Matematicas discretas

Matemáticas Discretas (Fundación Universitaria Konrad Lorenz)

CD interactivo
en esta edición

MATEMÁTICAS discretas

aplicaciones y ejercicios

José Francisco
Villalpando Becerra

Andrés
García Sandoval

GRUPO EDITORIAL PATRIA

Matemáticas discretas

Aplicaciones y ejercicios

José Francisco Villalpando Becerra

Andrés García Sandoval

Universidad de Guadalajara

Grupo Editorial Patria

Para establecer comunicación con nosotros puede hacerlo por:

correo:
Renacimiento 180, Col. San Juan Tlihuaca, Azcapotzalco, 02400, México, D.F.

fax pedidos:
(01 55) 5354 9109 • 5354 9102

e-mail:
info@editorialpatria.com.mx

home page:
www.editorialpatria.com.mx

Dirección editorial: Javier Enrique Callejas

Coordinadora editorial: Estela Delfín Ramírez

Supervisor de prepensa: Gerardo Briones González

Diseño de portada: Juan Bernardo Rosado Solís

Matemáticas discretas, aplicaciones y ejercicios

Renacimiento 180, Colonia San Juan Tlihuaca,

Delegación Azcapotzalco, Código Postal 02400, México, D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana

Registro núm. 43

ISBN ebook: 978-607-438-925-8

Impreso en México

Printed in Mexico

Primera edición ebook: 2014

Agradecimientos

Agradecemos a Editorial Patria, y en particular a la ing. Estela Delfín Ramírez, por creer en nosotros y darnos la oportunidad de aparecer en una de sus publicaciones, y así compartir nuestra experiencia con los lectores interesados en aprender matemáticas discretas.

También queremos agradecer a todas aquellas personas que nos apoyaron y nos dieron palabras de alienti para conluir esta obra

Prólogo

Este texto nació hace varios años como unos apuntes de clase para la materia de matemáticas discretas, constituido al principio solo por algunas decenas de páginas. Con el paso del tiempo los mismos fueron creciendo y tomando forma hasta ser lo que son hoy en día: un libro de texto en toda la extensión de la palabra. En el mismo se plasma nuestro interés y experiencia docente a lo largo de muchos años de impartir la materia.

Está diseñado para brindar a los estudiantes que cursan la materia de matemáticas discretas una herramienta adecuada, que cubra los conceptos fundamentales de sus principales áreas, pero abordados de una manera sencilla, clara y precisa, además de que sea fácil de leer y comprender, ya que no se pretende que sea un tratado demasiado riguroso sobre alguna parte concreta de las matemáticas discretas.

Cabe hacer mención que algunos de los capítulos requieren para su mayor entendimiento que el lector tenga conocimientos básicos de álgebra a nivel bachillerato; nos referimos en particular al capítulo 2 Lógica y cálculo proposicional, en el tema de inducción matemática; el capítulo 4 Relaciones de recurrencia; el capítulo 5 Combinatoria; el capítulo 8 Sistemas algebraicos y el capítulo 9 Álgebra de Boole, debido a que en los mismos se efectúan diversos procedimientos algebraicos que requieren conocimientos elementales de álgebra.

Muchos de nuestros alumnos que han tomado este curso expresaron que eran necesarios más problemas o ejercicios. Por ese motivo al final de cada capítulo se incluye una serie de problemas para resolver, además de los resueltos en los ejemplos de cada capítulo. Estos problemas también tienen la finalidad de reafirmar los conceptos aprendidos.

Hemos decidido no incluir programas de cómputo de manera explícita, esto debido al tiempo que se requiere para realizarlos; pero sí se presentan en algunos de los temas abordados diversos tratamientos algorítmicos que bien pueden resolverse con un programa.

Hasta estos momentos se ha hablado de la finalidad del libro, pero el lector se ha de estar haciendo las mismas preguntas que nos hacemos todos al iniciar un curso de esta naturaleza: ¿qué son las matemáticas discretas? y ¿por qué estudiar esta materia? En el CD anexo al libro se encuentra una animación con la respuesta a estas interrogantes. Por eso recomendamos ver dicha animación antes de dar inicio a la lectura del libro.

Por último, esperamos que esta obra cumpla con los requerimientos y esté a la altura de las expectativas del lector.

"En matemáticas uno no entiende las cosas, se acostumbra a ellas."
John von Neumann

Contenido

1

Conceptos fundamentales

Objetivos:

- Conocer las nociones básicas de la teoría de conjuntos.
- Comprender y aplicar las operaciones básicas de conjuntos en ejemplos cotidianos.
- Identificar las características que distinguen a los conjuntos finitos e infinitos numerables.
- Comprender las propiedades básicas presentes en el conjunto de los números enteros.
- Conocer el concepto de función.
- Comprender la dependencia de variables.
- Analizar el concepto de matriz como una herramienta básica para el uso ordenado y eficiente de datos.
- Comprender y aplicar las operaciones básicas de matrices.

1.1 Conjuntos

Este capítulo tiene como finalidad presentar y analizar los fundamentos básicos para el desarrollo y la aplicación de las matemáticas discretas. En esta sección abordamos las nociones básicas de la teoría de conjuntos, la cual ha permitido, en gran medida, la formalización y el desarrollo de las matemáticas. En un principio, Georg Cantor, matemático alemán (1845-1918), comenzó esta tarea mediante el análisis de las bases de las matemáticas, explicando todo con base en los conjuntos (por ejemplo, la definición de función se hizo estrictamente a través de conjuntos). El alcance del colosal trabajo realizado por Cantor, logró unificar las matemáticas y permitió la comprensión de nuevos conceptos.

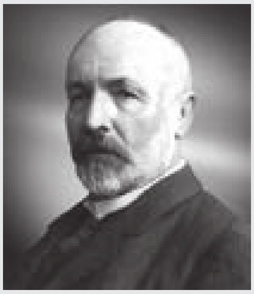


Figura 1.1 Georg Cantor (1845-1918).

George Cantor (San Petersburgo, 1845-Halle, Alemania, 1918), matemático alemán de origen ruso. En 1874, publicó su primer trabajo sobre teoría de conjuntos. Entre 1874 y 1897 demostró que el conjunto de los números enteros tenía el mismo número de elementos que el conjunto de los números pares, y que el número de puntos en un segmento es igual al número de puntos de una línea infinita, de un plano y de cualquier espacio. Es decir, que todos los conjuntos infinitos tienen "el mismo tamaño". Sin embargo, hasta entonces, el concepto de infinito en matemáticas había sido un tabú, por lo que se ganó algunos enemigos, en especial Leopold Kronecker, quien hizo todo lo imposible por arruinar la carrera de Cantor. Estancado en una institución docente de tercera clase, privado del reconocimiento por su trabajo y con frecuencia atacado por Kronecker, Cantor comenzó a tener problema de salud mental, lo que provocó que en 1884 sufriera su primera crisis nerviosa.

En la actualidad, se le considera como el padre de la teoría de conjuntos, punto de partida de excepcional importancia en el desarrollo de la matemática moderna.

Cantor murió en 1918 recluido en una institución para enfermos mentales.

Definiciones básicas de conjuntos

Para las matemáticas en general, la función que desempeñan las definiciones es básica, debido a que con ello se pretende establecer, sin ambigüedad, los conceptos utilizados. Aunque parezca poco increíble, la definición formal de un conjunto es una de las más difíciles de establecer en matemáticas. Pues, si por ejemplo usamos la definición: "Un conjunto es una colección bien definida de objetos"; entonces, surge la siguiente pregunta: ¿qué es una colección? Luego, entonces, es posible definir, por ejemplo, una colección como "un agregado de cosas"; pero, ¿qué es un agregado?, y así sucesivamente hasta desarrollar más definiciones. Como se puede observar, es fácil deducir que esto se vuelve cíclico; por tanto, los matemáticos consideran que debe haber conceptos primitivos o sin una definición formal.

No obstante, para efectos prácticos, en este libro **un conjunto** se considera **una colección bien definida de objetos**, con la esperanza de que, aunque dicha definición no es formal, la cotidianidad de la palabra "colección" nos permita avanzar sin mayores dificultades hacia el logro de los objetivos planteados. En otras palabras, esto significa que un conjunto no es solo cualquier colección de objetos, sino que además este debe estar bien definido en el sentido de que, si se considera cualquier objeto, se puede saber con certeza si es parte o no de la colección.

Es importante establecer que a los objetos de un conjunto se les llama **elementos** o **miembros** del conjunto, y es común representarlos con letras minúsculas, a, b, c…, mientras que la notación usual para los propios conjuntos es con letras mayúsculas, A, B, C….

Por otra parte, hay dos maneras comunes de especificar un conjunto dado. La primera es mediante la presentación de un listado de sus elementos entre llaves; por ejemplo, si aw consiste de todas las letras del alfabeto español, entonces a puede presentarse en la forma:

$$a = \{a, b, c, \ldots, z\}$$

La segunda forma de presentar un conjunto es especificando una regla que establece la propiedad o propiedades que un objeto debe satifacer para ser considerado como un miembro del conjunto. Si se utiliza esta notación, el con

$$A = \{a, \text{t} \cdot \text{q} \cdot a \text{ es una letra del alfabeto español}\}$$

Y se lee: "A es el conjunto de todos los elementos a, tales que a es una letra del alfabeto español".
La notación que se usa para especificar que un objeto a es un elemento de un conjunto A es:

$$a \in A$$

Y se lee: "a es un elemento de A" o, en forma alternativa, "a pertenece a A".
Por otro lado, si el objeto a no es un elemento del conjunto A, entonces se escribe:

$$a \notin A$$

Y se lee: "a no es un elemento de A" o, en forma alternativa, "a no pertenece a A". Por ejemplo, si $A = \{\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\delta}\}$, se tiene que $\boldsymbol{\gamma}\ \boldsymbol{\varepsilon}\ A$, pero $\boldsymbol{\theta} \notin A$.

De acuerdo con el concepto de conjunto definido antes, resulta claro que para que un conjunto A sea igual a un conjunto B, lo cual se denota por $A=B$, ambos deben tener exactamente los mismo elementos.

EJEMPLO

Sean A, B, C los siguientes conjuntos:

$$A = \{1, 2, 3, 4\}$$
$$B = \{1, 2, 3, 4, 5\}$$
$$C = \{1, 3, 5, 2, 4\}$$

Entonces, como B y C tienen exactamente los mismos elementos (aunque, en este caso, en orden distinto) $B = C$, pero $A \neq B$ y $A \neq C$, ya que $5 \notin A$ y $5 \in C$, pero $5 \notin A$.

Como se puede notar en el ejemplo anterior, todos los elementos de A pertenecen al conjunto B; es decir, todo el conjunto A está contenido en B. Esto es, formalmente se dice que A es un **subconjunto** de B y se denota por $A \subseteq B$ si cada elemento de un conjunto A es también un elemento del conjunto B. En caso de que A no sea subconjunto de B, se escribe $A \nsubseteq B$.

A partir de esta definición, se puede ver que $A = B$ si y solo si $A \subseteq B$ y $B \subseteq A$.

EJEMPLO

De acuerdo con los conjuntos A, B y C del ejemplo anterior, es fácil ver que $A \subseteq C$. Además, $B \subseteq C$ y $C \subseteq B$; por tanto, $B = C$. Si $D = \{1, 3, 5, 7\}$, entonces $D \nsubseteq A$ y $A \nsubseteq D$.

Es común utilizar la notación $A \subset B$ para el caso en que $A \subseteq B$, pero $A \neq B$; entonces, se dice que A es **subconjunto propio** de B.

EJEMPLO

Si $A = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ y $B = \{\delta, \varepsilon, \theta, \rho\}$ se tiene que $B \subset A$.

El conjunto que no contiene elementos se conoce como **conjunto vacío** y se denota por $\varnothing$ o $\{\,\}$. El conjunto vacío, $\varnothing$, a su vez, es subconjunto de cada conjunto A. Para ver esto, solo basta observar que $\varnothing$ no tiene elementos y, por tanto, no contiene elementos que no estén en A, es decir $\varnothing \subseteq A$.

Como contraparte del conjunto vacío, se tiene otro extremo, "el más grande", que se denomina **conjunto universo**. Un conjunto universo (o conjunto universal) es el conjunto de todos los elementos de interés en una discusión particular.

Operaciones con conjuntos

Así como los números se pueden sumar, restar, multiplicar o dividir, entre otras operaciones, para obtener nuevos números también se tienen diversas operaciones que se pueden realizar con conjuntos dados para obtener nuevos conjuntos. En esta sección se ilustran algunas de estas.

Unión

La **unión** de dos conjuntos A y B es el conjunto formado con todos los elementos que están en A y/o en B, y se denota por $A \cup B$.

Esto se simboliza de la siguiente forma:

$$A \cup B = \{x \text{ t} \cdot \text{q} \cdot x \in A \text{ o } x \in B \text{ o } x \text{ está en ambos}\}$$

EJEMPLO

Sean:

$$A = \{\alpha, \beta, \gamma, \delta, \varepsilon\} \text{ y } B = \{\delta, \varepsilon, \theta, \rho\}$$

entonces:

$$A \cup B = \{\alpha, \beta, \gamma, \delta, \varepsilon, \theta, \rho\}$$

Intersección

La **intersección** de dos conjuntos A y B es el conjunto formado con todos los elementos que están tanto en A como en B, y se denota por $A \cap B$. Esto se simboliza de la siguiente forma:

$$A \cap B = \{x \text{ t} \cdot \text{q} \cdot x \in A \text{ y } x \in B\}$$

EJEMPLO

Sean:

$$A = \{1, 2, 3, 4, 5\}, B = \{1, 3, 5, 7\} \text{ y } C = \{2, 4, 6, 8\}$$

entonces:

$$A \cap B = \{1, 3, 5\}$$
$$A \cap C = \{2, 4\}$$
$$B \cap C = \varnothing$$

Sea U el conjunto universo y A es un subconjunto de U entonces el conjunto de todos los elementos en U que no están en A se conoce como el complemento de A y se denota por A^c o A'. En símbolos se tiene:

$$A^c = \{x, \text{ t} \cdot \text{q} \cdot x \in U, x \notin A\}$$

EJEMPLO

Sean:

$$U = \{1, 2, 3, 4, 5, 6, 7, 8\} \text{ y } A = \{1, 3, 5, 7\}$$

entonces:

$$A^c = \{2, 4, 6, 8\}$$

Diferencia

La **diferencia** de conjuntos $A - B$ es el conjunto de todos los elementos de A que no están en B, en símbolos:

$$A - B = \{x \text{ t} \cdot \text{q} \cdot x \in A \text{ y } x \notin B\}.$$

La **diferencia simétrica** de A y B, que se denota por:

EJEMPLO

Sean:

$$A = \{a, b, c, d\} \text{ y } B = \{a, b, d, e\}$$

entonces:

$$A - B = \{c\}$$

$$A \oplus B = \{c, e\}$$

Las siguientes propiedades rigen las operaciones en conjuntos.

Sea U un conjunto universo. Si A, B y C son subconjuntos arbitrarios de U, entonces:

Tabla 1.1 Propiedades de las operaciones en conjuntos

$A \cup B = B \cup A$	Ley conmutativa para la unión
$A \cap B = B \cap A$	Ley conmutativa para la intersección
$A \cup (B \cup C) = (A \cup B) \cup C$	Ley asociativa para la unión
$A \cap (B \cap C) = (A \cap B) \cap C$	Ley asociativa para la intersección
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Ley distributiva para la unión
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Ley distributiva para la intersección
$(A \cup B)^c = A^c \cap B^C$	Ley de Morgan 1
$(A \cap B)^c = A^c \cup B^C$	Ley de Morgan 2

Los diagramas de Venn son de gran utilidad para entender los conjuntos resultantes de cada operación definida en conjuntos, pero sobre todo para resolver problemas de aplicación que incluyen conjuntos. En dichos diagramas, el conjunto universo U se representa por un rectángulo, mientras que los subconjuntos de U se representan por regiones dentro del rectángulo. En la figura 1.2 se muestran los diagramas de Venn de las principales operaciones sobre conjuntos.

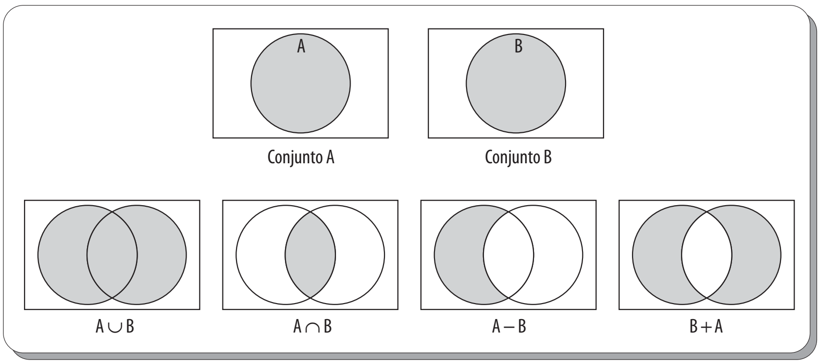


Figura 1.2 Diagramas de Venn de algunas operaciones sobre conjuntos.

1.2 Conjuntos finitos e infinitos contables

Cuando se habla de conjuntos infinitos, mucho del sentido común y de la intuición carecen precisamente de sentido, pues resulta imposible considerar que dos conjuntos, en apariencia uno con muchos más elementos que el otro, tengan en realidad la misma cantidad de elementos. No obstante, esto se aclara en la presente sección.

Recuérdese que la cardinalidad de un conjunto A es la cantidad de elementos distintos que posee el conjunto y se denota como: $|A|$.

EJEMPLO

a) Si $A = \{a, b, c\}$, $A = \{a, b, c\}$ o $A = \{a, \emptyset, d\}$, entonces $|A| = 3$.
b) Si $A = \{\{a, b\}, \{c\{d, e, f, g\}\}\}$, entonces $|A| = 2$.
c) Si $A = \emptyset$, entonces $|A| = 0$.
d) Si $A = \{1, 2, 3, ..., n\}$, entonces $|A| = n$.

Para encontrar el tamaño de dos conjuntos A y B, de manera comparativa, se utiliza el concepto de **correspondencia biunívoca**, que se define como: dados dos conjuntos A y B, se dice que existe una correspondencia uno a uno (biunívoca) entre los elementos de A y los de B, si es posible "hacer corresponder" los elementos de A y los de B, de tal manera que para cada par de elementos distintos de A les "correspondan" dos elementos distintos de B.

EJEMPLO

Existe una correspondencia biunívoca entre los elementos de $\{a, b\}$ y los de $\{y, z\}$ (véase figura 1.3a), también entre los de $\{a, b, c\}$ y los de $\{\emptyset, y, z\}$ (véase figura 1.3b). Pero, no existe una correspondencia biunívoca entre los elementos de $\{a, b, c\}$ y los de $\{y, z\}$ (véase figura 1.3c).

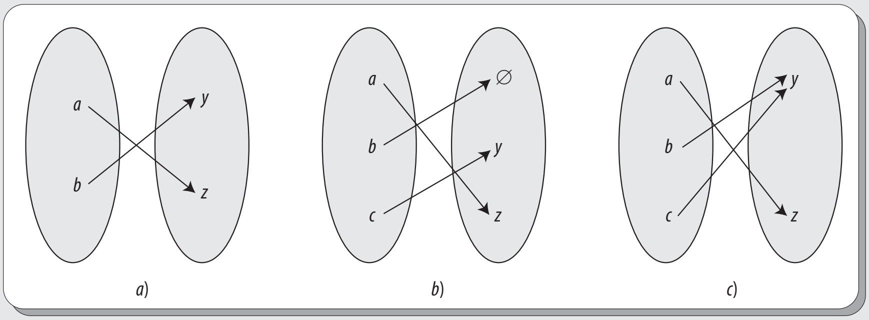


Figura 1.3 a) y b) son correspondencias biunívocas; c) no es correspondencia biunívoca.

EJEMPLO

Existe una correspondencia biunívoca entre los elementos de $\{a, b\}$ y los de $\{c, d\}$ y entre los de $\{a, b, c\}$ y los de $\{\emptyset, a, b\}$. Pero no existe una correspondencia biunívoca entre los elementos de $\{a, b, c\}$ y los de $\{a, d\}$.

Ahora, es posible establecer de manera concisa el concepto de conjunto finito: se dice que un conjunto A es finito si existe una correspondencia biunívoca entre los elementos de A y los elementos de un conjunto de la forma $\{1, 2, \ldots, n\}$, donde n es algún entero positivo fijo. Es fácil ver que si existe tal correspondencia biunívoca se tiene que: $|A| = n$.

EJEMPLO

Tanto el conjunto $A = \{a, \emptyset, d\}$ como el conjunto $B = \{a, b, d\}$ son finitos y de cardinalidad 3, ya que existe una correspondencia biunívoca entre los elementos de ambos conjuntos y los elementos del conjunto $\{1, 2, 3\}$, como se muestra en la figura 1.4.

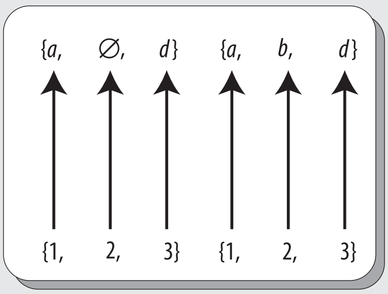


Figura 1.4 La cardinalidad de ambos conjuntos es 3.

El concepto de **conjunto infinito contable** se establece de una extensión "natural" del caso de conjuntos finitos; se dice que un conjunto es infinito contable (o infinito numerable) si existe una correspondencia biunívoca entre los elementos del conjunto y los elementos de $\mathbb{N} = \{1, 2, 3, \ldots\}$.

EJEMPLO

El conjunto de los números naturales $\mathbb{N}$ es por sí mismo un conjunto infinito contable, dado que se puede establecer la correspondencia biunívoca de $\mathbb{N}$ a $\mathbb{N}$ (véase figura 1.5).

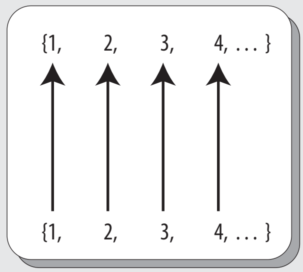


Figura 1.5 $\mathbb{N}$ es un conjunto infinito contable.

EJEMPLO

El conjunto de todos los enteros pares no negativos $P = \{2, 4, 6,\ldots\}$ es un conjunto infinito contable, pues existe una correspondencia biunívoca entre dicho conjunto y los números naturales (véase figura 1.6); a saber, al entero $2k$ se le puede hacer corresponder el número natural k, para $k = 1, 2, \ldots$; es decir:

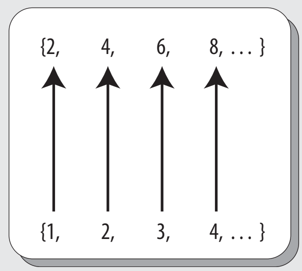


Figura 1.6 El conjunto de los pares es infinito contable.

EJEMPLO

De manera similar, el conjunto de todos los múltiplos de 7 no negativos $\{7, 14, 21, \ldots\}$ es infinito contable (véase figura 1.7).

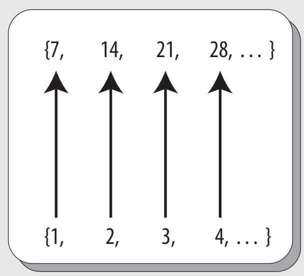


Figura 1.7 Los múltiplos de 7 son un conjunto infinito contable.

Una manera intuitiva de concebir lo que es un conjunto infinito contable es: un conjunto A es infinito contable si, comenzando con algún elemento fijo de A, es posible listar de manera sucesiva, uno detrás de otro, todos los elementos de A. Es fácil ver que de existir dicha lista, la correspondencia biunívoca del conjunto A con los números naturales estaría garantizada.

EJEMPLO

El conjunto $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ es un conjunto infinito contable porque sus elementos pueden ser listados como $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3 \ldots\}$, y, por tanto, se tiene una correspondencia biunívoca entre los elementos de $\mathbb{Z}$ y los de $\mathbb{N}$ (véase figura 1.8); es decir:

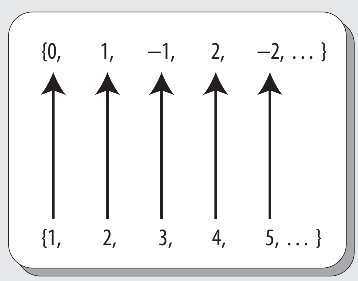


Figura 1.8 $\mathbb{Z}$ es un conjunto infinito contable.

EJEMPLO

El conjunto de los números racionales $\mathbb{Q}$ es un conjunto infinito contable, debido a que este puede ser listado como se muestra en la figura 1.9. Además, como se observa, es posible obtener una cantidad infinita contable de sublistas, en donde cada una es, al mismo tiempo, un conjunto infinito contable; la unión de todas estas es el conjunto $\mathbb{Q}$.

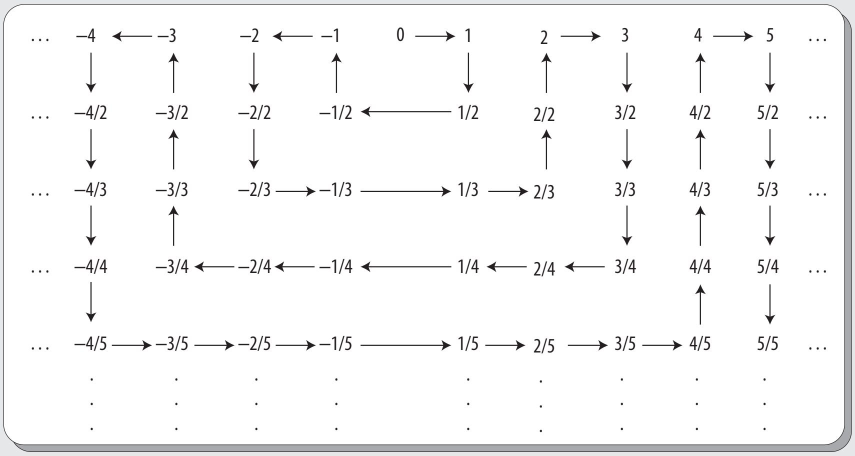


Figura 1.9 Lista de números racionales que demuestra que $\mathbb{Q}$ es un conjunto infinito contable.

Se dice que la cardinalidad de un conjunto infinito contable es $\aleph_0$. ($\aleph$ *Aleph* es la primera letra del alfabeto hebreo.)

Pero, también es posible encontrar conjuntos infinitos no contables, como el caso de los números reales entre 0 y 1. La manera de demostrarlo es a través de la reducción al absurdo; esto es, suponer que $\mathbb{R}$ es un conjunto infinito contable y llegar a una contradicción.

Esto es, suponiendo que el conjunto $(0, 1) \subset \mathbb{R}$ es infinito contable, necesariamente debe existir una correspondencia biunívoca entre $(0, 1)$ y el conjunto $\mathbb{N}$. En consecuencia, es posible listarlos de manera sucesiva, uno detrás de otro, de forma decimal, como se aprecia a continuación:

$$\begin{array}{c} 0.\, a_{11}\, a_{12}\, a_{13}\, a_{14}\ldots \\ 0.\, a_{21}\, a_{22}\, a_{23}\, a_{24}\ldots \\ 0.\, a_{31}\, a_{32}\, a_{33}\, a_{34}\ldots \\ \vdots \\ 0.\, a_{i1}\, a_{i2}\, a_{i3}\, a_{i4}\ldots \\ \vdots \end{array}$$

donde a_{ij} denota el j-ésimo dígito decimal del i-ésimo número de la lista.

Ahora, considérese el número donde:

$$b_i \begin{cases} 1 & \text{si} \quad a_{ii} = 9 \\ 9 - a_{ii} & \text{si} \quad a_{ii} = 0, 1, 2, \ldots, 8 \end{cases}$$

Para todo i.

El número $0.\, b_1\, b_2\, b_3\, b_4\ldots$ es un número real entre 0 y 1 que es distinto de cada uno de los números de la lista anterior, porque difiere del primer número listado en el primer dígito, del segundo en el segundo dígito,… del i-ésimo número en el i-ésimo dígito y así sucesivamente. En consecuencia, se puede concluir que la lista anterior no incluye a todos los elementos del conjunto $(0, 1)$, lo cual contradice el supuesto de que $(0, 1)$ es infinito contable.

1.3 El conjunto de los números enteros

El sistema de los números naturales $\mathbb{N}$ tiene un defecto manifiesto; a saber, dados $m, n \in \mathbb{N}$, la ecuación $m + x = n$ puede o no tener solución; por ejemplo, la ecuaciones $m + x = m$ y $m + x = n$ ($m < m$) carecen de solución. Es sabido que esto se soluciona introduciendo a los números naturales el cero y los números enteros negativos, a fin de formar el conjunto de los números enteros $\mathbb{Z}$.

Recuérdese que:

$$\mathbb{N} = \{1, 2, 3\} \text{ y } \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

A continuación, se describen las propiedades algebraicas que satisfacen el conjunto de los números enteros con las operaciones de adición y multiplicación $\mathbb{Z}$.

Nota

El símbolo $\mathbb{Z}$ proviene del alemán *zahl*, que significa número.

Adición

Si $k, m, n \in \mathbb{Z}$ son tres números enteros cualesquiera, entonces:

1.	Propiedad de cerradura	$(k + m) \in \mathbb{Z}$
2.	Propiedad conmutativa	$k + m = m + k$
3.	Propiedad asociativa	$(k + m) + n = k + (n + m)$
4.	Neutro aditivo	$\exists$ un único elemento $0 \in \mathbb{Z}$, tal que $k + 0 = 0 + k = k, \forall k \in \mathbb{Z}$
5.	Inverso aditivo	Para cada $k \in \mathbb{Z}$ $\exists$ un único elemento $-k$, tal que $k + (-k) = (-k) + k = 0$

Multiplicación

1.	Propiedad de cerradura	$(k \cdot m) \in \mathbb{Z}$
2.	Propiedad conmutativa	$k \cdot m = m \cdot k$
3.	Propiedad asociativa	$(k \cdot m) \cdot n = k \cdot (n \cdot m)$
4.	Inverso aditivo	$\exists$ un único elemento $1 \in \mathbb{Z}$, tal que $k \cdot 1 = 1 \cdot k = k$

Leyes distributivas

1.	$k \cdot (m + n) = k \cdot m + k \cdot n$
2.	$(k + n) \cdot n = k \cdot n + m \cdot n$

Los números enteros poseen un conjunto de gran importancia por sus diversas aplicaciones: los números primos. Para definir con precisión qué es un número primo, primero introducimos el concepto de divisor: un entero $a \neq 0$ se llama divisor (o factor) de un $b \in \mathbb{Z}$, lo cual denota como $a \mid b$, si $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Cuando $a \mid b$, se dice que b es un múltiplo de a.

Ejemplo

a) $2|6$, ya que $6 = 2 \cdot 3$, con $3 \in \mathbb{Z}$.

b) $-3|15$, ya que $15 = (-3) \cdot (-5)$, con $-5 \in \mathbb{Z}$.

c) $a|0$, ya que $\forall\, a \in \mathbb{Z}$ se cumple $0 = a \cdot 0$, con $0 \in \mathbb{Z}$.

Nota

En este punto, es importante tener clara la diferencia que existe entre $a \mid 0$ y $0 \mid a$; de hecho, este último caso no es posible, pues implica una división por cero, la cual no está definida.

Entonces, se puede decir que ya se está en condiciones de aclarar, sin ambigüedad alguna, qué es un **número primo**: "se dice que un entero p es un número primo, si y solo si tiene exactamente cuatro divisores diferentes; a saber: ± 1 y $\pm p$.

EJEMPLO

a) 2 es primo, ya que sus únicos divisores son ± 2, ± 1.

b) -5 es primo, ya que sus únicos divisores son ± 5, ± 1.

c) 6 no es primo, ya que sus divisores son ± 6, ± 3, ± 2, ± 1.

d) 39 no es primo, ya que sus divisores son ± 39, ± 13, ± 3, ± 1.

e) 1 no es primo, ya que solo tiene dos divisores ± 1.

Es claro que $-p$ es primo si y solo si p lo es, por lo que solamente será necesario referirse a los primos positivos.

Por último, otro concepto importante acerca de los números enteros es el de **Máximo Común Divisor** (MCD), el cual, para dos enteros positivos, a y b se define como el mayor entero positivo que es divisor tanto de a como de b. Matemáticamente se expresa de la siguiente manera: si $a \mid b$ y $a \mid c$ se dice que a es un divisor común de b y c; pero, si además todo divisor común de b y c también es de a, se dice que a es el máximo común divisor de b y c.

EJEMPLO

El conjunto de divisores comunes (positivos) de 24 y 60 es {1, 2, 3, 4, 6, 12}. Entonces, en este caso, el MCD de 24 y 60 es 12.

1.4 Funciones

En matemáticas, el concepto de **función** es fundamental, incluyendo todas sus áreas de aplicación. Por ejemplo, en su desempeño profesional un biólogo puede necesitar conocer cómo depende el crecimiento de un cultivo de bacterias en función del tiempo y un químico puede requerir saber cuál es la rapidez de reacción inicial de una sustancia en función de la cantidad utilizada, entre otras cosas. Pues, la relación entre cantidades es descrita de manera conveniente usando el concepto de función.

De manera intuitiva, se puede comparar a una función con una máquina, de tal suerte que si se introduce un número a dicha máquina, esta lo transforma en otro número. Por supuesto, las funciones no se limitan a números y, en general, se puede considerar una **función** f de un conjunto X a un conjunto Y, que se denota por $f: X \to Y$ como una regla que asigna a cada elemento x de X uno y solo un elemento y de Y.

Por tanto, es útil representar al número en la forma $f(x)$, lo cual se lee f de x, pues dicha notación enfatiza el hecho de que el número y depende del número x.

EJEMPLO

Sea f la función que transforma cada entero en su cubo, es decir $f: \mathbb{Z} \to \mathbb{Z}$, donde f se define por $f(x) = x^3$. Entonces, por ejemplo, el número entero 2 es transformado por la regla f al número entero 8, ya que: $f(2) = 2^3 = 8$.

Dada una función $f: X \to Y$ al conjunto de todos los elementos $x \in X$ que f puede transformar sin ambigüedad a un elemento $y \in Y$, se le denomina dominio de f y se denota por $dom\{f\}$. Por su parte, al conjunto de todos los elementos $y = f(x)$ que se obtienen al recorrer todo $dom\{f\}$, se le denomina rango o imagen de f y se denota por $im\{f\}$.

EJEMPLO

Para la función f definida en $\mathbb{R}$ por: $f(x)=\dfrac{1+x}{2x}$

El dominio de la función son todos los números reales excepto $x = 0$, ya que dicho valor es el único que no tiene correspondencia con un valor real, pues la división por cero no está definida. Por tanto, podemos escribir:

$$dom\{f\} = \{x \in \mathbb{R} \text{ t} \cdot \text{q} \cdot x \neq 0\}$$

Si para una función en particular conocemos su regla de transformación $f(x)$, es útil, en diversas aplicaciones, averiguar cuál es el elemento x que fue transformado al $f(x)$ dado.

Por desgracia, no siempre es posible saber esto con certeza; por ejemplo, si consideramos al número 4 como un elemento convertido por la regla $f(x) = x^2$, es claro que existe ambigüedad para determinar el valor de x, ya que hay dos opciones posibles: $x = 2$ y $x = -2$. No obstante, dicha ambigüedad no existe para funciones f que tienen la característica de que para cada par de elementos $x_1, x_2 \in dom\{f\}$ con $x_1 \neq x_2$ las imágenes correspondientes también son distintas: $f(x_1) \neq f(x_2)$.

Una función de este tipo se denomina **biunívoca**, la cual, como se dijo antes, por supuesto es equivalente al concepto de correspondencia biunívoca descrito y utilizado en la sección anterior.

Ejemplo

Determinar si las funciones siguientes son o no biunívocas en todo su dominio.

a) $f(x) = 1 - 3x$

b) $f(x) = \dfrac{1}{1+2x}$

c) $f(x) = x^2$

Solución

Para verificar si una función es biunívoca o no, primero se puede asumir que dos valores transformados son iguales, $f(x_1) = f(x_2)$, y si dicha aseveración implica que los argumentos son iguales, $x_1 = x_2$, entonces es posible concluir que la función es biunívoca (¿por qué?).

Entonces:

a) Sea $f(x_1) = f(x_2)$, es decir, $1 - 3x_1 = 1 - 3x_2$. Si en la ecuación anterior restamos 1 en ambos lados se obtiene $-3x_1 = -3x_2$. Por último, si dividimos ambos lados de la ecuación por -3 se tiene que $x_1 = x_2$. Por tanto, es posible concluir que la función f es biunívoca.

b) Del mismo modo, sea $f(x_1) = f(x_2)$, es decir, $\dfrac{1}{1+2x_1}=\dfrac{1}{1+2x_2}$. En este caso, primero multiplicamos ambos lados de la ecuación por los factores $(1 + 2x_1)(1 + 2x_2)$, lo que da como resultado $1 + 2x_2 = 1 + 2x_1$. Ahora bien, restamos 1 en ambos lados, con lo que se obtiene $2x_2 = 2x_1$. Por último, dividimos ambos lados de la ecuación por 2 y se obtiene $2x_2 = 2x_1$. Por tanto, concluimos que la función f es biunívoca.

c) Ahora, aseguramos que la función dada no es biunívoca. Para ver esto, sea $f(x_1) = f(x_2)$, es decir, $(x_1)^2 = (x_2)^2$. Es importante destacar que es fácil cometer el error de concluir que la última ecuación implica que $x_1 = x_2$ cuando en realidad se tiene que $x_1 = \pm x_2$. Entonces, como no existe una único valor para el cual $f(x_1) = f(x_2)$, se concluye que la función dada no es biunívoca.

1.5 Sucesiones

Es importante hacer notar que el término sucesión se usa con mucha frecuencia en el ámbito coloquial, ya que se emplea por lo común para indicar una serie de eventos, donde uno sigue a otro en un orden definido. Algo análogo ocurre con las sucesiones numéricas, solo que en lugar de tratarse de eventos se trata de términos numéricos.

De manera intuitiva, una sucesión S es una simple lista de objetos llamados elementos, los cuales forman un conjunto, donde además los elementos están uno detrás de otro en el orden natural creciente de los números naturales $\mathbb{N}$.

Si la sucesión es finita, esta puede terminar después de un cierto número de términos o puede (en principio, al menos) seguir en forma indefinida; en este caso, se dice que es infinita. En este sentido, se puede decir que son conjuntos infinitos contables.

Una sucesión general, es decir una sucesión en la que no se especifican los términos, puede escribirse como:

$$x_1, x_2, x_3, \ldots$$

o algunas veces como:

$$x_n, 1 \leq n < \infty$$

Si x es una sucesión, entonces se escribe como:

$$X = (x_n)$$

En un sentido formal, se dice que una sucesión (x_n) es una función $S{:}\mathbb{N} \to \mathbb{R}$ de una variable n donde $dom\{S\} = \mathbb{N}$; es decir, a cada $n \in \mathbb{N}$ le corresponde un número real x_n, el término n-ésimo de la sucesión.

Una diferencia sustancial entre un conjunto cualquiera y una sucesión es que en una sucesión se pueden tener términos repetidos.

EJEMPLO

a) $(x_n) = \{1, 0, 0, 1, 1, 0, 0, \ldots\}$

b) $(x_n) = \{2, 4, 6, 8, \ldots, 2n, \ldots\}$

c) $x_n = n^2, 1 \leq n < \infty$, es decir $(x_n) = \{1, 4, 9, 16, \ldots\}$

d) $x_n = (-1)^n, 1 \leq n < \infty$, es decir $(x_n) = \{-1, 1, -1, 1, \ldots\}$

e) $x_n = \dfrac{1}{2^n}, 1 \leq n < \infty$, es decir $(x_n) = \left\{\dfrac{1}{2}, \dfrac{1}{4}, \dfrac{1}{8}, \dfrac{1}{16}, \ldots\right\}$

1.6 Matrices

Hoy día, en el ámbito cotidiano existen muchos problemas prácticos que pueden ser resueltos mediante operaciones aritméticas aplicadas a los datos asociados al problema dado. Organizando los datos en arreglos numéricos de filas y columnas, es factible llevar a cabo de manera eficiente los cálculos aritméticos necesarios para resolver un problema de este tipo. Además, una gran ventaja de utilizar un ordenamiento de filas y columnas para los datos, es que el manejo en una computadora es muy sencillo y, por tanto, todos los cálculos pueden realizarse con precisión y eficiencia.

Desde el punto de vista formal, un arreglo rectangular de datos se denomina **matriz**. De este modo, se dice que una matriz que consta de m filas y n columnas tiene tamaño $m \times n$; en tanto, cuando $m = n$ se dice que la matriz es cuadrada. La entrada en el i-ésimo renglón y j-ésima columna en una matriz A se denota por a_{ij}; es decir:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \end{bmatrix}$$

Una forma práctica de denotar la matriz A es $A = (a_{ij})$.

Ejemplo

Considerar la matriz:

$$A = \begin{bmatrix} 319 & 281 & 455 & 285 \\ 475 & 365 & 580 & 0 \\ 545 & 425 & 180 & 880 \end{bmatrix}$$

a) Determinar cuál es el tamaño de la matriz.
b) Encontrar a_{32}.
c) Determinar la suma de las entradas de la primera fila.
d) Establecer la suma de entradas de la cuarta columna.

Solución

a) El tamaño de la matriz es 3×4, ya que la matriz consta de 3 renglones y 4 columnas.
b) La entrada a_{32} corresponde al elemento de la matriz ubicado en el renglón 3 y columna 2, es decir $a_{32} = 425$
c) La suma del primer renglón es $319 + 281 + 455 + 285 = 1\,340$
d) La suma de la primera columna es $285 + 0 + 880 = 1\,165$

Dos matrices $A = (a_{ij})$ y $B = (b_{ij})$ son iguales si y solo si tienen el mismo tamaño y sus entradas correspondientes son iguales, es decir:

$$a_{ij} = b_{ij} \ \forall\ i, j \in \mathbb{N}$$

Ejemplo

Determinar $\boldsymbol{w}$, $\boldsymbol{x}$, $\boldsymbol{y}$, de manera que:

$$\begin{bmatrix} x & 1 & 2w \\ 2 & y-1 & -1 \end{bmatrix} = \begin{bmatrix} -3 & 1 & -4 \\ 2 & 0 & -1 \end{bmatrix}$$

Solución

Considerando que las entradas correspondientes de las dos matrices deben ser iguales, entonces: $x = -3$, $2 \cdot w = -4$, y $y - 1 = 0$; por tanto, $x = -3$, $w = -2$ y $y = 1$.

Dado que una matriz es un arreglo de datos, es posible definir operaciones sobre esta. En primer lugar, si A y B son dos matrices del mismo tamaño, el resultado de la **adición** de A y B es la matriz suma $A+B$, que se obtiene de la adición de todas y cada una las entradas correspondientes de A y B; es decir:

$$A+B = (a_{ij} + b_{ij})$$

De forma equivalente, la **diferencia** $A-B$ es la matriz obtenida por restar las correspondientes entradas en B de A; es decir:

$$A-B = (a_{ij} - b_{ij})$$

Ejemplo

Considerar las siguientes matrices A y B:

$$A = \begin{bmatrix} -2 & 7 \\ 3 & -5 \\ 1 & 0 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 1 & 14 \\ 10 & -5 \\ -1 & -3 \end{bmatrix}$$

entonces, se tiene que:

$$A+B = \begin{bmatrix} -2+1 & 7+14 \\ 3+10 & -5+(-5) \\ 1+(-1) & 0+(-3) \end{bmatrix} = \begin{bmatrix} -1 & 21 \\ 13 & -10 \\ 0 & -3 \end{bmatrix}$$

Y la diferencia de $A-B$ es:

$$A-B = \begin{bmatrix} -2-1 & 7-14 \\ 3-10 & -5-(-5) \\ 1-(-1) & 0-(-3) \end{bmatrix} = \begin{bmatrix} -3 & -7 \\ -7 & 0 \\ 2 & 3 \end{bmatrix}$$

Otra operación importante en aplicaciones de matrices es la **multiplicación por un escalar** (en este contexto, un escalar representa cualquier número real). De este modo, el producto de una matriz A por un escalar c es la matriz que se obtiene de la multiplicación de cada entrada de la matriz A por el escalar c, es decir:

$$cA = (ca_{ij})$$

EJEMPLO

Sean:

$$A = \begin{bmatrix} 3 & 2 & 1 \\ -1 & 0 & 4 \end{bmatrix} \text{ y } c = -4$$

Entonces , cA es la matriz:

$$cA = \begin{bmatrix} (-4)(3) & (-4)(2) & (-4)(1) \\ (-4)(-1) & (-4)(0) & (-4)(4) \end{bmatrix} = \begin{bmatrix} -12 & -8 & -4 \\ 4 & 0 & -16 \end{bmatrix}$$

Además de las anteriores, hay otra operación importante en aplicación matricial: la multiplicación de matrices. A diferencia de las operaciones consideradas hasta ahora, la multiplicación de matrices no tiene una definición "natural". De este modo, si A es una matriz de tamaño $m \times n$ y B es una matriz de tamaño $n \times k$; entonces, el **producto** de A con B, que se denota por $AB = (c_{ij})$, es la matriz de tamaño $m \times k$, cuya entrada en el renglón i y columna j, $1 \le i \le m$, $1 \le j \le k$, es:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$

Los puntos más importantes para recordar de esta definición son:

1. Para que exista el producto AB es necesario que el número de columnas de la primera matriz, de izquierda a derecha, A, sea igual al número de renglones de la segunda matriz, de izquierda a derecha, B.
2. Si se cumple el requisito del inciso a), con A de tamaño $m \times n$ y B es de tamaño $n \times k$, entonces la matriz producto tendrá el mismo número de renglones que A y el mismo número de columnas que B.
3. Para obtener el elemento de la matriz producto AB ubicado en el i-ésimo renglón y j-ésima columna, se deben sumar los productos que resultan de multiplicar la primera entrada del renglón i de A con la primera entrada de la columna j de B, la segunda entrada del renglón i de A con la segunda entrada de la columna j de B, y así sucesivamente.

EJEMPLO

Sean:

$$A = \begin{bmatrix} -1 & 2 & 6 \\ 0 & 3 & -2 \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} 1 & 0 & 3 \\ -1 & 1 & 6 \\ 5 & -1 & 1 \end{bmatrix}$$

Determinar AB, siempre que el producto matricial esté definido.

Solución

En este caso, primero debemos verificar si el producto matricial AB está bien definido; es decir, es indispensable comprobar que el número de columnas de la matriz A sea igual al número de renglones de la matriz B lo cual aquí se cumple. En segundo lugar, debemos establecer el tamaño de la matriz producto. La matriz producto debe tener el mismo número de renglones que A y el mismo número de columnas que B; por tanto, el tamaño de AB es 2×3. Entonces, el resultado esperado es una matriz de la forma

$$AB = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{bmatrix}$$

Continúa

en la que para obtener el elemento ubicado en el primer renglón y en la primera columna, c_{11}, se suman los productos obtenidos de la multiplicación del primer renglón de A con la primera columna de B, término a término, es decir:

$$c_{11} = a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31}$$
$$c_{11} = (-1)(1) + (2)(-1) + (6)(5) = 27$$

Del mismo modo, para calcular se suman los productos obtenidos de la multiplicación del primer renglón de A con la segunda columna de B, término a término, es decir:

$$c_{12} = a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{31}$$
$$c_{12} = (-1)(0) + (2)(1) + (6)(-1) = -4$$

Si seguimos con este procedimiento, al cabo del mismo se obtiene:

$$c_{13} = (-1)(3) + (2)(6) + (6)(1) = 15$$
$$c_{21} = (0)(1) + (3)(-1) + (-2)(5) = -13$$
$$c_{22} = (0)(0) + (3)(1) + (-2)(-1) = 5$$
$$c_{23} = (0)(3) + (3)(6) + (-2)(1) = 16$$

lo que completa la matriz producto:

$$AB = \begin{bmatrix} 27 & -4 & 15 \\ -13 & 5 & 16 \end{bmatrix}$$

A continuación se describen las propiedades algebraicas que satisfacen las matrices con las operaciones de adición, multiplicación por un escalar y multiplicación matricial (la diferencia de matrices $A-B$ se puede ver como la suma $A+(-B)$).

Si A, B, C son matrices del mismo tamaño, y c y d son dos números reales cualesquiera, entonces se cumplen las siguientes propiedades:

1.	Propiedad conmutativa	$A + B = B + A$
2.	Propiedad asociativa	$(A + B) + C = A + (B + C)$
3.	Leyes distributivas	$c(A + B) = cA + cB$ y $(A + B)c = Ac + Bc$
4.	Ley asociativa escalar	$c(dA) = (cd)A$

Además, si los productos y las sumas están definidos para A, B, C, entonces:

5.	Propiedad asociativa	$(AB)\,C = A\,(BC)$
6.	Ley distributiva	$A(B + C) = AB + AC$

EJEMPLO

Para:

$$A = \begin{bmatrix} 0 & 2 & -1 \\ -1 & 3 & 2 \\ 7 & 4 & -6 \end{bmatrix}, \qquad B = \begin{bmatrix} 2 & 4 & 10 \\ -8 & -1 & 2 \end{bmatrix}, \qquad C = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 1 & 1 \end{bmatrix}$$

Continúa

Realizar la operación indicada siempre que esté definida:

a) AB b) BA c) $BA - 2C$

Solución

a) El producto AB no está definido, ya que el número de columnas de la primera matriz (de izquierda a derecha), es 3 y este número es diferente al número de columnas de la segunda matriz, que es 2.

b) El producto BA sí está definido, pues B es de tamaño 2×3 (tres renglones) y la matriz A de tamaño 3×3 (tres columnas). Por tanto, la matriz producto será de tamaño 2×3 (número de filas de B $\times$ número de columnas de A). De este modo, la matriz BA es:

$$BA = \begin{bmatrix} 2(0) + 4(-1) + 10(7) & 2(2) + 4(3) + 10(4) & 2(-1) + 4(2) + 10(-6) \\ -8(0) + (-1)(-1) + 2(7) & -8(2) + (-1)(3) + 2(4) & -8(-1) + (-1)(2) + 2(-6) \end{bmatrix}$$

Es decir:

$$BA = \begin{bmatrix} 66 & 56 & -54 \\ 15 & -11 & -6 \end{bmatrix}$$

c) Considerando que la matriz $-2C$ es del mismo tamaño que la matriz BA, la operación $BA - 2C$ sí está definida:

$$BA - 2C = \begin{bmatrix} 66 & 56 & -54 \\ 15 & -11 & -6 \end{bmatrix} - 2\begin{bmatrix} 1 & 2 & -1 \\ 3 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 66 & 56 & -54 \\ 15 & -11 & -6 \end{bmatrix} - \begin{bmatrix} 2 & 4 & -2 \\ 6 & 2 & 2 \end{bmatrix}$$

Es decir:

$$BA - 2C = \begin{bmatrix} 64 & 52 & -52 \\ 9 & -13 & -8 \end{bmatrix}$$

Resumen

En este capítulo se presentaron y analizaron los principales conceptos fundamentales relacionados con el desarrollo y la aplicación de las matemáticas discretas y de diversos objetos discretos, con la finalidad de adoptar una terminología común a lo largo del libro para poder trabajar con ellos de una manera adecuada.

En primer lugar se abordaron las nociones básicas de la teoría de conjuntos, la cual ha permitido la formalización y desarrollo de las matemáticas, y por ende de las matemáticas discretas. Entre ellas pueden resaltar la de conjunto que, como se indicó, es una de las más difíciles de formalizar, además de analizar las principales operaciones que pueden efectuarse sobre los conjuntos.

Luego se habló de los conjuntos cuya cardinalidad es finita, y de aquellos cuya cardinalidad es infinita contable; esto es, en los que es posible establecer una correspondencia biunívoca entre los elementos del conjunto y los elementos de los números naturales.

Enseguida se presentaron las propiedades algebraicas del conjunto de los números enteros, para proseguir con la definición y análisis del concepto de función, que a final de cuentas es una regla que asigna a cada elemento de un conjunto un y solo un elemento de otro conjunto.

Problemas propuestos

En los ejercicios 1.1 a 1.8 determinar si la proposición es falsa o verdadera.

1.1 $\{1, 2, 3, 4\} = \{4, 1, 2, 3\}$

1.2 $\varnothing \in X$

1.3 $X \in X$

1.4 $X \subset X$

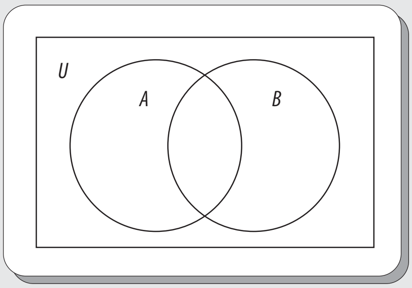
1.5 $0 = \varnothing$

1.6 $0 \in \varnothing$

1.7 $\{1, 2\} = \{1, 2, 3, 4\}$

1.8 {Sentra®, Tsuru®, Xtrail®} $\subset$ {Nissan®}

En los ejercicios 1.9 al 1.16 en un diagrama de Venn sombrear la región adecuada que represente la operación indicada.



1.9 $A^c \cap B$

1.10 $A^c \cap B^c$

1.11 $(A^c \cap B^c)$

1.12 $(A \cup B)^c$

1.13 $A - B$

1.14 $A^c - B$

1.15 $A^c - B^c$

1.16 $A \oplus B$

En los ejercicios 1.17 a 1.25 determinar el conjunto resultante de la operación indicada, considerando el conjunto universo como $U = \{x : x \in \mathbb{Z} \text{ y } 1 \leq x \leq 9\}$, y los subconjuntos $A = \{2x \text{t} \cdot \text{q} \cdot x \in \mathbb{Z} \text{ y } 1 \leq x \leq 4\}$, $B = \{2x + 1 \text{t} \cdot \text{q} \cdot x \in \mathbb{Z} \text{ y } 1 \leq x \leq 4\}$ y $C = \{x \text{ t} \cdot \text{q} \cdot x \in \mathbb{Z} \text{ y } 1 \leq x \leq 4\}$.

1.17 B^C

1.18 $A \cup B^c$

1.19 $A \cap A^c$

1.20 $(A \cap B) \cup C$

1.21 $(A \cup B) \cup C$

1.22 $(A \cup B) \cap C$

1.23 $(A \cup B) \cup A^c$

1.24 $(A \cup B)^c \cup C$

1.25 $(A \cup B)^c \cap C^c$

En los ejercicios 1.26 a 1.29 determinar si el conjunto dado es finito, infinito numerable o infinito no numerable.

1.26 $A = \{x \text{ t} \cdot \text{q} \cdot x \in \mathbb{R} \text{ y } 2 \leq x \leq 3\}$

1.27 $A = \{x \text{ t} \cdot \text{q} \cdot x \in \mathbb{Z} \text{ y } 2 \leq x \leq \infty\}$

1.28 $A = \{x \text{ t} \cdot \text{q} \cdot x \in \mathbb{Q} \text{ y } 0 \leq x \leq \infty\}$

1.29 $A = \{x \text{ t} \cdot \text{q} \cdot x \in \mathbb{Z} \text{ y } -100\,000 \leq x \leq 15\}$

En los ejercicios 1.30 a 1.34 analizar si la correspondencia dada define una función para todos los valores de su dominio.

1.30 $f(x) = 10^x$

1.31 $f(x) = x^3 + x$

1.32 $f(x) = -3 \pm \sqrt{x-2},\ x \geq 2$

1.33 $f(x) = -3 - \sqrt[3]{x-2}$

1.34 $f(x) = \dfrac{x}{x-5},\ x \neq 5$

En los ejercicios 1.35 a 1.40 determinar si la función dada es biunívoca para todos los valores de su dominio.

1.35 $f(x) = x^2 + x$

1.36 $f(x) = x^3 + x^2$

1.37 $f(x) = \sqrt{x-1},\ x \geq 1$

1.38 $f(x) = |x|$

1.39 $f(x) = \dfrac{x}{x-5},\ x \neq !$

1.40 $f(x) = \ln(x^2)$

1.41 Sea: $A = \begin{bmatrix} -1 & 2 \\ 3 & 1 \end{bmatrix}$ y $B = \begin{bmatrix} -1 & 2 \\ 2 & 1 \end{bmatrix}$

Determinar AB y BA. Con base en este ejemplo, definir si la mulwtiplicación matricial es conmutativa.

1.42 Considerar las matrices:

$$A = [1 \quad -1 \quad 7], \qquad B = \begin{bmatrix} -2 \\ 3 \\ 10 \end{bmatrix}$$

¿Es posible realizar la operación $AB - 6$? En caso afirmativo, realizar el cálculo.

En los ejercicios 1.43 a 1.50 considerar las matrices:

$$A = \begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 4 & -3 & 2 \\ 3 & 1 & 5 \end{bmatrix} \quad \text{y } C = \begin{bmatrix} 1 & 0 & 0 \\ 1 & -4 & 0 \\ 2 & -1 & 5 \end{bmatrix}$$

Determinar si la operación indicada está definida. En caso afirmativo, indicar el tamaño de la matriz resultante y realizar el cálculo explícito.

1.43 AB

1.44 BA

1.45 $(AB)C$

1.46 $2AB - BC$

1.47 $B + 10BC$

1.48 C^2

1.49 $(2AB - BC)^2$, donde $A^2 = AA$

1.50 IA y AI, donde $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

¿Qué efecto produce I en la multiplicación por A?

Problemas reto

Se dice que una matriz cuadrada A es invertible si existe una matriz B que satisface las siguientes relaciones:

$$AB = BA = I$$

donde I es la matriz cuadrada con unos en la diagonal principal y ceros en el resto de las posiciones. A la matriz B, que por lo general se denota por A^{-1}, se le denomina matriz inversa de A.

a) Determinar las condiciones que debe cumplir la matriz siguiente para ser invertible.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

b) Obtener la forma explícita de A^{-1}, si A es invertible.

c) Demostrar que un sistema de m ecuaciones lineales con n incógnitas $x_1, x_2, \ldots, x_n$:

$$\left\{ \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_{11} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_{21} \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_{m1} \end{array} \right\}$$

se puede escribir matricialmente como:

$$AX = B$$

d) Para el sistema cuadrado:

$$\left\{ \begin{array}{c} 2x_1 - 4x_2 = 2 \\ x_1 + 3x_2 = -2 \end{array} \right\}$$

Encontrar la matriz A^{-1} y demostrar que la solución del sistema es:

$$X = A^{-1}B$$

2

Lógica y cálculo proposicional

Objetivos

- Identificar las clases de proposiciones que se pueden encontrar en un enunciado.
- Analizar los enunciados para la elaboración de las tablas de verdad.
- Traducir proposiciones del lenguaje verbal a variables lógicas y viceversa.
- Identificar si un argumento es válido o inválido, así como demostrar su validez.
- Comprender los principios de las operaciones del cálculo proposicional y sus aplicaciones.

2.1 Introducción

Lógica es un término que deriva del griego λοφνεη o λοφικος (logiké o logikós), que a su vez proviene de λογος (logos), que significa **razón**. La lógica se considera una ciencia formal cuyo objeto de estudio son los distintos principios de demostración que permitan comprobar que una afirmación pueda ser considerada como válida.

La metodología de trabajo de la lógica consiste en examinar la validez o la invalidez de una afirmación mediante la aplicación de una sistematización en los argumentos y, por ende, de un análisis de su estructura lógica, sin tener en cuenta el contenido de lo que se ha argumentado ni considerar siquiera el lenguaje utilizado, y sin contemplar el estado de realidad del contenido.

La lógica se aplica en muy diversas áreas. En ingeniería es de gran utilidad en la electrónica, para el diseño de circuitos mediante compuertas lógicas, y en programación, para el diseño de programas que requieren la unión de operadores lógicos. En administración, porque esta hace uso de los conocimientos organizados para dar solución a problemas reales. En derecho, su aplicación se conoce como "lógica jurídica", considerada un método de investigación para entender a la ciencia del derecho, que obtiene su principal fuente del conocimiento en la razón y no de la experiencia.

Bertrand Arthur William Russell, filósofo, lógico, matemático y escritor británico, realizó aportaciones innovadoras a los fundamentos de las matemáticas y al desarrollo de la lógica formal contemporánea, así como a la filosofía analítica. Sus aportaciones a las matemáticas incluyen el descubrimiento de la paradoja Russell, la defensa del logicismo (la visión acerca de que las matemáticas son, en algún sentido significativo, reducibles a la lógica formal), la introducción a la teoría de los tipos y el perfeccionamiento y la divulgación de la lógica de primer orden o cálculo de predicados de primer orden. Se le considera, junto con Kurt Gödel, como uno de los dos logicistas más destacados del siglo XX.

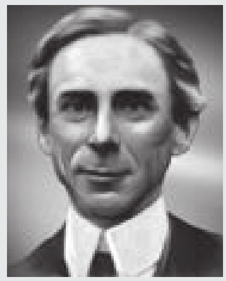


Figura 2.1 Bertrand Arthur William Russell (1872-1970).

2.2 Proposiciones y operadores lógicos

La proposición: características y estructura

Una proposición o enunciado constituye una oración que tiene un valor de verdad, es decir, puede ser verdadera o falsa, pero no ambas. La proposición es uno de los elementos fundamentales en lógica.

Si la oración es una pregunta, una orden, carece de sentido o es muy imprecisa, entonces no puede ser clasificada como verdadera o falsa, y por tanto no puede ser una proposición.

EJEMPLO

¿Cuáles de las siguientes oraciones son proposiciones?

1. La Tierra es plana.
2. $3 + 6 = 8$.
3. La temperatura del núcleo del Sol es de 6 000 °C.
4. $x + y = 24$.
5. ¿Vas a la tienda?
6. Toma tu medicina.
7. La selección mexicana ganará mañana la copa mundial.

Solución

- Las oraciones 1 y 2 son proposiciones, ya que pueden tomar un valor verdadero o falso.
- En estos momentos no es posible determinar la certeza o falsedad de la oración 3; sin embargo, en principio, sí puede determinarse si es verdadera o falsa, por tanto también se considera una proposición.
- La 4 es una oración, pero no una proposición, ya que es verdadera o falsa dependiendo de los valores de x y y en determinado momento.
- La oración 5 es una pregunta, no una proposición.
- La oración 6 es una orden, pero no una proposición.
- La oración 7 es una proposición que puede ser verdadera o falsa, pero debemos esperar hasta mañana para saber su valor de verdad.

Clasificación de las proposiciones

Antes de clasificar las proposiciones, es preciso considerar cómo representarlas para luego hacer referencia a estas en diversas expresiones lógicas.

En matemáticas, las letras x, y, z, … se utilizan para representar variables que pueden ser reemplazadas con números, las cuales pueden ser combinadas con diversos operadores, como: $+$, $-$, $\times$, $\div$.

Por su parte, en lógica las letras p, q, r, … se usan para representar variables proposicionales, esto es, variables que pueden ser reemplazadas por proposiciones simples.

Así, es posible utilizar una proposición haciendo referencia solo a la variable proposicional utilizada.

En lógica se pueden encontrar dos clases de proposiciones: simples o atómicas y compuestas o moleculares.

EJEMPLO

Si se tiene la siguiente proposición: "La Tierra es plana", esta se puede representar eligiendo una variable proposicional, digamos "p". De este modo, la proposición simple quedaría representada de la siguiente forma: "p: La Tierra es plana".

Proposiciones simples o atómicas

Las proposiciones simples o atómicas son aquellas que están estructuradas por una única oración. Para su representación, a la proposición se le asigna una variable proposicional.

EJEMPLO

p: El oro es un metal precioso.
q: Hoy es martes.
r: Benito Juárez nació en Oaxaca.
s: Rodolfo Neri Vela fue el primer astronauta mexicano.

Supóngase que se quiere negar alguna proposición simple, denotada como "$\sim$"; entonces, si se quiere decir que "Hoy no es martes", se puede escribir "$\sim q$", haciendo referencia a la variable proposicional elegida.

Proposiciones compuestas o moleculares

Las proposiciones compuestas o moleculares son aquellas que están estructuradas por dos o más proposiciones simples unidas por operadores lógicos, tales como $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, entre otros. En el caso de las proposiciones compuestas, a cada proposición simple que la forma se le puede asignar una variable proposicional.

EJEMPLO

a) Pitágoras era griego y geómetra.
b) El sentido de la calle es hacia el norte o hacia el sur.
c) Si salgo tarde, entonces no visitaré a la abuela.
d) Iré al cine si y solo si tú pagas las palomitas.

Al leer cualquiera de las proposiciones compuestas anteriores, es posible observar a simple vista que todas ellas están formadas por dos proposiciones simples.

Al analizar el inciso a), se comprueba que esta proposición compuesta está estructurada por las proposiciones simples:

p: Pitágoras era griego.
q: Pitágoras era geómetra.

Al combinar ambas proposiciones se utiliza el operador lógico "$\wedge$", que se estudiará más adelante. Dicha proposición compuesta se puede representar como: "p y q", haciendo referencia a las variables proposicionales utilizadas.

Es importante destacar que, en ocasiones, los operadores están presentes de manera implícita dentro de la oración.

Ejemplo

Sea la siguiente oración

Si estudio, triunfaré en la vida.

En primera instancia, esta parece una proposición simple, pero si se observa con mayor detalle, se nota que tiene dos verbos: estudiar y triunfar, lo que indica que tiene más de una proposición simple; por tanto, se trata de una proposición compuesta. En este caso el operador implícito es ***entonces***, y se puede expresar de la siguiente manera:

Si estudio, entonces triunfaré en la vida.

Esto permite destacar que no siempre se "descubren" a primera vista los operadores en una proposición compuesta.

Traducción del lenguaje natural al simbólico y del lenguaje simbólico al natural

Antes de estudiar cómo traducir del lenguaje natural al simbólico y viceversa, primero se define cada uno de estos lenguajes.

Lenguaje natural

Por lengua natural se entiende a la lengua utilizada normalmente (lengua materna) en una comunidad de individuos para la comunicación entre ellos. Es decir, el lenguaje que hablamos en nuestra vida cotidiana, que en nuestro caso es el español.

Lenguaje simbólico

La lógica cuenta con un sistema de símbolos construido en especial para lograr precisión y operatividad. La lógica se expresa, pues, en un lenguaje artificial. El lenguaje de la lógica es, además, un lenguaje formal constituido por símbolos.

Al simbolizar un lenguaje lo que se persigue es, básicamente, sencillez, claridad y exactitud. Pues, en este caso, es más sencillo y resulta más claro y exacto representar las cosas mediante símbolos.

Por este motivo, la simbolización del lenguaje lógico permite examinar con mayor facilidad las formas del pensamiento y sus leyes.

Traducir

Trabajar con proposiciones requiere la aptitud de poder traducirlas del lenguaje natural al simbólico (también denominada traducción simbólica) y viceversa.

En el apartado anterior vimos cómo representar proposiciones mediante variables proposicionales, las cuales pueden ser reemplazadas por proposiciones simples, lo cual constituye una traducción simbólica de dichas proposiciones.

Nota

Aunque en la próxima sección se estudiarán los operadores lógicos con más detalle, aquí se pueden utilizar algunos de los ya vistos de una manera informal.

Para traducir proposiciones compuestas, primero se eligen las variables proposicionales necesarias con base en las proposiciones simples involucradas, además de los respectivos operadores lógicos que las relacionan.

En muchas ocasiones, elegimos las variables proposicionales de tal manera que hagan alusión al contenido mismo de la proposición.

EJEMPLO

Si se tiene la proposición simple: "Miguel Hidalgo es el padre de la Patria", es posible escoger las variables proposicionales *m* para hacer alusión a "Miguel Hidalgo" y *p* para "padre de la Patria".

También es posible hacer lo mismo para las proposiciones compuestas.

EJEMPLO

Hacer la traducción lógica de la proposición compuesta:

Miss Universo es atractiva e inteligente.

En primera instancia, se puede observar que la proposición en cuestión está constituida por las proposiciones simples:

a: Miss Universo es atractiva.

i: Miss Universo es inteligente.

por lo que $a \wedge i$ es su traducción lógica.

Pero, no solo se requiere traducir del lenguaje natural al simbólico; en muchas ocasiones también se requiere hacer una traducción del lenguaje simbólico al natural.

EJEMPLO

Sean las proposiciones simples:

g: Guadalajara gana el campeonato.

a: América gana el campeonato.

Y se desea traducir las siguientes proposiciones al lenguaje natural:

1. $g \wedge \sim a$
2. $\sim g \wedge a$
3. $\sim g$
4. $\sim a$

Solución

1. Guadalajara gana el campeonato y América no gana el campeonato.
2. Guadalajara no gana el campeonato y América gana el campeonato.
3. Guadalajara no gana el campeonato.
4. América no gana el campeonato.

Cuando se vean más a fondo los operadores lógicos, entonces se podrán traducir proposiciones compuestas constituidas por más de dos proposiciones simples.

Operadores lógicos

Los operadores lógicos son aquellos símbolos que permiten decidir qué valor de verdad tiene una proposición.

El valor de verdad de una proposición simple puede ser verdadero o falso, y los únicos operadores lógicos que se pueden utilizar en estas proposiciones son la negación y la doble negación.

El valor de verdad de una proposición compuesta es verdadero o falso y depende de los valores de verdad de las proposiciones simples que la estructuran, las cuales están combinadas por operadores lógicos.

Ahora, se definen y analizan los operadores lógicos, incluyendo su tabla de verdad; aunque algunos de estos ya se mencionaron en el apartado anterior.

Negación ($\sim$)

La negación de cualquier proposición *p* será falsa cuando se niegue una proposición verdadera y será verdadera cuando se niegue una proposición falsa.

Algunas formas de la negación son: no, nunca, ni, jamás, es falso, no es cierto, no ocurre, de ninguna forma, por nada de, en lo absoluto, entre otras. La tabla de verdad de la negación se muestra en la tabla 2.1.

Tabla 2.1 Tabla de verdad de la negación

p	$\sim p$
V	F
F	V

EJEMPLO

p: El acusado dice la verdad.

$\sim p$: El acusado no dice la verdad.

En este caso, $\sim p$ también se puede traducir como: "no es cierto que el acusado dice la verdad" o "es falso que el acusado dice la verdad".

Doble negación

Si la negación de cualquier proposición p verdadera es falsa, entonces cuando se vuelve a negar será nuevamente verdadera; en caso contrario, si la negación de una proposición falsa es verdadera, al volverse a negar esta será falsa de nuevo.

La tabla de verdad de la doble negación se representa en la tabla 2.2, donde se observa que $\sim(\sim p)$ y p tienen los mismos valores de verdad. Entonces, la doble negación de una proposición es igual a la proposición original.

Tabla 2.2 Tabla de verdad de la doble negación

p	$\sim(\sim p)$
V	F
F	V

Algunas formas de la doble negación son: no es cierto que no, no ocurre que no, no es falso que, no es cierto que no ocurre que, no es cierto que jamás, etcétera.

EJEMPLO

p: El acusado dice la verdad.

$\sim p$: El acusado no dice la verdad.

$\sim(\sim p)$: No es cierto que el acusado no dice la verdad.

Por tanto: el acusado dice la verdad.

Conjunción ($\wedge$)

Si p y q representan dos proposiciones simples, entonces la proposición compuesta $p \wedge q$, solo será verdadera cuando las dos proposiciones lo sean.

Algunas formas de la conjunción son: y, además de, también, así como, pero, e, entre muchas otras.

Además, la conjunción es conmutativa, es decir:

$$p \wedge q = q \wedge \mathrm{p}$$

La tabla de verdad de la conjunción se muestra en la tabla 2.3.

Tabla 2.3 Tabla de verdad de la conjunción

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

EJEMPLO

p: El acusado es pobre.
q: El acusado es honesto.
$p \wedge q$: El acusado es pobre, pero honesto.
r: El helio es más liviano que el aire.
s: El helio es explosivo.
$r \wedge s$: El helio es más liviano que el aire y es explosivo.

Disyunción inclusiva ($\vee$)

Si p y q representan dos proposiciones simples, entonces la proposición compuesta $p \vee q$ solo será falsa cuando las dos proposiciones lo sean.

Algunas formas de la disyunción inclusiva son: o, o bien, u, entre otras.

La disyunción también es conmutativa, es decir:

$$p \vee q = q \vee p$$

La tabla de verdad de la disyunción inclusiva se muestra en la tabla 2.4.

Este operador se denomina inclusivo, precisamente porque es verdadero, aun cuando se cumplen las dos disyuntivas.

Tabla 2.4 Tabla de verdad de la disyunción inclusiva

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

EJEMPLO

r: Lloverá en la tarde.
s: Saldrá el Sol.
$r \vee s$: Lloverá en la tarde o saldrá el Sol.

Disyunción exclusiva ($\oplus$)

Si p y q representan dos proposiciones simples, entonces la proposición compuesta $p \oplus q$ solo será falsa cuando las dos proposiciones tuvieren el mismo valor de verdad.

Se denomina disyunción exclusiva porque se tiene que elegir una de cualquiera de las dos disyuntivas, pero no ambas.

Algunas formas de la disyunción exclusiva son: o, o bien, u, o… o, entre otras.

La disyunción exclusiva es conmutativa, es decir:

$$p \oplus q = q \oplus p$$

La tabla de verdad de la disyunción exclusiva se muestra en la tabla 2.5.

Tabla 2.5 Tabla de verdad de la disyunción inclusiva

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

EJEMPLO

t: Apruebas el ciclo escolar.
u: Repruebas el ciclo escolar.
$t \oplus u$: Apruebas o repruebas el ciclo escolar.
r: Estoy en Guadalajara.
s: Estoy en Monterrey.
$r \oplus s$: Estoy o en Guadalajara o en Monterrey.

Ya que, como es evidente, no es posible que una persona se encuentre en ambos lugares al mismo tiempo, por eso solo debe estar en un solo lugar.

2.3 Proposiciones condicionales

Condicional o implicación ($\Rightarrow$)

Si p y q representan dos proposiciones simples, entonces la proposición compuesta $p \Rightarrow q$ solo será falsa cuando p, llamado antecedente o hipótesis, sea verdadero y q, llamado consecuente o conclusión, sea falso.

Algunas formas de la condicional o implicación son: si … entonces, se sigue, por tanto, se infiere, de ahí que, se deduce, implica, entre otras.

La condicional no es conmutativa, es decir:

$$p \Rightarrow q \neq q \Rightarrow p$$

La tabla de verdad de la condicional se muestra en la tabla 2.6.

Este operador tiene diversos sentidos, pero uno de los más utilizados es cuando no es posible que p sea verdadera y que, al mismo tiempo, q sea falsa. En este caso, la única posibilidad es que la condicional sea falsa.

Tabla 2.6 Tabla de verdad de la condicional

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

EJEMPLO

t: Llueve.
u: Me mojaré.
$t \Rightarrow u$: Si llueve, entonces me mojaré.
p: Estudio.
q: Aprobaré el ciclo escolar.
$p \Rightarrow q$: Si estudio, entonces aprobaré el ciclo escolar.

La condicional también se puede encontrar en alguna de las formas siguientes:

- Si p entonces q.
- Si p, q.
- p entonces q.
- q si p.
- p es condición suficiente para q.
- q es condición necesaria para p.
- p implica a q.

En todos los casos anteriores, p es el antecedente y q el consecuente; en otras palabras, todos se representan $p \Rightarrow q$.

Bicondicional o equivalencia ($\Leftrightarrow$)

Si p y q representan dos proposiciones simples, entonces la proposición compuesta $p \Leftrightarrow q$, solo será verdadera cuando ambas proposiciones tengan el mismo valor de verdad.

Algunas formas de la bicondicional son: si y solo si, entonces y solo entonces, es idéntico, equivale a, es equivalente a, entre otras más.

La bicondicional es conmutativa, es decir:

$$p \Leftrightarrow q = q \Leftrightarrow p$$

La tabla de verdad de la bicondicional se muestra en la tabla 2.7.

Además, si $p \Rightarrow q$ y $q \Rightarrow p$ entonces $p \Leftrightarrow q$.

Tabla 2.7 Tabla de verdad de la bicondicional

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

EJEMPLO

p: Si un polígono tiene cuatro lados, entonces es un cuadrilátero.
q: Si un polígono es un cuadrilátero, entonces tiene cuatro lados.
$p \Leftrightarrow q$: Un polígono es cuadrilátero si y solo si tiene cuatro lados.

2.4 Tablas de verdad

Aunque ya se han utilizado las tablas de verdad para obtener los valores de verdad de proposiciones simples y compuestas, aún no las hemos definido formalmente.

Una tabla de verdad, o tabla de valores de verdad, es una tabla que muestra el valor de verdad de una proposición compuesta, así como de algunos casos de proposiciones simples, cuando estas utilizan los operadores lógicos de negación y doble negación, dependiendo de los operadores lógicos usados y de los valores de verdad de las proposiciones simples involucradas.

La tabla de verdad de todos los operadores lógicos vistos antes se muestra en la tabla 2.8.

Las tablas de verdad fueron desarrolladas por el filósofo y matemático estadounidense Charles Sanders Peirce el año 1880, pero el formato más popular es el que introdujo el matemático y filósofo británico Ludwig Wittgenstein (1889-1951) en su obra *Tractatus logico-philosophicus*, publicado en 1921. Según Wittgenstein, el método de tablas de verdad sirve para determinar las condiciones de verdad de un enunciado; es decir su significado, en función de las condiciones de verdad de sus elementos atómicos. En otras palabras, la tabla de verdad nos dice en qué situaciones el enunciado es verdadero y en cuáles es falso.

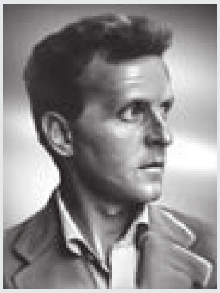


Figura 2.2 Ludwig Josef Johann Wittgenstein (1889-1951).

Tabla 2.8 Tabla de verdad de los operadores lógicos										
p	q	$\sim p$	$\sim q$	$\sim(\sim p)$	$\sim(\sim q)$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \Rightarrow q$	$p \Leftrightarrow q$
V	V	F	F	V	V	V	V	F	V	V
V	F	F	V	V	F	F	V	V	F	F
F	V	V	F	F	V	F	V	V	V	F
F	F	V	V	F	F	F	F	F	V	V

Construcción de una tabla de verdad

La importancia de las tablas de verdad radica en que gran parte del razonamiento lógico y de las relaciones entre proposiciones se pueden ilustrar a través de estas.

Para construir una tabla de verdad se efectúan los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Obtener la traducción lógica de la proposición compuesta.
3. Obtener la cantidad de todas las combinaciones de valores de verdad de las premisas. La cantidad de valores de verdad está dado por la fórmula 2^n, donde n es la cantidad de variables proposicionales de las premisas.
   Así:

Tabla 2.9	
Núm. de variables proposicionales	Combinaciones
1	2
2	4
3	8
4	16
5	32
6	64
$\vdots$	$\vdots$
n	2^n

4. Asignar a cada variable proposicional los valores de verdad correspondientes.
5. Resolver las operaciones lógicas.

Ejemplo

Construir la tabla de verdad de la proposición compuesta:

Mi tío no vino a dormir y no fue a trabajar.

Solución

1. Asignar variables proposicionales.
   Dicha proposición está compuesta por las proposiciones simples:
   p: Mi tío no vino a dormir.
   q: Mi tío no fue a trabajar.

Continúa

2. Realizar traducción lógica.

   Como se observa, las proposiciones p y q están negadas, por lo que su traducción lógica es:

$$\sim p \wedge \sim q$$

3. Obtener la cantidad de combinaciones de valores de verdad.

   Como se tienen dos variables proposicionales, la cantidad de combinaciones de valores de verdad será:

$$2^2 = 4$$

4. Asignar valores de verdad a variables proposicionales.

   En este caso, también se incluyen los valores de verdad de las proposiciones negadas.

Tabla 2.10

p	q	$\sim p$	$\sim q$
V	V	F	F
V	F	F	V
F	V	V	F
F	F	V	V

5. Resolver las operaciones lógicas.

Tabla 2.11

p	q	$\sim p$	$\sim q$	$\sim p \wedge \sim q$
V	V	F	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

2.5 Los argumentos: premisas y conclusiones

Los razonamientos que estudia la lógica se llaman argumentos y su tarea consiste en descubrir qué es lo que hace que un argumento sea válido y constituya una inferencia correcta.

Por su parte, la inferencia es una actividad con la cual se afirma una proposición sobre otra y otras proposiciones se aceptan como punto de partida del proceso.

Un argumento es un conjunto de una o más proposiciones, la última de las cuales se denomina conclusión, mientras que las anteriores se llaman premisas.

De manera intuitiva, las premisas son la evidencia o las razones que deben convencernos de la veracidad de la conclusión, y el argumento es la concatenación de las primeras con la última.

Es habitual representar los argumentos haciendo un listado de las premisas y la conclusión, separando la última mediante una línea, como se observa a continuación:

$$\left.\begin{array}{c}\text{Proposición 1}\\ \text{Proposición 2}\\ \vdots \\ \hline \text{Conclusión}\end{array}\right\}\ \text{Premisas}$$

Otra manera de representar los argumentos es haciendo un listado de las premisas y la conclusión, separándolos con el símbolo $\therefore$, que significa: por tanto.

Conviene hacer notar que cada argumento tiene solo una conclusión. El siguiente es un ejemplo que contiene tres proposiciones simples (en dos premisas).

EJEMPLO

Si Alfredo es elegido presidente de la asociación de colonos, entonces Bernardo es elegido vicepresidente y Carlos es elegido tesorero. Bernardo no es elegido vicepresidente, por tanto Alfredo no es elegido presidente de la asociación de colonos.

En este caso, la proposición: "Si Alfredo es elegido presidente de la asociación de colonos, entonces Bernardo es elegido vicepresidente y Carlos es elegido tesorero", representa la primera premisa; mientras que la proposición "Bernardo no es elegido vicepresidente" es la segunda premisa. De estas dos premisas se obtiene una tercera proposición: "Alfredo no es elegido presidente de la asociación de colonos", que es la conclusión.

Ahora, hay que asignar variables proposicionales a cada proposición simple que aparece en el argumento; esto es:

a: Alfredo es elegido presidente de la asociación de colonos.

b: Bernardo es elegido vicepresidente.

c: Carlos es elegido tesorero.

Enseguida, se hace la traducción lógica de dicho argumento y se escribe en alguna de las dos formas descritas, para representar los argumentos:

$$\begin{array}{l} 1.\ (a \Rightarrow b) \wedge c \\ 2.\ \sim b \\ \quad \therefore \sim a \end{array} \qquad \text{o} \qquad \begin{array}{l} 1.\ (a \Rightarrow b) \wedge c \\ 2.\ \underline{\sim b} \\ \quad \sim a \end{array}$$

Por último, solo falta verificar si el argumento es válido; no obstante, esa cuestión se analizará en las siguientes secciones.

Como se puede observar, en el ejemplo anterior fue fácil identificar las premisas y la conclusión; sin embargo, no siempre resulta sencillo poder identificar las premisas y la conclusión de un argumento, para esto pueden ser útiles los adverbios que se listan en la tabla 2.12:

Tabla 2.12 Adverbios que indican premisas o conclusiones

Adverbios que indican premisa	Adverbios que indican conclusión
Puesto que	Por tanto
Dado que	Se sigue que
Si	Resulta que
Considerando	Se infiere que
Puesto	Luego
Como	Tomando en cuenta
Ya que	Por consiguiente
Por que	En consecuencia
Aunque	Se deduce que
Toda vez que	Por lo que

Clasificación de argumentos: tautología, contradicción y contingencia

A partir del resultado de las tablas de verdad, es posible clasificar los argumentos en tres tipos: tautología, contradicciones y contingencias.

Una **tautología** es una proposición que es verdadera para todos los posibles valores de verdad de sus componentes simples.

Ejemplo

Tabla 2.13

p	$p \Leftrightarrow p$
V	V
F	V

Una proposición es llamada **contradicción** o **absurdo** si ofrece un resultado falso para todos los posibles valores de verdad de sus componentes simples.

Ejemplo

Tabla 2.14

p	$\sim p$	$p \wedge \sim p$
V	F	F
F	V	F

Una proposición es una **contingencia** cuando puede ser verdadera o falsa, dependiendo de los valores de verdad de sus componentes simples.

Ejemplo

Tabla 2.15

p	q	$\sim p$	$\sim p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

2.6 Métodos de demostración

La demostración es un razonamiento o serie de razonamientos que prueba la validez de un nuevo conocimiento mediante el establecimiento de sus conexiones necesarias con otros conocimientos.

Cuando un conocimiento queda demostrado, entonces se le reconoce como válido y es admitido dentro de la disciplina correspondiente. La demostración es, por tanto, el enlace entre los conocimientos recién adquiridos y el conjunto de los conocimientos adquiridos con anterioridad. El enlace entre los conocimientos recién adquiridos y los adquiridos con anterioridad está constituido por una sucesión finita de proposiciones que bien son postulados o bien son conocimientos cuya validez se ha inferido de otras proposiciones mediante operaciones lógicas perfectamente coordinadas. La demostración permite explicar unos conocimientos por otros; por tanto, constituye una prueba rigurosamente racional.

Hoy día, hay diversos métodos para demostrar la validez de un argumento, entre los principales destacan: el de las tablas de verdad, la prueba formal de validez, la prueba de invalidez, la prueba condicional y la prueba indirecta.

Método de tablas de verdad

Cuando un argumento es una tautología se considera que este es válido, pero si es una contradicción es inválido; lo mismo ocurre con una contingencia.

Para obtener la validez de un argumento por tabla de verdad se efectúan los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Obtener la traducción lógica de las premisas.
3. Organizar el argumento en forma horizontal, uniendo las premisas con el operador lógico $\wedge$.
4. Obtener la cantidad de todas las combinaciones de valores de verdad de las premisas. La cantidad de valores de verdad está dado por la fórmula 2^n, donde n es la cantidad de variables proposicionales de las premisas.

Nota

Por lo general, se utilizan líneas en la parte inferior de la tabla de verdad para ayudar a identificar las variables lógicas involucradas en una operación lógica.

5. Asignar a cada variable proposicional los valores de verdad correspondientes.
6. Resolver las operaciones lógicas, iniciando por las premisas y finalizando con la conclusión. El símbolo de por tanto ($\therefore$) equivale a la condicional $\Rightarrow$.

Ejemplo

De acuerdo con el argumento de un ejemplo anterior: "Si Alfredo es elegido presidente de la asociación de colonos, entonces Bernardo es elegido vicepresidente y Carlos es elegido tesorero". "Bernardo no es elegido vicepresidente, por tanto Alfredo no es elegido presidente de la asociación de colonos", verificar su validez por tablas de verdad.

Solución

1. Asignar variables proposicionales.

   a: Alfredo es elegido presidente de la asociación de colonos.

   b: Bernardo es elegido vicepresidente.

   c: Carlos es elegido tesorero.

2. Realizar traducción lógica.

   a. $(a \Rightarrow b) \wedge c$

   b. $\sim b$

   $\therefore \sim a$

3. Organizar argumento.

   $\{[(a \Rightarrow b) \wedge c] \wedge \sim b\} \therefore \sim a$

4. Obtener la cantidad de combinaciones de valores de verdad.

   Como en este caso se tienen tres variables proposicionales, la cantidad de combinaciones de valores de verdad será: $2^3 = 8$.

5. Asignar valores de verdad a variables proposicionales.

Tabla 2.16

a	*b*	*c*	{[(*a*	⇒	*b*)	∧	*c*]	∧	∼*b*}	∴	∼*a*
V	V	V	V		V		V		F		F
V	V	F	V		V		F		F		F
V	F	V	V		F		V		V		F
V	F	F	V		F		F		V		F
F	V	V	F		V		V		F		V
F	V	F	F		V		F		F		V
F	F	V	F		F		V		V		V
F	F	F	F		F		F		V		V

6. Resolver las operaciones lógicas.

Tabla 2.17

a	*b*	*c*	{[(*a*	⇒	*b*)	∧	*c*]	∧	∼*b*}	∴	∼*a*
V	V	V	V	V	V	V	V	F	F	V	F
V	V	F	V	V	V	F	F	F	F	V	F
V	F	V	V	F	F	F	V	F	V	V	F

V	F	F	V	F	F	F	F	F	V	V	F
F	V	V	F	V	V	V	V	F	F	V	V
F	V	F	F	V	V	F	F	F	F	V	V
F	F	V	F	V	F	V	V	V	V	V	V
F	F	F	F	V	F	F	F	F	V	V	V

Como el argumento es una tautología, entonces se considera que es válido.

Ejemplo

Considerar el siguiente argumento:

"Si Enrique estudia, entonces aprobará lógica y geometría. Enrique no aprobó lógica, en consecuencia, Enrique no estudió y no aprobó geometría".

Verificar su validez por tablas de verdad.

Solución

1. Asignar variables proposicionales.

   e: Ernesto estudia.

   l: Aprobará lógica.

   g: Aprobará geometría.

2. Realizar traducción lógica.

   a. $e \Rightarrow (l \wedge g)$

   b. $\sim l$

   $\therefore (\sim e \wedge \sim g)$

3. Organizar argumento.

   $\{[e \Rightarrow (l \wedge g)] \wedge \sim l\} \therefore (\sim l \wedge \sim g)$

4. Obtener la cantidad de combinaciones de valores de verdad.

   Como se tienen tres variables proposicionales, la cantidad de combinaciones de valores de verdad será: $2^3 = 8$.

5. Asignar valores de verdad a variables proposicionales.

Tabla 2.18

e	l	g	$\{[e$	$\Rightarrow$	$(l$	$\wedge$	$g)]$	$\wedge$	$\sim l\}$	$\therefore$	$(\sim e$	$\wedge$	$\sim g)$
V	V	V	V		V		V		F		F		F
V	V	F	V		V		F		F		F		V
V	F	V	V		F		V		V		F		F
V	F	F	V		F		F		V		F		V
F	V	V	F		V		V		F		V		F
F	V	F	F		V		F		F		V		V
F	F	V	F		F		V		V		F		F
F	F	F	F		F		F		V		V		V

Continúa

6. Resolver las operaciones lógicas.

Tabla 2.19

e	l	g	$\{[e$	$\Rightarrow$	$(l$	$\wedge$	$g)]$	$\wedge$	$\sim l\}$	$\therefore$	$(\sim e$	$\wedge$	$\sim g)$
V	V	V	V	V	V	V	V	F	F	V	F	F	F
V	V	F	V	F	V	F	F	F	F	V	F	F	V
V	F	V	V	F	F	F	V	F	V	V	F	F	F
V	F	F	V	F	F	F	F	F	V	V	F	F	V
F	V	V	F	V	V	V	V	F	F	V	V	F	F
F	V	F	F	V	V	F	F	F	F	V	V	V	V
F	F	V	F	V	F	F	V	V	V	F	F	F	F
F	F	F	F	V	F	F	F	V	V	V	V	V	V

Como el argumento es una contingencia, entonces se considera como inválido.

Prueba formal de validez

Cuando el argumento tiene más de tres proposiciones simples diferentes no es fácil determinar la validez o invalidez de un argumento mediante tablas de verdad, pues resultaría bastante tedioso hacer dicha tabla de verdad, además de que se puede incurrir en errores involuntarios.

Por ese motivo, el método más conveniente para obtener la validez de los argumentos es la prueba formal de validez, la cual utiliza reglas válidas, como las reglas de inferencia y las reglas de reemplazo o equivalencia.

Pero, antes de utilizar las reglas de inferencia y las reglas de reemplazo o equivalencia, primero es necesario conocer su definición y sus aspectos fundamentales.

Reglas de inferencia

Las reglas de inferencia son formas de argumentos cuya validez puede ser demostrada por tablas de verdad; además, estas reglas permiten establecer conclusiones muy bien formadas y válidas a partir de otras premisas. En general son usadas para analizar los argumentos con muchas premisas o cuando se tienen cuatro o más proposiciones simples.

1. Modus ponens (MP)

Permite eliminar el antecedente siempre que la segunda premisa sea dicho antecedente.

$p \Rightarrow q$

p

$\therefore q$

2. Modus tollens (MT)

Permite eliminar el consecuente siempre y cuando esté negado en la segunda premisa, dando como consecuencia el antecedente negado.

$p \Rightarrow q$

$\sim q$

$\therefore \sim p$

3. **Silogismo disyuntivo (SD)**
   Permite eliminar una de las dos disyunciones siempre que una de las dos esté negada en la segunda premisa.

$p \vee q$	$p \vee q$
$\sim p$	$\sim q$
$\therefore q$	$\therefore p$

4. **Silogismo hipotético (SH)**
   Permite eliminar el consecuente de la primera premisa y el antecedente de la segunda premisa, siempre y cuando sean iguales.
   $p \Rightarrow q$
   $q \Rightarrow r$
   $\therefore p \Rightarrow r$

5. **Adición (AD)**
   Permite agregar las variables proposicionales que se necesiten.
   p
   $\therefore p \vee q$

6. **Simplificación (SIM)**
   Permite eliminar las variables proposicionales que no se necesiten.

$p \wedge q$	$p \wedge q$
$\therefore p$	$\therefore q$

7. **Conjunción (CONJ)**
   Permite unir dos premisas diferentes.
   p
   q
   $\therefore p \wedge r$

8. **Dilema constructivo (DC)**
   Permite eliminar los antecedentes de las dos condicionales, dando como resultado la disyunción de los consecuentes.
   $(p \Rightarrow q) \wedge (r \Rightarrow s)$
   $p \vee r$
   $\therefore q \vee s$

9. **Dilema destructivo (DD)**
   Permite eliminar los antecedentes de las dos condicionales, dando como resultado la disyunción de la negación de los consecuentes.
   $(p \Rightarrow q) \wedge (r \Rightarrow s)$
   $\sim q \vee \sim s$
   $\therefore \sim p \vee \sim q$

10. **Absorción (ABS)**
    Permite reescribir el consecuente, dando como resultado la conjunción del antecedente y consecuente.
    $p \Rightarrow q$
    $\therefore p \Rightarrow (p \wedge q)$

Reglas de reemplazo o equivalencia

No siempre un argumento válido o inválido se puede comprobar por medio de las reglas de inferencia; por eso, se utilizan otras reglas conocidas como reglas de reemplazo o reglas de equivalencia, que sustituyen o reemplazan (según sea necesario) para lograr la demostración o prueba de validez del argumento.

Nota

Se utiliza el símbolo $\equiv$ para indicar la equivalencia de las proposiciones y no confundirlo con el símbolo $\Leftrightarrow$, aunque lógicamente sean equivalentes.

1. **Leyes de De Morgan (DM)**
   Permite cambiar de disyunción a conjunción y viceversa, negando ambas variables lógicas.
   $\sim(p \vee q) \equiv \sim p \wedge \sim q$
   $\sim(p \wedge q) \equiv \sim p \vee \sim q$

2. **Conmutación (CONM)**
   Permite cambiar el orden de las variables lógicas sin cambiar el operador lógico.
   $(p \vee q) \equiv (q \vee p)$
   $(p \wedge q) \equiv (q \wedge p)$
   $(p \Leftrightarrow q) \equiv (q \Leftrightarrow p)$

3. **Doble negación (DN)**
   Si la negación de cualquier proposición p verdadera es falsa, entonces cuando se vuelve a negar esta será nuevamente verdadera y viceversa.
   $\sim(\sim p) \equiv p$

4. **Distribución (DIS)**
   Permite distribuir la variable lógica de afuera y su operador lógico con las variables lógicas de dentro y su operador lógico.
   $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge q)$
   $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee q)$

5. **Tautología (TAU)**
   Permite unir dos variables lógicas en una sola.
   $(p \wedge p) \equiv p$
   $(p \vee p) \equiv p$

6. **Asociación (ASO)**
   Permite agrupar diferentes formas de las variables lógicas, siempre y cuando sea el mismo operador lógico.
   $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
   $p \vee (q \vee r) \equiv (p \vee q) \vee r$

7. **Implicación material (IMP)**
   Permite cambiar de disyunción a condicional y viceversa.
   $(p \Rightarrow q) \equiv (\sim p \vee q)$

8. **Transposición (TRAN)**
   Permite conmutar las variables lógicas de la condicional negando cada una de estas.
   $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$

9. **Exportación (EXP)**
   Permite cambiar de conjunción a condicional y viceversa, modificando su agrupación.
   $[(p \wedge q) \Rightarrow r] \equiv [p \Rightarrow (q \Rightarrow r)]$

10. **Equivalencia material (EM)**
    Permite reescribir la bicondicional.
    $(p \Leftrightarrow q) \equiv [(p \Rightarrow q) \wedge (q \Rightarrow p)]$
    $(p \Leftrightarrow q) \equiv [(p \wedge q) \vee (\sim p \wedge \sim q)]$

Pasos para demostrar la validez de un argumento

La prueba formal de validez consiste en deducir la conclusión del argumento en función de sus premisas, esto es, que las premisas infieran la conclusión.

A fin de que una demostración, por la prueba formal de validez, resulte perfectamente clara, se deben seguir los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Realizar la traducción lógica de las premisas.
3. Organizar el argumento con sus premisas en forma vertical, escribiendo antes de cada premisa un número de premisa consecutivo.
4. Utilizar las reglas de inferencia y/o de reemplazo que conduzcan a nuevas premisas (inferencias). Estas siempre deben ser antecedidas por un nuevo número de premisa. Al utilizar las reglas se debe escribir su abreviatura y el número o números de las premisas de las que se ha deducido.
5. El proceso de inferencia termina cuando se llega a la conclusión del argumento.

Además del proceso anterior, también es necesario considerar algunas condiciones para la demostración:

1. Utilizar todas las premisas.
2. Utilizar todas las nuevas premisas obtenidas.
3. Es posible utilizar las premisas las veces que sean necesarias.

Para entender el proceso descrito antes, se verá un par de ejemplos más detallados.

Ejemplo

Considerar el siguiente argumento: “Si la ley no fue aprobada, entonces la constitución del país queda sin modificaciones. Si la constitución del país queda sin modificaciones no se puede elegir nuevos diputados. O se eligen nuevos diputados o el informe del presidente del país se retrasará. El informe no se retrasó un mes. Por lo que la ley fue aprobada”.

Verificar su validez por la prueba formal de validez.

Solución

1. Asignar variables proposicionales.

- l: La ley fue aprobada.
- c: La constitución del país quedará sin modificaciones.
- d: Se pueden elegir nuevos diputados.
- i: El informe del presidente se retrasará un mes.

2. Realizar traducción lógica.

$\sim l \Rightarrow c$

$c \Rightarrow \sim d$

$d \vee i$

$\sim i$

$\therefore l$

3. Organizar argumento.

1. $\sim l \Rightarrow c$
2. $c \Rightarrow \sim d$
3. $d \vee i$
4. $\sim i$

$\therefore l$

4. Utilizar las reglas de inferencia y/o equivalencia.

1. $\sim l \Rightarrow c$
2. $c \Rightarrow \sim d$
3. $d \vee i$
4. $\sim i$

$\therefore l$

5. d	SD	3,4
6. $\sim c$	MT	2,5
7. l	MT	1,6

5. Como se llega a la conclusión, el proceso de inferencia termina.

Este proceso intenta obtener la conclusión mediante el uso de las reglas citadas antes. La premisa 5 se obtiene de las premisas 3 y 4, por un silogismo disyuntivo. En tanto, la premisa 6 se deduce de las premisas 2 y 5 por un modus tollens. Por último, la premisa 7 se obtiene de las premisas 1 y 6, también por un modus tollens.

Ya que en este punto se obtiene la conclusión, aquí termina el proceso de inferencia, lo que indica que el argumento es válido.

Ejemplo

Considerar el siguiente argumento: "Si el tiempo es agradable, entonces el cielo está despejado. Si el cielo está despejado, entonces iré de día de campo. Si el tiempo es agradable, entonces iré de día de campo implica que si el cielo está despejado entonces nadaré en el río. Si el tiempo es agradable, entonces nadaré en el río implica que me broncearé todo el cuerpo. Por tanto, me broncearé el cuerpo".

Verificar su validez por la prueba formal de validez.

Solución

1. Asignar variables proposicionales.
   - a: El tiempo es agradable.
   - d: El cielo está despejado.
   - c: Iré de día de campo.
   - n: Nadaré en el río.
   - b: Me broncearé el cuerpo.
2. Realizar traducción lógica.
   - $a \Rightarrow d$
   - $d \Rightarrow c$
   - $(a \Rightarrow c) \Rightarrow (d \Rightarrow n)$
   - $(a \Rightarrow n) \Rightarrow b$
   - $\therefore b$
3. Organizar argumento.
   1. $a \Rightarrow d$
   2. $d \Rightarrow c$
   3. $(a \Rightarrow c) \Rightarrow (d \Rightarrow n)$
   4. $(a \Rightarrow n) \Rightarrow b$

   $\therefore b$
4. Utilizar las reglas de inferencia y/o equivalencia.

1. $a \Rightarrow d$		
2. $d \Rightarrow c$		
3. $(a \Rightarrow c) \Rightarrow (d \Rightarrow n)$		
4. $(a \Rightarrow n) \Rightarrow b$		
$\therefore b$		
5. $a \Rightarrow c$	SH	1,2
6. $(d \Rightarrow n)$	MP	3,5
7. $(a \Rightarrow n)$	SH	1,6
8. b	MP	4,7

5. Como se llega a la conclusión, el proceso de inferencia termina.

La premisa 5 se obtiene de las premisas 1 y 2 por un silogismo hipotético. La premisa 6 se deduce de las premisas 3 y 5 por un modus ponens, mientras que la premisa 7 se deduce de las premisas 1 y 6, también por un silogismo hipotético. Por último, la premisa 8 se obtiene de las premisas 4 y 7 por un modus ponens.

Ya que en este punto se obtiene la conclusión, aquí termina el proceso de inferencia, lo que indica que el argumento es válido.

En ocasiones se requiere verificar la validez de un argumento, del cual ya se da su traducción lógica. En este caso se ahorran los dos primeros pasos del proceso de verificación de la validez de dicho argumento.

Ejemplo

Verificar la validez del siguiente argumento por la prueba formal de validez, dada su traducción lógica:

2. Traducción lógica.
   - $(\sim h \vee i) \Rightarrow (j \Rightarrow k)$
   - $(\sim l \wedge \sim m) \Rightarrow (k \Rightarrow n)$

Continúa

$(h \Rightarrow l) \wedge (l \Rightarrow h)$
$(\sim l \wedge \sim m) \wedge \sim c$
$\therefore\ j \Rightarrow n$

3. Organizar argumento.

1. $(\sim h \vee i) \Rightarrow (j \Rightarrow k)$
2. $(\sim l \wedge \sim m) \Rightarrow (k \Rightarrow n)$
3. $(h \Rightarrow l) \wedge (l \Rightarrow h)$
4. $(\sim l \wedge \sim m) \wedge \sim c$

$\therefore\ j \Rightarrow n$

4. Utilizar las reglas de inferencia y/o equivalencia.

1.	$(\sim h \vee i) \Rightarrow (j \Rightarrow k)$		
2.	$(\sim l \wedge \sim m) \Rightarrow (k \Rightarrow n)$		
3.	$(h \Rightarrow l) \wedge (l \Rightarrow h)$		
4.	$(\sim l \wedge \sim m) \wedge \sim c$		
$\therefore$	$j \Rightarrow n$		
5.	$\sim l \wedge \sim m$	SIM	4
6.	$\sim l$	SIM	5
7.	$h \Rightarrow l$	SIM	3
8.	$k \Rightarrow n$	MP	2,5
9.	$\sim h$	MT	6,7
10.	$\sim h \vee i$	AD	9
11.	$j \Rightarrow k$	MP	1,10
12.	$j \Rightarrow n$	SH	11,8

5. Como se llega a la conclusión, el proceso de inferencia termina aquí.

En este caso, la premisa 5 se obtiene de la simplificación de la premisa 4; la premisa 6 de la simplificación de la premisa 5; la premisa 7 de la simplificación de la 3. Mientras que la premisa 8 de las premisas 2 y 5, por un modus ponens. La premisa 9 de un modus tollens de las premisas 6 y 7. La premisa 10 se obtiene al hacer una adición a la premisa 9. La premisa 11 se obtiene de las premisas 1 y 10 por un modus ponens y la premisa 12 de las premisas 11 y 8, por un silogismo hipotético.

Ya que en este punto se obtiene la conclusión, aquí termina el proceso de inferencia, lo que indica que el argumento es válido.

Prueba de invalidez

Este método también se conoce como prueba por asignación de valores. Está muy relacionado con el método de tablas de verdad, la diferencia consiste en que en lugar de construir la tabla de verdad para el argumento, la demostración de la invalidez se hace de tal modo que se asignan valores de verdad a las proposiciones simples, de modo que las premisas sean verdaderas y la conclusión falsa; es decir, se dan valores a la conclusión tal que su resultado sea falso y luego se trata de utilizar esos valores de verdad en los antecedentes, junto con la combinación de estos, según sea la conveniencia.

Para obtener la invalidez de un argumento por el método de la prueba de invalidez se efectúan los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Obtener la traducción lógica de las premisas.
3. Organizar el argumento de forma horizontal, uniendo las premisas con el operador lógico $\wedge$.
4. Asignar valores de verdad a la conclusión, de tal manera que esta resulte falsa.
5. Tomando en cuenta los valores de verdad asignados a la conclusión, hacer que las premisas del argumento sean verdaderas, resolviendo las operaciones lógicas indicadas. El símbolo de por tanto ($\therefore$) equivale a la condicional $\Rightarrow$.

Ejemplo

Se pretende demostrar la invalidez del siguiente argumento por la prueba de invalidez: “Si llueve entonces me mojo. Si sale el Sol entonces me pondré ropa ligera. Me mojo o sale el Sol. Por tanto, llueve o me pongo ropa ligera”.

Solución

1. Asignar variables proposicionales.

l: Llueve.

m: Me mojo.

s: Sale el Sol.

r: Me pondré ropa ligera.

2. Realizar traducción lógica.

1. $l \Rightarrow m$
2. $s \Rightarrow r$
3. $(m \vee s)$

$\therefore\ (l \vee r)$

3. Organizar argumento.

$[(l \Rightarrow m) \wedge (s \Rightarrow r)] \wedge (m \vee s)]\ \therefore\ (l \vee r)$

4. Asignar valores a la conclusión para que sea falsa.

$[(1 \Rightarrow n) \wedge (s \Rightarrow c)] \wedge (n \vee s)]\ \therefore\ (l \vee r)$

F F

F

5. Hacer que las premisas sean verdaderas, tomando en cuenta los valores asignados a la conclusión.

$[(1 \Rightarrow m) \wedge (s \Rightarrow r)] \wedge (m \vee s)]\ \therefore\ (l \vee r)$

F V F F V F F F

V V V F

V

V

F

Como se puede observar, las premisas son verdaderas y la conclusión es falsa, por lo que el argumento es inválido.

La prueba de invalidez también se puede utilizar directamente para la traducción lógica del argumento.

Ejemplo

Demostrar la invalidez del siguiente argumento por el método de la prueba de invalidez, dada su traducción lógica.

Solución

2. Traducción lógica.

1. $a \Rightarrow (b \Rightarrow c)$
2. $b \Rightarrow (\sim c \Rightarrow d)$
3. $(c \vee d) \Rightarrow e$

$\therefore\ a \Rightarrow e$

3. Organizar argumento.

$\{[a \Rightarrow (b \Rightarrow c)] \wedge [b \Rightarrow (\sim c \Rightarrow d)]\} \wedge (c \vee d) \Rightarrow e]\ \therefore\ a \Rightarrow e$

4. Asignar valores a la conclusión para que sea falsa.

$\{[a \Rightarrow (b \Rightarrow c)] \wedge [b \Rightarrow (\sim c \Rightarrow d)]\} \Rightarrow e]\ \therefore\ a \Rightarrow e$

V F

F

Continúa

5. Hacer que las premisas sean verdaderas, tomando en cuenta los valores asignados a la conclusión.

$\{[a \Rightarrow (b \Rightarrow c)] \wedge [b \Rightarrow (\sim c \Rightarrow d)]\} \wedge (c \vee d) \Rightarrow e] \therefore a \Rightarrow e$

```
V   F   F   F     V   F    F   F    F  V   F
     V             F        F         F
 V          V              V
        V
               V
                    F
```

Como se puede observar, las premisas son verdaderas y la conclusión es falsa, por lo que el argumento es inválido.

Prueba condicional

Este método se aplica solo a argumentos que tengan como conclusión una condicional; en otros casos no sería posible utilizarlo, ya que el antecedente de la condicional resulta ser una premisa más, mientras que la conclusión se determina como una nueva conclusión a la cual se debe llegar con una prueba formal de validez.

Para demostrar la validez de un argumento por el método de la prueba condicional se deben seguir los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Obtener la traducción lógica de las premisas.
3. Organizar el argumento con sus premisas en forma vertical, escribiendo antes de cada premisa un número de premisa consecutivo.
4. El antecedente de la conclusión se convierte en una premisa más, escribiendo a su derecha PC, para indicar que la premisa obtenida es por prueba condicional, y se deja el consecuente como la conclusión.
5. Utilizar el procedimiento de la prueba formal de validez tomando en cuenta la nueva conclusión.
6. El proceso de inferencia concluye cuando se llega a la nueva conclusión del argumento.

Para entender este proceso, se analiza un ejemplo con mayor detalle.

Ejemplo

Demostrar la validez del siguiente argumento por el método de la prueba condicional: "Si salgo temprano de trabajar, entonces iré a la fiesta. Si voy a la fiesta, entonces veré a la chica que me gusta. Si veo a la chica que me gusta, entonces bailaré toda la noche. Por lo que si salgo temprano de trabajar, entonces bailaré toda la noche".

Solución

1. Asignar variables proposicionales.

t: Salgo temprano de trabajar.

f: Iré a la fiesta.

c: Veré a la chica que me gusta.

b: Bailaré toda la noche.

2. Realizar traducción lógica.

$t \Rightarrow f$

$f \Rightarrow c$

$c \Rightarrow b$

$\therefore t \Rightarrow b$

3. Organizar el argumento.

1. $t \Rightarrow f$
2. $f \Rightarrow c$
3. $c \Rightarrow b$

$\therefore t \Rightarrow b$

Continúa

4. El antecedente de la conclusión se convierte en una premisa más y se deja el consecuente como la conclusión.
   1. $t \Rightarrow f$
   2. $f \Rightarrow c$
   3. $c \Rightarrow b$
   4. t PC

   $\therefore b$
5. Utilizar la prueba formal de validez.
   1. $t \Rightarrow f$
   2. $f \Rightarrow c$
   3. $c \Rightarrow b$
   4. t PC

   $\therefore b$

   5. f MP 1,4
   6. c MP 2,5
   7. b MP 3,6
6. Como se llega a la nueva conclusión, el proceso de inferencia termina.

De esta manera, se ha verificado la validez del argumento.

Si la conclusión está formada por varias condicionales, resulta necesario aplicar varias veces el paso 4, hasta que no quede ninguna condicional.

Ejemplo

Demostrar la validez del siguiente argumento por el método de la prueba condicional: “Si estudio implica que sí apruebo lógica, entonces pasaré el semestre. Por tanto, si estudio, entonces aprobaré lógica implica que si estudio, entonces pasaré el semestre”.

Solución

1. Asignar variables proposicionales.

   e: Estudio.

   l: Aprobaré lógica.

   s: Pasaré el semestre.
2. Realizar traducción lógica.

   $e \Rightarrow (l \Rightarrow s)$

   $\therefore (e \Rightarrow l) \Rightarrow (e \Rightarrow s)$
3. Organizar el argumento.
   1. $e \Rightarrow (l \Rightarrow s)$

   $\therefore (e \Rightarrow l) \Rightarrow (e \Rightarrow s)$
4. El antecedente de la conclusión se convierte en una premisa más y se deja el consecuente como la conclusión; las veces que sea necesario.
   1. $e \Rightarrow (l \Rightarrow s)$
   2. $e \Rightarrow l$ PC
   3. e PC

   $\therefore s$
5. Utilizar la prueba formal de validez.
   1. $e \Rightarrow (l \Rightarrow s)$
   2. $e \Rightarrow l$ PC
   3. e PC

   $\therefore s$

   4. $l \Rightarrow s$ MP 1,3
   5. l MP 2,3
   6. s MP 4,5
6. Como se llega a la nueva conclusión, el proceso de inferencia termina.

De esta manera se ha verificado la validez del argumento.

Prueba indirecta

Este método también se conoce como prueba de reducción al absurdo. Mediante este, una demostración indirecta de validez para un argumento dado se construye como premisa adicional a la negación o la contradicción de su conclusión, con lo que se deduce una contradicción explícita del conjunto aumentado de las premisas.

Por lo general, este método de demostración se utiliza cuando resulta complicado demostrar la validez de un argumento utilizando la prueba formal de validez.

Para demostrar la validez de un argumento por el método de prueba indirecta, se deben seguir los siguientes pasos:

1. Asignar variables proposicionales a cada proposición simple.
2. Obtener la traducción lógica de las premisas.
3. Organizar el argumento con sus premisas en forma vertical, escribiendo antes de cada premisa un número de premisa consecutivo.
4. Negar la conclusión escribiendo a su derecha PI, para indicar que la premisa es obtenida por prueba indirecta, e incluirla como una premisa más.
5. Del conjunto total de premisas, empleando las leyes lógicas, deducir una contradicción.
6. El proceso de inferencia concluye cuando se llega a dicha contradicción.

Para entender este proceso, a continuación se presenta un ejemplo más detallado.

Ejemplo

Demostrar la validez del siguiente argumento por el método de la prueba indirecta: "Si el mar está tranquilo, entonces el cielo está despejado y hace calor. Si el cielo está despejado o viajaré en lancha, entonces se verán las estrellas en la noche. Viajaré en lancha o el mar está tranquilo. Por tanto, se verán estrellas en la noche".

Solución

1. Asignar variables proposicionales.

- t: El mar está tranquilo.
- d: El cielo está despejado.
- c: Hace calor.
- e: Se verán estrellas en la noche.
- l: Viajaré en lancha.

2. Realizar traducción lógica.

$t \Rightarrow (d \wedge c)$

$(d \vee c) \Rightarrow e$

$(l \vee t)$

$\therefore\ e$

3. Organizar el argumento.

1. $t \Rightarrow (d \wedge c)$
2. $(d \vee l) \Rightarrow e$
3. $(l \vee t)$

$\therefore\ e$

4. Negar la conclusión.

1. $t \Rightarrow (d \wedge c)$
2. $(d \vee l) \Rightarrow e$
3. $(l \vee t)$

$\therefore\ e$

4. $\sim e$ PI

5. Deducir una contradicción.

1.	$t \Rightarrow (d \wedge c)$	
2.	$(d \vee l) \Rightarrow e$	
3.	$(l \vee t)$	
$\therefore$	e	
4.	$\sim e$	PI
5.	$\sim(d \vee l)$	MT 2,4
6.	$\sim d \wedge \sim l$	DM 5
7.	$\sim l$	SIM 6
8.	t	SD 3,7
9.	$d \wedge c$	MP 1,8
10.	d	SIM 9
11.	$\sim d$	SIM 6
12.	$d \wedge \sim d$	CONJ

6. Como la premisa 12 representa una contradicción, entonces termina el proceso de inferencia.

El proceso anterior indica que el supuesto $\sim e$ no es cierto y por consiguiente la conclusión e es válida.

Cabe señalar que el hecho de haber inferido en el ejemplo que $d \wedge \sim d$ representa solo una alternativa para la demostración de la validez del argumento. Pues, la validez también se puede demostrar si se puede inferir la contradicción de cualquier otra variable lógica que esté contenida en el argumento.

2.7 Inducción matemática

La inducción matemática es un método de demostración que se aplica sobre los conjuntos de los números enteros positivos $\mathbb{Z}^+$ o el de los números naturales $\mathbb{N}$.

En el lenguaje coloquial o cotidiano, el término *inducción* hace referencia al hecho de que se deben obtener conclusiones o resultados mediante un examen que va de lo general a lo particular. En este tema se mostrará cómo dicha palabra tiene un significado distinto, pues aquí generalizamos una propiedad, regla o condición utilizando fórmulas, que llamaremos fórmulas inductivas.

Se dará inicio con un ejemplo intuitivo, el cual dará idea general acerca de qué es la inducción matemática y cómo aplicarla.

EJEMPLO

Intuitivo

A este ejemplo lo llamaremos: "efecto dominó". La figura 2.3 muestra, en la secuencia inicial, las primeras cinco fichas de un dominó compuesto por n fichas; como se puede ver, las fichas están dispuestas en forma vertical. En la segunda secuencia se empuja la primera ficha hacia la derecha, la cual origina un "efecto dominó"; esto se puede considerar la base de la inducción, ya que se da un empujón inicial que pone en movimiento todo el proceso.

Al caer la primera ficha golpea a la segunda, la cual también cae, como se observa en la tercera secuencia de la figura. Entonces, la intuición nos hace pensar que el proceso debe continuar; esto es, que al caer la segunda ficha golpea a la tercera, la cual cae y así sucesivamente hasta llegar a la n-ésima ficha y no quede ninguna ficha en forma vertical, como se ve en la cuarta secuencia de la figura.

Entonces, sabemos que las n fichas deben caer. Ahora bien, ¿cómo sabremos si la ficha n-ésima $+ 1$ caerá como en la última secuencia de la figura 2.3? Como todas las fichas anteriores a la ficha n-ésima caen, entonces sabemos que la ficha n-ésima $+ 1$ también caerá.

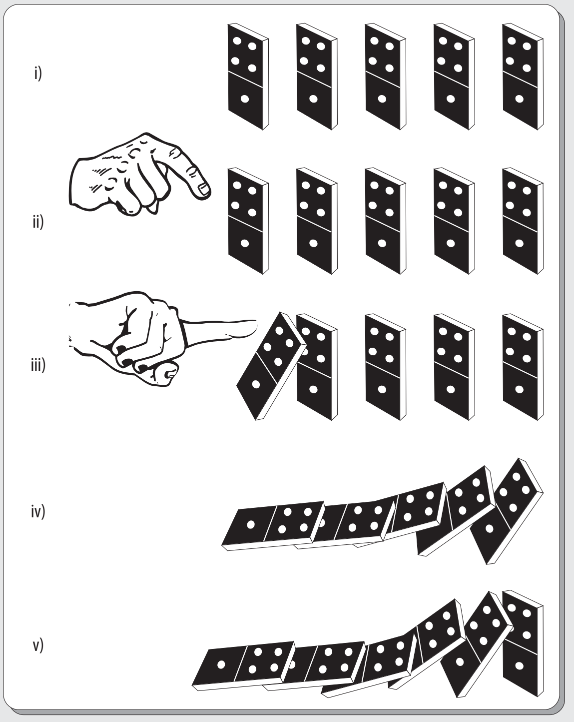


Figura 2.3 Efecto dominó.

Primer principio de inducción matemática

Consideremos una lista de proposiciones: $p(1), p(2), p(3), \ldots$, con índices en los enteros positivos $\mathbb{Z}^+$. Todas las proposiciones $p(n)$ son verdaderas a condición que:

(B) $p(1)$ sea verdadera.
(I) $p(n + 1)$ es verdadera siempre que $p(n)$ lo sea.

Nos referimos a (B), es decir al hecho de que $p(1)$ es verdadera, como la base de la inducción, y nos referimos a (I) como el paso inductivo. En la notación del cálculo proposicional, (I) equivale decir que:

$$\textbf{La implicación } p(n) \Rightarrow p(n+1) \textbf{ es verdadera } \forall n \in \mathbb{Z}^+$$

Antes de analizar algunos ejemplos de cómo aplicar el primer principio de inducción matemática, es conveniente dar a conocer el siguiente concepto.

Notación sigma

Hay una abreviatura conveniente que se utiliza con frecuencia en conexión con las sumas. Esta es la letra griega Σ (sigma), debido a que la primera letra de la palabra ***suma*** es la letra s, y en griego esta equivale precisamente a Σ (sigma).

En matemáticas se utiliza la Σ para indicar la operación conocida como sumatoria. En general:

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + a_3 + \cdots + a_n$$

El símbolo k debajo de la sigma indica dónde empezar la suma de los términos a_i (en este caso 1), pero además se conoce como límite inferior. La n de la parte superior indica dónde detenerse o terminar, y se conoce como límite superior. La variable k recorre los valores enteros desde el límite inferior hasta el límite superior.

Siempre debe cumplirse que:

límite inferior ≤ límite superior

EJEMPLO

A continuación se presentan algunos ejemplos de la notación sigma:

$$\sum_{k=1}^{4} a_k = a_1 + a_2 + a_3 + \cdots + a_4$$

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + \cdots + n^2$$

$$\sum_{k=1}^{n} 5k = 5 + 10 + 15 + \ldots 150$$

$$\sum_{k=1}^{4} \frac{1}{k(k+1)} = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \frac{1}{20}$$

$$\sum_{k=1}^{7} b_k = b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7$$

$$\sum_{k=1}^{8} 3k = 3 + 6 + 9 + 12 + 15 + 18 + 21 + 24$$

$$\sum_{k=1}^{5} 2^{k-1} = 1 + 2 + 4 + 8 + 16$$

$$\sum_{k=1}^{5} (3k-2) = 1 + 4 + 7 + 10 + 13$$

$$\sum_{k=1}^{6} \frac{1}{(2k-1)(2k+1)} = \frac{1}{3} + \frac{1}{3.5} + \frac{1}{5.7} + \frac{1}{7.9} + \frac{1}{9.11} + \frac{1}{11.13}$$

Ahora se verán con detalle algunos ejemplos de la aplicación del primer principio de inducción matemática.

Ejemplo

Demostrar por inducción que:

$$\sum_{k=1}^{n} (3k-2) = \frac{1}{2}\left(3n^2 - n\right) \forall n \in \mathbb{Z}^+$$

Solución

Se supone que $p(n)$ es verdadera, es decir que el resultado es verdadero para $n = k$, para algún $k \in \mathbb{Z}^+$. Esto se conoce como *hipótesis de la inducción*. La parte derecha de la igualdad se conoce como fórmula inductiva.

Demostración

Nótese que $p(1)=1=\frac{1}{2}[3(1)^2-1]$, de aquí que 1 = 1 es verdadera por inspección y esto establece la base de la inducción.

Ahora, supóngase que $p(n)$ es verdadera para alguna n, esto es:

$$p(n)=\sum_{k=1}^{n}(3k-2)=\frac{1}{2}\left(3n^2-n\right)$$

es verdadera.

Ahora se quiere probar que para $p(n+1)$ se tiene que:

$$p(n+1)=\sum_{k=1}^{n}(3k-2)+\frac{1}{2}[3(k+1)^2-(k+1)]$$

es verdadera, tal como lo establece el paso inductivo. Además en este paso n toma el valor de $k+1$.

Utilizando $p(n)$ tenemos que:

$$\sum_{k=1}^{n+1}(3k-2)=\sum_{k=1}^{n}(3k-2)+[3(k+1)-2]=\frac{1}{2}\left(3k^2-k\right)+(3k+1)$$

Para verificar $p(n+1)$ necesitamos comprobar que:

$$\frac{1}{2}\left(3k^2-k\right)+(3k+1)=\frac{1}{2}\ 3(k+1)^2-(k+1)$$

Esto ya es un problema puramente algebraico, para lo cual se trabajará con el lado izquierdo de la igualdad; esto es:

$$\begin{aligned}
\frac{1}{2}\left(3k^2-k\right)+(3k+1)&=\frac{1}{2}\left(3k^2-k+6k+2\right)\\
&=\frac{1}{2}\left(3k^2+5k+2\right)\\
&=\frac{1}{2}(3k+2)(k+1)\\
&=\frac{1}{2}[3(k+1)-1](k+1)\\
&=\frac{1}{2}[3(k+1)^2-(k+1)]
\end{aligned}$$

Entonces, $p(n+1)$ es verdadera siempre que $p(n)$ lo sea. Por el primer principio de inducción matemática, se concluye que es verdadera $\forall\, n \in \mathbb{Z}^+$.

No siempre es necesario el uso del símbolo de sumatoria para aplicar la inducción matemática, también puede utilizarse parte del desarrollo de la misma, como se muestra en los siguientes ejemplos.

Ejemplo

Demostrar por inducción que:

$$p(n)=1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

Demostración

La n-ésima proposición $p(n)$ es:

$$p(n)=1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

Nótese que $p(1)=1=\frac{1(1+1)}{2}$, donde $1 = 1$. Así $p(1)$ asegura que $1 = 1$; es verdadera por inspección, tal como lo establece la base de la inducción matemática.

Para el paso inductivo, supongamos que $p(n)$ es verdadera para algún n, esto es:

$$p(n)=1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

es verdadera.

Ahora, queremos probar que es verdadera para $p(n+1)$, y como en este paso $n = k + 1$:

$$p(n+1)=1+2+3+\cdots+k+(k+1)=\frac{(k+1)[(n+1)+1]}{2}$$

es decir:

$$p(n+1)=1+2+3+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}$$

es verdadera, tal como lo establece el paso inductivo.

Como $p(n)$ es verdadera por hipótesis, trabajando con el lado izquierdo de la igualdad tenemos que:

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

Entonces, $p(n+1)$ es verdadera siempre que $p(n)$ lo sea. Por el primer principio de inducción matemática, se concluye que $p(n)$ es verdadera $\forall\, n \in \mathbb{Z}^+$.

Johann Carl Friedrich Gauss, matemático y físico alemán, es considerado uno de los mejores matemáticos de todos los tiempos, al grado que en algunos ámbitos se le denomina el "Príncipe de las Matemáticas".

Cuando tenía 8 años y cursaba el equivalente a la educación primaria, su maestro le encomendó el "ejercicio" de determinar el resultado de sumar los números del 1 al 100; Gauss en menos de un minuto escribió en su pequeña pizarra la respuesta correcta: 5050.

¿Cómo obtuvo el resultado? Muy fácil, $1 + 100$ es igual que $2 + 99$, que $3 + 98$, y así sucesivamente; como hay 50 de estas sumas y cada una de estas operaciones suma 101, en total se tiene 101 por 50, cuyo resultado es 5050.

Entonces, la demostración anterior constituye una generalización de dicho "ejercicio".

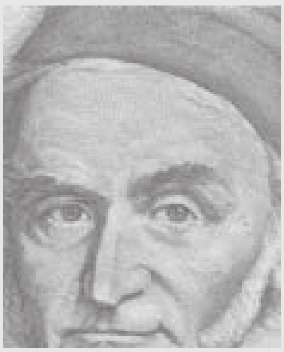


Figura 2.4 Johann Carl Friedrich Gauss (1772-1855).

Ejemplo

Demostrar por inducción que:

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

Demostración

La n-ésima proposición es:

$$p(n)=2+4+6+\cdots+2(n)=n(n+1)$$

Nótese que $p(1) = 2 = (1)(2)$, donde $2 = 2$. Así $p(1)$ asegura que $2 = 1(1 + 1)$ y como es verdadera por inspección, tal como lo establece la base de la inducción matemática.

Para el paso inductivo, supongamos que $p(n)$ es verdadera para algún n, esto es:

$$p(n)=2+4+6+\cdots+2(n)=n(n+1)$$

es verdadera.

Ahora, queremos probar que para $p(n + 1)$, y como en este paso $n = k + 1$:

$$p(n+1)=2+4+6+\cdots+\ 2(k)+2(k\ +\ 1)=(k\ +\ 1)[(k\ +\ 1)+1]$$

es decir:

$$p(n+1)=2+4+6+\cdots+2(k)+2(k+1)=(k+1)(k+2)$$

es verdadera, tal como lo establece el paso inductivo.

Como $p(n)$ es verdadera por hipótesis, y trabajando con el lado izquierdo de la igualdad, tenemos que:

$$\begin{aligned}2+4+6+\cdots+2(k)+2(k+1)&=[2+4+6+\cdots+2k]+2(2k+2)\\&=k(k+1)+(2k+2)\\&=k(k+1)+2(k+1)\\&=(k+1)(k+2)\end{aligned}$$

Entonces, $p(n + 1)$ es verdadera siempre que $p(n)$ lo sea. Por el primer principio de inducción matemática, se concluye que $p(n)$ es verdadera $\forall\, n \in \mathbb{Z}^+$.

Es importante hacer notar que no todas las demostraciones tienen que ver con sumas, también se puede aplicar la inducción para demostrar desigualdades, como se muestra en el siguiente ejemplo.

Ejemplo

Demostrar por inducción que:

$$2+5(n-1)\leq 5n \forall n\in\mathbb{Z}^+$$

Demostración

La n-ésima proposición $p(n)$ es: $2+5(n-1)\leq 5n$ y nótese que:

$$p(1)=2\leq 5$$

Entonces, como $p(1)$ es verdadera por inspección, esto es lo que establece la base de la inducción.

Ahora, supóngase que $p(n)$ es verdadera para algún n; esto es:

$$2+5(n-1)\leq 5n$$

es verdadera.

Ahora, queremos probar que para $p(n+1)$:

$$2+5\big((k+1)-1\big)\leq 5(k+1)$$

Esta debe ser verdadera como lo establece el paso inductivo.

Simplificando:

$$2+5k\leq 5k+5$$

Como $p(n)$ es verdadera por hipótesis, y trabajando con la desigualdad, tenemos que:

$$2+5k-5k\leq 5k-5k+5$$
$$2\leq 5$$

Entonces, $p(n+1)$ es verdadera siempre que $p(n)$ lo sea. Por el primer principio de inducción matemática se concluye que $p(n)$ es verdadera $\forall\, n\in\mathbb{Z}^+$.

En ocasiones, la base de la inducción cambia un poco en el sentido en que no necesariamente se debe cumplir $p(1)$, pero puede ser cierto para algunos valores de p mayores que cierto valor de n.

Ejemplo

Demostrar por inducción que:

$$2^n<n!\forall n\geq 4$$

Demostración

La n-ésima proposición $p(n)$ es $2^n<n!$ y nótese que $p(1)$, $p(2)$ y $p(3)$ no son verdaderas, y no necesitamos que sean verdaderas.

Ahora bien:

$$p(4)=2^4=16<4!=24$$

Así que $p(4)$ es válida, como lo establece nuestra base inductiva.

Ahora, supóngase que $p(n)$ es verdadera para algún n, esto es:

$$2^n<n!$$

es verdadera.

