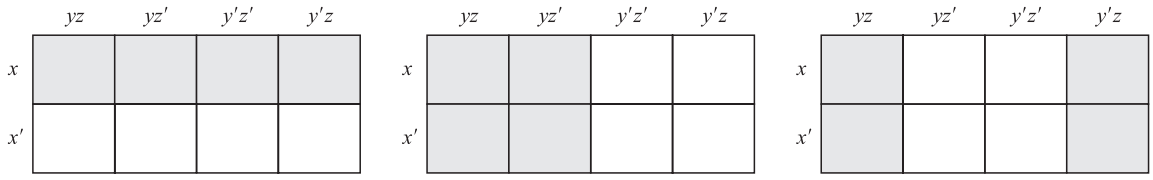
Además, para que cada par de productos adyacentes en la figura 15-18*a*) sea geométricamente adyacente, es necesario identificar los bordes derecho e izquierdo del mapa. Esto equivale a cortar, doblar y pegar el mapa a lo largo de los bordes, o aristas, identificados para obtener el cilindro que aparece en la figura 15-18*b*), donde ahora los productos adyacentes se representan por cuadrados que tienen un borde en común.



a) *b*)

Figura 15-18

Al considerar el mapa de Karnaugh en la figura 15-18*a*) como un diagrama de Venn, las áreas representadas por las variables x, y, z se muestran en la figura 15-19. En específico, la variable x sigue representada por los puntos en la mitad superior del mapa, según el sombreado en la figura 15-19*a*), y la variable y sigue representada por los puntos en la mitad izquierda del mapa, según el sombreado en la figura 15-19*b*). La nueva variable z se representa con los puntos



a) Sombreado *x* *b*) Sombreado *y* *c*) Sombreado *z*

Figura 15-19

en los cuadrantes izquierdo y derecho del mapa, según el sombreado en la figura 15-19*c*). Por tanto, x', y' y z' están representados, respectivamente, por puntos en la mitad inferior, en la mitad derecha y en los dos cuadrantes centrales del mapa.

Por un *rectángulo básico* en el mapa de Karnaugh con tres variables se entiende un cuadrado, dos cuadrados adyacentes o cuatro cuadrados que forman un rectángulo de uno por cuatro o de dos por dos. Estos rectángulos básicos corresponden a productos fundamentales de tres, dos y una literal, respectivamente. Además, el producto fundamental representado por un rectángulo básico es el producto de justo aquellas literales que aparecen en cada cuadrado del rectángulo.

Suponga que una expresión booleana completa de suma de productos $E = E(x, y, z)$ está representada en el mapa de Karnaugh al colocar verificaciones en los cuadrados apropiados. Un implicante primo de E es un *rectángulo básico maximal de E*; es decir, un rectángulo básico contenido en E que no está contenido en ningún rectángulo básico más grande en E. Una forma de suma de productos minimal para E consiste de una *cubierta minimal* de E; es decir, un número minimal de rectángulos básicos maximales de E que juntos incluyen a todos los cuadrados de E.

EJEMPLO 15.16 Encuentre los implicantes primos y la forma de suma de productos minimal para cada una de las siguientes expresiones booleanas completas de suma de productos:

a) $E_1 = xyz + xyz' + x'yz' + x'y'z$.

b) $E_2 = xyz + xyz' + xy'z + x'yz + x'y'z$.

c) $E_3 = xyz + xyz' + x'yz' + x'y'z' + x'y'z$.

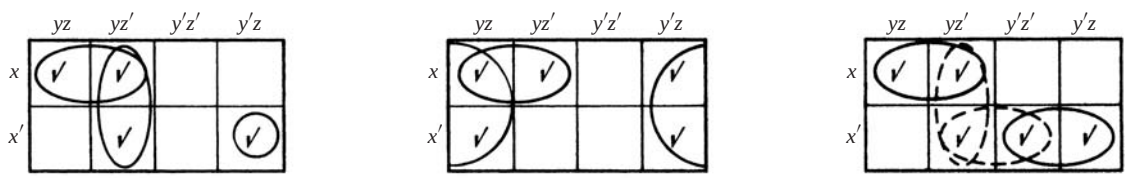
Esto puede resolverse mediante el mapa de Karnaugh:

a) Se comprueban los cuadrados correspondientes a los cuatro sumandos como en la figura 15-20*a*). Observe que E_1 tiene tres implicantes primos (rectángulos básicos maximales), encerrados en un círculo; se trata de xy, yz' y $x'y'z$. Todos se requieren para cubrir a E_1; por tanto, la suma minimal para E_1 es

$$E_1 = xy + yz' + x'y'z$$

b) Se comprueban los cuadrados correspondientes a los cinco sumandos como en la figura 15-20*b*). Observe que E_2 tiene dos implicantes primos encerrados en un círculo. Uno es los dos cuadrados adyacentes que representan xy, y el otro es el cuadrado de dos por dos (que genera los bordes identificados) que representa a z. Ambos se requieren para cubrir a E_2; por tanto, la suma minimal para E_2 es

$$E_2 = xy + z$$



a) E_1 *b*) E_2 *c*) E_3

Figura 15-20

c) Se comprueban los cuadrados correspondientes a los cinco sumandos como en la figura 15-20*c*). Como se indica con los óvalos, E_3 tiene tres implicantes primos xy, yz', $x'z'$ y $x'y'$. Sin embargo, sólo uno de los dos sombreados; es decir, uno de yz' o $x'z'$ es necesario en una cubierta minimal de E_3. Por tanto, E_3 tiene dos sumas minimales:

$$E_3 = xy + yz' + x'y' = xy + x'z' + x'y'$$

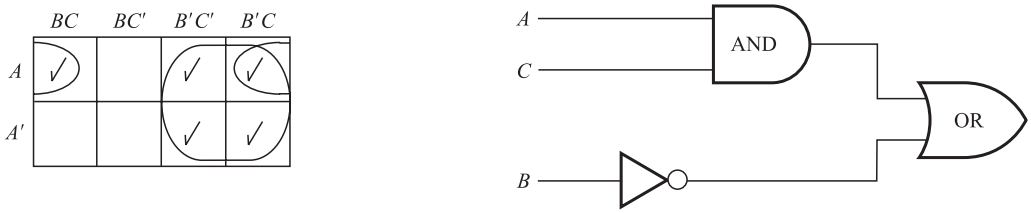
EJEMPLO 15.17 Diseñe un circuito L AND-OR minimal de tres entradas con la siguiente tabla de verdad:

$$T = [A, B, C; L] = [00001111, 00110011, 01010101; 11001101]$$

A partir de la tabla de verdad puede leerse la forma de suma de productos completa para L (como en el ejemplo 15.10):

$$L = A'B'C' + A'B'C + AB'C' + AB'C + ABC$$

El mapa de Karnaugh asociado se muestra en la figura 15-21*a*). Observe que L tiene dos implicantes primos, B' y AC, en su cubierta minimal; por tanto, $L = B' + AC$ es una suma minimal para L. En la figura 15-21*b*) se proporciona el circuito minimal correspondiente AND-OR para L.



a) *b*)

Figura 15-21

Caso de cuatro variables

El mapa de Karnaugh correspondiente a las expresiones booleanas $E = E(x, y, z, t)$ con cuatro variables x, y, z, t se muestra en la figura 15-22. Cada uno de los 16 cuadrados corresponde a uno de los 16 minterms con cuatro variables.

$$xyzt, \quad xyzt', \quad xyz't', \quad xyz't, \quad \ldots, x'yz't$$

como se indica por las identificaciones del renglón y la columna del cuadrado. Observe que la línea superior y el lado izquierdo están identificados de modo que los productos adyacentes difieren precisamente en una literal. De nuevo, es necesario identificar el borde izquierdo con el borde derecho (como se hizo con tres variables), aunque también es necesario identificar el borde superior con el borde inferior. (Estas identificaciones originan una superficie en forma de dona denominada *toro*, y el mapa puede considerarse como si realmente fuese un toro.)

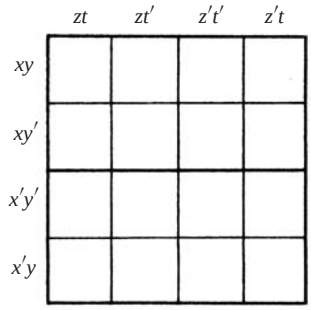


Figura 15-22

Un *rectángulo básico* en un mapa de Karnaugh de cuatro variables es un cuadrado, dos cuadrados adyacentes, cuatro cuadrados que forman un rectángulo de uno por cuatro o de dos por dos, u ocho cuadrados que forman un rectángulo de dos por cuatro. Estos rectángulos corresponden a productos fundamentales con cuatro, tres, dos y una literal, respectivamente. De nuevo, los rectángulos básicos maximales son los implicantes primos. La técnica de minimización para una expresión booleana $E(x, y, z, t)$ es la misma que antes.

EJEMPLO 15.18 Encuentre el producto fundamental P representado por el rectángulo básico en los mapas de Karnaugh que se muestran en la figura15-23.

En cada caso encuentre las literales que aparecen en todos los cuadrados del rectángulo básico; P es el producto de esas literales.

a) xy y z' aparecen en ambos cuadrados; por tanto, $P = xy'z'$.

b) Sólo y y z aparecen en los cuatro cuadrados; por tanto, $P = yz$.

c) Sólo t aparece en los ocho cuadrados; por tanto, $P = t$.

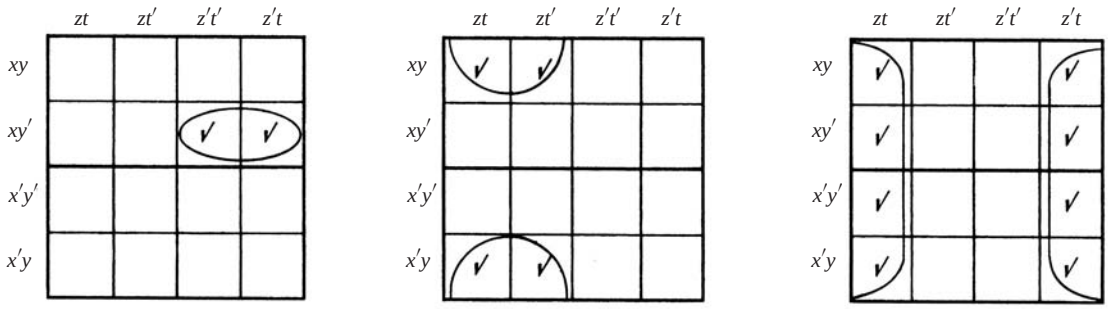


Figura 15-23

EJEMPLO 15.19 Use un mapa de Karnaugh para encontrar una forma de suma de productos minimal para

$$E = xy' + xyz + x'y'z' + x'yzt'$$

Se comprueban todos los cuadrados que representan a cada producto fundamental. Es decir, se comprueban los cuatro cuadrados que representan a xy', los dos cuadrados que representan a xyz, los dos cuadrados que representan a $x'y'z'$ y al cuadrado que representa a $x'yzt'$ como en la figura 15-24. Una cubierta minimal del mapa consiste de los tres rectángulos básicos maximales designados.

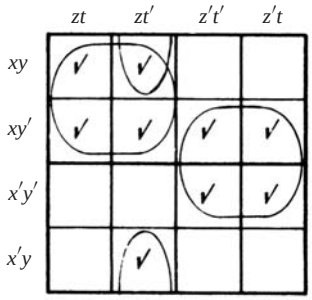


Figura 15-24

Los cuadrados de dos por dos representan los productos fundamentales xz y $y'z'$, y los dos cuadrados adyacentes (en las partes superior e inferior) representan a yzt'. Por tanto,

$$E = xz + y'z' + yzt'$$

es una suma minimal para E.

PROBLEMAS RESUELTOS

ÁLGEBRAS BOOLEANAS

15.1 Escriba el dual de cada ecuación booleana: *a*) $(a * 1) * (0 + a') = 0$; *b*) $a + a'b = a + b$.

a) Para obtener la ecuación dual, se intercambian $+$ y $*$ y se intercambian 0 y 1. Así,

$$(a + 0) + (1 * a') = 1$$

b) Primero se escribe la ecuación con $*$ para obtener $a + (a' * b) = a + b$. Luego, el dual es $a * (a' + b) = a * b$, que puede escribirse como

$$a(a' + b) = ab$$

15.2 Recuerde (capítulo 14) que el conjunto $\mathbf{D}_m$ de divisores de m es un retículo acotado distributivo con

$$a + b = a \vee b = \text{mcm}(a, b) \quad \text{y} \quad a * b = a \wedge b = \text{mcd}(a, b).$$

a) Demuestre que $\mathbf{D}_m$ es un álgebra booleana si m está libre de cuadrados; es decir, si m es un producto de primos distintos.
b) Encuentre los átomos de $\mathbf{D}_m$.

a) Sólo es necesario demostrar que $\mathbf{D}_m$ está complementado. Sea x en $\mathbf{D}_m$ y sea $x' = m/x$. Puesto que m es un producto de primos distintos, x y x' tienen divisores primos distintos. Por tanto, $x * x' = \text{mcd}(x, x') = 1$ y $x + x' = \text{mcm}(x, x') = m$. Recuerde que 1 es el elemento cero (cota inferior) de $\mathbf{D}_m$ y que m es el elemento identidad (cota superior) de $\mathbf{D}_m$. Por tanto, x' es un complemento de x, por lo que $\mathbf{D}_m$ es un álgebra booleana.

b) Los átomos de $\mathbf{D}_m$ son los divisores primos de m.

15.3 Considere el álgebra booleana $\mathbf{D}_{210}$.

a) Escriba sus elementos y trace su diagrama.
b) Encuentre el conjunto A de átomos.
c) Encuentre dos subálgebras con ocho elementos.
d) ¿$X = \{1, 2, 6, 210\}$ es un subretículo de $\mathbf{D}_{210}$? ¿Una subálgebra?
e) ¿$Y = \{1, 2, 3, 6\}$ es un subretículo de $\mathbf{D}_{210}$? ¿Una subálgebra?

a) Los divisores de 210 son 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 y 210. El diagrama de $\mathbf{D}_{210}$ se muestra en la figura 15-25.

b) $A = \{2, 3, 5, 7\}$, el conjunto de divisores primos de 210.

c) $B = \{1, 2, 3, 35, 6, 70, 105, 210\}$ y $C = \{1, 5, 6, 7, 30, 35, 42, 210\}$ son subálgebras de $\mathbf{D}_{210}$.

d) X es un subretículo puesto que está linealmente ordenado. Sin embargo, X no es una subálgebra puesto que 35 es el complemento de 2 en $\mathbf{D}_{210}$ pero 35 no pertenece a X. (De hecho, un álgebra booleana con más de dos elementos está linealmente ordenada.)

e) Y es un subretículo de $\mathbf{D}_{210}$ puesto que está cerrado bajo $+$ y $*$. Sin embargo, Y no es una subálgebra de $\mathbf{D}_{210}$ puesto que no es cerrada bajo complementos de $\mathbf{D}_{210}$; por ejemplo, $35 = 2'$ no pertenece a Y. (Se observa que Y en sí es un álgebra booleana; de hecho, $Y = \mathbf{D}_6$).

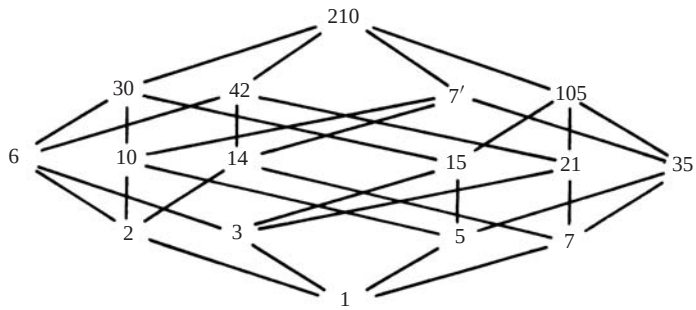


Figura 15-25

15.4 Encuentre el número de subálgebras de $\mathbf{D}_{210}$.

Una subálgebra de $\mathbf{D}_{210}$ debe contener dos, cuatro, ocho o dieciséis elementos.

i) Sólo puede haber una subálgebra con dos elementos que consiste de la cota superior 210 y la cota inferior 1; es decir, $\{1, 210\}$.

ii) Puesto que $\mathbf{D}_{210}$ contiene dieciséis elementos, la única subálgebra con dieciséis elementos es $\mathbf{D}_{210}$ mismo.

iii) Cualquier subálgebra con cuatro elementos es de la forma $\{1, x, x', 210\}$; es decir, consiste de las cotas superior e inferior y de un elemento no acotado y su complemento. En $\mathbf{D}_{210}$ hay catorce elementos no acotados, de modo que hay $14/2 = 7$ pares $\{x, x'\}$. Por tanto, $\mathbf{D}_{210}$ tiene siete subálgebras de cuatro elementos.

iv) Cualquier subálgebra S de ocho elementos contiene de suyo tres átomos s_1, s_2, s_3. Es posible escoger s_1 y s_2 como cualquiera de los cuatro átomos de $\mathbf{D}_{210}$ y luego s_3 debe ser el producto de los otros dos átomos; por ejemplo, puede hacerse $s_1 = 2$, $s_2 = 3$, $s_3 = 5 \cdot 7 = 35$ (lo cual determina la subálgebra B anterior), o puede hacerse $s_1 = 5$, $s_2 = 7$, $s_3 = 2 \cdot 3 = 6$ (que determina la subálgebra C anterior). Hay $\binom{4}{2} = 6$ formas de escoger s_1 y s_2 de los cuatro átomos de $\mathbf{D}_{210}$ y así $\mathbf{D}_{210}$ tiene seis subálgebras de ocho elementos.

En consecuencia, $\mathbf{D}_{210}$ tiene $1 + 1 + 7 + 6 = 15$ subálgebras.

15.5 Demuestre el teorema 15.2: sean a, b, c elementos arbitrarios en un álgebra booleana B.

i) Leyes de idempotencia:

5*a*) $a + a = a$ 5*b*) $a * a = a$

ii) Leyes de acotamiento:

6*a*) $a + 1 = 1$ 6*b*) $a * 0 = 0$

iii) Leyes de absorción:

7*a*) $a + (a * b) = a$ 7*b*) $a * (a + b) = a$

iv) Leyes asociativas:

8*a*) $(a + b) + c = a + (b + c)$ 8*b*) $(a * b) * c = a * (b * c)$

5*b*) $a = a * 1 = a * (a + a') = (a * a) + (a * a') = (a * a) + 0 = a * a$

5*a*) Se concluye del inciso 5*b*) y la dualidad.

6*b*) $a * 0 = (a * 0) + 0 = (a * 0) + (a * a) = a * (0 + a') = a * (a' + 0) = a * a' = 0$

6*a*) Se concluye del inciso 6*b*) y la dualidad.

7*b*) $a * (a + b) = (a + 0) * (a + b) = a + (0 * b) = a + (b * 0) = a + 0 = a$

7*a*) Se concluye del inciso 7*b*) y la dualidad.

8*b*) Sean $L = (a * b) * c$ y $R = a * (b * c)$. Es necesario demostrar que $L = R$. Primero se demuestra que $a + L = a + R$. Al usar los dos últimos pasos de las leyes de absorción,

$$a + L = a + ((a * b) * c) = (a + (a * b)) * (a + c) = a * (a + c) = a$$

También, al usar el último paso de la ley de absorción,

$$a + R = a + (a * (b * c)) = (a + a) * (a + (b * c)) = a * (a + (b * c)) = a$$

Por tanto, $a + L = a + R$. A continuación se demuestra que $a' + L = a' + R$. Se tiene

$$\begin{aligned} a' + L = a' + ((a * b) * c) &= (a' + (a * b)) * (a' + c) \\ &= ((a' + a) * (a' + b)) * (a' + c) = (1 * (a' + b)) * (a' + c) \\ &= (a' + b) * (a' + c) = a' + (b * c) \end{aligned}$$

También,

$$\begin{aligned} a' + R = a' + (a * (b * c)) &= (a' + a) * (a' + (b * c)) \\ &= 1 * (a' + (b * c)) = a' + (b * c) \end{aligned}$$

Por tanto, $a' + L = a' + R$. En consecuencia,

$$\begin{aligned} L = 0 + L = (a * a') + L &= (a + L) * (a' + L) = (a + R) * (a' + R) \\ = (a * a') + R &= 0 + R = R \end{aligned}$$

8*a*) Se concluye del inciso 8*b*) y la dualidad.

15.6 Demuestre el teorema 15.3: sea a cualquier elemento de un álgebra booleana B.

i) (Unicidad del complemento) Si $a + x = 1$ y $a * x = 0$, entonces $x = a'$.
ii) (Ley de involución) $(a')' = a$.
iii) 9*a*) $0' = 1$; 9*b*) $1' = 0$.

i) Se tiene:

$$a' = a' + 0 = a' + (a * x) = (a' + a) * (a' + x) = 1 * (a' + x) = a' + x$$

También,

$$x = x + 0 = x + (a * a') = (x + a) * (x + a') = 1 * (x + a') = x + a'$$

Por tanto, $x = x + a' = a' + x = a'$.

ii) Por definición de complemento, $a + a' = 1$ y $a * a' = 0$. Por conmutatividad, $a' + a = 1$ y $a' * a = 0$. Por unicidad del complemento, a es el complemento de a'; es decir, $a = (a')'$.

iii) Por la ley de acotamiento 6*a*); $0 + 1 = 1$, y por el axioma de identidad 3*b*), $0 * 1 = 0$. Por la unicidad del complemento, 1 es el complemento de 0; es decir, $1 = 0'$. Por dualidad, $0 = 1'$.

15.7 Demuestre el teorema 15.4: (leyes de DeMorgan): 10*a*) $(a + b)' = a' * b'$. 10*b*) $(a * b)' = a' + b'$.

10*a*) Es necesario demostrar que $(a + b) + (a * b') = 1$ y $(a + b) * (a' * b') = 0$; así, por unicidad del complemento, $a' * b' = (a + b')$. Se tiene:

$$\begin{aligned} (a + b) + (a' * b') = b + a + (a' * b') &= b + (a + a') * (a + b') \\ &= b + 1 * (a + b') = b + a + b' = b + b' + a = 1 + a = 1 \end{aligned}$$

También,

$$\begin{aligned} (a + b) * (a' * b') &= ((a + b) * a') * b' \\ &= ((a * a') + (b * a')) * b' = (0 + (b * a')) * b' \\ &= (b * a') * b' = (b * b') * a' = 0 * a' = 0 \end{aligned}$$

Por tanto, $a' * b' = (a + b)'$.

10*b*) Principio de dualidad (teorema 15.1).

15.8 Demuestre el teorema 15.5: las siguientes expresiones son equivalentes en un álgebra booleana:

1) $a + b = b$; *2*) $a * b = a$; *3*) $a' + b = 1$; *4*) $a * b' = 0$.

Por el teorema 14.4, *1*) y *2*) son equivalentes. Se demuestra que *1*) y *3*) son equivalentes. Suponga que *1*) se cumple. Entonces

$$a' + b = a' + (a + b) = (a' + a) + b = 1 + b = 1$$

Ahora suponga que *3*) se cumple. Entonces

$$a + b = 1 * (a + b) = (a' + b) * (a + b) = (a' * a) + b = 0 + b = b$$

Por tanto, *1*) y *3*) son equivalentes.

A continuación se demuestra que *3*) y *4*) son equivalentes. Suponga que *3*) se cumple. Entonces por las leyes de De Morgan y la ley de involución,

$$0 = 1' = (a' + b')' = a'' * b' = a * b'$$

A la inversa, si *4*) se cumple, entonces

$$1 = 0' = (a * b')' = a' + b'' = a' + b$$

Por tanto, *3*) y *4*) son equivalentes. En consecuencia, las cuatro expresiones son equivalentes.

15.9 Demuestre el teorema 15.6: la transformación $f: B \to P(A)$ es un isomorfismo donde B es un álgebra booleana, $P(A)$ es el conjunto potencia del conjunto A de átomos y

$$f(x) = \{a_1, a_2, \ldots, a_n\}$$

donde $x = a_1 + \cdots + a_n$ es la única representación de a como una suma de átomos.

Recuerde (capítulo 14) que si las a son átomos, entonces $a_i^2 = a_i$ pero $a_i a_j = 0$ para $a_i \neq a_j$. Suponga que x, y están en B y que

$$x = a_1 + \cdots + a_r + b_1 + \cdots + b_s$$
$$y = b_1 + \cdots + b_s + c_1 + \cdots + c_t$$

donde

$$A = \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t, d_1, \ldots, d_k\}$$

es el conjunto de átomos de B. Entonces

$$x + y = a_1 + \cdots + a_r + b_1 + \cdots + b_s + c_1 + \cdots + c_t$$
$$xy = b_1 + \cdots + b_s$$

Por tanto

$$\begin{aligned} f(x + y) &= \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cup \{b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= f(x) \cup f(y) \\ f(xy) &= \{b_1, \ldots, b_s\} \\ &= \{a_1, \ldots, a_r, b_1, \ldots, b_s\} \cap \{b_1, \ldots, b_s, c_1, \ldots, c_t\} \\ &= f(x) \cap f(y) \end{aligned}$$

Sea

$y = c_1 + \cdots + c_t + d_1 + \cdots + d_k$. Entonces $x + y = 1$ y $xy = 0$, y así $y = x'$

Por consiguiente

$$f(x') = \{c_1, \ldots, c_t, d_1, \ldots, d_k\} = \{a_1, \ldots, a_r, b_1, \ldots, b_s\}^c = (f(x))^c$$

Puesto que la representación es única, f es uno a uno y sobre. Por tanto, f es un isomorfismo de un álgebra booleana.

EXPRESIONES BOOLEANAS

15.10 Reduzca los siguientes productos booleanos a 0 o a un producto fundamental:

a) $xyx'z$; *b*) $xyzy$; *c*) $xyz'yx$; *d*) $xyz'yx'z'$

Use las leyes conmutativa $x * y = y * x$, de complemento $x * x' = 0$ y de idempotencia $x * x = x$:

a) $xyx'z = xx'yz = 0yz = 0$

b) $xyzy = xyyz = xyz$

c) $xyz'yx = xxyyz' = xyz'$

d) $xyz'yx'z' = xx'yyz'z' = 0yz' = 0$

15.11 Exprese cada expresión booleana $E(x, y, z)$ como una suma de productos y luego en su forma completa de suma de productos: *a*) $E = x(xy' + x'y + y'z)$; *b*) $E = z(x' + y) + y'$.

Primero se usa el algoritmo 15.1 para expresar E como una suma de productos, y luego se usa el algoritmo 15.2 para expresar E como una suma de productos completa.

a) Primero se tiene $E = xxy' + xx'y + xy'z = xy' + xy'z$. Luego

$$E = xy'(z + z') + xy'z = xy'z + xy'z' + xy'z = xy'z + xy'z'$$

b) Primero se tiene

$$E = z(x' + y) + y' = x'z + yz + y'$$

Luego

$$\begin{aligned} E = x'z + yz + y' &= x'z(y + y') + yz(x + x') + y'(x + x')(z + z') \\ &= x'yz + x'y'z + xyz + x'yz + xy'z + xy'z' + x'y'z + x'y'z' \\ &= xyz + xy'z + xy'z' + x'yz + x'y'z + x'y'z' \end{aligned}$$

15.12 Exprese $E(x, y, z) = (x' + y)' + x'y$ en su suma de productos completa.

Se tiene $E = (x' + y)' + x'y = xy' + x'y$, que sería la forma de suma de productos completa de E si E fuese una expresión booleana en x y y. No obstante, se ha especificado que E es una expresión booleana en las tres variables x, y, z. Entonces,

$$E = xy' + x'y = xy'(z + z') + x'y(z + z') = xy'z + xy'z' + x'yz + x'yz'$$

es la forma completa de suma de productos de E.

15.13 Escriba cada expresión booleana $E(x, y, z)$ como una suma de productos y luego en su forma completa de suma de productos: *a*) $E = y(x + yz)'$; *b*) $E = x(xy + y' + x'y)$.

a) $E = y(x'yz)') = yx'(y' + z') = yx'y' + x'yz = x'yz'$
que ya está en su forma completa de suma de productos.

b) Primero se tiene $E = xxy + xy' + xx'y = xy + xy'$. Luego

$$E = xy(z + z') + xy'(z + z') = xyz + xyz' + xy'z + xy'z'$$

15.14 Enuncie cada expresión de $E(A, B, C)$ de conjuntos A, B, C como una unión de intersecciones:

a) $E = (A \cup B)^c \cap (C^c \cup B)$; *b*) $E = (B \cap C)^c \cap (A^c \cap C)^c$

Se usa notación booleana: $'$ para el complemento, $+$ para la unión y $*$ (o yuxtaposición) para la intersección, y luego E se expresa como una suma de productos (unión de intersecciones).

a) $E = (A + B)'(C' + B) = A'B'(C' + B) = A'B'C' + A'B'B = A'B'C'$ o $E = A^c \cap B^c \cap C^c$

b) $E = (BC)'(A' + C)' = (B' + C')(AC^c) = AB'C' + AC'$ o $E = (A \cap B^c \cap C^c) \cap (A \cap C^c)$

15.15 Sea $E = xy' + xyz' + x'yz'$. Demuestre que *a*) $xz' + E = E$; *b*) $x + E \neq E$; *c*) $z' + E \neq E$.

Puesto que la forma completa de suma de productos es única, $A + E = E$, donde $A \neq 0$, si y solo si los sumandos en forma completa de suma de productos para A están entre los sumandos en forma completa de suma de productos para E. Así, primero se encuentra la forma completa de suma de productos para E:

$$E = xy'(z + z') + xyz' + x'yz' = xy'z + xy'z' + xyz' + x'yz'$$

a) Exprese xz' en forma completa de suma de productos:

$$xz' = xz'(y + y') = xyz' + xy'z'$$

Puesto que los sumandos de xz' están entre los de E, se tiene $xz' + E = E$.

b) Exprese x en forma completa de suma de productos:

$$x = x(y + y')(z + z') = xyz + xyz' + xy'z + xy'z'$$

El sumando xyz de x no es un sumando de E; por tanto, $x + E \neq E$.

c) Exprese z' en forma completa de suma de productos:

$$z' = z'(x + x')(y + y') = xyz' + xy'z' + x'yz' + x'y'z'$$

El sumando $x'y'z'$ de z' no es un sumando de E; por tanto, $z' + E \neq E$.

EXPRESIONES BOOLEANAS MINIMALES, IMPLICANTES PRIMOS

15.16 Para cualquier expresión booleana de suma de productos E, sean E_L el número de literales en E (contando la multiplicidad) y E_S el número de sumandos en E. Encuentre E_L y E_S para cada una de las siguientes expresiones:

a) $E = xy'z + x'z' + yz' + x$ *c*) $E = xyt' + x'y'zt + xz't$
b) $E = x'y'z + xyz + y + yz' + x'z$ *d*) $E = (xy' + z)' + xy'$

Simplemente se suma el número de literales y el número de sumandos a cada expresión:

a) $E_L = 3 + 2 + 2 + 1 = 8$, $E_S = 4$.
b) $E_L = 3 + 3 + 1 + 2 + 2 = 11$, $E_S = 5$.
c) $E_L = 3 + 4 + 3 = 10$, $E_S = 3$.
d) Debido a que E no está escrito como una suma de productos, E_L y E_S no están definidos.

15.17 Dado que E y F son sumas de productos booleanas equivalentes, se define:

a) E es más simple que F; *b*) E es minimal.

a) E es más simple que F si $E_L < F_L$ y $E_S < F_S$ o si $E_L \leq F_L$ y $E_S < F_S$.
b) E es minimal si no hay ninguna expresión equivalente de suma de productos más simple que E.

15.18 Encuentre el consenso Q de los productos fundamentales P_1 y P_2 donde:

a) $P_1 = xy'z'$, $P_2 = xyt$ *c*) $P_1 = xy'z'$, $P_2 = x'y'zt$
b) $P_1 = xyz't$, $P_2 = xzt$ *d*) $P_1 = xyz'$, $P_2 = xz't$

El consenso Q de P_1 y P_2 existe si hay exactamente una variable; por ejemplo x_k, que está complementada en una de P_1 y P_2 e incomplementada en la otra. Así, Q es el producto (sin repetición) de las literales en P_1 y P_2 después que se han eliminado x_k y x_k':

a) Se eliminan y' y y y luego se multiplican las literales P_1 y P_2 (sin repetición) para obtener $Q = xz't$.
b) La eliminación de z' y z lleva a $Q = xyt$.
c) No tienen consenso puesto que tanto x como z aparecen complementadas en uno de los productos e incomplementadas en el otro.
d) No tienen consenso puesto que ninguna variable aparece complementada en uno de los productos e incomplementada en el otro.

15.19 Demuestre el lema 15.10: suponga que Q es el consenso de P_1 y P_2. Entonces $P_1 + P_2 + Q = P_1 + P_2$.

Puesto que las literales se conmutan sin pérdida de generalidad, puede suponerse que

$$P_1 = a_1 a_2 \cdots a_r, t, \quad P_2 = b_1 b_2 \cdots b_s, t', \quad Q = a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s$$

Luego, $Q = Q(t + t') = Qt + Qt'$. Debido a que Qt contiene a P_1, $P_1 + Qt = P_1$; y porque Qt' contiene a P_2, $P_2 + Qt' = P_2$. Entonces

$$P_1 + P_2 + Q = P_1 + P_2 + Qt + Qt' = (P_1 + Qt) + (P_2 + Qt') = P_1 + P_2$$

15.20 Sea $E = xy' + xyz' + x'yz'$. Encuentre: *a*) Los implicantes primos de E; *b*) una suma minimal para E.

a) El algoritmo 15.3 (método del consenso) se aplica como sigue:

$$\begin{aligned} E &= xy' + xyz' + x'yz' + xz' && \text{(consenso de } xy' \text{ y } xyz') \\ &= xy' + x'yz' + xz' && (xyz' \text{ incluye a } xz') \\ &= xy' + x'yz' + xz' + yz' && \text{(consenso de } x'yz' \text{ y } xz') \\ &= xy' + xz' + yz' && (x'yz' \text{ incluye a } yz') \end{aligned}$$

Ningún paso en el método del consenso puede aplicarse ahora. Por tanto, xy', xz' y yz' son los implicantes primos de E.

b) El algoritmo 15.4 se aplica con cada implicante primo de E en forma completa de suma de productos para obtener:

$$\begin{aligned} xy' &= xy'(z + z') = xy'z + xy'z' \\ xz' &= xz'(y + y') = xyz' + xy'z' \\ yz' &= yz'(x + x') = xyz' + x'yz' \end{aligned}$$

Sólo los sumandos xyz' y $xy'z'$ de xz' aparecen entre los otros sumandos y entonces es posible eliminar xz' como superfluo. Así, $E = xy' + yz'$ es una suma minimal para E.

15.21 Sea $E = xy + y't + x'yz' + xy'zt'$. Encuentre: *a*) Los implicantes primos de E; *b*) una suma minimal para E.

a) El algoritmo 15.3 (método del consenso) se aplica como sigue:

$$\begin{aligned} E &= xy + y't + x'yz' + xy'zt' + xzt' && \text{(consenso de } xy \text{ y } xy'zt') \\ &= xy + y't + x'yz' + xzt' && (xy'zt' \text{ incluye a } xzt') \\ &= xy + y't + x'yz' + xzt' + yz' && \text{(consenso de } xy \text{ y } x'yz') \\ &= xy + y't + xzt' + yz' && (x'yz' \text{ incluye a } yz') \\ &= xy + y't + xzt' + yz' + xt && \text{(consenso de } xy \text{ y } y't) \\ &= xy + y't + xzt' + yz' + xt + xz && \text{(consenso de } xzt' \text{ y } xt) \\ &= xy + y't + yz' + xt + xz && (xzt' \text{ incluye a } xz) \\ &= xy + y't + yz' + xt + xz + z' && \text{(consenso de } y't \text{ y } yz') \end{aligned}$$

Ningún paso en el método del consenso puede aplicarse ahora. Por tanto, los implicantes primos de E son xy, $y't$, yz', xt, xz, y $z't$.

b) Se aplica el algoritmo 15.4; es decir, cada implicante primo de E se escribe en forma completa de suma de productos y luego se eliminan uno por uno los superfluos, es decir, aquellos sumandos que aparecen entre otros sumandos. Al final da

$$E = y't + xz + yz'$$

como una suma minimal para E.

