Estructuras Discretas

José de Jesús Lavalle Martínez
FCC, BUAP
Traducción de partes del libro
Discrete Mathematics and Its Applications
Rosen K. H. 8th Edition (2018)
jlavalle@cs.buap.mx

Primavera 2021

Índice general

Capítulo 1

Conjuntos

Gran parte de las matemáticas discretas se dedica al estudio de estructuras discretas, que se utilizan para representar objetos discretos. Muchas estructuras discretas importantes se construyen utilizando conjuntos, que son colecciones de objetos.

Entre las estructuras discretas construidas a partir de conjuntos se encuentran combinaciones, colecciones desordenadas de objetos que se utilizan ampliamente en el conteo; relaciones, conjuntos de pares ordenados que representan relaciones entre objetos; grafos, conjuntos de vértices y aristas que conectan vértices; y máquinas de estados finitos, utilizadas para modelar máquinas que hacen cálculos.

1.1. Introducción

En esta sección, estudiamos la estructura discreta fundamental sobre la que se construyen todas las demás estructuras discretas, a saber, el conjunto. Los conjuntos se utilizan para agrupar objetos. A menudo, pero no siempre, los objetos de un conjunto tienen propiedades similares.

Por ejemplo, todos los estudiantes que están actualmente matriculados en su escuela forman un conjunto. Asimismo, todos los alumnos que actualmente cursan un curso de matemática discreta en cualquier escuela forman un conjunto. Además, aquellos estudiantes matriculados en su escuela que están tomando un curso de matemáticas discretas forman un conjunto que se puede obtener tomando los elementos comunes a las dos primeras colecciones.

El lenguaje de los conjuntos es un medio para estudiar estas colecciones

de manera organizada. A continuación, proporcionamos una definición de conjunto. Esta definición es una definición intuitiva, que no forma parte de una teoría formal de conjuntos.

Definición 1.1.1 Un conjunto es una colección desordenada de objetos distintos, llamados elementos o miembros del conjunto. Se dice que un conjunto contiene a sus elementos. Escribimos $a \in A$ para denotar que a es un elemento del conjunto A. La notación $a \notin A$ denota que a no es un elemento del conjunto A.

Es común que los conjuntos se denoten con letras mayúsculas. Las letras minúsculas se utilizan generalmente para denotar los elementos de los conjuntos.

Hay varias formas de describir un conjunto. Una forma es enumerar todos los miembros de un conjunto, cuando sea posible. Usamos una notación en la que todos los miembros del conjunto se enumeran entre llaves. Por ejemplo, la notación $\{a, b, c, d\}$ representa el conjunto con los cuatro elementos a, b, c y d. Esta forma de describir un conjunto se conoce como **método de lista**.

Ejemplo 1.1.1 El conjunto V de todas las vocales del alfabeto Inglés se puede escribir como $V = \{a, e, i, o, u\}$. □

Ejemplo 1.1.2 El conjunto O de todos los enteros positivos impares menores que 10 se puede escribir como $O = \{1, 3, 5, 7, 9\}$. □

Ejemplo 1.1.3 Aunque los conjuntos se utilizan generalmente para agrupar elementos con propiedades comunes, no hay nada que impida que un conjunto tenga elementos aparentemente no relacionados. Por ejemplo, el conjunto que contiene los cuatro elementos $a, 2$, Fred y New Jersey se puede denotar por $\{a, 2, \text{Fred}, \text{New Jersey}\}$. □

A veces, el método de lista se utiliza para describir un conjunto sin enumerar a todos sus miembros. Se enumeran algunos miembros del conjunto, y luego se utilizan puntos suspensivos (...) cuando el patrón general de los elementos es obvio.

Ejemplo 1.1.4 El conjunto de los enteros positivos menores que 100 puede ser denotado por $\{1, 2, 3, ..., 99\}$. □

Otra forma de describir un conjunto es utilizar la notación de **constructor de conjuntos**. Caracterizamos todos aquellos elementos del conjunto indicando la propiedad o propiedades que deben tener para ser miembros. La forma general de esta notación es $\{x|x$ tiene la propiedad $P\}$ y se lee "el conjunto de todo x tal que x tiene la propiedad P".

Por ejemplo, el conjunto O de todos los enteros positivos impares menores que 10 se puede escribir como

$$O = \{x|x \text{ es un entero positivo impar menor que } 10\},$$

o, especificando el universo como el conjunto de todos los enteros positivos, como

$$O = \{x \in \mathbb{Z}^+|x \text{ es impar y } x < 10\}.$$

A menudo usamos este tipo de notación para describir conjuntos cuando es imposible enumerar todos los elementos del conjunto. Por ejemplo, el conjunto $\mathbb{Q}^+$ de todos los números racionales positivos se puede escribir como

$$\mathbb{Q}^+ = \{x \in \mathbb{R}|x = \frac{p}{q}, \text{ para enteros positivos } p \text{ y } q\}.$$

Estos conjuntos juegan un papel importante en las matemáticas discretas:

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, el conjunto de todos los **números naturales**,
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, el conjunto de todos los **números enteros**,
$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, el conjunto de todos los **enteros positivos**,
$\mathbb{Q} = \{p/q|p \in \mathbb{Z}, q \in \mathbb{Z} \text{ y } q \neq 0\}$, el conjunto de todos los **números racionales**,
$\mathbb{R}$, el conjunto de todos los **números reales**,
$\mathbb{R}^+$, el conjunto de todos los números **reales positivos**,
$\mathbb{C}$, el conjunto de todos los **números complejos**.

(Tenga en cuenta que algunas personas no consideran el 0 como un número natural, así que tenga cuidado de verificar cómo se usa el término números naturales cuando lea otros libros).

Entre los conjuntos estudiados en cálculo y otras materias se encuentran los intervalos, conjuntos de todos los números reales entre dos números a y b, con o sin a y b. Si a y b son números reales con $a \leq b$, denotamos estos intervalos por

$$[a, b] = \{x | a \leq x \leq b\},$$
$$[a, b) = \{x | a \leq x < b\},$$
$$(a, b] = \{x | a < x \leq b\},$$
$$(a, b) = \{x | a < x < b\}.$$

Tenga en cuenta que $[a, b]$ se denomina **intervalo cerrado** de a a b y (a, b) se denomina **intervalo abierto** de a a b. Cada uno de los intervalos $[a, b]$, $[a, b)$, $(a, b]$ y (a, b) contiene todos los números reales estrictamente entre a y b. Los dos primeros contienen a a y el primero y tercero contienen a b.

Los conjuntos pueden tener otros conjuntos como miembros, como lo ilustra el siguiente ejemplo.

Ejemplo 1.1.5 El conjunto $\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ es un conjunto que contiene cuatro elementos, cada uno de los cuales es un conjunto. Los cuatro elementos de este conjunto son $\mathbb{N}$, el conjunto de números naturales; $\mathbb{Z}$, el conjunto de números enteros; $\mathbb{Q}$, el conjunto de números racionales; y $\mathbb{R}$, el conjunto de números reales. □

Observación 1.1.1 Tenga en cuenta que el concepto de tipo de datos, o tipo, en ciencias de la computación se basa en el concepto de conjunto. En particular, un tipo de datos o tipo es el nombre de un conjunto, junto con un conjunto de operaciones que se pueden realizar sobre objetos de ese conjunto. Por ejemplo, *boolean* es el nombre del conjunto $\{0, 1\}$, junto con los operadores sobre uno o más elementos de este conjunto, tales como **AND, OR** y **NOT**.

□

Debido a que muchos enunciados matemáticos afirman que dos colecciones de objetos especificadas de manera diferente son en realidad el mismo conjunto, debemos comprender qué significa que dos conjuntos sean iguales.

Definición 1.1.2 Dos conjuntos son iguales si y sólo si tienen los mismos elementos. Por lo tanto, si A y B son conjuntos, entonces A y B son iguales si y sólo si $\forall x(x \in A \leftrightarrow x \in B)$. Escribimos $A = B$ si A y B son conjuntos iguales.

Ejemplo 1.1.6 Los conjuntos $\{1, 3, 5\}$ y $\{3, 5, 1\}$ son iguales porque tienen los mismos elementos. Tenga en cuenta que el orden en el que se enumeran los elementos de un conjunto no importa. Tenga en cuenta también que no importa si un elemento de un conjunto aparece más de una vez, por lo que $\{1, 3, 3, 3, 5, 5, 5, 5\}$ es lo mismo que el conjunto $\{1, 3, 5\}$ porque tienen los mismos elementos. □

Hay un conjunto especial que no tiene elementos. Este conjunto se llama **conjunto vacío**, o **conjunto nulo**, y se denota por $\emptyset$. El conjunto vacío también se puede denotar por $\{\}$ (es decir, representamos el conjunto vacío con un par de llaves que encierran todos los elementos de este conjunto).

A menudo, un conjunto de elementos con determinadas propiedades resulta ser el conjunto nulo. Por ejemplo, el conjunto de todos los enteros positivos que son mayores que sus cuadrados es el conjunto nulo.

Un conjunto con un elemento se llama **conjunto singleton**. Un error común es confundir el conjunto vacío $\emptyset$ con el conjunto $\{\emptyset\}$, que es un conjunto singleton. ¡El único elemento del conjunto $\{\emptyset\}$ es el conjunto vacío mismo!

Una analogía útil para recordar esta diferencia es pensar en carpetas en un sistema de archivos de computadora. El conjunto vacío se puede considerar como una carpeta vacía y el conjunto que consiste sólo en el conjunto vacío se puede considerar como una carpeta con exactamente una carpeta dentro, es decir, la carpeta vacía.

Tenga en cuenta que el término objeto se ha utilizado en la definición de un conjunto, Definición 1.1.1, sin especificar qué es un objeto. Esta descripción de un conjunto como una colección de objetos, basada en la noción intuitiva de un objeto, fue establecida por primera vez en 1895 por el matemático alemán Georg Cantor.

La teoría que resulta de esta definición intuitiva de un conjunto, y el uso de la noción intuitiva de que para cualquier propiedad, hay un conjunto que consiste exactamente en los objetos con esta propiedad, conduce a paradojas o inconsistencias lógicas. Esto fue demostrado por el filósofo inglés Bertrand Russell en 1902.

Estas inconsistencias lógicas se pueden evitar construyendo la teoría de conjuntos comenzando con axiomas. Sin embargo, usaremos la versión original de Cantor de la teoría de conjuntos, conocida como teoría de conjuntos ingenua, en este libro porque todos los conjuntos considerados en este libro pueden tratarse de manera consistente usando la teoría original de Cantor.

Los estudiantes encontrarán útil la familiaridad con la teoría de conjuntos ingenua si continúan aprendiendo sobre la teoría de conjuntos axiomática. También encontrarán el desarrollo de la teoría de conjuntos axiomáticos mucho más abstracto que el material de este texto.

1.2. Diagramas de Venn

Los conjuntos se pueden representar gráficamente mediante diagramas de Venn, que llevan el nombre del matemático inglés John Venn, quien introdujo su uso en 1881.

En los diagramas de Venn, el conjunto universal U, que contiene todos los objetos considerados, se representa mediante un rectángulo. (Tenga en cuenta que el conjunto universal varía según los objetos de interés.) Dentro de este rectángulo, se utilizan círculos u otras figuras geométricas para representar conjuntos.

A veces, los puntos se utilizan para representar los elementos particulares del conjunto. Los diagramas de Venn se utilizan a menudo para indicar las relaciones entre conjuntos. Mostramos cómo se puede usar un diagrama de Venn en el Ejemplo 1.2.1.

Ejemplo 1.2.1 Dibuje un diagrama de Venn que represente a V, el conjunto de las vocales del alfabeto Inglés.

Solución: Dibujamos un rectángulo para indicar el conjunto universal U, que es el conjunto de las 26 letras del alfabeto Inglés. Dentro de este rectángulo dibujamos un círculo para representar a V. Dentro de este círculo indicamos los elementos de V con puntos (ver Figura 1.1). □

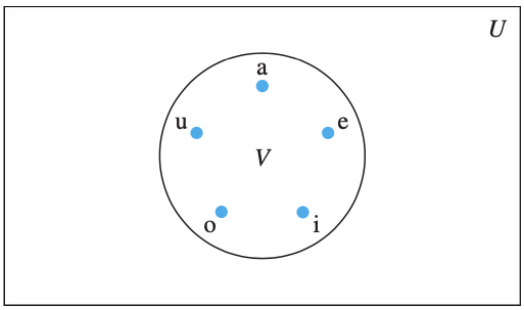


Figura 1.1: Diagrama de Venn para el conjunto de vocales.

1.3. Subconjuntos

Es común encontrar situaciones en las que los elementos de un conjunto también son elementos de un segundo conjunto. Introducimos ahora algo de terminología y notación para expresar tales relaciones entre conjuntos.

Definición 1.3.1 El conjunto A es un subconjunto de B, y B es un superconjunto de A, si y solo si cada elemento de A es también un elemento de B. Usamos la notación $A \subseteq B$ para indicar que A es un subconjunto del conjunto B. Si, en cambio, queremos enfatizar que B es un superconjunto de A, usamos la notación equivalente $B \supseteq A$. (Entonces, $A \subseteq B$ y $B \supseteq A$ son declaraciones equivalentes).

Vemos que $A \subseteq B$ si y sólo si la cuantificación

$$\forall x(x \in A \rightarrow x \in B)$$

es verdadera. Tenga en cuenta que para mostrar que A no es un subconjunto de B, solo necesitamos encontrar un elemento $x \in A$ con $x \notin B$. Tal x es un contraejemplo de la afirmación de que $x \in A$ implica $x \in B$.

Tenemos estas reglas útiles para determinar si un conjunto es un subconjunto de otro:

Demostrar que A es un subconjunto de B Para demostrar que $A \subseteq B$, demuestre que si x pertenece a A, entonces x también pertenece a B.
Demostrar que A no es un subconjunto de B Para demostrar que $A \nsubseteq B$, encuentre una sola $x \in A$ tal que $x \notin B$.

Ejemplo 1.3.1 El conjunto de todos los números enteros positivos impares menores que 10 es un subconjunto del conjunto de todos los números enteros positivos menores que 10, el conjunto de números racionales es un subconjunto del conjunto de números reales, el conjunto de todos los estudiantes de computación en su universidad es un subconjunto del conjunto de todos los estudiantes de su universidad, y el conjunto de todas las personas en China es un subconjunto del conjunto de todas las personas en China (es decir, es un subconjunto de sí mismo). Cada uno de estos hechos se sigue inmediatamente al señalar que un elemento que pertenece al primer conjunto, en cada par de conjuntos, también pertenece al segundo conjunto en ese par. □

Ejemplo 1.3.2 El conjunto de enteros con cuadrados menores que 100 no es un subconjunto del conjunto de enteros no negativos porque -1 está en el primer conjunto (ya que $(-1)^2 < 100$), pero no en el último conjunto. El conjunto de personas que han cursado matemáticas discretas en su universidad no es un subconjunto del conjunto de todas las personas que cursan computación si hay al menos un estudiante que ha cursado matemáticas discretas que no es estudiante de computación. □

El teorema 1.3.1 muestra que se garantiza que todo conjunto S no vacío tiene al menos dos subconjuntos, el conjunto vacío y el conjunto S mismo, es decir, $\emptyset \subseteq S$ y $S \subseteq S$.

Teorema 1.3.1 Para todo conjunto S, $\emptyset \subseteq S$ y $S \subseteq S$.

Demostración: Primero demostramos que $\emptyset \subseteq S$.

Sea S un conjunto. Para demostrar que $\emptyset \subseteq S$, debemos demostrar que $\forall x(x \in \emptyset \rightarrow x \in S)$ es verdadera. Dado que el conjunto vacío no contiene elementos, se deduce que $x \in \emptyset$ siempre es falso.

De ello se deduce que el enunciado condicional $x \in \emptyset \rightarrow x \in S$ es siempre verdadero, porque su hipótesis siempre es falsa y un enunciado condicional con una hipótesis falsa es verdadero.

Por lo tanto, $\forall x(x \in \emptyset \rightarrow x \in S)$ es verdadera. Esto completa la prueba. Tenga en cuenta que este es un ejemplo de una prueba por vacuidad.

Para demostrar que $S \subseteq S$ tenemos que ver si $\forall x(x \in S \rightarrow x \in S)$ es verdadera, lo cual se cumple ya que cualquier enunciado siempre se implica a sí mismo, en este caso $x \in S \rightarrow x \in S$ es verdadero y como escogimos un $x \in S$ arbitrario entonces $S \subseteq S$ es cierto.

También podemos demostrar el Teorema 1.3.1 por contradicción, de la siguiente manera.

Para demostrar que $\emptyset \subseteq S$, empezamos suponiendo que la afirmación es falsa. Así, tenemos que $\forall x(x \in \emptyset \rightarrow x \in S)$, lo cual implica que $x \in \emptyset$ es verdadera y $x \in S$ es falsa; pero como $\emptyset$ por definición no tiene elementos, llegamos a una contradicción. Por lo tanto es falsa nuestra suposición de que $\emptyset \subseteq S$ es falsa, así $\emptyset \subseteq S$ es verdadera.

De la misma manera para demostrar por contradicción que $S \subseteq S$, empezamos suponiendo que la afirmación $\forall x(x \in S \rightarrow x \in S)$ es falsa. Por lo tanto debemos tener que $x \in S \rightarrow x \in S$ es falsa, lo cual implica que $x \in S$ es al mismo tiempo verdadera y falsa, lo cual es una contradicción, de esta manera $S \subseteq S$ es verdadera. ■

Cuando deseamos enfatizar que un conjunto A es un subconjunto de un conjunto B pero que $A \neq B$, escribimos $A \subset B$ y decimos que A es un **subconjunto propio** de B. Para que $A \subset B$ sea verdadero, debe ser el caso de que $A \subseteq B$ y debe existir un elemento x de B que no es un elemento de A. Es decir, A es un subconjunto propio de B si y sólo si

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists(x \in B \wedge x \notin A)$$

es verdadera. Los diagramas de Venn se pueden utilizar para ilustrar que un conjunto A es un subconjunto de un conjunto B. Dibujamos el conjunto universal U como un rectángulo. Dentro de este rectángulo dibujamos un círculo para B. Debido a que A es un subconjunto de B, dibujamos el círculo para A dentro del círculo para B. Esta relación se muestra en la Figura 1.2.

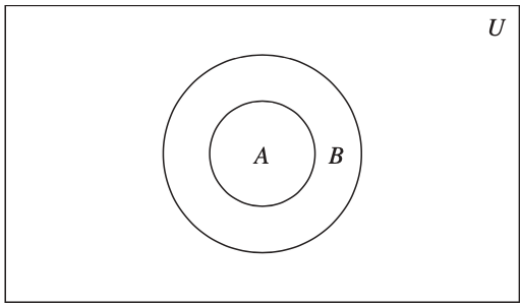


Figura 1.2: Diagrama de Venn que muestra que A es un subconjunto de B.

Recuerde de la Definición 1.1.2 que los conjuntos son iguales si tienen los mismos elementos. Una forma útil de mostrar que dos conjuntos tienen los mismos elementos es mostrar que cada conjunto es un subconjunto del otro.

En otras palabras, podemos demostrar que si A y B son conjuntos con $A \subseteq B$ y $B \subseteq A$, entonces $A = B$. Es decir, $A = B$ si y sólo si $\forall x(x \in A \rightarrow x \in B)$ y $\forall x(x \in B \rightarrow x \in A)$ o equivalentemente si y sólo si $\forall x(x \in A \leftrightarrow x \in B)$, que es lo que significa que A y B sean iguales. Debido a que este método de mostrar que dos conjuntos son iguales es tan útil, lo resaltamos aquí.

Demostrar que dos conjuntos son iguales Para demostrar que dos conjuntos A y B son iguales, muestre que $A \subseteq B$ y $B \subseteq A$.

Los conjuntos pueden tener otros conjuntos como miembros. Por ejemplo, tenemos los conjuntos

$A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ y $B = \{x | x$ es un subconjunto del conjunto $\{a, b\}\}$.

Tenga en cuenta que estos dos conjuntos son iguales, es decir, $A = B$. También tenga en cuenta que $\{a\} \in A$, pero $a \notin A$.

1.4. El tamaño de un conjunto

Los conjuntos se utilizan ampliamente en los problemas de conteo, y para tales aplicaciones necesitamos discutir los tamaños de los conjuntos.

Definición 1.4.1 Sea S un conjunto. Si hay exactamente n elementos distintos en S donde n es un número entero no negativo, decimos que S es un conjunto finito y que n es la cardinalidad de S. La cardinalidad de S se denota por $|S|$.

Observación 1.4.1 El término cardinalidad proviene del uso común del término número cardinal como el tamaño de un conjunto finito.

□

Ejemplo 1.4.1 Sea A el conjunto de números enteros positivos impares menores que 10. Entonces $|A| = 5$. □

Ejemplo 1.4.2 Sea S el conjunto de letras del alfabeto Inglés. Entonces $|S| = 26$. □

Ejemplo 1.4.3 Como el conjunto vacío (nulo) no tiene elementos, se sigue que $|\emptyset| = 0$. □

También nos interesarán conjuntos que no sean finitos.

Definición 1.4.2 Se dice que un conjunto es infinito si no es finito.

Ejemplo 1.4.4 El conjunto de enteros positivos es infinito. □

1.5. Conjunto potencia

Muchos problemas implican probar todas las combinaciones de elementos de un conjunto para ver si satisfacen alguna propiedad. Para considerar todas estas combinaciones de elementos de un conjunto S, construimos un nuevo conjunto que tiene como miembros todos los subconjuntos de S.