Ahora, queremos probar que para $p(n+1)$ se tiene que:

$$p(n+1)=2^{k+1}<(k+1)!$$

tal como lo establece el paso inductivo. Utilizando $p(n)$, se multiplican ambos lados de la desigualdad por 2, para obtener $n\geq 4$:

$$(2)\left(2^k\right)=2^{k+1}<2(k!)<(k+1)(k!)=(k+1)!$$

Entonces, $p(n+1)$ es verdadera siempre que $p(n)$ lo sea. Por el primer principio de inducción matemática se concluye que $p(n)$ es verdadera $\forall n\geq 4$.

Resumen

Cuando se desea establecer una verdad, o se quiere convencer a alguien de que una posición o idea son correctas, por lo general se recurre a un razonamiento o se presentan evidencias que lo respaldan.

Este razonamiento o evidencia presentada con el propósito de demostrar algo constituye un argumento. Entonces, un argumento es un conjunto de dos o más proposiciones simples, la última de las cuales se denomina conclusión, mientras que las anteriores se llaman premisas.

Las premisas son la evidencia o razones que deben convencer acerca de la veracidad de la conclusión. Así, el argumento es la concatenación de las primeras con la última.

La lógica estudia las formas del pensamiento desde el punto de vista de la estructura de los argumentos; esto es, analiza las relaciones entre las proposiciones y no el contenido de estas; en particular, se analiza la veracidad o falsedad de un razonamiento.

Existen diversos métodos para demostrar la validez de un argumento, si se tienen pocas proposiciones (dos o máximo tres), se utiliza el método por tablas de verdad. Pero, si se tienen más de tres proposiciones simples se debe hacer uso de otros métodos, como la prueba formal de validez, la prueba de invalidez, la prueba condicional o la prueba indirecta.

Problemas propuestos

2.1 ¿Cuáles de las siguientes oraciones son proposiciones? Justificar la respuesta.

a) El uranio es un elemento radiactivo.
b) ¡Camina rápido!
c) $4 + y = 2x$
d) ¿A qué hora llegaste?
e) Es tarde.
f) La casa de la esquina es azul.
g) México limita al norte con Canadá.
h) Haré lo que pueda.
i) El agua es un líquido incoloro.
j) La Luna gira alrededor de la Tierra.
k) El Sol es el centro del Universo.
l) El oro es muy lujoso y costoso.
m) El Everest no es la montaña más alta de la Tierra.

2.2 Traducir del lenguaje natural al simbólico las siguientes proposiciones:

a) Si llueve, entonces me mojo.
b) Los meteorólogos no se equivocan.
c) Si llueve o hace frío, entonces no es cierto que los meteorólogos no se equivocan.
d) No es cierto que llueva y me mojo.
e) Si llueve, entonces habrá buenas cosechas y abundantes frutas.
f) Llueve, nieva y graniza.
g) Si llueve y hace frío, entonces granizará.
h) Iré al cine si y solo si no llueve y no hace frío.
i) Iremos de vacaciones o a la playa o a la montaña.
j) No llueve o no me mojo.
k) Si Pedro va al cine y Luis al circo, entonces tomarán un taxi o el autobús.
l) Si la Luna gira alrededor de la Tierra hay mareas.
m) Si hay estrellas o el cielo está sereno, entonces no lloverá.

2.3 Si las proposiciones simples p y q son falsas y r y s son verdaderas, ¿cuál es el valor de verdad de las siguientes proposiciones compuestas?

a) $\sim(p \vee r)$
b) $\sim p \vee \sim r$
c) $\sim q \wedge s$
d) $p \vee q$
e) $\sim(\sim p \wedge \sim q)$
f) $\sim[(p \wedge q) \vee r]$
g) $\sim(\sim p \vee \sim q) \Rightarrow s$
h) $p \Rightarrow \sim p \vee \sim r$
i) $\sim[(p \wedge q) \Leftrightarrow (\sim r \vee s)]$
j) $\sim[\sim(\sim p) \wedge \sim(\sim q)]$

2.4 Sean las proposiciones simples:

f: Como frutas y verduras
s: Estoy sano

Traducir del lenguaje simbólico al natural las siguientes proposiciones:

a) $f \wedge s$
b) $\sim f$
c) $\sim(\sim f)$
d) $f \wedge \sim s$
e) $\sim(f \vee s)$
f) $(f \Rightarrow \sim s)$
g) $\sim(f \Leftrightarrow s)$
h) $f \Rightarrow \sim(f \wedge s)$
i) $\sim(f \Rightarrow s)$
j) $\sim(\sim f) \Rightarrow \sim(\sim s)$

2.5 Obtener la tabla de verdad de las siguientes proposiciones compuestas:

a) $\sim r \wedge \sim s$
b) $\sim(r \wedge s)$
c) $\sim r \vee \sim s$
d) $r \wedge (r \vee s)$
e) $(r \vee \sim r) \wedge \sim s$
f) $(r \wedge s) \wedge \sim s$
g) $\sim(r \vee s)$
h) $\sim(\sim r) \vee (s \wedge t)$
i) $(r \wedge \sim s) \Rightarrow (r \vee t)$
j) $r \wedge (s \Rightarrow \sim t)$

2.6 Traducir y verificar la validez de los siguientes argumentos por tablas de verdad.

a) Si el proveedor surte las semillas, entonces si las semillas se siembran a tiempo, entonces las plantas nacen en agosto. Las plantas nacen en agosto. Por tanto, si el proveedor surte las semillas, entonces las semillas se siembran a tiempo.

b) Si el proveedor surte las semillas, entonces si las semillas se siembran a tiempo, entonces las plantas nacen en agosto. Las semillas se siembran a tiempo. Por tanto, si el proveedor surte las semillas, entonces las semillas se siembran a tiempo. Luego, si las plantas no nacen en agosto, entonces el proveedor no surtió las semillas.

2.7 Verificar la validez de los siguientes argumentos por tablas de verdad.

a) 1. $(a \Rightarrow b) \wedge (b \Rightarrow c)$
2. $b \vee c$
$\therefore\ \sim a$

b) 1. $a \Rightarrow (b \vee c)$
2. $a \vee c$
$\therefore\ \sim b$

c) 1. $a \Rightarrow (b \Rightarrow c)$
2. $\sim b$
$\therefore\ a \vee c$

d) 1. $a \Rightarrow (\sim b \wedge c)$
2. $\sim c \vee a$
$\therefore\ b \wedge a$

e) 1. $a \Rightarrow (b \Leftrightarrow c)$
2. $c \Rightarrow \sim a$
3. $a \Rightarrow b$
$\therefore\ c \Rightarrow \sim b$

f) 1. $(a \Rightarrow b) \wedge (b \Rightarrow d)$
2. $a \Rightarrow \sim b$
$\therefore\ \sim d$

g) 1. $a \Rightarrow (a \Rightarrow b)$
2. $a \Rightarrow \sim a$
$\therefore\ \sim a \Rightarrow \sim b$

h) 1. $a \Rightarrow (b \wedge c)$
2. $a \vee (b \wedge c)$
$\therefore\ b \wedge c$

2.8 Verificar la validez de los siguientes argumentos por la prueba formal de validez.

a) 1. $a \Rightarrow b$
2. $b \Rightarrow d$
3. $\sim b \vee \sim d$
4. $\sim\sim a$
5. $(e \wedge f) \Rightarrow c$
$\therefore\ \sim(e \wedge f)$

b) 1. $e \vee m$
2. $m \Rightarrow s$
3. $s \Rightarrow t$
4. $\sim e$
$\therefore\ t$

c) 1. $(m \vee n) \Rightarrow (e \wedge f)$
2. $\sim e$
$\therefore\ \sim n$

d) 1. $y \Rightarrow w$
2. $y \vee (w \vee \sim v)$
3. $\sim w$
$\therefore\ \sim v \wedge \sim w$

e) 1. $(t \Rightarrow b)$
2. $(b \Rightarrow p)$
3. $(t \Rightarrow p) \Rightarrow (b \Rightarrow j)$
4. $(t \Rightarrow j) \Rightarrow k$
$\therefore\ k$

f) 1. $a \vee b$
2. $\sim a \wedge \sim c$
$\therefore\ b$

g) 1. $(w \wedge v) \wedge (c \vee t)$

2. $(w \Rightarrow s)$
$\therefore\ s$

h) 1. $(c \Rightarrow t) \wedge (d \Rightarrow v)$
2. $(t \Rightarrow p) \wedge (s \vee c)$
4. $(p \Rightarrow k) \wedge t$
$\therefore\ c \Rightarrow k$

i) 1. $a \wedge b$
2. $a \Rightarrow c$
3. $c \Rightarrow d$
$\therefore\ d$

j) 1. $a \Rightarrow \sim b$
2. a
$\therefore\ \sim b \vee c$

2.9 Verificar la invalidez de los siguientes argumentos por la prueba formal de invalidez.

a) 1. $a \Leftrightarrow b$
2. $c \Rightarrow d$
3. $b \Leftrightarrow c$
$\therefore\ a \wedge d$

b) 1. $a \Rightarrow (b \Rightarrow c)$
2. $b \Rightarrow (\sim c \Rightarrow d)$
3. $(c \vee d) \Rightarrow e)$
$\therefore\ a \Rightarrow e$

c) 1. $a \Leftrightarrow b$
2. $b \Leftrightarrow (c \wedge d)$
3. $c \Leftrightarrow (a \vee e)$
4. $a \vee e$
$\therefore\ a \wedge e$

d) 1. $a \Leftrightarrow (b \Rightarrow c)$
2. $b \Leftrightarrow (\sim a \wedge \sim c)$
3. $c \Leftrightarrow (a \vee \sim b)$
4. b
$\therefore\ a \vee c$

e) 1. $a \Rightarrow b$
2. $c \Rightarrow d$
3. $b \vee c$
$\therefore\ a \vee d$

f) 1. $h \Rightarrow (i \vee j)$
2. $j \Rightarrow (s \wedge x)$
3. $\sim s$
$\therefore\ h \Rightarrow x$

g) 1. $(p \vee j) \Rightarrow k$
2. $k \Rightarrow (j \vee d)$
3. $p \Rightarrow (\sim c \Rightarrow j)$
4. $(c \Rightarrow p) \Rightarrow \sim d$
$\therefore\ j \Leftrightarrow k$

2.10 Demostrar la validez de los siguientes argumentos por la prueba condicional.

a) 1. $a \Rightarrow (b \Rightarrow c)$
$\therefore\ b \Rightarrow (a \Rightarrow c)$

b) 1. $(a \Rightarrow b) \wedge (a \Rightarrow c)$
$\therefore\ a \Rightarrow (b \vee c)$

c) 1. $a \Rightarrow b$
2. $b \Rightarrow c$
3. $c \Rightarrow d$
$\therefore\ a \Rightarrow d$

d) 1. $(a \Rightarrow b) \wedge (a \Rightarrow c)$
$\therefore\ a \Rightarrow (b \wedge c)$

e) 1. $(a \Rightarrow b)$
$\therefore\ a \Rightarrow (a \wedge b)$

f) 1. $(m \Rightarrow n) \wedge (n \Rightarrow e)$
2. $(f \Rightarrow m) \wedge (e \Rightarrow f)$
$\therefore\ (\sim m \vee \sim e) \Rightarrow (\sim m \wedge \sim e)$

g) 1. $(m \wedge n) \Rightarrow (e \wedge f)$
2. $(h \Rightarrow m) \wedge (i \Rightarrow a)$
3. $(i \Rightarrow n) \wedge (f \Rightarrow a)$
4. $\sim e$
$\therefore\ h \Rightarrow \sim i$

h) 1. $b \Rightarrow p$
2. $j \Rightarrow k$
3. $\sim b \Rightarrow (\sim j \Rightarrow d)$
4. $\sim d$
$\therefore\ \sim p \Rightarrow k$

i) 1. $(j \Rightarrow k) \Rightarrow (\sim d \Rightarrow c)$
2. $\sim k \Rightarrow c$
3. $j \Rightarrow \sim c$
$\therefore\ \sim d \Rightarrow c$

j) 1. $y \Rightarrow w$
2. $(w \wedge v) \Rightarrow t$
$\therefore\ v \Rightarrow (y \Rightarrow t)$

2.11 Demostrar la validez de los siguientes argumentos por la prueba indirecta.

a) 1. $(a \Rightarrow b) \wedge (c \Rightarrow d)$

2. $(b \vee d) \Rightarrow e$
3. $\sim e$
$\therefore \sim(a \vee c)$

b) 1. $(a \vee b) \Rightarrow (c \wedge d)$
2. $(c \vee e) \Rightarrow (\sim f \wedge g)$
3. $(f \vee h) \Rightarrow (a \wedge b)$
$\therefore \sim e$

c) 1. $(a \Rightarrow \sim b) \wedge (c \Rightarrow d)$
2. $(\sim b \Rightarrow e) \wedge (d \Rightarrow \sim f)$
3. $(e \Rightarrow \sim g) \wedge (\sim f \Rightarrow h)$
4. $a \wedge c$
$\therefore \sim g \wedge h$

d) 1. $a \vee (b \wedge c)$
2. $a \Rightarrow c$
$\therefore c$

e) 1. $(a \vee b) \Rightarrow (c \Rightarrow d)$
2. $(\sim d \vee e) \Rightarrow (a \wedge c)$
$\therefore d$

f) 1. $(a \Rightarrow b) \wedge (c \Rightarrow d)$
$\therefore (a \vee c) \Rightarrow (b \vee d)$

g) 1. $(a \Rightarrow b) \wedge (c \Rightarrow d)$
$\therefore (\sim b \vee \sim d) \Rightarrow (\sim a \vee \sim c)$

h) 1. $(a \Rightarrow b)$
$\therefore (a \Rightarrow b) \Rightarrow (a \Rightarrow c)$

2.12 Demostrar por inducción que:

a) $\sum_{k=1}^{n} k\left(2^k\right) = 2 + (n-1)\ 2^{n+1}$

b) $\sum_{k=1}^{n} 2^{k-1} = 2^n - 1$

c) $\sum_{k=1}^{n} k^3 = \dfrac{n^2(n+1)^2}{4}$

d) $\sum_{k=1}^{n} \dfrac{1}{k(k+1)} = \dfrac{n}{n+1}$

e) $\sum_{k=1}^{n} 2\left(3^{k-1}\right) = 3^n - 1$

f) $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$

g) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{(n+1)(2n+1)}{6}$

h) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$

i) $\dfrac{1}{1\cdot 4} + \dfrac{1}{4\cdot 7} + \dfrac{1}{7\cdot 10} + \cdots + \dfrac{1}{(3n-2)(3n+1)} = \dfrac{n}{3n+1}$

j) $\dfrac{1}{1\cdot 3} + \dfrac{1}{3\cdot 5} + \dfrac{1}{5\cdot 7} + \cdots + \dfrac{1}{(2n-1)(2n+1)} = \dfrac{n}{2n+1}$

k) $\dfrac{1^2}{1\cdot 3} + \dfrac{2^2}{3\cdot 5} + \dfrac{3^2}{5\cdot 7} + \cdots + \dfrac{n^2}{(2n-1)(2n+1)} = \dfrac{n(n+1)}{2(2n+1)}$

Problemas reto

I. Verificar la validez del siguiente argumento por tablas de verdad.

1. $[(a \wedge b) \Rightarrow c] \wedge d$
2. $\sim(b \Rightarrow c)$

$\therefore \sim a$

II. Verificar la invalidez del siguiente argumento por la prueba de invalidez.

1. $p \Leftrightarrow (q \Leftrightarrow \sim r)$
2. $q \Rightarrow (\sim r \vee \sim s)$
3. $[r \Rightarrow (q \vee \sim t)] \wedge (p \Rightarrow q)$
4. $[u \Rightarrow (s \wedge t)] \wedge (t \Rightarrow w)$
5. $[(q \wedge r) \Rightarrow \sim u] \wedge [u \Rightarrow (q \vee r)]$
6. $(q \vee v) \Rightarrow \sim v$

$\therefore \sim u \vee \sim v$

3

Relaciones

Objetivos

- Aplicar los conceptos de relaciones binarias desde un punto de vista discreto.
- Determinar diversas relaciones binarias sobre los elementos de uno o dos conjuntos.
- Efectuar diversas operaciones entre relaciones binarias.
- Definir las propiedades que satisface determinada relación binaria.
- Identificar tipos especiales de relaciones binarias (relaciones de equivalencia y órdenes parciales).

3.1 Introducción

Las relaciones entre los elementos de dos o más conjuntos son frecuentes tanto en matemáticas como en sus aplicaciones, en especial en informática.

Algunos ejemplos prácticos de relaciones son las de orden y divisibilidad entre números, las relaciones de equivalencia entre los datos de entrada de un programa respecto a la detección de posibles errores de programación (validación de programas), la relación de dependencia entre las distintas fases de producción en una industria o la agrupación de datos aislados en complejas bases de datos con relaciones de dependencia entre sus campos.

Desde el punto de vista matemático, estas relaciones se pueden describir simplemente como subconjuntos de un cierto producto cartesiano.

De entre los diversos tipos de relaciones, las funciones pueden considerarse un caso especial en donde se interpreta que uno de los campos es el resultado de realizar determinada operación con el resto de estos.

Por su parte, las relaciones de equivalencia describen similitudes entre elementos con respecto a una propiedad particular. En tanto, las relaciones de orden establecen una jerarquía con respecto a un criterio fijado. Por último, las relaciones entre múltiples conjuntos son el fundamento matemático del modelo relacional de bases de datos, que es el más extendido hoy día por su simplicidad, potencia y coherencia teórica y práctica.

3.2 Definición y representación

En la forma intuitiva, una relación es una comparación entre dos elementos de un conjunto; esta se expresa usando pares ordenados. Por tanto, en la forma abstracta, una relación, **R**, se define como un conjunto de pares ordenados. En este contexto, se considera que el primer elemento del par ordenado está relacionado con el segundo elemento del par ordenado.

Existen varias definiciones de par ordenado, aunque la que se considera más común es la formulada en 1921 por Kazimierz Kuratowski, matemático y lógico polaco, la cual en la actualidad también es la más aceptada. La idea básica es muy sencilla: un par ordenado se distingue de una mera colección de dos elementos en que el primero está ordenado y el segundo no. Esto significa que para que un par sea ordenado basta que podamos distinguir su primer elemento del segundo. En otras palabras, basta poder reconocer que el par ordenado está relacionado de manera diferente con cada miembro.

Figura 3.1 Kazimierz Kuratowski (1896-1980).

Por lo general, la forma de relacionar ambos elementos es mediante una regla o característica que permita establecer una relación entre dichos elementos; por ejemplo, decir que el segundo elemento es el doble que el primer elemento, como el par ordenado (2, 4), o que el primer elemento es igual al triple del segundo elemento, como el par ordenado (6, 2).

Para iniciar, es necesario primero recordar el concepto de producto cartesiano, que se enuncia a continuación.

Producto cartesiano

Si A y B son dos conjuntos no vacíos, entonces el producto cartesiano $A \times B$ será el conjunto de todos los pares ordenados (a, b), donde $a \in A$ y $b \in B$. Es decir:

$$A \times B = \{(a, b)\ \mathrm{t} \cdot \mathrm{q} \cdot a \in A \wedge b \in B\}$$

Ejemplo

Sean los conjuntos $A = \{1, 2, 3\}$ y $B = \{r, s\}$

Entonces:

$$A \times B = \{(1, r), (1, s), (2, r), (2, s), (3, r), (3, s)\} \text{ y}$$
$$B \times A = \{(r, 1), (r, 2), (r, 3), (s, 1), (s, 2), (s, 3)\}$$

Como se puede observar en el ejemplo anterior, $A \times B \neq B \times A$; es decir, en este caso el producto cartesiano no es conmutativo.

En el contexto de las relaciones binarias, el producto cartesiano juega el papel de conjunto universal o de universo de discusión.

Relación binaria

Una relación binaria **R** de un conjunto A en un conjunto B es un subconjunto del producto cartesiano $A \times B$, es decir:

$$\mathbf{R} \subseteq (A \times B)$$

En este caso, $A \neq B$; por tanto, se dice que **R** es una relación del conjunto A en el conjunto B, o simplemente que **R** es una relación de A en B. Si el par ordenado $(a, b) \in \mathbf{R}$ se escribe $a\,\mathbf{R}\,b$ y significa que a está en relación con b.

Además, si el par ordenado $(a, b) \notin \mathbf{R}$ se escribe $a \not\mathbf{R}\, b$, para indicar que a no está relacionado con b.

Si $A = B$, es decir los dos conjuntos son iguales, o si simplemente se utiliza un único conjunto, se dice que **R** es una relación sobre el conjunto A, o simplemente que **R** es una relación sobre A. En este caso, se tiene que la relación **R** es un subconjunto de $A \times A$. Es decir:

$$\mathbf{R} \subseteq (A \times A)$$

Nota

Como siempre se trabajará con relaciones entre los elementos de dos conjuntos, se omitirá la palabra *binaria* en el resto del capítulo.

Como se mencionó antes, los elementos de los conjuntos se relacionan por una regla o característica. Hay tres formas diferentes para representar la regla que permita relacionar a dichos elementos.

Véase un ejemplo en el cual se trata de expresar las condiciones que forman la relación, primero de una forma verbal y luego de una manera formal.

Ejemplo

Si A es un conjunto cualquiera de números naturales y se quiere establecer una relación, **R**, sobre el conjunto A, en la cual se tenga que el primer elemento es menor o igual al segundo elemento del par ordenado; entonces, las diferentes formas de representar o expresar a **R** son las siguientes:

a) $\mathbf{R} = \{(a, b)\ \text{t} \cdot \text{q} \cdot a \leq b, a, b \in A\}$

b) $(a, b) \in \mathbf{R}$ si $a \leq b, a, b \in A$

c) $a\,\mathbf{R}\,b$ si $a \leq b, a, b \in A$

En el ejemplo, la primera es la forma más común para representar a las relaciones. Si no existe confusión con respecto a los elementos del conjunto, entonces se puede omitir que $a, b \in A$.

Cuando $A \neq B$ también se pueden utilizar las tres formas mencionadas, veamos a continuación cómo.

Ejemplo

Supóngase que A y B son dos conjuntos cualesquiera y que se quiere establecer una relación, **R**, del conjunto A en el conjunto B, en la cual el primer elemento es diferente al segundo elemento; entonces, dicha relación se puede expresar de las siguientes maneras:

a) $\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a \neq b, a \in A \wedge b \in B\}$

b) $(a, b) \in \mathbf{R}$ si $a \neq b, a \in A \wedge b \in B$

c) $a\,\mathbf{R}\,b$ si $a \neq b, a \in A \wedge b \in B$

De nueva cuenta, si no existe confusión con respecto a los elementos de los respectivos conjuntos se puede omitir que $a \in A \wedge b \in B$.

Ahora, se verá un ejemplo de cómo obtener los pares ordenados de una relación a partir de la regla que permite relacionar los elementos de los conjuntos.

Ejemplo

Sean el conjunto $A = \{1, 2, 3, 4\}$ y **R** una relación sobre el conjunto A definida como sigue:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a \mid b \text{ (división entera)}\}$$

¿Cuáles pares ordenados forman dicha relación?

Solución

Entonces, se tiene que el primer elemento debe dividir en forma entera al segundo elemento; es decir, con residuo igual a cero. Entonces:

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

En este caso, **R** es una relación sobre el conjunto A.

Como se observa en los ejemplos anteriores, existe una analogía entre la regla para formar una relación y la forma de definir un conjunto por comprensión; así, en la relación que se obtuvo hay una analogía con la forma de definir un conjunto por extensión, esto se debe precisamente a que las relaciones son conjuntos.

En una relación **R** de un conjunto A en un conjunto B, se identifican dos conjuntos especiales, denominados **dominio** y **codominio**.

Dominio

Si $\mathbf{R} \subseteq (A \times B)$ es una relación de A en B, el dominio de **R**, que se escribe Dom(**R**), es el conjunto de los elementos del conjunto A que están relacionados con elementos del conjunto B. El dominio se expresa de manera formal como sigue:

$$\text{Dom}(\mathbf{R}) = \{a \in A \text{ t} \cdot \text{q} \cdot (a, b) \in \mathbf{R}, \text{ para algún } b \in B\}$$

Ejemplo

Sean los conjuntos $A = \{1, 2, 3, 4, 5\}$ y $B = \{r, s, t\}$. Sea **R** una relación del conjunto A en el conjunto B definida como sigue:

$$\mathbf{R} = \{(1, r), (1, s), (2, s), (3, s)\}$$

Entonces:

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

Una manera intuitiva de determinar el dominio de **R** es escribir los primeros elementos de los pares ordenados de **R** sin repetirlos.

Codominio

Si $\mathbf{R} \subseteq (A \times B)$ es una relación de un conjunto A en un conjunto B, el codominio (también conocido como rango, imagen o recorrido) de **R**, se escribe Cod(**R**)y es el conjunto de los elementos de B que están relacionados con elementos del conjunto A. Es decir:

$$\text{Cod}(\mathbf{R}) = \{b \in B \text{ t} \cdot \text{q} \cdot (a, b) \in \mathbf{R}, \text{ para algún } a \in A\}$$

EJEMPLO

Sean los conjuntos $A = \{x, y, z, w\}$ y $B = \{a, b, c, d\}$ y **R** una relación del conjunto A en el conjunto B definida como sigue:

$$\mathbf{R} = \{(x, a), (x, b), (y, b), (z, a)\}$$

Entonces:

$$\text{Cod}(\mathbf{R}) = \{a, b\}$$

Nota

Con respecto a la relación **R** de los dos ejemplos anteriores, es importante hacer notar que no se ha dado la regla para formarla, aunque sí se han dado los elementos de la misma. En este caso, se debe trabajar con dicha relación tal cual y no preocuparse por la regla que la formó.

De nueva cuenta, una manera intuitiva para determinar el codominio de **R** consiste en escribir los segundos elementos de los pares ordenados de **R** sin repetirlos.

Las relaciones, además de ser representadas como conjuntos de pares ordenados, también se pueden representar de otras formas.

Una representación gráfica adecuada facilita la comprensión del producto cartesiano de dos conjuntos por ende, también de las relaciones, debido a eso se utilizan diversas maneras de representar las relaciones.

Entre las formas más comunes de representar a las relaciones, además de los pares ordenados, se pueden mencionar las siguientes:

1. **Tablas** Esta representación se utiliza con mucha frecuencia cuando se requiere expresar la relación de forma tabular. Pero, hay dos variantes de esta representación. En la primera, los elementos del primer conjunto corresponden a las filas o los renglones de la tabla y las columnas de la tabla a los elementos del segundo conjunto; en esta, los elementos relacionados se representan con una "palomita" (✓) o un signo de bien u "OK". En la segunda, las columnas corresponden a los conjuntos, y en esta se representan únicamente los elementos que están relacionados; esta forma es poco utilizada, ya que si **R** tiene muchos elementos, la tabla tiende a crecer de modo considerable.
2. **Diagramas** Es muy similar a los diagramas de Venn, donde los elementos relacionados se unen con flechas. En el caso de las relaciones es una representación muy poco utilizada.
3. **Matriz de relación** Es una representación matricial de una relación. En esta, los elementos del primer conjunto corresponden a las filas o los renglones de la matriz, mientras que las columnas pertenecen a los elementos del segundo conjunto. Si dos elementos están relacionados son representados con un 1 (en la intersección fila-columna correspondiente) y con un 0 en caso contrario.
4. **Dígrafos** Aunque más adelante se estudia con detalle qué es un dígrafo (grafo dirigido) y los elementos que lo constituyen, aquí se puede decir de manera intuitiva que es la representación gráfica de los elementos de un conjunto y las relaciones que existen entre estos. Por lo general, dicha representación se utiliza cuando **R** es una relación sobre A.
5. **Cartesiana** Es una representación que hace uso del plano en un sistema de ejes de coordenadas cartesianas. Por lo común, esta se utiliza cuando tanto los elementos del conjunto A como los del conjunto B pueden ser representados en un plano con un sistema de coordenadas cartesianas, aunque más habitualmente se utiliza cuando **R** es una relación sobre A.

EJEMPLO

Sean los conjuntos $A = \{1, 2, 3\}$ y $B = \{r, s\}$ y **R** una relación del conjunto A en el conjunto B definida como sigue:

$$\mathbf{R} = \{(1, r), (1, s), (2, r), (3, s)\}$$

Continúa

Además de la representación por pares ordenados, en la figura 3.2 se observan las representaciones por tablas, diagrama y matriz de relación para la relación **R** anterior.

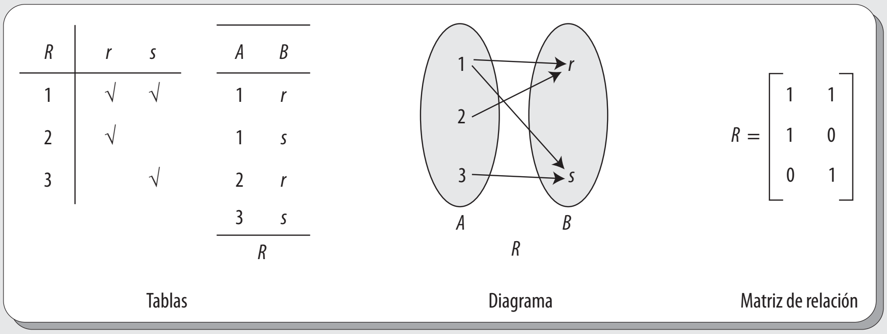


Figura 3.2 Tres representaciones para la relación **R** de **A** en **B**.

Como se mencionó antes, la representación mediante grafos dirigidos y de forma cartesiana, se utiliza por lo general cuando **R** es relación sobre *A*.

EJEMPLO

Sean el conjunto $A = \{1, 2, 3, 4\}$ y **R** una relación sobre el conjunto A definida como sigue:

$$\mathbf{R} = \{(a, b)\ \mathrm{t} \cdot \mathrm{q} \cdot a \leq b\}$$

De este modo:

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

Su representación como dígrafo y cartesiana se observan en la figura 3.3.

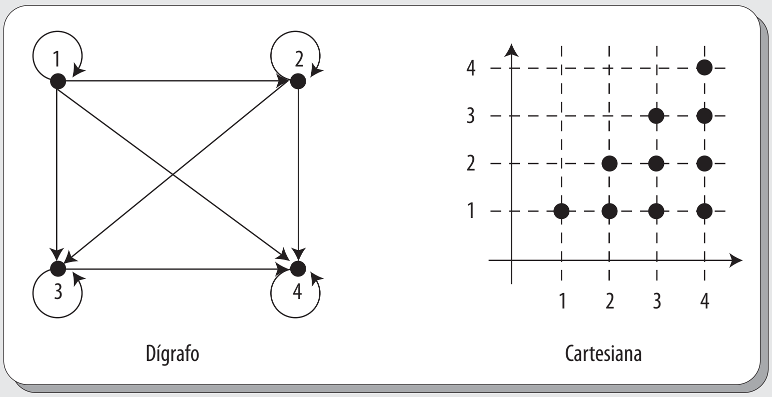


Figura 3.3 Representaciones como dígrafo y cartesiana para la relación **R** sobre **A**.

En la representación como dígrafo, los puntos reciben el nombre de vértices y representan los elementos del conjunto A.

Las flechas reciben el nombre de aristas dirigidas (o lados dirigidos) de a hacia b y representan el hecho de que $(a, b) \in \mathbf{R}$; es decir, los elementos que están relacionados.

Las flechas que representan elementos de la forma (a, a), es decir los elementos que están relacionados consigo mismos, se llaman lazos.

3.3 Operaciones con relaciones

Puesto que las relaciones son conjuntos de pares ordenados, las nociones de unión, intersección, diferencia y diferencia simétrica de dos relaciones se obtienen de manera similar a las correspondientes para los conjuntos.

A continuación se hace una recapitulación breve de dichas operaciones sobre conjuntos, extendiendo sus definiciones a las relaciones, y al final se aborda un ejemplo donde se utilizan operaciones con relaciones.

Antes que nada, no hay que olvidar que el conjunto universal, en las relaciones, es el producto cartesiano $A \times B$ o $A \times A$, dependiendo si es una relación de A en B o sobre A, respectivamente.

Unión de relaciones

La unión de dos relaciones **R** y **S**, denotada por $\mathbf{R} \cup \mathbf{S}$, es la relación cuyos pares ordenados son exactamente los pares ordenados de **R** o **S**, o en ambas relaciones. De manera formal se expresa como:

$$a(\mathbf{R} \cup \mathbf{S})b \equiv a \mathbf{R} b \vee a \mathbf{S} b$$

En forma gráfica se puede representar como se ve en la figura 3.4.

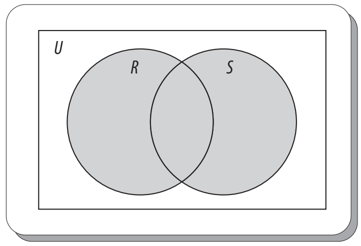


Figura 3.4 Unión de dos relaciones.

Intersección de relaciones

La intersección de dos relaciones **R** y **S**, denotada por $\mathbf{R} \cap \mathbf{S}$, es la relación cuyos pares ordenados son exactamente los pares ordenados que están tanto en **R** como en **S**. Desde el punto de vista formal, se expresa como:

$$a(\mathbf{R} \cap \mathbf{S})b \equiv a \mathbf{R} b \wedge a \mathbf{S} b$$

De manera gráfica se representa como se ve en la figura 3.5.

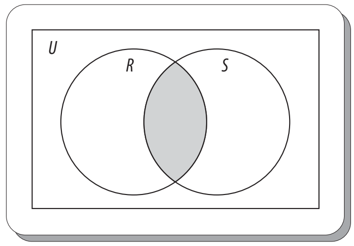


Figura 3.5 Intersección de dos relaciones.

Diferencia de relaciones

La diferencia de dos relaciones **R** y **S**, denotada por $\mathbf{R} - \mathbf{S}$, es la relación que contiene exactamente aquellos pares ordenados de **R** que no están en **S**. De manera formal, se expresa como:

$$a(\mathbf{R} \div \mathbf{S})b \equiv a \mathbf{R} b \wedge a \not{\mathbf{S}}\, b$$

En forma gráfica se representa como se ve en la figura 3.6.

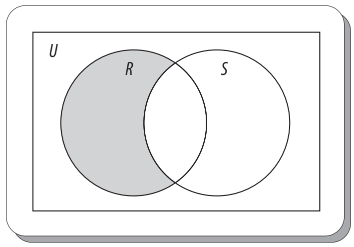


Figura 3.6 Diferencia de dos relaciones.

La diferencia simétrica

La diferencia simétrica de dos relaciones **R** y **S**, denotada por $\mathbf{R} \oplus \mathbf{S}$, es la relación que contiene todos los pares ordenados que están en **R** o en **S**, pero no en ambas relaciones. La diferencia simétrica equivale a la unión menos la intersección de ambas relaciones, es decir:

$$\mathbf{R} \oplus \mathbf{S} = (\mathbf{R} \cup \mathbf{S}) - (\mathbf{R} \cap \mathbf{S})$$

De manera formal, se expresa como:

$$a(\mathbf{R} \oplus \mathbf{S})b \equiv (a \mathbf{R} b \vee a \mathbf{S} b) - (a \mathbf{R} b \wedge a \mathbf{S} b)$$

De modo gráfico se representa como se ve en la figura 3.7.

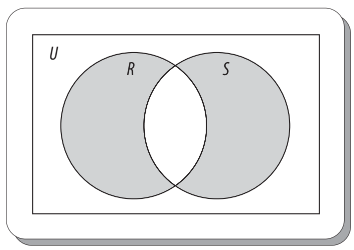


Figura 3.7 Diferencia simétrica de dos relaciones.

Además, se tiene que si **R** y **S** son dos relaciones del conjunto A en el conjunto B, entonces: $\mathbf{R} \cup \mathbf{S}$, $\mathbf{R} \cap \mathbf{S}$, $\mathbf{R} \oplus \mathbf{S}$ y $\mathbf{R} \oplus \mathbf{S}$ son también relaciones del conjunto A en el conjunto B.

Ejemplo

Sean los conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3\}$ y sean **R** y **S** dos relaciones del conjunto A en el conjunto B definidas como sigue:

$$\mathbf{R} = \{(a, 1), (a, 2), (b, 3)\} \text{ y}$$
$$\mathbf{S} = \{(a, 2), (b, 3)\}$$

Determinar $\mathbf{R} \cup \mathbf{S}$, $\mathbf{R} \cap \mathbf{S}$, $\mathbf{R} - \mathbf{S}$ y $\mathbf{R} \oplus \mathbf{S}$.

Solución

$\mathbf{R} \cup \mathbf{S} = \{(a, 1), (a, 2), (b, 3)\}$

$\mathbf{R} \cap \mathbf{S} = \{(a, 2), (b, 3)\}$

$\mathbf{R} - \mathbf{S} = \{(a, 1)\}$

$\mathbf{R} \oplus \mathbf{S} = \{(a, 1)\}$

Otra operación utilizada con frecuencia con conjuntos es el complemento. La cual, extendida a relaciones, se define como:

Complemento de una relación

Sean A y B dos conjuntos. El complemento de una relación **R** son todos los pares ordenados del producto cartesiano $A \times B$ (el cual juega el papel de conjunto universal) que no forman parte de la relación **R**; se denota como **R'** o $\mathbf{R}^C$. De manera formal, se expresa como:

$$a(\mathbf{R'})b \equiv a \not{\mathbf{R}}\, b$$

En forma gráfica, el complemento de una relación se puede representar como en la figura 3.8.

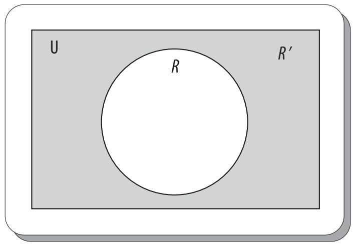


Figura 3.8 Complemento de una relación.

Ejemplo

Sean los conjuntos $A = \{a, b, c\}$ y $B = \{x, y, z\}$ y sean **R** y **S** dos relaciones del conjunto A en el conjunto B definidas como sigue:

$$\mathbf{R} = \{(a, x), (a, y), (b, z)\}$$
$$\mathbf{S} = \{(a, y), (b, z)\}.$$

Determinar **R'** y **S'**.

Solución

Si $A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\}$

Entonces:

$\mathbf{R}' = \{(a, z), (b, x), (b, y), (c, x), (c, y), (c, z)\}$ y

$\mathbf{S}' = \{(a, x), (a, z), (b, x), (b, y), (c, x), (c, y), (c, z)\}$

Una operación que se utiliza a menudo es el inverso de una relación, la cual no se aplica en conjuntos; en este caso, se define como:

Inverso de una relación

Sea **R** una relación de un conjunto A en un conjunto B, el inverso u opuesto de **R**, que se denota como $\mathbf{R}^{-1}$ o $\mathbf{R}^{\sim}$, es la relación del conjunto B en el conjunto A, expresada de manera formal como:

$$\mathbf{R}^{-1} = \{(b, a) \text{ t} \cdot \text{q} \cdot (a, b) \in \mathbf{R}\}$$

Ejemplo

Sean los conjuntos $A = \{2, 3, 4\}$ y $B = \{3, 4, 5, 6, 7\}$ y sea **R** una relación del conjunto A en el conjunto B, definida como sigue:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a \mid b\}$$

Determinar $\mathbf{R}^{-1}$.

Solución

Primero, es necesario determinar los elementos de **R**.

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

Entonces:

$\mathbf{R}^{-1} = \{(4, 2), (6, 2), (3, 3), (6, 3), (4, 4)\}$

De lo anterior se deduce que $a\,\mathbf{R}\,b \equiv b\,\mathbf{R}^{-1}\,a$.

En muchos casos, también resulta muy importante determinar la cantidad de elementos de una relación.

Cardinalidad de una relación

La cardinalidad de una relación **R** de un conjunto A en un conjunto B se representa como: $|\mathbf{R}|$, y constituye el número de pares ordenados distintos que forman la relación.

Ejemplo

Si $\mathbf{R} = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$

Entonces:

$|\mathbf{R}| = 5$

Una última operación sobre conjuntos, que también se aplica a las relaciones, es el conjunto potencia de una relación, la cual se define y explica a continuación.

Conjunto potencia de una relación

Sea **R** una relación de un conjunto A en conjunto B, el conjunto potencia de **R**, denotado como $P(\mathbf{R})$, es el conjunto que contiene a todos los subconjuntos de **R**; es decir:

$$P(\mathbf{R}) = \{\mathbf{S} \text{ t} \cdot \text{q} \cdot \mathbf{S} \subseteq \mathbf{R}\}$$

Además si $|\mathbf{R}| = n$, entonces $|P(\mathbf{R})| = 2^n$. Este valor indica la cantidad de elementos de $P(\mathbf{R})$.

Ejemplo

Sean el conjunto $A = \{1, 2, 3\}$ y **R** una relación sobre el conjunto A definida como:

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

Determinar $|P(\mathbf{R})|$.

Solución

Primero, $|\mathbf{R}| = 3$ y $|P(\mathbf{R})| = 2^3 = 8$.

Esto significa que el conjunto potencia de **R** tiene 8 subconjuntos:

$P(\mathbf{R}) = \{\varnothing, \{(1, 1)\}, \{(1, 2)\}, \{(1, 3)\}, \{(1, 1), (1, 2)\}, \{(1, 1), (1, 3)\}, \{(1, 2), (1, 3)\}, \{(1, 1), (1, 2), (1, 3)\}\}$

3.4 Composición de relaciones

La composición de relaciones también constituye una operación frecuente, la única diferencia radica en que en vez de requerir uno o dos conjuntos se requieren tres (que pudiera ser el mismo para los tres conjuntos), además de dos relaciones con las características dadas en la siguiente definición.

Definición de composición de relaciones

Sean **R** una relación de un conjunto A en un conjunto B y **S** una relación de un conjunto B en un conjunto C. La composición de **R** y **S**, denotada $\mathbf{S}\circ\mathbf{R}$, es una relación consistente de los pares ordenados (a, c), donde $a \in A$ y $c \in C$, para los cuales existe un $b \in B$, tal que $(a, b) \in \mathbf{R}$ y $(b, c) \in \mathbf{S}$; es decir, $a\ \mathbf{R}\ b$ y $b\ \mathbf{S}\ c$. De manera formal, se expresa como:

$$\mathbf{S}\circ\mathbf{R} = \{(a, c) \text{ t} \cdot \text{q} \cdot (a, b) \in \mathbf{R} \wedge (b, c) \in \mathbf{S}, a \in A, b \in B, c \in C\}$$

Ejemplo

Sean los conjuntos $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4\}$ y $C = \{0, 1, 2\}$ y sean las relaciones:

$\mathbf{R} = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$ de A en B y

$\mathbf{S} = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$ de B en C.

Determinar $\mathbf{S}\circ\mathbf{R}$.

Solución

$\mathbf{S}\circ\mathbf{R} = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$

Después de ver el ejemplo, nos cabe la pregunta: ¿$\mathbf{S}\circ\mathbf{R} = \mathbf{R}\circ\mathbf{S}$? Esto es: ¿la composición de relaciones es conmutativa? Antes de

Ejemplo

Sean los conjuntos $A = \{1, 2, 3\}$, $B = \{2, 4, 6, 8\}$ y $C = \{s, t, u\}$ y sean las relaciones:

$\mathbf{R} = \{(1, 2), (1, 6), (2, 4), (3, 4), (3, 6), (3, 8)\}$ de A en B

$\mathbf{S} = \{(2, u), (4, s), (4, t), (6, t), (8, u)\}$ de B en C.

Determinar $\mathbf{S} \circ \mathbf{R}$.

Solución

$\mathbf{S} \circ \mathbf{R} = \{(1, u), (1, t), (2, s), (2, t), (3, s), (3, t), (3, u)\}$

Con ambos ejemplos se puede afirmar que $\mathbf{S} \circ \mathbf{R} \neq \mathbf{R} \circ \mathbf{S}$; es decir, que la composición de relaciones no es conmutativa. Para reafirmar la respuesta, se verá otro ejemplo.

Ejemplo

Sean los conjuntos $A = \{a, b, c, d\}$, $B = \{s, t, u, v\}$ y $C = \{1, 2, 3, 4, 5\}$ y sean las relaciones:

$\mathbf{R} = \{(a, s), (a, t), (c, v), (d, u)\}$ de A en B y

$\mathbf{S} = \{(s, 2), (t, 1), (t, 4), (u, 3)\}$ de B en C

Determinar $\mathbf{S} \circ \mathbf{R}$.

Solución

$\mathbf{S} \circ \mathbf{R} = \{(a, 1), (a, 2), (a, 4), (d, 3)\}$

La composición de relaciones también puede representarse en forma gráfica. Esta representación ayuda a visualizar cómo se relacionan los pares ordenados de las relaciones.

En dicha representación gráfica, primero se escriben los conjuntos A, B y C, así como sus elementos debajo de cada uno de los conjuntos. Luego, se unen con flechas aquellos elementos que están relacionados en las relaciones **R** y **S**, respectivamente. Acto seguido, se escriben los conjuntos A y C, debajo los elementos de cada uno y se unen con flechas aquellos elementos que inician en el conjunto A y terminan en el conjunto C. Por último, dichos elementos se escriben como pares ordenados.

Ejemplo

Representar de manera gráfica la composición $\mathbf{S} \circ \mathbf{R}$ obtenida en el ejemplo anterior.

Solución

Como se recordará, en el ejemplo anterior se tienen los conjuntos:

$A = \{a, b, c, d\}$, $B = \{s, t, u, v\}$ y $C = \{1, 2, 3, 4, 5\}$.

Y las relaciones:

$\mathbf{R} = \{(a, s), (a, t), (c, v), (d, u)\}$ de A en B y

$\mathbf{S} = \{(s, 2), (t, 1), (t, 4), (u, 3)\}$ de B en C

Desde el punto de vista gráfico, la composición $\mathbf{S} \circ \mathbf{R}$ se representa como se observa en la figura 3.9.

Por tanto:

$\mathbf{S} \circ \mathbf{R} = \{(a, 1), (a, 2), (a, 4), (d, 3)\}$

Este es el mismo resultado obtenido en el ejemplo anterior.

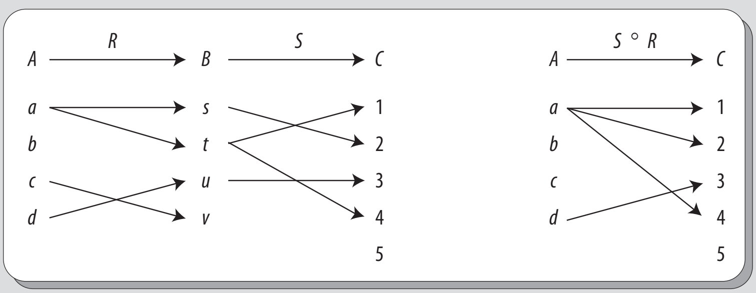


Figura 3.9 Representación gráfica de la composición de relaciones.

Pero el concepto de composición de relaciones también se puede extender a más de dos relaciones.

Composición de tres relaciones

Sean **R** una relación de un conjunto A en un conjunto B, **S** una relación de un conjunto B en un conjunto C y **T** una relación de un conjunto C en un conjunto D. La composición de **R**, **S** y **T** constituye una relación consistente de los pares ordenados (a, d), donde $a \in A$ y $d \in D$, y para los cuales existen un $b \in B$ y un $c \in C$, tal que $(a, b) \in \mathbf{R}$, $(b, c) \in \mathbf{S}$ y $(c, d) \in \mathbf{T}$. Es decir: $a\ \mathbf{R}\ b$, $b\ \mathbf{S}\ c$ y $c\ \mathbf{T}\ d$. La composición de tres relaciones se denota como $\mathbf{T} \circ \mathbf{S} \circ \mathbf{R}$, si **R**, **S** y **T** son relaciones.

Además, se tiene que $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) = (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$, lo que significa que la composición de más de dos relaciones es asociativa.

Ejemplo

Sean los conjuntos: $A = \{a, b, c, d\}$, $B = \{s, t, u, v\}$, $C = \{1, 2, 3, 4, 5\}$ y $D = \{*, \#, +\}$.

Sean las relaciones:

$\mathbf{R} = \{(a, s), (a, t), (c, v), (d, u)\}$ de A en B,

$\mathbf{S} = \{(s, 2), (t, 1), (t, 4), (u, 3)\}$ de B en C,

$\mathbf{T} = \{(2, *), (1, \#), (4, +), (5, \#)\}$ de C en D

Determinar $\mathbf{T} \circ \mathbf{S} \circ \mathbf{R}$ y comprobar que $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) = (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$.

Solución

El primer paso consiste en obtener $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R})$. Se inicia determinando:

$$\mathbf{S} \circ \mathbf{R} = \{(a, 1), (a, 2), (a, 4), (d, 3)\}$$

Después se determina:

$$\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) = \{(a, \#), (a, *), (a, +)\}$$

Ahora, se obtiene $(\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$. Para esto hay que determinar en primera instancia:

$$\mathbf{T} \circ \mathbf{S} = \{(s, *), (t, \#), (t, +)\}$$

y por último:

$$(\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R} = \{(a, \#), (a, *), (a, +)\}$$

Como se observa, este resultado es igual al resultado anterior.

Por otra parte, las potencias de una relación **R** se pueden definir utilizando la composición de funciones.

Potencias de relaciones

Sean A un conjunto y **R** una relación sobre el conjunto A. La composición de la relación **R** consigo misma se denota como sigue:

$$\begin{aligned}
\mathbf{R} &= \mathbf{R}^1 \\
\mathbf{R} \circ \mathbf{R} &= \mathbf{R}^2 \\
\mathbf{R} \circ \mathbf{R} \circ \mathbf{R} &= \mathbf{R} \circ \mathbf{R}^2 = \mathbf{R}^3 \\
\mathbf{R} \circ \mathbf{R} \circ \mathbf{R} \circ \mathbf{R} &= \mathbf{R} \circ \mathbf{R}^3 = \mathbf{R}^4 \\
&\vdots \\
\mathbf{R} \circ \mathbf{R}^{m-1} &= \mathbf{R}^m
\end{aligned}$$

Y se dice que son las potencias de la relación dada.

Ejemplo

Sean el conjunto $A = \{a, b, c, d\}$ y la relación **R** sobre el conjunto A definida como:

$$\mathbf{R} = \{(a, a), (b, a), (c, b), (d, c)\}$$

Encontrar las potencias $\mathbf{R}^m$.

Solución

Como $\mathbf{R} \circ \mathbf{R} = \mathbf{R}^2$, entonces:

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

Continúa

Además, como $\mathbf{R} \circ \mathbf{R}^2 = \mathbf{R}^3$, entonces:

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

Siguiendo con el proceso $\mathbf{R} \circ \mathbf{R}^3 = \mathbf{R}^4$, entonces:

$$\mathbf{R}^4 = \{(a, a), (b, a), (c, a), (d, a)\}$$

Pero, como $\mathbf{R}^4 = \mathbf{R}^3$, y si se siguiera el proceso siempre se obtendría $\mathbf{R}^3$, por lo que se deduce que:

$$\mathbf{R}^m = \mathbf{R}^3$$

3.5 Propiedades de las relaciones

A continuación se definirán y presentarán algunos ejemplos de las principales propiedades de las relaciones. Es importante destacar que dichas propiedades se utilizan, entre otras cosas, para clasificar las relaciones sobre un conjunto determinado.

Primero, se definen algunas relaciones que serán útiles a lo largo de esta sección.

Sean el conjunto $A = \{1, 2, 3, 4\}$ y las siguientes relaciones sobre A:

$$\begin{aligned}
\mathbf{R} &= \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}\\
\mathbf{S} &= \{(1, 1), (1, 2), (2, 1)\}\\
\mathbf{T} &= \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}\\
\mathbf{U} &= \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}\\
\mathbf{V} &= \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}\\
\mathbf{W} &= \{(3, 4)\}
\end{aligned}$$

Relación reflexiva

A la relación $\mathbf{R}$ sobre un conjunto A se le conoce con el nombre de **reflexiva**; esto es, si $(a, a) \in \mathbf{R}, \forall a \in A$. Se expresa de manera formal como sigue:

$$\mathbf{R} \text{ es reflexiva} \equiv \forall a \, (a \mathbf{R} a)$$

Lo anterior significa que para que una relación $\mathbf{R}$ sea reflexiva debe contener todos los elementos del conjunto A relacionados consigo mismos en $\mathbf{R}$.

Ejemplo	Solución
Determinar cuáles relaciones son reflexivas.	En este caso, $\mathbf{T}$ y $\mathbf{V}$ son reflexivas, ya que todos los pares ordenados de la forma $(a, a) \, \forall a \in A$ son elementos de $\mathbf{T}$ o de $\mathbf{V}$, respectivamente; es decir, (1, 1,), (2, 2), (3, 3), (4, 4) son elementos de $\mathbf{T}$ o de $\mathbf{V}$.

Relación irreflexiva

A la relación $\mathbf{R}$ sobre un conjunto A se le conoce como irreflexiva si$(a, a) \notin \mathbf{R}, \forall a \in A$; este tipo de relación se expresa de manera formal como sigue:

$$\mathbf{R} \text{ es irreflexiva} \equiv \forall a \, (a \not\mathbf{R} \, a)$$

Entonces, para que una relación sea irreflexiva no debe contener ninguno de los elementos del conjunto A relacionados consigo mismos en $\mathbf{R}$.

Ejemplo

Determinar cuáles relaciones son irreflexivas.

Solución

En este caso, **U** y **W** son irreflexivas, ya que ninguno de los pares ordenados de la forma $(a, a)\ \forall a \in A$ son elementos de **U** o de **W**; esto es: (1, 1,), (2, 2), (3, 3) y (4, 4) no son elementos de **U** o de **W**.

Por medio de tablas es fácil reconocer o determinar cuándo una relación es reflexiva o irreflexiva, basta con observar la diagonal principal de las mismas.

En el caso de que en la tabla todos los elementos de la diagonal estén marcados, se puede asumir que la relación es reflexiva (véase figura 3.10b); por el contrario, si ninguno de los elementos de la diagonal está marcado, entonces se asume que la relación es irreflexiva (véase figura 3.10c). Pero, si en la tabla solo algunos de los elementos de la diagonal están marcados, entonces se considera que la relación no es reflexiva ni irreflexiva (véase figura 3.10a).

R	1	2	3	4
1	√	√		
2	√	√		
3				√
4	√			√

a)

T	1	2	3	4
1	√	√		√
2	√	√		
3			√	
4	√			√

b)

U	1	2	3	4
1				
2	√			
3	√	√		
4	√	√	√	

c)

Figura 3.10 a) Relación que no es reflexiva ni irreflexiva. b) Relación reflexiva. c) Relación irreflexiva.

En las matrices de relación, si la diagonal principal tiene exclusivamente unos, representa una relación reflexiva; en caso contrario, si la diagonal tiene exclusivamente ceros representa una relación irreflexiva.

En los dígrafos, si todos los vértices tienen lazos, representa una relación reflexiva; por el contrario, si ningún vértice los tiene, entonces el dígrafo representa una relación irreflexiva.

Relación simétrica

Una relación **R** sobre un conjunto *A* es simétrica si $\forall(a, b) \in \mathbf{R}$, lo que implica que $(b, a) \in \mathbf{R}$. La relación simétrica se expresa de manera formal como:

$$\mathbf{R} \text{ es simétrica} \equiv \forall a \forall b\ (a\ \mathbf{R}\ b \Rightarrow b\ \mathbf{R}\ a)$$

Entonces, para que una relación **R** sea simétrica, todo par ordenado de **R** debe tener su inverso.

Ejemplo

Determinar cuáles relaciones son simétricas.

Solución

En este caso, **S** y **T** son simétricas, ya que todo par ordenado (b, a) es elemento de **S** o de **T** siempre que (a, b) sea elemento de **S** o de **T**, es decir, cada par ordenado de **S** o **T** tiene su inverso.

Relación antisimétrica

Una relación **R** sobre un conjunto *A* es antisimétrica si $(a, b) \in \mathbf{R}$ y $(b, a) \in \mathbf{R}$, entonces $a = b, \forall a, \forall b \in A$. De manera formal, una rel

$$\mathbf{R} \text{ es antisimétrica} \equiv \forall a \forall b\ (a\ \mathbf{R}\ b \wedge b\ \mathbf{R}\ a \Rightarrow a = b)$$

Una forma equivalente de expresar esta relación es diciendo: si $a \neq b$ se tiene que $a \not\mathbf{R}\ b$ o $b \not\mathbf{R}\ a$. Lo que de manera formal se denota:

$$\mathbf{R} \text{ es antisimétrica} \equiv \forall a \forall b\ (a \not\mathbf{R}\ b \vee b \not\mathbf{R}\ a)$$

Pero, si todavía queda duda, para que una relación **R** sea antisimétrica ningún par ordenado de esta debe tener su inverso; por tanto, hay que olvidarse de los pares ordenados de la forma (a, a).

Ejemplo

Determinar cuáles de las relaciones anteriores son antisimétricas.

Solución

Las relaciones antisimétricas son **U**, **V** y **W**, ya que en estas no hay pares de elementos (a, b) con $a \neq b$, tales que (a, b) sean elementos de **U**, **V** o de **W** y (b, a) sean elementos de **U**, **V** o de **W**; es decir, ningún par ordenado de **U**, **V** o de **W** tienen su inverso, sin considerar a los pares ordenados de la forma (a, a).

Gracias a las tablas es posible identificar con rapidez este tipo de relaciones. En este caso, aquí no deben importar los elementos de la diagonal, pues estos únicamente sirven como un *eje de simetría*, para verificar si cada par ordenado de la relación tiene su respectivo inverso.

En el caso de que la relación tenga la propiedad de simetría (véase figura 3.11b), todo par ordenado tiene su inverso, o si ningún par ordenado tiene su inverso, esto en el caso de que la relación tenga la propiedad de antisimetría (véase figura 3.11c).

No obstante, también puede darse el caso de que la relación no sea ni simétrica ni antisimétrica; en este caso, solo algunos elementos tendrán su inverso (véase figura 3.11a).

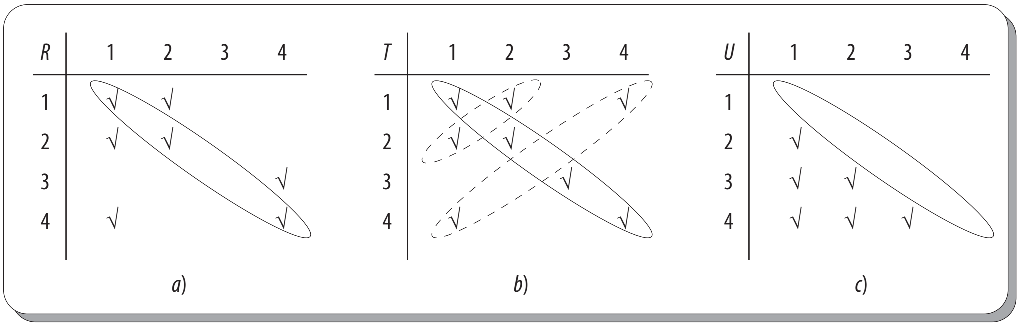


Figura 3.11 a) Relación ni simétrica ni antisimétrica. b) Relación simétrica. c) Relación antisimétrica.

En las matrices de relación, si los unos están dispuestos en forma simétrica con respecto a la diagonal principal, esto representa una relación simétrica. En caso contrario, si ninguno de los unos está dispuesto de forma simétrica con respecto a la diagonal principal, esto representa una relación antisimétrica.

En los dígrafos, si un vértice tiene una arista que sale a otro vértice, este último debe tener su correspondiente arista de regreso desde ese vértice; en este caso, esto representa una relación simétrica. Pero, si un vértice tiene una arista que sale a otro vértice y este último no tiene una arista de regreso, entonces esto representa una relación antisimétrica.

Es importante destacar que estas dos propiedades pueden presentarse en la misma relación; sin embargo, esto no ocurre con la reflexividad e irreflexividad. Si una relación **R** posee elementos exclusivamente en la diagonal principal, entonces **R** tiene las propiedades de simetría y antisimetría al mismo tiempo.

Relación transitiva

Una relación **R** sobre un conjunto A recibe el nombre de transitiva si $(\forall a, \forall b, \forall c) \in A$, donde $(a, b) \in \mathbf{R} \wedge (b, c) \in \mathbf{R}$; esto es, $(a, c) \in \mathbf{R}$. De manera formal esta se denota como:

$$\mathbf{R} \text{ es transitiva} \equiv \forall a \forall b\, \forall c\, (a\, \mathbf{R}\, b \wedge b\, \mathbf{R}\, c \Rightarrow a\, \mathbf{R}\, c)$$

Ejemplo

Determinar cuáles relaciones son transitivas.

Solución

En este caso, se puede comprobar que **U**, **V** y **W** son relaciones transitivas, ya que si (a, b) son elementos de **U**, **V** o de **W** y (b, c) son elementos de **U**, **V** o de **W**; entonces (a, c) **U**, **V** o de **W**, respectivamente.

La relación transitiva se representa en una tabla como se muestra en la figura 3.12.

Se sabe que la relación **U** es transitiva puesto que:

$$(3, 2) \in \mathbf{U} \text{ y } (2, 1) \in \mathbf{U} \Rightarrow (3, 1) \in \mathbf{U}$$

$$(4, 2) \in \mathbf{U} \text{ y } (2, 1) \in \mathbf{U} \Rightarrow (4, 1) \in \mathbf{U}$$

$$(4, 3) \in \mathbf{U} \text{ y } (3, 1) \in \mathbf{U} \Rightarrow (4, 1) \in \mathbf{U}$$

$$(4, 3) \in \mathbf{U} \text{ y } (3, 2) \in \mathbf{U} \Rightarrow (4, 2) \in \mathbf{U}$$

U	1	2	3	4
1				
2	√			
3	√	√		
4	√	√	√	

Figura 3.12 Tabla que representa una relación transitiva.

En una tabla no es fácil reconocer a simple vista si la relación es transitiva, por lo que es más conveniente utilizar la representación mediante un dígrafo.

Un dígrafo de una relación transitiva tiene la propiedad de que si existen aristas dirigidas de x a y y de y a z, también existe una arista dirigida de x a z, tal como se observa en el dígrafo de la figura 3.13.

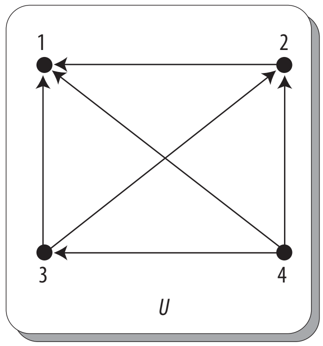


Figura 3.13 Relación transitiva representada por un dígrafo.

Para comprobar la condición de transitividad de una relación como pares ordenados, hay que tener en cuenta que si $a = b$ y si $(a, b) \in \mathbf{R} \wedge (b, c) \in \mathbf{R}$, entonces $(a, c) \in \mathbf{R}$; en este caso, $(a, c) = (b, c)$. Si $b = c$ y $(a, b) \in \mathbf{R} \wedge (b, c) \in \mathbf{R}$, entonces $(a, c) \in \mathbf{R}$; en este caso, $(a, c) = (a, b)$, por lo que no hay que verificar de manera explícita toda la condición en dichos casos.

Para comprobar la condición de transitividad, primero hay que eliminar los casos $a = b$ y $b = c$ y luego solo hay que verificar los pares ordenados restantes. Esto ahorrará una gran cantidad de comparaciones.

Extensión transitiva

Sea una relación **R** sobre un conjunto A, la extensión transitiva de **R**, denotada por $\mathbf{R}_1$, es la relación sobre A tal que $\mathbf{R} \subseteq \mathbf{R}_1$; es decir, $\mathbf{R}_1$ contiene a **R**, y además si $(a, b) \in \mathbf{R} \wedge (b, c) \in \mathbf{R}$, entonces $(a, c) \in \mathbf{R}_1$.

Ejemplo

Sean el conjunto $A = \{a, b, c, d\}$ y **R** una relación sobre el conjunto A definida como:

$$\mathrm{R} = \{(a, b), (b, c), (c, b), (c, d)\}$$

Determinar la extensión transitiva de **R**.

Solución

$$\mathrm{R}_1 = \{(a, b), (a, c), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d)\}$$

Cerradura transitiva

Si $\mathbf{R_2}$ denota la extensión transitiva de $\mathbf{R_1}$, y en general $\mathbf{R_{i+1}}$ denota la extensión transitiva de $\mathbf{R_i}$, la cerradura transitiva de $\mathbf{R}$, denotada por $\mathbf{R^*}$, es el conjunto unión de $\mathbf{R}$, $\mathbf{R_1}$, $\mathbf{R_2}$,…, $\mathbf{R_j}$.

De acuerdo con la definición anterior:

$$\mathbf{R^*} = \{\mathbf{R} \cup \mathbf{R_1} \cup \mathbf{R_2} \cup \ldots \cup \mathbf{R_{j-1}} \cup \mathbf{R_j}\}$$

Sin embargo, por definición de extensión transitiva se tiene que:

$$\mathbf{R} \subseteq \mathbf{R_1} \subseteq \mathbf{R_2} \subseteq \ldots \subseteq \mathbf{R_{j-1}} \subseteq \mathbf{R_j}$$

Entonces:

$$\mathbf{R^*} = \mathbf{R_j}$$

Hay que tener en cuenta que si $\mathbf{R}$ es una relación transitiva, entonces $\mathbf{R_1} = \mathbf{R}$; si $\mathbf{R_1}$ es una relación transitiva entonces $\mathbf{R_2} = \mathbf{R_1}$; si $\mathbf{R_2}$ es una relación transitiva entonces $\mathbf{R_3} = \mathbf{R_2}$ y en general si $\mathbf{R_{j-1}}$ es una relación transitiva, entonces $\mathbf{R}_j = \mathbf{R}_{j-1}$.

Así, se concluye que la cerradura transitiva $\mathbf{R^*}$ de una relación $\mathbf{R}$ siempre deberá ser una relación transitiva.

Ejemplo

Sean el conjunto $A=\{a, b, c, d\}$ y R una relación sobre el conjunto A definida como sigue:

$$R=\{(a, b), (b, c), (c, b), (c, d)\}$$

Determinar la cerradura transitiva de **R.**

Solución

$R_1 = \{(a, b), (a, c), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d)\}$

$R_2 = \{(a, b), (a, c), (a, d), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d)\}$

Y como $\mathbf{R_2}$ es una relación transitiva, entonces:

$R^* = R_2 = \{(a, b), (a, c), (a, d), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d)\}$

En la figura 3.14 se representa el proceso para obtener $\mathbf{R^*}$ mediante dígrafos.

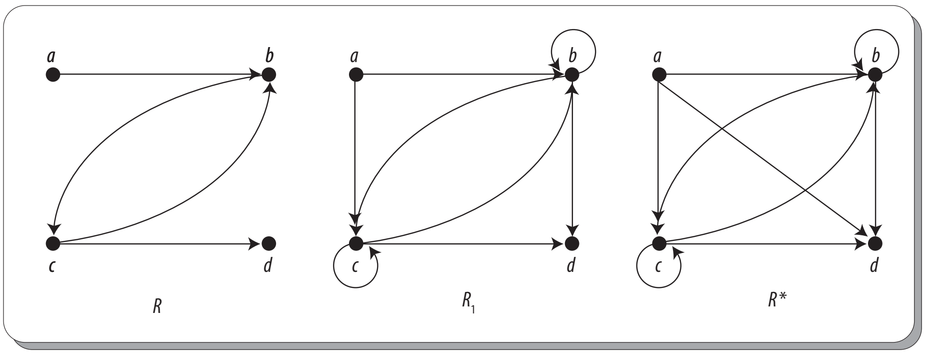


Figura 3.14 Proceso para obtener R*.

3.6 Relaciones de equivalencia

Para definir una relación de equivalencia, primero se debe establecer el concepto de partición de un conjunto, debido a que una partición puede generar dicha relación.

Partición de un conjunto

Una partición **S** de un conjunto A es una colección de subconjuntos disjuntos no vacíos de A que tienen a A como su unión; en otras palabras, la colección de subconjuntos A_i, $i \in I$ (donde I es un conjunto de índices), forma una partición **S** del conjunto **A** si y solo si:

$$A_i \neq \varnothing, i \in I, A_i \cap A_j = \varnothing \text{ cuando } i \neq j \text{ y además}$$

$$\bigcup_{i \in I} A_i$$

Entonces, $\mathbf{S} = \{A_1, A_2, \ldots, A_k\}$ es una partición de A; por tanto:

$$A = A_1 \cup A_2 \cup \ldots \cup A_k$$

Los subconjuntos A_i reciben el nombre de bloques de la partición.

Ejemplo

Sea el conjunto $A = \{x \text{ t} \cdot \text{q} \cdot x \text{ son letras del alfabeto}\}$ y sean los siguientes subconjuntos de A:

$A_1 = \{a, e, i, o, u\}$,

$A_2 = \{w, c\}$,

$A_3 = \{b, f, g, h, j, k, l\}$,

$A_4 = \{m, n, ñ, p, q\}$,

$A_5 = \{r, s, t, v\}$,

$A_6 = \{x, y\}$ y

$A_7 = \{d, z\}$

Entonces:

$$\mathbf{S} = \{\{a, e, i, o, u\}, \{w, c\}, \{b, f, g, h, j, k, l\}, \{m, n, ñ, p, q\}, \{r, s, t, v\}, \{x, y\}, \{d, z\}\}$$

O también

$$\mathbf{S} = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7\}$$

Es una partición de A, ya que todos los subconjuntos Ai son no vacíos. Además, cualesquiera dos subconjuntos distintos son disjuntos. Por último, la unión de todos los subconjuntos da como resultado el conjunto A.

Por tanto:

$$A = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 \cup A_6 \cup A_7$$

Los elementos del mismo bloque de una partición también se pueden representar con una barra sobre sí mismos, aunque esta representación es poco utilizada, ya que si el conjunto es numérico puede existir confusión con los elementos del bloque.

Ejemplo

Sean el conjunto $A = \{a, b, c, d, e, f, g, h\}$ y $\mathbf{S} = \{\{a, b\}, \{c, d, e\}, \{f\}, \{g, h\}\}$ una partición de A.

En este caso, la partición $\mathbf{S}$ también se puede representar como:

$$\mathbf{S} = \left\{\overline{ab}, \overline{cde}, \overline{f}, \overline{gh}\right\}$$

Ahora, resulta conveniente ejemplificar esta representación de los bloques de una partición mediante el uso de valores numéricos.

Ejemplo

Sean el conjunto $A = \{2, 4, 6, 8, 10, 12\}$ y $\mathbf{S} = \{\{2, 4\}, \{6, 8, 10\}, \{12\}\}$ una partición de A.

En este caso, si los elementos de los bloques de la partición $\mathbf{S}$ se representan con una barra sobre estos, dicha representación quedaría:

$$\mathbf{S} = \left\{\overline{24}, \overline{6810}, \overline{12}\right\}$$

Como se puede ver, hay una confusión entre los elementos de cada bloque.

En muchas ocasiones, una partición es útil para definir una relación **R**. Por tanto, el siguiente teorema es importante para definir relaciones generadas por una partición.

Teorema 3.1
Sea **S** una partición sobre un conjunto A. Se dice que a **R** b si para algún A_i en **S**,$a \in A_i \wedge b \in A_i$. Entonces, **R** es reflexiva, simétrica y transitiva.

Demostración
Sean A un conjunto y $a \in A$. Además, sea **S** una partición de A. Por definición de partición, todo $a \in A$ debe pertenecer a algún bloque A_i de **S**. Entonces, al obtener la relación **R** siempre va a ocurrir que $(a, a) \in$ **R** $\forall a \in A$.

Ahora, supóngase que $(a, b) \in$ **R**, entonces tanto $a \in A_i$ como $b \in A_i$; esto es, pertenecen al mismo bloque A_i de **S**. Y como pertenecen al mismo bloque, entonces: $(a, b) \in$ **R** y $(b, a) \in$ **R**, lo que significa que **R** es simétrica.

Por último, supóngase que $(a, b) \in$ **R** y $(b, c) \in$ **R**, entonces tanto $a \in A_i$ como $b \in A_i$; esto es, pertenecen al mismo bloque A_i de **S**. Además, se tiene $b \in A_j$ como $c \in A_j$, lo que indica que también pertenecen al mismo bloque A_j de **S**, pero como b debe pertenecer exactamente al único bloque de **S**, entonces se tiene que $A_j = A_j$. Por tanto, a como c deben ser parte de A_i y $(a, c) \in$ **R**. Con esto se demuestra que **R** es transitiva.

Para aplicar el teorema 3.1 sobre una partición se efectúa el producto cartesiano de cada uno de los bloques de la partición.

Ejemplo

Sean $A = \{a, b, c, d, e, f\}$ y $S = \{\{a, c, e\}, \{b, f\}, \{d\}\}$ una partición de A. La relación R definida por el teorema 3.1 es:

$$R = \{(a, a), (a, c), (a, e), (c, a), (c, c), (c, e), (e, a), (e, c), (e, e), (b, b), (b, f), (f, b), (f, f), (d, d)\}$$

Solución

En este caso:

R es reflexiva, puesto que (a, a), (b, b), (c, c), (d, d), (e, e) y (f, f) son elementos de R.

R es simétrica, ya que siempre que $(a, b) \in$ R también $(b, a) \in$ R; es decir, todo par ordenado tiene su inverso.

R es transitiva, puesto que siempre que (a, b) y $(b, c) \in$ R también $(a, c) \in$ R.

Al representar la relación **R** obtenida por el teorema 3.1 a través de dígrafos, como en la figura 3.15, es posible observar con claridad que los elementos de cada bloque son independientes por completo con respecto a los elementos de otro bloque.

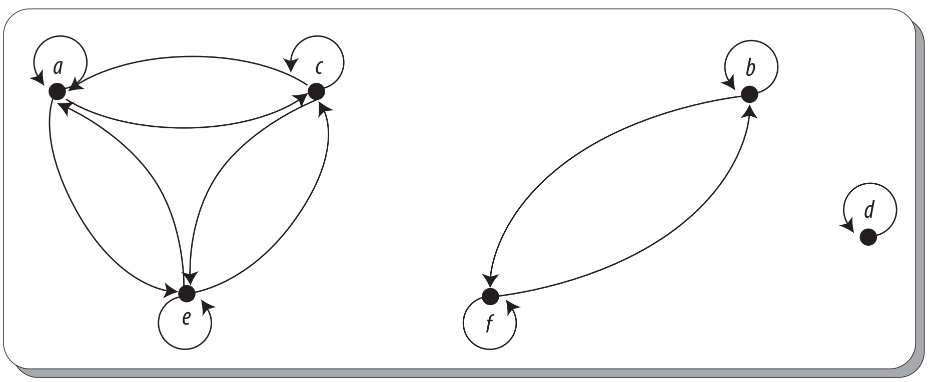


Figura 3.15 Dígrafo de una partición.

Relación de equivalencia

Se dice que una relación **R** que es reflexiva, simétrica y transitiva, sobre un conjunto A, es una relación de equivalencia sobre un conjunto A o simplemente que es una relación de equivalencia sobre A.

Ejemplo

Sea la relación **R** obtenida en el ejemplo anterior.

Solución

Como **R** es reflexiva, simétrica y transitiva, entonces **R** es una relación de equivalencia sobre A.

Ejemplo

Sean $A = \{1, 2, 3, 4\}$ y **R** una relación sobre el conjunto A.

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

Determinar si **R** es una relación de equivalencia sobre el conjunto A.

Solución

R es reflexiva, ya que (1, 1), (2, 2), (3, 3) y (4, 4) son elementos de **R**.

R es antisimétrica, ya que (2, 1), (3, 1), (4, 1), (3, 2), (4, 3) y (4, 2) no son elementos de **R**.

R es transitiva, puesto que siempre que si (a, b) y $(b, c) \in \mathbf{R}$ también $(a, c) \in \mathbf{R}$.

Dado que **R** no es simétrica, se tiene que no es una relación de equivalencia sobre el conjunto A.

Dada una relación de equivalencia sobre un conjunto A, es posible hacer una partición **S** de dicho conjunto, ya que puede suponerse que los elementos relacionados son parte del mismo bloque.

La siguiente definición muestra cómo obtener dicha partición.

Clases de equivalencia

Sea **R** una relación de equivalencia sobre un conjunto A. El conjunto de todos los $x \in A$ que están relacionados a un $a \in A$ se conoce con el nombre de clase de equivalencia de a y se denota por $[a]$. De manera formal se expresa como:

$$[a] = \{x \in A \text{ t} \cdot \text{q} \cdot x \, \mathbf{R} \, a\}$$

Además, se tiene el conjunto:

$$\mathbf{S} = \{[a] \text{ t} \cdot \text{q} \cdot a \in A\}$$

que es una partición de A; en otras palabras, el conjunto de todas las clases de equivalencia de A forman una partición del conjunto A.

Ejemplo

Sean el conjunto $A = \{a, b, c, d, e, f\}$ y **R** una relación de equivalencia sobre A definida como:

$$\mathbf{R} = \{(a, a), (a, c), (a, e), (c, a), (c, c), (c, e), (e, a), (e, c), (e, e), (b, b), (b, f), (f, b), (f, f), (d, d)\}$$

Obtener las clases de equivalencia de A.

Solución

Se tiene que:

$[a] = \{a, c, e\}$, $[c] = \{a, c, e\}$, $[e] = \{a, c, e\}$ y

$[b] = \{b, f\}$, $[d] = \{d\}$, $[f] = \{b , f\}$

Continúa

Donde:

$[a] = [c] = [e] = \{a, c, e\}$,

$[b] = [f] = \{b, f\}$ y

$[d] = \{d\}$

Esto significa que solo se tienen tres clases de equivalencia de A.

Además, se tiene que:

$$\mathbf{S} = \{\{a, c, e\}, \{b, f\}, \{d\}\}$$

es una partición de A.

Enseguida se ve un ejemplo con un conjunto numérico.

Ejemplo

Sean el conjunto $A = \{1, 2, 3, 4\}$ y $\mathbf{R}$ una relación de equivalencia sobre A definida como:

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

Obtener las clases de equivalencia de A.

Solución

Se tiene que:

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

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

$[3] = \{3, 4\}$ y

$[4] = \{3, 4\}$

por lo cual

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

$[3] = [4] = \{3, 4\}$

Además, se tiene que:

$$\mathbf{S} = \{\{1, 2\}, \{3, 4\}\}$$

es una partición de A.

De los ejemplos anteriores, es posible distinguir las siguientes propiedades de las clases de equivalencia:

Si $a \mathbf{R} b$, entonces $[a] = [b]$.
Si $[a] = [b]$, entonces $[a] \cap [b] \neq \varnothing$.
Si $[a] \cap [b] \neq \varnothing$, entonces $a \mathbf{R} b$.

En resumen, dos clases de equivalencia de dos elementos de A son idénticas o disjuntas.

3.7 Órdenes parciales

En muchas ocasiones, las relaciones resultan útiles cuando se quieren ordenar los elementos de algún conjunto bajo cierto criterio. Un orden parcial implica un orden determinado, tal como se ve a continuación.

Relación de orden parcial

Se dice que una relación $\mathbf{R}$ sobre un conjunto A es una relación de orden parcial si es reflexiva, antisimétrica y transitiva sobre dicho conjunto.

Si $\mathbf{R}$ es una relación de orden parcial (o simplemente orden parcial) sobre un conjunto A, se utiliza la notación $a \leq b$ para indicar que $(a, b) \in \mathbf{R}$. Esta notación sugiere que se está interpretando la relación como orden sobre los elementos.

EJEMPLO

Sean el conjunto $A = \{1, 2, 3, 4, 5\}$ y **R** una relación sobre el conjunto A definida como:

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

Representada en una tabla en la figura 3.16.

Como **R** es reflexiva, antisimétrica y transitiva, se trata de una relación de orden parcial sobre el conjunto A.

R	1	2	3	4	5
1	√	√	√	√	√
2		√	√		√
3			√		√
4				√	√
5					√

Figura 3.16 Relación de orden parcial.

Conjunto parcialmente ordenado

Un conjunto A junto con un orden parcial **R** sobre A se conoce con el nombre de conjunto parcialmente ordenado y se denota por (A, **R**). Un conjunto parcialmente ordenado también se conoce como POSET (del inglés: *Partially Ordered SET*).

En realidad, un conjunto parcialmente ordenado se denota como $(A, \preccurlyeq)$.

Ejemplo

Sean A el conjunto de $\mathbb{Z}^+$ y **R** una relación sobre A, t · q · $(a, b) \in \mathbf{R}$ si $a|b$.

Determinar si (A, **R**) es un conjunto parcialmente ordenado.

Solución

Como cualquier entero se divide a sí mismo, es decir, $a|a$, entonces **R** es reflexiva.

Si $a|b$ significa que $b|a$, a menos que sea $a = b$, por lo que **R** es antisimétrica.

Por último, ya que si $a|b$ y $b|c$, entonces $a|c$, por lo que **R** es transitiva.

En consecuencia, **R** es un orden parcial sobre $\mathbb{Z}^+$ y (A,**R**) es un conjunto parcialmente ordenado, por lo que se debe denotar como $(A, \preccurlyeq)$.

Comparabilidad e incomparabilidad

Sea **R** un orden parcial sobre el conjunto A. Si $a \in A$ y $b \in A$ y si $a \npreceq b \vee a \npreceq$ b, se dice que a y b son comparables.

Y si $a \in A$ y $b \in A$ y $a \npreceq b \wedge a \npreceq b$ se dice que a y b son incomparables.

EJEMPLO

Sean el conjunto $A = \{1, 2, 3, 4, 5\}$ y **R** el orden parcial sobre el conjunto A definida como:

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

Determinar cuáles elementos del conjunto A son comparables o incomparables.

Solución

Como $1 \npreceq 1, 1 \npreceq 2, 1 \npreceq 3, 1 \npreceq 4$ y $1 \npreceq 5$, entonces 1 es comparable con 1, 2, 3, 4 y 5.

Como $2 \npreceq 2, 2 \npreceq 3$ y $2 \npreceq 5$, entonces 2 es comparable con 2, 3 y 5.

Como $3 \npreceq 3$ y $3 \npreceq 5$, entonces 3 es comparable con 3 y 5.

Continúa

Como $4 \preccurlyeq 4$ y $4 \preccurlyeq 5$, entonces 4 es comparable con 4 y 5.

Como $5 \preccurlyeq 5$, entonces 5 es comparable con 5.

Como $2 \not\preccurlyeq 4$ ni $4 \not\preccurlyeq 2$, entonces 2 y 4 son incomparables.

Como $3 \not\preccurlyeq 4$ ni $4 \not\preccurlyeq 3$, entonces 3 y 4 son incomparables.

También se puede establecer la relación de un conjunto A junto con su orden parcial **R** si todos los elementos de A son comparables, de acuerdo con la siguiente definición.

Conjunto totalmente ordenado

Sea **R** un orden parcial sobre un conjunto A. Si cualquier par de elementos de A son siempre comparables, se dice que **R** es un orden total. Es decir, un orden parcial **R** sobre un conjunto A es un orden total si y solo si $\forall a, \forall b, a \preccurlyeq b \vee b \preccurlyeq a$ es siempre verdadero. En este caso, se dice que $(A, \preccurlyeq)$ es un conjunto totalmente ordenado.

Ejemplo

Sean A el conjunto de los números naturales $\mathbb{N}$ y **R** una relación sobre A, t · q · $(a, b) \in$ **R** si $a \geq b$.

Determinar si $(A, \preccurlyeq)$ es un conjunto totalmente ordenado.

Solución

Como cualquier natural o entero es mayor o igual a sí mismo, es decir, $a \leq a$, entonces **R** es reflexiva.

Si $a \leq b$ significa que ba, a menos que sea $a = b$, por lo que **R** es antisimétrica.

Por último, ya que si $a \geq b$ y $b \geq c$, entonces $a \geq c$, por lo que **R** es transitiva.

En consecuencia, **R** es un orden parcial sobre $\mathbb{N}$ y $(A, \mathbf{R})$ es un conjunto parcialmente ordenado.

Ahora, si tomamos cualesquiera dos elementos de $\mathbb{N}$, se puede comprobar que $a \preccurlyeq b \vee b \preccurlyeq a$; es decir, son comparables, ya que por la propiedad de la tricotomía, al comparar dos números se tiene que:

$$a > b, a = b \text{ o } a < b$$

Por tanto, en este caso **R** es un orden total y $(A, \mathbf{R})$ es un conjunto totalmente ordenado.

Cadena

Sean A un conjunto y $(A, \preccurlyeq)$ un conjunto parcialmente ordenado, y sea A_i un subconjunto de A. Se dice que A_i es una *cadena* si cualesquiera dos elementos de A_i son comparables; es decir, si están relacionados.

De acuerdo con la definición anterior, también se cumple que un conjunto totalmente ordenado $(A, \mathbf{R})$ sea una cadena, ya que es un orden parcial donde cada par de elementos es comparable. Debido a esto, también se le suele llamar *cadena* a un conjunto totalmente ordenado $(A, \mathbf{R})$.

De igual modo, también es posible establecer la relación de un conjunto A junto con su orden parcial **R** si todos los elementos de A son incomparables, de acuerdo con la siguiente definición.

Anticadena

Sean A un conjunto y $(A, \preccurlyeq)$ un conjunto parcialmente ordenado, y sea A_i un subconjunto de A. Se dice que A_i es una *anticadena* si cualesquiera dos elementos de A_i son incomparables; es decir, no están relacionados. En otras palabras, en A_i no hay dos elementos distintos que estén relacionados.

Lo mismo ocurre si todos los elementos del conjunto A son incomparables, por lo que también se dice que $(A, \npreceq)$ es una anticadena.

El siguiente ejemplo involucra tanto cadenas como anticadenas.

Ejemplo

Sean el conjunto $A = \{1, 2, 3, 4, 5\}$ y **R** un orden parcial sobre el conjunto A definido como:

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

En este caso, entonces $(A, \mathbf{R})$ es un conjunto parcialmente ordenado.

Ahora, sean los siguientes subconjuntos de A:

$\{1, 2, 3, 5\}$	$\{1\}$
$\{2, 4\}$	$\{3, 4\}$
$\{1, 2, 3\}$	$\{1, 2, 4\}$
$\{1, 4, 5\}$	

Determinar cuáles subconjuntos son cadenas y cuáles anticadenas.

Solución

$\{1, 2, 3, 5\}$	es una cadena.	$\{1\}$	es una cadena y una anticadena.
$\{2, 4\}$	es una anticadena.	$\{3, 4\}$	es una anticadena.
$\{1, 2, 3\}$	es una cadena.	$\{1, 2, 4\}$	no es ni cadena ni anticadena.
$\{1, 4, 5\}$	es una cadena.		

3.8 Diagrama de Hasse y láttices

Cuando se tiene un orden parcial $(A, \preccurlyeq)$, su representación mediante un dígrafo (grafo dirigido) puede simplificarse.

Como un orden parcial $(A, \preccurlyeq)$ es reflexivo, cada vértice está conectado con sí mismo a través de un lazo. Pero, para simplificar, en el dígrafo se borrarán todos los lazos.

Ejemplo

El dígrafo representado en la figura 3.17 a) puede representarse como en la figura 3.17 b), después de haberse eliminado todos los lazos.

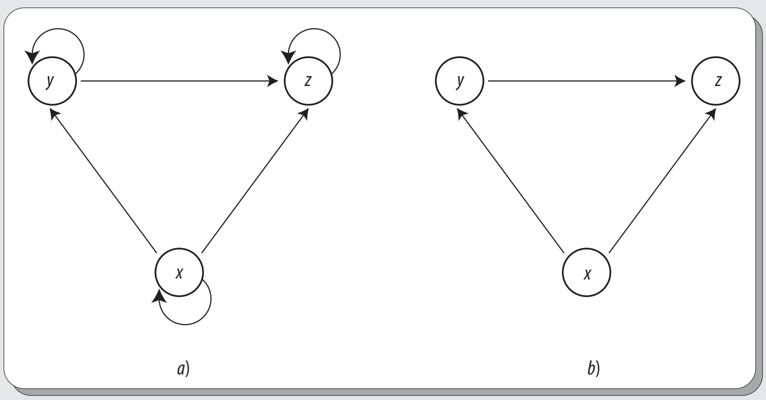


Figura 3.17 Eliminación de lazos en un dígrafo.

En el dígrafo también pueden eliminarse todas las aristas que están implicadas por la propiedad transitiva. Por tanto, si $a \npreceq b$ y $b \npreceq c$ implica que $a \npreceq c$. En este caso, se omite la arista que va desde a hasta c; sin embargo, sí se dejan las aristas que van de a a b y de b a c.

EJEMPLO

Si se eliminan las aristas que están involucradas por la propiedad transitiva del dígrafo de la figura 3.17 b), el dígrafo resultante se ve como el que se muestra en la figura 3.18.

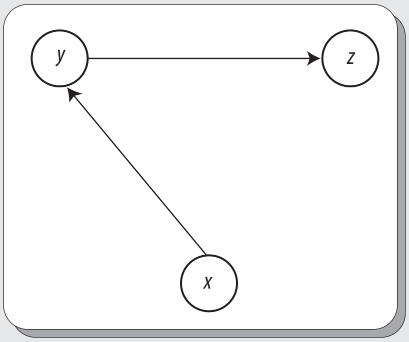


Figura 3.18 Eliminación de elementos transitivos.

Es importante destacar que también conviene dibujar el dígrafo de un orden parcial $(A, \preccurlyeq)$ con todas las aristas apuntando hacia arriba, puesto que las flechas pueden omitirse de las aristas.

Por último, los círculos de los vértices se reemplazan por puntos.

EJEMPLO

Al eliminar las flechas de las aristas y al reemplazar los círculos por puntos en el dígrafo, el diagrama final de la figura 3.17 b) se observa en la figura 3.19.

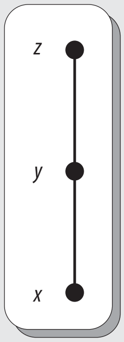


Figura 3.19 Eliminación de las fechas y reemplazo de los círculos.

El diagrama resultante de un orden parcial $(A, \preccurlyeq)$ es más simple que su dígrafo; a este se le denomina *diagrama de Hasse* de un orden parcial o de un conjunto parcialmente ordenado.

Los diagramas de Hasse deben su nombre al matemático alemán Helmut Hasse, quien los introdujo en 1926 en su libro *Höhere Algebra (Álgebra Superior)* como ayuda para el estudio de las soluciones de ecuaciones polinomiales. El **diagrama de Hasse** es una representación gráfica de un conjunto parcialmente ordenado finito. Esto se consigue mediante la eliminación de información redundante. En el diagrama de Hasse, la representación se hace mediante un dígrafo (grafo dirigido). Este diagrama es útil cuando se necesita un orden total que incluya un orden parcial dado.

Figura 3.20 Helmut Hasse (1898-1979).

Para comprender mejor este concepto se presenta otro ejemplo.

EJEMPLO

Sean el conjunto $A = \{1, 2, 3, 4, 12\}$ y **R** un orden parcial sobre el conjunto A definido como:

$$\mathrm{R} = \{(a, b)\ \mathrm{t} \cdot \mathrm{q} \cdot a|b\}$$

Esto es, si $a \in A \wedge b \in A$, $a \preccurlyeq b$, si y solo si $a|b$.

Obtener el diagrama de Hasse de $(A, \preccurlyeq)$.

Solución

Primero, se obtienen los elementos de **R:**

$$\mathrm{R} = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 12), (2, 2), (2, 4), (2, 12), (3, 3), (3, 12), (4, 4), (4, 12), (12, 12)\}$$

A continuación, se representa $(A, \preccurlyeq)$ como el dígrafo de la figura 3.21.

Luego, se eliminan los lazos del dígrafo (véase figura 3.22).

A continuación, se eliminan las aristas de los elementos (a, c) que están involucradas por la propiedad transitiva del dígrafo (véase figura 3.23).

Enseguida, se redibuja el dígrafo para que todas las aristas apunten hacia arriba (véase figura 3.24).

Luego, se eliminan las flechas de las aristas (véase figura 3.25).

Por último, se reemplazan los círculos por puntos y el diagrama de Hasse queda listo (véase figura 3.26).

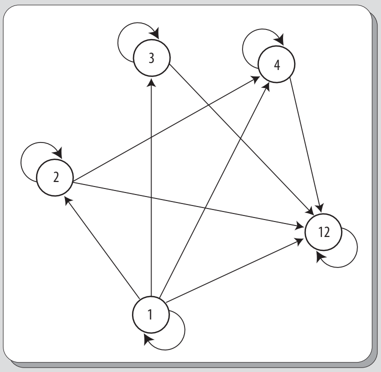


Figura 3.21 Representación del orden parcial como dígrafo.

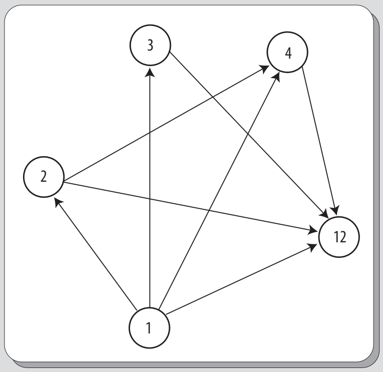


Figura 3.22 Eliminación de lazos.

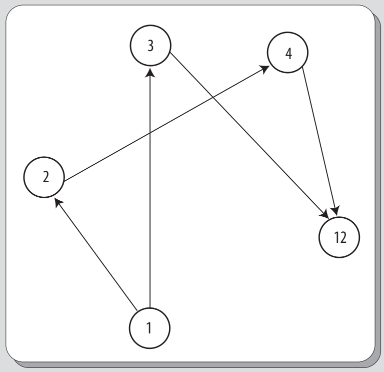


Figura 3.23 Eliminación de los elementos transitivos (a, c).

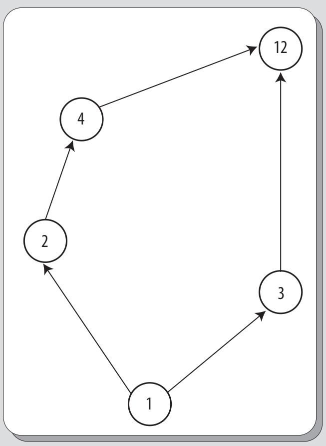


Figura 3.24 Redibujando el grafo para que las aristas apunten hacia arriba.

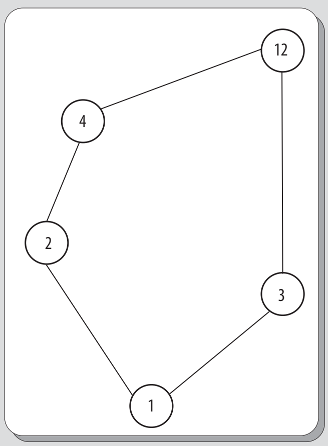


Figura 3.25 Eliminación de flechas.

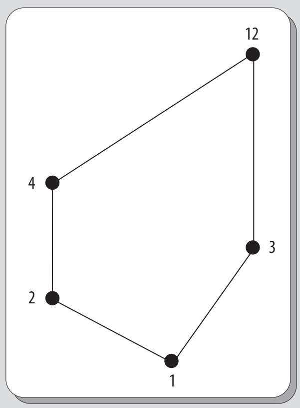


Figura 3.26 Mediante el reemplazo de círculos por puntos el diagrama de Hasse queda listo.

Otro ejemplo interesante es el siguiente.

EJEMPLO

Sean la relación $\mathbf{R} = \{(1, 1), (1, 2), (1, 3)\}$ y $P(\mathbf{R})$ el conjunto potencia de $\mathbf{R}$.

Obtener el diagrama de Hasse del conjunto parcialmente ordenado $P(\mathbf{R})$ con el orden parcial $\subseteq$; es decir, $(P(\mathbf{R}), \subseteq)$.

Solución

Primero, sea:

$$P(\mathbf{A}) = \{\varnothing, \{(1, 1)\}, \{(1, 2)\}, \{(1, 3)\}, \{(1, 1), (1, 2)\}, \{(1, 1), (1, 3)\}, \{(1, 2), (1, 3)\}, \{(1, 1), (1, 2), (1, 3)\}\}$$

El conjunto potencia de la relación $\mathbf{R}$.

Por lo que el conjunto parcialmente ordenado $(P(\mathbf{R}), \subseteq)$ que se obtiene es el siguiente:

$$\begin{array}{l}
\{\varnothing, \\
\{\{(1, 1)\}, \{(1, 1)\}\}, \\
\{\{(1, 2)\}, \{(1, 2)\}\}, \\
\{\{(1, 3)\}, \{(1, 3)\}\}, \\
\{\{(1, 1), (1, 2)\}, \{(1, 1), (1, 2)\}\}, \\
\{\{(1, 1), (1, 3)\}, \{(1, 1), (1, 3)\}\}, \\
\{\{(1, 2), (1, 3)\}, \{(1, 2), (1, 3)\}\}, \\
\{\{(1, 1), (1, 2), (1, 3)\}, \{(1, 1), (1, 2), (1, 3)\}\} \\
\{\varnothing, \{(1, 1)\}\}, \\
\{\varnothing, \{(1, 2)\}\}, \\
\{\varnothing, \{(1, 3)\}\}, \\
\{\varnothing, \{(1, 1), (1, 2)\}\}, \\
\{\varnothing, \{(1, 1), (1, 3)\}\}, \\
\{\varnothing, \{(1, 2), (1, 3)\}\}, \\
\{\varnothing, \{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 1)\}, \{\{(1, 1), (1, 2)\}\}, \\
\{\{(1, 1)\}, \{\{(1, 1), (1, 3)\}\}, \\
\{\{(1, 1)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 2)\}, \{\{(1, 1), (1, 2)\}\}, \\
\{\{(1, 2)\}, \{\{(1, 2), (1, 3)\}\}, \\
\{\{(1, 2)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 3)\}, \{\{(1, 1), (1, 3)\}\}, \\
\{\{(1, 3)\}, \{\{(1, 2), (1, 3)\}\}, \\
\{\{(1, 3)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 1), (1, 2)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 1), (1, 3)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}, \\
\{\{(1, 2), (1, 3)\}, \{\{(1, 1), (1, 2), (1, 3)\}\}\}
\end{array}$$

El cual se representa mediante un dígrafo como se observa en la figura 3.27.

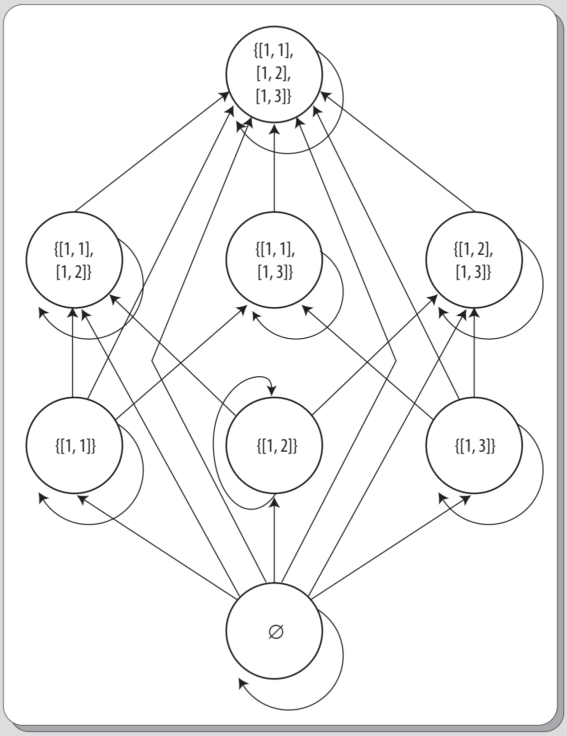


Figura 3.27 Representación del orden parcial como dígrafo.

Enseguida, se eliminan los lazos (véase figura 3.28).

Acto seguido, se continúa con la eliminación de las aristas de los elementos (a, c) que están involucradas en la propiedad transitiva del dígrafo (véase figura 3.29).

En este caso, no se redibuja el dígrafo para que todas las aristas apunten hacia arriba, pues estas ya lo hacen.

Entonces, lo que se hace es eliminar las flechas de las aristas (véase figura 3.30).

Por último, se reemplazan los círculos por puntos. El diagrama de Hasse resultante es el que se muestra en la figura 3.31.

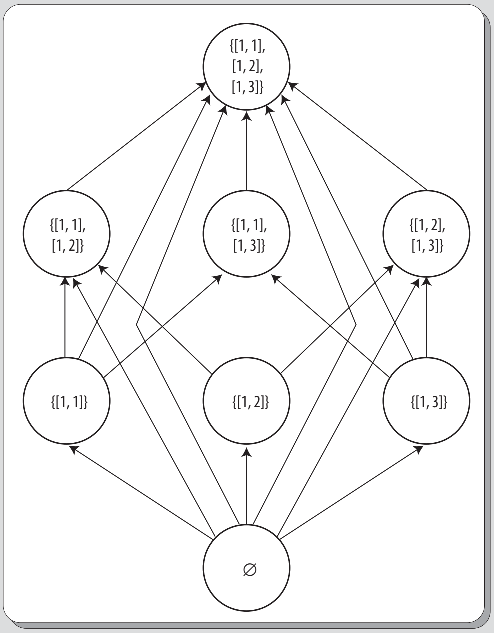


Figura 3.28 Eliminación de lazos.

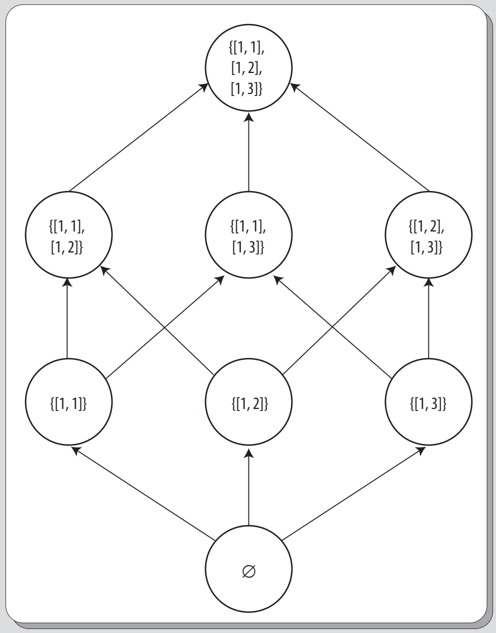


Figura 3.29 Eliminación de elementos transitivos (*a*, *c*).

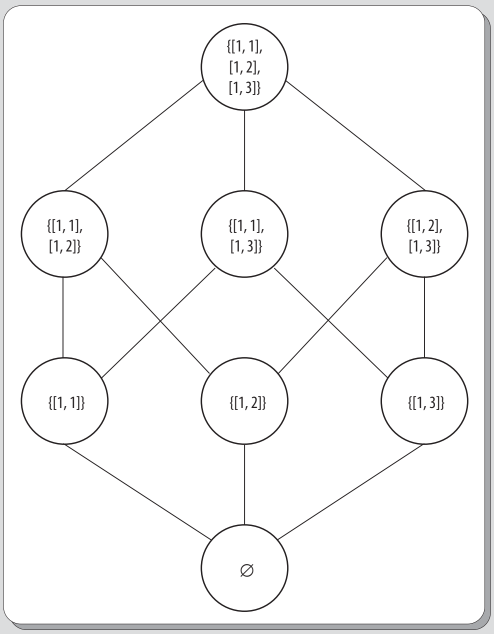


Figura 3.30 Eliminación de flechas.

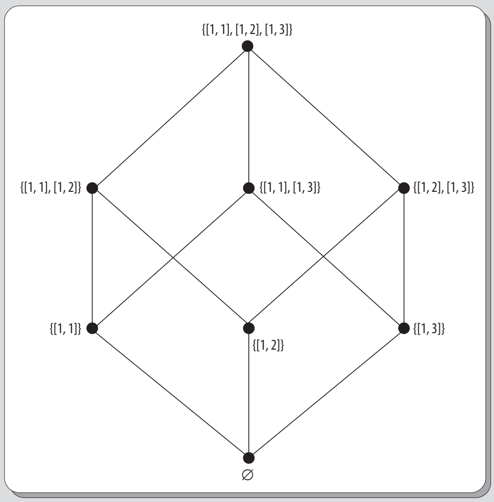


Figura 3.31 Reemplazando los círculos por puntos se obtiene el diagrama de Hasse.

El diagrama de Hasse de un conjunto ordenado totalmente siempre será una línea recta, como el que se observa en la figura 3.19.

Elementos extremos de un conjunto parcialmente ordenado

En los conjuntos parcialmente ordenados $(A, \preccurlyeq)$ (o POSET) se distinguen ciertos elementos que tienen propiedades especiales, que tienen alguna importancia en diversas aplicaciones. A estos se les denomina *elementos extremos* o *elementos extrémales*. A continuación, se presentan y definen dichos elementos.

Elemento maximal

Sean un conjunto parcialmente ordenado $(A, \preccurlyeq)$ y $a \in A$. Se dice que a es un *elemento maximal* de A si $a \preccurlyeq x$ implica que $a = x$, para todo x perteneciente a A. Desde el punto de vista formal, este elemento se expresa como:

$$\forall x \in A(a \preccurlyeq x \Rightarrow a = x)$$

Y significa que $a \in A$ es un elemento maximal si y solo si no existe en A un elemento distinto que lo siga.

Elemento minimal

Sean un conjunto parcialmente ordenado $(A, \preccurlyeq)$ y $a \in A$. Se dice que a es un *elemento minimal* de A si $x \preccurlyeq a$ implica que $x = a$, para todo x perteneciente a A. Desde el punto de vista formal, este elemento se denota como:

$$\forall x \in A(x \preccurlyeq a \Rightarrow x = a)$$

Lo que quiere decir que $a \in A$ es un elemento minimal si y solo si no existe en A un elemento distinto que lo preceda.

EJEMPLO

Sea un conjunto parcialmente ordenado $(A, \preccurlyeq)$, cuyo diagrama de Hasse se muestra en la figura 3.32.

Los elementos *a, b* y *c* son elementos maximales de *A*, y los elementos *d, e* y *f* son los elementos minimales de *A*. Se puede observar que como no existe una línea recta entre *e* y *f*, no se puede decir que $e \preccurlyeq f$ ni que $f \preccurlyeq e$.

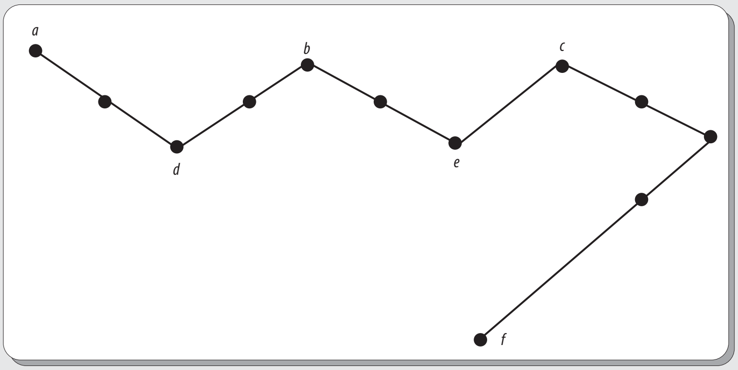


Figura 3.32 Diagrama de Hasse de un conjunto parcialmente ordenado.

EJEMPLO

Sea *A* el conjunto parcialmente ordenado $(A, \preccurlyeq)$ de todos los números reales no negativos $\mathbb{R}^+$ con el orden usual $\leq$. Entonces, el cero es el elemento minimal de *A* y no existen elementos maximales.

En tanto, el conjunto parcialmente ordenado con el orden usual $\leq$ no tiene elementos maximales ni minimales.

Máximo y mínimo

A un elemento $a \in A$ se le llama *máximo* de A, si x a para todo $x \in A$. En tanto, a un elemento $b \in A$ se le llama *mínimo* de A, si $b \preccurlyeq x$ para todo $x \in A$. Lo que formalmente se denota como:

$$a \text{ es elemento máximo de A si y solo si } \forall x(x \in A \Rightarrow x \preccurlyeq a)$$
$$\text{y}$$
$$b \text{ es elemento mínimo de A si y solo si } \forall x(x \in A \Rightarrow b \preccurlyeq x).$$

EJEMPLO

Sean la relación $\mathbf{R} = \{(1, 1), (1, 2), (1, 3)\}$ y $P(\mathbf{R})$ el conjunto potencia de $\mathbf{R}$.

Sea el conjunto parcialmente ordenado $P(\mathbf{R})$ con el orden parcial $\subseteq$; es decir, $(P(\mathbf{R}), \subseteq)$.

Entonces, el conjunto vacío es el elemento mínimo de $(P(\mathbf{R}), \subseteq)$ y $\mathbf{R}$ es el elemento máximo, como se muestra en la figura 3.31. En tanto que el conjunto parcialmente ordenado $\preccurlyeq$ con el orden habitual $\leq$ no tiene ni máximo ni mínimo.

Teorema 3.2

Un conjunto parcialmente ordenado tiene a lo sumo un elemento máximo y uno mínimo.

Demostración

Supóngase que a y b son los elementos máximos de un conjunto parcialmente ordenado $(A, \preccurlyeq)$. Entonces, $a \preccurlyeq b$, puesto que b es máximo y $b \preccurlyeq a$, porque a también es máximo. Por la propiedad antisimétrica se concluye que $a = b$.

Cota superior (mayorante) y cota inferior (minorante)

Sea $(A, \preccurlyeq)$ un conjunto parcialmente ordenado y $B \subseteq A$. A un elemento $a \in A$ se le llama *cota superior* o *mayorante* de B si $b \preccurlyeq a$ para todo $b \in B$. En tanto, a un elemento $c \in A$ se le llama *cota inferior* o *minorante* de B si $c \preccurlyeq x$ para todo $x \in B$.

EJEMPLO

Sea el conjunto parcialmente ordenado $(A, \preccurlyeq)$ representado por el diagrama de Hasse que se muestra en la figura 3.33.

Determinar las cotas superiores e inferiores de los siguientes subconjuntos de A:

$B = \{a, b\}$

$C = \{c, d, e\}$

Solución

En este caso, el subconjunto B no tiene cota inferior, mientras que sus cotas superiores son c, d, e, f, g y h.

El subconjunto C tiene como cotas superiores f, g y h y como cotas inferiores c, a y b.

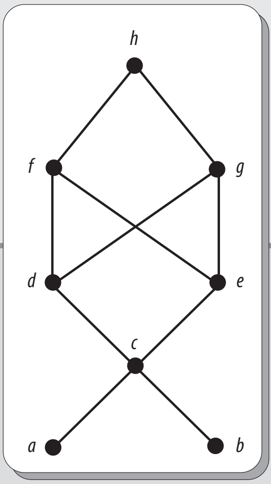


Figura 3.33 Diagrama de Hasse de un conjunto parcialmente ordenado.

Mínima cota superior (supremo)

Sea $(A, \preccurlyeq)$ un conjunto parcialmente ordenado y $B \subseteq A$. A un elemento $a \in A$ se le llama *mínima cota superior* o *supremo* de B si a es una cota superior de B y se cumple que $a \preccurlyeq a_1$ siempre que a_1 sea una cota superior de B. El supremo de B se denota como $sup(B)$.

Máxima cota inferior (ínfimo)

Sea $(A, \preccurlyeq)$ un conjunto parcialmente ordenado y $B \subseteq A$. A un elemento $a \in A$ se le llama *máxima cota inferior* o ínfimo de B si a es una cota inferior de B y se cumple que $a_1 \preccurlyeq a$ siempre que a_1 sea una cota inferior de B. El ínfimo de B se denota como $inf(B)$.

Las cotas inferiores en $(A, \leq)$ corresponden a las cotas superiores en $(A, \geq)$ y las cotas superiores en $(A, \leq)$ corresponden a las cotas inferiores en $(A, \geq)$. Lo mismo puede decirse de las máximas cotas inferiores y las mínimas cotas superiores.

Ejemplo

Sea el conjunto parcialmente ordenado $(A, \preccurlyeq)$, representado por el diagrama de Hasse de la figura 3.33. Y sean los subconjuntos de A:

$$B = \{a, b\} \text{ y}$$
$$C = \{c, d, e\}$$

Determinar la mínima cota superior y la máxima cota inferior de B y C.

Solución

El subconjunto B no tiene cotas inferiores; por tanto, carece de máxima cota inferior. En este caso, la mínima cota superior de B es c.

Puesto que las cotas inferiores de C son c, a y b, entonces la máxima cota inferior es c.

Las cotas superiores de C son f, g y h; pero, f y g no son comparables, por tanto C no tiene mínima cota superior.

Láttice

Los láttices son una nueva familia de conjuntos parcialmente ordenados. Estos poseen características especiales que los convierten en herramientas útiles en diversas aplicaciones relacionadas con los modelos de flujo de datos, además de que juegan un papel importante en el álgebra de Boole.

Definición de láttice

Sea $(A, \preccurlyeq)$ un conjunto parcialmente ordenado. Se dice que $(A, \preccurlyeq)$ es un láttice (retículo o red) si en todos sus subconjuntos de dos elementos $\{a, b\}$, elementos de A, existe un supremo y un ínfimo de dicho par; entonces, se dice que $(A, \preccurlyeq)$ es un láttice.

Todo conjunto totalmente ordenado es un láttice. En efecto, dados cualesquiera dos elementos de dicho conjunto, como son comparables, uno será el supremo y el otro será el ínfimo del conjunto que estos constituyen.

Ejemplo

Sea A el conjunto de los números naturales $\mathbb{N}$ y sea la relación $\mathbf{R}$ sobre el conjunto A definida como sigue:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a|b\}$$

Antes quedó demostrado que $(A, \mathbf{R})$ es un orden parcial y que además $(A, \preccurlyeq)$ es un conjunto parcialmente ordenado donde todos sus elementos son comparables, por lo que $(A, \preccurlyeq)$ es un conjunto totalmente ordenado.

Sea además $d = \text{mcd}(a, b)$; dado que d divide a a y a b. Por otra parte, d es múltiplo de cualquier otro divisor común de a y de b. Es decir, d será el ínfimo.

De manera similar, haciendo $d' = \text{mcm}\,(a, b)$, entonces d' será un múltiplo de a y de b. Asimismo, d' es un divisor de cualquier otro múltiplo común de a y b. En consecuencia, d' será el supremo.

Por lo general, el supremo y el ínfimo de un láttice $(A, \preccurlyeq)$ se denotan como $a \vee b$ y $a \wedge b$, respectivamente; es decir:

$$a \vee b = \sup\{a, b\}$$
$$a \wedge b = \inf\{a, b\}$$

Entonces, en el ejemplo anterior se tiene que:

$$d' = a \vee b = \sup\{a, b\}$$
$$d = a \wedge b = \inf\{a, b\}$$

Resumen

Las relaciones binarias, o simplemente relaciones, son la forma más básica de relacionar los elementos de dos conjuntos. Además, sobre dichas relaciones se pueden aplicar la mayoría de las operaciones sobre conjuntos, ya que, a fin de cuentas, las relaciones binarias son conjuntos de pares ordenados.

Para poder clasificar las relaciones, también es muy importante conocer sus propiedades, y así enfocarse en los dos tipos más importantes de relaciones binarias: las relaciones de equivalencia y las de orden parcial.

Las relaciones de equivalencia son las que permiten clasificar los elementos de un conjunto. El objetivo del estudio de relaciones de equivalencia es reconocer que el resultado de toda equivalencia da lugar a una partición de los elementos del conjunto y viceversa; en otras palabras, toda partición de un conjunto procede de una relación de equivalencia.

Las relaciones de orden parcial son aquellas que ordenan los elementos de un conjunto. El objetivo del estudio de un orden parcial es conocer los diferentes tipos de órdenes que existen y, en particular, entender la estructura de orden de los diferentes conjuntos de números, ya sean naturales, enteros o reales.

Problemas propuestos

Responder en forma correcta lo que se pide en cada caso.

3.1 Sean las siguientes relaciones en el conjunto de los números enteros:

$R = \{(a, b) \text{ t} \cdot \text{q} \cdot a \leq b\}$
$S = \{(a, b) \text{ t} \cdot \text{q} \cdot a > b\}$
$T = \{(a, b) \text{ t} \cdot \text{q} \cdot a = b \text{ o } a = -b\}$
$U = \{(a, b) \text{ t} \cdot \text{q} \cdot a = b\}$
$V = \{(a, b) \text{ t} \cdot \text{q} \cdot a = b + 1\}$
$W = \{(a, b) \text{ t} \cdot \text{q} \cdot a + b \leq 3\}$

¿Cuáles de estas relaciones contienen a los pares ordenados de la tabla 3.1?

Tabla 3.1

	R	S	T	U	V	W
(1, 1)						
(1, 2)						
(2, 1)						
(1, −1)						
(2, 2)						
(4, 3)						
(1, 3)						
(−1, −2)						
(3, −3)						
(2, 5)						
(−3, 2)						
(2, 4)						
(−1, 3)						

3.2 Sean el conjunto $A = \{a \text{ t} \cdot \text{q} \cdot a < 10, a \in \mathbb{N}\}$ y $R = \{(a, b) \text{ t} \cdot \text{q} \cdot 5|(a - b), a \neq b\}$ una relación sobre el conjunto A.

Determinar los elementos de **R**.

3.3 Sea **R** una relación de equivalencia sobre $\mathbb{Z}$.

Determinar el codominio de **R**.

3.4 Sean el conjunto $A = \{1, 2, 3, 4\}$ y $R = \{(x, y) \text{ t} \cdot \text{q} \cdot x + y = 3\}$ una relación sobre el conjunto A.

Determinar el dominio de **R**.

3.5 Sean el conjunto $A = \{1, 2, 3\}$ y $R = \{(1, 1), (2, 1), (3, 2), (1, 3)\}$ una relación sobre el conjunto A.

¿Cuáles declaraciones son verdaderas y cuáles falsas?

a) $1 \, R \, 1$
b) $1 \not R \, 2$
c) $2 \, R \, 3$

3.6 Sean los conjuntos $A = \{1, 2, \ldots, 10\}$ y $B = \{1, 2, 3, 4\}$ y sea $R = \{(a, b) \text{ t} \cdot \text{q} \cdot a + 3b = 13\}$ una relación de A en B.

Determinar los elementos de **R**.

3.7 Sea el conjunto $A = \{1, 2, 3\}$ y sea $R = \{(1, 1), (2, 1), (3, 2), (1, 3)\}$ una relación sobre el conjunto A.

¿Cuáles declaraciones son verdaderas y cuáles falsas?

a) $2 \not R \, 1$
b) $3 \, R \, 2$
c) $3 \not R \, 1$

3.8 Sean los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{1, 2, \ldots, 10\}$ y sea $\mathbf{R} = \{(a, b)$ t · q · $3a + b = 13\}$ una relación de A en B.

Determinar los elementos de **R**.

3.9 ¿Cuáles de los siguientes conjuntos son relaciones del conjunto $A = \{a, b, c\}$ en el conjunto $B = \{1, 2\}$?

a) $\mathbf{R} = \{(a, 1), (a, 2), (c, 2)\}$

b) $\mathbf{U} = \{(1, a), (2, a), (2, c)\}$

c) $\mathbf{T} = \varnothing$

3.10 Sean los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{5, 6, 7\}$ y sean las relaciones $\mathbf{R} = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$, $\mathbf{S} = \{(1, 2), (3, 2)\}$ y $\mathbf{T} = \{(1, 7), (2, 6)\}$.

¿Cuáles declaraciones sobre las relaciones son verdaderas y cuáles son falsas?

a) **R** sobre A, **S** de A en B, **T** de A en B.

b) **R** de A en B, **S** de A en B, **T** de A en B.

c) **R** sobre A, **S** sobre A, **T** de A en B.

d) **R** sobre A, **S** sobre A, **T** sobre A.

3.11 Sean los conjuntos $A = \{a, b, c\}$ y $B = \{1, 2\}$

¿Cuáles conjuntos son relaciones de A en B?

a) $\mathbf{R} = \{(a, 2), (b, 1)\}$

b) $\mathbf{S} = A \times B$

c) $\mathbf{T} = \{(2, a), (1, b)\}$

3.12 Sean los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{5, 6, 7\}$ y sean las relaciones $\mathbf{R} = \{(1, 2), (2, 3), (3, 4)\}$, $\mathbf{S} = \{(3, 5), (4, 6)\}$ y $\mathbf{T} = \{(1, 7), (4, 6)\}$.

¿Cuáles declaraciones sobre las relaciones son verdaderas y cuáles falsas?

a) **R** de A en B, **S** de A en B, **T** de A en B

b) **R** sobre A, **S** de A en B, **T** de A en B

c) **R** sobre A, **S** sobre B, **T** de A en B

d) **R** sobre A, **S** sobre B, **T** sobre A

3.13 Sea el conjunto $A = \{a \in \mathbb{N}$ t · q · $a|10\}$ y sea $\mathbf{R} = \{(a, b)$ t · q · $a|b\}$ una relación sobre A.

Determinar los elementos de **R**.

3.14 Sea $\mathbf{R} = \{(a, b)$ t · q $2|b\}$ una relación sobre $\mathbb{Z}^+$.

Determinar el codominio **R**.

3.15 Sea el conjunto $A = \{a \in \mathbb{N}$ t · q · $a|8\}$ y sea $\mathbf{R} = \{(x, y)$ t · q · $a|b\}$ una relación sobre A.

Obtener la matriz de relación resultante.

3.16 Sea el conjunto $A = \{1, 2, 3\}$ y sean $\mathbf{R} = \{(1, 1), (2, 2), (3, 3)\}$ y $\mathbf{S} = \{(1, 1), (1, 2), (1, 3)\}$ dos relaciones sobre A.

Efectuar las siguientes operaciones sobre las relaciones.

a) $\mathbf{R} \cup \mathbf{S}$

b) $\mathbf{R} \cap \mathbf{S}$

c) $\mathbf{R} - \mathbf{S}$

d) $\mathbf{S} - \mathbf{R}$

e) $\mathbf{R} \oplus \mathbf{S}$

f) **R’**

g) **S’**

h) $\mathbf{S}^{-1}$

i) $\mathbf{S} \circ \mathbf{R}$

j) $\mathbf{R}_1$

3.17 Sea el conjunto $A = \{1, 2, 3, 4, 5\}$ y sea $\mathbf{R} = \{(a, b)$ t · q · $a = b-1\}$ una relación sobre el conjunto A.

Obtener lo que se pide en cada caso.

a) Los elementos de **R**.

b) Los elementos de $\mathbf{R}^{-1}$.

c) El dominio de **R**.

d) El dominio de $\mathbf{R}^{-1}$.

3.18 ¿Cuál de las siguientes operaciones sobre relaciones siempre es verdadera?

a) $\mathbf{R} \cup \varnothing = \varnothing$

b) $\mathbf{R} \oplus \mathbf{R} = \varnothing$

c) $\mathbf{R} - \varnothing = \varnothing$

d) $\mathbf{R} \cap \varnothing = \mathbf{R}$

3.19 Las siguientes operaciones sobre relaciones son siempre verdaderas, excepto una. Indicar cuál.

a) $\mathbf{R} \cup \varnothing = \mathbf{R}$

b) $\mathbf{R} \cap \varnothing = \varnothing$

c) $\mathbf{R} - \varnothing = \varnothing$

d) $\mathbf{R} \oplus \mathbf{R} = \varnothing$

3.20 Sean **R** y **S** dos relaciones reflexivas. ¿Será verdadero que $\mathbf{R} \cup \mathbf{S}$ y $\mathbf{R} \cap \mathbf{S}$ son reflexivas?

3.21 Sean los conjuntos $A = \{1, 2\}$, $B = \{a, b, c\}$ y $C = \{c, d\}$.

Determinar $(A \times B) \cap (A \times C)$.

3.22 Sean A el conjunto de los números naturales y $\mathbf{R} = \{(a, b)\ \text{t} \cdot \text{q} \cdot 3a + 4b = 17\}$ una relación sobre A.

Determinar $\mathbf{R}^{-1}$.

3.23 Sean $\mathbf{R}$ y $\mathbf{S}$ dos relaciones simétricas sobre algún conjunto A; entonces, ¿será siempre verdadero que $\mathbf{R} \cup \mathbf{S}$ y $\mathbf{R} \cap \mathbf{S}$ son simétricas?

3.24 Sean los conjuntos $A = \{a, b\}$, $B = \{1, 2\}$ y $C = \{2, 3\}$.

Determinar $(A \times B) \cap (A \times C)$.

3.25 Sean A el conjunto de los números naturales y $\mathbf{R} = \{(a, b)\ \text{t} \cdot \text{q} \cdot 4a + 3b = 17\}$ una relación sobre A.

Determinar $\mathbf{R}^{-1}$.

3.26 Sea el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ y sean las relaciones $\mathbf{R} = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$ y $\mathbf{S} = \{(3, 3), (4, 2), (4, 4), (6, 2), (6, 3)\}$ dos relaciones sobre A.

¿De qué operación es resultado la relación $\mathbf{S}$ con respecto a la relación $\mathbf{R}$?

3.27 Sean el conjunto $A = \{1, 2, 3, 4\}$ y $\mathbf{R} = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$ una relación sobre A.

Determinar $(\mathbf{R} \circ \mathbf{R})^{-1}$

3.28 Sean el conjunto $A = \{1, 2, 3, 4\}$ y $\mathbf{R} = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$ una relación sobre A.

Determinar $\mathbf{R} \circ \mathbf{R}$.

3.29 Las siguientes propiedades de la composición de relaciones son verdaderas excepto:

a) $\mathbf{S} \circ \mathbf{R} = \mathbf{R} \circ \mathbf{S}$

b) $\mathbf{S} \circ \mathbf{R} \neq \mathbf{R} \circ \mathbf{S}$

c) $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) = (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$.

d) $(\mathbf{S} \circ \mathbf{R})^{-1} = \mathbf{R}^{-1} \circ \mathbf{S}^{-1}$

3.30 Sean el conjunto $A = \{1, 2, 3, 4\}$ y $\mathbf{R} = \{(1, 2), (3, 2)\}$ una relación sobre A.

Determinar el codominio de $\mathbf{R} \circ \mathbf{R}^{-1}$.

3.31 Sean el conjunto $A = \{1, 2, 3, 4\}$ y $\mathbf{R} = \{(1, 2), (3, 2)\}$ una relación sobre A.

Determinar el dominio de $\mathbf{R}^{-1} \circ \mathbf{R}$.

3.32 ¿Cuál propiedad de la composición de relaciones es siempre verdadera?

a) $\mathbf{S} \circ \mathbf{R} = \mathbf{R} \circ \mathbf{S}$

b) $\mathbf{S} \circ \mathbf{R} \neq \mathbf{R} \circ \mathbf{S}$

c) $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) \neq (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$

d) $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) = \mathbf{R}(\mathbf{S} \circ \mathbf{T})$

3.33 Sean $\mathbf{R} = \{(1, 1), (1, 2), (2, 1)\}$ y $\mathbf{S} = \{(1, 1), (1, 2), (2, 2)\}$ dos relaciones.

Determinar la matriz de relación que representa $\mathbf{S} \circ \mathbf{R}$.

3.34 Sea $\mathbf{R} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ una relación definida sobre el conjunto $A = \{1, 2, 3\}$.

Determinar el conjunto resultante de $\mathbf{R} \circ \mathbf{R}$.

3.35 Sean el conjunto $A = \{a, b, c, d\}$ y $\mathbf{R} = \{(a, b), (a, c), (c, b)\}$ una relación sobre el conjunto A.

Determinar el codominio de $\mathbf{R} \circ \mathbf{R}$.

3.36 Sean el conjunto $A = \{a, b, c, d\}$ y $\mathbf{R} = \{(a, b), (a, c), (c, b)\}$ una relación sobre el conjunto A.

Determinar $\mathbf{R} \circ \mathbf{R}$.

3.37 Sean $\mathbf{R} = \{(1, 2), (2, 2), (3, 4)\}$ y $\mathbf{S} = \{(1, 3), (2, 5), (3, 1), (4, 2)\}$ dos relaciones. Encontrar $\mathbf{R} \circ (\mathbf{S} \circ \mathbf{R})$.

3.38 ¿Cuáles propiedades tiene cada una de las siguientes relaciones sobre el conjunto $A = \{a, b, c, d\}$?

Tabla 3.2

R	*a*	*b*	*c*	*d*
a				✓
b			✓	
c		✓		
d	✓			

S	*a*	*b*	*c*	*d*
a	✓			
b		✓		
c			✓	
d				✓

T	*a*	*b*	*c*	*d*
a	✓		✓	✓
b		✓		✓
c		✓	✓	
d				✓

U	*a*	*b*	*c*	*d*
a		✓		✓
b				✓
c				
d				

V	*a*	*b*	*c*	*d*
a	✓	✓		✓
b	✓	✓		
c			✓	
d	✓			✓

3.39 ¿Cuáles propiedades tiene cada una de las siguientes relaciones sobre el conjunto $A = \{1, 2, 3\}$?

a) $\{(a, b)$ tal que $a \leq b\}$

b) $\{(a, b)$ tal que $a > b\}$

c) $\{(a, b)$ tal que $a = b\}$

d) $\{(a, b)$ tal que $a + b \leq 3\}$

3.40 ¿Cuáles de las siguientes declaraciones sobre las relaciones son verdaderas y cuáles falsas?

a) Si **R** es simétrica, entonces $\mathbf{R}^{-1}$ es simétrica.

b) Si **R** y **S** son transitivas, entonces **R**∘**S** es transitiva.

c) Si **R** y **S** son reflexivas, entonces $\mathbf{R} \cap \mathbf{S}$ es reflexiva.

3.41 ¿Cuáles declaraciones sobre las relaciones son verdaderas y cuáles falsas?

a) Si **R** y **S** son transitivas, entonces $\mathbf{R} \cup \mathbf{S}$ es transitiva.

b) Si **R** es reflexiva, entonces $\mathbf{R}^{-1}$ es reflexiva.

c) Si **R** y **S** son reflexivas, entonces $\mathbf{R} \cup \mathbf{S}$ es reflexiva.

3.42 ¿Cuáles propiedades tiene cada una de las siguientes relaciones sobre el conjunto $A = \{1, 2, 3, 4\}$?

a) $\{(1, 2), (2, 3), (1, 3)\}$

b) $\{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3), (4, 4)\}$

c) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$

3.43 Sea L el conjunto de las rectas del plano. ¿Qué relación será transitiva sobre L?

$\mathbf{U} = L_1\mathbf{R}L_2$ si L_1 es paralela a L_2

$\mathbf{T} = L_1\mathbf{R}L_2$ si L_1 es perpendicular a L_2

3.44 Una relación **R** es simétrica sobre un conjunto A si

a) $(a, b) \in \mathbf{R} \rightarrow (b, a) \notin \mathbf{R}\ \forall a \forall b \in A$

b) $(a, b) \in \mathbf{R}\ \forall a \in A$

c) $(a, b) \notin \mathbf{R} \rightarrow (b, a) \in \mathbf{R}\ \forall a \forall b \in A$

d) $(a, b) \in \mathbf{R} \rightarrow (b, a) \in \mathbf{R}\ \forall a \forall b \in A$

3.45 ¿Cuáles propiedades tiene la relación representada por el siguiente dígrafo?