COMPUERTAS LÓGICAS

15.22 Exprese la salida Y como una expresión booleana en las entradas A, B, C para el circuito lógico en:

a) Figura 15-26*a*); *b*) Figura 15-26*b*).

a) Las entradas a la primera compuerta AND son A y B', y a la segunda compuerta AND son B' y C. Por tanto, $Y = AB' + B'C$.

b) Las entradas a la primera compuerta AND son A y B', y a la segunda compuerta AND son A' y C. Por tanto, $Y = AB' + A'C$.

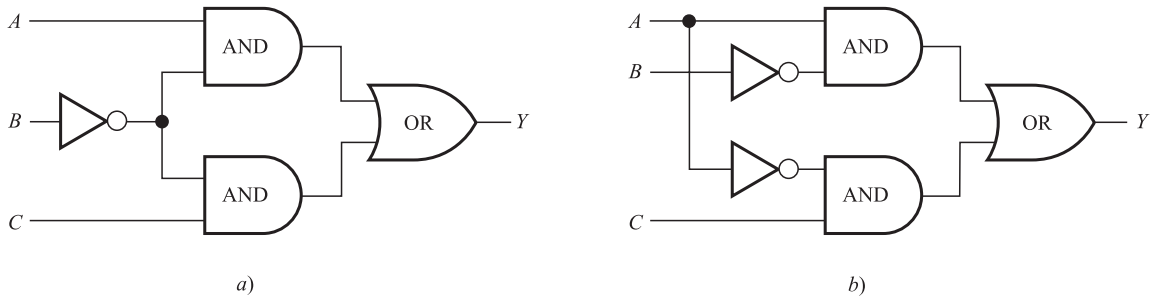


Figura 15-26

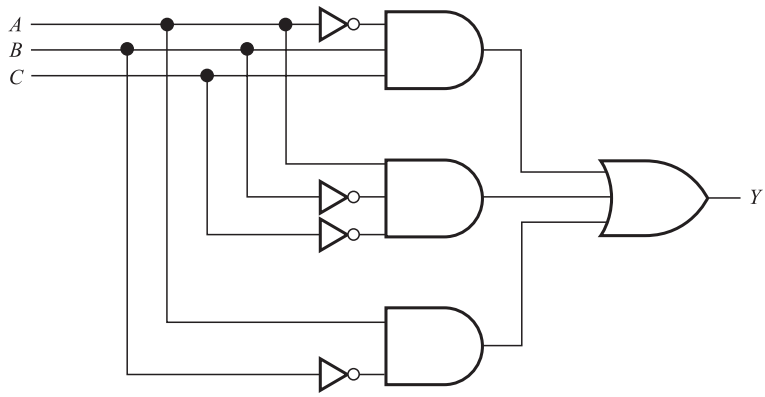


Figura 15-27

15.23 Exprese la salida Y como una expresión booleana en las entradas A, B, C para el circuito lógico en la figura 15-27.

La salida de la primera compuerta AND es $A'BC$, de la segunda compuerta AND es $AB'C'$, y de la última compuerta AND es AB'. Así,

$$Y = A'BC + AB'C' + AB'$$

15.24 Exprese la salida Y como una expresión booleana en las entradas A, B, C para el circuito lógico en:

a) Figura 15-28*a*); *b*) Figura 15-28*b*).

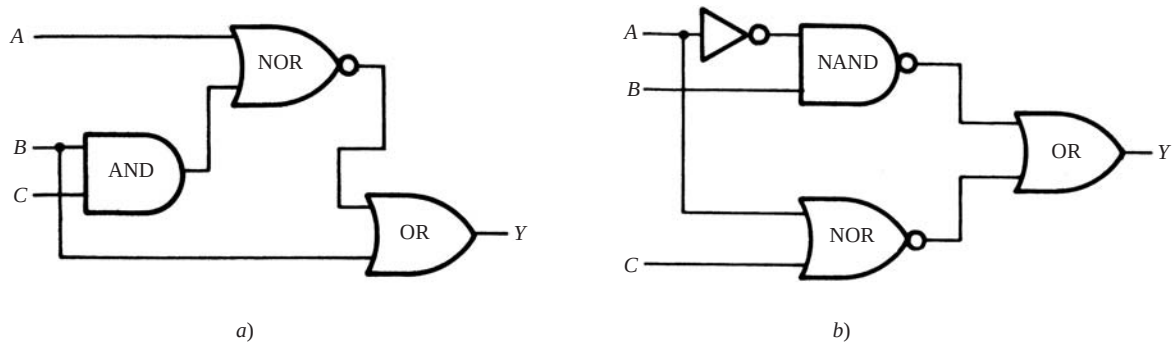


Figura 15-28

a) La salida de la compuerta AND es BC, de modo que las entradas a la compuerta NOR son A y BC. Por tanto, $(A + BC)'$ es la salida de la compuerta NOR. En consecuencia, las entradas a la compuerta OR son $(A + BC)'$ y B; por tanto, $Y = (A + BC)' + B$.

b) La salida de la compuerta NAND es $(A'B)'$, y la salida de la compuerta NOR es $(A + C)'$. Por tanto, $Y = (A'B)' + (A + C)'$.

15.25 Exprese la salida Y como una expresión booleana en las entradas A y B para el circuito lógico en la figura 15-29.

Aquí, un pequeño círculo en el circuito significa complemento. Por tanto, la salida de las tres compuertas a la izquierda son AB', $(A + B)'$ y $(A'B)'$. Por tanto,

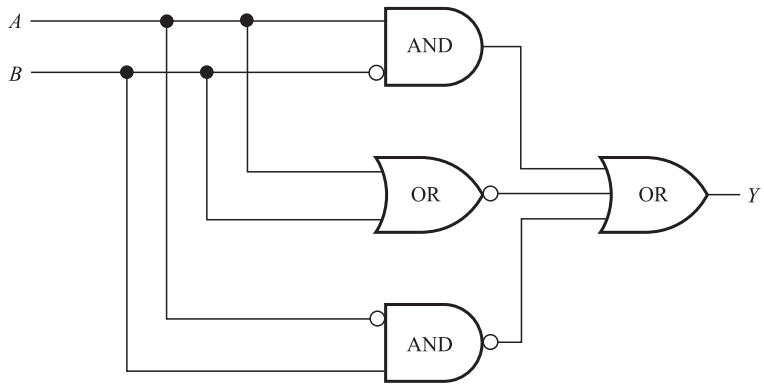
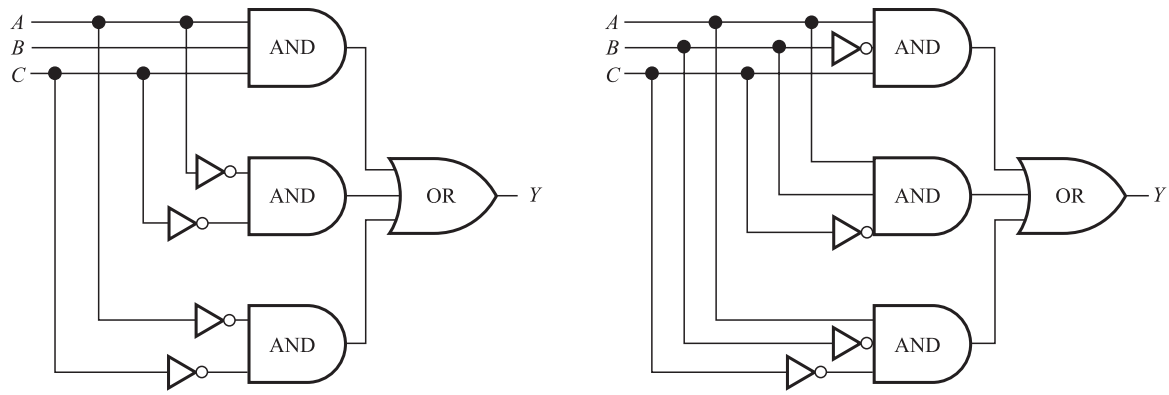


Figura 15-29

15.26 Dibuje el circuito lógico L con entradas A, B, C y salida Y que corresponde a cada expresión booleana:

a) $Y = ABC + A'C' + B'C'$; *b*) $Y = AB'C + ABC' + AB'C'$.

Estas expresiones son sumas de productos. Por tanto, L es un circuito AND-OR que tiene una compuerta AND para cada producto y una compuerta OR para la suma. El circuito necesario se muestra en la figura 15-30*a*) y *b*).



a) $Y = ABC + A'C' + B'C'$ *b*) $Y = AB'C + ABC' + AB'C'$

Figura 15-30

TABLAS DE VERDAD

15.27 Encuentre la secuencia de salida Y para una compuerta AND con entradas A, B, C (o, en forma equivalente, para $Y = ABC$), donde:

a) $A = 111001$; $B = 100101$; $C = 110011$.
b) $A = 11111100$; $B = 10101010$; $C = 00111100$.
c) $A = 00111111$; $B = 11111100$; $C = 11000011$.

La salida $Y = 1$ para una compuerta AND si y solo si hay unos en todas las posiciones de las secuencias de entrada. Así:

a) Sólo las posiciones primera y última tienen unos en las tres secuencias. Por tanto, $Y = 100001$.

b) Sólo las posiciones tercera y quinta (al leer de izquierda a derecha) tienen unos en las tres secuencias. Por tanto, $Y = 00101000$.

c) Ninguna posición tiene unos en las tres secuencias. Por tanto, $Y = 00000000$.

15.28 Encuentre la secuencia de salida Y para una compuerta OR con entradas A, B, C (o, en forma equivalente, para $Y = A + B + C$), donde:

a) $A = 100001$; $B = 100100$; $C = 110000$.
b) $A = 11000000$; $B = 10101010$; $C = 00000011$.
c) $A = 00111111$; $B = 11111100$; $C = 11000011$.

La salida $Y = 0$ para una compuerta OR si y solo si hay ceros en todas las posiciones de las secuencias de entrada. Así:

a) Sólo las posiciones tercera y quinta tienen ceros en las tres secuencias. Por tanto, $Y = 110101$.

b) Sólo las posiciones cuarta y sexta (al leer de izquierda a derecha) tienen ceros en las tres secuencias. Por tanto, $Y = 11101011$.

c) Ninguna posición tiene ceros en las tres secuencias. Por tanto, $Y = 11111111$.

15.29 Encuentre la secuencia de salida Y para una compuerta NOT con entrada A (o, en forma equivalente, para $Y = A'$), donde:

a) $A = 00111111$; *b*) $A = 11111100$; *c*) $A = 11000011$.

La compuerta NOT cambia 0 a 1 y 1 a 0. Por tanto:

a) $A' = 11000000$; *b*) $A' = 00000011$; *c*) $A' = 00111100$.

15.30 Considere el circuito lógico L con $n = 5$ entradas A, B, C, D, E o, en forma equivalente, considere una expresión booleana E con cinco variables x_1, x_2, x_3, x_4, x_5.

a) Encuentre las secuencias especiales para las variables (entradas).
b) ¿De cuántas formas diferentes es posible asignar un bit (0 o 1) a cada una de las $n = 5$ variables?
c) ¿Cuál es la propiedad más importante de las secuencias especiales?

a) Todas las secuencias tienen longitud $2^n = 2^5 = 32$. Consisten de bloques alternos de ceros y unos, donde las longitudes de los bloques son $2^{n-1} = 2^4 = 16$ para x_1, $2^{n-2} = 2^3 = 8$ para $x_2, \ldots, 2^{n-5} = 2^0 = 1$ para x_5. Así:

$$\begin{aligned} x_1 &= \ 00000000000000001111111111111111 \\ x_2 &= \ 00000000111111110000000011111111 \\ x_3 &= \ 00001111000011110000111100001111 \\ x_4 &= \ 00110011001100110011001100110011 \\ x_5 &= 01010101010101010101010101010101 \end{aligned}$$

b) Hay dos formas, 0 o 1, de asignar un bit a cada variable, de modo que hay $2^n = 2^5 = 32$ formas de asignar un bit a cada una de las $n = 5$ variables.

c) Las 32 posiciones en las secuencias especiales proporcionan las 32 combinaciones posibles de bits para las cinco variables.

15.31 Encuentre la tabla de verdad $T = T(E)$ para la expresión booleana $E = E(x, y, z)$ donde:

a) $E = xz + x'y$; *b*) $E = xy'z + xy + z'$.

Las secuencias especiales para las variables x, y, z y sus complementos son:

$$x = 00001111, \quad y = 00110011, \quad z = 01010101$$
$$x' = 11110000, \quad y' = 11001100, \quad z' = 10101010$$

a) Aquí $xz = 00000101$ y $x'y = 00110000$. Entonces $E = xz + x'y = 00110101$. Por tanto

$$T(00001111, 00110011, 01010101) = 00110101$$

o simplemente $T(E) = 00110101$, donde se supone que la entrada consiste de las secuencias especiales.

b) Aquí $xy'z = 00000100$, $xy = 00000011$, y $z' = 01010101$. Entonces $E = xy'z + xy + z' = 01010111$. Por tanto

$$T(00001111, 00110011, 01010101) = 01010111$$

15.32 Encuentre la tabla de verdad $T = T(E)$ para la expresión booleana $E = E(x, y, z)$ donde:

a) $E = xyz' + x'yz$; *b*) $E = xyz + xy'z + x'y'z$.

Aquí E es una expresión completa de suma de productos que es la suma de minterms. En el ejemplo 15.13 se proporcionan las tablas de verdad de los minterms (usando las secuencias especiales). Cada minterm contiene un solo 1 en su tabla de verdad; por tanto, la tabla de verdad de E tiene unos en las mismas posiciones que los unos en los minterms en E. Así:

a) $T(E) = 00001010$; *b*) $T(E) = 01000101$

15.33 Encuentre la tabla de verdad $T = T(E)$ para la expresión booleana

$$E = E(x, y, z) = (x'y)'yz' + x'(yz + z')$$

Primero exprese E como una suma de productos:

$$\begin{aligned} E = (x + y')yz' + x'yz + x'z' &= xyz' + y'yz' + x'yz + x'z' \\ &= xyz' + x'yz + x'z' \end{aligned}$$

Luego, exprese E como una suma de productos completa:

$$\begin{aligned} E &= xyz' + x'yz + x'z'(y + y') \\ &= xyz' + x'yz + x'yz' + x'y'z' \end{aligned}$$

Así como en el problema 15.32, se usan tablas de verdad para los minterms que aparecen en el ejemplo 15.13 para obtener $T(E) = 10101010$.

15.34 Encuentre la expresión booleana $E = (x, y, z)$ correspondiente a la tabla de verdad:

a) $T(E) = 01001001$; *b*) $T(E) = 00010001$.

Cada 1 en $T(E)$ corresponde al minterm con el 1 en la misma posición (use las tablas de verdad para los minterms que aparecen en el ejemplo 15.13). Por ejemplo, el 1 en la segunda posición corresponde a $x'y'z$ cuya tabla de verdad tiene un solo 1 en la segunda posición. Entonces, E es la suma de esos minterms. Así:

a) $E = x'y'z + x'yz + xyz'$; *b*) $E = xy'z' + xyz$

(De nuevo se supone que la entrada consiste de las secuencias especiales.)

MAPAS DE KARNAUGH

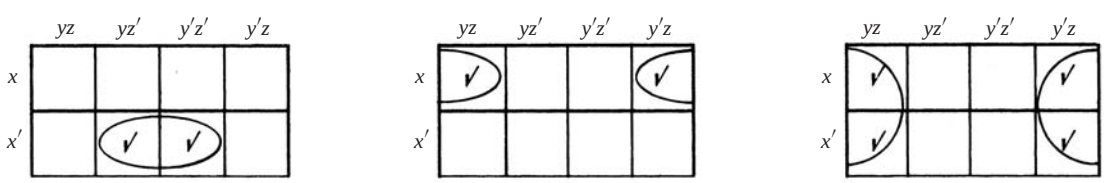
15.35 Encuentre el producto fundamental P representado por cada rectángulo básico en el mapa de Karnaugh en la figura 15-31.

En cada caso se encuentran las literales que aparecen en todos los cuadrados del rectángulo básico; así, P es el producto de esas literales.

a) x' y z' aparecen en ambos cuadrados; por tanto, $P = x'z'$.

b) x y z aparecen en ambos cuadrados; por tanto, $P = xz$.

c) Sólo z aparece en los cuatro cuadrados; por tanto, $P = z$.



a) *b*) *c*)

Figura 15-31

15.36 Sea R un rectángulo básico en un mapa de Karnaugh para cuatro variables x, y, z, t. Determine el número de literales en el producto fundamental P correspondiente a R en términos del número de cuadrados en R.

P tendrá una, dos, tres o cuatro literales en tanto que R tenga ocho, cuatro, dos o un cuadrado.

15.37 Encuentre el producto fundamental P representado por cada rectángulo básico en el mapa de Karnaugh en la figura 15-32.

En cada caso se encuentran las literales que aparecen en todos los cuadrados del rectángulo básico; así, P es el producto de esas literales. (El problema 15.36 indica el número de tales literales en P.)

a) En R hay dos cuadrados; por tanto, P tiene tres literales. En este caso, x', y', t' aparecen en ambos cuadrados; por tanto, $P = x'y't'$.

b) En R hay cuatro cuadrados; por tanto, P tiene dos literales. Aquí, sólo y' y t aparecen en los cuatro cuadrados; por tanto, $P = y't$.

c) En R hay ocho cuadrados; por tanto, P tiene sólo una literal. Específicamente, sólo y aparece en los ocho cuadrados; por tanto, $P = y$.

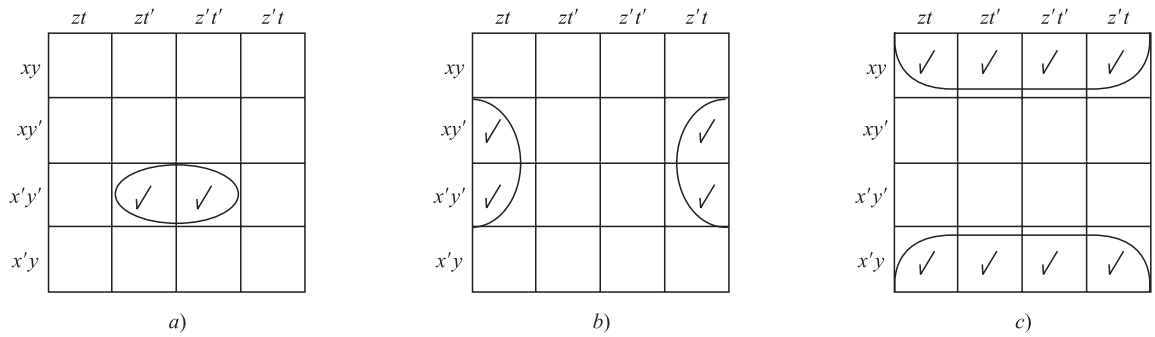


Figura 15-32

15.38 Sea E la expresión booleana proporcionada en el mapa de Karnaugh en la figura 15-33.

a) Escriba E en su forma completa de suma de productos. *b*) Encuentre una forma minimal para E.

a) Los siete productos fundamentales verificados se enumeran para obtener

$$E = xyz't' + xyz't + xy'zt + xy'zt' + x'y'zt + x'y'zt' + x'yz't'$$

b) El rectángulo básico maximal de dos por dos representa a $y'z$ puesto que sólo y' y z aparecen en los cuatro cuadrados. El par horizontal de cuadrados adyacentes representan xyz', y los cuadrados adyacentes que se traslapan en los bordes superior e inferior representan a $yz't'$. Ya que para una cubierta minimal se requieren los tres rectángulos,

$$E = y'z + xyz' + yz't$$

es la suma minimal para E.

15.39 Considere las expresiones booleanas E_1 y E_2 en las variables x, y, z, t proporcionadas por los mapas de Karnaugh en la figura 15-34. Encuentre una suma minimal para *a*) E_1; *b*) E_2.

a) Sólo y' aparece en los ocho cuadrados del rectángulo básico maximal de dos por cuatro, y el par designado de cuadrados adyacentes representa a xzt'. Ya que para una cubierta minimal se requieren los dos rectángulos,

$$E = y' + xzt'$$

es la suma minimal para E_1.

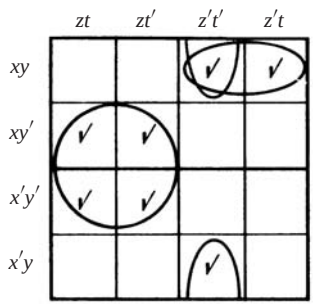
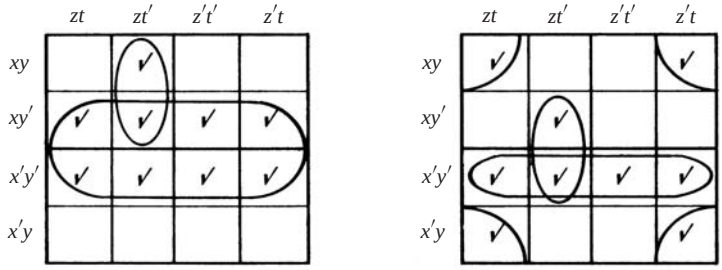


Figura 15-33



a) E_1 *b*) E_2

Figura 15-34

b) Los cuatro cuadrados en las esquinas forman un rectángulo básico maximal de dos por dos que representa a yt, puesto que sólo y y t aparecen en los cuatro cuadrados. El rectángulo básico maximal de cuatro por uno representa a $x'y'$ y los dos cuadros adyacentes representan a $y'zt'$. Ya que para una cubierta minimal se requieren los tres rectángulos,

$$E_2 = yt + x'y' + y'zt'$$

es la suma minimal para E_2.

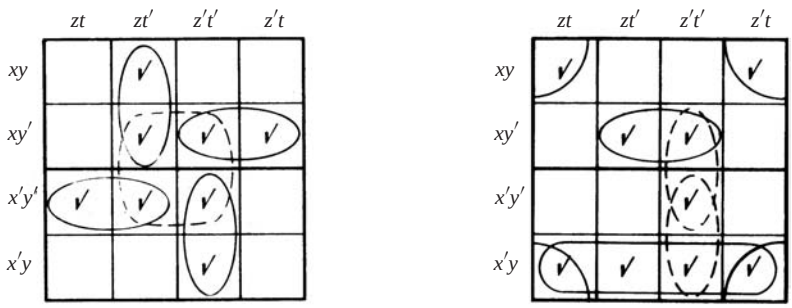
15.40 Considere las expresiones booleanas E_1 y E_2 en las variables x, y, z, t proporcionadas por los mapas de Karnaugh en la figura 15-35. Encuentre una suma minimal para *a*) E_1; *b*) E_2.

a) Hay cinco implicantes primos, designados por los cuatro óvalos y el círculo con línea discontinua. Sin embargo, este círculo no es necesario para cubrir a todos los cuadrados, mientras que los cuatro óvalos sí son necesarios. Por tanto, los cuatro óvalos constituyen la suma minimal para E_1; es decir,

$$E_1 = xzt' + xy'z' + x'y'z + x'z't'$$

b) Hay cinco implicantes primos, designados por los cinco óvalos, dos de los cuales aparecen con línea discontinua. Sólo uno de estos dos óvalos se requiere para cubrir el cuadrado $x'y'z't'$. Así, para E_2 hay dos sumas minimales, como sigue:

$$E_2 = x'y + yt + xy't' + y'z't' = x'y + yt + xy't' + x'z't'$$



a) E_1 *b*) E_2

Figura 15-35

15.41 Use un mapa de Karnaugh a fin de encontrar una suma minimal para:

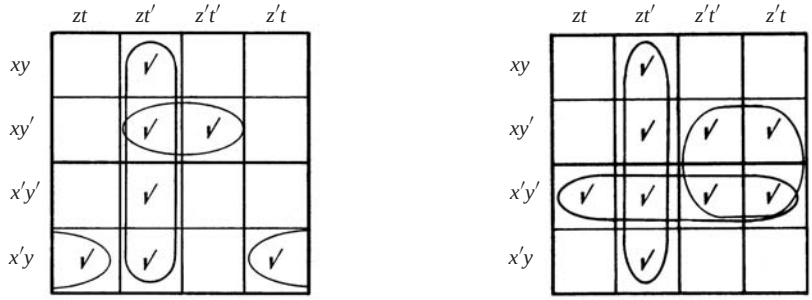
a) $E_1 = x'yz + x'yz't + y'zt' + xyzt' + xy'z't'$.
b) $E_2 = y't' + y'z't + x'y'zt + yzt'$.

a) Se comprueban los dos cuadrados correspondientes a cada uno de $x'yz$ y $y'zt'$, y se comprueba el cuadrado correspondiente a cada uno de $x'yz't$ y $xy'z't'$. Así se obtiene el mapa de Karnaugh en la figura 15-36*a*). Una cubierta minimal consiste de los tres óvalos designados. Por tanto, una suma minimal para E_1 es la siguiente:

$$E_1 = zt' + xy't' + x'yt$$

b) Se comprueban los cuatro cuadrados correspondientes a zt', los dos cuadrados correspondientes a cada uno de $y'z't$ y yzt', y el cuadrado correspondiente a $x'y'zt$. Así se obtiene el mapa de Karnaugh en la figura 15-36*b*). Una cubierta minimal consiste de los tres rectángulos básicos maximales designados. Así, una suma minimal para E_2 es la siguiente:

$$E_2 = zt' + xy't' + x'yt$$



a) E_1 *b*) E_2

Figura 15-36

15.42 Encuentre una forma de suma de productos minimal para la expresión booleana E con las siguientes tablas de verdad:

a) $T(00001111, 00110011, 01010101) = 10100110$.
b) $T(00001111, 00110011, 01010101) = 00101111$.

a) A partir de la tabla de verdad T (y las tablas de verdad en el ejemplo 15.13 para los minterms en las variables x, y, z) es posible leer la forma completa de suma de productos para E:

$$E = x'y'z' + x'yz' + xy'z + xyz'$$

Su mapa de Karnaugh se muestra en la figura 15-37*a*). Hay tres implicantes primos, como se indica mediante los tres óvalos, que constituyen una cubierta minimal de E. Por tanto, una forma minimal para E es la siguiente:

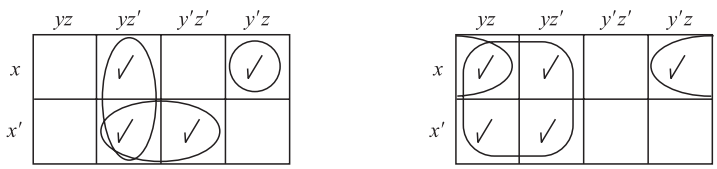
$$E = yz' + x'z' + xy'z$$

b) A partir de la tabla de verdad es posible leer la forma completa de suma de productos para E:

$$E = x'yz' + x'yz + xy'z + xyz' + xyz$$

Su mapa de Karnaugh se muestra en la figura 15-37*b*). Hay dos implicantes primos, como se indica mediante los dos óvalos, que constituyen una cubierta minimal de E. Por tanto, una forma minimal para E es la siguiente:

$$E = xz + y$$



a) *b*)

Figura 15-37

PROBLEMAS SUPLEMENTARIOS

ÁLGEBRAS BOOLEANAS

15.43 Escriba el dual de cada expresión booleana:

a) $a(a' + b) = ab$ *b*) $(a + 1)(a + 0) = a$ *c*) $(a + b)(b + c) = ac + b$

15.44 Considere las retículas $\mathbf{D}_m$ de divisores de m (donde $m > 1$).

a) Demuestre que $\mathbf{D}_m$ es un álgebra booleana si y sólo si m es *libre de cuadrados*; es decir, si m es un producto de primos distintos.

b) Si $\mathbf{D}_m$ es un álgebra booleana, demuestre que los átomos son los divisores primos distintos de m.

15.45 Considere los siguientes retículos: *a*) $\mathbf{D}_{20}$; *b*) $\mathbf{D}_{55}$; *c*) $\mathbf{D}_{99}$; *d*) $\mathbf{D}_{130}$. ¿Cuáles de ellos son álgebras booleanas, y cuáles son sus átomos?

15.46 Considere el álgebra booleana $\mathbf{D}_{110.}$

a) Escriba sus elementos y trace su diagrama.

b) Encuentre todas sus subálgebras.

c) Encuentre el número de subretículos con cuatro elementos.

d) Encuentre el conjunto A de átomos de $\mathbf{D}_{110.}$

e) Proporcione la transformación isomorfa f: $\mathbf{D}_{110} \to P(A)$ según se define en el teorema 15.6.

15.47 Sea B un álgebra booleana. Demuestre que:

a) Para cualquier x en B, $0 \leq x \leq 1$. *b*) $a < b$ si y sólo si $b' < a'$.

15.48 Un elemento x en un álgebra booleana B se denomina *maxterm* si su único sucesor es el elemento identidad 1. Encuentre los maxterms en el álgebra booleana $\mathbf{D}_{210}$ que se muestra en la figura 15-25.

15.49 Sea B un álgebra booleana.

a) Demuestre que los complementos de los átomos de B son los maxterms.

b) Demuestre que cualquier elemento x en B puede expresarse en forma única como un producto de maxterms.

15.50 Sea B un álgebra booleana con 16 elementos y sea S una subálgebra booleana de B con 8 elementos. Demuestre que dos de los átomos de S deben ser átomos de B.

15.51 Sea $B = (B, +, *, ', 0, 1)$ un álgebra booleana. En B se define una operación Δ (denominada *diferencia simétrica*) por

$$x \Delta y = (x * y') + (x' * y)$$

demuestre que $R = (B, \Delta, *)$ es un anillo booleano conmutativo. (Vea la sección B.6 y el problema B.72.)

15.52 Sea $R = (B, \oplus, \cdot)$ un anillo booleano conmutativo con identidad $1 \neq 0$. Se define

$$x' = 1 \oplus x, \quad x + y = x \otimes y \oplus x \cdot y, \quad x * y = x \cdot y$$

Demuestre que $B = (R, +, *, ', 0, 1)$ es un álgebra booleana.

EXPRESIONES BOOLEANAS, IMPLICANTES PRIMOS

15.53 Reduzca los siguientes productos booleanos a 0 o a un producto fundamental:

a) $xy'zxy'$; *b*) $xyz'sy'ts$; *c*) $xy'xz'ty'$; *d*) $xyz'ty't$.

15.54 Escriba cada expresión booleana $E(x, y, z)$ como una suma de productos y luego en su forma completa de suma de productos:

a) $E = x(xy' + x'y + y'z)$; *b*) $E = (x + y'z)(y + z')$; *c*) $E = (x' + y)' + y'z$.

15.55 Escriba cada expresión booleana $E(x, y, z)$ como una suma de productos y luego en su forma completa de suma de productos:

a) $E = (x'y)'(x' + xyz')$; *b*) $E = (x + y)'(xy')'$; *c*) $E = y(x + yz)'$.

15.56 Encuentre el consenso Q de los productos fundamentales P_1 y P_2, donde

a) $P_1 = xy'z, P_2 = xyt$; *c*) $P_1 = xy'zt, P_2 = xyz'$;
b) $P_1 = xyz't', P_2 = xzt'$; *d*) $P_1 = xy't, P_2 = xzt$.

15.57 Para cualquier expresión booleana E de suma de productos, sea E_L el número de literales en E (contando la multiplicidad), y E_S el número de sumandos en E. Encuentre E_L y E_S para cada una de las siguientes opciones:

a) $E = xyz't + x'yt + xy'zt$; *b*) $E = xyzt + xt' + x'y't + yt$.

15.58 Aplique el método del consenso (algoritmo 15.3) para encontrar los implicantes primos de cada una de las siguientes expresiones booleanas:

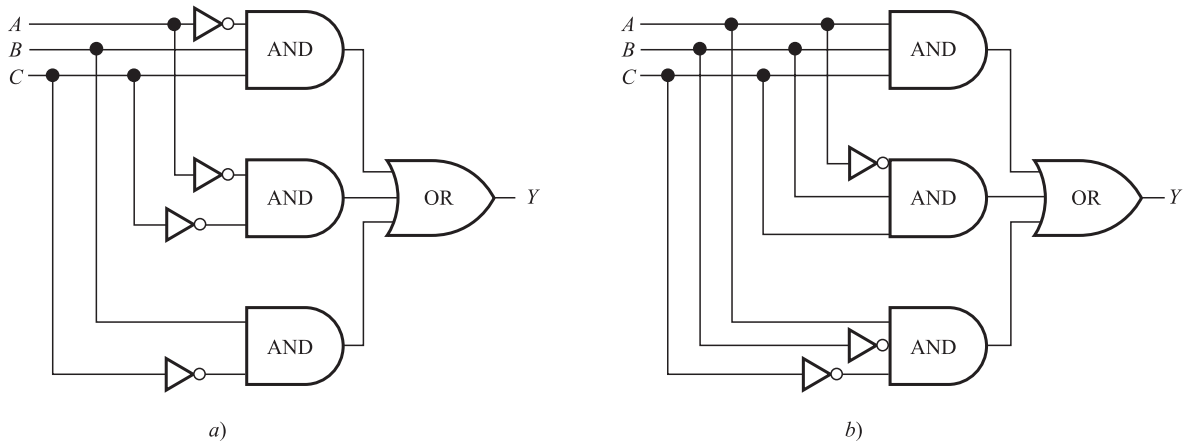
a) $E_1 = xy'z' + x'y + x'y'z' + x'yz$;
b) $E_2 = xy' + x'z't + xyzt' + x'y'zt'$;
c) $E_3 = xyzt + xyz't' + xz't' + x'y'z' + x'yz't$.

15.59 Encuentre una forma de suma de productos minimal para cada una de las expresiones booleanas en el problema 15.58.

COMPUERTAS LÓGICAS, TABLAS DE VERDAD

15.60 Exprese la salida Y como una expresión booleana en las entradas A, B, C para el circuito lógico en la:

a) Figura 15-38*a*); *b*) Figura 15-38*b*).



a) *b*)

Figura 15-38

15.61 Exprese la salida Y como una expresión booleana en las entradas A, B, C para el circuito lógico en la:

a) Figura 15-39*a*); *b*) Figura 15-39*b*).

15.62 Dibuje el circuito lógico L con entradas A, B, C y salida Y que corresponde a cada expresión booleana:

a) $Y = AB'C + AC' + A'C$; *b*) $Y = A'BC + A'BC' + ABC'$.

15.63 Encuentre la secuencia de salida Y para una compuerta AND con entradas A, B, C (o, en forma equivalente, para $Y = ABC$) donde:

a) $A = 110001$; $B = 101101$; $C = 110011$.
b) $A = 01111100$; $B = 10111010$; $C = 00111100$.
c) $A = 00111110$; $B = 01111100$; $C = 11110011$.

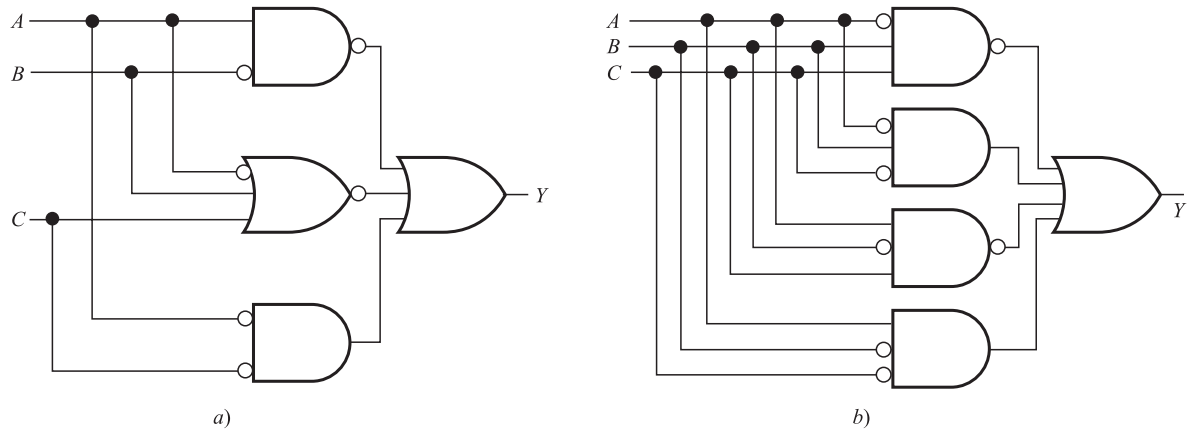


Figura 15-39

15.64 Encuentre la secuencia de salida Y para una compuerta OR con entradas A, B, C (o, en forma equivalente, para $Y = A + B + C$) donde:

a) $A = 100011$; $B = 100101$; $C = 1000001$.

b) $A = 10000001$; $B = 00100100$; $C = 00000011$.

c) $A = 00111100$; $B = 11110000$; $C = 10000001$.