Definición 1.5.1 Dado un conjunto S, el **conjunto potencia** de S es el conjunto de todos los subconjuntos del conjunto S. El conjunto potencia de S se denota por $\mathscr{P}(S)$.

Ejemplo 1.5.1 ¿Cuál es el conjunto potencia del conjunto $\{0, 1, 2\}$?

Solución: El conjunto potencia $\mathscr{P}(\{0, 1, 2\})$ es el conjunto de todos los subconjuntos de $\{0, 1, 2\}$. Por lo tanto,

$$\mathscr{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

Tenga en cuenta que el conjunto vacío y el conjunto en sí son miembros de este conjunto de subconjuntos. □

Ejemplo 1.5.2 ¿Cuál es el conjunto potencia del conjunto vacío? ¿Cuál es el conjunto potencia del conjunto $\{\emptyset\}$?

Solución: El conjunto vacío tiene exactamente un subconjunto, a saber, él mismo. Por consiguiente, $\mathscr{P}(\emptyset) = \{\emptyset\}$.

El conjunto $\{\emptyset\}$ tiene exactamente dos subconjuntos, a saber, $\emptyset$ y el propio conjunto $\{\emptyset\}$. Por lo tanto, $\mathscr{P} = \{\emptyset, \{\emptyset\}\}$. □

Si un conjunto tiene n elementos, entonces su conjunto potencia tiene 2^n elementos. Demostraremos este hecho de varias formas en secciones posteriores del texto.

1.6. Producto cartesiano

El orden de los elementos de una colección suele ser importante. Debido a que los conjuntos no están ordenados, se necesita una estructura diferente para representar colecciones ordenadas. Esto es proporcionado por ***n*−tuplas ordenadas**.

Definición 1.6.1 La $n-$tupla ordenada $(a_1, a_2, \ldots, a_n)$ es la colección ordenada que tiene a_1 como primer elemento, a_2 como segundo elemento, $\ldots$, y a_n como $n-$ésimo elemento.

Decimos que dos $n-$tuplas ordenadas son iguales si y solo si cada par correspondiente de sus elementos es igual. En otras palabras, $(a_1, a_2, \ldots, a_n) =$

$(b_1, b_2, \ldots, b_n)$ si y sólo si $a_i = b_i$, para $i = 1, 2, \ldots, n$. En particular, las $2-$tuplas ordenadas se denominan **pares ordenados**. Los pares ordenados (a, b) y (c, d) son iguales y sólo si $a = c$ y $b = d$. Observe que (a, b) y (b, a) no son iguales a menos que $a = b$.

Muchas de las estructuras discretas que estudiaremos en capítulos posteriores se basan en la noción del producto cartesiano de conjuntos (llamado así por René Descartes). Primero definimos el producto cartesiano de dos conjuntos.

Definición 1.6.2 Sean A y B conjuntos. El **producto cartesiano** de A y B, denotado por $A \times B$, es el conjunto de todos los pares ordenados (a, b), donde $a \in A$ y $b \in B$. Por lo tanto,

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}.$$

Ejemplo 1.6.1 Sea A el conjunto de todos los estudiantes de una universidad y B el conjunto de todos los cursos ofrecidos en la universidad. ¿Qué es el producto cartesiano $A \times B$ y cómo se puede utilizar?

Solución: El producto cartesiano $A \times B$ consta de todos los pares ordenados de la forma (a, b), donde a es un estudiante en la universidad y b es un curso ofrecido en la universidad.

Una forma de utilizar el conjunto $A \times B$ es representar todas las posibles inscripciones de estudiantes en los cursos de la universidad.

Además, observe que cada subconjunto de $A \times B$ representa una posible configuración de inscripción total, y $\mathscr{P}(A \times B)$ representa todas las configuraciones posibles de inscripción. □

Ejemplo 1.6.2 ¿Cuál es el producto cartesiano de $A = \{1, 2\}$ y $B = \{a, b, c\}$?

Solución: El producto cartesiano $A \times B$ es

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

□

Tenga en cuenta que los productos cartesianos $A \times B$ y $B \times A$ no son iguales a menos que $A = \emptyset$ o $B = \emptyset$ (por lo tanto $A \times B = \emptyset$) o $A = B$. Esto se ilustra en el Ejemplo 1.6.3.

Ejemplo 1.6.3 Demuestre que el producto cartesiano $B \times A$ no es igual al producto cartesiano $A \times B$, donde A y B son como en el Ejemplo 1.6.2.

Solución: El producto cartesiano $B \times A$ es

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

Esto no es igual al $A \times B$ que se encontró en el Ejemplo 1.6.2. □

También se puede definir el producto cartesiano de más de dos conjuntos.

Definición 1.6.3 El **producto cartesiano** de los conjuntos $A_1, A_2, \ldots, A_n$, denotado por $A_1 \times A_2 \times \cdots \times A_n$, es el conjunto de $n-$tuplas ordenadas $(a_1, a_2, \ldots, a_n)$, donde a_i pertenece a A_i para $i = 1, 2, \ldots, n$. En otras palabras,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i \text{ para } i = 1, 2, \ldots, n\}.$$

Ejemplo 1.6.4 ¿Cuál es el producto cartesiano $A \times B \times C$, donde $A = \{0,1\}, B = \{1,2\}$ y $C = \{0,1,2\}$?

Solución: El producto cartesiano $A \times B \times C$ consta de todos los triples ordenados (a,b,c), donde $a \in A, b \in B$ y $c \in C$. Por lo tanto,

$$\begin{aligned} A \times B \times C = \{&(0,1,0),(0,1,1),(0,1,2),(0,2,0),(0,2,1),(0,2,2),\\ &(1,1,0),(1,1,1),(1,1,2),(1,2,0),(1,2,1),(1,2,2)\}. \end{aligned}$$

□

Observación 1.6.1 Tenga en cuenta que cuando A, B y C son conjuntos, $(A \times B) \times C$ no es lo mismo que $A \times B \times C$.

□

Usamos la notación A^2 para denotar $A \times A$, el producto cartesiano del conjunto A consigo mismo. De manera similar, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$, y así sucesivamente. Más generalmente,

$$A^n = \{(a_1, a_2, \ldots, a_n) | a_i \in A \text{ para } i = 1, 2, \ldots, n\}.$$

Ejemplo 1.6.5 Suponga que $A = \{1,2\}$. Se sigue que

$A^2 = \{(1,1),(1,2),(2,1),(2,2)\}$ y
$A^3 = \{(1,1,1),(1,1,2),(1,2,1),(1,2,2),(2,1,1),(2,1,2),(2,2,1),(2,2,2)\}.$

□

Un subconjunto R del producto cartesiano $(A \times B)$ se denomina una **relación** del conjunto A con el conjunto B. Los elementos de R son pares ordenados, donde el primer elemento pertenece a A y el segundo a B.

Por ejemplo, $R = \{(a, 0), (a, 1), (a, 3), (b, 1), (b, 2), (c, 0), (c, 3)\}$ es una relación del conjunto $\{a, b, c\}$ con el conjunto $\{0, 1, 2, 3\}$, y también es una relación del conjunto $\{a, b, c, d, e\}$ con el conjunto $\{0, 1, 2, 3, 4\}$. (Esto ilustra que una relación no necesita contener un par (x, y) para cada elemento x de A y y de B.) Una relación de un conjunto A consigo mismo se llama una relación sobre A.

Ejemplo 1.6.6 ¿Cuáles son los pares ordenados en la relación menor o igual a, que contiene (a, b) si $a \leq b$, sobre el conjunto $\{0, 1, 2, 3\}$?

Solución: El par ordenado (a, b) pertenece a R si y sólo si tanto a como b pertenecen a $\{0, 1, 2, 3\}$ y $a \leq b$. En consecuencia,

$$R = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}.$$

□

1.7. Ejercicios

1. Liste los miembros de estos conjuntos.

   a) $\{x | x$ es un número real tal que $x^2 = 1\}$,

   b) $\{x | x$ es un entero positivo menor que $12\}$,

   c) $\{x | x$ es el cuadrado de un entero y $x < 100\}$,

   d) $\{x | x$ es un entero tal que $x^2 = 2\}$.

2. Utilice la notación de constructor de conjuntos para dar una descripción de cada uno de estos conjuntos.

   a) $\{0, 3, 6, 9, 12\}$,

   b) $\{-3, -2, -1, 0, 1, 2, 3\}$,

   c) $\{m, n, o, p\}$.

3. Para cada uno de estos pares de conjuntos, determine si el primero es un subconjunto del segundo, el segundo es un subconjunto del primero, o ninguno es un subconjunto del otro.

   a) el conjunto de personas que hablan Inglés, el conjunto de personas que hablan Inglés con acento australiano.

   b) el conjunto de frutas, el conjunto de frutas cítricas.

   c) el conjunto de estudiantes que estudian estructuras discretas, el conjunto de estudiantes que estudian estructuras de datos.

4. Suponga que $A = \{2, 4, 6\}, B = \{2, 6\}, C = \{4, 6\}$ y $D = \{4, 6, 8\}$. Determine cuáles de estos conjuntos son subconjuntos de alguno de los restantes conjuntos.

5. ¿Cuál es la cardinalidad de cada uno de estos conjuntos?

   a) $\emptyset$,

   b) $\{\emptyset\}$,

   c) $\{\emptyset, \{\emptyset\}\}$,

   d) $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

6. Encuentre el conjunto potencia de cada uno de estos conjuntos, en los que a y b son elementos distintos.

   a) $\{a\}$,

   b) $\{a, b\}$,

   c) $\{\emptyset, \{\emptyset\}\}$.

7. ¿Cuántos elementos tiene cada uno de estos conjuntos, donde a y b son elementos distintos?

   a) $\mathscr{P}(\{a, b, \{a, b\}\})$,

   b) $\mathscr{P}(\{\emptyset, a, \{a\}, \{\{a\}\}\})$,

   c) $\mathscr{P}(\mathscr{P}(\emptyset))$.

8. ¿Cuál es el producto cartesiano $A \times B \times C$, donde A es el conjunto de todas las aerolíneas, B y C son ambos el conjunto de todas las ciudades de Estados Unidos? Dé un ejemplo de cómo se puede utilizar este producto cartesiano.

9. Sean $A = \{a, b, c\}, B = \{x, y\}$, y $C = \{0, 1\}$. Encuentre

   a) $A \times B \times C$,

   b) $C \times B \times A$,

   c) $C \times A \times B$,

   d) $B \times B \times B$.

10. Encuentre A^3 si

    a) $A = \{a\}$,

    b) $A = \{0, a\}$.

1.8. Operaciones sobre conjuntos

1.8.1. Introducción

Se pueden combinar dos o más conjuntos de muchas formas diferentes. Por ejemplo, comenzando con el conjunto de especializaciones en matemáticas en su escuela y el conjunto de especializaciones en ciencias de la computación en su escuela, podemos formar el conjunto de estudiantes que se especializan en matemáticas o en ciencias de la computación, el conjunto de estudiantes que tienen especializaciones conjuntas en matemáticas y ciencias de la computación, el conjunto de todos los alumnos que no se especializan en matemáticas, etc.

Definición 1.8.1 Sean A y B conjuntos. La *unión* de los conjuntos A y B, denotada por $A \cup B$, es el conjunto que contiene aquellos elementos que están en A o en B, o en ambos.

Un elemento x pertenece a la unión de los conjuntos A y B si y sólo si x pertenece a A o x pertenece a B. Esto nos dice que

$$A \cup B = \{x | x \in A \vee x \in B\}.$$

El diagrama de Venn que se muestra en la Figura 1.3 representa la unión de dos conjuntos A y B. El área que representa $A \cup B$ es el área sombreada dentro del círculo que representa a A o del círculo que representa a B.

Daremos algunos ejemplos de unión de conjuntos.

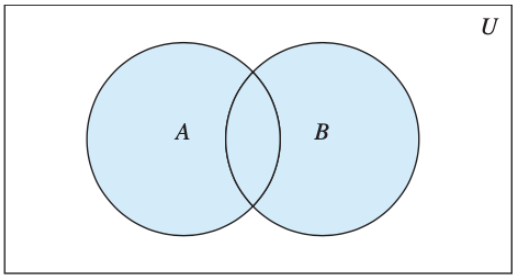


Figura 1.3: Diagrama de Venn de la unión de A yB.

Ejemplo 1.8.1 La unión de los conjuntos $\{1, 3, 5\}$ y $\{1, 2, 3\}$ es el conjunto $\{1, 2, 3, 5\}$; es decir, $\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$. □

Ejemplo 1.8.2 La unión del conjunto de todas las especialidades en ciencias de la computación de su universidad y el conjunto de todas las especializaciones en matemáticas de su universidad es el conjunto de estudiantes de su universidad que se especializan en matemáticas o en ciencias de la computación (o en ambas). □

Definición 1.8.2 Sean A y B conjuntos. La *intersección* de los conjuntos A y B, denotada por $A \cap B$, es el conjunto que contiene aquellos elementos tanto en A como en B.

Un elemento x pertenece a la intersección de los conjuntos A y B si y sólo si x pertenece a A y x pertenece a B. Esto nos dice que

$$A \cap B = \{x | x \in A \wedge x \in B\}.$$

El diagrama de Venn que se muestra en la Figura 1.4 representa la intersección de dos conjuntos A y B. El área sombreada que está dentro de ambos círculos que representan a los conjuntos A y B es el área que representa la intersección de A y B.

Damos algunos ejemplos de la intersección de conjuntos.

Ejemplo 1.8.3 La intersección de los conjuntos $\{1, 3, 5\}$ y $\{1, 2, 3\}$ es el conjunto $\{1, 3\}$; es decir, $\{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$. □

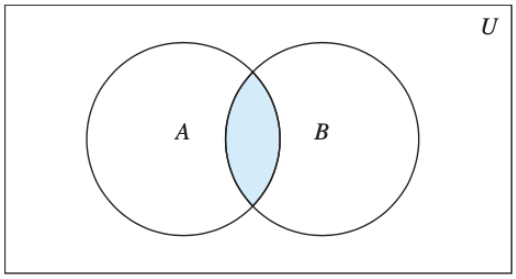


Figura 1.4: Diagrama de Venn de la intersección de A y B.

Ejemplo 1.8.4 La intersección del conjunto de todas las especializaciones en ciencias de la computación de su escuela y el conjunto de todas las especializaciones en matemáticas es el conjunto de todos los estudiantes que tienen especializaciones conjuntas en matemáticas y ciencias de la computación. □

Definición 1.8.3 Dos conjuntos se denominan *disjuntos* si su intersección es el conjunto vacío.

Ejemplo 1.8.5 Sea $A = \{1, 3, 5, 7, 9\}$ y $B = \{2, 4, 6, 8, 10\}$. Como $A \cap B = \emptyset$, A y B son disjuntos. □

A menudo nos interesa encontrar la cardinalidad de una unión de dos conjuntos finitos A y B. Observe que $|A| + |B|$ cuenta cada elemento que está en A pero no en B o en B pero no en A exactamente una vez, y cada elemento que está en A y B exactamente dos veces. Por lo tanto, si el número de elementos que están tanto en A como en B se resta de $|A| + |B|$, los elementos de $A \cap B$ se contarán sólo una vez. Por lo tanto,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

La generalización de este resultado a uniones de un número arbitrario de conjuntos se denomina **principio de inclusión-exclusión**. El principio de inclusión-exclusión es una técnica importante utilizada en la enumeración. Discutiremos este principio y otras técnicas de conteo en detalle más adelante.

Definición 1.8.4 Sean A y B conjuntos. La *diferencia* de A y B, denotada por $A - B$, es el conjunto que contiene los elementos que están en A pero

no en B. La diferencia de A y B también se llama *complemento de B con respecto de A*.

Un elemento x pertenece a la diferencia de A y B si y sólo si $x \in A$ y $x \notin B$. Esto nos dice que

$$A - B = \{x | x \in A \wedge x \notin B\}.$$

El diagrama de Venn que se muestra en la Figura 1.5 representa la diferencia de los conjuntos A y B. El área sombreada dentro del círculo que representa a A y fuera del círculo que representa a B es el área que representa a $A - B$.

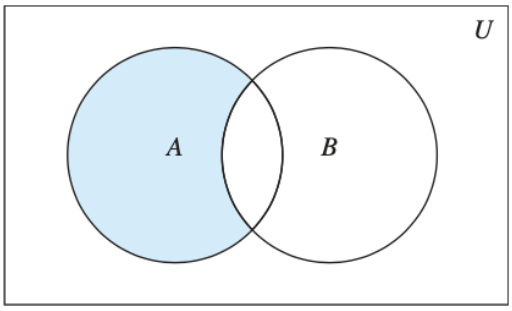


Figura 1.5: Diagrama de Venn de la diferencia de A y B.

Damos algunos ejemplos de diferencias de conjuntos.

Ejemplo 1.8.6 La diferencia de $\{1, 3, 5\}$ y $\{1, 2, 3\}$ es el conjunto $\{5\}$; es decir, $\{1, 3, 5\} - \{1, 2, 3\} = \{5\}$. Esto es diferente de la diferencia de $\{1, 2, 3\}$ y $\{1, 3, 5\}$, que es el conjunto $\{2\}$. □

Una vez que se ha especificado un conjunto universal U, se puede definir el **complemento** de un conjunto.

Definición 1.8.5 Sea U el conjunto universal. El *complemento* del conjunto A, denotado por $\overline{A}$, es el complemento de A con respecto a U. Por lo tanto, el complemento del conjunto A es $U - A$.

Observación 1.8.1 La definición del complemento de A depende de un conjunto universal particular U. Esta definición tiene sentido para cualquier superconjunto U de A. Si queremos identificar el conjunto universal U, escribiremos "el complemento de A con respecto al conjunto U".

□

Un elemento pertenece a $\overline{A}$ si y sólo si $x \notin A$. Esto nos dice que $A = \{x \in U | x \notin A\}$. En la Figura 1.6, el área sombreada fuera del círculo que representa a A es el área que representa a $\overline{A}$.

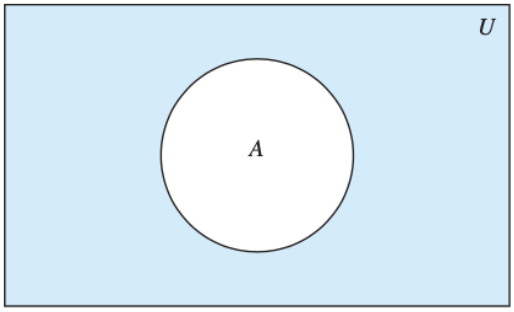


Figura 1.6: Diagrama de Venn del complemento de A.

Damos algunos ejemplos del complemento de un conjunto.

Ejemplo 1.8.7 Sea $A = \{a, e, i, o, u\}$ (donde el conjunto universal es el conjunto de letras del alfabeto Inglés).

Entonces $\overline{A} = \{b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z\}$. □

Ejemplo 1.8.8 Sea A el conjunto de enteros positivos mayores que 10 (donde el conjunto universal es el conjunto de todos los enteros positivos). Entonces $\overline{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. □

1.8.2. Identidades de conjuntos

La Tabla 1.1 enumera las identidades más importantes de uniones, intersecciones y complementos de conjuntos. Aquí probaremos varias de estas identidades, usando tres métodos diferentes.

Estos métodos se presentan para ilustrar que a menudo hay muchos enfoques diferentes para la solución de un problema. Las pruebas de las identidades restantes se dejarán como ejercicios. El lector debe notar la similitud

entre estas identidades de conjuntos y las equivalencias lógicas discutidas en su curso de Matemáticas Discretas.

De hecho, las identidades de conjuntos dadas se pueden probar directamente a partir de las equivalencias lógicas correspondientes. Además, ambos son casos especiales de identidades que son válidas para el álgebra de Boole.

Identity	***Name***
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

Tabla 1.1: Identidades de conjuntos.

Antes de discutir los diferentes enfoques para probar las identidades de conjuntos, discutimos brevemente el papel de los diagramas de Venn. Aunque estos diagramas pueden ayudarnos a comprender los conjuntos construidos utilizando dos o tres conjuntos atómicos (los conjuntos utilizados para construir combinaciones más complicadas de estos conjuntos), proporcionan

mucha menos información cuando están involucrados cuatro o más conjuntos atómicos.

Los diagramas de Venn para cuatro o más conjuntos son bastante complejos porque es necesario utilizar elipses en lugar de círculos para representar los conjuntos. Esto es necesario para garantizar que todas las combinaciones posibles de los conjuntos estén representadas por una región no vacía. Aunque los diagramas de Venn pueden proporcionar una prueba informal de algunas identidades, tales pruebas deben formalizarse utilizando uno de los tres métodos que describiremos a continuación.

Una forma de demostrar que dos conjuntos son iguales es mostrar que cada uno es un subconjunto del otro. Recuerde que para mostrar que un conjunto es un subconjunto de un segundo conjunto, podemos mostrar que si un elemento pertenece al primer conjunto, entonces también debe pertenecer al segundo conjunto. Generalmente usamos una prueba directa para hacer esto. Ilustramos este tipo de prueba estableciendo la primera de las leyes de De Morgan.

Ejemplo 1.8.9 Pruebe que $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
Solución: Demostraremos que los dos conjuntos $\overline{A \cap B}$ y $\overline{A} \cup \overline{B}$ son iguales mostrando que cada conjunto es un subconjunto del otro.

Primero, mostraremos que $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Hacemos esto mostrando que si x está en $\overline{A \cap B}$, entonces también debe estar en $\overline{A} \cup \overline{B}$. Ahora suponga que $x \in \overline{A \cap B}$. Por la definición de complemento, $x \notin A \cap B$. Usando la definición de intersección, vemos que la proposición $\neg((x \in A) \wedge (x \in B))$ es verdadera.