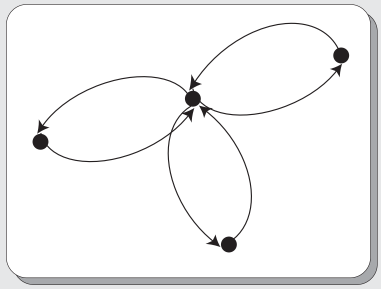


Figura 3.34

3.46 Una relación **R** es irreflexiva sobre un conjunto A si:

a) $(a, b) \in \mathbf{R} \rightarrow (b, a) \notin \mathbf{R}\ \forall a \forall b \in A$

b) $(a, a) \notin \mathbf{R}\ \forall a \in A$

c) $(a, b) \notin \mathbf{R} \rightarrow (b, a) \in \mathbf{R}\ \forall a \forall b \in A$

d) $(a, a) \in \mathbf{R}\ \forall a \in A$

3.47 ¿Cuáles propiedades tiene la relación representada por el siguiente dígrafo?

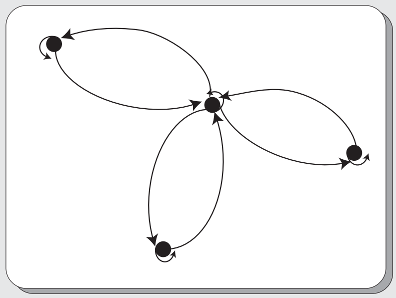


Figura 3.35

3.48 Sean el conjunto $A = \{a, b, c, d\}$ y $\mathbf{R} = \{(a, b), (b, c), (c, b), (c, d)\}$ una relación sobre A.

Determinar $\mathbf{R}_1$.

3.49 Sea el conjunto $A = \{1, 2, 3, 4\}$.

Determinar cuál matriz de relación representa una relación irreflexiva.

$$a)\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad b)\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$c)\ \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \qquad d)\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Figura 3.36

3.50 Sea **R** $= \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5)\}$ una relación de equivalencia sobre el conjunto $A = \{1, 2, 3, 4, 5\}$.

Obtener la partición **S** sobre A originada por **R**.

3.51 Determinar la relación de equivalencia cuyas clases de equivalencia son: $[a] = \{a\}$, $[b] = [d] = \{b, d\}$ y $[c] = \{c\}$.

3.52 Determinar la relación de equivalencia cuyas clases de equivalencia son: $[1] = [2] = \{1, 2\}$, $[3] = \{3\}$, $[4] = \{4\}$.

3.53 Sean el conjunto $A = \{1, 2, 3, \ldots, 10\}$ y **R** $= \{(a, b)$ t · q · $a - b$ es divisible por 5$\}$ una relación sobre A.

Determinar $[2]$.

3.54 Sean el conjunto $A = \{1, 2, 3, \ldots, 20\}$ y **R** $= \{(a, b)$ t · q · $a - b$ es divisible por 4$\}$ una relación sobre A.

Determinar $[1]$.

3.55 Sean el conjunto $A = \{1, 2, 3, \ldots, 20\}$ y **R** $= \{(a, b)$ t · q · $a - b$ es divisible por 5$\}$ una relación sobre A.

Determinar $[5]$.

3.56 Sea el conjunto $A = \{1, 2, 3, \ldots, 15\}$. Considerar la relación de equivalencia $\approx$ sobre $A \times A$, definida por $(a, b) \approx (c, d)$, si $ad \approx bc$.

Determinar la clase de equivalencia de $(3, 2)$.

3.57 Sea $A = \{1, 2, 3, \ldots, 15\}$. Considerar la relación de equivalencia ~ sobre $A \times A$, definida por (a, b) ~ (c, d), si $a + d = b + c$.

Determinar la clase de equivalencia de $(2, 11)$.

3.58 Sean el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ y **R** $= \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4), (5, 5), (5, 6), (6, 5), (6, 6)\}$ una relación sobre el conjunto A.

Determinar cuál es la partición **S** originada por la relación anterior sobre A.

3.59 Sea **R** la relación "tiene el mismo tamaño que", definida en todos los subconjuntos finitos de $\mathbb{Z}$; es decir, a **R** b si y solo si $|A| = |B|$.

Demostrar que **R** es una relación de equivalencia sobre $\mathbb{Z}$.

3.60 En una relación de equivalencia sobre un conjunto A son válidas las siguientes afirmaciones excepto:

a) Si a **R** b, entonces $[a] \cap [b] = \varnothing$.

b) **S** $= \{[a]$ t · q · $a \in$ A$\}$ es una partición de A.

c) Si a **R** b, entonces $[a] = [b]$.

d) Si $[a] = [b]$, entonces $[a] \cap [b] \neq \varnothing$.

3.61 Sea **R** la relación "es semejante a", definida en el conjunto de todos los triángulos, es decir, T_1 **R** T_2 si y solo si T_1 es semejante a T_2.

Demostrar que **R** es una relación de equivalencia.

3.62 Sea **R** $= \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$ una relación sobre el conjunto $A = \{1, 2, 3, 4, 5, 6\}$.

Determinar cuál es la partición originada por la relación anterior sobre el conjunto A.

3.63 En una relación de equivalencia sobre un conjunto A, ¿cuál de las siguientes afirmaciones es válida?

a) Si $a \not R\, b$, entonces $[a] = [b]$.

b) Si a **R** b, entonces $[a] \cap [b] \neq \varnothing$.

c) Si $[a] = [b]$, entonces $[a] \cap [b] = \varnothing$.

d) Si a **R** b, entonces $[a] \cap [b] = \varnothing$.

3.64 Sea el conjunto $A = \{1, 2, 3, 4, 5\}$ y sean las siguientes relaciones sobre A.

¿Cuáles relaciones son de equivalencia sobre A?

a) $\{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 4), (5, 5)\}$

b) $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$

c) $\{(1, 1), (1, 3), (1, 5), (2, 2), (3, 1), (3, 3), (3, 5), (4, 4), (5, 1), (5, 3), (5, 5)\}$

d) $\{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4), (5, 5)\}$

3.65 ¿Cuáles de las siguientes relaciones son órdenes parciales sobre $\mathbb{Z}$?

R $= \{(a, b)$, tal que $a = b + 1\}$

S $= \{(a, b)$, tal que $a \leq b\}$

T $= \{(a, b)$, tal que $a > b\}$

U $= \{(a, b)$, tal que $a|b\}$

V $= \{(a, b)$, tal que $a + b \leq 3\}$

W $= \{(a, b)$, tal que $a = b*2\}$

3.66 Una relación **R** sobre un conjunto A, que es reflexiva, antisimétrica y transitiva recibe el nombre de ____________.

3.67 Todas las siguientes relaciones sobre $\mathbb{Z}$ son órdenes parciales excepto:

$R = \{(a, b) \text{ t} \cdot \text{q} \cdot a > b\}$

$S = \{(a, b) \text{ t} \cdot \text{q} \cdot a|b\}$

$T = \{(a, b) \text{ t} \cdot \text{q} \cdot a \leq b\}$

$U = \{(a, b) \text{ t} \cdot \text{q} \cdot a \leq \text{b}\}$

3.68 Sean el conjunto $A = \{1, 2, 3, 4\}$ y **R** una relación de orden parcial sobre A definida como:

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

¿Cuáles de los siguientes subconjuntos de A son cadenas y cuáles son anticadenas?

a) $A = \{2\}$

b) $B = \{2, 4\}$

c) $C = \{1, 2, 3\}$

d) $D = \{1, 2, 3, 4\}$

3.69 En un orden parcial **R** sobre un conjunto A, si $a \in A$, $b \in A$ y $c \in A$ y si $a\,\mathbf{R}\,b$ y $b\,\mathbf{R}\,c$. Las siguientes afirmaciones se cumplen excepto:

a) $b\,\mathbf{R}\,b$

b) $b\,\mathbf{R}\,a$

c) $a\,\mathbf{R}\,a$

d) $a\,\mathbf{R}\,c$

3.70 Sean A un conjunto cualesquiera y P(A) el conjunto potencia de A y sea **R** una relación sobre el conjunto P(A) definida como:

$$\mathbf{R} = \{\mathbf{S} \in \text{P}(A) \text{ t} \cdot \text{q} \cdot \mathbf{S} \subseteq A\}$$

Demostrar que (P(A), **R**) es un conjunto parcialmente ordenado.

3.71 Sean A el conjunto $\mathbb{N}$ y **R** una relación sobre A definida como:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a + b \text{ es par}\}$$

¿Será (A, **R**) un conjunto parcialmente ordenado (POSET)?

3.72 Sean A el conjunto $\mathbb{Z}^+$ y **R** una relación sobre A definida como:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a < b\}$$

Demostrar que **R** no es un orden parcial sobre A.

3.73 Sean el conjunto $A = \{1, 2, 3, 4\}$ y (P(A), $\subseteq$) un conjunto parcialmente ordenado sobre A. Sean, además, los siguiente pares de subconjuntos de A:

a) $\{2, 4, 1\}$ y $\{1, 2\}$

b) $\{1, 2, 3\}$ y $\{2, 3, 4\}$

¿Son comparables o incomparables? Justificar la respuesta.

3.74 Sean A el conjunto $\mathbb{N}$ y **R** una relación de orden parcial sobre A definida como:

$$\mathbf{R} = \{(a, b) \text{ t} \cdot \text{q} \cdot a|b\}$$

¿Cuáles de los siguientes subconjuntos de A son cadenas y cuáles son anticadenas?

a) $A = \{5, 8, 21\}$

b) $B = \{6, 30, 10\}$

c) $C = \{4, 16, 64, 8\}$

d) $D = \{7\}$

e) $E = \{30, 10, 60\}$

f) $\mathbb{N} = \{1, 2, 3, \ldots\}$

3.75 Sea el conjunto $A = \{a, b, c, d, e\}$ con la relación **R** correspondiente al orden lexicográfico habitual de las letras del alfabeto.

Dibujar el diagrama de Hasse correspondiente.

3.76 Sea el siguiente dígrafo de una relación de orden parcial.

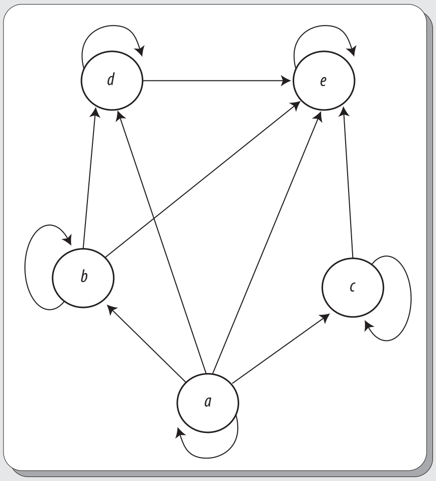


Figura 3.37

Dibujar el diagrama de Hasse correspondiente.

3.77 Sean el conjunto $A = \{2, 4, 6, 12, 18, 36\}$ y **R** la relación de orden parcial sobre el conjunto A definida como:

$$\mathrm{R} = \{(a, b)\ \mathrm{t \cdot q \cdot}\ a|b\}$$

Dibujar el diagrama de Hasse correspondiente.

3.78 Sea un conjunto parcialmente ordenado $(A, \preccurlyeq)$, cuyo diagrama de Hasse es el siguiente:

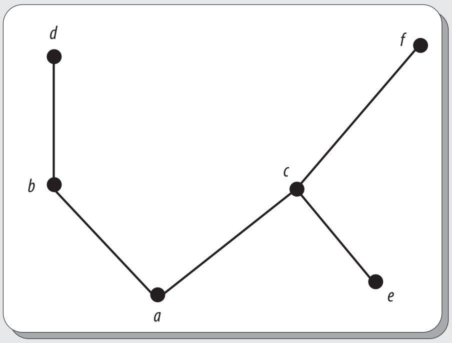


Figura 3.38

Determinar sus elementos maximales y minimales.

3.79 Sea un conjunto parcialmente ordenado $(A, \preccurlyeq)$ sobre el conjunto $A = \{8, 12, 16\}$, cuyo diagrama de Hasse es el siguiente:

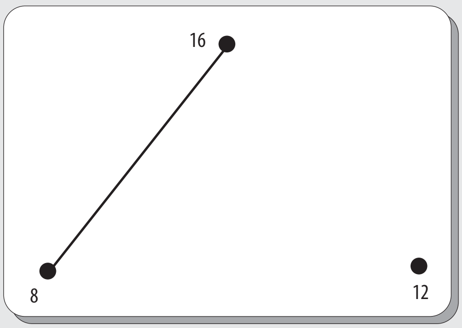


Figura 3.39

Determinar sus elementos maximales y minimales.

3.80 Sean un conjunto parcialmente ordenado $(A, \preccurlyeq)$ sobre el conjunto $A = \{2, 4, 6, 12, 20\}$ y **R** una relación de orden parcial definida como:

$$\mathrm{R} = \{(a, b)\ \mathrm{t \cdot q \cdot}\ a|b\}$$

Determinar sus máximos y mínimos.

3.81 Sea un conjunto parcialmente ordenado $(A, \preccurlyeq)$, cuyo diagrama de Hasse es el siguiente:

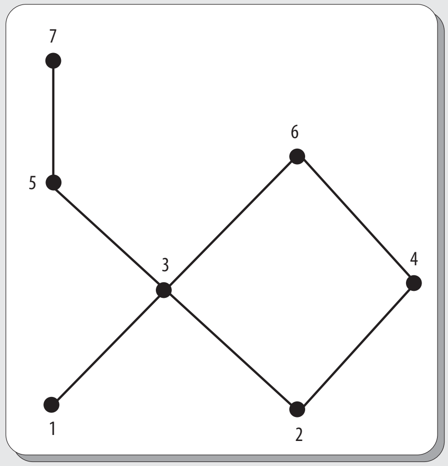


Figura 3.40

Determinar sus máximos y mínimos.

3.82 Sea un conjunto parcialmente ordenado $(A, \preccurlyeq)$ sobre el conjunto $A = \{1, 2, 3, 4, 5, 6, 7\}$, cuyo diagrama de Hasse es el siguiente:

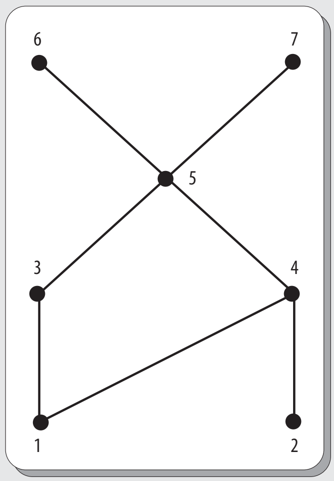


Figura 3.41

Determinar las cotas superiores e inferiores del subconjunto $B = \{3, 4, 5\}$.

3.83 Sea un conjunto parcialmente ordenado (A, $\preccurlyeq$), cuyo diagrama de Hasse es el siguiente:

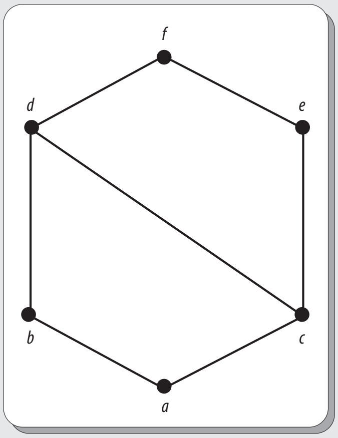


Figura 3.42

Determinar si es un láttice.

3.84 Sea un conjunto parcialmente ordenado (A, $\preccurlyeq$), cuyo diagrama de Hasse es el siguiente:

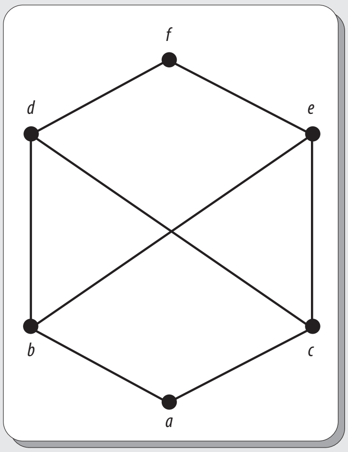


Figura 3.43

Problemas reto

Dar las razones por las cuáles no es un láttice.

1. Encontrar alguna relación que al mismo tiempo sea una relación de equivalencia y una relación de orden parcial.

2. Sea el siguiente diagrama de Hasse de un conjunto parcialmente ordenado:

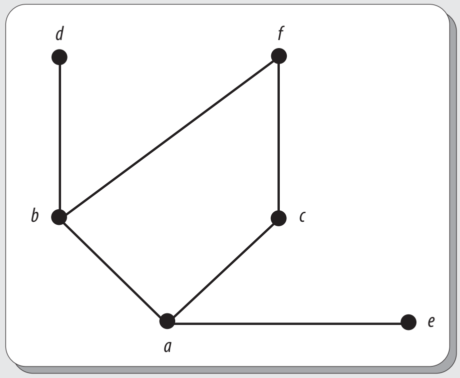
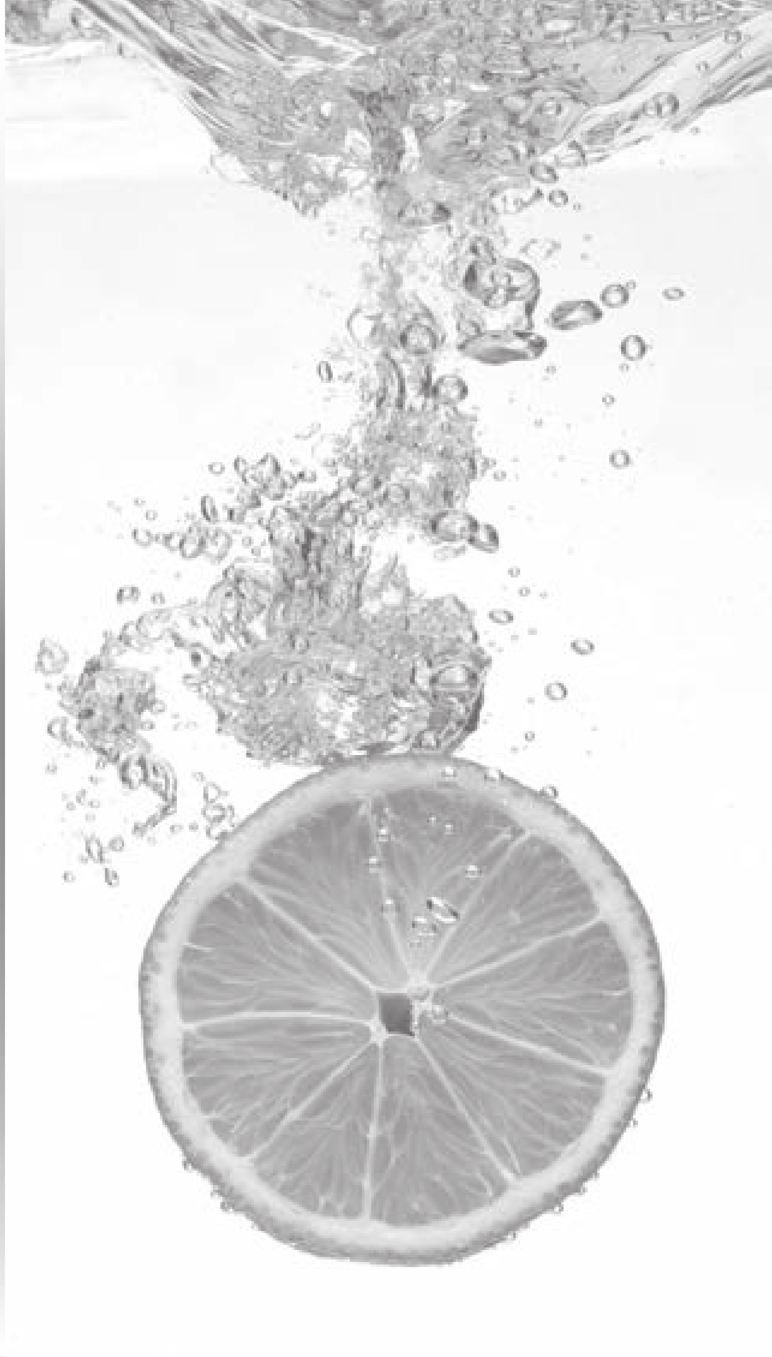


Figura 3.44

Obtener el dígrafo que dio origen a dicho diagrama.

4

Relaciones de recurrencia



Objetivos

- Aplicar los conceptos de relaciones binarias desde un punto de vista discreto.
- Determinar diversas relaciones binarias sobre los elementos de uno o dos conjuntos.
- Efectuar diversas operaciones entre relaciones binarias.
- Definir las propiedades que satisface determinada relación binaria.
- Identificar tipos especiales de relaciones binarias (relaciones de equivalencia y órdenes parciales).

4.1 Introducción

La solución de las relaciones de recurrencia es un tema de vital importancia para abordar distintos tipos de problemas en matemáticas y ciencias de la computación.

De manera tradicional, la bibliografía que propone métodos de resolución de recursividades lineales se basa en el planteamiento de ecuaciones polinómicas difícilmente programables, pero solucionables mediante relaciones de recurrencia.

Sin embargo, como las relaciones de recurrencia mantienen una relación muy cercana con los algoritmos recursivos, estas surgen de manera natural con el análisis de este tipo de algoritmos.

Asimismo, las relaciones de recurrencia pueden considerarse técnicas avanzadas de conteo, ya que estas pueden resolver cierto tipo de problemas que no pueden resolverse con el uso de las técnicas tradicionales de conteo, como permutaciones, combinaciones o técnicas derivadas del principio de inclusión-exclusión.

4.2 Progresiones aritméticas y geométricas

Las progresiones constituyen casos especiales de sucesiones. Así, una progresión se define como una sucesión numérica que cumple con ciertas condiciones con respecto al valor entre un término y el siguiente.

Su origen, al igual que el de tantas otras ramas de las matemáticas, es incierto. No obstante, se conservan algunos documentos que atestiguan la presencia de progresiones desde varios siglos antes de nuestra era, por lo que no debe atribuirse su paternidad a ningún matemático en especial.

Bhaskara, matemático hindú del siglo XII, también conocido como Bhaskara II o Bhaskaracharya, que significa "Bhaskara el maestro", es probablemente el matemático hindú más conocido de la antigüedad. En su obra más conocida, el *Lilavati*, plantea diversos problemas sobre progresiones aritméticas y geométricas, además de estudiar algunas ecuaciones diofánticas y geometría plana. Bhaskara también es reconocido por la aportación de dos famosos algoritmos de multiplicación de números en base diez.

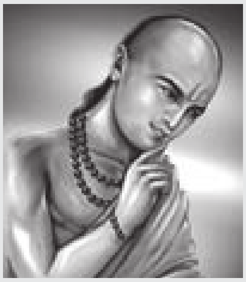


Figura 4.1 Bhaskara, matemático hindú del siglo XII.

A pesar de que hoy día el problema de calcular el tiempo en que se duplicaría una cantidad de dinero a un determinado interés compuesto es muy conocido, se sabe que este fue propuesto por los babilonios (2000 a.C.-600 a.C.), lo que nos permite deducir que esta cultura conocía de alguna manera la fórmula del interés compuesto y, por tanto, las progresiones geométricas.

No obstante, en el libro IX de *Los elementos* de Euclides, que data aproximadamente del año 300 a.C., aparece la transcripción de una fórmula de la suma de n términos consecutivos de una progresión geométrica muy semejante a la actual.

Progresiones aritméticas

Antes de definir qué es una progresión aritmética, a continuación se trata un ejemplo en el que aparece una progresión de este tipo.

EJEMPLO

Escalera de Jacob

Jacob posee un rascacielos en el que hay una escalera que va desde el ras del suelo hasta la cima de la construcción. El primer escalón mide 18 centímetros, mientras que los posteriores miden 19 centímetros.

Continúa

¿A qué altura del ras del suelo está el escalón 800? (véase figura 4.2).

Con base en un análisis de la figura 4.2, se tiene que:

$a_1 = 18$

$a_2 = 18 + 1(19) = 37$

$a_3 = 18 + 2(19) = 56$

$a_4 = 18 + 3(19) = 75$

$\vdots$

$a_{800} = 18 + 799(19) = 15\,199$

Por tanto, como se puede observar, el escalón 800 está a 15 199 centímetros sobre el ras del suelo.

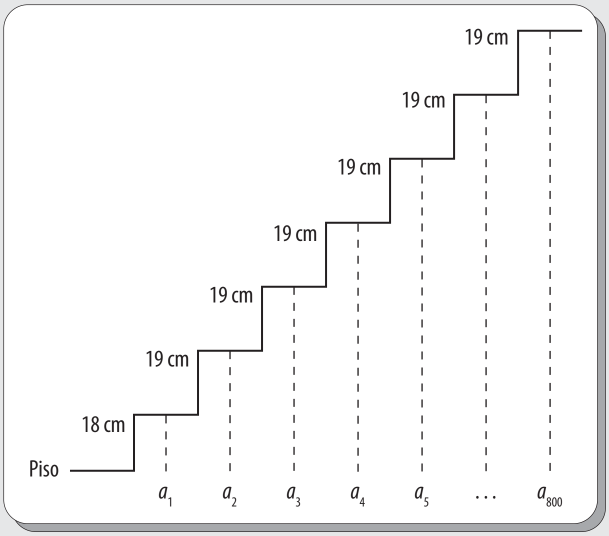


Figura 4.2 Escalera de Jacob hasta el escalón 800.

Asimismo, también se genera la siguiente sucesión:

$$\{a_n\} = \{18, 37, 56, 75, \ldots, 15\,199\}$$

la cual, como se ve más adelante, es en efecto una progresión aritmética.

Ahora, se considerarán las siguientes sucesiones:

$\{a_n\} = \{10, 14, 18, 22, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$
$\{b_n\} = \{3, 3.5, 4, 4.5, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$
$\{c_n\} = \{9, 6, 3, 0, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$

El objetivo es detectar el patrón que siguen estas y llenar los espacios en blanco en cada una.

Como se puede observar, no es difícil encontrar el valor de dichos términos; pero, ¿qué tienen en común estas tres sucesiones? Simplemente que, en cada caso, se puede obtener un término sumando un número fijo al término anterior.

Estas sucesiones también son casos de progresiones aritméticas, por lo que ahora es tiempo de definirlas.

Progresiones aritméticas

Una progresión aritmética constituye una sucesión infinita de números donde cualquier término (distinto del primero) se obtiene sumando un número fijo al anterior.
Si se denota a tal sucesión como:

$$a_1, a_2, a_3, \ldots$$

entonces, se satisface la fórmula recursiva (que más adelante se define de manera formal):

$$a_n = a_{n-1} + d$$

donde d es un número fijo llamado diferencia común.
Además, el valor de d es muy importante, ya que si es:

- **Positivo**, entonces la progresión aritmética es creciente; es decir, cada término es mayor que el anterior.

- **Cero**, entonces la progresión aritmética es constante; es decir, tiene todos sus términos iguales.
- **Negativo**, entonces la progresión es decreciente; es decir, cada término es menor que el anterior.

Ahora bien, ¿se puede obtener una fórmula explícita?; es decir, una fórmula para encontrar de manera directa el valor de cualquier término sin necesidad de determinar estos de uno en uno, como se haría con la fórmula recursiva. La respuesta es sí. Para ello, primero véase la figura 4.3.

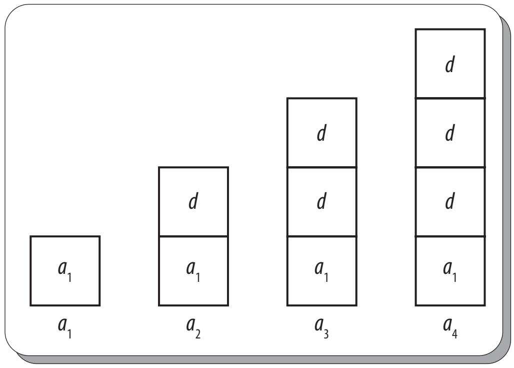


Figura 4.3 Auxiliar para obtener la fórmula explícita para una progresión aritmética.

Como se puede ver, los valores de la parte inferior de esta figura (a_1, a_2, a_3, a_4) corresponden a los cuatro primeros términos de una progresión aritmética general; así que aplicando la fórmula recursiva se tiene que:

$$\begin{aligned}
a_1 &= a_1 \\
a_2 &= a_1 + d \\
a_3 &= a_2 + d = (a_1 + d) + d = a_1 + 2d \\
a_4 &= a_3 + d = (a_1 + d + d) + d = a_1 + 3d \\
&\vdots
\end{aligned}$$

Como se observa, las d deben sumarse con a_1 una vez menos que el subíndice de a. Esto significa que:

$$a_n = a_1 + (n-1)d$$

A esta ecuación se le conoce como **fórmula explícita para progresiones aritméticas** y con esta es posible calcular cualesquier término a_n en función del primer término a_1, del total de términos n o número de términos que preceden a $n-1$, y de la diferencia común d.

Ejemplo

Retomar las siguientes progresiones aritméticas:

$\{a_n\} = \{10, 14, 18, 22, \ldots\}$

$\{b_n\} = \{3, 3.5, 4, 4.5, \ldots\}$

$\{c_n\} = \{9, 6, 3, 0, \ldots\}$

Determinar el valor del término 100 en cada caso.

Si se utiliza la fórmula recursiva, se tendría que determinar los términos de uno en uno, hasta llegar al término 100.

Solución

Así que, en este caso, primero se determinará la fórmula explícita correspondiente para cada una de las progresiones aritméticas. De este modo, se tiene que:

$$\begin{aligned}
a_n &= 10 + (n-1)(4) = 6 + 4n \\
b_n &= 3 + (n-1)(0.5) = 2.5 + 0.5n \\
c_n &= 9 + (n-1)(-3) = 12 - 3n
\end{aligned}$$

Una vez que se determinaron las **fórmulas** explícitas correspondientes, es fácil encontrar el valor de cualquier término de forma independiente.

Así, el valor del término 100 en cada caso es:

$$\begin{aligned}
a_{100} &= 6 + 4(100) = 406 \\
b_{100} &= 2.5 + 0.5(100) = 52.5 \\
c_{100} &= 12 - 3(100) = -288
\end{aligned}$$

Además de la fórmula explícita, también es posible deducir otros elementos de la progresión aritmética:

- El primer término: $a_1 = a_n - (n-1)d$
- La diferencia común: $d = \dfrac{a_n - a_1}{n-1}$
- La cantidad de términos: $n = \dfrac{a_n - a_1}{d} + 1$

A continuación se ve un ejemplo de cada uno de estos elementos que es posible deducir.

Ejemplo

Determinar el valor del término a_1 de una progresión aritmética, donde el término $a_9 = 12$ y la diferencia común $d = 2$.

Solución

Como $a_1 = a_n - (n-1)\,d$, entonces, al sustituir los valores dados, se tiene que:

$$\begin{aligned} a_1 &= 12 - (9-1) \cdot 2 \\ &= 12 - (8) \cdot 2 \\ &= 12 - 16 \\ &= -4 \end{aligned}$$

De este modo, la progresión aritmética resultante es:

$$\{a_n\} = \{-4, -2, 0, 2, 4, 6, 8, 10, 12, \ldots\}$$

Ejemplo

Determinar el valor de la diferencia común d en una progresión aritmética donde el valor del término $a_1 = -2$ y el del término $a_7 = 16$.

Solución

Como $d = \dfrac{a_n - a_1}{n-1}$, entonces al sustituir los valores dados, se tiene que:

$$\begin{aligned} d &= \frac{16-(-2)}{(7-1)} \\ &= \frac{18}{6} \\ &= 3 \end{aligned}$$

donde la progresión aritmética resultante es:

$$\{a_n\} = \{-2, 1, 4, 7, 10, 13, 16, \ldots\}$$

Ejemplo

Determinar la cantidad de términos de una progresión aritmética donde el valor del término $a_1 = 4$ y el del término $a_7 = 34$, además de que el valor de la diferencia común es $d = 5$.

Solución

Como $n = \left(\dfrac{a_n - a_1}{d}\right) + 1$, si se sustituyen los valores dados, entonces se tiene que:

$$\begin{aligned} n &= \left(\frac{34-4}{5}\right) + 1 \\ &= 6 + 1 \\ &= 7 \end{aligned}$$

De este modo, la progresión aritmética resultante es:

$$\{a_n\} = \{4, 9, 14, 19, 24, 29, 34, \ldots\}$$

Asimismo, también es posible calcular cualquier término a_n en función de otro término cualesquiera a_k, siempre y cuando dicho término sea anterior a a_n; es decir, $k < n$.

Por ejemplo, sea la progresión aritmética:

$$a_1, a_2, a_3, \ldots, a_{n-1}, a_n$$

De acuerdo con la fórmula explícita para progresiones aritméticas, se tiene que:

$$a_n = a_1 + (n-1)d$$
$$a_k = a_1 + (k-1)d$$

Y si se hace la sustracción de $a_n - a_k$, entonces se tiene que:

$$a_n - a_k = n_d - k_d$$
$$a_n - a_k = (n-k)d$$
$$a_n = a_k + (n-k)d$$

Ahora bien, si ocurriera que $k > n$, es decir, que se buscara algún término en función de otro posterior, se tendría la sustracción en forma invertida; esto es, $a_k - a_n$, y entonces se tendría que:

$$a_n = a_k - (k-n)d$$

Ejemplo

Calcular el valor del término a_9 de una progresión aritmética, sabiendo que el término $a_3 = 1$ y la diferencia común $d = 2$.

Solución

Como $a_n = a_k + (n-k)d$, si se sustituyen los valores dados, entonces se tiene que:

$$a_n = 1 + (9-3)(2)$$
$$= 1 + 12$$
$$= 13$$

De este modo, la progresión aritmética resultante es:

$$\{a_n\} = \{-3, -1, 1, 3, 5, 7, 9, 11, 13, \ldots\}$$

Suma de términos de progresiones aritméticas

Supóngase que $a_1, a_2, a_3, \ldots$ es una progresión aritmética y sea:

$$A_n = a_1 + a_2 + a_3 + \cdots + a_{n-1} + a_n$$

Entonces, debe hacerse esta suma dos veces, una de ida y otra de vuelta, y después hay que sumar término a término:

$$\begin{array}{ccccccccccc} A_n & = & a_1 & + & a_2 & + & \cdots & + & a_{n-1} & + & a_n \\ A_n & = & a_n & + & a_{n-1} & + & \cdots & + & a_2 & + & a_1 \\ \hline 2A_n & = & (a_1 + a_n) & + & (a_2 + a_{n-1}) & + & \cdots & + & (a_{n-1} + a_2) & + & (a_n + a_1) \end{array}$$

En este caso, cada par de elementos resultantes tiene la misma suma, es decir:

$$(a_1 + a_n)$$

Además, también véase que:

$$(a_2 + a_{n-1}) = a_1 + d + a_{n-1} - d = a_1 + a_n$$

Como hay n adiciones, entonces:

$$A_n = \frac{n}{2}(a_1 - a_n)$$

A esta fórmula se le conoce como **fórmula de suma para una progresión aritmética**.

Ejemplo

Determinar la suma de los términos de la siguiente progresión aritmética:

$$1 + 2 + 3 + \cdots + 100$$

Solución

Aquí $n = 100$, $a_1 = 1$ y $a_n = 100$. Por tanto:

$$\begin{aligned} A_{100} &= 1 + 2 + 3 + \cdots + 100 \\ &= \frac{100}{2}(1 + 100) \\ &= (50)(51) \\ &= 5\ 050 \end{aligned}$$

Otro buen ejemplo sería el siguiente:

Nota

El resultado anterior también puede obtenerse con facilidad en la siguiente fórmula inductiva:

$$\frac{n(n+1)}{2}$$

Antes, por inducción matemática, se demostró que esta fórmula era válida para cualquier valor de n. (Para recordar la demostración, véase el capítulo 2.)

Ejemplo

Calcular la suma de los primeros 350 términos de la progresión aritmética:

$$1 + 3 + 5 + \cdots + (2n - 1)$$

Solución

Para calcular a_n, primero se utiliza la fórmula explícita:

$$a_n = a_1 + (n - 1)\,d$$

Donde $n = 350$, $d = 2$ y $a_1 = 1$; entonces:

$$a_{350} = 1 + (349)2 = 699$$

Por último, utilizando la fórmula de suma con $n = 350$, se tiene que:

$$\begin{aligned} A_{350} &= 1 + 3 + 5 + \cdots + 699 \\ &= \frac{350}{2}(1 + 699) \\ &= (175)(700) \\ &= 122\,500 \end{aligned}$$

Propiedad de los términos equidistantes de una progresión aritmética

Sea la progresión aritmética:

$$a_1, a_{1+1}, a_{1+2}, \ldots, a_{1+k}, \ldots, a_{n-k}, \ldots, a_{n-2}, a_{n-1}, a_n$$

donde los términos:

$$a_{1+k} \text{ y } a_{n+k}$$

son dos términos equidistantes, respectivamente, de:

$$a_1 \text{ y } a_n$$

Por la fórmula explícita para progresiones aritméticas, se tiene que:

$$a_{1+k} = a_1 + kd$$

$$a_{n-k} = a_n - kd$$

Ahora bien, si se suman los términos de las ecuaciones anteriores se tiene que:

$$a_{1+k} + a_{n-k} = a_1 + a_n$$

lo cual significa que la suma de dos términos equidistantes de los extremos es igual a la suma de los dos términos extremos.

Ejemplo

En una progresión aritmética se sabe que los términos $a_1 = -2$, $a_{32} = 91$ y $a_{16} = 43$.

Determinar el valor del término a_{17}.

Solución

Primero, se tiene que $1 + 32 = 16 + 17 = 33$, entonces se dice que los términos a_{16} y a_{17} son equidistantes de los extremos; por la propiedad de los términos equidistantes se tiene que:

$$a_1 + a_{32} = a_{16} + a_{17}$$
$$-2 + 91 = 43 + a_{17}$$
$$a_{17} = 46$$

Además, también es posible encontrar el valor de la diferencia común d; esto es:

$$\begin{aligned} d &= \frac{a_n - a_1}{n-1} \\ &= \frac{91-(-2)}{32-1} \\ &= \frac{93}{31} \\ &= 3 \end{aligned}$$

Que se verifica con los términos a_{16} y a_{17}.

Interpolación de medios aritméticos

En primera instancia, podemos decir que la palabra interpolar equivale a intercalar o insertar; pero, tratándose de términos de una progresión aritmética, significa situar o intercalar dichos términos entre otros dos.

Entonces, interpolar uno o más términos, llamados **medios aritméticos**, entre otros dos términos dados, es determinar los términos que hacen falta en una progresión aritmética, de la cual uno de estos debe ser el primer término a_1 y el otro debe ser el último a_n, intercalando tantos términos intermedios como número de términos que se quiera interpolar.

Si se quiere interpolar k medios aritméticos entre a_1 y a_n, basta con calcular la diferencia común de la progresión aritmética que van a formar esos k términos con los a_1 y a_n, en total $n = k + 2$ términos; esto es, los k términos que se desea interpolar más los términos inicial y final a_1 y a_n.

De este modo, en la fórmula:

$$a_n = a_1 + (n-1)d$$

se tiene que despejar el valor de la diferencia común d:

$$a_n - a_1 = (n-1)d$$

$$d = \frac{a_n - a_1}{n-1}$$

La fórmula anterior es correcta cuando no se tiene que interpolar ningún término, pero para un caso de interpolación no funciona, porque en lugar de n, se tienen $k + 2$ términos.

Entonces, en la fórmula para el cálculo del valor de la diferencia común d, se tiene que sustituir n por $k+2$, esto es:

$$d = \frac{a_n - a_1}{(k+2)-1}$$

$$d = \frac{a_n - a_1}{k+1}$$

Ejemplo

Determinar la diferencia común d para interpolar 5 medios aritméticos entre 26 y 80.

Solución

Para calcular d se tiene que:

$$d = \frac{a_n - a_1}{k+1} = \frac{80-26}{5+1} = \frac{54}{6} = 9$$

La progresión aritmética resultante es:

$$\{a_n\} = \{26, 35, 44, 53, 62, 71, 80, \cdots\}$$

Progresiones geométricas

Antes de definir qué es una progresión geométrica, también se analiza primero un ejemplo en el cual aparece una progresión de dicho tipo.

Ejemplo

Escalera de oro de Jacob

En sus sueños, Jacob visualizó una escalera de oro por la que subían y bajaban ángeles. En el sueño de Jacob, el primer escalón de la escalera medía 18 centímetros, pero en adelante cada escalón tenía una altura de 5/4 centímetros más que el anterior. Determinar a qué altura estará el escalón 800 (véase figura 4.4).

Con base en un análisis de la figura 4.4, se tiene que:

$$a_1 = 18$$

$$a_2 = (18)\left(\frac{5}{4}\right)$$

$$a_3 = (18)\left(\frac{5}{4}\right)^2$$

$$a_4 = (18)\left(\frac{5}{4}\right)^3$$

$$\vdots$$

$$a_{800} = (18)\left(\frac{5}{4}\right)^{799}$$

Continúa

De este modo, la altura del escalón 800 es de $(18)\left(\frac{5}{4}\right)^{799}$ centímetros arriba del ras del suelo.

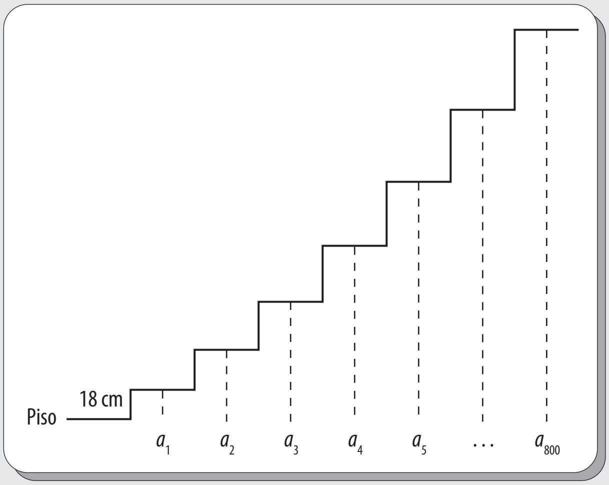


Figura 4.4 Escalera de oro de Jacob.

Como se puede deducir del planteamiento anterior, esta escalera de oro de Jacob es para ángeles y no para humanos. Por tanto, el escalón 800 tiene 4.86×10^{74} kilómetros de alto.

A modo de comparación, podemos decir que el Sol está a 14.88×10^{7} kilómetros de distancia de la Tierra, mientras que Alpha Centauri, la estrella más cercana a la Tierra, está a 4×10^{13} kilómetros de nuestro planeta.

De acuerdo con las dimensiones que alcanza, podemos decir que esta escalera en verdad alcanza el cielo y los límites del universo conocido.

En la sucesión anterior, cada término era $\frac{5}{4}$ centímetros veces más alto que el anterior.

Además, se generó la sucesión siguiente:

$$\{a_n\} = \left\{18, (18)\left(\frac{5}{4}\right), (18)\left(\frac{5}{4}\right)^2, (18)\left(\frac{5}{4}\right)^3, \ldots\right\}$$

la cual, como se ve más adelante, es una progresión geométrica.

A continuación, se consideran las siguientes sucesiones. De nueva cuenta, la idea es detectar el patrón que siguen estas sucesiones y llenar los espacios en blanco de cada una.

$\{a_n\} = \{3, 6, 12, 24, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$
$\{b_n\} = \{12, 4, 4/3, 4/9, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$
$\{c_n\} = \{0.6, 6, 60, 600, \_\_\_\_, \_\_\_\_, \_\_\_\_, \ldots\}$

Aquí tampoco resulta difícil encontrar el valor de dichos términos. El rasgo común de estas tres sucesiones es que en cada caso se puede obtener un término multiplicando el término anterior por un número fijo.

Por tanto, se puede decir que estas sucesiones también son casos de progresiones geométricas; así que es tiempo de definirlas.

Progresiones geométricas

Una progresión geométrica consiste en una sucesión infinita de números, donde cualquier término (distinto del primero) se obtiene luego de multiplicar un número fijo al término anterior.

De este modo, una progresión geométrica, $a_1, a_2, a_3, \ldots$, satisface la fórmula recursiva:

$$a_n = ra_{n-1}$$

donde r es un número fijo llamado razón común.

En esta fórmula, el valor de r también es importante, ya que si:

- es mayor que uno, la progresión es creciente; es decir, cada término es mayor que el anterior.
- está comprendida entre cero y uno, la progresión es decreciente; es decir, cada término es menor que el anterior.
- es igual a uno, la progresión es constante; es decir, tiene todos los términos iguales.
- es menor que cero, la progresión es alterna; es decir, sus términos son alternativamente positivos y negativos.

Además, al dividir cualquier término con el término antecesor se observa que:

$$\frac{a_2}{a_1} = \frac{a_2}{a_1} = \frac{a_2}{a_1} = \cdots = \frac{a_n}{a_{n-1}} = r$$

lo que significa que la razón de cualquier término con su antecesor siempre debe ser el mismo valor, en este caso la razón común r.

Para obtener la fórmula explícita correspondiente se tiene que:

$$\begin{aligned}
a_2 &= r(a_1) \\
a_3 &= r(a_2) = r(r \cdot a_1) = r^2(a_1) \\
a_4 &= r(a_3) = r(r^2 \cdot a_1) = r \geq (a_1) \\
&\vdots \\
a_n &= r^{n-1} \cdot a_1
\end{aligned}$$

En este caso, el exponente de r es uno menos que el subíndice de a.

Esto significa que:

$$a_n = a_1 \cdot r^{n-1}$$

A esta ecuación se le conoce como **fórmula explícita para progresiones geométricas** y con esta se puede calcular un término cualquiera a_n en función del primer término a_1, del total de términos n o número de términos que le precede $n - 1$ y de la razón común r.

Ejemplo

Si se retoman las siguientes progresiones aritméticas:

$\{a_n\} = \{3, 6, 12, 24, \ldots\}$

$\{b_n\} = \{12, 4, \frac{4}{3}, \frac{4}{9}, \ldots\}$

$\{c_n\} = \{0.6, 6, 60, 600, \ldots\}$

Determinar el valor del término 20 en cada caso.

Solución

Si se utiliza la fórmula recursiva, sería necesario determinar los términos de uno en uno, hasta llegar al término 20.

En este caso, primero se determina la fórmula explícita correspondiente, que para cada una sería:

$a_n = (3)(2)^{n-1}$

$b_n = (12)\left(\frac{1}{3}\right)^{n-1}$

$c_n = (0.6)(10)^{n-1}$

Continúa

Ahora bien, una vez que se determinaron dichas fórmulas, resulta muy fácil encontrar el valor de cualquier término de forma independiente.

De este modo, el valor del término 20 en cada caso es:

$a_{20} = (3)(2)^{19}$

$b_{20} = (12)\left(\frac{1}{3}\right)^{19}$

$c_{20} = (0.6)(10)^{19}$

Además de la fórmula explícita, también es posible deducir otros elementos de la progresión geométrica:

El primer término: $a_1 = \dfrac{a_n}{r^{n-1}}$

La razón común: $r = \sqrt[n-1]{\dfrac{a_n}{a_1}}$

La cantidad de términos: $n = \dfrac{\log \dfrac{a_n}{a_1}}{\log r} + 1$

Para una mayor comprensión de este tema, a continuación se analiza un ejemplo de cada elemento que es posible deducir.

Ejemplo

Determinar a_1 de una progresión geométrica donde el término $a_3 = 4$ y la razón común $r = \sqrt{2}$.

Solución

Como $a_1 = \dfrac{a_n}{r^{n-1}}$, al sustituir los valores dados se tiene que:

$$a_1 = \frac{a_3}{r^{3-1}}$$

$$= \frac{4}{\left(\sqrt{2}\right)^2}$$

$$= 2$$

Por tanto, la progresión resultante es:

$$\{a_n\} = \left\{2,\ 2\sqrt{2},\ 4,\ 4\sqrt{2},\ 8,\ 8\sqrt{2},\ \ldots\right\}$$

Ejemplo

Determinar el valor de la razón común r en una progresión geométrica donde los términos $a_1 = 2$ y $a_6 = 64$.

Solución

Como: $r = \sqrt[n-1]{\dfrac{a_n}{a_1}}$

Al sustituir los valores dados, se tiene que:

$$r = \sqrt[5]{\frac{64}{2}}$$

$$= \sqrt[5]{32}$$

$$= 2$$

Por tanto, la progresión resultante es:

$$\{a_n\} = \{2, 4, 8, 16, 32, 64, \ldots\}$$

Ejemplo

Determinar la cantidad de términos de una progresión geométrica donde los términos $a_1 = 1$ y $a_5 = 81$ y la razón común $r = 3$.

Solución

Como:

$$n = \frac{\log \dfrac{a_n}{a_1}}{\log r} + 1$$

Al sustituir los valores dados, se tiene que:

$$n = \frac{\log\left(\dfrac{81}{1}\right)}{\log 3} + 1$$

$$= \frac{\log 81}{\log 3} + 1$$

$$= 4 + 1$$

$$= 5$$

Por tanto, la progresión resultante es:

$$\{a_n\} = \{1, 3, 9, 27, 81, \ldots\}$$

Asimismo, también se puede calcular cualquier término a_n en función de otro término cualquiera a_k, siempre y cuando sea anterior a a_n; es decir, $k < n$.

Sea la progresión geométrica

$$a_1, a_2, a_3, \ldots, a_{n-1}, a_n$$

De acuerdo con la fórmula explícita para progresiones geométricas, se tiene que:

$$a_n = a_1 \cdot r^{n-1}$$
$$a_k = a_1 \cdot r^{k-1}$$

Si se hace la división de $\frac{a_n}{a_k}$, entonces:

$$\frac{a_n}{a_k} = \frac{r^{n-1}}{r^{k-1}}$$

$$\frac{a_n}{a_k} = r^{k-1}$$

$$a_n = a_k \cdot r^{n-k}$$

Ahora bien, si ocurriera que $k > n$; es decir, que se buscara algún término en función de otro posterior, se tendría la división en forma invertida, esto es:

$$\frac{a_k}{a_n}$$

Entonces, se obtendría que:

$$a_k = a_n \cdot r^{n-k}$$

Ejemplo

Determinar el término a_{10} de una progresión geométrica donde el término $a_3 = 4$ y la razón común $r = \sqrt{2}$.

Solución

Como $a_n = a_k \cdot r^{n-k}$, entonces al sustituir los valores dados, se tiene que:

$$\begin{aligned} a_{10} &= a_3 \cdot r^{10-3} \\ &= 4\left(\sqrt{2}\right)^7 \\ &= 32\sqrt{2} \end{aligned}$$

Por tanto, la progresión geométrica resultante es:

$$\{a_n\} = \left\{2,\ 2\sqrt{2},\ 4,\ 4\sqrt{2},\ 8,\ 8\sqrt{2},\ 16,\ 16\sqrt{2},\ 32,\ 32\sqrt{2},\ldots\right\}$$

Suma de términos de progresiones geométricas

Supóngase que $a_1, a_2, a_3,\ldots$ es una progresión geométrica y sea:

$$A_n = a_1 + a_2 + a_3 + \cdots + a_{n-1} + a_n$$

Que puede escribirse como:

$$A_n = a_1 + a_1 r + a_1 r_2 + \cdots + a_1 r^{n-2} + a^1 r^{n-1}$$

Ahora se multiplica A_n por r, se resta el resultado de A_n, y haciendo un poco de álgebra para obtener A_n, se tiene que:

$$\begin{array}{rcccccccccccc} A_n & = & a_1 & + & a_1 r & + & a_1 r^2 & + & \cdots & + & a_1 r^{n-1} & & \\ -\,rA_n & = & & - & a_1 r & - & a_1 r^2 & - & \cdots & - & a_1 r^{n-1} & - & a_1 r^n \\ \hline A_n - rA_n & = & a_1 & + & 0 & + & 0 & + & \cdots & + & 0 & - & a_1 r^n \end{array}$$

Donde se obtiene que:

$$A_n - rA_n = a_1 - a_1 r^n$$

Al factorizar se tiene que:

$$A_n \cdot (1 - r) = a_1 \cdot (1 - r^n)$$

Por último, despejando A_n se obtiene:

$$A_n = \frac{a_1 \cdot \left(1 - r^n\right)}{1 - r}, r \neq 1$$

A esta fórmula se le conoce como **fórmula de suma para una progresión geométrica**.

Ejemplo

Hay una antigua leyenda que dice que cuando el rey de Persia aprendió a jugar ajedrez estaba tan contento que intentó recompensar al inventor.

Luego de que el hombre estuvo ante la presencia del rey, este prometió cumplirle cualquier petición que hiciera. Ante esta oportunidad, el hombre pidió un grano de trigo por el primer cuadro del tablero del ajedrez, dos por el segundo, cuatro por el tercero y así sucesivamente. Es decir, el hombre había pedido $1 + 2 + 2^2 + 2^3 + \cdots + 2^{63}$ granos de trigo.

El rey pronto se dio cuenta que dicha petición nunca podría ser cumplida. A continuación, véase por qué.

Solución

Si $n = 64$, $a_1 = 1$ y $r = 2$, se tiene que:

$$\begin{aligned} A_{64} &= \frac{1(1-2^{64})}{1-2} \\ &= 2^{64} - 1 \\ &\approx 18446744073709600000 \\ &\approx 1.845 \times 10^{19} \end{aligned}$$

Algo así como dieciocho trillones, cuatrocientos cuarenta y seis mil setecientos cuarenta y cuatro billones, setenta y tres mil setecientos nueve millones, seiscientos mil granos de trigo.

Ante tal petición del hombre, el rey sonrió y solo le dio un saco de trigo.

Comentario

Como se puede observar, el resultado del número de granos de trigo está dado por 20 cifras. Por ende, el peso aproximado de semejante cantidad de granos sería 10,000’000,000 toneladas.

Toda la producción mundial de trigo de un siglo no sería suficiente para obtener tal cantidad de granos.

Además, si toda la superficie del planeta fuera cultivada con sembradíos de trigo, aún no llegaría a dar semejante cantidad de trigo en varios años.

Propiedad de los términos equidistantes de una progresión geométrica

Sea la progresión geométrica:

$$a_1, a_{1+1}, a_{1+2}, \dots, a_{1+k}, \dots, a_{n-k}, \dots, a_{n-2}, a_{n-1}, a_n$$

donde los términos:

$$a_{1+k} \text{ y } a_{n-k}$$

son dos términos equidistantes, respectivamente, de:

$$a_1 \text{ y } a_n$$

Por la fórmula explícita para progresiones geométricas se tiene que:

$$a_{1+k} = a_1 \cdot r^k$$
$$a_{n-k} = a_n \cdot r^{-k}$$

Y si se suman término a término las ecuaciones anteriores, se tiene que:

$$a_{1+k} + a_{n-k} = a_1 \cdot a_n$$

lo que significa que el producto de dos términos equidistantes de los extremos es igual al producto de los dos términos extremos.

Ejemplo

En una progresión geométrica se sabe que los términos $a_1 = 6$, $a_{12} = 0.0029296875$ y $a_6 = 0.1875$.

Determinar el valor del término a_7.

Solución

Primero, se tiene que:

$6 + 7 = 1 + 12 = 13$

Entonces, los términos a_6 y a_7 son equidistantes de los extremos, y por la propiedad de los términos equidistantes se tiene que:

$a_6 \cdot a_7 = a_1 \cdot a_{12}$

$(0.1875) \cdot a_7 = (6)(0.0029296875)$

$a_7 = 0.09375$

Así, la progresión resultante sería:

$\{a_n\} = \{6, 3, 1.5, 0.75, 0.375, 0.1875, 0.09375, \ldots\}$

Además, también se podría encontrar el valor de la razón común r; esto es:

$$\begin{aligned} r &= \sqrt[n-1]{\frac{a_n}{a_1}} \\ &= \sqrt[11]{(0.0029296875)/6} \\ &= \sqrt[11]{0.00048828125} \\ &= 0.5 \end{aligned}$$

que se verifica con los términos a_6 y a_7.

Producto P_n de términos de progresiones geométricas

Sea la progresión geométrica:

$$a_1, a_2, a_3, \cdots, a_{n-2}, a_{n-1}, a_n$$

Entonces, el producto de todos los términos de dicha progresión sería:

$$P_n = a_1 \cdot a_2 \cdot a_3 \cdot, \cdots, \cdot a_{n-2} \cdot a_{n-1} \cdot a_n \qquad \text{(i)}$$

Además, como el orden de los factores no altera el producto, también es posible decir que:

$$P_n = a_n \cdot a_{n-1} \cdot a_{n-2} \cdot, \cdots, \cdot a_3 \cdot a_2 \cdot a_1 \qquad \text{(ii)}$$

Ahora bien, teniendo en cuenta la propiedad de los términos equidistantes de una progresión geométrica, si se multiplican (i) y (ii) y después se multiplican término a término, se tiene que:

$$\begin{array}{ccccccc} P_n & = & a_1 \cdot a_2 & \cdot & \cdots & \cdot & a_1 \cdot r^{n-1} \\ P_n & = & a_n \cdot a_{n-1} & \cdot & \cdots & \cdot & a_1 \cdot r^{n-1} \\ \hline P_n^2 & = & (a_1 \cdot a_n) \cdot (a_2 \cdot a_{n-1}) & \cdot & \cdots & \cdot & (a_{n-1} \cdot a_2) \cdot (a_n \cdot a_1) \end{array}$$

Lo cual es lo mismo que:

$$P_n = \frac{(a_1 \cdot a_n) \cdot (a_1 \cdot a_n) \cdot \cdots \cdot (a_1 \cdot a_n)}{n \text{ factores}}$$

Es decir:

$$P_n^2 = (a_1 \cdot a_n)^n$$

O bien:

$$P_n = \sqrt{(a_1 \cdot a_n)^n}$$

Esta igualdad también puede expresarse como:

$$
\begin{aligned}
P_n &= \sqrt{(a_1 \cdot a_n)^n} \\
&= \sqrt{(a_1 \cdot a_1 r^{n-1})^n} \\
&= \sqrt{a_1^{2n} \cdot r^{n(n-1)}} \\
&= a_1^n \cdot r^{\frac{n(n-1)}{2}}
\end{aligned}
$$

que da el valor de P_n, en función de a_1, r y n.

Ejemplo

Sea la progresión geométrica:

$$1, 2, 4, 8, 16, 32$$

Determinar el producto de sus términos.

Solución

Como en este caso son pocos los términos, se puede hacer la multiplicación de forma manual y luego comprobarla con la fórmula respectiva.

El producto de dichos términos es:

$$1 \times 2 \times 4 \times 8 \times 16 \times 32 = 32\,768$$

Al aplicar la fórmula del producto de términos de una progresión geométrica, se tiene que:

$$
\begin{aligned}
P_n &= \sqrt{(a_1 \cdot a_n)^n} \\
P_n &= \sqrt{(1 \cdot 64)^6} \\
&= \sqrt{(64)^6} \\
&= 64^3 \\
&= 32\ 768
\end{aligned}
$$

con lo cual se comprueba que es el mismo resultado.

Otro ejemplo sería:

Ejemplo

Sea la progresión geométrica:

$$1, 3, 9, \ldots, 59\,049, 177\,147, 531\,441$$

Determinar el producto de sus términos.

Solución

Primero, hay que determinar el valor de n para poder utilizar la fórmula para el producto de términos de una progresión geométrica.

Luego, para calcular el valor de n, es decir, la cantidad de términos de la sucesión, se tiene la fórmula vista antes:

$$n = \frac{\log \frac{a_n}{a_1}}{\log r} + 1 \qquad \text{(i)}$$

Continúa

Para aplicar esta fórmula, primero se requiere el valor de r, el cual puede obtenerse con dos términos consecutivos. Entonces:

$$r = \frac{9}{3}$$
$$= 3$$

Ahora, al sustituir este valor en la expresión (i) se tiene que:

$$n = \frac{\log\left(\frac{531\ 441}{1}\right)}{\log 3} + 1$$

$$= \frac{\log 531\ 441}{\log 3} + 1$$
$$= 12 + 1$$
$$= 13$$

Una vez que ya se obtuvo el valor de n, es posible utilizar la fórmula para calcular el producto de términos de una progresión geométrica. Entonces:

$$P_n = \sqrt{(a_1 \cdot a_n)^n}$$

Sustituyendo de a_1, a_n y n, se tiene que:

$$= \sqrt{(1 \cdot 531\ 441)^{13}}$$
$$\approx 1.64 \times 10^{37}$$

Asimismo, también puede calcularse con la fórmula:

$$P_n = a_1^n \cdot r^{\frac{n(n-1)}{2}}$$

donde, al sustituir los valores de a_1, r y n, se obtiene:

$$= 1^{13} \cdot 3^{((13)(12))/2}$$
$$= 3^{78}$$
$$\approx 1.64 \times 10^{37}$$

cuyo resultado, como se puede observar, es el mismo valor obtenido antes.

El valor exacto del producto de los términos de la progresión geométrica es:

16’423,203’268,260’658,146’231,467’800,709’255,289

Interpolación de medios geométricos

Como en el caso de las progresiones aritméticas, también es posible la interpolación de uno o más términos, denominados ***medios geométricos***, en una progresión geométrica entre dos términos dados: el término inicial a_1 y el final a_n de una progresión geométrica.

Si se quiere interpolar k medios geométricos entre a_1 y a_n, primero se debe calcular la razón común r de la progresión geométrica que van a formar esos k términos con los a_1 y a_n, en total $n = k + 2$ términos; esto es, los k términos que se desean interpolar más los términos inicial y final, a_1 y a_n respectivamente.

Antes, ya se obtuvo la fórmula siguiente:

$$r = \sqrt[n-1]{\frac{a_n}{a_1}}$$

Esta fórmula es correcta cuando no es necesario interpolar ningún término; no obstante, para el caso de interpolación no funciona, porque en lugar de n términos, se tienen $k+2$.

Por tanto, en la fórmula para el cálculo del valor de d se debe sustituir n por $k+2$; esto es:

$$\begin{aligned} r &= \sqrt[(k+2)-1]{\frac{a_n}{a_1}} \\ &= \sqrt[k+1]{\frac{a_n}{a_1}} \end{aligned}$$

Ejemplo

Determinar la razón común r para interpolar 8 medios geométricos entre 11 y 5 632.

Solución

Para calcular r se tiene que:

$$\begin{aligned} r &= \sqrt[k+1]{\frac{a_n}{a_1}} \\ &= \sqrt[10+1]{\frac{5\,632}{11}} \\ &= \sqrt[9]{512} \\ &= \sqrt[9]{2^9} \end{aligned}$$

Y la progresión geométrica resultante es:

$\{a_n\} = \{11, 22, 44, 88, 176, 352, 704, 1\,048, 2\,816, 5\,632, \ldots\}$

Suma de los términos de una progresión geométricacuando la razón común *r* es menor que 1 y el número de términos es infinito

Si a la fórmula:

$$A_n = \frac{a_1 \cdot (1-r^n)}{1-r}$$

se le cambia el orden en el que se han colocado los valores del numerador y el denominador, el resultado no cambia.

Esto significa que:

$$A_n = \frac{a_1 \cdot (1-r^n)}{1-r}$$

Es lo mismo que:

$$A_n = \frac{a_1 \cdot (r^n-1)}{r-1}$$

Los valores de A_n son iguales porque si la razón común r es mayor que 1, tanto el numerador como el denominador serían negativos, pero el cociente de dos números negativos será positivo.

Si la razón común r es menor que 1, tanto el numerador como el denominador serán positivos, al igual que el cociente.

Nota

No hay que olvidar que se está tratando el caso en que el número de términos es ∞ (infinito) y la razón común r es menor que la unidad.

Obsérvese que la operación $\frac{34-21}{7}$ también puede escribirse como $\frac{34}{7} - \frac{21}{7}$, y el resultado es el mismo.

Lo mismo que para dividir una suma o diferencia indicada por un número, se divide cada término por el denominador o divisor.

Esto quiere decir que:

$$A \;= \frac{a_1 \cdot (r^n-1)}{}$$

puede escribirse como:

$$A_n = \frac{a_1 \cdot r^n - a_1}{r-1}$$
$$= \frac{a_1 \cdot r^n}{r-1} - \frac{a_1}{r-1}$$

Un número menor que 1 es una fracción de la unidad, como: $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{7}$, etcétera.

Si la razón común $r = \frac{1}{5}$, y este valor se eleva a infinito, se tiene que:

$$\frac{1}{5}^{\infty} = \frac{1^{\infty}}{5^{\infty}}$$

Como se puede observar, el numerador vale 1 (sin tener en cuenta las indeterminaciones), mientras que el denominador vale infinito.

Esto es como dividir 1 entre un número extremadamente grande, digamos 123’456,789’000,000’000,000’000,000 y todavía no se llega ni remotamente a ∞. El cociente sería algo como:

$$0{,}000000000000000000000000000000000009\ldots$$

Que en realidad sería cero.
Luego de la igualdad:

$$A_n = \frac{a_1 \cdot r^n - a_1}{r-1}$$
$$= \frac{a_1 \cdot r^n}{r-1} - \frac{a_1}{r-1}$$

Se observa que:

$$\frac{a_1 \cdot r_n}{r-1} = 0$$

Debido a que $r^n = 0$, el producto de este valor multiplicado por a_1 también será cero. Pero, si a 0 lo dividimos por cualquier valor que no sea cero, es posible afirmar que el cociente también vale cero, con lo cual la fórmula para el cálculo de la suma de infinitos términos quedaría como sigue:

$$A_n = -\frac{a_1}{r-1}$$

O bien:

$$A_n = \frac{a_1}{1-r}$$

Ejemplo

Calcular la suma de los 100 mil millones de términos de la progresión:

$$\{a_n\} = \frac{1}{3}, \frac{1}{9}, \frac{1}{21}, \frac{1}{81}, \ldots$$

Solución

En este caso, primero es necesario determinar la razón común r:

$$r = \frac{\frac{1}{9}}{\frac{1}{3}}$$
$$= \frac{3}{9}$$
$$= \frac{1}{3}$$

Continúa

Entonces, la suma de los términos infinitos será:

$$
\begin{aligned}
A_n &= \frac{a_1}{1-r} \\
&= \frac{\frac{1}{3}}{1-\frac{1}{3}} \\
&= \frac{\frac{1}{3}}{\frac{3}{3}-\frac{1}{3}} \\
&= \frac{\frac{1}{3}}{\frac{2}{3}} \\
&= \frac{1}{2}
\end{aligned}
$$

4.3 Relación de recurrencia y sucesión de recurrencia

Con frecuencia, es posible desarrollar relaciones entre los elementos de una sucesión, las cuales reciben el nombre de **relaciones de recurrencia**. A continuación, se ilustra el concepto con un ejemplo y luego se ofrece una definición más formal.

Ejemplo

Una persona invierte 10 000 pesos a una tasa de 15% de interés compuesto anual. Si A_n representa el monto de cada n años.

Determinar una relación entre A_n y A_{n-1}.

Solución

Al cabo de $n - 1$ años el monto será A_{n-1}. Esto es, después de un año más se tendrá la cantidad de A_{n-1} más el interés del año, entonces:

$$
\begin{aligned}
A_n &= A_{n-1} + (0.15)\, A_{n-1} \\
&= 1.15\, A_{n-1}
\end{aligned}
$$

El valor inicial $A_0 = 10\,000$, junto con la ecuación anterior, permiten calcular el valor de $A_n\ \forall n$. Por ejemplo:

$$
\begin{aligned}
A_3 &= 1.15\,(A_2) \\
&= (1.15)\,(1.15)\,(A_1) \\
&= (1.15)\,(1.15)\,(1.15)\,(A_0) \\
&= (1.15)^3\,(10\,000) \\
&= 15\,208.75
\end{aligned}
$$

Por tanto, al final del tercer año, la cantidad sería de 15 208.75 pesos.

En este caso, se puede efectuar el cálculo para cualquier valor de n y se obtiene:

$$
\begin{aligned}
A_n &= 1.15\,(A_{n-1}) \\
&= (1.15)\,(1.15)\,(A_{n-2}) = (1.15)^2\,(A_{n-2}) \\
&= (1.15)^2\,(1.15)\,(A_{n-3}) = (1.15)^3\,(A_{n-3}) \\
&\ \ \vdots
\end{aligned}
$$

Continúa

$$= (1.15)^{n-2}(A_2)$$
$$= (1.15)^{n-1}(A_2)$$
$$= (1.15)^{n}(10\,000)$$

Así que si se quiere saber la cantidad resultante al cabo de 20 años, entonces:

$$(1.15)^{20}(10\,000) = 163\,665.37$$

Resultado con base en la fórmula obtenida antes.

La ecuación $A_n = (1.15)A_{n-1}$ proporciona un ejemplo de una relación de recurrencia. Y dicha relación define una progresión geométrica dando el n-ésimo valor en términos de uno antecesor.

Hasta aquí hemos trabajado con el concepto de relación de recurrencia; sin embargo, aún no se ha dado una definición formal, así que es momento de hacerlo.

Relación de recurrencia

Una relación de recurrencia para una sucesión $a_0, a_1, a_2, \ldots, a_n$, constituye una ecuación que relaciona a a_n con algunos de sus antecesores:

$$a_0, a_1, a_2, \ldots, a_{n-1}$$

Además, se llaman valores iniciales a los dados en forma explícita:

$$a_0, a_1, a_2, \ldots, a_{n-1}$$

Los cuales son necesarios para empezar a calcular los términos de la sucesión, mediante el uso de la relación de recurrencia.

Sucesión de recurrencia

La sucesión originada por la relación de recurrencia junto con los valores iniciales se conoce como **sucesión de recurrencia** o **sucesión recurrente**.

Ejemplo

Una de las más antiguas relaciones de recurrencia define la sucesión de recurrencia conocida como sucesión de Fibonacci.

Esta sucesión se encuentra por primera vez en el libro de este autor, *Liber abaci*, donde él se preguntó lo siguiente:

Nota

¿Cuántas parejas de conejos habrá después de un año, si al comienzo solo hay una pareja, y sabemos que cada pareja produce al mes una nueva pareja, la cual se vuelve productiva al mes? Se da por sentado que no ocurren muertes y que la pareja inicial es recién nacida.

Solución

Sea fib_1 el número de parejas de conejos al cabo del i-ésimo mes. Como al inicio solo hay una pareja de conejos, entonces:

$$fib_0 = 1 \qquad (i)$$

Continúa

Y como al final del primer mes sigue habiendo solo una pareja, ya que comienza a ser productiva al cabo de este tiempo, se tiene que:

$$fib_1 = 1 \qquad (ii)$$

En este caso, las ecuaciones (i) y (ii) constituyen los valores iniciales para la sucesión de Fibonacci. El aumento en las parejas de conejos fib_{n-1}, fib_n, del mes ($n-1$) al mes (n) se debe a que cada pareja viva del mes ($n-2$) produce una pareja adicional.

Esto es:

$$fib_n - fib_{n-1} = fib_{n-2},$$

O

$$fib_n = fib_{n-1} + fib_{n-2} \qquad (iii)$$

La relación de recurrencia (iii), con los valores iniciales (i) y (ii), define la sucesión de Fibonacci.

Véase la figura 4.5, la cual muestra lo que ocurre con los conejos hasta el mes cuatro.

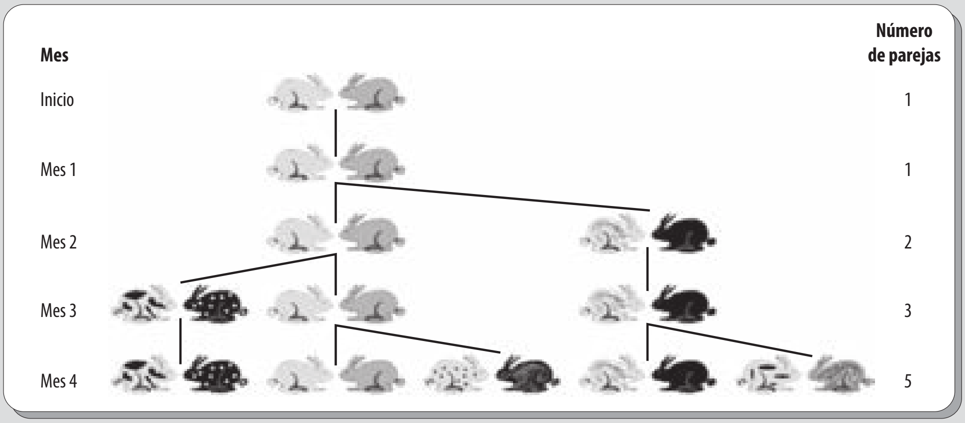


Figura 4.5 Primeros cuatro meses del crecimiento de conejos.

De acuerdo con lo que se planteó, es necesario completar hasta el término fib_{12}, para conocer la cantidad de conejos que se tendrían al cabo de un año:

$$fib_0 = fib_1 = 1$$
$$fib_2 = fib_1 + fib_0 = 1 + 1 = 2$$
$$fib_3 = fib_2 + fib_1 = 2 + 1 = 3$$
$$fib_4 = fib_3 + fib_2 = 3 + 2 = 5$$
$$fib_5 = fib_4 + fib_3 = 5 + 3 = 8$$
$$fib_6 = fib_5 + fib_4 = 8 + 5 = 13$$
$$fib_7 = fib_6 + fib_5 = 13 + 8 = 21$$
$$fib_8 = fib_7 + fib_6 = 21 + 13 = 34$$
$$fib_9 = fib_8 + fib_7 = 34 + 21 = 55$$
$$fib_{10} = fib_9 + fib_8 = 55 + 34 = 89$$
$$fib_{11} = fib_{10} + fib_9 = 89 + 55 = 144$$
$$fib_{12} = fib_{11} + fib_{10} = 144 + 89 = 233$$

Esto significa que después de un año se tienen 233 parejas de conejos.

Leonardo de Pisa, Leonardo Pisano o Leonardo Bigollo, también conocido como Fibonacci, matemático italiano del siglo XIII, fue el primero en describir la sucesión matemática que lleva su nombre. Hacia 1202, Fibonacci ya hablaba de dicha sucesión cuando publicó su *Liber abaci* (*Libro del ábaco* o *Libro del cálculo*).

Algunos de sus principales aportes se refieren a la geometría, la aritmética comercial y los números irracionales, además de haber sido vital para el desarrollo del concepto del cero.

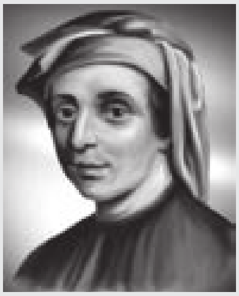


Figura 4.6 Leonardo de Pisa, Leonardo Pisano o Leonardo Bigollo, también conocido como Fibonacci (1170-1250).

La sucesión de Fibonacci es la base para construir una sucesión de cuadrados adyacentes, como la que se muestra en la figura 4.7, cuyos lados miden los números de Fibonacci y se adhieren unos con otros en el sentido del giro de las agujas del reloj.

Como se puede observar, dentro de esa sucesión de cuadrados se pueden ir trazando de manera continua cuadrantes de circunferencia que dan lugar a una bonita espiral llamada ***espiral de Fibonacci***.

Es sorprendente ver cómo la **espiral de Fibonacci** aparece de manera recurrente en la naturaleza; así, puede observarse:

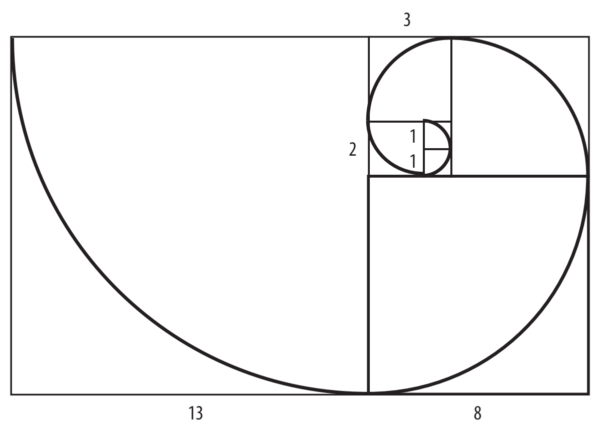


Figura 4.7 Espiral de Fibonacci.

a) Al contar las escamas de una piña (véase figura 4.8). Tras observar este fruto, es posible distinguir que aparecen espirales alrededor del vértice, en igual número a los términos citados en la sucesión de Fibonacci.
b) En las piñas del girasol (véase figura 4.9). En estas se forma una red de espirales, donde unas van en el sentido de las agujas del reloj y otras en sentido contrario; aunque, en cualquiera de los casos, las cantidades de unas y de otras siempre son los términos consecutivos de la sucesión de Fibonacci.
c) En las ramas de los árboles, en la flor de la alcachofa, en el arreglo de un cono o en la disposición de las hojas en el tallo. Solo hay que tener en cuenta que en estos casos se distribuyen buscando la luz del Sol (véase figura 4.10).

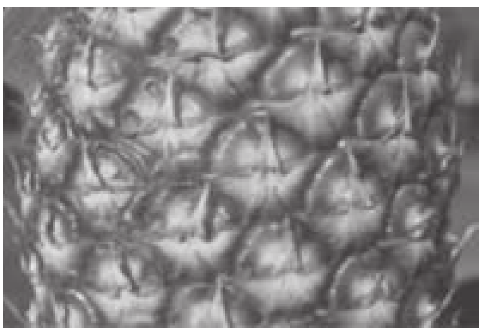


Figura 4.8 Escamas de una piña.

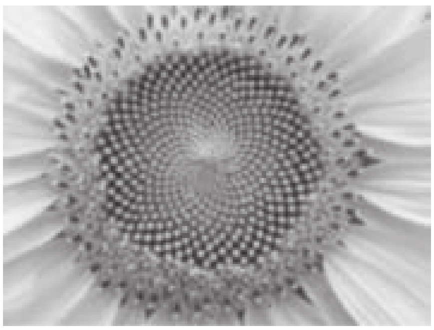


Figura 4.9 Piña de un girasol.

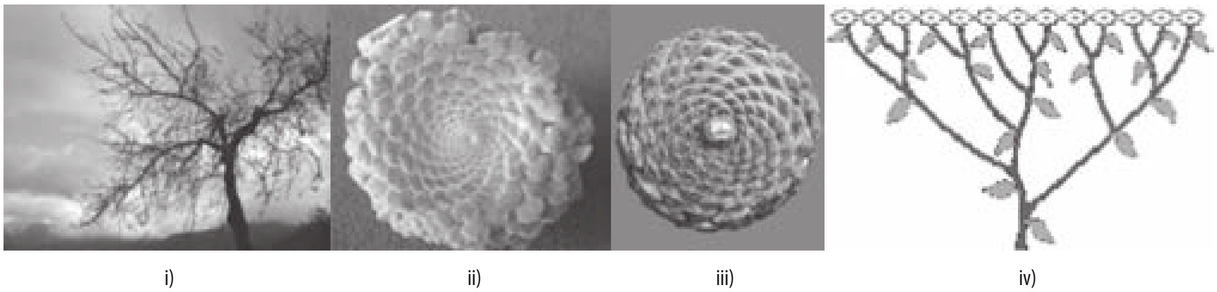


Figura 4.10 Espiral de Fibonacci en la naturaleza. i) Ramas de un árbol; ii) flor de la alcachofa; iii) arreglo de un cono; iv) disposición de la hojas de un tallo.

d) El número de espirales en numerosas flores y frutos también se ajusta a parejas consecutivas de términos de esta sucesión (véase figura 4.11).

e) También está presente en los huracanes (véase figura 4.12 i), en algunas galaxias (véase figura 4.12 ii) y en las conchas tipo caracoles, entre otras (véase figura 4.12 iii).

f) En algunas partes del cuerpo de los seres humanos y de los animales, como en el caso de la relación entre la altura de un ser humano y la altura de su ombligo, la relación entre la distancia del hombro y sus dedos y la distancia del codo a los dedos o la relación entre las articulaciones de las manos y los pies (véase figura 4.13).

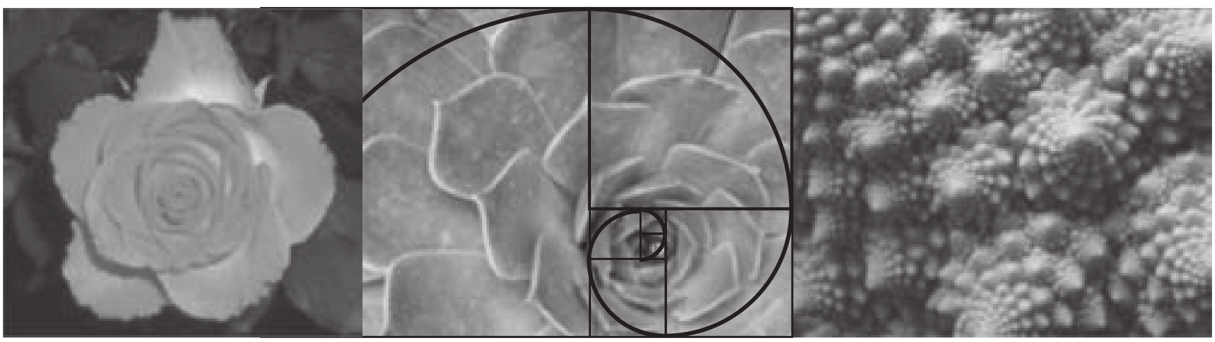


Figura 4.11 La espiral de Fibonacci en diversos flores y frutos.

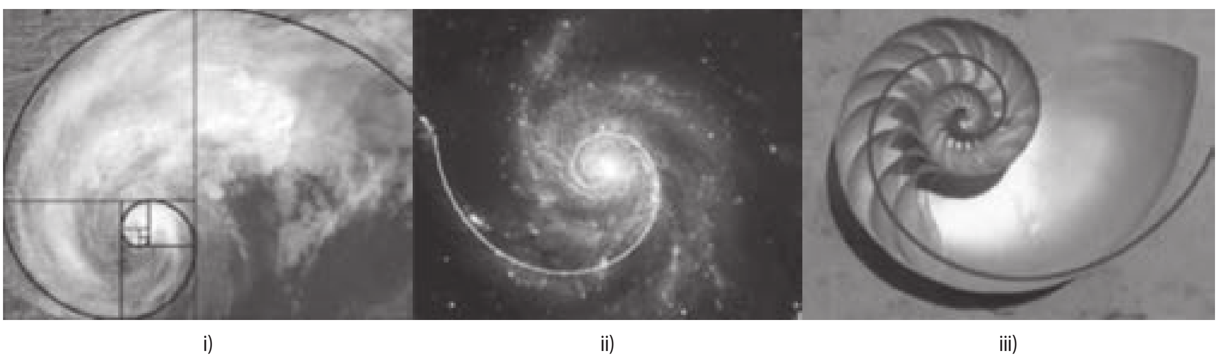


Figura 4.12 La espiral de Fibonacci de nuevo en la naturaleza.

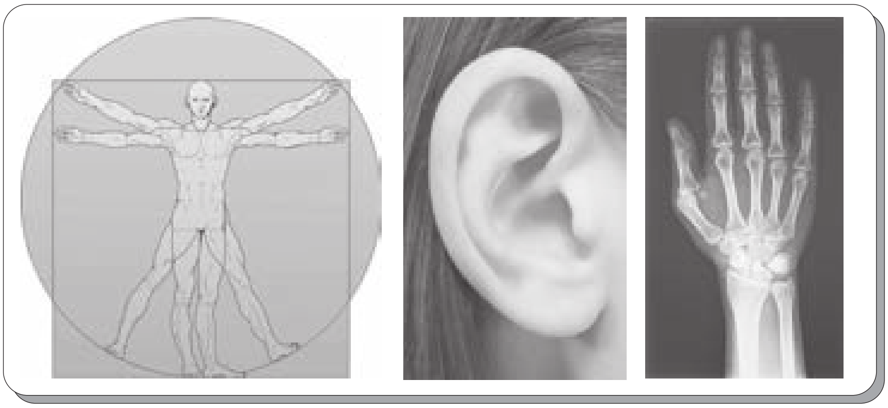
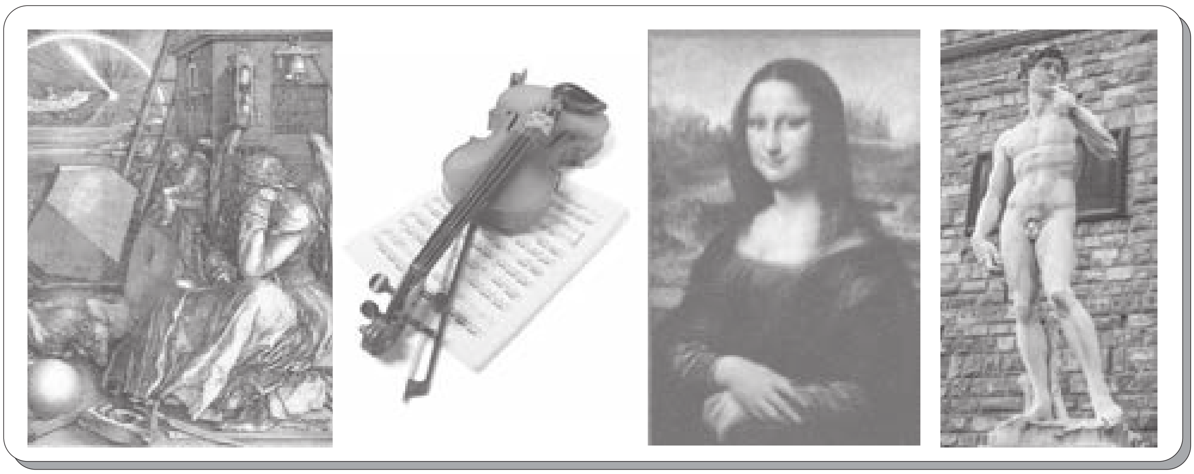


Figura 4.13 La espiral de Fibonacci en partes corporales de los seres humanos.

g) La espiral de Fibonacci también está presente en el arte, como en los violines; en estos, se pueden ver en la ubicación de las efes (los "oídos" u orificios en la tapa) (véase figura 4.14 i). Además, también aparece en las relaciones entre altura y ancho de los objetos y las personas que aparecen en las obras de Miguel Ángel (véase figura 4.14 ii), Durero (véase figura 4.14 iii) y Da Vinci (véase figura 4.14 iv), entre otros.



Otro problema interesante donde aparecen las relaciones de recurrencias es el siguiente.

Ejemplo

Problema de las torres de Hanói

Considérese que se tienen n discos y 3 torres. Los discos están apilados en la torre 1, ordenados de mayor a menor (véase figura 4.15).

El objetivo es pasar los discos uno por uno a la torre 3, colocados en el orden original. No obstante, en el proceso no se permite que un disco mayor se coloque sobre otro menor.

Si a_n es el número de movimientos que se requieren para pasar los disco de la torre 1 a la torre 2, determinar la relación de recurrencia para calcular a_n.

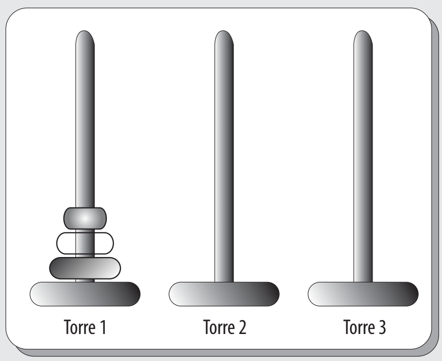


Figura 4.15 Juego de las torres de Hanói.

Solución

Para mover n discos basta con mover $n-1$ discos a una torre libre, mover el disco mayor a la otra torre libre y mover de nuevo los $n-1$ discos sobre el disco mayor.

Por tanto, a_n cumple la relación de recurrencia:

$$a_n = 2 \cdot a_{n-1} + 1$$

En este caso, hace falta un valor inicial, por lo que aquí se va a considerar que $a_1 = 1$, ya que para un único disco se tiene que efectuar solo un movimiento. De acuerdo con la relación de recurrencia y el valor inicial, se tiene que:

$$\begin{aligned}
a_1 &= 1 \\
a_2 &= 2 \cdot a_1 = 2(1) + 1 = 3 \\
a_3 &= 2 \cdot a_2 = 2(3) + 1 = 7 \\
a_4 &= 2 \cdot a_3 = 2(7) + 1 = 15 \\
a_5 &= 2 \cdot a_4 = 2(15) + 1 = 31 \\
&\vdots
\end{aligned}$$

Para comprobar en forma gráfica que la relación anterior es correcta, a continuación se ve el caso donde $n = 3$; es decir, cuando se tienen tres discos, lo que implica que deben utilizarse solo 7 movimientos para pasar los discos de la torre 1 a la torre 3, como se observa en la figura 4.16.

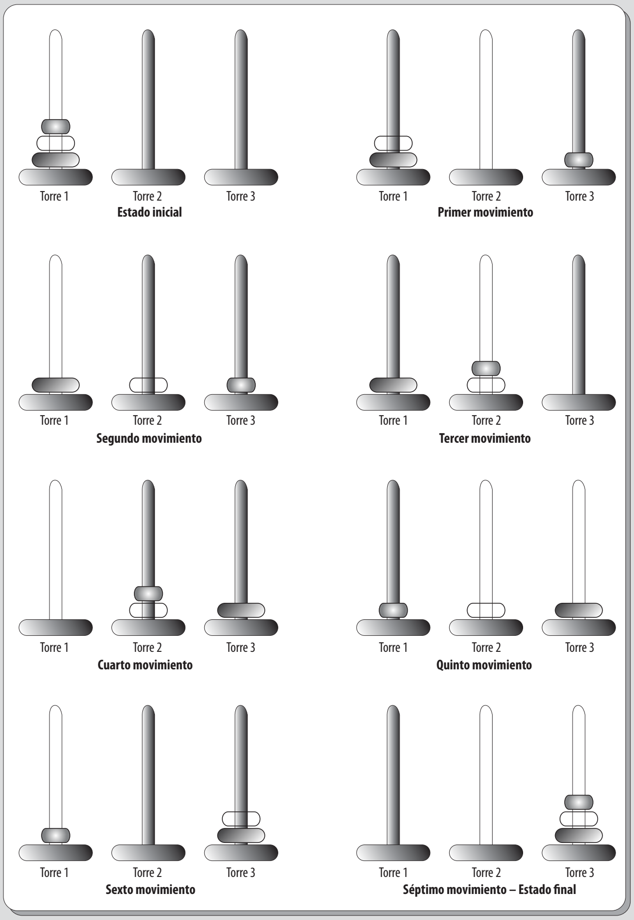


Figura 4.16 Movimientos de las torres de Hanói para 3 discos.

François Édouard Anatole Lucas fue un importante matemático francés, reconocido sobre todo por sus trabajos sobre la serie de Fibonacci y por el test de primalidad que lleva su nombre. Asimismo, también fue el creador de algunos juegos recreativos matemáticos, como el de las torres de Hanói.

No obstante, es reconocido principalmente por su estudio de las llamadas sucesiones generalizadas de Fibonacci, las cuales comienzan por dos enteros positivos cualesquiera y, a partir de ahí, cada número de la sucesión es la suma de los dos predecesores. La sucesión más sencilla es la conocida como **sucesión de Fibonacci**: 1, 1, 2, 3, 5, 8, 13, 21, …; y quizá la inmediatamente más sencilla es: 1, 3, 4, 7, 11, 18, … , la cual es conocida como **sucesión de Lucas**.

Figura 4.17 François Édouard Anatole Lucas, matemático francés (1842-1891).

Un ejemplo interesante aplicado a la geometría es el que se analiza a continuación:

Ejemplo

Se quiere determinar el número de regiones en las cuales queda dividido un plano al trazar en este n rectas, de forma que estas se corten de dos en dos, y de tal manera que tres rectas no tengan un punto común.

Si a_n es el número total de regiones, encontrar una relación de recurrencia para calcular a_n.

Solución

Los cuatro primeros casos de división del plano, con las condiciones mencionadas, se observan en la figura 4.18.

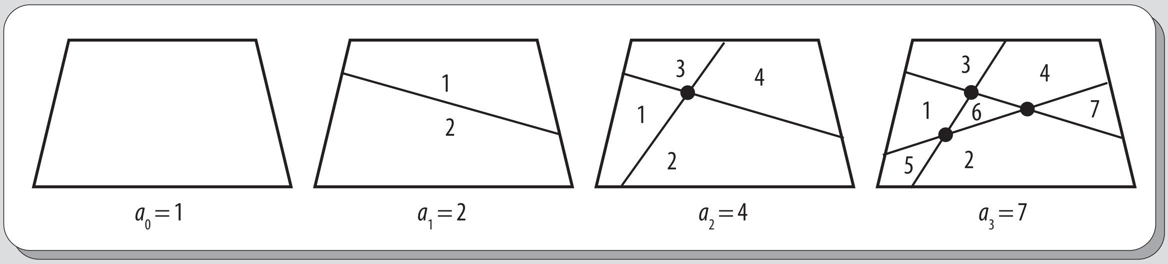


Figura 4.18 División del plano.

Como se puede observar, el caso $a_0 = 1$ es trivial. Mientras que en los demás casos, es decir, cuando $n \geq 1$, se observa que la n-ésima recta corta a las otras en $n-1$ puntos distintos; por tanto, la n-ésima recta quedará dividida en n segmentos distintos, cada uno de los cuales divide, a su vez, a las regiones obtenidas, en el caso inmediato anterior, en dos partes.

Como consecuencia, la relación de recurrencia que se obtiene es:

$$a_n = a_{n-1} + n$$

Sin embargo, en esta hace falta un valor inicial, el cual se obtiene del caso trivial antes mencionado.

Así, de acuerdo con la relación de recurrencia y el valor inicial, se tiene que:

$$\begin{aligned}
&a_0 = 1\\
&a_1 = a_0 + 1 = 1 + 1 = 2\\
&a_2 = a_1 + 2 = 2 + 2 = 4\\
&a_3 = a_2 + 3 = 4 + 3 = 7\\
&a_4 = a_3 + 4 = 7 + 4 = 11\\
&\qquad\vdots
\end{aligned}$$

Asimismo, se pueden encontrar relaciones de recurrencia en la ciencia de la biología.

Ejemplo

Considérese que el número de bacterias de una colonia se duplica cada hora. Si a_n es el número total de bacterias en n horas, encontrar una relación de recurrencia para calcular a_n.

Solución

Dado que el número de bacterias en la hora n es el doble de las que había en la hora $n-1$, entonces, como consecuencia, la relación de recurrencia que se obtiene es:

$$a_n = 2a_{n-1}$$

Si suponemos que la colonia comienza solo con un par de bacterias, es decir, $a_0 = 2$; entonces, de acuerdo con la relación de recurrencia, se tiene que:

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 2a_0 = 2(2) = 4 \\ a_2 &= 2a_1 = 2(4) = 8 \\ a_3 &= 2a_2 = 2(8) = 16 \\ a_4 &= 2a_3 = 2(16) = 32 \\ &\vdots \end{aligned}$$

De este modo, una relación de recurrencia define una sucesión de recurrencia única, siempre y cuando se definan los valores iniciales. Pero, si a dicha relación no se le especifican los valores iniciales, entonces esta relación define una infinidad de sucesiones de recurrencia.

Ejemplo

La relación de recurrencia $a_n = 3a_{n-1}$, $n \geq 0$, puede definir las siguientes sucesiones de recurrencia:

$$\begin{aligned} \{a_n\} &= \{5, 15, 45, \ldots\} \\ \{b_n\} &= \{7, 21, 63, \ldots\} \\ \{c_n\} &= \{2, 6, 18, \ldots\} \\ \{d_n\} &= \{3, 9, 27, \ldots\} \\ &\vdots \end{aligned}$$

Es decir, puede definir una infinidad de sucesiones de recurrencia.

Ahora bien, si se especifica que en:

$$\begin{aligned} &\{a_n\} \text{ el término } a_0 = 5 \\ &\{b_n\} \text{ el término } a_0 = 7 \\ &\{c_n\} \text{ el término } a_0 = 2 \\ &\{d_n\} \text{ el término } a_0 = 3 \end{aligned}$$

Entonces, en cada caso se define una sucesión de recurrencia única.

La misma relación de recurrencia con valor inicial $a_0 = 1$, define la siguiente sucesión de recurrencia, la cual también es única:

$$\{a_n\} = \{1, 3, 9, 27, \ldots\}$$

la cual, además, también es una progresión geométrica.

Los valores iniciales no necesariamente son los primeros términos de la sucesión de recurrencia, pues dichos valores pueden ocupar cualquier posición en dicha sucesión, con los cuales también es posible calcular tanto términos anteriores como posteriores.

Ejemplo

Considérese la relación de recurrencia siguiente:

$$3a_n - 5a_{n-1} + 2a_{n-2} = 0$$

cuyos valores iniciales son: $a_3 = 1$ y $a_4 = 4$.

Calcular los términos a_5 y a_6, además de los términos a_2, a_1 y a_0.

Solución

Primero, se despeja a_n:

$$a_n = [5a_{n-1} - 2a_{n-2}] / 3$$

Luego, se calculan los términos a_5 y a_6:

$$\begin{aligned} a_5 &= [5a_4 - 2a_3] / 3 \\ &= [(5)(4) - (2)(1)] / 3 \\ &= [20 - 2] / 3 = 18 / 3 = 6 \end{aligned}$$

y

$$\begin{aligned} a_6 &= [5a_5 - 2a_4] / 3 \\ &= [(5)(6) - (2)(4)] / 3 \\ &= [30 - 8] / 3 = 22 / 3 \end{aligned}$$

y así sucesivamente, para cualquier término posterior.

De igual modo, es posible calcular a_2, a_1 y a_0, aunque dichos términos sean anteriores; en cuyo caso, lo único que varía es el despeje de a_n, ya que en realidad se tiene que despejar a_{n-2} y el valor de n; en este caso, no va a ser el valor del subíndice, ya que, por ejemplo, para encontrar a_2, n debe valer 4, es decir, si:

$$a_{n-2} = [-3a_n - 5a_{n-1}] / 2$$

entonces:

$$\begin{aligned} a_2 &= [-3a_4 + 5a_3] / 2 \\ &= [-(3)(4) + (5)(1)] / 2 \\ &= [-12 + 5] / 2 = -7 / 2 \\ a_1 &= [-3a_3 + 5a_2] / 2 \\ &= [-(3)(1) + (5)(-7 / 2)] / 2 \\ &= [-3 + (-35 / 2)] / 2 = -41 / 2 \end{aligned}$$

y por último:

$$\begin{aligned} a_0 &= [-3a_2 + 5a_1] / 2 \\ &= [-(3)(-7 / 2) + (5)(-41 / 2)] / 2 \\ &= [21 / 2 + (-205 / 2)] / 2 = -184 / 2 \end{aligned}$$

De este modo, la sucesión de recurrencia resultante es:

$$\{a_n\} = \{-184/2, -41/2, -7/2, 1, 4, 6, 22/3, \ldots\}$$

Relación de recurrencia lineal con coeficientes constantes

De los ejemplos vistos hasta aquí, se puede concluir que las relaciones de recurrencia constituyen un modelo, ya sea para crecimiento de conejos, para obtener la tasa de interés compuesto o para el pago con granos de trigo; no obstante, estas también pueden aplicarse en otras áreas, como crecimiento de colonias de bacterias, regiones producidas en el plano, etcétera.

Es importante resaltar que también existe una familia de relaciones de recurrencia, las cuales pueden resolverse aplicando algunas reglas fijas; esta familia es la que está integrada por las relaciones de recurrencia lineales con coeficientes constantes, las cuales se estudian a continuación.

Relación de recurrencia lineal con coeficientes constantes

Una relación de recurrencia que tiene la forma:

$$a_n = C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = f(n)$$

o bien que en su forma implícita es:

$$C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = f(n)$$

donde:

$C_0, C_1, C_2,\ldots, C_k$ son constantes; es decir, $C_i \in \mathbb{R}$.

Dicha relación de recurrencia se denomina ***relación de recurrencia lineal con coeficientes constantes*** (RRLCC) de k-ésimo orden, siempre que $C_0 \neq 0$ y $C_k \neq 0$.

Cuando $f(n) = 0$, se dice que es una relación de recurrencia lineal homogénea con coeficientes constantes (RRLHCC), es decir:

$$C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = 0$$

A esta relación de recurrencia se le llama *lineal*, porque cada a_n se eleva a la potencia 1 y no hay productos como $a_n \cdot a_m$. Además de que para obtener el orden de la misma, es necesario obtener la diferencia entre los subíndices mayor y menor de los miembros de la secuencia que ocurre en la relación de recurrencia.

Ejemplo

Determinar cuáles de las siguientes relaciones de recurrencia son lineales con coeficientes constantes y de estas determinar su orden.

a) $2a_n + 2a_{n-1} = 2^n$

b) $a_n + 3ra_{n-1}$

c) $3a_n - 5a_{n-1} + 2a_{n-2} = n^2 + 5$

d) $a_n = 7a_{n-2}$

e) $a_n = 3a_{n-1} \cdot a_{n-2}$

f) $a_n = 3a_{n-3}$

g) $2a_r + a_{n-1}^2 = 2^n$

Solución

a) Es una RRLCC de primer orden.

b) No es una RRLCC, ya que su coeficiente de un término no es constante.

c) Es una RRLCC de segundo orden.

d) Es una relación de RRLHCC de segundo orden.

e) No es una RRLCC, ya que no debe haber productos entre los términos.

f) Es una RRLHCC de tercer orden.

g) No es una RRLCC, ya que no debe haber ningún término que esté elevado a una potencia diferente de 1.

4.4 Soluciones homogéneas

A través del tiempo se han formulado diversos procedimientos sistemáticos para resolver las relaciones de recurrencia lineales con coeficientes constantes. De estos, a continuación se analizan algunos de los más importantes.

Sin embargo, antes de profundizar en dichos métodos, resulta indispensable formular la siguiente pregunta: ¿qué es resolver una relación de recurrencia? Como se recordará, en el tratamiento de los temas de las progresiones aritméticas y geométricas se encontró una fórmula explícita para determinar el valor de cualquier término de [illegible] ría con las relaciones de recurrencia respectivas. Con base en la experiencia de las progresiones aritméticas y geométricas, se pretende hacer algo similar con las relaciones de recurrencia lineales con coeficientes constantes, es decir, encontrar una fórmula o ecuación que se utilice para determinar el valor de cualquier término de la relación de recurrencia.

A esta fórmula se le denomina **solución total** o **solución explícita** de la relación de recurrencia lineal con coeficientes constantes, la cual consiste en la suma de dos funciones numéricas discretas, una denominada **solución homogénea** $a_n^{(h)}$, la cual satisface la relación de recurrencia cuando $f(n) = 0$, esto es:

$$C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = 0$$

Y otra denominada **solución particular**, $a_n^{(p)}$ la cual satisface la relación de recurrencia cuando $f(n) \neq 0$; esto es:

$$C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = f(n)$$

Por tanto, la función numérica discreta (la cual sería análoga a la fórmula explícita de las progresiones aritméticas y geométricas, por lo que también suele recibir el nombre de ***solución explícita***), que es solución de la relación de recurrencia lineal con coeficientes constantes, es la suma de la solución homogénea y la solución particular, es decir:

$$a_n = a_n^{(h)} + a_n^{(p)}$$

Nota

Se llama ecuación característica asociada a la relación de recurrencia, como se ve en siguiente ejemplo, pero por simplicidad se conoce simplemente como ecuación característica.

Una solución homogénea para la relación de recurrencia lineal con coeficientes constantes tiene la siguiente forma exponencial:

$$\lambda_1^n, \lambda \neq 0$$

donde λ_1 se conoce como una raíz característica.

Ahora bien, si se sustituye λ^n por a_n en la relación de recurrencia

$$C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \cdots + C_ka_{n-k} = 0$$

se obtiene

$$C_0\lambda^n + C_1\lambda^{n-1} + C_2\lambda^{n-2} + \cdots + C_k\lambda^{n-k} = 0$$

que puede simplificarse como:

$$C_0\lambda^k + C_1\lambda^{k-1} + C_2\lambda^{k-2} + \cdots + C_k = 0$$

Esta ecuación recibe el nombre de ***ecuación característica*** (o ***polinomio característico***) asociada a la relación de recurrencia lineal con coeficientes constantes.

En general, la ecuación característica de k-ésimo grado tendrá k raíces características λ_i, $i = 1,\ldots, k$.

En este caso, cada una de las raíces características respectivas dará lugar a las respectivas soluciones de la relación de recurrencia.

Por tanto, si λ_1 es una de las raíces de la ecuación característica (esta es la razón por la cual λ_1 recibe el nombre de ***raíz característica***), entonces λ_1^r es una solución homogénea de la relación de recurrencia.

Para determinar la solución homogénea $a_n^{(h)}$, primero es necesario encontrar la ecuación característica, la cual se obtiene a través del siguiente proceso:

1. Se hace $f(n) = 0$.
2. Se obtiene el orden de la relación de recurrencia lineal homogénea con coeficientes constantes resultante.
3. Se sustituye cada a_n por λ, conservando los signos y los coeficientes de cada término de la relación de recurrencia.
4. Se construye la ecuación característica de grado igual al orden de la relación de recurrencia lineal homogénea con coeficientes constantes.

Ejemplo

Sea la relación de recurrencia lineal con coeficientes constantes:

$$3a_n - 5a_{n-1} + 2a_{n-2} = n^2 + 5.$$

Determinar su ecuación característica.

Solución

Para esto se realiza cada uno de los pasos del proceso para encontrar la ecuación característica:

1. Se hace $f(n) = 0$, esto es:

$$3a_n - 5a_{n-1} + 2a_{n-2} = 0$$

2. Se obtiene el orden de la RRLHCC resultante, en este caso: segundo orden.
3. Se sustituye cada a_n por λ, conservando los signos y coeficientes, esto es:

$$3\lambda - 5\lambda + 2\lambda = 0$$

4. Se construye el polinomio característico de grado igual al orden de la RRLHCC:

$$3\lambda^2 - 5\lambda + 2 = 0$$

El resultado de este proceso constituye la ecuación característica asociada a la relación de recurrencia.

Ahora, si todas las raíces características de la ecuación característica son distintas, la forma general de la solución homogénea es:

$$a_n^{(h)} = A_1\lambda_1^n + A_2\lambda_2^n + \cdots + A_k\lambda_k^n$$

donde $\lambda_1, \lambda_2, \ldots, \lambda_k$ son las distintas raíces características de la ecuación característica y $A_1, A_2, \ldots, A_k$ son las constantes que van a ser determinadas por los valores iniciales en la solución total.

Pero, si algunas de las raíces de la ecuación característica son raíces múltiples, entonces si λ_1 es una raíz de multiplicidad m, la forma general que deberá tener la solución homogénea es:

$$a_n^{(h)} = \left(A_1 n^{m-1} + A_2 n^{m-2} + \cdots + A_{m-1} n + A_m\right)\left(\lambda_1^n\right)$$

donde también $A_1, A_2, \ldots, A_m$ son constantes que serán determinadas por los valores iniciales en la solución total.

Ejemplo

Determinar la solución homogénea de la relación de recurrencia lineal con coeficientes constantes:

$$3a_n - 5a_{n-1} + 2a_{n-2} = 0$$

Solución

Ya en el ejemplo anterior se determinó la ecuación característica asociada a dicha relación de recurrencia:

$$3\lambda^2 - 5\lambda + 2 = 0$$

Como se puede observar, esta ecuación característica tiene dos raíces características:

$$\lambda_1 = 2/3 \text{ y } \lambda_1 = 1$$

De esta ecuación se obtiene, por la forma general para cuando todas las raíces características son distintas, que la solución homogénea correspondiente es:

$$a_n^{(h)} = A_1\left(2/3\right)^n + A_2$$

Donde las dos constantes, A_1 y A_2, son determinadas a partir de los valores iniciales en la solución total.

Otro ejemplo para obtener la solución homogénea de una relación de recurrencia lineal con coeficientes constantes es el siguiente:

Ejemplo

Determinar la solución homogénea para la sucesión de Fibonacci.

Solución

La relación de recurrencia lineal homogénea con coeficientes constantes de segundo orden para la sucesión de Fibonacci es:

$$a_n = a_{n-1} + a_{n-2} \text{ o } a_n - a_{n-1} - a_{n-2} = 0$$

Entonces, la correspondiente ecuación característica es:

$$\lambda^2 - \lambda - 1 = 0$$

la cual tiene dos raíces características distintas:

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \text{ y } \lambda_2 = \frac{1-\sqrt{5}}{2}$$

de donde se obtiene, por la forma general para cuando todas las raíces características son distintas, que la solución homogénea correspondiente es:

$$a_n^{(h)} = A_1 {\frac{1+\sqrt{5}}{2}}^{n} + A_2 {\frac{1-\sqrt{5}}{2}}^{n}$$

donde las dos constantes A_1 y A_2 serán determinadas a partir de los valores iniciales $a_0 = 1$ y $a_1 = 1$ en la solución total.

En los ejemplos anteriores todas las raíces características son diferentes; ahora bien, en el siguiente solo existe una raíz de multiplicidad.

Ejemplo

Determinar la solución homogénea de la relación de recurrencia lineal con coeficientes constantes:

$$a_n + 9a_{n-1} + 27a_{n-2} + 27a_{n-3} = 0$$

Solución

La ecuación característica asociada a la relación de recurrencia es:

$$\lambda^3 + 9\lambda^2 + 27\lambda + 27 = 0$$

la cual tiene una raíz característica triple, ya que al factorizar la ecuación característica se tiene que:

$$(\lambda + 3)(\lambda + 3)(\lambda + 3) = (\lambda + 3)^3 = 0$$

Esto es:

$$\lambda_1 = \lambda_2 = \lambda_3 = -3$$

de donde se tiene, por la forma general para cuando existen raíces de multiplicidad, que la solución homogénea correspondiente es:

$$a_n^{(h)} = \left(A_1 n^2 + A_2 n + A_3\right)\left(-3\right)^n$$

donde las constantes A_1, A_2 y A_3 se determinarán a partir de los valores iniciales en la solución total.

Pero, también puede darse el caso de que al determinar las raíces características se obtengan alguna raíz de multiplicidad y otras diferentes.

Ejemplo

Determinar la solución homogénea de la siguiente relación de recurrencia lineal con coeficientes constantes:

$$a_r - 7a_{r-1} + 16a_{r-2} - 12a_{r-3} = 0$$

Solución

La ecuación característica asociada es:

$$\lambda^3 - 7\lambda^2 + 16\lambda - 12 = 0$$

y las raíces características son:

$$\lambda_1 = \lambda_2 = 2, \text{ y } \lambda_3 = 3$$

En consecuencia, combinando las dos formas generales, la solución homogénea es:

$$a_n^{(h)} = \left(A_1 n + A_2\right)2^n + A_3 3^n$$

donde las constantes A_1, A_2 y A_3 se determinarán a partir de los valores iniciales en la solución total.

4.5 Soluciones particulares

En este punto, es importante hacer notar que no hay un procedimiento general para determinar la solución particular de una relación de recurrencia lineal con coeficientes constantes. Sin embargo, para ciertas funciones $f(n)$, tales como polinomios de grado t en n y potencias de constantes, se conocen formas generales de soluciones particulares.

A continuación, se analizan algunos de los principales casos en los cuales aparecen con mayor frecuencia, al determinar la solución particular de las relaciones de recurrencia lineales con coeficientes constantes.

Caso 1

Cuando $f(n)$ es de la forma de un polinomio de grado t en n, es decir:

$$f(n) = C_1 n^t + C_2 n^{t-1} + \cdots + C_t n + C_{t+1}$$

donde los $C_i \in \mathbb{R}$ son los coeficientes del polinomio, entonces la solución particular correspondiente tiene la forma:

$$A_1 n^t + A_2 n^{t-1} + \cdots + A_t n + A_{t+1}$$

donde las A_i son constantes a determinar.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes siguiente:

$$a_n + 5a_{n-1} + 6a_{n-2} = 3n^2 - 2n + 5 \qquad (i)$$

Solución

Como $f(n)$ tiene la forma de un polinomio de grado 2 en n, entonces la solución particular tiene la forma:

$$A_1 n^2 + A_2 n + A_3 \qquad (ii)$$

donde A_1, A_2 y A_3 son constantes a determinar.

Al sustituir la expresión (*ii*) en el lado izquierdo de (*i*) se obtiene que:

$$A_1 n^2 + A_2 n + A_3 + 5A_1(n-1)^2 + 5A_2(n-1) + 5A_3 + 6A_1(n-2)^2 + 6A_2(n-2) + 6A_3$$

Continúa

lo que puede simplificarse como:

$$12A_1n^2 + (-34A_1 + 12A_2)n + (29A_1 - 17A_2 + 12A_3) \qquad (iii)$$

Ahora bien, si se compara (*iii*) en la parte derecha de (*i*) se obtienen las siguientes ecuaciones:

$$12A_1 = 3$$
$$-34A_1 + 12A_2 = -2$$
$$29A_1 - 17A_2 + 12A_3 = 5$$

donde:

$$A_1 = \frac{1}{4}$$
$$A_2 = \frac{13}{24}$$
$$A_3 = \frac{167}{288}$$

Por tanto, la solución particular es:

$$a_n^{(p)} = \frac{1}{4}n^2 + \frac{13}{24}n + \frac{167}{288}$$

Caso 2
Cuando $f(r)$ es una constante, la solución particular es una constante A.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes siguiente:

$$a_n - 5a_{n-1} + 6a_{n-2} = 8$$

Solución

Puesto que $f(r)$ es una constante, la solución particular también lo es, así que dicha constante es A.

Al sustituir A en la parte izquierda de la relación de recurrencia, se tiene que:

$$A - 5A + 6A = 8$$

Simplificando se tiene que:

$$2A = 8$$

o bien:

$$A = 4$$

Por tanto, la solución particular es:

$$a_n^{(p)} = 4$$

Caso 3
Cuando $f(n)$ tiene la forma:

$$C\alpha^n$$

la correspondiente solución particular tiene la forma:

$$A\alpha^n$$

donde $C \in \mathbb{R}$, y A es una constante a determinar, siempre y cuando α no sea una raíz característica de la relación de recurrencia lineal con coeficientes constantes.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes siguientes:

$$a_n + 5a_{n-1} + 6a_{n-2} = 84 \cdot 4^n \qquad (i)$$

Solución

La forma general de la solución particular es:

$$A4^n \qquad (ii)$$

Sustituyendo (*ii*) en el lado izquierdo de (*i*) se tiene que:

$$A4^n + 5A4^{n-1} + 6A4^{n-2}$$

que se puede simplificar como:

$$\frac{21}{8}A4^n \qquad (iii)$$

Comparando (*iii*) con el lado derecho de (*i*), se tiene que:

$$\frac{21}{8}A = 84$$

o bien:

$$A = 32$$

Por tanto, la solución particular es:

$$a_n^{(p)} = 32 \cdot 4^n$$

Caso 4
Cuando $f(n)$ es de tipo:

$$\alpha^n$$

la correspondiente solución particular tiene la forma:

$$An^{m-1}\alpha^n$$

siempre que α sea una raíz característica de multiplicidad $m - 1$ de la relación de recurrencia lineal con coeficientes constantes.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes siguiente:

$$a_n - 2a_{n-1} = 6 \cdot 2^n \qquad (i)$$

Solución

Como 2 es una raíz característica de multiplicidad 1, entonces la forma general de la solución particular es:

$$An2^n \qquad (ii)$$

Si se sustituye (*ii*) en el lado izquierdo de (*i*), se obtiene:

$$An2^n - 2A(n-1)2^{n-1}$$

Simplificando:

$$A2^n \qquad (iii)$$

y comparando (*iii*) con el lado derecho de (*i*), se tiene que:

$$A2^n = 6 \cdot 2^n$$

o lo que es lo mismo:

$$A = 6$$

Por tanto, la solución particular es:

$$a_n^{(p)} = 6n2^n$$

Caso 5

Cuando $f(n)$ es de tipo de un polinomio de grado t en n por α^n, es decir:

$$(C_1n^t + C_2n^{t-1} + \cdots + C_tn + C_{t+1})\alpha^n$$

donde los $C_i \in \mathbb{R}$ son los coeficientes del polinomio; entonces, la correspondiente solución particular tendrá la forma:

$$(A_1n^t + A_2n^{t-1} + \cdots + A_tn + A_{t+1})\alpha^n$$

donde las A_i son las constantes a determinar, siempre y cuando α no sea una raíz característica de la relación de recurrencia lineal con coeficientes constantes.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes siguiente:

$$a_n + a_{n-1} = 9n2^n \qquad (i)$$

Solución

En este caso, la forma general para la solución particular es:

$$(A_1n + A_2)2^n \qquad (ii)$$

Ya que $9n$ es un polinomio de grado 1 y al sustituir (ii) en el lado izquierdo de (i) se tiene que:

$$(A_1n + A_2)2^n + [A_1(n-1) + A_2]2^{n-1}$$

lo que se puede simplificar como:

$$\left(\frac{3}{2}\right)A_1n2^n + \left[\left(-\frac{1}{2}\right)A_1 + \left(\frac{1}{3}\right)A_2\right]2^n \qquad (iii)$$

Comparando (iii) con el lado derecho de (i) se obtienen las siguientes ecuaciones:

$$\left(\frac{3}{2}\right)A_1 = 9$$

$$\left(-\frac{1}{2}\right)A_1 + \left(\frac{3}{2}\right)A_2 = 0$$

de donde se obtiene que:

$$A_1 = 6 \text{ y } A_2 = 2$$

Por tanto, la correspondiente solución particular es:

$$a_n^{(p)} = (6n+2)2^n$$

Caso 6

Cuando $f(n)$ es de tipo de un polinomio de grado t en n por α^r, es decir:

$$(C_1n^t + C_2n^{t-1} + \cdots + C_tn + C_{t+1})\alpha^n$$

donde los $C_i \in \mathbb{R}$ son los coeficientes del polinomio, entonces la correspondiente solución particular tendrá la forma:

$$n^m(A_1n^t + A_2n^{t-1} + \cdots + A_tn + A_{t+1})\alpha^n$$

donde las A_i son las constantes a determinar, siempre y cuando α sea una raíz característica de multiplicidad m de la relación de recurrencia lineal con coeficientes constantes.

Ejemplo

Encontrar la solución particular para la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 4a_{n-1} + 4a_{n-2} = (n+1)2^n \qquad (i)$$

Solución

Ya que 2 es una raíz característica de multiplicidad $m = 2$, entonces la forma general que tiene la solución particular es:

$$n^2(A_1 n + A_2)2^n \qquad (ii)$$

Al sustituir (*ii*) en el lado izquierdo de (*i*) se obtiene que:

$$n^2(A_1 n + A_2)\, 2^n + (n-1)\, 2\, [A_1(n-1) + A_2]\, 2^{n-1} +$$
$$(n-2)\, 2\, [A_1(n-2) + A_2]\, 2^{n-2}$$

Al simplificar queda:

$$6A_1 n 2^n + (-6A_1 + 2A_2)2^n \qquad (iii)$$

Al comparar (*iii*) con el lado derecho de (*i*) se obtienen las ecuaciones:

$$6A_1 n 2^n = n2^n$$
$$(-6A_1 + 2A_2)2^n = 2^n$$

o lo que es lo mismo:

$$6A_1 = 1$$
$$-6A_1 + 2A_2 = 1$$

donde se tiene que:

$$A_1 = \frac{1}{6} \text{ y } A_2 = 1$$

Por tanto, la correspondiente solución particular es:

$$a_n^{(p)} = n^2\left(\frac{n}{6} + 1\right)2^n$$

4.6 Soluciones totales

Para obtener la solución total, es necesario realizar la suma de la solución homogénea $a_n^{(h)}$ y la solución particular $a_n^{(p)}$; es decir:

$$a_n = a_n^{(h)} + a_n^{(p)}$$

Además de determinar las constantes $A_1, A_2, \ldots, A_k$ de la solución homogénea.

Para una relación de recurrencia de k-ésimo orden, las k constantes de la solución homogénea pueden determinarse mediante los valores iniciales:

$$a_0, a_1, \ldots, a_{k-1}$$

Pero, dichos valores deben ser consecutivos.

Si todas las raíces de la relación de recurrencia son distintas, entonces la solución total es de la forma:

$$a_n = A_1\lambda_1^n + A_2\lambda_2^n + \cdots + Ak\lambda_k^n + p(n)$$

donde $p(n)$ es la solución particular.

Además se tiene el siguiente sistema de ecuaciones lineales:

$$\begin{aligned} a_0 &= A_1 + A_2 + \cdots + A_k + p(0) \\ a_1 &= A_1\lambda_1 + A_2\lambda_2 + \cdots + A_k\lambda_k + p(1) \\ a_2 &= A_1\lambda_1^2 + A_2\lambda_2^2 + \cdots + A_k\lambda_k^2 + p(2) \\ &\vdots \\ a_{k-1} &= A_1\lambda_1^{k-1} + A_2\lambda_2^{k-1} + \cdots + A_k\lambda_k^{k-1} p(k-1) \end{aligned}$$

de k ecuaciones, que sirven para obtener las constantes:

$$A_1, A_2, \ldots, A_k$$

Ejemplo

Determinar la solución total para la relación de recurrencia asociada a la sucesión de Fibonacci.

Solución

En páginas anteriores, en este mismo capítulo, se obtuvo la solución homogénea de la relación de recurrencia asociada a la sucesión de Fibonacci, la cual es:

$$a_n = A_1\left[\frac{1+\sqrt{5}}{2}\right]^n + A_2\left[\frac{1-\sqrt{5}}{2}\right]^n$$

Con valores iniciales $a_0 = 1$ y $a_1 = 1$.

La forma general para la solución total es:

$$a_n = a_n^{(h)} + a_n^{(p)}$$

Pero, como la relación de recurrencia para la sucesión de Fibonacci es lineal homogénea con coeficientes constantes, entonces no tendrá solución particular. Por tanto, la forma de la solución total es:

$$a_n = A_1\left[\frac{1+\sqrt{5}}{2}\right]^n + A_2\left[\frac{1-\sqrt{5}}{2}\right]^n$$

Ahora bien, al utilizar los valores iniciales se obtiene el siguiente sistema de ecuaciones:

$$a_0 = A_1\left[\frac{1+\sqrt{5}}{2}\right]^0 + A_2\left[\frac{1-\sqrt{5}}{2}\right]^0$$

$$a_1 = A_1\left[\frac{1+\sqrt{5}}{2}\right]^1 + A_2\left[\frac{1-\sqrt{5}}{2}\right]^1$$

Sustituyendo los valores iniciales se tiene que:

$$\begin{aligned} 1 &= A_1 + A_2 \\ 1 &= A_1\left[\frac{1+\sqrt{5}}{2}\right] + A_2\left[\frac{1-\sqrt{5}}{2}\right] \end{aligned}$$

Ahora, al despejar A_1 y A_2 de las ecuaciones anteriores se tiene que:

$$A_1 = \frac{1}{\sqrt{5}} \text{ y } A_2 = -\frac{1}{\sqrt{5}}$$

Continúa

Solución

Por tanto, la solución total para la relación de recurrencia asociada a la sucesión de Fibonnaci es:

$$a_n = \frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2}\right]^n - \frac{1}{\sqrt{5}}\left[\frac{1-\sqrt{5}}{2}\right]^n$$

o bien:

$$a_n = \frac{1}{\sqrt{5}}\left(\left[\frac{1+\sqrt{5}}{2}\right]^n - \left[\frac{1-\sqrt{5}}{2}\right]^n\right)$$

Otro buen ejemplo es determinar la solución total del problema de las torres de Hanói.

Ejemplo

Determinar la solución total para la relación de recurrencia asociada al problema de las torres de Hanói.

Solución

Como se vio antes, la relación de recurrencia lineal con coeficientes constantes asociada al problema de las torres de Hanói es:

$$a_n = 2a_{n-1} + 1$$

o bien:

$$a_n - 2a_{n-1} = 1$$

Con valor inicial $a_0 = 1$.

La ecuación característica asociada a la relación de recurrencia es:

$$\lambda - 2 = 0$$

la cual tiene una única raíz característica:

$$\lambda = 2$$

de donde se tiene, por la forma general para cuando todas las raíces características son distintas, que la solución homogénea correspondiente es:

$$a_n^{(h)} = A_1 \cdot 2^n$$

Dado que $f(r)$ es una constante, la solución particular también lo será; dicha constante es A. Ahora bien, al sustituir A en la parte izquierda de la relación de recurrencia, se obtiene:

$$A - 2A = 1$$
$$-A = 1$$
$$A = -1$$

por lo que la solución particular es:

$$a_n^{(p)} = -1$$

Como la forma general para la solución total es:

$$a_n = a_n^{(h)} + a_n^{(p)}$$

Continúa

Solución

Entonces, se tiene que:

$$a_n = A_1 \cdot 2^n - 1$$

Utilizando el valor inicial, se tiene la ecuación siguiente:

$$a_1 = A_1 \cdot 2^1 - 1$$

o bien:

$$1 = A \cdot 2 - 1$$

donde:

$$2 = 2A$$

$$\mathrm{A} = 1$$

Por tanto, la solución total es:

$$a_n = 2^n - 1$$

Ejemplo

Sea la relación de recurrencia:

$$a_n + 5a_{n-1} + 6a_{n-2} = 42 \cdot 4^n \qquad (i)$$

Con valores iniciales $a_0 = 19$ y $a_1 = 56$.

Por tanto, la ecuación característica asociada a la relación de recurrencia es:

$$\lambda^2 + 5\lambda + 6 = 0$$

la cual tiene dos raíces diferentes:

$$\lambda_1 = -3 \text{ y } \lambda_2 = -2$$

de donde se obtiene, por la forma general para cuando todas las raíces características son distintas, que la solución homogénea correspondiente es:

$$a_n^{(h)} = A_1(-3)^n + A_2(-2)^n$$

Por tanto, la forma general de la solución particular es:

$$A4^n \qquad (ii)$$

Al sustituir (*ii*) en el lado izquierdo de (*i*) se tiene que:

$$A4^n + 5A4^{n-1} + 6A4^{n-2}$$

Lo que se puede simplificar como:

$$\left(-\frac{21}{8}\right)A4^n \qquad (iii)$$

Comparando (*iii*) con el lado derecho de (*i*), se tiene que:

$$\left(-\frac{21}{8}\right)A = 42$$

donde:

$$A = 16$$

Por tanto, se tiene que la solución particular es:

$$a_n^{(p)} = 16 \cdot 4n$$

Continúa

Por último, la solución total queda como sigue:

$$a_n = A_1(-3)^n + A_2(-2)^n + 16 \cdot 4^n$$

Utilizando los valores iniciales se tiene el siguiente sistema de ecuaciones:

$$a_0 = A_1(-3)^0 + A_2(-2)^0 + 16 \cdot 4^0$$
$$a_1 = A_1(-3)^1 + A_2(-2)^1 + 16 \cdot 4^1$$

Al sustituirlos se tiene que:

$$19 = A_1 + A_2 + 16$$
$$56 = -3A_1 - 2A_2 + 64$$

donde se tiene que:

$$A_1 = 2 \text{ y } A_2 = 1$$

Así, la solución total queda como sigue:

$$a_n = 2 \cdot (-3)^n + (-2)^n + 16 \cdot 4^n$$

EJEMPLO

Encontrar la solución total de la relación de recurrencia siguiente:

$$a_n - 7a_{n-1} + 10a_{n-2} = 3^n \qquad (i)$$

con los valores iniciales $a_0 = 0$ y $a_1 = 1$.

La ecuación característica asociada a la relación de recurrencia es:

$$\lambda^2 - 7\lambda + 10 = 0$$

En esta se tienen dos raíces diferentes:

$$\lambda_1 = 2 \text{ y } \lambda_2 = 5$$

de donde se obtiene, por la forma general para cuando todas las raíces características son distintas, que la solución homogénea correspondiente es:

$$a_n^{(h)} = A_1(2)^n + A_2(5)^n$$

La forma general de la solución particular es $C\alpha^n$; entonces, la correspondiente solución particular tiene la forma:

$$A3^n \qquad (ii)$$

Al sustituir (*ii*) en el lado izquierdo de (*i*) se tiene que:

$$A3^n - 7A3^{n-1} + 10A4^{n-2}$$

la cual se puede simplificar como:

$$\left(-\frac{2}{9}\right)A3^n \qquad (iii)$$

Al comparar (*iii*) con el lado derecho de (*i*), se tiene que:

$$\left(-\frac{2}{9}\right)A = 1$$

donde:

$$A = -\frac{9}{2}$$

Por tanto, la solución particular es:

$$a_n^{(p)} = \left(-\frac{2}{9}\right)(3)^n$$

Continúa

Entonces, la solución total es:

$$a_n = A_1(2)^n + A_2(5)^n - \left(\frac{9}{2}\right)(3)^n$$

Ahora, al sustituir los valores iniciales se tiene que:

$$0 = A_1 + A_2 - \frac{9}{2}$$
$$1 = 2A_1 + 5A_2 - \frac{27}{2}$$

donde se obtiene que:

$$A_1 = \left(\frac{8}{3}\right)$$

$$A_2 = \left(\frac{11}{6}\right)$$

Por tanto, la solución total es:

$$a_n = \left(\frac{8}{3}\right)(2)^n + \left(\frac{11}{6}\right)(5)^n - \left(\frac{9}{2}\right)(3)^n$$

Si algunas de las raíces de la ecuación característica son raíces múltiples y si λ_1 es una raíz de multiplicidad m, donde $2 \leq m \leq k$, y k es el grado de la relación de recurrencia lineal con coeficientes constantes, entonces la parte de la solución total relacionada con la raíz λ_1 es de la forma:

$$a_n = \left(A_1 n^{m-1} + A_1 n^{m-2} + \cdots + A_{m-1} n + A_m\right)\left(\lambda_1^n\right) + p(n)$$

donde $A_1, A_2, \ldots, A_m$, son constantes y $p(n)$ es la solución particular.

EJEMPLO

Encontrar la solución total de la relación de recurrencia:

$$a_r - 4a_{r-1} + 4a_{r-2} = 0$$

con los valores iniciales $a_0 = 1$ y $a_1 = 3$.