15.65 Encuentre la secuencia de salida Y para una compuerta NOT con entrada A o, en forma equivalente, para $Y = A'$, donde:

a) $A = 11100111$; *b*) $A = 10001000$; *c*) $A = 11111000$.

15.66 Considere un circuito lógico L con $n = 6$ entradas A, B, C, D, E, F o, en forma equivalente, una expresión booleana E con seis variables $x_1, x_2, x_3, x_4, x_5, x_6$.

a) ¿De cuántas formas diferentes es posible asignar un bit (0 o 1) a cada una de las $n =$ seis variables?

b) Encuentre las tres primeras secuencias especiales para las variables (entradas).

15.67 Encuentre la tabla de verdad $T = T(E)$ para la expresión booleana $E = E(x, y, z)$ donde:

a) $E = xy + x'z$; *b*) $E = xyz' + y + xy'$.

15.68 Encuentre la tabla de verdad $T = T(E)$ para la expresión booleana $E = E(x, y, z)$ donde:

a) $E = x'yz' + x'y'z$; *b*) $E = xyz' + xy'z' + x'y'z'$.

15.69 Encuentre la expresión booleana $E = E(x, y, z)$ correspondiente a las tablas de verdad:

a) $T(E) = 10001010$; *b*) $T(E) = 00010001$; *c*) $T(E) = 00110000$.

15.70 Encuentre todas las sumas minimales posibles para cada expresión booleana E dada por el mapa de Karnaugh en la figura 15-40.

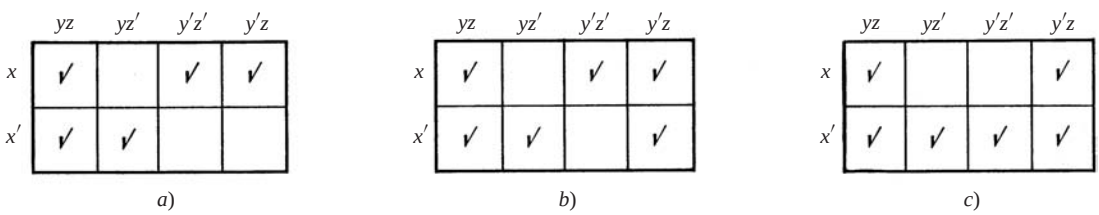


Figura 15-40

15.71 Encuentre todas las sumas minimales posibles para cada expresión booleana E dada por los mapas de Karnaugh en la figura 15-41.

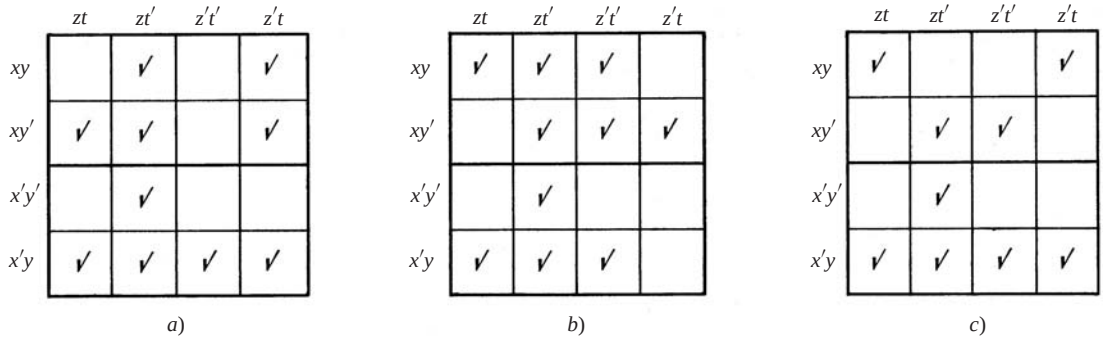


Figura 15-41

15.72 Use un mapa de Karnaugh para encontrar una suma minimal para la expresión booleana:

a) $E = xy + x'y + x'y'$; *b*) $E = x + x'yz + xy'z'$.

15.73 Encuentre la suma minimal para cada expresión booleana:

a) $E = y'z + y'z't' + z't$; *b*) $E = y'zt + xzt' + xy'z'$.

15.74 Use mapas de Karnaugh para rediseñar cada circuito de la figura 15-42 de modo que se convierta en un circuito minimal AND-OR.

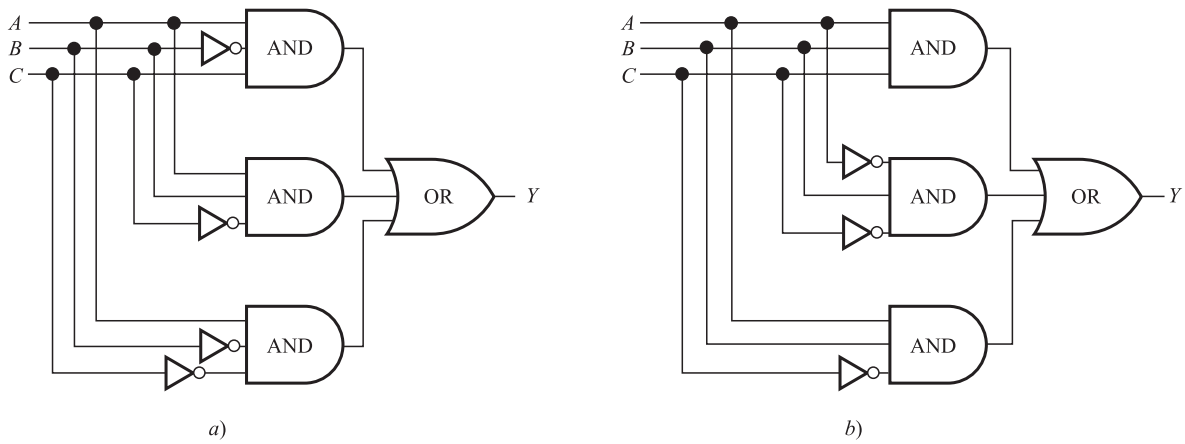


Figura 15-42

15.75 Suponga que tres interruptores A, B, C están conectados a la misma lámpara en una sala. En cualquier momento, un interruptor puede estar "arriba", se denota con 1, o "abajo", se denota con 0. Un cambio en cualquier interruptor modifica la paridad (impar o par) del número de unos. Los interruptores pueden controlar la luz si asocia, por ejemplo, una paridad impar con la luz en estado "encendido" (lo que se representa con 1), y una paridad par cuando la luz está "apagada" (lo que se representa con 0).

a) Demuestre que las siguientes tablas de verdad cumplen estas condiciones:

$$T(A, B, C) = T(00001111, 00110011, 01010101) = 01101001$$

b) Diseñe un circuito L AND-OR minimal con la tabla de verdad anterior.

Respuestas a los problemas suplementarios

15.43 *a*) $a + a'b = a + b$.
b) $a \cdot 0 + a \cdot 1 = a$.
c) $ab + bc = (a + c)b$.

15.45 *b*) $\mathbf{D}_{55}$; átomos 5 y 11. *d*) $\mathbf{D}_{130}$; átomos 2, 5 y 13.

15.46 *a*) Hay ocho elementos 1, 2, 5, 10, 11, 22, 55, 110. Vea la figura 15-43*a*).
b) Hay cinco subálgebras: {1, 110}, {1, 2, 55, 110}, {1, 5, 22, 110}, {1, 10, 11, 110}, $\mathbf{D}_{110}$.
c) Hay 15 subretículos que incluyen las cinco subálgebras anteriores.
d) $A = \{2, 5, 11\}$.
e) Vea la figura 15-43*b*).

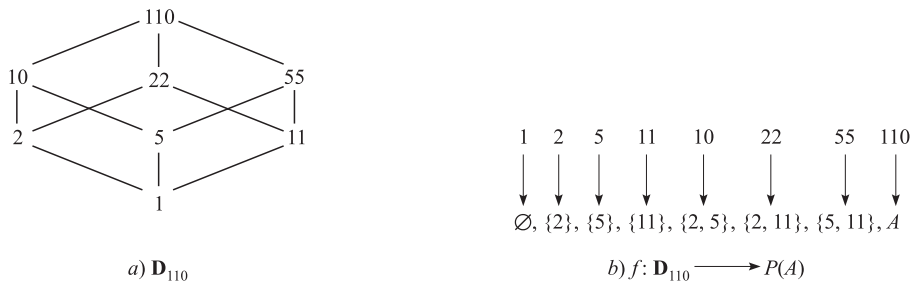


Figura 15-43

15.48 Maxterms: 30, 42, 70, 105

15.49 *b*) *Sugerencia:* use dualidad.

15.53 *a*) $xy'z$; *b*) 0; *c*) $xy'z't$; *d*) 0.

15.54 *a*) $E = xy' + xy'z = xy'z' + xy'z$.
b) $E = xy + xz' = xyz + xyz' + xy'z'$.
c) $E = xy' + y'z = xy'z + xy'z' + x'y'z$.

15.55 *a*) $E = xyz' + x'y = xyz' + x'y'z + x'y'z'$.
b) $E = x'y' = x'y'z + x'y'z'$.
c) $E = x'yz'$.

15.56 *a*) $Q = xzt$. *b*) $Q = xyt'$. *c*) y *d*) No existe.

15.57 *a*) $E_L = 11$, $E_S = 3$; *b*) $E_L = 11$, $E_S = 4$.

15.58 *a*) $x'y$, $x'z$, $y'z'$.
b) xy', xzt', $y'zt'$, $x'z't$, $y'z't'$.
c) $xyzt$, $xz'y'$, $y'z't'$, $x'y'z'$, $x'z't$.

15.59 *a*) $E = x'y + x'z'$.
b) $E = xy' + xzt' + x'z't + y'z't$.
c) $E = xyzt + xz't' + x'y'z' + x'z't$.

15.60 *a*) $Y = A'BC + A'C' + BC'$;
b) $ABC + A'BC + AB'C'$.

15.61 *a*) $Y = (AB') + (A' + B + C)' + AC$
b) $Y = (A'BC)' + A'BC' + (AB'C)' + AB'C'$

15.62 Vea la figura 15-44.

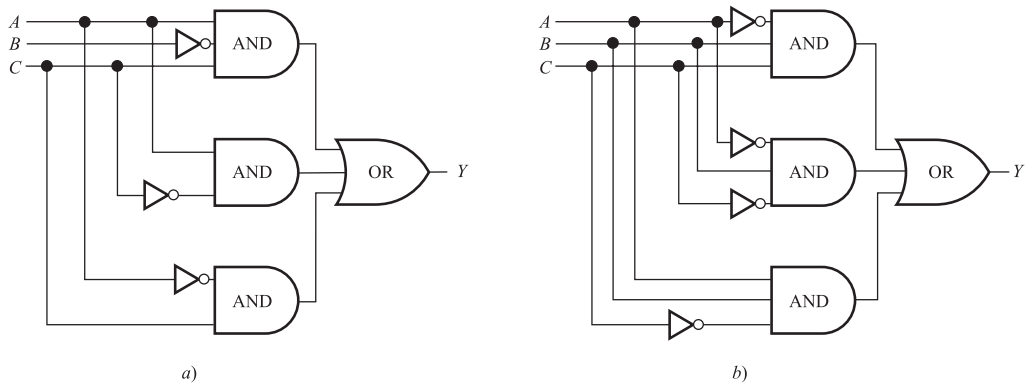


Figura 15-44

15.63 *a*) $Y = 100001$; *b*) $Y = 00111000$;
c) $Y = 00110000$.

15.64 *a*) $Y = 100111$; *b*) $Y = 10100111$;
c) $Y = 11111101$.

15.65 *a*) $A' = 00011000$; *b*) $A' = 01110111$;
c) $A' = 00000111$.

15.66 *a*) $2^n = 2^6 = 64$.
b) $x_1 = 000 \cdots 00111 \ldots 11$(32 ceros)(32 unos).
$x_2 = (00000000000000000111111111111111)^2$.
$x_3 = (0000000011111111)^4$.

15.67 *a*) $T(E) = 01010011$; *b*) $T(E) = 00111111$.

15.68 *a*) $T(E) = 01000000$; *b*) $T(E) = 10001010$.

15.69 Use tablas de verdad para los minterms en el ejemplo 15.13.
a) $E = x'y'z' + x'yz + xyz'$.
b) $E = xy'z' + xyz$.
c) $E = x'yz' + xy'z'$.

15.70 *a*) $E = xy' + x'y + yz = xy' + x'y + xz'$.
b) $E = xy' + x'y + z$.
c) $E = x' + z$.

15.71 *a*) $E = x'y + zt' + xz't + xy'z$.
$= x'y + zt' + xz't + xy't$.
b) $E = yz + yt' + zt' + xy'z'$.
c) $E = x'y + yt + xy't' + x'zt$.
$= x'y + yt + xy't' + y'zt$.

15.72 *a*) $E = x' + y$; *b*) $E = xz' + yz$.

15.73 *a*) $E = y' + z't$; *b*) $E = xy' + zt' + y'zt$.

15.74 *a*) Vea la figura 15-45.

15.75 *b*) Vea la figura 15-46.

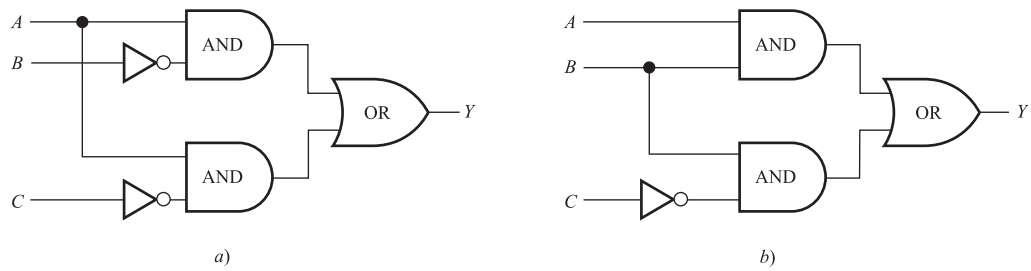


Figura 15-45

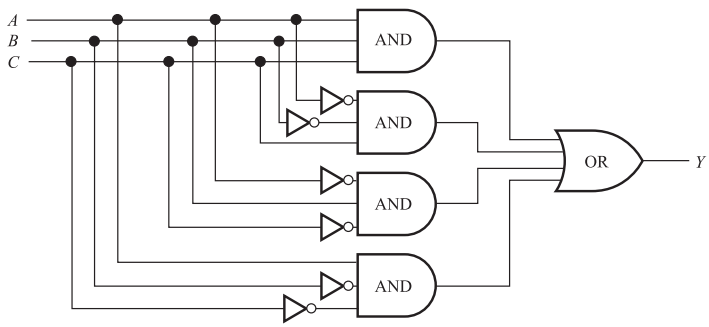


Figura 15-46

A Vectores y matrices

APÉNDICE

A.1 INTRODUCCIÓN

Los datos suelen escribirse en *arreglos*; es decir, en conjuntos cuyos elementos están indexados por uno o más subíndices. Si los datos son números, entonces un arreglo unidimensional se denomina *vector* y uno bidimensional se denomina *matriz* (la dimensión denota el número de subíndices) En este apéndice se analizan los vectores y matrices y las operaciones algebraicas que implican. En este contexto los números se consideran *escalares*.

A.2 VECTORES

Por un *vector u* se entiende una lista de números; por ejemplo, $a_1, a_2, \ldots, a_n$. Un vector así se denota por

$$u = (a_1, a_2, \ldots, a_n)$$

Los números a_i se denominan *componentes* o *entradas* de u. Si todas las $a_i = 0$, entonces u se denomina *vector cero*. Dos vectores así, u y v, son *iguales*, lo que se escribe $u = v$, si tienen el mismo número de componentes éstas son iguales.

EJEMPLO A.1

a) Las siguientes expresiones son vectores, donde los primeros dos tienen dos componentes y los dos últimos tienen tres componentes:

$$(3, -4), \quad (6, 8), \quad (0, 0, 0), \quad (2, 3, 4)$$

El tercer vector es el vector cero con tres componentes.

b) Aunque los vectores (1, 2, 3) y (2, 3, 1) tienen los mismos números, no son iguales porque las componentes correspondientes no son iguales.

Operaciones con vectores

Considere dos vectores arbitrarios u y v con el mismo número de componentes, sean estos

$$u = (a_1, a_2, \ldots, a_n) \quad \text{y} \quad v = (b_1, b_2, \ldots, b_n)$$

La *suma* de u y v, que se escribe $u + v$, es el vector que resulta de sumar las componentes correspondientes de u y v; es decir,

$$u + v = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

El *producto escalar*, o simplemente *producto* de un escalar k y el vector u, que se escribe ku, es el vector que resulta de multiplicar cada componente de u por k; es decir,

$$ku = (ka_1, ka_2, \ldots, ka_n)$$

También se define

$$-u = -1(u) \quad \text{y} \quad u - v = u + (-v)$$

y se acostumbra que 0 denote el vector cero. El vector $-u$ es el *negativo* de u.

El *producto punto* o *producto interno* de los vectores anteriores u y v se denota y define por

$$u \cdot v = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

La *norma* o *longitud* del vector u se denota y define por

$$\|u\| = \sqrt{u \cdot u} = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$$

Se observa que $\|u\| = 0$ si y sólo si $u = 0$; en caso contrario, $\|u\| > 0$.

EJEMPLO A.2 Sean $u = (2, 3, -4)$ y $v = (1, -5, 8)$. Entonces

$$\begin{aligned} u + v &= (2 + 1,\ 3 - 5,\ -4 + 8) = (3, -2, 4) \\ 5u &= (5 \cdot 2,\ 5 \cdot 3,\ 5 \cdot (-4)) = (10, 15, -20) \\ -v &= -1 \cdot (1, -5, 8) = (-1, 5, -8) \\ 2u - 3v &= (4, 6, -8) + (-3, 15, -24) = (1, 21, -32) \\ u \cdot v &= 2 \cdot 1 + 3 \cdot (-5) + (-4) \cdot 8 = 2 - 15 - 32 = -45 \\ \|u\| &= \sqrt{2^2 + 3^2 + (-4)^2} = \sqrt{4 + 9 + 16} = \sqrt{29} \end{aligned}$$

Los vectores bajo las operaciones de adición vectorial y multiplicación escalar poseen varias propiedades; por ejemplo,

$$k(u + v) = ku + kv$$

donde k es un escalar y u y v son vectores. Muchas de tales propiedades aparecen en el teorema A.1, que también se cumple para vectores, puesto que los vectores se consideran un caso especial de las matrices.

Vectores columna

Algunas veces una lista de números se escribe en forma vertical, no horizontal, entonces la lista se denomina *vector columna*. En este contexto, los vectores anteriores escritos en forma horizontal se denominan *vectores renglón*. Las operaciones anteriores para vectores renglón se definen en forma semejante para vectores columna.

A.3 MATRICES

Una *matriz A* es un arreglo rectangular de números que suele presentarse en la forma

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Las m listas horizontales de números se denominan *renglones* de A y las n listas verticales de números se denominan *columnas* de A. Así, el elemento a_{ij}, también se denomina *entrada ij*, aparece en el renglón i y en la columna j. A menudo, una matriz como ésta se identifica al escribir simplemente $A = [a_{ij}]$.

Una matriz con m renglones y n columnas se denomina matriz de m por n, que se escribe $m \times n$. El par de números m y n se denominan *tamaño* de la matriz. Dos matrices A y B son iguales, lo cual se escribe $A = B$, si tienen el mismo tamaño y sus elementos correspondientes son iguales. Por tanto, la igualdad de dos matrices de $m \times n$ es equivalente a un sistema de mn igualdades, una para cada par de elementos correspondientes.

Una matriz que tiene un solo renglón se denomina *matriz renglón* o *vector renglón*, y una matriz con sólo una columna se denomina *matriz columna* o *vector columna*. Una matriz cuyos elementos son todos iguales a cero se denomina *matriz cero* y suele denotarse por 0.

EJEMPLO A.3

a) El arreglo rectangular $A = \begin{bmatrix} 1 & -4 & 5 \\ 0 & 3 & -2 \end{bmatrix}$ es una matriz de 2×3. Sus renglones son $[1, -4, 5]$ y $[0, 3, -2]$, y sus columnas son $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 3 \end{bmatrix}, \begin{bmatrix} 5 \\ -2 \end{bmatrix}$.

b) La matriz cero de 2×4 es $0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

c) Suponga que

$$\begin{bmatrix} x+y & 2z+t \\ x-y & z-t \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 5 \end{bmatrix}$$

Entonces las cuatro entradas correspondientes deben ser iguales. Es decir,

$$x + y = 3, \quad x - y = 1, \quad 2z + t = 7, \quad z - t = 5$$

La solución del sistema de ecuaciones es

$$x = 2, \quad \text{y} = 1, \quad z = 4, \quad t = -1$$

A.4 ADICIÓN DE MATRICES Y MULTIPLICACIÓN POR UN ESCALAR

Sean $A = [a_{ij}]$ y $B = [b_{ij}]$ dos matrices del mismo tamaño; por ejemplo, matrices de $m \times n$. La *suma* de A y B, que se escribe $A + B$, es la matriz que se obtiene al sumar los elementos correspondientes de A y B. El *producto* (*escalar*) de la matriz A por el escalar k, que se escribe kA, es la matriz que se obtiene al multiplicar cada elemento de A por k. Estas operaciones se muestran en la figura A-1.

$$A + B = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{bmatrix} \quad \text{y} \quad kA = \begin{bmatrix} ka_{11} & ka_{12} & \dots & ka_{1n} \\ ka_{21} & ka_{22} & \dots & ka_{2n} \\ \dots & \dots & \dots & \dots \\ ka_{m1} & ka_{m2} & \dots & ka_{mn} \end{bmatrix}$$

Figura A-1

Observe que $A + B$ y kA también son matrices de $m \times n$. Asimismo, se define

$$-A = (-1)A \quad \text{y} \quad A - B = A + (-B)$$

La matriz $-A$ se denomina *negativa* de A. La suma de matrices de tamaños distintos no está definida.

EJEMPLO A.4 Sean $A = \begin{bmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \end{bmatrix}$ y $B = \begin{bmatrix} 4 & 6 & 8 \\ 1 & -3 & -7 \end{bmatrix}$. Entonces

$$A + B = \begin{bmatrix} 1+4 & -2+6 & 3+8 \\ 0+1 & 4+(-3) & 5+(-7) \end{bmatrix} = \begin{bmatrix} 5 & 4 & 11 \\ 1 & 1 & -2 \end{bmatrix}$$

$$3A = \begin{bmatrix} 3(1) & 3(-2) & 3(3) \\ 3(0) & 3(4) & 3(5) \end{bmatrix} = \begin{bmatrix} 3 & -6 & 9 \\ 0 & 12 & 15 \end{bmatrix}$$

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 0 & 8 & 10 \end{bmatrix} + \begin{bmatrix} -12 & -18 & -24 \\ -3 & 9 & 21 \end{bmatrix} = \begin{bmatrix} -10 & -22 & -18 \\ -3 & 17 & 31 \end{bmatrix}$$

Las matrices bajo la adición de matrices y la multiplicación por un escalar poseen las propiedades siguientes.

Teorema A.1: Sean A, B, C matrices del mismo tamaño y sean k y k' escalares. Entonces:

i) $(A + B) + C = A + (B + C)$	*v*) $k(A + B) = kA + kB$
ii) $A + 0 = 0 + A$	vi) $(k + k')A = kA + k'A$
iii) $A + (-A) = (-A) + 0 = A$	*vii*) $(kk')A = k(k'A)$
iv) $A + B = B + A$	*viii*) $1A = A$

Primero observe que el 0 en los incisos *ii*) y *iii*) se refiere a la matriz cero. También, por los incisos *i*) y *iv*), cualquier suma de matrices

$$A_1 + A_2 + \cdots + A_n$$

no requiere paréntesis, y la suma no depende del orden de las matrices. Además, al usar los incisos *vi*) y *viii*), también se tiene

$$A + A = 2A, \quad A + A + A = 3A, \quad \cdots$$

Por último, puesto que los vectores con n componentes pueden identificarse con matrices de $1 \times n$ o con matrices de $n \times 1$, el teorema A.1 también se cumple para vectores bajo adición vectorial y multiplicación por un escalar.

La demostración del teorema A.1 se reduce a probar que las entradas ij en ambos miembros de cada ecuación matricial son iguales.

A.5 MULTIPLICACIÓN DE MATRICES

El producto de las matrices A y B, que se escribe AB, es algo más complicado. Por ello, primero se empieza con un caso especial. (El lector puede consultar en la sección 3.5 un análisis del símbolo griego de sumatoria Σ, la letra sigma mayúscula.)

El producto AB de una matriz renglón $A = [a_i]$ y una matriz columna $B = [b_i]$ con el mismo número de elementos se define como sigue:

$$AB = [a_1, a_2, \ldots, a_n] \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix} = a_1b_1 + a_2b_2 + \cdots + a_nb_n = \sum_{k=1}^{n} a_k b_k$$

Es decir, AB se obtiene al multiplicar las entradas correspondientes en A y B y luego al sumar todos los productos. Se recalca que AB es un escalar (o una matriz de 1×1). El producto AB no está definido cuando A y B tienen un número de elementos distinto.

EJEMPLO A.5

a) $[7, -4, 5] \begin{bmatrix} 3 \\ 2 \\ -1 \end{bmatrix} = 7(3) + (-4)(2) + 5(-1) = 21 - 8 - 5 = 8$

b) $[6, -1, 8, 3]\begin{bmatrix} 4 \\ -9 \\ -2 \\ 5 \end{bmatrix} = 24 + 9 - 16 + 15 = 32$

Ahora ya es posible definir la multiplicación de matrices en general.

Definición A.1: Sean $A = [a_{ik}]$ y $B = [b_{kj}]$ matrices tales que el número de columnas de A es igual al número de renglones de B; por ejemplo, A es una matriz de $m \times p$ y B es una matriz de $p \times n$. Entonces el producto AB es la matriz de $m \times n$, $C = [c_{ij}]$ cuya entrada ij se obtiene al multiplicar el i-ésimo renglón de A por la j-ésima columna de B; es decir,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}$$

El producto AB se muestra en la figura A-2.

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \cdot & \cdots & \cdot \\ a_{i1} & \cdots & a_{ip} \\ \cdot & \cdots & \cdot \\ a_{m1} & \cdots & a_{mp} \end{bmatrix} \begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ b_{p1} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \cdot & \cdots & \cdot \\ \cdot & c_{ij} & \cdot \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

Figura A-2

Se recalca que el producto AB no está definido si A es una matriz de $m \times p$ y B es una matriz de $q \times n$, donde $p \neq q$.

EJEMPLO A.6

a) Encuentre AB, donde $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ y $B = \begin{bmatrix} 2 & 0 & -4 \\ 5 & -2 & 6 \end{bmatrix}$.

Puesto que A es de 2×2 y B es de 2×3, el producto AB está definido y AB es una matriz de 2×3. Para obtener el primer renglón de la matriz producto AB, el primer renglón (1, 3) de A se multiplica por cada columna de B,

$$\begin{bmatrix} 2 \\ 5 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ -2 \end{bmatrix}, \quad \begin{bmatrix} -4 \\ 6 \end{bmatrix}$$

respectivamente. Es decir,

$$AB = \begin{bmatrix} 2+15 & 0-6 & -4+18 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \end{bmatrix}$$

Para obtener el segundo renglón del producto AB, el segundo renglón $(2, -1)$ de A se multiplica por cada columna de B, respectivamente. Así,

$$AB = \begin{bmatrix} 17 & -6 & 14 \\ 4-5 & 0+2 & -8-6 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \\ -1 & 2 & -14 \end{bmatrix}$$

b) Suponga que $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ y $B = \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}$. Entonces

$$AB = \begin{bmatrix} 5+0 & 6-4 \\ 15+0 & 18-8 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{y} \quad BA = \begin{bmatrix} 5+18 & 10+24 \\ 0-6 & 0-8 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

El ejemplo A.6*b*) muestra que la multiplicación de matrices no es conmutativa; es decir, que los productos AB y BA de matrices no necesariamente son iguales.

La multiplicación de matrices, no obstante, satisface las siguientes propiedades:

Teorema A.2: Sean A, B, C matrices. Entonces, siempre que los productos y las sumas estén definidos:

i) $(AB)C = A(BC)$ (Ley asociativa).
ii) $A(A + B) = AB + AC$ (Ley distributiva por la izquierda).
iii) $(B + C)A = BA + CA$ (Ley distributiva por la derecha).
iv) $k(AB) = (kA)B = A(kB)$ donde k es un escalar.

Multiplicación de matrices y sistemas de ecuaciones lineales

Cualquier sistema S de ecuaciones lineales es equivalente a la ecuación matricial

$$AX = B$$

donde A es la matriz que contiene los coeficientes, X es el vector columna de las incógnitas y B es el vector columna de las constantes. (Aquí *equivalente* significa que cualquier solución del sistema S es una solución de la ecuación matricial $AX = B$, y viceversa.) Por ejemplo, el sistema

$$\begin{array}{r} x + 2y - 3z = 4 \\ 5x - 6y + 8z = 9 \end{array} \quad \text{es equivalente a} \quad \begin{bmatrix} 1 & 2 & -3 \\ 5 & -6 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix}$$

Observe que el sistema está determinado completamente por la matriz

$$M = [A, B] = \begin{bmatrix} 1 & 2 & -3 & 4 \\ 5 & -6 & 8 & 9 \end{bmatrix}$$

que se denomina *matriz aumentada* del sistema.

A.6 TRASPUESTA

La *traspuesta* de una matriz A, que se escribe A^T, es la matriz que se obtiene al escribir los renglones de A, en orden, como columnas. Por ejemplo

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} \quad \text{y} \quad [1, -3, -5]^T = \begin{bmatrix} 1 \\ -3 \\ -5 \end{bmatrix}$$

Observe que si A es una matriz de $m \times n$, entonces A^T es una matriz de $n \times m$. En particular, la traspuesta de un vector renglón es un vector columna y viceversa. Además, si $B = [b_{ij}]$ es la traspuesta de $A = [a_{ij}]$, entonces $b_{ij} = a_{ji}$ para todo i y j.

A.7 MATRICES CUADRADAS

Una matriz que tiene el mismo número de renglones que de columnas se denomina *cuadrada*. Se dice que una matriz cuadrada con n renglones y n columnas es de *orden n* y se denomina *matriz cuadrada n*.

La *diagonal principal*, o simplemente la *diagonal*, de una matriz cuadrada $A = [a_{ij}]$ consiste de los elementos a_{11}, $a_{22}, \ldots, a_{nn}$; es decir, de los elementos que están desde la esquina superior izquierda hasta la esquina inferior derecha de la matriz. La *traza* de A, que se escribe $\text{tr}(A)$, es la suma de los elementos en la diagonal; es decir, $\text{tr}(A) = a_{11} + a_{22} + \ldots + a_{nn}$.

La matriz *cuadrada unitaria n*, que se denota por I_n, o simplemente por I, es la matriz cuadrada con unos a lo largo de la diagonal y ceros en el resto. La matriz unitaria I desempeña el mismo papel en la multiplicación de matrices que el número 1 en la multiplicación común y corriente de números. En este caso, para cualquier matriz A,

$$AI = IA = A$$

Considere, por ejemplo, las matrices

$$\begin{bmatrix} 1 & -2 & 0 \\ 0 & -4 & -6 \\ 5 & 3 & 2 \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ambas matrices son cuadradas. La primera es de orden 3 y su diagonal consiste de los elementos 1, −4, 2, de modo que su traza es igual a $1 - 4 + 2 = -1$. La segunda matriz es de orden 4; su diagonal consiste sólo de unos y en el resto sólo hay ceros. Así, la segunda matriz es la matriz unitaria de orden 4.

Álgebra de matrices cuadradas

Sea A cualquier matriz cuadrada. Entonces es posible multiplicar A por sí misma. De hecho todas las *potencias* no negativas de A se obtienen como sigue:

$$A^2 = AA, \quad A^3 = A^2A, \ldots, \quad A^{n+1} = A^nA, \ldots, \quad \text{y} \quad A^0 = I \text{ (cuando } A \neq 0)$$

En la matriz A también están definidos los polinomios. En específico, para cualquier polinomio,

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

donde las a_i son escalares, $f(A)$ se define como la matriz

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_nA^n$$

Observe que $f(A)$ se obtiene a partir de $f(x)$ al sustituir la matriz A por la variable x y sustituir la matriz escalar a_0I por el término escalar a_0. Si $f(A)$ es la matriz cero, entonces la matriz A se denomina *cero* o *raíz* del polinomio $f(x)$.

EJEMPLO A.7 Suponga que $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$. Entonces

$$A^2 = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} \quad \text{y}$$

$$A^3 = A^2A = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} -11 & 38 \\ 57 & -106 \end{bmatrix}$$

Suponga que $f(x) = 2x^2 - 3x + 5$. Entonces

$$f(A) = 2\begin{bmatrix} 7 & -6 \\ -9 & -22 \end{bmatrix} - 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 16 & -18 \\ -27 & 61 \end{bmatrix}$$

Suponga que $g(x) = x^2 + 3x - 10$. Entonces

$$g(A) = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} - 10\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Entonces A es un cero del polinomio $g(x)$.

A.8 MATRICES INVERTIBLES (NO SINGULARES), INVERSAS

Se dice que una matriz cuadrada A es *invertible* (o *no singular*) si existe una matriz B tal que

$$AB = BA = I, \quad \text{(la matriz identidad).}$$

La matriz B es única; se denomina *inversa* de A y se denota por A^{-1}. Observe que B es la inversa de A si y sólo si A es la inversa de B. Por ejemplo, suponga

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

Entonces

$$AB = \begin{bmatrix} 6-5 & -10+10 \\ 3-3 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{y} \quad BA = \begin{bmatrix} 6-5 & 15-15 \\ -2+2 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Por tanto, A y B son inversas.

Se sabe que $AB = I$ si y sólo si $BA = I$; por tanto, sólo es necesario probar un producto para determinar si dos matrices son inversas. Por ejemplo,

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -11+0+12 & 2+0-2 & 2+0-2 \\ -22+4+18 & 4+0-3 & 4-1-3 \\ -44-4+48 & 8+0-8 & 8+1-8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Entonces las dos matrices son invertibles e inversas entre sí.

A.9 DETERMINANTES

A cada matriz cuadrada n $A = [a_{ij}]$ se asigna un número específico denominado *determinante* de A que se denota con det(A), $|A|$ o

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

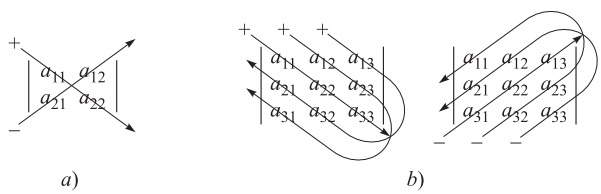
Se recalca que un arreglo cuadrado de números delimitado por líneas rectas, denominado *determinante de orden n*, no es una matriz, sino que denota el número que la función determinante asigna al arreglo delimitado de números; es decir, la matriz cuadrada delimitada.