Al aplicar la ley de De Morgan a las proposiciones, vemos que $\neg(x \in A)$ o $\neg(x \in B)$. Usando la definición de negación de proposiciones, tenemos $x \notin A$ o $x \notin B$. Usando la definición del complemento de un conjunto, vemos que esto implica que $x \in \overline{A}$ o $x \in \overline{B}$. En consecuencia, por la definición de unión, vemos que $x \in \overline{A} \cup \overline{B}$. Así hemos demostrado que $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

A continuación, mostraremos que $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Hacemos esto mostrando que si x está en $\overline{A} \cup \overline{B}$, entonces también debe estar en $\overline{A \cap B}$. Ahora suponga que $x \in \overline{A} \cup \overline{B}$. Según la definición de unión, sabemos que $x \in \overline{A}$ o $x \in \overline{B}$. Usando la definición de complemento, vemos que $x \notin A$ o $x \notin B$. En consecuencia, la proposición $\neg(x \in A) \vee \neg(x \in B)$ es verdadera. Según la ley de De Morgan para las proposiciones, concluimos que $\neg((x \in A) \wedge (x \in B))$ es verdadero. Por la definición de intersección, se sigue que $\neg(x \in A \cap B)$. Ahora usamos la definición de complemento para concluir que $x \in \overline{A \cap B}$.

Esto muestra que $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Como hemos demostrado que cada conjunto es un subconjunto del otro, los dos conjuntos son iguales y se demuestra la identidad. □

Ejemplo 1.8.10 Utilice la notación de constructor de conjuntos y las equivalencias lógicas para establecer la primera ley de De Morgan $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
Solución: Podemos probar esta identidad con los siguientes pasos.

$$\begin{aligned}
\overline{A \cap B} &= \{x | x \notin A \cap B\} && \text{por definición de complemento} \\
&= \{x | \neg(x \in (A \cap B))\} && \text{por definición del símbolo no pertenece} \\
&= \{x | \neg(x \in A \wedge x \in B)\} && \text{por definición de intersección} \\
&= \{x | \neg(x \in A) \vee \neg(x \in B)\} && \text{por De Demorgan en prop. lógicas} \\
&= \{x | x \notin A \vee x \notin B\} && \text{por definición del símbolo no pertenece} \\
&= \{x | x \in \overline{A} \vee x \in \overline{B}\} && \text{por definición de complemento} \\
&= \{x | x \in \overline{A} \cup \overline{B}\} && \text{por definición de unión} \\
&= \overline{A} \cup \overline{B} && \text{por notación de constructor de conjuntos}
\end{aligned}$$

Tenga en cuenta que, además de las definiciones de complemento, unión, membresía de conjunto y notación de constructor de conjuntos, esta demostración utiliza la segunda ley de De Morgan para equivalencias lógicas. □

Para demostrar una identidad que involucra más de dos conjuntos, mostrando que cada lado de la identidad es un subconjunto del otro, a menudo se requiere que llevemos un registro de diferentes casos, como lo ilustra la prueba del Ejemplo 1.8.11 de una de las leyes distributivas para conjuntos.

Ejemplo 1.8.11 Demuestre la segunda ley distributiva de la Tabla 1.1, que establece que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ para todos los conjuntos A, B y C.
Solución: Demostraremos esta identidad mostrando que cada lado es un subconjunto del otro lado.

Suponga que $x \in A \cap (B \cup C)$. Entonces $x \in A$ y $x \in B \cup C$. Por la definición de unión, se deduce que $x \in A$ y ($x \in B$ o $x \in C$) (o ambos). En otras palabras, sabemos que la proposición compuesta $(x \in A) \wedge ((x \in B) \vee (x \in C))$ es verdadera. Por la ley distributiva para la conjunción sobre la disyunción, se deduce que $((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))$.

Concluimos que $x \in A$ y $x \in B$ o $x \in A$ y $x \in C$. Por la definición de intersección, se sigue que $x \in A \cap B$ o $x \in A \cap C$. Usando la definición de

unión, tenemos que $x \in (A \cap B) \cup (A \cap C)$. Concluimos que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Ahora suponga que $x \in (A \cap B) \cup (A \cap C)$. Entonces, por la definición de unión, $x \in A \cap B$ o $x \in A \cap C$. Por la definición de intersección, se sigue que $x \in A$ y $x \in B$ o que $x \in A$ y $x \in C$. De esto vemos que $x \in A$ y ($x \in B$ o $x \in C$).

En consecuencia, por la definición de unión vemos que $x \in A$ y $x \in B \cup C$. Además, por la definición de intersección, se sigue que $x \in A \cap (B \cup C)$. Concluimos que $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Esto completa la prueba de la identidad. □

Las identidades de conjuntos también se pueden probar mediante **tablas de pertenencia**. Consideramos cada combinación de los conjuntos atómicos (es decir, los conjuntos originales utilizados para producir los conjuntos en cada lado) a los que un elemento puede pertenecer y verificamos que los elementos en las mismas combinaciones de conjuntos pertenecen a ambos conjuntos en la identidad.

Para indicar que un elemento está en un conjunto, se usa un 1; para indicar que un elemento no está en un conjunto, se usa un 0. (El lector debe notar la similitud entre las tablas de membresía y las tablas de verdad).

Ejemplo 1.8.12 Utilice una tabla de pertenencia para mostrar que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
Solución: La tabla de pertenencia para estas combinaciones de conjuntos se muestra en la Tabla 1.2. Esta tabla tiene ocho filas. Debido a que las columnas para $A \cap (B \cup C)$ y $((A \cap B) \cup (A \cap C))$ son las mismas, la identidad es válida. □

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Tabla 1.2: Tabla de pertenencia para la propiedad distributiva.

Una vez que hemos probado las identidades establecidas, podemos usarlas para probar nuevas identidades. En particular, podemos aplicar una serie de identidades, una en cada paso, para llevarnos de un lado de una identidad deseada al otro. Es útil indicar explícitamente la identidad que se usa en cada paso, como lo hacemos en el Ejemplo 1.8.13.

Ejemplo 1.8.13 Sean A, B y C conjuntos. Demuestre que

$$A \cup (B \cap C) = (C \cup B) \cap A.$$

Solución: Tenemos

$$\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{(B \cap C)} && \text{por la primera ley De Demorgan} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{por la segunda ley De Demorgan} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{por la ley conmutativa para la intersección} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{por la ley conmutativa para la unión}
\end{aligned}$$

□

Resumimos las tres formas diferentes de probar las identidades de conjuntos en la Tabla 1.3.

Descripción	Método
Método de subconjunto	Muestre que cada lado de la identidad es un subconjunto del otro lado.
Tabla de pertenencia	Para cada combinación posible de los conjuntos atómicos, demuestre que un elemento en exactamente estos conjuntos atómicos debe pertenecer a ambos lados o pertenecer a ninguno.
Aplicar identidades existentes	Comience con un lado, transfórmelo en el otro lado usando una secuencia de pasos aplicando una identidad establecida.

Tabla 1.3: Métodos para probar identidades de conjuntos.

1.8.3. Uniones e intersecciones generalizadas

Debido a que las uniones e intersecciones de conjuntos satisfacen las leyes asociativas, los conjuntos $A \cup B \cup C$ y $A \cap B \cap C$ están bien definidos; es decir, el significado de esta notación no es ambiguo cuando A, B y C son conjuntos.

Es decir, no tenemos que usar paréntesis para indicar qué operación viene primero porque $A \cup (B \cup C) = (A \cup B) \cup C$ y $A \cap (B \cap C) = (A \cap B) \cap C$. Tenga en cuenta que $A \cup B \cup C$ contiene aquellos elementos que están en al menos uno de los conjuntos A, B y C, y que $A \cap B \cap C$ contiene aquellos elementos que están en todos A, B y C. Estas combinaciones de los tres conjuntos, A, B y C, se muestran en la Figura 1.7.

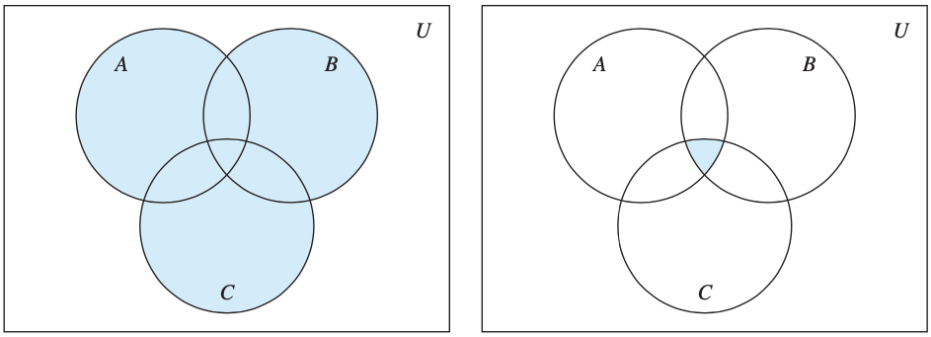


Figura 1.7: La unión e intersección de A, B y C.

También podemos considerar uniones e intersecciones de un número arbitrario de conjuntos. Introducimos estas definiciones.

Definición 1.8.6 La *unión* de una colección de conjuntos es el conjunto que contiene aquellos elementos que son miembros de al menos un conjunto de la colección.

Usamos la notación

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

para denotar la unión de los conjuntos $A_1, A_2, \ldots, A_n$.

Definición 1.8.7 La *intersección* de una colección de conjuntos es el conjunto que contiene los elementos que son miembros de todos los conjuntos de la colección.

Usamos la notación

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

para denotar la intersección de los conjuntos $A_1, A_2, \ldots, A_n$. Ilustramos las uniones e intersecciones generalizadas con el Ejemplo 1.8.14.

Ejemplo 1.8.14 Para $i = 1, 2, \ldots$, sea $A_i = \{i, i+1, i+2, \ldots\}$. Entonces

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{1, 2, 3, \ldots\}$$

y

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{n, n+1, n+2, \ldots\} = A_n.$$

□

Podemos extender la notación que hemos introducido para uniones e intersecciones a otras familias de conjuntos. En particular, para denotar la unión de la familia infinita de conjuntos $A_1, A_2, \ldots, A_n, \ldots$, usamos la notación

$$A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots = \bigcup_{i=1}^{\infty} A_i.$$

Similarmente, la intersección de estos conjuntos se denota mediante

$$A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots = \bigcap_{i=1}^{\infty} A_i.$$

De manera más general, cuando I es un conjunto, las notaciones $\bigcap_{i \in I} A_i$ y $\bigcup_{i \in I} A_i$, se usan para denotar la intersección y unión de los conjuntos A_i para $i \in I$, respectivamente. Tenga en cuenta que

$$\bigcap_{i \in I} A_i = \{x | \forall i \in I (x \in A_i)\}$$

y

$$\bigcup_{i\in I} A_i = \{x | \exists i \in I(x \in A_i)\}.$$

Ejemplo 1.8.15 Suponga que $A_i = \{1, 2, 3, \ldots, i\}$ para $i = 1, 2, 3, \ldots$. Entonces

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \mathbb{Z}^+$$

y

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \{1\}.$$

Para ver que la unión de estos conjuntos es el conjunto de enteros positivos, observe que todo entero positivo n está en al menos uno de los conjuntos, porque pertenece a $A_n = \{1, 2, \ldots, n\}$, y cada elemento de los conjuntos en la unión es un número entero positivo.

Para ver que la intersección de estos conjuntos es el conjunto $\{1\}$, observe que el único elemento que pertenece a todos los conjuntos $A_1, A_2, \ldots$ es 1. Para ver esto note que, $A_1 = \{1\}$ y $1 \in A_i$ para $i = 1, 2, \ldots$. □

1.8.4. Ejercicios

1. Sean $A = \{a, b, c, d, e\}$ y $B = \{a, b, c, d, e, f, g, h\}$.

   a) $A \cup B$.
   b) $A \cap B$.
   c) $A - B$.
   d) $B - A$.

2. Demuestre las siguientes identidades de conjuntos, mostrando que cada lado es un subconjunto del otro y también usando la notación de constructor de conjuntos.

   a) $\overline{\overline{A}} = A$.
   b) $A \cup \emptyset = A$.
   c) $A \cap U = A$.
   d) $A \cup U = U$.
   e) $A \cap \emptyset = \emptyset$.
   f) $A \cup A = A$.
   g) $A \cap A = A$.
   h) $A \cup \overline{A} = U$.
   i) $A \cap \overline{A} = \emptyset$.
   j) $A - \emptyset = A$.

$k)$ $\emptyset - A = \emptyset$.

$l)$ $A \cup B = B \cup A$.

$m)$ $A \cap B = B \cap A$.

$n)$ $A \cup (A \cap B) = A$.

Capítulo 2

Relaciones y Funciones

Las relaciones entre elementos de conjuntos ocurren en muchos contextos. Todos los días tratamos con relaciones como las que existen entre una empresa y su número de teléfono, un empleado y su salario, una persona y un familiar, etc.

En matemáticas estudiamos relaciones como las que existen entre un número entero positivo y otro que divide, un número entero y otro que es congruente con módulo 5, un número real y otro mayor que él, un número real x y el valor $f(x)$ donde f es una función, y así sucesivamente.

Relaciones como la que existe entre un programa y una variable que utiliza, y la que existe entre un lenguaje de programación y una declaración válida en este lenguaje, surgen a menudo en las ciencias de la computación.

Las relaciones entre elementos de dos conjuntos se representan mediante la estructura denominada relación binaria, que es sólo un subconjunto del producto cartesiano de los conjuntos.

Las relaciones se pueden utilizar para resolver problemas tales como determinar qué pares de ciudades están vinculadas por vuelos de aerolíneas en una red o encontrar un orden viable para las diferentes fases de un proyecto complicado. Introduciremos una serie de propiedades diferentes que pueden disfrutar las relaciones binarias.

Las relaciones entre elementos de más de dos conjuntos surgen en muchos contextos. Estas relaciones se pueden representar mediante relaciones n-arias, que son colecciones de $n-$tuplas. Estas relaciones son la base del modelo de datos relacionales, la forma más común de almacenar información en las bases de datos de las computadoras.

En secciones posteriores del capítulo se introducirán y usarán dos méto-

dos para representar relaciones, usando matrices cuadradas y usando grafos dirigidos, que consisten en vértices y aristas dirigidas. También estudiaremos las relaciones que tienen ciertas colecciones de propiedades que las relaciones pueden disfrutar.

Por ejemplo, en algunos lenguajes de programación, solo importan los primeros 31 caracteres del nombre de una variable. La relación que consta de pares ordenados de cadenas en las que la primera cadena tiene los mismos 31 caracteres iniciales que la segunda cadena es un ejemplo de un tipo especial de relación, conocida como relación de equivalencia. Las relaciones de equivalencia surgen a lo largo de las matemáticas y las ciencias de la computación.

Finalmente, estudiaremos relaciones llamadas ordenamientos parciales, que generalizan la noción de relación menor o igual que. Por ejemplo, el conjunto de todos los pares de cadenas de letras en inglés en el que la segunda cadena es la misma que la primera cadena o viene después de la primera en el orden del diccionario es un orden parcial.

2.1. Relaciones y sus propiedades

2.1.1. Introducción

La forma más directa de expresar una relación entre elementos de dos conjuntos es utilizar pares ordenados formados por dos elementos relacionados. Por esta razón, los conjuntos de pares ordenados se denominan relaciones binarias. En esta sección presentamos la terminología básica utilizada para describir las relaciones binarias.

Definición 2.1.1 Sean A y B conjuntos. Una *relación binaria* de A a B es un subconjunto de $A \times B$.

En otras palabras, una relación binaria de A a B es un conjunto R de pares ordenados, donde el primer elemento de cada par ordenado proviene de A y el segundo elemento proviene de B. Usamos la notación aRb para denotar que $(a, b) \in R$ y $a \not R b$ para denotar que $(a, b) \notin R$. Además, cuando (a, b) pertenece a R, se dice que a está **relacionado** con b mediante R.

Las relaciones binarias representan relaciones entre los elementos de dos conjuntos. Introduciremos relaciones $n-$arias, que expresan relaciones entre

elementos de más de dos conjuntos, más adelante en este capítulo. Omitiremos la palabra "binario" cuando no haya peligro de confusión.

Los ejemplos 2.1.1 a 2.1.3 ilustran la noción de relación.

Ejemplo 2.1.1 Sea A el conjunto de estudiantes de su escuela y B el conjunto de cursos. Sea R la relación que consta de aquellos pares (a, b), donde a es un estudiante matriculado en el curso b. Por ejemplo, si Jason Goodfriend y Deborah Sherman están inscritos en CS518, las parejas (Jason Goodfriend, CS518) y (Deborah Sherman, CS518) pertenecen a R.

Si Jason Goodfriend también está inscrito en CS510, entonces la pareja (Jason Goodfriend, CS510) también está en R. Sin embargo, si Deborah Sherman no está inscrita en CS510, entonces la pareja (Deborah Sherman, CS510) no está en R.

Tenga en cuenta que si un estudiante no está inscrito actualmente en ningún curso, no habrá pares en R que tengan a este estudiante como primer elemento. Del mismo modo, si un curso no se ofrece actualmente, no habrá pares en R que tengan este curso como segundo elemento. □

Ejemplo 2.1.2 Sea A el conjunto de ciudades de EE. UU. Y B el conjunto de los 50 estados de EE. UU. Defina la relación R especificando que (a, b) pertenece a R si una ciudad con el nombre a está en el estado b .

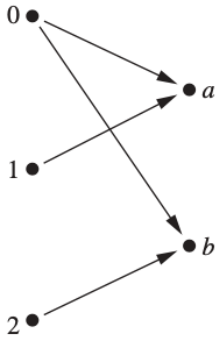
Por ejemplo, (Boulder, Colorado), (Bangor, Maine), (Ann Arbor, Michigan), (Middletown, Nueva Jersey), (Middletown, Nueva York), (Cupertino, California) y (Red Bank, Nueva Jersey) están en R. □

Ejemplo 2.1.3 Sean $A = \{0, 1, 2\}$ y $B = \{a, b\}$. Entonces una relación de A a B es $\{(0, a), (0, b), (1, a), (2, b)\}$. Esto significa, por ejemplo, que $0Ra$, pero que $1\not{R}b$. Las relaciones se pueden representar gráficamente, como se muestra en la Figura 2.1, usando flechas para representar pares ordenados. Otra forma de representar esta relación es usar una tabla, que también se muestra en la Figura 2.1. Discutiremos las representaciones de relaciones con más detalle más adelante. □

2.1.2. Relaciones sobre un conjunto

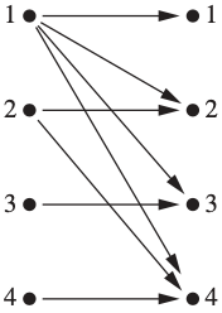
Las relaciones de un conjunto A consigo mismo son de especial interés.

Definición 2.1.2 Una relación sobre un conjunto A es una relación de A a A.



R	a	b
0	×	×
1	×	
2		×

Figura 2.1: Mostrando los pares ordenados en la relación R del Ejemplo 2.1.3.



R	1	2	3	4
1	×	×	×	×
2		×		×
3			×	
4				×

Figura 2.2: Mostrando los pares ordenados en la relación R del Ejemplo 2.1.4.

En otras palabras, una relación sobre un conjunto A es un subconjunto de $A \times A$.

Ejemplo 2.1.4 Sea A el conjunto $\{1, 2, 3, 4\}$. ¿Qué pares ordenados están en la relación $R = \{(a, b)|a \text{ divide a } b\}$?

Solución: Debido a que (a, b) está en R si y sólo si a y b son números enteros positivos que no excedan 4 tales que a divide a b, vemos que

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

Los pares en esta relación se muestran tanto gráficamente como en forma de tabla en la Figura 2.2. □

Ejemplo 2.1.5 Considere las siguientes relaciones sobre el conjunto de enteros:

$$\begin{aligned}
R_1 &= \{(a,b)|a \leq b\},\\
R_2 &= \{(a,b)|a > b\},\\
R_3 &= \{(a,b)|a = b \text{ o } a = -b\},\\
R_4 &= \{(a,b)|a = b\},\\
R_5 &= \{(a,b)|a = b+1\},\\
R_6 &= \{(a,b)|a+b \leq 3\}.
\end{aligned}$$

¿Cuáles de estas relaciones contienen cada uno de los pares $(1,1), (1,2), (2,1), (1,-1)$ y $(2,2)$?

Observación 2.1.1 A diferencia de las relaciones de los Ejemplos 2.1.1 a 2.1.4, estas son relaciones sobre un conjunto infinito.

□

Solución: El par $(1,1)$ está en R_1, R_3, R_4 y R_6; $(1,2)$ está en R_1 y R_6; $(2,1)$ está en R_2, R_5 y R_6; $(1,-1)$ está en R_2, R_3 y R_6; y finalmente, $(2,2)$ está en R_1, R_3 y R_4.

□

No es difícil determinar el número de relaciones en un conjunto finito, porque una relación sobre un conjunto A es simplemente un subconjunto de $A \times A$.

Ejemplo 2.1.6 ¿Cuántas relaciones hay en un conjunto con n elementos?