La ecuación característica asociada a dicha relación de recurrencia es:

$$\lambda^2 - 4\lambda + 4 = 0$$

la cual tiene una raíz característica doble, ya que al factorizar la ecuación característica se obtiene que:

$$(\lambda - 2)(\lambda - 2) = (\lambda - 2)^2 = 0$$

esto es:

$$\lambda_1 = \lambda_2 = 2$$

donde se tiene, por la forma general para cuando existen raíces de multiplicidad, que la solución homogénea correspondiente es:

$$a_n^{(h)} = (A_1 n + A_2)2^n$$

En este caso no existe solución particular, ya que es una relación de recurrencia lineal homogénea con coeficientes constantes; entonces, la solución total es precisamente:

$$a_n = (A_1 n + A_2)2^n$$

donde se tiene que $\lambda_1 = 2$ es una raíz de multiplicidad $m = 2$.

Ahora, al sustituir los valores iniciales se tiene que:

$$1 = A_2$$

Continúa

$$3 = 2A_1 + 2A_2$$

donde:

$$A_1 = \frac{1}{2}$$

$$A_2 = 1$$

Por tanto, la solución total queda:

$$\begin{aligned} a_n &= \left(\frac{n}{2}\right) + 1\ 2^n \\ &= \left(\frac{1}{2}\right) n2^n + 2^n \\ &= n\left(\frac{2^n}{2}\right) + 2^n \\ &= n(2^n)\ (2^{-1}) + 2^n \\ &= n(2^{n-1}) + 2^n \end{aligned}$$

Resumen

Desde los inicios de la historia de las matemáticas se han estudiado las propiedades de las progresiones y de las sucesiones de recurrencia, mismas que han sido aplicadas en diversas áreas de las matemáticas, las ciencias e incluso en el arte y la música.

El estudio de las progresiones aritméticas es paralelo al de las progresiones geométricas por cuanto las propiedades de estas últimas emanan de las primeras, sin más que convertir las sumas en productos, diferencias en cocientes y el producto por un número natural en una potencia de exponente natural.

Toda relación de recurrencia para una sucesión de recurrencia es simplemente una fórmula que expresa cada término en función de uno o más de los términos que le preceden. Los valores de los términos necesarios para empezar a calcular la sucesión de recurrencia son los valores iniciales.

Además, dada su naturaleza, las relaciones de recurrencia ponen de manifiesto la necesidad de determinar, de manera explícita, mediante algún método o técnica, el término n-ésimo de la sucesión que representan.

Problemas propuestos

4.1 Dada la sucesión $\{a_n\} = \{1, 4, 7, 10, \ldots\}$, responder lo siguiente:

a) ¿Qué tipo de progresión es?
b) ¿Cuál término tiene el valor de 88?

4.2. Dada la sucesión $\{a_n\} = \{2, 6, 18, 54, \ldots\}$, responder lo siguiente:

a) ¿Qué tipo de progresión es?
b) ¿Cuál término tiene el valor de 118 098?

4.3 Determinar el término a_7 de una progresión geométrica si $a_1 = 3$ y $a_2 = 3^{5/3}$.

4.4 Determinar la razón común r de la progresión geométrica:

$$\{a_n\} = \left\{\frac{x^3}{9}, -\frac{x^3}{27}, \frac{x^3}{81}, \ldots\right\}$$

4.5 Una pelota se deja caer desde 2 048 metros de altura. Su elasticidad es tal que rebota hasta llegar a $\frac{3}{4}$ partes de la altura desde la cual cayó. ¿A qué altura llega la pelota en el quinto rebote?

4.6 Dada la sucesión $\{a_n\} = \{1, 1, 1, 1, \ldots\}$, determinar qué tipo de progresión es.

4.7 Dada la sucesión $\{a_n\} = \{3, 5, 7, 9, \ldots\}$, responder lo siguiente:

a) ¿Qué tipo de progresión es?
b) ¿Cuál término de la sucesión tiene el valor de 163?

4.8 Determinar la razón común r de la progresión geométrica:

$$\{a_n\} = \{2, 2^{x+1}, 2^{2x+1}, 2^{3x+1}, \ldots\}$$

4.9 Determinar la razón común r de la progresión geométrica:

$$\{a_n\} = \{10, 10^{2x-1}, 10^{4x-3}, 10^{6x-5}, \ldots\}$$

4.10 Dadas las siguientes sucesiones, determinar si son progresiones aritméticas o geométricas:

a) $\{a_n\} = \; 2\text{sen}\frac{\pi}{4},\ 2,\ \dfrac{4}{\sqrt{2}}, \ldots$
b) $\{b_n\} = \{100(1.05), 100(1.07), 100(1.09), 100(11.1), \ldots\}$
c) $\{c_n\} = \{1, 3, 6, 10, \ldots\}$
d) $\{d_n\} = \{\log(10000), \log(1000), \log(100), \ldots\}$
e) $\{e_n\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right\}$

4.11 Determinar el término a_1 de una progresión aritmética si:

$$a_8 = 47 \text{ y } a_9 = 53$$

4.12 Determinar el término a_5 de una progresión geométrica si:

$$a_1 = 4 \text{ y } a_2 = 6$$

4.13 Calcular el primer término a_1 de una sucesión geométrica cuyos términos son:

$$a_6 = 10^{10x-9} \text{ y } a_5 = 10^{8x-7}$$

4.14 Calcular el primer término a_1 de una sucesión aritmética cuyos términos son:

$$a_{10} = x + 37 \text{ y } a_{11} = x + 42$$

4.15 Obtener el octavo término a_8 de la progresión geométrica:

$$\{a_n\} = \{300, -30, 3, \ldots\}$$

4.16 Sabiendo que, de una progresión geométrica, el término $a_8 = \frac{1}{2}$ y $r = \frac{1}{2}$. Determinar el valor del término a_2.

4.17 Dadas las siguientes sucesiones, determinar si son progresiones aritméticas o geométricas:

a) $\{a_n\} = \{1, -1, 1, -1, \ldots\}$
b) $\{b_n\} = \{96, 48, 24, 12, \ldots\}$
c) $\{c_n\} = \{2, -4, 8, -16, \ldots\}$
d) $\{d_n\} = \{2, 2^{x+1}, 22^{x+1}, 23^{x+1}, \ldots\}$
e) $\{e_n\} = \{1, 1, 2, 3, 5, \ldots\}$
f) $\{f_n\} = \{25(1.03), 25(1.07), 25(1.011), 25(1.15), \ldots\}$
g) $\{g_n\} = \{25(1.01), 25(1.04), 25(1.09), 25(1.16), \ldots\}$
h) $\{h_n\} = \{25(1.05), 25(1.05)^2, 25(1.05)^3, 25(1.05)^4, \ldots\}$
i) $\{i_n\} = \{22, -44, 88, -176, \ldots\}$
j) $\{j_n\} = \{\log_2(2), \log_2(4), \log_2(8), \ldots\}$
k) $\{k_n\} = \{1, (-x/3), (x^2/9), (-x^3/27), \ldots\}$
l) $\{l_n\} = \{ln(3), ln(9), ln(27), ln(81), \ldots\}$
m) $\{m_n\} = \{12(2.01), 12(2.04), 12(2.08), 12(2.13), \ldots\}$
n) $\{n_n\} = \{12(2.01), 12(2.01)^2, 12(2.01)^3, 12(2.01)^4, \ldots\}$
o) $\{o_n\} = \{12(2.01), 12(2.02), 12(2.03), 12(2.04), \ldots\}$

4.18 Calcular el término a_{11} de una sucesión aritmética cuyos términos son:

$$a_1 = 2 + \sqrt{2} \text{ y } a_2 = 3$$

4.19 Determinar la razón común r de la sucesión geométrica $10, 10^{2x+1}, 10^{4x+1}, 10^{6x+1}$.

4.20 Sabiendo que, de una progresión aritmética, los términos $a_8 = 47$ y $a_9 = 53$, calcular el valor del término a_1.

4.21 Sea la progresión geométrica $\{a_n\} = \{3, 6, 12, 24, \dots\}$. Calcular el producto de los primeros 5 términos.

4.22 En la progresión geométrica $\{a_n\} = \{\frac{1}{25}, \frac{1}{5}, 1, \dots\}$, si se supone que la misma consta solo de 10 términos.

Calcular:

a) El valor del último término.

b) La suma de los 10 términos.

c) El producto de todos los términos.

4.23 En una progresión aritmética, el primer término a_1 vale 4 y el último 16. Si se sabe que la diferencia común d vale 2. ¿Cuántos términos tiene la progresión?

4.24 Calcular el valor del término a_{11}, en forma de fracción, de la progresión:

$$\{a_n\} = \{3^{-2}, 3^{-3}, 3^{-4}, 3^{-5}, \dots\}$$

4.25 Calcular la suma de los 20 primeros términos de la progresión aritmética:

$$\{a_n\} = \{2, 4, 6, 8, \dots\}$$

4.26 En la progresión aritmética $\{a_n\} = \{1, 3, 5, 7, \dots\}$, la suma de todos sus términos es 196. ¿Cuántos términos tiene la progresión?

4.27 Calcular la suma de los 1000 primeros números naturales.

4.28 Calcular la suma de los 1000 primeros números impares.

4.29 Calcular la suma de los 1000 primeros números pares.

4.30 Entre 65 y 165 queremos interpolar 9 medios aritméticos. Calcular:

a) La diferencia común d.

b) La suma de todos los términos.

4.31 Entre -5 y -35 se quieren interpolar 5 medios aritméticos.

a) Determinar la diferencia común d para interpolar dichos términos.

b) Escribir la progresión resultante.

4.32 Las edades de 11 personas están en progresión aritmética y la suma de todas estas es de 561 años; si la mayor de dichas personas tiene 86 años, ¿cuántos años tiene la más joven?

4.33 Sea la progresión geométrica:

$$\{a_n\} = \left\{7, \sqrt{7}, 1, \frac{\sqrt{7}}{7}, \dots\right\}$$

Calcular:

a) La razón común r.

b) El valor del término a_7.

c) La suma de los 7 términos.

4.34 La suma de dos términos consecutivos de la progresión geométrica $\{a_n\} = \{6, 18, 54, 162, \dots\}$ es 157 464. ¿Cuáles son estos términos?

4.35 En la progresión geométrica $\{a_n\} = \{\frac{3}{4}, \frac{3}{2}, 3, 6, \dots\}$, el producto de dos términos consecutivos es 1152. ¿Cuáles son estos términos?

4.36 Entre 11 y 5 632 se quieren interpolar 8 medios geométricos.

a) Determinar la razón común r para interpolar dichos términos.

b) Escribir la progresión resultante.

4.37 La suma de los términos infinitos de una progresión geométrica indefinida de razón común $r = \frac{1}{2}$ es igual a 1. ¿Cuánto vale el primer término?

4.38 Sean las siguientes relaciones de recurrencia:

a) $(\pi/2)a_{n-2} = 3na_{n+1} + a_n$

b) $a_{n-2} = \pi a_{n-1} - a_n$

c) $a_n = \pi a_n - 1 - 2^{a}{}_{n-2} + 3n$

d) $a_n = 2^n a_{n-1}$

Determinar cuál es lineal homogénea con coeficientes constantes.

4.39 Sean las siguientes relaciones de recurrencia:

a) $a_n = 3a_{n-1} + a_{n-2} - 8a_{n-3}$
b) $2a_n = 2a_{n-1} + n2^n$
c) $4a_n = 3a_{n-1} \cdot 3a_{n-2}$
d) $a_n = 5na_{n-1} - 2a_{n-2} - 6n^2$

Determinar cuál es lineal homogénea con coeficientes constantes.

4.40 Todas las siguientes relaciones de recurrencia son lineales con coeficientes constantes EXCEPTO:

a) $a_n - 9a_{n-1} + 7a_{n-2} - 2a_{n-3} = 0$
b) $a_n + 3a_{n-1} + a_{r-2} = 6n^3 + 2n^2 + n + 3$
c) $a_n + 2na_{n-1} - 5a_{n-2} = 6n^3 + 5$
d) $a_n - 2a_{n-1} = n2^n$

4.41 Sean las siguientes relaciones de recurrencia:

a) $n^2 \frac{1}{3} a_n + \operatorname{sen}\frac{\pi}{2}\, a_{n-1} = \ln(5)a_{n-2}$
b) $a_r + 5na_{n-1} - 2a_{n-2} = 6n^2 + 5$
c) $4a_n + 3a_{n-1} \cdot 3a_{n-2} = 0$
d) $a_{n-3} = (a_{n-2} + a_n + 7a_{n-1})/5$
e) $2a_n - 2a_{n-1} = n2^n + 3$
f) $a_n^2 + 4a_{n-1} + 2a_{n-2} = 6n^2 + 5$
g) $a_n - 3a_{n-1} + a_{r-2} - 8a_{n-3} = 0$
h) $a_n = a_{n-1} \cdot a_{n-2}$
i) $a_n = a_{n-1} + 4a_{n-2} - 7a_{n-3}$
j) $a_n = 5n^2 + 2 + 5na_{n-1} - 2a_{n-2}$
k) $a_n = a_{n-1} + 3a_{n-2} \cdot a_{n-3} + a_{n-4}$
l) $a_n = (3^n - 4a_{n-1})/3$

Determinar cuáles de estas son:

1) Lineales con coeficientes constantes (RRLCC).
2) Lineales homogéneas con coeficientes constantes (RRLHCC).
3) Además, determinar el orden de las que lo sean.

4.42 En cada uno de los siguientes casos se da una fórmula explícita. Determinar el término indicado en cada caso.

a) $a_n = 2n + 3;\quad a_4 =$
b) $a_n = n/(n + 1);\quad a_5 =$
c) $a_n = (2n - 1)^2;\quad a_4 =$
d) $a_n = (-3)^{n;}\quad a_3 =$

4.43 Determinar la fórmula explícita que representa cada una de las siguientes progresiones.

a) 1, 3, 5, 7, …
b) 17, 14, 11, 8, …
c) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}$
d) 1, 9, 25, 49, …

4.44 Sean las siguientes sucesiones de recurrencia:

a) $-9, -3, 3, 9, \ldots$
b) $-1, 3, 3, 15, \ldots$
c) $-9, -3, 9, -2457, \ldots$
d) $-9, 3, -1, 1/3, \ldots$
e) $-9, -3, 3, 45/8, \ldots$

Y sean las siguientes relaciones de recurrencia:

1) $a_n = (-a_{n-1})/3$
2) $a_n = (12a_{n-1} - 12a_{n-2} + a_{n-3})/8$
3) $a_n = 2a_{n-1} - a_{n-2}$
4) $a_n = -3a_{n-1} + 81a_{n-2} - 243a_{n-3}$
5) $a_n = 2a_{n-1} + 3a_{n-2}$

Hacer corresponder cada sucesión de recurrencia con su respectiva relación de recurrencia.

4.45 Encontrar el valor del término a_3 en la sucesión generada por $a_n = (2n - 1)^2$

4.46 Sean las siguientes sucesiones de recurrencia:

a) 2, 6, 10, 14, …
b) 2, 6, 12, 20, …
c) 2, 4, 6, 10, …
d) 2, 5, 10, 17, …
e) 2, 9, 37, 148, …
f) 2, 6, 17, 50, …

Y sean las siguientes relaciones de recurrencia:

1) $a_n = a_{n-1} + a_{n-2}$
2) $a_n = a_{n-1} + 2_{n-1}$
3) $a_n = a_{n-1} + 2n$
4) $a_n = a_{n-1} + 4$
5) $a_n = 3a_{n-1} - 1$
6) $a_n = 4a_{n-1} + 1$

Hacer corresponder cada sucesión de recurrencia con su respectiva relación de recurrencia.

4.47 Un concurso tiene 5 premios que suman un total de 5 000 pesos. Entre los premios sucesivos habrá una diferencia de 100 pesos. Calcular el valor del quinto premio.

4.48 Sea la relación de recurrencia lineal con coeficientes constantes:

$$-a_{n-1} - n = n^2 - a_n$$

Determinar su solución homogénea.

4.49 Sea la relación de recurrencia lineal con coeficientes constantes:

$$2a_n = 7a_{n-1} - 3a_{n-2} + 2^n$$

Determinar la ecuación característica asociada.

4.50 Sea la relación de recurrencia lineal con coeficientes constantes:

$$\sqrt{a_n} = \sqrt{a_{n-1} + a_{n-2}}$$

Determinar la ecuación característica asociada.

4.51 Determinar la relación de recurrencia con lineal con coeficientes constantes, si $\lambda_1 = 3$ y $\lambda_2 = 2$ son las raíces características asociadas a la ecuación característica.

4.52 Sea la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 6a_{n-1} + 5a_{n-2} = 0$$

Determinar su solución homogénea.

4.53 Sea la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 3a_{n-1} - 2a_{n-2} = 0$$

Determinar la ecuación característica asociada.

4.54 Determinar la relación de recurrencia lineal con coeficientes constantes, si $\lambda_1 = 5$ y $\lambda_2 = 1$ son las raíces características asociadas a la ecuación característica.

4.55 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 5a_{n-1} + 6a_{n-2} = 0$$

Determinar su solución homogénea.

4.56 Dada la ecuación característica:

$$\lambda^2 + 8\lambda + 16 = 0$$

Determinar la relación de recurrencia lineal con coeficientes constantes correspondiente.

4.57 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 3a_{n-1} - 2a_{n-2} - 3a_{n-3} = 0$$

Determinar la ecuación característica correspondiente.

4.58 Determinar la relación de recurrencia lineal con coeficientes constantes, si $\lambda_1 = 1$ y $\lambda_2 = 2$ son las raíces características asociadas a la ecuación característica.

4.59 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 4a_{n-1} + 3a_{n-2} = 0$$

Determinar su solución homogénea.

4.60 Dada la relación de recurrencia lineal con coeficientes constantes:

$$2a_n = 7a_{n-1} - 3a_{n-2} - 2^n$$

Determinar la ecuación característica asociada.

4.61 Determinar la relación de recurrencia lineal con coeficientes constantes, si $\lambda_1 = 3$ y $\lambda_2 = -2$ son las raíces características asociadas a la ecuación característica.

4.62 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n + 5a_{n-1} + 6a_{n-2} = 0$$

Determinar su solución homogénea.

4.63 Determinar la relación de recurrencia con coeficientes constantes, si $\lambda_1 = 1$ y $\lambda_2 = -2$ son las raíces de la ecuación característica.

4.64 Dada la relación de recurrencia lineal con coeficientes constantes:

$$2a_n = 7a_{n-1} + 3a_{n-2} - 2^r$$

Determinar la ecuación característica asociada.

4.65 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n + 3a_{n-1} + 3a_{n-2} + a_{n-3} = 0$$

Determinar su solución homogénea.

4.66 Determinar la relación de recurrencia lineal con coeficientes constantes si $\lambda_1 = \lambda_2 = 1$ son las raíces características de la ecuación característica.

4.67 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n = -\,3a_{n-4}$$

Determinar la ecuación característica asociada.

4.68 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - n = 3n^2 + a_{n-1}$$

Determinar su solución homogénea.

4.69 Determinar la relación de recurrencia lineal con coeficientes constante si $\lambda_1 = 1$ y $\lambda_2 = 4$ son las raíces características de la ecuación característica.

4.70 Dada la relación de recurrencia lineal con coeficientes constantes:

$$2a_n = 7a_{n-1} - 3a_{n-2} + 2^r$$

Determinar su solución homogénea.

4.71 Dada la relación de recurrencia lineal con coeficientes constantes:

$$3a_n = 3^n - a_{n-1} + 7a_{n-2}$$

Determinar la forma de la solución particular.

4.72 Dada la relación de recurrencia lineal con coeficientes constantes:

$$3a_n = 3n - a_{n-1} + 7a_{n-2}$$

Determinar la forma de la solución particular.

4.73 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 2a_{n-1} = 3^n$$

Con valor inicial $a_0 = 3$.

Determinar su solución total.

4.74 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - 2a_{n-1} = 2^n$$

Con valor inicial $a_0 = 2$.

Determinar su solución total.

4.75 Dada la relación de recurrencia lineal con coeficientes constantes:

$$a_n - a_{n-1} = 3n^2 - n$$

Con valor inicial $a_0 = 3$.

Determinar su solución total.

Problemas reto

1. En una progresión geométrica $a_1 = 4$ y la razón común $r = 3$. La suma de dos términos consecutivos es 1 296 y el producto de estos mismos términos es 314 928.

2. Determinar cuáles son estos dos términos consecutivos.

3. Dada la relación de recurrencia lineal con coeficientes constantes:

$$9a_n - 6a_{n-1} + a_{n-2} = 3(2^n) + 7(3^n)$$

Con valores iniciales $a_0 = 1$ y $a_1 = 4$.

Determinar su solución total.

4. En algunas ocasiones, una relación de recurrencia, que en apariencia no es lineal con coeficientes constantes, puede transformarse en una relación de este tipo haciendo un cambio de variable adecuado.

En los siguientes problemas, hacer el cambio de variable apropiado para después obtener la solución total a la relación de recurrencia resultante.

a) Sea la relación de recurrencia:

$$\sqrt{b_n} = \sqrt{b_{n+1}} + 2\sqrt{b_{n-2}}$$

cuyos valores iniciales son $b_0 = b_1 = 1$.
Determinar su solución total.

Sugerencia: hacer el cambio de variable

$$x_n = \sqrt{b_n}$$

b) Sea la relación de recurrencia:

$$c_n = \sqrt{\frac{c_{n-2}}{c_{n-1}}}$$

cuyos valores iniciales son $c_0 = 8$ y $c_1 = \frac{1}{2}\sqrt{2}$.

Determinar su solución total.

Sugerencia: hacer el cambio de variable $x_n = \log_2 c_n$.

5

Combinatoria

Objetivos

- Conocer los principios básicos de conteo.
- Entender la diferencia esencial entre permutaciones y combinaciones para resolver problemas de conteo.
- Aplicar los métodos de conteo para resolver problemas de la vida cotidiana.

5.1 Introducción

En este capítulo se estudian las diferentes técnicas o reglas para contar los elementos de un conjunto específico, para lo cual estos deben cumplir una condición o característica específica. El estudio y la aplicación de las técnicas o reglas de conteo es lo que en el lenguaje propio de las matemáticas se conoce como **combinatoria**.

Los primeros indicios del surgimiento de la combinatoria datan del año 2200 a.C., con el problema de los cuadrados mágicos (arreglos numéricos que tienen la propiedad de que la suma de todos los elementos de cualquier columna, renglón o diagonal siempre es el mismo número). El problema de los cuadrados mágicos fue encontrado por primera vez en un libro de origen chino, el cual era de carácter religioso. No obstante, no fue sino hasta principios del siglo XVIII que se fundó una auténtica escuela de matemática combinatoria, que fue creada y liderada por Leonhard Euler.

En sus publicaciones acerca de la partición y descomposición de enteros positivos en sumandos, Euler estableció las bases del método de las funciones generadoras. De igual modo, Euler planteó y resolvió el problema de los *Puentes de Königsberg* mediante el uso, por primera vez, de los conceptos y métodos de la teoría de grafos. El problema de los cuatro colores (planteado a mediados del siglo XIX), que consiste en demostrar que cuatro colores son suficientes para pintar las regiones de un mapa, de tal manera que todas aquellas regiones con frontera tengan asignado un color distinto, pasó de ser un mero acertijo matemático a una fuente de importantes problemas y resultados en teoría de gráficas de interés tanto teórico como en aplicaciones.

Hoy día, dicho acertijo constituye uno de los problemas teóricos más desafiantes en la historia de la combinatoria, además de que se considera el detonante de que la combinatoria haya alcanzado una gran importancia tanto en la investigación teórica como en diversas aplicaciones de ingeniería.

Figura 5.1 Leonhard Paul Euler (1707-1783), matemático y físico suizo.

Leonhard Paul Euler cursó estudios en la universidad de Basilea, Suiza, con el matemático suizo Johann Bernoulli, donde obtuvo el grado de doctor a la edad de 17 años. En 1727, invitado por la emperatriz de Rusia, se integró como miembro del profesorado de la Academia de Ciencias de San Petersburgo, donde impartió las asignaturas de física en 1730 y de matemáticas en 1733. En 1741, se convirtió en profesor de matemáticas en la Academia de Ciencias de Berlín, a petición del rey de Prusia, Federico el Grande. En su obra *Introducción al análisis de los infinitos* (1748), Euler realizó el primer tratamiento analítico completo de álgebra, la teoría de ecuaciones, la trigonometría y la geometría analítica. Asimismo, en otras de sus obras, también trató el desarrollo de series de funciones y formuló la regla por la cual solo las series convergentes infinitas pueden ser evaluadas de manera adecuada. También abordó las superficies tridimensionales y demostró que las secciones cónicas se representan mediante la ecuación general de segundo grado en dos dimensiones.

Euler es conocido en el mundo de la ciencia como poseedor de una asombrosa facilidad para los números y del raro don de realizar cálculos mentales de largo alcance. Como anécdota, se dice que en cierta ocasión cuando dos de sus discípulos realizaban la suma de unas series de 17 términos y no estaban de acuerdo con los resultados en una unidad de la quincuagésima cifra significativa, tuvieron que recurrir a Euler, quien repasó el cálculo mentalmente y en poco tiempo llegó al resultado correcto.

Euler también realizó aportaciones a la astronomía, la mecánica, la óptica y la acústica. Entre sus obras más destacadas se encuentran: *Instituciones del cálculo diferencial* (1755), *Instituciones del cálculo integral* (1768-1770) e *Introducción al álgebra* (1770).

Antes de cumplir los 30 años de edad perdió parcialmente la visión y se quedó casi ciego al final de su vida. Regresó a San Petersburgo en 1766, donde murió el 18 de septiembre de 1783.

5.2 Reglas de la suma y el producto

En combinatoria existen dos principios sencillos básicos que dan lugar a expresiones matemáticas sofisticadas para el conteo: 1. la regla de la suma y 2. la regla del producto.

En esta sección solo nos enfocamos en el estudio de la primera de estas, para lo cual, de nuevo, debemos considerar que para cualquier conjunto finito S, se escribe $|S|$ para denotar su cardinalidad; de esta manera, $|S| = |T|$ precisamente cuando S y T tienen la misma cantidad de elementos. Observemos que $|\varnothing| = 0$ y $|\{1, 2, 3, \ldots, n\}| = n \; \forall \, n \in \mathbb{N}$.

Principio o regla de la suma

El **principio o regla de la suma** puede enunciarse de la siguiente manera:
Si S y T son dos sucesos mutuamente excluyentes o disjuntos, es decir, que no se presentan al mismo tiempo, el suceso S se puede realizar de m maneras y el suceso T de n maneras; ello significa que los sucesos S o T pueden realizarse de $m + n$ maneras distintas. Este principio también puede extenderse a más de dos sucesos mutuamente excluyentes. Desde la perspectiva de las matemáticas, el principio de la suma se escribe como:

$$|S \cup T| = |S| + |T|$$

siempre que S y T sean finitos y $S \cap T = \varnothing$.

En general, si S y T son dos conjuntos finitos no disjuntos, la cardinalidad de la unión de S y T se puede escribir como:

$$|S \cup T| = |S| + |T| - |S \cap T|$$

La razón intuitiva por la cual se cumple la ecuación anterior es que cuando se calcula $|S| + |T|$ se están contando dos veces los elementos de $S \cap T$ (una vez cuando se considera $|S|$ y otra vez cuando se considera $|T|$), por lo que debemos restar $|S \cap T|$ de la suma de $|S| + |T|$ para obtener el valor exacto de $|S \cup T|$.

Cuando se considera el caso de conjuntos no disjuntos, el principio es mejor conocido como **principio de inclusión**−**exclusión**. De manera gráfica, la regla de la suma se muestra en la figura 5.2:

Ejemplo

Una biblioteca tiene 40 libros de texto de sociología y 50 de antropología. Determinar por el principio o regla de la suma de cuántos libros de texto se dispone para conocer acerca de estos temas.

Solución

Por la regla de la suma, un alumno puede elegir entre $40 + 50 = 90$ libros de texto para aprender acerca de alguno de estos temas.

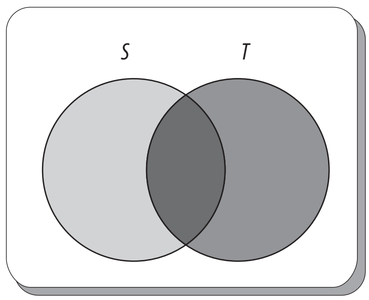


Figura 5.2 Representación gráfica de la regla de la suma.

Ejemplo

En una escuela, 20 alumnos toman clases de computación, 30 de física y 7 de ellos toman ambas asignaturas. ¿Cuántos alumnos hay en total?

Solución

Sean:

$$C = \{x \text{ t} \cdot \text{q} \cdot x \text{ es un alumno que toma la clase de computación}\}$$

y

$$F = \{x \text{ t} \cdot \text{q} \cdot x \text{ es un alumno que toma la clase de física}\}$$

Al aplicar la regla de la suma se tiene:

$$|C \cup F| = |C| + |F| - |C \cap T| = 20 + 30 - 70 = 43$$

De este modo, hay 43 alumnos en total.

Ejemplo

De 200 estudiantes que conforman la matrícula de un plantel educativo, 50 toman el curso de matemáticas discretas, 140 el curso de economía y 24 cursan ambas asignaturas. Como los profesores de ambos cursos programaron exámenes para el mismo día, solo los estudiantes que no cursen ninguna de estas asignaturas podrán asistir a la fiesta programada para la noche. Determinar cuántos estudiantes pueden asistir a la fiesta.

Solución

Sean:

$$A_1 = \{x \text{ t} \cdot \text{q} \cdot x \text{ es alumno de matemáticas discretas}\}$$

y

$$A_2 = \{x \text{ t} \cdot \text{q} \cdot x \text{ es alumno de economía}\}$$

Por la regla de la suma se tiene que:

$$|A_1 \cup A_2| = 50 + 140 - 24 = 166$$

Esto es, el número de alumnos que toman uno o ambos cursos.

Por tanto:

$$200 - 166 = 34$$

Entonces, 34 estudiantes son quienes pueden asistir a la fiesta en cuestión.

Ejemplo

¿Cuántos enteros en $A = \{1, 2, 3, \ldots, 1\,000\}$ son divisibles entre 3 y/o entre 5?

Solución

Sean:

$$D_3 = \{n \in A \text{ t} \cdot \text{q} \cdot n \text{ es divisible por 3}\}$$

Y

$$D_{5+} = \{n \in A \text{ t} \cdot \text{q} \cdot n \text{ es divisible por 5}\}$$

En este caso, se busca $|D_3 \cup D_5|$, que no es tan obvio. Como puede verse, $|D_3| = 333$; entonces, basta con dividir 1000 entre 3 y tomar la parte entera. De forma similar, se tiene que:

$$|D_5| = 200$$

Además, se tiene que:

$$|D_3 \cap D_5| = |D_{15}| = 66$$

Por tanto:

$$|D_3 \cup D_5| = |D_3| - |D_5| - |D_3 \cap D_5| = 333 + 200 - 66 = 467$$

Esto es, 467 números de A son divisibles entre 3 y/o entre 5.

En muchas ocasiones, en matemáticas es mucho más fácil contar los elementos de un conjunto que no cumplen con la condición requerida para restar dicho número del total. A continuación, se presenta un ejemplo representativ[illegible]

Ejemplo

¿Cuántos números naturales menores a 1 000 000 no son capicúas (capicúa es un número que se lee igual de izquierda a derecha que de derecha a izquierda; por ejemplo, 21 312).

Solución

Sean:

$$U = \{n \in \mathbb{N} \text{ t} \cdot \text{q} \cdot n < 1\,000\,000\}$$

y

$$A = \{n \text{ t} \cdot \text{q} \cdot n \text{ no es capicúa}\}$$

Entonces, se desea calcular $|A|$ pero esto es equivalente a $|A| = |U| - |U - A|$. Los elementos de $U - A$ tienen 1, 2, 3, 4, 5 o 6 cifras.

Calculando por separado, según el número de cifras, se tiene que:

- **Capicúas con una cifra:** Hay 9 en total: 1, 2, ..., 9.
- **Capicúas con dos cifras:** La segunda cifra debe ser igual a la primera; por tanto, hay 9 en total.
- **Capicúas con tres cifras:** La primera y tercer cifras deben ser iguales y distintas de cero. La elección de la segunda cifra es independiente de las otras; entonces, se tiene en total: $9 \times 10 = 90$.
- **Capicúas con cuatro cifras:** Las únicas que pueden elegirse ahora son la primera y la segunda cifras; ya que la primera debe ser igual a la última y la segunda igual a la penúltima, se tienen 9 elecciones posibles para la primera cifra y 10 para la segunda. Esto es, en total $9 \times 10 = 90$.

Razonando de forma análoga se tiene que:

- Hay $9 \times 10 \times 10 = 900$ capicúas de 5 cifras.
- Hay $9 \times 10 \times 10 = 900$ capicúas de 6 cifras.

Por tanto, el resultado deseado es:

$$|A| = |U| - |U - A| = 999\,999 - (9 + 9 + 90 + 90 + 900 + 900) = 998\,001$$

Ejemplo

¿Cuántos números hay del 50 al 12 000, excluyendo los múltiplos de 3 y de 5?

Solución

En este caso, lo primero es analizar el problema: del 50 al 12 000 hay $12\,000 - 50 + 1 = 11\,951$ números. Entonces, de esta cantidad se tiene que restar todos aquellos números que son múltiplos de 3 y/o 5

Así, sean:

$$N_3 = \{n \in A \text{ t} \cdot \text{q} \cdot n \text{ es múltiplo de 3 y } 50 \leq n \leq 12\,000\}$$

y:

$$N_5 = \{n \in A \text{ t} \cdot \text{q} \cdot n \text{ es múltiplo de 5 y } 50 \leq n \leq 12\,000\}$$

entonces, la solución se puede calcular a partir de:

$$11\,951 - |N_3 \cup N_5|$$

Sea además:

$$|N_3 \cup N_5| = |N_3| + |N_3| - |N_3 \cap N_5|$$

Nótese que ser múltiplo de 3 y de 5 es lo mismo que ser múltiplo de 15, por lo que:

$$N_{15} = \{n \in A \text{ t} \cdot \text{q} \cdot n \text{ es múltiplo de 15 y } 50 \leq n \leq 12\,000\}$$

Además, se tiene que: $|N_k| \leq (12\,000/k) - (49/k)$ la división es entera.

Entonces:

$$|N_3| = (12\,000/3) - (49/3) = 4\,000 - 16 = 3\,984$$

$$|N_5| = (12\,000/5) - (49/5) = 2\,400 - 9 = 2\,391$$

y:

$$|N_3| = (12\,000/15) - (49/15) = 800 - 3 = 797.$$

Así:

$$|N_3 \cup N_5| = 3\,984 + 2\,391 - 797 = 5\,578$$

Por tanto, la cantidad buscada es:

$$11\,951 - 5\,578 = 6\,373$$

EJEMPLO

Un instructor de ciencias de la computación tiene cinco libros de cada uno de los cuatro siguientes lenguajes de programación: Basic, Fortran, C y Pascal, por lo que puede recomendar cualquiera de estos 20 libros a un estudiante interesado en aprender un lenguaje de programación.

El ejemplo anterior muestra que se puede generalizar la regla de la suma.

Formalmente, si $A_1, \ldots, A_n$ son n conjuntos finitos con cardinalidad $|A_1|, \ldots, |A_n|$, respectivamente, se verifica que si $A = \{A_1, A_2 \ldots, A_n\}$ es una partición del conjunto A entonces:

$$|A| = |A_1| + |A_2| + \cdots + |A_n|$$

O bien

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

Más adelante, se retoma el estudio de la generalización de la regla de la suma cuando los conjuntos no son necesariamente disjuntos; es decir, el principio de inclusión-exclusión.

Regla del producto (principio de elección)

El segundo principio básico del conteo es el **principio de elección o regla del producto** y se enuncia de la siguiente manera: si U es un suceso que puede descomponerse en dos etapas sucesivas e independientes entre sí, S y T, la etapa S se puede realizar de m maneras y la etapa T de n maneras, independientemente de cuál haya sido el resultado en la etapa; entonces, U se podrá realizar de $m \cdot n$ maneras distintas. Este principio, al igual que el principio de la suma, también puede generalizarse a más de dos etapas.

Para conjuntos finitos S y T se tiene que $|S \times T| = |S| \cdot |T|$, ya que:

$$S \times T = \{(s, t) \text{ t} \cdot \text{q} \cdot a \in S \text{ y } t \in T\}$$

En tanto, para cada una de las $|S|$ selecciones de s en S hay $|T|$ elecciones para t en T.

Ejemplo

Sean $S = \{1, 2\}$ y $T = \{a, b, c\}$, entonces $|S| = 2$ y $|T| = 3$, por lo que:

$$|S \times T| = |S| \cdot |T| = 2 \cdot 3 = 6$$

Solución

Dichos elementos son:

$$S \times T = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

La generalización del principio del producto es muy simple, para ver esto, sean los conjuntos finitos S_1, S_2, …, S_k donde se tiene que:

$$|S_1 \times S_2 \times \cdots \times S_k| = \prod_{j=1}^{k} |S_j|$$

De manera más general, supongamos que un conjunto dado puede verse como n-adas ordenadas (S_1, …, S_n) con la siguiente estructura: hay n_1 elecciones posibles s_1.; dado s_1 hay n_2 elecciones posibles s_2. Dados s_1 y s_2 hay n_3 elecciones posibles de s_3. En general, dados S_1, S_2, …, S_n hay n_n elecciones posibles S_n. Entonces, el conjunto tiene $n_1 \cdot n_2 \cdot \cdots \cdot n_n$ elementos.

Ejemplo

Calcular el número de maneras distintas de seleccionar 5 cartas con reemplazo de una baraja de 52 cartas.

Solución

Aquí, lo primero es contar quintillas ordenadas de cartas de la baraja. El término reemplazo significa que cada carta se regresa a la baraja antes de sacar la nueva carta. El conjunto de formas de seleccionar 5 cartas con reemplazo está en correspondencia uno a uno con $D \cdot D \cdot D \cdot D \cdot D = D^5$, donde D es el conjunto de todas las cartas ($|D| = 52$).

Por tanto, por la regla del producto, el conjunto tiene 52^5 elementos diferentes a seleccionar.

Otra forma de ver esto es la que se relata a continuación. Como se puede observar, hay 52 maneras de seleccionar la primera carta; después, al regresar la carta hay 52 maneras de seleccionar la segunda y así sucesivamente; por tanto, hay $52 \cdot 52 \cdot 52 \cdot 52 \cdot 52 = 380\,204\,032$ formas de seleccionar cinco cartas con reemplazo.

Ejemplo

Calcular la forma de seleccionar 5 cartas distintas sin reemplazo de una baraja de 52 cartas. Sin reemplazo significa que una vez seleccionada una carta ya no es posible regresarla a la baraja.

Solución

En primera instancia, se puede aplicar la regla del producto de la siguiente manera: la primera carta puede seleccionarse de 52 maneras. Una vez seleccionada, la segunda carta puede elegirse de 51 maneras. La tercera puede escogerse de 50 formas, la cuarta de 49 y la quinta de 48. De manera que para elegir 5 cartas sin reemplazo existen $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48 = 311\,875\,200$ formas diferentes.

Ejemplo

El club de teatro de una universidad realiza ensayos para una obra de teatro que se presentará el próximo año.

Si seis hombres y ocho mujeres ensayan para los papeles principales (masculino y femenino), por la regla del producto, el director puede elegir a la pareja principal de $6 \cdot 8 = 48$ formas diferentes.

Ejemplo

En una fábrica donde se producen placas de automóvil, cada placa consta de dos letras y cuatro dígitos, como se observa en la figura 5.3.

a) Si ninguna letra o dígitos se puede repetir habrá:

$$27 \cdot 26 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 3\,538\,080$$

placas diferentes posibles.

b) Si se permite repetir las letras y los dígitos será posible tener:

$$27 \cdot 27 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 7\,290\,000$$

placas diferentes.

c) Si no se permite que dos dígitos juntos se repitan, entonces habrá:

$$27 \cdot 27 \cdot 10 \cdot 9 \cdot 9 \cdot 9 = 5\,314\,410$$

placas diferentes.

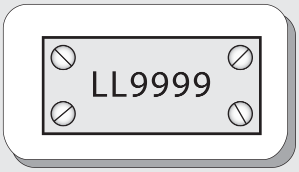


Figura 5.3 Placas de un automóvil.

5.3 Recursos de conteo: listas y árboles

Tanto las listas como los árboles constituyen importantes recursos de conteo, además de que son herramientas indispensables que se utilizan cuando se quieren conocer los posibles resultados de un evento o de una sucesión de eventos, con el fin de poder visualizarlo mediante una enumeración detallada de los elementos resultantes; es decir, mediante una lista o una forma gráfica de árbol (en el capítulo 7 se verá con más detalle qué son los árboles).

Para comprender mejor estos recursos, a continuación se observa un ejemplo detallado:

Ejemplo

El menú de un restaurante consta de dos entradas, tres platos principales y cuatro bebidas, como se observa a continuación:

Entrada	Plato principal	Bebida
Nachos (N)	Hamburguesa (H)	Té helado (T)
Ensalada (E)	Quesadillas (Q)	Limonada (L)
	Filete de res (F)	Cerveza (C)
		Refresco (R)

Determinar cuántas posibles combinaciones de comidas diferentes se pueden realizar que consten de un plato principal y una bebida.

Solución

Si se listan todas las posibles comidas que constan de un plato principal y una bebida se tiene:

HT, HL, HC, HR,
QT, QL, QC, QR,
FT, FL, FC, FR

Esto significa que hay 12 comidas (opciones) diferentes.

Ya que hay 3 platos principales y 4 bebidas, por la regla del producto se tiene que:

$$3 \cdot 4 = 12$$

comidas diferentes.

Además, existen 24 comidas diferentes que constan de una entrada, un plato principal y una bebida, las cuales son:

NHT, NHL, NHC, NHR, NQT, NQL,
NQC, NQR, NFT, NFL, NFC, NFR,
EHT, EHL, EHC, EHR, EQT, EQL,
EQC, EQR, EFT, EFL, EFC, EFR

Dado que hay dos entradas, tres platos principales y cuatro bebidas, se tiene que (por la regla del producto) existen:

$$2 \cdot 3 \cdot 4 = 24$$

comidas diferentes.

Las posibles opciones de comidas en el menú se pueden representar no solo por listas que sirven para enumerar las posibles alternativas, sino que también se pueden representar en forma gráfica mediante árboles, como se muestra en la figura 5.4.

Mediante el árbol que se observa en la figura 5.4 se representan las 12 posibles opciones para elegir una comida que conste de un plato principal y una bebida.

En cambio, en la figura 5.5 se muestra el árbol de las 24 diferentes opciones que constan de una entrada, un plato principal y una bebida.

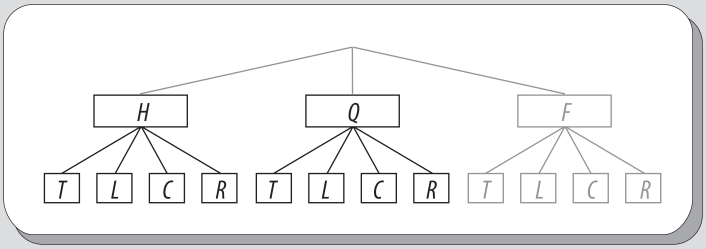


Figura 5.4 Árbol que representa las opciones que constan de un plato principal y una bebida.

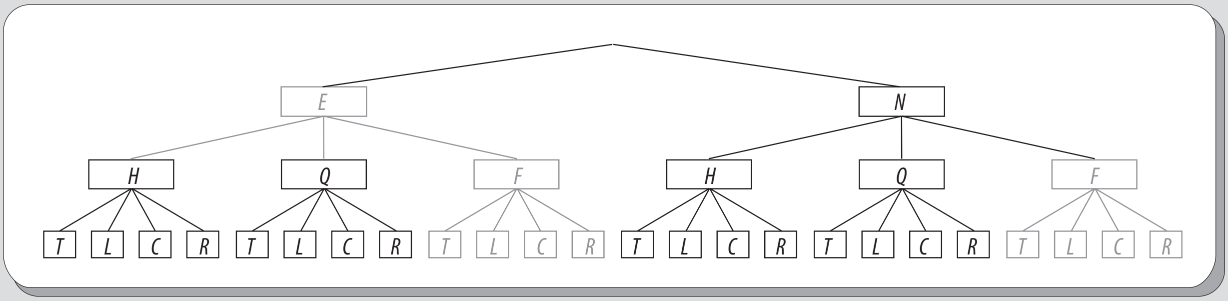


Figura 5.5 Árbol que representa las diferentes opciones de una comida compuesta por una entrada, una bebida y un plato principal.

Como se observa en el ejemplo anterior, estos recursos de conteo (listas o árboles) son útiles cuando los elementos a representar son pocos.

Pero, cuando los elementos que es necesario representar constituyen un número considerable, entonces no es práctico utilizarlos, ya que sería bastante complicado tratar de hacerlo con estos recursos.

5.4 Permutaciones y combinaciones

Es común que cada uno de los pasos en que se divide un proceso de conteo se interprete como un ordenamiento o selección de k objetos diferentes elegidos de un conjunto de n objetos, también diferentes.

Con el objetivo de contabilizar las selecciones posibles en un conjunto, estas pueden dividirse en dos categorías esencialmente distintas: **permutaciones** y **combinaciones**.

La diferencia entre una permutación y una combinación radica en que en las permutaciones el orden en que se realiza la selección es importante mientras que en las combinaciones el orden no importa.

De manera formal, dado un conjunto que contiene n elementos distintos $X = \{x_1, x_2, \ldots, x_n\}$, se tiene que:

a) Una permutación de X es una ordenación de los n elementos $x_1, x_2, \ldots, x_n$
b) Una permutación-k, o k-permutación, de X, donde $k \leq n$ es una ordenación de un subconjunto de k elementos de X.
c) El número de permutaciones–k de un subconjunto de n elementos distintos se denota como $P(n, k)$ o nPk
d) Una combinación-k, o k-combinación, es una selección no ordenada de k elementos de X,; es decir, un subconjunto de elementos de X.
e) El número de combinaciones-k de un conjunto de n elementos distintos se denota como $C(n, k)$, $\binom{n}{k}$ o nCk.

Ejemplo

Si consideramos el conjunto $X = \{a, b, c\}$ en este caso las posibles permutaciones de X son: *abc*, *bac*, *bca*, y *cba*.

Esto es, existen seis formas distintas de ordenar los tres elementos de X; desde el punto de vista de una selección de objetos, por ejemplo para *cab* esto significa que en primer lugar se selecciona *c*, luego *a* y, por último *b*.

Además

- Las permutaciones-1 de X son: *a*, *b*, *c*.
- Las permutaciones-2 de X son: *ab*, *ba*, *ac*, *ca*, *bc*, *cb*.
- Las permutaciones-3 de X son: las permutaciones de X, es decir, *abc*, *acb*, *bac*, *bca*, *cab* y *cba*.

Por otro lado, solo existe una combinación de X puesto que, al no ser importante el orden de selección, se tiene que $abc = acb = bca = cab = cba$.

Además

- Las combinaciones-1 de X son: *a*, *b*, y *c*.
- Las combinaciones-2 de X son: *ab*, *ac*, *bc*.

La importancia del orden (permutaciones) se debe a que cada selección representa algo diferente; para comprender con más detalle esto, en el siguiente ejemplo se observa un caso práctico que se presenta por lo común en la vida cotidiana.

Ejemplo

De un grupo de 15 personas se deberá elegir un comité formado por un presidente, un secretario y un vocal, ¿de cuántas formas se puede formar dicho comité?

Solución

Este, con toda claridad, es un problema donde el orden es muy importante; a saber, si consideramos el conjunto de todas las personas elegibles $P = \{P_1, P_2, \ldots, P_{15}\}$ y que la primera persona seleccionada será presidente, la segunda el secretario y la tercera el vocal, es claro que, por ejemplo, la selección $P_1P_2P_3$ es diferente a la selección $P_1P_3P_2$, pues mientras en la primera la persona etiquetada como P_2 tomaría el puesto de secretario y P_3 de vocal, en la segunda P_3 tomaría el puesto de secretario y P_2 el de vocal.

Por lo anterior, para calcular los distintos comités que es posible formar, primero se deben calcular las permutaciones-3 de P. Así, para elegir al presidente se tienen 15 opciones; una vez elegido el presidente, entonces se dispone de solo 14 opciones para elegir al secretario; por último, el vocal se puede elegir de 13 opciones. Por la regla del producto, el total de comités equivale a:

$$15 \cdot 14 \cdot 13 = 2\,730$$

El método utilizado en este ejemplo se generaliza en el siguiente teorema.

Teorema

El número de permutaciones-k de un conjunto de n objetos distintos es $P(n, k) = (n)(n-1)(n-2)\ldots(n-k+1)$. La demostración de este teorema es directa aplicando la regla del producto.

Ejemplo

De acuerdo con este teorema, el número de permutaciones-2 de $X = \{a, b, c, d\}$ es: $4 \cdot 3 = 12$, las cuales son:

ab, ac, ad, ba, bc, bd, ca, cb, cd, da, db, dc

Existe una forma alternativa de calcular el número de permutaciones en un conjunto de n elementos considerando lo siguiente:

$$P(n, n) = n(n-1)(n-2)\ldots(3)(2)(1) = n!$$

y que

$$(n-k)! = (n-k)\ldots(3)(2)(1)$$

Además:

$$P(n, k)\cdot(n-k)! = n!$$

Por tanto:

$$\begin{aligned} P(n, k) &= (n)(n-1)(n-2)\ldots(n-k+1) \\ &= \frac{(n)(n-1)(n-2)\ldots(n-k+1)(n-k)\cdots(1)}{(n-k)(n-k-1)\cdots(1)} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

Ejemplo

¿De cuántas maneras se pueden seleccionar un presidente, un vicepresidente, un secretario y un tesorero entre un grupo de 10 personas?

Solución

De acuerdo con el teorema sobre permutaciones, la respuesta es:

$$P(10,\ 4)=\frac{10!}{(10-4)!}=5\,040$$

Por supuesto, si se aplica la regla del producto se obtiene el mismo resultado:

$$10\cdot 9\cdot 8\cdot 7=5\,040$$

Ejemplo

¿De cuántas maneras posibles pueden formarse en una fila 7 personas con nacionalidad mexicana y 5 estadounidenses si ninguna pareja de estadounidenses puede estar junta?

Solución

Se puede formar a los mexicanos y a los estadounidenses mediante un proceso de dos partes. Los mexicanos pueden formarse de $7!=5\,040$ maneras distintas.

Ahora bien, una vez formados los mexicanos, como ninguna pareja de estadounidenses puede estar junta, estos últimos tienen 8 posiciones en las cuales pueden acomodarse; esto es:

$$\_\_M1\ \_\_\ M2\ \_\_M3\ \_\_M4\ \_\_M5\ \_\_M6\ \_\_M7\ \_\_$$

Así, los estadounidenses pueden formarse de:

$$P(8,\ 5)=\frac{8!}{(8-5)!}=6\,720$$

maneras distintas.

Por último, por la regla del producto tenemos que existen:

$$5\,040\cdot 6\,720=33\,868\,800$$

filas diferentes de mexicanos y estadounidenses con las condiciones mencionadas.

Ejemplo

Se requiere colocar 3 pelotas, una de color rojo, una azul y una blanca, en cajas numeradas del 1 al 10. Por tanto, se desea conocer el número de maneras distintas en que pueden ser colocadas las pelotas en las cajas, considerando que cada caja solo puede contener una pelota.

Solución

Primero, colocamos las pelotas una a la vez, iniciando con la pelota roja, luego la azul y después la blanca. Puesto que la pelota roja puede colocarse en cualquiera de las 10 cajas, la azul en cualquiera de las 9 restantes y la blanca en cualquiera de las 8 restantes, el número total de maneras distintas de colocar estas pelotas es:

$$P(10,\ 3)=\frac{10!}{(10-3)!}=720$$

Ejemplo

Determinar de cuántas maneras posibles pueden ser programados tres exámenes dentro de un periodo de 5 días, de modo que no sean programados 2 exámenes el mismo día.

Solución

En total, hay 60 formas de hacer la programación de exámenes:

$$P(5, 3) = \frac{5!}{(5-3)!} = 60$$

Ejemplo

Determinar cuántas maneras distintas de ordenar las letras ABCDEF contienen las letras DEF juntas, y en ese orden.

Solución

Para garantizar la presencia del patrón DEF, en los ordenamientos, se puede considerar a las letras DEF como un solo objeto, pues estas tres letras deben estar juntas y en ese orden. Entonces, se desea calcular el número de permutaciones del conjunto $X = \{DEF, A, B, C\}$, es decir, el número de selecciones de cuatro objetos distintos de X, considerando que el orden es importante, por lo que la respuesta es:

$$P(4, 4) = 4! = 24$$

Ejemplo

Determinar cuántas maneras distintas de ordenar las letras ABCDEF contienen las letras DEF juntas, pero en cualquier orden.

Solución

Este problema se puede resolver en dos pasos. Primero, si se fija un ordenamiento para las letras DEF, el número de ordenamientos de acuerdo al ejemplo anterior es 24. En segundo lugar, es necesario considerar que las letras DEF se pueden ordenar de $P(3, 3) = 3! = 6$ formas distintas, por lo que el número de ordenamientos que contiene a las letras DEF juntas pero en cualquier orden es:

$$6 \cdot 24 = 144$$

Ejemplo

Se requiere colocar tres pelotas de colores diferentes en 10 cajas con numeración distinta; para ello, supóngase que una caja puede contener tantas pelotas como se quiera.

Solución

En este caso, la primera pelota puede colocarse en cualquiera de las 10 cajas, como puede hacerse con la segunda y la tercera pelotas; de acuerdo con esto, el número total de colocaciones diferentes es:

$$10 \cdot 10 \cdot 10 = 1000$$

En general, hay n^k maneras de colocar k pelotas de colores dentro de n cajas numeradas, si una caja puede contener tantas pelotas como queramos.

Ahora, regresemos al tema de las combinaciones. Como se discutió antes, en problemas de conteo donde el orden es importante, es claro que las permutaciones-k son relevantes. No obstante, muchas veces el orden no es importante, en cuyo caso la habilidad para contar conjuntos también adquiere importancia.

Se sabe que un conjunto S con n elementos tiene 2^n subconjuntos en total. Para $0 \leq r \leq n$ sea $\binom{n}{k}$ el número de subconjuntos de S con k elementos. El número $\binom{n}{k}$ se llama coeficiente binomial y se lee "n en k"; en ocasiones, también se le llama el número de combinaciones de n objetos, tomando k a la vez.

El siguiente teorema formaliza la relación que existe entre $\binom{n}{k}$ (número de combinaciones-k) con $\frac{n'}{(n-k)!}$ (número de permutaciones$-k$) de un conjunto con n elementos.

Teorema

Para $0 \leq k \leq n$ se tiene que:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

DEMOSTRACIÓN

Sea S un conjunto con n elementos. Para cada subconjunto de T en S elementos hay $k!$ permutaciones de S que utilizan elementos de T; por tanto, hay $\binom{n}{k}k!$ permutaciones de S en total, es decir:

$$\begin{matrix} n \\ k \end{matrix}\, k! = P(n, k) = \frac{n!}{(n-k)!}$$

Entonces:

$$\begin{matrix} n \\ k \end{matrix} = \frac{n!}{(n-k)!k!}$$

Ejemplo

¿Cuántas manos diferentes de póker hay en una baraja de 52 cartas?

Solución

Es claro que el orden de selección de las cinco cartas que conforman una mano de póker no importa; es decir, al ser las mismas cinco cartas no es relevante el orden en que fueron seleccionadas, pues constituye la misma mano de póker. Entonces, el número total de manos de póker es:

$$\begin{matrix} 52 \\ 2 \end{matrix} = \frac{52!}{(52-5)!5!} = 258\,960$$

Ejemplo

Se quieren colocar tres pelotas, todas del mismo color, en 10 cajas que están numeradas del 1 al 10. El objetivo es conocer el número de maneras distintas en que las pelotas pueden distribuirse, si cada caja puede contener solo una pelota.

Solución

La respuesta (otra vez) equivale a una combinación- k; es decir:

$$\begin{matrix} 10 \\ 3 \end{matrix} = \frac{10!}{(10-3)!3!} = 120$$

maneras distintas de colocar las pelotas.

Ejemplo

Una ama de casa desea programar cenas que incluyan espagueti tres veces por semana. Determinar de cuántas maneras distintas puede el ama de casa hacer dicha programación de cenas.

Solución

La cantidad de maneras distintas de programar las cenas es:

$$\binom{7}{3} = \frac{7!}{(7-3)!3!} = 35$$

En el siguiente ejemplo se plantea el hecho de elegir un comité de tres personas, en el cual ninguna de estas tendrá cargo alguno. Por tanto, en este caso el orden de selección no es importante (combinaciones), a diferencia del ejemplo donde se buscaba seleccionar un presidente, un secretario y un vocal (permutaciones) para un comité.

Ejemplo

Un grupo de cinco estudiantes, María, Pedro, Rosa, Andrés y Norma decidió hablar con el jefe del Departamento de Matemáticas para solicitar que esta área ofrezca más cursos de matemáticas discretas.

El jefe de departamento notificó que solo hablará con tres estudiantes en su oficina. Determinar de cuántas maneras se puede elegir los tres estudiantes para hablar con el jefe del departamento.

Solución

Como ya se aclaró antes, el orden de selección no es importante; por tanto, el resultado es:

$$\binom{5}{3} = \frac{5!}{(5-3)!3!} = 10$$

maneras diferentes de elegir a las tres personas del grupo de cinco personas.

Ejemplo

Determinar de cuántas formas puede elegirse un comité de k personas de entre un grupo de n personas ($n \geq k$).

Solución

Este ejemplo generaliza el resultado anterior. Por tanto, existen:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

maneras distintas de elegir el comité.

Ejemplo

Determina de cuántas maneras distintas puede elegirse un comité de dos mujeres y tres hombres de un grupo de cinco mujeres y seis hombres.

Solución

En este caso, las mujeres pueden elegirse de $\binom{5}{2} = 10$ formas y los hombres de $\binom{6}{3} = 20$ formas. Por la regla del producto, se tiene que el número total de maneras que se puede seleccionar el comité es $10 \cdot 20 = 200$.

Ejemplo

Determinar cuántas cadenas de 8 bits contienen exactamente 4 unos.

Solución

La respuesta es (¿por qué?):

$$\binom{8}{4} = 70$$

cadenas diferentes.

5.5 Permutaciones y combinaciones generalizadas

Hasta ahora se han visto las combinaciones y permutaciones donde todos los elementos del conjunto son distintos entre sí. Pero en ocasiones se presentan problemas en los cuales existen objetos idénticos dentro de un conjunto.

En este caso, se dice que son permutaciones generalizadas si el orden de los objetos es importante o combinaciones generalizadas si el orden no es relevante.

Permutaciones generalizadas (particiones ordenadas)

Con frecuencia, en el mundo cotidiano, es necesario encontrar el número de permutaciones de ciertos elementos, algunos de los cuales están repetidos. La fórmula general para calcular tales ordenamientos se establece en el siguiente teorema:

Teorema

Supóngase que una sucesión S de n objetos tiene n_1 objetos idénticos del tipo 1, n_2 objetos idénticos del tipo 2,... n_t, objetos idénticos del tipo t, tal que $n_1 + n_2 + \cdots + n_t = n$; es decir, forman una partición del entero n. Entonces, el número de ordenamientos de S es:

$$\frac{n!}{n_1!n_2!\cdots n_t!}$$

Demostración

Para crear un orden de S, primero se deben asignar las posiciones de cada uno de los n objetos. Es posible asignar las posiciones de los n objetos del tipo 1 en $C(n, n_1)$ formas. Una vez realizada esta asignación, pueden asignarse las posiciones de los n_2 objetos del tipo 2 en $C(n - n_1, n_2)$ maneras, etcétera. Entonces, por la regla del producto se tiene:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{t-1}}{n_t} =$$

$$= \frac{n!}{(n-n_1)!n_1!}\cdot\frac{(n-n_1)!}{(n-n_1-n_2)!n_2!}\cdots\frac{(n-n_1-n_2-\cdots-n_{t-1})!}{(n-n_1-n_2-\cdots n_{t-1}-n_t)!n_t!}$$

Por último, simplificando se tiene:

$$\frac{n!}{n_1!n_2!\cdots n_t!}$$

Ejemplo

Determinar de cuántas maneras es posible ordenar las letras de la palabra ISSTE.

Solución

Debido a la repetición (dos veces) de la letra S, la respuesta no es 5!, sino un número inferior. Para comprobar esto, consideremos el problema de llenar 5 espacios en blanco:

— — — — —

con las letras dadas.

Esto significa que hay $\binom{5}{2}$ maneras de escoger posiciones para las dos letras S. Una vez seleccionadas las dos posiciones para la letra S, existen $\binom{3}{1}$ maneras de elegir la posición para la letra I. Ahora, una vez seleccionada la posición para la letra I, hay $\binom{2}{1}$ maneras de escoger un lugar para la letra T. Por último, queda un único lugar para ser llenado por la letra E, $\binom{1}{1}$.

Combinando este razonamiento con el teorema enunciado antes, se tiene que existen:

$$\frac{5!}{2!\cdot 1!\cdot 1!\cdot 1!} = \binom{5}{2}\binom{3}{1}\binom{2}{1}\binom{1}{1} = 60$$

maneras distintas de ordenar dichas letras.

Ejemplo

Determinar de cuántas formas se pueden repartir ocho libros distintos entre tres estudiantes, si Guillermo recibe cuatro libros, en tanto que María y Silvia reciben dos libros cada una.

Solución

Si representamos a Guillermo con la letra G, a Silvia con la letra S y a María con la letra M, es posible representar cada repartición posible con un ordenamiento de las letras GGGGMMSS, considerando, por ejemplo, que el ordenamiento GGGGMMSS significa que a Guillermo se le dan los primeros 4 libros, a María los libros 5 y 6 y a Silvia los libros 7 y 8. Por tanto, el total de formas de repartir los libros con las condiciones dadas es:

$$\frac{8!}{4!\,2!\,2!} = 420$$

Ejemplo

Determina de cuántas maneras pueden formarse tres comités distintos de un grupo de 20 personas, si los comités deben tener 3, 5 y 7 personas, respectivamente.

Solución

La respuesta es:

$$\frac{20!}{3!\,5!\,7!\,5!}$$

maneras posibles de formar dichos comités.

Recuérdese que las permutaciones generalizadas en realidad son particiones de un entero, por ese motivo fue necesario completar con 5!, que es el número de personas que no son elegidas en este momento para un comité.

Ejemplo

Una partida de bridge es una partición ordenada de 52 cartas que comprende 4 conjuntos de 13 cartas cada uno. ¿Cuántas partidas distintas de bridge existen?

Solución

En total hay:

$$\frac{52!}{13!\,13!\,13!\,13!} = 5.3645 \times 10^{28}$$

partidas de bridge.

Ejemplo

Determinar de cuántas maneras distintas pueden distribuirse 12 estudiantes en 3 grupos, cada uno conformado con 4 estudiantes, de manera que el primer grupo estudie un tema, el segundo un tema diferente y el tercero otro diferente a los dos anteriores.

Solución

El número total de formas de distribuir los estudiantes en los tres grupos es:

$$\frac{12!}{4!\,4!\,4!} = 34\,650$$

Ejemplo

Determinar de cuántas maneras pueden distribuirse 19 estudiantes en 5 grupos, de tal manera que 2 grupos queden integrados por 5 estudiantes y 3 grupos por 3, con el fin de que cada grupo estudie un tema distinto entre sí.

Solución

Para este caso se tienen en total:

$$\frac{19!}{5!\,5!\,3!\,3!\,3!} = 3.911 \times 10^{10}$$

posibles maneras de distribuir a los estudiantes.

Ejemplo

Determinar de cuántas formas es posible hacer una partición de un conjunto de 100 elementos en 50 conjuntos diferentes de 2 elementos cada uno.

Solución

En total, se tiene que hay:

$$\frac{100!}{\underbrace{2!\cdot 2!\cdot 2!\cdot \ldots 2!\cdot 2!}_{50 \text{ veces}}} = \frac{100!}{2^{50}} \approx 8.28903 \cdot 10^{142}$$

formas posibles.

Ejemplo

De forma más general, el mismo problema del ejemplo anterior puede enunciarse de la siguiente manera: Determinar de cuántas formas es posible hacer una partición de un conjunto con $2n$ elementos en n conjuntos de 2 elementos cada uno.

Solución

Entonces, la respuesta es:

$$\frac{(2n)!}{\underbrace{2!\cdot 2!\cdot 2!\cdot \ldots 2!\cdot 2!}_{n \text{ veces}}} = \frac{(2n)!}{2^{n}}$$

formas posibles.

Combinaciones generalizadas

No obstante, en diversas ocasiones también será necesario encontrar el número de combinaciones de ciertos elementos, algunos de los cuales están repetidos. La fórmula general se cita en el siguiente teorema.

Teorema

Si X es un conjunto que contiene elementos, entonces el número de selecciones de k elementos, no ordenadas, con repeticiones permitidas y tomando del conjunto X es:

$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Es importante destacar que puede utilizarse de manera indistinta cualquiera de los dos términos de la igualdad. Más adelante se demostrará la misma.

En el siguiente ejemplo se busca verificar que se cumple la igualdad combinatoria del teorema.

Ejemplo

Sea $n = 8$ y $k = 3$, entonces:

$$\begin{aligned}\binom{n+k-1}{k} &= \binom{8+3-1}{8} \\ &= \binom{10}{8} \\ &= \frac{10!}{(10-8)!8!} \\ &= 45\end{aligned}$$

Por otro lado:

$$\begin{aligned}\binom{n+k-1}{n-1} &= \binom{10}{2} \\ &= \frac{10!}{(10-2)!2!} \\ &= 45\end{aligned}$$

Nota

Es posible que k sea mayor que n cuando se permiten repeticiones.

Ejemplo

Supóngase que se tienen tres pilas de pelotas, una de pelotas rojas, una de azules y una de verdes, cada una de las cuales contiene al menos ocho pelotas.

a) Determinar de cuántas formas se pueden seleccionar 8 pelotas.
b) Determinar de cuántas maneras se pueden seleccionar 8 pelotas si se debe tener al menos una de cada color.

Solución

a) Por el teorema inmediato anterior, el número de formas para elegir 8 pelotas es:

$$\binom{8+3-1}{8} = \binom{10}{8} = 45$$

b) Si se selecciona exactamente una pelota de cada color (esto asegura que haya al menos una pelota de cada color), para completar la elección, deben escogerse 5 pelotas más. Esto es:

$$\binom{5+3-1}{3-1} = \binom{7}{2} = 21$$

formas diferentes.

Ejemplo

Determinar de cuántas maneras es posible colocar 10 canicas rojas en 5 bolsas.

Solución

El resultado se obtiene con facilidad a partir de:

$$\binom{10+5-1}{5-1} = \binom{14}{4} = 1\,001$$

Ejemplo

Determinar de cuántas maneras es posible seleccionar 10 monedas de un abasto ilimitado de monedas de dos, cinco, diez y veinte pesos.

Solución

El número total de selecciones es:

$$\binom{10+4-1}{4-1} = \binom{13}{3} = 286$$

Ejemplo

Determinar de cuántas formas pueden distribuirse 12 libros idénticos de matemáticas discretas entre 4 estudiantes.

Solución

En total, se pueden distribuir de:

$$\binom{12+4-1}{4-1} = \binom{15}{3} = 455$$

formas diferentes.

Ejemplo

Establecer cuántas soluciones enteras no negativas tiene la ecuación $x_1 + x_2 + x_3 + x_4 = 29$.

Solución

Cada solución es equivalente a elegir 29 elementos x_i del tipo i, $i = 1, 2, 3, 4$. Por tanto, el número de soluciones es:

$$\binom{29+4-1}{4-1} = \binom{32}{3} = 4\,960$$

Ejemplo

Una tienda ofrece 20 tipos diferentes de donas. Si suponemos que al menos hay una docena de cada tipo cuando entramos a la tienda, determinar de cuántas formas se puede elegir una docena de donas.

Solución

Se puede elegir una docena de donas de:

$$\binom{12+20-1}{20-1} = \binom{31}{19} = 141\,120\,525$$

formas diferentes.

5.6 Principio de inclusión-exclusión

El principio de inclusión-exclusión hace referencia al tamaño de una unión de conjuntos no disjuntos.

Sean $A_1, A_2, \ldots, A_n$ conjuntos finitos.

Recuérdese que si estos conjuntos forman una partición de un conjunto A, entonces:

$$|A_2 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

Para una mejor comprensión, veamos primero que:

Para $n = 2$ la regla de la suma afirma que:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Para $n = 3$ el principio de inclusión-exclusión afirma que:

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \\
&= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| - |A_1 \cap A_3| - |A_2 \cap A_3| + |(A_1 \cap A_3) \cap (A_2 \cap A_3)| \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|
\end{aligned}$$

Para $n = 4$ el principio de inclusión-exclusión afirma que:

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| = {} & |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - \\
& |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| - \\
& |A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \\
& |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - \\
& |A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

Generalizando:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{\substack{i,\, j=1 \\ i<j}}^{n} |A_i \cap A_j| + \sum_{\substack{i,\, j,\, k=1 \\ i<j<k}}^{n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|$$

En general, el **principio de inclusión-exclusión** se puede enunciar de la siguiente forma: para calcular la cardinalidad de $A_1 \cup A_2 \cup \cdots \cup A_n$, primero debemos calcular el tamaño de todas las posibles intersecciones de conjuntos $\{A_1, A_2, \cdots, A_n\}$, sumar los resultados obtenidos al intersecar un número impar de conjuntos y restar los resultados obtenidos al intersecar un número par de conjuntos.

En este caso, los términos "inclusión-exclusión" indican que hay que incluir o sumar los tamaños de los conjuntos, después excluir o restar los tamaños de las intersecciones de dos conjuntos, luego incluir o sumar los tamaños de todas las intersecciones de tres conjuntos, y así sucesivamente.

Tal como se analiza en la regla de la suma, este principio también puede utilizarse como una alternativa a dicha regla, sin alterar el resultado.

Ejemplo

Contar el número de enteros en $S = \{1, 2, 3, \ldots, 2\,000\}$ que son divisibles por 9, 11, 13 o 15.

Solución

Primero, para cada $k \in \mathbb{N}$ hacemos $|D_k| = \{n \in S\text{: t} \cdot \text{q} \cdot n \text{ es divisible por } k\}$ y buscamos:

$$|D_9 \cup D_{11} \cup D_{13} \cup D_{15}|$$

utilizando el principio de inclusión-exclusión.

Nótese que:

$$|D_k| \leq \frac{2\,000}{k}$$

con división entera. Por tanto, en primer lugar se calcula la cardinalidad de cada conjunto individual:

$$|D_9| = \text{Parte entera de } \frac{2\,000}{9} = 222$$
$$|D_{11}| = \text{Parte entera de } \frac{2\,000}{11} = 181$$
$$|D_{13}| = \text{Parte entera de } \frac{2\,000}{13} = 153$$
$$|D_{15}| = \text{Parte entera de } \frac{2\,000}{15} = 133$$

En segundo lugar, se calcula de la misma manera la cardinalidad de las intersecciones por parejas, es decir:

$$|D_9 \cap D_{11}| = |D_{99}| = 20$$
$$|D_9 \cap D_{13}| = |D_{117}| = 17$$
$$|D_9 \cap D_{15}| = |D_{45}| = 44$$
$$|D_9 \cap D_{13}| = |D_{143}| = 13$$
$$|D_{11} \cap D_{15}| = |D_{165}| = 12$$
$$|D_{13} \cap D_{15}| = |D_{195}| = 10$$

Aquí, por ejemplo $|D_9 \cap D_{11}| = |D_{99}|$, significa que para que un número esté en la intersección de D_9 y D_{11} dicho número deberá ser divisible por ambos de manera simultánea, es decir, debe ser divisible por $9 \cdot 11 = 99$

Obsérvese, por ejemplo, que $D_9 \cap D_{15} = D_{45}$ y no D_{135}, ya que el mínimo común múltiplo de 9 y 15 es 45.

En tercer lugar, se considera la cardinalidad de las intersecciones por ternas, es decir:

$$|D_9 \cap D_{11} \cap D_{13}| = |D_{1287}| = 1$$
$$|D_9 \cap D_{11} \cap D_{15}| = |D_{495}| = 4$$
$$|D_9 \cap D_{13} \cap D_{15}| = |D_{585}| = 3$$

Por último, se considera la intersección de los cuatro conjuntos:

$$|D_9 \cap D_{11} \cap D_{13} \cap D_{15}| = |D_{6435}| = 0$$

Ahora, por el principio de inclusión-exclusión se tiene:

$$|D_9 \cup D_{11} \cup D_{13} \cup D_{15}| = 222 + 181 + 153 + 133 - (20 + 17 + 44 + 13 + 12 + 10) + (1 + 4 + 3 + 0) - 0 = 581$$

Entonces, hay 581 enteros en S que son divisibles por 9, 11, 13 o 15.

Ejemplo

Supóngase que se tienen seis computadoras con las siguientes especificaciones que se listan en la tabla:

Computadora	Quemador Blue Ray (A_1)	Procesador CoreQuad (A_2)	Pantalla HD (A_3)
I	SÍ	SÍ	NO
II	SÍ	SÍ	SÍ
III	NO	NO	NO
IV	NO	SÍ	SÍ
V	NO	SÍ	NO
VI	NO	SÍ	SÍ

Determinar cuántas computadoras tienen uno o más de los 3 tipos de hardware.

Solución

Por el principio de inclusión-exclusión, se tiene que:

$$|A_1| = 2, |A_2| = 5, |A_3| = 3$$
$$|A_1 \cap A_2| = 2, |A_1 \cap A_3| = 1, |A_2 \cap A_3| = 3$$
$$|A_1 \cap A_2 \cap A_3| = 1$$

Por tanto:

$$|A_1 \cup A_2 \cup A_3| = 2 + 5 + 3 - 2 - 1 - 3 + 1 = 5$$

Esto es, 5 computadoras tienen uno o más de los tipos de hardware.

Ejemplo

Determinar el número de enteros positivos n de A = {1, 2, 3, ..., 100} y tal que n no es divisible entre 2, 3 o 5.

Solución

Sean:

$$D_2 = \{n \in A \text{ t} \cdot \text{q} \cdot \text{n es divisible por 2}\}$$
$$D_3 = \{n \in A \text{ t} \cdot \text{q} \cdot \text{n es divisible por 3}\}$$
$$D_5 = \{n \in A \text{ t} \cdot \text{q} \cdot \text{n es divisible por 5}\}$$

Entonces:

$$|D_2| = 50, |D_3| = 33, |A_5| = 20$$
$$|D_2 \cap D_3| = |D_6| = 16$$
$$|D_2 \cap D_5| = |D_{10}| = 10$$
$$|D_3 \cap D_5| = |D_{15}| = 6$$
$$|D_2 \cap D_3 \cap D_5| = |D_{30}| = 3$$

Aplicando el principio de exclusión—inclusión, tenemos que:

$$|D_2 \cup D_3 \cup D_5| = 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

Por tanto, 100 – 74 = 26, números que no son divisibles entre 2, 3 o 5. Estos números son los siguientes:

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97

Ejemplo

En una fábrica de automóviles se armaron 50 vehículos. Las opciones existentes son: equipado con reproductor MP3, con aire acondicionado y con frenos ABS. Se tiene que 15 de los vehículos tienen reproductor MP3, 17 aire acondicionado y 20 frenos ABS, además 5 tienen reproductor MP3 y aire acondicionado, 8 aire acondicionado y frenos ABS, 7 reproductor MP3 y frenos ABS y 3 tienen las 3 opciones. Entonces, sean:

$$A_1 = \{x \in A \text{ t} \cdot \text{q} \cdot x \text{ es un vehículo que tiene reproductor MP3}\}$$

$$A_2 = \{x \in A \text{ t} \cdot \text{q} \cdot x \text{ es un vehículo que tiene aire acondicionado}\}$$

$$A_2 = \{x \in A \text{ t} \cdot \text{q} \cdot x \text{ es un vehículo que tiene frenos ABS}\}$$

De este modo:

$$|A_1| = 15, |A_2| = 17, |A_3| = 20$$
$$|A_1 \cap A_2| = 5, |A_1 \cap A_3| = 7, |A_2 \cap A_3| = 8$$
$$|A_1 \cap A_2 \cap A_3| = 3$$

El dueño de la fábrica le ha pedido a su supervisor que le entregue un informe donde solicita lo siguiente:

a) ¿Cuántos vehículos distintos hay que tienen al menos una opción?
b) ¿Cuántos vehículos distintos hay que no tienen ninguna opción?
c) ¿Cuántos vehículos distintos hay que tienen únicamente una o dos opciones?
d) ¿Cuántos vehículos distintos hay que tienen exactamente dos opciones?
e) ¿Cuántos vehículos distintos hay que tienen exactamente una opción?

Solución

En este ejemplo, solo las dos primeras preguntas pueden ser contestadas en forma directa con el principio de inclusión-exclusión.

a) La respuesta a la pregunta del inciso a) es: todos los vehículos que tienen una, dos o las tres opciones; esto es:

$$|A_1 \cup A_2 \cup A_3| = 15 + 17 + 20 - 5 - 7 - 8 + 3 = 35$$

b) La respuesta a la pregunta del inciso b) es: todos los vehículos, excepto aquellos que tienen al menos una opción, es decir: 50 – 35 = 15 vehículos.

Para contestar las restantes preguntas tenemos que auxiliarnos de un diagrama de Venn.

Como se sabe, en este se dibujan tres círculos, uno para cada conjunto, como se observa en la figura 5.6 *i*).

Luego, se etiqueta cada círculo con la del conjunto, tal como se ve en la figura 5.6 *ii*). Acto seguido, se escribe la cardinalidad de la intersección de los tres conjuntos, como se muestra en la figura 5.6 *iii*).

Después, se escriben las cardinalidades de las intersecciones de dos conjuntos; considérese que ya hay elementos, como se distingue en la figura 5.6 *iv*).

Por último, escribimos los valores restantes para completar las cardinalidades de cada conjunto, como se ve en la figura 5.6 *v*).

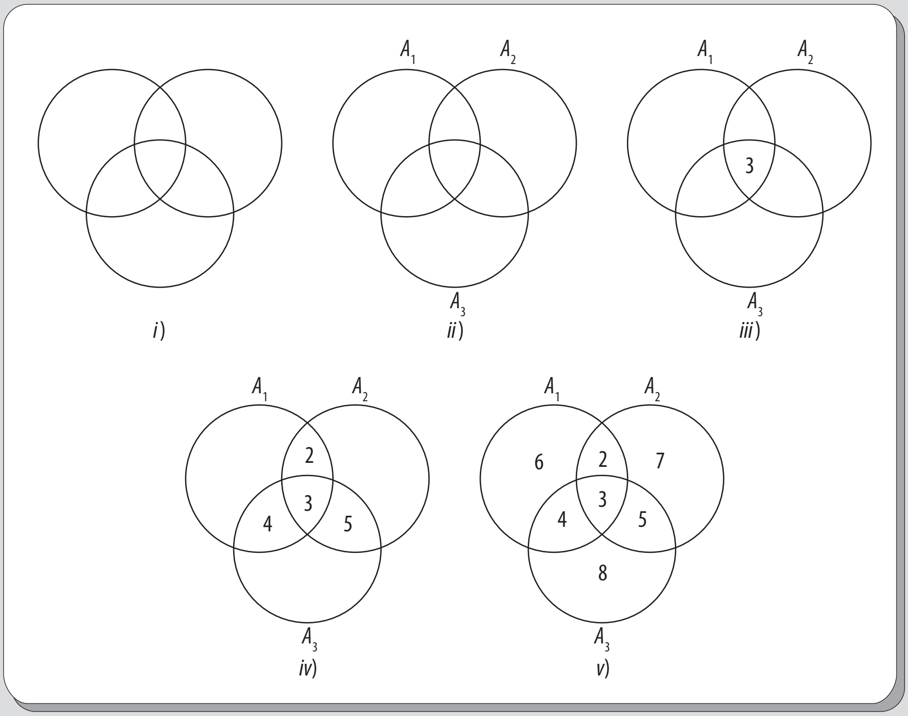


Figura 5.6 Diagrama de Venn del principio de inclusión-exclusión.

Una vez construido el diagrama de Venn, ya estamos listos para contestar las preguntas restantes.

c) Así pues, la respuesta a la pregunta del inciso c) es sumar todas las cardinalidades de los conjuntos, sin considerar la cardinalidad de la intersección de los tres conjuntos, esto es: $6 + 8 + 7 + 2 + 4 + 5 = 32$ vehículos.

d) Para la respuesta a la pregunta del inciso d), hay que sumar únicamente las cardinalidades de las intersecciones de dos conjuntos, esto es: $2 + 4 + 5 = 11$ vehículos.

e) Por último, para responder la pregunta del inciso e), es necesario sumarlas cardinalidades de los conjuntos que tienen una única opción, es decir: $6 + 7 + 8 = 21$ vehículos.

5.7 Principio de Dirichlet

Otro principio muy útil en combinatoria es el denominado **principio de Dirichlet**, también conocido como el **principio del palomar**, debido a que este se concibe a partir del siguiente problema: "si se introducen n palomas a un palomar con k nidos, $k < n$, al menos en un nido habrá 2 o más palomas".

Para ello, imaginemos 5 palomas introduciéndose en los 3 nidos de un palomar; en este caso, es claro que al menos dos de las palomas se meterán en el mismo nido (véase figura 5.7).

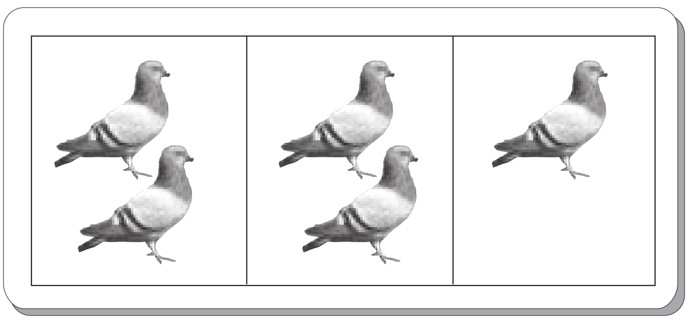


Figura 5.7 Como hay más palomas que nidos, algún nido debe tener al menos dos palomas.

Este principio no hace referencia al hecho de cómo localizar el nido que contiene 2 o más palomas, solo afirma la existencia de un nido con 2 o más palomas.

Para aplicar ese principio, primero se debe establecer cuáles objetos desempeñan el papel de las palomas y cuáles el de los nidos.

Ejemplo

En un conjunto de 32 personas, al menos 2 celebran su cumpleaños el mismo día del mes.

Solución

En este caso, si consideramos a las personas como palomas y a los días del mes como los nidos y aplicamos el principio de Dirichlet, al menos dos o más personas cumplirán años el mismo día del mes.

Ejemplo

Los nombres de un conjunto de 10 personas son: María, Bernardo y Carlos, mientras que sus apellidos son García, Pérez y López. Demostrar que al menos 2 personas tienen el mismo nombre y apellido.

Solución

Hay 9 nombres y apellidos diferentes que seleccionar, pero son diez personas en total.

Si consideramos a las 10 personas como las palomas y a los nombres y apellidos como los nidos, por el principio de Dirichlet se puede decir que al menos dos personas tienen el mismo nombre y apellido.

Ejemplo

Juan regresa de la lavandería con 12 pares de calcetines (cada par de distinto color) en una bolsa, al sacar cada calcetín de la bolsa aleatoriamente tendrá que sacar cuando mucho trece calcetines para obtener el primer par.

Ejemplo

María opera una computadora que tiene una unidad de disco duro externo para respaldar la información de la oficina donde trabaja. Un día le dan otro disco duro externo que contiene 600 000 “palabras” de cuatro o menos letras minúsculas. En el disco duro las palabras consecutivas se separan con un carácter en blanco. ¿Puede suceder que las 600 000 palabras sean distintas entre sí?

Solución

A partir de las reglas del producto y de la suma, el número total de palabras distintas posibles de cuatro o menos letras es:

$$27^4 + 27^3 + 27^2 + 27 = 551\,880$$

Si a estas 551 880 palabras las consideramos como los nidos y a las 600 000 palabras del disco duro como a las palomas, de acuerdo con el principio de Dirichlet, es posible afirmar que al menos una palabra se repite en el disco duro externo.

Ejemplo

Demostrar que cualquier subconjunto de tamaño seis del conjunto $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ contiene al menos dos elementos cuya suma es 10.

Solución

En este caso, con base en el principio de Dirichlet, los números 1, 2, 3, 4, 5, 6, 7, 8, 9 representan el papel de las palomas, mientras que son los subconjuntos $\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}$ desempeñan el papel de los nidos.

Entonces, cuando las palomas van a sus respectivos nidos, deben ocupar al menos uno de los subconjuntos cuyos miembros suman 10.

Ejemplo

Demostrar que en cualquier conjunto de 8 números enteros existen al menos dos números a y b, tales que $(a - b)$ es múltiplo de 7.

Solución

El resto de dividir un número por 7 es uno de los siete números enteros entre 0 y 6. En consecuencia, si tenemos un conjunto de 8 números, al menos dos de ellos, a y b tienen el mismo resto, r, en la división por 7.

Esto es:

$$a = 7q + r \text{ y } b = 7q' + r$$

donde:

$$0 \leq r \leq 6$$

Por tanto, $(a - b) = 7(q - q')$ es múltiplo de 7.

5.8 Identidades básicas combinatorias

En la sección combinaciones generalizadas se hace mención de que el cálculo de combinaciones generalizadas puede realizarse ya sea con el número combinatorio:

$$\binom{n+k-1}{k}$$

o con el número combinatorio:

$$\binom{n+k-1}{n-1}$$

Es decir, se afirma que tales números son iguales, lo cual en conteo se denomina "identidad combinatoria".

Dicha identidad sugiere la posibilidad de que algunos números combinatorios que, en apariencia, son distintos, en realidad representan el mismo entero.

En esta sección demostramos algunas identidades combinatorias que son muy útiles en el desarrollo matemático de la combinatoria.

En general, cualquier identidad que se obtiene de un proceso de conteo es considerada como una identidad combinatoria. Los siguientes ejemplos están destinados a presentar algunas identidades combinatorias, así como a su demostración matemática

Antes de iniciar los ejemplos, es importante recordar que por definición:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

para los enteros positivos n y k que satisfacen la desigualdad $k \leq n$.

Ejemplo

Demostrar las siguientes identidades:

a) $\binom{n}{k} = \binom{n}{n-k}$

b) $\binom{n}{k} = \binom{n}{n-k} + \binom{n-1}{k-1}$

Solución

a) Para demostrar cualquier identidad, siempre debe tomarse uno de los dos lados de esta y transformarlo al otro, mediante el uso de álgebra y, por supuesto, de la información y las identidades disponibles (que ya han sido verificadas antes).

Entonces, si para el inciso a) se toma el lado derecho y se aplica esta definición, se obtiene:

$$\begin{aligned}\genfrac{}{}{0pt}{}{n}{n-k} &= \frac{n!}{(n-(n-k))!(n-k)!}\\ &= \frac{n!}{(n-n+k)!(n-k)!}\\ &= \frac{n!}{(k)!(n-k)!}\end{aligned}$$

donde se puede ver, de la última expresión, que se obtiene:

$$\frac{n!}{(k)!(n-k)!} = \genfrac{}{}{0pt}{}{n}{k}$$

Para el caso del inciso b), si tomamos el lado derecho de la identidad y aplicamos la definición, entonces se obtiene:

$$\genfrac{}{}{0pt}{}{n-1}{k} + \genfrac{}{}{0pt}{}{n-1}{k-1} = \frac{(n-1)!}{(n-1-k)!k!} + \frac{(n-1)!}{(n-1-(k-1))!(k-1)!}$$

Simplificando la última expresión obtenemos:

$$\genfrac{}{}{0pt}{}{n-1}{k} + \genfrac{}{}{0pt}{}{n-1}{k-1} = \frac{(n-1)!}{(n-1-k)!k!} + \frac{(n-1)!}{(n-k)!(k-1)!}$$

Ahora, para sumar estas dos fracciones elegimos como denominador el mínimo común múltiplo de ambos denominadores, el cual es:

$$(n-k)!(k)!$$

pues, por definición de factorial:

$$\begin{aligned}(n-k)! &= (n-k)(n-k-1)!\\ k! &= k(k-1)!\end{aligned}$$

Entonces, la suma de las dos fracciones es:

$$\frac{(n-1)!}{(n-1-k)!k!} + \frac{(n-1)!}{(n-k)!(k-1)!} = \frac{(n-k)(n-1)! + k(n-1)!}{(n-k)!k!}$$

(recordar que $\frac{a}{b} + \frac{c}{d} = \frac{da+bc}{bd}$)

Ahora, factorizando el término $(n-1)!$ y simplificando se llega al resultado deseado:

$$\begin{aligned}\frac{(n-1)!(n-k+k)}{(n-k)!k!} &= \frac{(n-1)!(n)}{(n-k)!k!}\\ &= \frac{n!}{(n-k)!k!}\\ &= \genfrac{}{}{0pt}{}{n}{k}\end{aligned}$$

Ejemplo

Comprobar que se cumple la identidad del inciso b) del ejemplo anterior para $n = 10$ y $k = 4$.

Solución

En este caso, en primer lugar calculamos el número combinatorio:

$$\binom{n}{k} = \binom{10}{4} = \frac{10!}{(10-4)!4!} = 210$$

Por otro lado, también calculamos la suma:

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \binom{9}{4} + \binom{9}{3} \\ &= \frac{9!}{(9-4)!4!} + \frac{9!}{(9-3)!3!} \\ &= 126 + 84 \\ &= 210\end{aligned}$$

donde se verifica la identidad para este caso.

Ejemplo

Demostrar la siguiente identidad de números combinatorios:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k}$$

Solución

Aquí, primero tomamos el lado izquierdo de la igualdad y la aplicamos a la identidad (ya demostrada):

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n+1}{k+1}$$

Por tanto:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Enseguida, se vuelve a aplicar la misma identidad al último número combinatorio y se obtiene:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \binom{n-1}{k+1}$$

Repitiendo este mismo proceso (aplicación de la identidad al último número combinatorio), entonces se logra el resultado deseado:

$$\binom{n+1}{k+1} = \binom{n}{k} = \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{k}{k}$$

Ejemplo

Determinar el valor de la suma $1+2+\cdots+n$.

Solución

En primer lugar, hay que notar que:

$$\binom{n}{1}=n,$$

pues:

$$\begin{aligned}\binom{n}{1}&=\frac{n!}{(n-1)!1!}\\&=\frac{n(n-1)!}{(n-1)!1!}\\&=n\end{aligned}$$

Entonces, la suma $1+2+\cdots+n$ se puede escribir como:

$$1+2+\cdots+n=\binom{1}{1}+\binom{2}{1}+\cdots+\binom{n}{1}$$

Utilizando la identidad del ejemplo anterior ($k=1$), entonces se puede reescribir:

$$\binom{1}{1}+\binom{2}{1}+\cdots+\binom{n}{1}$$

a la forma:

$$\begin{aligned}\binom{1}{1}+\binom{2}{1}+\cdots+\binom{n}{1}&=\binom{n+1}{2}\\&=\frac{(n+1)!}{(n+1-2)2!}\\&=\frac{(n+1)(n)(n-1)!}{(n-1)!2!}\\&\frac{n(n+1)}{2}\end{aligned}$$

para al final obtener:

$$1+2+\cdots+n=\frac{n(n+1)}{2}$$

La suma del ejemplo anterior fue calculada por Gauss a la edad de 11 años, cuando su profesor le pidió a él y a sus compañeros de clase calcular la suma de los primeros 100 números naturales (al parecer con el fin de dormir un rato durante la clase). Al contrario de lo que pensaba el mentor de Gauss, este calculó la respuesta de forma casi inmediata utilizando esta identidad combinatoria. En el siguiente ejemplo se puede observar el resultado obtenido por Gauss.

Ejemplo

Calcular la suma de los primeros 100 números naturales.

Solución

Ahora que se conoce la identidad del ejemplo anterior, lo que podría representar un trabajo muy tedioso, esta se transforma a una multiplicación y una división. Es decir:

$$\begin{aligned} 1+2+\cdots+100 &= \frac{100(101)}{2} \\ &= 50 \cdot 101 \\ &= 5\,050 \end{aligned}$$

Un ejemplo de extrema importancia en el uso de las identidades combinatorias es el **teorema del binomio**, por tanto decidimos dedicar en este libro toda una sección a este y a una construcción numérica íntimamente relacionada: el **triángulo de Pascal**.

5.9 Teorema del binomio (binomio de Newton) y triángulo de Pascal

Los números combinatorios $\binom{n}{k}$ también reciben el nombre de coeficientes binomiales, pues aparecen en el desarrollo del binomio $(a+b)$ elevado a alguna potencia n. Entonces, el teorema del binomio proporciona una expresión explícita para calcular los coeficientes que se obtienen en el desarrollo de $(a+b)^n$ donde:

$$(a+b)^n = \overbrace{(a+b)(a+b)\ldots(a+b)}^{n \text{ factores}}$$

Ejemplo

Si $n=2$, se tiene:

$$\begin{aligned} (a+b)^2 &= (a+b)(a+b) \\ &= aa + ab + ba + bb \\ &= a^2 + 2ab + b^2 \end{aligned}$$

Ejemplo

Si $n=2$, se tiene:

$$\begin{aligned} (a+b)^3 &= (a+b)(a+b)(a+b) \\ &= aaa+aab+aba+abb+baa+bab+bba+bbb \end{aligned}$$

Simplificando la última expresión, por último se obtiene:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

De los dos ejemplos anteriores se puede inferir que un término de la forma $a^{n-k}b^k$ proviene de tomar el número real a de $n-k$ factores y el número real b de k factores.

Sin embargo, esta puede hacerse de $\binom{n}{k}$ formas. En la sección 5.4, Permutaciones y combinaciones, se probó que el término $\binom{n}{k}$ constituye el número de formas de seleccionar k de los n objetos dados. Por tanto, $a^{n-k}b^k$ aparece $\binom{n}{k}$ veces. Este análisis sugiere que el desarrollo del binomio debe ser de la forma:

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \cdots + \binom{n}{n} a^0 b^n$$

Este resultado se conoce como teorema del binomio, que se enuncia y se demuestra de manera formal a continuación.

Teorema

Si a y b son números reales y $n \in \mathbb{N}$, entonces

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Demostración

La siguiente demostración se llevará a cabo por inducción sobre n.

- **Paso base.** Primero, llevamos a cabo el paso base de la inducción; es decir, verificamos que el resultado sea verdadero para el primer valor de n. Si $n = 1$, el lado derecho de la igualdad en el teorema es:

  $$(a+b)$$

  El paso base se completa comprobando que se obtiene el mismo resultado del lado derecho:

  $$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^{1-1} b^1 = 1 \cdot a + 1 \cdot b = a + b$$

- **Paso inductivo.** En segundo lugar se lleva a cabo el paso inductivo, que consiste en establecer la hipótesis de inducción (la cual ya está fundamentada por el paso base) y probar que se cumple la igualdad para el siguiente entero.
- **Hipótesis inductiva.** Supóngase que el resultado es correcto hasta un entero m, $m = 1, 2 \ldots$; es decir, afirmamos que:

  $$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k$$

  Con base en la hipótesis inductiva, se debe probar que:

  $$(a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k$$

  Tomando el lado izquierdo de la igualdad anterior, se debe llegar al lado derecho solo con el uso de la hipótesis inductiva y álgebra. Entonces, en primer lugar $(a+b)^m$ se puede expresar como:

  $$(a+b)^{m+1} = (a+b)(a+b)^m$$

  Enseguida, el último término se puede reemplazar mediante el uso de la hipótesis inductiva:

  $$(a+b)(a+b)^m = (a+b)\sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k = \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k + \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^{k+1}$$

  De la primera suma se extrae el primer término y de la segunda el último para, respectivamente, obtener:

  $$\sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k = \binom{m}{0} a^{m+1} b^0 + \sum_{k=0}^{m} \binom{m}{k} a^{m-k+1} b^k$$

y

$$\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^{k+1}=\binom{m}{m}a^{0}b^{m+1}+\sum_{k=0}^{m-1}\binom{m}{k}a^{m-k}b^{k+1}$$

Considerando que se quiere expresar el resultado en una sola sumatoria, se realiza el cambio de variable (en la segunda sumatoria) $k+1=j$, con el cual se logra que, cuando $k=0$, $j=1$ y cuando $k=j-1$, $j=m$. Para la primera sumatoria, solo se toma $k=j$ y se obtiene:

$$\binom{m+1}{0}a^{m+1}b^{0}+\sum_{j=1}^{m}\binom{m}{j}a^{m-j+1}b^{j}+\binom{m+1}{m+1}a^{0}b^{m+1}+\sum_{j=1}^{m}\binom{m}{j-1}a^{m-(j-1)}b^{j}$$

$$\binom{m+1}{0}a^{m+1}b^{0}+\sum_{j=1}^{m}\left[\binom{m}{j}+\binom{m}{j-1}\right]a^{m-j+1}b^{j}+\binom{m+1}{m+1}a^{0}b^{m+1}$$

$$\binom{m+1}{0}a^{m+1}b^{0}+\sum_{j=1}^{m}\binom{m}{j-1}a^{m-j+1}b^{j}+\binom{m+1}{m+1}a^{0}b^{m+1}$$

$$=\sum_{j=0}^{m+1}\binom{m+1}{j}a^{m-j+1}b^{j}$$

Donde se hizo uso del hecho de que $\binom{m}{0}=\binom{m+1}{0}$, $\binom{m}{m}=\binom{m+1}{m+1}$ y de la identidad $\binom{m+1}{j}=\binom{m}{j}+\binom{m}{j-1}$. Entonces, por último se obtiene:

$$(a+b)^{m+1}=\sum_{j=0}^{m+1}\binom{m+1}{j}a^{m-j+1}b^{j}$$

Esto completa la demostración.

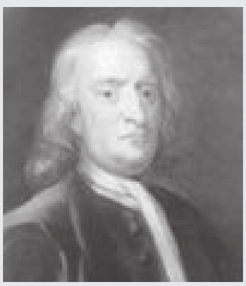


Figura 5.8 Isaac Newton (1642-1727).

Isaac Newton (Woolsthorpe, Lincolnshire, 1642-Londres, 1727) científico inglés. Durante sus primeros años de vida, su madre preparó para él un destino de granjero; sin embargo, luego de un tiempo se convenció del talento de su hijo y lo envió a la Universidad de Cambridge, en donde tuvo que trabajar para pagarse los estudios. Allí, Newton no destacó especialmente, pero asimiló los conocimientos y principios científicos de mediados del siglo XVII, con las innovaciones introducidas por Galileo, Bacon, Descartes, Kepler y otros.

Y fue hasta el año de 1665 que descubrió y postuló el teorema del binomio, el cual fue notificado por primera vez en dos cartas que envió el funcionario y administrativo de la Royal Society, Henry Oldenburg, en 1676. La primera de estas cartas fue fechada el 13 de junio de 1676, en respuesta a un pedido del filósofo, jurista y matemático alemán Gottfried Wilhelm von Leibniz, quien quería tener conocimiento de las labores e investigaciones de matemáticos británicos acerca del tema de series infinitas. A partir de este hallazgo, Newton intuyó que era posible operar con series infinitas del mismo modo que con expresiones polinómicas finitas.

Es importante destacar que Newton no se encargó de publicar jamás el teorema del binomio; tarea que realizó el matemático británico, John Wallis, en 1685, en su libro *Álgebra*, en el cual atribuyó a Newton el gran hallazgo.

Es importante notar que en el desarrollo de $(a+b)^n$ se presentan las siguientes propiedades:

- Se generan $n+1$ términos.
- La suma de los exponentes de a y b en cada término es siempre n.
- Los exponentes de a decrecen desde n hasta 0 mientras que los de b crecen de 0 a n.

- Los coeficientes de los términos equidistantes de los extremos son iguales.
- $\binom{n}{k}$ es el coeficiente de cualquier término, donde k siempre es el exponente del término b y $n-k$ el de a.

Ejemplo

Tomando $n = 3$, para el desarrollo del binomio se tiene $(a+b)^3$.

$$(a+b)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3$$

Solución

Reemplazando los valores de cada número combinatorio que aparece en la igualdad anterior, por último se obtiene:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Ejemplo

Tomando $n = 5$, para el desarrollo del binomio se tiene $(a+b)^5$.

$$(a+b)^5 = \binom{5}{0}a^5 + \binom{5}{1}a^4b + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}ab^4 + \binom{5}{5}b^5$$

Solución

Reemplazando los valores de cada número combinatorio que aparece en la igualdad anterior, al final se obtiene:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Es posible que no se desee encontrar todo el desarrollo del binomio, sino solo algún término de dicho desarrollo; en estos casos, también es muy útil el uso del teorema del binomio.

A continuación, se presenta un ejemplo para observar con mayor detalle cómo se utiliza el teorema del binomio en estos casos.

Ejemplo

Encontrar el quinto término que se obtiene del desarrollo del binomio $(a+b)^{10}$.

Solución

La expresión:

$$\binom{n}{k}a^{n-k}b^k$$

representa precisamente cómo se obtendría un término en particular.

Como n es el valor del exponente y el término solicitado menos uno representa el valor de k (recuérdese que k corre a partir de 0, donde el quinto término es $k = 4$); entonces, el término buscado es:

$$\binom{10}{4}a^{10-4}b^4 = 210a^6b^4$$

Asimismo, también se puede expresar cualquier binomio sin importar el formato de sus términos.

Ejemplo

Desarrollar el binomio $(2xy^3 + 3z^2)^3$.

Solución

Para obtener el desarrollo basta con identificar el monomio $2xy^3$ con a y el monomio $3z^2$ con b, con el fin de aplicar directamente el teorema del binomio; es decir, como en un ejemplo anterior, se obtuvo:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Haciendo el cambio de variable $a = 2xy^3$ y $b = 3z^2$ se obtiene:

$$\left(2xy^3 + 3z^2\right)^3 = \left(2xy^3\right)^3 + 3\left(2xy^3\right)^2\left(3z^2\right) + 3\left(2xy^3\right)\left(3z^2\right)^2 + \left(3z^2\right)^3$$

Por último, para obtener el resultado final solo es necesario simplificar:

$$\left(2xy^3 + 3z^2\right)^3 = 8x^3y^9 + 36x^2y^6z^2 + 54xy^3z^4 + 27z^6$$

El teorema del binomio también es útil si se quiere encontrar el desarrollo de un trinomio, cuadrinomio, etcétera.

En estos casos, lo primero que se debe hacer es agrupar los términos y utilizar de manera normal dicho teorema.

El siguiente ejemplo ilustra con mayor detalle cómo hacerlo.

Ejemplo

Desarrollar el trinomio $(x + y + z)^3$.

Solución

Primero, se agrupan dos términos del trinomio para poder identificarlo como un binomio $[(x + y) + z]^3$; es decir, el cambio de variable:

$$a = x + y \text{ y } b = z$$

transforma el trinomio a la forma:

$$[(x + y) + z]^3 = (a + b)^3$$

cuya expansión es:

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Por tanto:

$$\begin{aligned}[(x+y)+z]^3 &= (x+y)^3 + 3(x+y)^2 z + 3(x+y)z^2 + z^3\\ &= x^3 + 3x^2y + 3xy^2 + y^3 + 3x^2z + 6xyz + 3y^2z + 3xz^2 + 3yz^2 + z^3\end{aligned}$$

Triángulo de Pascal

Los coeficientes binomiales también pueden expresarse mediante un arreglo triangular conocido como **triángulo de Pascal**, donde los dos lados superiores están formados por números 1 y cualquier valor interior constituye la suma de los dos números que están por encima y a los lados de este (véase figura 5.9).

Estos coeficientes se utilizan de manera directa al escribir el desarrollo de un binomio. A continuación se presenta un ejemplo en el que se desarrolla con mayor detalle uno de estos casos.

Ejemplo

Encontrar el desarrollo del binomio $(a+b)^5$.

Solución

En este caso, primero utilizamos los valores de los coeficientes en el triángulo de Pascal (véase figura 5.9), así obtenemos en forma directa los coeficientes buscados, es decir:

$$
\begin{array}{c}
1\\
1 \quad 1\\
1 \quad 2 \quad 1\\
1 \quad 3 \quad 3 \quad 1\\
1 \quad 4 \quad 6 \quad 4 \quad 1\\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1\\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1\\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1\\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1\\
1 \quad 9 \quad 36 \quad 84 \quad 126 \quad 126 \quad 84 \quad 36 \quad 9 \quad 1\\
1 \quad 10 \quad 45 \quad 120 \quad 210 \quad 252 \quad 210 \quad 120 \quad 45 \quad 10 \quad 1\\
\vdots
\end{array}
$$

Figura 5.9 Triángulo de Pascal.

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

En apariencia, resulta muy sencillo utilizar este triángulo; sin embargo, el problema empieza cuando se pretende desarrollar un binomio grande, pues es muy posible cometer errores en los coeficientes.

El triángulo de Pascal también puede expresarse en forma de coeficientes binomiales (véase figura 5.11).

$$
\begin{array}{c}
\binom{0}{0}\\
\binom{1}{0} \quad \binom{1}{1}\\
\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}\\
\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}\\
\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}\\
\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}\\
\binom{6}{0} \quad \binom{6}{1} \quad \binom{6}{2} \quad \binom{6}{3} \quad \binom{6}{4} \quad \binom{6}{5} \quad \binom{6}{6}\\
\binom{7}{0} \quad \binom{7}{1} \quad \binom{7}{2} \quad \binom{7}{3} \quad \binom{7}{4} \quad \binom{7}{5} \quad \binom{7}{6} \quad \binom{7}{7}\\
\binom{8}{0} \quad \binom{8}{1} \quad \binom{8}{2} \quad \binom{8}{3} \quad \binom{8}{4} \quad \binom{8}{5} \quad \binom{8}{6} \quad \binom{8}{7} \quad \binom{8}{8}\\
\vdots
\end{array}
$$

Figu

Figura 5.10 Blaise Pascal (Clermont-Ferrand, Francia, 1623-París, 1662), filósofo, físico y matemático francés.

Blaise Pascal filósofo, físico y matemático francés, fue un genio precoz a quien su padre inició muy pronto en la geometría e introdujo en el círculo de Mersenne, la Academia, a la que él mismo pertenecía. Allí, Pascal se familiarizó con las ideas de Girard Desargues, por lo que en 1640 redactó su *Ensayo sobre las cónicas* (*Essai pour les coniques*), que contenía lo que hoy se conoce como teorema del hexágono de Pascal.

En el *Traité du triangle arithmétique* (*Tratado del triángulo aritmético*), publicado en 1654, Blaise Pascal reúne varios resultados ya conocidos sobre el triángulo y los emplea para resolver problemas ligados a la teoría de la probabilidad; a través de estos, él demuestra la relación entre el triángulo y la fórmula del binomio. El triángulo de Pascal fue nombrado así por Pierre Raymond de Montmort (1708), quien lo llamó "Tabla del Sr. Pascal para las combinaciones", y por Abraham de Moivre (1730) quien lo llamó *Triangulum Arithmeticum Pascalianum* (del latín: *Triángulo aritmético de Pascal*), que se convirtió en el nombre occidental moderno.

Ejemplo

Demostrar que cada elemento en el triángulo de Pascal corresponde a un número combinatorio $\binom{n}{k}$.

Solución

En primer lugar, se etiquetan los renglones del triángulo con el entero n (al renglón inicial se le asigna $n = 0$) y las diagonales con el entero k (a la diagonal inicial, de izquierda a derecha se le asigna $k = 0$). Entonces, es fácil ver que todos los elementos de la diagonal $k = 0$ son de la forma $\binom{n}{0}$, ya que:

$$\binom{n}{0} = \frac{n!}{(n-0)!0!} = \frac{n!}{n!} = 1$$

En segundo lugar, los elementos finales de cada renglón son de la forma $\binom{n}{n}$, ya que:

$$\binom{n}{n} = \frac{n!}{(n-n)!n!} = \frac{n!}{n!} = 1$$

Por último, los elementos restantes del triángulo, ubicados en el renglón n-ésimo y diagonal k-ésima, se obtienen mediante la suma de los elementos ubicados en el renglón anterior ($n - 1$), de la misma diagonal (k) y de la diagonal siguiente ($k - 1$); es decir, debemos probar que:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

No obstante, este resultado es la identidad probada en el inciso b) del primer ejemplo de la sección 5.8, Identidades básicas combinatorias.

Coeficientes multinomiales

Otra manera de desarrollar el trinomio, o en general un polinomio, es considerándolo como un coeficiente multinomial. Dados los enteros no negativos $n_1, n_2, \ldots, n_k$, tales que $n_1 + n_2 + \ldots + n_k = n$, el número:

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1!n_2!\cdots nk!}$$

es conocido como **coeficiente multinomial.** Dicho coeficiente se utiliza para generalizar el teorema del binomio, el cual se enuncia a continuación.

Teorema

Si $a_1, a_2, \ldots, a_k$ son k números reales y n un entero positivo, entonces:

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{n_1+n_2+\cdots+n_t=n} \binom{n}{n_1, n_2, \ldots, n_k} a_1^{n_1} + a_1^{n_2} + \cdots + a_{k_1}^{n_k}$$

Ejemplo

Calcular el coeficiente multinomial $\binom{8}{4, 2, 2}$.

Solución

Por la definición de coeficiente binomial se tiene:

$$\binom{8}{4, 2, 2} = \frac{8!}{4!2!2!} = 420$$

Ejemplo

Utilizar el teorema anterior para desarrollar el siguiente trinomio:

$$(a + b + c)^3$$

Solución

En este caso, primero hay que considerar todas las tripletas de enteros no negativos (n_1, n_2, n_3), para los cuales se cumple la igualdad $n_1 + n_2 + n_3 = 3$. Es fácil ver aquí que tales tripletas son:

$$(3, 0, 0), (2, 1, 1), (2, 0, 1), (1, 1, 1), (0, 3, 0), (0, 2, 1), (1, 2, 0), (0, 0, 3), (1, 0, 2), (0, 1, 2)$$

Entonces, de acuerdo con el teorema inmediato anterior se obtiene:

$$\begin{aligned}(a+b+c)^3 &= \binom{3}{3,0,0} a^3b^0c^0 + \binom{3}{2,1,0} a^2b^1c^0 + \binom{3}{2,0,1} a^2b^0c^1 \\ &\quad + \binom{3}{3,1,1} a^1b^1c^1 + \binom{3}{0,3,0} a^0b^3c^0 + \binom{3}{0,2,1} a^0b^2c^1 \\ &\quad + \binom{3}{1,2,0} a^1b^2c^0 + \binom{3}{0,0,3} a^0b^0c^3 + \binom{3}{1,0,2} a^1b^0c^2 + \binom{3}{0,1,2} a^0b^1c^2 \\ &= a^3 + 3a^2b + 3a^2c + 6abc + b^3 + 3b^2c + 3ab^2 + c^3 + 3ac^2 + 3bc^2\end{aligned}$$

Como se observa, este coincide con el desarrollo obtenido antes.

Resumen

Los principios básicos de conteo, la regla de la suma y la regla del producto representan la base para el desarrollo de técnicas más sofisticadas de la combinatoria. Por un lado, la regla de la suma es aplicable cuando se desea conocer el número de elementos (sin redundancia) que existe en una unión de n conjuntos finitos disjuntos.

Por su parte, en el caso de que tales conjuntos no sean disjuntos, la regla de la suma es mejor conocida como el **principio de inclusión-exclusión**. Por otro lado, la regla del producto es aplicable cuando se desea contabilizar el número de elementos que existe en un producto cartesiano de n conjuntos finitos.

A partir de los principios básicos de conteo, es posible obtener técnicas de conteo más sofisticadas, entre las que destacan las permutaciones y las combinaciones. Mientras que una permutación puede identificarse como una selección ordenada de objetos (es decir, donde el orden de elección es importante), una combinación consiste en una selección no ordenada de objetos (selecciones donde el orden de elección no importa). Cuando los objetos seleccionados son indistinguibles (iguales) las selecciones ordenadas y no ordenadas reciben el nombre de permutaciones y combinaciones generalizadas, respectivamente.

En la siguiente tabla se resumen los principales resultados de las técnicas de conteo contempladas en este capítulo; además, en esta también se destaca el tipo de problema con el que se relacionan.

Tabla 5.1

Selecciones de *k* objetos elegidos de un conjunto de *n* objetos		**Distribución de *k* objetos en *n* cajas diferentes**
Selecciones **ordenadas** (no existen elementos idénticos).	$\frac{n!}{(n-k)!}$	Distribución de ***k*** objetos distintos en una sola caja.
Selecciones **no ordenadas** (no existen elementos idénticos).	$\binom{n}{k}=\frac{n!}{(n-k)!k!}$	Distribución de ***k*** objetos idénticos, uno por caja.
Selecciones **ordenadas** (existen elementos idénticos, que se repiten n_1 veces,…, n_k veces, respectivamente).	$\frac{n!}{n_1!n_2!\cdots n_k!}$	Distribución de ***k*** objetos distintos, sin límite de objetos por cada caja.
Selecciones **no ordenadas** (no existen elementos idénticos).	$\binom{n+k-1}{k}=\binom{n+k-1}{n-1}$	Distribución de ***k*** objetos idénticos, sin límite de objetos por cada caja.

El teorema del binomio de Newton y su relación con el triángulo de Pascal se establecen como parte de las aplicaciones de las técnicas de conteo y de las identidades combinatorias.

El teorema del binomio afirma que la expansión del binomio $(a+b)^n$ está dado por:

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

Problemas propuestos

Los problemas 5.1 a 5.5 se refieren a una escuela de deportes, donde hay 140 alumnos, de los cuales 40 toman clases de basquetbol, 50 de natación, 45 de ciclismo, 7 de natación y de basquetbol, 6 de natación y de ciclismo, 8 de basquetbol y de ciclismo y 3 que toman los tres cursos.

5.1 Determinar cuántos alumnos distintos hay que solo toman uno o dos cursos.

5.2 Establecer cuántos alumnos distintos hay que no toman ninguno de estos cursos.

5.3 Determinar cuántos alumnos distintos hay que toman al menos un curso.

5.4 Definir cuántos alumnos distintos hay que toman exactamente dos cursos.

5.5 Determinar cuántos alumnos distintos hay que toman exactamente un curso.

Los problemas 5.6 a 5.9 hacen referencia a una escuela donde se ofrecen cinco cursos por la mañana y siete por la tarde. Determinar cuántas opciones tiene un alumno si quiere inscribirse en:

5.6 Un curso en la mañana y otro en la tarde.

5.7 Un único curso.

5.8 Dos cursos en la mañana y dos en la tarde.

5.9 Todos los cursos posibles.

Los problemas 5.10 a 5.14 se refieren a una escuela de artes marciales en la que hay 110 alumnos, de los cuales 30 toman la clase de karate, 40 la de tae kwan do, 35 la de judo, 9 las de karate y tae kwan do, 11 las de tae kwan do y judo, 8 las de karate y judo y 6 que toman los 3 cursos.

5.10 Determinar cuántos alumnos distintos hay que toman uno o dos cursos únicamente.

5.11 Establecer cuántos alumnos distintos hay que no toman ninguno de estos cursos.

5.12 Definir cuántos alumnos distintos hay que toman al menos un curso.

5.13 Determinar cuántos alumnos distintos hay que toman exactamente dos cursos.

5.14 Establecer cuántos alumnos distintos hay que toman exactamente un curso.

Los problemas 5.15 a 5.18 hacen referencia a una escuela donde se ofrecen ocho cursos por la mañana y seis por la tarde. Cuántas opciones tiene un alumno para tomar cursos en dicha escuela si quiere inscribirse en:

5.15 Un curso en la mañana y otro en la tarde.

5.16 Un único curso.

5.17 Dos cursos en la mañana y dos en la tarde.

5.18 Todos los cursos posibles.

Los problemas 5.19 a 5.22 se refieren a una academia en la cual hay 130 alumnos, de los cuales 43 toman un curso de cerámica, 57 uno de pintura y 29 uno de escultura; en tanto, en los cursos de cerámica y pintura hay 10 alumnos, 5 en los de pintura y escultura, 5 en los de cerámica y escultura y 2 alumnos que toman los tres cursos.

5.19 Establecer cuántos alumnos distintos hay que toman exactamente un curso.

5.20 Definir cuántos alumnos distintos hay que toman al menos un curso.

5.21 Determinar cuántos alumnos distintos hay que toman exactamente dos cursos.

5.22 Establecer cuántos alumnos distintos hay que toman uno o dos cursos únicamente y cuántos alumnos distintos hay que no están inscritos en ninguno de estos cursos.

5.23 En un torneo de futbol participan 32 equipos. Los premios a entregarse son: copa de oro, copa de plata, copa de cobre y copa de bronce, del primero al cuarto lugares, respectivamente. Establecer de cuántas formas pueden repartirse las copas, si un equipo solo puede ganar una copa.

5.24 Definir cuántas maneras diferentes hay de asignar la posición de salida de ocho autos que participan en una carrera de fórmula 1.

Los problemas 5.25 a 5.28 hacen referencia a la asignación de los números del seguro social en México, los cuales constan de nueve dígitos. Para su formación, se permiten repeticiones. Determinar cuántos números distintos de seguridad social existen en los siguientes casos.

5.25 Si se toman todos los posibles números que se puedan formar.

5.26 Si el primero y el último dígitos no pueden ser ceros.

5.27 Si ningún dígito puede ser un 8.

5.28 Si todos los dígitos deben ser pares.

5.29 Determinar cuántas cadenas se pueden formar con las letras BENZENE.

5.30 Definir de cuántas maneras puede un agricultor sembrar cinco productos diferentes en cinco campos agrícolas si solo cultiva un producto en cada campo.

5.31 En el Mundial de Futbol Alemania 2006 participaron 32 equipos. Los premios fueron medallas de oro, plata y bronce, para el primero, el segundo y el tercer lugar, respectivamente. Establecer de cuántas formas distintas se pudieron repartir las medallas, si un equipo solo podía ganar una de estas.

5.32 Establecer cuántas cadenas de 8 bits tienen exactamente 3 ceros.

5.33 Si se tiene un conjunto de 6 hombres y 7 mujeres, establecer de cuántas maneras se puede elegir un comité de 5 personas.

5.34 Determinar de cuántas maneras es posible repartir 12 libros idénticos de matemáticas discretas entre 4 estudiantes.

5.35 Establecer cuántas cadenas se pueden formar con las letras de la palabra FANTASMA.

5.36 Determinar cuántas cadenas de 8 bits tienen exactamente 5 ceros.

5.37 Definir de cuántas maneras puede un agricultor sembrar 4 productos diferentes en 4 campos agrícolas, si solo cultiva un producto en cada campo.

5.38 De un conjunto de 8 hombres y 4 mujeres, ¿de cuántas maneras se puede elegir un comité de 5 personas?

5.39 Definir cuántas "palabras" pueden formarse reordenando las letras de la palabra SALESPERSONS, si las cuatro S deben ser consecutivas (juntas).

5.40 Establecer cuántos números telefónicos de siete dígitos podemos obtener si el primero, el quinto y el último dígitos no pueden ser cero y se permiten repeticiones.

5.41 El gerente general de un centro comercial desea implementar ventas nocturnas tres veces a la semana. Definir de cuántas maneras distintas se pueden implementar dichas ventas.

5.42 Un cargamento de 50 microprocesadores contiene 4 piezas defectuosas. Establecer de cuántas maneras es posible seleccionar 4 microprocesadores no defectuosos.

5.43 En una casa de huéspedes hay 30 habitaciones; durante una temporada vacacional llega una excursión con 35 personas que desean alojarse en el lugar y no quieren estar juntas. De acuerdo con esto, ¿qué asegura el principio de Dirichlet?

5.44 Determinar de cuántas formas puede elegirse un comité de 4 republicanos,3 demócratas y 2 independientes de un grupo de 10 republicanos, 12 demócratas y 4 independientes.

5.45 Establecer de cuántas maneras se pueden repartir 15 libros de matemáticas idénticos entre 6 estudiantes.

5.46 Calcular el coeficiente del término xy^3 que resulta del desarrollo del binomio $(3x - 2y)^4$.

5.47 Definir cuántos términos (distintos monomios) tiene en total el desarrollo del trinomio $(2x + 3y + z)^3$?.

5.48 Determinar el coeficiente del término x^4y^7 que se obtiene al desarrollar el binomio $(x + y)^{11}$.

5.49 Calcular el coeficiente del término x^2y^2 que resulta del desarrollo del binomio $(3x - 2y)^4$.

5.50 Establecer cuántos términos se obtienen en total del desarrollo del trinomio $(x + y + z)^2$?.

5.51 Considerar la expansión del binomio $(x^2 - y)^n$. Determine y determinar el valor que debe tomar el entero positivo n para que el cuarto término de la expansión contenga x^{10}, así como también determinar el monomio completo.

En los problemas 5.52 a 5.53 calcular la suma indicada.

5.52 $\binom{n}{0} + 2\binom{n}{1} + \cdots + 2^n\binom{n}{n}$

5.53 $\binom{n}{0} + 2\binom{n}{1} + \cdots + 2^n\binom{n}{n}$

En los problemas 5.54 a 5.56 demostrar la identidad de los números combinatorios que se indica.

5.54 $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$

5.55 $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k}$

5.56 $\binom{m+n}{k} = \binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{n}{k-1} + \cdots + \binom{m}{k}\binom{n}{0}$

Problemas reto

En el siguiente problema se pide combinar el conteo con la probabilidad; por tanto, es necesario que quien se disponga a resolverlo tenga nociones básicas de probabilidad junto con cierta destreza en el conteo, a fin de poder responder el problema de manera satisfactoria.

En un cierto día, la combinación de un sorteo público para ganar una bolsa de 60 000 000 resultó ser:

$$3, 7, 13, 19, 32, 37$$

Como la bolsa no fue repartida, al día siguiente se efectuó un nuevo sorteo, en el cual se obtuvieron las siguientes combinaciones de números:

$$10, 16, 19, 37, 47, 49$$

Como se puede apreciar, en ambos sorteos aparece la misma pareja de números: 19 y 37.

Entonces, si se considera que en el sorteo se seleccionan 6 números de entre 1 y 99, ¿cuál es la probabilidad de que en dos sorteos consecutivos aparezca la pareja de números 19 y 37? O lo que es lo mismo, ¿cuál es la probabilidad de que en dos sorteos consecutivos aparezca la misma pareja de números, fija pero arbitraria?

6

Teoría de grafos

Objetivos

- Conocer la nomenclatura y la simbología utilizadas en la teoría de grafos.
- Diferenciar los diversos tipos de grafos con base en sus propiedades y características.
- Exponer diversos algoritmos para grafos y mostrar su aplicación en problemas cotidianos.
- Comprender y utilizar algunos de los métodos usados en las demostraciones en la teoría de grafos.
- Relacionar la teoría de grafos con problemas de otras ramas de las matemáticas y de otras disciplinas.

6.1 Introducción

La teoría de grafos es considerada una de las ramas más importantes de las matemáticas modernas, dada su relativa novedad, pues su nacimiento tuvo lugar en 1736 y estuvo a cargo del matemático suizo Leonhard Euler.

Su objeto de estudio son las propiedades y las características de los grafos, que constituyen una de las herramientas básicas para la modelización de fenómenos discretos, además de que se consideran la piedra angular para la fundamentación matemática en varias áreas de las ciencias de la computación, como la teoría de cambio y lógica de diseño, la inteligencia artificial, los lenguajes formales, los gráficos por computadora, los sistemas operativos, los compiladores y la organización y recuperación de información; así como también para la comprensión de las estructuras de datos y el análisis de algoritmos.

Pero, los grafos no solo son importantes para los matemáticos y las ciencias de la computación, también son de gran utilidad para la representación de circuitos eléctricos, además de que se pueden emplear para determinar el trayecto óptimo de una empresa de mensajería (el menor costo y el más rápido) que debe repartir y recoger numerosos paquetes a diversos clientes; asimismo, la red de carreteras puede modelarse por un grafo, cuyas líneas son las vías carreteras de una ciudad a otra, donde a cada línea del grafo se le pueden asociar varios valores: longitud del camino correspondiente, tiempo de recorrido, peajes, entre otras. Con un grafo también se pueden representar las líneas del ferrocarril, entre muchos otros usos.

Por si fuera poco, los grafos también pueden utilizarse en áreas como las ciencias sociales, la lingüística, las ciencias físicas (como la física teórica o la física nuclear), las ciencias económicas, la antropología, la química, la biología, la zoología, y en diversas ingenierías (como la ingeniería en comunicaciones), entre otras muchas áreas donde es posible aplicar dicha teoría.

Por desgracia, hasta hoy día no existe una terminología estandarizada en la teoría de los grafos, por lo que es importante señalar que las definiciones y los conceptos de este libro pueden variar con respecto a otras publicaciones donde se trate este mismo tema.

Este hecho es hasta cierto punto natural, dada la gran diversidad de campos en los que la teoría de grafos se aplica; sin embargo, en ocasiones, esto suele ser complicado, en especial cuando un mismo término, en particular, se utiliza en diferentes publicaciones para referirse a conceptos diferentes; además, tampoco es raro encontrar que varios términos diferentes suelen ser usados como sinónimos.

6.2 Definiciones básicas y su representación

Para empezar a conocer el concepto de grafo, iniciaremos con un ejemplo intuitivo y después definiremos sus componentes básicos.

Ejemplo

Sea el mapa de las carreteras de algún lugar, como el que se muestra en la figura 6.1.

Determinar si existe una ruta por carretera entre dos ciudades (puntos específicos) en el mapa.

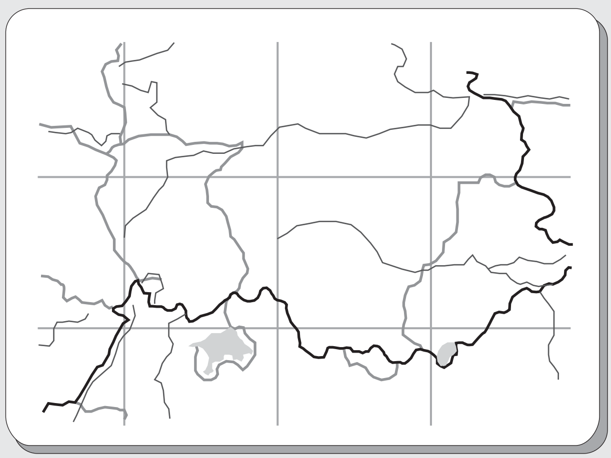


Figura 6.1 Mapa carretero.

Solución

Primero, en el caso de que exista una carretera entre dos ciudades que las una directamente, estas se unirán en el mapa con una línea recta, como se muestra en la figura 6.2.

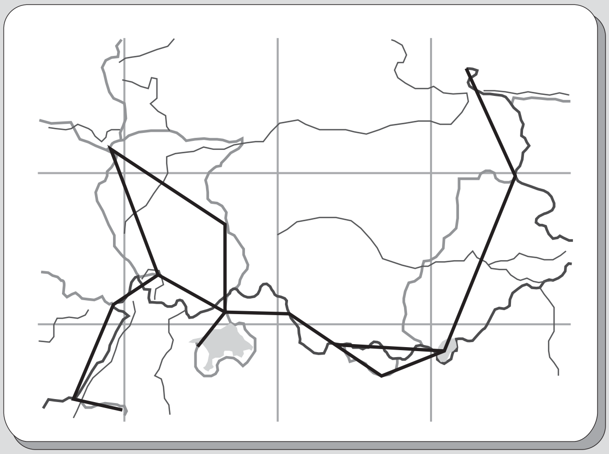


Figura 6.2 Unión de dos ciudades con una línea recta si hay una carretera entre estas.

Después, si se representan las ciudades con puntos y a continuación se borra todo, excepto los puntos y las líneas de unión, el dibujo resultante (véase figura 6.3) se conoce como grafo.

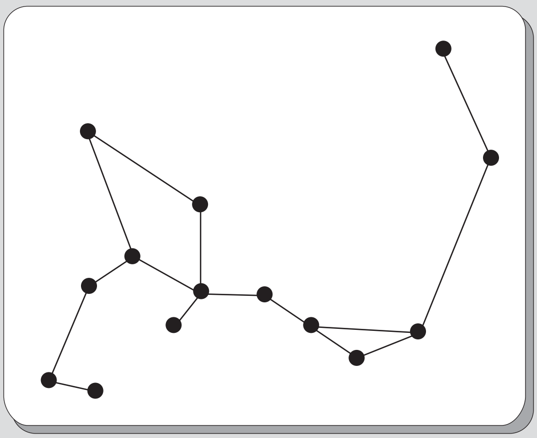


Figura 6.3 Grafo de ciudades de algún lugar y las carreteras que las unen.

Como se ve en el capítulo 3, una relación binaria puede representarse mediante un grafo, al igual que todo grafo puede ser representado como una relación binaria (véase el siguiente ejemplo).

Ejemplo

Sea el conjunto $C = \{a, b, c, \ldots, n\}$ de las ciudades y **R** una relación binaria sobre C definida como:

$$R = \{(a, b) \text{ t} \cdot \text{q} \cdot \text{existe una carretera de la ciudad } a \text{ a la ciudad } b\}$$

Determinar los elementos de esta relación binaria.

Solución

Para obtener los elementos de dicha relación binaria, primero se pueden etiquetar los vértices del grafo de la figura 6.3, como se muestra en la figura 6.4 y luego obtener la relación binaria correspondiente.

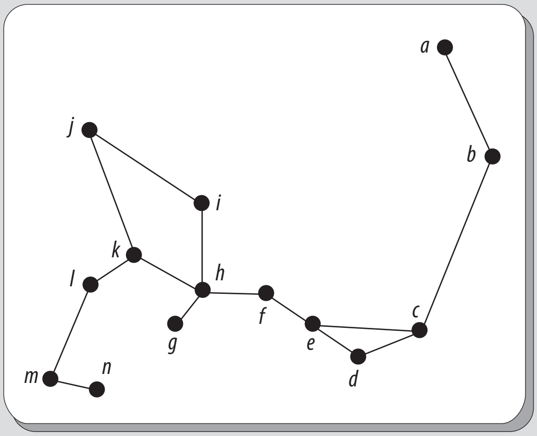


Figura 6.4 Grafo con los vértices etiquetados.