Los determinantes de orden 1, 2, y 3 se definen como sigue:

$$|a_{11}| = a_{11} \qquad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

El diagrama en la figura A-3*a*) ayuda a recordar el determinante de orden 2. Es decir, el determinante es igual a la diferencia del producto de los elementos a lo largo de la flecha identificada por el signo más, menos el producto de los elementos a lo largo de la flecha identificada por el signo menos. Hay un diagrama semejante para recordar el determinante de orden 3, que se muestra en la figura A-3*b*). Por conveniencia en la notación, se han separado las tres flechas identificadas con el signo más y las tres flechas identificadas con el signo menos. Se recalca que para recordar determinantes de orden superior no hay este tipo de recursos visuales.



a) *b*)

Figura A-3

EJEMPLO A.8

a) $\begin{vmatrix} 5 & 4 \\ 2 & 3 \end{vmatrix} = 5(3) - 4(2) = 15 - 8 = 7, \quad \begin{vmatrix} 2 & 1 \\ -4 & 6 \end{vmatrix} = 2(6) - 1(-4) = 12 + 4 = 16.$

$$b)\ \begin{vmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{vmatrix} = 2(6)(0) + 1(-1)(5) + 3(1)(4) - 5(6)(3) - 1(-1)(2) - 0(1)(4)$$
$$= 0 - 5 + 12 - 90 + 2 - 0 = 81$$

Definición general de los determinantes

A continuación se proporciona la definición general de un determinante de orden n.

$$\det(A) = \sum \text{sgn}(\sigma) a_{1j_1} a_{2j_2} \dots a_{nj_n}$$

donde la sumatoria se toma sobre todas las permutaciones $\sigma = \{j_1, j_2, \dots, j_n\}$ de $\{1, 2, \dots, n\}$. Aquí sgn(σ) es igual a $+1$ o -1 según sea necesario un número par o impar de intercambios para modificar σ de modo que sus números estén en el orden de costumbre. La definición general de la función determinante se ha incluido para cubrir el tema. Si el lector desea conocer técnicas para calcular determinantes de orden superior a 3, se le aconseja consultar libros de teoría de matrices o álgebra lineal. Las permutaciones se estudiaron en el capítulo 5 de este texto.

Una propiedad importante de la función determinante es que es multiplicativa. Es decir:

Teorema A.3: Sean A y B matrices cuadradas n arbitrarias. Entonces

$$\det(AB) = \det(A) \cdot \det(B)$$

La demostración del teorema anterior rebasa el alcance de este texto.

Determinantes e inversas de matrices de 2 × 2

Considere una matriz arbitraria de 2×2: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Suponga que $|A| = ad - bc \neq 0$. Entonces puede demostrarse que

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix} = \frac{1}{|A|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

En otras palabras, cuando $|A| \neq 0$, > la inversa de una matriz A de 2×2 se obtiene como sigue:

1) Se intercambian los elementos en la diagonal principal.

2) Se toman los negativos de los demás elementos.

3) La matriz se multiplica por $1/|A|$ o, en forma equivalente, cada elemento se divide entre $|A|$.

Por ejemplo, si $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$, por tanto, $|A| = -2$ y entonces

$$A^{-1} = \frac{1}{-2} \begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}$$

Por otra parte, si $|A| = 0$, entonces A^{-1} no existe. Aunque no hay ninguna fórmula simple para matrices de orden superior, este resultado es verdadero en general. A saber:

Teorema A.4: Una matriz A es invertible si y solo si su determinante es diferente de cero.

A.10 OPERACIONES ELEMENTALES EN LOS RENGLONES, ELIMINACIÓN GAUSSIANA (OPCIONAL)

En esta sección se aborda el algoritmo de eliminación gaussiana en el contexto de operaciones elementales en los renglones.

Operaciones elementales en los renglones

Considere una matriz $A = [a_{ij}]$ cuyos renglones se denotan, respectivamente, por R_1, R_2,..., R_m. El primer elemento distinto de cero en un renglón R_i se denomina *elemento principal* distinto de cero. Un renglón con todos sus elementos iguales a cero se denomina *renglón cero*. Así, un renglón cero no tiene elemento principal distinto de cero.

Las tres operaciones siguientes sobre A se denominan *operaciones elementales en los renglones*:

[$\mathbf{E_1}$] Intercambiar el renglón R_i y el renglón R_j. Esta operación se indica al escribir "Intercambiar R_i y R_j".

[$\mathbf{E_2}$] Multiplicar cada elemento en un renglón R_i por una constante k diferente de cero. Esta operación se indica al escribir "Multiplicar R_i por k".

[$\mathbf{E_3}$] Sumar un múltiplo de un renglón R_i a otro renglón R_j o, en otras palabras, sustituir R_j por la suma $kR_i + R_j$. Esta operación se indica al escribir "Sumar kR_i a R_j".

Para evitar fracciones, [$\mathbf{E_1}$] y [$\mathbf{E_2}$] se realizan en un paso, se aplica la siguiente operación:

[$\mathbf{E}$] Sumar un múltiplo de un renglón R_i a un múltiplo distinto de cero de otro renglón R_j o, en otras palabras, sustituir R_j por la suma $kR_i + k'R_j$, donde $k' \neq 0$. Esta operación se indica al escribir "Sumar kR_i a $k'R_j$".

Se recalca que, en las operaciones [$\mathbf{E_3}$] y [$\mathbf{E}$], en realidad sólo se modifica el renglón R_j.

Notación: Se dice que las matrices A y B son *equivalentes por renglones*, lo cual se escribe $A \sim B$, si la matriz B se obtiene a partir de la matriz A mediante operaciones elementales en los renglones.

Matrices escalonadas

Una matriz A se denomina *escalonada*, o se dice que está en *forma escalonada*, si cumplen las dos condiciones siguientes:

i) Todos los renglones cero, en caso de haberlos, están en la parte inferior de la matriz.

ii) Todo elemento principal distinto de cero está a la derecha del elemento principal distinto de cero del renglón precedente.

Se dice que la matriz está en *forma canónica por renglones* si además cuenta con las dos propiedades siguientes:

iii) Todo elemento principal distinto de cero es 1.

iv) Todo elemento principal distinto de cero es el único elemento distinto de cero en esa columna.

La matriz cero 0, para cualquier número de renglones o columnas, es un caso especial de una matriz en forma canónica por renglones. Otro ejemplo de una matriz en forma canónica por renglones es la matriz identidad cuadrada n: I_n.

Se dice que una matriz cuadrada A está en *forma triangular* si sus elementos a_{11}, a_{22}, . . . , a_{nn} de la diagonal principal, encabezan los elementos distintos de cero de su renglón. Por tanto, una matriz cuadrada en forma triangular constituye un caso especial de una matriz escalonada. La matriz identidad I es el único ejemplo de una matriz cuadrada que está en forma triangular y en forma canónica por renglones.

EJEMPLO A.9 Considere las matrices en forma escalonada en la figura A-4, cuyos elementos principales distintos de cero están en un círculo. (Los ceros precedentes y abajo del elemento principal distinto de cero en una matriz escalonada forman un patrón de "escalera", como remarca el sombreado.) La tercera matriz tiene la forma canónica de renglón. La segunda matriz no tiene la forma canónica de renglón porque la tercera columna no contiene un elemento principal distinto de cero y otro elemento distinto de cero. La primera matriz no tiene la forma canónica de renglón porque algunos elementos principales distintos de cero no son 1. La última matriz tiene forma triangular.

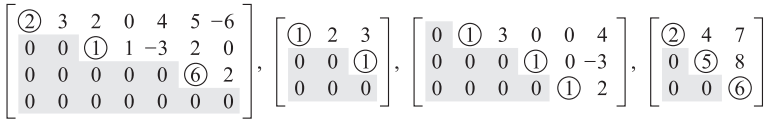


Figura A-4

Eliminación gaussiana en forma matricial

Considere cualquier matriz A. En la figura A-5 y en la figura A-6 se proporcionan dos algoritmos, el A-1 y el A-2, respectivamente. El primero transforma la matriz A en una forma escalonada (mediante operaciones elementales en los renglones) y el segundo transforma la matriz escalonada en una matriz en forma canónica en renglones. (Los dos algoritmos juntos se denominan *eliminación gaussiana.*)

Al final del algoritmo A-1, los elementos *pivote* (los elementos principales distintos de cero) son

$$a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$$

donde r denota el número de renglones distintos de cero en la matriz en forma escalonada.

Observación 1: El número $m = -\dfrac{a_{ij_1}}{a_{1j_1}} = -\dfrac{\text{coeficiente a eliminar}}{\text{pivote}}$ se denomina *multiplicador*.

Observación 2: La operación en el paso 1*b*) puede sustituirse por

"Sumar $-\,a_{ij_1}R_1$ a $a_{1j_1}R_i$"

Así se evitan fracciones en caso de que originalmente todos los escalares fuesen enteros.

EJEMPLO A.10 Encuentre la forma canónica por renglones de $A = \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 2 & 4 & -4 & 6 & 10 \\ 3 & 6 & -6 & 9 & 13 \end{bmatrix}$.

Primero se usa el algoritmo A-1 para reducir A a forma escalonada. En específico, como pivote se usa $a_{11} = 1$ para obtener ceros abajo de a_{11}; es decir, se aplican las operaciones en los renglones "Sumar $-2R_1$ a R_2" y "Sumar $-3R_1$ a R_3". Luego, como pivote se usa $a_{23} = 2$ para obtener ceros abajo de a_{23}; es decir, se aplica la operación "Sumar $-\frac{3}{2}R_2$ a R_3". Así se obtiene

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 3 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

Ahora la matriz A está en forma escalonada.

A continuación, se aplica el algoritmo A-2 para reducir aún más a A a la forma canónica por renglones. Específicamente, R_3 se multiplica por $-\frac{1}{2}$, de modo que el pivote es $a_{35} = 1$, y luego, se usa $a_{35} = 1$ como pivote para obtener ceros arriba de éste mediante las operaciones "Sumar $-6R_3$ a R_2" y "Sumar $-2R_3$ a R_1". Así se obtiene

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

R_2 se multiplica por $\frac{1}{2}$, de modo que el pivote es $a_{23} = 1$, y luego, como pivote se usa $a_{23} = 1$ para obtener ceros arriba de éste mediante la operación "Sumar $3R_1$ a R_1". Así se obtiene

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 7 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

La última matriz es la forma canónica por renglones de A.

Algoritmo A-1: (eliminación hacia delante): La entrada es una matriz arbitraria $A = [a_{ij}]$.

Paso 1. Se encuentra la primera columna con un elemento distinto de cero. De no haber una columna así, entonces EXIT. (Se tiene la matriz cero.) En caso contrario, sea j_1 el número de esta columna.

a) Se hace un nuevo arreglo de modo que $a_{1j_1} \neq 0$. Es decir, en caso de ser necesario, se intercambian renglones de modo que en el primer renglón en la columna j_1 haya un elemento distinto de cero.

b) Se usa a_{1j_1} como *pivote* para obtener ceros abajo de a_{1j_1}. Es decir, para $i > 1$:

1) Se hace $m = -a_{ij_1}/a_{1j_1}$.
2) Se suma aL_1 a L_i.

(Esto sustituye el renglón R_i por $-(a_{ij_1}/a_{1j_1})\, R_1 + R_j$.)

Paso 2. El paso 1 se repite con la submatriz formada por todos los renglones, excluyendo el primero. Aquí se deja que j_2 denote la primera columna en la submatriz con un elemento distinto de cero. Por tanto, al final del paso 2 se tiene $a_{2j_2} \neq 0$.

Paso 3 a r + 1. El proceso anterior se continúa hasta que la submatriz no tiene elementos distintos de cero.

Figura A-5

Con el paso final *r* del algoritmo A-2 en la figura A-6, el primer pivote cambia a 1.

Algoritmo A-2: (eliminación hacia atrás): La entrada es una matriz $A = [a_{ij}]$ en forma escalonada con elementos pivote $a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$.

Paso 1. *a*) El último renglón distinto de cero R_r se multiplica por $1/a_{rj_r}$ de modo que el pivote sea igual a 1.

b) Se usa $a_{rj_r} = 1$ para obtener ceros arriba del pivote. Es decir, para $i = r-1, r-2, \ldots, 1$:

1) Se hace $m = -a_{ij_r}$.
2) Se suma mR a R_i.

En otras palabras, se aplican las operaciones elementales en los renglones

"Sumar $-a_{ir_1}\, R_r$ a R_i"

(Esto sustituye el renglón R_i por $-a_{ir_1}R_r + R_i$.)

Paso 2 a r – 1. El paso 1 se repite en los renglones $R_{r-1}, R_{r-2}, \ldots, R_2$.

Paso r. R_i se multiplica por $1/a_{1j_1}$.

Figura A-6

Los algoritmos A-1 y A-2 muestran que cualquier matriz es equivalente por renglones a por lo menos una matriz en forma canónica por renglones. En realidad, en álgebra lineal se demuestra que una matriz así es única; se denomina *forma canónica por renglones* de *A*.

Teorema A-5: Cualquier matriz *A* es equivalente por renglones a una matriz única en forma canónica por renglones.

Solución matricial de un sistema de ecuaciones lineales

Considere un sistema *S* de ecuaciones lineales o, en forma equivalente, una ecuación matricial $AX = B$ con matriz aumentada $M = [A, B]$. El sistema se resuelve al aplicar a *M* el algoritmo de eliminación gaussiana recién estudiado, como sigue.

Parte A (*reducción*): la matriz aumentada M se reduce a forma escalonada. Si se presenta un renglón de la forma $(0, 0, \ldots, 0, b)$ con $b \neq 0$, entonces *parar*. El sistema no tiene solución.

Parte B (*sustitución hacia atrás*): la matriz aumentada M se reduce aún más a su forma canónica por renglones.

La solución única del sistema, o cuando la solución no es única, la forma de variables libres de la solución se obtiene fácilmente a partir de la forma canónica por renglones de M.

En el siguiente ejemplo se aplica el algoritmo anterior al sistema S con una solución única. Los casos en que S no tiene solución y donde S tiene una infinidad de soluciones se muestran en el problema A.23.

EJEMPLO A.11

Resuelva el sistema: $\begin{cases} x + 2y + z = 3 \\ 2x + 5y - z = -4 \\ 3x - 2y - z = 5 \end{cases}$

Su matriz aumentada M se reduce a forma escalonada y luego a forma canónica por renglones como sigue:

$$M = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 5 & -1 & -4 \\ 3 & -2 & -1 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & -8 & -4 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & -28 & -84 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Por tanto, el sistema tiene la solución única $x = 2$, $y = -1$, $z = 3$ o, en forma equivalente, el vector $u = (2, -1, 3)$. Observe que la forma escalonada de M ya indica que la solución es única, puesto que corresponde a un sistema triangular.

Inversa de una matriz de $n \times n$

La figura A-7 contiene el algoritmo A-3, que encuentra la inversa A^{-1} de cualquier matriz arbitraria de $n \times n$.

Algoritmo A-3: Encontrar la inversa de una matriz A de $n \times n$.

Paso 1. Se forma la matriz $M = [A, I]$ de $n \times 2n$; es decir, A está en la mitad izquierda de M y la matriz identidad I está en la mitad derecha de M.

Paso 2. M se reduce a la forma escalonada. Si durante el proceso se obtiene un renglón cero en la mitad A de M, entonces *parar* (A no tiene inversa). En caso contrario, la mitad A está ahora en forma triangular.

Paso 3. M se reduce aún más a la forma canónica por renglones

$$M \sim [I, B]$$

donde I ha sustituido a A en la mitad izquierda de M.

Paso 4. Sea $A^{-1} = B$, donde B es la matriz que ahora está en la mitad derecha de M.

Figura A-7

EJEMPLO A.12

Encuentre la inversa de $A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix}$.

Se forma la matriz $M = (A, I)$ y M se reduce a forma escalonada:

$$M = \left[\begin{array}{ccc:ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & -1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & 2 & 1 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 0 & -1 & -6 & 1 & 1 \end{array}\right]$$

Una vez en forma escalonada, la mitad izquierda de M está en forma triangular; por tanto, A es invertible. Luego, M se reduce aún más a forma canónica por renglones:

$$M \sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & -1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right]$$

La matriz identidad está en la mitad izquierda de la matriz final; por tanto la mitad derecha es A^{-1}. En otras palabras,

$$A^{-1} = \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix}$$

A.11 MATRICES BOOLEANAS (CERO-UNO)

Los *dígitos binarios* o *bits* son los símbolos 0 y 1. Considere las siguientes operaciones con estos dígitos:

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

Si estos bits se consideran como valores lógicos (0 que representa FALSO y 1 que representa VERDADERO), las operaciones anteriores corresponden, respectivamente, a las operaciones lógicas de OR ($\vee$) y AND ($\wedge$); es decir,

$\vee$	F	V
F	F	V
V	V	V

$\wedge$	F	V
F	F	F
V	F	V

(Las operaciones anteriores con 0 y 1 se denominan *operaciones booleanas,* puesto que también corresponden a las operaciones de un álgebra booleana analizadas en el capítulo 15.)

Ahora, sea $A = [a_{ij}]$ una matriz cuyos elementos son los bits 0 y 1 sujetos a las operaciones booleanas anteriores. Entonces A se denomina *matriz booleana*. El *producto booleano* de dos de estas matrices es el producto de costumbre, excepto que ahora se usan las operaciones booleanas de adición y multiplicación. Por ejemplo, si

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ y } B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \text{ entonces } AB = \begin{bmatrix} 0+0 & 1+1 \\ 0+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Resulta fácil demostrar que si A y B son matrices booleanas, entonces el producto booleano AB puede obtenerse al determinar el producto de costumbre de A y B y luego al sustituir cualquier dígito distinto de cero por 1.

PROBLEMAS RESUELTOS

VECTORES

A.1 Sean $u = (2, -7, 1)$, $v = (-3, 0, 4)$ y $w = (0, 5, -8)$. Encuentre: *a*) $3u - 4v$; *b*) $2u + 3v - 5w$.

Primero se efectúa la multiplicación por el escalar y luego la adición vectorial.

a) $3u - 4v = 3(2, -7, 1) - 4(-3, 0, 4) = (6, -21, 3) + (12, 0, -16) = (18, -21, -13)$.

b) $2u + 3v - 6w = 2(2, -7, 1) + 3(-3, 0, 4) - 5(0, 5, -8) = (4, -14, 2) + (-9, 0, 12) + (0, -25, 40)$
$= (-5, -39, 54)$.

A.2 Para el vector u, v, w en el problema A.1, encuentre *a*) $u \cdot v$; *b*) $u \cdot w$; *c*) $v \cdot w$.

Primero se multiplican las componentes correspondientes y luego se suma:

a) $u \cdot v = 2(-3) - 7(0) + 1(4) = -6 + 0 + 4 = -2$.

b) $u \cdot w = 2(0) - 7(5) + 1(-8) = 0 - 35 - 8 = -43$.

c) $v \cdot w = -3(0) + 0(5) + 4(-8) = 0 + 0 - 32 = -32$.

A.3 Encuentre $\|u\|$ donde: *a*) $u = (3, -12, -4)$; *b*) $u = (2, -3, 8, -7)$.

Primero se encuentra $\|u\|^2 = u \cdot u$ al elevar al cuadrado las componentes y sumar. Luego $\|u\| = \sqrt{\|u\|^2}$.

a) $\|u\|^2 = (3)^2 + (-12)^2 + (-4)^2 = 9 + 144 + 16 = 169$. Por tanto $\|u\| = \sqrt{169} = 13$.

b) $\|u\|^2 = 4 + 9 + 64 + 49 = 126$. Así que $\|u\| = \sqrt{126}$.

A.4 Encuentre x y y si $x(1, 1) + y(2, 1) = (1, 4)$.

Primero se multiplica por los escalares x y y y luego se suma:

$$x(1, 1) + y(2, -1) = (x, x) + (2y, -y) = (x + 2y, x - y) = (1, 4)$$

Dos vectores son iguales sólo cuando sus componentes correspondientes son iguales; por tanto, las componentes correspondientes se igualan unas a otras para obtener $x + 2y = 1$ y $x - y = 4$. Por último, se resuelve el sistema de ecuaciones para obtener $x = 3$ y $y = -1$.

A.5 Suponga que $u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix}$, $w = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$. Encuentre: *a*) $5u - 2v$; *b*) $-2u + 4v - 3w$.

a) $5u - 2v = 5\begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} - 2\begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \\ -20 \end{bmatrix} + \begin{bmatrix} 2 \\ -10 \\ -4 \end{bmatrix} = \begin{bmatrix} 27 \\ 5 \\ -24 \end{bmatrix}$.

b) $-2u + 4v - 3w = \begin{bmatrix} -10 \\ -6 \\ 8 \end{bmatrix} + \begin{bmatrix} -4 \\ 20 \\ 8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} -23 \\ 17 \\ 22 \end{bmatrix}$.

ADICIÓN DE MATRICES Y MULTIPLICACIÓN POR UN ESCALAR

A.6 Encuentre $2A - 3B$, donde $A = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 5 & -6 \end{bmatrix}$ y $B = \begin{bmatrix} 3 & 0 & 2 \\ -7 & 1 & 8 \end{bmatrix}$.

Primero se efectúan las multiplicaciones por los escalares y luego una adición de matrices:

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 8 & 10 & -12 \end{bmatrix} + \begin{bmatrix} -9 & 0 & -6 \\ 21 & -3 & -24 \end{bmatrix} = \begin{bmatrix} -7 & -4 & 0 \\ 29 & 7 & -36 \end{bmatrix}$$

(Observe que B se multiplica por -3 y luego se suma, en lugar de multiplicar B por 3 y restar. Así es posible evitar errores.)

A.7 Encuentre x, y, z, t donde $3\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} x & 6 \\ -1 & 2t \end{bmatrix} + \begin{bmatrix} 4 & x+y \\ z+t & 3 \end{bmatrix}$.

Primero, cada miembro se escribe como una matriz simple:

$$\begin{bmatrix} 3x & 3y \\ 3z & 3t \end{bmatrix} = \begin{bmatrix} x+4 & x+y+6 \\ z+t-1 & 2t+3 \end{bmatrix}$$

Las entradas correspondientes se igualan entre sí para obtener el sistema de cuatro ecuaciones.

$$3x = x+4, \quad 3y = x+y+6, \quad 3z = z+t = 1, \quad 3t = 2t+3$$

o

$$2x = 4, \quad 2y = 6+x, \quad 2z = t-1, \quad t = 3$$

La solución es $x = 2$, $y = 4$, $z = 1$, $t = 3$.

A.8 Demuestre el teorema A.1(v): $k(A+B) = kA + kB$.

Sean $A = [a_{ij}]$ y $B = [b_{ij}]$. Entonces la entrada ij de $A + B$ es $a_{ij} + b_{ij}$. Por tanto, $k(a_{ij} + b_{ij})$ es la entrada ij de $k(A + B)$. Por otra parte, las entradas ij de kA y kB son ka_{ij} y kb_{ij}, respectivamente. Así, $ka_{ij} + kb_{ij}$ es la entrada ij de $kA + kB$. Sin embargo, para escalares $k(a_{ij} + b_{ij}) = ka_{ij} + kb_{ij}$. Así, $k(A + B)$ y $kA + kB$ tienen las mismas entradas ij. En consecuencia, $k(A + B) = kA + kB$.

MULTIPLICACIÓN Y TRASPUESTA DE MATRICES

A.9 Calcule: *a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix}$; *b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix}$.

Las entradas correspondientes se multiplican y luego se suma:

a) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix} = 18 - 2 - 20 = -4$. *b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix} = 10 + 3 - 42 + 36 = 7$.

A.10 Sean $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ y $B = \begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix}$. Encuentre: *a*) AB; *b*) BA.

a) Puesto que A es de 2×2 y B es de 2×3, el producto AB está definido y es una matriz es de 2×3. Para obtener el primer renglón de AB, el primer renglón $[1, 3]$ de A se multiplica por las columnas $\begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ -2 \end{bmatrix}, \begin{bmatrix} -4 \\ 6 \end{bmatrix}$ de B, respectivamente:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 1(6)+3(3) & 1(0)+3(-2) & 1(-4)+3(6) \end{bmatrix}$$
$$= \begin{bmatrix} 2+9 & 0-6 & -4+18 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \end{bmatrix}$$

Para obtener las entradas del segundo renglón de AB, el segundo renglón $[2, -1]$ de A se multiplica por las columnas de B, respectivamente:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ 4-3 & 0+2 & -8-6 \end{bmatrix}$$

Así,

$$AB = \begin{bmatrix} 11 & -6 & 14 \\ 1 & 2 & -14 \end{bmatrix}$$

b) Observe que B es de 2×3 y que A es de 2×2. Puesto que los números internos, 3 y 2, no son iguales, entonces el producto BA no está definido.

A.11 Encuentre la traspuesta de cada matriz:

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 7 & 8 & -9 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}; \quad C = [1,\ -3,\ 5,\ -7]; \quad D = \begin{bmatrix} 2 \\ -4 \\ 6 \end{bmatrix}$$

Los renglones de cada matriz vuelven a escribirse como columnas para obtener las traspuestas de las matrices:

$$A^T = \begin{bmatrix} 1 & 7 \\ -2 & 8 \\ 3 & -9 \end{bmatrix}, \quad B^T = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}, \quad C^T = \begin{bmatrix} 1 \\ -3 \\ 5 \\ -7 \end{bmatrix}, \quad D^T = [2,\ -4,\ 6]$$

(Observe que $B^T = B$; se dice que esta matriz es *simétrica*. Observe también que la traspuesta del vector renglón C es un vector columna, y que la traspuesta del vector columna D es un vector renglón.)

A.12 Demuestre el teorema A.2 *i*): $A(BC) = A(BC)$.

Sean $A = [a_{ij}]$, $B = [b_{jk}]$ y $C = [c_{kl}]$. Además, sean $AB = S = [s_{ik}]$ y $BC = T = [t_{jl}]$.
Entonces

$$s_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk} = \sum_{j=1}^{m} a_{ij}b_{jk}$$
$$t_{jl} = b_{j1}c_{1i} + b_{j2}c_{2i} + \cdots + b_{jn}c_{nl} = \sum_{k=l}^{n} b_{jk}c_{kl}$$

Luego, al multiplicar S por C; es decir (AB) por C, el elemento en el renglón i y en la columna l de la matriz $(AB)C$ es

$$s_{i1}c_{1l} + s_{i2}c_{2l} + \cdots + s_{in}c_{nl} = \sum_{k=1}^{n} s_{ik}c_{kl} = \sum_{k=1}^{n}\sum_{j=1}^{m} (a_{ij}b_{jk})c_{kl}$$

Por otra parte, al multiplicar A por T; es decir A por BC, el elemento en el renglón i y en la columna j de la matriz $A(BC)$ es

$$a_{i1}t_{1l} + a_{i2}t_{2l} + \cdots + a_{im}t_{ml} = \sum_{j=1}^{m} a_{ij}t_{jl} = \sum_{k=1}^{m}\sum_{j=1}^{n} a_{ij}(b_{jk}c_{kl})$$

Puesto que las sumas anteriores son iguales, se ha demostrado el teorema.

MATRICES CUADRADAS, DETERMINANTES, INVERSAS

A.13 Encuentre la diagonal y la traza de cada una de las siguientes matrices:

$$a)\ A = \begin{bmatrix} 1 & 3 & 6 \\ 2 & -5 & 8 \\ 4 & -2 & 7 \end{bmatrix}; \quad b)\ B = \begin{bmatrix} t-2 & 3 \\ -4 & t+5 \end{bmatrix}; \quad c)\ C = \begin{bmatrix} 1 & 2 & -3 \\ 4 & -5 & 6 \end{bmatrix}.$$

a) La diagonal consiste de los elementos a_{11}, a_{22}, a_{33}; es decir, los escalares 1, -5, 7. La traza es la suma de los elementos en la diagonal; por tanto, $\text{tr}(A) = 1 - 5 + 7 = 3$.

b) La diagonal consiste del par $\{t-2, t+5\}$. Así $\text{tr}(B) = t - 2 + t + 5 = 2t + 3$.

c) La diagonal y la traza están definidas sólo para matrices cuadradas.

A.14 Sea $A = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}$. Encuentre: *a*) A^2; *b*) A^3; *c*) $f(A)$ donde $f(x) = 2x^3 - 4x + 5$; *d*) $g(A)$ donde $g(x) = x^2 + 2x - 11$.

$$a)\ A^2 = AA = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} = \begin{bmatrix} 1+8 & 2-6 \\ 4-12 & 8+9 \end{bmatrix} = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix}.$$

$$b)\ A^3 = AA^2 = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} = \begin{bmatrix} 9-16 & -4+34 \\ 36+24 & -16-51 \end{bmatrix} = \begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix}.$$

c) Calcule $f(A)$ al sustituir primero A por x y $5I$ por el término constante 5 en $f(x) = 2x^3 - 4x + 5$:

$$f(A) = 2A^3 - 4A + 5I = 2\begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix} - 4\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Luego, cada matriz se multiplica por su escalar respectivo:

$$f(A) = \begin{bmatrix} -14 & 60 \\ 120 & -134 \end{bmatrix} + \begin{bmatrix} -4 & -8 \\ -16 & 12 \end{bmatrix} + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

Por último, los elementos correspondientes en las matrices se suman:

$$f(A) = \begin{bmatrix} -14 & -4+5 & 60 & -8+0 \\ 120-16+0 & -134+12+5 \end{bmatrix} = \begin{bmatrix} -13 & 52 \\ 104 & -117 \end{bmatrix}$$

d) Calcule $g(A)$ al sustituir primero A por x y $11I$ por el término constante 11 en $g(x) = x^2 + 2x - 11$:

$$g(A) = A^2 + 2A - 11I = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + 2\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} - 11\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ 8 & -6 \end{bmatrix} + \begin{bmatrix} -11 & 0 \\ 0 & -11 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

[Puesto que $g(A) = 0$, la matriz A es un cero del polinomio $g(x)$].

A.15 Calcule cada determinante: *a*) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix}$; *b*) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix}$.

a) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix} = 4(-2) - (-3)(5) = -8 + 15 = 7.$

b) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix} = (a-b)(a+b) - b^2 = a^2 - b^2 - b^2 = a^2 - 2b^2.$

A.16 Encuentre el determinante de cada matriz:

$$a)\ A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{bmatrix}; \quad b)\ B = \begin{bmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{bmatrix}; \quad c)\ C = \begin{bmatrix} 2 & -3 & 4 \\ 1 & 2 & -3 \\ -1 & -2 & 5 \end{bmatrix}$$

(Sugerencia: use el diagrama en la figura A-3*b*):

a) $|A| = 2 + 0 + 60 - 0 - 15 + 8 = 55$

b) $|B| = 8 + 15 + 0 + 20 + 24 + 0 = 67$

c) $|C| = 20 - 9 - 8 + 8 - 12 + 15 = 14$

A.17 Encuentre la inversa de: *a*) $A = \begin{bmatrix} 5 & 3 \\ 4 & 2 \end{bmatrix}$; *b*) $B = \begin{bmatrix} -2 & 6 \\ 3 & -9 \end{bmatrix}$.

Use la fórmula en la sección A.9.

a) Primero se encuentra $|A| = 5(2) - 3(4) = 10 - 12 = -2$. Luego se intercambian los elementos en la diagonal, se toman los negativos de los elementos que no están en la diagonal y se multiplica por $1/|A|$:

$$A^{-1} = -\frac{1}{2}\begin{bmatrix} 2 & -3 \\ -4 & 5 \end{bmatrix} = \begin{bmatrix} -1 & \frac{3}{2} \\ 2 & -\frac{5}{2} \end{bmatrix}$$

b) Primero se encuentra $|B| = -2(-9) - 6(3) = 18 - 18 = 0$. Puesto que $|B| = 0$, B no tiene inversa.

A.18 Encuentre la inversa de: *a*) $A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -3 & 6 \\ 1 & 1 & 7 \end{bmatrix}$; *b*) $B = \begin{bmatrix} 1 & 3 & -4 \\ 1 & 5 & -1 \\ 3 & 13 & -6 \end{bmatrix}$.

a) Se forma la matriz $M = [A, I]$ y M se reduce por renglones a forma escalonada:

$$M = \left[\begin{array}{ccc:ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 2 & -3 & 6 & 0 & 1 & 0 \\ 1 & 1 & 7 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 3 & 5 & -1 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & -1 & 5 & -3 & 1 \end{array}\right]$$

En forma escalonada, la mitad izquierda de M está en forma triangular; por tanto, A tiene inversa. M se reduce aún más a forma canónica por renglones:

$$M = \left[\begin{array}{ccc:ccc} 1 & -2 & 0 & 11 & -6 & 2 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 27 & -16 & 6 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right]$$

La matriz final tiene la forma $[I, A^{-1}]$; es decir, A^{-1} es la mitad derecha de la última matriz. Así,

$$A^{-1} = \begin{bmatrix} 27 & -16 & 6 \\ 8 & -5 & 2 \\ -5 & 3 & -1 \end{bmatrix}$$

b) Se forma la matriz $M = [B, I]$ y luego M se reduce a forma escalonada:

$$M = \left[\begin{array}{ccc:ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 1 & 5 & -1 & 0 & 1 & 0 \\ 3 & 13 & -6 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 4 & 6 & -3 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc:ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -2 & 1 \end{array}\right]$$

En forma escalonada, M tiene un renglón cero en su mitad izquierda; es decir, B ahora ya no es reducible por renglones a forma triangular. En consecuencia, B no tiene inversa.

MATRICES ESCALONADAS, REDUCCIÓN POR RENGLONES, ELIMINACIÓN GAUSSIANA

A.19 Intercambie renglones en cada matriz para obtener una matriz escalonada:

$$a) \begin{bmatrix} 0 & 1 & -3 & 4 & 6 \\ 4 & 0 & 2 & 5 & -3 \\ 0 & 0 & 7 & -2 & 8 \end{bmatrix}; \quad b) \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 5 & -4 & 7 \end{bmatrix}; \quad c) \begin{bmatrix} 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

a) Se intercambian los renglones primero y segundo.

b) El renglón cero se lleva a la parte inferior de la matriz.

c) Ningún número de intercambio de renglones puede producir una matriz escalonada.

A.20 Reduzca por renglones la matriz $A = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 2 & 4 & -2 & 2 \\ 3 & 6 & -4 & 3 \end{bmatrix}$ a forma escalonada.

Se usa a_{11} como pivote para obtener ceros abajo de a_{11}, es decir, se aplican las operaciones en renglones "Sumar $-2R_1$ a R_2" y "Sumar $-3R_1$ a R_3"; y luego como pivote se usa $a_{23} = 4$ para obtener un cero abajo de a_{23}, es decir, al aplicar la operación en renglón "Sumar $-5R_2$ a $4R_3$". Estas operaciones producen lo siguiente, donde la última matriz está en forma escalonada:

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 5 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

A.21 ¿Cuál de las siguientes matrices está en forma canónica por renglones?

$$\begin{bmatrix} 1 & 2 & -3 & 0 & 1 \\ 0 & 0 & 5 & 2 & -4 \\ 0 & 0 & 0 & 7 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 7 & -5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 5 & 0 & 2 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 7 \end{bmatrix}$$

La primera matriz no está en forma canónica por renglones ya que, por ejemplo, dos elementos principales distintos de cero son 5 y 7, no 1. También hay elementos distintos de cero arriba de los elementos principales distintos de cero 5 y 7. Las matrices segunda y tercera están en forma canónica por renglones.

A.22 Reduzca la matriz $A = \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 1 & 1 & 4 & -1 & 3 \\ 2 & 5 & 9 & -2 & 8 \end{bmatrix}$ a forma canónica por renglones.

Primero, A se reduce a forma escalonada aplicando las operaciones "Sumar $-R_1$ a R_2" y "Sumar $-2R_1$ a R_3", y luego la operación "Sumar $-3R_2$ a R_3". Estas operaciones producen

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 9 & 3 & -4 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Luego se usa sustitución hacia atrás en la matriz en forma escalonada para obtener la forma canónica por renglones de A. Específicamente, primero se multiplica R_3 por $\frac{1}{2}$ para obtener el pivote $a_{34} = 1$, y luego se aplican las operaciones "Sumar $2R_3$ a R_2" y "Sumar $-R_3$ a R_1 Estas operaciones producen

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 3 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Luego, R_2 se multiplica por $\frac{1}{3}$ para obtener el pivote $a_{22} = 1$, y después se aplica la operación "Sumar $2R_2$ a R_1". Se obtiene

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \frac{11}{3} & 0 & \frac{17}{6} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Puesto que $a_{11} = 1$, la última matriz es la forma canónica por renglones deseada de A.