Solución: Una relación sobre un conjunto A es un subconjunto de $A \times A$. Como $A \times A$ tiene n^2 elementos cuando A tiene n elementos, y un conjunto con m elementos tiene 2^m subconjuntos, hay 2^{n^2} subconjuntos de $A \times A$. Por lo tanto, hay 2^{n^2} relaciones en un conjunto con n elementos. Por ejemplo, hay $2^{3^2} = 2^9 = 512$ relaciones sobre el conjunto $\{a, b, c\}$. □

2.1.3. Propiedades de las Relaciones

Hay varias propiedades que se utilizan para clasificar relaciones en un conjunto. Aquí presentaremos las más importantes. En algunas relaciones, un elemento siempre está relacionado consigo mismo. Por ejemplo, sea R la relación en el conjunto de todas las personas que consta de parejas (x, y)

donde x y y tienen la misma madre y el mismo padre. Entonces xRx para cada persona x.

Definición 2.1.3 Una relación R sobre un conjunto A se llama *reflexiva* si $(a, a) \in R$ para cada elemento $a \in A$.

Observación 2.1.2 Usando cuantificadores vemos que la relación R sobre el conjunto A es reflexiva si $\forall a((a, a) \in R)$, donde el universo de discurso es el conjunto de todos los elementos en A.

□

Vemos que una relación sobre A es reflexiva si cada elemento de A está relacionado consigo mismo. Los ejemplos 2.1.7-2.1.9 ilustran el concepto de relación reflexiva.

Ejemplo 2.1.7 Considere las siguientes relaciones sobre $\{1, 2, 3, 4\}$:

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$,
$R_2 = \{(1,1), (1,2), (2,1)\}$,
$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$,
$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$,
$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$,
$R_6 = \{(3,4)\}$.

¿Cuáles de estas relaciones son reflexivas?

Solución: Las relaciones R_3 y R_5 son reflexivas porque ambas contienen todos los pares de la forma (a, a), a saber, $(1, 1), (2, 2), (3, 3)$ y $(4, 4)$. Las otras relaciones no son reflexivas porque no contienen todos estos pares ordenados. En particular, R_1, R_2, R_4 y R_6 no son reflexivos porque $(3, 3)$ no se encuentra en ninguna de estas relaciones. □

Ejemplo 2.1.8 ¿Cuáles de las relaciones del ejemplo 2.1.5 son reflexivas?

Solución: Las relaciones reflexivas del ejemplo 2.1.5 son R_1 (porque $a \leq a$ para todo entero a, R_3 y R_4. Para cada una de las otras relaciones en este ejemplo, es fácil encontrar un par de la forma (a, a) que no está en la relación. □

Ejemplo 2.1.9 ¿Es reflexiva la relación "divide" en el conjunto de enteros positivos?

Solución: Como $a|a$ siempre que a es un número entero positivo, la relación "divide" es reflexiva. Tenga en cuenta que si reemplazamos el conjunto de enteros positivos con el conjunto de todos los enteros, la relación no es reflexiva porque, por definición, 0 no divide a 0. □

En algunas relaciones, un elemento está relacionado con un segundo elemento si y sólo si el segundo elemento también está relacionado con el primer elemento. La relación que consiste en pares (x, y), donde x y y son estudiantes en su escuela con al menos una clase común tiene esta propiedad.

Otras relaciones tienen la propiedad de que si un elemento está relacionado con un segundo elemento, este segundo elemento no está relacionado con el primero. La relación que consta de los pares (x, y), donde x y y son estudiantes en su escuela, donde x tiene un promedio de calificaciones más alto que y tiene esta propiedad.

Definición 2.1.4 Una relación R sobre un conjunto A se llama *simétrica* si $(b, a) \in R$ siempre que $(a, b) \in R$, para todo $a, b \in A$. Una relación R sobre un conjunto A tal que para todo $a, b \in A$, si $(a, b) \in R$ y $(b, a) \in R$, entonces $a = b$ se llama *antisimétrica*.

Observación 2.1.3 Usando cuantificadores, vemos que la relación R sobre el conjunto A es simétrica si $\forall a \forall b((a, b) \in R \rightarrow (b, a) \in R)$. De manera similar, la relación R sobre el conjunto A es antisimétrica si $\forall a \forall b(((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b))$.

□

En otras palabras, una relación es simétrica si y sólo si a está relacionada con b siempre implica que b está relacionada con a. Por ejemplo, la relación de igualdad es simétrica porque $a = b$ si y sólo si $b = a$.

Una relación es antisimétrica si y sólo si no hay pares de elementos distintos a y b con a relacionado con b y b relacionados con a. Es decir, la única forma de tener a relacionado con b y b relacionado con a es que a y b sean el mismo elemento.

Por ejemplo, la relación menor o igual a es antisimétrica. Para ver esto, tenga en cuenta que $a \leq b$ y $b \leq a$ implica que $a = b$.

Los términos simétrico y antisimétrico no son opuestos, porque una relación puede tener estas dos propiedades o puede carecer de ambas. Una relación no puede ser simétrica y antisimétrica si contiene algún par de la forma (a, b) en la que $a \neq b$.

Ejemplo 2.1.10 ¿Cuáles de las relaciones del ejemplo 2.1.7 son simétricas y cuáles antisimétricas?

Solución: Las relaciones R_2 y R_3 son simétricas, porque en cada caso (b, a) pertenece a la relación siempre que (a, b) lo hace. Para R_2, lo único que se debe verificar es que tanto $(2, 1)$ como $(1, 2)$ están en la relación.

Para R_3, es necesario comprobar que tanto $(1, 2)$ como $(2, 1)$ pertenecen a la relación, y también $(1, 4)$ y $(4, 1)$ pertenecen a la relación. El lector debe verificar que ninguna de las otras relaciones sean simétricas. Esto se hace encontrando un par (a, b) tal que esté en la relación pero (b, a) no lo esté.

R_4, R_5 y R_6 son todas antisimétricas. Para cada una de estas relaciones no hay un par de elementos a y b con $a \neq b$ tal que tanto (a, b) como (b, a) pertenezcan a la relación.

El lector debe verificar que ninguna de las otras relaciones sean antisimétricas. Esto se hace encontrando un par (a, b) con $a \neq b$ tal que (a, b) y (b, a) estén ambos en la relación. □

Ejemplo 2.1.11 ¿Cuáles de las relaciones del Ejemplo 2.1.5 son simétricas y cuáles antisimétricas?

Solución: Las relaciones R_3, R_4 y R_6 son simétricas. R_3 es simétrica, porque si $a = b$ o $a = -b$, entonces $b = a$ o $b = -a$. R_4 es simétrica porque $a = b$ implica que $b = a$. R_6 es simétrica porque $a + b \leq 3$ implica que $b + a \leq 3$. El lector debe verificar que ninguna de las otras relaciones sea simétrica.

Las relaciones R_1, R_2, R_4 y R_5 son antisimétricas. R_1 es antisimétrica porque las desigualdades $a \leq b$ y $b \leq a$ implican que $a = b$. R_2 es antisimétrica porque es imposible que $a > b$ y $b > a$. R_4 es antisimétrica, porque dos elementos están relacionados con respecto a R_4 si y sólo si son iguales. R_5 es antisimétrica porque es imposible que $a = b + 1$ y $b = a + 1$. El lector debe verificar que ninguna de las otras relaciones sea antisimétrica. □

Ejemplo 2.1.12 ¿Es simétrica la relación "divide" en el conjunto de enteros positivos? ¿Es antisimétrica?

Solución: Esta relación no es simétrica porque $1|2$, pero $2 \not| 1$. Sin embargo, es antisimétrica. Para ver esto, tenga en cuenta que si a y b son números enteros positivos con $a|b$ y $b|a$, entonces $a = b$. □

Sea R la relación que consta de todos los pares (x, y) de estudiantes de su escuela, donde x ha obtenido más créditos que y. Suponga que x está relacionado con y y y está relacionado con z. Esto significa que x ha obtenido más créditos que y y y ha obtenido más créditos que z. Podemos concluir que x ha tomado más créditos que z, por lo que x está relacionado con z. Lo que hemos demostrado es que R tiene la propiedad transitiva, que se define como sigue.

Definición 2.1.5 Una relación R sobre un conjunto A se llama *transitiva* si siempre que $(a, b) \in R$ y $(b, c) \in R$, entonces $(a, c) \in R$, para todo $a, b, c \in A$.

Observación 2.1.4 Usando cuantificadores vemos que la relación R sobre un conjunto A es transitiva si tenemos

$$\forall a \forall b \forall c(((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R).$$

□

Ejemplo 2.1.13 ¿Cuáles de las relaciones del ejemplo 2.1.7 son transitivas?

Solución: R_4, R_5 y R_6 son transitivas. Para cada una de estas relaciones, podemos demostrar que es transitiva verificando que si (a, b) y (b, c) pertenecen a esta relación, entonces (a, c) también lo está.

Por ejemplo, R_4 es transitiva, porque $(3, 2)$ y $(2, 1)$; $(4, 2)$ y $(2, 1)$; $(4, 3)$ y $(3, 1)$; además de $(4, 3)$ y $(3, 2)$ son los únicos conjuntos de pares de este tipo, y $(3, 1), (4, 1)$ y $(4, 2)$ pertenecen a R_4. El lector debe verificar que R_5 y R_6 sean transitivas.

R_1 no es transitiva porque $(3, 4)$ y $(4, 1)$ pertenecen a R_1, pero $(3, 1)$ no. R_2 no es transitiva porque $(2, 1)$ y $(1, 2)$ pertenecen a R_2, pero $(2, 2)$ no. R_3 no es transitiva porque $(4, 1)$ y $(1, 2)$ pertenecen a R_3, pero $(4, 2)$ no. □

Ejemplo 2.1.14 ¿Cuáles de las relaciones del ejemplo 2.1.5 son transitivas?

Solución: Las relaciones R_1, R_2, R_3 y R_4 son transitivas. R_1 es transitiva porque $a \leq b$ y $b \leq c$ implican que $a \leq c$. R_2 es transitiva porque $a > b$ y $b > c$ implican que $a > c$. R_3 es transitiva porque $a = \pm b$ y $b = \pm c$ implican que $a = \pm c$. R_4 es claramente transitiva, como debe verificar el lector. R_5 no es transitiva porque $(2, 1)$ y $(1, 0)$ pertenecen a R_5, pero $(2, 0)$ no. R_6 no es transitiva porque $(2, 1)$ y $(1, 2)$ pertenecen a R_6, pero $(2, 2)$ no. □

Ejemplo 2.1.15 ¿Es la relación "divide" en el conjunto de enteros positivos transitiva?

Solución: Suponga que a divide a b y b divide a c. Entonces hay enteros positivos k y l tales que $b = ak$ y $c = bl$. Por lo tanto, $c = a(kl)$, entonces a divide a c. De ello se deduce que esta relación es transitiva. □

Ejemplo 2.1.16 ¿Cuántas relaciones reflexivas hay en un conjunto con n elementos?

Solución: Una relación R sobre un conjunto A es un subconjunto de $A \times A$. En consecuencia, una relación se determina especificando si cada uno de los n^2 pares ordenados en $A \times A$ está en R.

Sin embargo, si R es reflexiva, cada uno de los n pares ordenados (a, a) para $a \in A$ deben estar en R. Cada uno de los otros $n(n-1)$ pares ordenados de la forma (a, b), donde $a \neq b$, puede estar o no en R.

Por lo tanto, por la regla del producto para contar, hay $2^{n(n-1)}$ relaciones reflexivas, este es el número de formas de elegir si cada elemento (a, b), con $a \neq b$, pertenece a R. □

Las fórmulas para el número de relaciones simétricas y el número de relaciones antisimétricas en un conjunto con n elementos se pueden encontrar usando un razonamiento similar al del Ejemplo 2.1.16.

Sin embargo, no se conoce ninguna fórmula general que cuente las relaciones transitivas en un conjunto con n elementos. Actualmente, $T(n)$, el número de relaciones transitivas en un conjunto con n elementos, se conoce sólo para $0 \leq n \leq 18$.

2.1.4. Combinando Relaciones

Debido a que las relaciones de A a B son subconjuntos de $A \times B$, dos relaciones de A a B se pueden combinar de cualquier manera que se puedan combinar dos conjuntos. Considere los ejemplos 2.1.17-2.1.19.

Ejemplo 2.1.17 Sean $A = \{1, 2, 3\}$ y $B = \{1, 2, 3, 4\}$. Las relaciones $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ y $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$ se pueden combinar

para obtener

$$\begin{aligned}
R_1 \cup R_2 =& \{(1,1),(1,2),(1,3),(1,4),(2,2),(3,3)\},\\
R_1 \cap R_2 =& \{(1,1)\},\\
R_1 - R_2 =& \{(2,2),(3,3)\},\\
R_2 - R_1 =& \{(1,2),(1,3),(1,4)\}.
\end{aligned}$$

□

Ejemplo 2.1.18 Sean A y B el conjunto de todos los estudiantes y el conjunto de todos los cursos de una escuela, respectivamente. Suponga que R_1 consta de todos los pares ordenados (a, b), donde a es un estudiante que ha tomado el curso b, y R_2 consta de todos los pares ordenados (a, b), donde a es un estudiante que requiere el curso b para graduarse. ¿Cuáles son las relaciones $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 \oplus R_2$, $R_1 - R_2$ y $R_2 - R_1$?

Solución: La relación $R_1 \cup R_2$ consta de todos los pares ordenados (a, b), donde a es un estudiante que ha tomado el curso b o necesita el curso b para graduarse, $R_1 \cap R_2$ es el conjunto de todos los pares ordenados (a, b), donde a es un estudiante que ha tomado el curso b y necesita este curso para graduarse.

Además, $R_1 \oplus R_2$ consta de todos los pares ordenados (a, b), donde el estudiante a ha tomado el curso b pero no lo necesita para graduarse o necesita el curso b para graduarse pero no lo ha tomado.

$R_1 - R_2$ es el conjunto de pares ordenados (a, b), donde a ha tomado el curso b pero no lo necesita para graduarse; es decir, b es un curso electivo que ha tomado a. $R_2 - R_1$ es el conjunto de todos los pares ordenados (a, b), donde b es un curso que a necesita para graduarse pero que no lo ha tomado.

□

Ejemplo 2.1.19 Sea R_1 la relación menor que en el conjunto de números reales y sea R_2 la relación mayor que en el conjunto de números reales, es decir, $R_1 = \{(x, y)|x < y\}$ y $R_2 = \{(x, y)|x > y\}$. ¿Cuáles son $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$ y $R_1 \oplus R_2$?

Solución: Observamos que $(x, y) \in R_1 \cup R_2$ si y sólo si $(x, y) \in R_1$ o $(x, y) \in R_2$. Por lo tanto, $(x, y) \in R_1 \cup R_2$ si y sólo si $x < y$ o $x > y$. Debido a que la condición $x < y$ o $x > y$ es la misma que la condición $x \neq y$, se sigue que $R_1 \cup R_2 = \{(x, y)|x \neq y\}$. En otras palabras, la unión de la relación menor que y la relación mayor que es la relación no iguales.

A continuación, observe que es imposible que un par (x, y) pertenezca tanto a R_1 como a R_2 porque es imposible que $x < y$ y $x > y$. De ello se deduce que $R_1 \cap R_2 = \emptyset$. También vemos que $R_1 - R_2 = R_1$, $R_2 - R_1 = R_2$ y $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(x, y)|x \neq y\}$. □

Existe otra forma de combinar relaciones que es análoga a la composición de funciones.

Definición 2.1.6 Sea R una relación de un conjunto A en un conjunto B y S una relación de B en un conjunto C. La *composición* de R y S es la relación que consta de pares ordenados (a, c), donde $a \in A$, $c \in C$, y para el cual existe un elemento $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Denotamos la composición de R y S por $S \circ R$.

Calcular la composición de dos relaciones requiere que encontremos elementos que son el segundo elemento de pares ordenados en la primera relación y el primer elemento de pares ordenados en la segunda relación, como lo ilustran los Ejemplos 2.1.20 y 2.1.21.

Ejemplo 2.1.20 ¿Cuál es la composición de las relaciones R y S?, donde R es la relación de $\{1, 2, 3\}$ a $\{1, 2, 3, 4\}$ y S es la relación de $\{1, 2, 3, 4\}$ a $\{0, 1, 2\}$ con:

$$R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$$
$$S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$$

Solución: $S \circ R$ se construye utilizando todos los pares ordenados en R y los pares ordenados en S, donde el segundo elemento del par ordenado en R concuerda con el primer elemento del par ordenado en S.

Por ejemplo, los pares ordenados $(2, 3)$ en R y $(3, 1)$ en S producen el par ordenado $(2, 1)$ en $S \circ R$. Calculando todos los pares ordenados en la composición, encontramos

$$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}.$$

La Figura 2.3 ilustra cómo se encuentra esta composición. En la figura, examinamos todos los caminos que viajan a través de dos aristas dirigidas desde los elementos más a la izquierda a los elementos más a la derecha a través de un elemento en el medio. □

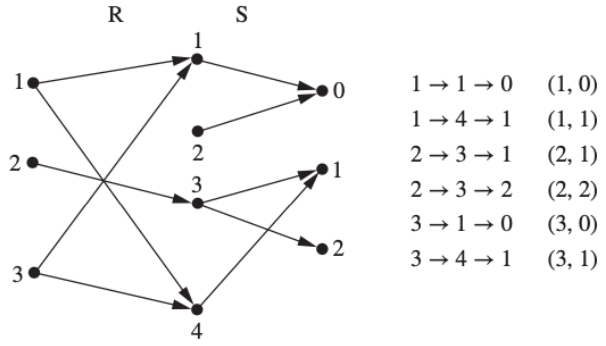


Figura 2.3: Construcción de $S \circ R$ para el Ejemplo 2.1.20.

Ejemplo 2.1.21 Componiendo la relación padre consigo misma Sea R la relación sobre el conjunto de todas las personas tal que $(a, b) \in R$ si la persona a es un padre de la persona b. Entonces $(a, c) \in R \circ R$ si y solo si hay una persona b tal que $(a, b) \in R$ y $(b, c) \in R$, es decir, si y sólo si hay una persona b tal que a es padre de b y b es padre de c. En otras palabras, $(a, c) \in R \circ R$ si y solo si a es abuelo de c. □

Las potencias de una relación R se pueden definir de forma recursiva a partir de la definición de la composición de dos relaciones.

Definición 2.1.7 Sea R una relación sobre el conjunto A. Las potencias $R^n, n = 1, 2, 3, \ldots$, se definen recursivamente por

$$R^1 = R \qquad \text{y} \qquad R^{n+1} = R^n \circ R.$$

La definición muestra que $R^2 = R \circ R$, $R^3 = R^2 \circ R = (R \circ R) \circ R$, y así sucesivamente.

Ejemplo 2.1.22 Sea $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$. Encuentre las potencias $R^n, n = 2, 3, 4, \ldots$.

Solución: Como $R^2 = R \circ R$, encontramos que

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

Además, debido a que $R^3 = R^2 \circ R$,

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

Un cálculo adicional muestra que R^4 es lo mismo que R^3, por lo que

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

También se deduce que $R^n = R^3$ para $n = 4, 5, 6, 7, \ldots$. □

El siguiente teorema muestra que las potencias de una relación transitiva son subconjuntos de esta relación.

Teorema 2.1.1 La relación R sobre un conjunto A es transitiva si y sólo si $R^n \subseteq R$ para $n = 1, 2, 3, \ldots$.

Demostración: Primero probamos la parte "si" del teorema. Suponemos que $R^n \subseteq R$ para $n = 1, 2, 3, \ldots$. En particular, $R^2 \subseteq R$. Para ver que esto implica que R es transitiva, tenga en cuenta que si $(a, b) \in R$ y $(b, c) \in R$, entonces, según la definición de composición, $(a, c) \in R^2$. Como $R^2 \subseteq R$, esto significa que $(a, c) \in R$. Por tanto, R es transitiva.

Usaremos inducción matemática para demostrar la parte "sólo si" del teorema. Tenga en cuenta que esta parte del teorema es trivialmente cierta para n = 1.

Suponga que $R^n \subseteq R$, donde n es un número entero positivo. Esta es la hipótesis inductiva. Para completar el paso inductivo debemos demostrar que esto implica que R^{n+1} es también un subconjunto de R.

Para mostrar esto, suponga que $(a, b) \in R^{n+1}$. Entonces, debido a que $R^{n+1} = R^n \circ R$, hay un elemento x con $x \in A$ tal que $(a, x) \in R$ y $(x, b) \in R^n$. La hipótesis inductiva, a saber, que $R^n \subseteq R$, implica que $(x, b) \in R$.

Además, debido a que R es transitiva y $(a, x) \in R$ y $(x, b) \in R$, se sigue que $(a, b) \in R$. Esto muestra que $R^{n+1} \subseteq R$, completando la demostración. ■

2.1.5. Ejercicios

1. Para cada una de estas relaciones sobre el conjunto $\{1, 2, 3, 4\}$, decida si es reflexiva, si es simétrica, si es antisimétrica y si es transitiva.

   a) $\{(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\}$.

   b) $\{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$.

   c) $\{(2,4),(4,2)\}$.

   d) $\{(1,2),(2,3),(3,4)\}$.

e) $\{(1,1),(2,2),(3,3),(4,4)\}$.

f) $\{(1,3),(1,4),(2,3),(2,4),(3,1),(3,4)\}$.

2. Sean

$$R_1 = \{(1,2),(2,3),(3,4)\} \text{ y}$$

$$R_2 = \{(1,1),(1,2),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3),(3,4)\}$$

relaciones de $\{1,2,3\}$ a $\{1,2,3,4\}$. Encontrar

a) $R_1 \cup R_2$.

b) $R_1 \cap R_2$.

c) $R_1 - R_2$.

d) $R_2 - R_1$.

3. Sean R la relación $\{(1,2),(1,3),(2,3),(2,4),(3,1)\}$ y sea S la relación $\{(2,1),(3,1),(3,2),(4,2)\}$. Encuentre $S \circ R$.