Entonces:

$$\mathrm{R} = \{(a, b), (b, c), (c, d), (c, e), (d, e), (e, f), (f, g), (g, h), (g, i), (g, k), (i, j), (j, k), (k, l), (l, m), (m, n)\}$$

es la relación binaria obtenida para dicho grafo.

El término ***grafo*** proviene de la expresión ***graphic notation*** (notación gráfica), usada por primera vez por Edward Frankland y adoptada posteriormente por Alexander Crum Brown, en 1884, la cual hacía referencia a la representación gráfica de los enlaces entre los átomos de una molécula.

Aún, hoy día, no existe una definición precisa acerca de lo que es un grafo, aunque, de manera intuitiva, siempre se ha trabajado con ellos; por tanto, este es el momento preciso para hacerlo. No obstante, cabe señalar que hay dos maneras de definirlo:

a) Grafo: definición geométrica

Desde el punto de vista geométrico, a la representación gráfica de los elementos de un conjunto y las relaciones binarias sobre estos se les conoce como grafo y consta de puntos en el espacio, algunos de los cuales están unidos entre sí mediante líneas.

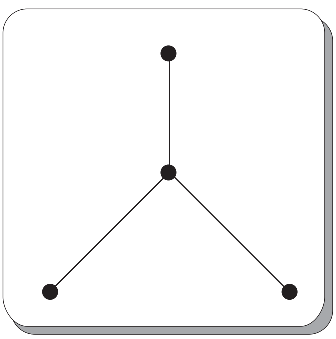


Figura 6.5 Representación de un grafo.

Los puntos del grafo se llaman ***vértices*** o nodos y representan los elementos del conjunto. Por su parte, las líneas se conocen con el nombre de ***lados*** o aristas y representan a aquellos elementos de la forma (i, j) que establecen relación entre los vértices; esto es, los vértices i y j están relacionados.

Así, de acuerdo con la definición anterior, el dibujo de la figura 6.5 representa un grafo.

Es importante señalar que un grafo solo contiene información topológica; es decir, datos sobre la conectividad o, lo que es lo mismo, acerca de la relación que existe entre los elementos del conjunto; sin embargo, estos carecen de toda información geométrica en el sentido euclidiano, como distancias, ángulos, etcétera. De este modo, los dos dibujos de la figura 6.6 representan el mismo grafo.

b) Grafo: definición algebraica

Un grafo $G = (V, E, \varphi)$, es una tripleta que consta de un conjunto V no vacío de los vértices del grafo, un conjunto $E \subseteq (V \times V)$ de los lados del grafo y una función φ, la cual es una función de los lados del conjunto E a un conjunto de pares ordenados o no ordenados de los elementos (repetidos o no) de V. Donde los conjuntos V y E del grafo son finitos. Por su parte, la función φ se conoce como ***función de incidencia*** (más adelante se define el concepto de incidencia).

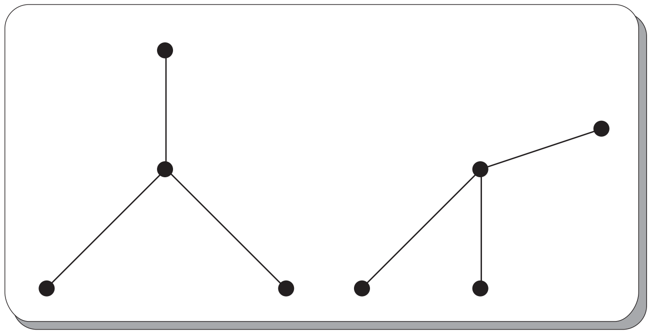


Figura 6.6 Dos dibujos que representan el mismo grafo.

En el caso de que algún lado $e \in E$, se tiene que:

$$\varphi(e) = (i, j)$$

Donde:

i y j son los ***vértices extremos*** de e, también conocidos como los extremos de e.

Para representar algebraicamente un grafo, primero es preciso etiquetar los vértices del grafo por v_i y los lados por e_j y enseguida aplicar la función de incidencia a los lados de E.

EJEMPLO

Si el primer grafo de la figura 6.6 se etiqueta como se mencionó antes, resulta el grafo que se observa en la figura 6.7. Entonces, algebraicamente se puede expresar de la siguiente forma:

$$G = (V, E, \varphi)$$

Donde:

$$V = \{v_1, v_2, v_3, v_4\}$$
$$E = \{e_1, e_2, e_3\} \text{ y}$$

Y φ está definida por:

$$\varphi(e_1) = (v_1, v_2)$$
$$\varphi(e_2) = (v_2, v_3)$$
$$\varphi(e_3) = (v_2, v_4)$$

O lo que es lo mismo:

$$\varphi(e_1) = (v_2, v_1)$$
$$\varphi(e_2) = (v_3, v_2)$$
$$\varphi(e_3) = (v_4, v_2)$$

Debido a que, como se dijo antes, no importa el orden en que se tome el par de vértices.

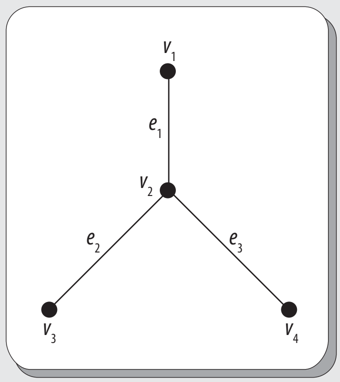


Figura 6.7 Grafo etiquetado para su representación algebraica.

En lugar de escribir $\varphi(e) = (i, j)$ es más común escribir simplemente $e = (i, j)$ para denotar a cualquier lado de un grafo.

Como se observa en el ejemplo anterior, al aplicar la función de incidencia a cada uno de los lados del grafo y al hacer la unión de los mismos, en realidad se obtiene la relación binaria **R** que origina al grafo.

EJEMPLO

En el caso del grafo de la figura 6.7 se tienen tres vértices, por lo que:

$$\bigcup_{j=1}^{3}(e_j) = \{(v_1, v_2), (v_2, v_3), (v_2, v_4)\}$$

O también:

$$\bigcup_{j=1}^{3}(e_j) = \{(v_2, v_1), (v_3, v_2), (v_4, v_2)\}$$

Como se puede observar, cualquiera de los dos casos equivale a la relación binaria **R** que da origen a dicho grafo, esto es:

$$\mathbf{R} = \{(v_1, v_2), (v_2, v_3), (v_2, v_4)\}$$

o:

$$\mathbf{R} = \{(v_2, v_1), (v_3, v_2), (v_4, v_2)\}$$

Además, es más conveniente denotar a un grafo como $G = (V, E)$, pues es la nomenclatura más utilizada, aunque también se puede denotar simplemente como G.

Hay que hacer notar que la definición de grafo implica que para cada lado del grafo se puede asociar un par ordenado o no ordenado de vértices pertenecientes al grafo.

6.3 Terminología y caracterización de los grafos

Al interior de la terminología básica de la teoría de grafos hay inmersos diversos conceptos, entre los que destacan: grafo dirigido, grafo no dirigido, orden, tamaño, grafo finito, grafo nulo, grafo completo, entre otros. Dichos conceptos y otros más se analizan con mayor detalle a continuación.

Grafo dirigido

Un grafo dirigido (o dígrafo) $G = (V, E)$ consta de un conjunto V de vértices y un conjunto $E \subseteq (V \times V)$ de lados, tal que cada $e \in E$ está asociado a un único par ordenado de vértices $i, j \in V$ y se escribe $e = (i, j)$.

Además, la dirección de un lado en un grafo dirigido se indica o denota mediante una flecha dirigida sobre este.

EJEMPLO

La figura 6.8 representa un grafo dirigido $G = (V, E)$, donde:

$V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$

O también:

$E = \{(v_2, v_1), (v_2, v_5), (v_2, v_3), (v_3, v_2), (v_3, v_6), (v_6, v_4), (v_6, v_6)\}$

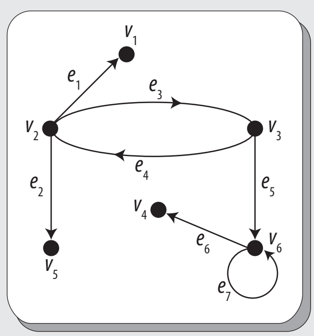


Figura 6.8 Grafo dirigido G.

Grafo no dirigido

Un grafo (o grafo no dirigido) $G = (V,\ E)$ consta de un conjunto V de vértices y un conjunto $E \subseteq (V \times V)$ de lados tales que cada lado $e \in E$ está asociado a un par no ordenado de vértices.

Si un lado e está asociado a un único par no ordenado de vértices $i, j \in V$ se escribe $e = (i, j)$ o $e = (j, i)$.

También se suele denotar a un par no ordenado de vértices como $\{i, j\}$, lo que representa $\{(i, j), (j, i)\}$. Aunque $(i, j) = (j, i)$ solo si $i = j$, se tiene que $\{i, j\} = \{j, i\}$ para cualquier par de vértices $i, j \in V$.

EJEMPLO

La figura 6.9 representa un grafo no dirigido $G = (V, E)$, donde:

$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}\}$

o también

$$E = \{\{v_1, v_4\}, \{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_8\}, \{v_7, v_8\}, \{v_6, v_7\}, \{v_5, v_6\}, \{v_4, v_5\}, \{v_1, v_5\}, \{v_2, v_7\}, \{v_2, v_8\}\}$$

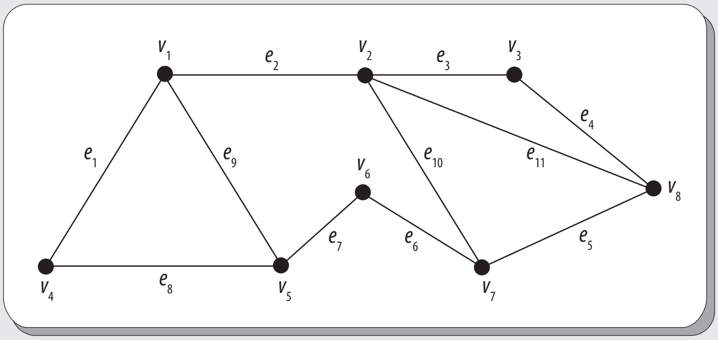


Figura 6.9 Grafo no dirigido G.

En el contexto de grafos, el lado (i, j) denota un lado de un grafo dirigido o no dirigido y no a un par ordenado de números.

Además, en general, si no se especifica que un grafo $G = (V, E)$ es dirigido o no, se entiende que este es no dirigido.

Orden y tamaño

En un grafo (dirigido o no dirigido) $G = (V, E)$, el número de vértices de G, denotado como $|V|$, se denomina ***orden*** del grafo. Por lo general, se utiliza n para denotar el orden del grafo; esto es:

$$n = |V|$$

En tanto, el número de lados de G, denotado como $|E|$, se conoce como ***tamaño*** del grafo. Por lo común, se utiliza m para denotar el tamaño del grafo; esto es:

$$m = |E|$$

EJEMPLO

Sea el grafo de la figura 6.8, su orden $|V| = 6$, mientras que su tamaño $|V| = 7$.

En tanto, si se considera la figura 6.9, su orden es $|V| = 8$ y su tamaño $|E| = 11$.

Grafo finito

Un grafo (dirigido o no dirigido) es finito si $|V|$ y $|E|$ son finitos; esto es, un grafo es finito si su orden y tamaño lo son.

Cabe hacer mención que en este libro solo se estudian grafos finitos.

Por ejemplo, tanto el grafo de la figura 6.8 como el de la figura 6.9 son finitos, ya que en ambos casos $|V|$ y $|E|$ son finitos.

Incidencia y adyacencia

En un grafo dirigido $G = (V, E)$, para cualquier lado $e = (i, j)$ se dice que e es *incidente* en los vértices i y j, los cuales son sus vértices extremos, i es *adyacente hacia* j, mientras que j es *adyacente desde* i. Además, el vértice i es el *origen* o *fuente* del lado (i, j) y el vértice j es el *término* o *vértice terminal* de dicho lado.

En un grafo no dirigido $G = (V, E)$, para todo lado $e = \{i, j\}$ se dice que e es incidente en los vértices i y j, los cuales son sus vértices extremos. Además, se dice que los vértices i y j son vértices adyacentes.

Por tanto, en cualquiera de los dos casos, se puede decir que dos vértices son adyacentes si están unidos por un mismo lado.

EJEMPLO

En el grafo no dirigido $G = (V, E)$ de la figura 6.10 se tiene que el lado e_1 está asociado al par no ordenado de vértices $\{v_1, v_2\}$, por lo que se escribe $e_1 = (v_1, v_2)$, o también $e_1 = (v_2, v_1)$.

Además, se tiene que el lado e_1 es incidente en los vértices v_1 y v_2, ya que son sus vértices extremos; por tanto v_1 y v_2 son vértices adyacentes, pues están unidos por el mismo lado.

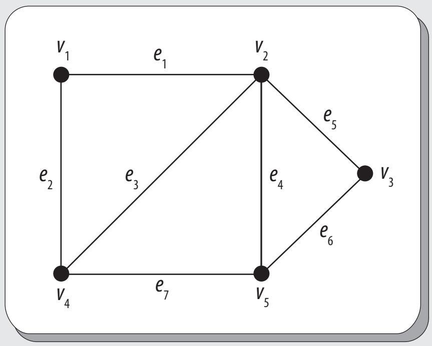


Figura 6.10 Grafo no dirigido G.

EJEMPLO

Si se considera el grafo dirigido $G = (V, E)$ de la figura 6.11, se tiene que los lados dirigidos están indicados por flechas y que el lado e_1 está asociado al par ordenado de vértices (v_2, v_1), por lo que se escribe $e_1 = (v_2, v_1)$.

También se tiene que el lado e_1 es incidente en los vértices v_1 y v_2, ya que son sus vértices extremos; por tanto, v_1 y v_2 son vértices adyacentes, pues están unidos por el mismo lado.

Además, el lado e_7 está asociado con el par ordenado de vértices (v_6, v_6), por lo que se escribe $e_6 = (v_6, v_6)$, donde e_6 es incidente en v_6 y dicho vértice es adyacente consigo mismo.

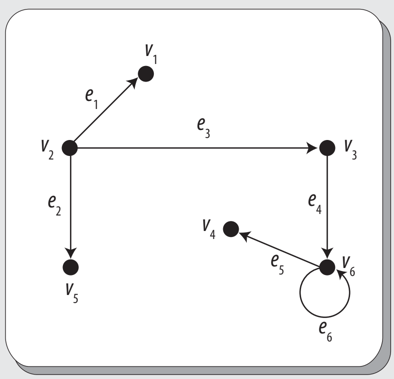


Figura 6.11 Grafo dirigido G.

Grafo nulo

Se dice que un grafo (dirigido o no dirigido) $G = (V, E)$ es nulo si tiene todos sus vértices aislados. Por vértice aislado se entiende aquel que no es extremo de ningún lado o que no tiene ningún lado incidente sobre sí.

En este caso, se ti

EJEMPLO

En la figura 6.12 se observa un grafo $G = (V, E)$ nulo, ya que todos sus vértices son aislados.

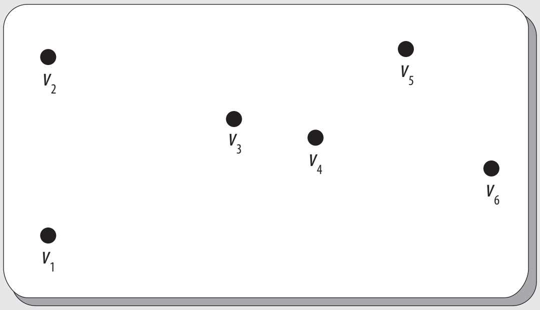


Figura 6.12 Grafo nulo G.

Lados paralelos y lazos

En un grafo (dirigido o no dirigido) $G = (V, E)$, cuando dos o más lados distintos son incidentes al mismo par de vértices, estos reciben el nombre de ***lados paralelos***.

Por su parte, un lado de la forma (i, i) que inicia y termina en el mismo vértice se conoce como ***lazo***; es decir, el vértice es adyacente consigo mismo.

EJEMPLO

Sea $G = (V, E)$ el grafo no dirigido de la figura 6.13, donde: $e_1 = (v_1, v_2)$ y $e_2 = (v_1, v_2)$, lo que significa que tiene lados paralelos, pues son incidentes con el mismo par de vértices.

Además, el lado $e_3 = (v_2, v_2)$ es un lazo, ya que es incidente consigo mismo.

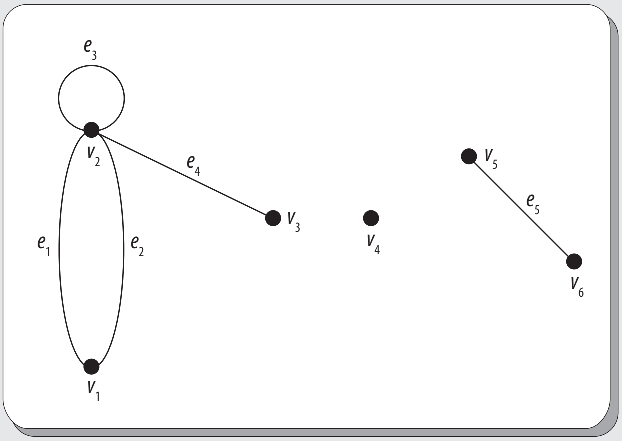


Figura 6.13 Grafo con lados paralelos y lazo.

Grafo simple

Un grafo (dirigido o no dirigido) $G = (V, E)$ que no tiene lazos ni lados paralelos recibe el nombre de grafo simple.

EJEMPLO

Sean los grafos no dirigidos de la figura 6.14. En este caso, el grafo G_1 es un grafo simple y el grafo G_2 es un grafo no simple, ya que este último tiene un lazo.

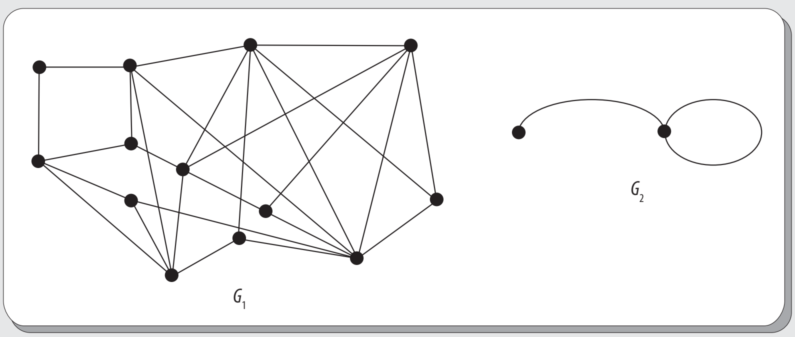


Figura 6.14 Ejemplo de grafos. G_1 grafo simple y G_2 grafo no simple.

Valencia de un vértice

En un grafo no dirigido, $G = (V, E)$, se llama ***valencia*** (o grado) de un vértice, v, al número de lados incidentes en v, y se denota como $\delta(v)$.

En un vértice que sea adyacente consigo mismo, solo se considerará una vez para el cálculo de la valencia; sin embargo, hay ocasiones que se considerará como doble, por ejemplo para determinar la existencia de un paseo o circuito de Euler en grafos no dirigidos, que se trata más adelante.

Además, se tiene que la suma de las valencias de todos los vértices de un grafo no dirigido, $G = (V, E)$, es igual al doble del número de lados; es decir, el tamaño $|E|$ del grafo, siempre y cuando el grafo no contenga lazos.

De manera formal, se denota como:

$$\sum_{i=1}^{n} \delta(v_i) = 2|E|$$

En un grafo dirigido, $G = (V, E)$, la valencia de entrada de un vértice v es el número de lados incidentes hacia este, es decir, la cantidad de flechas que llegan al vértice, y se denota como $\delta_e(v)$; mientras que la valencia de salida es el número de lados que son incidentes desde este, es decir, la cantidad de flechas que salen de dicho vértice, y se denota como $\delta_s(v)$.

Es importante resaltar aquí, que en el caso de que un vértice sea adyacente consigo mismo, solo se considerará una vez, ya sea de entrada o de salida, pero no ambas.

EJEMPLO

Sea $G = (V, E)$ el grafo no dirigido de la figura 6.13. Entonces, la valencia de cada vértice de G es:

$$\delta(v_1) = 4$$
$$\delta(v_2) = 3$$
$$\delta(v_3) = 4$$
$$\delta(v_4) = 4$$
$$\delta(v_5) = 3$$

En este caso, se tiene que la suma de las valencias de los vértices es:

$$4 + 3 + 4 + 4 + 3 = 18$$

que es el doble del tamaño del grafo $|E| = 9$.

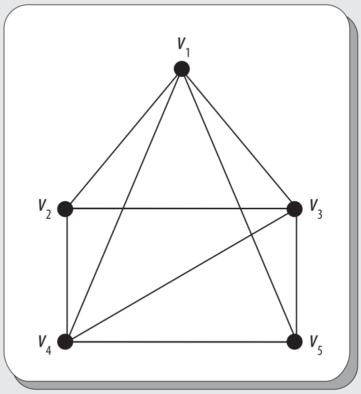


Figura 6.15 Grafo no dirigido G.

Grafo completo

Un grafo $G = (V, E)$ recibe el nombre de ***grafo completo*** de n vértices, que se denota K_n, si es simple con n vértices y además existe un lado entre cada par de vértices distintos.

De la definición anterior, se puede inferir que para que un grafo sea completo, cada vértice de **G** debe ser adyacente con todos los demás vértices del grafo.

EJEMPLO

En la figura 6.16 se muestran los primeros cinco grafos completos.

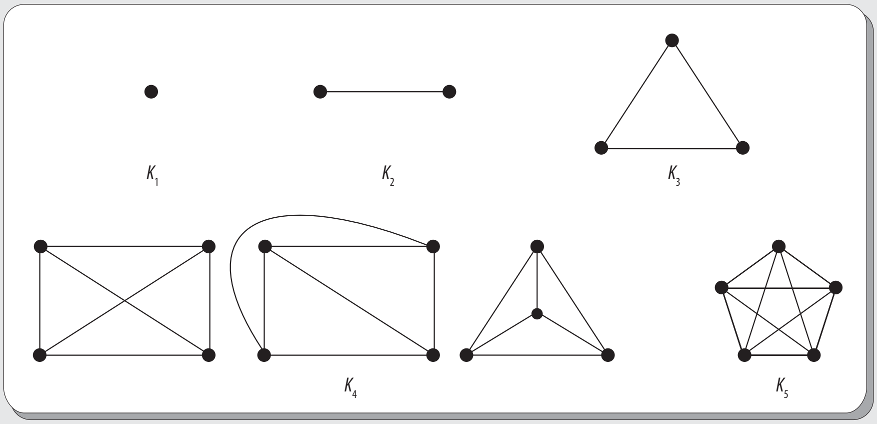


Figura 6.16 Primeros cinco grafos completos.

En el ejemplo anterior también se observa que K_4 se ha representado de varias formas diferentes, lo mismo ocurre con la mayoría de los grafos.

Ahora, sea un grafo completo K_n, este tiene las siguientes propiedades:

- El grafo tiene exactamente n vértices.
- La cantidad total de lados del grafo es:

$$\frac{n(n-1)}{2} = \binom{n}{2}.$$

- Cada vértice tiene valencia $n - 1$.

En este caso, se puede comprobar con facilidad que $\frac{n(n-1)}{2} = \binom{n}{2}$, ya que: $\binom{n}{2} = \frac{n(n-1)(n-2)!}{(n-2)!2!} = \frac{n(n-1)}{2}$

EJEMPLO

Para verificar las propiedades de los grafos completos, se ha elaborado la tabla 6.1, en la cual se observa el cumplimiento de las mismas, tomando como base los grafos completos que se observan en la figura 6.16.

Tabla 6.1 Grafos completos y sus propiedades

Grafo completo	Vértices	Lados	Valencia de cada vértice
K_1	1	0	0
K_2	2	1	1
K_3	3	3	2
K_4	4	6	3
K_5	5	10	4
⋮	⋮	⋮	⋮
K_n	n	$\frac{n(n-1)}{2}$	$n-1$

También se puede comprobar que el grafo completo K_6 (véase figura 6.17) cumple dichas propiedades, ya que tiene 6 vértices, 15 lados y 5 lados que son incidentes en cada uno de los vértices del grafo; es decir, cada vértice tiene valencia 5.

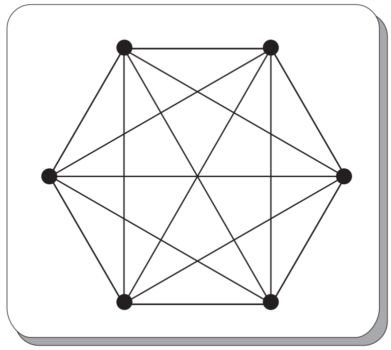


Figura 6.17 Grafo completo K_6.

Grafo regular

Sea $G = (V, E)$ un grafo simple. Si todo vértice $v_i \in V$ tiene la misma valencia, entonces se dice que el grafo es regular, pero si la valencia es n, es decir $\delta(v_i) = n$, entonces el grafo recibe el nombre de n-regular. En la figura 6.18 se muestran diversos grafos n-regulares.

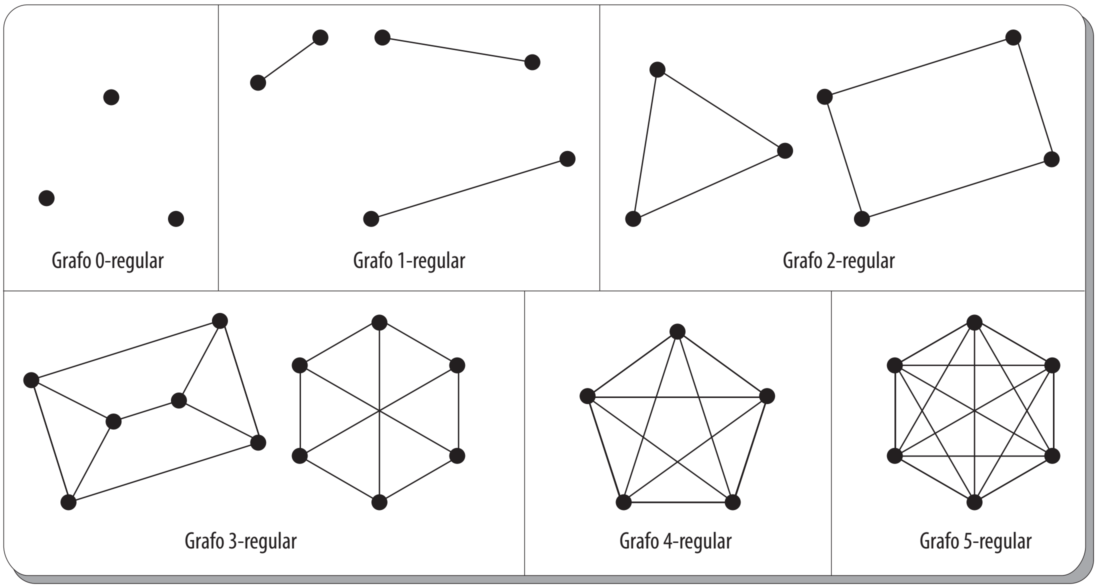


Figura 6.18 Grafos n-regulares.

Como se observa en la figura anterior, el grafo completo K_1 es 0-regular, el K_2 es 1-regular, el K_3 es 2-regular y así sucesivamente, por lo que se puede inferir que todo grafo completo K_n es un grafo $(n-1)$-regular.

Además, se tiene que en un grafo n-regular el tamaño del grafo es igual al orden por la n (que es la valencia de cualquier vértice) dividido entre dos; es decir:

$$|E| = \frac{|V| \cdot n}{2}$$

EJEMPLO

Sea el grafo 5-regular de la figura 6.18; entonces, se tiene que su tamaño es:

$$\begin{aligned} |E| &= \frac{|6| \cdot 5}{2} \\ &= 15 \end{aligned}$$

que, en efecto, es el tamaño del grafo.

Grafo bipartita

Sea $G = (V, E)$ un grafo simple. Se dice que G es ***bipartita*** si el conjunto de vértices V se puede dividir en dos conjuntos disjuntos no vacíos de vértices V_1 y V_2; es decir:

$$V_1 \cup V_2 = V \text{ y } V_1 \cap V_2 = \varnothing$$

De tal manera que cada vértice del conjunto V_1 sea adyacente en los vértices del conjunto V_2.

Del mismo modo, se dice que un grafo bipartita es completo si todos los vértices del conjunto V_1 son adyacentes en todos los vértices del conjunto V_2.

Si $m = |V_1|$ y $n = |V_2|$, entonces el grafo bipartita se denota como $K_{m,n}$.

EJEMPLO

Los grafos de la figura 6.19 son los grafos bipartitas $K_{4,6}$ y $K_{2,4}$; aunque no son completos.

Por su parte, los grafos de la figura 6.20 son grafos bipartitas completos $K_{2,3}$, $K_{3,3}$ y $K_{2,5}$.

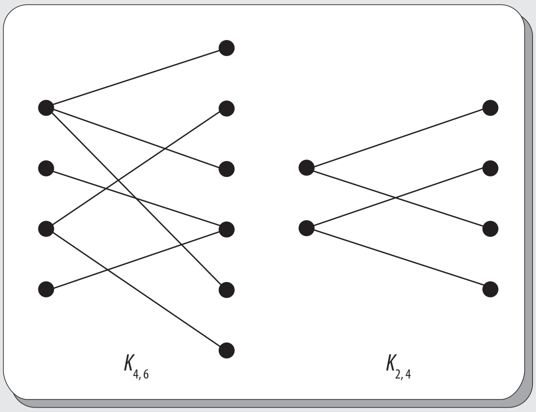


Figura 6.19 Grafos bipartitas.

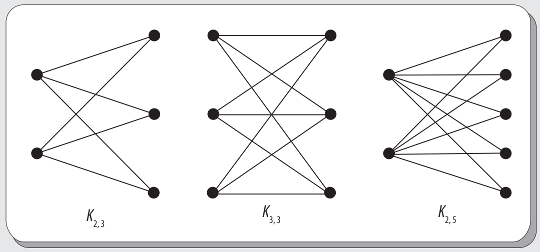


Figura 6.20 Grafos bipartitas completos.

Ejemplo

Determinar si es posible conectar tres casas con los números 1, 2 y 3 a los servicios públicos de luz, agua y drenaje, de tal manera que no haya dos líneas de conexión de dichos servicios que se crucen una con otra; es decir, establecer si es posible resolver este problema modelándolo mediante un grafo aplanable.

Solución

Como se observa en la figura 6.21, el único resultado posible para dicho problema es el grafo bipartita $K_{3,3}$. El cual no es un grafo aplanable. Más adelante se verá por qué.

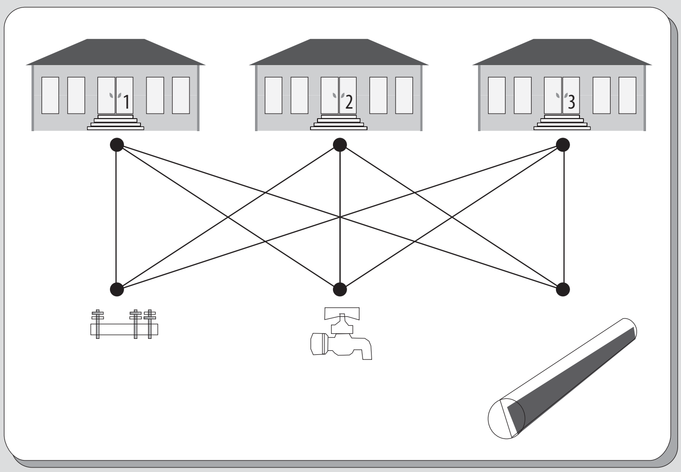


Figura 6.21 Grafo $K_{3,3}$ como solución al problema.

Subgrafos

Sea $G = (V, E)$ un grafo (dirigido o no dirigido). Se dice que un grafo $G_1 = (V_1, E_1)$ es un subgrafo de G si $E_1 \subseteq E$ y $V_1 \subseteq V$, tal que los lados de E_1 sean incidentes en los vértice de V_1.

Por otra parte, si $E_1 \subset E$ y $V_1 \subset V$, entonces se dice que G_1 es un subgrafo propio de G.

De acuerdo con la definición anterior, se puede intuir que un subgrafo $G_1 = (V_1, E_1)$ es un grafo contenido dentro de otro más grande $G = (V, E)$.

Esto sugiere que para obtener el subgrafo G_1, lo que hay que hacer es eliminar algunos de los lados del grafo G. Y, en efecto, así es. Pero, siempre hay que tener en cuenta que no hay ningún problema al eliminar cualquier lado; aunque no es posible eliminar solo un vértice sin razón alguna, ya que el resultado no sería un grafo, sino que también es necesario quitar todos los lados que lo tengan por extremo.

En resumen, para obtener un subgrafo a partir de un grafo, se requiere:

1. Eliminar lados de G.
2. Eliminar vértices de G, en cuyo caso se deben borrar también todos los lados que tengan por extremo a estos vértices.

Además, se dice que el complemento de un subgrafo $G_1 = (V_1, E_1)$ con respecto a un grafo $G = (V, E)$ es otro subgrafo $G_2 = (V_2, E_2)$, también con respecto a G, donde: $E_2 = E - E_1$ o $E = E_1 + E_2$ y V_2 contiene a todos los vértices con los cuales E_2 son incidentes.

Cuando un subgrafo $G_1 = (V_1, E_1)$ contiene a todos los vértices del grafo $G = (V, E)$, entonces se dice que G_1 es un subgrafo generador de G, por lo que en este caso $V_1 = V$.

EJEMPLO

Sea el grafo $G = (V, E)$ de la figura 6.22*i*), donde:

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\} \text{ y}$$

$$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}\}$$

Y sea el grafo $G_1 = (V_1, E_1)$ de la figura 6.22*ii*), donde:

$$V_1 = \{v_2, v_3, v_4, v_5, v_6, v_7, v_8\} \text{ y}$$

$$E_1 = \{e_4, e_5, e_7, e_8, e_{11}, e_{12}\}$$

Como $E_1 \subset E$ y $V_1 \subset V$, tal que los lados de E_1 son incidentes en los vértices de V_1; por tanto G_1 es un subgrafo de G.

Ahora, considérese el grafo $G_2 = (V_2, E_2)$ de la figura 6.22*iii*), donde:

$$V_2 = \{v_1, v_2, v_3, v_4, v_6, v_8, v_9\} \text{ y}$$

$$E_2 = \{e_1, e_2, e_3, e_6, e_9, e_{10}\}$$

En este caso, se tiene que $E_2 = E - E_1$ y V_2 contiene a los vértices con los cuales E_2 son incidentes, por lo que G_2 es el complemento del subgrafo de G_1 con respecto al grafo G.

Ahora, sea el grafo $G_1 = (V_1, E_1)$ de la figura 6.22 *iv*), donde:

$$V_1 = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\} \text{ y}$$

$$E_1 = \{e_1, e_3, e_5, e_7, e_8, e_9, e_{11}\}$$

Como $E_1 \subset E$ y $V_1 \subset V$, tal que los lados de E_1 son incidentes en los vértice de V_1; por tanto G_1 es un subgrafo de G.

Continúa

Como V_1 contiene todos los vértices de G, entonces G_1 es un subgrafo generador de G.

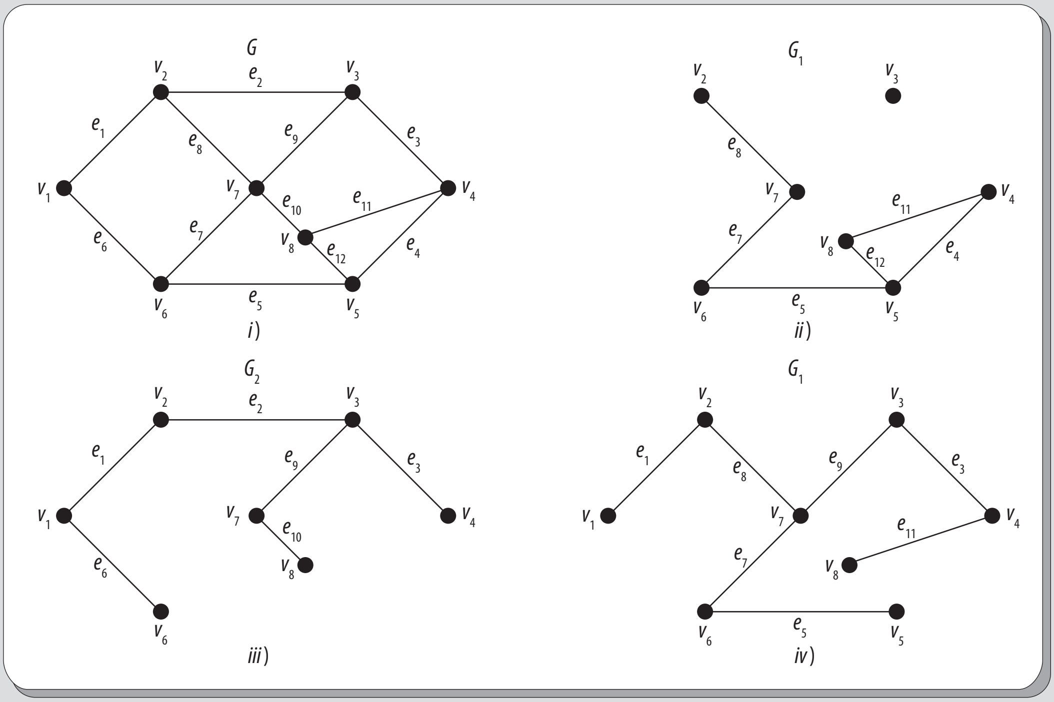


Figura 6.22 Grafo, subgrafo, complemento del subgrafo y subgrafo generador.

6.4 Paseos y circuitos

Para iniciar esta sección, primero se aborda un problema interesante donde intervienen paseos y circuitos, y se continúa con una definición más formal de estos conceptos.

Es importante destacar aquí que muchos problemas que surgen de situaciones en la vida cotidiana pueden ser modelados mediante el uso de grafos. Uno de los primeros modelos de los que se tiene conocimiento fue desarrollado en 1736, cuando Leonhard Euler publicó un artículo que contenía la solución del famoso problema de los puentes de Königsberg. A continuación, se aborda en qué consiste dicho problema.

Nota

Problema de los puentes de Königsberg
Conocido más específicamente como el problema de los siete puentes de Königsberg, consiste en el hecho de que dos islas, situadas en el río Pregel, en Königsberg (antes Prusia Oriental, en la antigua Alemania, en la actualidad perteneciente a Rusia y se conoce como Kaliningrado), están conectadas entre sí y con la margen del río a través de siete puentes, como se muestra en la figura 6.23.

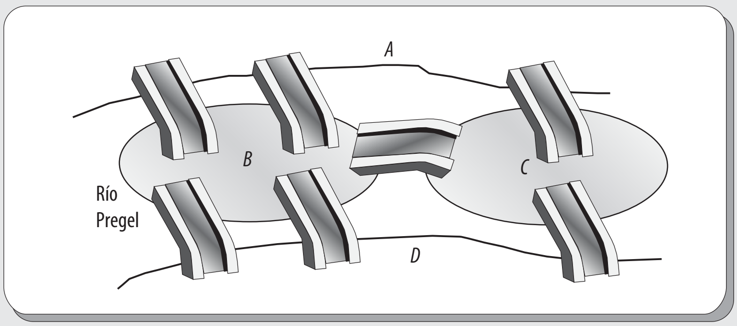


Figura 6.23 Distribución de los puentes de Königsberg.

Continúa

El problema radica básicamente en partir desde cualquier lugar de tierra firme (*A*, *B*, *C* o *D*), seguir caminando y pasar por cada uno de los puentes una sola vez y luego volver al punto de partida.
A un recorrido de este tipo se le llama "circuito de Euler" (este se analiza con detalle más adelante) y puede representarse mediante un grafo como se ve en la figura 6.24.
La solución o no solución de este tipo de problemas se obtiene fácilmente mediante el uso del concepto de valencia de un vértice.
Más adelante se retoma el tema y se demuestra que el problema de los puentes de Königsberg no tiene solución.
Como dato interesante se tiene que dos de los siete puentes originales fueron destruidos por el bombardeo de Königsberg durante la Segunda Guerra Mundial y otros dos fueron demolidos más adelante y reemplazados por carreteras modernas; los tres puentes restantes aún permanecen en pie, aunque solo dos de ellos datan de la época de Euler, pues uno fue reconstruido en 1935.
Por tanto, en la actualidad solo existen cinco puentes en Kaliningrado, distribuidos de tal manera que ahora es posible obtener un ***camino euleriano***, es decir, un recorrido que comienza en una isla y termina en otra; sin embargo, todavía no es posible obtener un ***circuito euleriano***, es decir, un recorrido donde la ruta comience y termine en el mismo lugar, lo cual era necesario para cumplir con las condiciones iniciales del problema.

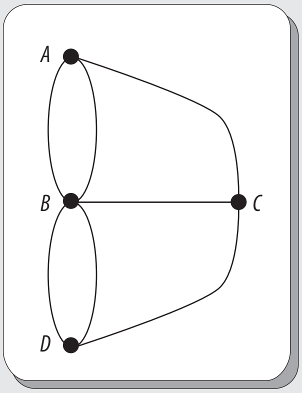


Figura 6.24 Representación del problema de los puentes de Königsberg mediante un grafo.

Ahora es tiempo de definir qué es un camino y un circuito y luego los de Euler.

Caminos y circuitos

Existen muchos problemas en los cuales se pretende determinar si existe un camino o un circuito en un grafo determinado o simplemente entre dos vértices cualesquiera.

Pero, antes de definirlos, primero es necesario conocer qué es una sucesión de lados.

Sucesión de lados

Una sucesión de lados es un conjunto de lados consecutivos donde termina un lado y comienza otro.

Con frecuencia, una sucesión de lados:

$$\{(v_0, v_1), (v_1, v_2), \dots , (v_{n-1}, v_n)\}$$

se abrevia como:

$$(v_0, v_1, v_2, \dots , v_n)$$

EJEMPLO

Sea $G = (V, E)$ el grafo no dirigido de la figura 6.25.

La sucesión de lados:

$$\{(v_1, v_2), (v_2, v_7), (v_7, v_6), (v_6, v_5)\}$$

se puede abreviar como:

$$(v_1, v_2, v_7, v_6, v_5)$$

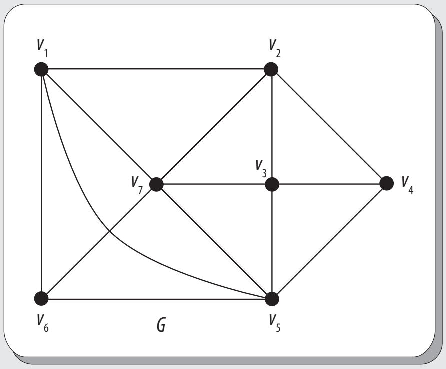


Figura 6.25 Grafo no dirigido *G*.

Es importante recordar aquí que un lado e también puede escribirse como $e = (i, j)$, por lo que dicha sucesión de lados también puede escribirse como:

$$(e_1, e_2, e_3, \ldots, e_n)$$

Caminos y circuitos

Sea $G = (V, E)$ un grafo no dirigido y sean i y j dos vértices de G.

Una sucesión de lados de i a j puede clasificarse como:

a) ***Camino*** de longitud n de i a j, si va de i a j, y tiene n lados distintos entre sí.

b) ***Camino simple*** de longitud n de i a j, si es de la forma $(v_0, v_1, v_2, \ldots, v_n)$, donde $v_0 = i$ y $v_n = j$ y $v_0, v_1, v_2, \ldots, v_n$ son distintos entre sí.

c) ***Circuito*** si es un camino de v a v.

d) ***Circuito simple*** si es un circuito de la forma $(v_0, v_1, v_2, \ldots, v_n)$, donde $v_0 = v_n$ y $v_1, v_2, \ldots, v_{n-1}$ son distintos entre sí.

En otras palabras, un **camino** es una sucesión de lados en la cual todos los lados son distintos. Así, un **camino simple** es una sucesión de lados en la cual todos los lados y todos los vértices son distintos; un **circuito** es un camino que inicia y termina en el mismo vértice donde todos sus lados son distintos y un **circuito simple** es un circuito en el cual todos los lados y todos los vértices son distintos, a excepción del primero y último vértices, que en realidad son el mismo.

Ejemplo

Sea $G = (V, E)$ el grafo no dirigido de la figura 6.26.

Determinar si las sucesiones de lados de la tabla 6.2 corresponden a un camino, camino simple, circuito o circuito simple.

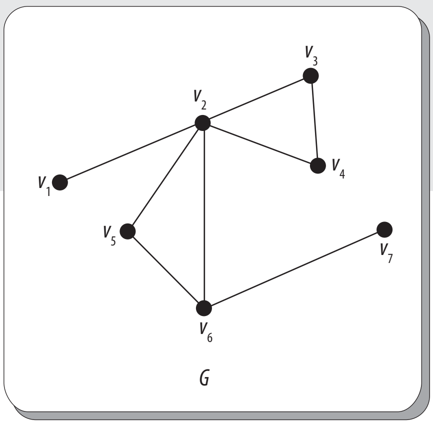


Figura 6.26 Grafo no dirigido G.

Tabla 6.2 Sucesiones de lados del grafo de la figura 6.26

Núm.	Sucesión de lados
1	$(v_1, v_2, v_3, v_2, v_1)$
2	$(v_6, v_5, v_2, v_4, v_3, v_2, v_1)$
3	(v_6, v_5, v_2, v_4)
4	$(v_2, v_6, v_5, v_2, v_4, v_3, v_2)$
5	(v_5, v_6, v_2, v_5)

Solución

En la tabla 6.3 se muestra a qué corresponde cada una de las sucesiones de lados de la tabla 6.2.

Tabla 6.3 Solución de las sucesiones de lados de la tabla 6.2

Núm.	Camino	Camino simple	Circuito	Circuito simple
1	NO	NO	NO	NO
2	SÍ	NO	NO	NO
3	SÍ	SÍ	NO	NO
4	SÍ	NO	SÍ	NO
5	SÍ	NO	SÍ	SÍ

Como se observa en el ejemplo anterior, la primera sucesión de lados no puede ser un circuito, pues, aunque inicia y termina en el mismo vértice, que es una condición necesaria, pero no suficiente para la existencia de un circuito, y esta no representa ni siquiera un camino, pues no todos los lados son distintos entre sí, como ocurre con el lado $\{v_1, v_2\}$.

Asimismo, se observa con claridad que una sucesión de lados no puede ser simultáneamente de los cuatro tipos de sucesiones consideradas, pues como máximo puede ser de tres tipos diferentes.

Paseos y circuitos de Euler (eulerianos)

Existen tipos especiales de paseos y circuitos, los cuales implican ciertas restricciones al momento de visitar o recorrer los vértices de un grafo dado, estos son los paseos y circuitos denominados de Euler (eulerianos) y de Hamilton (hamiltonianos).

En primera instancia, se verán los de Euler.

Paseo de Euler

Un paseo de Euler (o euleriano) es un camino que incluye todos los lados de un grafo dado una y solo una vez.

Circuito de Euler

Un circuito de Euler (o euleriano) es un circuito que incluye todos los lados de un grafo dado una y solo una vez.

Al recorrer todos los lados del grafo, también se recorren todos los vértices del grafo; sin embargo, no importa la repetición de vértices, mientras no se repitan los lados.

Condiciones para determinar la existencia de un paseo o circuito de Euler en un grafo no dirigido

Es importante destacar que existen algunas condiciones para determinar si un grafo no dirigido tiene un paseo o un circuito de Euler, las cuales implican que el grafo debe ser conexo; por esa razón, lo primero es definir dicho concepto.

Grafo conexo

Sea $G = (V, E)$ un grafo no dirigido; se dice que G es un ***grafo conexo*** si, para cualquier par de vértices i y j distintos entre sí, existe un camino de i a j.

De acuerdo con la definición anterior, entonces los grafos no dirigidos de las figuras 6.24, 6.25 y 6.26 se consideran conexos.

Si un grafo no es conexo, entonces se dice que es disconexo.

EJEMPLO

Sea $G = (V, E)$ el grafo no dirigido de la figura 6.27. Como se puede ver, este grafo es disconexo, ya que no existe un camino entre algunos de sus vértices, como de v_1 a v_4 o de v_2 a v_5, entre otros.

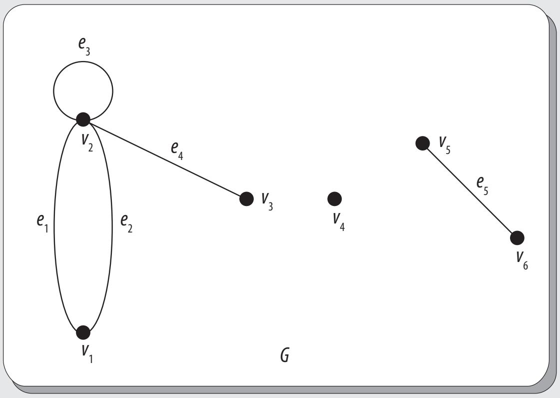


Figura 6.27 Grafo no dirigido G disconexo.

Si $G = (V, E)$ es un grafo dirigido, su grafo no dirigido asociado es el grafo obtenido de G si se omiten las direcciones de los lados. Cuando este grafo asociado es conexo, se considera que G es conexo; pero, si es disconexo, entonces se considera que G es disconexo.

EJEMPLO

Sea $G = (V, E)$ el grafo dirigido de la figura 6.28. Como se puede ver, este grafo es disconexo, ya que su grafo no dirigido asociado (véase figura 6.29) es disconexo.

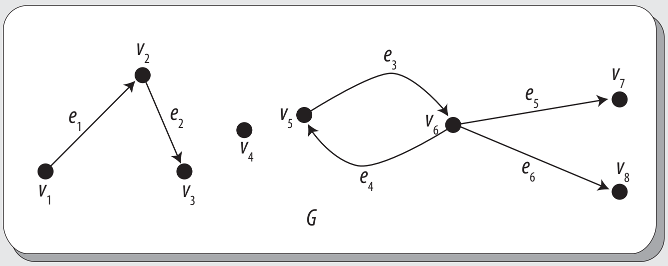


Figura 6.28 Grafo no dirigido G.

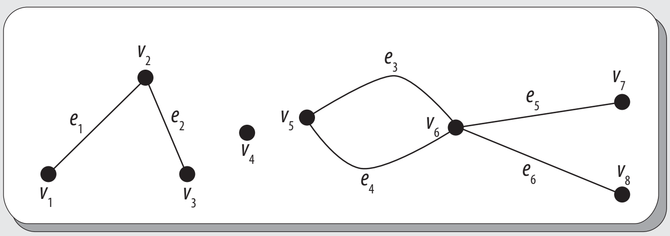


Figura 6.29 Grafo no dirigido asociado al grafo dirigido de la figura 6.28.

Cuando un grafo es disconexo, entonces se dice que está formado por componentes, donde la cantidad de componentes es la cantidad de grafos individuales conexos que tiene el grafo; se denota como $K(G)$.

Por ejemplo, el grafo dirigido de la figura 6.29 consta de tres componentes; es decir: $K(G) = 3$.

También se puede decir que un grafo no dirigido $G = (V, E)$ es disconexo si y solo si V puede separarse en al menos dos subconjuntos V_1 y V_2, tales que no haya un lado en E de la forma $\{i, j\}$; donde: $i \in V_1$ y $j \in V_2$. Y que un grafo es conexo si y solo si tiene una componente conexa.

A continuación se muestran las condiciones para determinar la existencia de un paseo o un circuito de Euler en un grafo no dirigido G.

1. Un grafo no dirigido G tiene un paseo de Euler si y solo si es conexo y tiene cero o dos vértices de valencia impar.
2. Un grafo no dirigido G tiene un circuito de Euler si y solo si es conexo y todo vértice de G tiene valencia par.
3. Un grafo no dirigido G tiene un paseo de Euler de $i \neq j$ si y solo si i y j son los únicos vértices de valencia impar. Esta condición indica que el único paseo de Euler posible en el grafo es iniciar en uno de los vértices de valencia impar y terminar en el otro o viceversa.

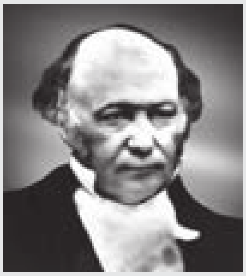


Figura 6.30 Carl Hierholzer (1840-1871), matemático alemán.

Carl Hierholzer, matemático alemán que estudió matemáticas en la Universidad de Karlsruhe y obtuvo su doctorado en la Universidad de Heidelberg, en 1865. En 1870, Hierholzer escribió sobre secciones canónicas, en su obra titulada *Ueber Kegelschnitte im Raum* (*Acerca de las secciones esféricas en el espacio*), en Karlsruhe, donde después fue profesor.

Hierholzer demostró que un grafo tiene un ciclo euleriano si y solo si es conexo y cada vértice tiene valencia par. Este resultado había sido dado, sin demostración, por Leonhard Euler en 1736. Se presume que Hierholzer hizo una demostración a un colega justo antes de su prematura muerte en 1871, quien luego organizó el contenido para su publicación póstuma, la cual apareció en 1873, bajo el nombre *Über die Möglichkeit, einen Linienzug ohne Wiederholung und ohne Unterbrechung zu umfahren* (*Sobre la posibilidad de evitar una polilínea sin repetición y sin interrupción).*

Ejemplo

Sean los grafos no dirigidos de la figura 6.31.

Determinar cuáles de estos grafos tendrán un paseo o un circuito de Euler.

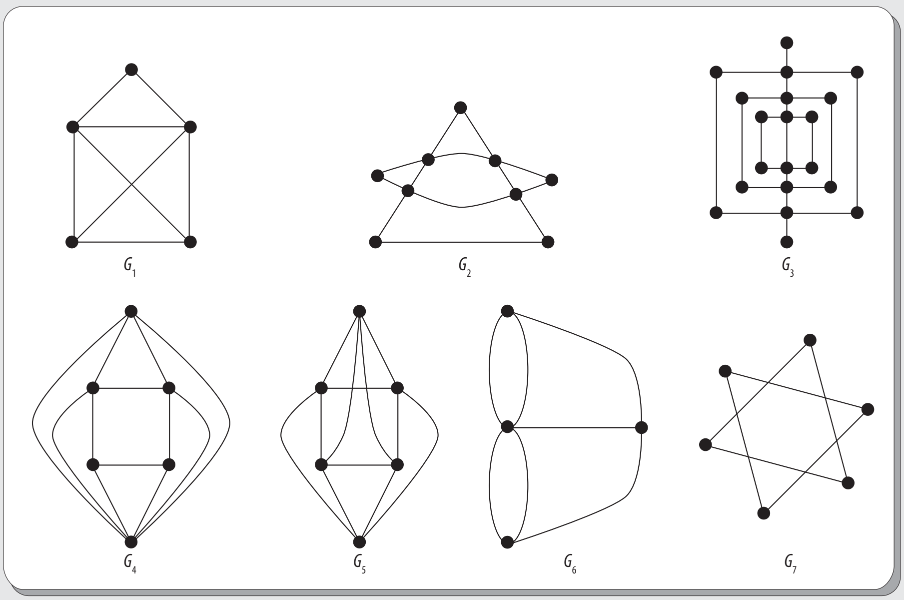


Figura 6.31 Grafos no dirigidos.

Solución

En la tabla 6.4 se muestran cuáles de los grafos no dirigidos de la figura 6.31 tienen un paseo o un circuito de Euler.

Tabla 6.4 Grafos de la figura 6.31 que tienen paseo o circuito de Euler

Grafo	Paseo de Euler	Circuito de Euler
G_1	SÍ	NO
G_2	SÍ	SÍ
G_3	SÍ	NO
G_4	SÍ	NO
G_5	SÍ	SÍ
G_6	NO	NO
G_7	NO	NO

El grafo G_6 del ejemplo anterior corresponde al problema de los puentes de Königsberg; como se observa, todos sus vértices tienen valencia impar, por lo que no puede tener paseo ni circuito de Euler, lo que significa, por tanto, que dicho problema no tiene solución.

En el mismo ejemplo, el grafo G_7 tampoco tiene ni paseo ni circuito de Euler, debido a que es disconexo. En realidad, se trata de dos triángulos, uno sobre otro, pero sin conexión alguna entre los vértices de uno al otro.

Paseo y circuito de Euler en grafos dirigidos

Los resultados obtenidos para grafos no dirigidos pueden extenderse de inmediato para grafos dirigidos.

Sin embargo, también existen algunas condiciones para determinar si un grafo dirigido tiene un paseo o un circuito de Euler:

1. Un grafo dirigido G tiene un circuito de Euler si y solo si es conexo y la valencia de entrada de cualquier vértice es igual a su valencia de salida.
2. Un grafo dirigido G tiene un paseo de Euler si y solo si es conexo y la valencia de entrada de cualquier vértice es igual a la valencia de salida con la posible excepción de solo dos vértices. Para estos dos vértices la valencia de entrada de uno de ellos es mayor que su valencia de salida y la valencia de entrada del otro es menor que su valencia de salida.
3. Un grafo dirigido G tiene un paseo de Euler de $i \neq j$, si y solo si i es el vértice de valencia de salida mayor y j es el vértice de valencia de entrada mayor. Esta condición indica que el único paseo de Euler posible en el grafo es iniciar en el vértice de valencia de salida mayor y terminar en el vértice de valencia de entrada mayor.

Dénes König, matemático húngaro judío, trabajó y escribió el primer libro de texto sobre el campo de la teoría de grafos en 1936, titulado *Theorie und de endlichen unendlichen graphen* (*Teoría de grafos finitos e infinitos*). En este libro, uno de los principales resultados obtenidos afirma que un gráfo dirigido D es euleriano si y solo si las valencias de entrada y salida de cada vértice de D son iguales. Esto marcó el comienzo de la teoría de grafos como su propia rama de las matemáticas. König también trabajó en la factorización de grafos bipartitas, en conjunto con Philip Hall. Asimismo, usó grafos para dar una prueba más simple de un resultado determinante de Frobenius, lo que parece haber causado cierta hostilidad entre los hombres de su época.

Figura 6.32 Dénes König (1884-1944) matemático húngaro.

Ejemplo

Sean los grafos dirigidos de la figura 6.33. Verificar si dichos grafos tienen un paseo o un circuito de Euler.

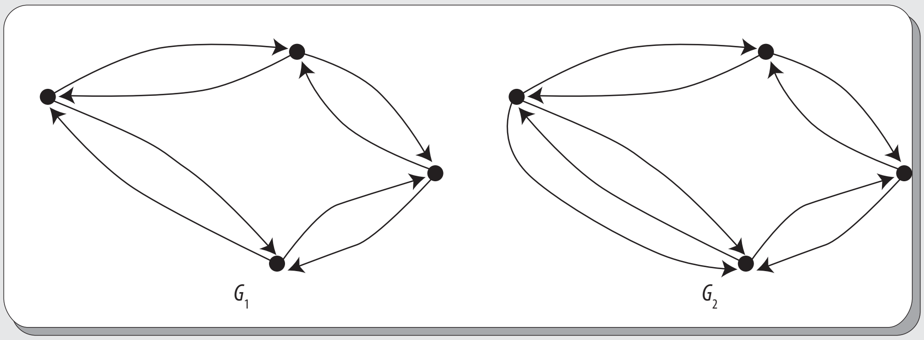


Figura 6.33 Grafos dirigidos.

Solución

Si consideramos las condiciones antes descritas, el grafo G_1 tiene tanto un paseo como un circuito de Euler, ya que cualquiera de sus vértices, de manera individual, tiene la misma valencia de entrada que de salida.

En cambio, el grafo G_2 únicamente tendrá un paseo de Euler, pero no un circuito de Euler, ya que la valencia de entrada de cualquier vértice, de manera individual, es igual a su valencia de salida, con la posible excepción de solo dos vértices.

Paseos y circuitos de Hamilton (hamiltonianos)

Un problema similar a la determinación de un paseo o un circuito de Euler, es el de determinar un paseo o circuito de Hamilton, los que se definen a continuación:

Paseo de Hamilton

Un paseo de Hamilton (o hamiltoniano) constituye un camino que pasa a través de cada uno de los vértices de un grafo dado exactamente una vez.

Circuito de Hamilton

Un circuito de Hamilton (o hamiltoniano) es un circuito que pasa a través de cada uno de los vértices de un grafo dado exactamente una vez.

Al recorrer todos los vértices del grafo, no es importante si no se recorren todos los lados del grafo.

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ que se observa en la figura 6.34.

En dicho grafo, la sucesión de lados:

$(v_1, v_2, v_3, v_4, v_5, v_6, v_7)$

es un paseo de Hamilton.

En tanto que la sucesión de lados:

$(v_1, v_7, v_2, v_3, v_4, v_5, v_6, v_1)$

es un circuito de Hamilton.

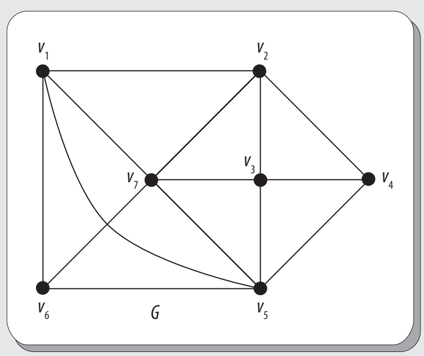


Figura 6.34 Grafo no dirigido G.

EJEMPLO

En el grafo no dirigido de la figura 6.35 se muestra un circuito de Hamilton, donde se observa que se recorren todos los vértices (cada uno solo una vez), pero no se recorren todos los lados.

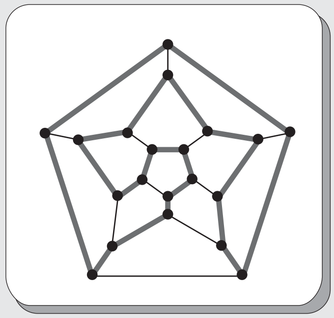


Figura 6.35 Grafo no dirigido con circuito de Hamilton.

Pero, en realidad, el grafo de la figura 6.35 corresponde a una solución del juego de ingenio denominado el "juego icosiano" (véase figura 6.36) diseñado por William Rowan Hamilton en 1859. A continuación, se analiza en qué consiste dicho juego.

En ese mismo año, Hamilton presentó en una reunión de la British Association, en Dublín, un curioso pasatiempo al que él denominó ***The Icosian Game*** (El juego icosiano), cuyo objetivo es encontrar un camino sobre un dodecaedro que pase una, y solo una vez, por cada uno de sus veinte vértices; no obstante sí está permitido pasar por un mismo lado más de una vez, como se observa en la figura 6.36.

Un dodecaedro es uno de los cinco poliedros regulares existentes en la naturaleza, el cual, como su nombre lo indica, está formado por 12 pentágonos regulares iguales; por tanto, tiene 12 caras, 20 vértices y 30 lados. Además, es importante notar que el hecho de que Hamilton designara a su juego con el nombre de *Icosian* no se debió a que utilizara un icosaedro en su desarrollo (otro de los cinco poliedros regulares de la naturaleza, formado por veinte triángulos equiláteros iguales), sino que Hamilton tomó el prefijo *Ico* (que en griego significa veinte) en alusión al número de vértices del dodecaedro.

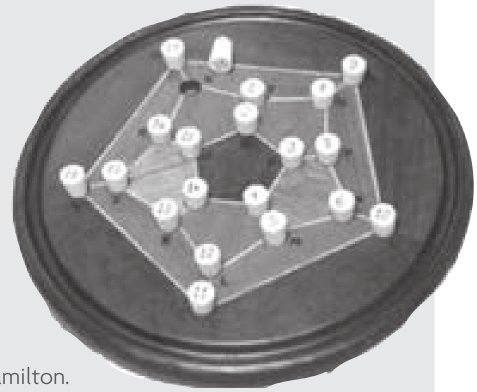


Figura 6.36 Juego icosiano de Hamilton.

William Rowan Hamilton realizó importantes contribuciones a la dinámica y la óptica, inventó los cuaterniones y comercializó el novedoso juego de ingenio, conocido como *Juego Icosiano*, que posteriormente se convertiría en una especialidad a desarrollar dentro de la teoría de grafos, que había visto la luz con Euler y el famoso problema: "Los siete puentes de Königsberg". A lo largo de su vida, Hamilton se dedicó a la investigación de diversas disciplinas. Cabe destacar que en 1859 vendió por 25 libras los derechos del *Juego icosiano* o *Juego del viajero* que, como se vio antes, consistía en conectar mediante un camino simple los vértices de una figura formada por tres pentágonos concéntricos encajados unos dentro de los otros. Este juego serviría para desarrollar en mayor medida la teoría de grafos.

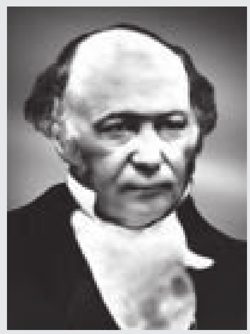


Figura 6.37 William Rowan Hamilton (1805-1865).

EJEMPLO

Problema del caballo

El llamado "problema del caballo" es un antiguo problema matemático relacionado con el ajedrez, el cual consiste en encontrar una secuencia de movimientos (válidos) de esta pieza, a fin de que recorra todas las casillas del tablero, visitando cada una solo una vez.

Desde su aparición, muchos matemáticos han buscado solución a este problema, entre ellos Euler; no obstante, **aún** sigue sin conocerse el número exacto de soluciones que existe. Además, el problema ha sido planteado para tableros de diferentes tamaños y distintas condiciones iniciales, y sigue siendo tan atractivo como hace 1 200 años.

Nota

Determinar la existencia de un paseo o un circuito de Hamilton en un grafo puede ser una tarea complicada, sobre todo si se trata de un grafo grande, ya que no se conoce ninguna condición necesaria y suficiente para demostrar la existencia de un paseo o un circuito de Hamilton en un grafo.

Continúa

Asimismo, algunas variaciones de este problema han sido estudiadas por los matemáticos, como:

- Buscar soluciones cíclicas (a través de las cuales se debe llegar a la misma casilla de la cual se partió).
- Tableros de diferente número de columnas o bien de diferente número de filas, como el tablero de 5×5 que se muestra en la figura 6.38.
- Juegos de dos jugadores basados en la misma idea.
- Problemas usando ligeras variaciones en la forma de mover el caballo.

El problema del caballo es una forma más general de determinar un paseo o circuito de Hamilton.

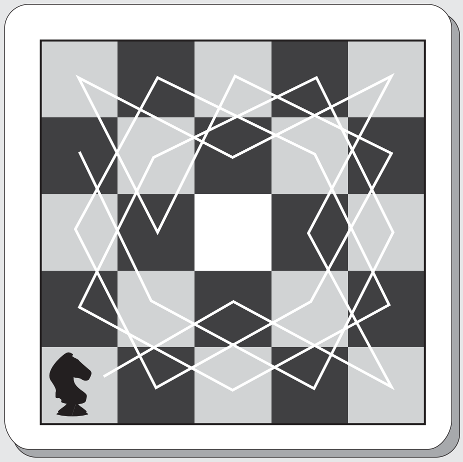


Figura 6.38 Solución a la variación del problema del caballo en un tablero de 5×5.

Los teoremas siguientes son resultados generales que establecen *condiciones suficientes* sobre la existencia de circuitos de Hamilton en un grafo.

Teorema

Teorema de Dirac

Sea G un grafo no dirigido con n vértices para $n \geq 3$, tal que todos los vértices de G tienen valencia mayor o igual que $\frac{n}{2}$. Entonces, G contiene un circuito de Hamilton.

Este teorema fue demostrado en 1952 por A. Dirac, a quien debe su nombre, mediante el uso de la reducción al absurdo.

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.39, el cual, como se observa, tiene cuatro vértices y cuatro lados.

Entonces, se tiene que $\delta(v_i) = 2$, $i = 1, \dots, 4$ y que $\frac{n}{2} = 2$.

Al ser:

$$\delta(v_i) = 2 = \frac{n}{2} = 2$$

Entonces, se cumple el teorema de Dirac y se tiene que G debe tener un circuito de Hamilton que podría ser $(v_1, v_2, v_4, v_3, v_1)$.

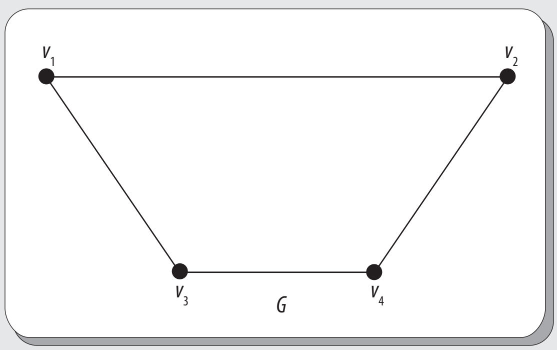


Figura 6.39 Grafo no dirigido G.

Sin embargo, existen circuitos de Hamilton en un grafo que no cumplen con dicho teorema.

EJEMPLO

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.40, el cual, como se observa, tiene ocho vértices y ocho lados.

Entonces, se tiene que $\delta(v_i) = 2$, $i = 1, \ldots ,8$ y que $\frac{n}{2} = 4$.

Por lo que no se cumple el teorema de Dirac.

Pero, se tiene que G sí tiene un circuito de Hamilton:

$$(v_3, v_4, v_5, v_6, v_7, v_8, v_1, v_2, v_3)$$

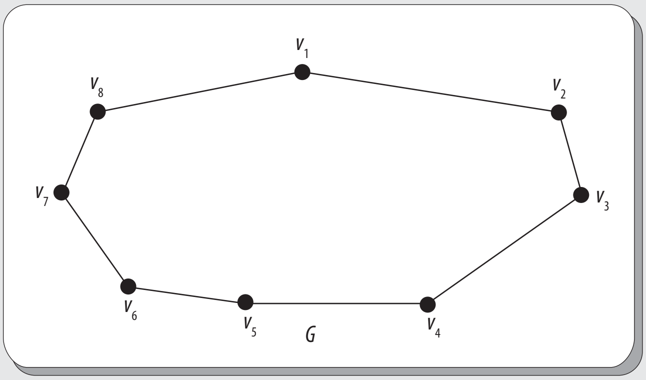


Figura 6.40 Grafo no dirigido G.

Otro resultado general sobre la existencia de paseos de Hamilton en un grafo es el teorema que se cita a continuación.

Teorema

Teorema de Ore

Sea G un grafo no dirigido con n vértices para $n \geq 3$, tal que: $\delta(i) + \delta(j) \geq n$, para cada par de vértices no adyacentes i y j de G.

Entonces, G contiene un circuito de Hamilton.

El teorema de Ore es una aplicación del teorema de Dirac, el cual fue demostrado por *Oystein Ore* en 1960, también mediante el uso de la reducción al absurdo.

EJEMPLO

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.41, el cual, como se observa, tiene cuatro vértices y cinco lados.

Entonces, se tiene que:

$$\delta(v_1) = 2,$$
$$\delta(v_2) = 3,$$
$$\delta(v_3) = 2 \text{ y}$$
$$\delta(v_4) = 3$$

Dado que $\delta(v_i) + \delta(v_j) \geq n = 4$, para cualquier par de vértices no adyacentes, entonces se cumple el teorema de Ore.

Y se tiene que G debe tener un circuito de Hamilton que podría ser:

$$(v_1, v_2, v_3, v_4, v_1)$$

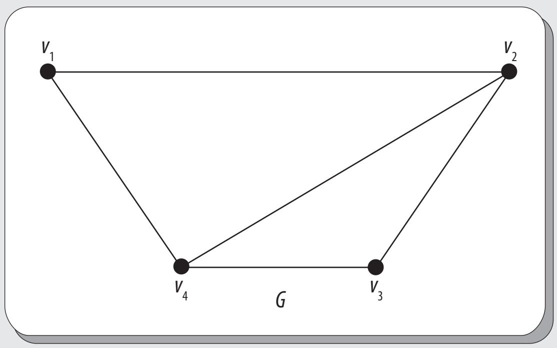


Figura 6.41 Grafo no dirigido G.

Pero, también existen circuitos de Hamilton en un grafo que no cumple con el teorema de Ore, como se ve en el siguiente ejemplo.

EJEMPLO

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.42, el cual, como se observa, tiene 16 vértices.

En este caso, al ser $\delta(v_i) + \delta(v_j) \ngeq n = 16$, para cualquier par de vértices no adyacentes, no se cumple el teorema de Ore.

Pero, se tiene que G sí tiene un circuito de Hamilton:

$$(v_1, v_2, v_3, v_4, v_8, v_7, v_6, v_{10}, v_{11}, v_{12}, v_{16}, v_{15}, v_{14}, v_{13}, v_9, v_5, v_1)$$

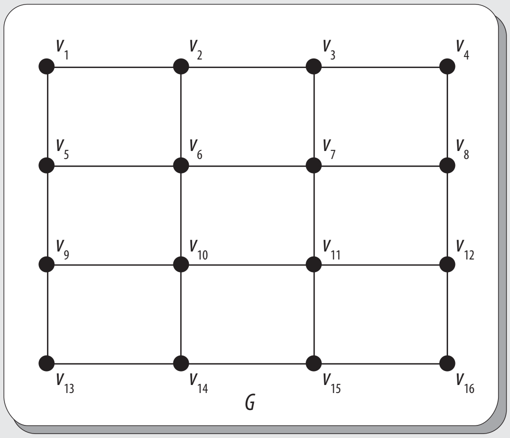


Figura 6.42 Grafo no dirigido G.

Los resultados anteriores son condiciones suficientes para la existencia de un paseo o circuito de Hamilton en un grafo; sin embargo, no ofrecen condiciones necesarias para su existencia.

EJEMPLO

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.43. Como se puede observar, este grafo contiene un circuito de Hamilton, pero no cumple con ninguna de las condiciones descritas antes en los teoremas de Dirac o de Ore, pues la suma de las valencias de cualesquiera dos de sus vértices es 4.

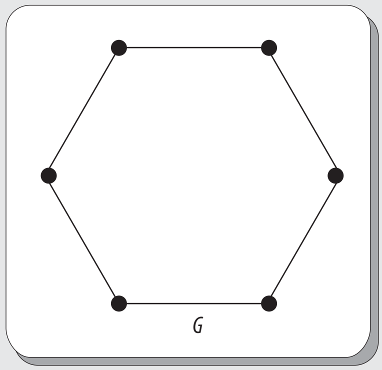


Figura 6.43 Grafo con paseo de Hamilton.

6.5 Multígrafos y grafos pesados (grafos ponderados)

Cuando se requiere que no exista duda en la terminología de grafos, suele utilizarse el término multígrafo para indicar que un grafo tiene lados paralelos. Por tanto, a continuación, se define de manera formal dicho concepto.

Multígrafo dirigido

Sea $G = (V, E)$ un grafo dirigido, donde V es un conjunto de vértices y E es un ***multiconjunto*** de pares ordenados de $V \times V$.

En estos términos, G es llamado ***multígrafo dirigido*** o multidígrafo, y en forma geométrica puede representarse como un conjunto de vértices V y un conjunto de flechas E entre los vértices, donde no existe restricción en el número de flechas de un vértice a otro.

EJEMPLO

Sea el grafo $G = (V, E)$ de la figura 6.44 donde:

$V = \{v_1, v_2, v_3, v_4\}$ y

$E = \{(v_3, v_1), (v_3, v_1), (v_1, v_3), (v_2, v_1), (v_4, v_2), (v_4, v_2), (v_2, v_4), (v_1, v_4), (v_4, v_1), (v_3, v_4)\}$

En este caso, como G tiene un multiconjunto E de pares ordenados de $V \times V$, entonces se dice que es un multígrafo dirigido.

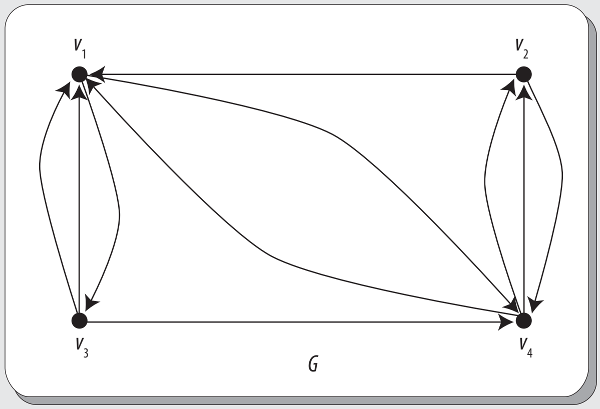


Figura 6.44 Multígrafo dirigido.

Con el fin de que el concepto de multígrafo quede más comprensible, cabe aclarar qué es un *multiconjunto*.

Multiconjunto

En matemáticas, un multiconjunto (también llamado ***bolsa***, o ***bag*** en inglés) difiere de un conjunto en que cada miembro del multiconjunto tiene asociada una multiplicidad $m \in \mathbb{N}$, que indica cuántas veces este elemento es miembro del conjunto.

EJEMPLO

Sea el multiconjunto $\{a, a, b, b, b, c\}$.

Las multiplicidades de los miembros a, b y c son 2, 3 y 1, respectivamente.

Más formalmente, un multiconjunto se define como el par (A, m) donde:

A es un conjunto y m: $A \rightarrow \mathbb{N}$ es una función de A a $\mathbb{N}$.

En este caso, A se conoce como el conjunto subyacente de elementos. Esto es, para cada $a \in A$, la multiplicidad de a es el número $m(a)$.

Es común escribir la función m como un conjunto de pares ordenados $\{(a,m(a))$ tal que $a \in A\}$. Siendo esta, sin duda, la definición de la función m.

EJEMPLO

Sean los multiconjuntos $A = \{a, b, b\}$, $B = \{a, a, b\}$ y $C = \{a, b\}$.

Estos se pueden definir respectivamente como:

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

$$B = \{(a, 2), (b, 1)\} \text{ y}$$

$$C = \{(a, 1), (b, 1)\}$$

EJEMPLO

Utilizando la definición de multiconjunto, se puede decir que el grafo $G = (V, E)$ de la figura 6.44 quedaría definido como:

$V = \{v_1, v_2, v_3, v_4\}$ y

$E = \{((v_3, v_1), 2), ((v_1, v_3), 1), ((v_2, v_1), 1), ((v_4, v_2), 2), ((v_2, v_4), 1), ((v_1, v_4), 1), ((v_4, v_1), 1), ((v_3, v_4), 1)\}$

EJEMPLO

Considérese una representación gráfica de un mapa de las carreteras de algún lugar cualquiera, en el que un lado entre dos ciudades corresponde a un carril de una autopista entre las dos ciudades. Debido a que, a menudo, hay autopistas de varios carriles entre dos ciudades, esta representación origina un multígrafo.

La noción de multígrafo no dirigido puede definirse de manera similar a la de un multígrafo dirigido, como se ve a continuación.

Multígrafo no dirigido

Sea $G = (V, E)$ un grafo no dirigido, donde V es un conjunto de vértices y E es un ***multiconjunto*** de pares no ordenados de $V \times V$.

En estos términos, G es llamado un multígrafo no dirigido o simplemente multígrafo, y desde el punto de vista geométrico puede representarse como un conjunto de vértices V y un conjunto de lados E entre los vértices, donde no existe restricción en el número de lados de un vértice a otro.

EJEMPLO

Sea el grafo $G = (V, E)$ de la figura 6.45, donde:

$V = \{v_1, v_2, v_3, v_4\}$ y

$E = \{\{v_1, v_4\}, \{v_1, v_4\}, \{v_1, v_4\}, \{v_1, v_4\}, \{v_1, v_4\}, \{v_2, v_3\},$

$\{v_2, v_3\}, \{v_1, v_3\}, \{v_2, v_4\}, \{v_2, v_2\}, \{v_3, v_3\}\}$

En este caso, como G tiene un multiconjunto E de pares no ordenados de $V \times V$, entonces se trata de un multígrafo no dirigido.

Ahora bien, si se utiliza la definición de multiconjunto, entonces este quedaría definido como:

$$G = (V, E)$$

donde:

$V = \{v_1, v_2, v_3, v_4\}$ y

$E = \{(\{v_1, v_4\}, 5), (\{v_2, v_3\}, 2), (\{v_1, v_3\}, 1), (\{v_2, v_4\}, 1), (\{v_2, v_2\}, 1), (\{v_3, v_3\}, 1)\}$

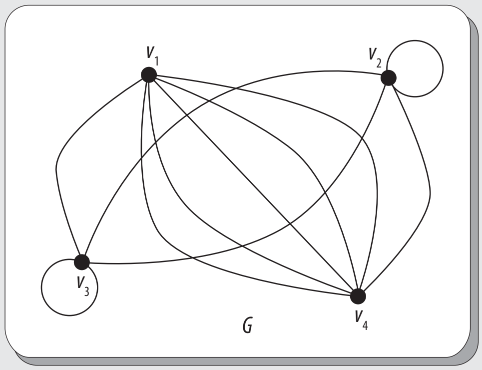


Figura 6.45 Multígrafo no dirigido.

En resumidas cuentas, un multígrafo, ya sea dirigido o no dirigido, es aquel grafo dirigido o no dirigido que contiene lados paralelos.

Grafo ponderado

En muchos casos, es preciso atribuir o asignar a cada lado de un grafo un número o valor específico, conocido como ponderación, peso, valuación o coste, según el contexto del que se trate, con lo que se obtiene un grafo ponderado (también denominado pesado, con peso o valuado).

El valor no negativo $w(i, j)$ que está asociado con el lado (i, j) es la ponderación de dicho lado.

Además, la ponderación de un grafo es la suma de los pesos de sus lados.

EJEMPLO

Supóngase un mapa carretero; si en este se interpretan las ciudades como vértices y los caminos entre estas como sus lados, al asignarles un valor a los caminos, como la distancia que hay entre las ciudades, que será la ponderación de cada lado, entonces resulta un grafo ponderado.

EJEMPLO

En la figura 6.46 se muestra un grafo ponderado, el cual es simplemente un grafo con datos o valores que le han sido asignados a sus lados.

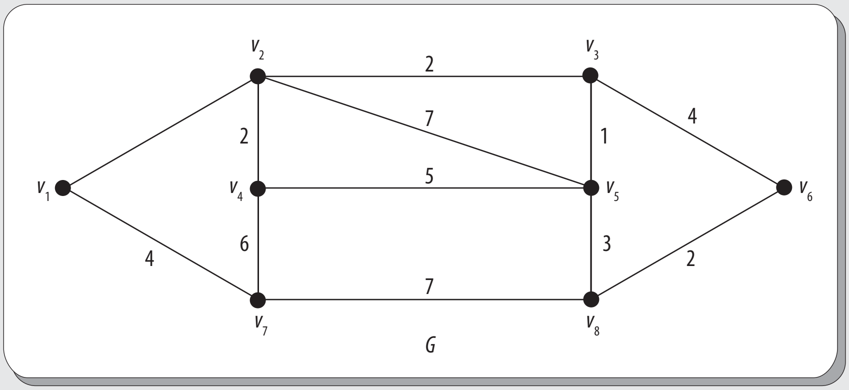


Figura 6.46 Grafo ponderado.

Matriz de pesos en un grafo ponderado

Sea $G = (V, E)$ un grafo ponderado finito tal que $V = \{v_1, \dots, v_n\}$. Se denomina matriz de peso del grafo G a la siguiente matriz de orden $n \times n$:

$$W = \begin{cases} w_{ij} \ \text{si} \ (v_i, v_j) \in E \\ \infty \ \text{si} \ (v_i, v_j) \notin E \end{cases}$$

EJEMPLO

La matriz de pesos del grafo de la figura 6.46 es:

$$\begin{pmatrix} \infty & 7 & \infty & \infty & \infty & \infty & 6 & \infty \\ 7 & \infty & 2 & 2 & 5 & \infty & \infty & \infty \\ \infty & 2 & \infty & \infty & 1 & 4 & \infty & \infty \\ \infty & 2 & \infty & \infty & 7 & \infty & 4 & \infty \\ \infty & 5 & 1 & 7 & \infty & \infty & \infty & 3 \\ \infty & \infty & \infty & 4 & \infty & \infty & \infty & 2 \\ 6 & \infty & \infty & 4 & \infty & \infty & \infty & 4 \\ \infty & \infty & \infty & \infty & \infty & 2 & 4 & \infty \end{pmatrix}$$

En un grafo ponderado, se denomina **camino más corto** o **camino liviano entre dos vértices** al camino de pesos mínimo entre dichos vértices, así como **camino más largo** o **camino crítico entre dos vértices** al camino de peso máximo entre dichos vértices.

6.6 Representaciones matriciales

Hasta ahora, se ha visto cómo representar un grafo a través de su representación geométrica o su representación algebraica.

Ahora bien, cuando se desea analizar un grafo en una computadora, se requiere de una presentación más formal, la cual se realiza principalmente a través de una matriz de adyacencia o de incidencia, cuya construcción se trata a continuación.

Matriz de adyacencia

Para obtener la matriz de adyacencia de un grafo $G = (V, E)$, la cual se representa como $A_G = [a_{ij}]$, primero se selecciona un orden arbitrario de vértices. A continuación, se le asigna a las filas y a las columnas de una matriz el mismo orden dado a los vértices.

El elemento de la matriz a_{ij} es 1, si los vértices correspondientes a la fila (renglón) y a la columna de dicho elemento están unidos por un lado, es decir, si estos son adyacentes, y 0 si no lo son. Otra forma de expresar lo anterior es:

$$a_{ij} = \begin{cases} 1 \text{ si } (v_1, v_j) \text{ son adyacentes} \\ 0 \text{ en caso contrario} \end{cases}$$

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.47.

Obtener su matriz de adyacencia.

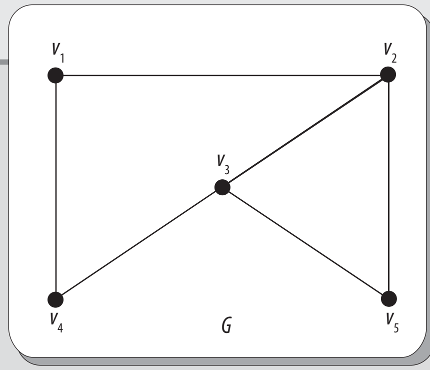


Figura 6.47 Grafo no dirigido G.

Solución

La matriz de adyacencia de dicho grafo es:

$$A_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

En el caso de que un vértice de G sea adyacente consigo mismo, se considera su valencia como 1.

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.48.

Obtener su matriz de adyacencia.

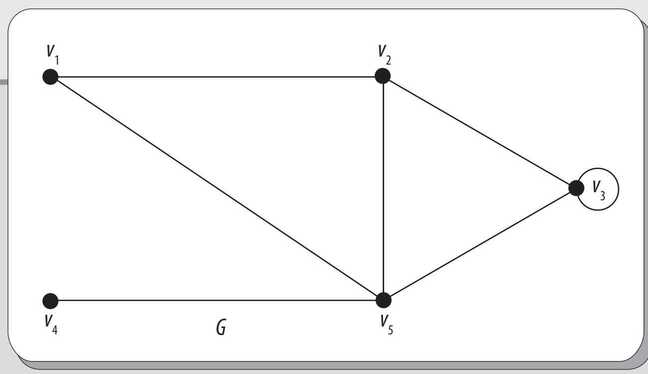


Figura 6.48 Grafo no dirigido G.

Solución

La matriz de adyacencia del grafo es:

$$A_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Es importante destacar aquí que en la matriz de adyacencia no es posible representar lados paralelos.

Con base en los dos ejemplos anteriores, entonces se puede decir que las características de la matriz de adyacencia son:

1. No es posible representar lados paralelos.
2. Un 1 en la diagonal principal representa un lazo.
3. Todas las matrices de adyacencia son cuadradas.
4. Como todas las matrices de adyacencia son simétricas con respecto a la diagonal principal, la información, a excepción de la contenida en la diagonal, aparece dos veces.
5. La valencia de un vértice v se obtiene mediante la suma de la fila o la columna correspondiente.

De manera similar, los grafos dirigidos se pueden representar mediante una matriz de adyacencia, la cual quizá no sea simétrica.

Ejemplo

Sea el grafo dirigido $G = (V, E)$ de la figura 6.49.

Obtener su matriz de adyacencia.

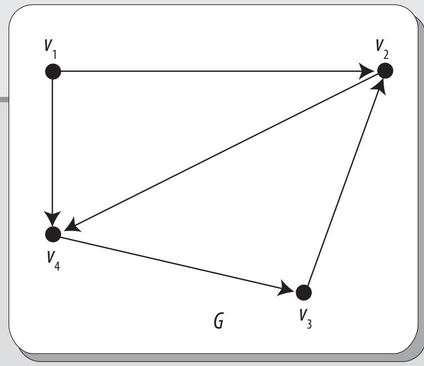


Figura 6.49 Grafo dirigido G.

Solución

La matriz de adyacencia de dicho grafo es:

$$A_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Como se observa en el ejemplo anterior, la matriz de adyacencia del grafo en cuestión no es simétrica; sin embargo, se contempla una nueva propiedad:

6. La valencia de salida de un vértice v se obtiene mediante la suma de la fila correspondiente y la valencia de entrada mediante la suma de la columna correspondiente.

En general, la matriz de adyacencia no es una manera muy eficaz de representar un grafo.

Matriz de incidencia

Otra representación útil de un grafo es la **matriz de incidencia**.

Para obtener la matriz de incidencia de un grafo, representada como $I_G = [b_{ij}]$, primero se selecciona un orden arbitrario de vértices y lados, y luego se asigna a las filas las marcas correspondientes a los vértices y a las columnas las correspondientes a los lados.

El elemento que corresponde a la fila y a la columna e es 1, si es incidente en algún vértice v, y 0 en cualquier otro caso. Esto es:

$$a_{ij} = \begin{cases} 1 \text{ si } e \text{ son adyacentes } v_1 \\ 0 \text{ en caso contrario} \end{cases}$$

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.50.

Solución

Obtener su matriz de incidencia.

La matriz de incidencia de dicho grafo es:

$$
I_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array}
\begin{array}{c}
\begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\
\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}
\end{array}
$$

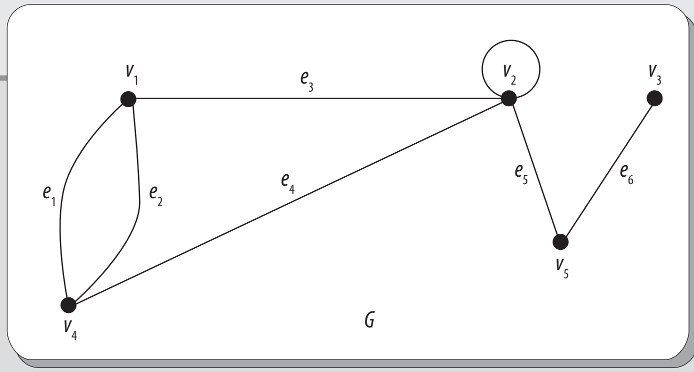


Figura 6.50 Grafo no dirigido G.

Con base en el ejemplo anterior, se puede decir que la matriz de incidencia tiene las siguientes características:

1. Permite representar lados paralelos y lazos de manera simultánea.
2. Un grafo sin lazos en cada columna tiene dos cifras 1.
3. La suma de cada fila da como resultado la valencia del vértice correspondiente.
4. Una columna en la cual se tiene un único 1, representa un lazo.
5. Dos columnas iguales, no necesariamente juntas, representan lados paralelos.

6.7 Isomorfismo de grafos

De manera coloquial, se dice que dos grafos son isomorfos si tienen la misma figura o se pueden modificar para obtener la misma figura, excepto por los nombres de los vértices.

Ahora bien, de manera más formal se dice que dos grafos, $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$, son isomorfos si existe una función biunívoca f entre los vértices de G_1 y G_2, y una función biunívoca g, entre lados de G_1 y G_2, tales que un lado e es incidente a i y j en G_1 si y solo si el lado $g(e)$ es incidente a los vértices $f(i)$ y $f(j)$ en G_2. A las funciones f y g se les denomina *isomorfismo* de G_1 en G_2.

Una vez definido el isomorfismo de G_1 en G_2 se procede a etiquetar los grafos de tal manera que se conserve la adyacencia de los vértices y la incidencia de los lados.

Ejemplo

Sean los grafos no dirigidos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ de la figura 6.51.

Determinar un isomorfismo para dichos grafos.

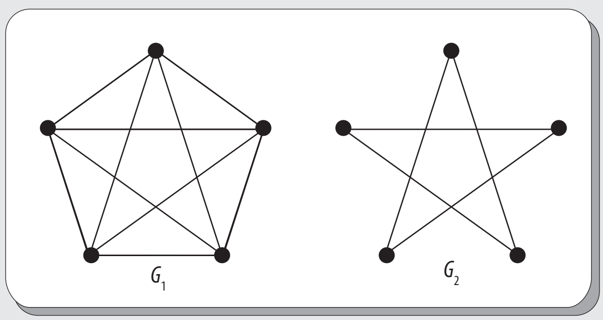


Figura 6.51 Grafos no dirigidos G_1 y G_2.

Solución

Un isomorfismo para los grafos G_1 y G_2 está definido por:

$$f(v_i) = V_i,\ i = 1, \ldots, 5$$

Es decir:

$$f(v_1) = V_1$$
$$f(v_2) = V_2$$
$$f(v_3) = V_3$$
$$f(v_4) = V_4$$
$$f(v_5) = V_5$$

Y:

$$g(e_i) = E_i,\ i = 1, \ldots, 5$$

Es decir:

$$g(e_1) = E_1$$
$$g(e_2) = E_2$$
$$g(e_3) = E_3$$
$$g(e_4) = E_4$$
$$g(e_5) = E_5$$

Ahora, se etiquetan los grafos de acuerdo con el isomorfismo definido, conservando la adyacencia y la incidencia, como se muestra en la figura 6.52.

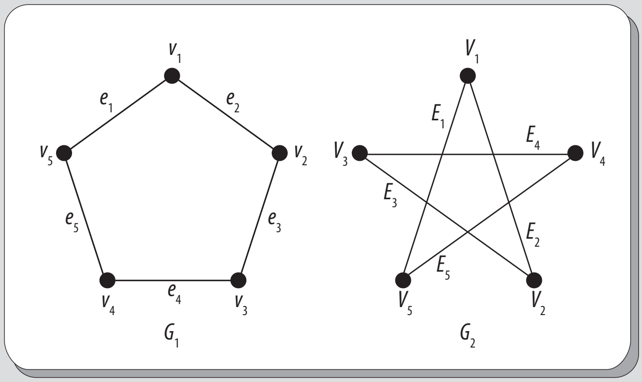


Figura 6.52 Isomorfismo de G_1 en G_2.

Otra forma de demostrar que dos grafos son isomorfos es la que se cita a continuación.

Dos grafos G_1 y G_2 son isomorfos si y solo si para alguna ordenación de vértices y lados sus matrices de incidencia son iguales.

EJEMPLO

Sean las matrices de incidencia de la figura 6.52, las que corresponden a los grafos G_1 y G_2, respectivamente, de la figura 6.51.

$$I_{G_1} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \qquad I_{G_2} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Como estas matrices son iguales, entonces se dice que los grafos G_1 y G_2 son isomorfos.

Para verificar si dos grafos dirigidos, G_1 y G_2, son isomorfos, primero se omite la dirección de los lados y luego se obtienen sus matrices de incidencia. Si dichas matrices de incidencia son iguales, se considera que esta es una condición necesaria, pero no suficiente, para verificar si son isomorfos. El siguiente paso es verificar si se conserva la incidencia de lados, respetando el sentido de los lados. Si esto ocurre, entonces los grafos dirigidos G_1 y G_2 son isomorfos.

6.8 Grafos aplanables

Este tipo de grafos, además de ser muy frecuentes, también cuentan con muchas propiedades interesantes. A continuación se analizan algunas de las más importantes.

Grafo aplanable

Se dice que un grafo $G = (V, E)$ es aplanable si este puede dibujarse sobre un plano de tal manera que ningún lado se cruce con otro, excepto, desde luego, en los vértices comunes.

Por ejemplo, el grafo $G = (V, E)$ de la figura 6.53 es aplanable.

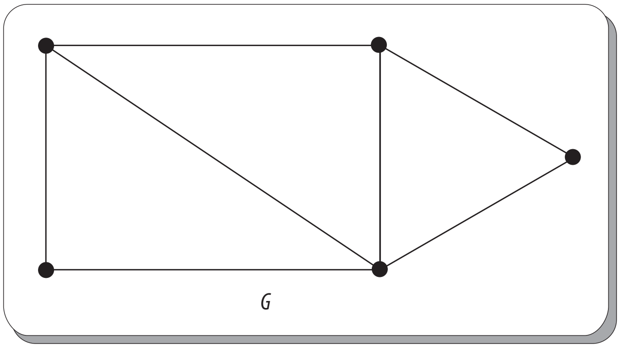


Figura 6.53 Grafo G aplanable.

EJEMPLO

En apariencia, el grafo G_1 de la figura 6.54 no es aplanable, ya que sus lados se cortan en un punto distinto de sus cuatro vértices; sin embargo, este también puede representarse como se muestra en el grafo G_2 de la misma figura. Por tanto, se dice que G_1 sí es aplanable.

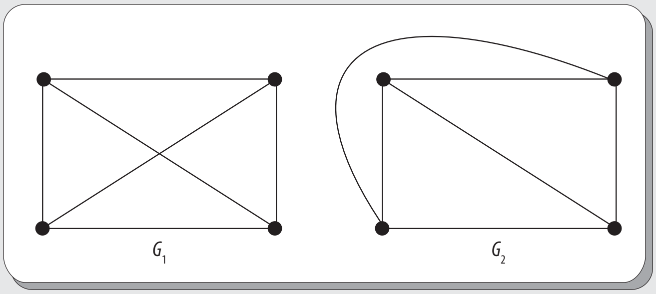


Figura 6.54 El G_1 es aplanable ya que puede representarse como G_2.

Entonces, si un grafo, en apariencia, es no aplanable, pero se puede representar o redibujar como un grafo aplanable, se considera que el grafo original es aplanable. Aunque, en realidad, dichos grafos tienen que ser isomorfos.

Un grafo aplanable divide al plano en diversas áreas, y cada una se denomina región de un grafo aplanable, la cual se define a continuación.

Región de un grafo aplanable

Una región (o cara) R de un grafo aplanable es un área del plano que está acotada por los lados y no puede continuar dividiéndose en subáreas.

Además, se dice que una región R es infinita si su área es infinita y finita si su área también lo es.

En un grafo aplanable se tiene exactamente una región infinita.

Ejemplo

Sea el grafo no dirigido aplanable $G = (V, E)$ de la figura 6.55. Obtener la cantidad de regiones que tiene el mismo.

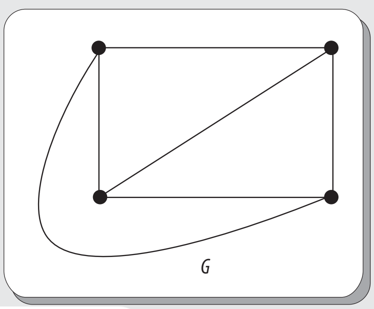


Figura 6.55 Grafo no dirigido aplanable G.

Solución

Como se puede observar, el grafo en cuestión tiene cuatro regiones; las primeras tres se muestran en la figura 6.56*i*), las cuales son finitas, mientras que la cuarta región es infinita y se muestra en la figura 6.56 *ii*).

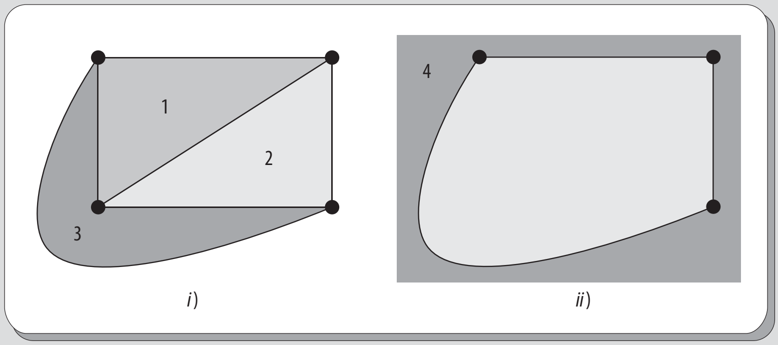


Figura 6.56 Regiones del grafo *G*. i) Tres finitas y ii) una infinita.

Fórmula de Euler para grafos aplanables

En ocasiones, resulta complicado identificar las regiones de un grafo aplanable. No obstante, Euler demostró que todas las representaciones aplanables de un mismo grafo dividen al plano en igual número de regiones, lo que logró hallando una relación entre el número de regiones, el tamaño y el orden de un grafo aplanable. Dicha relación se conoce como **fórmula de Euler para grafos aplanables**, la cual se representa de la siguiente manera:

$$|V| - |E| + R = 2$$

donde $|V|$, $|E|$ y R son el orden, el tamaño y la cantidad de regiones, respectivamente.

Sin excepción alguna, todos los grafos aplanables conexos siempre deben satisfacer la fórmula de Euler.

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ de la figura 6.57. Obtener la cantidad de regiones que tiene el mismo.

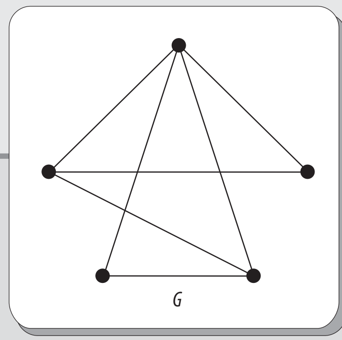


Figura 6.57 Grafo no dirigido *G*.

Solución

Dado que $|V| = 5$ y $|E| = 7$, si se utiliza la fórmula de Euler para grafos aplanables y se despeja R, se tiene que:

$$R = |E| - |V| + 2$$
$$7 - 5 + 2 = 4$$

Esto es, el grafo tiene cuatro regiones.

Para comprobar que esta es la cantidad correcta de regiones, se tiene que buscar una representación aplanable de dicho grafo; es decir, un grafo isomorfo aplanable.

Así, un grafo isomorfo aplanable al de la figura 6.57 es el que se observa en la figura 6.58, donde se puede ver que, en efecto, este tiene las mismas cuatro regiones obtenidas por la fórmula de Euler para grafos aplanables.

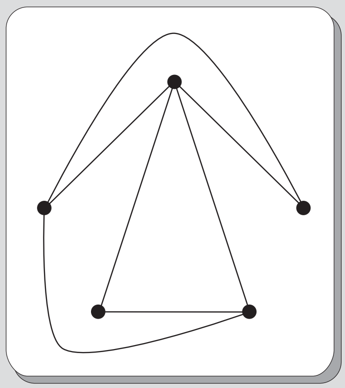


Figura 6.58 Grafo isomorfo aplanable al grafo de la figura 6.57.

Una relación que se obtiene de la fórmula de Euler para grafos aplanables es la siguiente:

En cualquier grafo aplanable conexo que no tenga lazos ni lados paralelos y que tenga dos o más lados, se cumple la desigualdad:

$$|E| \leq 3\,|V| - 6$$

Debido a que el grafo no tiene lazos ni lados paralelos, cada región es acotada por tres o más lados, por tanto el número es mayor o igual que $3R$. En la frontera, a lo largo de dos regiones, el número total es igual o menor a $2|E|$, así se tiene que:

$$2|E| \geq 3R$$

o:

$$\frac{2}{3}|E| \geq R$$

Así, de acuerdo con la fórmula de Euler, se tiene que:

$$|V| - |E| + \frac{2\,|E|}{3} \geq 2$$

o:

$$3|V| - 6 \geq |E|$$

EJEMPLO

La figura 6.54 en realidad constituye el grafo completo K_4, que, como ya se vio antes, es aplanable; por tanto, se debe cumplir:

$$3|V| - 6 \geq |E|$$

En este caso, primero se tiene que:

$$|V| = 4,\ |E| = 6$$

Luego, se sustituyen dichos valores en la desigualdad:

$$(3) \cdot (4) - 6 \geq 6$$

$$6 = 6$$

con lo que se cumple la desigualdad.

EJEMPLO

Sea el grafo completo K_5; entonces, se tiene que:

$$|V| = 5,\ |E| = 10$$

Si se sustituyen estos valores en la desigualdad mencionada, se tiene:

$$3 \cdot 5 - 6 \geq 10$$

$$9 \not\geq 10$$

Como no se cumple la desigualdad, se puede inferir que K_5 no es grafo aplanable. Más adelante se ratifica esta afirmación.

Homeomorfismo de grafos

Es evidente que el hecho de que un grafo no dirigido $G = (V, E)$ sea aplanable no se ve afectado porque un lado sea dividido en dos lados por la inserción de un vértice de valencia 2, como se observa en la figura 6.59 *i*) o si dos lados se combinan en un solo lado, al eliminar un vértice de este tipo, como se ve en la figura 6.59 *ii*).

Dos grafos no dirigidos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$, ambos sin lazos, son ***homeomorfos*** (o grafos isomorfos bajo vértices de valencia 2) si:

- Son isomorfos.
- Pueden transformarse en grafos isomorfos mediante repeticiones de inserciones y/o eliminaciones de vértices de valencia 2.

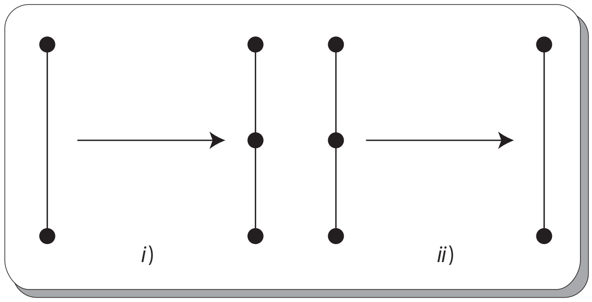


Figura 6.59 Inserción y eliminación de vértices de valencia 2 en un lado de un grafo.

Ejemplo

Sean los grafos no dirigidos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ de la figura 6.60.

Determinar si estos grafos son homeomorfos.

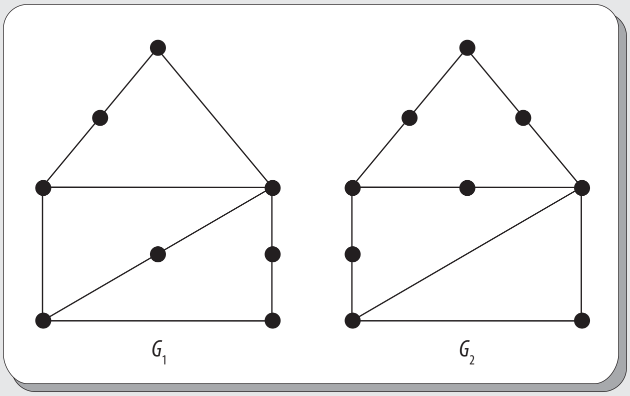


Figura 6.60 Grafos no dirigidos.

Solución

Como G_1 y G_2 son grafos isomorfos mediante repeticiones de inserciones y eliminaciones de vértices de valencia 2, como se muestra en la figura 6.61; entonces, se considera que son homeomorfos.

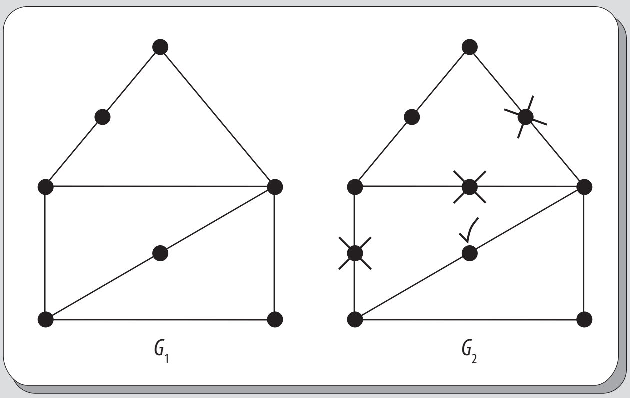


Figura 6.61 Grafos homeomorfos.

En su época, el matemático polaco Kazimiers Kuratowski (1896-1980) demostró que un grafo es aplanable mediante el uso del concepto de homeomorfismo de grafos y formuló el teorema de Kuratowski, que se cita a continuación.

Teorema

Teorema de Kuratowski

Un grafo es aplanable si, y solo si, no contiene ningún subgrafo que sea homeomorfo a alguno de los llamados ***grafos de Kuratowski***.

Los grafos de Kuratowski se observan con detalle en la figura 6.62. Dichos grafos son K_5 y $K_{3,3}$, respectivamente.

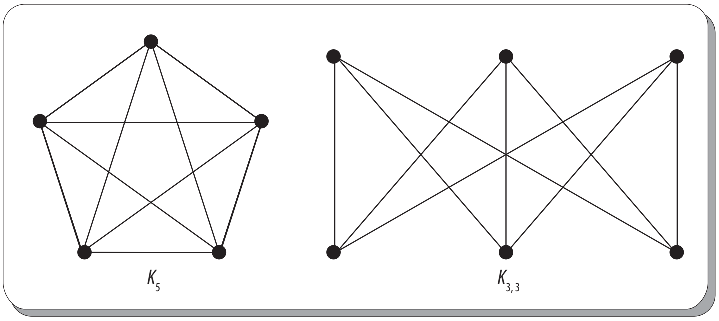


Figura 6.62 Grafos de Kuratowski.

Ejemplo

Sea el grafo $G = (V, E)$ completo K_6, que se muestra en la figura 6.63. Determinar si este grafo es aplanable.

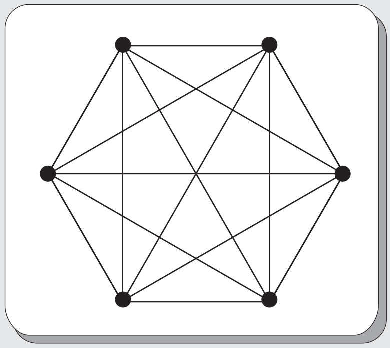


Figura 6.63 Grafo completo K_6.

Solución

En este caso, primero se rota a K_6, como se muestra en la figura 6.64*i*). Si se eliminan los lados horizontales internos, se obtiene el subgrafo que se observa en la figura 6.64*ii*). Después, si se eliminan los lados inclinados externos, tanto superiores como inferiores, se obtiene el subgrafo de la figura 6.64*iii*), el cual es $K_{3,3}$. Por último, alargando o reduciendo la distancia de los lados verticales, se obtiene el subgrafo de la figura 6.64*iv*), el cual efectivamente ratifica que es $K_{3,3}$. Por tanto, se dice que K_6 tiene un subgrafo homeomorfo a $K_{3,3}$, por lo que dicho grafo no es aplanable.

Otra opción es rotar nuevamente a K_6, como se muestra en la figura 6.64*v*). Luego, se elige un vértice y se eliminan todos los lados que surjan de este, como en la figura 6.64*vi*), el cual se observa que es K_5. Por último, alargando o reduciendo la distancia entre los lados de la parte inferior, se obtiene el subgrafo de la figura 6.64*vii*), que ratifica que es K_5. Por tanto, K_6 tiene un subgrafo homeomorfo a K_5, con lo cual se comprueba, nuevamente, que dicho grafo no es aplanable.

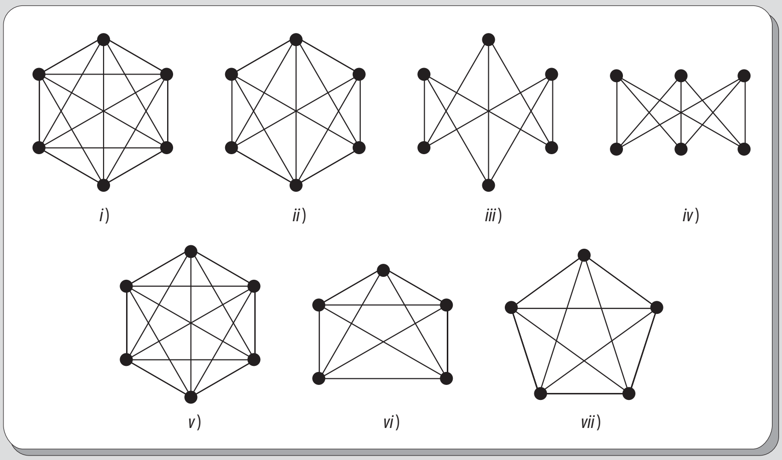


Figura 6.64 Procesos para verificar que K_6 no es aplanable.

Del ejemplo anterior se deduce que todo grafo completo K_n, $n \geq 5$, no es aplanable, ya que siempre contendrá un subgrafo homeomorfo a K_5 o a $K_{3,3}$.

6.9 Algoritmos para grafos

Para el tratamiento de esta sección, antes que nada se debe conocer lo que es un ***algoritmo***, para luego aplicar este concepto en los grafos.

Algoritmo

El término **algoritmo** proviene del árabe *al-Khowârizmî*, sobrenombre del célebre matemático árabe Mohámed ben Musa.

Por algoritmo, comúnmente se entiende a la descripción de cómo resolver un problema. El conjunto de instrucciones que especifican la secuencia de operaciones a realizar, en orden, para resolver un sistema específico o clase de problemas, también se denomina algoritmo. En otras palabras, un algoritmo es una "especie de fórmula" para la resolución de un problema.

Existen diversos algoritmos para grafos, los cuales se utilizan para resolver problemas específicos; dos de los más importantes son el algoritmo de Fleury y el algoritmo de Dijkstra.

Algoritmo de Fleury

El **algoritmo de Fleury** se utiliza para determinar si un grafo tiene un circuito de Euler.

Los pasos de dicho algoritmo son:

1. Comprobar que el grafo sea conexo y que todos los vértices tengan valencia par.
2. Elegir un vértice inicial de forma arbitraria.
3. En cada paso, recorrer cualquier lado disponible siempre y cuando el grafo siga siendo conexo.
4. Después de recorrer el lado, borrarlo y recorrer otro lado disponible.
5. Cuando ya no se pueda seguir el recorrido, se debe terminar; entonces, se dice que se ha encontrado un circuito de Euler.

Ejemplo

Sea el grafo $G = (V, E)$ que se observa en la figura 6.65.

Utilizando el algoritmo de Fleury, encontrar un circuito de Euler en dicho grafo.

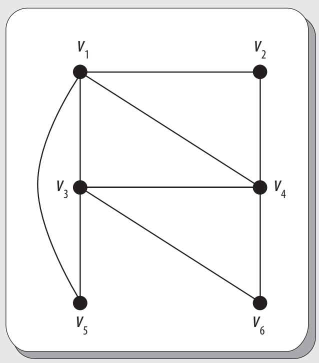


Figura 6.65 Grafo no dirigido.

Solución

De acuerdo con el algoritmo de Fleury, primero se debe verificar que el grafo sea conexo y que todos los vértices tengan valencia par; en este caso, el grafo cumple las condiciones necesarias. Luego, se elige en forma arbitraria un vértice, sea v_6 dicho vértice.

Continúa

Enseguida, siguiendo el algoritmo, se recorren los lados disponibles, de tal forma que el grafo siga siendo conexo. Todo lado recorrido se borra y se recorre otro lado disponible.

Por último, el algoritmo concluye cuando ya no es posible seguir recorriendo lados.

Todo el proceso se muestra en la figura 6.66.

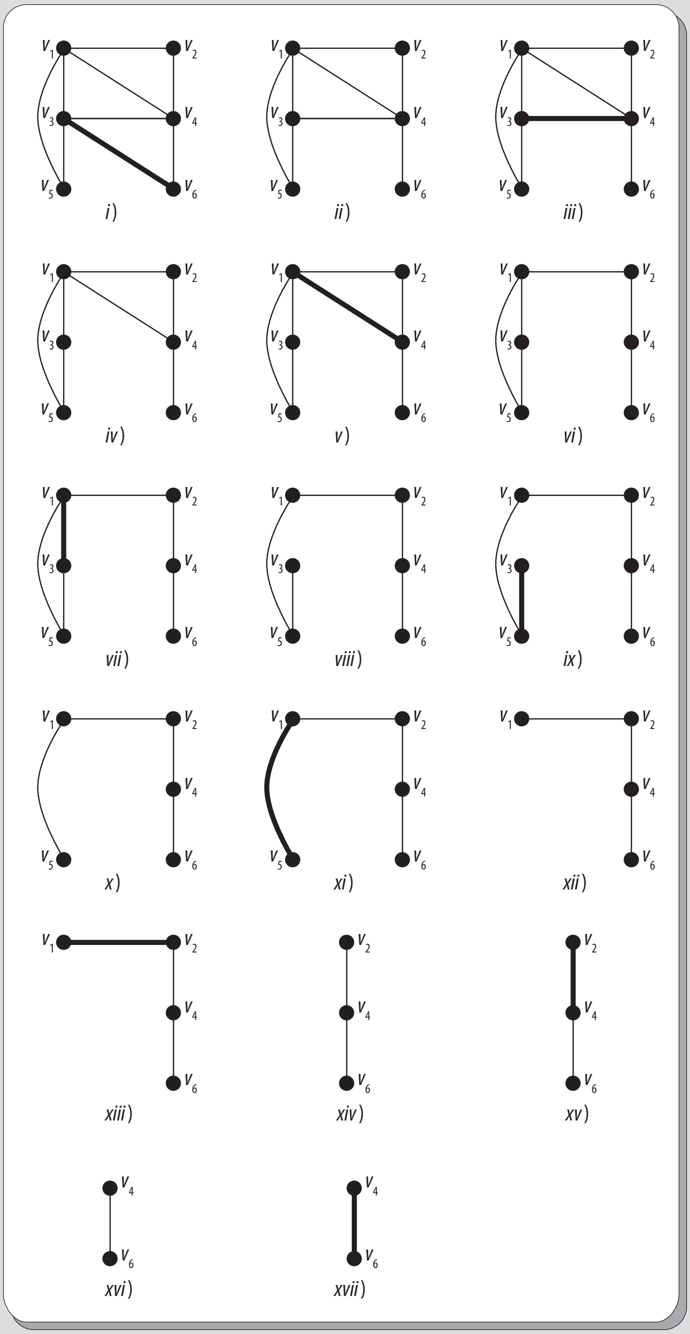


Figura 6.66 Proceso para obtener un circuito de Euler mediante el algoritmo de Fleury.

El circuito de Euler obtenido mediante el uso del algoritmo de Fleury es el siguiente:

$\{v_6, v_3, v_4, v_1, v_3, v_5, v_1, v_2, v_4, v_6\}$

Algoritmo de Dijkstra

El algoritmo de Dijkstra debe su nombre al matemático Edsger Dijkstra, quien lo descubrió en 1959. Este algoritmo se utiliza para determinar el camino más corto entre dos vértices en un grafo ponderado.

Existen muchas versiones para encontrar el camino más corto entre dos vértices, pero la versión de Dijkstra se aplica a grafos ponderados no dirigidos conexos que no tengan lados con pesos negativos.

Uno de los aspectos principales del algoritmo de Dijkstra es que todos los vértices del grafo se tienen que etiquetar; sea $L(i)$ la etiqueta del vértice i.

Además, en este se considera el hecho de que habrá vértices que tendrán etiquetas temporales y otros que tendrán etiquetas permanentes.

Es importante aclarar que antes de iniciar con el algoritmo, primero se debe seleccionar un vértice inicial.

Sean un grafo no dirigido ponderado conexo de N vértices, x el vértice inicial, D un vector de tamaño N que guardará, al final del algoritmo, las distancias desde x al resto de los vértices.

Los pasos de dicho algoritmo son:

1. Inicializar todas las distancias en D con un valor infinito relativo, ya que estas son desconocidas al principio, exceptuando la de x, que se debe colocar en 0, debido a que la distancia de x a x sería 0.
2. Sea $a = x$; es decir, se toma el vértice a como el actual.
3. Se recorren todos los nodos adyacentes de a, excepto los nodos marcados (a estos se les llama v_i).
4. Si la distancia desde x hasta v_i guardada en D es mayor que la distancia desde x hasta a, sumada a la distancia desde a hasta v_i; esta se sustituye con la segunda nombrada, esto es:

   Si $(Di > Da + d(a, v_i))$, entonces $Di = Da + d(a, v_i)$
5. Se marca como completo el nodo a.
6. Se toma como próximo nodo actual el de menor valor en D (los valores pueden haberse almacenado en una cola de prioridad) y se vuelve al paso 3, siempre y cuando haya nodos no marcados.

Una vez terminado el algoritmo, D estará completamente lleno.

Ejemplo

Sea el grafo $G = (V, E)$ de la figura 6.67.

Utilizando el algoritmo de Dijkstra, encontrar el camino más corto del vértice v_1 al v_8 en dicho grafo.

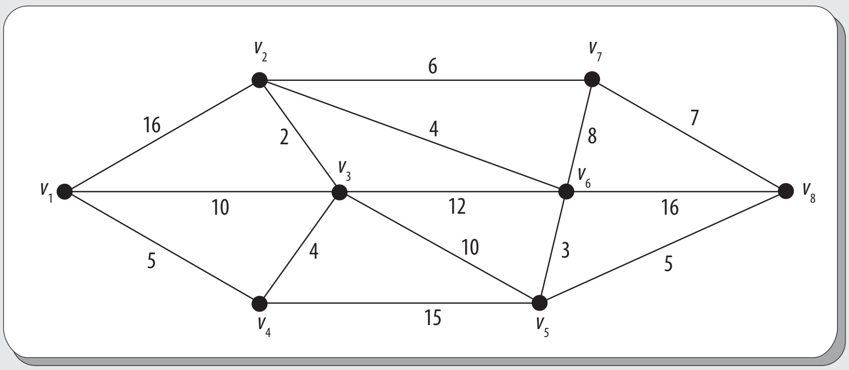
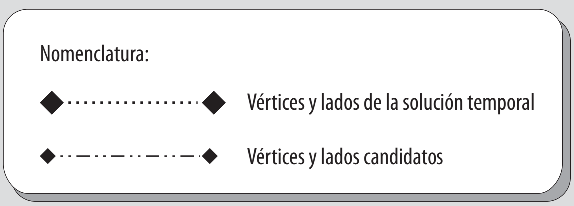


Figura 6.67 Grafo no dirigido.

Solución

Para la solución de este problema, a continuación se muestra y se describe cada uno de los pasos del proceso para obtener el camino más corto del vértice v_1 al v_8.



Continúa

Paso 1

En este paso hay tres candidatos: los vértices v_2, v_3 y v_4. En este caso, se toma el camino del vértice v_1 al v_4, ya que es el camino más corto de los tres (véase figura 6.68).

Solución temporal:

Camino: v_1, v_4

Distancia: 5

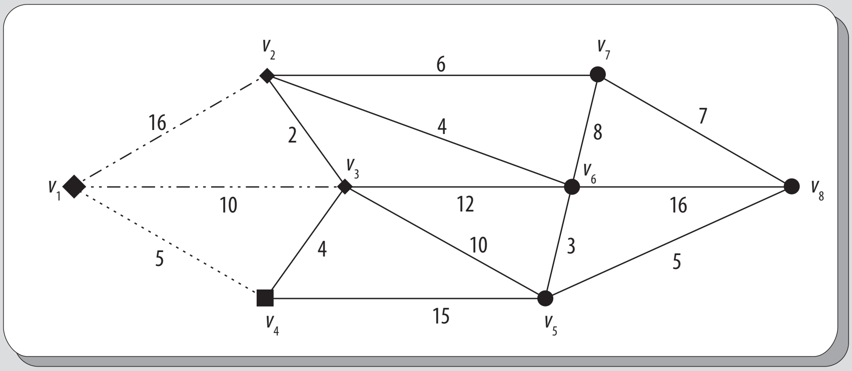


Figura 6.68 Paso 1.

Paso 2

Ahora, se añade un nuevo candidato, el vértice v_5, y el vértice v_3, pero esta vez a través del vértice v_4. No obstante, el camino mínimo surge al añadir el vértice v_3 (véase figura 6.69).

Solución temporal:

Camino: v_1, v_4, v_3

Distancia: 9

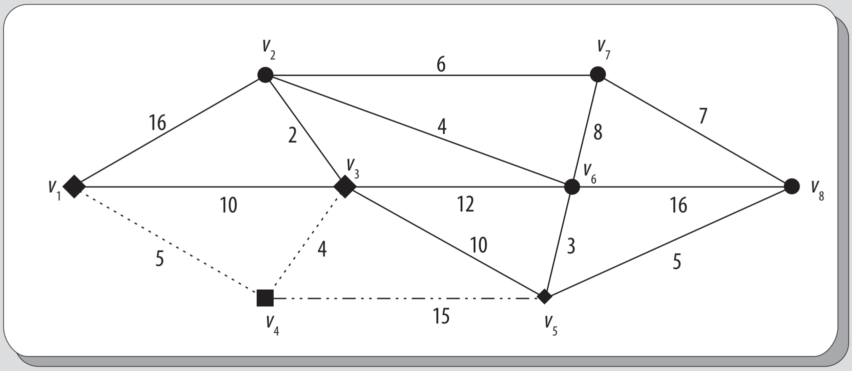


Figura 6.69 Paso 2.

Paso 3

En este paso no se añade ningún candidato más, ya que el último vértice es el mismo que en el paso anterior. En este caso, el camino mínimo (véase figura 6.70) hallado es:

Solución temporal:

Camino: v_1, v_4, v_3, v_2

Distancia: 11

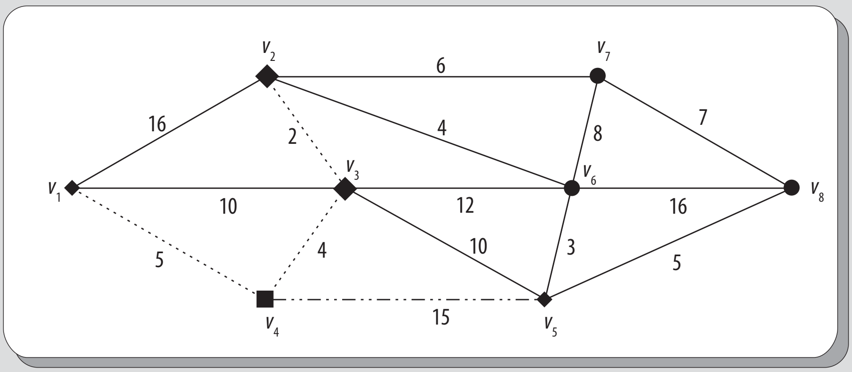


Figura 6.70 Paso 3.

Continúa

Paso 4

En este paso se añaden dos candidatos nuevos, los vértices v_6 y v_7, ambos a través del vértice v_2. El camino mínimo hallado en todo el grafo hasta ahora (véase figura 6.71) es:

Solución temporal:

Camino: v_1, v_4, v_3, v_2, v_6

Distancia: 15

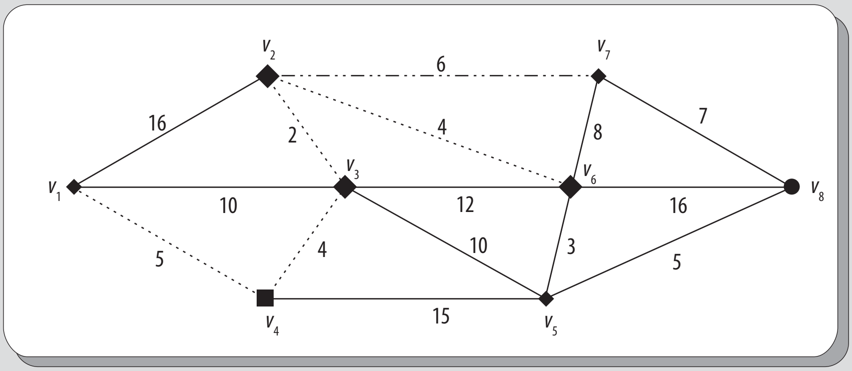


Figura 6.71 Paso 4.

Paso 5

En este paso se añaden tres vértices candidatos: los vértices v_7, v_8 y v_5, aunque este último ya estaba, pero en este paso aparece a través del vértice v_6. En este caso, el camino mínimo (véase figura 6.72), que cambia un poco con respecto al anterior, es:

Solución temporal:

Camino: v_1, v_4, v_3, v_2, v_7

Distancia: 17

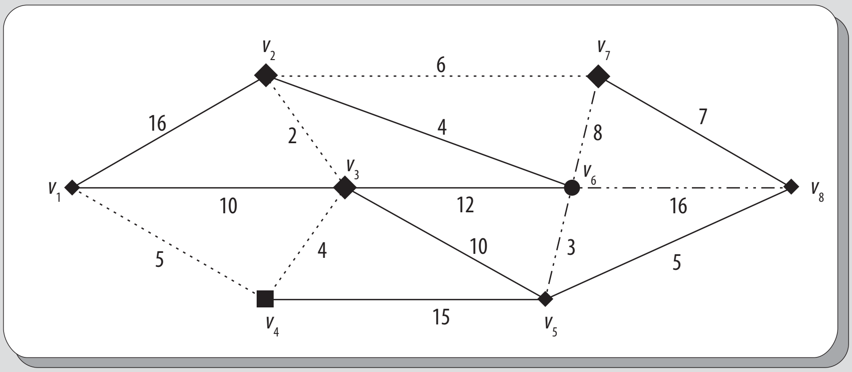


Figura 6.72 Paso 5.

Paso 6

En este paso vuelve a aparecer otro candidato: el vértice v_8, pero esta vez a través del vértice v_7. De todas formas, el camino mínimo (véase figura 6.73), aunque vuelve a cambiar para retomar el camino que venía siguiendo en los pasos anteriores, es:

Solución temporal:

Camino: v_1, v_4, v_3, v_2, v_6, v_5

Distancia: 18

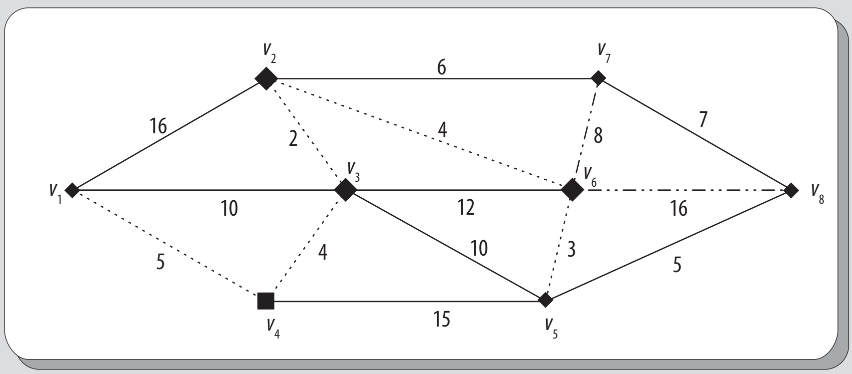


Figura 6.73 Paso 6.