A.23 Resuelva cada sistema usando su matriz aumentada M:

$$a) \quad \begin{aligned} x + y - 2z + 4t &= 5 \\ 2x + 2y - 3z + t &= 4 \\ 3x + 3y - 4z - 2t &= 3 \end{aligned} \qquad b) \quad \begin{aligned} x - 2y + 4z &= 2 \\ 2x - 3y + 5z &= 3 \\ 3x - 4y + 6z &= 7 \end{aligned}$$

a) Su matriz aumentada M se reduce a forma escalonada y luego a forma canónica por renglones:

$$M = \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 2 & 2 & -3 & 1 & 4 \\ 3 & 3 & -4 & -2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 0 & 0 & 1 & -7 & -6 \\ \cancel{0} & \cancel{0} & \cancel{2} & \cancel{14} & \cancel{12} \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & -10 & -7 \\ 0 & 0 & 1 & -7 & -6 \end{bmatrix}$$

(El tercer renglón de la segunda matriz se ha eliminado puesto que es un múltiplo del segundo renglón y podría originar un renglón cero.)

Se escribe el sistema correspondiente a la forma canónica por renglones de M y luego las variables libres se transfieren al otro miembro para obtener la forma de variables libres de la solución:

$$\begin{aligned} x + y - 10t &= -7 \\ z - 7t &= -6 \end{aligned} \quad \text{y entonces} \quad \begin{aligned} x &= -7 - y + 10t \\ z &= -6 + 7t \end{aligned}$$

Aquí x y z son las variables básicas y y y t son las variables libres.

La forma *paramétrica* de la solución puede obtenerse al igualar las variables libres a los *parámetros*; por ejemplo, $y = a$ y $t = b$. Este proceso produce $x = -7 - a + 10b$, $y = a$, $z = -6 + 7b$, $t = b$ o $u = (-7 - a + 10b, a - 6 + 7b, b)$ (que es otra forma de la solución).

Puede obtenerse una *solución particular* al asignar valores arbitrarios a las variables libres (o parámetros) y despejando las variables básicas mediante cualquier forma de la solución general. Por ejemplo, al hacer $y = 2$, $t = 3$, se obtiene $x = 21$, $z = 15$. Así, a continuación se presenta una solución particular del sistema:

$$x = 21, \quad y = 2, \quad z = 15, \quad t = 3 \quad \text{o} \quad u = (21, 2, 15, 3)$$

b) Primero, la matriz aumentada M se reduce por renglones a su forma escalonada:

$$M = \begin{bmatrix} 1 & -2 & 4 & 2 \\ 2 & -3 & 5 & 3 \\ 3 & -4 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 2 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

En forma escalonada, el tercer renglón corresponde a la ecuación degenerada $0x + 0y + 0z = 3$.

Por tanto, el sistema no tiene solución. (Observe que la forma escalonada indica si el sistema tiene solución o no.)

PROBLEMAS DIVERSOS

A.24 Sean $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ y $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ matrices booleanas. Encuentre los productos booleanos AB, BA y A^2.

Se encuentra el producto matricial de costumbre y luego 1 se sustituye por cualquier escalar distinto de cero. Así:

$$AB = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}; \quad BA = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

A.25 Sea $A = \begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}$. *a*) Encuentre un vector columna $u = \begin{bmatrix} x \\ y \end{bmatrix}$ distinto de cero tal que $Au = 3u$. *b*) Describa todos los vectores similares.

a) Primero se plantea la ecuación matricial $Au = 3u$ y luego cada miembro se escribe como una matriz simple (vector columna):

$$\begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = 3\begin{bmatrix} x \\ y \end{bmatrix} \quad \text{y} \quad \begin{bmatrix} x + 3y \\ 4x - 3y \end{bmatrix} = \begin{bmatrix} 3x \\ 3y \end{bmatrix}$$

Los elementos correspondientes se igualan entre sí para obtener un sistema de ecuaciones y el sistema se reduce a forma escalonada:

$$\begin{matrix} x + 3y = 3x \\ 4x - 3y = 3y \end{matrix} \quad \text{o} \quad \begin{matrix} 2x - 3y = 0 \\ 4x - 6y = 0 \end{matrix} \quad \text{para} \quad \begin{matrix} 2x - 3y = 0 \\ 0 = 0 \end{matrix} \quad \text{o} \quad 2x - 3y = 0$$

El sistema se reduce a una ecuación lineal (no degenerada) con dos incógnitas, de modo que tiene una infinidad de soluciones. Para obtener una solución distinta de cero se hace $y = 2$, por ejemplo; entonces $x = 3$. Así, una solución deseada distinta de cero es $u = [3, 2]^T$.

b) Para encontrar la solución general, se hace $y = a$, donde a es un parámetro. $y = a$ se sustituye en $2x - 3y = 0$ para obtener $x = 3a/2$. Así, $u = [3a/2, a]^T$ representa todas estas soluciones. En forma alterna, sea $y = 2b$, de modo que $v = [3b, 2b]$ representa todas estas soluciones.

PROBLEMAS SUPLEMENTARIOS

VECTORES

A.26 Sea $u = (2, -1, 0, -3)$, $v = (1, -1, -1, 3)$, $w = (1, 3, -2, 2)$. Encuentre: *a*) $2u - 3v$; *b*) $5u - 3v - 4w$; *c*) $-u + 2v - 2w$; *d*) $u \cdot v$, $u \cdot w$, $v \cdot w$, *e*) $\|u\|$, $\|v\|$, $\|w\|$.

A.27 Sea $u = \begin{bmatrix} 1 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}$, $w = \begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$. Encuentre: *a*) $5u - 3v$; *b*) $2u + 4v - 6w$; *c*) $u \cdot v$, $u \cdot w$, $v \cdot w$; *d*) $\|u\|$, $\|v\|$, $\|\mathrm{w}\|$.

A.28 Encuentre x y y donde *a*) $x(2, 5) + y(4, -3) = (8, 33)$; *b*) $x(1, 4) + y(2, -5) = (7, 2)$.

OPERACIONES CON MATRICES

A.29 Sea $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 0 \\ -6 & 7 \end{bmatrix}$, $C = \begin{bmatrix} 1 & -3 & 4 \\ 2 & 6 & -5 \end{bmatrix}$, $D = \begin{bmatrix} 3 & 7 & -1 \\ 4 & -8 & 9 \end{bmatrix}$. Encuentre:

a) $5A - 2B$ y $2C - 3D$; *c*) AC y AD; *e*) A^T y C^T;
b) AB y BA; *d*) BC y BD; *f*) A^2, B^2, C^2.

A.30 Sea $A = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 4 & 0 & -3 \\ -1 & -2 & 3 \end{bmatrix}$, $C = \begin{bmatrix} 2 & -3 & 0 & 1 \\ 5 & -1 & -4 & 2 \\ -1 & 0 & 0 & 3 \end{bmatrix}$, $D = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}$.

Encuentre: *a*) $3A - 4B$; *b*) AB, AC, AD; *c*) BC, BD, CD; *d*) A^T y A^TB.

A.31 Sea $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$. Encuentre una matriz B de 2×2 con entradas diferentes tal que $AB = 0$.

MATRICES CUADRADAS

A.32. Encuentre la diagonal y la traza de *a*) $A = \begin{bmatrix} 2 & -7 & 8 \\ 3 & -6 & -5 \\ 4 & 0 & -1 \end{bmatrix}$; *b*) $B = \begin{bmatrix} 1 & 2 & -9 \\ -3 & 2 & 8 \\ 5 & -6 & -1 \end{bmatrix}$.

A.33 Sea $A = \begin{bmatrix} 2 & -5 \\ 3 & 1 \end{bmatrix}$. Encuentre: *a*) A^2 y A^3; *b*) $f(A)$ donde $f(x) = x^3 - 2x^2 - 5$.

A.34 Sea $B = \begin{bmatrix} 4 & -2 \\ 1 & -6 \end{bmatrix}$. Encuentre: *a*) B^2 y B^3; *b*) $f(B)$ donde $f(x) = x^2 + 2x - 22$.

A.35 Sea $A = \begin{bmatrix} 6 & -4 \\ 3 & -2 \end{bmatrix}$. Encuentre un vector distinto de cero $u = \begin{bmatrix} x \\ y \end{bmatrix}$ tal que $Au = 4u$.

DETERMINANTES E INVERSAS

A.36 Encuentre cada determinante: *a*) $\begin{vmatrix} 2 & 5 \\ 4 & 1 \end{vmatrix}$; *b*) $\begin{vmatrix} 6 & 1 \\ 3 & -2 \end{vmatrix}$; *c*) $\begin{vmatrix} -2 & 8 \\ -5 & -2 \end{vmatrix}$; *d*) $\begin{vmatrix} a-b & a \\ a & a+b \end{vmatrix}$.

A.37 Calcule el determinante de cada una de las matrices en el problema A.32.

A.38 Encuentre la inversa de *a*) $A = \begin{bmatrix} 7 & 4 \\ 5 & 3 \end{bmatrix}$; *b*) $B = \begin{bmatrix} 5 & -2 \\ 6 & -3 \end{bmatrix}$; *c*) $C = \begin{bmatrix} 4 & -6 \\ -2 & 3 \end{bmatrix}$.

A.39 Encuentre la inversa de cada matriz (en caso de existir):

$$A = \begin{bmatrix} 1 & 2 & -4 \\ -1 & -1 & 5 \\ 2 & 7 & -3 \end{bmatrix}; \quad B = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 2 & -2 \\ 1 & 3 & -1 \end{bmatrix}; \quad C = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & -1 \\ 5 & 12 & 1 \end{bmatrix}.$$

MATRICES EN FORMA ESCALONADA, REDUCCIONES POR RENGLONES, ELIMINACIÓN GAUSSIANA

A.40 Reduzca A a forma escalonada y luego a forma canónica por renglones, donde:

a) $A = \begin{bmatrix} 1 & 2 & -1 & 2 & 1 \\ 2 & 4 & 1 & -2 & 3 \\ 3 & 6 & 2 & -6 & 5 \end{bmatrix}$; *b*) $A = \begin{bmatrix} 2 & 3 & -2 & 5 & 1 \\ 3 & -1 & 2 & 0 & 4 \\ 4 & -5 & 6 & -5 & 7 \end{bmatrix}$.

A.41 Use sólo ceros y unos para enumerar todas las matrices de 2×2 en forma escalonada.

A.42 Use sólo ceros y unos para encontrar las matrices de 3×3 en forma canónica por renglones.

A.43 Resuelva cada uno de los siguientes sistemas:

a) $\begin{aligned} x + 2y - 4z &= -3 \\ 2x + 6y - 5z &= 2 \\ 3x + 11y - 4z &= 12 \end{aligned}$ *b*) $\begin{aligned} x + 2y - 4z &= 3 \\ 2x + 6y - 5z &= 10 \\ 3x + 10y - 6z &= 14 \end{aligned}$

A.44 Resuelva cada uno de los siguientes sistemas:

a) $\begin{aligned} x - 3y + 2z - t &= 2 \\ 3x - 9y + 7z - t &= 7 \\ 2x - 6y + 7z + 4t &= 7 \end{aligned}$ *b*) $\begin{aligned} x + 2y + 3z &= 7 \\ x + 3y + z &= 6 \\ 2x + 6y + 5z &= 15 \\ 3x + 10y + 7z &= 23 \end{aligned}$

PROBLEMAS DIVERSOS

A.45 Sea $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. Encuentre: *a*) A^n; *b*) A^{-1}; *c*) matriz B tal que $B^2 = A$.

A.46 Se dice que las matrices A y B conmutan si $AB = BA$. Encuentre todas las matrices $\begin{bmatrix} x & y \\ z & t \end{bmatrix}$ que conmutan con $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

A.47 Sean $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ y $B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ matrices booleanas.

Encuentre las matrices booleanas *a*) $A + B$; *b*) AB; *c*) BA; *d*) A^2; *e*) B^2.

Respuestas a los problemas suplementarios

Notación: $M = [R_1; R_2; \ldots; R_n]$ denota una matriz con renglones $R_1, \ldots, R_n$.

A.26 *a*) (1, 1, 3, −15); *b*) (3, −14, 11, −32); *c*) (−2, −7, 2, 5); *d*) −6, −7, 6; *e*) $\sqrt{14}$, $\sqrt{12} = 2\sqrt{3}$, $\sqrt{18} = 3\sqrt{2}$.

A.27 *a*) $[-1, 12, -35]^T$; *b*) $[-8, 22, -24]^T$; *c*) −15, −27, 34; *d*) $\sqrt{26}$, $\sqrt{30}$, 7.

A.28 *a*) $x = 6, y = -1$; *b*) $x = 3, y = 2$.

A.29 *a*) [−5, 10; 27, −34], [−7, 27, 11; −8, 36, −37]; *b*) [−7, 14; 39, −28], [5, 10; 15, −40]; *c*) [5, 9, −6; −5, −33, 32], [11, −9, 17; −7, 53, 39]; *d*) [5, −15, 20; 8, 60, −59], [15, 35, −5; 10, −98, 69]; *e*) [1, 3; 2, −4], [1, 2; −3, 6; 4, −5]; *f*) [7, −6; −9, 22], [25, 0; −72, 49], C^2 no está definida.

A.30 *a*) [−13, −3, 18; 4, 17, 0]; *b*) AB no está definida, [−5, −2, 4, 5; 11, −3, −12, 18], [9; 9]; *c*) [11, −12, 0, −5; −15, 5, 8, 4], [−1; 9], CD no está definida; *d*) [1, 0; −1, 3; 2, 4], [4, 0, −3; −7, −6, 12; 4, −8, 6].

A.31 [2, 4, 6; −1, −2, −3]

A.32 *a*) [2, −6, −1], −5; *b*) [1, 2, −1], 2

A.33 *a*) [−11, −15; 9, −14], [−67, 40; −24, −59]; *b*) [−50, 70; −42, −36].

A.34 *a*) [14, 4; −2, 34], [60, −52; 26, −200] *b*) $f(B) = 0$.

A.35 [2*a*; *a*], para *a* arbitraria distinta de cero.

A.36 *a*) −18; *b*) −15; *c*) 44; *d*) $-b^2$.

A.37 *a*) 323; *b*) 48.

A.38 *a*) [3, −4; −5, 7]; *b*) [1, −2/3; 2, −5/3]; *c*) No está definida.

A.39 *a*) [−16, −11, 3; 7/2, 5/2, −1/2; −5/2, −3/2, 1/2]; *b*) [1, 1/2, 0; −1/2, −1/2, 1/2; −1/2, −1, 1/2]; *c*) No está definida.

A.40 *a*) [1, 2, −1, 2, 1; 0, 0, 3, −6, 1; 0, 0, 0, −6, 1], **[1,** 2, 0, 0, 4/3; 0, 0, 1, 0, 0; 0, 0, 0, 1, −1/6]; *b*) [2, 3, −2, 5, 1; 0, −11, 10, −15, 5; 0, . . . , 0], [1, 0, 4/11, 5/11, 13/11; 0, 1, −10/11, 15/11, −5/11; 0, . . . , 0]

A.41 [1, 1; 0, 1], [1, 1; 0, 0], [1, 0; 0, 0], [0, 1; 0, 0], **[0,** 0; 0, 0], [1, 0; 0, 1]

A.42 Hay 13.

A.43 *a*) $x = 3, y = 1, z = 2$; *b*) No hay solución.

A.44 *a*) $x = 3y + 5t, z = 1 - 2t$; *b*) $x = 2, y = 1, z = 1$.

A.45 *a*) [1, 2*n*; 0, 1]; *b*) [1, −2; 0, 1]; *c*) [1, 1; 0, 1].

A.46 [*a*, *b*; 0, *a*]

A.47 *a*) [110; 101; 111]; *b*) [100; 111; 100]; *c*) [010; 010; 101]; *d*) [101; 110; 010]; *e*) [100; 100; 111].

B Sistemas algebraicos

APÉNDICE

B.1 INTRODUCCIÓN

En este apéndice se investigan algunos de los sistemas algebraicos más importantes en matemáticas: semigrupos, grupos, anillos y campos. También se definen los conceptos de homomorfismo y estructura cociente. Se empieza con la definición formal de una operación y se estudian varios tipos de operaciones.

B.2 OPERACIONES

El lector ya está familiarizado con las operaciones de suma y multiplicación de números, unión e intersección de conjuntos y composición de funciones. Estas operaciones se denotan como sigue:

$$a + b = c, \quad a \cdot b = c, \quad A \cup B = C, \quad A \cap B = C, \quad g \circ f = h.$$

En cada situación, un elemento (c, C o h) se asigna a un par original de elementos. A continuación se precisa esta idea.

Definición B.1: Sea S un conjunto no vacío. Una *operación* sobre S es una función $*$ de $S \times S$ en S. En este caso, en lugar de $*$ (a, b) suele escribirse

$$a * b \text{ o algunas veces } ab$$

El conjunto S y una operación $*$ en S se denotan por $(S, *)$, o simplemente por S cuando se sobrentiende la operación.

Observación: Una operación $*$ de $S \times S$ en S algunas veces se denomina *operación binaria*. Una operación *unaria* es una función de S en S. Por ejemplo, el valor absoluto $|n|$ de un entero n es una operación unaria en $\mathbf{Z}$, y el complemento A^C de un conjunto A es una operación unaria en el conjunto potencia $P(X)$ de un conjunto X. Una operación *ternaria* es una función de $S \times S \times S$ en S. En términos generales, una operación n-aria es una función de $S \times S \cdots \times S$ (n factores) en S. A menos que se establezca otra cosa, la palabra operación significa operación binaria. También se supondrá que el conjunto S en cuestión no es vacío.

Suponga que S es un conjunto finito. Entonces una operación $*$ en S puede presentarse mediante su tabla de operación (de multiplicar), donde la entrada en el renglón identificado por a y la columna identificada por b es $a * b$.

Suponga que S es un conjunto con una operación $*$, y suponga que A es un subconjunto de S. Entonces se dice que A es *cerrado bajo* $*$ si $a * b$ pertenece a A para elementos a y b arbitrarios en A.

EJEMPLO B.1 Considere el conjunto **N** de enteros positivos.

a) La adición ($+$) y la multiplicación ($\times$) son operaciones en **N**. Sin embargo, la sustracción ($-$) y la división ($/$) no son operaciones en **N** puesto que la diferencia y el cociente de enteros positivos no necesariamente son enteros positivos. Por ejemplo, $2 - 9$ y $7/3$ no son enteros positivos.

b) Sean A y B los conjuntos, respectivamente, de enteros positivos pares e impares. Entonces A es cerrado bajo la adición y la multiplicación, puesto que la adición y el producto de números pares son pares. Por otra parte, B es cerrado bajo la multiplicación pero no bajo la adición puesto que, por ejemplo, $3 + 5 = 8$ es par.

EJEMPLO B.2 Sea $S = \{a, b, c, d\}$. Las tablas en la figura B-1 definen las operaciones $*$ y $\cdot$ en S. Observe que $*$ puede definirse mediante la siguiente operación, donde x y y son elementos arbitrarios de S:

$$x * y = x$$

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

a)

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	a	b
c	c	b	a	a
d	d	a	a	a

b)

Figura B-1

A continuación se enumeran varias propiedades importantes de las operaciones.

Ley asociativa:

Se dice que una operación $*$ en un conjunto S es *asociativa* o que satisface la *ley asociativa* si, para elementos arbitrarios a, b y c en S, se tiene

$$(a * b) * c = a * (b * c)$$

En términos generales, si una operación no es asociativa, entonces puede haber varios modos de formar el producto. Por ejemplo, en seguida aparecen cinco modos de formar $abcd$:

$$((ab)c)d, \quad (ab)(cd), \quad (a(bc))d, \quad a((bc)d), \quad a(b(cd))$$

Si la operación es asociativa, entonces el siguiente teorema (que se demuestra en el problema B.4) es válido.

Teorema B.1: Suponga que $*$ es una operación asociativa en un conjunto S. Entonces cualquier producto $a_1 * a_2 * \cdots * a_n$ no requiere paréntesis; es decir, todos los productos posibles son iguales.

Ley conmutativa:

Se dice que una operación $*$ en un conjunto S es *conmutativa* o que satisface la *ley conmutativa* si, para elementos arbitrarios a y b en S,

$$a * b = b * a$$

EJEMPLO B.3

a) Considere el conjunto **Z** de enteros. La adición y la multiplicación de enteros son asociativas y conmutativas. Por otra parte, la sustracción no es asociativa. Por ejemplo,

$$(8 - 4) - 3 = 1 \quad \text{pero} \quad 8 - (4 - 3) = 7$$

Además, la sustracción no es conmutativa puesto que, por ejemplo, $3 - 7 \neq 7 - 3$.

b) Considere la operación multiplicación de matrices en el conjunto M de matrices cuadradas n. Puede demostrarse que la multiplicación de matrices es asociativa. Por otra parte, la multiplicación de matrices no es conmutativa. Por ejemplo,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{pero} \quad \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

Elemento identidad:

Considere una operación $*$ en un conjunto S. Un elemento e en S se denomina elemento *identidad* para $*$ si, para cualquier elemento a en S,

$$a * e = e * a = a$$

En términos más generales, un elemento e se denomina *identidad izquierda* o *identidad derecha* según sea el caso si $e * a = a$ o $a * e = a$, donde a es cualquier elemento en S. El siguiente teorema es válido.

Teorema B.2: Suponga que e es una identidad izquierda y que f es una identidad derecha para una operación en un conjunto S. Entonces $e = f$.

La demostración es muy fácil. Puesto que e es una identidad izquierda, $ef = f$; pero como f es una identidad derecha, $ef = e$. Así, $e = f$. Este teorema establece que, en particular, un elemento identidad es único, y si una operación tiene más de una identidad izquierda, entonces no tiene identidad derecha y viceversa.

Inversos:

Suponga que una operación $*$ en un conjunto S tiene un elemento identidad e. El *inverso* de un elemento a en S es un elemento b tal que

$$a * b = b * a = e$$

Si la operación es asociativa, entonces el inverso de a, en caso de existir, es único (problema B.2). Observe que si b es el inverso de a, entonces a es el inverso de b. Por tanto, la relación inverso es simétrica, y puede afirmarse que los elementos a y b son inversos entre sí.

Notación: Si la operación en S se denota por $a * b$, $a \times b$, $a \cdot b$, o ab, entonces se dice que S está escrito *en forma multiplicativa* o *multiplicativamente* y el inverso de un elemento $a \in S$ suele denotarse por a^{-1}. Algunas veces, cuando S es conmutativo, la operación se denota por $+$ y entonces se dice que S está escrito *aditivamente*. En este caso, el elemento identidad suele denotarse por 0 y se denomina elemento *cero*; y el inverso se denota por $-a$ y se denomina *negativo* de a.

EJEMPLO B.4 Considere los números racionales **Q**. Bajo la adición, 0 es el elemento identidad y -3 y 3 son inversos (aditivos), puesto que

$$(-3) + 3 = 3 + (-3) = 0$$

Por otra parte, bajo la multiplicación, 1 es el elemento identidad y -3 y $-1/3$ son inversos (multiplicativos), puesto que

$$(-3)(-1/3) = (-1/3)(-3) = 1$$

Observe que 0 no tiene inverso multiplicativo.

Leyes de cancelación:

Se dice que una operación $*$ en un conjunto S satisface la *ley de cancelación izquierda* o la *ley de cancelación derecha* según sea el caso:

$$a * b = a * c \text{ implica } b = c \quad \text{o} \quad b * a = c * a \text{ implica } b = c$$

La adición y la sustracción de enteros en **Z** y la multiplicación de enteros distintos de cero en **Z** satisfacen las leyes de cancelación izquierda y derecha. Por otra parte, la multiplicación de matrices no satisface las leyes de cancelación. Por ejemplo, suponga

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & -3 \\ 1 & 5 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

Entonces $AB = AC = D$, pero $B \neq C$.

B.3 SEMIGRUPOS

Sea S un conjunto no vacío con una operación. Entonces S se denomina *semigrupo* si la operación es asociativa. Si la operación también tiene un elemento identidad, S se denomina *monoide*.

EJEMPLO B.5

a) Considere los enteros positivos **N**. Entonces, (**N**, $+$) y (**N**, $\times$) son semigrupos puesto que la adición y la multiplicación en **N** son asociativas. En particular, (**N**, $\times$) es un monoide, ya que tiene al elemento identidad 1. Sin embargo, (**N**, $+$) no es un monoide, puesto que la adición en **N** no tiene elemento cero.

b) Sea S un conjunto finito y sea $F(S)$ la colección de todas las funciones $f : S \to S$ bajo la operación de composición de funciones. Puesto que la composición de funciones es asociativa, $F(S)$ es un semigrupo. De hecho, $F(S)$ es un monoide, ya que la función identidad es un elemento identidad para $F(S)$.

c) Sea $S = \{a, b, c, d\}$. Las tablas de multiplicación en la figura B-1 definen las operaciones $*$ y $\cdot$ en S. Observe que $*$ puede definirse mediante la fórmula $x * y = x$ para cualesquiera x y y en S. Por tanto

$$(x * y) * z = x * z = x \quad \text{y} \quad x * (y * z) = x * y = x$$

En consecuencia, $*$ es asociativa y así $(S, *)$ es un semigrupo. Por otra parte, $\cdot$ no es asociativa puesto que, por ejemplo,

$$(b \cdot c) \cdot c = a \cdot c = c \quad \text{pero} \quad b \cdot (c \cdot c) = b \cdot a = b$$

Así, $(S, \cdot)$ no es un semigrupo.

Semigrupo libre, monoide libre

Sea A un conjunto no vacío. Una *palabra* w en A es una secuencia finita de sus elementos. Por ejemplo, las siguientes expresiones son palabras en $A = \{a, b, c\}$:

$$u = ababbbb = abab^4 \quad \text{y} \quad v = baccaaaa = bac^2a^4$$

(Se escribe a^2 por aa, a^3 por aaa, y así sucesivamente.) La *longitud* de una palabra w, denotada por $l(w)$, es el número de elementos en w. Así, $l(u) = 7$ y $l(v) = 8$.

La concatenación de las palabras u y v en un conjunto A, que se escribe $u * v$ o uv, es la palabra obtenida al escribir los elementos de u seguidos por los elementos de v. Por ejemplo,

$$uv = (abab^4)(bac^2a^4) = abab^5c^2a^4$$

Ahora, sea $F = F(A)$ la colección de todas las palabras en A bajo la operación de concatenación. Resulta evidente que para palabras arbitrarias u, v, w, las palabras $(uv)w$ y $u(vw)$ son idénticas; simplemente consisten de los elementos de u, v, w escritos uno después del otro. Así, F es un semigrupo; se denomina *semigrupo libre* de A, y los elementos de A se denominan *generadores* de F.

La secuencia vacía, denotada por λ, también se considera una palabra en A. Sin embargo, no se supone que λ pertenezca al semigrupo libre $F = F(A)$. El conjunto de todas las palabras en A, incluso λ suele denotarse por A^*. Así, A^* es un monoide bajo concatenación; se denomina *monoide libre* en A.

Subsemigrupos

Sea A un subconjunto no vacío de un semigrupo S. Entonces A se denomina subsemigrupo de S si A mismo es un semigrupo respecto de la operación en S. Puesto que los elementos de A también son elementos de S, la ley asociativa se cumple en forma automática para los elementos de A. En consecuencia, A es un subsemigrupo de S si y sólo si A es cerrado bajo la operación en S.

EJEMPLO B.6

a) Sean A y B el conjunto de enteros pares y el conjunto de enteros impares, respectivamente. Entonces $(A, \times)$ y $(B, \times)$ son subsemigrupos de $(\mathbf{N}, \times)$, puesto que A y B son cerrados bajo la multiplicación. Por otra parte, $(A, +)$ es un subsemigrupo de $(\mathbf{N}, +)$ puesto que A es cerrado bajo la adición, pero $(B, \times)$ no es un subsemigrupo de $(\mathbf{N}, +)$, ya que B no es cerrado bajo la adición.

b) Sea F el semigrupo libre en el conjunto $A = \{a, b\}$. Sea H que consiste de todas las palabras pares; es decir, las palabras de longitud par. La concatenación de dos de estas palabras también es par. Por tanto, H es un subsemigrupo de F.

Relaciones de congruencia y estructuras cociente

Sea S un subsemigrupo y sea $\sim$ una relación de equivalencia en S. Recuerde que la relación de equivalencia $\sim$ induce una partición de S en clases de equivalencia. También, $[a]$ denota la clase de equivalencia que contiene al elemento $a \in S$ y que la colección de clases de equivalencia se denota por S/$\sim$.

Suponga que la relación de equivalencia $\sim$ en S tiene la siguiente propiedad:

$$\boxed{\text{Si } a \sim a' \text{ y } b \sim b', \text{ entonces } ab \sim a'b'.}$$

Entonces, $\sim$ se denomina *relación de congruencia* en S. Además, ahora es posible definir una operación en las clases de equivalencia por

$$[a] * [b] = [a * b] \quad \text{o, simplemente,} \quad [a]\,[b] = [ab]$$

Más aún, esta operación en $S/\sim$ es asociativa; por tanto, $S/\sim$ es un semigrupo. Este hecho se plantea formalmente a continuación.

Teorema B.3: Sea $\sim$ una relación de congruencia en un semigrupo S. Entonces S/$\sim$, las clases de equivalencia bajo $\sim$, constituyen un semigrupo bajo la operación $[a]\,[b] = [ab]$.

Este semigrupo $S/\sim$ se denomina cociente de S por $\sim$.

EJEMPLO B.7

a) Sea F el semigrupo libre en un conjunto A. Se define $u \sim u'$ si u y u' tienen la misma longitud. Entonces, $\sim$ es una relación de equivalencia en F. Además, suponga $u \sim u'$ y $v \sim v'$; por ejemplo,

$$l(u) = l(u') = m \quad \text{y} \quad l(v) = l(v') = n$$

Entonces $l(uv) = l(u'v') = m + n$ y así $uv \sim u'v'$. Así, $\sim$ es una relación de congruencia en F.

b) Considere los enteros $\mathbf{Z}$ y un entero positivo $m > 1$. Recuerde (sección 11.8) que a es congruente con b módulo m, lo cual se escribe

$$a \equiv b \ (\text{mód } m)$$

si m divide a la diferencia $a - b$. El teorema 11.21 establece que es una relación de equivalencia en $\mathbf{Z}$. Además, el teorema 11.22 establece que si $a \equiv c$ (mód m) y $b \equiv d$ (mód m), entonces:

$$a + b \equiv c + d \ (\text{mód } m) \quad \text{y} \quad ab \equiv cd \ (\text{mód } m)$$

En otras palabras, es una relación de congruencia en $\mathbf{Z}$.

Homomorfismo de semigrupos

Considere dos semigrupos $(S, *)$ y $(S', *')$. Una función $f: S \to S'$ se denomina *homomorfismo de semigrupos* o, simplemente, *homomorfismo*, si

$$f(a * b) = f(a) *' f(b) \quad \text{o, simplemente} \quad f(ab) = f(a)f(b)$$

Suponga que f también es uno a uno y sobre. Entonces f se denomina *isomorfismo* entre S y S', y se dice que S y S' son semigrupos *isomorfos*, lo cual se escribe $S \cong S$.

EJEMPLO B.8

a) Sea M el conjunto de todas las matrices de 2×2 con entradas enteras. El determinante de cualquier matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ se denota y define por $\det(A) = |A| = ad - bc$. En álgebra lineal se demuestra que el determinante es una *función multiplicativa*; es decir, que para matrices A y B arbitrarias,

$$\det(AB) = \det(A) \cdot \det(B)$$

Así, la función determinante es un homomorfismo de semigrupos en $(M, \times)$, las matrices bajo matrices de multiplicación. Por otra parte, la función determinante no es aditiva; es decir, para algunas matrices

$$\det(A + B) \neq \det(A) + \det(B)$$

Así, la función determinante no es un homomorfismo de semigrupos en $(M, +)$.

b) En la figura B-2*a*) se proporciona la tabla de adición para $\mathbf{Z_4}$, los enteros módulo 4 bajo la adición; y en la figura B-2*b*) se proporciona la tabla de multiplicar para $S = \{1, 3, 7, 9\}$ en $\mathbf{Z_{10}}$. (Se observa que S es un sistema reducido de residuos para los enteros $\mathbf{Z}$ módulo 10.) Sea $f: \mathbf{Z_4} \to S$ definida por

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 9, \quad f(3) = 7$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

a)

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

b)

Figura B-2

Puede demostrarse que f es un homomorfismo. Puesto que f es uno a uno y sobre, f es un isomorfismo. Por tanto, $\mathbf{Z_4}$ y S son semigrupos isomorfos.

c) Sea $\sim$ una relación de congruencia sobre un semigrupo S. Sea $\phi: S \to S/\sim$ la *transformación natural* de S en el semigrupo de factores $S/\sim$ definida por

$$\phi(a) = [a]$$

Es decir, cada elemento a en S se asigna a su clase de equivalencia $[a]$. Entonces ϕ es un homomorfismo puesto que

$$\phi(ab) = [ab] = [a]\,[b] = \phi(a)\phi(b)$$

Teorema fundamental de homomorfismos de semigrupos

Recuerde que la imagen de una función $f: S \to S'$, que se escribe $f(S)$ o Im f, consiste de las imágenes de los elementos de S bajo f. A saber:

$$\text{Im } f = \{b \in S' \mid \text{existe } a \in S \text{ para el cual } f(a) = b\}$$

El siguiente teorema (que se demuestra en el problema B.5) es fundamental en teoría de semigrupos.

Teorema B.4: Sea $f: S \to S'$ un homomorfismo de semigrupos. Sea $a \sim b$ si $f(a) = f(b)$. Entonces: *i*) $\sim$ es una relación de congruencia en S. *ii*) $S/\sim$ es isomorfo para $f(S)$.

EJEMPLO B.9

a) Sea F el semigrupo libre en $A = \{a, b\}$. La función $f: F \to \mathbf{Z}$ definida por

$$f(u) = \text{l}(u)$$

es un homomorfismo. Observe que $f(F) = \mathbf{N}$. Así, $F/\sim$ es isomorfo para $\mathbf{N}$.

b) Sea M el conjunto de matrices de 2×2 con entradas enteras. Considere la función determinante $M \to \mathbf{Z}$. Se observa que la imagen de det es $\mathbf{Z}$. Por el teorema B.4 $M/\sim$ es isomorfo para $\mathbf{Z}$.

Productos de semigrupos

Sean $(S_1, *_1)$ y $(S_2, *_2)$ semigrupos. Un nuevo semigrupo $S = S_1 \otimes S_2$, denominado producto directo de S_1 y S_2, se forma como sigue:

1) Los elementos de S provienen de $S_1 \times S_2$; es decir, son pares ordenados (a, b), donde $a \in S_1$ y $b \in S_2$.

2) La operación $*$ en S se define componente por componente; es decir,

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \quad \text{o, simplemente} \quad (a, b)(a', b') = (aa', bb')$$

Resulta fácil demostrar (problema B.3) que la operación anterior es asociativa.

B.4 GRUPOS

Sea G un conjunto no vacío con una operación binaria (denotada por yuxtaposición). Entonces G se denomina *grupo* si se cumplen los siguientes axiomas:

[$\mathbf{G_1}$] Ley asociativa: para a, b, c arbitrarios en G, se tiene $(ab)c = a(bc)$.
[$\mathbf{G_2}$] Elemento identidad: existe un elemento e en G tal que $ae = ea$ para todo a en G.
[$\mathbf{G_3}$] Inversos: para todo a en G existe un elemento a^{-1} en G (el *inverso* de a) tal que

$$aa^{-1} = a^{-1}a = e$$

Se dice que un grupo G es *abeliano* (o *conmutativo*) si $ab = ba$ para cualesquiera $a, b \in G$; es decir, si G satisface la ley conmutativa.

Cuando la operación binaria se usa por yuxtaposición como antes, se dice que el grupo está escrito en forma *multiplicativa*. Algunas veces, cuando G es abeliano, la operación binaria se denota por $+$ y se dice que G está escrito en forma *aditiva*. En este caso, el elemento identidad e se denota por 0 y se denomina elemento *cero*; y el inverso se denota por $-a$ y se denomina *negativo* de a.