4. Sea R la relación del conjunto $\{1,2,3,4,5\}$ que contiene los pares ordenados (1, 1), (1, 2), (1, 3), (2, 3), (2, 4), (3, 1), (3, 4), (3, 5), (4, 2), (4, 5), (5, 1), (5, 2) y (5, 4). Encontrar

a) R^2. *b*) R^3. *c*) R^4. *d*) R^5.

2.2. Representación de Relaciones

2.2.1. Introducción

En esta sección, y en el resto de este capítulo, todas las relaciones que estudiamos serán relaciones binarias. Por ello, en esta sección y en el resto de este capítulo, la palabra relación siempre se referirá a una relación binaria.

Hay muchas formas de representar una relación entre conjuntos finitos. Como vimos en la sección 2.1, una forma es enumerar sus pares ordenados. Otra forma de representar una relación es usar una tabla, como hicimos en el Ejemplo 2.1.3 de la sección 2.1.

En esta sección discutiremos dos métodos alternativos para representar relaciones. Un método utiliza matrices cero-uno. El otro método usa representaciones pictóricas llamadas grafos dirigidos, que discutiremos más adelante en esta sección.

Generalmente, las matrices son apropiadas para la representación de relaciones en programas de computadora. Por otro lado, las personas a menudo

encuentran útil la representación de relaciones utilizando grafos dirigidos para comprender las propiedades de estas relaciones.

2.2.2. Representación de Relaciones usando Matrices

Una relación entre conjuntos finitos se puede representar utilizando una matriz cero-uno. Suponga que R es una relación de $A = \{a_1, a_2, \ldots, a_m\}$ a $B = \{b_1, b_2, \ldots, b_n\}$. (Aquí los elementos de los conjuntos A y B se han enumerado en un orden particular, pero arbitrario. Además, cuando $A = B$ usamos el mismo orden para A y B.) La relación R se puede representar mediante la matriz $M_R = [m_{ij}]$, donde

$$m_{ij} = \begin{cases} 1 \text{ si } (a, b) \in R, \\ 0 \text{ si } (a, b) \notin R. \end{cases}$$

En otras palabras, la matriz cero-uno que representa a R tiene un 1 como su entrada (i, j) cuando a_i está relacionada con b_j, y un 0 en esta posición si a_i no está relacionada con b_j. (Esta representación depende de los ordenamientos utilizados para A y B.)

El uso de matrices para representar relaciones se ilustra en los ejemplos 2.2.1-6.

Ejemplo 2.2.1 Suponga que $A = \{1, 2, 3\}$ y $B = \{1, 2\}$. Sea R la relación de A a B que contiene (a, b) si $a \in A, b \in B$ y $a > b$. ¿Cuál es la matriz que representa a R si $a_1 = 1, a_2 = 2$ y $a_3 = 3$, y $b_1 = 1$ y $b_2 = 2$?

Solución: Como $R = \{(2, 1), (3, 1), (3, 2)\}$, la matriz para R es

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

Los 1s en M_R muestran que los pares $(2, 1), (3, 1)$ y $(3, 2)$ pertenecen a R. Los 0s muestran que ningún otro par pertenece a R. □

Ejemplo 2.2.2 Sean $A = \{a_1, a_2, a_3\}$ y $B = \{b_1, b_2, b_3, b_4, b_5\}$. ¿Qué pares ordenados están en la relación R representada por la matriz

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

Solución: Como R consiste de los pares ordenados (a_i, b_j) con $m_{ij} = 1$, se sigue que

$$R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}.$$

□

La matriz de una relación en un conjunto, que es una matriz cuadrada, se puede utilizar para determinar si la relación tiene ciertas propiedades. Recuerde que una relación R sobre A es reflexiva si $(a, a) \in R$ siempre que $a \in A$. Por lo tanto, R es reflexiva si y sólo si $(a_i, a_i) \in R$ para $i = 1, 2, \ldots, n$.

Así, R es reflexiva si y sólo si $m_{ii} = 1$, para $i = 1, 2, \ldots, n$. En otras palabras, R es reflexiva si todos los elementos de la diagonal principal de M_R son iguales a 1, como se muestra en la Figura 2.4. Tenga en cuenta que, en general, los elementos de la diagonal principal pueden ser 0 o 1.

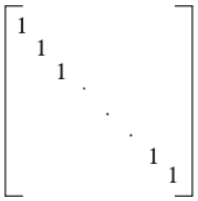


Figura 2.4: Matriz cero-uno para una relación reflexiva, los elementos fuera de la diagonal puden ser 0 o 1.

La relación R es simétrica si $(a, b) \in R$ implica que $(b, a) \in R$. En consecuencia, la relación R en el conjunto $A = \{a_1, a_2, \ldots, a_n\}$ es simétrica si y sólo si $(a_j, a_i) \in R$ siempre que $(a_i, a_j) \in R$. En términos de las entradas de M_R, R es simétrica si y sólo si $m_{ji} = 1$ siempre que $m_{ij} = 1$.

Esto también significa $m_{ji} = 0$ siempre que $m_{ij} = 0$. En consecuencia, R es simétrica si y sólo si $m_{ij} = m_{ji}$, para todos los pares de enteros i y j con $i = 1, 2, \ldots, n$ y $j = 1, 2, \ldots, n$. Recordando la definición de la transpuesta de una matriz vemos que R es simétrica si y sólo si

$$M_R = (M_R)^t,$$

es decir, si M_R es una matriz simétrica. La forma de la matriz para una relación simétrica se ilustra en la Figura 2.5(a).

La relación R es antisimétrica si y sólo si $(a, b) \in R$ y $(b, a) \in R$ implican que $a = b$. En consecuencia, la matriz de una relación antisimétrica tiene

la propiedad de que si $m_{ij} = 1$ con $i \neq j$, entonces $m_{ji} = 0$. O, en otras palabras, $m_{ij} = 0$ o $m_{ji} = 0$ cuando $i \neq j$. La forma de la matriz para una relación antisimétrica se ilustra en la Figura 2.5(b).

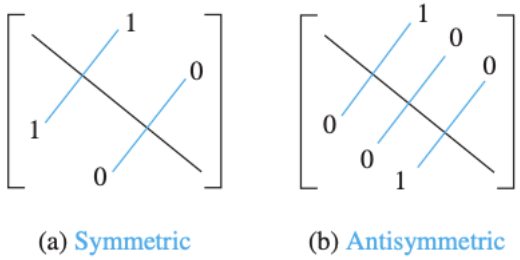


Figura 2.5: Las matrices cero-uno para relaciones simétricas y antisimétricas.

Ejemplo 2.2.3 Suponga que la relación R sobre un conjunto está representada por la matriz

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

¿R es reflexiva, simétrica y/o antisimétrica?

Solución: Como todos los elementos diagonales de esta matriz son iguales a 1, R es reflexiva. Además, como M_R es simétrica, se sigue que R es simétrica. También es fácil ver que R no es antisimétrica.

□

Las operaciones booleanas **join** y **meet** se pueden usar para encontrar las matrices que representan la unión y la intersección de dos relaciones. Suponga que R_1 y R_2 son relaciones sobre un conjunto A representadas por las matrices M_{R_1} y M_{R_2}, respectivamente. La matriz que representa la unión de estas relaciones tiene un 1 en las posiciones donde M_{R_1} o M_{R_2} tienen un 1. La matriz que representa la intersección de estas relaciones tienen un 1 en las posiciones donde tanto M_{R_1} como M_{R_2} tienen un 1. Por lo tanto, las matrices que representan la unión y la intersección de estas relaciones son

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} \qquad \text{y} \qquad M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}.$$

Ejemplo 2.2.4 Suponga que las relaciones R_1 y R_2 sobre un conjunto A están representadas por las matrices

$$M_{R_1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \text{y} \qquad M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

¿Cuáles son las matrices que representan $R_1 \cup R_2$ y $R_1 \cap R_2$?

Solución: Las matrices de estas relaciones son

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

□

Ahora dirigimos nuestra atención a determinar la matriz para la composición de relaciones. Esta matriz se puede encontrar usando el producto booleano de las matrices para estas relaciones.

En particular, suponga que R es una relación de A a B y que S es una relación de B a C. Suponga que A, B y C tienen m, n y p elementos, respectivamente. Sean las matrices cero-uno $M_{S \circ R} = [t_{ij}]$, $M_R = [r_{ij}]$ y $M_S = [s_{ij}]$ para $S \circ R$, R y S, respectivamente (estas matrices tienen tamaños $m \times p$, $m \times n$ y $n \times p$, respectivamente).

El par ordenado (a_i, c_j) pertenece a $S \circ R$ si y sólo si hay un elemento b_k tal que (a_i, b_k) pertenece a R y (b_k, c_j) pertenece a S. Se sigue que $t_{ij} = 1$ si y sólo si $r_{ik} = s_{kj} = 1$ para algún k. Por la definición del producto booleano, esto significa que

$$M_{S \circ R} = M_R \odot M_S.$$

Ejemplo 2.2.5 Encuentre la matriz que representa la relación $S \circ R$, donde las matrices que representan R y S son

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad \text{y} \qquad M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Solución: La matriz para $S \circ R$ es

$$M_{S\circ R} = M_R \odot M_S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

□

La matriz que representa la composición de dos relaciones se puede utilizar para encontrar la matriz para M_{R^n}. En particular,

$$M_{R^n} = M_R^{[n]},$$

por la definición de potencias Booleanas.

Ejemplo 2.2.6 Encuentre la matriz que representa la relación R^2, donde la matriz que representa a R es

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

Solución: La matriz para R^2 es

$$M_{R^2} = M_R^{[2]} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

□

2.2.3. Representación de Relaciones usando Digrafos

Hemos demostrado que una relación se puede representar enumerando todos sus pares ordenados o usando una matriz cero-uno. Existe otra forma importante de representar una relación mediante una representación pictórica.

Cada elemento del conjunto está representado por un punto, y cada par ordenado se representa mediante un arco con su dirección indicada por una flecha. Usamos tales representaciones pictóricas cuando pensamos en las relaciones en un conjunto finito como **grafos dirigidos** o **digrafos**.

Definición 2.2.1 Un *grafo dirigido*, o *digrafo*, consiste en un conjunto V de *vértices* (o *nodos*) junto con un conjunto E de pares ordenados de elementos de V llamados *aristas* (o *arcos*). El vértice a se llama *vértice inicial* de la arista (a, b) y el vértice b se llama *vértice terminal* de esta arista.

Una arista de la forma (a, a) se representa mediante una arista del vértice hacia sí mismo. Tal arista se llama ciclo.

Ejemplo 2.2.7 El grafo dirigido con vértices a, b, c y d, y aristas (a, b), (a, d), (b, b), (b, d), (c, a), (c, b), y (d, b) se muestra en la Figura 2.6.

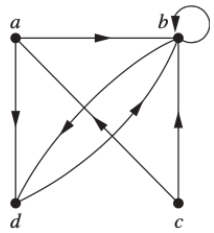


Figura 2.6: El grafo dirigido del Ejemplo 7.

□

Ejemplo 2.2.8 El grafo dirigido de la relación

$$R_1 = \{(1,1), (1,3), (2,1), (2,3), (2,4), (3,1), (3,2), (4,1)\}$$

sobre el conjunto $\{1, 2, 3, 4\}$ se muestra en la Figura 2.7.

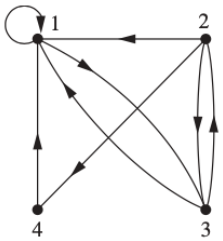


Figura 2.7: El grafo dirigido de la relación R_1 del Ejemplo 2.2.8.

□

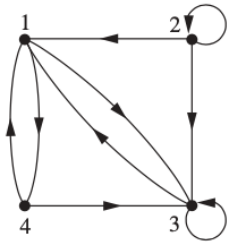


Figura 2.8: El grafo dirigido de la relación R_2 del Ejemplo 2.2.9.

Ejemplo 2.2.9 ¿Cuáles son los pares ordenados en la relación R_2 representados por el grafo dirigido que se muestra en la Figura 2.8?

Solución: Los pares ordenados (x, y) en la relación son

$$R_2 = \{(1,3), (1,4), (2,1), (2,2), (2,3), (3,1), (3,3), (4,1), (4,3)\}.$$

Cada uno de estos pares corresponde a una arista del grafo dirigido, $(2,2)$ y $(3,3)$ corresponden a los dos ciclos en el grafo. □

El grafo dirigido que representa una relación se puede utilizar para determinar si la relación tiene varias propiedades. Por ejemplo, una relación es reflexiva si y sólo si hay un ciclo en cada vértice del grafo dirigido, de modo que cada par ordenado de la forma (x, x) ocurre en la relación.

Una relación es simétrica si y sólo si para cada arista entre vértices distintos en su digrafo hay una arista en la dirección opuesta, de modo que (y, x) está en la relación siempre que (x, y) está en la relación. De manera similar, una relación es antisimétrica si y sólo si nunca hay dos aristas en direcciones opuestas entre vértices distintos.

Finalmente, una relación es transitiva si y sólo si siempre que hay una arista de un vértice x a un vértice y y una arista de un vértice y a un vértice z, hay una arista de x a z (completando un triángulo donde cada lado es una arista dirigida con la dirección correcta).

Observación 2.2.1 Tenga en cuenta que una relación simétrica se puede representar mediante un grafo no dirigido, que es un grafo en el que las aristas no tienen direcciones.

□

Ejemplo 2.2.10 Determine si las relaciones para los grafos dirigidos que se muestran en la Figura 2.9 son reflexivas, simétricas, antisimétricas y/o transitivas.

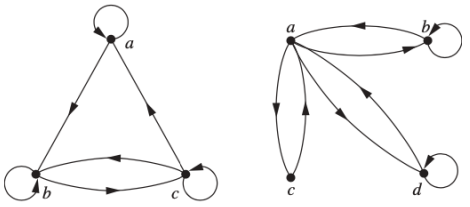


Figura 2.9: Los grafos dirigidos de las relaciones S_1 y S_2 del Ejemplo 2.2.10.

Solución: Debido a que hay ciclos en cada vértice del grafo dirigido de S_1, es reflexiva. La relación S_1 no es simétrica ni antisimétrica porque hay una arista de a a b pero no una de b a a, pero hay aristas en ambas direcciones que conectan b y c. Por último, S_1 no es transitiva porque hay una arista de a a b y una arista de b a c, pero no hay arista de a a c.

Ya que los ciclos no están presentes en todos los vértices del grafo dirigido de S_2, esta relación no es reflexiva. Es simétrica y no antisimétrica, porque cada arista entre vértices distintos está acompañada por una arista en la dirección opuesta. Tampoco es difícil ver en el grafo dirigido que S_2 no es transitiva, porque (c, a) y (a, b) pertenecen a S_2, pero (c, b) no pertenece a S_2.

□

2.2.4. Ejercicios

1. Represente cada una de estas relaciones sobre $\{1, 2, 3, 4\}$ con una matriz (con los elementos de este conjunto enumerados en orden creciente).

   a) $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$

   b) $\{(1, 1), (1, 4), (2, 2), (3, 3), (4, 1)\}$

   c) $\{(1, 2), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (3, 4), (4, 1), (4, 2), (4, 3)\}$

   d) $\{(2, 4), (3, 1), (3, 2), (3, 4)\}$

2. Enumere los pares ordenados en las relaciones sobre $\{1, 2, 3, 4\}$ correspondientes a estas matrices (donde las filas y columnas corresponden a los números enteros listados en orden creciente).

$a)$ $\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ $b)$ $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ $c)$ $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

3. Determine si las relaciones representadas por las matrices en el ejercicio 2 son reflexivas, simétricas, antisimétricas y/o transitivas.

4. Sean R_1 y R_2 relaciones sobre un conjunto A representadas por las matrices

$$M_{R_1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad \text{y} \qquad M_{R_2} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Encuentre las matrices que representan

$a)$ $R_1 \cup R_2$. $c)$ $R_1 \circ R_2$. $e)$ $R_1 \oplus R_2$.
$b)$ $R_1 \cap R_2$. $d)$ $R_2 \circ R_1$.

5. Sea R la relación representada por la matriz

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

Encuentre las matrices que representan

$a)$ R^2. $b)$ R^3. $c)$ R^4.

6. Enumere los pares ordenados en las relaciones representadas por los grafos dirigidos de la Figura 2.10.

7. Determine si las relaciones representadas por los grafos dirigidos de la Figura 2.10 son reflexivas, simétricas, antisimétricas, y/o transitivas.

8. Sea R una relación sobre un conjunto A. Explique cómo usar el grafo dirigido que representa a R para obtener el grafo dirigido que representa la relación inversa R^{-1}.

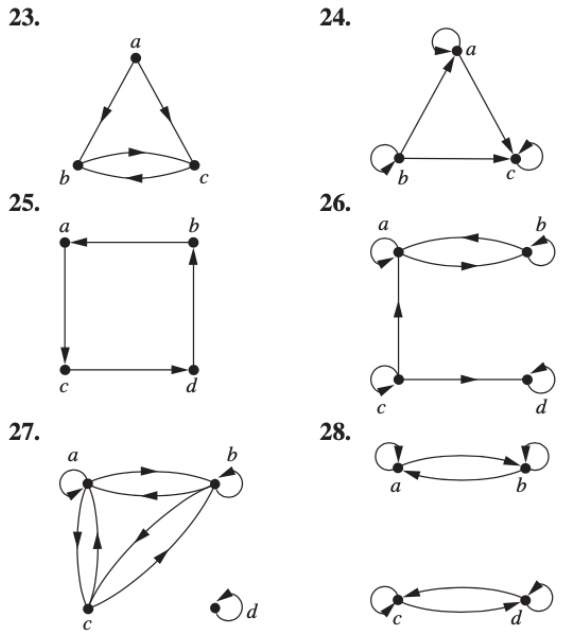


Figura 2.10: Grafos dirigidos para los Ejercicios 6 y 7.

2.3. Cerraduras de Relaciones

2.3.1. Introducción

Una red de computadoras tiene centros de datos en Boston, Chicago, Denver, Detroit, Nueva York y San Diego. Hay líneas telefónicas directas unidireccionales de Boston a Chicago, de Boston a Detroit, de Chicago a Detroit, de Detroit a Denver y de Nueva York a San Diego.

Sea R la relación que contiene (a, b) si hay una línea telefónica desde el centro de datos en a hasta el de b. ¿Cómo podemos determinar si existe algún enlace (posiblemente indirecto) compuesto por una o más líneas telefónicas de un centro a otro?

Debido a que no todos los enlaces son directos, como el enlace de Boston a Denver que pasa por Detroit, R no se puede utilizar directamente para responder a esto. En el lenguaje de las relaciones, R no es transitiva, por lo que no contiene todos los pares que se pueden vincular.

Como mostraremos en esta sección, podemos encontrar todos los pares de centros de datos que tienen un enlace al construir una relación transitiva

S que contenga R tal que S sea un subconjunto de toda relación transitiva que contenga R. Aquí, S es la relación transitiva más pequeña que contiene R. Esta relación se llama **cerradura transitiva** de R.

2.3.2. Diferentes tipos de cerraduras

Si R es una relación sobre un conjunto A, puede tener o no alguna propiedad P, como reflexividad, simetría o transitividad. Cuando R no tiene la propiedad P, nos gustaría encontrar la relación más pequeña S sobre A con la propiedad P que contiene R.

Definición 2.3.1 Si R es una relación sobre un conjunto A, entonces la *cerradura* de R con respecto a P, si existe, es la relación S sobre A con la propiedad P que contiene R y es un subconjunto de cada subconjunto de $A \times A$ que contiene R con propiedad P.

Si hay una relación S que es un subconjunto de cada relación que contiene R con propiedad P, debe ser única.

Para ver esto, suponga que las relaciones S y T tienen la propiedad P y son subconjuntos de toda relación con la propiedad P que contiene R. Entonces, S y T son subconjuntos entre sí y, por lo tanto, son iguales.

Tal relación, si existe, es la relación más pequeña con la propiedad P que contiene R porque es un subconjunto de toda relación con la propiedad P que contiene R.

Mostraremos cómo se pueden encontrar cerraduras reflexivas, simétricas y transitivas de relaciones.

La relación $R = \{(1,1),(1,2),(2,1),(3,2)\}$ sobre el conjunto $A = \{1,2,3\}$ no es reflexiva. ¿Cómo podemos producir una relación reflexiva que contenga R que sea lo más pequeña posible? Esto se puede hacer agregando $(2,2)$ y $(3,3)$ a R, porque estos son los únicos pares de la forma (a,a) que no están en R.

Esta nueva relación contiene R. Además, cualquier relación reflexiva que contiene R también debe contener $(2,2)$ y $(3,3)$. Debido a que esta relación contiene R, es reflexiva y está contenida dentro de cada relación reflexiva que contiene R, se denomina **cerradura reflexiva** de R.

Como ilustra este ejemplo, dada una relación R sobre un conjunto A, la cerradura reflexiva de R se puede formar sumando a R todos los pares de la

forma (a, a) con $a \in A$, que no estaban en R. La suma de estos pares produce una nueva relación que es reflexiva, contiene R, y está contenida dentro de cualquier relación reflexiva que contiene R. Vemos que la cerradura reflexiva de R es igual a $R \cup \Delta$, donde $\Delta = \{(a, a)|a \in A\}$ es la **relación diagonal** en A.

Ejemplo 2.3.1 ¿Cuál es la cerradura reflexiva de la relación $R = \{(a, b)|a < b\}$ sobre el conjunto de números enteros?