Continúa

Paso 7

En este paso solo se añade un candidato: el vértice v_8, a través del vértice v_5. El camino mínimo (véase figura 6.74) y final obtenido es:

Solución final:

Camino: $v_1, v_4, v_3, v_2, v_6, v_5, v_8$

Distancia: 23

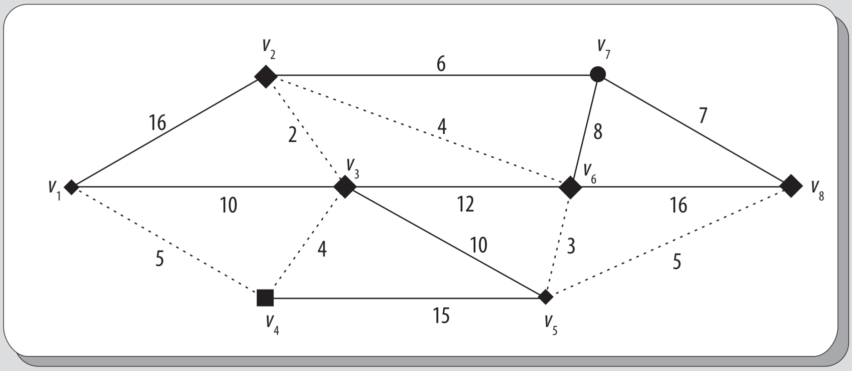


Figura 6.74 Paso 7.

6.10 Coloreado de grafos

El coloreado de un grafo no dirigido conexo $G = (V, E)$ ocurre cuando se asignan colores a los vértices de G, de modo que si v_i y v_j son adyacentes, entonces v_i y v_j tendrán colores distintos asignados. El número mínimo de colores necesarios para el coloreado propio de un grafo es lo que se conoce como número cromático del grafo.

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ que se observa en la figura 6.75. Obtener el número cromático de dicho grafo.

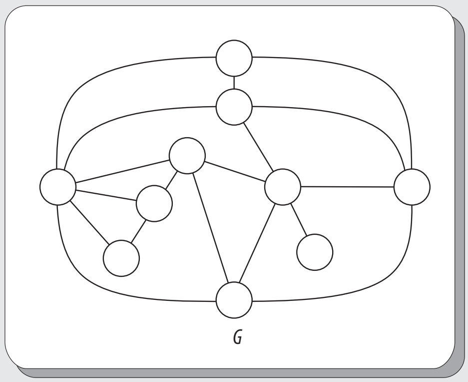


Figura 6.75 Grafo no dirigido.

Solución

Se desea colorear los vértices de G, de modo que no haya dos vértices conectados del mismo color y utilizando la mínima cantidad de colores posible.

En este grafo, el número cromático es 4 (1 = rojo, 2 = azul, 3 = verde y 4 = amarillo), ya que es el número mínimo de colores para el coloreado (véase figura 6.76).

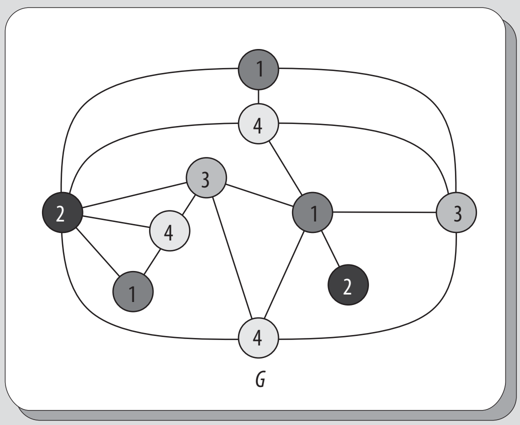


Figura 6.76 Grafo no dirigido G coloreado.

Es importante destacar que no hay ningún algoritmo eficiente para colorear un grafo. No obstante, a continuación se muestra uno simple que consiste en comenzar coloreando los vértices de mayor valencia; sin embargo, este algoritmo no siempre produce el mejor coloreado.

Algoritmo para colorear vértices

Los pasos para este algoritmo son:

1. Hacer lista de vértices según el orden de su valencia, de mayor a menor:

$$\delta(v_1) \geq \delta(v_2) \geq \ldots \geq \delta(v_n)$$

   Se elige una ordenación cuando dos vértices tienen igual valencia.
2. Asignar a v_1 el color 1, así como a todos los vértices de la lista, en orden, que no sean adyacentes a uno coloreado con el color 1.
3. Asignar el color 2 al primer vértice de la lista que no haya sido coloreado con el color 1. Seguir coloreando con el color 2 los vértices de la lista no coloreados que no sean adyacentes a vértices con el color 2.
4. Continuar el coloreado hasta que se hayan agotado todos los vértices.

Ejemplo

Sea el grafo no dirigido $G = (V, E)$ que se muestra en la figura 6.77. Utilizando el algoritmo para coloreado de vértices, colorear dicho grafo.

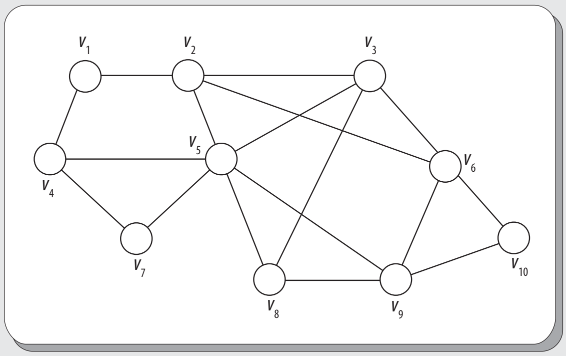


Figura 6.77 Grafo no dirigido *G* coloreado.

Solución

De acuerdo con el algoritmo para el coloreado de vértices, los pasos para colorear el grafo son:

Paso 1

Obtener las valencias de cada vértice:

$$\delta(v_1) = 2,\ \delta(v_2) = 4,\ \delta(v_3) = 4,\ \delta(v_4) = 3,\ \delta(v_5) = 6,$$
$$\delta(v_6) = 4,\ \delta(v_7) = 2,\ \delta(v_8) = 3,\ \delta(v_9) = 4,\ \delta(v_{10}) = 2$$

Luego, los vértices se ordenan de mayor a menor, de acuerdo con su valencia, quedando:

$$v_5, v_2, v_4, v_6, v_9, v_4, v_8, v_1, v_7, v_{10}$$

Continúa

Paso 2

Sean los colores rojo = 1, azul = 2, verde = 3 y amarillo = 4. De este modo, al vértice v_5 se le asigna el color 1, que es el rojo, así como a todos los vértices de la lista, en orden, que no sean adyacentes a uno coloreado con el color rojo (véase figura 6.78).

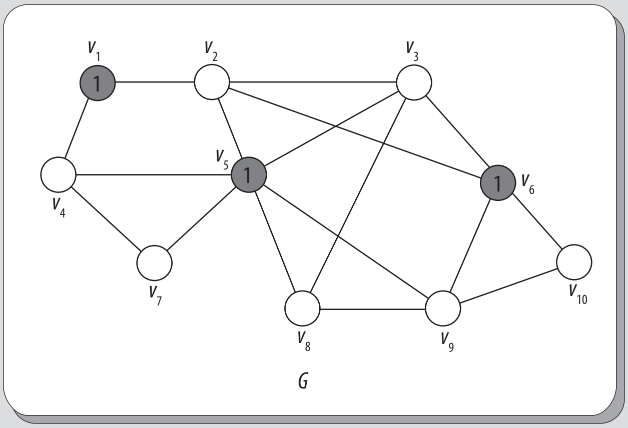


Figura 6.78 Paso 2 en el coloreado del grafo.

Paso 3

A continuación se asigna el color 2 (azul) al primer vértice de la lista que no haya sido coloreado con el color rojo, en este caso v_2 y se sigue coloreando con el color azul los vértices de la lista no coloreados que no sean adyacentes a vértices con el color azul (véase figura 6.79).

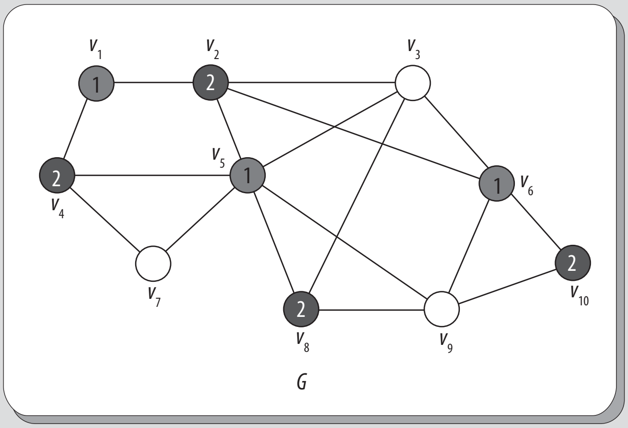


Figura 6.79 Paso 3 en el coloreado del grafo.

Paso 4

Como en este paso aún hay vértices sin colorear, se repite el procedimiento del paso anterior, y se asigna el color 3 (verde) al primer vértice de la lista que no haya sido coloreado con el color azul, en este caso v_9. Colorear con el color verde todos los vértices de la lista no coloreados que no sean adyacentes a vértices con el color azul (véase figura 6.80).

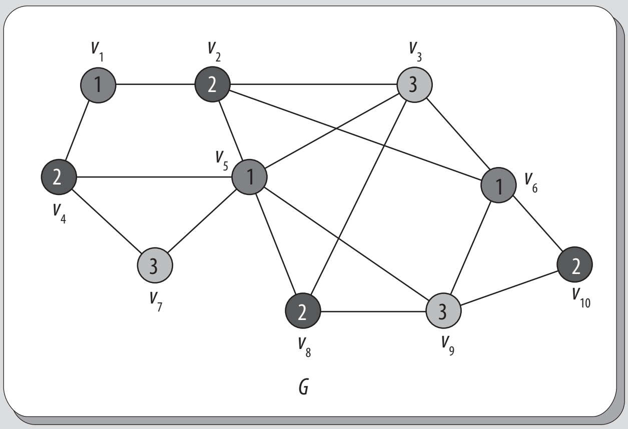
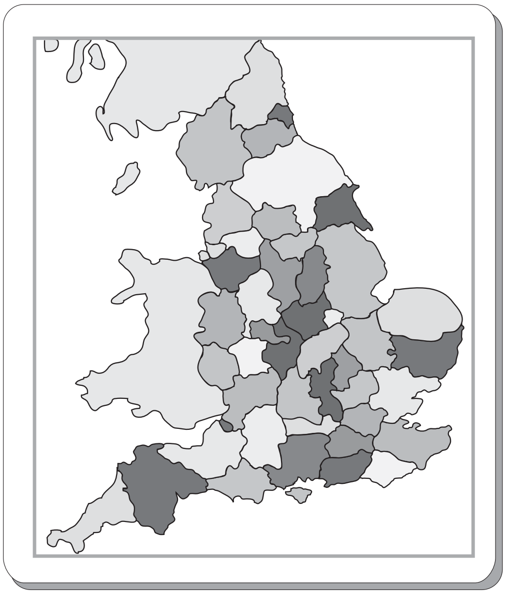


Figura 6.80 Paso 4 en el coloreado del grafo.

Como después de este punto ya no quedan vértices sin colorear, se termina el algoritmo y se concluye que como solo se utilizaron tres colores para colorear el grafo, entonces su número cromático es precisamente tres.

Teorema de los cuatro colores



Francis Guthrie, estudiante de Augustus de Morgan, se dio cuenta de que solo bastaban cuatro colores para colorear un mapa completo de los condados de Inglaterra (véase figura 6.81, donde solo se muestran los condados sin aplicar el teorema).

Aquí nació la conjetura. Augustus de Morgan hizo publicidad del problema entre los matemáticos. Hasta la fecha se han dado varias pruebas incorrectas del teorema de los cuatro colores, la más famosa es la del abogado inglés Alfred Kempe, quien la publicó en 1879 y fue aceptada como correcta por los matemáticos hasta 1890, cuando Pearcy Heawood encontró un error en su demostración.

Al final, este teorema fue demostrado por Kenneth Appel y Wolfgang Haken(Estados Unidos de América) en 1976, quienes para su demostración utilizaron una supercomputadora para examinar 2 000 configuraciones diferentes de mapas, a las que habían reducido el problema. Para la demostración se necesitaron 1 000 horas de proceso.

Sin embargo, esta demostración no es aceptada por todos los matemáticos, dado que sería impracticable por su gran cantidad de detalles, de manera que una persona se vería imposibilitada para verificarlo en forma manual.

Solo queda aceptar la exactitud del programa, el compilador y la computadora donde se ejecutó la prueba. Otro aspecto de la demostración, el cual puede ser considerado negativo, es su falta de elegancia.

Solución

Aunque este grafo es mucho más complejo que el de la figura 6.75, en este también es posible observar que el número cromático es 4 (rojo, azul, verde y amarillo), pues (de nueva cuenta) es la mínima cantidad de colores para el coloreado (véase figura 6.83).

1. Rojo
2. Azul
3. Verde
4. Amarillo

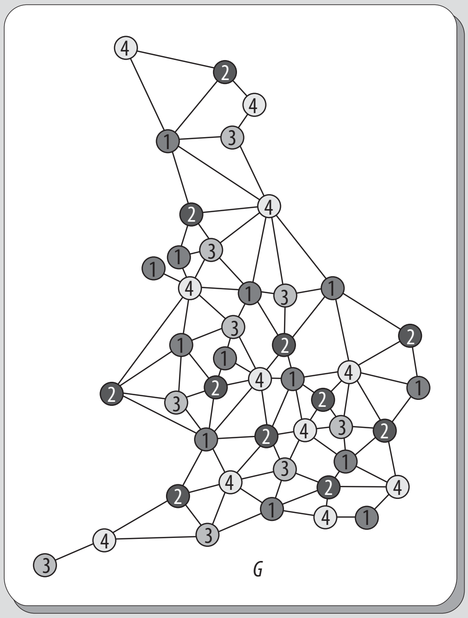


Figura 6.83 Coloreado de la representación de los condados de Inglaterra.

Determinación del número cromático utilizando álgebra lineal

Una manera de determinar el número cromático de un grafo simple no dirigido conexo $G = (V, E)$ es mediante el análisis de los **autovalores** asociados a su matriz de adyacencia A_G.

La matriz de adyacencia depende de la ordenación de los vértices; como se recordará, siempre será una matriz simétrica con diagonal principal.

El procedimiento para calcular los **autovalores** o **eigenvalores** es relativamente sencillo; no obstante, se debe mantener el orden y evitar confusiones. El procedimiento es el siguiente:

1. Se crea el polinomio característico, que es de la siguiente forma:

$$p(\lambda) = \text{determinante}(A_G - \lambda \cdot \mathbf{I})$$

Esto se hace armando la matriz A_G y restando en cada uno de los componentes de la diagonal. Se debe tener en cuenta que $\mathbf{I}$ es la matriz identidad, es decir la matriz que tiene todos 1 en la diagonal y todos 0 en las otras posiciones de la matriz.

2. Se encuentran las raíces λ igualando el polinomio característico a cero. De esta forma, se encuentran todos los autovalores para esta matriz.

Si se considera el grafo de la figura 6.84:

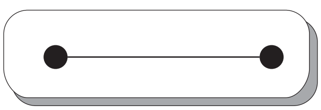


Figura 6.84 Grafo no dirigido sin lazos ni lados paralelos.

Este tiene como matriz de adyacencia:

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Y como **I**:

$$I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Entonces:

$$|AG - \lambda I| = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = 0$$

Del determinante se obtiene el polinomio característico:

$$\lambda^2 - 1 = (\lambda - 1)(\lambda + 1) = 0$$

Entonces, $\lambda_1 = 1$ y $\lambda_1 = -1$, son los autovalores.

Como la matriz de adyacencia es simétrica, los autovalores asociados a la misma son siempre números reales. Por tanto, estos pueden ser ordenados de menor a mayor. Además, el grafo debe ser conexo.

Sea λ_1 el autovalor más grande y λ_n el autovalor más pequeño. Si x es el número cromático de un grafo simple, entonces se cumple:

$$1 - \frac{\lambda_1}{\lambda_n} \le x \le 1 + \lambda_1$$

En este caso: $\lambda_1 = 1$ y $\lambda_1 = -1$. Aplicando la desigualdad se tiene que:

$$1 - \frac{1}{-1} \le x \le 1 + 1,$$
$$1 + 1 \le x \le 1 + 1,$$
$$2 \le x \le 2$$

Por tanto, el número cromático es 2.

El coloreado se muestra en la figura 6.85, utilizando los dos colores de acuerdo con el número cromático obtenido.

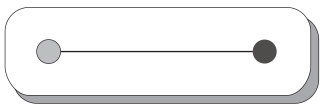


Figura 6.85 Grafo coloreado.

Es importante destacar que un problema es determinar el número cromático de un grafo y otro muy distinto es el de colorear el mismo.

Resumen

En este capítulo se estudian las propiedades y características de los grafos, las cuales, a fin de cuentas, son solo abstracciones matemáticas. Además, también se trata la utilidad de los grafos en la práctica, pues estos ayudan a resolver numerosos problemas importantes de la vida cotidiana.

Además, también se muestran diferentes alternativas para la representación de los mismos, ya sea de manera gráfica, algebraica o formal mediante matrices y su posterior manipulación en una computadora.

Asimismo, se estudia la clasificación de los grafos y se muestran los diversos recorridos en los mismos (caminos, caminos simples, circuitos y circuitos simples), además de casos especiales, como: paseos y circuitos de Euler y Hamilton.

Por último, se tratan aspectos formales de la teoría de grafos, como algunos algoritmos para grafos y el coloreado de grafos.

Problemas propuestos

6.1 Determinar el número de lados que tiene el grafo K_9.

6.2 Determinar qué valencia tiene cada vértice de un grafo K_6.

6.3 Establecer qué valencia tiene cada vértice de un grafo K_n.

6.4 Determinar cómo se denomina un grafo en el que hay datos asociados a sus lados.

6.5 Establecer qué tipo es cada uno de los grafos que se muestran en las figuras siguientes.

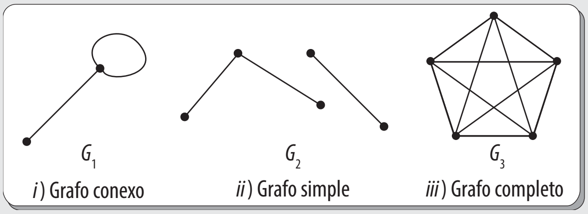


Figura 6.86

Nota:
Un grafo puede ser de más de un tipo.

6.6 Determinar cuál de los siguientes grafos representa un subgrafo generador para K_4.

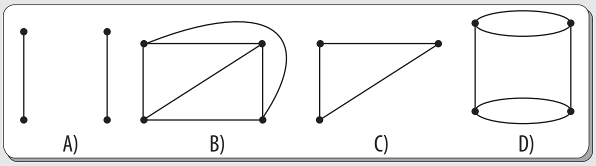


Figura 6.87

6.7 Establecer cuál de los siguientes subgrafos es el complemento del subgrafo con respecto a K_4.

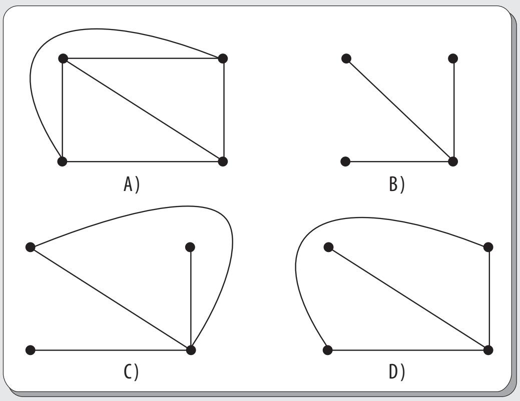


Figura 6.88

6.8 Es un grafo en el que no existen lazos ni lados paralelos.

6.9 Todos los siguientes subgrafos son generadores de K_4, excepto:

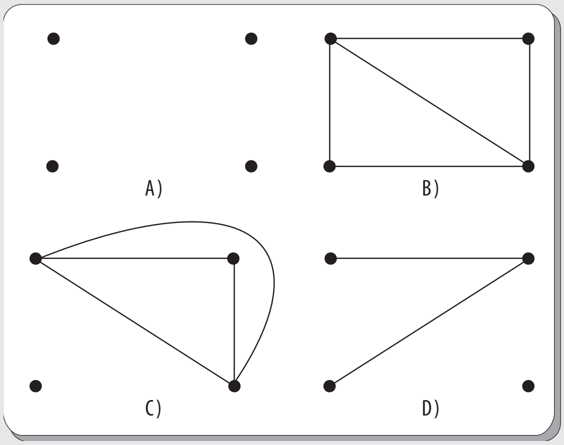


Figura 6.89

6.10 Se dice que un G_1 es un subgrafo generador de G si contiene ______________________.

6.11 El grafo G_2 es con respecto al grafo G_1:

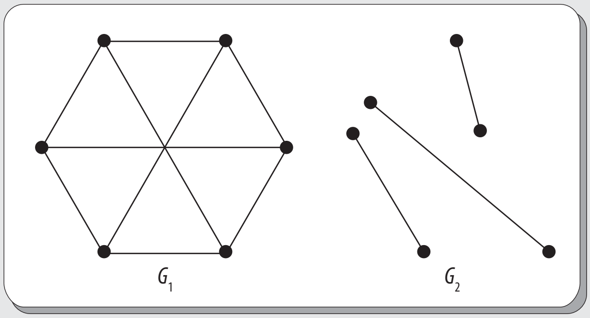


Figura 6.90

a) Isomorfo con G_1
b) Complemento de G_1
c) Subgrafo generador de G_1
d) Homeomorfo con G_1

6.12 ¿Qué tipo es cada uno de los siguientes grafos?

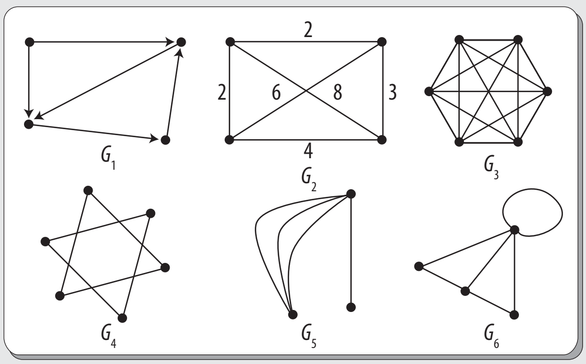


Figura 6.91

Nota:
Un grafo puede ser de más de un tipo.

a) Grafo ponderado d) Dígrafo
b) Grafo no simple e) Grafo disconexo
c) Grafo completo f) Multígrafo

6.13 ¿Cuáles de los siguientes grafos contienen un circuito de Euler?

a) K_4 b) K_9 c) K_6 d) K_3
e) K_{11} f) K_2 g) K_4 h) K_7

Con base en el grafo siguiente, responder lo que se pide en los problemas 6.14 a 6.17.

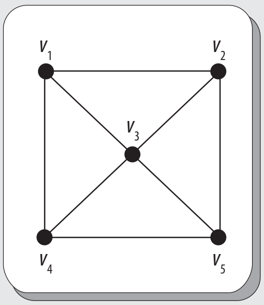


Figura 6.92

6.14 ¿Cuál de las siguientes sucesiones de lados es un camino?

a) $(v_1, v_2, v_3, v_2, v_1, v_4)$ b) $(v_1, v_2, v_3, v_4, v_1, v_2)$
c) $(v_1, v_2, v_3, v_4, v_5, v_3)$ d) $(v_1, v_2, v_1, v_3, v_1, v_4)$

6.15 ¿Cuál de las siguientes sucesiones de lados es un camino simple?

a) $(v_1, v_2, v_3, v_5, v_4, v_1)$ b) $(v_1, v_2, v_3, v_4, v_5, v_3)$
c) $(v_1, v_2, v_3, v_1, v_4)$ d) $(v_1, v_2, v_3, v_5, v_4)$

6.16 ¿Cuál de las siguientes sucesiones de lados es un circuito?

a) $(v_1, v_3, v_4, v_1, v_2, v_1)$ b) $(v_1, v_2, v_3, v_5, v_4, v_3, v_1)$
c) $(v_1, v_2, v_3, v_4, v_3, v_1)$ d) $(v_1, v_2, v_1, v_3, v_1)$

6.17 ¿Cuál de las siguientes sucesiones de lados es un circuito simple?

a) $(v_1, v_2, v_3, v_5, v_4, v_1)$ b) $(v_1, v_2, v_3, v_4, v_3, v_1)$
c) $(v_1, v_3, v_5, v_4, v_3, v_1)$ d) $(v_1, v_2, v_3, v_5, v_4, v_3, v_1)$

Con base en el grafo siguiente, responder lo que se pide en los problemas 6.18 a 6.21.

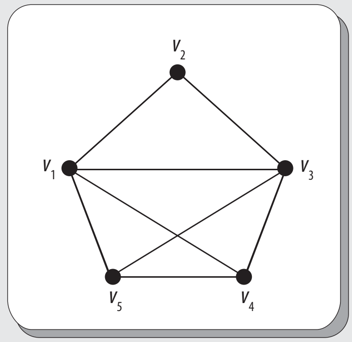


Figura 6.93

6.18 ¿Cuál de las siguientes sucesiones de lados es un camino?

a) $(v_1, v_2, v_3, v_2, v_1, v_5)$ b) $(v_1, v_2, v_3, v_4, v_5, v_3)$
c) $(v_1, v_2, v_3, v_4, v_1, v_2)$ d) $(v_1, v_2, v_1, v_5, v_1, v_2)$

6.19 ¿Cuál de las siguientes sucesiones de lados es un camino simple?

a) $(v_1, v_2, v_3, v_4, v_5)$ b) $(v_1, v_2, v_3, v_4, v_5, v_3)$
c) $(v_1, v_2, v_3, v_1, v_4)$ d) $(v_1, v_2, v_3, v_4, v_5, v_1)$

6.20 ¿Cuál de las siguientes sucesiones de lados es un circuito?

a) $(v_1, v_5, v_3, v_4, v_3, v_1)$ b) $(v_1, v_3, v_4, v_1, v_2, v_1)$
c) $(v_1, v_2, v_3, v_5, v_4, v_1)$ d) $(v_1, v_4, v_5, v_4, v_3, v_1)$

6.21 ¿Cuál de las siguientes sucesiones de lados es un circuito simple?

a) $(v_1, v_2, v_3, v_5, v_4, v_3, v_1)$ b) $(v_1, v_2, v_3, v_4, v_5, v_1)$
c) $(v_1, v_2, v_3, v_4, v_3, v_1)$ d) $(v_1, v_5, v_4, v_1, v_3, v_2, v_1)$

6.22 Determinar cuál de los siguientes grafos tiene en forma simultánea un circuito de Euler y un circuito de Hamilton.

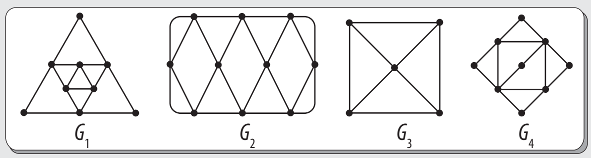


Figura 6.94

6.23 En el siguiente grafo, todas las sucesiones de lados representan un circuito de Hamilton, excepto:

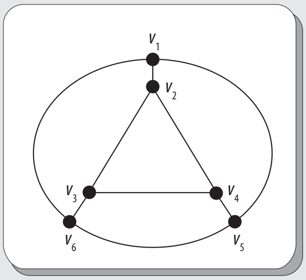


Figura 6.95

a) $(v_2, v_3, v_4, v_5, v_6, v_3, v_2)$ b) $(v_1, v_2, v_3, v_4, v_5, v_6, v_1)$
c) $(v_2, v_3, v_4, v_5, v_6, v_1, v_2)$ d) $(v_3, v_6, v_1, v_5, v_4, v_2, v_3)$

Con base en el grafo siguiente, responder lo que se pide en los problemas 6.24 a 6.27.

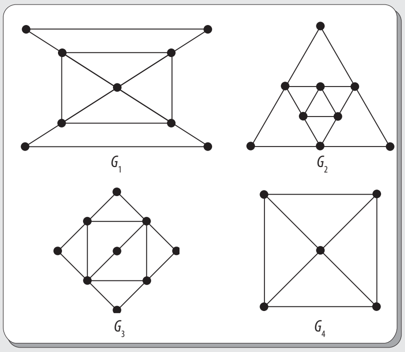


Figura 6.96

6.24 ¿Cuáles grafos tienen en forma simultánea un paseo y un circuito de Euler?

6.25 ¿Cuáles grafos no tienen un circuito de Euler?

6.26 ¿Cuál grafo tiene un paseo pero no un circuito de Euler?

6.27 Todos los grafos tienen un paseo de Euler, excepto ____________________.

6.28 El siguiente grafo tiene un paseo de Euler porque ____________________.

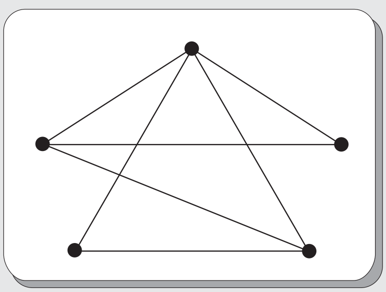


Figura 6.97

a) Un número impar de vértices tiene grado par.
b) Hay dos vértices de grado impar.
c) Hay al menos dos vértices de grado impar.
d) Algunos vértices tienen grado par.

6.29 ¿Cuáles de los siguientes grafos tienen un paseo de Euler, un circuito de Euler o ambos?

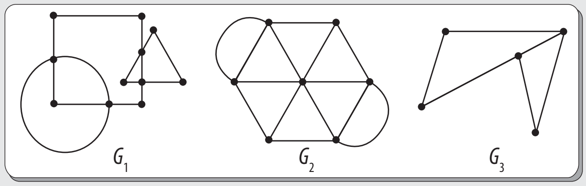


Figura 6.98

6.30 Para cuáles valores de n, el grafo completo K_n no contiene un circuito de Euler.

a) Para todo n par b) Para cualquier $n \geq 5$
c) Para todo n primo d) Para todo n impar

Con base en el grafo siguiente, responder lo que se pide en los problemas 6.31 a 6.34, considerando que cada una de las sucesiones de lados es un:

a) Camino
b) Camino y camino simple
c) Camino y circuito
d) Camino, circuito y circuito simple

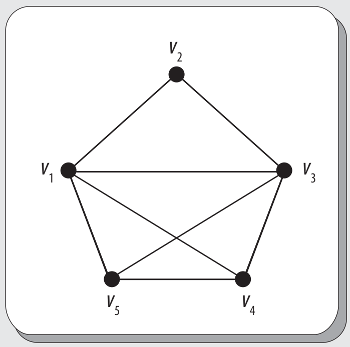


Figura 6.99

6.31 $(v_3, v_5, v_1, v_4, v_5, v_3)$

6.32 $(v_3, v_4, v_5, v_1, v_3)$

6.33 $(v_1, v_2, v_3, v_4, v_5, v_3)$

6.34 $(v_1, v_2, v_3, v_4, v_5)$

6.35 ¿Cuáles de los siguientes grafos tienen un circuito de Euler?

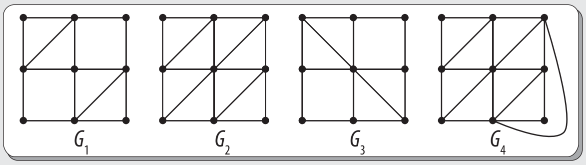


Figura 6.100

6.36 Obtener la matriz de adyacencia que representa el siguiente grafo.

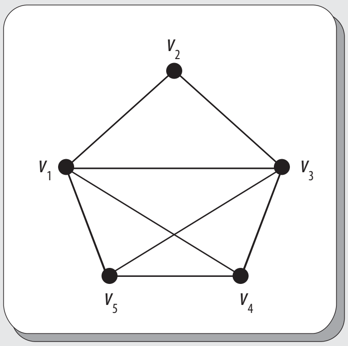


Figura 6.101

6.37 Obtener la matriz de adyacencia que representa el grafo completo K_3.

6.38 La matriz de adyacencia que representa un grafo G con todos sus vértices aislados entre sí es:

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad A_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6.39 ¿Cuál de las siguientes matrices de incidencia representa un grafo simple?

$$I_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad I_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$I_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad I_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

6.40 Obtener la matriz de incidencia que representa el grafo completo K_3.

6.41 La matriz de incidencia que representa un grafo G con exactamente un vértice aislado es:

$$I_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad I_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$I_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad I_4 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

6.42 Todas las siguientes matrices de incidencia representan grafos que contienen un paseo de Euler, excepto:

$$I_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad I_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$I_3 \qquad I_4$

6.43 ¿Cuál de las siguientes matrices de incidencia representa un grafo que contienen un circuito de Euler?

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$I_1 \qquad I_2$

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$I_3 \qquad I_4$

6.44 Las siguientes matrices de incidencia representan un grafo completo K_3, excepto:

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$I_1 \qquad I_2 \qquad I_3 \qquad I_4$

6.45 Determinar el grafo no dirigido que corresponde a la matriz de adyacencia:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Utilizando el acomodo de vértices que se muestra a continuación:

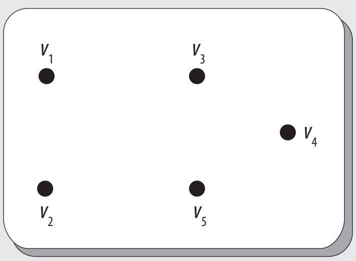


Figura 6.102

6.46 Obtener la matriz de adyacencia que representa el siguiente grafo.

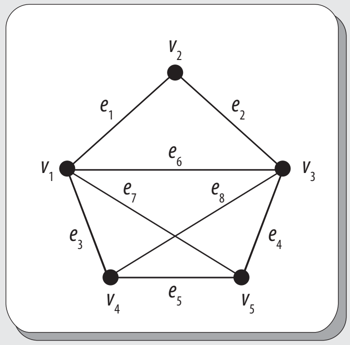
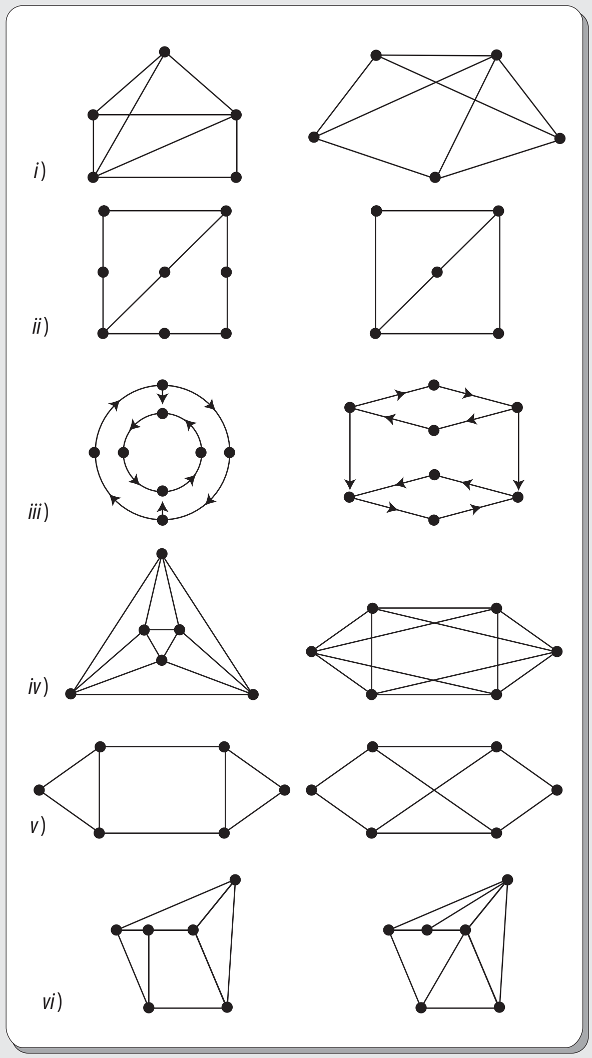


Figura 103

6.47 Comprobar si las siguientes parejas de grafos son homeomorfas.



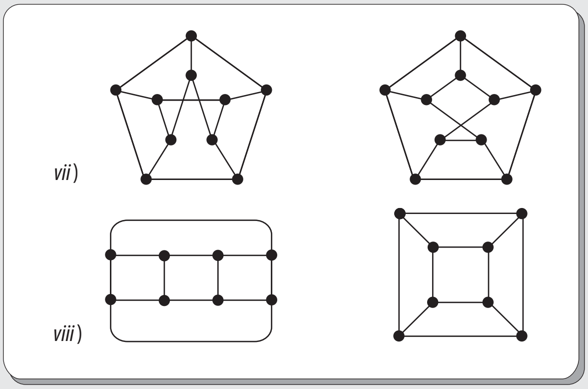


Figura 6.104

6.48 Determinar el número de regiones del siguiente grafo y obtener un grafo isomorfo aplanable a dicho grafo para comprobar el resultado obtenido.

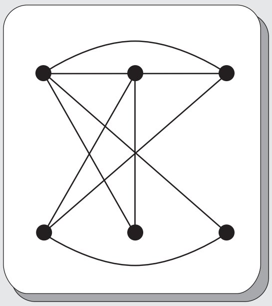


Figura 6.105

Con base en los siguientes grafos, contestar lo que se pide en los problemas 6.49 a 6.53.

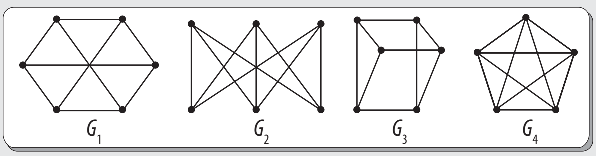


Figura 6.106

6.49 ¿Cuáles grafos no son aplanables?

6.50 ¿Cuáles grafos tienen un circuito de Hamilton?

6.51 ¿Cuáles grafos son aplanables?

6.52 ¿Cuáles grafos tienen un circuito de Euler?

6.53 ¿Cuáles grafos son isomorfos?

6.54 Si $G = (V, E)$ es un grafo aplanable, determinar cuándo un subgrafo G_1 de G será aplanable.

a) Nunca b) A veces
c) No siempre d) Siempre

6.55 Determinar el número de regiones del siguiente grafo y obtener un grafo isomorfo aplanable a dicho grafo para comprobar el resultado obtenido.

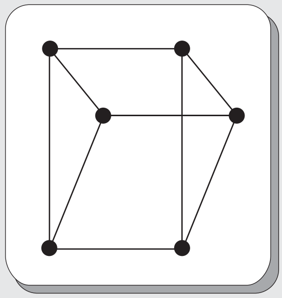


Figura 6.107

6.56 Obtener el número cromático de los siguientes grafos, así como el grafo coloreado respectivo.

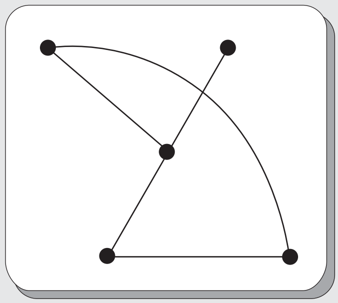


Figura 6.108

6.57

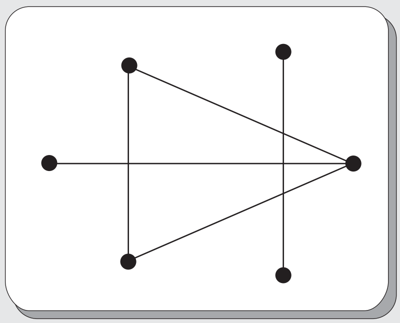


Figura 6.109

6.58

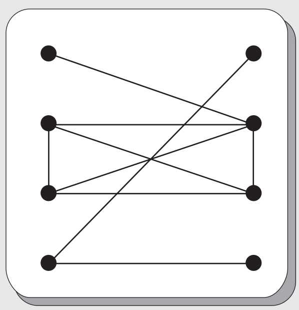


Figura 6.110

6.59

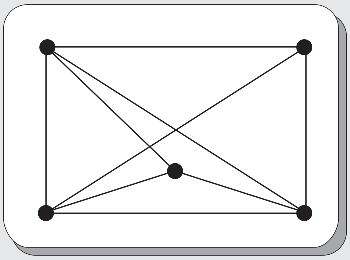


Figura 6.111

6.60

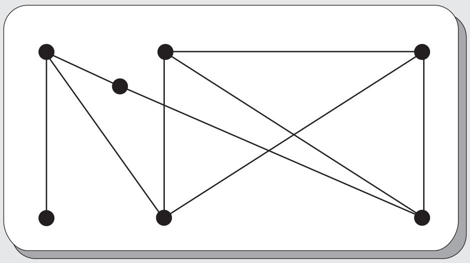


Figura 6.112

6.61

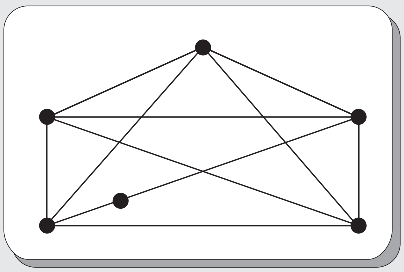


Figura 6.113

6.62

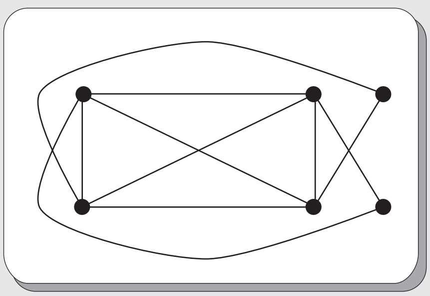


Figura 6.114

6.63

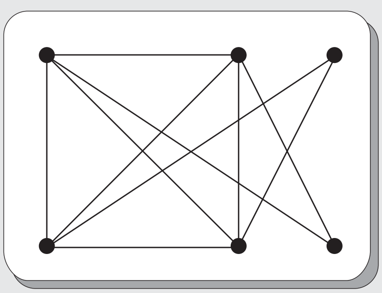


Figura 6.115

6.64

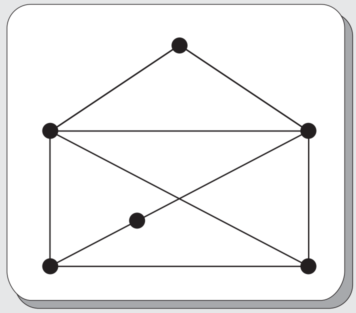


Figura 6.116

Problemas reto

Con base en el siguiente grafo, contestar los siguientes 10 problemas

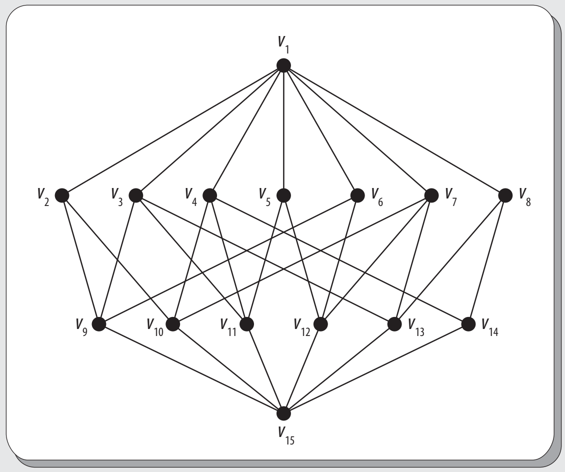


Figura 6.117

1. Determinar si el grafo es conexo.
2. Determinar si el grafo es simple.
3. Determinar el número cromático y dibujar el grafo coloreado.
4. Obtener la matriz de adyacencia.
5. Determinar si existe un circuito de Euler.
6. Determinar si existe un paseo de Euler.
7. Determinar si existe un paseo de Hamilton; en caso afirmativo, representarlo en forma gráfica.
8. Determinar si existe un circuito de Hamilton.
9. Determinar qué sucede al eliminar el lado (v_1, v_5), ¿habrá paseos y circuitos de Euler?
10. Utilizar el algoritmo de Fleury y comprobar si existe o no un circuito de Euler.

7

Árboles

Objetivos

- Distinguir los distintos tipos de árboles.
- Conocer los conceptos básicos de los árboles.
- Evaluar expresiones algebraicas mediante el uso de árboles binarios.
- Construir árboles de búsqueda binaria.

7.1 Introducción

Hay un tipo especial de grafos que se presentan en múltiples aplicaciones que reciben el nombre de árboles, los cuales son útiles en especial en ciencias de la computación. Pues, por ejemplo, casi todos los sistemas operativos almacenan sus archivos en una estructura de árbol. A continuación, se listan algunas otras aplicaciones de árboles en informática: 1. organización de información, con el fin de que sea posible efectuar con eficacia operaciones que conciernan a esa información; 2. construcción de algoritmos eficientes para localizar artículos en una lista; 3. construcción de códigos eficientes para almacenar y transmitir datos; 4. modelación de procedimientos que son llevados a cabo al utilizar una secuencia de decisiones.

Toda vez que los árboles solo son un caso especial de grafos que se utilizan de manera particular en computación, es precisamente un especialista en cómputo a quien se considera el principal representante de esta clase de grafos: Robert W. Floyd. A continuación, se presenta una pequeña biografía de este importante científico estadounidense.

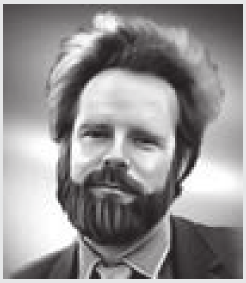


Figura 7.1 Robert W. (Bob) Floyd (1936-2001), científico estadounidense en computación.

Robert W. (Bob) Floyd nació el 8 de junio de 1936, en Nueva York, y murió el 25 de septiembre de 2001, en Stanford, California; fue un eminente científico en computación. Sus contribuciones incluyen el diseño del algoritmo de Floyd-Warshall (independientemente de Stephen Warshall), que se encuentra de manera eficiente en todos los caminos más cortos en un gráfico, el ciclo del hallazgo de Floyd, algoritmo para la detección de los ciclos en una secuencia, y su trabajo en el análisis. En un artículo independiente, Floyd introdujo el concepto importante de difusión de error, también llamado tramado Floyd-Steinberg (aunque también distingue el tramado de difusión). Fue pionero en el campo de la verificación de programas con afirmaciones lógicas; esto es, *asignar significados a los programas*. Esta fue una importante contribución a lo que más tarde se convirtió en la lógica de Hoare. En 1978, Floyd recibió el Premio Turing "por tener una clara influencia sobre las metodologías para la creación de software eficiente y fiable, y por ayudar a encontrar los siguientes subcampos importantes de la ciencia de la computación: la teoría del análisis, las semánticas de los lenguajes de programación, el manual del programa, la verificación automática, la síntesis de programas y el análisis de algoritmos".

7.2 Árboles

En esta sección se abordan los conceptos generales de los árboles, como definición, componentes, características distintivas, entre otros aspectos. Por supuesto, en secciones posteriores, el texto se centra en los árboles que tienen mayor aplicación en el campo de la computación: los **árboles binarios**.

Con base en los conceptos vistos en el capítulo 6, es fácil definir el concepto central del presente capítulo. Entonces, se puede definir que un **árbol** es cualquier grafo no dirigido, conexo y que no contiene circuitos. A continuación se presentan algunos ejemplos.

EJEMPLO

Considérense los grafos *i*) y *ii*) de la figura 7.2. Ambos son grafos no dirigidos (es decir, sus lados no contienen dirección alguna), son conexos (esto es, entre cada par de vértices existe un camino que los conecta).

Además, ninguno de los dos tiene circuitos (es decir, no existe forma de dar un paseo partiendo de un vértice y regresar a este sin pasar dos veces por el mismo lado); por tanto, se dice que son árboles.

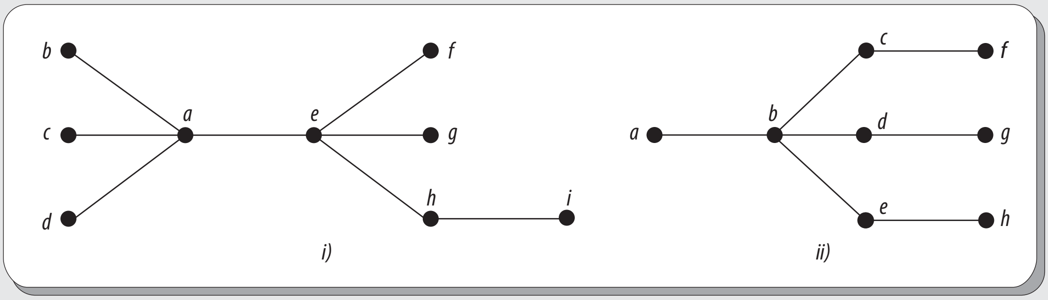


Figura 7.2 Grafos que son árboles.

EJEMPLO

Tómense en cuenta los grafos *i*) y *ii*) de la figura 7.3.

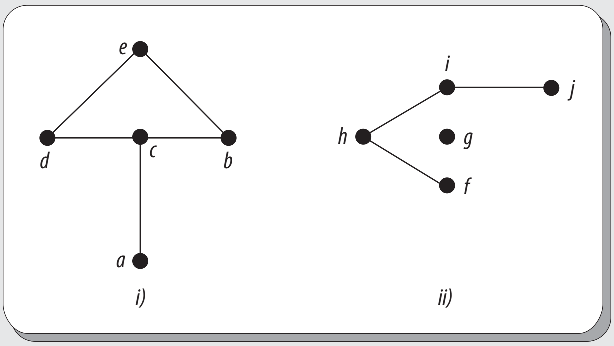


Figura 7.3 Grafos que no son árboles.

En este caso, ninguno de estos grafos es árbol. El grafo 7.3 *i)* no puede considerarse árbol porque contiene circuitos; por ejemplo, la sucesión de lados (*b, e, c, b*) es un circuito; el grafo 7.3 *ii)* tampoco es **árbol**, ya que es disconexo, pues contiene un vértice aislado (vértice *g*).

Con frecuencia, es necesario considerar una colección de árboles disjuntos, a dicha colección se le denomina **bosque**.

EJEMPLO

Considérense los grafos *i*) y *ii*) de la figura 7.2; como se vio antes, estos son árboles y como ambos son disjuntos, entonces forman un bosque.

En los árboles se utilizan nombres especiales para identificar sus vértices; a saber, un vértice de valencia 1 en un árbol se le llama nodo hoja (o simplemente hoja) o nodo terminal y un vértice de valencia mayor que 1 recibe el nombre de nodo rama (o simplemente rama) o nodo interno.

EJEMPLO

Considérese el grafo *i*) de la figura 7.2; entonces, se tiene que los vértices *b*, *c*, *d*, *f*, *g*, *i* son nodos hoja, mientras que los vértices *a*, *e*, *h*, son nodos rama.

A continuación, se detallan algunas de las propiedades que distinguen a los árboles.

- Existe un único paseo entre dos vértices cualesquiera.
- El número de vértices es mayor que el número de lados.
- Un árbol con dos o más vértices tiene al menos una hoja.

Además de su definición, es posible identificar si un grafo dado es un árbol a partir de las siguientes características:

- Un grafo $G = (V, E)$ en el cual existe un único paseo entre cada par de vértices es un árbol.
- Un grafo conexo $G = (V, E)$ con $|E| = |V| - 1$ es un árbol, donde $|E|$ y $|V|$ son el tamaño y orden del grafo, respectivamente.
- Un grafo $G = (V, E)$ con $|E| = |V| - 1$ que no tiene circuitos es un árbol.

Estas propiedades y los resultados pueden verificarse con mucha facilidad a partir de la definición de árbol.

7.3 Árboles enraizados

Al contrario de los árboles que existen en la naturaleza, cuyas raíces se localizan en la parte inferior del mismo, arraigadas en la tierra, en la teoría de árboles, los árboles enraizados pueden verse con la raíz en la parte superior, como se trata en esta sección.

Árbol dirigido

Un grafo dirigido es un **árbol dirigido**, si se convierte en un árbol cuando se ignoran las direcciones de sus lados.

EJEMPLO

El grafo dirigido de la figura 7.4*i*) constituye un árbol dirigido, pues al omitir la dirección de los lados cumple con las características de un árbol, como se observa en la figura 7.4*ii*).

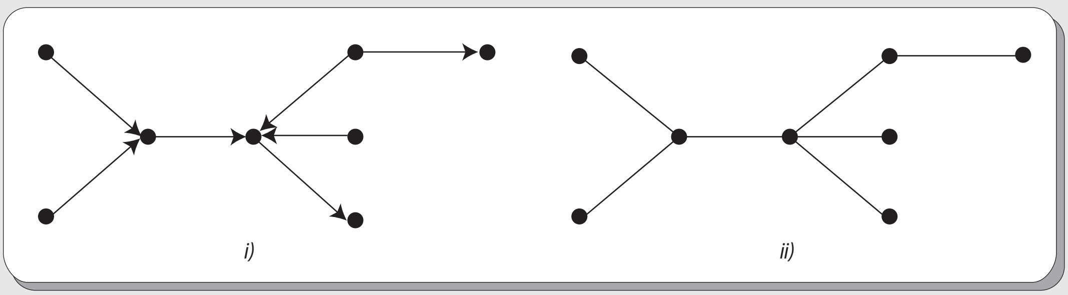


Figura 7.4 Grafo dirigido que es un árbol dirigido.

Árbol enraizado

Un árbol dirigido es un **árbol enraizado** si existe exactamente un vértice cuya valencia de entrada sea 0 y las valencias de entrada de los otros vértices sean 1.

El vértice con valencia de entrada 0 se llama raíz del árbol enraizado.

EJEMPLO

El grafo de la figura 7.5 es un árbol enraizado.

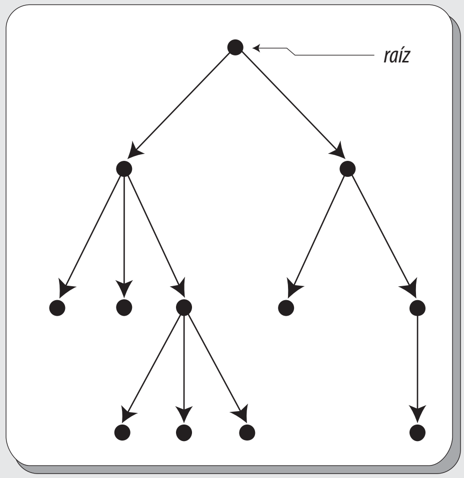


Figura 7.5 Árbol enraizado.

En un árbol enraizado, un vértice cuya valencia de salida es cero se denomina hoja o nodo terminal; en tanto, un vértice cuya valencia de salida es diferente de cero se denomina rama o nodo rama o nodo interno.

EJEMPLO

Considérese el árbol dirigido de la figura 7.6.

Entonces, se tiene que los vértices *a, b, c, f, h* son nodos rama, en tanto que los vértices *d, e, g, i, j, k, l* son nodos hoja.

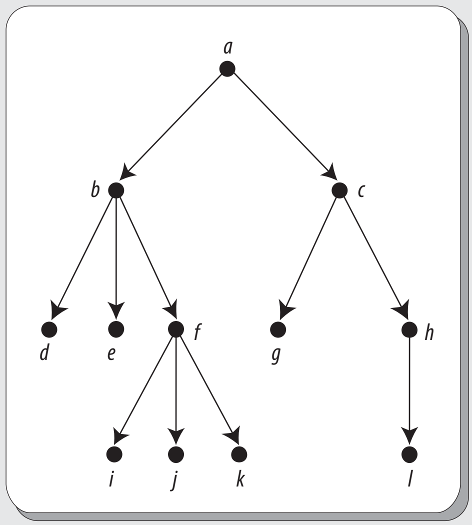


Figura 7.6 Árbol enraizado con raíz en *a*.

Relaciones entre los vértices de un árbol enraizado

También existen las relaciones entre los vértices de un árbol enraizado, las cuales se identifican con nombres especiales. Veamos cuáles son.

Sea a un nodo rama en un árbol enraizado T. Se dice que un vértice b es un **hijo** de a si existe un lado dirigido del vértice a al vértice b. Además, se dice que el vértice a es el **padre** del vértice b. Por su parte, dos vértices son **hermanos** si son hijos del mismo vértice. En tanto, se dice que un vértice *c* es un descendiente del vértice *a* si existe un paseo dirigido del vértice *a* al vértice *c*. Además, se dice que el vértice *a* es un ancestro del vértice *c*.

EJEMPLO

Considérese el árbol dirigido de la figura 7.6.

Entonces, se tienen las siguientes relaciones entre sus vértices:

b y c son hijos de *a*
d, *e* y *f* son hijos de *b*
g y *h* son hijos de *c*
i, *j* y *k* son hijos de *f*
l es hijo de *h*

a es padre de *b* y *c*
b es padre de *d*, *e* y *f*
c es padre de *g* y *h*
f es padre de *i*, *j* y *k*
h es padre de *l*

b y *c* son hermanos
d, *e* y *f* son hermanos
g y *h* son hermanos
i, *j* y *k* son hermanos
l no tiene hermanos

Además, se tiene que:

b, *c*, *d*, *e*, *f*, *g*, *h*, *i*, *j*, *k* y *l* son descendientes de *a*
d, *e*, *f*, *i*, *j* y *k son* descendientes de *b*
i, *j* y *k* son descendientes de *f*
g, *h* y *l* son descendientes de *c*
l es descendiente de *h*

a es ancestro de *b*, *c*, *d*, *e*, *f*, *g*, *h*, *i*, *j*, *k*, *l*
b es ancestro de *d*, *e*, *f*, *i* y *j*
f es ancestro de *i*, *j* y *k*
c es ancestro de *g*, *h* y *l*
h es ancestro de *l*

Subárbol

Sea a un nodo rama en un árbol enraizado $T = (V, E)$. Por el **subárbol** con raíz a se entiende el subgrafo $T' = (V', E')$ de T, tal que V' contiene a a y a todos sus descendientes y E' contiene los lados de todos los paseos dirigidos que surjan de a. Por un subárbol de a, se entiende un subárbol que tiene a a como raíz.

EJEMPLO

Considérese el árbol dirigido *i)* de la figura 7.7. Los árboles de *ii), iii), iv)* y *v)* son todos subárboles de *i)*.

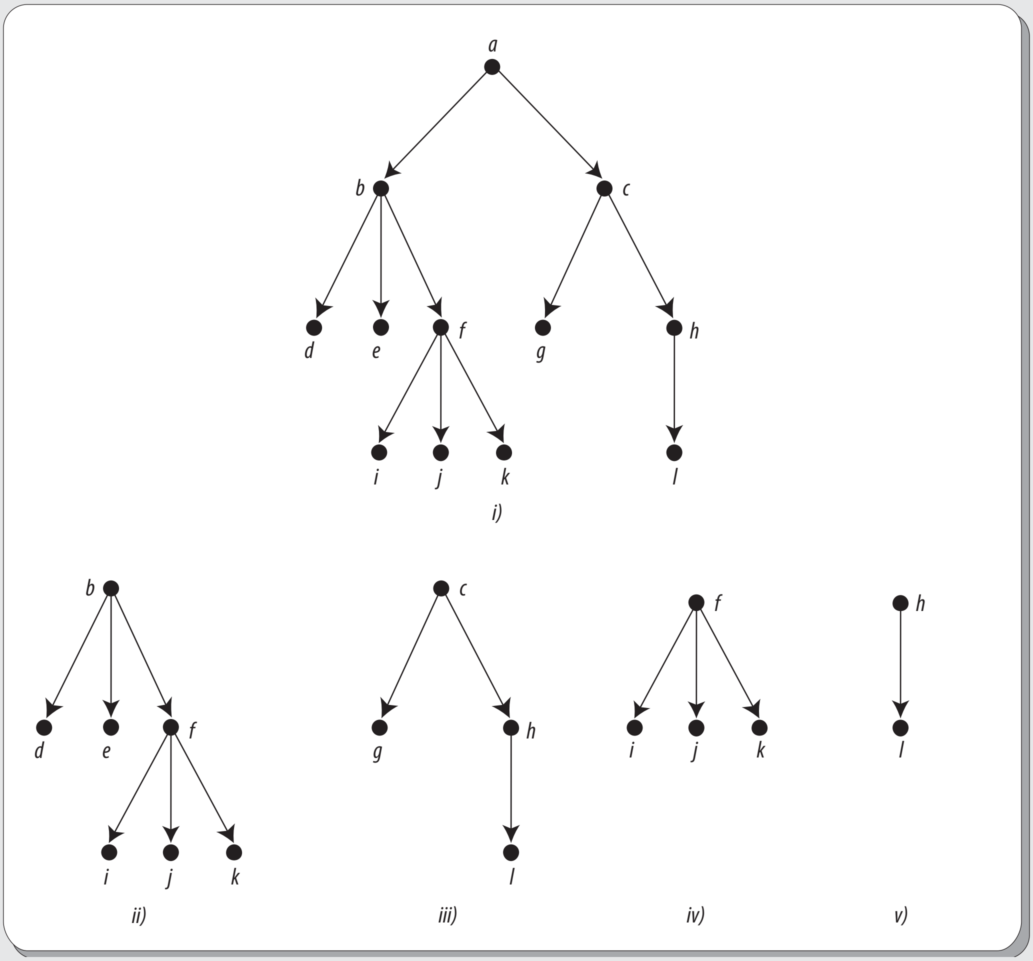


Figura 7.7 *ii*), *iii*), *iv*) y *v*) subárboles del árbol *i*).

Del ejemplo anterior, es fácil ver que los árboles ii), *iii*), *iv*) y *v*) de la figura 7.7 son subárboles de *i*) con raíces a, b, f, c y h, respectivamente.

Es importante aclarar que para un árbol dado existen tantos subárboles como nodos rama tenga el árbol.

Nota

Cuando se traza un árbol enraizado, es posible omitir las direcciones de los lados siguiendo la convención de colocar los hijos de un nodo rama debajo de este, ya que con dicho acuerdo se entiende que las direcciones de todos los lados son hacia abajo.

EJEMPLO

Si se considera el árbol enraizado de la figura 7.7 y se toma en cuenta el acuerdo de la nota anterior, el resultado es el árbol que se muestra en la figura 7.8.

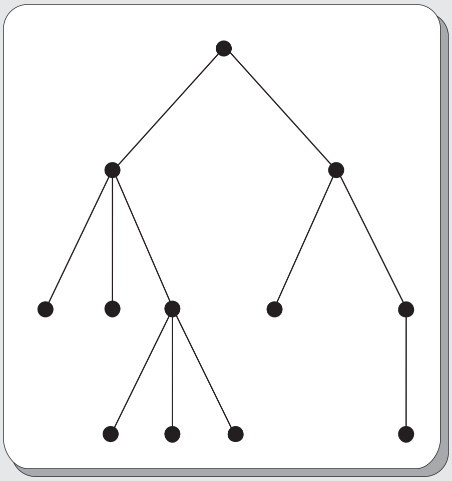


Figura 7.8 Árbol enraizado de la figura 7.7 omitiendo la dirección de sus lados.

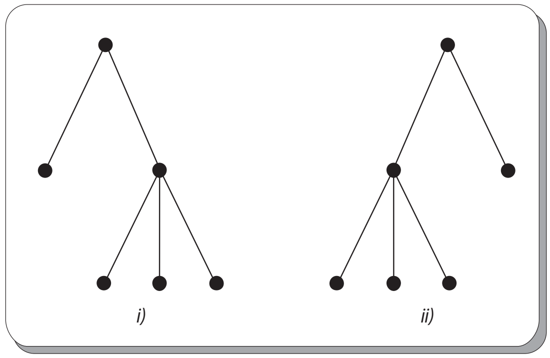


Figura 7.9 Árboles isomorfos (solo si se consideran como grafos).

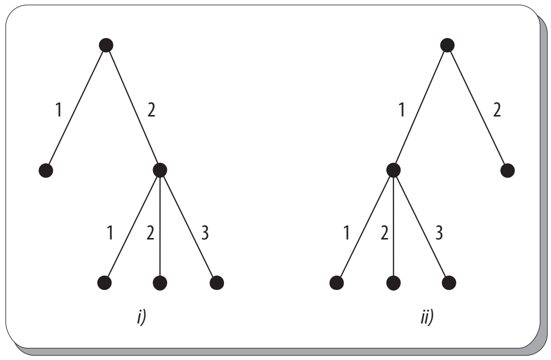


Figura 7.10 Árboles ordenados.

A pesar de que los árboles enraizados i) y *ii*) de la figura 7.9 son isomorfos (si se consideran como grafos), en ciertas aplicaciones estos pueden representar dos situaciones por completo diferentes.

Esto motiva a la definición de un árbol ordenado, lo cual permitirá referirse sin ambigüedades a cada uno de los subárboles de un nodo rama.

Árbol ordenado

Un **árbol ordenado** es un árbol enraizado con lados etiquetados con los enteros 1, 2, … , *i*… . Por tanto, los **subárboles** de un nodo rama pueden ser referidos como el primero, el segundo, ... , y el *i*-ésimo subárbol del nodo rama, los cuales corresponden a los lados incidentes desde el nodo, y que pueden ser enteros no consecutivos.

Ahora, supóngase que los árboles de la figura 7.9 se etiquetan como se observa en la figura 7.10.

Árboles isomorfos

Se dice que dos árboles ordenados son **isomorfos** si existe un isomorfismo de grafos entre estos, de tal suerte que las etiquetas de los lados correspondientes coincidan.

EJEMPLO

Los árboles ordenados *i*) y *ii*) de la figura 7.10 no son isomorfos; en cambio, los de la figura 7.11 sí lo son.

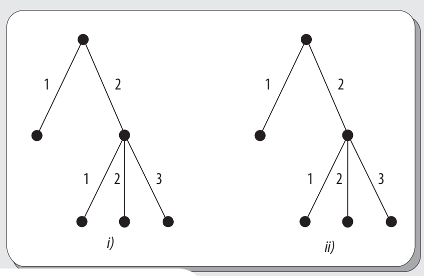


Figura 7.11 Árboles isomorfos.

Árbol *m*-ario

Un árbol ordenado en el que cada nodo rama tiene a lo más m hijos se conoce con el nombre de **árbol** m**−ario**. Se dice que un árbol m-ario es regular si cada uno de sus nodos ramas tiene exactamente m hijos.

Una clase importante de árboles m-arios son los llamados árboles binarios. En los **árboles binarios**, en lugar de referirse al primero o al segundo subárbol de un nodo rama, a menudo se hace referencia a estos como subárbol izquierdo o subárbol derecho del nodo.

EJEMPLO

Considérense los árboles T_1 y T_2 de la figura 7.12. En este caso, el árbol T_1 es ternario, ya que cada nodo rama tiene a lo más tres hijos, pero además es ternario regular, pues cada nodo rama tiene exactamente tres hijos. En cambio, el árbol T_2 es únicamente ternario.

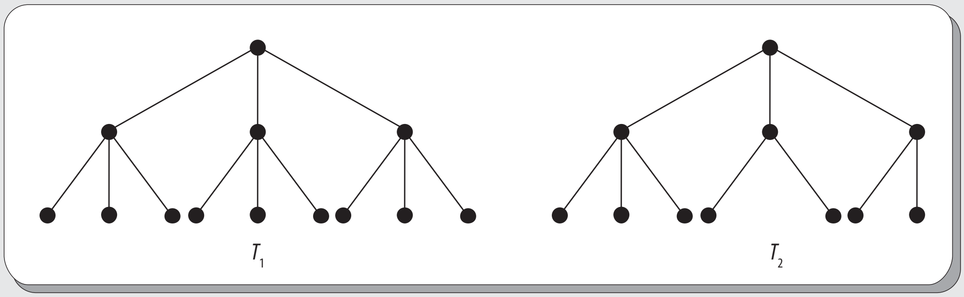


Figura 7.12 T_1 es un árbol ternario regular y T_2 es un árbol ternario.

7.4 Longitud de paseo en árboles enraizados

Cuando se representa un problema mediante un árbol, en muchas ocasiones es necesario determinar la cantidad de lados que existen desde la raíz de árbol enraizado hasta determinado vértice.

La **longitud** de un paseo para un vértice en un árbol enraizado es el número de lados en el paseo desde la raíz hasta el vértice.

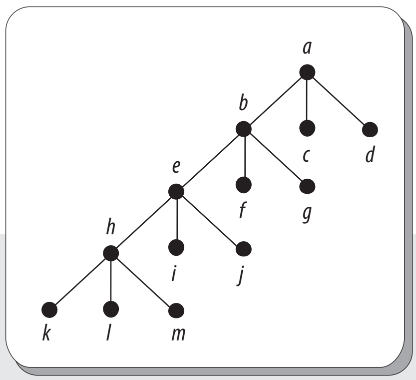


Figura 7.13 Árbol enraizado T.

EJEMPLO

Considérese el árbol enraizado T, que se observa en la figura 7.13. En este, como la raíz de T es a, entonces la longitud de paseo del vértice k es 4, mientras que la del vértice j es 3; por su parte, la longitud de paseo para el vértice a (que es la raíz) es cero, pues no hay aristas que recorrer.

Altura de un árbol

La altura h de un árbol T es el máximo de las longitudes de los paseos en un árbol, y se denota como: $h(T)$.

EJEMPLO

La altura del árbol enraizado T de la figura 7.13 es 4; de acuerdo con la definición anterior, entonces también puede escribirse como: $h(T) = 4$, y es el máximo de las longitudes de todos los paseos posibles en T.

7.5 Código de prefijos (prefijos codificados)

A continuación se analiza cómo codificar las diferentes longitudes de paseos en las hojas de los árboles binarios regulares; de este modo, entonces cada nodo hoja del árbol debe tener exactamente dos hijos.

Código de prefijos

Se dice que un conjunto de sucesiones es un **código de prefijos**, si no existe una sucesión del conjunto que sea un prefijo de otra sucesión del conjunto. Por ejemplo, el conjunto **{000, 001, 01, 10, 11}** es un código de prefijos, ya que ninguna sucesión es un prefijo de otra sucesión en el mismo conjunto. En tanto, el conjunto **{1, 00, 01, 000, 0001}** no es un código de prefijos, ya que, en este caso, la sucesión **00** es un prefijo de la sucesión **000**.

Cabe mencionar que es posible obtener un código de prefijos a partir de un árbol binario, mediante el etiquetado de sus lados de una manera adecuada, con ceros y unos: los lados que corresponden al subárbol izquierdo se etiquetan con 0 y los que corresponden al subárbol derecho con 1.

EJEMPLO

Considérese el árbol binario de la figura 7.14 *i*). En este, es fácil ver que el conjunto de sucesiones asignadas a sus hojas es un código de prefijos, como se observa en la figura 7.13*ii*). El código de prefijos obtenido es: {000, 001, 01, 10, 11}

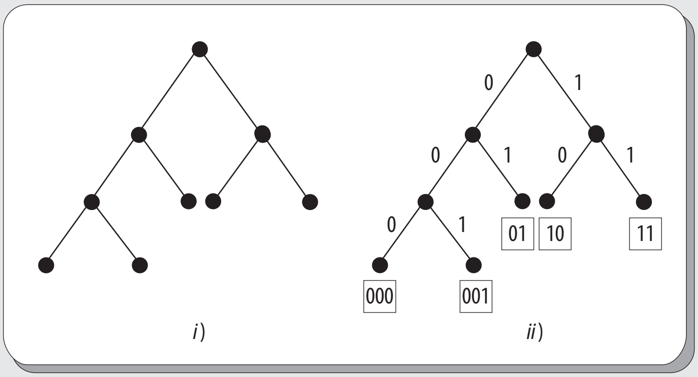


Figura 7.14 Árbol binario y código de prefijos obtenido en dicho árbol.

Respecto al ejemplo anterior, es fácil ver en este que la correspondencia entre un árbol binario y un código de prefijos es biunívoca; por tanto, dado un código de prefijos, también es posible reconstruir el árbol binario correspondiente.

EJEMPLO

Considérese el código de prefijos {001, 000, 01, 1} con el que se obtiene el árbol binario de altura 3, que se observa en la figura 7.15.

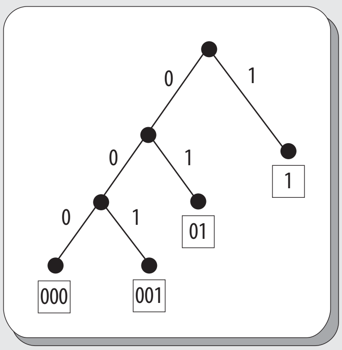


Figura 7.15 Árbol binario obtenido a partir de un código de prefijos.

EJEMPLO

Ejemplo práctico

Al almacenar o transmitir grandes cantidades de texto, con frecuencia conviene buscar la forma de comprimirlo en el menor número posible de bits. Pues, el tiempo necesario para transmitir cierto mensaje es proporcional a su número de bits; por tanto, al comprimir los datos a enviar, puede reducirse el tiempo de transmisión. Además, los datos comprimidos necesitan menos bits para su almacenamiento o transmisión.

Una manera común de hacerlo es mediante la eliminación de la restricción de que todos los códigos de caracteres deben tener la misma longitud. Si en un idioma, los códigos de letras comunes como *e* y *t* fueran más cortos que los códigos de los menos comunes como *x* y *z*, disminuiría el número de bits totales necesarios para almacenar o transmitir el texto. Dicho esquema de codificación se conoce con el nombre de **código dependiente de frecuencia** o **código Huffman**, y se basa precisamente en códigos de prefijos. Al utilizar este método de codificación para cualquier aplicación particular, primero han de conocerse las frecuencias de aparición *a priori* a cada carácter.

El primer paso para construir el código Huffman es escribir la probabilidad de cada carácter debajo de este. El orden en que se acomodan los caracteres no importa y pueden combinarse durante la construcción, para mayor legibilidad. Después, se buscan las dos probabilidades más pequeñas y se añade una nueva probabilidad igual a la suma de aquellas. Las dos probabilidades se marcan para no ser utilizadas de nuevo y se trazan dos lados que unan a la nueva probabilidad con las que le dieron origen. Este proceso se repite una y otra vez, hasta que solo quede una probabilidad sin marcar, que será igual a 1.00.

A continuación se construye el código Huffman para una supuesta transmisión de datos que solo consta de dígitos 0, … , 9, basándose en las frecuencias de aparición de cada dígito mostradas en la tabla 7.1.

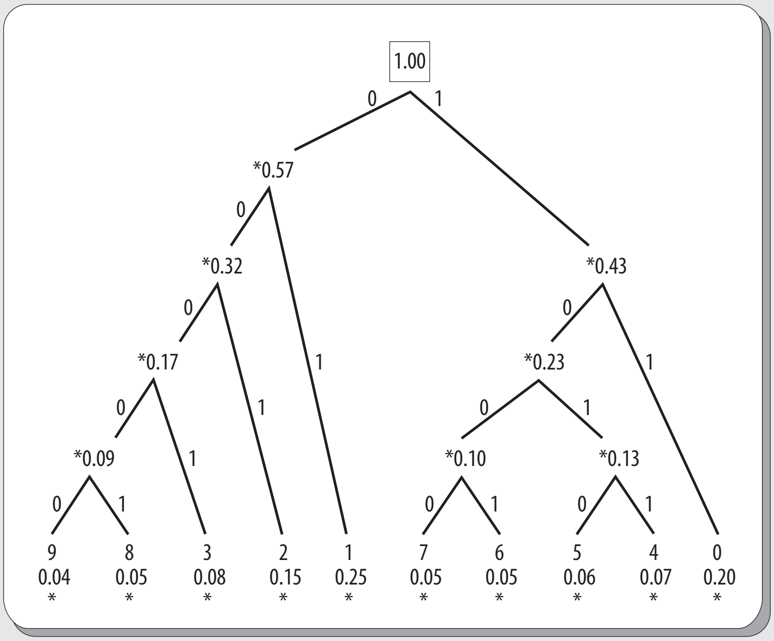


Figura 7.16 Árbol binario para obtener código Huffman.

Tabla 7.2										
Dígito	0	1	2	3	4	5	6	7	8	9
Frecuencia	0.20	0.25	0.15	0.08	0.07	0.06	0.05	0.05	0.05	0.04

El árbol resultante es el que se muestra en la figura 7.16.

Así, el código Huffman resultante para cada dígito es mostrado en la tabla 7.2.

Tabla 7.2 Código Huffman resultante										
Dígito	0	1	2	3	4	5	6	7	8	9
Código	11	01	001	0001	1011	1010	1001	1000	00001	00000

7.6 Árboles de búsqueda binaria

Supóngase que se dispone de una cantidad determinada de objetos sobre los cuales existe un ordenamiento lineal <. Para fines prácticos, el ordenamiento puede ser numérico, alfabético, alfanumérico, etcétera.

Por ejemplo, sean $K_1, K_2, \ldots, K_n$ los n objetos de una lista ordenada, los cuales son conocidos como las claves; considérese que el orden lineal es de la forma $K_1 < K_2 < \ldots < K_n$. Entonces, dado un objeto x el problema consiste en buscar las claves y determinar si x es igual a alguna de estas.

Un procedimiento de búsqueda consiste en una serie de comparaciones entre x y las claves, donde cada comparación de x con una clave indica si x es igual, menor que o mayor que dicha clave.

Un **árbol de búsqueda binaria** para las claves $K_1, K_2, \ldots, K_n$ es un árbol binario, en el cual los nodos están etiquetados con los elementos de una lista ordenada, esto es:

$$K_1 < K_2 < \ldots < K_n$$

En dicho árbol, todos los elementos de cualquier subárbol izquierdo con raíz x son menores que x y todos los elementos de su subárbol derecho con raíz x son mayores de x. En este caso, las claves pueden ser numéricas, alfabéticas o alfanuméricas.

EJEMPLO

Sean las claves {6, 8, 10, 12, 14, 15, 18} y sean los árboles T_1 y T_2 de la figura 7.17. En este caso, el árbol T_1 es un árbol de búsqueda binaria para dichas claves, mientras que el árbol binario T_2 no es de búsqueda binaria, ya que si se considera el elemento 10, todos los elementos del subárbol izquierdo son menores; sin embargo, no todos los elementos del subárbol derecho son mayores, ya que en este, el elemento 6 es menor que 10 y debería ir en el subárbol izquierdo.

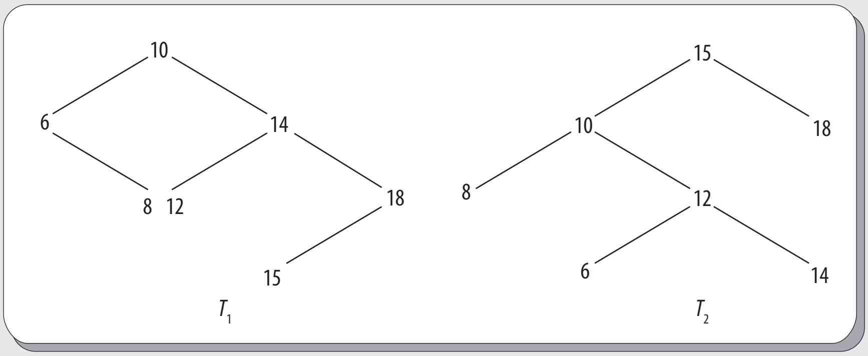


Figura 7.17 El árbol T_1 es un árbol de búsqueda binaria y T_2 es solo un árbol binario.

Operaciones en árboles de búsqueda binaria

Las operaciones que se pueden realizar en árboles de búsqueda binaria son:

- Búsqueda de un nodo
- Inserción y eliminación de un nodo
- Recorrido

Es importante dejar en claro que en esta sección solo se aborda la búsqueda, inserción y eliminación de nodos, ya que para el recorrido se dedica una sección completa más adelante (véase sección 7.9).

Búsqueda de un nodo

Como lo dice su nombre, un árbol de búsqueda corresponde a un procedimiento de búsqueda; en este, se comienza con la raíz del árbol de búsqueda binaria y luego se compara un objeto dado x con la etiqueta de la raíz K_i. Si x es igual a K_i, se dice que la búsqueda ha terminado, pero si x es menor que K_i, entonces x se compara con el hijo izquierdo, y si x es mayor que K_i se compara con el hijo derecho de la raíz.

Esta comparación se continúa para los nodos rama sucesivamente, hasta que x concuerde con una clave o se alcance una hoja; es este caso, x no se encuentra en el árbol de búsqueda.

Además, se puede realizar la búsqueda para claves con valores numéricos, alfabéticos, alfanuméricos, entre otros.

EJEMPLO

Sean {*AB*, *CF*, *EG*, *PP*} las claves K_1, K_2, K_3, K_4 en un árbol de búsqueda binaria, como se muestra en la figura 7.18. Dado el objeto $x = BB$, los pasos de búsqueda son:

1. Comparar *BB* con *EG*.
2. Como *BB* es menor que *EG*, se compara *BB* con *AB*.
3. Como *BB* es mayor que *AB*, se compara *BB* con *CF*, que es una hoja.

Así, se concluye que el objeto *BB* no se encuentra en el árbol de búsqueda binaria.

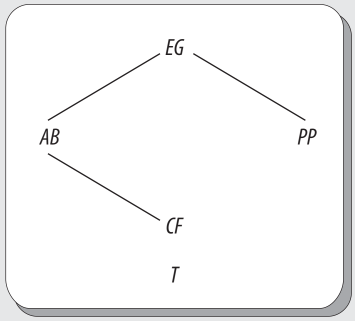


Figura 7.18 Proceso de búsqueda en un árbol de búsqueda binaria *T*.

Inserción de un nodo

Los algoritmos para insertar nodos utilizan la ubicación de un elemento, de tal forma que si se encuentra el elemento buscado, no es necesario hacer nada; en otro caso, se realiza la inserción del nuevo elemento exactamente en el lugar donde finalizó la búsqueda.

EJEMPLO

Considérese el caso de agregar el nodo 6 al árbol de la figura 7.19. En este caso, el recorrido debe comenzar en el nodo raíz 24; por tanto, la inserción debe estar en el subárbol izquierdo de 24 ($6 < 24$). Por su parte, en el nodo 8, la posición de 6 debe ubicarse en el subárbol izquierdo de 8, que es vacío. Por último, el nodo 6 se inserta como hijo izquierdo de 8 y se obtiene el árbol que se observa en la figura 7.20.

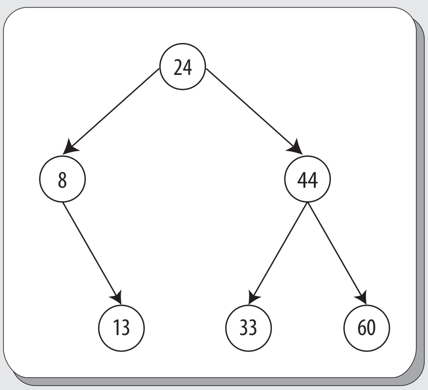


Figura 7.19 Árbol binario antes de insertar el nodo 6.

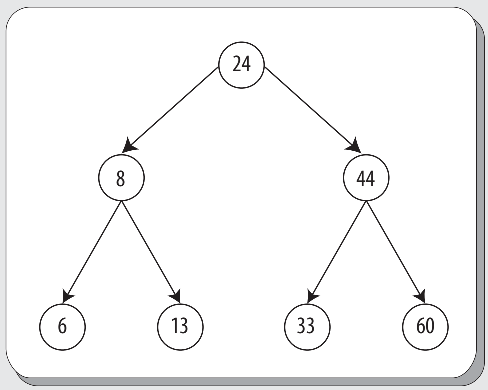


Figura 7.20 Árbol binario después de insertar el nodo 6.

Eliminación de un nodo

De manera equivalente a la inserción de nodos, la eliminación de nodos debe preservar la propiedad que establece que el árbol resultante sea, nuevamente, un árbol de búsqueda. Los pasos que deben seguirse para lograr la eliminación son:

1. Lo primero es buscar en el árbol hasta encontrar la posición del nodo que se ha de eliminar.
2. Si el nodo a eliminar tiene menos de dos hijos, es necesario reajustar los lados de sus antecesores.

Ejemplo

Considérese el árbol de la figura 7.21. Eliminar el elemento 33 de este árbol.

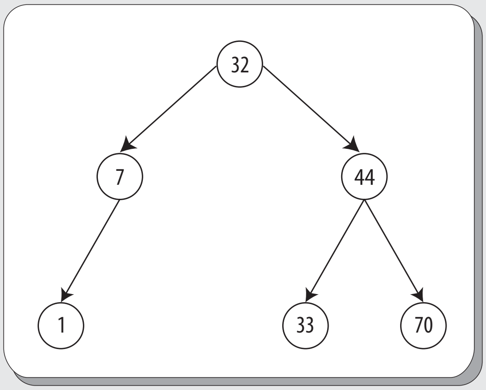


Figura 7.21 Árbol binario antes de eliminar el nodo 33.

Solución

Dado que el subárbol donde se encuentra el nodo 33 es una hoja, en este caso solo es necesario reajustar los lados del nodo precedente en el camino de búsqueda. Entonces, el árbol que se obtiene después de realizar los ajustes mencionados es el que se muestra en la figura 7.22.

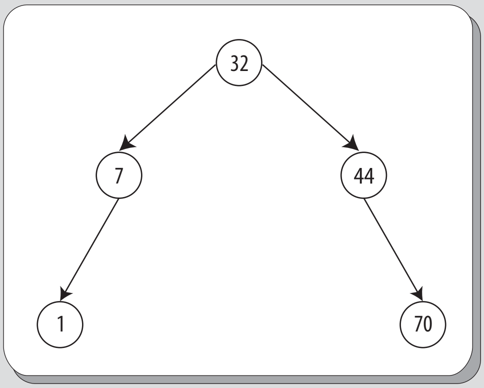


Figura 7.22 Árbol binario después de eliminar el nodo 33.

7.7 Árboles generadores y conjuntos de corte

La situación que se describe a continuación constituye un ejemplo de un problema práctico donde surge la necesidad del concepto de árboles generadores. Sea *G* un grafo conexo donde los vértices representan edificios y los lados túneles de conexión entre los edificios. Se requiere determinar un subconjunto de túneles que deben mantenerse, a fin de poder llegar a un edifico desde otro a través de estos túneles. Además, se desea determinar los subconjuntos de túneles que al ser obstruidos separarían a algunos edificios de otros (subconjunto de lados de conexión y subconjunto de lados de no conexión de un grafo).

Árbol y árbol generador de un grafo

El **árbol de un grafo** es un subgrafo del grafo que es, en sí mismo, un árbol. En tanto, un **árbol generador de un grafo** conexo con

EJEMPLO

Considérese el grafo *G* de la figura 7.23. En la misma figura, *G'* es un árbol del grafo *G*, ya que es un subgrafo de *G*, que es un árbol. Por último, en esta figura, *G''* es un árbol generador del grafo *G*, ya que es un subgrafo generador de *G*, que es un árbol.

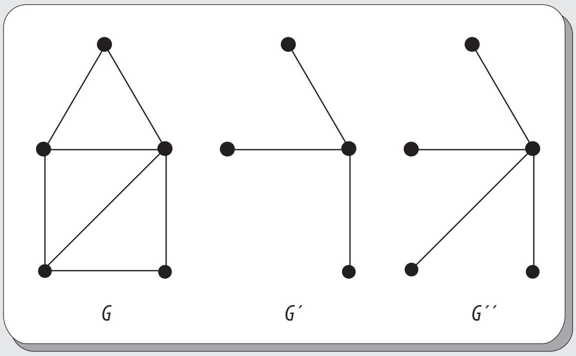


Figura 7.23 Grafo *G*; *G'* árbol de *G* y *G''* árbol generador de *G*.

Cuerda

Una cuerda o enlace de un árbol es un lado del grafo que no está en el árbol. El conjunto de cuerdas de un árbol se conoce como el complemento del árbol.

EJEMPLO

Considérese el grafo *G* de la figura 7.23; entonces, el subgrafo de la figura 7.24 es el complemento del árbol de la figura *G''*, con respecto a *G*.

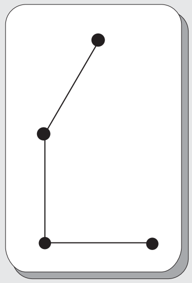


Figura 7.24 Complemento del árbol *G''* de la figura 7.23.

Un grafo conexo siempre contiene un árbol generador. Por tanto, si un grafo es conexo y no contiene circuitos, entonces es un árbol. Por su parte, si el grafo contiene uno o más circuitos, se puede eliminar un lado de los circuitos y aun así tener un subgrafo conexo.

Conjunto de corte

Un **conjunto de corte** es un conjunto (mínimo) de lados en un grafo, tal que la eliminación del conjunto incrementa el número de componentes conexas en el subgrafo restante, en tanto que la eliminación de cualquier subconjunto propio de este no lo haría.

De esto se tiene que en un grafo conexo, la eliminación de un conjunto de corte divide el grafo en dos partes; es decir, crea un grafo disconexo con dos componentes, esto es $K(G) = 2$.

EJEMPLO

Sea *G* el grafo conexo de la figura 7.25, para este grafo los conjuntos de lados siguientes:

$$\{e_1, e_4, e_5, e_6, e_7\} \text{ y } \{e_2, e_4, e_5, e_8\}$$

Constituyen conjuntos de corte, ya que su eliminación dejará subgrafos disconexos con dos componentes conexas, como las de la figura 7.27.

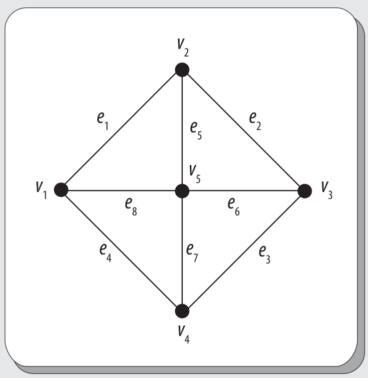


Figura 7.25 Grafo conexo *G*.

Por su parte, el grafo de la figura 7.26 es isomorfo al grafo de la figura 7.25; donde es posible ver con más claridad la división de los vértices para obtener un subgrafo disconexo con dos componentes, como el que se muestra en la figura 7.27.

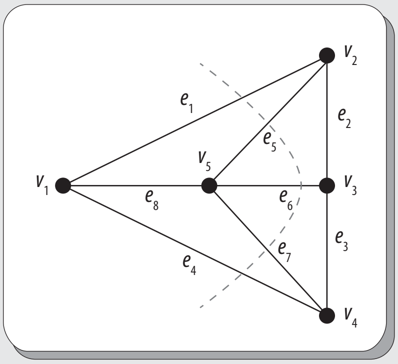


Figura 7.26 Grafo isomorfo al grafo de la figura 7.25.

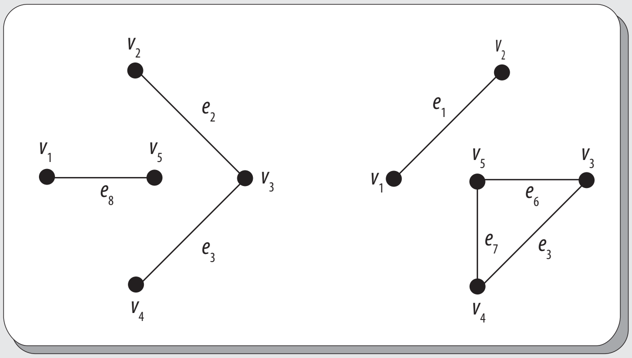


Figura 7.27 Subgrafos disconexos con dos componentes.

7.8 Árboles generadores mínimos

Una interpretación física de este problema consiste en considerar los vértices de un grafo como ciudades y los pesos de los lados como las distancias entre estas ciudades. Supóngase que se quiere construir una red de comunicaciones que conecte a todas las ciudades del grafo a un costo mínimo. Entonces, el problema consiste en determinar un árbol generador mínimo. El peso de un árbol generador es la suma de los pesos de los lados del árbol. Por tanto, un árbol generador mínimo es aquel con peso mínimo.

Un procedimiento para resolver este problema se basa en observar que, entre todos los lados en un circuito, el lado con mayor peso no está en el árbol generador mínimo.

Enseguida, se construye un subgrafo del grafo pesado, paso por paso, al tiempo que se examina cada lado en orden creciente de pesos. Luego, se agrega un lado al subgrafo parcialmente construido, si esta no origina un circuito, y se descarta en caso contrario. La construcción termina cuando todos los lados han sido examinados. Es claro que esta construcción da origen a un subgrafo que no contiene un circuito, el cual también es conexo. Así, el subgrafo construido es un árbol, que además es generador mínimo.

EJEMPLO

Considérese el grafo pesado de figura 7.28 *i*). De acuerdo con el proceso descrito antes, primero se construye el grafo de la figura 7.28 *ii*), que es un árbol generador mínimo.

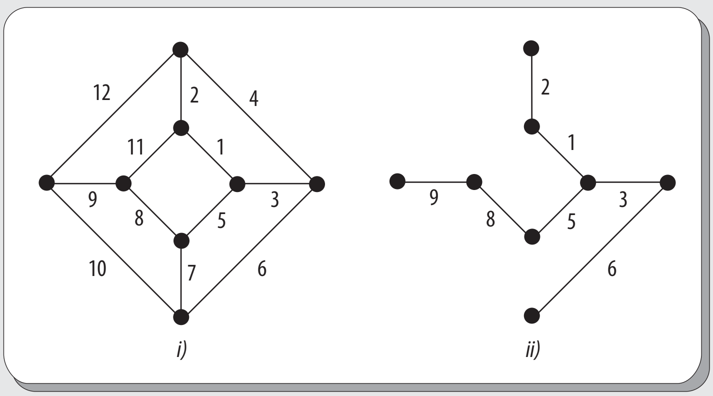


Figura 7.28 Grafo pesado y su árbol generador mínimo.

7.9 Recorridos en un árbol

Como se mencionó al inicio de este capítulo, la principal utilidad de los árboles es su aplicación en el área de la computación y la informática. Por esa razón, y con el fin de lograr su correcta utilización en una computadora, en esta sección se describe la estructura de un árbol binario y, sobre todo, cómo recorrerlo de modo eficiente. Dado que la intención del presente texto no es utilizar un lenguaje en particular, por tanto solo se aborda el tema en forma genérica (con algunos usos en lenguaje C), aunque sin pretender ser un texto especializado en codificación de árboles.

Estructura de árboles binarios

La estructura de un árbol binario se realiza a partir de nodos, cada uno de los cuales debe contener el campo dato (datos a almacenar) y dos campos de tipo puntero: uno al subárbol izquierdo y otro al subárbol derecho. Para indicar un árbol o un subárbol vacío se utiliza el valor NULL. En lenguaje C, para representar un nodo se utiliza "struct", en donde se agrupan todos los campos que lo conforman. Cada nodo contiene los campos dato: "izdo" (nodo rama izquierda) y "dcho" (nodo rama derecha). Pero, el tipo de dato de los elementos se generaliza como "tipoElemento".

Es posible acceder a los demás nodos de un árbol a partir de la raíz; por tanto, el puntero que permite acceder al árbol es el que hace referencia a la raíz. Considerando, además, que las ramas izquierda y derecha son, a su vez, árboles binarios con su propia raíz, se procede en forma recursiva hasta que se llega a las hojas del árbol.

Para lograr la formación de un árbol se construye cada uno de los nodos y el enlace con el correspondiente nodo padre. Además, es necesario reservar memoria para cada nodo, asignar el dato al campo correspondiente e inicializar los punteros izdo, dcho a NULL.

EJEMPLO

En este ejemplo se utiliza un esquema secuencial y una estructura auxiliar de tipo Pila para generar un árbol binario de cadenas de caracteres en C, mismo que se observa en la figura 7.29.

```
Árbol Binario raíz, ar1, ar2;
Pila pila1;

nuevoArbol (&ar1, NULL, "Alicia", NULL);
nuevoArbol (&ar2, NULL, "Francisco", NULL);
nuevoArbol (&raiz, ar1, "Martha", ar2);
insertar(&pila1, raiz);

nuevoArbol (&ar1, NULL, "Alma", NULL);
nuevoArbol (&ar2, NULL, "Martín", NULL);
nuevoArbol (&raiz, ar1, "Andrea", ar2);
insertar(&pila1, raiz);

ar2=quitar(&pila1);
ar1=quitar(&pila1);
nuevoArbol(&raíz, ar1,"Erika",ar2);
```

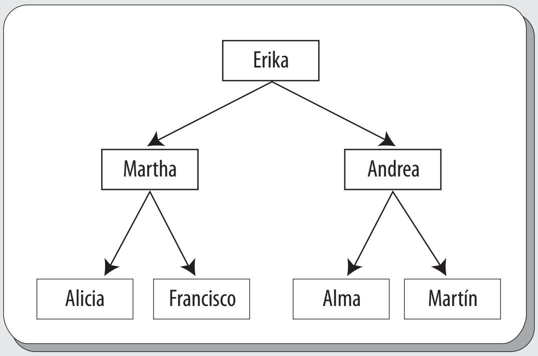


Figura 7.29 Árbol binario de cadenas de caracteres generado en lenguaje C.

Recorridos en árboles binarios

Para acceder a los datos almacenados en un árbol, primero es necesario recorrer el árbol o visitar los nodos de este. Para lograr el recorrido de un árbol existen diferentes métodos, pues en la mayoría de las aplicaciones resulta muy importante el orden en que son visitados los nodos.

Se dice que se logra un **recorrido de un árbol binario** siempre que cada nodo del árbol sea visitado una y solo una vez. Básicamente hay dos formas principales de llevar a cabo el recorrido de un árbol, las cuales se describen a continuación:

1. **Recorrido en profundidad.** En este tipo de recorrido se sigue un camino, comenzando desde la raíz, a través de un hijo, siguiendo al descendiente más cercano del primer hijo antes de continuar con el segundo hijo. En resumen, en el recorrido de profundidad se recorren todos los descendientes del primer hijo, después se recorren todos los descendientes del segundo hijo, y así sucesivamente.

2. **Recorrido en anchura.** En este tipo de recorrido se sigue un camino "horizontal", que empieza en la raíz, a través de todos sus hijos, luego se recorren los hijos de sus hijos y así sucesivamente, hasta que se recorren todos los nodos. En resumen, en el recorrido de anchura se recorre por completo cada nivel, antes de comenzar con el siguiente nivel.

En este texto solo se analiza el recorrido en profundidad, el cual puede llevarse a cabo en tres formas en esencia distintas: recorrido en **"preorden"**, recorrido **"enorden"** y recorrido **"postorden".**

Recorrido en preorden

El recorrido en preorden (nodo–izquierdo–derecho o NID) se resume en tres pasos principales:

1. Visitar el nodo raíz (N)
2. Recorrer el árbol izquierdo (I) en preorden (NID)
3. Recorrer el subárbol derecho (D) en preorden (NID)

Por tanto, en el recorrido en preorden, en primer lugar se visita la raíz del árbol y luego el subárbol izquierdo (que es a su vez un árbol), utilizando el orden nodo–izquierdo–derecho. Una vez recorrido el subárbol izquierdo se continúa con el derecho utilizando el orden NID.

EJEMPLO

Considérese el árbol de la figura 7.30. En este caso, para este árbol se realiza el recorrido en preorden de acuerdo con los dos pasos siguientes: 1. se visita la raíz (nodo *r*); 2. se recorre el subárbol izquierdo de *r*, el cual se compone de los nodos *a*, *c* y *d*. Considerando que el subárbol es, a su vez, un árbol, primero se recorre el nodo *a*, después el *c* (izquierdo) y por último el *d* (derecho). Acto seguido, se continúa con el recorrido del subárbol derecho de *r*, que es un árbol con nodos *b*, *e* y *f*. Otra vez se sigue el orden NID, recorriendo en primer lugar el nodo *b*, luego el nodo *e* (I) y al final el nodo *f* (D). Por tanto, el recorrido en preorden para el árbol de la figura 7.30 es:

$$r-a-c-d-b-e-f$$

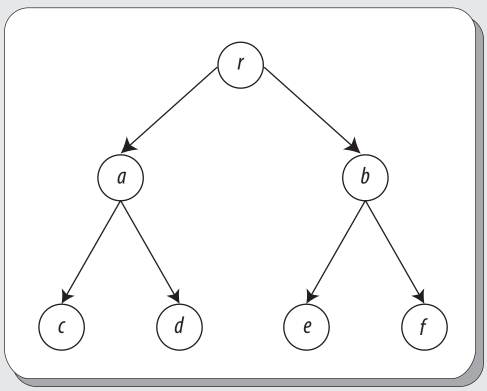


Figura 7.30 Árbol binario recorrido en preorden.

EJEMPLO

Considérese el árbol de la figura 7.31. En este caso, para este árbol se realiza el recorrido en preorden de acuerdo con los pasos siguientes: 1. se visita la raíz (nodo *r*); 2. se recorre el subárbol izquierdo de *r*, que se compone de los nodos *a*, *c* y el subárbol con raíz *d* y nodos *g*, *h*. Por tanto, primero se recorre el nodo *a*, después el *c* (izquierdo) y finalmente el *d*; considerado como subárbol, este se recorre en preorden (NID), es decir se visita *d*, luego *g* y por último *h*. Luego, se continúa recorriendo el subárbol derecho de *r*, que es un árbol con nodos *b*, *e* y *f*. Otra vez se sigue el orden NID, recorriendo en primer lugar el nodo *b*, luego el nodo *e* (I) y finalmente el nodo *f* (D). Por tanto, el recorrido en preorden para el árbol de la figura 7.31 es:

r—a—c—d—g—h—b—e—f

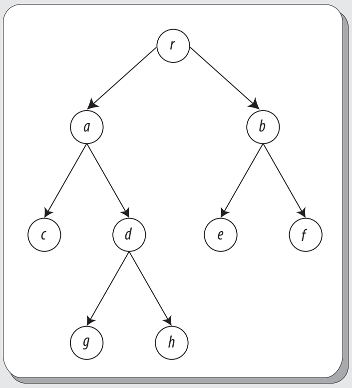


Figura 7.31 Árbol binario recorrido en preorden.

Recorrido en enorden

El recorrido en enorden (izquierdo—nodo—derecho o IND) puede resumirse en tres pasos principales:

- Recorrer el subárbol izquierdo (I) en enorden (IND)
- Visitar el nodo raíz (N)
- Recorrer el subárbol derecho (D) en enorden

Entonces, de acuerdo con lo expuesto antes, en este tipo de recorrido de un árbol binario, primero se recorre el subárbol izquierdo, después la raíz y por último el subárbol derecho.

EJEMPLO

Considérese el árbol de la figura 7.32. En este caso, para este árbol se realiza el recorrido enorden de acuerdo con los pasos siguientes: 1. se visita el subárbol izquierdo del nodo raíz, el cual contiene los nodos *a*, *c* y *d*, y es, en sí mismo, otro árbol con raíz *a*; para recorrerlo se sigue el orden IND, es decir, se recorre en primer lugar el nodo *c* (nodo izquierdo), a continuación el nodo *a* (raíz) y finalmente el nodo *d* (nodo derecho); 2. una vez recorrido el subárbol izquierdo, se visita la raíz *r* y 3. por último se visita el subárbol derecho, que consta de los nodos *b*, *d* y *e*. Siguiendo el orden IND en el subárbol derecho, se visita primero el nodo *e* (nodo izquierdo), luego el nodo *b* (raíz) y finalmente el nodo *e* (nodo derecho). Por tanto, el recorrido en enorden para el árbol de la figura 7.32 es:

c—a—d—r—e—b—f

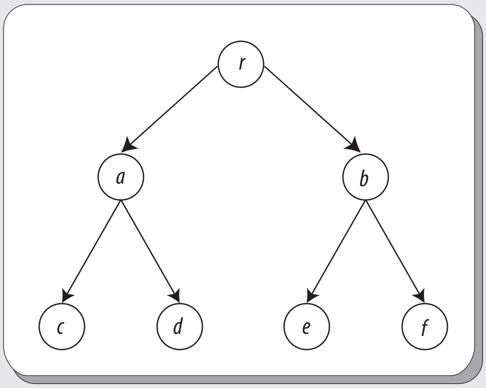


Figura 7.32 Árbol binario recorrido en enorden.

EJEMPLO

Considérese el árbol de la figura 7.33. En este caso, para este árbol se realiza el recorrido enorden conforme los pasos siguientes: 1. se visita el subárbol izquierdo del nodo raíz, el cual contiene los nodos *a*, *c* y *d*, y es, en sí mismo, otro árbol con raíz *a*; para recorrerlo se sigue el orden IND, es decir, se recorre en primer lugar el nodo *c* (nodo izquierdo), a continuación el nodo *a* (raíz) y al final el subárbol con raíz *d*; al recorrerse este enorden, entonces se visitan los nodos en el orden *g*, *d*, *h* (IND); 2. una vez recorrido el subárbol izquierdo se visita la raíz *r* y 3. por último el subárbol derecho, que consta de los nodos *b*, *d* y *e*. Siguiendo el orden IND en el subárbol derecho, se visita primero el nodo *e* (nodo izquierdo), luego el nodo *b* (raíz) y por último el nodo *e* (nodo derecho). Por tanto, el recorrido enorden para el árbol de la figura 7.33 es:

$$c—a—g—d—h—r—e—b—f$$

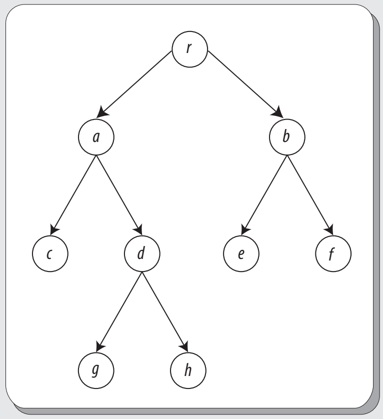


Figura 7.33 Árbol binario recorrido en enorden.

Recorrido en postorden

El recorrido en postorden (izquierdo—derecho—nodo o IDN) se resume en tres pasos principales:

1. Recorrer el subárbol izquierdo (I) en postorden (IDN)
2. Recorrer el subárbol derecho (D) en postorden (IDN)
3. Visitar el nodo raíz (N)

Entonces, en este tipo de recorrido de un árbol binario, primero se recorre el subárbol izquierdo, después el subárbol derecho y por último el nodo raíz.

EJEMPLO

Considérese el árbol de la figura 7.34. En este caso, se realiza el recorrido postorden de acuerdo con los siguientes pasos: 1. se visita el subárbol izquierdo del nodo raíz, el cual contiene los nodos *a*, *c* y *d*, y es, en sí mismo, otro árbol con raíz *a*; para recorrerlo se sigue el orden IDN, es decir, se recorre en primer lugar el nodo *c* (nodo izquierdo), a continuación el nodo *d* (nodo derecho) y al final el nodo *a* (nodo raíz); 2. una vez recorrido el subárbol izquierdo se recorre el subárbol derecho de *r*, que consta de los nodos *b*, *d* y *e*; siguiendo el orden IDN en el subárbol derecho, se visita primero el nodo *e* (nodo izquierdo), luego el nodo *f* (nodo derecho) y enseguida el nodo *b* (nodo raíz). 3. Por ultimo, se visita el nodo raíz *r*. Por tanto, el recorrido en postorden para el árbol de la figura 7.34 es:

$$c—d—a—e—f—b—r$$

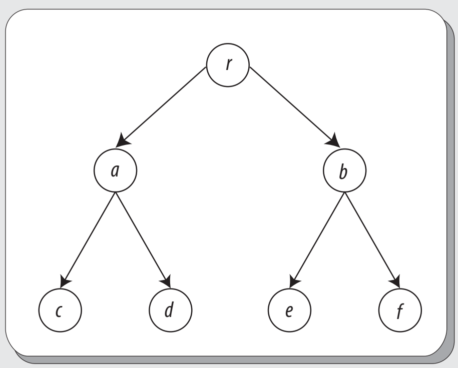


Figura 7.34 Árbol binario recorrido en postorden.

EJEMPLO

Considérese el árbol de la figura 7.35. En este caso, se realiza el recorrido postorden conforme los pasos siguientes: 1. se visita el subárbol izquierdo del nodo raíz, el cual contiene los nodos *a*, *c* y el subárbol con raíz *d*; para recorrerlo se sigue el orden IDN, es decir, se recorre en primer lugar el nodo *c* (nodo izquierdo), a continuación el subárbol derecho con raíz *d*, en orden IND, esto es *g*, *h*, *d*, y por último el nodo *a* (nodo raíz). 2. se recorre el subárbol derecho de *r*, que consta de los nodos *b*, *d* y *e*; siguiendo el orden IDN en el subárbol derecho, se visita primero el nodo *e* (nodo izquierdo), luego el nodo *f* (nodo derecho) y enseguida el nodo *b* (nodo raíz). 3. Por último, se visita el nodo raíz *r*. Por tanto, el recorrido en postorden para el árbol de la figura 7.35 es:

$$c—g—h—d—a—e—f—b—r$$

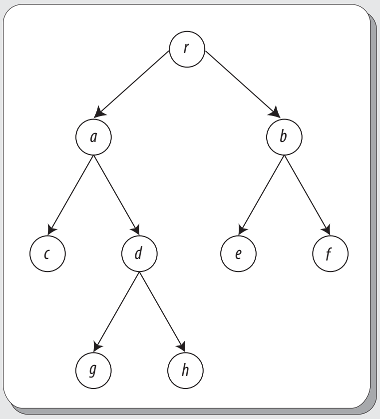


Figura 7.35 Árbol binario recorrido en postorden.

7.10 Árboles de expresión

Una de las más importantes aplicaciones de los árboles binarios son los árboles de expresión. En este contexto, una expresión se define de manera formal como una secuencia de **tokens** (componentes de algún léxico que guardan ciertas reglas establecidas). Cada token puede ser un operando o un operador.

En términos formales, un árbol de expresión constituye un árbol binario que cumple con las tres propiedades siguientes:

1. Cada hoja es un operando
2. Tanto el nodo raíz como los nodos rama son operadores
3. Los subárboles son subexpresiones con la característica de que su nodo raíz es un operador

EJEMPLO

Considérese la expresión

$$a * (b + c) + d * (e + f)$$

la cual se representa en la figura 7.36 mediante un árbol binario de expresión.

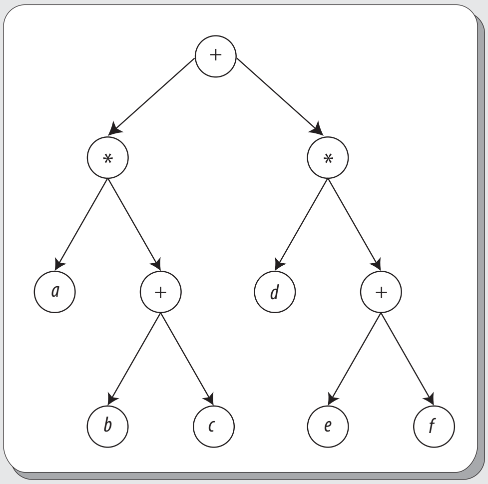


Figura 7.36 Árbol binario de expresión.

Una observación importante aquí es que los paréntesis no se almacenan en el árbol, sino que se representan de manera implícita en la forma que tiene el árbol en sí mismo. Tomando en cuenta que los operadores contemplados son binarios (cada operador contempla dos operandos), un árbol de expresión se puede construir considerando la raíz como un operador y a los subárboles izquierdo y derecho como los operandos izquierdo y derecho, respectivamente. Cada uno de los subárboles puede ser una literal (a, b, x, etc.) o una subexpresión representada como un subárbol.

Ejemplo

Dibujar el árbol binario que representa la expresión:

$$(x - y) * (z + w)$$

Solución

En este caso, el operador * constituye el operador que se considera en la raíz, pues en el subárbol izquierdo se considera la operación $(x - y)$ y en el derecho la operación $(z + w)$, cuyos resultados son operadas entre sí con el operador *.

En la figura 7.37 se observa el árbol resultante de la expresión $(x - y) * (z + w)$.

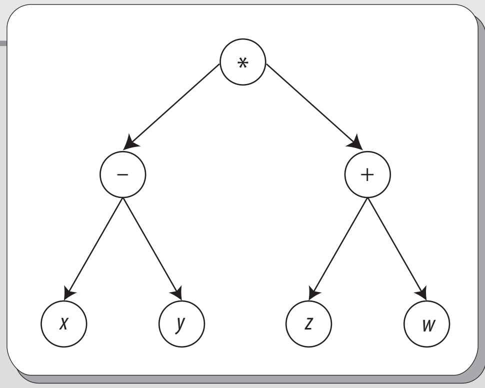


Figura 7.37 Árbol de expresión para la expresión $(x - y) * (z + w)$.

Ejemplo

Dibujar el árbol binario que representa la expresión:

$$a * (b + c) - (a - b)$$

Solución

En este caso, el operador $-$ es el operador que se considera en la raíz, pues en el subárbol izquierdo se considera la operación $a * (b + c)$ y en el derecho la operación $(a - b)$, cuyos resultados son operadas entre sí con el operador $-$.

En la figura 7.38 se observa el árbol resultante de la expresión $a * (b + c) - (a - b)$.

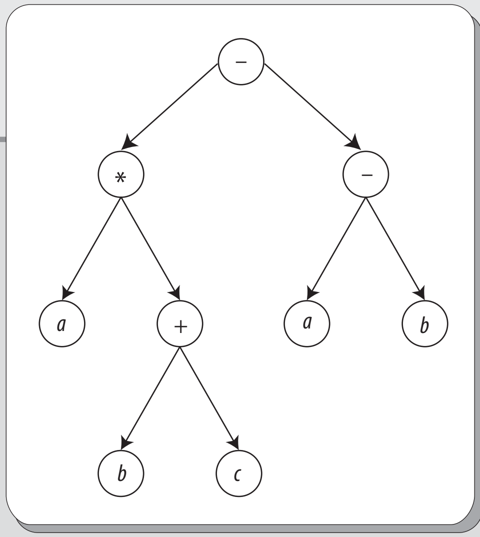


Figura 7.38 Árbol binario para la expresión $a * (b + c) - (a - b)$.

Ejemplo

Obtener la expresión dada por el árbol de expresión binario de la figura 7.39.

Solución

La expresión que resulta es:

$$a + \left(\frac{b}{c - d}\right)$$

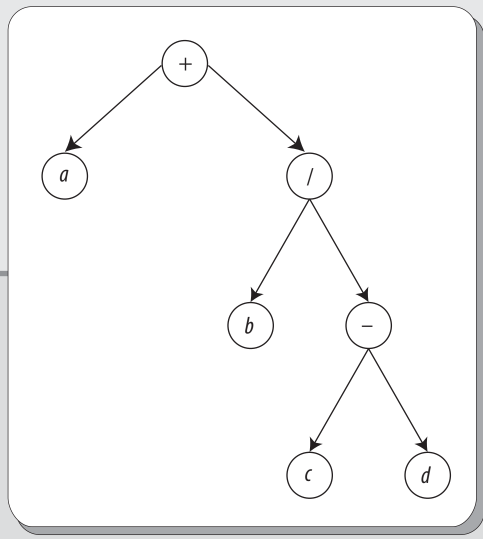


Figura 7.39 Árbol de expresión binario.

Ejemplo

Obtener la expresión dada por el árbol de expresión binario de la figura 7.40.

Solución

La expresión resultante es:

$$a - \frac{b}{-(c+b)}$$

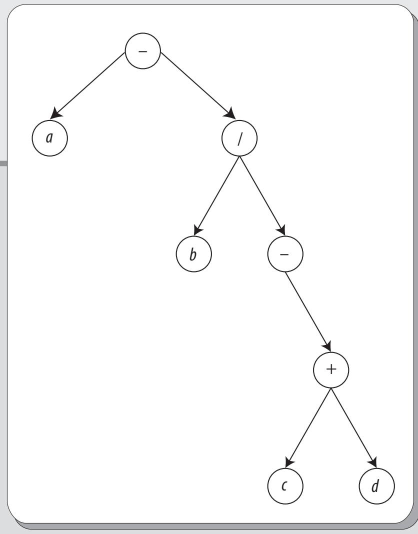


Figura 7.40 Árbol de expresión binario.

Ejemplo

Obtener el árbol binario correspondiente a cada una de las siguientes expresiones:

1. $\dfrac{a*b}{(c-d)*e}$ 2. $\dfrac{a*(b+c)}{d}$

Solución

El árbol de expresión correspondiente se muestra en la figura 7.41.

El árbol de expresión correspondiente se muestra en la figura 7.42.

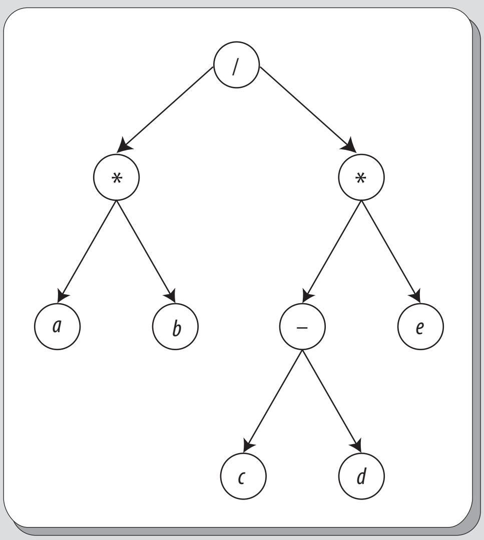


Figura 7.41 Árbol binario para la expresión $a * b / (c - d) * e$.

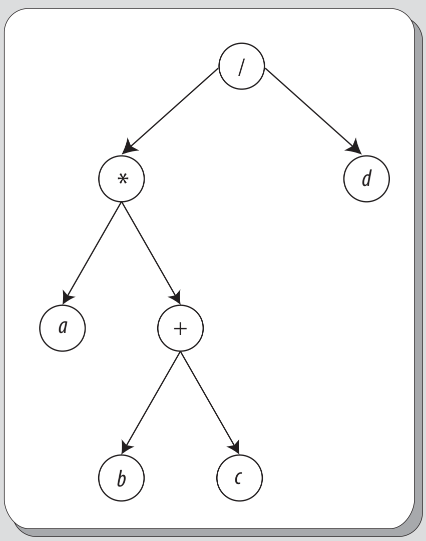


Figura 7.42 Árbol binario para la expresión $a * (b + c) / d$.

Algoritmo para construir árboles de expresión

De manera primordial, los árboles de expresión se utilizan para evaluar expresiones en programación. Por tanto, es importante establecer el algoritmo básico para la construcción de un árbol de expresión, el cual se puede resumir en cinco pasos:

1. Al encontrar el primer paréntesis izquierdo se genera un nodo y se hace en el nodo raíz. Este nodo se considera como nodo actual y su puntero se coloca en una pila.
2. Cada que se encuentra un nuevo paréntesis izquierdo, se crea un nuevo nodo. De este modo, si el nodo actual no tiene hijo izquierdo, el nodo recién creado se establece como hijo izquierdo, en caso contrario se establece como hijo derecho y el nuevo nodo se establece como el nodo actual.
3. Al encontrar un operando, se crea un nodo nuevo y se asigna el operando al correspondiente campo de datos. Si el nodo actual no tiene hijo izquierdo, el nodo recién creado se establece como hijo izquierdo, en caso contrario se establece como hijo derecho.
4. Al encontrar un operador, se debe sacar un puntero de la pila y colocar el operador en campo de datos del nodo del puntero.
5. Se deben ignorar los paréntesis derechos y espacios en blanco.

7.11 Árboles balanceados o árboles AVL

Se dice que un árbol es o está **balanceado** (equilibrado), si y solo si en cada nodo las alturas de sus dos subárboles difieren cuando más en 1. Los árboles balanceados son útiles sobre todo en el manejo adecuado de datos organizados en forma jerárquica. Los árboles balanceados también se conocen como árboles AVL, en honor a los matemáticos rusos G. M. Adelson-Velsitii y E. M. Landis. Entonces, un árbol AVL es un árbol binario de búsqueda con una condición de equilibrio, la cual asegura que la complejidad de la búsqueda es logarítmica: $O(\log(n))$.

La idea más simple de equilibrio consiste en exigir que los subárboles izquierdo y derecho tengan la misma altura, sin solicitar que el árbol sea poco profundo. Por lo anterior, esta idea de equilibrio es poco eficiente, como se muestra en la figura 7.43.

Otra condición de equilibrio exige que todo nodo debe tener subárboles izquierdo y derecho a la misma altura. Si la altura de un árbol vacío se define como -1, solo los árboles perfectamente equilibrados de $2^k - 1$ nodos satisfacen este criterio. No obstante, aunque esto garantiza árboles de profundidad pequeña, la condición de equilibrio es demasiado rígida para ser útil, ya que es necesario que esta sea moderada.

Un árbol AVL es idéntico a un árbol binario de búsqueda, excepto porque en un árbol AVL la altura de todos sus subárboles, izquierdo y derecho, pueden diferir a lo más en 1. La altura de un árbol vacío se define como -1.

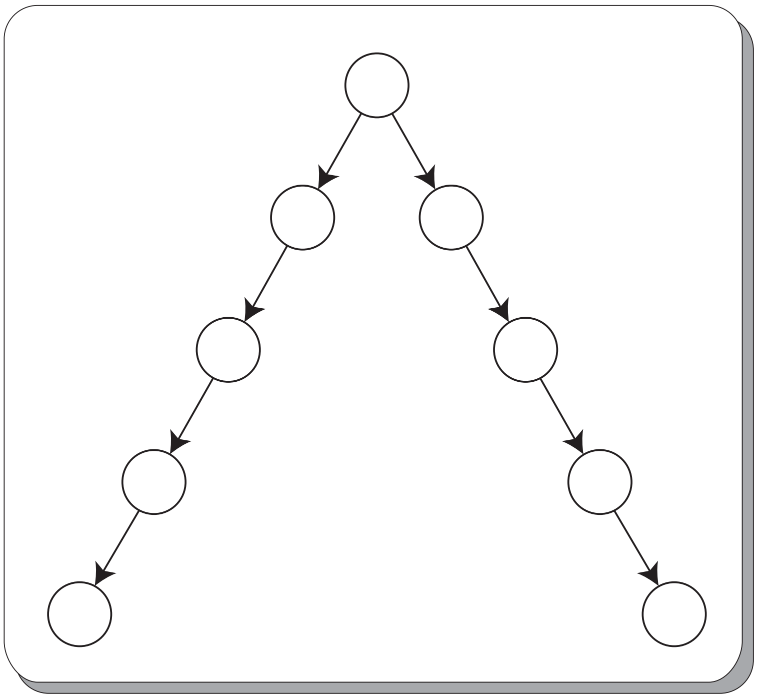


Figura 7.43 Un mal árbol binario, pues la condición en la raíz no es suficiente (esto significa que no es AVL).

EJEMPLO

En la figura 7.44*i*) se observa un árbol de búsqueda, mientras que en la figura 7.43*ii*) se distingue un árbol AVL.

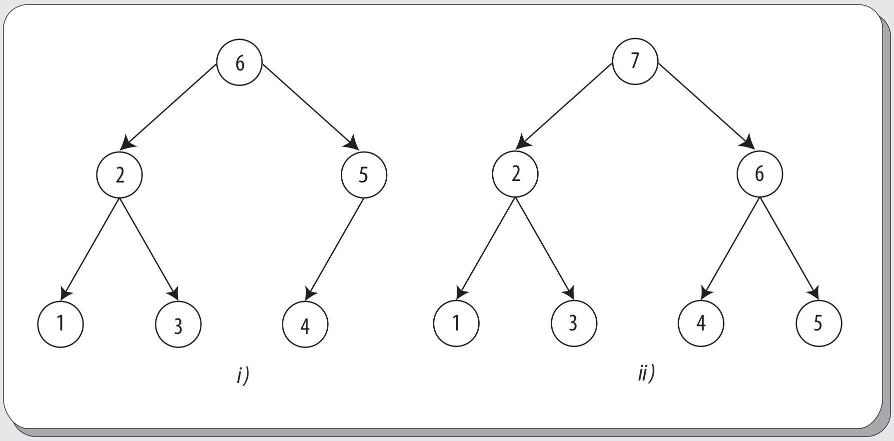


Figura 7.44 i) Árbol AVL. ii) Árbol de búsqueda.

EJEMPLO

En la figura 7.45 se muestran cinco árboles, todos son ejemplos de árboles AVL.

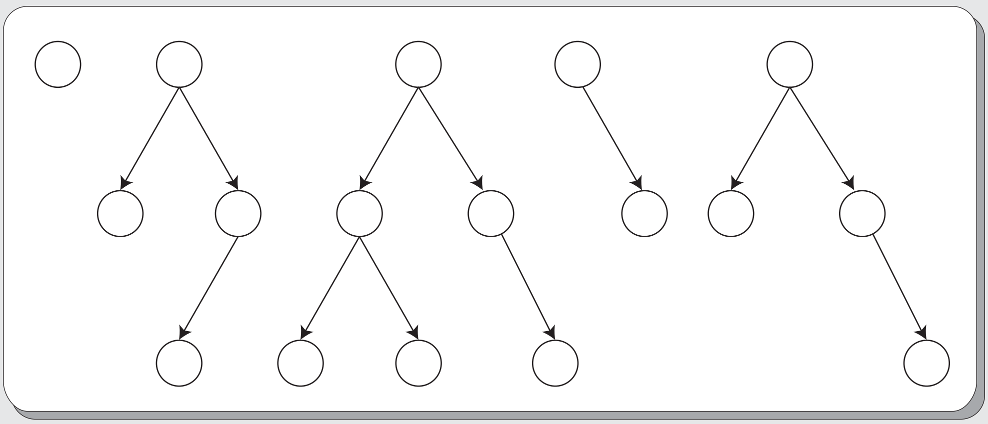


Figura 7.45 Árboles AVL.

Para determinar la altura de un árbol AVL, por lo común se acostumbra utilizar la altura máxima, pues calcular la altura promedio puede llegar a ser complicado. El objetivo de calcular la altura es que el número resultante representa el número de iteraciones que se realizan para bajar desde la raíz hasta el nivel más profundo. Por tanto, la eficacia de los algoritmos utilizados en árboles depende de su altura.

El árbol AVL, de n nodos, menos denso tiene como altura:

$$h \approx 1.44\log(n)$$

Donde n es el número de nodos, en el peor de los casos, de un árbol AVL de altura h y; por tanto, se puede afirmar que la complejidad de una búsqueda es: $O(\log(n))$.

Ahora bien, cuando se hace una inserción es necesario actualizar toda la información de equilibrio para los nodos en el camino a la raíz; la razón de que la inserción sea potencialmente difícil se debe a que insertar un nodo puede violar la propiedad de ser AVL. Si este es el caso, es necesario restaurar la propiedad antes de considerar terminado el paso de inserción. Esto se puede hacer modificando siempre en forma sencilla el árbol; dicho paso se conoce como rotación.

Rotación simple o sencilla

Considérense los árboles de búsqueda binaria de la figura 7.46, los cuales tienen los mismos elementos.

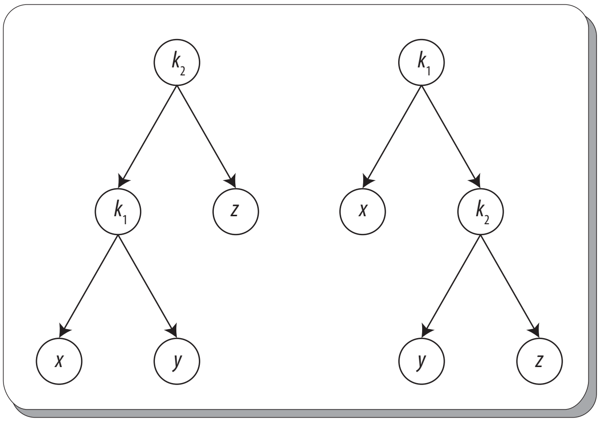


Figura 7.46 Rotación simple o sencilla.

Como se puede ver en la figura, en primer lugar estos dos árboles son $k_1 < k_2$. En segundo lugar, todos los elementos del subárbol son menores que k_1, en ambos árboles. En tercer lugar, todos los elementos del subárbol son mayores que k_2. Por último, todos los elementos del subárbol z están entre k_1 y k_2. El proceso de transformación de uno de los árboles a otro es a lo que se denomina **rotación**. En una rotación solo intervienen unos cuantos cambios de apuntadores y cambia a estructura del árbol que preserva la propiedad de búsqueda.

No es preciso que la rotación se realice en la raíz del árbol, esta también se puede hacer en cualquier nodo del árbol, ya que cualquier nodo es la raíz de algún subárbol, y puede transformar cualquier árbol en otro. Este se considera un método sencillo para arreglar un árbol AVL. Si la inserción causa que algún nodo pierda la condición de equilibrio, entonces se hace una rotación en ese nodo. El algoritmo básico de la rotación consiste en iniciar en el nodo insertado y subir en el árbol, actualizando la información de equilibrio en cada nodo del camino. De este modo, si se llega a la raíz sin encontrar ningún nodo desequilibrado, el proceso termina. En caso contrario, se aplica una rotación al primer nodo incorrecto que se encuentre.

EJEMPLO

En el árbol de la figura 7.47 *i)* se observa la inserción del nodo 6.5, el cual genera desequilibrio en el árbol AVL, mientras que la rotación que se observa en el árbol 7.47 *ii)* corrige dicho desequilibrio.

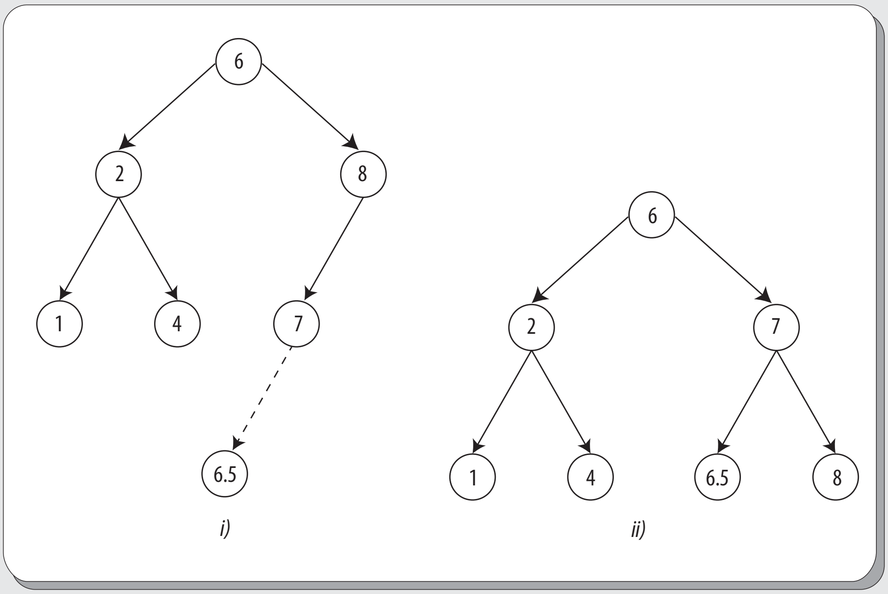


Figura 7.47 i) Árbol con propiedad AVL destruida con la inserción del nodo 6.5. ii) Árbol i) con propiedad AVL restablecida después de una rotación.