El número de elementos en un grupo G, que se denota por $|G|$, se denomina *orden* de G. En particular, G se denomina *grupo finito* si su orden es finito.

Suponga que A y B son subconjuntos de un grupo G. Entonces se escribe:

$$AB = \{ab \mid a \in A, \quad b \in B\} \quad \text{o} \quad A + B = \{a + b \mid a \in A, \quad b \in B\}$$

EJEMPLO B.10

a) Los números racionales $\mathbf{Q}\backslash\{0\}$ distintos de cero constituyen un grupo abeliano bajo la multiplicación. El elemento identidad es el número 1 y q/p es el inverso multiplicativo del número racional p/q.

b) Sea S el conjunto de matrices de 2×2 con entradas de números racionales bajo la operación de multiplicación de matrices. Entonces S no es un grupo puesto que los inversos no siempre existen. Sin embargo, sea G el subconjunto de matrices de 2×2 con determinante cero. Entonces G es un grupo bajo la operación de multiplicación de matrices. El elemento identidad es

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ y la inversa de } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ es } A^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix}$$

Éste es un ejemplo de grupo no abeliano, puesto que la multiplicación de matrices no es conmutativa.

c) Recuerde que $\mathbf{Z}_m$ denota a todos los enteros módulo m. $\mathbf{Z}_m$ es un grupo bajo la adición, pero no lo es bajo la multiplicación. Sin embargo, sea $\mathbf{U}_m$ un sistema reducido de residuos módulo m que consiste de los enteros primos relativos con m. Entonces $\mathbf{U}_m$ es un grupo bajo la multiplicación (módulo m). En la figura B-3 se proporciona la tabla de multiplicar para $\mathbf{U}_{12} = \{1, 5, 7, 11\}$.

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Figura B-3

	ε	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ε	ε	ϕ_1	σ_3	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ε	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ε	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ε	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ε
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ε	ϕ_1

Figura B-4

Grupo simétrico S_n

Una transformación σ uno a uno del conjunto $\{1, 2, \ldots, n\}$ en sí mismo se denomina *permutación*. Una permutación así se denota como sigue, donde $j_i = \sigma(i)$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

El conjunto de todas estas permutaciones se denota por S_n, y hay $n! = n(n-1) \cdot \ldots \cdot 2 \cdot 1$ de ellas. La composición y los inversos de las permutaciones en S_n pertenecen a S_n, y la función identidad ε pertenece a S_n. Así, S_n forma un grupo bajo la composición de funciones, denominado *grupo simétrico de grado n*.

El grupo simétrico S_3 tiene $3! = 6$ elementos, como sigue:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

La tabla de multiplicar de S_3 se muestra en la figura B-4.

MAP(A), PERM(A) y AUT(A)

Sea A un conjunto no vacío. La colección MAP(A) de todas las funciones (transformaciones) $f: A \to A$ es un semigrupo bajo composición de funciones; no es un grupo puesto que algunas funciones no tienen inversa. No obstante, el subsemigrupo PERM(A) de todas las correspondencias uno a uno de A en sí mismo (denominadas *permutaciones* de A) es un grupo bajo composición de funciones.

Además, suponga que A cuenta con algún tipo de estructura geométrica o algebraica; por ejemplo, A puede ser el conjunto de vértices de una gráfica, o bien ser un conjunto ordenado o un semigrupo. Entonces el conjunto AUT(A) de todos los isomorfismos de A en sí mismo (denominados *automorfismos* de A) también es un grupo bajo composición de funciones.

B.5 SUBGRUPOS, SUBGRUPOS NORMALES Y HOMOMORFISMOS

Sea H un subconjunto de un grupo G. Entonces H se denomina *subgrupo* de G si H mismo es un grupo bajo la operación de G. A continuación se proporcionan criterios simples para determinar subgrupos.

Proposición B.5: Un subconjunto H de un grupo G es un subgrupo de G si:

i) El elemento identidad $e \in H$.
ii) H es cerrado bajo la operación de G; es decir, si $a, b \in H$, entonces $ab \in H$.
iii) H es cerrado bajo inversos; es decir, si $a \in H$, entonces $a^{-1} b \in H$.

Todo grupo G tiene los subgrupos $\{e\}$ y G mismo. Cualquier otro subgrupo de G se denomina *subgrupo no trivial*.

Clases laterales

Suponga que H es un subgrupo de G y que $a \in G$. Entonces el conjunto

$$Ha = \{ha \mid h \in H\}$$

se denomina *clase lateral derecha* de H. (En forma semejante, aH se denomina *clase lateral izquierda* de H.) Se tienen los siguientes resultados importantes (que se demuestran en los problemas B.13 y B.15).

Teorema B.6: Sea H un subgrupo de G. Entonces las clases laterales derechas Ha forman una partición de G.

Teorema B.7 (de Lagrange): Sea H un subgrupo de un grupo finito de G. Entonces el orden de H divide al orden de G.

El número de clases laterales derechas de H en G, denominado índice de H en G, es igual al número de clases laterales izquierdas de H en G; y ambos números son iguales a $|G|$ dividido entre $|H|$.

Subgrupos normales

La siguiente definición es válida:

Definición B.2: Un subgrupo H de G es un subgrupo *normal* si $a^{-1}Ha \subseteq H$, para todo $a \in G$ o, en forma equivalente, si $aH = Ha$; es decir, si las clase laterales derechas e izquierdas coinciden.

Observe que todo subgrupo de un grupo abeliano es normal.

La importancia de los subgrupos normales procede del siguiente resultado (demostrado en el problema B.17).

Teorema B.8: Sea H un subgrupo normal de un grupo G. Entonces las clases laterales de H forman un grupo bajo multiplicación de clase lateral:

$$(aH)(bH) = abH$$

Este grupo se denomina *grupo cociente* y se denota por G/H.

Suponga que la operación en G es la suma o, en otras palabras, que G está escrito en forma aditiva. Entonces las clases laterales de un subgrupo H de G son de la forma $a + H$. Además, si H es un subgrupo normal de G, entonces las clases laterales forman un grupo bajo adición de clases laterales; es decir,

$$(a + H) + (b + H) = (a + b) + H$$

EJEMPLO B.11

a) Considere el grupo de permutaciones S_3 de grado 3 que acaba de investigar. El conjunto $H = \{\varepsilon, \sigma_1\}$ es un subgrupo de S_3. A continuación se presentan sus clases laterales derecha e izquierda:

Clases laterales derechas	**Clases laterales izquierdas**
$H = \{\varepsilon, \sigma_1\}$	$H = \{\varepsilon, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi 2, \sigma 3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Observe que las clases laterales derechas y las clases laterales izquierdas son distintas; por tanto, H no es un subgrupo normal de S_3.

b) Considere el grupo G de matrices de 2×2 con entradas de números racionales y determinantes distintos de cero. (Vea el ejemplo A.10.) Sea H el subconjunto de G que consta de las matrices cuya entrada superior derecha es cero; es decir, las matrices de la forma

$$\begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$$

Entonces H es un subgrupo de G puesto que H es cerrado bajo multiplicación e inversos e $I \in H$. Sin embargo, H no es un subgrupo normal porque, por ejemplo, el siguiente producto no pertenece a H:

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} -1 & -4 \\ 1 & 3 \end{bmatrix}$$

Por otra parte, sea K el subconjunto de G que consiste de las matrices con determinante 1. Puede demostrarse que K también es un subgrupo de G. Además, para cualquier matriz X en G y cualquier matriz A en K, se tiene

$$\det(X^{-1}AX) = 1$$

Por tanto, $X^{-1}AX$ pertenece a K, de modo que K es un subgrupo normal de G.

Enteros módulo *m*

Considere el grupo $\mathbf{Z}$ de enteros bajo adición. Sea H el conjunto de múltiplos de 5; es decir,

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Entonces H es un subgrupo (necesariamente normal) de $\mathbf{Z}$. Las clases laterales de H en $\mathbf{Z}$ se muestran en la figura B-5*a*). Por el teorema B.8, $\mathbf{Z}/H = \{0, 1, 2, 3, 4\}$ es un grupo bajo la adición de clases laterales; su tabla de sumar se muestra en la figura B-5*b*).

Este grupo cociente $\mathbf{Z}/H$ se denomina enteros módulo 5 y a menudo se denota por $\mathbf{Z}_5$. En forma semejante, para cualquier entero positivo n, existe el grupo cociente $\mathbf{Z}_n$, denominado *enteros módulo n*.

$\overline{0} = 0 + H = H = \{..., -10, -5, 0, 5, 10, ...\}$
$\overline{1} = 1 + H = \{..., -9, -4, 1, 6, 11, ...\}$
$\overline{2} = 2 + H = \{..., -8, -3, 2, 7, 12, ...\}$
$\overline{3} = 3 + H = \{..., -7, -2, 3, 8, 13, ...\}$
$\overline{4} = 4 + H = \{..., -6, -1, 4, 9, 14, ...\}$

a)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

b)

Figura B-5

Subgrupos cíclicos

Sea G cualquier grupo y sea a cualquier elemento de G. Como de costumbre, se define $a^0 = e$ y $a^{n+1} = a^n \cdot a$. Resulta evidente que $a^m a^n = a^{m+n}$ y $(a^m)^n = a^{mn}$, para enteros arbitrarios m y n. Sea S el conjunto de todas las potencias de a; es decir,

$$S = \{\cdots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \cdots\}$$

Entonces S es un subgrupo de G denominado grupo cíclico generado por a. Este grupo se denota por $gp(a)$.

Además, suponga que las potencias de a no son distintas, por ejemplo, $a^r = a^s$ con, por ejemplo, $r > s$. Entonces $a^{r-s} = e$ donde $r, s > 0$. El menor entero positivo m tal que $a^m = e$ se denomina *orden* de a y se denota por $|a|$. Si $|a| = m$, entonces el subgrupo cíclico $gp(a)$ tiene m elementos como sigue:

$$gp(a) = \{e, a, a^2, a^3, \ldots, a^{m-1}\}$$

Considere, por ejemplo, el elemento ϕ_1 en el grupo simétrico S_3 que acaba de analizarse. Entonces:

$$\phi_1{}^1 = \phi_1, \quad \phi_1{}^2 = \phi_2, \quad \phi_1{}^3 = \phi_2 \cdot \phi_1 = e$$

Por tanto, $|\phi_1| = 3$ y $gp(\phi_1) = \{e, \phi_1, \phi_2\}$. Observe que $|\phi_1|$ divide el orden de S_3. Esto es cierto en general; es decir, para cualquier elemento a en un grupo G, $|a|$ es igual al orden de $gp(a)$ y entonces $|a|$ divide a $|G|$ por el teorema de Lagrange B.7. También se observa que un grupo G es *cíclico* si tiene un elemento a tal que $G = gp(a)$.

Conjuntos generadores, generadores

Considere cualquier subconjunto A de un grupo G. Sea $gp(A)$ el conjunto de todos los elementos x en G tales que x es igual al producto de los elementos donde cada elemento proviene del conjunto $A \cup A^{-1}$ (donde A^{-1} denota el conjunto de inversos de elementos de A); es decir,

$$gp(A) = \{x \in G \mid x = b_1 b_2 \ldots b_m \text{ donde cada } b_i \in A \cup A^{-1}\}$$

Entonces $gp(A)$ es un subgrupo de G con *conjunto generador* A. En particular, se dice que A genera el grupo G si $G = gp(A)$; es decir, si toda g en G es un producto de elementos de $A \cup A^{-1}$. Se dice que A es un *conjunto mínimo de generadores* de G si A genera a G y si ningún conjunto con menos elementos que A genera a G. Por ejemplo, las permutaciones $a = \sigma_1$ y $b = \phi_1$ constituyen un conjunto mínimo de generadores del grupo simétrico S_3 (figura B-4). Específicamente,

$$e = a^2, \quad \sigma_1 = a, \quad \sigma_2 = ab, \quad \sigma_3 = ab^2, \quad \phi_1 = b, \quad \phi_2 = b^2$$

y S_3 no es cíclico, de modo que no puede ser generado por un elemento.

Homomorfismos

Una transformación f de un grupo G en un grupo G' se denomina homomorfismo si, para toda $a, b \in G$,

$$f(ab) = f(a)f(b)$$

Además, si f es uno a uno y sobre, entonces f se denomina *isomorfismo*; y se dice que G y G' son *isomorfos*, lo cual se escribe $G \cong G'$.

Si $f: G \to G'$ es un homomorfismo, entonces el kernel (núcleo) de f, que se escribe Ker f, es el conjunto de elementos cuya imagen es el elemento identidad e' de G'; es decir,

$$\text{Ker } f = \{a \in G \mid f(a) = e'\}$$

Recuerde que la imagen de f, que se escribe $f(G)$ o Im f, consiste de las imágenes de los elementos bajo f; es decir,

$$\text{Im } f = \{b \in G' \mid \text{existe } a \in G \text{ para la cual } f(a) = b\}.$$

El siguiente teorema (que se demuestra en el problema B.19) es fundamental en teoría de grupos.

Teorema B.9: Suponga que $f: G \to G'$ es un homomorfismo con kernel K. Entonces K es un subgrupo normal de G y el grupo cociente G/K es isomorfo a $f(G)$.

EJEMPLO B.12

a) Sea G el grupo de números reales bajo la adición, y sea G' el grupo de números reales positivos bajo la multiplicación. La transformación $f: G \to G'$ definida por $f(a) = 2^a$ es un homomorfismo puesto que

$$f(a + b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$$

De hecho, f también es uno a uno y sobre; por tanto, G y G' son isomorfos.

b) Sea a cualquier elemento en un grupo G. La función $f: \mathbf{Z} \to G$ definida por $f(n) = a^n$ es un homomorfismo puesto que

$$f(m + n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$

La imagen de f es $gp(a)$, el subgrupo cíclico generado por a. Por el teorema B.9,

$$gp(a) \cong \mathbf{Z}/\mathbf{K}$$

donde K es el kernel de f. Si $K = \{0\}$, entonces $gp(a) = \mathbf{Z}$. Por otra parte, si m es de orden a, entonces $K = \{\text{múltiplos de } m\}$, y así $gp(a) \cong \mathbf{Z}_m$. En otras palabras, cualquier grupo cíclico es isomorfo ya sea a los enteros $\mathbf{Z}$ bajo la adición, o a $\mathbf{Z}_m$, los enteros bajo la adición módulo m.

B.6 ANILLOS, DOMINIOS DE INTEGRIDAD Y CAMPOS

Sea R un conjunto no vacío con dos operaciones binarias: una operación de adición (denotada por $+$) y una operación de multiplicación (denotada por yuxtaposición). Entonces R se denomina *anillo* si se cumplen los axiomas siguientes:

$[\mathbf{R_1}]$ Para toda $a, b, c \in R$, se tiene $(a + b) + c = a + (b + c)$.

$[\mathbf{R_2}]$ Existe un elemento $0 \in R$ denominado elemento *cero* tal que, para toda $a \in R$.

$$a + 0 = 0 + a = 0.$$

$[\mathbf{R_3}]$ Para toda $a \in R$ existe un elemento $-a \in R$ denominado *negativo* de a, tal que

$$a + (-a) = (-a) + a = 0.$$

$[\mathbf{R_4}]$ Para toda $a, b \in R$, se tiene $a + b = b + a$.

$[\mathbf{R_5}]$ Para toda $a, b, c \in R$, se tiene $(ab)c = a(bc)$.

$[\mathbf{R_6}]$ Para toda $a, b, c \in R$, se tiene *i*) $a(b + c) = ab + ac$, y *ii*) $(b + c)a = ba + ca$.

Observe que los axiomas $[\mathbf{R_1}]$ a $[\mathbf{R_4}]$ se resumen con la frase: R es un grupo abeliano bajo la suma.

La sustracción se define en R como $a - b = a + (-b)$.

Puede demostrarse (problema B.21) que $a \cdot 0 = 0 \cdot a = 0$ para toda $a \in R$.

Un subconjunto S de R es un *subanillo* de R si S mismo es un anillo bajo las operaciones en R. Se observa que S es un subanillo de R si: *i*) $0 \in S$ y *ii*) para toda $a, b \in S$ se tiene $a - b \in S$ y $ab \in S$.

Tipos especiales de anillos: dominios de integridad y campos

En esta subsección se definen varios tipos de anillos, incluso dominios de integridad y campos.

R se denomina *anillo conmutativo* si $ab = ba$ para toda $a, b \in R$.

R se denomina *anillo con elemento identidad 1* si el elemento 1 tiene la propiedad de que $a \cdot 1 = 1 \cdot a = a$ para todo elemento $a \in R$. En este caso, un elemento $a \in R$ se denomina *unidad* si a tiene inverso multiplicativo; es decir, si en R existe un elemento a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

R se denomina *anillo con divisores cero* si existen elementos $a, b \in R$ distintos de cero tales que $ab = 0$. En este caso, a y b se denominan *divisores cero*.

Definición B.3: Un anillo conmutativo R es un *dominio de integridad* si R no tiene divisores cero; es decir, si $ab = 0$ implica $a = 0$ o $b = 0$ (o ambos $a = 0$ y $b = 0$). (*N. del t.*)

Definición B.4: Un anillo conmutativo R con elemento identidad 1 (no igual a 0) es un campo si toda $a \in R$ distinta de cero es una unidad; es decir, tiene inverso multiplicativo.

Un campo necesariamente es un dominio de integridad, ya que si $ab = 0$ y $a \neq 0$, entonces

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

Se observa que un campo también puede considerarse como un anillo conmutativo en el que los elementos diferentes de cero constituyen un grupo bajo la multiplicación.

EJEMPLO B.13

a) El conjunto $\mathbf{Z}$ de enteros con las operaciones adición y multiplicación de costumbre es el ejemplo clásico de un dominio de integridad (con elemento identidad). Las unidades en $\mathbf{Z}$ son sólo 1 y -1; es decir, ningún otro elemento en $\mathbf{Z}$ tiene inverso multiplicativo.

b) El conjunto $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ bajo las operaciones de adición y multiplicación módulo m es un anillo; se denomina *anillo de los enteros módulo m*. Si m es primo, entonces $\mathbf{Z}_m$ es un campo. Por otra parte, si m no es primo, entonces $\mathbf{Z}_m$ tiene divisores cero. Por ejemplo, en el anillo $\mathbf{Z}_6$,

$$2 \cdot 3 = 0 \quad \text{pero} \quad 2 \not\equiv 0 \ (\text{mód } 6) \quad \text{y} \quad 3 \not\equiv 0 \ (\text{mód } 6)$$

c) Los números racionales $\mathbf{Q}$ y los números reales $\mathbf{R}$ constituyen, cada uno, un campo con respecto a las operaciones adición y multiplicación de costumbre.

d) Sea M el conjunto de matrices de 2×2 con entradas enteras o reales. Entonces M es un anillo no conmutativo con divisores cero bajo las operaciones adición y multiplicación de matrices. M tiene elemento identidad: la matriz identidad.

e) Sea R cualquier anillo. Entonces el conjunto $R[x]$ de todos los polinomios sobre R es un anillo con respecto a las operaciones adición y multiplicación de polinomios. Además, si R es un dominio de integridad, entonces $R[x]$ también es un dominio de integridad.

Ideales

Un subconjunto J de un anillo se denomina *ideal* en R si se cumplen las tres propiedades siguientes:

i) $0 \in J$.

ii) Para toda $a, b \in J$, se tiene $a - b \in J$.

iii) Para toda $r \in R$ y $a \in J$, se tiene $ra, ar \in J$.

Primero observe que J es un subanillo de R. También, J es un subgrupo (necesariamente normal) del grupo aditivo de R. Así es posible formar la siguiente colección de clases laterales, que forman una partición de R:

$$\{a + J \mid a \in R\}$$

La importancia de los ideales proviene del siguiente teorema, que es semejante al teorema B.7 para subgrupos normales.

Teorema B.10: Sea J un ideal en un anillo R. Entonces las clases laterales $\{a + J \mid a \in R\}$ forman un anillo bajo las operaciones de clases laterales

$$(a + J) + (b + J) = a + b + J \quad \text{y} \quad (a + J)(b + J) = ab + J$$

Este anillo se denota por R/J y se denomina *anillo cociente*.

Ahora, sea R un anillo conmutativo con un elemento identidad 1. Para toda $a \in R$, el siguiente conjunto es un ideal:

$$(a) = \{ra \mid r \in R\} = aR$$

Se denomina *ideal principal generado* por a. Si todo ideal en R es ideal principal, entonces R se denomina *anillo ideal principal*. En particular, si R también es un dominio de integridad, entonces R se denomina *dominio ideal principal* (DIP).

EJEMPLO B.14

a) Considere el anillo $\mathbf{Z}$ de los enteros. Entonces todo ideal J en $\mathbf{Z}$ es un ideal principal; es decir, $J = (m) = m\mathbf{Z}$, para algún entero m. Así, $\mathbf{Z}$ es un dominio ideal principal (DIP). El anillo cociente $\mathbf{Z}_m = \mathbf{Z}/(m)$ es simplemente el anillo de enteros módulo m. Aunque $\mathbf{Z}$ es un dominio de integridad (sin divisores cero), el anillo cociente $\mathbf{Z}_m$ puede tener divisores cero; por ejemplo, 2 y 3 son divisores cero en $\mathbf{Z}_6$.

b) Sea R cualquier anillo. Entonces $\{0\}$ y R son ideales. En particular, si R es un campo, entonces los únicos ideales son $\{0\}$ y R.

c) Sea K un campo. Entonces el anillo $K[x]$ de polinomios sobre K es un DIP (dominio ideal principal). Por otra parte, el anillo $K[x, y]$ de polinomios en dos variables no es un DIP.

Homomorfismos de anillos

Una transformación f de un anillo R en un anillo R' se denomina *homomorfismos de anillos* o, simplemente, *homomorfismo* si, para toda $a, b \in R$,

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

Además, si f es uno a uno y sobre, entonces f se denomina *isomorfismo*; y se dice que R y R' son *isomorfos*, lo cual se escribe $R \cong R'$.

Suponga que $f: R \to R'$ es un homomorfismo. Entonces el kernel de f, que se escribe Ker f, es el conjunto de elementos cuya imagen es el elemento 0 de R'; es decir,

$$\text{Ker } f = \{r \in R \mid f(r) = 0\}$$

El siguiente teorema (semejante al teorema B.9 para grupos) es fundamental en teoría de anillos.

Teorema B.11: Sea $f: R \to R'$ un homomorfismo de anillos con kernel K. Entonces K es un ideal en R, y el anillo cociente R/K es isomorfo para $f(R)$.

Divisibilidad de dominios de integridad

Sea D un dominio de integridad. Se dice que b divide a a en D si $a = bc$ para alguna $c \in D$. Un elemento $u \in D$ se denomina *unidad* si u divide a 1; es decir, si u tiene inverso multiplicativo. Un elemento $b \in D$ se denomina *asociado* de $a \in D$ si $b = ua$ para alguna unidad $u \in D$. Se dice que una no unidad $p \in D$ es *irreducible* si $p = ab$ implica que a o b es una unidad.

Un dominio de integridad D se denomina *dominio de factorización única* (DFU) si toda no unidad $a \in D$ puede escribirse de manera única (dependiendo de asociados y orden) como un producto de elementos irreducibles.

EJEMPLO B.15

a) El anillo **Z** de enteros es el ejemplo clásico de un dominio de factorización única. Las unidades de **Z** son 1 y -1. Los únicos asociados de $n \in Z$ son n y $-n$. Los elementos irreducibles de **Z** son los números primos.

b) El conjunto $D = \{a + b\sqrt{13} \mid a, b \text{ enteros}\}$ es un dominio de integridad. Las unidades de D son las siguientes:

$$\pm 1, \quad 18 \pm 5\sqrt{13}, \quad -18 \pm 5\sqrt{13}$$

Los elementos 2, $3 - \sqrt{13}$ y $-3 - \sqrt{13}$ son irreducibles en D. Observe que

$$4 = 2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$

Por tanto, D no es un dominio de factorización única. (Vea el problema B.97.)

B.7 POLINOMIOS SOBRE UN CAMPO

En esta sección se investigan polinomios cuyos coeficientes provienen de un dominio de integridad o campo K. En particular, se demuestra que los polinomios sobre un campo K tienen muchas de las propiedades de los enteros.

Definiciones básicas

Sea K un dominio de integridad o un campo. Formalmente, un polinomio f sobre K es una secuencia infinita de elementos de K donde todos excepto un número finito de ellos son 0; es decir,

$$f = (\ldots, 0, a_n, \ldots, a_1, a_0) \quad \text{o, en forma equivalente,} \quad f(t) = a_n t^n + \cdots + a_1 t + a_0$$

donde el símbolo t se usa como indeterminado. La entrada a_k se denomina k-ésimo coeficiente de f. Si n es el mayor entero $a \neq 0$, entonces se dice que el grado del f es n, y se escribe $\text{gr}(f) = n$. También, a_n se denomina coeficiente principal de f. Si $a_n = 1$, f se denomina *monomio*. Por otra parte, si todo coeficiente de f es 0, entonces f se denomina polinomio *cero*, lo cual se escribe $f \equiv 0$. El grado del polinomio cero no está definido.

Sea $K[t]$ la colección de todos los polinomios $f(t)$ sobre K. Considere los polinomios

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{y} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

Entonces la suma $f + g$ es el polinomio que se obtiene al sumar los coeficientes correspondientes; es decir, si $m \leq n$, entonces

$$f(t) + g(t) = a_n t^n + \cdots + (a_m + b_m)t^m + \cdots + (a_1 + b_1)t + (a_0 + b_0)$$

Además, el producto de f y g es el polinomio

$$f(t)g(t) = (a_n b_m)t^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)t + (a_0 b_0)$$

Es decir,

$$f(t)g(t) = c_{n+m}t^{n+m} + \cdots + c_1 t + c_0 \quad \text{donde} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

El conjunto K de escalares se considera como un subconjunto de $K[t]$. Específicamente, el escalar $a_0 \in K$ se identifica con el polinomio

$$f(t) = a_0 \quad \text{o} \quad a_0 = (\cdots, 0, 0, a_0)$$

Entonces, los operadores de adición y multiplicación escalar se preservan mediante esta identificación. Por tanto, la transformación $\psi: K \to K[t]$ definida por $\psi(a_0) = a_0$ es un isomorfismo que inserta K en $K[t]$.

Teorema B.12: Sea K un dominio de integridad. Entonces $K[t]$ bajo las operaciones de adición y multiplicación de polinomios es un anillo conmutativo con elemento identidad 1.

El siguiente resultado simple tiene consecuencias importantes.

Lema B.13: Suponga que f y g son polinomios sobre un dominio de integridad K. Entonces

$$\text{gr}(fg) = \text{gr}(f) + \text{gr}(g).$$

La demostración se deduce directamente de la definición de producto de polinomios. A saber, suponga que

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{y} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

donde $a_n \neq 0$ y $b_m \neq 0$. Por tanto, $\text{gr}(f) = n$ y $\text{gr}(g) = m$. Entonces

$$f(t)g(t) = a_n b_m t^{n+m} + \text{términos de grado inferior}$$

También, puesto que K es un dominio de integridad sin divisores cero, $a_n b_m \neq 0$. Entonces

$$\text{gr}(fg) = m + n = \text{gr}(f) + \text{gr}(g)$$

y se ha demostrado el lema.

La siguiente proposición enumera muchas propiedades de los polinomios. (Recuerde que un polinomio *g divide* a un polinomio f si existe un polinomio h tal que $f(t) = g(t)h(t)$.)

Proposición B.14: Sea K un dominio de integridad y sean f y g polinomios sobre K.

i) $K[t]$ es un dominio de integridad.
ii) Las unidades de $K[t]$ son las unidades en K.
iii) Si g divide a f, entonces $\text{gr}(g) \leq \text{gr}(f)$ o $f \equiv 0$.
iv) Si g divide a f y f divide a g, entonces $f(t) = kg(t)$ donde k es una unidad en K.
v) Si d y d' son monomios tales que d divide a d' y d' divide a d, entonces $d = d'$.

Algoritmo euclidiano, raíces de un polinomio

En esta subsección se analizan las raíces de un polinomio $f(t)$, donde ahora se supone que los coeficientes de $f(t)$ provienen de un campo K. Recuerde que un escalar $a \in K$ es una *raíz* del polinomio $f(t)$ si $f(a) = 0$. Primero se empieza con un teorema importante bastante semejante a un teorema correspondiente para los enteros $\mathbf{Z}$.

Teorema B.15 (algoritmo euclidiano de la división): Sean $f(t)$ y $g(t)$ polinomios sobre un campo K con $g(t) \neq 0$.

Entonces existen polinomios $q(t)$ y $r(t)$ tales que

$$f(t) = q(t)g(t) + r(t)$$

donde $r(t) \equiv 0$ o $\text{gr}(r) < \text{gr}(g)$.

El teorema anterior (que se demuestra en el problema B.30) formaliza el proceso conocido como "división larga". El polinomio $q(t)$ se denomina *cociente* y el polinomio $r(t)$ se denomina *residuo* cuando $f(t)$ se divide entre $g(t)$.

Corolario B.16 (teorema del residuo): Suponga que $f(t)$ se divide entre $g(t) = t - a$. Entonces el residuo es $f(a)$.

La demostración se deduce a partir del algoritmo euclidiano. Es decir, al dividir $f(t)$ entre $t - a$ se obtiene

$$f(t) = q(t)(t - a) + r(t)$$

donde $\text{gr}(r) < \text{gr}(t - a) = 1$. Por tanto, $r(t) = r$ es un escalar. Al sustituir $t = a$ en la ecuación para $f(t)$ se obtiene

$$f(a) = q(a)(a - a) + r = q(t) \cdot 0 + r = r$$

Así, $f(a)$ es el residuo, como se afirmó.

El corolario B.16 también establece que $f(a) = 0$ si y sólo si el residuo $r = r(t) \equiv 0$. En consecuencia:

Corolario B.17 (teorema del factor): El escalar $a \in K$ es una raíz de $f(t)$ si y sólo si $t - a$ es un factor de $f(t)$.

El siguiente teorema (que se demuestra en el problema B.31) indica el número de raíces posibles de un polinomio.

Teorema B.18: Suponga que $f(t)$ es un polinomio sobre un campo K, y que $gr(f) = n$. Entonces $f(t)$ tiene a lo más n raíces.

El siguiente teorema (que se demuestra en el problema B.32) constituye la herramienta más importante para encontrar raíces racionales de un polinomio con coeficientes enteros.

Teorema B.19: Suponga que un racional p/q (reducido a su mínima expresión) es la raíz de un polinomio

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

donde todos los coeficientes $a_n, \ldots, a_1, a_0$ son enteros. Entonces p divide al término constante a_0 y q divide al coeficiente principal a_n. En particular, si $c = p/q$ es un entero, entonces c divide al término constante a_0.

EJEMPLO B.16

a) Suponga que $f(t) = t^3 + t^2 - 8t + 4$. Suponga que $f(t)$ tiene una raíz racional y encuentre todas las raíces de $f(t)$.

Puesto que el coeficiente principal es 1, las raíces racionales de $f(t)$ deben ser enteros de entre ± 1, ± 2, ± 4. Observe que $f(1) \neq 0$ y que $f(-1) \neq 0$. Por división sintética, o al dividir entre $t - 2$, se obtiene

$$\begin{array}{r|rcrcrcr} 2 & 1 & + & 1 & - & 8 & + & 4 \\ & & & 2 & + & 6 & - & 4 \\ \hline & 1 & + & 3 & - & 2 & + & 0 \end{array}$$

En consecuencia, $t = 2$ es una raíz y $f(t) = (t - 2)(t^2 + 3t - 2)$. Al aplicar la fórmula cuadrática para $t^2 + 3t - 2 = 0$, se obtienen las tres siguientes raíces de $f(t)$:

$$t = 2, \quad t = (-3 + \sqrt{17})/2, \quad t = (-3 - \sqrt{17})/2$$

b) Suponga que $h(t) = t^4 - 2t^3 + 11t - 10$. Encuentre todas las raíces reales de $h(t)$, asumiendo que hay dos raíces enteras.

Las raíces enteras deben encontrarse entre ± 1, ± 2, ± 5, ± 10. Por división sintética, o al dividir entre $t - 1$ y luego entre $t + 2$, se obtiene

$$\begin{array}{r|rcrcrcrcr} 1 & 1 & - & 2 & + & 0 & + & 11 & - & 10 \\ & & & 1 & - & 1 & - & 1 & + & 10 \\ \hline -2 & 1 & - & 1 & - & 1 & + & 10 & + & 0 \\ & & - & 2 & + & 6 & - & 10 & & \\ \hline & 1 & - & 3 & + & 5 & + & 0 & & \end{array}$$

Así, $t = 1$ y $t = -2$ son raíces y $h(t) = (t - 1)(t + 2)(t^2 - 3t + 5)$. La fórmula cuadrática con $t^2 - 3t + 5$ indica que no hay ninguna otra raíz real. Es decir, $t = 1$ y $t = -2$ son las únicas raíces reales de $h(t)$.

K[*t*] como DIP y DFU

El siguiente teorema (que se demuestra en los problemas B.33 y B.34) es válido.

Teorema B.20: El anillo $K[t]$ de polinomios sobre un campo K es un dominio ideal principal (DIP). Es decir, si J es un ideal en $K[t]$, entonces existe un monomio único d que genera a J; es decir, todo polinomio f en J es un múltiplo de d.

Teorema B.21: Sean f y g polinomios en $K[t]$, ninguno es cero. Entonces existe un monomio único d tal que:

i) d divide a f y a g.
ii) Si d' divide a f y a g, entonces d' divide a d.

El polinomio d en el teorema B.21 se denomina *máximo común divisor* de f y g, lo cual se escribe $d = \text{mcd}(f, g)$. Si $d = 1$, entonces se dice que f y g son *primos relativos*.

Corolario B.22: Sea d el máximo común divisor de f y g. Entonces existen polinomios m y n tales que $d = mf + ng$. En particular, si f y g son primos relativos, entonces existen polinomios m y n tales que $mf + ng = 1$.

Se dice que un polinomio $p \in K[t]$ es *irreducible* si p no es un escalar y si $p = fg$ implica que f o g es un escalar. En otras palabras, p es irreducible si sus únicos divisores son sus asociados (múltiplos escalares). El siguiente lema (que se demuestra en el problema B.36) es válido.

Lema B.23: Suponga que $p \in K[t]$ es irreducible. Si p divide al producto fg de polinomios f y g en $K[t]$, entonces p divide a f o p divide a g. En términos más generales, si p divide al producto $f_1 f_2 \cdots f_n$ de n polinomios, entonces p divide a uno de ellos.

El siguiente teorema (que se demuestra en el problema B.37) establece que los polinomios sobre un campo forman un *dominio de factorización única* (DFU).

Teorema B.24 (teorema de factorización única): Sea f un polinomio distinto de cero en $K[t]$. Entonces f puede escribirse en forma única (salvo por el orden) como un producto

$$f = kp_1 p_2 \cdots p_n$$

donde $k \in K$ y los p son monomios únicos irreducibles en $K[t]$.

Teorema fundamental del álgebra

La demostración del siguiente teorema rebasa el alcance de este texto.

Teorema fundamental del álgebra: Cualquier polinomio distinto de cero $f(t)$ sobre el campo complejo $\mathbf{C}$ tiene una raíz en $\mathbf{C}$.

Por tanto, es posible escribirlo en forma única (salvo por el orden) como un producto

$$f(t) = k(t - r_1)(t - r_2) \cdots (t - r_n)$$

donde k y los r_i son números complejos y $\text{gr}(f) = n$.

Ciertamente, el teorema anterior no es verdadero para el campo real $\mathbf{R}$. Por ejemplo, $f(t) = t^2 + 1$ es un polinomio sobre R, pero $f(t)$ no tiene ninguna raíz real.

El siguiente teorema (que se demuestra en el problema B.38) es válido.

Teorema B.25: Suponga que $f(t)$ es un polinomio sobre el campo real $\mathbf{R}$, y suponga que el número complejo $z = a + bi$, $b \neq 0$, es una raíz de $f(t)$. Entonces el conjugado complejo $\bar{z} = a - bi$ también es una raíz de $f(t)$. Por tanto, la siguiente expresión es un factor de $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

El siguiente teorema se concluye a partir del teorema B.35 y del teorema fundamental del álgebra.