Solución: La cerradura reflexiva de R es

$$R \cup \Delta = \{(a, b)|a < b\} \cup \{(a, a)|a \in \mathbb{Z}\} = \{(a, b)|a \leq b\}.$$

□

La relación

$$\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$$

en $\{1, 2, 3\}$ no es simétrica. ¿Cómo podemos producir una relación simétrica que sea lo más pequeña posible y contenga R? Para hacer esto, solo necesitamos sumar $(2, 1)$ y $(1, 3)$, porque estos son los únicos pares de la forma (b, a) con $(a, b) \in R$ que no están en R.

Esta nueva relación es simétrica y contiene R. Además, cualquier relación simétrica que contiene R debe contener esta nueva relación, porque una relación simétrica que contiene R debe contener $(2, 1)$ y $(1, 3)$. En consecuencia, esta nueva relación se denomina **cerradura simétrica** de R.

Como ilustra este ejemplo, la cerradura simétrica de una relación R se puede construir sumando todos los pares ordenados de la forma (b, a), donde (a, b) está en la relación, que no están ya presentes en R. Sumando estos pares produce una relación que es simétrica, que contiene R, y que está contenida en cualquier relación simétrica que contiene R.

La cerradura simétrica de una relación se puede construir tomando la unión de una relación con su inversa, es decir, $R \cup R^{-1}$ es la cerradura simétrica de R, donde $R^{-1} = \{(b, a)|(a, b) \in R\}$.

Ejemplo 2.3.2 ¿Cuál es la cerradura simétrica de la relación $R = \{(a, b)|a > b\}$ en el conjunto de enteros positivos?

Solución: La cerradura simétrica de R es la relación

$$R \cup R^{-1} = \{(a, b)|a > b\} \cup \{(b, a)|a > b\} = \{(a, b)|a \neq b\}.$$

Esta última igualdad se sigue porque R contiene todos los pares ordenados de enteros positivos, donde el primer elemento es mayor que el segundo elemento, y R^{-1} contiene todos los pares ordenados de enteros positivos, donde el primer elemento es menor que el segundo. □

Suponga que una relación R no es transitiva. ¿Cómo podemos producir una relación transitiva que contenga R de manera que esta nueva relación esté contenida dentro de cualquier relación transitiva que contenga R? ¿Puede producirse la cerradura transitiva de una relación R sumando todos los pares de la forma (a, c), donde (a, b) y (b, c) ya están en la relación?

Considere la relación $R = \{(1, 3), (1, 4), (2, 1), (3, 2)\}$ sobre el conjunto $\{1, 2, 3, 4\}$. Esta relación no es transitiva porque no contiene todos los pares de la forma (a, c) donde (a, b) y (b, c) están en R. Los pares de esta forma que no están en R son $(1, 2), (2, 3), (2, 4)$ y $(3, 1)$. Sumar estos pares no produce una relación transitiva, porque la relación resultante contiene $(3, 1)$ y $(1, 4)$ pero no contiene $(3, 4)$.

Esto muestra que construir la cerradura transitiva de una relación es más complicado que construir las cerraduras reflexiva o simétrica. El resto de esta sección desarrolla algoritmos para construir cerraduras transitivas.

Como se mostrará más adelante en esta sección, la cerradura transitiva de una relación se puede encontrar agregando nuevos pares ordenados que deben estar presentes y luego repitiendo este proceso hasta que no se necesiten nuevos pares ordenados.

2.3.3. Rutas en grafos dirigidos

Veremos que representar relaciones mediante grafos dirigidos ayuda en la construcción de cerraduras transitivas. A continuación, presentamos algunos términos que usaremos para este propósito. Una ruta (o camino) en un grafo dirigido se obtiene atravesando las aristas (en la misma dirección que indica la flecha en la arista).

Definición 2.3.2 Una *ruta* (o *camino*) de a a b en el grafo dirigido G es una secuencia de aristas (x_0, x_1), (x_1, x_2), (x_2, x_3), $\ldots, (x_{n-1}, x_n)$ en G, donde n es un número entero no negativo, $x_0 = a$ y $x_n = b$, es decir, una secuencia de aristas donde el vértice terminal de una arista es el mismo que el vértice inicial en la siguiente arista de la ruta. Esta ruta se denota por $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ y tiene una longitud n. Vemos el conjunto vacío de aristas como una ruta de

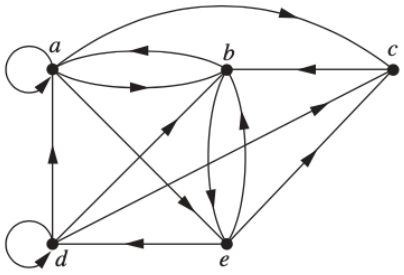


Figura 2.11: Grafo dirigido para el Ejemplo 2.3.3.

longitud cero de a a a. Una ruta de longitud $n \geq 1$ que comienza y termina en el mismo vértice se llama *circuito* o *ciclo*.

Una ruta en un grafo dirigido puede pasar por un vértice más de una vez. Además, una arista en un grafo dirigido puede ocurrir más de una vez en una ruta.

Ejemplo 2.3.3 ¿Cuáles de los siguientes son caminos en el grafo dirigido que se muestra en la Figura 2.11: a, b, e, d; a, e, c, d, b; b, a, c, b, a, a, b; d, c; c, b, a; e, b, a, b, a, b, e? ¿Cuáles son las longitudes de esos caminos? ¿Cuáles de los caminos de esta lista son circuitos?

Solución: Debido a que cada uno de $(a, b), (b, e)$ y (e, d) es una arista, a, b, e, d es una ruta de longitud tres. Como (c, d) no es una arista, a, e, c, d, b no es una ruta. Además, b, a, c, b, a, a, b es un camino de longitud seis porque $(b, a), (a, c), (c, b), (b, a), (a, a)$ y (a, b) son aristas. Vemos que d, c es un camino de longitud uno, porque (d, c) es una arista. También c, b, a es un camino de longitud dos, porque (c, b) y (b, a) son aristas. Todos $(e, b), (b, a), (a, b), (b, a), (a, b)$ y (b, e) son aristas, por lo que e, b, a, b, a, b, e es un camino de longitud seis.

Los dos caminos b, a, c, b, a, a, b y e, b, a, b, a, b, e son circuitos porque comienzan y terminan en el mismo vértice. Los caminos a, b, e, d; c, b, a y d, c no son circuitos. □

El término *ruta* también se aplica a las relaciones. Trasladando la definición de grafos dirigidos a relaciones, hay una **ruta** de a a b en R si hay una secuencia de elementos $a, x_1, x_2, \ldots, x_{n-1}, b$ con $(a, x_1) \in R$, $(x_1, x_2) \in R, \ldots$ y $(x_{n-1}, b) \in R$. El teorema 2.3.1 puede obtenerse de la definición de una

ruta en una relación.

Teorema 2.3.1 Sea R una relación sobre un conjunto A. Hay un camino de longitud n, donde n es un entero positivo, de a a b si y sólo si $(a, b) \in R^n$.

Demostración: Usaremos inducción matemática. Por definición, hay un camino de a a b de longitud uno si y sólo si $(a, b) \in R$, por lo que el teorema es verdadero cuando $n = 1$.

Suponga que el teorema es cierto para el entero positivo n. Esta es la hipótesis inductiva. Hay un camino de longitud $n + 1$ desde a hasta b si y sólo si hay un elemento $c \in A$ tal que hay un camino de longitud uno desde a hasta c, entonces $(a, c) \in R$, y un camino de longitud n de c a b, es decir, $(c, b) \in R^n$.

En consecuencia, según la hipótesis inductiva, hay un camino de longitud $n+1$ desde a hasta b si y sólo si hay un elemento c con $(a, c) \in R$ y $(c, b) \in R^n$. Pero existe tal elemento si y sólo si $(a, b) \in R^{n+1}$. Por lo tanto, hay un camino de longitud $n + 1$ de a a b si y sólo si $(a, b) \in R^{n+1}$. Esto completa la prueba. ■

2.3.4. Cerraduras transitivas

Ahora mostramos que encontrar la cerradura transitiva de una relación es equivalente a determinar qué pares de vértices en el grafo dirigido asociado están conectados por una ruta. Con esto en mente, definimos una nueva relación.

Definición 2.3.3 Sea R una relación sobre un conjunto A. La *relación de conectividad* R^* consta de los pares (a, b) tales que hay un camino de longitud al menos uno desde a hasta b en R.

Dado que R^n consta de los pares (a, b) tales que hay un camino de longitud n desde a hasta b, se deduce que R^* es la unión de todos los conjuntos R^n. En otras palabras,

$$R^* = \bigcup_{n=1}^{\infty} R^n.$$

La relación de conectividad es útil en muchos modelos.

Ejemplo 2.3.4 Sea R la relación sobre el conjunto de todas las personas en el mundo que contiene (a, b) si a ha conocido a b. ¿Qué es R^n, donde n es un número entero positivo mayor que uno? ¿Qué es R^*?

Solución: La relación R^2 contiene (a, b) si hay una persona c tal que $(a, c) \in R$ y $(c, b) \in R$, es decir, si hay una persona c tal que a ha conocido a c y c ha conocido a b.

De manera similar, R^n consta de esos pares (a, b) tales que hay personas $x_1, x_2, \ldots, x_{n-1}$ tales que a ha conocido a x_1, x_1 ha conocido a $x_2, \ldots,$ y x_{n-1} ha conocido a b.

La relación R^* contiene (a, b) si hay una secuencia de personas, comenzando con a y terminando con b, de manera que cada persona en la secuencia ha conocido a la siguiente persona en la secuencia.

Hay muchas conjeturas interesantes sobre R^*. ¿Crees que esta relación de conectividad incluye a la pareja contigo como primer elemento y al presidente de Mongolia como segundo elemento? □

Ejemplo 2.3.5 Sea R la relación del conjunto de todas las paradas del metro en la ciudad de Nueva York que contiene (a, b) si es posible viajar desde la parada a hasta la parada b sin cambiar de tren. ¿Qué es R^n cuando n es un número entero positivo? ¿Qué es R^*?

Solución: La relación R^n contiene (a, b) si es posible viajar desde la parada a hasta la parada b haciendo como máximo $n - 1$ cambios de trenes. La relación R^* consta de los pares ordenados (a, b) donde es posible viajar desde la parada a hasta la parada b haciendo tantos cambios de tren como sea necesario. □

Ejemplo 2.3.6 Sea R la relación del conjunto de todos los estados de los Estados Unidos que contiene (a, b) si el estado a y el estado b tienen una frontera común. ¿Qué es R^n, donde n es un número entero positivo? ¿Qué es R^*?

Solución: La relación R^n consta de los pares (a, b), donde es posible pasar del estado a al estado b cruzando exactamente n fronteras estatales. R^* consta de los pares ordenados (a, b), donde es posible pasar del estado a al estado b cruzando tantas fronteras como sea necesario.

Los únicos pares ordenados que no están en R^* son los que contienen estados que no están conectados a los Estados Unidos continentales (es decir, los pares que contienen Alaska o Hawai). □

El Teorema 2.3.2 muestra que la cerradura transitiva de una relación y la relación de conectividad asociada son lo mismo.

Teorema 2.3.2 La cerradura transitiva de una relación R es igual a la relación de conectividad R^*.

Demostración: Tenga en cuenta que R^* contiene R por definición. Para mostrar que R^* es la cerradura transitiva de R, también debemos mostrar que R^* es transitiva y que $R^* \subseteq S$ siempre que S es una relación transitiva que contiene R.

Primero, mostramos que R^* es transitiva. Si $(a, b) \in R^*$ y $(b, c) \in R^*$, entonces hay caminos de a a b y de b a c en R. Obtenemos un camino de a a c al comenzar con el camino de a a b y seguirlo con el camino de b a c. Por tanto, $(a, c) \in R^*$. De ello se deduce que R^* es transitiva.

Suponga ahora que S es una relación transitiva que contiene R. Dado que S es transitiva, S^n también es transitiva (el lector debe verificarlo) y $S^n \subseteq S$ (según el Teorema 2.1.1). Aún más, ya que

$$S^* = \bigcup_{k=1}^{\infty} S^k$$

y $S^k \subseteq S$, se sigue que $S^* \subseteq S$.

Ahora observe que si $R \subseteq S$, entonces $R^* \subseteq S^*$, porque cualquier camino en R también es un camino en S. En consecuencia, $R^* \subseteq S^* \subseteq S$. Por lo tanto, cualquier relación transitiva que contenga R también debe contener R^*. Así, R^* es la cerradura transitiva de R. ■

Ahora que sabemos que la cerradura transitiva es igual a la relación de conectividad, dirigimos nuestra atención al problema de calcular esta relación. No es necesario examinar trayectorias arbitrariamente largas para determinar si existe una trayectoria entre dos vértices en un grafo dirigido finito. Como muestra el Lema 2.3.1, es suficiente examinar caminos que no contengan más de n aristas, donde n es el número de elementos del conjunto.

Lema 2.3.1 Sea A un conjunto con n elementos, y sea R una relación sobre A. Si hay un camino de longitud al menos uno en R desde a hasta b, entonces existe un camino con una longitud que no excede a n. Además, cuando $a \neq b$, si hay un camino de longitud al menos uno en R desde a hasta b, entonces existe un camino con una longitud que no excede a $n - 1$.

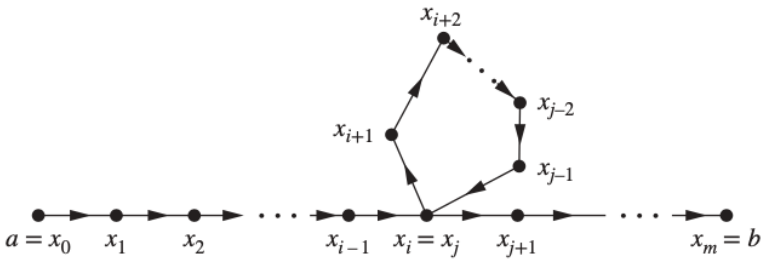


Figura 2.12: Produciendo un camino con longitud no mayor a n.

Demostración: Suponga que hay un camino desde a hasta b en R. Sea m la longitud del camino más corto. Suponga que $x_0, x_1, x_2, \ldots, x_{m-1}, x_m$, donde $x_0 = a$ y $x_m = b$, es ese camino. Suponga también que $a = b$ y que $m > n$, de modo que $m \geq n + 1$. Por el principio del casillero, porque hay n vértices en A, entre los m vértices $x_0, x_1, \ldots, x_{m-1}$, al menos dos son iguales (ver Figura 2.12).

Suponga que $x_i = x_j$ con $0 \leq i < j \leq m-1$. Entonces, el camino contiene un circuito desde x_i a sí mismo. Este circuito se puede eliminar de la ruta de a a b, dejando una ruta, a saber, $x_0, x_1, \ldots, x_i, x_j + 1, \ldots, x_{m-1}, x_m$, de a a b de menor longitud. Por tanto, la ruta de menor longitud debe tener una longitud menor o igual que n.

El caso donde $a \neq b$ se deja como ejercicio para el lector. ■

Del Lema 2.3.1, vemos que la cerradura transitiva de R es la unión de $R, R^2, R^3, \ldots$ y R^n. Esto se debe a que hay una ruta en R^* entre dos vértices si y sólo si hay una ruta entre estos vértices en R^i, para algún entero positivo i con $i \leq n$. Porque

$$R^* = R \cup R^2 \cup R^3 \cup \ldots \cup R^n$$

y la matriz cero-uno que representa una unión de relaciones es la unión de las matrices cero-uno de estas relaciones. La matriz cero-uno para la cerradura transitiva es la unión de las matrices cero-uno de las primeras n potencias de la matriz cero-uno de R.

Teorema 2.3.3 Sea M_R la matriz cero-uno de la relación R sobre un conjunto con n elementos. Entonces la matriz cero-uno de la cerradura transitiva R^* es

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}.$$

■

Ejemplo 2.3.7 Encuentre la matriz cero-uno de la cerradura transitiva de la relación R donde

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

Solución: Por el Teorema 2.3.3, se sigue que la matriz cero-uno de R^* es

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]}$$

Dado que

$$M_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{y} \qquad M_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

se sigue que

$$M_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

□

El Teorema 2.3.3 se puede utilizar como base para un algoritmo para calcular la matriz de la relación R^*. Para encontrar esta matriz, se calculan las sucesivas potencias booleanas de M_R, hasta la enésima potencia.

A medida que se calcula cada potencia, se forma su unión con la unión de todas las potencias menores. Cuando se hace esto con la enésima potencia, se ha encontrado la matriz para R^*. Este procedimiento se muestra como el Algoritmo 1.

procedure *transitive closure* ($\mathbf{M}_R$: zero–one $n \times n$ matrix)
$\mathbf{A} := \mathbf{M}_R$
$\mathbf{B} := \mathbf{A}$
for $i := 2$ **to** n
  $\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$
  $\mathbf{B} := \mathbf{B} \vee \mathbf{A}$
return $\mathbf{B}$ {$\mathbf{B}$ is the zero–one matrix for R^*}

Algoritmo 1: Un procedimiento para calcular la cerradura transitiva.

2.3.5. Ejercicios

1. Sea R la relación del conjunto $\{0, 1, 2, 3\}$ que contiene los pares ordenados $(0, 1)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 2)$ y $(3, 0)$. Encuentra la

   a) cerradura reflexiva de R. *b*) cerradura simétrica de R.

2. Sea R la relación $\{(a, b)|a \neq b\}$ sobre el conjunto de enteros. ¿Cuál es la cerradura reflexiva de R?

3. Dibuje el grafo dirigido de la cerradura reflexiva para cada una de las relaciones cuyos grafos dirigidos se muestran en la Figura 2.13.

4. Dibuje el grafo dirigido de la cerradura simétrica para cada una de las relaciones cuyos grafos dirigidos se muestran en la Figura 2.13.

5. Sea R la relación del conjunto $\{1, 2, 3, 4, 5\}$ que contiene los pares ordenados $(1, 3)$, $(2, 4)$, $(3, 1)$, $(3, 5)$, $(4, 3)$, $(5, 1)$, $(5, 2)$ y $(5, 4)$. Encuentre

   a) R^2. *b*) R^3. *c*) R^4. *d*) R^5. *e*) R^6. *f*) R^*.

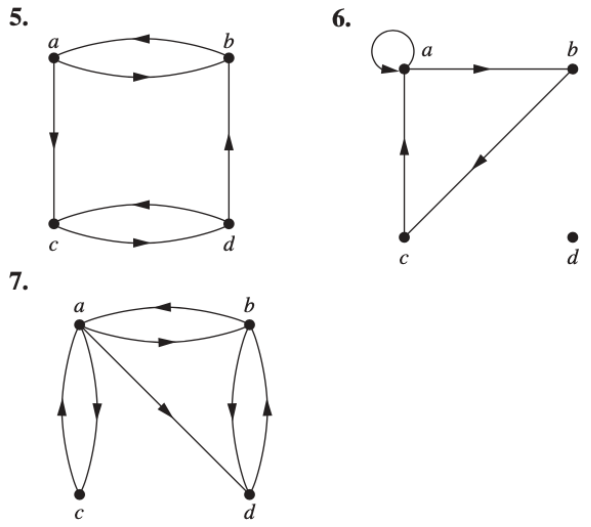


Figura 2.13: Grafos dirigidos para los Ejercicios 3 y 4.

6. Utilice el Algoritmo 1 para encontrar las cerraduras transitivas de las siguientes relaciones sobre $\{1, 2, 3, 4\}$.

   a) $\{(1,2),(2,1),(2,3),(3,4),(4,1)\}$,
   b) $\{(2,1),(2,3),(3,1),(3,4),(4,1),(4,3)\}$,
   c) $\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$,
   d) $\{(1,1),(1,4),(2,1),(2,3),(3,1),(3,2),(3,4),(4,2)\}$.

2.4. Relaciones de Equivalencia

2.4.1. Introducción

En algunos lenguajes de programación, los nombres de las variables pueden contener un número ilimitado de caracteres. Sin embargo, existe un límite en el número de caracteres que se comprueban cuando un compilador determina si dos variables son iguales.

Por ejemplo, en C tradicional, el compilador solo verifica los primeros ocho caracteres de un nombre de variable. (Estos caracteres son letras mayúsculas o minúsculas, dígitos o guiones bajos). En consecuencia, el compilador considera las cadenas de más de ocho caracteres que coinciden en sus primeros ocho caracteres como iguales.

Sea R la relación en el conjunto de cadenas de caracteres tal que sRt, donde s y t son dos cadenas, si s y t tienen al menos ocho caracteres de longitud y los primeros ocho caracteres de s y t concuerdan, o $s = t$. Es fácil ver que R es reflexiva, simétrica y transitiva. Además, R divide el conjunto de todas las cadenas en clases, donde todas las cadenas de una clase en particular son consideradas iguales por un compilador de C.

Los enteros a y b están relacionados por la relación de "congruencia módulo 4" cuando 4 divide $a - b$. Más adelante mostraremos que esta relación es reflexiva, simétrica y transitiva.

No es difícil ver que a está relacionado con b si y sólo si a y b tienen el mismo resto cuando se dividen por 4. De ello se deduce que esta relación divide el conjunto de números enteros en cuatro clases diferentes. Cuando sólo nos importa el resto que deja un entero cuando se divide entre 4, sólo necesitamos saber en qué clase está, no su valor particular.

Estas dos relaciones, R y congruencia módulo 4, son ejemplos de relaciones de equivalencia, es decir, relaciones reflexivas, simétricas y transitivas. En esta sección mostraremos que tales relaciones dividen conjuntos en clases disjuntas de elementos equivalentes.

Las relaciones de equivalencia surgen siempre que nos preocupemos sólo de si un elemento de un conjunto pertenece a una determinada clase de elementos, en lugar de preocuparnos por su identidad particular.