Ejemplo

Construir un árbol AVL de 7 vértices.

Solución

Se comienza con un árbol vacío y se insertan las llaves del 1 al 7, en forma secuencial. El primer problema surge al momento de insertar la llave 3, porque la propiedad AVL se viola en la raíz. Dicho problema se resuelve, como se vio antes, a través de una rotación (véase figura 7.48).

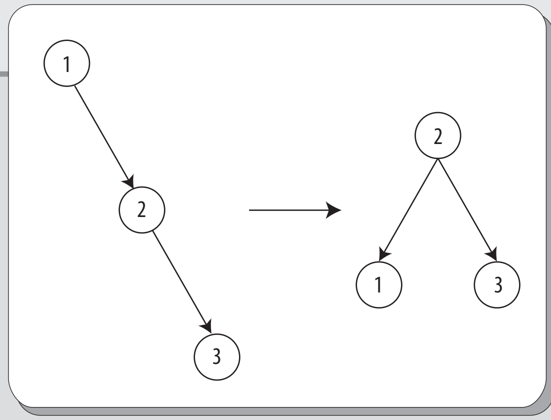


Figura 7.48 Rotación simple para preservar la propiedad AVL.

Una vez hecha la rotación, se inserta el nodo 4, lo que no ocasiona problemas con la propiedad AVL. Sin embargo, al colocar el nodo 5, se produce una violación en el nodo 3, por tanto se vuelve a aplicar una rotación para corregir el problema generado (véase figura 7.49).

Después, se inserta el nodo 6, lo que ocasiona un problema de equilibrio en la raíz, ya que el subárbol derecho tendrá altura 2 y el izquierdo altura 0. Ante esto, se lleva a cabo una rotación simple entre 2 y 4 (véase figura 7.50).

Por último, se inserta el nodo 7, lo que origina otra violación en el nodo 6; por tanto, se vuelve a efectuar una rotación simple (véase figura 7.51).

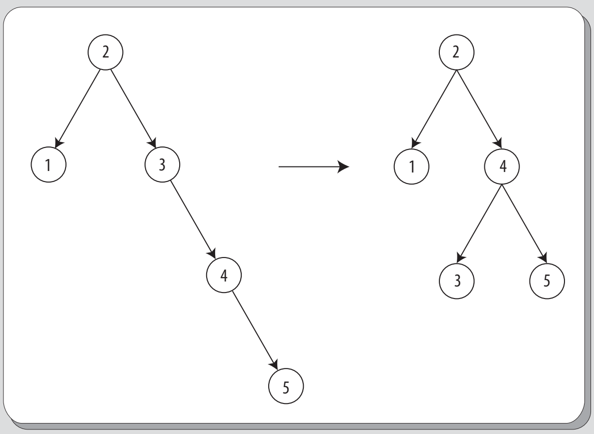


Figura 7.49 Rotación simple para preservar la propiedad AVL.

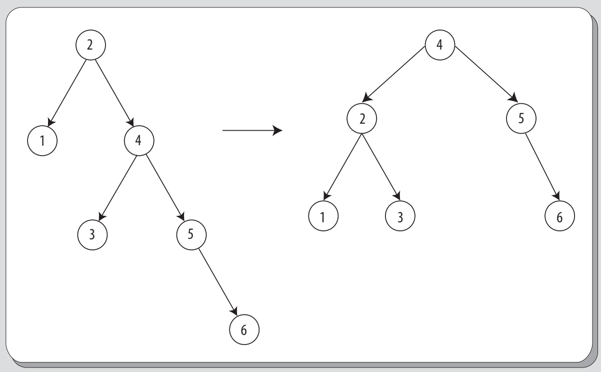


Figura 7.50 Rotación simple para preservar la propiedad AVL.

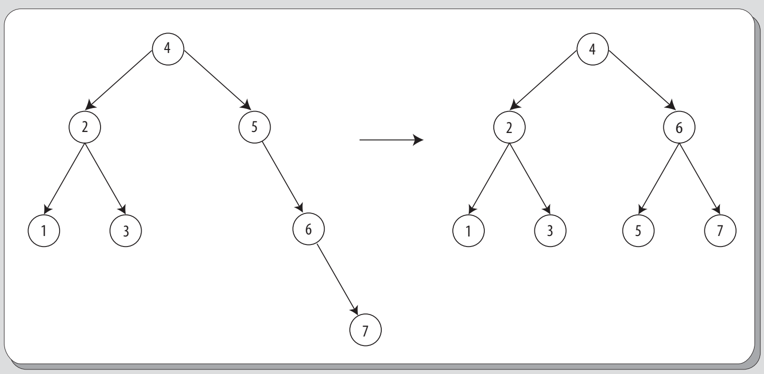


Figura 7.51 Rotación simple para preservar la propiedad AVL.

Rotación doble

Existe un caso en el que una rotación simple no es suficiente para restablecer la propiedad AVL. Por ejemplo, si en el último árbol obtenido (véase figura 7.51), se insertan los nodos del 1 al 15 en orden inverso; la inserción del 15 es fácil, ya que no destruye la propiedad AVL, pero al insertar el 14 se ocasiona un desequilibrio de altura en el nodo 7; por tanto, como se muestra en la figura 7.52, una rotación simple no corrige el problema.

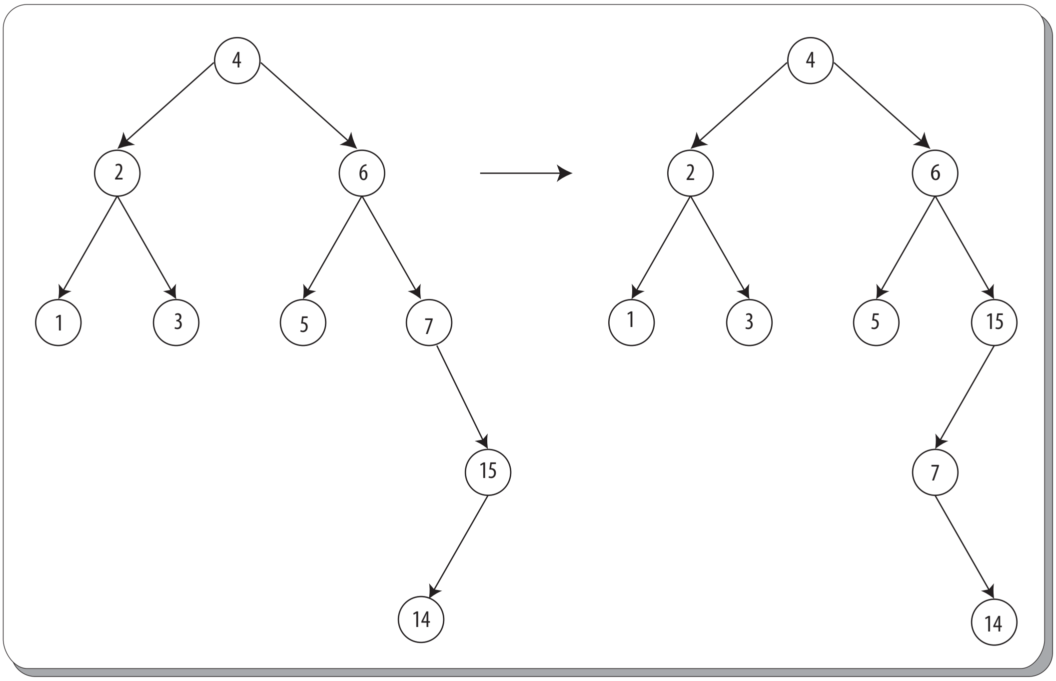


Figura 7.52 La rotación simple no recupera la propiedad AVL.

Como se puede ver en la figura 7.52, la rotación simple no corrige el desequilibrio de altura. El problema es que el desequilibrio fue ocasionado por un nodo insertado en el árbol que contiene los elementos medios, al tiempo que los otros árboles tienen altura idéntica. La solución se conoce como rotación doble, que es semejante a la rotación simple, solo que esta abarca cuatro subárboles en lugar de solo tres (véase figura 7.53).

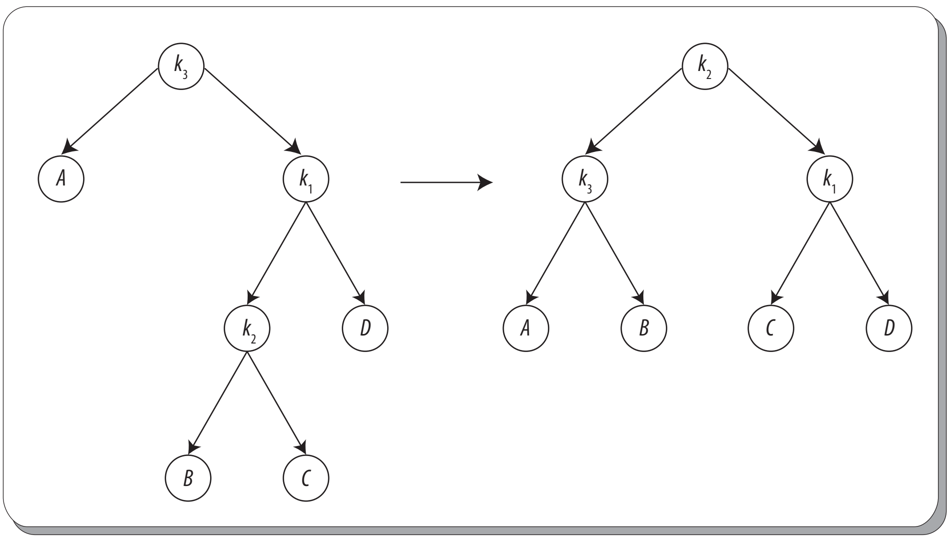


Figura 7.53 Rotación doble, derecha-izquierda.

De manera similar, es posible realizar la rotación doble izquierda-derecha (véase figura 7.54).

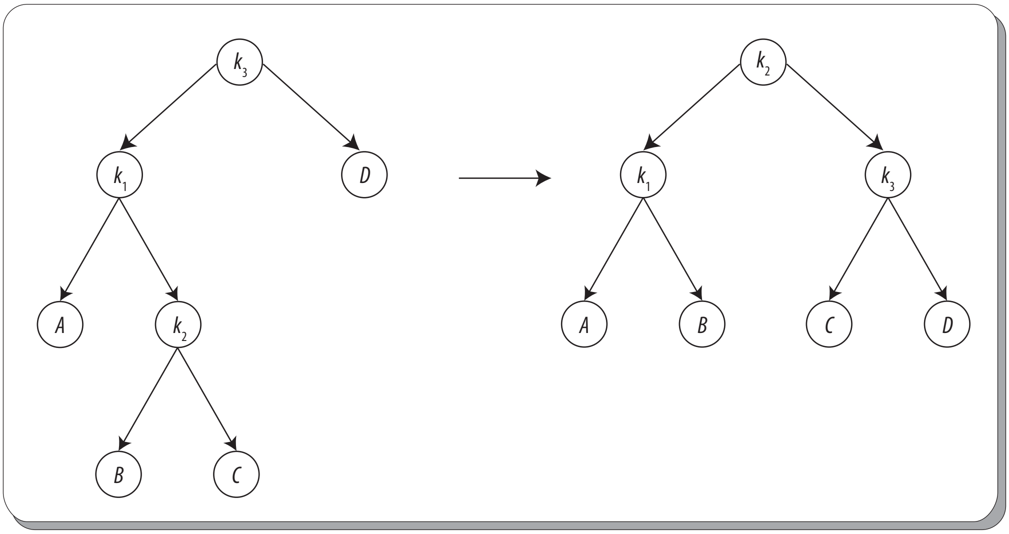


Figura 7.54 Rotación doble, izquierda—derecha.

Ejemplo

Considérese el árbol de la figura 7.52. Realizar una rotación doble para lograr la propiedad AVL en dicho árbol y continuar con la inserción de los nodos 13, 12 y 11.

Solución

En este caso, primero se lleva a cabo una rotación doble, derecha-izquierda (véase figura 7.55).

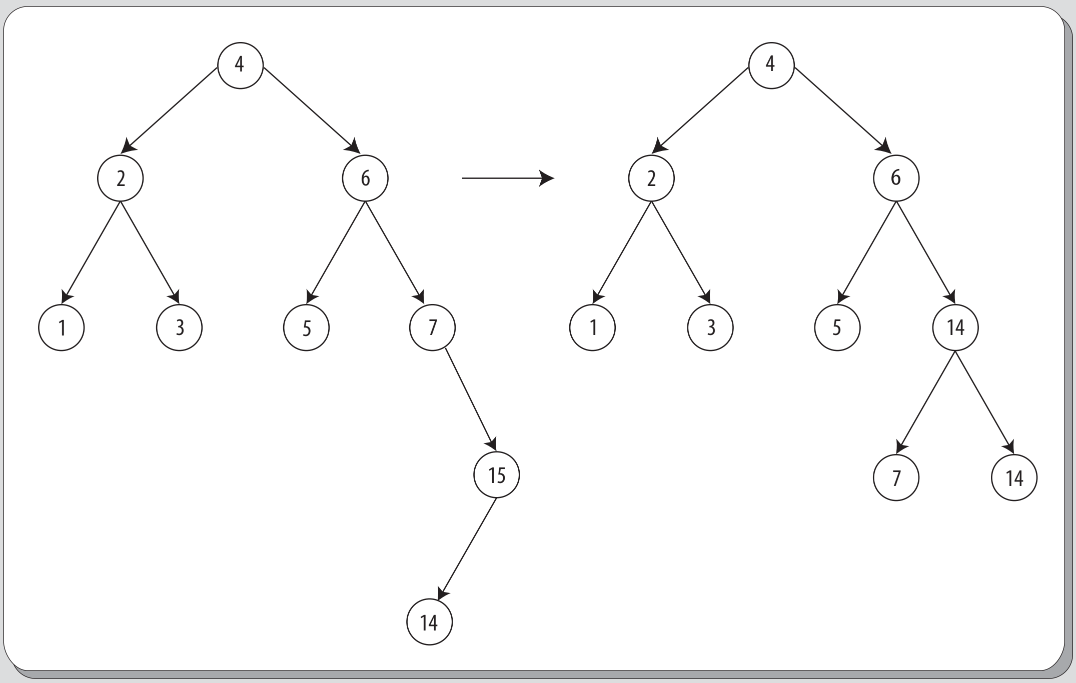


Figura 7.55 Rotación doble, se recupera la propiedad AVL.

Una vez recuperada la propiedad AVL, se inserta el siguiente nodo: 13. Es importante hacer notar que esta inserción también requiere una rotación doble para recuperar el estatus AVL del árbol (véase figura 7.56).

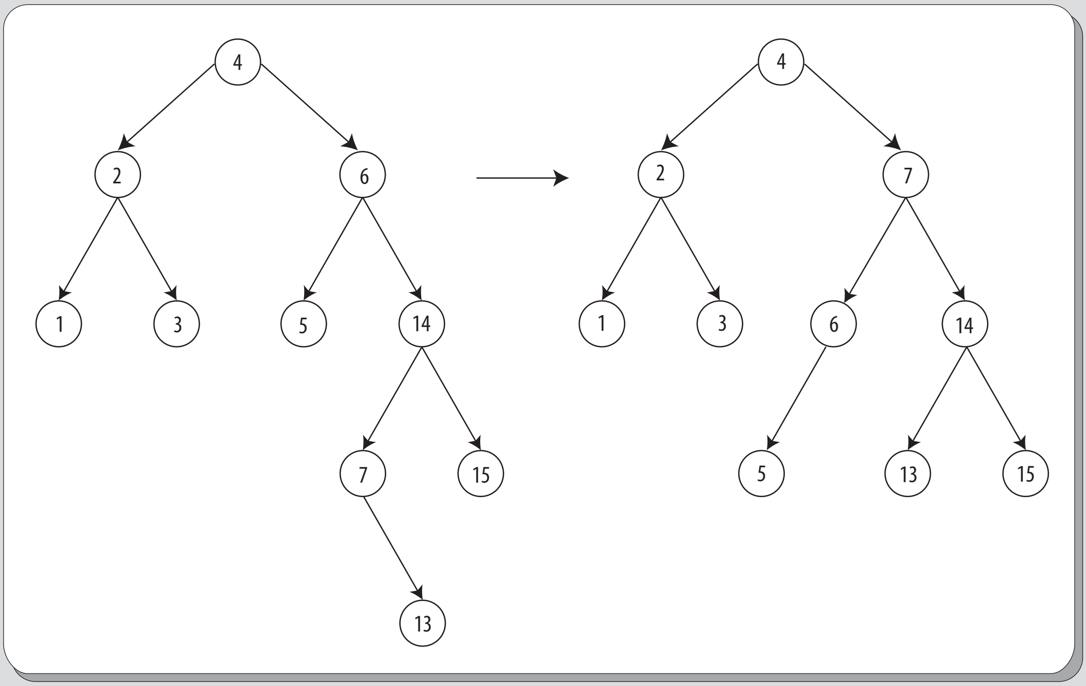


Figura 7.56 Rotación doble, mediante la cual se recupera la propiedad AVL.

Si ahora se inserta el nodo 12, entonces aparece un desequilibrio con la raíz, pero una rotación simple basta aquí para lograr recuperar la propiedad AVL (véase figura 7.57).

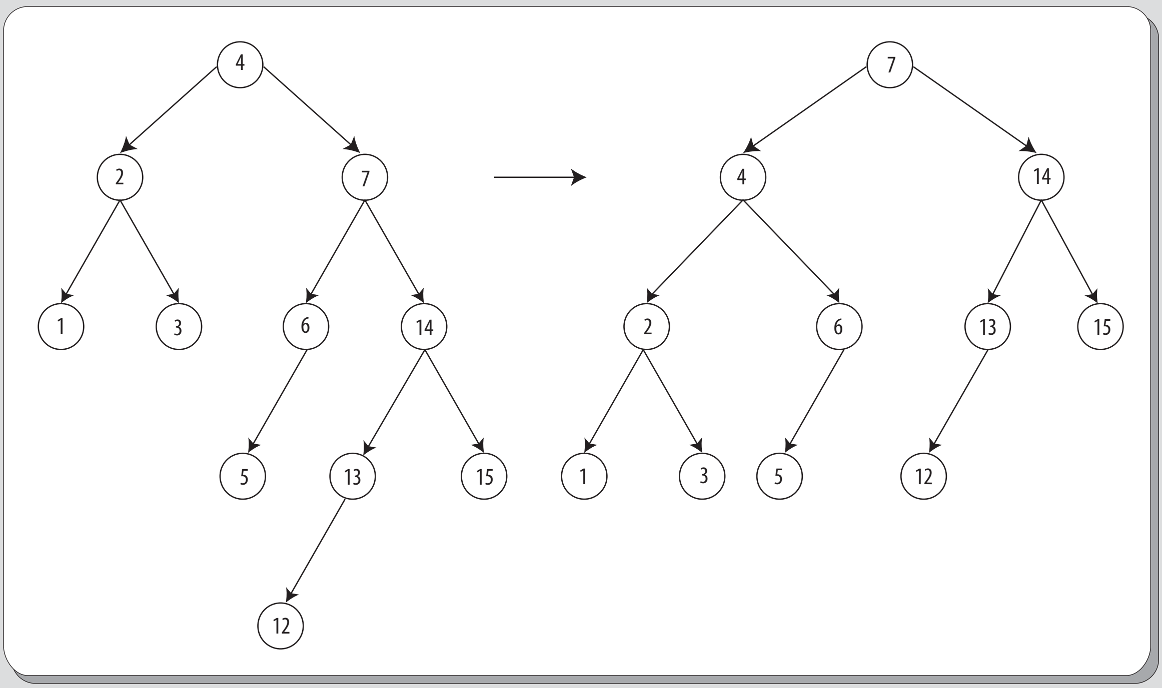


Figura 7.57 Rotación simple mediante la cual se recupera la propiedad AVL.

Luego, se inserta el nodo 11; esta inserción también requiere una rotación simple para obtener un árbol AVL (véase figura 7.58).

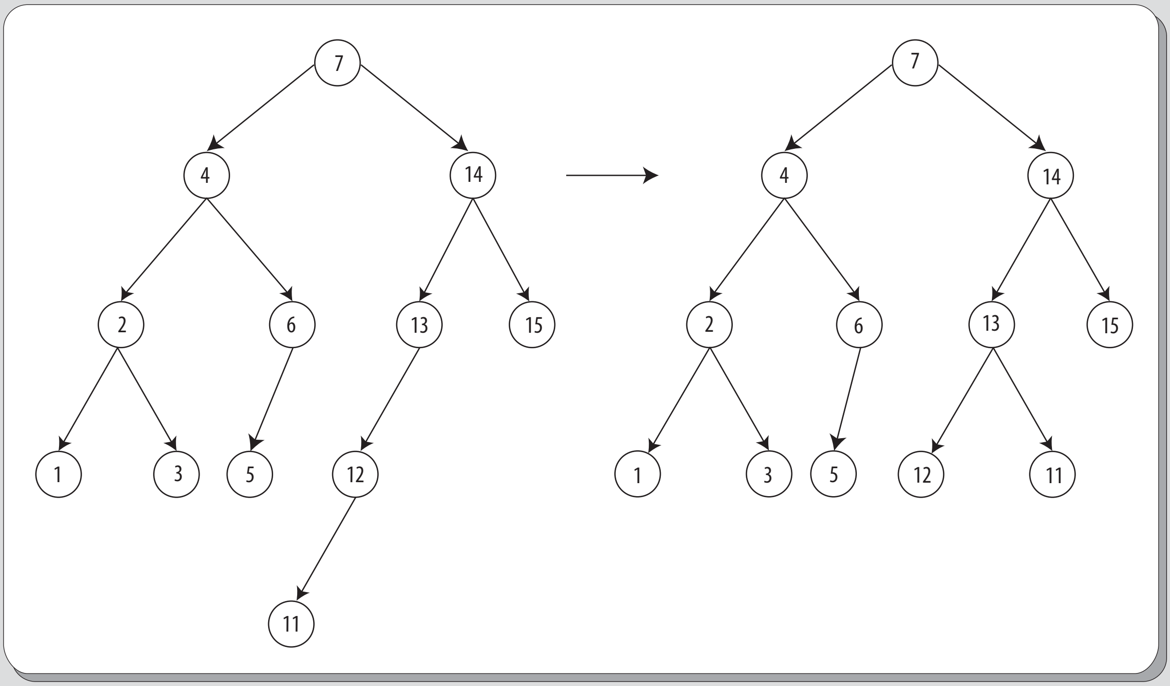


Figura 7.58 Rotación simple mediante la cual se recupera la propiedad AVL.

Por último, se inserta el nodo 10, y de nuevo es necesaria una rotación simple, pues dicha inserción viola la propiedad AVL. Lo mismo sucede para el caso del vértice 9, no así para el 8, que no requiere rotación. Al final, después de realizar las dos rotaciones mencionadas, se obtiene el árbol AVL de la figura 7.59.

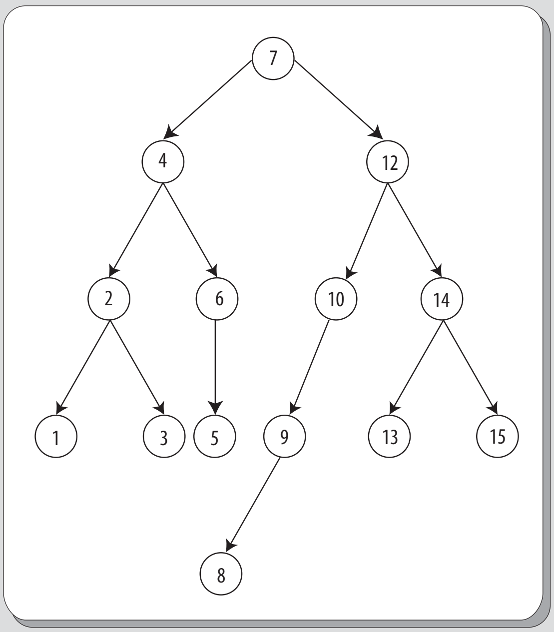


Figura 7.59 Árbol AVL de 15 vértices.

Resumen

En este capítulo se introduce el concepto de árbol y su estructura formal, que se utiliza en una gran variedad de aplicaciones de programación. El tipo de estructura de árbol que más se utiliza es el árbol binario. Se dice que un árbol es binario si cada uno de los vértices que lo componen tiene a lo más dos hijos. La altura de un árbol se define como la longitud máxima de todos los caminos que existen en el árbol desde la raíz. Los tipos de árboles binarios más utilizados en aplicaciones son los árboles de búsqueda, los de expresión y los balanceados o AVL.

Los **árboles de búsqueda** son estructuras que permiten la localización de una clave de búsqueda con una complejidad logarítmica. No obstante, para árboles degenerados, la eficiencia en la búsqueda deja de ser adecuada.

Los **árboles balanceados** o **AVL** son árboles de búsqueda en los que las longitudes de sus subárboles izquierdo y derecho difieren a lo más en 1. Esta característica hace que los árboles AVL optimicen el proceso de búsqueda. No obstante, las operaciones de inserción y eliminación en estos árboles son más costosas que en los árboles no equilibrados.

Problemas propuestos

En los problemas 7.1 a 7.8 conteste **V**, si el enunciado se refiere a un árbol, o **F** en caso contrario.

7.1 Contiene exactamente un circuito. [ ]

7.2 Es un grafo no conexo. [ ]

7.3 Un árbol de cinco vértices es isomorfo a K_5. [ ]

7.4 Un árbol con dos o más vértices tiene una hoja. [ ]

7.5 Es un grafo en que el número de lados es mayor que el número de vértices. [ ]

7.6 Es un grafo con $|E| = |V| - 1$ que no contiene circuitos. [ ]

7.7 Es un grafo en el que hay un único paseo entre cada par de vértices. [ ]

7.8 Es un grafo que es conexo. [ ]

En los problemas 7.9 a 7.17 complete el enunciado.

7.9 Un grafo dirigido es un árbol dirigido si se convierte en un árbol cuando se ignora __________.

7.10 Un vértice de un árbol con valencia igual a 1 se conoce como nodo __________.

7.11 Para que un grafo con vértices sea un árbol debe tener __________.

7.12 Para que un grafo con nueve lados sea un árbol tiene que tener __________.

7.13 Un vértice de un árbol enraizado con valencia de salida 0 se conoce como nodo __________.

7.14 Un vértice de un árbol enraizado con valencia de salida diferente de 0 se conoce como nodo __________.

7.15 Un vértice de un árbol enraizado con valencia de entrada 0 se conoce como nodo __________.

7.16 Un árbol donde cada nodo rama tiene exactamente m hijos se denomina __________.

7.17 Un árbol donde cada nodo rama tiene a lo más m hijos se denomina __________.

En los problemas 7.18 a 7.25 determinar si el conjunto dado es un código de prefijos.

7.18 {1, 001, 01, 010}

7.19 {1, 011, 010, 001, 000}

7.20 {1, 00, 01, 000, 0001}

7.21 {1, 01, 10, 000, 001}

7.22 {1, 01, 001, 000}

7.23 {1, 01, 10, 000, 001}

7.24 {11, 10, 01, 000, 001}

7.25 {1, 011, 010, 001, 000}

En los problemas 7.26 a 7.29 determinar si el grafo correspondiente es un árbol.

7.26

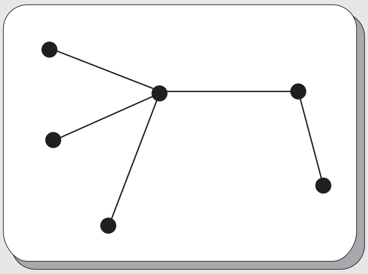


Figura 7.60

7.27

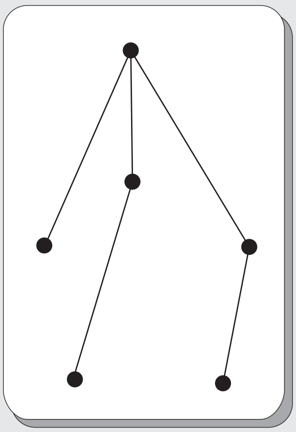


Figura 7.61

7.28

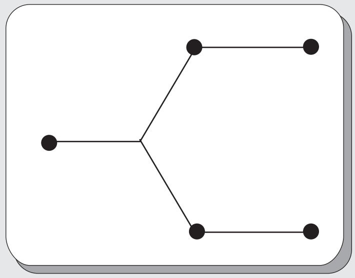


Figura 7.62

7.29

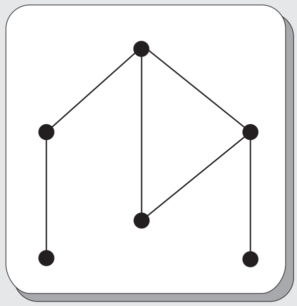


Figura 7.63

Para los problemas 7.30 a 7.33 considerar los siguientes árboles.

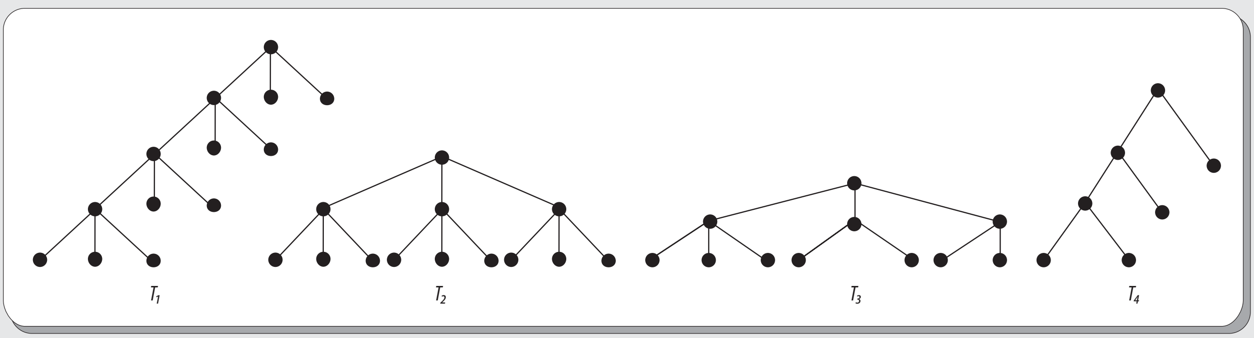


Figura 7.64

7.30 Todos son árboles m-arios regulares, **excepto**:

7.31 Es un árbol ternario de altura 4.

7.32 Es un árbol binario.

7.33 Son conexos.

Dados los siguientes árboles, contestar lo que se pide en los problemas 7.34 a 7.37.

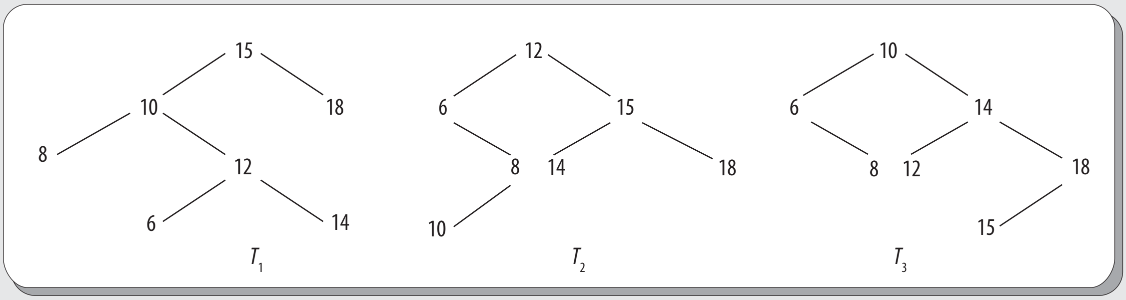


Figura 7.65

7.34 Es un árbol de búsqueda binaria.

7.35 Es un árbol binario.

7.36 Es un árbol binario regular.

7.37 Es un árbol enraizado.

Dado el siguiente grafo, contestar los problemas 7.38 a 7.41.

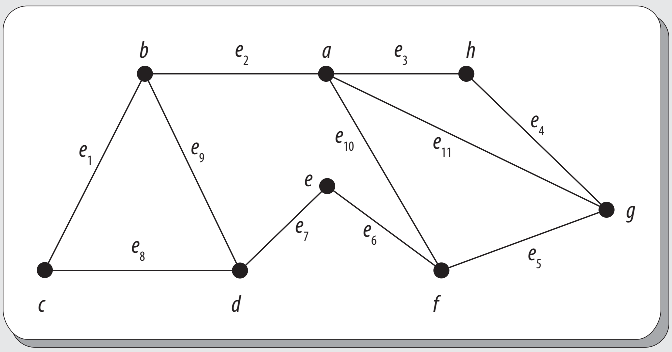


Figura 7.66

7.38 Dar un ejemplo de un árbol generador del grafo.

7.39 Dar un ejemplo de un conjunto de corte.

7.40 Dar un ejemplo de un árbol del grafo.

7.41 Si $\{e_1, e_2, e_3, e_4, e_5, e_7, e_9\}$ es un árbol de dicho grafo, encontrar su complemento.

8

Sistemas algebraicos

Objetivos

- Conocer los conceptos básicos de las estructuras algebraicas: grupos, anillos y campos.
- Manejar de modo eficiente las estructuras algebraicas básicas para comprender sus aplicaciones en informática, física, química y otras ciencias básicas.
- Conocer las aplicaciones de las estructuras algebraicas finitas en encriptación de información.

8.1 Introducción

El álgebra abstracta (o álgebra moderna) es la rama de las matemáticas que estudia las estructuras algebraicas conocidas como grupos, anillos, campos (también conocidos como cuerpos) y los espacios vectoriales. En la actualidad, todas estas estructuras son vistas como conjuntos dotados de operaciones que satisfacen ciertos axiomas, que juegan un papel fundamental en diversas aplicaciones de interés. A continuación se mencionan algunos ejemplos de las citadas aplicaciones:

1. Sistemas físicos, como los cristales y el átomo de hidrógeno, pueden ser modelados por grupos de simetría. De este modo, se puede decir que la teoría de grupos está en estrecha relación con diversas aplicaciones en la física y la química.
2. En la actualidad, los campos finitos de orden 2^n (campos binarios) han logrado especial importancia debido a sus múltiples aplicaciones en seguridad informática, como en la banca electrónica, las tarjetas inteligentes, la votación electrónica, etcétera.

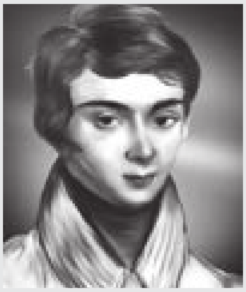


Figura 8.1 Évariste Galois (1811-1832), matemático francés.

Évariste Galois (Bourg-la-Reine 1811-París, 1832) matemático francés. Proveniente de una familia de políticos y juristas, Galois fue educado por sus padres hasta los 12 años, edad en que ingresó al College Royal de Louis-le-Grand, donde enseguida mostró extraordinarias aptitudes para las matemáticas.

A la edad de 16 años, interesado en hallar las condiciones necesarias para definir si una ecuación algebraica era susceptible de ser resuelta por el método de los radicales, empezó a esbozar lo que más adelante se conocería con el nombre de *teoría de Galois*, mediante el análisis de todas las permutaciones posibles de las raíces de una ecuación que cumplieran condiciones determinadas.

Mediante dicho proceso, que en terminología actual equivale al de hallar el grupo de automorfismos de un cuerpo, sentó las bases de la moderna teoría de grupos, una de las ramas más importantes del álgebra. Galois intuyó que la solubilidad mediante radicales estaba sujeta a la solubilidad del grupo de automorfismos relacionado.

A pesar de sus revolucionarios descubrimientos, o tal vez por esa misma causa, todas las memorias que publicó con sus resultados fueron rechazadas por la Academia de las Ciencias, algunas por matemáticos tan eminentes como Cauchy, Fourier o Poisson. Los fallidos intentos por ingresar a la Escuela Politécnica estuvieron acompañados de importantes fracasos, lo que le provocó una profunda crisis personal, agravada en 1829 por el suicidio de su padre.

Miembro activo de la oposición antimonárquica, se vio implicado en un duelo cuyos motivos aún hoy son confusos. Previendo su inminente muerte en el lance, trabajó con ahínco y dedicación en una especie de testamento científico que dirigió a su amigo Auguste Chevalier. A los pocos días tuvo lugar el duelo y el matemático, herido en el vientre, murió unas horas después, apenas cumplidos 21 años.

8.2 Grupos

La primera estructura algebraica que se analiza aquí se conoce como **grupo**. Un grupo consta de un conjunto G de objetos y una operación binaria * (que opera elementos por parejas) que satisface las siguientes cuatro condiciones (denominadas axiomas de grupo):

1. **Para todo $g_1, g_2 \in G$ se cumple $g_1 * g_2 \in G$.** A este axioma se le conoce como *cerradura* e implica, en términos generales, que el resultado de operar dos elementos del conjunto con la operación debe ser igual a otro elemento del mismo conjunto.
2. **Para todo $g_1, g_2, g_3 \in G$ se cumple $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.** A este axioma se le conoce como *asociatividad* e implica, en términos generales, que, dado que la operación es binaria (se realiza por parejas), al tener tres elementos operándose, existen dos opciones de operar por parejas, pero sin importar cual pareja se tome primero, el resultado es igual.
3. **Existe un elemento en G que se denota por e, que satisface $g * e = g$ para todo $g \in G$**. A este axioma se le conoce como *existencia del neutro* y tiene la característica peculiar de que cualquier elemento del conjunto que sea operado con este permanece invariante.

4. **Para todo $g \in G$ existe otro elemento g' también en G que satisface $g * g' = g' * g = e$.** A este axioma se le conoce como *existencia de los inversos* e implica, en términos generales, que cada elemento en el grupo contiene su inverso, es decir, un elemento que operado con g produce el elemento identidad e.

La forma correcta de referirse a un grupo es mediante la idea de conjunto y a la operación binaria definida en este. Esto se debe a que en un mismo conjunto se pueden definir diferentes operaciones binarias que satisfacen los axiomas de grupo, aunque es evidente que estos representan grupos diferentes. Para denotarlo se utiliza la notación <G,∗>.

EJEMPLO

Considérese el conjunto de los números enteros $\mathbb{Z}$. Como es conocido, la operación adición satisface ciertas propiedades en dicho conjunto, aunque en particular satisface los axiomas de grupo:

1. **Cerradura**. Si $n, m, \in \mathbb{Z}$ se cumple que $n + m \in \mathbb{Z}$. Es decir, la suma (resultado de la adición) de dos enteros siempre es otro entero.
2. **Asociatividad**. Si $n, m, k \in \mathbb{Z}$ se cumple que $(n + m) + k = n + (m + k)$.
3. **Existencia del neutro**. Existe un elemento, que se denota por 0, que satisface $n + 0 = 0 + n = n$ para todo entero n.
4. **Existencia de inversos**. Para cada entero existe otro entero $-n$, que satisface la relación $n + (-n) = (-n) + n = 0$.

Por tanto, el conjunto de los enteros con la operación adición es un grupo y se denota por $\langle \mathbb{Z}, + \rangle$.

Está claro que el conjunto de los enteros satisface una condición extra a los axiomas de grupo: la **conmutatividad**. En general, si <G,∗> es un grupo que satisface la condición de que $g_1 * g_2 = g_2 * g_1$ (conmutatividad) para todo par de elementos $g_1, g_2 \in G$ recibe el nombre de **grupo abeliano**, en honor al matemático Niels H. Abel, cuyo trabajo fue fundamental en la unificación de la teoría de grupos.

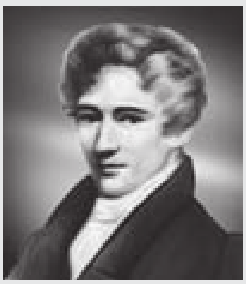


Figura 8.2 Niels Henrik Abel (Finnöy, 1802-Cristianía, 1829), matemático noruego.

Neils Henrik Abel (Finnöy, 1802-Cristiania, hoy Oslo, 1829), matemático norego. Hijo de un pastor protestante, creció en un ambiente familiar de gran tensión a causa del alcoholismo que padecía sus padres. Enviado junto con su hermano a una escuela de la capital, sus precoces aptitudes para las matemáticas fueron muy apreciadas por uno de sus profesores, Holmboe, quien tras la muerte de su padre le financió sus primeros años en la universidad.

La propuesta de Holmboe, C. Hansteen y otros profesores, Abel recibió por decreto real una beca de viaje. Así, entre 1000 825,827, conoció a los demás eminentes matemáticos de Alemania y Francia, y al mismo tiempo recibió la mayor parte de sus trabajos, los cuales se publicaron una revista alemana en matemáticasCrelles Journal. Entre los matemáticos de su tiempo, el profesor Degen, de Copenhague, y el consejero Crelle, de Berlín, fueron quienes de inmediato comprendieron la gran la grandeza de Abel. Crelle se encargó de Abel tuviera una plaza de profesor en Berlín, pero la tuberculosis pulmonar acabo con su vida antes de poder ejercer dicho cargo; y 1829, a la temprana edad de 27 años, moría este genial matemático.

Teniendo en cuenta su corta vida, la mente de Neils Henrik Abel fue sumamente por prolífica, y son numerosas sus aportaciones a las matemáticas. Vemos lo que las ecuaciones álgebra ica generales no pueden resolverse algebraica mente cuando son de grado superior al cuatro; estudio las funciones algebraica, las elípticas, las trascendentes de orden superior y las integrales definidas; estableció la doble periodicidad de las funciones elípticas y descubrió su teorema día adición; finalmente, descubre una nueva clase de ecuaciones, las llamadas ecuaciones abelianas.

EJEMPLO

Además de los números enteros, es fácil verificar que los siguientes pares forman grupos abelianos con la adición:

1. $\langle \mathbb{Q}, + \rangle$ Números racionales.
2. $\langle \mathbb{R}, + \rangle$ Números reales.
3. $\langle \mathbb{C}, + \rangle$ Números complejos.

El siguiente ejemplo permite aclarar por qué es tan importante hacer alusión al conjunto y a la operación para denotar un grupo.

EJEMPLO

En el ejemplo anterior se especifica que el conjunto de los números reales forma, a su vez, un grupo con la operación adición. No obstante, el mismo conjunto no forma un grupo con la multiplicación. Para comprobarlo, basta con ver que los primeros tres axiomas de grupo se satisfacen para todo número real, donde destaca el 1, que es el neutro, pues $1 \cdot a = a \cdot 1 = a$ para todo número real a. Sin embargo, para el 0 no existe inverso multiplicativo, pues no existe ningún número real que multiplicado por 0 sea igual a 1; es decir, la ecuación $0 \cdot x = 1$ no tiene solución en los números reales. Por tanto, debido a que no se satisface el axioma 4 para todos los números reales con la multiplicación se concluye que dicho par no forma un grupo.

EJEMPLO

Del ejemplo anterior es fácil ver que los números racionales y los números complejos no forman un grupo con la multiplicación; no obstante, debido a que lo único que falla es la no existencia del inverso multiplicativo para el 0, es evidente que los siguientes conjuntos sí forman grupos abelianos con la multiplicación:

$\langle \mathbb{Q}^*, \cdot \rangle$ Números racionales sin el cero.

$\langle \mathbb{R}^*, \cdot \rangle$ Números reales sin el cero.

$\langle \mathbb{C}^*, \cdot \rangle$ Números complejos sin el cero.

Es importante destacar que los grupos no se limitan a conjuntos de números; aunque hasta ahora solo se han abordado estos por constituir los ejemplos más comunes, hay una diversidad de ejemplos importantes de grupos en geometría, análisis, etcétera. A continuación se presenta un ejemplo de estos casos.

EJEMPLO

Considérese un triángulo equilátero en el plano y sea G el conjunto de todas las rotaciones del triángulo en el plano que lo dejan sin cambio. Es fácil ver que el conjunto G consta de tres rotaciones: 120°, 240° y 360° (véase figura 8.3).

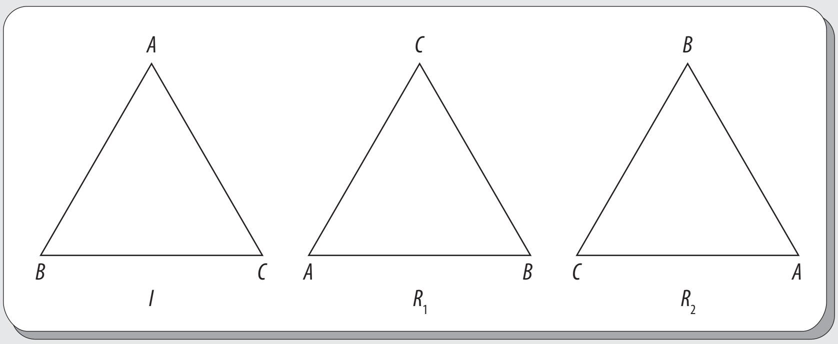


Figura 8.3 Rotaciones que dejan invariante a un triángulo equilátero.

La rotación de 360° deja al triángulo en su posición original; por tanto, esta rotación es el elemento identidad (I). La rotación de 240° (I) equivale a rotar 2 veces 120° R_1. La operación definida en G se denota por el símbolo ° y se denomina *composición de rotaciones*. Como se puede observar, $R_1 \circ R_2 = R_2 \circ R_1 = \mathrm{I}$ pues $R_1 \circ R_2$ consiste en rotar el triángulo en 240° y luego en 120° y $R_2 \circ R_1$ equivale a rotar el triángulo en 120° y luego en 240°. Es fácil ver aquí que los cuatro axiomas de grupo se satisfacen para en G, por lo que $\langle G, \circ \rangle$ es un grupo.

En la siguiente lista de teoremas se destacan algunas de las propiedades más importantes en un grupo.

Teorema 8.1

Sea $\langle G, * \rangle$ un grupo y sean $g_1, g_2, g_3 \in G$. Entonces:

1. Si $g_1 * g_2 = g_1 * g_3$, se tiene que $g_2 = g_3$ (**Ley de cancelación por la izquierda**).
2. Si $g_2 * g_1 = g_3 * g_1$, se tiene que $g_2 = g_3$ (**Ley de cancelación por la derecha**).

DEMOSTRACIÓN

En primer lugar, supóngase que se cumple la igualdad:

$$g_1 * g_2 = g_1 * g_3 \;\; \text{R1 ° R2}$$

Como $\langle G, *\rangle$ es un grupo, por el axioma 4 existe g_1^{-1} y aplicando en ambos lados de la igualdad se tiene:

$$g_1^{-1} * (g_1 * g_2) = g_1^{-1} * (g_1 * g_3)$$

Ahora, al aplicar la ley asociativa se tiene:

$$(g_1^{-1} * g_1) * g_2 = (g_1^{-1} * g_1) * g_3$$
$$e * g_2 = e * g_3$$
$$g_2 = g_3$$

La demostración para el caso 2 es equivalente; por lo que se deja como ejercicio para el lector.

Teorema 8.2
Sea $\langle G, *\rangle$ un grupo. Entonces, el elemento neutro es único.

DEMOSTRACIÓN

Supóngase que existen dos elementos $e_1, e_2 \in G$ que satisfacen:

$$e_1 * g = g * e_1 = g$$
$$e_2 * g = g * e_2 = g$$

Para todo g en G. Entonces, se tiene que:

$$e_1 = e_1 * e_2 = e_2$$

de donde se concluye que $e_1 = e_2$; luego entonces, el elemento neutro es único.

Teorema 8.3
Sea $\langle G, *\rangle$ un grupo y $g \in G$. Entonces, existe un único inverso para g.

DEMOSTRACIÓN

Supóngase que existen dos elementos $g^{-1}, g'^{-1} \in G$ que satisfacen:

$$g^{-1} * g = g * g^{-1} = e$$
$$g'^{-1} * g = g * g'^{-1} = e$$

Entonces, se tiene que:

$$g * g^{-1} = g * g'^{-1} = e$$

y al aplicar la ley de cancelación por la izquierda se tiene:

$$g^{-1} = g'^{-1}$$

Esto es, el inverso de cualquier elemento g en un grupo $\langle G, *\rangle$ es único.

Cuando el conjunto en cuestión es finito, existe la posibilidad de representar la operación binaria definida en este mediante una tabla. Para la construcción de dicha tabla, primero se acomodan los elementos del grupo en un cierto orden, tanto en el lado izquierdo como en la parte superior de la tabla. Mientras que en la intersección del renglón i-ésimo con la columna j-ésima se coloca el resultado de:

(elemento i-ésimo $*$ elemento j-ésimo)

EJEMPLO

El grupo finito más simple es el que consta de un solo elemento, el cual debe ser el elemento neutro (grupo trivial). Por su parte, el primer caso no trivial es el grupo de dos elementos $G = \{e, g\}$, donde se asume que *e* es el elemento neutro necesario en cualquier grupo. En este caso, para construir la tabla de grupo se elige algún orden para los elementos de, por ejemplo, *e*, *g*, y se acomodan en la tabla en dicho orden (véase tabla 8.1).

Tabla 8.1 Orden para los elementos de G.

*	e	g
e		
g		

Como se puede observar, en la primera fila y la primera columna de esta tabla los elementos se repiten, ya que es el neutro y, por tanto, se debe cumplir:

$$e * e = e$$

$$e * g = g * e = g$$

Es decir:

Tabla 8.2 Acomodo parcial de la tabla para los elementos G.

*	e	g
e	e	g
g	g	e

Por último, *g* debe tener su elemento inverso en *G*, es decir debe existir un elemento que operado con *g* dé como resultado el neutro. Para este caso es evidente que la única opción es que *g* sea su propio inverso (pues *e* no funciona); esto es, que $g * g = e$. Por tanto, la tabla de grupo se muestra en la tabla 8.3.

Tabla 8.3 Tabla de grupo

*	e	g
e	e	g
g	g	e

Por construcción, la tabla anterior en automático satisface los axiomas de grupo 1, 3 y 4. Por tanto, se deja al lector verificar que la tabla construida así, también satisface el axioma 2 de grupos (asociatividad).

Del ejemplo anterior, por intuición se deduce que, a excepción del acomodo y el nombre de los elementos, solo existe una forma de construir la tabla de un grupo de cardinalidad 2. La observación anterior da lugar a un importante concepto en álgebra que se denomina: "isomorfismo de grupos". Este concepto es tan importante que se ha decidido dedicar la sección 8.3 a su estudio.

EJEMPLO

Con base en la misma idea tratada en el ejemplo anterior, en este ejemplo se busca construir un grupo de tres elementos. Así, por el axioma 3 de grupo, uno de los elementos de *G* debe ser el neutro; por tanto, *G* se denota en la forma:

$$G = \{e, g_1, g_2\}$$

El orden en que aparecen los elementos en G se muestra en la tabla 8.4.

Tabla 8.4 Orden para los elementos de G.

$*$	e	g_1	g_2
e			
g_1			
g_2			

Considerando que e es el neutro, la primera fila y la primera columna deben ser idénticas.

Tabla 8.5 Acomodo parcial de la tabla para los elementos G.

$*$	e	g_1	g_2
e	e	g_1	g_2
g_1	g_1		
g_2	g_2		

Pero, para llenar los cuatro lugares restantes y que se satisfagan los axiomas de grupo, la única opción es la que se observa en la tabla 8.6.

Tabla 8.6 Tabla de grupo.

$*$	e	g_1	g_2
e	e	g_1	g_2
g_1	g_1	g_2	e
g_2	g_2	e	g_1

Se deja como ejercicio para el lector probar que la tabla así construida satisface los axiomas de grupo.

Una observación importante acerca de las dos tablas de grupo construidas en ambos ejemplos es que cada elemento (sin tomar en cuenta los encabezados, primera fila y primera columna) aparece exactamente una vez por fila y por columna. Lo anterior no es casualidad, es una consecuencia de que, en un grupo, las ecuaciones siguientes tienen exactamente una y solo una solución.

$$g_1 * x = g_2$$
$$y * g = e$$

Este resultado es fácil de probar, considérese $x = g_1^{-1} * g_2$; sustituyendo en $g_1 * x = g_2$ se obtiene;

$$g1 * \left(g_1^{-1} * g_2\right) = \left(g1 * g_1^{-1}\right) * g_2 = e * g_2 = g_2$$

De donde se concluye que $g_1^{-1} * g_2$ es una solución, que además es única, debido a que los inversos en un grupo son únicos (teorema 8.3).

Grupos de congruencias

Una clase especial de grupos finitos, debido a sus múltiples aplicaciones en electrónica, informática, criptografía, entre otras disciplinas, son los **grupos de congruencias módulo**. Recuérdese que un número entero X

se dice congruente con un entero módulo n, lo que se denota por $x \equiv y \bmod(n)$ si la diferencia $x - y$ es un múltiplo de n; en símbolos:

$$x \equiv y \bmod(n) \text{ si y solo si } x - y = nk, \text{ con } k \in \mathbb{Z}$$

La relación de congruencias módulo n es una relación de equivalencia y por tanto genera una partición del conjunto $\mathbb{Z}$ en clases de equivalencia. Las clases de equivalencia se denotan por:

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

donde la clase $[x]$ es el conjunto de todos los números enteros "y" tal que $x - y$ es múltiplo de n, es decir:

1. $[0] = \{0, n, -n, 2n, -2n, \ldots\}$, ya que las diferencias $0 - n, 0 - 2n, 0 - (-2n), \ldots$, son múltiplos de n.
2. $[1] = \{1, n+1, -n+1, 2n+1, -2n+1, \ldots\}$, ya que las diferencias $1-(-2n+1), \ldots$, son múltiplos de n.

EJEMPLO

Para el caso de las cuatro clases de equivalencia son:

$$[0] = \{0, 4, -4, 8, -8, \ldots\},$$
$$[1] = \{1, 5, -3, 9, -7, \ldots\},$$
$$[2] = \{2, 6, -2, 10, -6, \ldots\},$$
$$[3] = \{3, 7, -1, 11, -5, \ldots\}.$$

De la forma de las clases de equivalencia del ejemplo anterior, se puede observar que la unión de estas es todo el conjunto de números enteros y que son disjuntas entre sí.

Con las clases de congruencias módulo n es posible definir dos operaciones importantes: *adición de clases* y *multiplicación de clases*, de la siguiente forma:

$$[x] + [y] = [x + y] \text{ y } [x] \cdot [y] = [xy]$$

A continuación, se enuncian dos teoremas (se omite la demostración) del conjunto de clases de congruencias módulo n con las dos operaciones definidas para las clases.

Teorema 8.4
El conjunto $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ es un grupo abeliano con la adición de clases, donde el neutro aditivo es $[0]$

Teorema 8.5
Si p es un número primo, entonces el conjunto $\mathbb{Z}_p^* = \{[1], \ldots, [p-1]\}$ es un grupo abeliano con la multiplicación de clases, donde el neutro multiplicativo es $[1]$.

EJEMPLO

Considérese el conjunto $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. De acuerdo con el teorema 8.4, este conjunto forma un grupo con la adición de clases. En la tabla 8.7 se muestra la tabla de grupo.

Tabla 8.7 Tabla de grupo con la adición

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

EJEMPLO

Considérese el conjunto $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$. De acuerdo con el teorema 8.5, este conjunto forma un grupo con la multiplicación de clases. En la tabla 8.8 se muestra la tabla de grupo.

Tabla 8.8 Tabla de grupo con la multiplicación

+	[1]	[2]	[3]	[4]
[0]	[1]	[2]	[3]	[4]
[1]	[2]	[2]	[1]	[3]
[2]	[3]	[1]	[0]	[2]
[3]	[4]	[3]	[2]	[1]

Grupos cíclicos

Otra clase especial de grupos es el que está constituido por aquellos grupos que pueden ser generados completamente por un solo elemento; a tales grupos se les denomina **grupos cíclicos**. De manera formal, si $\langle G, *\rangle$ es un grupo en el cual existe un elemento $x \in G$, tal que:

$$G = \{x^n \; t \cdot q \cdot n \in \mathbb{Z}\}$$

donde x^n representa a x operado consigo mismo n veces.

EJEMPLO

Considérese el conjunto $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. En la sección anterior se afirma que $\langle \mathbb{Z}_4, +\rangle$ es un grupo de congruencias, pero además es un grupo cíclico, pues el [1] genera todo $\mathbb{Z}_4$; a saber:

$$[1]$$
$$[1]+[1]=[2],$$
$$[1]+[1]+[1]=[3],$$
$$[1]+[1]+[1]+[1]=[0]$$

EJEMPLO

El grupo $\langle \mathbb{Z}_5^*, \cdot\rangle$ es además un grupo cíclico, pues el [2] genera todo $\mathbb{Z}_5^*$,; a saber:

$$[2]$$
$$[2]+[2]=[4]$$
$$[2]+[2]+[2]=[3]$$
$$[2]+[2]+[2]+[2]=[1]$$

Teorema 8.6
Cualquier grupo $\langle G, *\rangle$ cíclico es abeliano.

DEMOSTRACIÓN

Sea $\langle G, *\rangle$ cíclico. Entonces, como $\langle G, *\rangle$ es cíclico existe al menos un elemento en x en G que lo genera; es decir:

$$G = \{x^n \; t \cdot q \cdot n \in \mathbb{Z}\}$$

Para probar que $\langle G, *\rangle$ es abeliano se debe demostrar que para cualquier par de elementos $g_1, g_2 \in G$ se cumple que $g_1 * g_2 = g_2 * g_1$. En efecto, como x genera todo G se tiene que:

$$g_1 = x^{n_1} \text{ y } g_2 = x^{n_2}$$

de donde:

$$g_1 * g_2 = x^{n_1} * x^{n_2} = x^{n_1+n_2} = x^{n_1+n_2} = x^{n_2} * x^{n_1} = g_2 * g_1$$

Teorema 8.7
Todo subgrupo (véase sección 8.3) de un grupo cíclico es cíclico.

DEMOSTRACIÓN

Sea $\langle G, *\rangle$ cíclico y sea H un subgrupo de G. Entonces, como $\langle G, *\rangle$ es cíclico existe al menos un elemento en x en G que lo genera. Si H consta solo del elemento identidad, entonces H es cíclico.

En otro caso, si H consta de más de un elemento, es necesario encontrar un generador para H. Como H es subgrupo de G sus elementos son de la forma x^n. Sea m el entero positivo más pequeño tal que $x^m \in H$; entonces, este elemento debe ser el generador buscado. Es decir, cualquier otro elemento $y = x^n$ de H debe ser una potencia de x^m. Para demostrar esta última afirmación se puede utilizar el algoritmo de la división para escribir n:

$$n = mq + r$$

donde el residuo r satisface $0 \leq r \leq m$; entonces:

$$x^n = x^{mq+r} = \left(x^m\right)^q x^r$$

Y al despejar x^r se tiene:

$$x^r = \left(x^m\right)^{-q} x^n$$

Como $x^n \in H$ y $x^m \in H$ y H es un subgrupo, necesariamente:

$$\left(x^m\right)^{-q} x^n = x^r \in H$$

Por último, como m se eligió como el menor entero positivo, tal que $x^m \in H$ y $0 \leq r \leq m$, la única opción es que r $=$ 0; por tanto:

$$x^n = \left(x^m\right)^q$$

Grupos de permutaciones

En matemáticas de la simetría existe otra clase importante de grupos denominados **grupos de permutaciones.** Con el fin de dar una introducción al concepto estructura algebraica de permutaciones, supóngase que hay un conjunto de seis objetos acomodados en un cierto orden inicial, los cuales pueden ser etiquetados con los enteros 1, 2, 3, 4, 5 y 6. Este arreglo inicial, que se denota por l (permutación identidad), se representa de la siguiente manera:

$$I = \begin{pmatrix} 123456 \\ 123456 \end{pmatrix}$$

Para representar una permutación de elementos se usa la letra f, considerando que cada permutación puede verse como una función de un conjunto al conjunto mismo. Los cambios se representan en el renglón inferior, con lo cual se deja invariante el renglón de arriba; es decir, el renglón de arriba representa el dominio de f, mientras que el renglón de abajo representa la imagen. Por ejemplo, si se considera:

$$f(1) = 2,\ f(2) = 5,\ f(3) = 1,\ f(4) = 3,\ f(5) = 4,\ f(6) = 6$$

Se representa mediante:

$$f = \begin{pmatrix} 123456 \\ 251346 \end{pmatrix}$$

Ahora, es posible llevar a cabo una *sucesión de permutaciones*, lo que se puede expresar como una *composición de funciones* o, más específico, como una *composición de permutaciones*.

EJEMPLO

Para llevar a cabo la composición de permutaciones $f \circ g$, con:

$$f\begin{pmatrix} 123456 \\ 251346 \end{pmatrix}, g = \begin{pmatrix} 123456 \\ 214365 \end{pmatrix}$$

se lleva a cabo como una composición de funciones estándar, es decir:

$$f \circ g(x) = f(g(x))$$

De modo explícito, al recorrer los seis valores se obtiene:

$$f(g(1)) = f(2) = 5$$
$$f(g(2)) = f(1) = 2$$
$$f(g(3)) = f(4) = 3$$
$$f(g(4)) = f(3) = 1$$
$$f(g(5)) = f(6) = 6$$
$$f(g(6)) = f(5) = 4$$

Por último, se representa por:

$$f \circ g = \begin{pmatrix} 123456 \\ 523164 \end{pmatrix}$$

Es muy simple obtener la **permutación inversa** de una permutación dada mediante la representación que se ha utilizado. A continuación, se ilustra esto mediante un ejemplo.

Ejemplo

Encontrar f^{-1}, con:

$$f = \begin{pmatrix} 12345 \\ 25134 \end{pmatrix}$$

Solución

Para construir la función inversa de f, se busca una permutación que anule el efecto de f; es decir, $f^{-1} \circ f = I$:

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = x$$

De modo explícito, al recorrer los cinco valores se obtiene:

$$f^{-1}(f(1)) = f^{-1}(2) = 1$$
$$f^{-1}(f(2)) = f^{-1}(5) = 2$$
$$f^{-1}(f(3)) = f^{-1}(1) = 3$$
$$f^{-1}(f(4)) = f^{-1}(3) = 4$$
$$f^{-1}(f(5)) = f^{-1}(4) = 5$$

Por último, se representa por:

$$f^{-1} = \begin{pmatrix} 12345 \\ 31452 \end{pmatrix}$$

EJEMPLO

Verifique que la permutación:

$$f^{-1} = \begin{pmatrix} 12345 \\ 31452 \end{pmatrix}$$

es la inversa de la permutación:

$$f = \begin{pmatrix} 12345 \\ 25134 \end{pmatrix}$$

Es suficiente con mostrar que la composición de permutaciones produce la permutación identidad; es decir, $f^{-1} \circ f = I$

De modo explícito, al recorrer los cinco valores se obtiene:

$$f^{-1}(f(1)) = f^{-1}(2) = 1$$
$$f^{-1}(f(2)) = f^{-1}(5) = 2$$
$$f^{-1}(f(3)) = f^{-1}(1) = 3$$
$$f^{-1}(f(4)) = f^{-1}(3) = 4$$
$$f^{-1}(f(5)) = f^{-1}(4) = 5$$

Entonces:

$$f^{-1} = \begin{pmatrix} 12345 \\ 12345 \end{pmatrix} = I$$

Resulta importante destacar que existe una notación extra para representar permutaciones, que se conoce como **notación cíclica**. Para explicar esta notación, considérese que se cuenta con un tablero de ajedrez en el cual se ubican un alfil en la posición 1, una torre en la posición 2 y un caballo en la posición 3. Supóngase, además, que se lleva a cabo la siguiente permutación: se mueve el alfil de la posición 1 a la posición 2, la torre de la posición 2 a la posición 3 y el caballo de la posición 3 a la posición 1 (véase figura 8.4)

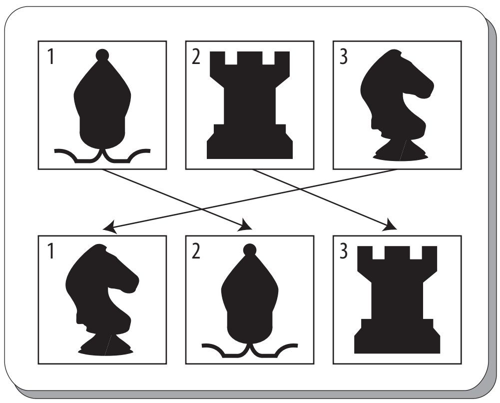


Figura 8.4 Ilustración que representa la notación cíclica.

La notación para representar esta permutación es (1, 2, 3), que se lee: el objeto ubicado en la posición 1 se permuta a la posición 2; el objeto ubicado en la posición 2 se permuta a la posición 3; el objeto ubicado en la posición 3 se permuta a la posición 1.

En general, un ciclo de longitud n de la forma $(x_1, x_2, \ldots, x_n)$ es un ciclo correspondiente a la permutación:

$$\begin{matrix} x_1 & x_2 & x_3 \cdots x_n \\ x_2 & x_3 & x_4 \cdots x_1 \end{matrix}$$

Cualquier permutación con un conjunto finito de elementos siempre se puede escribir como un producto de ciclos disjuntos. Mediante la notación cíclica, es posible construir una tabla de grupo para resumir las operaciones. Por ejemplo, el conjunto de todas las permutaciones de tres objetos se denomina grupo simétrico S_3. El elemento identidad que en notación cíclica se representa simplemente como (1) y el resto de las permutaciones son: (1, 2, 3), (1, 3, 2), (1, 2), (1, 3) y (2, 3).

El grupo de permutaciones de tres objetos es el que describe todas las permutaciones posibles entre las tres piezas (el alfil, la torre y el caballo) de la figura 8.4.

La tabla de grupo

Obsérvese la parte sombreada en color gris oscuro de la tabla; esta sección se resaltó porque por sí sola forma un grupo; es decir, es un subgrupo del grupo $\langle S_3, \circ \rangle$ (véase sección 8.3). Este es un subgrupo conocido como el grupo A_3 y se denomina **grupo alternante** de tres elementos. Los grupos alternantes son aquellos que consisten únicamente de todas las permutaciones que reciben el nombre de *pares*, que es el tema de estudio de la siguiente sección.

Tabla 8.9 Tabla de grupo para (S_3, o)

$\circ$	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(23)	(12)	(13)
(132)	(132)	(1)	(123)	(13)	(23)	(12)
(12)	(12)	(13)	(23)	(1)	(123)	(132)
(13)	(13)	(23)	(12)	(132)	(1)	(123)
(23)	(23)	(12)	(13)	(123)	(132)	(1)

8.3 Subgrupos

Toda vez que se consideran varios ejemplos de grupos, es común encontrar el caso en que algunos de estos están dentro de otros. Esta importante observación da lugar al siguiente concepto matemático: si $\langle G, * \rangle$ y $\langle H, * \rangle$ son dos grupos con la misma operación binaria $*$ y $H \quad G$ se dice que ***H*** es **subgrupo** de **G** y se denota por $H \leq G$. Cabe aclarar que no es suficiente con que un conjunto contenga al otro, es necesario que formen grupo con la misma operación. Entonces, un subconjunto H de un grupo $\langle G, * \rangle$ se dice que es subgrupo de si forma por si solo un grupo con la misma operación $*$.

Para un grupo $\langle G, * \rangle$ se tiene que $G \leq G$ y que $\{e\} \leq G$. Es decir, cada grupo es subgrupo de sí mismo y el elemento neutro también forma un subgrupo de G. A estos dos subgrupos se les conoce como *subgrupo impropio* y *subgrupo trivial*, respectivamente.

EJEMPLO

En la sección anterior se destacan varios ejemplos de grupos, entre los cuales aparecen $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{C}, + \rangle$. De acuerdo con la definición de subgrupo es fácil notar que se cumple:

$$\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{Q}, + \rangle \leq \langle \mathbb{R}, + \rangle \leq \langle \mathbb{C}, + \rangle$$

EJEMPLO

Considere los grupos $\langle \mathbb{Q}^*, \cdot \rangle$ y $\langle \mathbb{R}, + \rangle$. Es claro que $\mathbb{Q}^* \; \mathbb{C} \; \mathbb{R}$; no obstante, $\langle \mathbb{Q}^*, \cdot \rangle$ no es un subgrupo de $\langle \mathbb{R}, + \rangle$ pues son grupos con operaciones distintas.

EJEMPLO

Considérese el conjunto de todas las matrices invertibles de números reales de tamaño 2×2. Este conjunto, a su vez, forma un grupo con la multiplicación matricial, al que se conoce como grupo general lineal y se denota por $\langle GL_2(\mathbb{R}), \cdot \rangle$. El conjunto de todas las matrices de números reales de tamaño 2×2 con determinante igual a 1 es un subgrupo de $\langle GL_2(\mathbb{R}), \cdot \rangle$. El subgrupo en cuestión se conoce como grupo especial lineal y se denota por $\langle SL_2(\mathbb{R}), \cdot \rangle$.

EJEMPLO

Considérese el grupo $\langle \mathbb{Z}_{12}, + \rangle$. Entonces el conjunto $\{[0], [3], [6], [9]\}$ es un subgrupo de $\mathbb{Z}_{12}$ y su tabla de grupo se muestra en la tabla 8.10.

Tabla 8.10 Tabla de grupo para $\langle \mathbb{Z}_{12}, + \rangle$.

$+$	**[0]**	**[3]**	**[6]**	**[9]**
[0]	[0]	[3]	[6]	[9]
[3]	[3]	[6]	[9]	[0]
[6]	[6]	[9]	[0]	[3]
[9]	[9]	[0]	[3]	[6]

8.4 Isomorfismo de grupos

En la sección 8.2 se construyen tablas para grupos de orden 2 y orden 3. En dicho proceso y buscando que se cumplieran los axiomas de grupo, resultó ser única la forma de construir la tabla. Si se toma en cuenta que se manejan conjuntos y operaciones arbitrarias, se puede pensar en que solo existe, en esencia, un único grupo de orden 2 y un único grupo de orden 3. En efecto, cualquier grupo de orden 2 (o de orden 3) es estructuralmente único. En esta sección se establece de manera formal cuando dos grupos son estructuralmente idénticos (isomorfos).

Se dice que dos grupos $\langle G, * \rangle$ y $\langle G', \circ \rangle$ son **isomorfos**, si existe una función biyectiva *f* de G a G' que satisface la condición:

$$f(g_1 * g_2) = f(g_1) \circ f(g_2)$$

A la función *f* se le conoce como isomorfismo entre G y G'.

La condición de biyectividad garantiza que cada elemento del grupo G puede ser apareado con un elemento del grupo G'; de manera burda, esto significa que G tiene tantos elementos como G'. Por otro lado, la condición $f(g_1 * g_2) = f(g_1) \circ f(g_2)$ garantiza que la estructura dada por la operación ∘ en G es idéntica a la estructura dada por la operación ∘ en G' (a excepción del "nombre" de los elementos y del "nombre" de la operación).

EJEMPLO

Sean los grupos $\langle \mathbb{R}, + \rangle$ (números reales con la adición) y $\langle \mathbb{R}^+, \cdot \rangle$ (números reales positivos con la multiplicación). Además, considérese la función $f : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle$: definida por $f(x) = e^x$. A continuación, se demuestra que *f* define un isomorfismo de grupos:

1. $f(x) = f(y)$, si y solo si $e^x = e^y$ si y solo si $x = y$ por tanto, *f* es inyectiva.
2. Si $y \in \boxtimes^+$, entonces $f(\ln(y)) = e^{\ln(y)} = y$, donde $\ln(y) \in \mathbb{R}$; por tanto, *f* es sobreyectiva.
3. Sean $x, y \in \boxtimes$, entonces $f(x + y) = e^{x+y} = e^x e^y = f(x) \cdot f(y)$

De los puntos 1, 2 y 3 se concluye que *f* es un isomorfismo; por tanto, los grupos $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{R}^+, \cdot \rangle$ son estructuralmente idénticos (isomorfos).

La primera imagen que por lo general se tiene al comenzar con isomorfismo de grupos es que si son estructuralmente idénticos, entonces son de igual tamaño. No obstante, en grupos isomorfos infinitos, la frase *de igual tamaño* se debe cambiar por *tiene tantos elementos como el otro*. El ejemplo anterior ilustra esta situación: $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{R}^+, \cdot \rangle$ son *ma*[illegible] de $\mathbb{R}$.

EJEMPLO

Sean los grupos $\langle \mathbb{Z}, +\rangle$ (números enteros con la adición) y $\langle 3\mathbb{Z}, +\rangle$ (múltiplos enteros de 3 con la adición). Además, considérese la función $f : \langle \mathbb{Z}, +\rangle \to \langle 3\mathbb{Z}, +\rangle$: definida por $f(n) = 3n$. A continuación, se demuestra que f define un isomorfismo de grupos:

1. $f(n) = f(m)$ si y solo si $3n = 3m$ si y solo si $n = m$; por tanto, f es inyectiva.
2. Si $m \in 3\mathbb{Z}$, entonces m es un múltiplo entero de 3; es decir, es de la forma $m = 3k$, con $k \in \mathbb{Z}$; por tanto, como $k \in \mathbb{Z}$ se tiene que $f(k) = 3k = m$ luego, f es sobreyectiva.
3. Sean $m, n \in \mathbb{Z}$, entonces $f(m+n) = 3(m+n) = 3m + 3n = f(m) + f(n)$.

De los puntos 1, 2 y 3 se concluye que f es un isomorfismo; por tanto, los grupos $\langle \mathbb{Z}, +\rangle$ y $\langle 3\mathbb{Z}, +\rangle$ son isomorfos.

Cuando dos grupos son isomorfos, estos deben tener las mismas propiedades estructurales; es decir, si uno es abeliano el otro debe serlo, y si uno es cíclico el otro debe serlo, etcétera.

EJEMPLO

Considérense los grupos $\langle \mathbb{Z}, +\rangle$ y $\langle \mathbb{Q}, +\rangle$. Entonces, estos grupos no son isomorfos, pues mientras $\langle \mathbb{Z}, +\rangle$ es un grupo cíclico (con generador 1) $\langle \mathbb{Q}, +\rangle$ no lo es.

En la sección 8.1 se construyen los grupos de 1, 2 y 3 elementos. En ese punto se señala que su construcción es única, ahora se puede decir que son únicos salvo isomorfismos. Para el caso de cuatro elementos, existen dos grupos (salvo isomorfismos) que son estructuralmente diferentes. Uno de estos corresponde al grupo de congruencias $\langle \mathbb{Z}_4, +\rangle$ y el otro es el llamado grupo de Klein. A continuación, se muestran las tablas de grupo de ambos grupos.

1. Grupo $\langle \mathbb{Z}_4, +\rangle$ (véase tabla 8.11)

Tabla 8.11 Tabla de grupo para $\langle \mathbb{Z}_4, +\rangle$.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

2. Grupo de Klein (véase tabla 8.12)

Tabla 8.12 Tabla de grupo de Klein.

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[0]	[3]	[2]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[2]	[1]	[0]

Luego de observar las tablas de grupo resulta evidente que no son isomorfos, pues en el grupo de Klein cada elemento es su propio inverso, mientras que el grupo $\langle \mathbb{Z}_4, +\rangle$ no.

8.5 Grupos cociente

Es posible estudiar un grupo $\langle G, *\rangle$ a partir de sus subgrupos propios, lo cual resulta conveniente debido a que estos subgrupos tienen orden inferior al orden de G. Con este propósito, se define la siguiente relación de equivalencia. Si H es un subgrupo propio de G se define la relación:

$$x \equiv y(H) \text{ si y solo si } \left(x^{-1} * y\right) \in H$$

El conjunto de clases de equivalencia que se obtiene a partir de esta relación se denota por G/H y se conoce como ***conjunto cociente***. Para que el conjunto cociente pueda tener estructura de grupo es necesario, además de definir la operación de clases, que H sea un subgrupo normal; esto es, se dice que un subgrupo $\langle H, *\rangle$ de un grupo $\langle G, *\rangle$ es **normal,** y se denota por $H \triangleleft G$, si $(x * H) * (y * H) = (x * y) * H$. Aquí, $x * H$ significa operar x con todos los elementos de H, es decir:

$$x * H = \{x * h \text{ t} \cdot \text{q} \cdot h \in H\}$$

EJEMPLO

Para el grupo de los enteros con la adición $\langle \mathbb{Z}, +\rangle$ se toma el subgrupo $\langle 5\mathbb{Z}, +\rangle$ (conjunto de enteros múltiplos de 5). A continuación, se demuestra que $\langle 5\mathbb{Z}, +\rangle \triangleleft \langle \mathbb{Z}, +\rangle$.

Si x, y son enteros, entonces:

$$x + 5\mathbb{Z} = \{x + 5k \text{ t} \cdot \text{q} \cdot k \in \mathbb{Z}\} \text{ y } y + 5\mathbb{Z} = \{y + 5k \text{ t} \cdot \text{q} \cdot k \in \mathbb{Z}\}$$

De lo anterior queda claro que:

$$\begin{aligned}(x + 5\mathbb{Z}) + (y + 5\mathbb{Z}) &= \{(x + 5k) + (y + 5m) \text{ t} \cdot \text{q} \cdot k, m \in \mathbb{Z}\} \\ &= \{(x + y) + 5(k + m) \text{ t} \cdot \text{q} \cdot k, m \in \mathbb{Z}\} \\ &= \{(x + y) + 5k_1 \text{ t} \cdot \text{q} \cdot k_1 \in \mathbb{Z}\} \\ &= (x + y) + 5\mathbb{Z}\end{aligned}$$

Por tanto:

$$(x + 5\mathbb{Z}) + (y + 5\mathbb{Z}) = (x + y) + 5\mathbb{Z}$$

Y así:

$$\langle 5\mathbb{Z}, +\rangle \triangleleft \langle \mathbb{Z}, +\rangle$$

El ejemplo anterior es un caso particular del siguiente resultado. Si $\langle G, *\rangle$ es un grupo abeliano y $\langle H, *\rangle \leq \langle G, *\rangle$ entonces $H \triangleleft G$; es decir, cualquier subgrupo de un grupo abeliano es normal. Además, si $\langle G, *\rangle$ es un grupo finito y $\langle H, *\rangle$ es un subgrupo normal de G el orden del grupo cociente G/H está dado por:

$$|G/H| = \frac{|G|}{|H|}$$

EJEMPLO

Considérese el grupo $\langle \mathbb{Z}_{12}, +\rangle$ y sea H el subgrupo de $\mathbb{Z}_{12}$, dado por:

$$H = \{[0], [3], [6], [9]\}$$

Entonces, como $\mathbb{Z}_{12}$ es abeliano, H es normal y G/H forma un grupo con $12/4 = 3$ elementos diferentes, que son:

$$\begin{aligned}[0] + H &= \{[0], [3], [6], [9]\} \\ [1] + H &= \{[1], [4], [7], [10]\} \\ [2] + H &= \{[2], [5], [8], [11]\}\end{aligned}$$

8.6 Anillos

Antes, cuando se definió el concepto de grupo, se estableció que esta estructura matemática consta de un conjunto y una operación definida en este, la cual satisfface cuatro axiomas. No obstante, por la experiencia que se tiene desde la educación básica, en los conjuntos de números se define más de una operación. La generalización de esta idea da lugar a la estructura algebraica denominada anillo.

Formalmente, un **anillo** es un conjunto con dos operaciones binarias definidas en este, que se denota por $\langle R, +, \cdot\rangle$ y que satisfac[e los siguientes axiomas:]

1. $\langle R, +, \cdot \rangle$ forma un grupo abeliano.
2. La operación *multiplicación* es asociativa.
3. Para todo $x, y, z \in R$ se cumplen las leyes distributivas:

$$x \cdot (y+z) = x \cdot y + x \cdot z$$
$$(x+y) \cdot z = x \cdot z + y \cdot z$$

Cabe aclarar que la notación $\langle R, +, \cdot \rangle$ es la que más se utiliza para representar un anillo; sin embargo, los símbolos $+$ y $\cdot$ no necesariamente constituyen la *adición* y la *multiplicación estándares*, sino que esto depende del tipo de objetos que conforman a R. Luego de esta aclaración, y con cierto abuso del lenguaje, en lo sucesivo se hace referencia a las operaciones $+$ y $\cdot$ como adición y multiplicación.

EJEMPLO

Entre los diversos ejemplos de grupos abelianos que se han abordado en esta unidad, quizá los más comunes son: $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ y $\langle \mathbb{C}, + \rangle$. Pues, en dichos grupos abelianos, el lector ha manejado la multiplicación estándar y, como es bien sabido, esta operación es asociativa y se cumplen las leyes distributivas en los cuatro conjuntos. Por lo anterior, las cuatro tripletas $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$ son anillos.

Cuando el anillo cuenta con neutro multiplicativo, recibe el nombre de **anillo con unidad**. Pero, si además es conmutativo con la multiplicación, el anillo recibe el nombre de **anillo conmutativo.**

EJEMPLO

Los anillos $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$ considerados en el ejemplo anterior, son anillos conmutativos con unidad.

Al igual que los grupos, también existen anillos que contienen a otros anillos, lo cual da lugar al concepto de subanillo. Un subconjunto S de un anillo R se denomina **subanillo** de R si S satisface la cerradura con $+$ y con $\cdot$, y además S forma un anillo bajo esas operaciones.

EJEMPLO

El anillo $\langle \mathbb{Z}, +, \cdot \rangle$ es un subanillo de $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$. De manera similar, se tiene que $\langle \mathbb{Q}, +, \cdot \rangle$ es un subanillo de $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$, y que $\langle \mathbb{R}, +, \cdot \rangle$ es un subanillo de $\langle \mathbb{C}, +, \cdot \rangle$.

EJEMPLO

Sea $\langle \mathbb{R}, +, \cdot \rangle$ cualquier anillo, entonces el conjunto:

$$R[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \ \text{t} \cdot \text{q} \cdot a_i \in R,\, n \in \mathbb{N} \right\}$$

Y sean

$$P(x) = \sum_{i=1}^{n} a_i x_i \ \text{ y } \ Q(x) = \sum_{i=1}^{m} b a_i x^i$$

dos polinomios cualesquiera de $R[x]$. Entonces, el conjunto $R[x]$ forma un anillo con las operaciones $+$ y $\cdot$ (se supone, sin perder generalidad, que $n \geq m$):

$$P(x) + Q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$$

y

$$P(x)Q(x) = \sum_{i=0}^{n+m} c_i x^i$$

donde:

$$c_i = \sum_{\substack{j=0 \\ j \le n,\, i-j \le m}}^{i} a_j b_{i-j}$$

Con el fin de aclarar cómo llevar a cabo las operaciones del ejemplo anterior, a continuación se proponen dos ejemplos de anillos de polinomios específicos.

EJEMPLO

Considérese el anillo $\langle \mathbb{Z}, +, \cdot \rangle$, entonces el conjunto:

$$\mathbb{Z}[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \text{ t}\cdot\text{q}\cdot a_i \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

es un anillo de polinomios.

Sean:

$$P(x) = 3x^2 + x + 2 \text{ y } Q(x) = x^3 - x$$

Entonces, la suma de $P(x)$ con $Q(x)$ es:

$$P(x) + Q(x) = x^3 + 3x^2 + 2$$

Por otro lado, su producto es:

$$P(x)Q(x) = \left(3x^2 + x + 2\right)\left(x^3 - x\right) = 3x^5 + x^4 - x^3 - x^2 - 2x$$

EJEMPLO

Considérese el anillo $\langle \mathbb{Z}_6, +, \cdot \rangle$; entonces el conjunto:

$$\mathbb{Z}_6[x] = \left\{ [a_0] + [a_1]x + \cdots + [a_n]x^n \text{ t. q. } [a_i] \in \mathbb{Z}_6, n \in \mathbb{N} \right\}$$

es un anillo de polinomios.

Sean:

$$P(x) = [3]x^2 + [1]x + [2] \text{ y } Q(x) = [1]x^3 - [1]x$$

Entonces, la suma de $P(x)$ con $Q(x)$ es:

$$P(x) + Q(x) = x^3 + [3]x^2 + [2]$$

Por otro lado, para el producto se puede reescribir $Q(x)$ en la forma $Q(x) = [1]x^3 + [5]x$, ya que el inverso aditivo de $[1]$ es $[5]$, en $\mathbb{Z}_6$. Por tanto, se obtiene:

$$\begin{aligned} P(x)Q(x) &= \left([3]x^2 + [1]x + [2]\right)\left([1]x^3 + [5]x\right) \\ &= [3]x^5 + [1]x^4 + [5]x^3 + [5]x^2 + [4]x \end{aligned}$$

Un elemento $x \neq 0$ (donde 0 representa al neutro aditivo) de un anillo $\langle R, +, \cdot \rangle$, se dice que es un divisor de cero si existe un elemento $y \neq 0$, que satisface:

$$x \cdot y = 0 \text{ o bien } y \cdot x = 0$$

EJEMPLO

En $\langle \mathbb{Z}_6, +, \cdot \rangle$, [2] y [3] son divisores de cero, ya que:

$$[2] \cdot [3] = [0]$$

EJEMPLO

En no existen divisores de cero, ya que:

$$x \cdot y = 0$$

Esto implica que $x = 0$ y/o que $y = 0$

Considérese el anillo de todas las matrices de tamaño 2×2 con entradas reales, que se denota por $\langle M^2(\mathbb{R}), +, \cdot \rangle$. En este anillo sí existen divisores de cero, ya que, por ejemplo, las siguientes matrices son distintas de la matriz cero y no obstante su producto es la matriz cero:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Pero:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

En un anillo $\langle R, +, \cdot \rangle$ que no tiene divisores de cero, se satisfacen las leyes de cancelación por la izquierda y por la derecha; es decir, si:

$$x \cdot y = x \cdot z \text{ se tiene que } y = z$$
$$y \cdot z = z \cdot x \text{ se tiene que } z = y$$

para todo $x, y, z \in R$

A los anillos que no tienen divisores de cero, se les denomina **dominio integral** o **dominio de integridad**.

8.7 Isomorfismo de anillos

Del mismo modo en que dos grupos pueden ser estructuralmente idénticos, es posible que dos anillos sean matemáticamente iguales. Dados dos anillos $\langle R, +, \cdot \rangle$ y $\langle R', +, \cdot \rangle$ se dice que son isomorfos si existe una función biyectiva:

$$f : \langle R, +, \cdot \rangle \to \langle R', +, \cdot \rangle$$

Tal que todo par de elementos $x, y \in R$, se satisfacen:

$$f(x + y) = f(x) + f(y) \text{ y } f(x \cdot y) = f(x) \cdot f(y)$$

EJEMPLO

Considérense los anillos $\langle \mathbb{R}_2, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$, donde el producto en se $\mathbb{R}^2$ define por

$$(x, y) \cdot (z, w) = (xz - yw, xw + yz).$$

La función:

$$f:\langle \mathbb{R}_2, +, \cdot\rangle \rightarrow \langle \mathbb{C}, +, \cdot\rangle$$

definida por

$$f((x,\ y)) = x + iy$$

es un isomorfismo entre $\langle \mathbb{R}_2, +, \cdot\rangle$ y $\langle \mathbb{C}, +, \cdot\rangle$, ya que, f es, por definición, biyectiva y además:

$$\begin{aligned}
f((x,\ y)+(z,w)) &= f((x+z,\ y+w)) \\
&= (x+z)+(y+w)i \\
&= (x+iy)+(z+iw) \\
&= f((x,\ y))+f((z,w))
\end{aligned}$$

Y:

$$\begin{aligned}
f((x,\ y)\cdot(z,w)) &= f((xz-yw,\ xw+yz)) \\
&= (xz-yw)+(xw+yz)i \\
&= (x+iy)+(z+iw) \\
&= f(x,\ y)f(z,w)
\end{aligned}$$

EJEMPLO

Considérense los anillos $\langle \mathbb{C}, +, \cdot\rangle$ y $\langle M, +, \cdot\rangle$, donde:

$$M = \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \text{t}\cdot\text{q}\cdot x,\ y \in \mathbb{R} \right\}$$

con la adición y multiplicación estándar de matrices. La función:

$$f:\langle \mathbb{C}, +, \cdot\rangle \rightarrow \langle M, +, \cdot\rangle$$

definida por:

$$f(x+iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

es un isomorfismo entre $\langle M, +, \cdot\rangle$ y $\langle \mathbb{C}, +, \cdot\rangle$, ya que f es, por definición, biyectiva, y además:

$$\begin{aligned}
f((x+iy)+(z+iw)) &= f((x+z)+(y+w)i) \\
&= \begin{pmatrix} x+z & -(y+w) \\ y+w & x+z \end{pmatrix} \\
&= \begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} z & -w \\ w & z \end{pmatrix} \\
&= f(x+iy)+f(z+iw)
\end{aligned}$$

Y:

$$
\begin{aligned}
f((x+iy)\cdot(z+iw)) &= f((xz-yw)+(xw+yz)i)\\
&= \begin{bmatrix} xz-yw & -(xw+yz) \\ xw+yz & xz-yw \end{bmatrix}\\
&= \begin{bmatrix} x & -y \\ y & x \end{bmatrix} + \begin{bmatrix} z & -w \\ w & z \end{bmatrix}\\
&= f(x+iy)+f(z+iw)
\end{aligned}
$$

8.8 Campos

En sentido algebraico, un **campo** es un sistema aritmético con adición y multiplicación, tal que las operaciones son conmutativas, asociativas, distributivas e invertibles (excepto que no existe inverso multiplicativo para el cero). En otras palabras, un campo es un dominio integral conmutativo, con unidad, con inversos multiplicativos para cada elemento distinto de cero.

EJEMPLO

Los anillos $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$ son todos ejemplos de anillos conmutativos, con unidad, con inversos multiplicativos para cada elemento distinto de cero y sin divisores de cero; es decir, todos estos son campos.

EJEMPLO

El anillo $\langle \mathbb{Z}, +, \cdot \rangle$ es un anillo conmutativo con unidad y sin divisores de cero; sin embargo, no es un campo, ya que en $\mathbb{Z}$ no existen los inversos multiplicativos para enteros diferentes de 1 y -1.

Campos finitos

Los campos finitos son de gran importancia en la informática, la electrónica, la criptografía, entre otras muchas áreas de interés actuales. Para el estudio adecuado de estos campos, primero se muestran sus propiedades fundamentales. Como la intención del presente texto no es ser "rigurosamente matemático", algunas de las demostraciones se omitirán.

Teorema 8.8
El orden de cualquier grupo finito es una potencia de un número primo. Dada cualquier potencia de un número primo p^n existe, salvo isomorfismos, un único campo de dimensión p^n.

Así, en primer lugar se consideran los campos de orden primo p. De acuerdo con el teorema 8.8, existe, salvo isomorfismos, un único campo de dimensión p. Entonces, como los conjuntos de congruencias $\mathbb{Z}_p$ forman un grupo abeliano con la adición y (excepto el cero) forman un grupo abeliano con la multiplicación, $\langle \mathbb{Z}_p, +, \cdot \rangle$ es el único campo de dimensión p que existe.

EJEMPLO

Considérese el campo de orden 5; su álgebra completa puede analizarse con sus respectivas tablas de grupo (véanse tablas 8.13 y 8.14).

Tabla 8.13 Tabla de grupo para la adición.

$+$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Tabla 8.14 Tabla de grupo para multiplicación.

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

EJEMPLO

Considérese el anillo de congruencias $\langle \mathbb{Z}_4, +, \cdot \rangle$ de orden cuatro. De su tabla de multiplicación se puede ver que no forma un grupo con esta operación; por tanto, no es un campo (véase tabla 8.15).

Tabla 8.15 Tabla para el anillo de congruencias $\langle \mathbb{Z}_4, +, \cdot \rangle$, la cual muestra que no es un grupo con esta operación.

$\cdot$	[1]	[2]	[3]
[1]	[1]	[2]	[3]
[2]	[2]	[0]	[2]
[3]	[3]	[2]	[1]

Debido a que en esencia existe un único campo con exactamente p^n elementos (p primo y $n \in \mathbb{N}$) —dos representaciones cualesquiera son isomorfas— y que, como ya se discutió antes, los campos de orden primo p son precisamente los campos $\langle \mathbb{Z}_p, +, \cdot \rangle$, solo falta analizar los campos de dimensión p^n con $n > 1$. Los campos finitos, en general, reciben el nombre de **campos de Galois** y se representan como $GF(p^n)$

Si $n > 1$, $GF(p^n)$ no posee la aritmética modular, pero puede ser construido a partir del campo primo $\mathbb{Z}_p$; entonces, se dice que $GF(p^n)$ es una extensión de $\mathbb{Z}_p$.

Para ilustrar el proceso de extensión, primero se genera el campo $GF(2^n)$., para lo cual primero se encuentra un polinomio de grado 2, con coeficientes en $\mathbb{Z}_2$; sin embargo, este no puede ser factorizado en $\mathbb{Z}_2$ (para generar $GF(2^n)$. debe usarse un polinomio de grado n). En este caso, el único polinomio con tales características es $[1]x^2 + [1]x + [1]$, lo que significa que no existe solución en $\mathbb{Z}_2$ para la ecuación:

$$[1]x^2 + [1]x + [1] = [0]$$

Entonces, la extensión es creada mediante la introducción de un nuevo elemento σ, que es definido como solución de la ecuación anterior, justo como cuando son creados los números complejos a partir de los números reales, se define el elemento imaginario i para resolver la ecuación $x^2 + 1 = 0$. Además de o, también se debe agregar el elemento $\sigma + [1]$, para satisfacer la cerradura con la adición.
Así, se tiene:

$$GF(2^n) = \{[0], [1], \sigma, \sigma + [1]\}$$

Con aritmética determinada unívocamente por el hecho de que o satisface la ecuación cuadrática $[1]x^2 + [1]x + [1] = [0]$. Por ejemplo, se puede calcular el cuadrado de o de la siguiente manera:

Donde se hizo uso del hecho de que [1] es su propio inverso aditivo *mod*(2). De manera similar, se tiene:

$$(\sigma+[1])^2=\sigma^2+[1]=\sigma+[1]+[1]=\sigma$$

Las tablas de adición y multiplicación completas para $GF(2^2)$ se muestran a continuación.

- Adición en el campo: $GF(2^2)$

Tabla 8.16 Tabla de adición para $GF(2^2)$.

$+$	**1**	$\boldsymbol{\sigma}$	$\boldsymbol{\sigma^2}$
0	1	σ	σ^2
1	0	σ^2	σ
$\boldsymbol{\sigma}$	σ^2	0	1
$\boldsymbol{\sigma^2}$	0	1	σ

- Multiplicación en el campo:

Tabla 8.17 Tabla de multiplicación para $GF(2^2)-\{0\}$.

$\bullet$	**1**	$\boldsymbol{\sigma}$	$\boldsymbol{\sigma^2}$
1	1	σ	σ^2
$\boldsymbol{\sigma}$	σ	σ^2	1
$\boldsymbol{\sigma^2}$	σ^2	1	σ

En resumen, los elementos de $GF(2^2)$ son generados por potencias de un elemento primitivo σ, el cual es una raíz de un polinomio de grado n que es irreducible en $\mathbb{Z}_2$.

Por otro lado, el campo $GF(2^2)$ puede considerarse como un espacio lineal de dimensión n, así que cualquier $\alpha\in GF(2^2)$ es una combinación lineal de los elementos de una base $\{\theta_1, \theta_2, \ldots, \theta_n\}$:

$$\alpha=\sum_{i=1}^{n}a_i\theta_i, a_i\in\mathbb{Z}_2$$

El análogo de una base ortogonal es la llamada *base autodual* (la cual existe siempre para $GF(2^2)$), que satisface la condición $tr(\theta_i\theta_j)=\delta_{ij}$; así que $a_i=tr(\alpha\theta_i)$, donde la operación traza $tr:GF(2^n)\to\mathbb{Z}_2$ está definida por:

$$tr(\beta)=\beta+\beta^2+\beta^{2^2}+\cdots+\beta^{2^{n-1}}$$

Por ejemplo, $\{\sigma, \sigma^2\}$ es una base autodual para $GF(2^2)$, ya que cualquier elemento del campo puede escribirse como combinación lineal de estos; a saber:

$$1=\sigma+\sigma^2,\ \ (\sigma+1)=\sigma^2$$

Ejemplo

Construir el campo finito $GF(2^3)$.

Solución

De acuerdo con lo que se discute en páginas previas, para construir el campo finito primero se hace una extensión del campo $\mathbb{Z}_2$ tomando un polinomio cúbico irreducible en $\mathbb{Z}_2$. Es fácil verificar que el polinomio $[1]x^3+[1]x+[1]$ es irreducible en $\mathbb{Z}_2$, pues para la ecuación:

$$[1]x^3+[1]x+[1]=0$$

ninguno de los dos elementos de $\mathbb{Z}_2=\{[0],[1]\}$ son solución. Sea σ una solución de la ecuación anterior en el campo extendido, entonces de la ecuación $[1]\sigma^3+[1]\sigma+[1]=0$ se obtiene:

$$\sigma^3=\sigma+[1]$$

Si se multiplica sucesivamente por *o* se obtiene:

$$\sigma^4=\sigma^2+\sigma$$
$$\sigma^5=\sigma^3+\sigma^2=\sigma^2+\sigma+[1]$$
$$\sigma^6=\sigma^2+[1]$$
$$\sigma^7=[1]$$

Entonces, el campo finito de dimensión 8 se puede representar con los elementos:

$$GF\left(2^3\right)=\left\{[0],[1],\sigma,\sigma^2,\sigma+[1],\sigma^2+\sigma,\sigma^2+\sigma+[1],\sigma^2+[1]\right\}$$

Ejemplo

Escribir las tablas del campo finito $GF(2^3)$.

Solución

Del ejemplo anterior se sabe que los elementos de campo son:

$$GF\left(2^3\right)=\left\{[0],[1],\sigma,\sigma^2,\sigma^3=\sigma+[1],\sigma^4=\sigma^2+\sigma,\sigma^5=\sigma^2+\sigma+[1],\sigma^6=\sigma^2+[1]\right\}$$

y que σ satisface la ecuación:

$$[1]\sigma^3+[1]\sigma+[1]=0$$

Con esta información es fácil escribir las tablas de adición y multiplicación. Primero, se muestra la tabla de adición, luego se muestra la tabla de multiplicación.

Tabla 8.18 Tabla de adición para el campo finito $GF(2^3)$.

$+$	[0]	[1]	σ	σ^2	σ^3	σ^4	σ^5	σ^6
[0]	[0]	[1]	σ	σ^2	σ^3	σ^4	σ^5	σ^6
[1]	[1]	[0]	σ^3	σ^6	σ	σ^5	σ^4	σ^2
σ	σ	σ^3	[0]	σ^4	[1]	σ^2	σ^6	σ^5
σ^2	σ^2	σ^6	σ^4	[0]	σ^5	σ	σ^3	[1]
σ^3	σ^3	σ	[1]	σ^5	[0]	σ^6	σ^2	σ^4
σ^4	σ^4	σ^5	σ^2	σ	σ^6	[0]	[1]	σ^3
σ^5	σ^5	σ^4	σ^6	σ^3	σ^2	[1]	[0]	σ
σ^6	σ^6	σ^2	σ^5	[1]	σ^4	σ^3	σ	[0]

Tabla 8.19 Tabla de multiplicación para el campo finito $GF(2^3)$.

$\cdot$	[1]	σ	σ^2	σ^3	σ^4	σ^5	σ^6
[1]	[1]	σ	σ^2	σ^3	σ^4	σ^5	σ^6
σ	σ	σ^2	σ^3	σ^4	σ^5	σ^6	[1]
σ^2	σ^2	σ^3	σ^4	σ^5	σ^6	[1]	σ
σ^3	σ^3	σ^4	σ^5	σ^6	[1]	σ	σ^2
σ^4	σ^4	σ^5	σ^6	[1]	σ	σ^2	σ^3
σ^5	σ^5	σ^6	[1]	σ	σ^2	σ^3	σ^4
σ^6	σ^6	[1]	σ	σ^2	σ^3	σ^4	σ^5

8.9 Aplicaciones a criptografía de llave pública

La disciplina de la **criptografía** constituye el conjunto de procedimientos que se utilizan para transformar información, de tal manera que esta sea "invisible" para observadores sin autorización.

Desde que se tiene registro de la humanidad, siempre ha habido la necesidad de ocultar información a personas no deseadas. Por ejemplo, existe evidencia que indica que ya en la época del imperio egipcio se usaban métodos para encriptar información.

En la época moderna, la criptografía comenzó a tomar un gran auge con la aparición de nuevos medios de comunicación, como el telégrafo. Así que la tendencia fue buscar métodos cada vez mejores para la encriptación de datos. En este sentido, la Segunda Guerra Mundial es quizá el mejor ejemplo de la importancia de la encriptación de datos, pues como es bien sabido, muchas batallas fueron posibles gracias a la intercepción y descifrado de información entre los distintos rivales.

El tipo de criptografía utilizada durante la Segunda Guerra Mundial es aquella que se conoce como **criptografía de llave privada**, la cual consiste en que toda la protección de la información depende de la capacidad del método y de la capacidad de cada uno de los usuarios de mantener su clave privada en secreto. La principal desventaja de este método es que para descifrar la información es suficiente con tener dicha llave, lo cual hace que el sistema completo sea en extremo vulnerable.

Con el fin de corregir el problema de vulnerabilidad total del sistema, surgió una nueva técnica para encriptar datos: la **criptografía de llave pública**. En este tipo de criptografía, cada uno de los usuarios tiene dos llaves, una llave pública y una llave privada, pero solo una de estas es necesaria para descifrar la información que se cifra con la otra. Así, la seguridad del sistema se ve incrementada.

De este modo, si se combinan los dos tipos de criptografía (llave pública y llave privada), es posible lograr los siguientes puntos, mismos que son clave en la encriptación de datos:

a. Garantizar la autenticidad del origen de la información.
b. Garantizar la autenticidad del contenido e integridad del mismo.
c. Incorporar protocolos que dificulten ataques de espías.
d. Verificar la identidad de los comunicantes.

Hoy día, todavía continúa la tendencia a utilizar la criptografía de llave pública como complemento de la de llave privada, con lo que se logra incrementar la seguridad de los métodos criptográficos utilizados y eliminar las lagunas que existen en la aplicación de la criptografía de llave privada.

A continuación, se presenta una pequeña lista de algunos conceptos matemáticos necesarios para el desarrollo de la criptografía:

- **Números coprimos o primos entre sí.** Se dice que dos números enteros positivos son coprimos (o números primos entre sí) si su máximo común divisor es 1. Es decir, dados dos números $m, n, \in$ ⊠, se dice que son coprimos si y solo si:

$$m.\ c.\ d.\ (m, n) = 1$$

- **Función de Euler.** La función de Euler, para un entero positivo N se define como la cantidad de coprimos que existen menores que N. Es decir, considerando la descomposición de N en sus factores primos:

$$N = p_1^{k1} p_2^{k2} \cdots p_n^{k_n}$$

La función de Euler se calcula como:

$$\Phi(N) = \prod_{i=1}^{n} p_i^{k_i - 1}(p_i - 1)$$

- **Números primos fuertes:** Se dice que dos números primos, P y Q, son números primos fuertes si son números grandes (se considera "grande" a partir del orden de 200 dígitos) y de la forma:

$$P = 2p + 1$$
$$Q = 2q + 1$$

Donde p y q son números primos grandes.

- **Algoritmo de Diffie-Hellman.** En los algoritmos de llave secreta es necesario conservar la llave privada para evitar que toda comunicación posterior sea vulnerable con facilidad. Esta condición provoca que sea muy complicado el intercambio de las llaves, lo cual se debe hacer mediante el uso de protocolos jerárquicos rígidos.

En 1976, W. Diffie y M. E. Hellman inventaron un método de intercambio de llaves secretas a través de un canal abierto. Con lo que nació la criptografía de llave pública. Este algoritmo es muy simple de describirse:

Considérese un número primo grande p y un número entero cualquiera g. Para este caso, los valores de p y g son públicos. Ahora bien, sean K_A y K_B las llaves privadas que dos comunicantes, A y B, desean intercambiar. Para lograrlo, A genera un valor entero aleatorio x_A, donde $1 < x_A < p - 1$; de manera similar, B genera un valor aleatorio x_B con $1 < x_B < p - 1$. Acto seguido, A envía a B el valor público:

$$y_a \equiv g^{x_a} (\text{mod } p)$$

Y de manera análoga, B envía a A el valor (también público):

$$y_b \equiv g^{x_b} (\text{mod } p)$$

Así, B calcula el valor secreto:

$$z_{ab} \equiv y_a^{xb} \equiv g^{x_a x_b} (\text{mod } p)$$

Y de la misma forma, A calcula:

$$z_{ba} \equiv y_b^{x_a} \equiv g^{x_b x_a} (\text{mod } p)$$

Por último, se deduce, $z_{ab} = z_{ba}$, que puede ser utilizado como llave secreta compartida por ambos comunicantes.

- **Ataques al Diffie-Hellman.** Los ataques al método de Diffie–Hellman pueden catalogarse en dos partes: ataques pasivos y ataques activos.

  Un **ataque pasivo** es aquel en el que el "espía" trata de descifrar algo a partir de información cifrada interceptada. Por su parte, un **ataque activo** es aquel en el que el atacante desea no solo espiar información interceptada, sino también poder manipularla a su conveniencia.

  Por ejemplo, intentar obtener la llave secreta z_{ab}, a partir de p, g, y_a, y_b, constituye un ataque pasivo. Pero un intento de este tipo es muy difícil que pueda lograrse, pues se necesitaría obtener x_a o x_b, y para ello debería resolverse alguna de las siguientes operaciones:

$$x_a \equiv \log_g y_a (\text{mod p})$$
$$x_b \equiv \log_g y_b (\text{mod p})$$

  Lo cual es inviable para números grandes, pues solo bastaría elegir p y g lo suficientemente grandes para evitar este ataque.

  Para que exista un ataque activo, es posible que el atacante (que puede ser identificado por C) intervenga de forma activa en el intercambio. Así, por ejemplo, si C genera un entero aleatorio x_C con $1 < x_C < p - 1$ cuando A envíe a B y_a, C interceptará la comunicación y enviará a B $y_c \equiv g^{xc}(\text{mod p})$. Enseguida, B recibirá y_c con la creencia de que procede de A, y este responderá enviando y_b. Nuevamente, C interceptará la comunicación y enseguida enviará y_c a A.

  Así, A calcula:

$$z_{ca} \equiv y_c^{x_a} \equiv g^{x_c x_a} (\text{mod } p)$$

  y B calcula:

$$z_{cb} \equiv y_c^{x_b} \equiv g^{x_c x_b} (\text{mod } p)$$

  No obstante, ambas llaves también pueden ser calculadas por el atacante. Así, cuando A envíe una información cifrada con z_{ca} a B, el atacante la interceptará, la decodificará, la manipulará a su antojo, la encriptará con z_{cb} y la enviará a B. Y lo mismo sucederá cuando B envíe información cifrada a A.

  Este ataque es difícil de evitar y de descubrir, pero requiere la intervención continua del atacante para no ser descubierto.

- **Algoritmo RSA.** En 1977, R. L. Rivest, A. Shamir y L. Adleman propusieron un algoritmo de cifrado asimétrico de llave pública, que bautizaron como *RSA*, y que más tarde fue patentado por el MIT (*Massachussets Institute of Technology)*.

  Los **algoritmos de cifrado asimétrico** son aquellos en los que cada comunicante tiene dos llaves diferentes, una pública y una privada, siendo públicos el o los algoritmos de cifrado. Además, deben cumplir:

  – Ambos comunicantes calculan sus llaves en tiempo polinómico.
  – El emisor A puede, si conoce la llave pública de B, enviarle en tiempo polinómico un mensaje cifrado con la llave pública de B.
  – El receptor B debe poder descifrar el mensaje cifrado de A en tiempo polinómico con su llave secreta.
  – Un atacante deberá enfrentarse a costos cuya complejidad computacional los haga inviables cuando trate de calcular, bien las llaves secretas, bien los mensajes en claro a partir de los mensajes cifrados.

- **Algoritmo RSA.** Sean **p** y **q** dos números primos grandes, y sea $N = pq$ su producto común $\Phi(N)=(p-1)(q-1)$.

  Sea e, $1 < e < N$ un número aleatorio relativamente primo con $\Phi(N)$, y d un entero que verifica que $ed \equiv 1 \pmod{\Phi(N)}$. Así dispuesto, se verifica que para un cierto mensaje M, resulta que $M^{ed} \equiv M \pmod N$, y por tanto, si $C \equiv M^e \pmod N$, resulta que $M \equiv C^d \pmod N$.

  El algoritmo RSA utiliza estas propiedades para establecer un sistema criptográfico de cifrado asimétrico, en el que N, e corresponderían a la llave pública y d a la llave privada.
- **Ataques al RSA.** Nótese que en un sistema RSA existirá un conjunto de mensajes que no pueden ser cifrados. Se dice que un mensaje M no puede ser cifrado si $M^e \equiv M \pmod N$. Esto se puede reescribir de tal forma que M no podrá ser cifrado si:

$$M^e \equiv M \pmod p$$
$$M^e \equiv M \pmod q$$

  Así, se puede calcular que el número de mensajes no cifrables de un sistema RSA está definido por la expresión:

$$\sigma_N=[1 + \text{m.c.d.}(e-1, p-1)][1 + \text{m.c.d.}(e-1, q-1)]$$

  Mientras que los mensajes no cifrables serán de la forma:

$$M \equiv \{q[q^{-1} \pmod p)]M_p + p[p^{-1} \pmod q)]M_q\} \pmod N$$

  Donde:

$$M_p=[\, M^e \equiv M \pmod p)]$$
$$M_q=[\, M^e \equiv M \pmod q)]$$

  Se han propuesto multitud de ataques al algoritmo RSA, aunque hasta la fecha ninguno ha demostrado ser efectivo:
- **El ataque por factorización de la llave pública.** La forma más evidente de romper la seguridad de un sistema RSA pasa por factorizar su llave. Ello no obstante constituye la forma más difícil de lograrlo, ya que si los factores primos p y q son números lo suficientemente grandes, la complejidad computacional de los algoritmos de factorización hace inviable la factorización de N en un tiempo finito.
- **El ataque cíclico.** El ataque cíclico se basa en la idea de que los sistemas RSA son grupos multiplicativos con un número finito de elementos. Así, para descifrar $C \equiv M^e \pmod N$ no sería necesario conocer la llave privada d, sino que bastaría con realizar cifrados sucesivos con la llave pública e,

hasta obtener el mensaje cifrado C (recordemos que RSA se basa en la aritmética modular). Si C_i es el i–ésimo cifrado realizado con la llave pública e, y $C_i \equiv C(\text{mod } N)$, entonces resulta obvio que C_{i-1} debe corresponder a M.

Este ataque puede evitarse si los valores primos p y q que forman la factorización de N son números primos fuertes, ya que entonces la complejidad computacional aumenta hasta convertir el problema en irresoluble.

- **Ataque de Merkle-Hellman.** Este ataque, propuesto por R. Merkle y M. Hellman, en 1981, se basa en la idea de que se puede romper el cifrado de un sistema conociendo un mensaje cifrado y su correspondiente texto en claro (algo que en el RSA es a todas luces, posible).

  La justificación matemática del ataque es muy compleja, pero su modo de funcionamiento es relativamente simple de describir. Este se basa en realizar pruebas de encriptación con un mensaje M, hasta obtener una coincidencia que permita obtener la llave privada pareja de la llave pública (conocida) e. Se puede demostrar que este método de criptoanálisis es mejor que los métodos de fuerza bruta.

  No obstante, también se demuestra que la probabilidad de hallar una llave válida disminuye cuando los factores p y q son números primos fuertes. Si los números p y q están bien elegidos, entonces este ataque se vuelve impracticable.
- **Ataque por control de tiempos.** Este ataque se basa en la idea de medir el tiempo invertido por el dispositivo cifrante en realizar el cifrado de los mensajes, y a partir de estos tiempos medidos tratar de extraer información acerca de la llave usada. No obstante, es complicado y hay ciertas sencillas técnicas algorítmicas que permiten evitar este ataque.
- **Ataque por introducción de faltas.** La idea de este ataque se refiere a la introducción de alteraciones en el mensaje que se va a cifrar con la clave privada, para observar después la diferencia entre el mensaje cifrado con los valores erróneos y el mensaje que se hubiera cifrado de no haber introducido errores. Tiene el evidente inconveniente de que resulta necesario que el atacante tenga cierto control sobre el dispositivo a atacar.

  Como se puede observar, resulta bastante evidente que, a pesar de la multitud de ataques propuestos contra el algoritmo RSA, no hay ninguno de estos que tenga la suficiente efectividad como para comprometer seriamente la credibilidad de dicho algoritmo.

Otros algoritmos de cifrado de llave pública

Cabe aclarar que RSA no es el único algoritmo de cifrado de llave pública que existe, aunque seguramente sí es el más popular; no obstante, en la literatura es posible hallar algunos otros ejemplos interesantes.

- **Cifrado de Rabin.** Este método de cifrado fue descrito en 1979. Se basa en la existencia de dos números primos grandes, p y q, tal que $p \equiv q \equiv 3(\text{mod } 4)$, siendo $N = pq$ la llave pública, y el par (p,q) la llave privada. Así, el cifrado de un cierto mensaje M se obtendría:

  $$C \equiv M^2(\text{mod } N)$$

  Así, para descifrar el mensaje C sería necesario calcular su raíz cuadrada (mod N), lo cual solo es posible si se conocen los factores primos p y q, ya que en otro caso la complejidad de los algoritmos lo hace inviable. Aún así, existe el problema de que hay cuatro posibles soluciones para dicha raíz cuadrada, y de ahí el problema de elegir una, ya que si el mensaje M debe tener sentido en alguna lengua humana, entonces un operador humano podrá decidir, pero si el mensaje M es aleatorio o no tiene sentido para un operador humano, o no puede establecerse una relación con un diccionario, entonces este método de cifrado resulta inviable.

  Existe una modificación a este método de cifrado introducida por H. C. Williams en el año 1980, orientada a eliminar el inconveniente de la multiplicidad de las raíces cuadradas (mod N).

- **Cifrado de El Gamal.** Este sistema de cifrado fue propuesto por T. El Gamal en 1985. Se basa en la dificultad del cálculo de los logaritmos discretos con números enteros grandes.

  Sean p un número primo grande y g un número entero (grande). Ambos valores son públicos. Sea x tal que $1 < x < p - 1$ un valor aleatorio secreto, con una llave pública asociada y, definida por:

  $$y \equiv g^x \pmod p.$$

  Así, el cifrado de un cierto mensaje M se realizará eligiendo un valor aleatorio $k/1<k<p-1$, siendo k relativamente primo con $(p-1)$. Por tanto, el mensaje cifrado estará dado por la pareja de valores:

  $$r \equiv g^k \pmod p$$
  $$s \equiv My^k \pmod p$$

  La recuperación del mensaje en claro a partir del cifrado se calcula como:

  $$M \equiv (s/r^x) \pmod p$$

  Ya que:

  $$M \equiv (s/r^x) \pmod p \Rightarrow M \equiv (My^k/y^k) \pmod p \equiv M \pmod p.$$

  Este método de cifrado tiene la particularidad de que dado un mismo mensaje en claro puede tener varios cifrados diferentes. No obstante, tiene el problema de que el cifrado tiene una longitud doble del mensaje original, lo que puede dar como resultado problemas de espacio y de manejo de cifrado.

Aplicaciones de la criptografía de llave pública

Después de examinar los algoritmos de llave pública y comprobar su efectividad, cabe preguntarse por sus aplicaciones. Ya se ha explicado cómo es que estos algoritmos cumplen con su principal aplicación, que es la de cifrar (ocultar) la información. Así pues, a continuación se intenta dar una visión somera de las otras aplicaciones que tiene la criptografía de llave pública.

Recuérdese que al principio se planteaban las siguientes necesidades:

- Garantizar la autenticidad del origen de la información.
- Garantizar la autenticidad del contenido e integridad del mismo.
- Incorporación de protocolos que dificulten los ataques de espías.
- Verificar la identidad de los comunicantes.

La **autenticación** pretende, pues, obtener constancia de que la información que se recibe procede de un emisor esperado y no de un atacante. En la criptografía de llave pública la solución a este punto es trivial, ya que resulta evidente que cualquier información que se descifre con la llave pública del emisor tiene por fuerza haber sido cifrada con su llave privada. No obstante, la criptografía de llave pública suele presentar el inconveniente de que resulta más lenta en el cifrado y descifrado que la de llave privada.

Por lo expuesto antes, una posible solución puede ser la utilización de una llave de sesión para cifrar la información mediante un algoritmo de llave privada (p. ej. El DES), que permita ocultar de modo conveniente la información, y a continuación la encriptación de la llave de sesión mediante la llave privada de cada persona. El posterior descifrado del mensaje se realiza mediante el descifrado de la llave de sesión, que al ser de menor longitud que el mensaje, resulta más rápida.

Al respecto de la **identificación** de los comunicantes, existen protocolos establecidos para permitir la identificación electrónica, el más conocido y extendido de los cuales es la utilización de certificados. En este protocolo, una autoridad certificadora se encarga de dar constancia de que la llave pública contenida en el certificado procede del comunicante que realiza la afirmación, y no de otro individuo. Con esta medida, se prevé que toda comunicación contará con las garantías propias de la criptografía de llave pública.

Sobre la garantía de **integridad del contenido** se ha establecido un protocolo de firma digital que soluciona los problemas de integridad como parte de los problemas de autenticación de la fuente y de los ataques de espías. Este protocolo se basa en la existencia de funciones resumen (*hash*), tales que, dada una información, el resultado de la función resumen es único y cualquier modificación introducida en la información producirá un resultado distinto de la función resumen (la probabilidad de que exista una información similar a la original con un resumen de igual valor es ínfima). Así, se realizaría un resumen del texto a firmar, y el resultado se cifraría con la clave privada y se colocaría anexo al texto original. Cualquier alteración de la información sería detectada de inmediato solo con desencriptar el resumen, y además el hecho de estar encriptado este con la llave privada del firmante, permite autenticar la identidad del mismo.

Resumen

Existen diferentes estructuras algebraicas que pueden utilizarse en aplicaciones de informática, criptografía, física, química, entre otras disciplinas. Las principales estructuras algebraicas de interés son los grupos, los anillos y los campos.

Un **grupo** es un conjunto junto con una operación binaria que satisface las propiedades de cerradura, asociatividad, existencia de un elemento neutro y existencia de elementos inversos. Cuando un grupo H está dentro de otro grupo G se dice que H es un subgrupo de G. Un grupo en el cual existe un elemento que genera todos los demás elementos (operando dicho elemento consigo mismo) recibe el nombre de grupo cíclico. Se dice que dos grupos $\langle G, *\rangle$ y $\langle G', \circ\rangle$ son isomorfos, si existe una función biyectiva f entre G y G' que satisface $f(g_1 * g_2) = f(g_1) \circ f(g_2)$ para todo $g_1, g_2 \in G$.

Un **anillo** es un conjunto junto con dos operaciones binarias, $\langle R, +, \cdot\rangle$, tal que, $\langle R, +\rangle$ es un grupo y se satisfacen las leyes distributivas:

$$x(y+z) = xy + xz$$
$$(x+y)z = xz + yz$$

para todo $x, y, z \in R$.

Se dice que dos anillos $\langle R, +, \cdot\rangle$ y $\langle R', +, \cdot\rangle$ son isomorfos, si existe una función biyectiva f entre R y R' que satisface las siguientes propiedades:

$$f(x+y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(y)$$

$\forall x, y \in R$.

Por último, un campo es un anillo que forma también un grupo con la multiplicación.

Problemas propuestos

En los problemas 8.1 a 8.10 explicar si el conjunto dado, junto con la operación definida en este, forman un grupo. En caso de que no formen un grupo, especificar al menos un axioma de grupo que no se satisface.

8.1 $\mathbb{Z}$ con la operación – (resta).

8.2 $\mathbb{Z}$ con la multiplicación estándar.

8.3 $\mathbb{R}$ con la operación – (resta).

8.4 $\mathbb{R}$ con la multiplicación estándar.

8.5 $\mathbb{R}^*$ con la multiplicación estándar.

8.6 $\mathbb{Q}^+$ con la multiplicación estándar.

8.7 $S = \mathbb{R} - \{1, -1\}$ definida por $x * y = xy - xy$

8.8 $S = \mathbb{R} - \{1, -1\}$ con la multiplicación estándar.

8.9 $S = \mathbb{R} - \{1, -1\}$ con la adición estándar.

8.10 El conjunto de todas las matrices de la forma:

$$\left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \; t \cdot q \cdot x \in \mathbb{R} \right\}$$

8.11 Considérese la siguiente tabla:

Tabla 8.20

$\bullet$	e	x	y	z
e	e	x	y	z
x	x	x	e	e
y	y	e	y	e
z	z	e	e	z

Proporcionar al menos dos razones por las cuales no representa un grupo.

8.12 Examínese la operación $\wedge$ definida sobre el conjunto {Verdadero, Falso}. ¿Cuáles de los axiomas de grupo se satisfacen?

8.13 Demostrar que si $\langle G, *\rangle$ es un grupo y $g \in G$ entonces:

$$\left(g^{-1}\right)^{-1} = g$$

8.14 Demostrar que el conjunto de matrices invertibles de tamaño 2×2 forma un grupo con la multiplicación matricial.

8.15 Demostrar que si $\langle G, *\rangle$ es un grupo y $g, h \in G$ entonces:

$$(g * h)^{-1} = h^{-1} * g^{-1}$$

8.16 Demostrar que un grupo $\langle G, *\rangle$ es abeliano si y solo si:

$$(g * h)^{-1} = g^{-1} * h^{-1}$$

8.17 Sea $\langle G, *\rangle$ un grupo. Definir una nueva operación $\otimes$ en G, mediante:

$$g \quad h = h * g$$

Demostrar que: $\langle G, \otimes\rangle$

En los ejercicios 8.18 a 8.30 indicar si los grupos dados son o no isomorfos. En caso negativo, proporcionar al menos una propiedad estructural que tiene uno de estos y el otro no.

8.18 $\langle \mathbb{Z}_{10}, +\rangle$ y $\langle \mathbb{Z}^*_{11}, \cdot\rangle$

8.19 $\langle \mathbb{Z}, +\rangle$ y $\langle 5\mathbb{Z}, +\rangle$

8.20 $\langle \mathbb{Z}, +\rangle$ y $\langle \mathbb{R}, +\rangle$

8.21 $\langle 3\mathbb{Z}, +\rangle$ y $\langle 5\mathbb{Z}, +\rangle$

8.22 $\langle \mathbb{Q}^*, \cdot\rangle$ y $\langle \mathbb{Z}, +\rangle$

8.23 $\langle \mathbb{Q}^*, \cdot\rangle$ y $\langle \mathbb{R}, +\rangle$

8.24 $\langle \mathbb{Z}_6, +\rangle$ y $\langle S_3, \circ\rangle$ (donde S_3 es el grupo de todas las permutaciones de 3 objetos).

8.25 $\langle \mathbb{Z}_{11}, +\rangle$ y $\langle \mathbb{Z}^*_{11}, \cdot\rangle$

8.26 $\langle 5\mathbb{Z}, +\rangle$ y $\langle \mathbb{Z}_5, +\rangle$

8.27 $\langle \mathbb{Z}_2, +\rangle$ y $\langle S_2, \circ\rangle$

8.28 $\langle \mathbb{Z}_3, +\rangle$ y cualquier grupo $\langle G, *\rangle$ de tres elementos.

8.29 $\langle \mathbb{Z}_4, \cdot\rangle$ y $\langle G, \cdot\rangle$ donde $G = \{i, -1, -i, 1\}$, $i = \sqrt{-1}$

8.30 $\langle \mathbb{Z}, +\rangle$ y $\langle \mathbb{Q}, +\rangle$

En los ejercicios 8.31 a 8.40 indicar si H es subgrupo del grupo G dado.

8.31 $\langle H, *\rangle = \langle \mathbb{Z}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{R}, +\rangle$

8.32 $\langle H, *\rangle = \langle 3\mathbb{Z}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{R}, +\rangle$

8.33 $\langle H, *\rangle = \langle 3\mathbb{Z}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{Z}, +\rangle$

8.34 $\langle H, *\rangle = \langle \mathbb{R}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{C}, \cdot\rangle$

8.35 $\langle H, *\rangle = \langle \mathbb{R}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{R}, \cdot\rangle$

8.36 $\langle H, *\rangle = \langle \mathbb{Q}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{R}, \cdot\rangle$

8.37 $\langle H, *\rangle = \langle \mathbb{Z}_{11}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{Z}_{11}, +\rangle$

8.38 $\langle H, *\rangle = \langle \mathbb{Z}_{11}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{Z}_{20}, +\rangle$

8.39 $\langle H, *\rangle = \langle \mathbb{Z}_{11}, +\rangle$ y $\langle G, *\rangle = \langle \mathbb{Z}_{11}, \cdot\rangle$

8.40 $\langle H, *\rangle = \langle S_3, +\rangle$ y $\langle G, *\rangle = \langle S_4, +\rangle$

En los ejercicios 8.41 a 8.46 indicar si $\langle \mathrm{R}, +, \cdot\rangle$ es un anillo.

8.41 $\langle \mathbb{Z}_{11}, +\rangle$

8.42 $\langle \mathbb{N}, +, \cdot\rangle$

8.43 $\langle \mathbb{Q}, +, \cdot\rangle$

8.44 $\langle \mathbb{Z}_{11}, +, \cdot \rangle$

8.45 $\langle \mathbb{C}, +, \cdot \rangle$

8.46 $\langle 3\mathbb{Z}, +, \cdot \rangle$

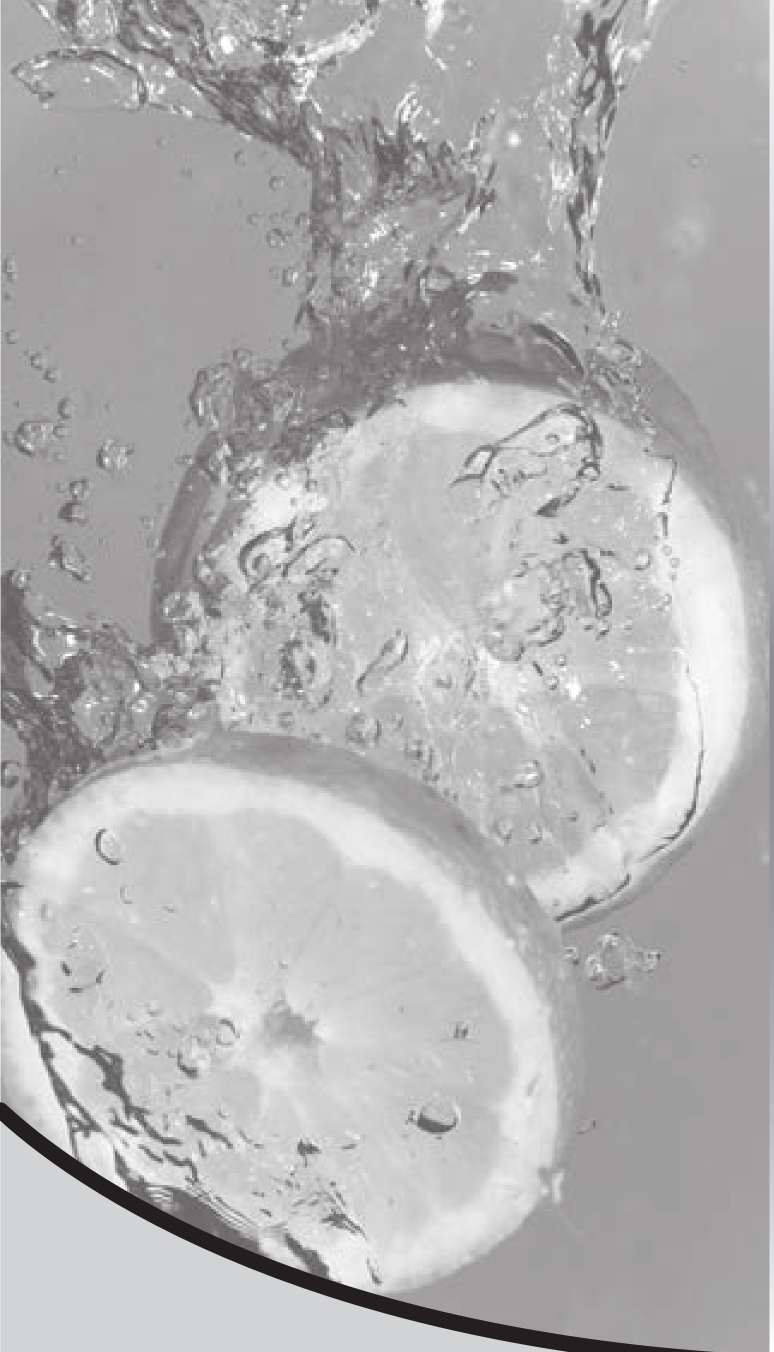
En los ejercicios 8.47 a 8.50 indicar si $\langle \mathbb{R}, +, \cdot \rangle$ es un campo.

8.47 $\langle \mathbb{Z}_{11}, +, \cdot \rangle$

8.48 $\langle \mathbb{N}, +, \cdot \rangle$

8.49 $\langle \mathbb{Q}, +, \cdot \rangle$

8.50 $\langle \mathbb{Z}_{7}, +, \cdot \rangle$



9

Álgebra de Boole

Objetivos

- Reconocer los principios algebraicos que sustentan el álgebra de Boole.
- Describir la relación entre el álgebra de Boole y las compuertas lógicas que constituyen los componentes básicos de los circuitos lógicos.
- Aplicar el álgebra de Boole a la resolución de problemas de operaciones automatizadas.
- Simplificar expresiones booleanas optimizando y aplicando sus propiedades.

9.1 Introducción

Por definición, el álgebra de Boole o álgebra booleana es un concepto del álgebra que permite abstraer las principales operaciones algebraicas en un sistema binario. Esta debe su nombre al matemático inglés George Boole, quien la creó y desarrolló a mediados del siglo XIX. Sin embargo, fue hasta mediados del siglo XX que el álgebra booleana adquiere auge y una gran importancia práctica, que se ha incrementado de manera considerable a últimas fechas, en especial en el terreno del manejo de información digital (en lo que se conoce como lógica digital). Gracias a esta, Claude Elwood Shannon (1949) pudo formular su teoría de la codificación y John von Neumann pudo enunciar el modelo de arquitectura que define la estructura interna de las computadoras desde la primera generación.

Por tanto, los principales campos de aplicación del álgebra booleana son la informática, la electrónica digital y la computación, en virtud del hecho de que la lógica de la computadora se basa en el sistema binario; esto es, en los circuitos electrónicos de una computadora la información se trata en esencia como una secuencia de ceros y unos.