Teorema B.26: Sea $f(t)$ un polinomio distinto de cero sobre el campo real $\mathbf{R}$. Entonces $f(t)$ puede escribirse en forma única (salvo por el orden) como un producto

$$f(t) = kp_1(t)p_2(t) \cdots p_n(t)$$

donde $k \in \mathbf{R}$ y los $p_i(t)$ son monomios reales de grado 1 o 2.

EJEMPLO B.17 Sea $f(t) = t^4 - 3t^3 + 6t^2 + 25t - 39$. Encuentre todas las raíces de $f(t)$ si $t = 2 + 3i$ es una raíz.

Puesto que $2 + 3i$ es una raíz, entonces $2 - 3i$ es una raíz y $c(t) = t^2 - 4t + 13$ es un factor de $f(t)$. Al dividir $f(t)$ entre $c(t)$ se obtiene

$$f(t) = t^2 - 4t + 13)(t^2 + t - 3)$$

La fórmula cuadrática con $t^2 + t - 3$ proporciona las otras raíces de $f(t)$. Es decir, las cuatro raíces de $f(t)$ son como sigue:

$$t = 2 + 3i, \quad t = 2 - 3i, \quad t = (-1 + \sqrt{13})/2, \quad t = (-1 - \sqrt{13})/2$$

PROBLEMAS RESUELTOS

OPERACIONES Y SEMIGRUPOS

B.1 Considere el conjunto **Q** de números racionales, y sea $*$ la operación en **Q** definida por

$$a * b = a + b - ab$$

a) Encuentre *i*) $3 * 4$; *ii*) $2 * (-5)$; *iii*) $7 * (1/2)$.
b) ¿(**Q**, $*$) es un semigrupo? ¿Es conmutativo?
c) Encuentre el elemento identidad para *.
d) ¿Alguno de los elementos de **Q** tiene inverso? ¿Cuál es?

a) *i*) $3 * 4 = 3 + 4 - 3(4) = 3 + 4 - 12 = -5$
ii) $2 * (-5) = 2 + (-5) + 2(-5) = 2 - 5 + 10 = 7$
iii) $7 * (1/2) = 7 + (1/2) - 7(1/2) = 4$

b) Se tiene

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc = a + b + c - ab - ac - bc + abc \\ a * (b * c) &= a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc\end{aligned}$$

Por tanto, $*$ es asociativa y (**Q**, $*$) es un semigrupo. También,

$$a * b = a + b - ab = b + a - ba = b * a$$

Así, (**Q**, $*$) es un semigrupo conmutativo.

c) Un elemento e es un elemento identidad si $a * e = a$ para toda $a \in \mathbf{Q}$. Se efectúan los cálculos siguientes:

$$a * e = a, \quad a + e - ae = a, \quad e - ea = 0, \quad e(1 - a) = 0, \quad e = 0$$

En consecuencia, 0 es el elemento identidad.

d) Para que a tenga un inverso x, es necesario tener $a * x = 0$, ya que por el inciso *c*), 0 es el elemento identidad. Se efectúan los cálculos siguientes:

$$a * x = 0, \quad a + x - ax = 0, \quad a = ax - x, \quad a = x(a - 1), \quad x = a/(a - 1)$$

si $a \neq 1$, entonces a tiene inverso que es $a/(a - 1)$.

B.2 Sea S un semigrupo con elemento identidad e, y sean b y b' inversos de a. Demuestre que $b = b'$; es decir que, en caso de existir, los inversos son únicos.

Se tiene:

$$b * (a * b') = b * e = b \quad \text{y} \quad (b * a) * b' = e * b' = b'$$

Puesto que S es asociativo, $(b * a) * b' = b * (a * b')$; por tanto, $b = b'$.

B.3 Sea $S = \mathbf{N} \times \mathbf{N}$. Sea $*$ la operación sobre S definida por $(a, b) * (a', b') = (aa', bb')$.

a) Demuestre que $*$ es asociativa. (Por tanto, S es un semigrupo.)
b) Defina $f : (S, *) \to (\mathbf{Q}, \times)$ por $f(a, b) = a/b$. Demuestre que f es un homomorfismo.
c) Encuentre la relación de congruencia $\sim$ en S definida por el homomorfismo f, es decir, donde $x \sim y$ si $f(x) = f(y)$. (Vea el teorema B.4.)
d) Describa $S/\sim$. ¿$S/\sim$ tiene elemento identidad? ¿Tiene inversos?

Suponga que $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.

a) Se tiene

$$(xy)z = (ac,\ bd) * (e,\ f) = [(ac)e, (bd)f]$$
$$x(yz) = (a,\ b) * (ce,\ df) = [a(ce), b(df)]$$

Puesto que a, b, c, d, e, f son enteros positivos, $(ac)e = a(ce)$ y $(bd)f = b(df)$. Por tanto, $(xy)z = x(yz)$ y entonces $*$ es asociativa. Es decir, $(S, *)$ es un semigrupo.

b) f es un homomorfismo puesto que

$$f(x * y) = f(ac, bd) = (ac)/(bd) = (a/b)(c/d) = f(x)\, f(y)$$

c) Suponga que $f(x) = f(y)$. Entonces $a/b = c/d$ y por tanto $ad = bc$. Así, f determina la relación de congruencia $\sim$ en S definida por $(a, b) \sim (c, d)$ si $ad = bc$.

d) La imagen de f es $\mathbf{Q}^+$, el conjunto de número racionales positivos. Por el teorema B.3, $S/\sim$ es isomorfo a $\mathbf{Q}^+$. Por tanto, $S/\sim$ tiene elemento identidad y todo elemento tiene inverso.

B.4 Demuestre el teorema B.1. Suponga que $*$ es una operación asociativa en un conjunto S. Entonces cualquier producto $a_1 * a_2 * \ldots * a_n$ no requiere paréntesis; es decir, todos los productos posibles son iguales.

La demostración es por inducción sobre n. Puesto que $*$ es asociativa, el teorema se cumple para $n = 1$, 2 y 3. Suponga que $n \geq 4$. Se usa la notación:

$$(a_1a_2, \cdots a_n) = (\cdots ((a_1a_2)a_3) \cdots)a_n \quad \text{y} \quad [a_1a_2 \cdots a_n] = \text{cualquier producto}$$

Se demuestra que $[a_1a_2, \cdots a_n] = (a_1a_2, \cdots a_n)$, de modo que todos los productos así son iguales. Puesto que $[a_1a_2, \cdots a_n]$ denota algún producto, existe una $r < n$ tal que $[a_1a_2, \cdots a_n] = [a_1a_2, \cdots a_r][a_{r+1} \cdots a_n]$. En consecuencia, por inducción,

$$\begin{aligned}[a_1a_2 \cdots a_n] &= [a_1a_2 \cdots a_r\,]\,a_{r+1} \cdots a_n] = [a_1a_2 \cdots a_r](a_{r+1} \cdots a_n) \\ &= [a_1 \cdots a_r\,]\,((a_{r+1} \cdots a_{n-1})a_n(\,= ([a_1 \cdots a_r\,])a_{r-1} \cdots a_{n-1}))a_n \\ &= [a_1 \cdots a_{n-1}]a_n = (a_1 \cdots a_{n-1})a_n = (a_1a_2 \cdots a_n)\end{aligned}$$

Así, se ha demostrado el teorema.

B.5 Demuestre el teorema B.4: Sea $f : S \to S'$ un homomorfismo de semigrupos. Sea $a \sim b$ si $f(a) = f(b)$. Entonces: *i*) $\sim$ es una relación de congruencia. *ii*) $S/\sim$ es isomorfo a $f(S)$.

i) Primero se demuestra que $\sim$ es una relación de equivalencia. Puesto que $f(a) = f(a)$, se tiene $a \sim a$.
Si $a \sim b$, entonces $f(a) = f(b)$ o $f(b) = f(a)$; por tanto, $b \sim a$. Por último, si $a \sim b$ y $b \sim c$, entonces $f(a) = f(b)$ y $f(b) = f(c)$; por tanto, $f(a) = f(c)$. Así, $a \sim c$. Es decir, $\sim$ es una relación de equivalencia. Luego se supone que $a \sim a'$ y $b \sim b'$. Entonces $f(a) = f(a')$ y $f(b) = f(b')$.
Puesto que f es un homomorfismo,

$$f(ab) = f(a)\, f(b) = f(a')\, f(b') = fa'b')$$

En consecuencia, $ab \sim a'b'$. Es decir, $\sim$ es una relación de congruencia.

ii) Se definen Ψ: $S/\sim \to f(S)$ por $\Psi([a]) = f(a)$. Es necesario demostrar que: 1) Ψ está bien definido; es decir, que $\Psi([a]) \in f(S)$, y que si $[a]) = [b]$, entonces $f([a]) = f([b])$. 2) Ψ es un isomorfismo; es decir, que Ψ es un homomorfismo, uno a uno y sobre.

1) *Demostración de que* Ψ *está bien definido*: Se tiene $\Psi([a]) = f(b)$. Puesto que $a \in S$ se tiene $f(a) \in f(S)$. Por tanto, $\Psi([a]) \in f(S)$ como se requería. Ahora se supone que $[a] = [b]$. Entonces $a \sim b$ y por tanto $f(a) = f(b)$. En consecuencia,

$$\Psi([a]) = f(a) = f(b) = \Psi([b])$$

Es decir, Ψ está bien definido.

2) *Demostración de que* Ψ *es un isomorfismo*: puesto que f es un homomorfismo,

$$\Psi([a][b]) = \Psi[ab] = f(ab) = f(a)\,f(b) = \Psi([a])\Psi([b])$$

Así, Ψ es un homomorfismo. Suponga que $\Psi([a]) = \Psi([b])$. Entonces $f(a) = f(b)$, y así $a \sim b$. Por tanto, $[a] = [b]$ y Ψ es uno a uno. Por último, sea $y \in f(S)$. Entonces, $f(a) = y$ para alguna $a \in S$. En consecuencia, $\Psi([a]) = f(a) = y$. Así, Ψ es sobre $f(S)$. En consecuencia, Ψ es un isomorfismo.

GRUPOS

B.6 Considere el grupo $G = \{1, 2, 3, 4, 5, 6\}$ bajo la multiplicación módulo 7.

a) Encuentre la tabla de multiplicar de G. *b*) Encuentre 2^{-1}, 3^{-1}, 6^{-1}.
c) Encuentre los órdenes y los subgrupos generados por 2 y 3. *d*) ¿G es cíclico?

a) Para determinar $a * b$ en G, se encuentra el residuo cuando el producto ab se divide entre 7.

Por ejemplo, $5 \cdot 6 = 30$, con lo cual se obtiene un residuo de 2 al dividir entre 7; por tanto, $5 * 6 = 2$ está en G. La tabla de multiplicar de G se muestra en la figura B-6*a*).

b) Primero se observa que el elemento identidad de G es 1. Recuerde que a^{-1} es el elemento de G tal que $aa^{-1} = 1$. Por tanto, $2^{-1} = 4$, $3^{-1} = 5$ y $6^{-1} = 6$.

c) Se tiene $2^1 = 2$, $2^2 = 4$, pero $2^3 = 1$. Por tanto $|2| = 3$ y $gp(2) = \{1, 2, 4\}$. Se tiene $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Por tanto $|3| = 6$ y $gp(3) = G$.

d) G es cíclico puesto que $G = gp(3)$.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a)

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

b)

Figura B-6

B.7 Sea G un sistema de residuos reducido módulo 15; por ejemplo, $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (el conjunto de enteros entre 1 y 15 que son coprimos con 15). Entonces G es un grupo bajo la multiplicación módulo 15.

a) Encuentre la tabla de multiplicar de G. *b*) Encuentre 2^{-1}, 7^{-1}, 11^{-1}.
c) Encuentre los órdenes y los subgrupos generados por 2, 7 y 11. *d*) ¿G es cíclico?

a) Para encontrar $a * b$ en G, se encuentra el residuo cuando el producto ab se divide entre 15. La tabla de multiplicar se muestra en la figura B-6*b*).

b) Los enteros r y s son inversos si $r * s = 1$. Por tanto: $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

c) Se tiene $2^2 = 4$, $2^3 = 8$, $2^4 = 1$. Por tanto, $|2| = 4$ y gp(2) = {1, 2, 4, 8}. También, $7^2 = 4$, $7^3 = 4 * 7 = 13$, $7^4 = 13 * 7 = 1$. Por tanto, $|7| = 4$ y gp(7) = {1, 4, 7, 13}. Así que, $11^2 = 2$. Finalmente $|11| = 2$ y gp(11) = {1, 1}.

d) No, puesto que ningún elemento genera *G*.

B.8 Considere el grupo simétrico S_3, cuya tabla de multiplicar se proporciona en la figura B-4.

a) Encuentre el orden y el grupo generado por cada elemento de S_3.

b) Encuentre el número y todos los subgrupos de S_3.

c) Sea $A = \{\sigma_1, \sigma_2\}$ y $B = \{\phi_1, \phi_2\}$. Encuentre *AB*, $\sigma_3 A$ y $A\sigma_3$.

d) Sean $H = gp(\sigma_1)$ y $K = gp(\sigma_2)$. Demuestre que *HK* no es un subgrupo de S_3.

e) ¿S_3 es cíclico?

a) Hay seis elementos: 1) ε, 2) σ_1, 3) σ_2, 4) σ_3, 5) ϕ_1, 6) ϕ_2. Encuentre las potencias de cada elemento *x* hasta que $x^n = \varepsilon$. Luego $|x| = n$ y $gp(x) = \{\varepsilon, x_1, x_2, \ldots, x^{n-1}\}$. Observe que $x^1 = x$, de modo que sólo es necesario empezar con $n = 2$ cuando $x \neq \varepsilon$.

1) $\varepsilon^1 = \varepsilon$; de modo que $|\varepsilon| = 1$ y $g(\varepsilon) = \{\varepsilon\}$.

2) $\sigma_1^2 = \varepsilon$; de modo que $|\sigma_1| = 2$ y $gp(\sigma_1) = \{\varepsilon, \sigma_1\}$.

3) $\sigma_2^2 = \varepsilon$; de modo que $|\sigma_2| = 2$ y $gp(\sigma_2) = \{\varepsilon, \sigma_2\}$.

4) $\sigma_3^2 = \varepsilon$; de modo que $|\sigma_3| = 2$ y $gp(\sigma_3) = \{\varepsilon, \sigma_3\}$.

5) $\phi_1^2 = \phi_2$, $\phi_1^3 = \phi_2\phi_1 = \varepsilon$; de modo que $|\phi_1| = 3$ y $gp(\phi_1) = \{\varepsilon, \phi_1, \phi_2\}$.

6) $\phi_2^2 = \phi_1$, $\phi_2^3 = \phi_1\phi_2 = \varepsilon$; de modo que $|\phi_2| = 3$ y $gp(\phi_1) = \{\varepsilon, \phi_2, \phi_1\}$.

b) Primero, $H_1 = \{\varepsilon\}$ y $H_2 = S_3$ son subgrupos de S_3. Cualquier otro subgrupo de S_3 debe ser de orden 2 o 3 puesto que su orden debe dividir a $|S_3| = 6$. Debido a que 2 y 3 son primos, estos subgrupos deben ser cíclicos (problema B.61) y entonces deben aparecer en el inciso *a*). Así, los otros subgrupos de S_3 son los siguientes:

$$H_3 = \{\varepsilon, \sigma_1\}, \quad H_4 = \{\varepsilon, \sigma 2\}, \quad H_5 = \{\varepsilon, \sigma_3\}, \quad H_6 = \{\varepsilon, \phi_1, \phi_2\}$$

En consecuencia, S_3 tiene seis subgrupos.

c) Cada elemento de *A* se multiplica por cada elemento de *B*:

$$\sigma_1\phi_1 = \sigma_2, \quad \sigma_1\phi_2 = \sigma_3, \quad \sigma_3\phi_1 = \sigma_3, \quad \sigma_2\phi_2 = \sigma_1$$

Por tanto, $AB = \{\sigma_1, \sigma_2, \sigma_3\}$.

σ_3 se multiplica por cada elemento de *A*:

$$\sigma_3\sigma_1 = \phi_1, \quad \sigma_3\sigma_2 = \phi_2, \quad \text{por tanto} \quad \sigma_3 A = \{\phi_1, \phi_2\}$$

Cada elemento de *A* se multiplica por σ_3:

$$\sigma_1\sigma_3 = \phi_2, \quad \sigma_2\sigma_3 = \phi_1, \quad \text{por tanto} \quad A\sigma_3 = \{\phi_1, \phi_2\}$$

d) $H = \{e, \sigma_1\}$, $K = \{e, \sigma_2\}$ y entonces $HK = \{e, \sigma_1, \sigma_2, \phi_1\}$, que no es un subgrupo de S_3 porque *HK* tiene cuatro elementos.

e) S_3 no es cíclico, puesto que S_3 no es generado por ninguno de sus elementos.

B.9 Sean σ y τ los siguientes elementos del grupo simétrico S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

Encuentre $\tau\sigma$, $\sigma\tau$, σ^2 y σ^{-1}. (Puesto que σ y τ son funciones, $\tau\sigma$ significa aplicar σ y luego τ.)

En la figura B-7 se muestra el efecto sobre 1, 2, . . . , 6 de la composición de las permutaciones:

a) σ y luego τ.

b) τ y luego σ.

c) σ y luego σ; es decir, σ^2.

Entonces:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix}, \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

σ^{-1} se obtiene al intercambiar los renglones superior e inferior de σ, y luego al reagrupar:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

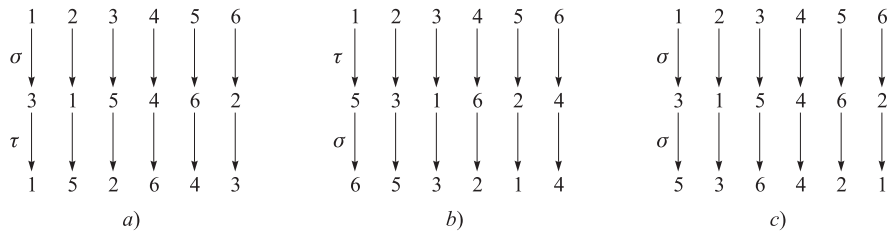


Figura B-7

B.10 Sean H y K grupos.

a) Defina el producto directo de H y K por $G = H \times K$.

b) ¿Cuál es el elemento identidad y cuál es el orden de $G = H \times K$?

c) Describa y encuentre la tabla de multiplicar del grupo $G = \mathbf{Z_2} \times \mathbf{Z_2}$.

a) Sea $G = H \times K$, el producto cartesiano de H y K, con la operación $*$ definida componente por componente por

$$(h, k) * h', k' = (hh', kk')$$

Entonces G es un grupo (problema B.68) denominado producto directo de H y K.

b) El elemento $e = (e_H, e_K)$ es el elemento identidad de G, y $|G| = |H| \cdot |K|$.

c) Puesto que $\mathbf{Z}_2$ tiene dos elementos, G tiene cuatro elementos. Sea

$$e = (0, 0), \quad a = (1, 0), \quad b = (0, 1), \quad c = (1, 1)$$

La tabla de multiplicar de G se muestra en la figura B-8*a*). Observe que G es abeliano puesto que la tabla es simétrica. También, $a^2 = e$, $b^2 = e$, $c^2 = e$. Así, G no es cíclico, por lo cual $G \ncong \mathbf{Z_4}$.

B.11 Sea S el cuadrado en el plano $\mathbf{R}^2$ representado en la figura B-8*b*), con su centro en el origen 0. Observe que los vértices de S están numerados en sentido contrario al movimiento de las manecillas del reloj de 1 a 4.

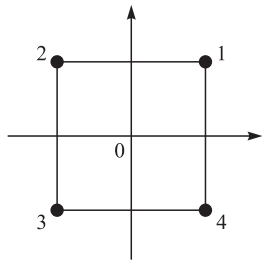
a) Defina el grupo G de simetrías de S.

b) Enumere los elementos de G.

c) Encuentre un conjunto mínimo de generadores de G.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

a)



b)

Figura B-8

a) Una simetría σ de S es una correspondencia rígida uno a uno entre S y S mismo. (Aquí *rígida* significa que las distancias entre puntos no varían.) El grupo G de simetrías de S es el conjunto de todas las simetrías de S bajo composición de transformaciones.

b) Hay ocho simetrías, como sigue. Para $\alpha = 0°, 90°, 180°, 270°$, sea $\sigma(\alpha)$ la simetría obtenida al rotar S α grados alrededor de su centro, y sea $\tau(\alpha)$ la simetría obtenida al reflejar S alrededor del eje y y luego rotar S α grados alrededor de su centro. Observe que cualquier simetría σ de S está determinada completamente por su efecto sobre los vértice de S, de modo que σ puede representarse como una permutación en S_4. Así:

$$\sigma(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\sigma(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 4 \end{pmatrix}, \quad \sigma(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau(0°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \tau(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\tau(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \tau(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

c) Sean $a = \sigma(90°)$ y $b = \tau(0°)$. Entonces a y b forman un conjunto máximo de generadores de G. Específicamente,

$$\sigma(0°) = a^4, \quad \sigma(90°) = a, \quad \sigma(180°) = a^2, \quad \sigma(270°) = a^3$$
$$\tau(0°) = b, \quad \tau(90°) = ba, \quad \tau(180°) = ba^2, \quad \tau(270°) = ba^3$$

y G no es cíclico, de modo que no es generado por un elemento. (Puede demostrarse que las relaciones $a^4 = e$, $b^2 = e$ y $bab = a^{-1}$ describen completamente a G.)

B.12 Sea G un grupo y sea A un conjunto no vacío.

a) Defina el significado de la afirmación "G actúa sobre A".

b) Defina el estabilizador H_a de un elemento $a \in A$.

c) Demuestre que H_a es un subgrupo de G.

a) Sea PERM(A) el grupo de todas las permutaciones de A. Sea $\psi : G \to$ PERM(A) cualquier homomorfismo. Entonces se dice que G actúa sobre A donde cada elemento g en G define una permutación $g : A \to A$ por

$$g(a) = (\psi(g))(a)$$

(A menudo la permutación $g : A \to A$ se proporciona directamente y entonces el homomorfismo está definido de manera implícita.)

b) El estabilizador H_a de $a \in A$ consta de todos los elementos en G que "fijan a a"; es decir,

$$H_a = \{g \in G \mid g(a) = a\}$$

c) Puesto que $e(a) = a$, se tiene $e \in H_a$. Suponga que $g, g' \in H_a$. Entonces $(gg')(a) = g(g'(a)) = g(a) = a$; de modo que $gg' \in H_a$. También, $g^{-1}(a) = a$ puesto que $g(a) = a$; así, $g^{-1} \in H_a$. En consecuencia, H_a es un subgrupo de G.

B.13 Demuestre el teorema B.6: sea H un subgrupo de un grupo G. Entonces las clases laterales derechas de Ha forman una partición de G.

Puesto que $e \in H$ se tiene $a = ea \in Ha$; así, todo elemento pertenece a una clase lateral. Ahora se supone que Ha y Hb no son ajenos. Por ejemplo, $c \in Ha \cap Hb$. La demostración está completa si se demuestra que $Ha = Hb$.

Puesto que c pertenece a Ha y a Hb, se tiene $c = h_1a$ y $c = h_2b$ donde $h_1, h_2 \in H$. Así, $h_1a = h_2b$, y así $a = h_1^{-1} h_2b$. Sea $x \in Ha$. Entonces

$$x = h_3a = h_3h_1^{-1} h_2b$$

donde $h_3 \in H$. Puesto que H es un subgrupo, $h_3h_1^{-1}h_2 \in H$; así, $x \in Hb$. Puesto que x es cualquier elemento de Ha, se tiene $Ha \subseteq Hb$. En forma semejante, $Hb \subseteq Ha$. Ambas inclusiones implican $Ha = Hb$, y se ha demostrado el teorema.

B.14 Sea H un subgrupo finito de G. Demuestre que H y cualquier clase lateral Ha tienen el mismo número de elementos.

Sea $H = \{h_1, h_2, \ldots, h_k\}$, donde H tiene k elementos. Entonces $Ha = \{h_1a, h_2a, \ldots, h_ka\}$.

No obstante, $h_ia = h_ja$ implica $h_i = h_j$; así, los k elementos enumerados en Ha son distintos. Por tanto, H y Ha tienen el mismo número de elementos.

B.15 Demuestre el teorema B.7 (de Lagrange): sea H un subgrupo de un grupo finito G. Entonces el orden de H divide al orden de G.

Suponga que H tiene r elementos y que hay s clases laterales derechas; por ejemplo

$$Ha_1, Ha_2, \ldots, Ha_s$$

Por el teorema B.6, las clases laterales parten a G y por el problema B.14 cada clase lateral tiene r elementos. En consecuencia, G tiene rs elementos, de modo que el orden de H divide al orden de G.

B.16 Demuestre lo siguiente: todo subgrupo de un grupo G cíclico es cíclico.

Puesto que G es cíclico, hay un elemento $a \in G$ tal que $G = gp(a)$. Sea H un subgrupo de G. Si $H = \{e\}$, entonces $H = gp(e)$ y H es cíclico. En caso contrario, H contiene una potencia a distinta de cero. Puesto que H es un subgrupo, debe ser cerrado bajo inversos, de modo que H contiene potencias positivas de a. Sea m la menor potencia positiva de a tal que a^m pertenece a H. Se afirma que $b = a^m$ genera a H. Sea x cualquier otro elemento de H; puesto que x pertenece a G se tiene $x = a^n$ para algún entero n. Al dividir n entre m se obtiene un cociente q y un residuo r; es decir,

$$n = mq + r$$

donde $0 \leq r < m$. Así,

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r \quad \text{por tanto} \quad a^r = b^{-q}a^n$$

Pero a^n, $b \in H$. Puesto que H es un subgrupo, $b^{-q}a^n \in H$, lo cual significa $a^r \in H$. Sin embargo, m es la menor potencia positiva de a que pertenece a H. En consecuencia, $r = 0$. Por tanto, $x = a^n = b^q$. En consecuencia, b genera a H, y H es cíclico.

B.17 Demuestre el teorema B.8: sea H un subgrupo normal de un grupo G. Entonces las clases laterales de H en G forman un grupo bajo multiplicación de clase lateral definida por $(aH)\,(bH) = abH$.

La multiplicación de clases laterales está bien definida, ya que

$$(aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$$

(Aquí se usó el hecho de que H es normal, de modo que $Hb = bH$ y, por el problema B.57, $HH = H$.) La propiedad asociativa de la multiplicación de clases laterales se concluye a partir del hecho de que la asociatividad se cumple en G. El elemento identidad de G/H es H, ya que

$$(aH)H = a(HH) = aH \quad \text{y} \quad H(aH) = (Ha)H = (aH)H = aH$$

Por último, $a^{-1}H$ es el inverso de aH, ya que

$$(a^{-1}H)(aH) = a^{-1}aHH = eH = H \quad \text{y} \quad (aH)(a^{-1}H) = aa^{-1}HH = eH = H$$

Por tanto, G/H es un grupo bajo multiplicación de clases laterales.

B.18 Suponga que $F : G \to G'$ es un homomorfismo de grupos. Demuestre: *a*) $f(e) = e'$; *b*) $(fa^{-6}) = f(a)^{-1}$.

a) Puesto que $e = ee$ y f es un homomorfismo, se tiene

$$f(e) = f(ee) = f(e)\,f(e)$$

Al multiplicar ambos miembros por $f(e)^{-1}$ se obtiene el resultado.

b) Al aplicar el inciso *a*) y el hecho de que $aa^{-1} = a^{-1}a = e$, se tiene

$$e' = f(e) = f(aa^{-1}) = f(a)\,f(a^{-1}) \quad \text{y} \quad e' = f(e) = f(a^{-1}a) = f(a^{-1})\,f(a)$$

Por tanto, $f(a^{-1})$ es el inverso de $f(a)$; es decir, $f(a^{-1}) = f(a)^{-1}$.

B.19 Demuestre el teorema B.9: sea $f : G \to G'$ un homomorfismo con kernel K. Entonces K es un subgrupo normal de G y G/K es isomorfo a la imagen de f. (Compare con el problema B.5 el teorema semejante para semigrupos.)

Demostración de que K es normal: por el problema B.18, $f(e) = e'$, de modo que $e \in K$. Luego, se supone que $a, b \in K$ y $g \in G$. Así, $f(a) = e'$ y $f(b) = e'$. Por tanto,

$$\begin{aligned} f(ab) &= f(a)\,f(b) = e'e' = e' \\ f(a^{-1}) &= f(a)^{-1} = e'^{-1} = e' \\ f(gag^{-1}) &= f(g)f(a)f(g^{-1}) = f(g)e'f(g)^{-1} = e' \end{aligned}$$

Entonces, ab, a^{-1} y gag^{-1} pertenecen a K, de modo que K es un subgrupo normal.

Demostración de que $G/K \cong H$, donde H es la imagen de f: sea φ: $G/K \to H$ definida por

$$\varphi(Ka) = f(a)$$

Se demuestra que φ está bien definido; es decir, si $Ka = Kb$ entonces $\varphi(Ka) = \varphi(Kb)$. Se supone que $Ka = Kb$. Entonces $ab^{-1} \in K$ (problema B.57). Así, $f(ab^{-1}) = e'$, y así

$$f(a)f(b)^{-1} = f(a)\,f(b^{-1}) = f(ab^{-1}) = e'$$

Por tanto, $f(a) = f(b)$, de modo que $\varphi(Ka) = \varphi(Kb)$. Así, φ está bien definido.

A continuación se demuestra que φ es un homomorfismo:

$$\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)\,f(b) = \varphi(Ka)\varphi(Kb)$$

Por tanto, φ es un homomorfismo. Luego se demuestra que φ es uno a uno. Se supone que $\varphi(Ka) = \varphi(Kb)$. Entonces

$$f(a) = f(b) \quad \text{o} \quad f(a)\,f(b)^{-1} = e' \quad \text{o} \quad f(a)\,f(b^{-1}) = e' \quad \text{o} \quad f(ab^{-1}) = e'$$

Entonces, $ab^{-1} \in K$, y por el problema B.57 se tiene $Ka = Kb$. Por tanto, φ es uno a uno. A continuación se demuestra que φ es sobre. Sea $h \in H$. Puesto que H es la imagen de f, existe $a \in G$ tal que $f(a) = h$. Así, $\varphi(Ka) = f(a) = h$, de modo que φ es sobre. En consecuencia, $G/K \cong H$ y así se ha demostrado el teorema.

ANILLOS, DOMINIOS DE INTEGRIDAD, CAMPOS

B.20 Considere el anillo $\mathbf{Z_{10}} = \{0, 1, 2, \ldots, 9\}$ de enteros módulo 10. *a*) Encuentre las unidades de $\mathbf{Z_{10}}$. *b*) Encuentre -3, -8 y 3^{-1}. *c*) Sea $f(x) = 2x^2 + 4x + 4$. Encuentre las raíces de $f(x)$ sobre $\mathbf{Z_{10}}$.

a) Por el problema B.78, los enteros primos relativos con el módulo $m = 10$ son las unidades de $\mathbf{Z_{10}}$. Por tanto, las unidades son 1, 3, 7 y 9.

b) Recuerde que $-a$ en un anillo R es el elemento tal que $a+(-a) = (-a)+a = 0$. Por tanto, $-3 = 7$, ya que $3 + 7 = 7 + 3 = 0$ en $\mathbf{Z_{10}}$. En forma semejante, $-8 = 2$. Recuerde que a^{-1} en un anillo R es el elemento tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Por tanto, $3^{-1} = 7$ puesto que $3 \cdot 7 = 7 \cdot 3 = 1$ en $\mathbf{Z_{10}}$.

c) Cada uno de los 10 elementos en $\mathbf{Z_{10}}$ se sustituye en $f(x)$ para ver cuál produce 0. Se tiene:

$$f(0) = 4, \quad f(2) = 0, \quad f(4) = 2, \quad f(6) = 0, \quad f(8) = 4$$
$$f(1) = 0, \quad f(3) = 4, \quad f(5) = 4, \quad f(7) = 0, \quad f(9) = 2$$

Por tanto, las raíces son 1, 2, 6 y 7. (Este ejemplo muestra que un polinomio de grado n puede tener más de n raíces sobre un anillo arbitrario. Esto no puede ocurrir si el anillo es un campo.)

B.21 Demuestre que en un anillo R: *i*) $a \cdot 0 = 0 \cdot a = 0$; *ii*) $a(-b) = (-a)b = -ab$; *iii*) $(-1)a = -a$ (cuando R tiene un elemento identidad 1).

i) Puesto que $0 = 0 + 0$, se tiene

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Al sumar $-(a \cdot 0)$ a ambos miembros se obtiene $0 = a \cdot 0$. En forma semejante, $0 \cdot a = 0$.

ii) Al usar $b + (-b) = (-b) + b = 0$, se tiene

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$$
$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

Por tanto, $a(-b)$ es el negativo de ab; es decir, $a(-b) = -ab$. En forma semejante, $(-a)b = -ab$.

iii) Se tiene

$$a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$$
$$(-1)a + a = (-1)a + 1 \cdot a = ((-1) + 1)a = 0 \cdot a = 0$$

Por tanto, $(-1)a$ es el negativo de a; es decir, $(-1)a = -a$.

B.22 Sea D un dominio de integridad. Demuestre que si $ab = ac$ con $a \neq 0$, entonces $b = c$.

Puesto que $ab = ac$, se tiene

$$ab - ac = 0 \text{ de modo que } a(b - c) = 0$$

Puesto que $a \neq 0$, debe tenerse $b - c = 0$, ya que D no tiene divisores cero. Por tanto, $b = c$.

B.23 Suponga que J y K son ideales en un anillo R. Demuestre que $J \cap K$ es un ideal en R.

Puesto que J y K son ideales, $0 \in J$ y $0 \in K$. Entonces, $0 \in J \cap K$. Luego, sea $a, b \in J \cap K$ y sea $r \in R$. Entonces $a, b \in J$ y $a, b \in K$. Puesto que J y K son ideales,

$$a - b, ra, ar \in J \quad \text{y} \quad a - b, ra, ar \in K$$

Entonces, $a - b, ra, ar \in J \cap K$. Por consiguiente, $J \cap K$ es un ideal.

B.24 Sea J un ideal en un anillo R con elemento identidad 1. Demuestre: *a*) Si $1 \in J$ entonces $J = R$; *b*) Si cualquier unidad $u \in J$ entonces $J = R$.

a) Si $1 \in J$ entonces para cualquier $r \in R$ se tiene $r \cdot 1 \in R$ o $r \in J$. Por tanto $J = R$.

b) Si $u \in J$ entonces $u^{-1} \cdot u \in J$ o $1 \in J$. Por tanto $J = R$ por el inciso *a*).

B.25 Demuestre lo siguiente: *a*) Un dominio de integridad finito D es un campo. *b*) $\mathbf{Z_p}$ es un campo, donde p es un número primo. *c*) (Fermat) Si p es primo, entonces $a^p \equiv a$ (mód p) para cualquier entero a.

a) Suponga que D tiene n elementos; por ejemplo, $D = \{a_1, a_2, \ldots, a_n\}$. Sea a cualquier elemento de D diferente de cero Considere los n elementos

$$aa_1, aa_2, \ldots, a_n$$

Puesto que $a \neq 0$, se tiene $aa_i = aa_k$ implica $a_i = a_k$ (problema B.22). Por tanto, los n elementos anteriores son distintos, de modo que deben ser un reagrupamiento de los elementos de D. Uno de ellos; por ejemplo aa_k, debe ser igual al elemento identidad 1 de D; es decir, $aa_k = 1$. Por tanto, a_k es el inverso de a. Puesto que a es cualquier elemento de D distinto de cero, se tiene que D es un campo.

b) Recuerde que $\mathbf{Z_p} = \{0, 1, 2, \ldots, p - 1\}$. Se demostrará que $\mathbf{Z_p}$ no tiene divisores cero. Suponga que $a * b = 0$ en $\mathbf{Z_p}$; es decir 0 (mód p). Entonces p divide a ab. Puesto que p es primo, p divide a a o p divide a b. Por tanto, $a \equiv 0$ (mód p) o $b \equiv 0$ (mód p); es decir, $a = 0$ o $b = 0$ en $\mathbf{Z_p}$. En consecuencia, $\mathbf{Z_p}$ no tiene divisores cero y por tanto $\mathbf{Z_p}$ es un dominio de integridad. Por el inciso *a*), $\mathbf{Z_p}$ es un campo.

c) Si p divide a a, entonces $a \equiv 0$ (mód p) y así $a^p \equiv a \equiv 0$ (mód p). Suponga que p no divide a a. Entonces a puede considerarse como un elemento distinto de cero de $\mathbf{Z_p}$. Puesto que $\mathbf{Z_p}$ es un campo, sus elementos distintos de cero forman un grupo G de orden $p - 1$ bajo la multiplicación. Por el problema B.45, $a^{p-1} = 1$ en $\mathbf{Z_p}$.