2.4.2. Relaciones de Equivalencia

En esta sección estudiaremos relaciones con una combinación particular de propiedades que les permite ser utilizadas para relacionar objetos que son similares de alguna manera.

Definición 2.4.1 Una relación sobre un conjunto A se llama *relación de equivalencia* si es reflexiva, simétrica y transitiva.

Las relaciones de equivalencia son importantes en matemáticas y ciencias de la computación. Una razón de esto es que en una relación de equivalencia, cuando dos elementos están relacionados, tiene sentido decir que son equivalentes.

Definición 2.4.2 Dos elementos a y b que están relacionados por una relación de equivalencia se denominan *equivalentes*. La notación $a \sim b$ se usa a

menudo para denotar que a y b son elementos equivalentes con respecto a una relación de equivalencia particular.

Para que la noción de elementos equivalentes tenga sentido, cada elemento debe ser equivalente a sí mismo, ya que la propiedad reflexiva garantiza una relación de equivalencia.

Tiene sentido decir que a y b están relacionados (no sólo que a está relacionado con b) por una relación de equivalencia, porque cuando a está relacionado con b, por la propiedad simétrica, b está relacionado con a.

Además, debido a que una relación de equivalencia es transitiva, si a y b son equivalentes y b y c son equivalentes, se deduce que a y c son equivalentes.

Los ejemplos 2.4.1 a 2.4.5 ilustran la noción de relación de equivalencia.

Ejemplo 2.4.1 Sea R la relación sobre el conjunto de enteros tal que aRb si y sólo si $a = b$ o $a = -b$. En la sección 2.1 mostramos que R es reflexiva, simétrica y transitiva. De ello se deduce que R es una relación de equivalencia. □

Ejemplo 2.4.2 Sea R la relación sobre el conjunto de números reales tal que aRb si y sólo si $a-b$ es un número entero. ¿Es R una relación de equivalencia?

Solución: Como $a - a = 0$ es un número entero para todos los números reales a, aRa para todos los números reales a. Por tanto, R es reflexiva. Ahora suponga que aRb. Entonces $a - b$ es un número entero, así que $b - a$ también es un número entero. Por lo tanto, bRa. De ello se deduce que R es simétrica. Si aRb y bRc, entonces $a - b$ y $b - c$ son números enteros. Por lo tanto, $a - c = (a - b) + (b - c)$ también es un número entero. Por lo tanto, aRc. Por tanto, R es transitiva. En consecuencia, R es una relación de equivalencia. □

Una de las relaciones de equivalencia más utilizadas es congruencia módulo m donde m es un número entero mayor que 1.

Ejemplo 2.4.3 Congruencia Módulo m. Sea m un número entero tal que $m > 1$. Demuestre que la relación

$$R = \{(a, b)|a \equiv b \pmod{m}\}$$

es una relación de equivalencia sobre el conjunto de números enteros.

Solución: Recuerde que $a \equiv b \pmod{m}$ si y sólo si m divide $a - b$. Tenga en cuenta que $a - a = 0$ es divisible entre m, porque $0 = 0 \cdot m$. Por tanto, $a \equiv a \pmod{m}$, por lo que la congruencia módulo m es reflexiva.

Ahora suponga que $a \equiv b \pmod{m}$. Entonces $a - b$ es divisible por m, entonces $a - b = km$, donde k es un número entero. De ello se deduce que $b - a = (-k)m$, entonces $b \equiv a \pmod{m}$. Por tanto, la congruencia módulo m es simétrica.

A continuación, suponga que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$. Entonces m divide tanto $a - b$ como $b - c$. Por tanto, hay enteros k y l con $a - b = km$ y $b - c = lm$. La suma de estas dos ecuaciones muestra que $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Por lo tanto, $a \equiv c \pmod{m}$.

De este modo, la congruencia módulo m es transitiva. De ello se deduce que la congruencia módulo m es una relación de equivalencia. □

Ejemplo 2.4.4 Suponga que R es la relación sobre el conjunto de cadenas de letras del alfabeto inglés tal que aRb si y sólo si $l(a) = l(b)$, donde $l(x)$ es la longitud de la cadena x. ¿Es R una relación de equivalencia?

Solución: Como $l(a) = l(a)$, se deduce que aRa siempre que a es una cadena, de modo que R es reflexiva.

A continuación, suponga que aRb, de modo que $l(a) = l(b)$. Entonces bRa, porque $l(b) = l(a)$. Por tanto, R es simétrica.

Finalmente, suponga que aRb y bRc. Entonces $l(a) = l(b)$ y $l(b) = l(c)$. Por tanto, $l(a) = l(c)$, entonces aRc. En consecuencia, R es transitiva. Como R es reflexiva, simétrica y transitiva entonces es una relación de equivalencia. □

Ejemplo 2.4.5 Sean n un entero positivo y S un conjunto de cadenas. Suponga que R_n es la relación sobre S tal que sR_nt si y sólo si $s = t$, o ambos s y t tienen al menos n caracteres y los primeros n caracteres de s y t son iguales.

Es decir, una cadena de menos de n caracteres está relacionada sólo consigo misma; una cadena s con al menos n caracteres está relacionada con una cadena t si y sólo si t tiene al menos n caracteres y t comienza con los n caracteres iniciales de s.

Por ejemplo, sea $n = 3$ y sea S el conjunto de todas las cadenas de bits. Entonces sR_3t cuando $s = t$ o tanto s como t son cadenas de bits de longitud 3 o más que comienzan con los mismos tres bits. Por ejemplo, $01R_301$ y $00111R_300101$, pero $01\not{R}_3010$ y $01011\not{R}_301110$.

Demuestre que para cada conjunto S de cadenas y cada entero positivo n, R_n es una relación de equivalencia sobre S.

Solución: La relación R_n es reflexiva porque $s = s$, de modo que sR_ns siempre que s es una cadena en S.

Si sR_nt, entonces $s = t$ o s y t tienen al menos n caracteres de longitud que comienzan con los mismos n caracteres. Esto significa que tR_ns. Concluimos que R_n es simétrica.

Ahora suponga que sR_nt y tR_nu. Entonces, $s = t$ o s y t tienen al menos n caracteres de longitud y s y t comienzan con los mismos n caracteres, y $t = u$ o t y u tienen al menos n caracteres de longitud y t y u comienzan con los mismos n caracteres.

A partir de esto, podemos deducir que $s = u$ o ambos s y u tienen n caracteres de longitud y s y u comienzan con los mismos n caracteres (porque en este caso sabemos que s, t y u tienen al menos n caracteres de longitud y tanto s como u comienzan con los mismos n caracteres que t). En consecuencia, R_n es transitiva. De ello se deduce que R_n es una relación de equivalencia. □

En los ejemplos 2.4.6 y 2.4.7 consideramos dos relaciones que no son relaciones de equivalencia.

Ejemplo 2.4.6 Muestre que la relación "divide" sobre el conjunto de enteros positivos no es una relación de equivalencia.

Solución: Por los ejemplos 2.1.9 y 2.1.15 de la sección 2.1, sabemos que la relación "divide" es reflexiva y transitiva. Sin embargo, por el ejemplo 2.1.12 de la sección 2.1, sabemos que esta relación no es simétrica (por ejemplo, $2|4$ pero $4\not|2$). Concluimos que la relación "divide" en el conjunto de enteros positivos no es una relación de equivalencia. □

Ejemplo 2.4.7 Sea R la relación sobre el conjunto de números reales tal que xRy si y sólo si x y y son números reales que difieren en menos de 1, es decir, $|x - y| < 1$. Muestre que R no es una relación de equivalencia.

Solución: R es reflexiva porque $|x - x| = 0 < 1$ siempre que $x \in \mathbb{R}$.

R es simétrica, porque si xRy, donde x y y son números reales, entonces $|x - y| < 1$, lo que nos dice que $|y - x| = |x - y| < 1$, de modo que yRx.

Sin embargo, R no es una relación de equivalencia porque no es transitiva. Tome $x = 2.8$, $y = 1.9$ y $z = 1.1$, de modo que $|x-y| = |2.8-1.9| = 0.9 < 1$, $|y - z| = |1.9 - 1.1| = 0.8 < 1$, pero $|x - z| = |2.8 - 1.1| = 1.7 > 1$. Es decir, $2.8R1.9$, $1.9R1.1$, pero $2.8\not R1.1$. □

2.4.3. Clases de Equivalencia

Sea A el conjunto de todos los estudiantes de su escuela que se graduaron de la escuela secundaria. Considere la relación R sobre A que consta de todos los pares (x, y), donde x y y se graduaron de la misma escuela secundaria.

Dado un estudiante x, podemos formar el conjunto de todos los estudiantes equivalentes a x con respecto a R. Este conjunto consta de todos los estudiantes que se graduaron de la misma escuela secundaria que x. Este subconjunto de A se denomina clase de equivalencia de la relación.

Definición 2.4.3 Sea R una relación de equivalencia sobre un conjunto A. El conjunto de todos los elementos que están relacionados con un elemento a de A se denomina la *clase de equivalencia* de a. La clase de equivalencia de a con respecto a R se denota por $[a]_R$. Cuando sólo se está considerando una relación, podemos eliminar el subíndice R y escribir $[a]$ para esta clase de equivalencia.

En otras palabras, si R es una relación de equivalencia sobre un conjunto A, la clase de equivalencia del elemento a es

$$[a]_R = \{s|(a, s) \in R\}.$$

Si $b \in [a]_R$, entonces b se denomina **representante** de esta clase de equivalencia. Cualquier elemento de una clase se puede utilizar como representante de esta clase. Es decir, no hay nada especial en el elemento particular elegido como representante de la clase.

Ejemplo 2.4.8 ¿Cuál es la clase de equivalencia de un número entero para la relación de equivalencia del ejemplo 2.4.1?

Solución: Dado que un número entero es equivalente a sí mismo y su negativo en esta relación de equivalencia, se sigue que $[a] = \{-a, a\}$. Este conjunto contiene dos números enteros distintos a menos que $a = 0$. Por ejemplo, $[7] = \{-7, 7\}$, $[-5] = \{-5, 5\}$ y $[0] = \{0\}$. □

Ejemplo 2.4.9 ¿Cuáles son las clases de equivalencia de 0, 1, 2 y 3 para la congruencia módulo 4?

Solución: La clase de equivalencia de 0 contiene todos los enteros a tales que $a \equiv 0 \pmod 4$. Los números enteros de esta clase son los divisibles por

4. Por tanto, la clase de equivalencia de 0 para esta relación es

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

La clase de equivalencia de 1 contiene todos los enteros a tales que $a \equiv 1 \pmod 4$. Los enteros en esta clase son aquellos que tienen un resto de 1 cuando se dividen por 4. Por lo tanto, la clase de equivalencia de 1 para esta relación es

$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}.$$

La clase de equivalencia de 2 contiene todos los enteros a tales que $a \equiv 2 \pmod 4$. Los enteros en esta clase son aquellos que tienen un resto de 2 cuando se dividen por 4. Por lo tanto, la clase de equivalencia de 2 para esta relación es

$$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}.$$

La clase de equivalencia de 3 contiene todos los enteros a tales que $a \equiv 3 \pmod 4$. Los enteros en esta clase son aquellos que tienen un resto de 3 cuando se dividen por 4. Por lo tanto, la clase de equivalencia de 3 para esta relación es

$$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

Tenga en cuenta que cada entero está en exactamente una de las cuatro clases de equivalencia y que el entero n está en la clase que contiene $n \bmod 4$. □

En el Ejemplo 2.4.9 se encontraron las clases de equivalencia de 0, 1, 2 y 3 con respecto a la congruencia módulo 4. El ejemplo 2.4.9 se puede generalizar fácilmente, reemplazando 4 con cualquier entero positivo m.

Las clases de equivalencia de la relación congruencia módulo m se denominan **clases de congruencia módulo** m. La clase de congruencia de un entero a módulo m se denota por $[a]_m$, entonces

$$[a]_m = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}.$$

Por ejemplo, del ejemplo 2.4.9 tenemos

$$\begin{aligned}
[0]_4 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\},\\
[1]_4 &= \{\ldots, -7, -3, 1, 5, 9, \ldots\},\\
[2]_4 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\},\\
[3]_4 &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}.
\end{aligned}$$

Ejemplo 2.4.10 ¿Cuál es la clase de equivalencia de la cadena 0111 con respecto a la relación de equivalencia R_3 del ejemplo 2.4.5 sobre el conjunto de todas las cadenas de bits? (Recuerde que sR_3t si y sólo si s y t son cadenas de bits con $s = t$ o s y t son cadenas de al menos tres bits que comienzan con los mismos tres bits).

Solución: Las cadenas de bits equivalentes a 0111 son las cadenas de bits con al menos tres bits que comienzan con 011. Estas son las cadenas de bits 011, 0110, 0111, 01100, 01101, 01110, 01111, etc. Por consiguiente,

$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\}.$$

□

2.4.4. Clases de Equivalencia y Particiones

Sea A el conjunto de estudiantes de su escuela que se especializan en exactamente una disciplina, y sea R la relación sobre A que consta de pares (x, y), donde x y y son estudiantes con la misma especialización. Entonces R es una relación de equivalencia, como debe verificar el lector.

Podemos ver que R divide a todos los estudiantes en A en una colección de subconjuntos disjuntos, donde cada subconjunto contiene estudiantes con una especialización específica. Por ejemplo, un subconjunto contiene a todos los estudiantes que se especializan (sólo) en ciencias de la computación, y un segundo subconjunto contiene a todos los estudiantes que se especializan en historia.

Además, estos subconjuntos son clases de equivalencia de R. Este ejemplo ilustra cómo las clases de equivalencia de una relación de equivalencia dividen un conjunto en subconjuntos disjuntos no vacíos. Precisaremos estas nociones en la siguiente discusión.

Sea R una relación sobre el conjunto A. El Teorema 2.4.1 muestra que las clases de equivalencia de dos elementos de A son idénticas o disjuntas.

Teorema 2.4.1 Sea R una relación de equivalencia sobre un conjunto A. Estos enunciados para los elementos a y b de A son equivalentes:

1. aRb
2. $[a] = [b]$
3. $[a] \cap [b] \neq \emptyset$

Demostración:

1. → 2. Asuma que aRb. Demostraremos que $[a] = [b]$ mostrando $[a] \subseteq [b]$ y $[b] \subseteq [a]$. Suponga $c \in [a]$. Entonces aRc. Como aRb y R es simétrica, sabemos que bRa.

Además, debido a que R es transitiva y bRa y aRc, se sigue que bRc. Por tanto, $c \in [b]$. Esto muestra que $[a] \subseteq [b]$. La prueba de que $[b] \subseteq [a]$ es similar y se deja como ejercicio para el lector.

2. → 3. Suponga que $[a] = [b]$. De ello se deduce que $[a] \cap [b] \neq \emptyset$ porque $[a]$ no está vacía (porque $a \in [a]$ y R es reflexiva).

3. → 1. Suponga que $[a] \cap [b] \neq \emptyset$. Entonces hay un elemento c con $c \in [a]$ y $c \in [b]$. En otras palabras, aRc y bRc. Por la propiedad simétrica, cRb. Luego, por transitividad, ya que aRc y cRb, tenemos aRb.

Ya que 1. → 2., 2. → 3. y 3. → 1., los tres enunciados son equivalentes. ■

Ahora estamos en condiciones de mostrar cómo una relación de equivalencia *particiona* un conjunto. Sea R una relación de equivalencia sobre un conjunto A. La unión de las clases de equivalencia de R es todo A, porque un elemento a de A está en su propia clase de equivalencia, a saber, $[a]_R$. En otras palabras,

$$\bigcup_{a \in A} [a]_R = A.$$

Además, del Teorema 2.4.1 se deduce que estas clases de equivalencia son iguales o disjuntas, por lo que

$$[a]_R \cap [b]_R = \emptyset,$$

cuando $[a]_R \neq [b]_R$.

Estas dos observaciones muestran que las clases de equivalencia forman una partición de A, porque dividen A en subconjuntos disjuntos. Más precisamente, una **partición** sobre un conjunto S es una colección de subconjuntos no vacíos disjuntos de S que tienen S 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 de S si y sólo si

$$A_i \neq \emptyset \text{ para } i \in I,$$

$$A_i \cap A_j = \emptyset \text{ cuando } i \neq j,$$

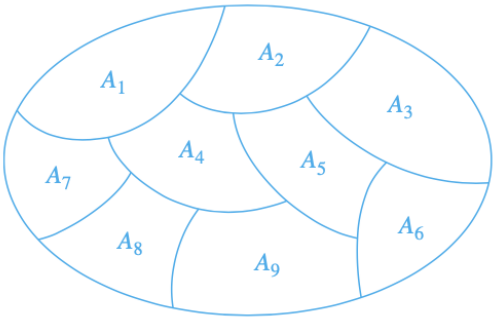


Figura 2.14: Una partición de un conjunto.

y

$$\bigcup_{i \in I} A_i = S.$$

La Figura 2.14 ilustra el concepto de partición de un conjunto.

Ejemplo 2.4.11 Suponga que $S = \{1, 2, 3, 4, 5, 6\}$. La colección de conjuntos $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$ y $A_3 = \{6\}$ forma una partición de S, porque estos conjuntos son disjuntos y su unión es S. □

Hemos visto que las clases de equivalencia de una relación de equivalencia sobre un conjunto forman una partición del conjunto. Los subconjuntos de S en esta partición son las clases de equivalencia.

A la inversa, cada partición de un conjunto se puede utilizar para formar una relación de equivalencia. Dos elementos son equivalentes con respecto a esta relación si y sólo si están en el mismo subconjunto de S en la partición.

Para ver esto, suponga que $\{A_i | i \in I\}$ es una partición sobre S. Sea R la relación sobre S que consta de los pares (x, y), donde x y y pertenecen al mismo subconjunto A_i en la partición. Para demostrar que R es una relación de equivalencia, debemos demostrar que R es reflexiva, simétrica y transitiva.

Vemos que $(a, a) \in R$ para todo $a \in S$, porque a está en el mismo subconjunto de S que él mismo. Por tanto, R es reflexiva.

Si $(a, b) \in R$, entonces b y a están en el mismo subconjunto de S en la partición, de modo que $(b, a) \in R$ también. Por tanto, R es simétrica.

Si $(a, b) \in R$ y $(b, c) \in R$, entonces a y b están en el mismo subconjunto X de S en la partición, y b y c están en el mismo subconjunto Y de S de la partición. Debido a que los subconjuntos de S en la partición son disjuntos y

b pertenece a X y Y, se sigue que $X = Y$. En consecuencia, a y c pertenecen al mismo subconjunto de S en la partición, por lo que $(a, c) \in R$. Por tanto, R es transitiva.

De ello se deduce que R es una relación de equivalencia. Las clases de equivalencia de R consisten en subconjuntos de S que contienen elementos relacionados y, según la definición de R, estos son los subconjuntos de S en la partición. El teorema 2.4.2 resume las conexiones que hemos establecido entre las relaciones de equivalencia y las particiones.

Teorema 2.4.2 Sea R una relación de equivalencia sobre un conjunto S. Entonces las clases de equivalencia de R forman una partición de S. A la inversa, dada una partición $\{A_i | i \in I\}$ del conjunto S, existe una relación de equivalencia R que tiene los conjuntos $A_i, i \in I$, como sus clases de equivalencia.

■

El Ejemplo 2.4.12 muestra cómo construir una relación de equivalencia a partir de una partición.

Ejemplo 2.4.12 Enumere los pares ordenados en la relación de equivalencia R producida por la partición $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$ y $A_3 = \{6\}$ de $S = \{1, 2, 3, 4, 5, 6\}$, dada en el Ejemplo 2.4.11.

Solución: Los subconjuntos de S en la partición son las clases de equivalencia de R. El par $(a, b) \in R$ si y sólo si a y b están en el mismo subconjunto de S en la partición. Los pares

$$(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)$$

pertenecen a R porque $A_1 = \{1, 2, 3\}$ es una clase de equivalencia; los pares

$$(4, 4), (4, 5), (5, 4), (5, 5)$$

pertenecen a R porque $A_2 = \{4, 5\}$ es una clase de equivalencia; y finalmente el par

$$(6, 6)$$

pertenece a R porque $\{6\}$ es una clase de equivalencia. Ningún par distinto a los enumerados pertenece a R. □

Las clases de congruencia módulo m proporcionan una ilustración útil del Teorema 2.4.2. Hay m clases de congruencia diferentes módulo m, correspondientes a los m posibles residuos diferentes cuando un número entero se divide por m. Estas m clases de congruencia se indican mediante $[0]_m, [1]_m, \ldots, [m-1]_m$ y forman una partición del conjunto de números enteros.

Ejemplo 2.4.13 ¿Cuáles son los conjuntos en la partición de los enteros que surgen de la congruencia módulo 4?

Solución: En el Ejemplo 2.4.9 encontramos las cuatro clases de congruencia, $[0]_4, [1]_4, [2]_4$ y $[3]_4$. Son los conjuntos

$$\begin{aligned}
[0]_4 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\}, \\
[1]_4 &= \{\ldots, -7, -3, 1, 5, 9, \ldots\}, \\
[2]_4 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\}, \\
[3]_4 &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}.
\end{aligned}$$

Estas clases de congruencia son disjuntas y cada entero está exactamente en una de ellas. En otras palabras, como dice el Teorema 2.4.2, estas clases de congruencia forman una partición. □

A continuación, proporcionamos un ejemplo de una partición del conjunto de todas las cadenas que surge de una relación de equivalencia en este conjunto.