Figura 9.1 Claude Elwood Shannon (1916-2001).

Claude Elwood Shannon dedicó gran parte de su trabajo al problema de la eficiencia de los diferentes métodos de transmisión de la información que hay, tanto mediante el flujo, a través de hilos o cables, como de tipo aéreo, por medio de corrientes eléctricas fluctuantes o bien moduladas por la radiación electromagnética. Orientó sus esfuerzos hacia la comprensión fundamental del problema, lo que le permitió desarrollar en 1948 un método para expresar la información de forma cualitativa. Sus publicaciones demostraron cómo se podía analizar dicha cuantificación (expresada en una magnitud a la que denominó bit) mediante métodos estrictamente matemáticos.

La rama de las matemáticas inaugurada por Shannon se denomina **teoría de la información** y resultó ser en extremo útil, no solo en el diseño de circuitos de computadoras y la tecnología de comunicaciones, sino que también ha hallado aplicaciones fecundas en campos tan diversos como la biología, la psicología, la fonética e, incluso, la semántica y la literatura.

Es importante destacar que todas las variables y constantes del álgebra booleana admiten solo uno de dos valores en sus entradas y salidas: sí/no, 1/0, encendido/apagado, con voltaje/sin voltaje o verdadero/falso. Estos valores bivalentes y opuestos pueden ser representados por números binarios de un dígito (bits); por tanto, el álgebra booleana se puede entender cómo el **álgebra del sistema binario**.

Al igual que en el álgebra tradicional, en el álgebra booleana también se utilizan letras del alfabeto para denominar a las variables y formar ecuaciones, con el objetivo de obtener el resultado de ciertas operaciones mediante una ecuación o expresión booleana; es evidente que los resultados de las operaciones correspondientes también serán binarios.

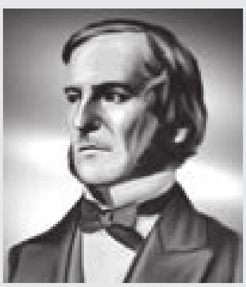


Figura 9.2 George Boole (1815-1864).

George Boole a mediados del siglo XIX, Boole en sus libros *The Mathematical Analysis of Logic* (*Un análisis matemático de las lógica*), escrito en 1847, y *An Investigation of the Laws of Thought* (*Una investigación de las leyes del pensamiento*), publicado en 1854, la idea de que las proposiciones lógicas podían ser tratadas mediante herramientas matemáticas.

Las proposiciones lógicas (frases o predicados de la lógica clásica) son aquellas que solo pueden tomar valores de verdadero/falso o preguntas cuyas únicas respuestas posibles son sí/no.

Según Boole, estas proposiciones solo pueden ser representadas mediante símbolos; por tanto, desarrolló una teoría que permite trabajar con estos símbolos, sus entradas (variables) y sus salidas (respuestas), a la que denominó **lógica simbólica**, misma que cuenta con operaciones lógicas que siguen el comportamiento de las reglas algebraicas. De este modo, al conjunto de reglas de la **lógica simbólica** se le denomina **álgebra de Boole**.

9.2 Álgebra de Boole (álgebra booleana)

El álgebra booleana constituye un sistema matemático deductivo centrado en los valores 1 y 0, que proporciona operaciones y reglas para trabajar con dichos valores.

Las operaciones booleanas básicas son: suma booleana, producto booleano y complemento booleano, las cuales se definen a continuación.

Suma booleana

La suma booleana de dos elementos del conjunto binario, que se denota por el símbolo $+$, es una operación con las reglas siguientes:

$$\begin{gathered} 1+1=1 \\ 0+1=1 \\ 1+0=1 \\ 0+0=0 \end{gathered}$$

La suma booleana equivale a la operación lógica disyunción inclusiva $\vee$, solo que en esta V y F cambian por 1 y 0.

Producto booleano

El producto booleano de dos elementos del conjunto binario, denotada por el símbolo $\cdot$, es una operación con las reglas siguientes:

$$\begin{gathered} 1\cdot 1=1 \\ 0\cdot 1=0 \\ 1\cdot 0=0 \\ 0\cdot 0=0 \end{gathered}$$

Esta equivale a la operación lógica conjunción $\wedge$, donde también solo cambia V y F por 1 y 0.

Complemento booleano

El complemento booleano de un elemento del conjunto binario es una operación con las reglas siguientes:

$$\begin{gathered} 1' = 0 \\ 0' = 1 \end{gathered}$$

El complemento booleano equivale a la operación lógica negación $\sim$, donde también solo cambia V y F por 1 y 0.

Un conjunto $\boldsymbol{B}$ se considera álgebra booleana si y solo si además de contener las dos operaciones binarias de suma booleana ($+$) y producto booleano ($\cdot$), así como la operación unaria de complemento booleano ('), se verifican las siguientes propiedades básicas sobre cualquier a, b, y $c \in \boldsymbol{B}$:

B1. Identidad

$$\begin{gathered} \text{a) } a+0=a \\ \text{b) } a\cdot 1=a \end{gathered}$$

B2. Propiedad conmutativa

$$a) \; a + b = b + a$$
$$b) \; a \cdot b = b \cdot a$$

B3. Propiedad distributiva

$$a) \; a + (b \cdot c) = (a + b) \cdot (a + c)$$
$$b) \; a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

B4. Propiedad asociativa

$$a) \; (a + b) + c = a + (b + c)$$
$$b) \; (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

B5. Propiedad de complementos

$$a) \; a + a' = 1$$
$$b) \; a \cdot a' = 0$$

El elemento 0 se denomina neutro respecto a la suma, en tanto que el elemento 1 se denomina elemento neutro respecto al producto.

Es importante destacar que por convención es posible eliminar el símbolo del producto booleano $\cdot$.

Nota

En álgebra booleana, 0 y 1 son nombres simbólicos que en general no tienen nada que ver los números 0 y 1. De igual manera, los símbolos $+$ y $\cdot$ son solo operadores binarios que no tienen relación con las operaciones de adición y multiplicación comunes.

Ejemplo

Con el uso de la convención anterior, la propiedad distributiva puede escribirse como:

$a + bc = (a + b)(a + c)$

$a(b + c) = ab + ac$

A lo largo de este capítulo puede utilizarse o no, de manera indistinta, el símbolo del producto booleano.

Asimismo, por convención se establece que el complemento booleano tiene mayor prioridad que el producto booleano, el cual, a su vez, tiene mayor prioridad que la suma booleana; no obstante, los paréntesis ( ) pueden cambiar el orden de la prioridad.

Ejemplo

Mediante el uso de la convención anterior, se tiene que:

$$a + b \cdot c$$

Esto significa:

$$a + (b \cdot c)$$

En vez de:

$$(a + b) \cdot c$$

Y que:

$$a \cdot b'$$

Esto significa:

$$a \cdot (b')$$

En lugar de:

$$(a \cdot b)'$$

Propiedades adicionales del álgebra booleana

En álgebra booleana existen propiedades adicionales que se pueden demostrar utilizando las propiedades básicas vistas antes.

Ley del doble complemento o ley de la involución

$$(a')' = a$$
$$\forall\, a \in \mathbf{B}.$$

DEMOSTRACIÓN

$a' + (a')'$	$= 1$	por B5
	$= a + a'$	por B5
	$= a' + a$	por B2
$(a')'$	$= a$	eliminando a' en ambos lados

O bien:

$a' \cdot (a')'$	$= 0$	por B5
	$= a \cdot a'$	por B5
	$= a' \cdot a$	por B2
$(a')'$	$= a$	eliminando a' en ambos lados

Ley de la dominación

$$a)\ a + 1 = 1$$
$$a \cdot 0 = 0$$
$$\forall\, a \in \mathbf{B}.$$

DEMOSTRACIÓN

a) $(a + 1)$	$= (a + 1) \cdot 1$	por B1
	$= (a + 1) \cdot (a + a')$	por B5
	$= a + (1 \cdot a')$	por B3
	$= a + a'$	por B1
	$= 1$	por B5

b) $(a \cdot 1)$	$= (a \cdot 1) + 0$	por B1
	$= (a \cdot 1) + (a \cdot a')$	por B5
	$= a \cdot (1 + a')$	por B3
	$= a \cdot a'$	por B1
	$= 0$	por B5

Ley de la idempotencia

$$a + a = a$$
$$a \cdot a = a$$
$$\forall\, a \in \mathbf{B}.$$

Demostración

a) $(a + a) = (a + a) \cdot 1$ por B1
$= (a + a) \cdot (a + a')$ por B5
$= a + (a \cdot a')$ por B3
$= a + 0$ por B5
$= a$ por B1

b) $(a \cdot a) = (a \cdot a) + 0$ por B1
$= (a \cdot a) + (a \cdot a')$ por B5
$= a \cdot (a + a')$ por B3
$= a \cdot 1$ por B5
$= a$ por B1

Ley de la absorción

a) $a + (a \cdot b) = a$
b) $a \cdot (a + b) = a$
$\forall\, a$ y $b \in \mathbf{B}$.

Demostración

a) $a + (a \cdot b) = (a \cdot 1) + (a \cdot b)$ por B1
$= a \cdot (1 + b)$ por B3
$= a \cdot (b + 1)$ por B2
$= a \cdot 1$ Ley de la dominación
$= a$ por B1

b) $a \cdot (a + b) = (a + 0) \cdot (a + b)$ por B1
$= a + (0 \cdot b)$ por B3
$= a + (b \cdot 0)$ por B2
$= a + 0$ Ley de la dominación
$= a$ por B1

Ley de De Morgan

a) $(a + b)' = a' \cdot b'$
b) $(a \cdot b)' = a' + b'$
$\forall\, a$ y $b \in \mathbf{B}$.

Demostración

La Ley de De Morgan solo se comprueba si se satisface B5; es decir, se debe demostrar que si y es el complemento de x, entonces:

$x + y = 1$

$x \cdot y = 0$

a) $(a + b) + a' \cdot b' = \{(a + b) + a'\} \cdot \{(a + b) + b'\}$ por B3
$= \{(b + a) + a'\} \cdot \{(a + b) + b'\}$ por B2
$= \{b + (a + a')\} \cdot \{a + (b + b')\}$ por B4
$= b + 1 \cdot a + 1$ por B5
$= 1 \cdot 1$ Ley de la dominación
$= 1$ por B1

$(a+b)\cdot a'\cdot b'$	$=\{a\cdot a'\cdot b'\}+\{b\cdot a'\cdot b'\}$	por B3
	$=\{a\cdot a'\cdot b'\}+\{b\cdot b'\cdot a'\}$	por B2
	$=\{(a\cdot a')\cdot b'\}+\{(b\cdot b')\cdot a'\}$	por B4
	$=0\cdot b'+0\cdot a'$	por B5
	$=0+0$	Ley de la dominación
	$=0$	por B1

b) $(a\cdot b)\cdot a'+b'$	$=\{(a\cdot b)\cdot a'\}+\{(a\cdot b)\cdot b'\}$	por B3
	$=\{(b\cdot a)\cdot a'\}+\{(a\cdot b)\cdot b'\}$	por B2
	$=\{b\cdot(a\cdot a')\}+\{a\cdot(b\cdot b')\}$	por B4
	$=b\cdot 0+a\cdot 0$	por B5
	$=0+0$	Ley de la dominación
	$=0$	por B1

$(a\cdot b)+a'+b'$	$=\{a+a'+b'\}\cdot\{b+a'+b'\}$	por B3
	$=\{a+a'+b'\}\cdot\{b+b'+a'\}$	por B2
	$=\{(a+a')+b'\}\cdot\{(b+b')+a'\}$	por B4
	$=1+b'\cdot 1+a'$	por B5
	$=1\cdot 1$	Ley de la dominación
	$=1$	por B1

Leyes de De Morgan generalizadas

Las leyes de De Morgan pueden generalizarse para cualquier cantidad de elementos de ***B***, como se muestra a continuación:

$$\text{a) } (a_1+a_2+\cdots+a_n)'=a'_1\cdot a'_2\cdot\cdots\cdot a'_n$$

Es decir, el complemento de la suma lógica de dos o más elementos de ***B*** equivale al producto lógico de los complementos de cada uno de estos elementos:

$$\text{b) } (a_1\cdot a_2\cdot\cdots\cdot a_n)'=a'_1+a'_2+\cdots+a'_n$$

Esto es, el complemento del producto lógico de dos o más elementos de ***B*** equivale a la suma lógica de los complementos de cada uno de dichos elementos.

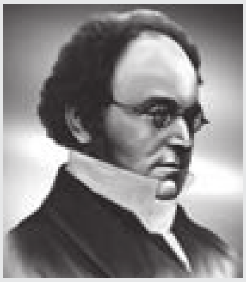


Figura 9.3 Augustus De Morgan (1806-1871), lógico y matemático británico.

Augustus De Morgan nacido en Madura (India), contribuyó de manera considerable al avance de la lógica en el siglo XIX.

A los 16 años ingresó al Trinity College de Cambrigde. Al concluir sus estudios universitarios fue nombrado profesor del University College, en Londres. Además, escribió diferentes libros sobre diversos temas, como aritmética, álgebra, análisis y lógica; es precisamente esta última disciplina el campo en el que más sobresalió.

De todas sus obras, *Trigonometry and double algebra* (*Trigonometría y álgebra doble*) es aquella en la que mejor expone una interpretación geométrica de los números complejos. Por su parte, *Formal Logic* (*Lógica formal*) constituye su obra más notable, ya que en esta es donde expone un buen sistema de notación para la lógica simbólica e incluye el concepto de cuantificación de predicados, con el cual era posible resolver algunas cuestiones que no tenían respuesta dentro de la lógica aristotélica; una de sus más grandes aportaciones. No obstante, es más reconocido por las leyes que llevan su nombre.

Asimismo, en estas páginas se establecen y desarrollan algunos teoremas importantes.

Teorema de la simplificación

$$\text{a) } a + (a' \cdot b) = a + b$$
$$\text{b) } a \cdot (a' + b) = a \cdot b$$
$$\forall\, a, b, \text{ y } c \in \mathbf{B}.$$

Demostración

a) $a + a' = 1$ por B5

$(a + a') \cdot b = b$ por B1

$(a \cdot b) + (a' \cdot b) = b$ por B3

$a + (a \cdot b) + (a' \cdot b) = a + b$ Sumando a

$a + (a' \cdot b) = a + b$ Ley de la absorción

b) $a \cdot a' = 0$ por B5

$(a \cdot a') + b = b$ por B1

$(a + b) \cdot (a' + b) = b$ por B3

$a \cdot (a + b) \cdot (a' + b) = a \cdot b$ Sumando a

$a \cdot (a' + b) = a \cdot b$ Ley de la absorción

Teorema del complemento único

Para $\forall\, a \in \mathbf{B}$, su complemento a' es único.

Demostración

Supóngase que se tienen dos complementos para a. Sean y dichos complementos.

Como y son complementos de a se debe cumplir que:

a) $a + a'_1 = 1$; $a + a'_2 = 1$ por B5

b) $a \cdot a'_1 = 0$; $a \cdot a'_2 = 0$ por B5

Para demostrar el incíso a) se tiene que:

$$\begin{aligned}
a'_2 &= a'_1 \cdot 1 && \text{por B1}\\
&= a'_1 \cdot (a + a'_2) && \text{por B5}\\
&= a'_1 \cdot a + a'_1 \cdot a'_2 && \text{por B3}\\
&= 0 + a'_1 \cdot a'_2 && \text{por B5}\\
&= a \cdot a'_2 + a'_1 \cdot a'_2 && \text{por B5}\\
&= (a + a'_1) \cdot a'_2 && \text{por B3}\\
&= 1 \cdot a'_2 && \text{por B5}\\
&= a'_2 && \text{por B1}
\end{aligned}$$

Ahora, para demostrar el incíso b) se tiene que:

$$\begin{aligned}
a'_2 &= a'_1 + 0 && \text{por B1}\\
&= a'_1 + (a \cdot a'_2) && \text{por B5}\\
&= a'_1 + a \cdot a'_1 + a'_2 && \text{por B3}\\
&= 1 \cdot a'_2 + a'_1 && \text{por B5}\\
&= a + a'_2 \cdot a'_1 + a'_2 && \text{por B5}\\
&= (a \cdot a'_1) + a'_2 && \text{por B3}\\
&= 0 + a'_2 && \text{por B5}\\
&= a'_2 && \text{por B1}
\end{aligned}$$

Por tanto, el complemento de cualquier elemento de ***B*** siempre es único.

Principio de dualidad

El álgebra booleana ***B*** satisface el principio de dualidad, que a la letra dice:
Por tanto, basta demostrar uno de los enunciados, para luego deducir el otro por dualidad.
Con base en esta definición del principio de dualidad, puede observarse que en la definición de álgebra de Boole las propiedades básicas en sus incisos b) son duales de los incisos a) y viceversa.

Nota

Todo enunciado deducible de las propiedades del álgebra booleana es válido si se intercambian los símbolos $+$ y $\cdot$, y los elementos 0 y 1, entre sí.

Ejemplo

Obtener el dual del enunciado:

$$(1 + a) \cdot (b + 0) = b$$

Solución

El dual del enunciado anterior es:

$$(0 \cdot a) + (b \cdot 1) = b$$

Además, se tiene que el dual de cualquier teorema en el álgebra booleana también es un teorema.

Así, en el ejemplo anterior solo sería suficiente demostrar el primer enunciado para que quede demostrado por dualidad el segundo o viceversa, aunque también es posible demostrarlo de manera independiente.

Como se puede observar, en las propiedades adicionales del álgebra booleana y en el teorema de simplificación se han demostrado tanto el inciso a) como el b), pero bastaría con haber utilizado el principio de dualidad para demostrar el inciso b) en cada caso.

9.3 Funciones booleanas o funciones lógicas

En el capítulo 1 de este libro se presenta el concepto de función, mismo que será aplicado en álgebra booleana.

Antes de continuar, es necesario definir algunos conceptos que se utilizan en forma amplia a lo largo de este tema.

Constante lógica o booleana

Una constante lógica es cualquier elemento del conjunto ***B***, es decir 0 o 1.

Variable lógica o booleana

Una variable x que solo puede tomar valores de 0 o 1 se denomina *variable lógica* o *variable booleana* y representa ya sea un elemento de ***B*** o una expresión booleana completa.

EJEMPLO

Sea la expresión:

$$x = (a + b)' \cdot c'$$

En esta expresión, la variable x es una variable lógica, ya que solo puede tomar el valor de 0 o 1. Lo mismo ocurre con a, b y c que también son variables lógicas.

Literal

Es toda ocurrencia de una variable, ya sea complementada o sin complementar, en una expresión de lógica.

EJEMPLO

Sea la expresión lógica:

$$a' \cdot b + c \cdot a + d + b' \cdot 1$$

Donde:

a, b, c y d son variables.

a, b, c, d, a' y b' son literales.

1 es una constante.

Funciones booleanas

Se llama **función booleana** o **función lógica** F a todo conjunto de variables lógicas relacionadas entre sí por una expresión que representa *la combinación de un conjunto finito de símbolos, mediante la representación de constantes o variables unidos por las operaciones producto lógico, suma lógica o sus complementos*.

Las funciones booleanas se describen con una expresión del álgebra booleana.

EJEMPLO

Sea la expresión booleana:

$$F(a, b, c) = a \cdot b + a' \cdot c + a \cdot b'$$

Esta es una función booleana.

Tipos de términos de una función booleana

Hay diferentes tipos de términos en una función booleana, entre los principales se tienen los siguientes:

- **Término producto:** es una expresión lógica que consiste en un conjunto de variables (o sus complementos) unidas por productos lógicos. Por ejemplo:

$$F(a, b, c) = a \cdot b$$

- **Término suma:** es una expresión lógica que consiste en un conjunto de variables (o sus complementos) unidas por las sumas lógicas. Por ejemplo:

$$F(a, b, c) = a + b'$$

- **Término mínimo o MINTERM :** es una expresión lógica que consiste en un conjunto de **TODAS** las variables (o sus complementos) unidas por productos lógicos. Por ejemplo:

$$F(a, b, c) = a' \cdot b \cdot c$$

- **Término máximo o MAXTERM :** es una expresión lógica que consiste en un conjunto de **TODAS** las variables (o sus complementos) unidas por sumas lógicas. Por ejemplo:

$$F(a, b, c) = a' + b' + c$$

Cuando una función booleana se expresa en forma de suma de *MINTERM*, se denomina **suma de expansión de productos** o **forma normal disyuntiva** (FND).

Ahora bien, cuando una función booleana se expresa en forma de producto de *MAXTERM*, se denomina **producto de expansión de sumas** o **forma normal conjuntiva** (FNC).

Además, con n variables lógicas se pueden formar 2^n *MINTERM* y 2^n *MAXTERM*; un ejemplo de esta situación se presenta en la tabla 9.2.

Representación de las funciones booleanas

Las funciones booleanas pueden representarse de dos formas diferentes: mediante una ***tabla de verdad*** o en ***forma canónica***.

Tablas de verdad

La manera más fácil de representar una función booleana es mediante una tabla de verdad, ya que en este tipo de tabla se muestran los valores lógicos de salida para cada combinación de las variables lógicas de entrada.

Las tablas de verdad de funciones booleanas son similares a las que se tratan en el capítulo 2, a excepción de que en este caso se sustituye la V por 1 y la F por 0.

Ejemplo

Dada la función lógica:

$$F(a, b, c) = a + (b \cdot c')$$

Obtener su tabla de verdad.

Solución

En la tabla 9.1 se muestra la tabla de verdad de la función lógica $a + (b \cdot c')$.

Tabla 9.1 Tabla de verdad de la función lógica $a + (b \cdot c')$.

a	b	c	$F(a, b, c)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Formas canónicas de una función

Cuando una función booleana se halla expresada en forma normal disyuntiva o en forma normal conjuntiva se dice que está en forma canónica. Esto significa que toda función booleana puede expresarse en alguna de estas dos formas canónicas.

Estas formas de una función booleana pueden simplificarse mediante la aplicación directa de las leyes del álgebra booleana, o bien de manera sistemática a través de métodos de reducción, los cuales se analizan más adelante.

Forma canónica disyuntiva

Es aquella forma canónica constituida de manera exclusiva por *MINTERMS* sumados que aparecen una sola vez.

EJEMPLO

Sea la función booleana:

$$F(a, b, c) = a'b'c + ab'c' + ab'c + abc' + abc$$

Esta función booleana está en forma canónica disyuntiva.

Para simplificar la escritura en forma de suma canónica de productos se utiliza una notación especial. Esto es, a cada *MINTERM*, denotado como m_i, se le asocia un número binario de n bits resultantes de considerar como 0 las variables complementadas y como 1 las variables sin complementar.

EJEMPLO

Al *MINTERM* $a'b'c$, le corresponde la combinación:

$$a = 0, b = 0, c = 1$$

Como se puede observar, esta combinación representa el número binario 001, cuyo valor decimal es 1. Por tanto, a este *MINTERM* se le identifica como m_1.

De esta forma, la función lógica:
$F(a, b, c) = a'b'c + ab'c' + ab'c + abc' + abc$

Se puede expresar como:

$$F(a, b, c) = \sum_m (1, 4, 5, 6, 7)$$

Esto significa que es la sumatoria de los *MINTERM* 1, 4, 5, 6, 7.

Forma canónica conjuntiva

Es aquella constituida exclusivamente por *MAXTERM* multiplicados que aparecen una sola vez.

Ejemplo

Sea la función booleana:

$$F(a, b, c) = (a + b + c)(a + b' + c)(a + b' + c')$$

Esta función booleana está en forma canónica conjuntiva.

De manera análoga al caso anterior, la expresión de la función booleana se puede simplificar indicando los *MAXTERM*; sin embargo, en este caso se hace al contrario del presentado antes.

Esto es, a cada *MAXTERM*, denotado como M_i, se le asocia un número binario de n bits resultantes de considerar como 1 las variables complementadas y como 0 las variables sin complementar.

Ejemplo

Al *MAXTERM* $a' + b + c$ le corresponde la combinación:

$$a = 1, b = 0, c = 0$$

Como se puede observar, esta combinación representa el número binario 100, cuyo valor decimal es 4. Por tanto, a este *MAXTERM* se le identifica como M_4.

De esta forma, la función lógica:

$$F(a, b, c) = (a + b + c)(a + b' + c)(a + b' + c')$$

se puede expresar como:

$$F(a, b, c) = \prod_M (0, 2, 3)$$

Esto significa que es el producto de los *MAXTERM* 0, 2, 3.

Además, a cada *MINTERM* se le asocia con la combinación de entrada, para la que la función produciría un 1, y a cada *MAXTERM* con la combinación de salida, para la que produciría un 0.

Ejemplo

Sea la función lógica:

$F(a, b, c) = a \cdot (b + c)$

Obtener los *MINTERM* y los *MAXTERM* asociados.

Solución

En la tabla 9.2 se muestran los *MINTERM* y los *MAXTERM* asociados con cada combinación en una tabla de verdad de tres variables lógicas, con $2^3 = 8$ *MINTERM* y *MAXTERM*.

Tabla 9.2 MINTERM y MAXTERM de la función booleana $a \cdot (b + c)$.

Valor decimal	a	b	c	$F(a, b, c)$	MINTERM	MAXTERM
0	0	0	0	0	$m_0 = a'b'c'$	$M_0 = a+b+c$
1	0	0	1	0	$m_1 = a'b'c$	$M_1 = a+b+c'$
2	0	1	0	0	$m_2 = a'bc'$	$M_2 = a+b'+c$
3	0	1	1	0	$m_3 = a'bc$	$M_3 = a+b'+c'$
4	1	0	0	0	$m_4 = ab'c'$	$M_4 = a'+b+c$
5	1	0	1	1	$m_5 = ab'c$	$M_5 = a'b+c'$
6	1	1	0	1	$m_6 = abc'$	$M_6 = a'+b'+c$
7	1	1	1	1	$m_7 = abc$	$M_7 = a'+b'+c'$

De acuerdo con la tabla 9.2, para determinar el término producto o suma, para los *MINTERMS* cada variable sin complementar se asocia con un 1 y cada variable complementada se asocia con 0, mientras que para los *MAXTERM* la regla es la inversa.

Ejemplo

Expresar como una suma de *MINTERM* la función booleana:

$$F(a, b, c) = a + b' \cdot c$$

Solución

Primero, se obtiene la tabla de verdad de la expresión y luego se toman los *MINTERM* (véase tabla 9.3).

Enseguida, se evalúa la función para todas las combinaciones y se toman los *MINTERM* de la tabla para los cuales la función vale 1.

Tabla 9.3 Tabla de verdad de la función lógica $a + b' \cdot c$ con MINTERM.

Valor decimal	a	b	c	$F(a, b, c)$	MINTERM
0	0	0	0	0	
1	0	0	1	1	$m_1 = a'b'c$
2	0	1	0	0	
3	0	1	1	0	
4	1	0	0	1	$m_4 = ab'c'$
5	1	0	1	1	$m_5 = ab'c$
6	1	1	0	1	$m_6 = abc'$
7	1	1	1	1	$m_7 = abc$

Entonces, la respuesta es:

$$F(a, b, c) = a'b'c + ab'c' + ab'c + abc' + abc$$

Otra notación que se puede utilizar es:

$$F(a, b, c) = \sum_m (1, 4, 5, 6, 7)$$

Que significa que es la sumatoria de los *MINTERM* 1, 4, 5, 6, 7.

Teoremas de expansión canónica

Otra forma de obtener una expresión booleana como una suma de *MINTERM* o como producto de *MAXTERM* es a través de la aplicación de los teoremas de expansión canónica para las variables faltantes, los cuales se describen a continuación.

Teorema 1

Para obtener la forma canónica de una función suma de productos se multiplica por un término de la forma

$$(x + x')$$

donde falte un literal, para que el término sea canónico.

Teorema 2

Para obtener la forma canónica de una función producto de sumas se suma un término de la forma

$$(x \cdot x')$$

donde falte un literal, para que el término sea canónico.

Ejemplo

Expresar la siguiente función booleana como una suma de *MINTERM* mediante el uso de los teoremas de expansión canónica:

$$F(a, b, c) = a + b' \cdot c$$

Solución

$$a + b'c$$

$$a(b + b')(c + c') + b'c(a + a')$$

$$(ab + ab')(c + c') + b'ca + b'c\,a'$$

$$abc + abc' + ab'c + ab'c' + ab'c + a'b'c$$

$$a'b'c + ab'c' + ab'c + abc' + abc$$

Entonces:

$$F(a, b, c) = a'b'c + ab'c' + ab'c + abc' + abc$$

Como se observa, este es el mismo resultado obtenido en el ejemplo anterior.

Ejemplo

Expresar la siguiente función booleana como un producto de *MAXTERM*:

$$F(a, b, c) = a + b' \cdot c$$

Solución

Hay dos formas de resolver este problema: 1) construyendo una tabla de verdad o 2) con manipulación algebraica mediante el uso de los teoremas de expansión canónica.

Forma 1

Primero, se obtiene la tabla de verdad de la función y luego se toman los *MAXTERM* desde dicha tabla de verdad (véase tabla 9.4).

Enseguida, se evalúa la función para todas las combinaciones y se toman los *MAXTERM* de la tabla para los cuales la función lógica vale 0.

Tabla 9.4 Tabla de verdad de la función lógica $a + b' \cdot c$ con MAXTERM.

Valor decimal	a	b	c	$F(a, b, c)$	MAXTERM
0	0	0	0	0	$M_0 = a+b+c$
1	0	0	1	1	
2	0	1	0	0	$M_2 = ab'c$
3	0	1	1	0	$M_3 = ab'c'$
4	1	0	0	1	
5	1	0	1	1	
6	1	1	0	1	
7	1	1	1	1	

Entonces, la respuesta es:

$$F(a, b, c) = (a + b + c)(a + b' + c)(a + b' + c')$$

Que puede expresarse como:

$$F(a, b, c) = \prod\nolimits_M (0, 2, 3)$$

Esto significa que es el producto de los *MAXTERM* 0, 2, 3.

Forma 2

Mediante manipulación algebraica, utilizando los teoremas de expansión canónica, se tiene que:

$a + b'c$

$(a + b')(a + c)$

$(a + b' + cc')(a + c + bb')$

$(a + b' + c)(a + b' + c')\,(a + c + b)(a + c + b')$

$(a + b' + c)(a + b' + c')\,(a + b + c)(a + b' + c)$

$(a + b' + c)(a + b' + c')(a + b + c)$

$(a + b + c)(a + b' + c)(a + b' + c')$

Entonces:

$$F(a, b, c) = (a + b + c)(a + b' + c)(a + b' + c')$$

Como se observa, este es el mismo resultado que el obtenido en la primera forma.

De acuerdo con lo visto antes, es muy importante observar la simetría que existe entre la suma de productos y el producto de sumas de una expresión. Así pues, si m_i es el *MINTERM* para la combinación i y M_i es el *MAXTERM*, se tiene que:

$$M_i = m_i'$$
$$m_i = M_i'$$

EJEMPLO

Sea el *MAXTERM*:

$$M_1 = a + b + c'$$

Si:

$$m_1 = a'b'c$$

Entonces, se tiene que:

$$m_1' = a + b + c'$$

EJEMPLO

Sea el *MINTERM*:

$$m_4 = ab'c'$$

Si:

$$M_4 = a' + b + c$$

Entonces, se tiene que:

$$M_4' = ab'c'$$

La transformación de una fórmula de *MINTERM* en otra de *MAXTERM* se basa en la del doble complemento, esto es:

$$(F')' = F$$

Además, para convertir de una forma canónica a otra se intercambian los signos Σ y Π, y se reemplazan los números correspondientes a las combinaciones no incluidas en la forma original.

Ejemplo

Sea la forma canónica de la suma de productos:

$$\sum\nolimits_m (0, 1, 3, 5, 7)$$

Convertir esta en forma canónica de productos de sumas.

Solución

La forma canónica equivalente en productos de sumas es:

$$\prod\nolimits_M (2, 4, 6)$$

Por tanto:

$$\sum\nolimits_m (0, 1, 3, 5, 7) = \prod\nolimits_M (2, 4, 6)$$

9.4 Circuitos lógicos

Al interior de la electrónica digital, se suscitan, con mucha regularidad, un gran número de problemas por resolver. Por ejemplo, es muy común que al diseñar un circuito electrónico se necesite tener el valor opuesto al de un punto determinado, o que cuando un cierto número de pulsadores estén activados, una salida permanezca apagada.

Todas estas situaciones pueden expresarse mediante ceros y unos, y tratarse a través de circuitos lógicos (o circuitos digitales).

Un circuito lógico es un dispositivo que tiene una o más entradas y exactamente una salida. En cada instante, cada entrada tiene un valor, 0 o 1; estos datos son procesados por el circuito para dar un valor en su salida, 0 o 1.

Los valores 0 y 1 pueden representar ciertas situaciones físicas, como presencia y/o ausencia de voltaje en un conductor (véase figura 9.4).

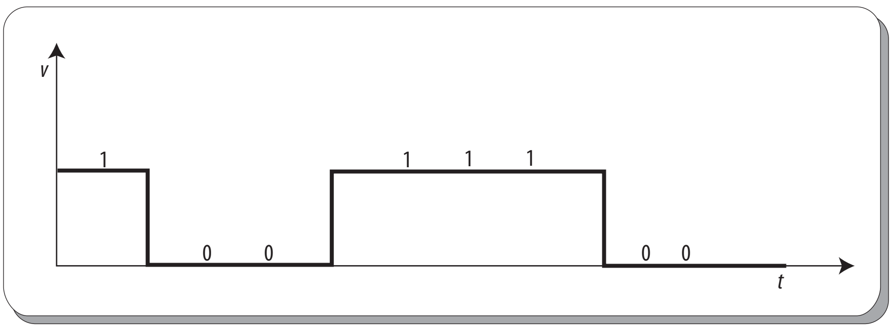


Figura 9.4 Presencia y ausencia de voltaje en un conductor.

Los circuitos lógicos se construyen a partir de ciertos circuitos elementales, denominados compuertas lógicas. Desde un punto de vista práctico, se puede considerar a cada compuerta como una caja negra, en la que se introducen valores digitales en sus entradas, mientras que el valor del resultado aparece en la salida.

En un circuito lógico, cada compuerta tiene asociada una tabla de verdad, la cual expresa, en forma de lista, para cada combinación posible de estados en la entrada, el estado de su salida.

Compuertas lógicas básicas

Existen tres tipos básicos de compuertas lógicas: *OR*, *AND* y *NOT*, cada una de las cuales realiza una determinada operación y se indica mediante símbolos especiales.

1. **Compuerta lógica *OR***

   Esta compuerta puede recibir dos o más entradas booleanas (unos y/o ceros) y produce una salida igual a la suma booleana de los valores de las variables lógicas de entrada. Donde:

$$x + y \begin{cases} 1 \text{ si } x = 1 \text{ o } y = 1 \\ 0 \text{ en cualquier otro caso} \end{cases}$$

El símbolo con dos entradas de esta compuerta se observa en la figura 9.5.

En el caso de esta compuerta, se utiliza como operador el mismo de la suma booleana, aunque también se puede utilizar el operador $\vee$.

Por su parte, el símbolo de esta compuerta con varias entradas se observa en la figura 9.6.

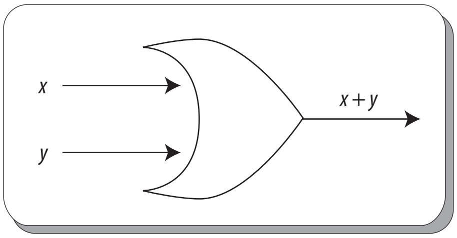


Figura 9.5 Símbolos de la compuerta lógica *OR* con dos entradas.

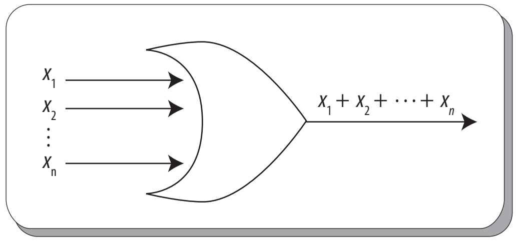


Figura 9.6 Símbolo de la compuerta lógica *OR* con más de dos entradas.

Su tabla de verdad se muestra en la tabla 9.5.

Tabla 9.5 Tabla de verdad de la compuerta lógica *OR*.

x	y	x + y
1	1	1
1	0	1
0	1	1
0	0	0

2. **Compuerta lógica *AND***

Esta compuerta puede recibir dos o más entradas booleanas (unos y/o ceros) y produce una salida igual al producto booleano · de los valores de las variables lógicas de entrada. Donde:

$$x \cdot y \begin{cases} 1 \text{ si } x = 1 \text{ o } y = 1 \\ 0 \text{ en cualquier otro caso} \end{cases}$$

El símbolo con dos entradas de esta compuerta lógica se observa en la figura 9.7.

En el caso de esta compuerta, se utiliza como operador el mismo del producto booleano; además, también se puede utilizar el operador $\wedge$ o eliminarlo al igual que en el producto booleano.

Por otra parte, el símbolo con varias entradas de esta compuerta se ve en la figura 9.8.

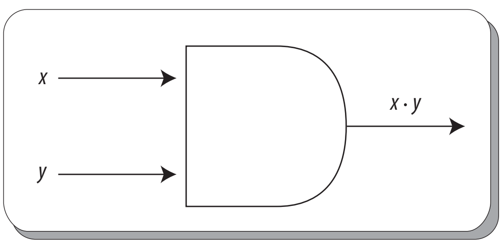


Figura 9.7 Símbolo de la compuerta lógica *AND* con dos entradas.

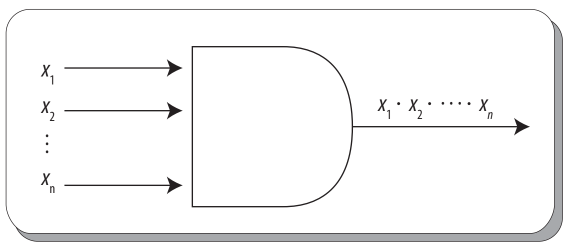


Figura 9.8 Símbolo de la compuerta lógica *AND* con más de dos entradas.

La tabla de verdad de esta compuerta lógica se muestra en la tabla 9.6.

Tabla 9.6 Tabla de verdad de la compuerta lógica *AND*.

x	y	$x \cdot y$
1	1	1
1	0	0
0	1	0
0	0	0

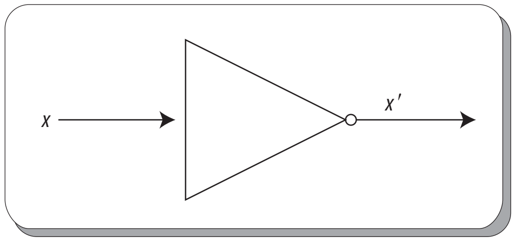


Figura 9.9 Símbolo de la compuerta lógica *NOT*.

3. **Compuerta NOT**

Este tipo de compuertas solo acepta una entrada booleana (uno o cero) y produce el complemento de este valor como salida. Donde:

$$x' = \begin{cases} 1 \text{ si } x = 0 \\ 0 \text{ si } x = 1 \end{cases}$$

El símbolo de esta compuerta se muestra en la figura 9.9. Su operador es ', aunque también se pueden utilizar los operadores o ~.
La tabla de verdad de esta compuerta se observa en la tabla 9.7.

Tabla 9.7 Tabla de verdad de la compuerta lógica NOT.

x	x'
1	0
0	1

Compuertas lógicas derivadas

Es importante destacar aquí que existen otras compuertas lógicas, las cuales, aunque no son básicas, son muy útiles al momento de combinarse en diferentes expresiones lógicas.

1. **Compuerta lógica *NOR***

Esta compuerta puede recibir dos o más entradas booleanas (unos y/o ceros) y produce una salida igual al complemento de la suma booleana de los valores de las variables lógicas de entrada. Donde:

$$(x + y) = \begin{cases} 0 \text{ si } x = 1 \text{ o } y = 1 \\ 1 \text{ en caso contrario} \end{cases}$$

El símbolo con dos entradas de esta compuerta se representa en la figura 9.10.
Esta compuerta equivale a una compuerta *OR* seguida de una compuerta *NOT* (véase figura 9.11).

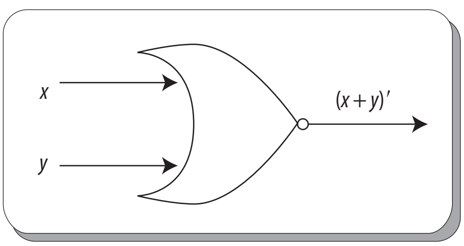


Figura 9.10 Símbolo de la compuerta lógica *NOR* con dos entradas.

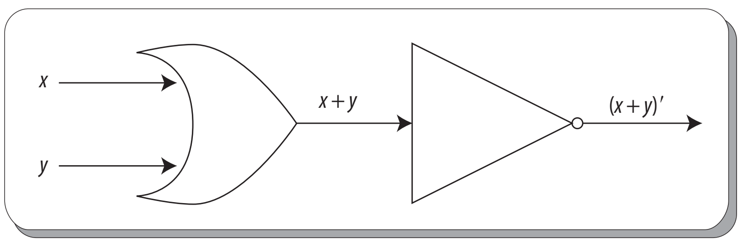


Figura 9.11 Equivalencia de la compuerta lógica *NOR* con dos entradas.

La tabla de verdad de la compuerta *NOR* se muestra en la tabla 9.8.

Tabla 9.8 Tabla de verdad de la compuerta lógica *NOR*.

x	y	$(x + y)'$
1	1	0
1	0	0
0	1	0
0	0	1

2. **Compuerta lógica *NAND***

Esta compuerta puede recibir dos o más entradas booleanas (unos y/o ceros) y produce una salida igual al complemento del producto booleano de los valores de las variables lógicas de entrada. Donde:

$$(x \cdot y)' = \begin{cases} 0 \text{ si } x = 1 \text{ o } y = 1 \\ 1 \text{ en cualquier otro caso} \end{cases}$$

El símbolo con dos entradas de esta compuerta lógica se observa con detalle en la figura 9.12.
Esta compuerta equivale a una compuerta *AND* seguida de una compuerta *NOT* (véase figura 9.13).

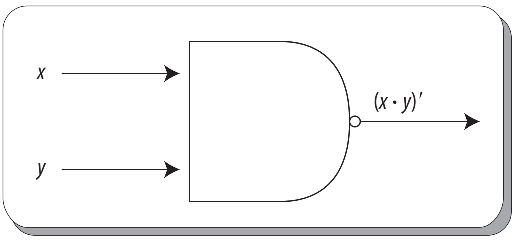


Figura 9.12 Compuerta lógica *NAND* con dos entradas.

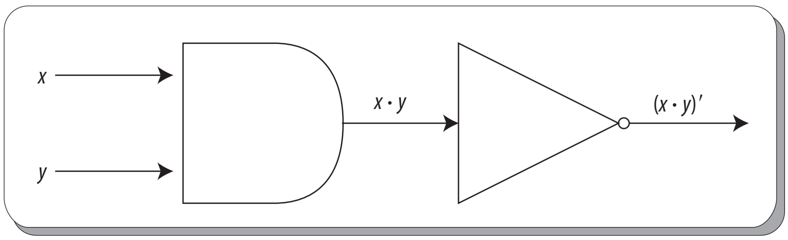


Figura 9.13 Equivalencia de la compuerta lógica *NAND* con dos entradas.

La tabla de verdad de esta compuerta lógica se muestra en la tabla 9.9.

Tabla 9.9 Tabla de verdad de la compuerta lógica *NAND*.

x	y	$(x \cdot y)'$
1	1	0
1	0	1
0	1	1
0	0	1

3. **Compuerta lógica *XOR***

Esta compuerta puede recibir dos o más entradas booleanas (unos y/o ceros) y produce una salida igual a cero si las variables de entrada son iguales y uno si son diferentes. Esta compuerta equivale a la *OR*, exclusiva del cálculo proposicional; donde:

$$(x \cdot y) = \begin{cases} 0 \text{ si } x = y \\ 1 \text{ en cualquier otro caso} \end{cases}$$

El símbolo con dos entradas de esta compuerta se muestra en la figura 9.14.
La tabla de verdad de la compuerta lógica *XOR* se muestra en la tabla 9.10.

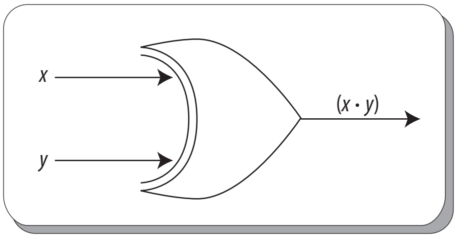


Figura 9.14 Compuerta lógica *XOR* con dos entradas.

Tabla 9.10 Tabla de verdad de la compuerta lógica XOR.

x	y	$(x \cdot y)$
1	1	0
1	0	1
0	1	1
0	0	0

Esta compuerta equivale a la expresión lógica:

$$x' \cdot y + x \cdot y'$$

que se representa en la figura 9.15. Para comprobar esta equivalencia basta con obtener la tabla de verdad de dicha expresión (tabla 9.11) y compararla con la de la *XOR* y verificar que son idénticas.

Tabla 9.11 Tabla de verdad de la expresión $x' \cdot y + x \cdot y'$.

x	y	x'	y'	$x' \cdot y$	$x \cdot y'$	$x' \cdot y + x \cdot y'$
1	1	0	0	0	0	0
1	0	1	1	0	1	1
0	1	1	0	1	0	1
0	0	1	1	0	0	0

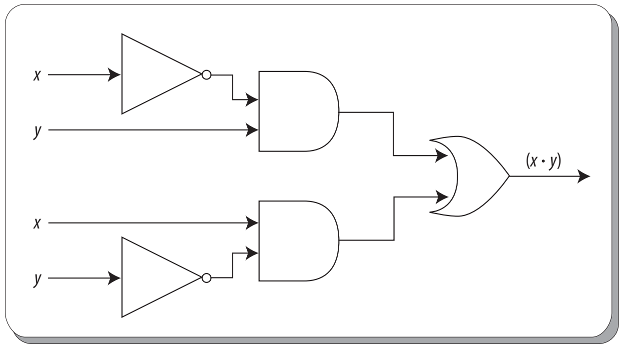


Figura 9.15 Equivalencia de la compuerta lógica *XOR* con dos entradas.

Circuitos lógicos

Las compuertas lógicas descritas antes pueden combinarse entre sí para formar circuitos lógicos y simbolizar diferentes expresiones lógicas.

Ejemplo

Sea la expresión lógica:

$$X = (x + y)' \cdot z'$$

Representar el circuito lógico correspondiente mediante el uso de las compuertas lógicas.

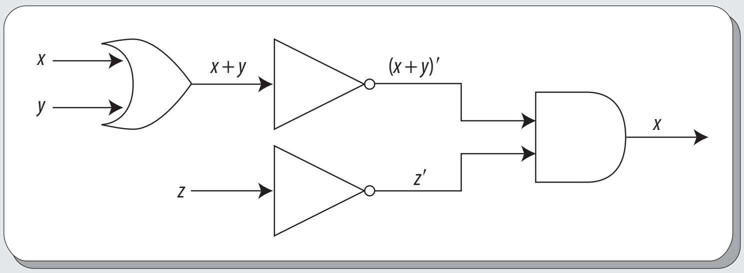


Figura 9.16 Circuito lógico utilizando compuertas lógicas básicas.

Solución

El circuito lógico correspondiente a la expresión lógica anterior puede representarse utilizando exclusivamente compuertas lógicas básicas (véase figura 9.16) o utilizando compuertas lógicas derivadas (véase figura 9.17).

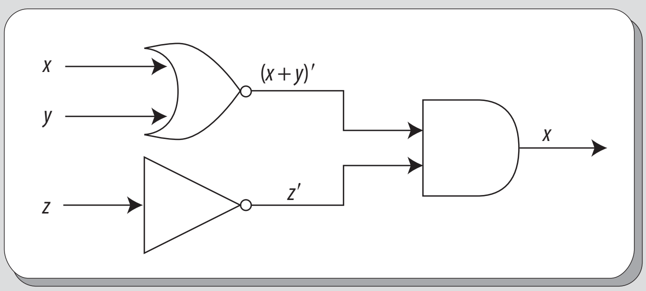


Figura 9.17 Circuito lógico utilizando compuertas lógicas derivadas.

Es fácil observar que las tablas de verdad correspondientes a las compuertas lógicas *OR*, *AND* y *NOT* son, respectivamente, idénticas a las tablas de verdad de la disyunción $\vee$, la conjunción $\wedge$ y la negación **~**, en el cálculo proposicional visto en el capítulo 2, solo que en estas se cambia V y F por 1 y 0, respectivamente.

Por tanto, cualquier expresión lógica tiene su equivalencia en el cálculo proposicional.

Ejemplo

Sea la expresión lógica:

$$X = (x_1 \cdot x_2 + x_3)'$$

Mediante el uso de compuertas lógicas representar el circuito lógico correspondiente y obtener su equivalencia en el cálculo proposicional.

Solución

El circuito lógico correspondiente a la expresión lógica anterior se representa en la figura 9.18.

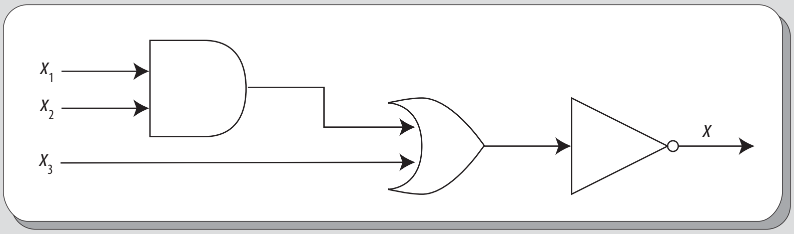


Figura 9.18 Circuito lógico de la expresión lógica $X = (x_1 \cdot x_2 + x_3)'$.

La expresión lógica equivalente en el cálculo proposicional es:

$$\sim((p \wedge q) \vee r)$$

Además, también es posible representar expresiones lógicas más complejas y obtener su equivalencia en el cálculo proposicional.

Ejemplo

Sea la expresión lógica:

$$X = (((x_1 + x_2 + x_3)' + x_4 \cdot x_5) + x_4 \cdot x_5 \cdot (x_5)')'$$

Utilizando las compuertas lógicas representar el circuito lógico correspondiente y obtener su equivalencia en el cálculo proposicional.

Solución

El circuito lógico correspondiente a la expresión lógica anterior se muestra en la figura 9.19.

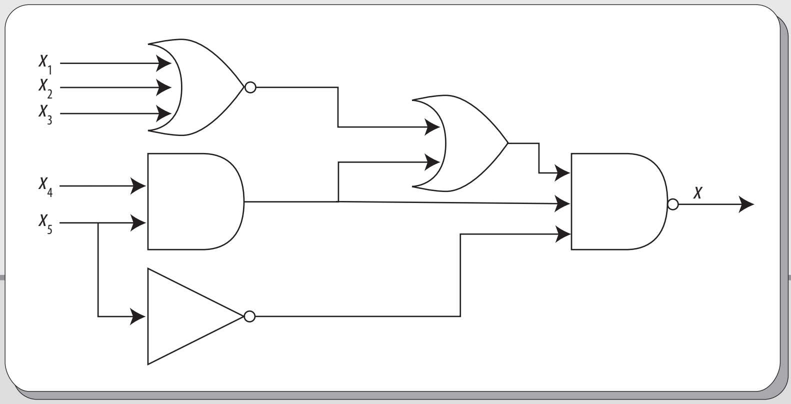


Figura 9.19 Circuito lógico de la expresión lógica $X = (((x_1 + x_2 + x_3)' + x_4 \cdot x_5) + x_4 \cdot x_5 \cdot (x_5)')'$.

La expresión lógica equivalente en el cálculo proposicional es:

$$\sim((\sim(p \vee q \vee r) \vee (s \wedge t)) \vee s \wedge t \wedge \sim t)$$

9.5 Propiedades de los circuitos lógicos

Luego de estudiar las compuertas lógicas *OR*, *AND* y *NOT* (véase sección 9.4), resulta pertinente resaltar que al combinarse estas pueden implementarse como circuitos lógicos, además de que se puede obtener la equivalencia de los circuitos lógicos en el cálculo proposicional.

Ahora, se analizan algunas de las propiedades de los circuitos lógicos utilizando las compuertas lógicas. Dichas propiedades pueden demostrarse mediante el uso de los valores de las variables lógicas de las tablas de verdad de cada una de las compuertas.

Si $+$ y $\cdot$ son los operadores binarios de las compuertas lógicas *OR* y *AND*, respectivamente, y' es el operador unario de la compuerta lógica *NOT*, entonces se deben cumplir las siguientes propiedades sobre cualquier x_1, x_2, y $x_3 \in \{1, 0\}$.

1. **Identidad**

a) $x_1 + 0 = x_1$
b) $x_1 \cdot 1 = x_1$

Demostración

Si se supone que en la figura 9.20*i*) $x_2 = 0$ y $x_3 = 0$; es decir, $x_2 + x_3 = 0$, entonces, sin importar el valor lógico de x_1, la salida correspondiente siempre será igual a x_1. Con lo que se comprueba el inciso a).

Ahora, si se supone que en la figura 9.20*ii*) $x_2 = 1$ y $x_3 = 1$; es decir, $x_2 \cdot x_3 = 1$, entonces, sin importar el valor lógico de x_1, la salida correspondiente siempre será igual a x_1. Con lo que queda comprobado el inciso b).

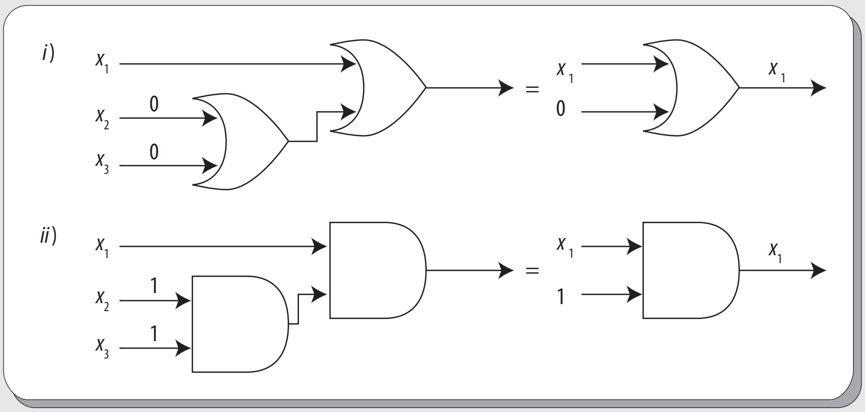


Figura 9.20 Circuitos lógicos para la propiedad identidad.

2. **Propiedad conmutativa**

a) $x_1 + x_2 = x_2 + x_1$
b) $x_1 \cdot x_2 = x_2 \cdot x_1$

Demostración

En este caso, tanto en la figura 9.21*i*) como en la figura 9.21*ii*), basta con observar las tablas 9.5 y 9.6, correspondientes a las tablas de verdad de las compuertas *OR* y *AND*, respectivamente, para verificar que se cumple dicha propiedad tanto en el inciso a) como en el b).

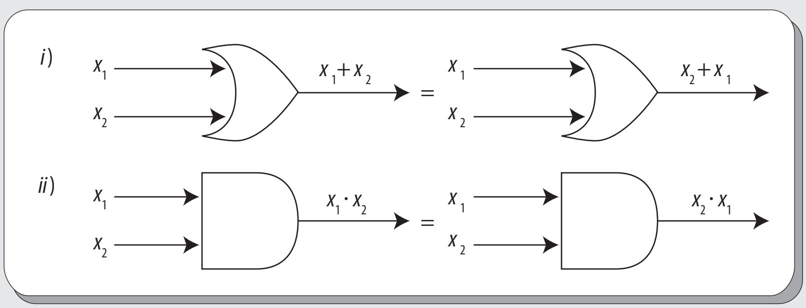


Figura 9.21 Circuitos lógicos para la propiedad conmutativa.

3. **Propiedad distributiva**

$$a)\ x_1 + (x_2 \cdot x_3) = (x_1 + x_2) \cdot (x_1 + x_3)$$
$$b)\ x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$$

DEMOSTRACIÓN

Para demostrar esta propiedad, la figura 9.22 *i*) nos permite obtener las tablas de verdad para ambos lados de la igualdad (véanse tablas 9.12 y 9.13), además de que en esta se observa que tienen los mismos valores de verdad de salida, con lo que se demuestra el inciso a).

Enseguida, se obtienen las tablas de verdad para *ii*) de la figura 9.22 (véanse tablas 9.14 y 9.15), donde se observa que se tienen los mismos valores de verdad de salida, con lo que también se comprueba el inciso b).

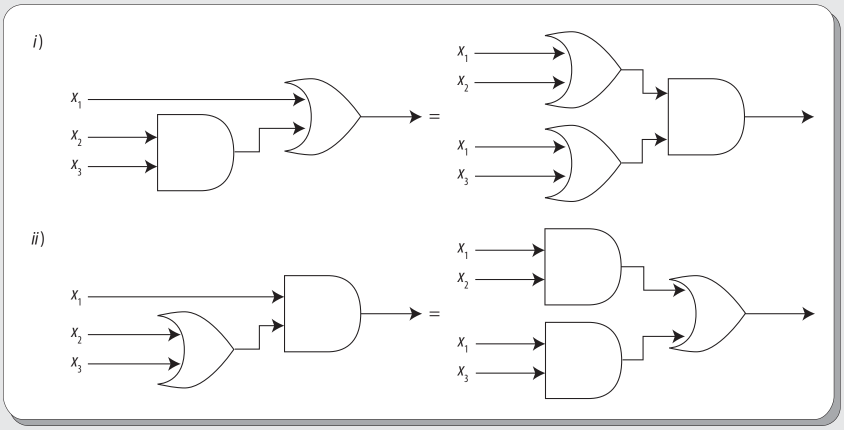


Figura 9.22 Circuitos lógicos para la propiedad distributiva.

Tabla 9.12 Tabla de verdad de la operación lógica $x_1 + (x_2 \cdot x_3)$.

x_1	x_2	x_3	$x_2 \cdot x_3$	$x_1 + (x_2 \cdot x_3)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Tabla 9.13 Tabla de verdad de la operación lógica $(x_1 + x_2)\cdot(x_1 + x_3)$.

x_1	x_2	x_3	x_1+x_2	x_1+x_3	$(x_1 + x_2)\cdot(x_1 + x_3)$
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

Tabla 9.14 Tabla de verdad de la operación lógica $x_1 \cdot (x_2 + x_3)$.

x_1	x_2	x_3	$x_2 + x_3$	$x_1 \cdot (x_2 + x_3)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Tabla 9.15 Tabla de verdad de la operación lógica $(x_1 \cdot x_2) + (x_1 \cdot x_3)$.

x_1	x_2	x_3	$x_1 \cdot x_2$	$x_1 \cdot x_3$	$(x_1 \cdot x_2) + (x_1 \cdot x_3)$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

4. **Propiedad asociativa**

$$a)\ (x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$$
$$b)\ (x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$$

DEMOSTRACIÓN

Para la demostración de esta propiedad, al igual que para la propiedad distributiva, primero deben obtenerse las tablas de verdad (véanse tablas 9.16 y 9.17) para ambos lados de la igualdad de la figura 9.23 *i*), donde se observa que ambos tienen los mismos valores de verdad de salida, con lo que se demuestra el inciso a).

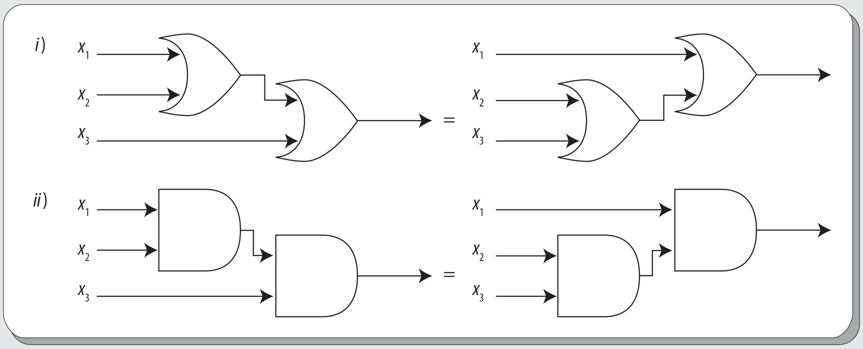


Figura 9.23 Circuitos lógicos para la propiedad asociativa.

Enseguida, también se obtienen las tablas de verdad para ambos lados de la figura 9.23 *ii*) (véanse tablas 9.18 y 9.19), donde de nuevo se observa que ambos tienen los mismos valores de verdad de salida, con lo que también se comprueba el inciso b).

Tabla 9.16 Tabla de verdad de la operación lógica $(x_1 + x_2) + x_3$.

x_1	x_2	x_3	$x_1 + x_2$	$(x_1 + x_2) + x_3$
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Tabla 9.17 Tabla de verdad de la operación lógica $x_1 + (x_2 + x_3)$.

x_1	x_2	x_3	$x_2 + x_3$	$x_1 + (x_2 + x_3)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Tabla 9.18 Tabla de verdad de la operación lógica $(x_1 \cdot x_2) \cdot x_3$.

x_1	x_2	x_3	$x_1 \cdot x_2$	$x_1 + (x_2 \cdot x_3)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	0	0
1	1	0	1	0
1	1	1	1	1

Tabla 9.18 Tabla de verdad de la operación lógica $(x_1 \cdot x_2) \cdot x_3$.

x_1	x_2	x_3	$x_2 \cdot x_3$	$x_1 \cdot (x_2 \cdot x_3)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	0
1	0	0	0	0
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

5. **Propiedad de complementos**

$$x_1 + \quad = 1$$
$$x_1 \cdot \quad = 0$$

DEMOSTRACIÓN

Para demostrar esta propiedad, tanto en la figura 9.24 *i*) como en la figura 9.24 *ii*), hay que observar las tablas 9.5 y 9.6, las cuales corresponden a las tablas de verdad de las compuertas *OR* y *AND*. Sin importar el valor lógico de x_1, se cumple tanto el inciso a) como el b).

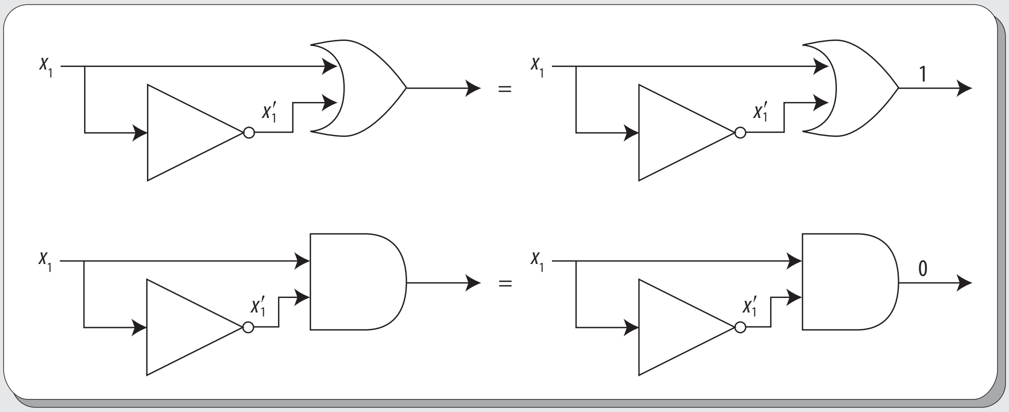


Figura 9.24 Circuitos lógicos para la propiedad de complementos.

6. **Leyes de De Morgan**

$$a)\ (x_1 + x_2)' = \quad \cdot$$
$$b)\ (x_1 \cdot x_2)' = \quad +$$

DEMOSTRACIÓN

Para demostrar esta propiedad, primero se obtiene la tabla de verdad para ambos lados de la igualdad en la figura 9.25 *i*) (véase tabla 9.20), donde se puede observar que se tienen los mismos valores de verdad de salida, con lo que se demuestra el inciso a).

Enseguida, se obtiene la tabla de verdad para la figura 9.25 *ii*) (véase tabla 9.21), donde se observa que tienen los mismos valores de verdad de salida, con lo que también se comprueba el inciso b).

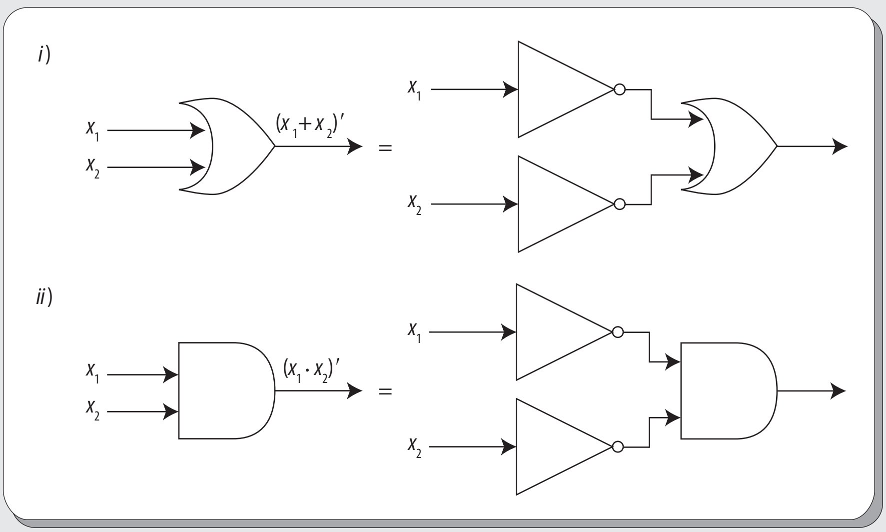


Figura 9.25 Circuitos lógicos para las Leyes de De Morgan.

Tabla 9.20 Tabla de verdad para el inciso a) de las Leyes de De Morgan.

x_1	x_2	$x_1 + x_2$	$(x_1+x_2)'$	x'_1	x'_2	$x'_1 \cdot x'_2$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

Tabla 9.21 Tabla de verdad para el inciso b) de las Leyes de De Morgan.

x_1	x_2	$x_1 \cdot x_2$	$(x_1 \cdot x_2)'$	x'_1	x'_2	$x'_1 + x'_2$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Como se deduce de la sección anterior, las propiedades de los circuitos lógicos son idénticas a las propiedades del álgebra booleana, ya que todas las operaciones de los circuitos lógicos son operaciones booleanas además de que, en ambos casos, producen salidas idénticas. Lo único que puede variar es la representación de los operadores y de las variables lógicas.

Circuitos lógicos equivalentes

Se dice que dos circuitos lógicos son equivalentes si cada uno tiene entradas $x_1, x_2, \ldots, x_n$ y una sola salida; los circuitos con las mismas entradas siempre producen las mismas salidas.

Ejemplo

Comprobar si los circuitos lógicos de las figuras 9.26 *i*) y 9.26 *ii*) son equivalentes.

Solución

Primero, se elaboran las tablas de verdad; en este caso, la tabla de la izquierda de la tabla 9.22 corresponde al circuito lógico de la figura 9.26 *i*), mientras que la de la derecha corresponde a la figura 9.26 *ii*).

Como se puede observar, las tablas de verdad tienen las mismas salidas, por lo que se dice que son circuitos lógicos equivalentes.

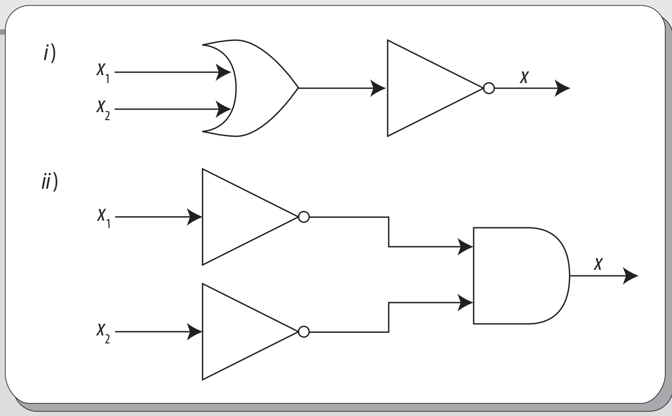


Figura 9.26 Circuitos lógicos equivalentes.

Tabla 9.22 Tablas de verdad para los circuitos lógicos i) y ii) de la figura 9.26.

x_1	x_2	$x_1 + x_2$	$(x_1 + x_2)'$	x_1	x_2	x'_1	x'_2	$x'_1 \cdot x'_2$
0	0	0	1	0	0	1	1	1
0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	0	1	0
1	1	1	0	1	1	0	0	0

9.6 Simplificación de circuitos

El proceso de la simplificación consiste en aplicar las propiedades y leyes del álgebra booleana para llegar a la expresión más simple de una expresión booleana, la cual, por lo general, se presenta en su forma de suma de productos mínima.

Ejemplo

Simplificar la expresión booleana:

$$F(a, b, c) = ab'(c + a + cb')$$

Solución

$F(a, b, c)$	$= ab'(c + a + cb')$	
	$= ab'c + ab'a + ab'cb'$	B3
	$= ab'c + ab' + ab'c$	Ley de idempotencia
	$= ab'c + ab'$	Ley de idempotencia
	$= ab'$	Ley de la absorción

Ejemplo

Simplificar la expresión booleana:

$$F(a, b, c) = a'bc' + a'bc + ab'c' + ab'c + abc$$

Solución

$F(a, b, c)$	$= a'bc' + a'bc + ab'c' + ab'c + abc$	
	$= a'b(c' + c) + ab'(c' + c) + abc$	B3
	$= (c' + c)(a'b + ab') + abc$	B3
	$= 1(a'b + ab') + abc$	B5
	$= a'b + ab' + abc$	B1
	$= a'b + a(b' + bc)$	B3
	$= a'b + a((b' + b)(b' + c))$	B3
	$= a'b + a(1(b' + c))$	B5
	$= a'b + a(b' + c)$	B1
	$= a'b + ab' + ac$	B3

Aunque de manera más estricta, todavía se tendría que:

$= a \oplus b + ac$	Definición $\oplus$

No obstante que este resultado es correcto no está expresado en sumas de productos, por lo que la simplificación es:

$$F(a, b, c) = a'b + ab' + ac$$

Expresiones booleanas minimales

Considérese una expresión booleana E. Dado que E puede representar un circuito lógico, es posible que se pretenda obtener una expresión F que, siendo equivalente a la expresión original, sea en algún sentido mínima; de esta forma, se lograría minimizar la cantidad de compuertas lógicas utilizadas para implementar la operación buscada, con la consecuente economía de recursos.

En este apartado se estudia la forma minimal de las expresiones booleanas que están en forma de suma de productos.

De este modo, si E es una expresión booleana en forma de suma de productos, E_L denota el número de literales en E (contados con sus repeticiones) y E_S denota el número de sumandos en E.

EJEMPLO

Si E es la expresión booleana:

$$E(a, b, c) = abc' + a'b'd + ab'c'd + a'bcd$$

Entonces:

$$E_L = 14 \text{ y } E_S = 4.$$

Sea F una expresión booleana de suma de productos equivalente a E. Entonces, se dice que E es más simple que F si se cumple que:

$$E_L \leq F_L \quad \text{y} \quad E_S \leq F_S$$

Y por lo menos una de las relaciones es una desigualdad estricta.

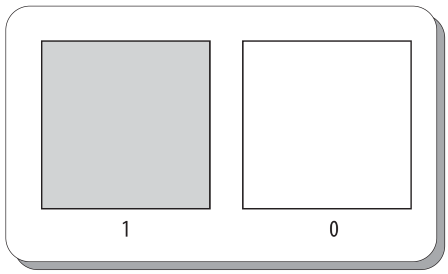


Figura 9.27 Representación del 1 y 0 lógicos utilizando diagramas de subconjuntos.

Diagramas de subconjuntos

Los diagramas de subconjuntos ofrecen una manera sencilla de visualizar las relaciones que puede haber entre diversas variables lógicas. Es probable que los diagramas más sencillos de todos sean los que representan al 1 lógico, el cual puede representarse como un cuadro completamente lleno, y al 0 lógico, el cual puede representarse como un cuadro vacío por completo, como se observa en la figura 9.27.

En este tipo de diagramas no solo se pueden representar el 1 y el 0, también es posible representar variables lógicas. El diagrama más sencillo de todos es el que se utiliza para representar una sola variable, mismo que está dividido en dos partes: una parte "llena", que es la parte en la cual la variable x toma el valor de 1 (la parte en color gris de la figura 9.28) y la parte "vacía", que es la parte en la cual la variable x toma el valor de 0 (la parte sin pantalla de la figura 9.28)

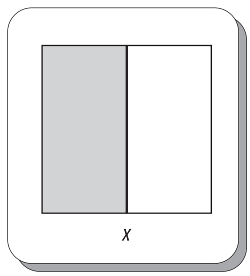


Figura 9.28 Representación de una variable lógica utilizando diagramas de subconjuntos.

Con estos diagramas no solo se puede representar una variable lógica, también es posible representar el complemento o inverso lógico de la variable, que se observa como se muestra en la figura 9.29.

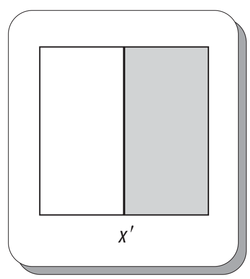


Figura 9.29 Representación del complemento de una variable lógica utilizando diagramas

Del mismo modo, también es posible representar una segunda variable y, además del complemento de la misma, como se muestra en la figura 9.30.

En la figura 9.31 se muestran las regiones en las que ambas variables lógicas se sup

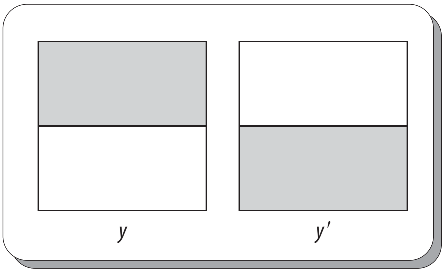


Figura 9.30 Representación de una segunda variable lógica y su complemento con el uso de diagramas de subconjuntos.

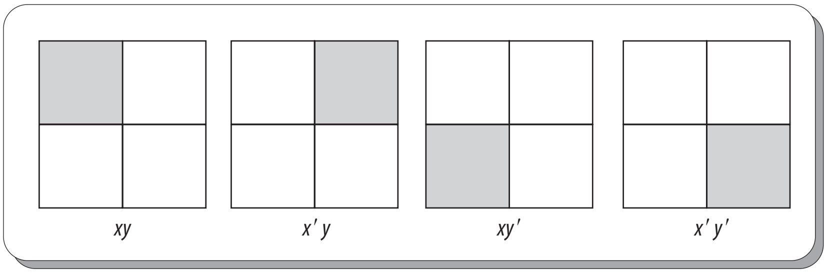


Figura 9.31 Regiones donde se intersecan las dos variables lógicas.

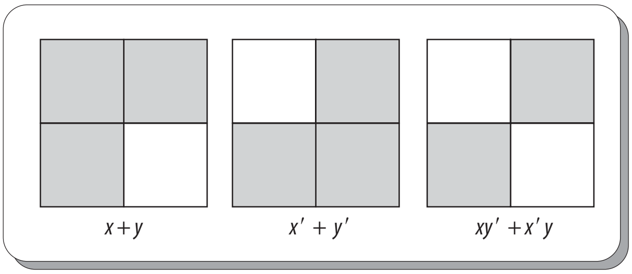


Figura 9.32 Regiones que representan las sumas booleanas $x + y$, $x' + y'$ y la *OR* exclusiva.

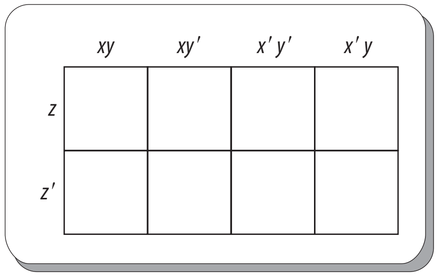


Figura 9.33 Diagrama de subconjuntos para tres variables.

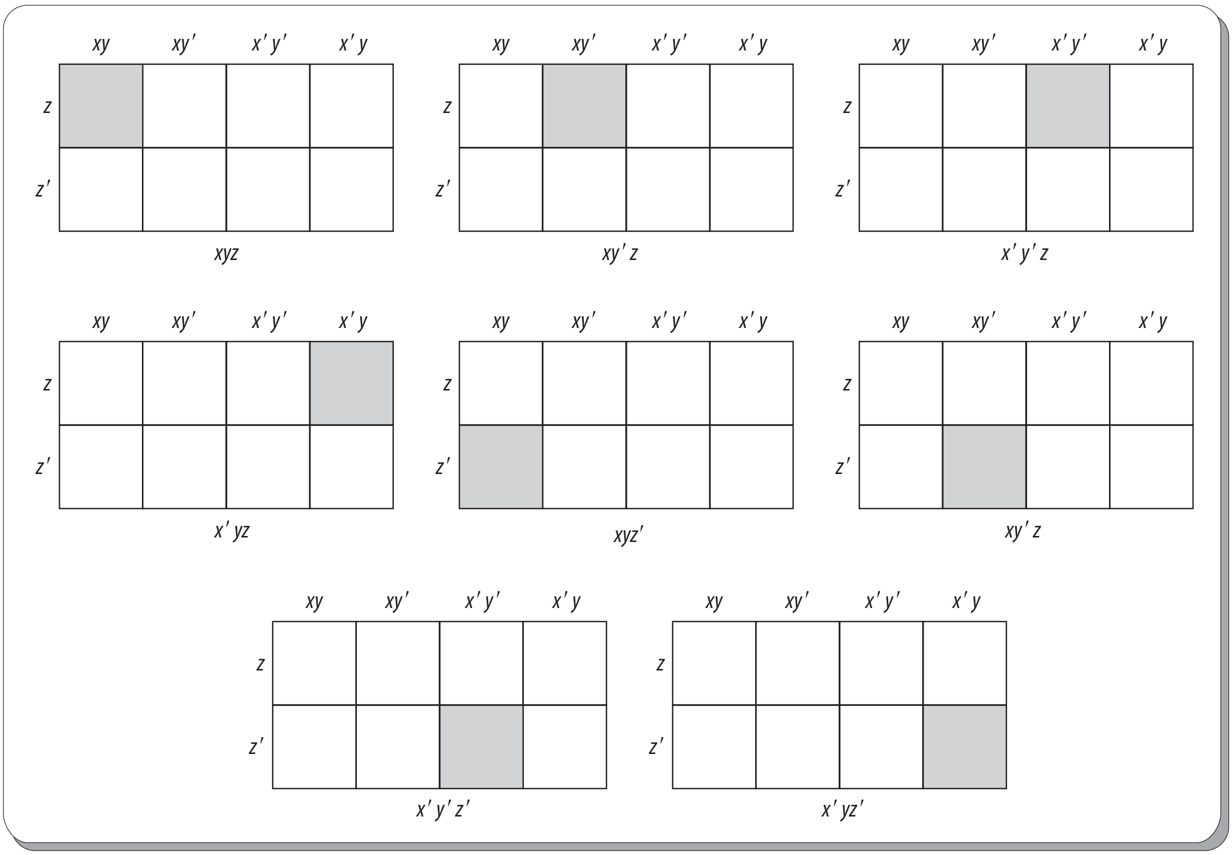


Figura 9.34 Regiones donde se intersecan las tres variables lógicas.

La región en la cual las variables lógicas x y y se unen, en vez de intersecarse, es la parte del diagrama en donde pueden estar ya sea en x o en y; es decir, la región que representaría la suma booleana $x + y$ de dichas variables. Lo mismo ocurre con la suma lógica de sus complementos. Asimismo, se puede representar la expresión booleana $xy' + x'y$, que representa la *OR* exclusiva. Estas sumas booleanas se representan como se observa en la figura 9.32.

Si se quiere representar una tercera variable z, se puede hacer en un arreglo como el que se muestra en la figura 9.33.

Al superponer las tres variables lógicas en el mismo diagrama, las regiones donde se intersecan se muestran en la figura 9.34.

Al superponer las tres variables lógicas en el mismo diagrama, las regiones donde se intersecan dos de las tres variables se muestran en la figura 9.35.

Por último, las regiones que representan una sola variable lógica se muestran en la figura 9.36.

La región en la cual las variables lógicas x, y, z se unen, en vez de intersecarse, es la parte del diagrama en donde pueden estar ya sea en x, o en y, o en z; es decir, la región que representaría la suma booleana $x + y + z$ de dichas variables. Lo mismo ocurre con la suma lógica de sus complementos, tal como se muestra en la figura 9.37.

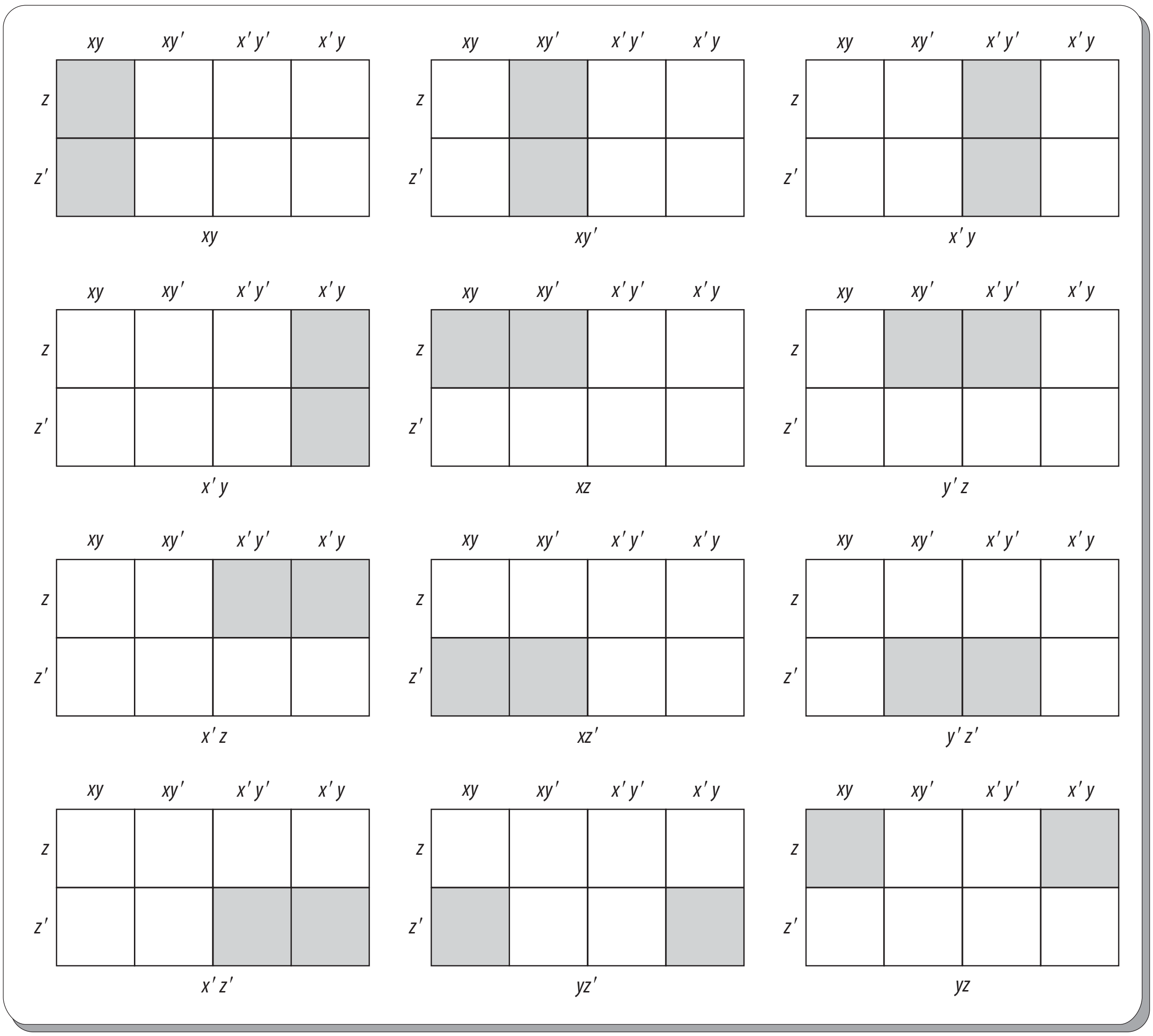


Figura 9.35 Regiones d

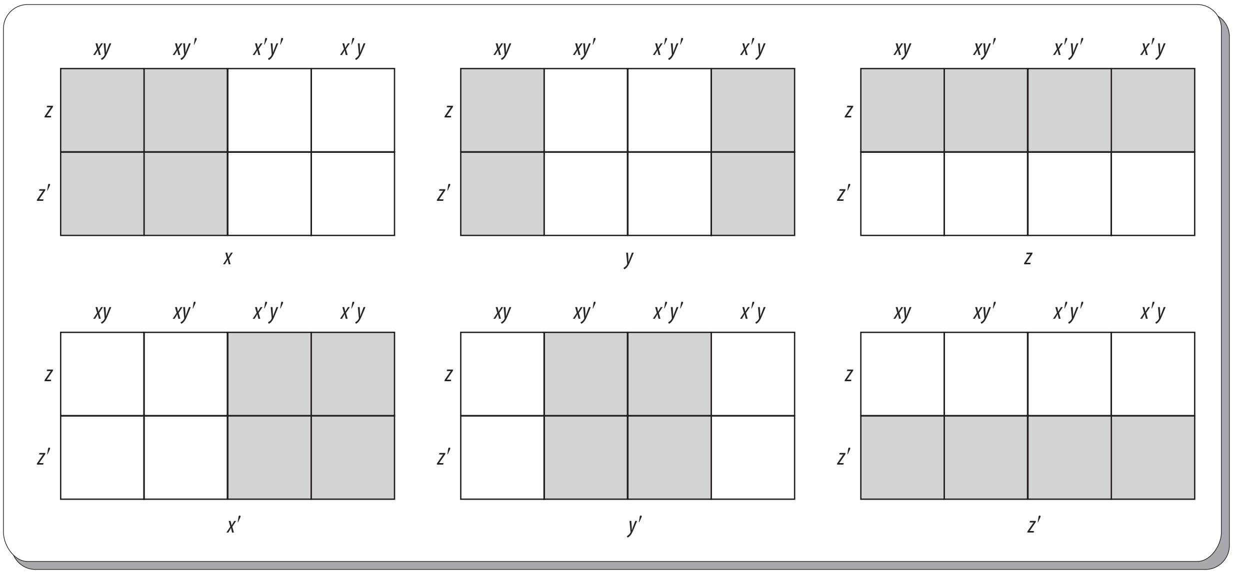


Figura 9.36 Regiones que representan una sola variable lógica.

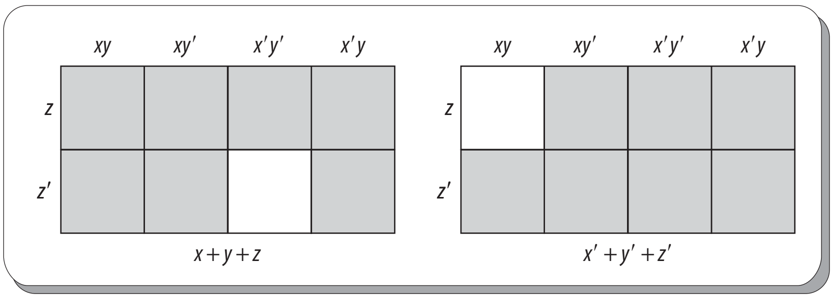


Figura 9.37. Regiones que representan las sumas booleanas $x + y + z$ y $x' + y' + z'$.

Además, se pueden representar diversas sumas booleanas considerando las regiones de las intersecciones de las variables consideradas.

Ejemplo

Sean las siguientes sumas booleanas:

a) $x'z + x'y'$

b) $x'y' + y'z'$

c) $xz + xy' + y'z'$

d) $x + z'$

e) $x'z' + xyz$

f) $xy + yz' + x'y'z$

Obtener el diagrama de subconjuntos correspondiente.

Solución

En cada caso basta con unir cada una de las regiones correspondientes de las intersecciones de las variables consideradas en cada uno de los términos de las sumas booleanas de cada inciso, como se observa en la figura 9.38.

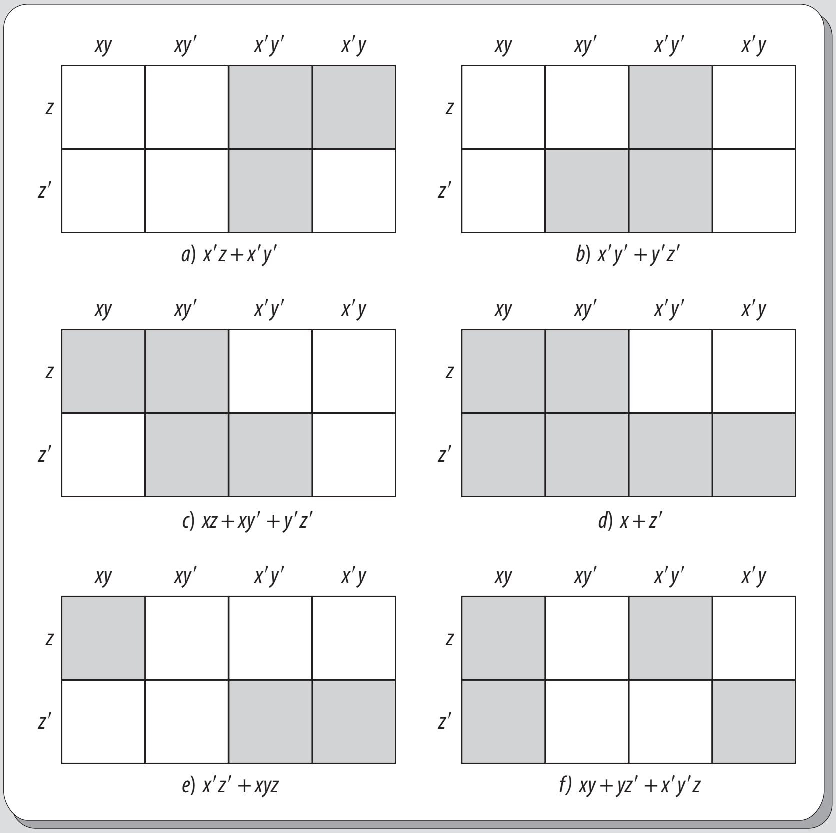


Figura 9.38 Diagramas de sumas booleanas.

Mapas de Karnaugh

El método de los mapas de Karnaugh constituye un método gráfico para encontrar las formas minimales de sumas de productos para expresiones booleanas que involucran un máximo de seis variables. No obstante, en esta sección solo se tratan los casos de dos, tres y cuatro variables lógicas.

Maurice Karnaugh graduado en la Universidad de Yale, en 1952. Trabajó como físico y matemático de los laboratorios Bell. Aunque es muy conocido por crear, en 1950, el método tabular o mapa de Karnaugh (también conocido como tabla de Karnaugh o diagrama de Veitch, abreviado como K-Mapa o KV-Mapa), un diagrama utilizado para la minimización de funciones algebraicas booleanas. Estos mapas o diagramas aprovechan la capacidad del cerebro humano de trabajar mejor con patrones que con ecuaciones y otras formas de expresión analítica.

Un mapa de Karnaugh consiste en una serie de cuadrados, cada uno de los cuales representa una línea de la tabla de verdad. Puesto que la tabla de verdad de una función de N variables posee 2^N filas, el mapa K correspondiente también debe poseer 2^N cuadrados. Cada cuadrado alberga un 0 o un 1, dependiendo del valor que toma la función en cada fila.

Figura 9.39 Maurice Karnaugh (n. 1924), ingeniero estadounidense en telecomunicaciones.

Producto fundamental

Un producto fundamental es un término producto de dos o más variables lógicas donde ninguna tiene la misma variable complementada o sin complementar.

EJEMPLO

Los términos producto:

$$xy'z\ ,\ x'y',\ zx't$$

son productos fundamentales, mientras que los términos producto:

$$x'x,\ y',\ zx'yx$$

no son productos fundamentales.

Sea un conjunto de variables lógicas $\{x_1, x_2, \ldots, x_n\}$, con estas se pueden formar los productos fundamentales P_i que contienen todas las variables, ya sea en su forma complementada o en su forma sin complementar.

Productos fundamentales adyacentes

Dados dos productos fundamentales, se dice que P_1 y P_2 son adyacentes si difieren exactamente en una literal, la cual tiene que ser una variable complementada en uno de los productos y sin complementar en el otro.

EJEMPLO

Sea el conjunto de variables lógicas $\{x, y, z, w\}$

Los productos fundamentales $x'yz$, xyz', xyw no son adyacentes, ya que tales productos no contienen todas las variables.

- Los pares de productos fundamentales:
  a) $x'yzw$, $xyzw'$
  b) $xyzw$, $x'yzw'$
  c) $xy'zw$, $xyz'w$

  No son adyacentes porque difieren en más de una literal.
- Los pares de productos fundamentales:
  a) $x'yzw$, $xyzw$
  b) $xyzw$, $xy'zw$
  c) $xy'zw$, $xy'z'w$

  Son adyacentes porque difieren exactamente en una literal, que es una variable complementada en uno de los productos y sin complementar en el otro o viceversa.

En un mapa de Karnaugh, cada uno de los productos fundamentales P_i que contienen todas las variables lógicas es representado en forma gráfica por un cuadrado, y la relación de adyacencia entre tales productos es representada por la adyacencia geométrica. Los cuadrados adyacentes son aquellos que representan *MINTERM* y que difieren solo en una variable lógica.

Mapas de Karnaugh de dos variables

Sean las variables lógicas x y y; con estas pueden formarse cuatro productos fundamentales P_i que contienen todas las variables:

xy x'y
xy' x'y'

Cada uno de estos productos fundamentales se representa por un cuadrado en la figura 9.40, respetando la relación de adyacencia de los *MINTERM*.

Los *MINTERM* que representan las celdas se escriben dentro de estas mismas, como se aprecia en la figura 9.41, la cual constituye la representación más utilizada; no obstante, también pueden representarse como se observa en la figura 9.42.

	x	x'
y		
y'		

Figura 9.40 Representación para mapas de Karnaugh de dos variables lógicas.

	x	x'
y	xy	x'y
y'	xy'	x'y'

Figura 9.41 Representación más usada de *MINTERM*.

y \ x	1	0
1	xy	x'y
0	xy'	x'y'

Figura 9.42 Segunda forma representación de *MINTERM*.

Mapas de Karnaugh de tres variables

Sean las variables lógicas x, y, z. Con estas pueden formarse ocho productos fundamentales P_i que contienen todas las variables:

xyz xy'z x'y'z x'yz
xy'z' xy'z' x'y'z' x'yz'

Cada uno de estos productos fundamentales se representa por un cuadrado (véase figura 9.43), respetando la relación de adyacencia de los *MINTERM*.

Los *MINTERM* que representan las celdas se escriben dentro de estas, como se observa en las figuras 9.44 y 9.45.

	xy	xy'	x'y'	x'y
z				
z'				

Figura 9.43 Representación para mapas de Karnaugh de tres variables lógicas.

	xy	xy'	x'y'	x'y
z	xyz	xy'z	x'y'z	x'yz
z'	xy'z'	xy'z'	x'y'z'	x'yz'

Figura 9.44 Representación de *MINTERM*.

	xy	xy'	x'y'	x'y
z	xyz	xy'z	x'y'z	x'yz
z'	xy'z'	xy'z'	x'y'z'	x'yz'

Figura 9.45 Segunda forma de representación de *MINTERM*.

Mapas de Karnaugh de cuatro variables

Sean las variables lógicas x, y, z, w. Con estas pueden formarse 16 productos fundamentales P_i que contienen todas las variables:

xyzw	xy'zw	x'y'zw	x'yzw
xyzw'	xy'zw'	x'y'zw'	x'yzw'
xyz'w'	xy'z'w'	x'y'z'w'	x'yz'w'
xyz'w	xy'z'w	x'y'z'w	x'yz'w

Cada uno de estos productos fundamentales se representa por un cuadrado (véase figura 9.46), respetando la relación de adyacencia de los *MINTERM*.

Cada uno de estos productos fundamentales se representa por un cuadrado (véanse figuras 9.47 y 9.48), respetando la relación de adyacencia de los *MINTERM*.

	xy	xy'	x'y'	x'y
zw				
zw'				
z'w'				
z'w				

Figura 9.46 Representación para mapas de Karnaugh de cuatro variables lógicas.

	xy	xy'	x'y'	x'y
zw	xyzw	xy'zw	x'y'zw	x'yzw
zw'	xyzw'	xy'zw'	x'y'zw'	x'yzw'
z'w'	xyz'w'	xy'z'w'	x'y'z'w'	x'yz'w'
z'w	xyz'w	xy'z'w	x'y'z'w'	x'yz'w

Figura 9.47 Representación de *MINTERM*.

Patrones básicos

Dado que las expresiones booleanas se minimizan mediante este método, también es conveniente estar familiarizado con los patrones de las posibles celdas adyacentes de los productos fundamentales y los grupos de unos, los cuales se encerrarán mediante óvalos.

Los patrones básicos para los productos fundamentales adyacentes de dos variables lógicas se observan con claridad en la figura 9.49.

zw \ xy	11	10	00	01
11	xyzw	xy'zw	x'y'zw	x'yzw
10	xyzw'	xy'zw'	x'y'zw'	x'yzw'
00	xyz'w'	xy'z'w'	x'y'z'w'	x'yz'w'
01	xyz'w	xy'z'w	x'y'z'w'	x'yz'w

Figura 9.48 Segunda forma de representación de *MINTERM*.

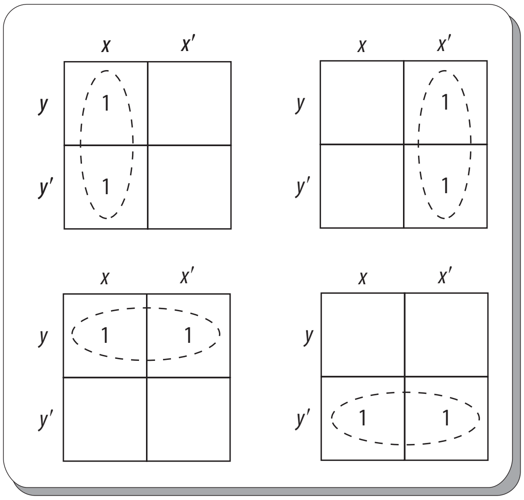


Figura 9.49 Celdas adyacentes de los productos fundamentales de dos variables lógicas.

Para los patrones básicos de los productos fundamentales adyacentes de tres variables lógicas, los cuadrados de los extremos izquierdo y derecho también se consideran adyacentes entre sí, como si los cuadrados fueran un cilindro unido por ambos extremos, como se muestra en la figura 9.50.

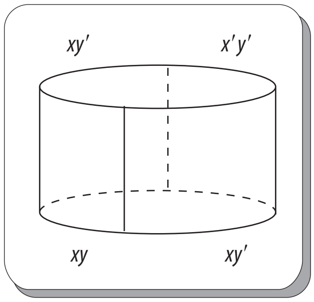


Figura 9.50 Extremos considerados como celdas adyacentes de los productos fundamentales.

Los patrones básicos para los productos fundamentales adyacentes de dos celdas para tres variables lógicas se muestran en la figura 9.51.

Los patrones básicos para los productos fundamentales adyacentes de cuatro celdas para tres variables lógicas se muestran en la figura 9.52.

De forma análoga al caso de tres variables, en este caso los cuadrados de los extremos izquierdo y derecho también se consideran adyacentes entre sí, lo mismo que los cuadrados de los extremos superior e inferior, que también se consideran adyacentes entre sí.

Dada la gran cantidad de productos fundamentales, solo se muestran aquí algunos casos. Así, en las figuras 9.53, 9.54 y 9.55 se observan algunos de los productos fundamentales que se representan mediante grupos de 2^n (2^1, 2^2 y 2^3) cuadrados adyacentes.

Los patrones básicos para los productos fundamentales adyacentes de dos celdas para cuatro variables lógicas se observan en la figura 9.53 y los de cuatro celdas para cuatro variables lógicas en la figura 9.54; por su parte, los de ocho celdas para cuatro variables lógicas se distinguen en la figura 9.55.

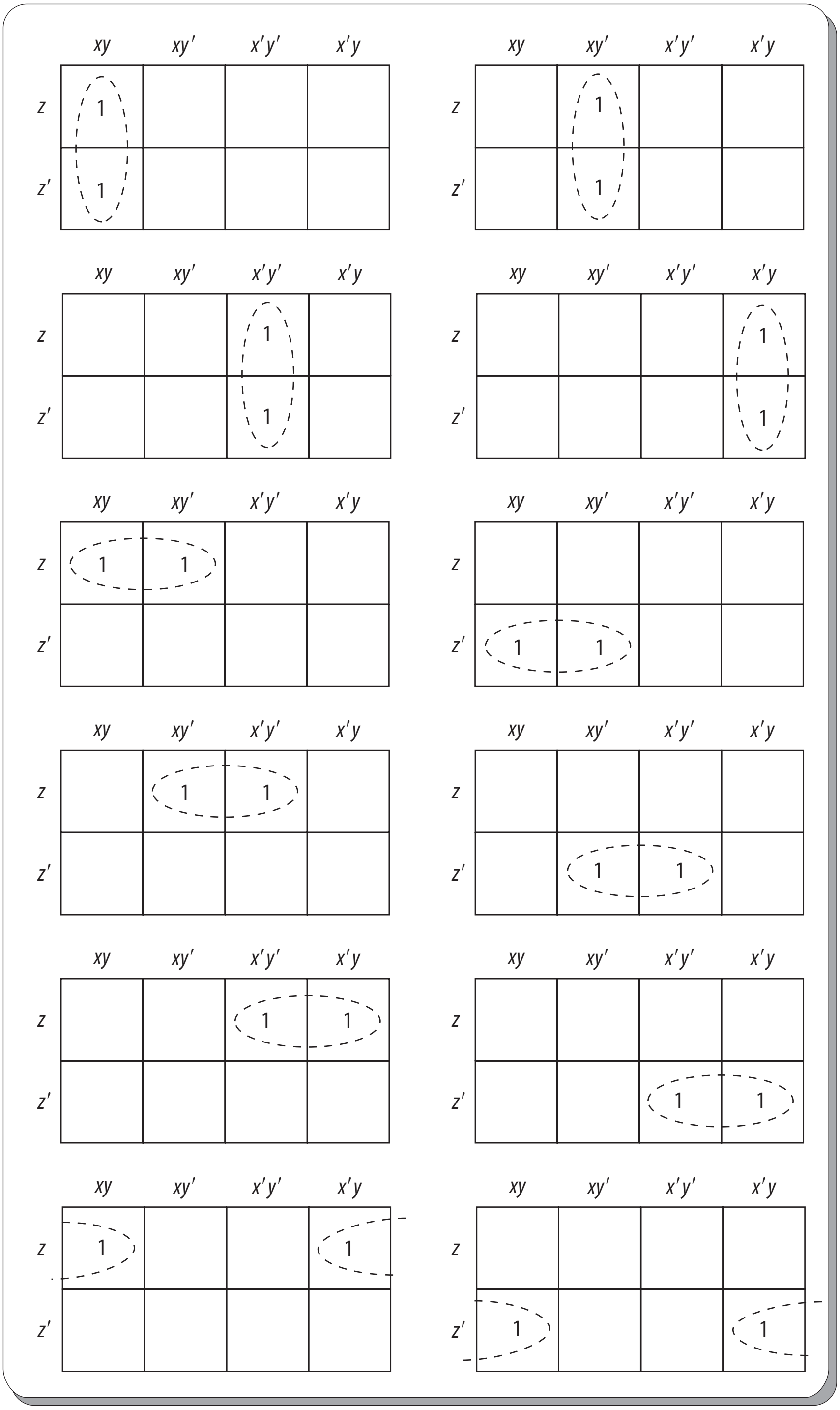


Figura 9.51 Celdas adyacentes de los productos fundamentales de dos celdas para tres variables lógicas.

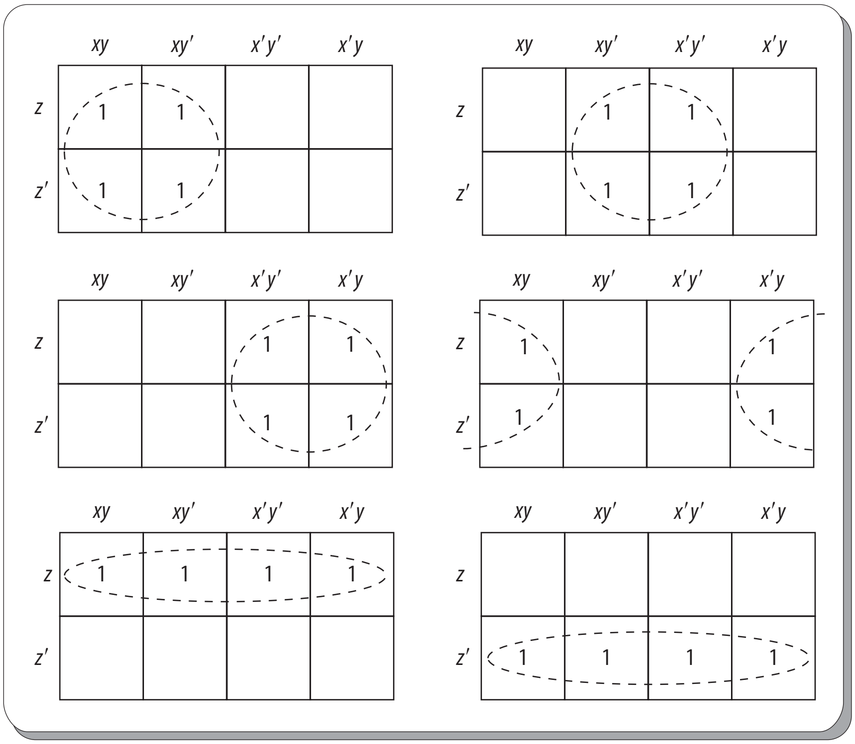


Figura 9.52 Celdas adyacentes de los productos fundamentales de cuatro celdas para tres variables lógicas.

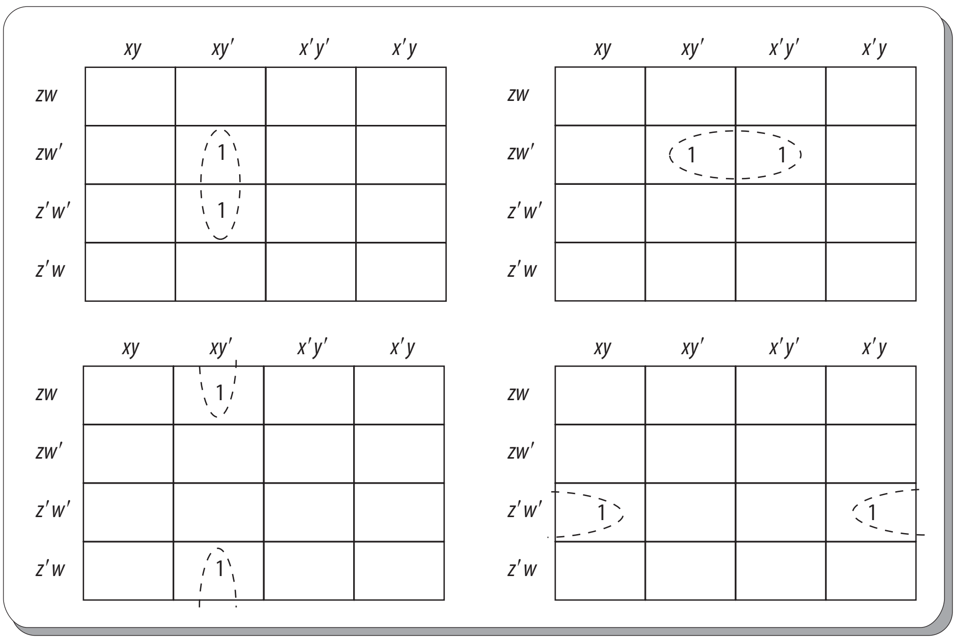


Figura 9.53 Celdas adyacentes de los productos fundamentales de dos celdas para cuatro variables lógicas.

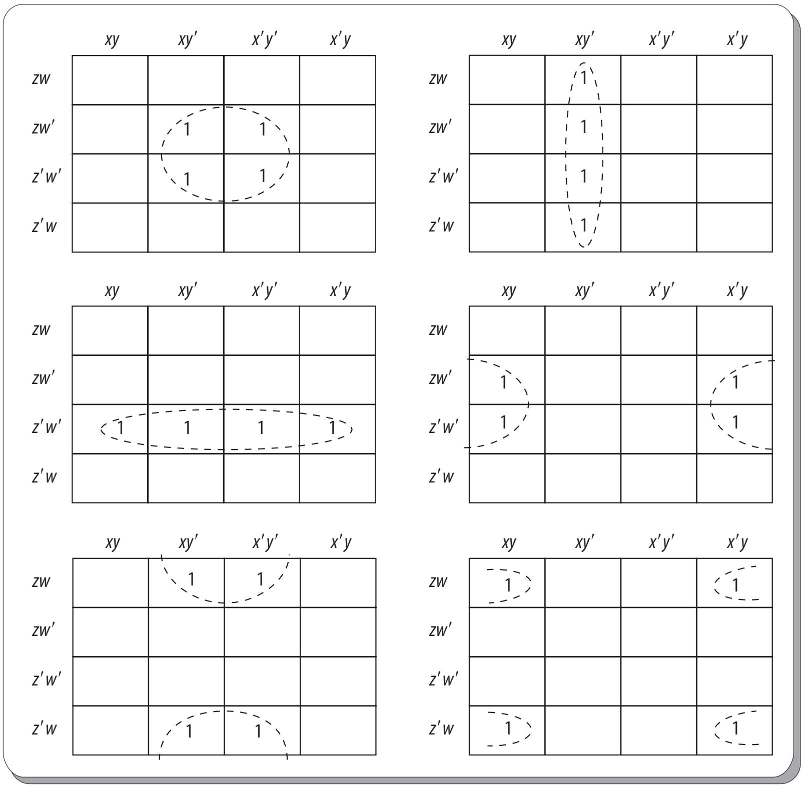


Figura 9.54 Celdas adyacentes de los productos fundamentales de cuatro celdas para cuatro variables lógicas.

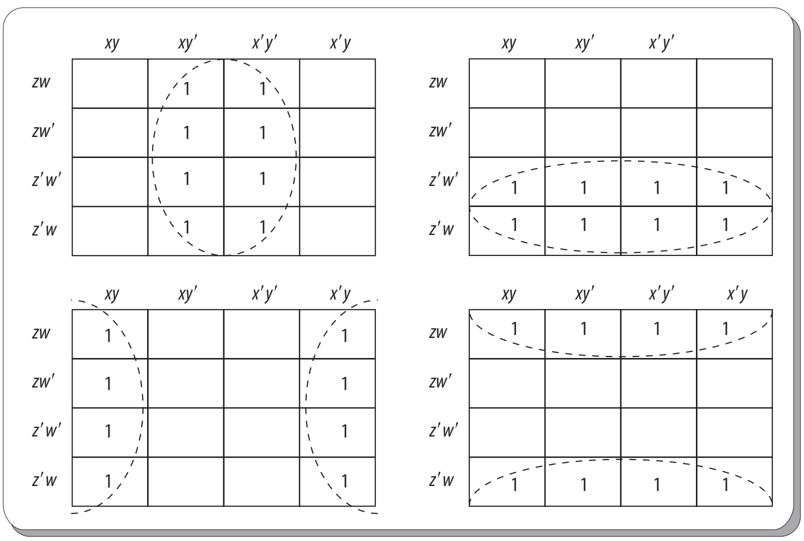


Figura 9.55 Celdas adyacentes de los productos fundamentales de ocho celdas para cuatro variables lógicas.

Minimización de circuitos mediante mapas de Karnaugh

Considérese una expresión booleana E en forma de suma de productos; a fin de encontrar la expresión booleana F equivalente a E en forma minimal de suma de productos, se deben seguir los siguientes pasos:

1. Se construye el mapa de Karnaugh, de acuerdo con el número de variables de E.
2. En el mapa de Karnaugh, todos los productos fundamentales de E se representan mediante cruces.
3. Todas las cruces se encierran con óvalos que contengan 2^n cruces adyacentes.
4. Cada óvalo debe encerrar la mayor cantidad posible de cruces.
5. Se escribe la expresión F como suma de los productos fundamentales representados por los óvalos resultantes.

Ejemplo

Sea la siguiente expresión booleana

$$E(x, y) = xy + xy' + y'$$

Encontrar su forma minimal de suma de productos F resultante utilizando el mapa de Karnaugh y dibujar el circuito lógico correspondiente.

Solución

El mapa de Karnaugh resultante de esta expresión booleana se muestra en la figura 9.56.

En la representación de las sumas de los términos representados en los óvalos, la forma minimal de E es:

$$F(x, y) = x + y'$$

Mientras que el circuito lógico correspondiente es como el que se observa en la figura 9.57.

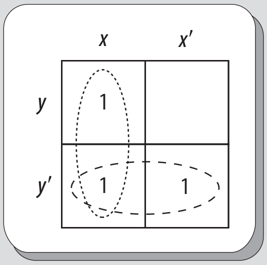


Figura 9.56 Mapa de Karnaugh.

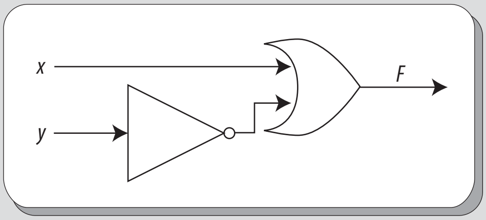


Figura 9.57 Circuito resultante.

Ahora, para comprobar que la simplificación es correcta, esta se hace de manera algebraica:

$$\begin{aligned} E(x, y) &= xy + xy' + y' \\ &= xy + y' && \text{Ley de la absorción} \\ &= x + y' && \text{Teorema de simplificación} \end{aligned}$$

Por tanto:

$$F(x, y) = x + y'$$

Como se observa, este es el mismo resultado obtenido utilizando un mapa de Karnaugh.

En diversas ocasiones, escribir la expresión F como suma de los productos fundamentales representados por los óvalos resultantes es una tarea complicada, pues, algunas veces, la interpretación de los mismos no es tan obvia.

Por lo general, para una mejor comprensión acerca de cómo interpretar los mapas de Karnaugh, es necesario hacer una analogía con los diagramas de subconjuntos.

Ejemplo

Sea la siguiente expresión booleana:

$$E(x, y, z) = xy'z + x'y'z + x'yz + x'y'z'$$

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

Solución

Primero, se realiza el mapa de Karnaugh resultante, que en este caso es como el que se observa en la figura 9.58.

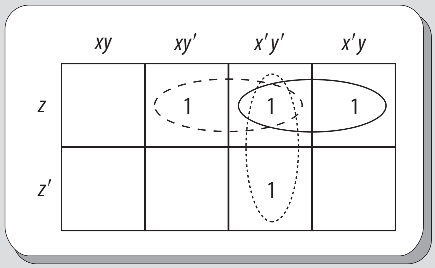


Figura 9.58 Mapa de Karnaugh.

Como se puede observar, este mapa tiene mucha similitud con los diagramas de subconjuntos vistos en la sección anterior, pues en este diagrama se tienen tres óvalos, cada uno de los cuales corresponde a cada una de las regiones que representan las intersecciones de las variables lógicas consideradas, donde el óvalo con líneas representa:

$y'z$

$x'z$

$x'y'$

Por tanto, la forma minimal de E es:

$$F(x, y, z) = x'y' + x'z + y'z$$

Ejemplo

Sea la siguiente expresión booleana:

$$E(x, y, z) = xyz + xy'z + x'y'z + xyz' + xy'z' + x'yz$$

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

Solución

Primero, se realiza el mapa de Karnaugh resultante, que en este caso es como el que se observa en la figura 9.59.

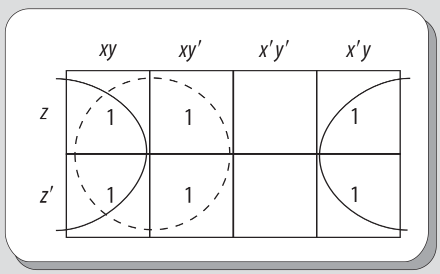


Figura 9.59 Mapa de Karnaugh.

Si se compara este mapa con los diagramas de subconjuntos, se obtienen las regiones representadas en cada óvalo:

x

y

Por tanto, la forma minimal de E es:

$$F(x, y, z) = x + y$$

Resumen

En este capítulo se estudia el álgebra de Boole o álgebra booleana, que no es más que una estructura matemática, la cual, como tal, abarca un sinnúmero de situaciones; además de que está centrada en los valores binarios 1 y 0, y proporciona operaciones y reglas para trabajar con dichos valores.

La aplicación más importante del álgebra booleana es en la informática, la computación y los circuitos lógicos, debido a que la lógica y el tratamiento de la información en estas áreas se basan precisamente en valores binarios.

Asimismo, en este capítulo se estudian las propiedades que deben cumplirse para que un conjunto, a la par con las operaciones de suma, producto y complemento booleano, sea considerado álgebra booleana. También se estudia qué son las funciones booleanas y cómo simplificarlas.

Aquí también se tratan aspectos fundamentales de los circuitos lógicos, los cuales están constituidos por circuitos más elementales llamados compuertas lógicas, las cuales, a su vez, tienen asociadas tablas de verdad y símbolos para representar los posibles estados binarios de entrada y la única salida binaria posible.

Por último, se estudia cómo dichos circuitos lógicos pueden ser simplificados, ya sea de forma algebraica o mediante el método de los mapas de Karnaugh.

Problemas propuestos

9.1 Sea la siguiente igualdad booleana:

$$a \cdot b + a' \cdot c = (a \cdot b) + (b \cdot c) + (a' \cdot c)$$

Escribir los pasos para demostrar que esta igualdad es verdadera.

$a \cdot b + a' \cdot c = a \cdot b + a' \cdot c$ ________________

$= (a \cdot b + a \cdot b \cdot c) + (a' \cdot c + a' \cdot c \cdot b)$

____

$= a \cdot b + a' \cdot c + a \cdot b \cdot c + a' \cdot c \cdot b$

____

$= a \cdot b + a' \cdot c + a \cdot b \cdot c + a' \cdot b \cdot c$

____

$= a \cdot b + a' \cdot c + (a + a') \cdot b \cdot c$

____

$= a \cdot b + a' \cdot c + (1) \cdot b \cdot c$

____

$= a \cdot b + a' \cdot c + b \cdot c$

____

$= a \cdot b + b \cdot c + a' \cdot c$

____

Justificar cada paso utilizando las propiedades y los teoremas del álgebra booleana.

9.2 Sea la siguiente expresión booleana:

$$(a' \cdot (b' \cdot (c + d)))$$

Representarla mediante compuertas lógicas.

9.3 Sea la función booleana:

$$F(a, b, c) = a' + b \cdot c$$

Expresar sus formas canónicas disyuntiva y conjuntiva.

9.4 Sea la siguiente la tabla de verdad de una función booleana.

Tabla 9.23

A	*b*	*c*	*F(a, b, c)*
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Expresarla en sus formas canónicas disyuntiva y conjuntiva.

9.5 Simplificar la siguiente función booleana utilizando las propiedades y los teoremas del álgebra booleana:

$$F(a, b, c) = a + a'b + abc' + ac + ac'$$

9.6 Simplificar la siguiente función booleana utilizando las propiedades y teoremas del álgebra booleana:

$$F(a, b, c) = (a + b) \cdot (a + b') \cdot (a' + b)$$

9.7 Simplificar la siguiente función booleana utilizando las propiedades y teoremas del álgebra booleana:

$$F(a, b, c, d) = (d + da' + bc)'$$

9.8 Simplificar la siguiente función booleana utilizando las propiedades y teoremas del álgebra booleana:

$$F(a, b, c, d) = ad + ab' + bc + ac'$$

9.9 Sea la siguiente expresión booleana:

$$E(x, y, z) = x'yz + xy'z + xyz' + xyz$$

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

9.10 Sea la siguiente la tabla de verdad de una expresión booleana:

Tabla 9.24

x	y	z	E(x, y, z)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

9.11 Simplificar la siguiente función booleana utilizando las propiedades y los teoremas del álgebra booleana:

$$F(a, b, c) = \{[(a'b')' + c] \cdot (a + c)\}'$$

9.12 Simplificar la siguiente función booleana utilizando las propiedades y teoremas del álgebra booleana:

$$F(a, b, c) = a'b + (abc)' + c(b' + a)$$

9.13 Sea la siguiente la tabla de verdad de una expresión booleana:

Tabla 9.25

X	y	z	E(x, y, z)
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

9.14 Sea la siguiente expresión booleana:

$$E(x, y, z) = x'y'z + x'y'z' + x'yz' + xy'z' + xyz'$$

Encontrar su forma minimal de suma de productos F resultante utilizando un mapa de Karnaugh.

En los problemas 9.15 a 9.19 obtener la expresión booleana que representa cada uno de los diversos circuitos lógicos que se muestran en la figura correspondiente.

9.15

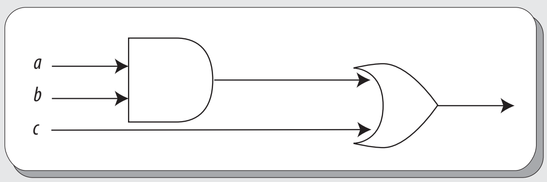


Figura 9.60

9.16

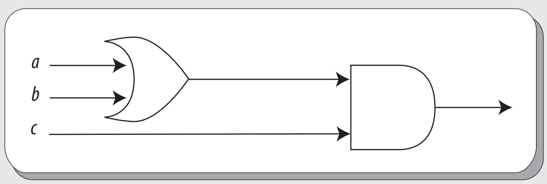


Figura 9.61

9.17

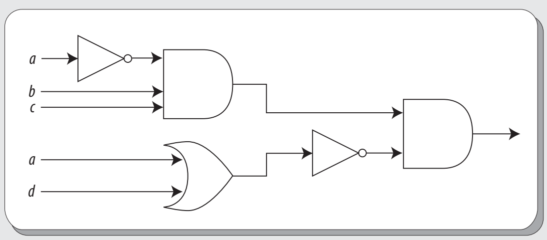


Figura 9.62

9.18

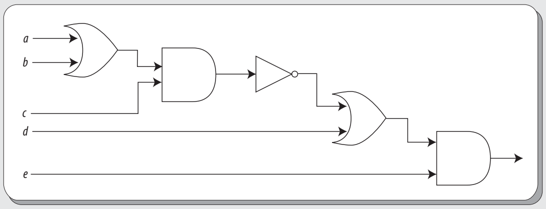


Figura 9.63

9.19

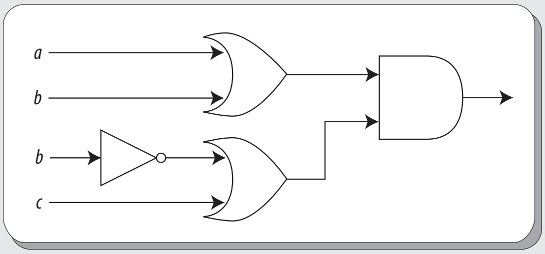


Figura 9.64

Con base en la siguiente expresión booleana, resolver los problemas 9.20 a 9.23.

$$F(x, y, z) = [(x \cdot y) \cdot (x + z)]'$$

9.20 Escribir su tabla de verdad.

9.21 Representar esta mediante compuertas lógicas.

9.22 Escribir los *MINTERM* y los *MAXTERM* asociados a cada combinación de variables.

9.23 Obtener las formas canónicas disyuntiva y conjuntiva.

9.24 Utilizando tablas de verdad, verificar la siguiente igualdad:

$$[(x \cdot y) + z]' = (x \cdot y)' \cdot z'$$

9.25 Sea la siguiente la tabla de verdad de una expresión booleana:

Tabla 9.26

x	y	z	w	F(x, y, z, w)
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

Obtener las formas canónicas disyuntiva y conjuntiva.

9.26 El complemento de una función booleana se puede obtener a partir de su función, reemplazando cada variable de esta última por su complemento. Obtener el complemento de la siguiente función booleana:

$$F(a, b, c, d) = (a \cdot b' \cdot c) + (d \cdot c) + (a' \cdot b)$$

9.27 Sea la siguiente igualdad booleana:

$$(x' \cdot y)' \cdot z + x \cdot z' + (y + z)' = x + y'$$

Escribir los pasos para demostrar que es verdadera dicha igualdad.

$(x' \cdot y)' \cdot z + x \cdot z' + (y + z)' = (x' \cdot y)' \cdot z + x \cdot z' + (y+z)'$ ____________________

$= (x' \cdot y)' \cdot z + x \cdot z' + y' \cdot z'$

____

$= (x' \cdot y) \cdot z + (x + y') \cdot z'$

____

$= (x + y') \cdot z + (x + y') \cdot z'$

____

$= (x + y') \cdot (z + z')$

____

$= (x + y') \cdot 1$ ____________________

$= x + y'$ ____________________

Justificar cada paso utilizando las propiedades y los teoremas del álgebra booleana.

Con base en la siguiente tabla de verdad contestar los problemas 9.28 a 9.31.

Tabla 9.27

x	y	z	F(x, y, z)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

9.28 Escribir una expresión booleana que la represente como suma de productos.

9.29 Representar esta expresión booleana mediante compuertas lógicas.

9.30 Encontrar su forma minimal de suma de productos *F* resultante utilizando un mapa de Karnaugh.

9.31 Representar *F* mediante compuertas lógicas, utilizando a lo sumo una compuerta *AND*, una compuerta *OR* y una compuerta *NOT*.

Con base en las siguientes formas canónicas disyuntiva y conjuntiva, resolver los problemas 9.32 a 9.34.

Forma canónica disyuntiva

$$F(x, y, z) = \sum_m (2, 3, 4, 5, 6, 7)$$

Forma canónica conjuntiva

$$F(x, y, z) = \prod_m (0, 1)$$

9.32 Escribir la tabla de verdad de la expresión booleana que representa.

9.33 Escribir la función booleana que se representa como producto de sumas.

9.34 Encontrar su forma minimal de suma de productos *F* resultante utilizando un mapa de Karnaugh.

9.35 Obtener la expresión booleana $x + y$ utilizando exclusivamente compuertas lógicas *NAND*.

Sugerencia

Se recomienda utilizar la ley de la idempotencia.

9.36 Obtener la expresión booleana $x \cdot y$ utilizando exclusivamente compuertas lógicas *NOR*.

Sugerencia

Se recomienda utilizar la ley de la idempotencia.

Con base en el siguiente enunciado, resolver los problemas 9.37 a 9.39.

Existe una compuerta lógica derivada denomina *XNOR*, la cual es el complemento de la compuerta lógica *XOR*; es decir $(x \cdot y)'$, cuyo símbolo es:

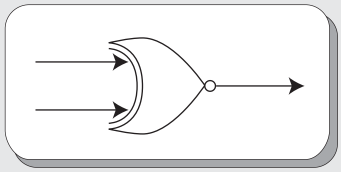


Figura 9.65

9.37 Obtener la tabla de verdad de la compuerta lógica derivada.

9.38 Representar la compuerta lógica *XNOR* exclusivamente con compuertas lógicas básicas.

9.39 Teniendo en cuenta la equivalencia lógica de la compuerta *XOR* $(x' \cdot y + x \cdot y')$, obtener la expresión lógica equivalente a la compuerta *XNOR*.

Con base en la siguiente igualdad, resolver los problemas 9.40 y 9.41.

$$x' \cdot y' \cdot (z + w) = (x' \cdot (y' \cdot (z+w)))$$

9.40 Utilizando tablas de verdad, verificar que se cumple la igualdad.

9.41 Utilizando compuertas lógicas, representar cada uno de los lados de la igualdad.

9.42 Sea la función booleana:

$$F(a, b, c) = a + bc' + abc$$

Expresar esta en sus formas canónicas disyuntiva y conjuntiva, utilizando los teoremas de expansión canónica.

9.43 Sea la función booleana:

$$F(a, b, c) = (a + b)(b + c')$$

Expresar esta en sus formas canónicas disyuntiva y conjuntiva, utilizando los teoremas de expansión canónica.

9.44 Simplificar la siguiente función booleana utilizando las propiedades y los teoremas del álgebra booleana:

$$F(x, y) = (x + y) + [(x + y')y]$$

9.45 Simplificar la siguiente función booleana utilizando las propiedades y los teoremas del álgebra booleana:

$$F(x, y, z, w) = x + xyz + x'yz + xw + xw' + x'y$$

9.46 Sea la función booleana:

$$F(x, y, z) = x + y'z$$

Expresarla en sus formas canónicas disyuntiva y conjuntiva utilizando los teoremas de expansión canónica.

Con base en el siguiente enunciado resolver los problemas 9.47 a 9.50. Toda compuerta lógica básica *AND*, *OR* y *NOT* puede ser sustituida utilizando exclusivamente compuertas lógicas derivadas *NAND* y *NOR*.

9.47 Obtener el circuito lógico equivalente a la compuerta lógica *AND* utilizando exclusivamente compuertas lógicas derivadas *NAND*.

9.48 Comprobar algebraicamente la equivalencia lógica del circuito obtenido utilizando las propiedades y los teoremas del álgebra booleana. Es decir, la salida del circuito obtenido debe ser igual a la salida de la compuerta lógica *AND*.

9.49 Obtener el circuito lógico equivalente a la compuerta lógica *OR* utilizando exclusivamente compuertas lógicas derivadas *NOR*.

9.50 Comprobar algebraicamente la equivalencia lógica del circuito obtenido utilizando las propiedades y los teoremas del álgebra booleana. Es decir, la salida del circuito obtenido debe ser igual a la salida de la compuerta lógica *OR*.

Problemas reto

Se desea construir un circuito lógico que se utilizará en un dispositivo electrónico para el registro de las votaciones en el Consejo del Instituto Estatal Electoral, el cual está conformado por un presidente, un vicepresidente y dos consejeros.

Las decisiones son tomadas por mayoría, pero el presidente tiene voto de calidad; es decir, en caso de empate su voto es el decisivo.

- Hallar la tabla de verdad que representa la situación antes mencionada.
- Simplificar al máximo la función booleana que se obtiene.
- Diseñar el circuito lógico para el dispositivo electrónico.

Sugerencia

Ante una determinada proposición, cada uno de los miembros del consejo puede votar a favor (1) o en contra (0); es decir, la decisión de cada integrante del Consejo del Instituto Estatal Electoral es una variable booleana binaria.

Índice analítico

S

T

U

V

W