En otras palabras, $a^{p-1} \equiv 1$ (mód p). Al multiplicar por a se obtiene $a^p \equiv a$(mód p), y así se ha demostrado el teorema.

POLINOMIOS SOBRE UN CAMPO

B.26 Suponga que $f(t) = 2t^3 - 3t^2 - 6t - 2$. Encuentre todas las raíces de $f(t)$ si se sabe que $f(t)$ tiene una raíz racional.

Las raíces racionales de $f(t)$ deben estar entre $\pm 1, \pm 2, \pm 1/2$. Al probar cada raíz posible, se obtiene, por división sintética (o al dividir entre $2t + 1$),

$$\begin{array}{r|l} -\frac{1}{2} & 2 - 3 - 6 - 2 \\ & \quad -1 + 2 + 2 \\ \hline & 2 - 4 - 4 + 0 \end{array}$$

En consecuencia, $t = -1/2$ es una raíz y

$$f(t) = (t + 1/2)(2t^2 - 4t - 4) = (2t + 1)(t^2 - 2t - 2)$$

Ahora es posible aplicar la fórmula cuadrática a $t^2 - 2t - 2$ para obtener las tres siguientes raíces de $f(t)$:

$$t = -1/2, \quad t = 1 + \sqrt{3}, \quad t = 1 - \sqrt{3}$$

B.27 Sea $f(t) = t^4 - 3t^3 + 3t^2 + 3t - 20$. Encuentre todas las raíces de $f(t)$ dado que $t = 1 + 2i$ es una raíz.

Puesto que $1 + 2i$ es una raíz, entonces $1 - 2i$ es una raíz y $c(t) = t^2 - 2t + 5$ es un factor de $f(t)$. Al dividir $f(t)$ entre $c(t)$ se obtiene

$$f(t) = (t^2 - 2t + 5)(t^2 - t - 4)$$

La fórmula cuadrática con $t^2 - t - 4$ proporciona las otras dos raíces de $f(t)$. Es decir, las cuatro raíces de $f(t)$ son las siguientes:

$$t = 1 + 2i, \quad t = 1 - 2i, \quad t = (1 + \sqrt{17})/2, \quad t = (1 - \sqrt{17})/2$$

B.28 Sea $K = \mathbf{Z_8}$. Encuentre todas las raíces de $f(t) = t^2 + 6t$.

Aquí $\mathbf{Z_8} = \{0, 1, 2, \ldots, 7\}$. Cada elemento de $\mathbf{Z_8}$ se sustituye en $f(t)$ para obtener:

$$f(0) = 0, \quad f(2) = 0, \quad f(4) = 0, \quad f(6) = 0$$

Así, $f(t)$ tiene cuatro raíces: $t = 0, 2, 4, 6$. (El teorema B.21 no se cumple en este caso porque K no es un campo.)

B.29 Suponga que $f(t)$ es un polinomio real con grado impar n. Demuestre que $f(t)$ tiene una raíz real.

Las raíces complejas (no reales) se presentan por pares. Puesto que $f(t)$ tiene un número impar n de raíces (contando multiplicidad), $f(t)$ debe tener por lo menos una raíz real.

B.30 Demuestre el teorema B.15 (algoritmo euclidiano de la división): sean $f(t)$ y $g(t)$ polinomios sobre un campo K con $g(t) \neq 0$. Entonces existen polinomios $q(t)$ y $r(t)$ tales que

$$f(t) = q(t)g(t) + r(t)$$

donde $r(t) \equiv 0$ o $\text{gr}(r) < \text{gr}(g)$.

Si $f(t) = 0$ o si $\text{gr}(f) < \text{gr}(g)$, entonces se tiene la representación requerida $f(t) = 0g(t) + f(t)$. Luego, se supone que $\text{gr}(f) \geq \text{gr}(g)$, por ejemplo,

$$f(t) = a_n t^n + \cdots + a_1 t + a_0 \quad \text{y} \quad g(t) = b_m t^m + \cdots + b_1 t + b_0$$

donde $a_n, b_m \neq 0$ y $n > m$. Se forma el polinomio

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t) \tag{1}$$

(Éste es el primer paso de la sustracción en la "división larga".) Entonces, $\text{gr}(f_1) < \text{gr}(f)$. Por inducción, existen polinomios $q_1(t)$ y $r(t)$ tales que $f_1(t) = q1(t)g(t) + r(t)$ donde $r(t) \equiv 0$ o $\deg(r) < \deg(g)$. Al sustituir esto en la ecuación (1) y despejar $f(t)$, se obtiene

$$f(t) = \left[q_1(t) + \frac{a_n}{b_m} t^{n-m}\right] g(t) + r(t)$$

que es la representación deseada.

B.31 Demuestre el teorema B.18: suponga que $f(t)$ es un polinomio sobre un campo K, y que $\text{gr}(f) = n$. Entonces $f(t)$ tiene cuando mucho n raíces.

La demostración es por inducción sobre n. Si $n = 1$, entonces $f(t) = at + b$ y $f(t)$ tiene la raíz única $t = -b/a$. Suponga que $n > 1$. Si $f(t)$ no tiene ninguna raíz, entonces el teorema es verdadero. Suponga que $a \in K$ es una raíz de $f(t)$. Entonces

$$f(t) = (t - a)g(t)$$

donde $\text{gr}(g) = n - 1$. Se afirma que cualquiera otra raíz de $f(t)$ también debe ser una raíz de $g(t)$.

Suponga que $b \neq a$ es otra raíz de $f(t)$. Al sustituir $t = b$ en (1) se obtiene $0 = f(b) = (b - a)g(b)$.

Puesto que K no tiene divisores cero y $b - a \neq 0$, debe tenerse $g(b) = 0$. Por inducción, $g(t)$ tiene a lo sumo $n - 1$ raíces. Por tanto, $f(t)$ tiene cuando mucho $n - 1$ raíces además de a. Así que, $f(t)$ tiene como máximo n raíces.

B.32 Demuestre el teorema B.19: suponga que un racional p/q (reducido a su mínima expresión) es la raíz del polinomio

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

donde todos los coeficientes $a_n, \ldots, a_1, a_0$ son enteros. Entonces p divide al término constante a_0 y q divide a los coeficientes principales a_n. En particular, si $c = p/q$ es un entero, entonces c divide al término constante a_0.

$t = p/q$ se sustituye en $f(t) = 0$ para obtener $a_n(p/q)^n + \cdots + a_1(p/q) + a_0 = 0$. Ambos miembros de la ecuación se multiplican por q^n para obtener

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \tag{1}$$

Puesto que p divide a todos los n primeros términos de (1), p debe dividir al último término, $a_0 q^n$. Si se supone que p y q son primos relativos, entonces p divide a a_0. En forma semejante, q divide a los n últimos términos de (1), de modo que q divide al primer término, $a_n p^n$. Debido a que p y q son primos relativos, q divide a a_n.

B.33 Demuestre el teorema B.20: el anillo $K[t]$ de polinomios sobre un campo K es un dominio ideal principal (DIP). Si J es un ideal en $K[t]$, entonces existe un monomio único d que genera a J; es decir, todo polinomio f en J es un múltiplo de d.

Sea d el polinomio de menor grado en J. Puesto que es posible multiplicar d por un escalar diferente de cero y seguir perteneciendo a J, es posible suponer sin pérdida de generalidad que d es un monomio (con coeficiente principal igual a 1). Luego, se supone que $f \in J$. Por el algoritmo de la división, existen polinomios q y r tales que $f = qd + r$, donde $r \equiv 0$ o $\text{gr}(r) < \text{gr}(d)$. Luego, $f, d \in J$ implica $qd \in J$ y por tanto $r = f - qd \in J$. Sin embargo, d es el polinomio de menor grado en J. En consecuencia, $r \equiv 0$ y $f = qd$; es decir, d divide a f. Queda por demostrar que d es único. Si d' es otro monomio que genera a J, entonces d divide a d' y d' divide a d. Esto implica que $d = d'$, ya que d y d' son monomios. Así, se ha demostrado el teorema.

B.34 Demuestre el teorema B.21: sean f y g polinomios en $K[t]$, ninguno es un polinomio cero. Entonces existe un monomio único d tal que: *i*) d divide a f y a g. *ii*) Si d' divide a f y a g, entonces d' divide a d.

El conjunto $I = \{mf + ng \mid m, n \in K[t]\}$ es un ideal. Sea d el monomio que genera a I. Observe que $f, g \in I$; por tanto, d divide a f y a g. Ahora se supone que d' divide a f y a g. Sea J el ideal generado por d'. Entonces $f, g \in J$ y por tanto $I \subseteq J$. En consecuencia, $d \in J$ y así d' divide a d, como se había afirmado. Queda por demostrar que d es único. Si d_1 es otro máximo común divisor (monomio) de f y g, entonces d divide a d_1 y d_1 divide a d. Esto implica que $d = d_1$ porque d y d_1 son monomios. Así, se ha demostrado el teorema.

B.35 Demuestre el corolario B.22: sea d el máximo común divisor de f y g. Entonces existen polinomios m y n tales que $d = mf + ng$. En particular, si f y g son primos relativos, entonces existen polinomios m y n tales que $mf + ng = 1$.

A partir de la demostración del teorema B.21 en el problema B.34, el máximo común divisor d genera el ideal $I = \{mf + ng \mid m, n \in K[t]\}$. Por tanto, existen polinomios m y n tales que $d = mf + ng$.

B.36 Demuestre el lema B.23: suponga que $p \in K[t]$ es irreducible. Si p divide al producto fg de polinomios $f, g \in K[t]$, entonces p divide a f o p divide a g. En términos más generales, si p divide al producto $f_1 f_2 \cdots f_n$ de n polinomios, entonces p divide a uno de ellos.

Suponga que p divide a fg pero no a f. Puesto que p es irreducible, los polinomios f y p deben ser primos relativos. Por tanto, existen polinomios $m, n \in K[t]$ tales que $mf + np = 1$. Al multiplicar esta ecuación por g, se obtiene $mfg + npg = g$. Sin embargo, p divide a fg y así p divide a mfg. También, p divide a npg. En consecuencia, p divide a la suma $g = mfg + npg$.

Ahora se supone que p divide a $f_1 f_2 \cdots f_n$. Si p divide a f_1, entonces ya se ha terminado. De no hacerlo, entonces por el resultado anterior p divide al producto $f_2 \cdots f_n$. Por inducción sobre n, p divide a uno de los polinomios en el producto $f_{22} \cdots f_n$. Así, se ha demostrado el lema.

B.37 Demuestre el teorema B.24 (teorema de factorización única): sea f un polinomio distinto de cero en $K[t]$. Entonces f puede escribirse en forma única (salvo por el orden) como un producto $f = kp_1p_2 \cdots p_n$ donde $k \in K$ y los p son monomios únicos irreducibles en $K[t]$.

Primero se demuestra la existencia de este producto. Si f es irreducible o si $f \in K$, entonces resulta evidente que este producto existe. Por otra parte, se supone que $f = gh$, donde g y h no son escalares. Entonces g y h tienen grado menor o igual que el grado de f. Por inducción, puede suponerse que $g = k_1g_1g_2 \cdots g_r$ y $h = k_2h_1h_2 \cdots h_s$ donde $k_1, k_2 \in K$ y los g_i y los h_j son monomios irreducibles. En consecuencia, la representación deseada es la siguiente:

$$f = (k_1k_2)g_1g_2 \cdots g_rh_1h_2 \cdots h_s$$

A continuación se demuestra la unicidad (salvo por el orden) de tal producto para f. Suponga que

$$f = kp_1p_2 \ldots p_n = k'q_1q2 \ldots q_m \quad \text{donde} \quad k, k' \in K$$

y los $p_1, \ldots, p_n, q_1, \ldots, q_m$ son monomios irreducibles. Así, p_1 divide a $k'q_1 \ldots q_m$. Puesto que p_1 es irreducible, debe dividir a uno de los q por el lema B.23. Por ejemplo, sea que p_1 divide a q_1. Puesto que p_1 y q_1 son monomios irreducibles, $p_1 = q_1$. En consecuencia, $kp_2 \ldots p_n = k' q_2 \ldots q_m$. Por inducción, se tiene que $n = m$ y $p_2 = q_2, \ldots, p_n = q_m$ para algún reordenamiento de los q. También se tiene que $k = k'$. Así, se ha demostrado el teorema.

B.38 Demuestre el teorema B.25: suponga que $f(t)$ es un polinomio sobre el campo real $\mathbf{R}$, y suponga que el número complejo $z = a + bi$, $b \neq 0$, es una raíz de $f(t)$. Entonces el conjugado complejo $\bar{z} = a - bi$ también es una raíz de $f(t)$. Por tanto, la siguiente expresión es un factor de $f(t)$:

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

Al dividir $f(t)$ entre $c(t)$, donde $\text{gr}(c) = 2$, existen $q(t)$ y números reales M y N tales que

$$f(t) = c(t)\,q(t) + Mt + N \tag{1}$$

Puesto que $z = a + bi$ es una raíz de $f(t)$ y $c(t)$, se tiene, al sustituir $t = a + bi$ en (1),

$$f(z) = c(z)\,q(z) + M(z) + n \quad \text{o} \quad 0 = 0q(z) + M(z) + N \quad \text{o} \quad M(a + bi) + N = 0$$

Por tanto, $Ma + N = 0$ y $Mb = 0$. Puesto que $b \neq 0$, debe tenerse $M = 0$. Entonces, $0 + N = 0$ o $N = 0$. En consecuencia, $f(t) = c(t)\,q(t)$ y $\bar{z} = a - bi$ es una raíz de $f(t)$.

PROBLEMAS SUPLEMENTARIOS

OPERACIONES Y SEMIGRUPOS

B.39 Considere el conjunto $\mathbf{N}$ de enteros positivos y sea * la operación mínimo común múltiplo (mcm) en $\mathbf{N}$.

a) Encuentre $4 * 6$, $3 * 5$, $9 * 18$, $1 * 6$.

b) ¿$(\mathbf{N}, *)$ es un semigrupo? ¿Es conmutativo?

c) Encuentre el elemento identidad de $*$.

d) ¿Cuáles elementos de $\mathbf{N}$, en caso de haberlos, tienen inverso y cuáles son?

B.40 Sea $*$ la operación en el conjunto $\mathbf{R}$ de números reales definida por $a * b = a + b + 2ab$.

a) Encuentre $2 * 3$, $3 * (-5)$, y $7 * (1/2)$.
b) ¿$(\mathbf{R}, *)$ es un semigrupo? ¿Es conmutativo?
c) Encuentre el elemento identidad de $*$.
d) ¿Cuáles elementos de $\mathbf{N}$ tienen inverso y cuáles son?

B.41 Sea A un conjunto no vacío con la operación $*$ definida por $a * b = a$, y suponga que A tiene más de un elemento.

a) ¿A es un semigrupo?
b) ¿A es conmutativo?
c) ¿A tiene elemento identidad?
d) ¿Cuáles elementos de A, en caso de haberlos, tienen inverso y cuáles son?

B.42 Sea $A = \{a, b\}$.

a) Encuentre el número de operaciones en A.
b) Muestre una operación que no sea asociativa ni conmutativa.

B.43 Para cada uno de los siguientes conjuntos, determine cuál es cerrado bajo *a*) multiplicación, *b*) adición.

$A = \{0, 1\}$, $B = \{1, 2\}$, $C = \{x \mid x \text{ es primo}\}$, $D = \{2, 4, 8, \ldots\} = \{x \mid x = 2^n\}$.

B.44 Sea $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, los múltiplos de 3. ¿$A$ es cerrado bajo

a) adición?
b) multiplicación?
c) sustracción?
d) división (excepto entre 0)?

B.45 Encuentre un conjunto A con tres enteros que sea cerrado bajo *a*) multiplicación; *b*) adición.

B.46 Sea S un conjunto infinito. Sean A la colección de conjuntos finitos de S y B la colección de conjuntos infinitos de S.

a) ¿A es cerrado bajo *i*) unión?; *ii*) intersección? *iii*) complementos?
b) ¿B es cerrado bajo *i*) unión?; *ii*) intersección? *iii*) complementos?

B.47 Sea $S = \mathbf{Q} \times \mathbf{Q}$, el conjunto de pares ordenados de números racionales, con la operación * definida por

$$(a, b) * (x, y) = (ax, ay + b)$$

a) Encuentre $(3, 4) * (1, 2)$ y $(-1, 3) * (5, 2)$.
b) ¿S es un semigrupo? ¿Es conmutativo?
c) Encuentre el elemento identidad de S.
d) ¿Cuáles elementos, en caso de haberlos, tienen inverso y cuáles son?

B.48 Sea $S = \mathbf{N} \times N$, el conjunto de pares ordenados de enteros positivos, con la operación * definida por

$$(a, b) * (c, d) = (ad + bc, bd)$$

a) Encuentre $(3, 4) * (1, 5)$ y $(2, 1) * (4, 7)$.
b) Demuestre que * es asociativa. (Y así, que S es un semigrupo.)
c) Defina $f : (S, *) \to (\mathbf{Q}, +)$ por $f(a, b) = a/b$. Demuestre que f es un homomorfismo.
d) Encuentre la relación de congruencia $\sim$ en S determinada por el homomorfismo f; es decir, $x \sim y$ si $f(x) = f(y)$.
e) Describa $S/\sim$. ¿$S/\sim$ tiene un elemento identidad? ¿Tiene inversos?

B.49 Sea $S = \mathbf{N} \times \mathbf{N}$. Sea * la operación en S definida por

$$(a, b) * (a', b') = (a + a', b + b')$$

a) Encuentre $(3, 4) * (1, 5)$ y $(2, 1) * (4, 7)$.
b) Demuestre que * es asociativa. (Y así, que S es un semigrupo.)
c) Defina $f : (S, *) \to (\mathbf{Z}, +)$ por $f(a,b) = a - b$. Demuestre que f es un homomorfismo.
d) Encuentre la relación de congruencia $\sim$ en S determinada por el homomorfismo f.
e) Describa $S/\sim$. ¿$S/\sim$ tiene un elemento identidad? ¿Tiene inversos?

GRUPOS

B.50 Considere $\mathbf{Z_{20}} = \{0, 1, 2, \ldots, 19\}$ bajo la adición módulo 20. Sea H el subgrupo generado por 5. *a*) Encuentre los elementos y el orden de H. *b*) Encuentre las clases laterales de H en $\mathbf{Z_{20}}$.

B.51 Considere $G = \{1, 5, 7, 11\}$ bajo la multiplicación módulo 12. *a*) Encuentre el orden de cada elemento. *b*) ¿G es cíclico? *c*) Encuentre todos los subgrupos de G.

B.52 Considere $G = \{1, 5, 7, 11, 13, 17\}$ bajo la multiplicación módulo 18. *a*) Escriba la tabla de multiplicar de G. *b*) Encuentre 5^{-1}, 7^{-1} y 17^{-1}. *c*) Encuentre el orden y el grupo generado por: *i*) 5; *ii*) 13 *d*) ¿G es cíclico?

B.53 Considere el grupo simétrico S_4. Sean $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

a) Encuentre $\alpha\beta$, $\beta\alpha$, α^2, α^{-1}. *b*) Encuentre los órdenes de α, β y $\alpha\beta$.

B.54 Demuestre los siguientes resultados para un grupo G.

a) El elemento identidad e es único.
b) Cada a en G tiene un inverso único a^{-1}.
c) $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$ y, en forma más general, $(a_r a_2 \ldots a_n) = a_n^{-1} \ldots a_2^{-1} a_1^{-1}$.
d) $ab = ac$ implica $b = c$ y $ba = ca$ implica $b = c$.
e) Para enteros arbitrarios r y s, se tiene $a^r a^s = a^{r+s}$, $(a^r)s = a^{rs}$.
f) G es abeliano si y sólo si $(ab)^2 = a^2 b^2$ para toda $a, b \in G$.

B.55 Sea H un subgrupo de G. Demuestre: *a*) $H = Ha$ si y sólo si $a \in H$. *b*) $Ha = Hb$ si y sólo si $ab^{-1} \in H$, *c*) $HH = H$.

B.56 Demuestre la proposición B.5: un subconjunto H de un grupo G es un subgrupo de G si: *i*) $e \in H$, *ii*) para toda $a, b \in H$, se tiene ab, $a^{-1} \in H$.

B.57 Sea G un grupo. Demuestre:

a) La intersección de cualquier número de subgrupos de G es un subgrupo de G.
b) Para cualquier $A \subseteq G$, $gp(A)$ es igual a la intersección de todos los subgrupos de G que contienen a A.
c) La intersección de cualquier número de subgrupos normales de G es un subgrupo normal de G.

B.58 Suponga que G es un grupo abeliano. Demuestre que cualquier grupo de factores G/H también es abeliano.

B.59 Suponga que $|G| = p$, donde p es primo. Demuestre: *a*) G no tiene subgrupos, excepto G y $\{e\}$. *b*) G es cíclico y todo elemento $a \neq e$ genera a G.

B.60 Demuestre que $G = \{1, -1, i, -i\}$ es un grupo bajo multiplicación y proporcione un isomorfismo explícito $G \cong \mathbf{Z_4}$ para demostrar que $f: G \to \mathbf{Z_4}$.

B.61. Sea H un subgrupo de G con sólo dos clases laterales derechas. Demuestre que H es normal.

B.62 Sea $S = \mathbf{R^2}$ el plano cartesiano. Encuentre el estabilizador H_a de $a = (1, 0)$ en S, donde G es el siguiente grupo que actúa sobre S:

a) $G = \mathbf{Z} \times \mathbf{Z}$ y G actúa sobre S por medio de $g(x, y) = (x + m, y + n)$ donde $g = (m, n)$. Es decir, cada elemento g en G es una traslación de S.
b) $G = (\mathbf{R}, +)$ y G actúa sobre S por medio de $g(x, y) = g(x \cos g - y \text{ sen } g, x \text{ sen } g + y \cos g)$. Es decir, cada elemento en G rota S un ángulo g alrededor del origen.

B.63 Sea S un polígono regular con n lados, y sea G el grupo de simetrías de S.

a) Encuentre el orden de G.
b) Demuestre que G es generado por dos elementos a y b tales que $a^n = e$, $b^2 = e$ y $b^{-1}ab = a^{-1}$. (G se denomina *grupo diédrico*.)

B.64 Suponga que un grupo G actúa sobre un conjunto S mediante, por ejemplo, el homomorfismo Ψ:→PERM(S).

a) Demuestre que, para cualquier $s \in S$: *i*) $e(s) = s$ y *ii*) $(gg')(s) = g(g'(s))$, donde $g, g \in G$.
b) La órbita G_S de cualquier $s \in S$ se define por $G_s = \{g(s) \mid g \in G\}$. Demuestre que las órbitas forman una partición de S.
c) Demuestre que $|G_S|$ = el número de clases laterales del estabilizador H_S de s en G. (Recuerde que $H_S = \{g \in G \mid g(s) \in s\}$.)

B.65 Sea G un grupo abeliano y sea n un entero positivo fijo. Demuestre que la función $f: G \to G$ definida por $f(a) = a^n$ es un homomorfismo.

B.66 Sea G el grupo multiplicativo de los números complejos z tales que $|z| = 1$, y sea $\mathbf{R}$ el grupo aditivo de números reales. Demuestre $G \cong \mathbf{R}/\mathbf{Z}$.

B.67 Suponga que H y N son subgrupos de G, donde N es normal. Demuestre que: *a*) HN es un subgrupo de G. *b*) $H \cap N$ es un subgrupo normal de H. *c*) $H/(H \cap N) \cong HN/N$.

B.68 Sean H y K subgrupos. Sea G el conjunto producto $H \times K$ con la operación

$$(h, k) * (h', k') = (hh' , kk').$$

a) Demuestre que G es un grupo (denominado *producto directo* de H y K).

b) Sea $H' = H \times \{e\}$. Demuestre que: *i*) $H' \cong H$; *ii*) H' es un subgrupo normal de G; *iii*) $G/H' \cong K$.

ANILLOS

B.69 Considere el anillo $\mathbf{Z_{12}} = \{0, 1, \ldots, 11\}$ de enteros módulo 12. *a*) Encuentre las unidades de $\mathbf{Z_{12}}$. *b*) Encuentre las raíces de $f(x) = x^2 + 4x + 4$ sobre $\mathbf{Z_{12}}$. *c*) Encuentre los asociados de 2.

B.70 Considere el anillo $\mathbf{Z_{30}} = \{0, 1, \ldots, 29\}$ de enteros módulo 30.

a) Encuentre -2, -7 y -11. *b*) Encuentre 7^{-1}, 11^{-1} y 26^{-1}.

B.71 Demuestre que en un anillo R: *a*) $(-a)(-b) = ab$; *b*) $(-1)(-1) = 1$, si R tiene un elemento identidad 1.

B.72 Suponga que $a^2 = a$ para toda $a \in R$. (Un anillo así se denomina anillo *booleano*.) Demuestre que R es conmutativo.

B.73 Sea R un anillo con elemento identidad 1. R se convierte en otro anillo R' al definir:

$$a \oplus b = a + b + 1 \quad \text{y} \quad a * b = ab + a + b$$

a) Compruebe que R' es un anillo. *b*) Determine el elemento 0 y el elemento 1 de R'.

B.74 Sea G cualquier grupo abeliano (aditivo). La multiplicación en G se define por $a * b = 0$ para todo $a, b \in G$. Demuestre que esto convierte a G en un anillo.

B.75 Sean J y K ideales en un anillo R. Demuestre que $J + K$ y $J \cap K$ también son ideales.

B.76 Sea R un anillo con unidad 1. Demuestre que $a) = \{ra \mid r \in R\}$ es el menor ideal que contiene a a.

B.77 Demuestre que R y $\{0\}$ son ideales de cualquier anillo R.

B.78 Demuestre lo siguiente: *a*) Las unidades de un anillo R forman un grupo bajo multiplicación. *b*) Las unidades en $\mathbf{Z_m}$ son los enteros que son primos relativos con m.

B.79 Para cualquier entero positivo m, compruebe que $m\mathbf{Z} = \{rm \mid r \in \mathbf{Z}\}$ es un anillo. Demuestre que $2\mathbf{Z}$ y $3\mathbf{Z}$ no son isomorfos.

B.80 Demuestre el teorema B.10: sea J un ideal en un anillo R. Entonces las clases laterales $\{a + J \mid a \in R\}$ forman un anillo bajo las operaciones de clases laterales $(a + J) + (b + J) = a + b + J$ y $(a + J)(b + J) = ab + J$.

B.81 Demuestre el teorema B.11: sea $f: R \to R'$ un homomorfismo de anillos con kernel K. Entonces K es un ideal en R, y el anillo cociente R/K es isomorfo a $f(R)$.

B.82 Sea J un ideal en un anillo R. Considere la transformación (canónica) $f: R \to R/J$ definida por $f(a) = a + J$. Demuestre que: *a*) f es un homomorfismo de anillos; *b*) f es una transformación sobre.

B.83 Suponga que J es un ideal en un anillo R. Demuestre que: *a*) Si R es conmutativo, entonces R/J es conmutativo. *b*) Si R tiene elemento unidad 1 y $1 \notin J$, entonces $1 + R$ es un elemento unidad para R/J.

DOMINIOS DE INTEGRIDAD Y CAMPOS

B.84 Demuestre que si $x^2 = 1$ en un dominio de integridad D, entonces $x = -1$ o $x = 1$.

B.85 Sea $R \neq \{0\}$ un anillo conmutativo finito sin divisores cero. Demuestre que R es un dominio de integridad; es decir, que R tiene un elemento identidad 1.

B.86 Demuestre que $F = \{a + b\sqrt{2}\,\}a, b$ racional$\}$ es un campo.

B.87 Demuestre que $F = \{a + b\sqrt{2}\,\}a, b$ enteros$\}$ es un dominio de integridad pero no un campo.

B.88 Un número complejo $a + bi$, donde a y b son enteros, se denomina *entero gaussiano*. Demuestre que el conjunto G de enteros gaussianos es un dominio de integridad. También demuestre que las unidades son $\pm 1, \pm i$.

B.89 Sea R un dominio de integridad y sea J un ideal en R. Demuestre que el anillo de factores R/J es un dominio de integridad si y sólo si J es un ideal primo. (Un ideal J es *primo* si $J \neq R$ y si $ab \in J$ implica $a \in J$ o $b \in J$.)

B.90 Sea R un anillo conmutativo con elemento unidad 1 y sea J un ideal en R. Demuestre que el anillo de factores R/J es un campo si y sólo si J es un ideal máximo. (Un ideal es máximo si $J \neq R$ y ningún ideal K está estrictamente entre J y R; es decir, si $J \subseteq K \subseteq R$ entonces $J = K$ o $K = R$.)

B.91 Sea D el anillo de matrices reales de 2×2 de la forma $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Demuestre que cuando D es un campo, D es isomorfo al campo complejo C.

B.92 Demuestre que el único ideal en un campo K es $\{0\}$ o K mismo.

B.93 Suponga que $f : K \to K'$ es un homomorfismo de un campo K en un campo K'. Demuestre que f es una *incrustación*; es decir, que f es uno a uno. (Se supone $f(1) \neq 0$.)

B.94 Considere el dominio de integridad $D = \{a + b\sqrt{13}\,\}a, b$ enteros$\}$. (Vea el ejemplo B.15*b*).) Si $\alpha = a + \sqrt{13}$, se define $N(\alpha) = a^2 - 13b^2$. Demuestre:

i) $N(\alpha) = N(\alpha)N(\beta)$.
ii) α es una unidad si y sólo si $N(\alpha) = +1$.
iii) Entre las unidades de D están ± 1, $18 \pm 5\sqrt{13}$; y $-18 \pm 5\sqrt{13}$.
iv) Los números 2, $3 - \sqrt{13}$ y $-3 - \sqrt{13}$ son irreducibles.

POLINOMIOS SOBRE UN CAMPO

B.95 Encuentre las raíces de $f(t)$ si se supone que $f(t)$ tiene una raíz entera: *a*) $f(t) = t^3 - 2t^2 - 6t - 3$; *b*) $f(t) = t^3 - t^2 - 11t - 10$, y *c*) $f(t) = t^3 + 2t^2 - 13t - 6$.

B.96 Encuentre las raíces de $f(t)$ si se supone que $f(t)$ tiene una raíz racional: *a*) $f(t) = 2t^3 - 3t^2 - 16t - 7$; *b*) $f(t) = 2t^3 - t^2 - 9t + 9$.

B.97 Encuentre las raíces de $f(t) = t^4 - 5t^3 + 16t^2 - 9t - 13$, dado que $t = 2 + 3i$ es una raíz.

B.98 Encuentre las raíces de $f(t) = t^4 - t^3 - 5t^2 + 12t - 10$, dado que $t = 1 - i$ es una raíz.

B.99 Para cualquier escalar $a \in K$, se define la *transformación evaluación* ψ_a: $K[t] \to K$ por $\psi_a(f(t)) = f(a)$. Demuestre que ψ_a es un homomorfismo de anillos.

B.100 Demuestre: *a*) la proposición B.14. *b*) El teorema B.26.

Respuestas a los problemas suplementarios

B.39 *a*) 12, 15, 18, 6; *b*) Sí, sí; *c*) Sólo 1 y es su propio inverso.

B.40 *a*) 17, -32, $29/2$; *b*) Sí, sí; *c*) Cero; *d*) Si $a \neq 1/2$, entonces a tiene un inverso, que es $-a/(1 + 2a)$.

B.41 *a*) Sí; *b*) No; *c*) No; *d*) No tiene sentido hablar de inversos cuando no existe un elemento identidad.

B.42 *a*) dieciséis, ya que hay dos opciones: a o b, para cada uno de los cuatro productos aa, ab, ba y bb. *b*) Sea $aa = b$, $ab = a$, $ba = b$, $bb = a$. Entonces $ab \neq ba$. También, $(aa)b = bb = a$, pero $a(ab)$ $as = b$.

B.43 *a*) A; *b*) Ninguno.

B.44 *a*) Sí; *b*) Sí; *c*) Sí; *d*) No.

B.45 *a*) $\{1, -1, 0\}$; *b*) No hay conjunto.

B.46 *a*) Sí, sí, no; *b*) Sí, no, no.

B.47 *a*) (3, 10), $(-5, 1)$; *b*) sí, no; *c*) (1, 0); *d*) El elemento (a, b) tiene inverso si $a \neq 0$, y su inverso es $(1/a, -b/a)$.

B.48 *a*) (19, 20), (18, 7). d) $(a, b) \sim (c, d)$ si $ad = bc$. e) $S/\sim$ es isomorfo a los números racionales positivos bajo la adición. Así, $S/\sim$ no tiene elemento identidad ni inversos.

B.49 *a*) (4, 9), (6, 8); *d*) $(a, b) \sim (c, d)$ si $a + d = b + c$. *e*) $S/\sim$ es isomorfo a $\mathbf{Z}$ puesto que todo entero es la diferencia de dos enteros positivos. Por tanto, $S/\sim$ tiene un elemento identidad, y todo elemento tiene inverso.

×	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

a)

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

b)

Figura B-9

B.50 *a*) $H = l\{0, 5, 10, 15\}$ y $|H| = 4$. *b*) H, $1 + H = \{1, 6, 11, 16\}$, $2 + H = \{2, 7, 12, 17\}$, $3 + H = \{3, 8, 13, 18\}$, $4 + H = \{4, 9, 14, 19\}$.

B.51 *a*) $x^2 = 1$ si $x \neq 1$. *b*) No. *c*) {1}, {1, 5}, {1, 7}, {1, 11}, G.

B.52 *a*) Vea la figura B-9*a*). *b*) 11, 13, 17; *c*) *i*) $|\%| = 6$, $gp(5 = G$; *ii*) $|13| = 3$, $gp(13) = \{1, 7, 13\}$; *d*) Sí, puesto que $G = gp(5)$.

B.53 *a*) Vea la figura B-9*b*). *b*) 4, 3, 4.

B.60 $f(1) = 0$, $f(i) = 1$, $f(-1) = 2$, $f(-i) = 3$

B.62 *a*) {(0, 0)}, *b*) $\{2\pi r \mid r \in Z\}$.

B.69 *a*) 1, 5, 7, 11; *b*) 4, 10; *c*) {2, 10}.

B.70 *a*) 28, 23, 19; *b*) 13, 11, 26^{-1} no existe puesto que 26 no es una unidad.

B.72 Demuestre que $-a = a$ usando $a + a = (a + a)^2$. Luego demuestre que $ab = -ba$ por $(a + b) = (a + b)^2$.

B.73 *b*) $-1 =$ elemento 0; $0 =$ elemento 1.

B.91 Demuestre que f es un isomorfismo donde

$$f\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a + bi.$$

B.93 *Sugerencia*: use el problema B.92.

B.95 *a*) -1, $(3 \pm \sqrt{21})/2$; *b*) -2, $(3 \pm \sqrt{29})/2$; *c*) 3, $(-5 \pm \sqrt{17})/2$

B.96 *a*) $-1)\, 2, 1 \pm 2\sqrt{2}$; *b*) 3/2, $(-1 \pm \sqrt{13})/2$

B.97 $2 \pm 3i$, $(1 \pm \sqrt{5})/2$

B.98 $1 \pm i$, $(-1 \pm \sqrt{21})/2$

Índice