Ejemplo 2.4.14 Sea R_3 la relación del Ejemplo 2.4.5. ¿Cuáles son los conjuntos en la partición del conjunto de todas las cadenas de bits que surgen de la relación R_3 en el conjunto de todas las cadenas de bits? (Recuerde que sR_3t, donde s y t son cadenas de bits, si $s = t$ o s y t son cadenas de bits con al menos tres bits que concuerdan en sus primeros tres bits).

Solución: Tenga en cuenta que cada cadena de bits de longitud inferior a tres es equivalente sólo a sí misma. Por tanto, $[\lambda]_{R_3} = \{\lambda\}$, $[0]_{R_3} = \{0\}$, $[1]_{R_3} = \{1\}$, $[00]_{R_3} = \{00\}$, $[01]_{R_3} = \{01\}$, $[10]_{R_3} = \{10\}$ y $[11]_{R_3} = \{11\}$. Tenga en cuenta que cada cadena de bits de longitud tres o más es equivalente a una de las ocho cadenas de bits 000, 001, 010, 011, 100, 101, 110 y 111.

Tenemos

$$
\begin{aligned}
[000]_{R_3} &= \{000, 0000, 0001, 00000, 00001, 00010, 00011, \ldots\},\\
[001]_{R_3} &= \{001, 0010, 0011, 00100, 00101, 00110, 00111, \ldots\},\\
[010]_{R_3} &= \{010, 0100, 0101, 01000, 01001, 01010, 01011, \ldots\},\\
[011]_{R_3} &= \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\},\\
[100]_{R_3} &= \{100, 1000, 1001, 10000, 10001, 10010, 10011, \ldots\},\\
[101]_{R_3} &= \{101, 1010, 1011, 10100, 10101, 10110, 10111, \ldots\},\\
[110]_{R_3} &= \{110, 1100, 1101, 11000, 11001, 11010, 11011, \ldots\},\\
[111]_{R_3} &= \{111, 1110, 1111, 11100, 11101, 11110, 11111, \ldots\}.
\end{aligned}
$$

Estas 15 clases de equivalencia son disjuntas y cada cadena de bits está exactamente en una de ellas. Como nos dice el Teorema 2.4.2, estas clases de equivalencia dividen el conjunto de todas las cadenas de bits. □

2.4.5. Ejercicios

1. ¿Cuáles de estas relaciones sobre $\{0, 1, 2, 3\}$ son relaciones de equivalencia? Determine la(s) propiedad(es) de una relación de equivalencia de la(s) que carece(n) la(s) que no lo es(son).

   a) $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$

   b) $\{(0, 0), (0, 2), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)\}$

   c) $\{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$

   d) $\{(0, 0), (1, 1), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

   e) $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)\}$

2. ¿Cuáles de estas relaciones sobre el conjunto de todas las personas son relaciones de equivalencia? Determine la(s) propiedad(es) de una relación de equivalencia de la(s) que carece(n) la(s) que no lo es(son).

   a) $\{(a, b) | a$ y b tienen la misma edad$\}$

   b) $\{(a, b) | a$ y b tienen los mismos progenitores$\}$

   c) $\{(a, b) | a$ y b tienen sólo un progenitor en común$\}$

   d) $\{(a, b) | a$ y b se conocen$\}$

e) $\{(a, b)|a$ y b hablan un idioma en común$\}$

3. ¿Cuáles son las clases de equivalencia de las relaciones de equivalencia en el ejercicio 1?

4. ¿Cuáles son las clases de equivalencia de las relaciones de equivalencia en el ejercicio 2?

5. ¿Cuál es la clase de congruencia $[n]_5$ (es decir, la clase de equivalencia de n con respecto a la congruencia módulo 5) cuando n es

   a) 2? *b*) 3? *c*) 6? *d*) -3?

6. ¿Cuál es la clase de congruencia $[4]_m$ cuando m es

   a) 2? *b*) 3? *c*) 6? *d*) 8?

7. ¿Cuáles de estas colecciones de subconjuntos son particiones del conjunto $\{1, 2, 3, 4, 5, 6\}$?

   a) $\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}$

   b) $\{1\}, \{2, 3, 6\}, \{4\}, \{5\}$

   c) $\{2, 4, 6\}, \{1, 3, 5\}$

   d) $\{1, 4, 5\}, \{2, 6\}$

8. ¿Cuáles de estas colecciones de subconjuntos son particiones del conjunto $\{-3, -2, -1, 0, 1, 2, 3\}$?

   a) $\{-3, -1, 1, 3\}, \{-2, 0, 2\}$

   b) $\{-3, -2, -1, 0\}, \{0, 1, 2, 3\}$

   c) $\{-3, 3\}, \{-2, 2\}, \{-1, 1\}, \{0\}$

   d) $\{-3, -2, 2, 3\}, \{-1, 1\}$

2.5. Ordenamientos Parciales

2.5.1. Introducción

A menudo usamos relaciones para ordenar algunos o todos los elementos de los conjuntos. Por ejemplo, ordenamos las palabras usando la relación que contiene pares de palabras (x, y), donde x está antes que y en el diccionario.

Programamos proyectos usando la relación que consta de pares (x, y), donde x y y son tareas en un proyecto de manera que x debe completarse antes de que comience y. Ordenamos el conjunto de números enteros usando la relación que contiene los pares (x, y), donde x es menor que y.

Cuando agregamos todos los pares de la forma (x, x) a estas relaciones, obtenemos una relación que es reflexiva, antisimétrica y transitiva. Estas son propiedades que caracterizan las relaciones utilizadas para ordenar los elementos de los conjuntos.

Definición 2.5.1 Una relación R sobre un conjunto S se denomina *ordenamiento parcial* u *orden parcial* si es reflexiva, antisimétrica y transitiva. Un conjunto S junto con un orden parcial R se denomina *conjunto parcialmente ordenado*, o *poset*, y se denota por (S, R). Los miembros de S se denominan elementos del poset.

Damos ejemplos de posets en los ejemplos 2.5.1-2.5.3.

Ejemplo 2.5.1 Demuestre que la relación mayor o igual que $(\geq)$ es un ordenamiento parcial en el conjunto de números enteros.

Solución: Debido a que $a \geq a$ para todo entero a, $\geq$ es reflexiva. Si $a \geq b$ y $b \geq a$, entonces $a = b$. Por tanto, $\geq$ es antisimétrica. Finalmente, $\geq$ es transitiva porque $a \geq b$ y $b \geq c$ implican que $a \geq c$. De ello se deduce que $\geq$ es un orden parcial sobre el conjunto de números enteros y $(\mathbb{Z}, \geq)$ es un poset.

□

Ejemplo 2.5.2 La relación de divisibilidad $|$ es un ordenamiento parcial sobre el conjunto de números enteros positivos, porque es reflexiva, antisimétrica y transitiva, como se mostró en la sección 2.1. Vemos que $(\mathbb{Z}^+, |)$ es un poset. Recuerde que ($\mathbb{Z}^+$ denota el conjunto de enteros positivos). □

Ejemplo 2.5.3 Demuestre que la relación de inclusión $\subseteq$ es un ordenamiento parcial sobre el conjunto de potencias de un conjunto S.

Solución: Como $A \subseteq A$ siempre que A es un subconjunto de S, $\subseteq$ es reflexiva. Es antisimétrica porque $A \subseteq B$ y $B \subseteq A$ implican que $A = B$. Finalmente, $\subseteq$ es transitiva, porque $A \subseteq B$ y $B \subseteq C$ implican que $A \subseteq C$. Por lo tanto, $\subseteq$ es un ordenamiento parcial sobre $\mathscr{P}(S)$ y $(\mathscr{P}(S), \subseteq)$ es un poset. □

El ejemplo 2.5.4 ilustra una relación que no es un ordenamiento parcial.

Ejemplo 2.5.4 Sea R la relación sobre el conjunto de personas tal que xRy si x y y son personas y x es mayor que y. Muestre que R no es un ordenamiento parcial.

Solución: Tenga en cuenta que R es antisimétrica porque si una persona x es mayor que una persona y, entonces y no es mayor que x. Es decir, si xRy, entonces $y \not R x$.

La relación R es transitiva porque si la persona x es mayor que la persona y y y es mayor que la persona z, entonces x es mayor que z. Es decir, si xRy y yRz, entonces xRz.

Sin embargo, R no es reflexiva, porque ninguna persona es mayor que él o ella. Es decir, $x \not R x$ para todas las personas x. De ello se deduce que R no es un ordenamiento parcial. □

En diferentes posets, se utilizan distintos símbolos como $\leq, \subseteq$ y $\mid$ para denotar un ordenamiento parcial. Sin embargo, necesitamos un símbolo que podamos usar cuando analicemos la relación de ordenamiento en un conjunto arbitrario.

Habitualmente, la notación $a \preccurlyeq b$ se usa para denotar que $(a, b) \in R$ en un poset arbitrario (S, R). Esta notación se usa porque la relación menor o igual a en el conjunto de números reales es el ejemplo más familiar de un orden parcial y el símbolo $\preccurlyeq$ es similar al símbolo $\leq$. (Tenga en cuenta que el símbolo $\preccurlyeq$ se usa para denotar la relación en cualquier poset, no solo la relación menor o igual a).

La notación $a \prec b$ denota que $a \preccurlyeq b$, pero $a \neq b$. Además, decimos "a es menor que b" o "b es mayor que a" si $a \prec b$. Cuando a y b son elementos del poset $(S, \preccurlyeq)$, no es necesario que $a \preccurlyeq b$ o $b \preccurlyeq a$.

Por ejemplo, en $(\mathscr{P}(\mathbb{Z}), \subseteq)$, $\{1, 2\}$ no está relacionado con $\{1, 3\}$, y viceversa, porque ningún conjunto está contenido dentro del otro. De manera

similar, en $(\mathbb{Z}^+, |)$, 2 no está relacionado con 3 y 3 no está relacionado con 2, porque $2 \not| 3$ y $3 \not| 2$. Esto conduce a la Definición 2.5.2.

Definición 2.5.2 Los elementos a y b de un poset $(S, \preccurlyeq)$ se denominan *comparables* si $a \preccurlyeq b$ o $b \preccurlyeq a$. Cuando a y b son elementos de S tales que ni $a \preccurlyeq b$ ni $b \preccurlyeq a$, a y b se denominan *incomparables*.

Ejemplo 2.5.5 En el poset $(\mathbb{Z}^+, |)$, ¿son comparables los números enteros 3 y 9? ¿Son comparables el 5 y el 7?

Solución: Los enteros 3 y 9 son comparables, porque $3|9$. Los enteros 5 y 7 son incomparables, porque $5 \not| 7$ y $7 \not| 5$. □

El adjetivo "parcial" se utiliza para describir ordenamientos parciales porque algunos pares de elementos pueden ser incomparables. Cuando cada dos elementos del conjunto son comparables, la relación se denomina **orden total**.

Definición 2.5.3 Si $(S, \preccurlyeq)$ es un poset y cada dos elementos de S son comparables, S se llama un *conjunto totalmente ordenado* o *linealmente ordenado*, y $\preccurlyeq$ se llama *orden total* u *orden lineal*. Un conjunto totalmente ordenado también se llama *cadena*.

Ejemplo 2.5.6 El poset $(\mathbb{Z}, \leq)$ está totalmente ordenado, porque $a \leq b$ o $b \leq a$ siempre que a y b son números enteros. □

Ejemplo 2.5.7 El poset $(\mathbb{Z}^+, |)$ no está totalmente ordenado porque contiene elementos incomparables, como 5 y 7. □

Definición 2.5.4 $(S, \preccurlyeq)$ es un *conjunto bien ordenado* si es un poset tal que $\preccurlyeq$ es un ordenamiento total y cada subconjunto no vacío de S tiene un elemento mínimo.

Ejemplo 2.5.8 El conjunto de pares ordenados de enteros positivos, $\mathbb{Z}^+ \times \mathbb{Z}^+$, con $(a_1, a_2) \preccurlyeq (b_1, b_2)$ si $a_1 < b_1$, o si $a_1 = b_1$ y $a_2 \leq b_2$ (el orden lexicografo), es un conjunto bien ordenado. La verificación de esto se deja como ejercicio para el lector. El conjunto $\mathbb{Z}$, con el orden $\leq$ habitual, no está

bien ordenado porque el conjunto de enteros negativos, que es un subconjunto de $\mathbb{Z}$, no tiene elemento mínimo. □

Teorema 2.5.1 EL PRINCIPIO DE INDUCCIÓN BIEN ORDENADA Suponga que S es un conjunto bien ordenado. Entonces $P(x)$ es cierto para todo $x \in S$, si
PASO INDUCTIVO: Para cada $y \in S$, si $P(x)$ es verdadero para todo $x \in S$ con $x \prec y$, entonces $P(y)$ es verdadero.

Demostración: Suponga que no es el caso de que $P(x)$ sea verdadero para todo $x \in S$. Entonces hay un elemento $y \in S$ tal que $P(y)$ es falso. En consecuencia, el conjunto $A = \{x \in S | P(x) \text{ es falso}\}$ no está vacío.

Como S está bien ordenado, A tiene un elemento mínimo a. Por la elección de a como elemento mínimo de A, sabemos que $P(x)$ es cierto para todo $x \in S$ con $x \prec a$. Esto implica que el paso inductivo $P(a)$ es cierto. Esta contradicción muestra que $P(x)$ debe ser verdadero para todo $x \in S$.

■

Observación 2.5.1 No necesitamos un paso base en una demostración que utilice el principio de inducción bien ordenada porque si x_0 es el elemento menor de un conjunto bien ordenado, el paso inductivo nos dice que $P(x_0)$ es verdadero. Esto se debe a que no hay elementos $x \in S$ con $x \prec x_0$, por lo que sabemos (usando una prueba vacía) que $P(x)$ es verdadero para todo $x \in S$ con $x \prec x_0$.

□

2.5.2. Orden Lexicografo

Las palabras en un diccionario se enumeran en orden alfabético o lexicografo, basándose en el orden de las letras en el alfabeto. Este es un caso especial de un ordenamiento de cadenas en un conjunto construido a partir de una ordenamiento parcial en el conjunto. Mostraremos cómo funciona esta construcción en cualquier poset.

Primero, mostraremos cómo construir un ordenamiento parcial sobre el producto cartesiano de dos posets, $(A_1, \preccurlyeq_1)$ y $(A_2, \preccurlyeq_2)$. El orden lexicografo $\preccurlyeq$ sobre $A_1 \times A_2$ se define especificando que un par es menor que un segundo par si la primera entrada del primer par es menor que (en A_1) la primera entrada del segundo par, o si las primeras entradas son iguales, pero la segunda

entrada de este par es menor que (en A_2) la segunda entrada del segundo par.

En otras palabras, (a_1, a_2) es menor que (b_1, b_2), es decir,

$$(a_1, a_2) \prec (b_1, b_2),$$

ya sea que $a_1 \prec_1 b_1$ o si ambos $a_1 = b_1$ y $a_2 \prec_2 b_2$. Obtenemos un ordenamiento parcial $\preccurlyeq$ agregando igualdad al ordenamiento $\prec$ sobre $A_1 \times A_2$. La verificación de esto se deja como ejercicio.

Ejemplo 2.5.9 Determine si $(3, 5) \prec (4, 8)$, si $(3, 8) \prec (4, 5)$ y si $(4, 9) \prec (4, 11)$ en el poset $(\mathbb{Z} \times \mathbb{Z}, \preccurlyeq)$, donde $\preccurlyeq$ es el orden lexicografo construido a partir de la relación $\leq$ habitual sobre $\mathbb{Z}$.

Solución: Como $3 < 4$, se sigue que $(3, 5) \prec (4, 8)$ y que $(3, 8) \prec (4, 5)$. Tenemos $(4, 9) \prec (4, 11)$, porque las primeras entradas de $(4, 9)$ y $(4, 11)$ son iguales pero $9 < 11$.

□

En la Figura 2.15 se resaltan los pares ordenados en $\mathbb{Z}^+ \times \mathbb{Z}^+$ que son menores que $(3, 4)$.

Un orden lexicografo se puede definir sobre el producto cartesiano de n posets $(A_1, \preccurlyeq_1)$, $(A_2, \preccurlyeq_2)$, ..., $(A_n, \preccurlyeq_n)$. Defina el orden parcial $\preccurlyeq$ sobre $A_1 \times A_2 \times \cdots \times A_n$ mediante

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n)$$

si $a_1 \prec_1 b_1$, o si hay un número entero $i > 0$ tal que $a_1 = b_1, \ldots, a_i = b_i$ y $a_{i+1} \prec_{i+1} b_{i+1}$. En otras palabras, una $n-$tupla es menor que una segunda $n-$tupla si la entrada de la primera $n-$tupla en la primera posición donde las dos $n-$tuplas no concuerdan es menor que la entrada en esa posición en la segunda $n-$tupla.

Ejemplo 2.5.10 Tenga en cuenta que $(1, 2, 3, 5) \prec (1, 2, 4, 3)$, porque las entradas en las dos primeras posiciones de estas 4-tuplas coinciden, pero en la tercera posición la entrada en la primera 4-tupla, 3, es menor que en la segunda 4-tupla, 4. (Aquí el orden en 4-tuplas es el orden lexicografo que proviene de la relación habitual menor o igual a en el conjunto de números enteros). □

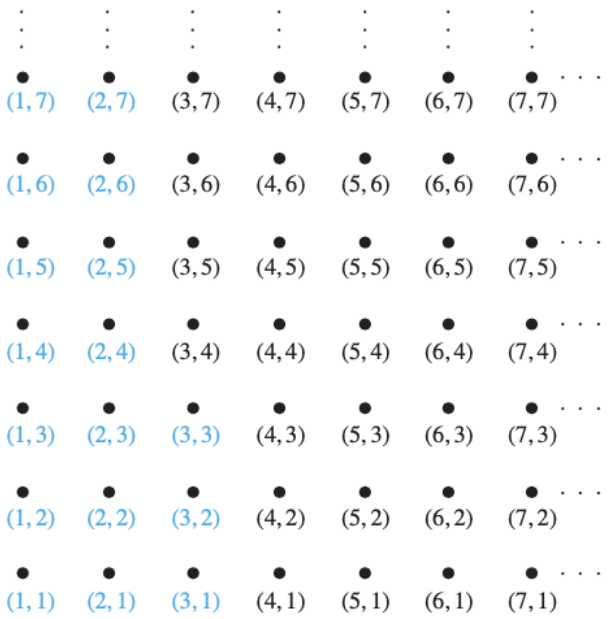


Figura 2.15: Los pares ordenados menores que $(3, 4)$ en orden lexicografo.

Ahora podemos definir el orden lexicografo de cadenas. Considere las cadenas $a_1a_2 \cdots a_m$ y $b_1b_2 \cdots b_n$ sobre un poset S. parcialmente ordenado. Suponga que estas cadenas no son iguales. Sea t el mínimo de m y n.

La definición de ordenamiento lexicografo es que la cadena $a_1a_2 \cdots a_m$ es menor que $b_1b_2 \cdots b_n$ si y sólo si

$$(a_1, a_2, \cdots, a_t) \prec (b_1, b_2, \cdots, b_t), \text{ o}$$
$$(a_1, a_2, \cdots, a_t) = (b_1, b_2, \cdots, b_t), \text{ y } m < n,$$

donde $\prec$ en esta desigualdad representa el orden lexicografo de S^t.

En otras palabras, para determinar el orden de dos cadenas diferentes, la cadena más larga se trunca a la longitud de la cadena más corta, es decir, $t = \text{mín}(m, n)$ términos. Luego, las $t-$tuplas compuestas por los primeros t términos de cada cadena se comparan usando el orden lexicografo en S^t. Una cadena es menor que otra cadena si la $t-$tupla correspondiente a la primera cadena es menor que la $t-$tupla de la segunda cadena, o si estas dos $t-$tuplas son iguales, pero la segunda cadena es más larga.

Ejemplo 2.5.11 Considere el conjunto de cadenas de letras minúsculas en inglés. Usando el orden de las letras en el alfabeto, se puede construir un orden lexicografo sobre el conjunto de cadenas.

Una cadena es menor que una segunda cadena si la letra en la primera cadena en la primera posición donde las cadenas difieren es anterior a la letra en la segunda cadena en esta posición, o si la primera cadena y la segunda cadena concuerdan en todas las posiciones, pero la segunda cadena tiene más letras. Este orden es el mismo que se utiliza en los diccionarios.

Por ejemplo,

$$discreet \prec discrete,$$

porque estas cadenas difieren primero en la séptima posición, y $e \prec t$. También,

$$discreet \prec discreetness,$$

porque las primeras ocho letras concuerdan, pero la segunda cadena es más larga. Además,

$$discrete \prec discretion,$$

porque

$$discrete \prec discreti.$$

□

2.5.3. Diagramas de Hasse

No es necesario mostrar muchas aristas en el grafo dirigido para un poset finito porque deben estar presentes. Por ejemplo, considere el grafo dirigido para el orden parcial $\{(a, b)|a \leq b\}$ en el conjunto $\{1, 2, 3, 4\}$, que se muestra en la Figura 2.16 (a).

Debido a que esta relación es un ordenamiento parcial, es reflexiva y su grafo dirigido tiene bucles en todos los vértices. En consecuencia, no tenemos que mostrar estos bucles porque deben estar presentes; en la Figura 2.16 (b) no se muestran los bucles.

Ya que un ordenamiento parcial es transitivo, no tenemos que mostrar esas aristas que deben estar presentes debido a la transitividad. Por ejemplo, en la Figura 2.16 (c) las aristas (1, 3), (1, 4) y (2, 4) no se muestran porque deben estar presentes.

Si asumimos que todos las aristas apuntan "hacia arriba"(como están dibujados en la figura), no tenemos que mostrar las direcciones de las aristas; la figura 2.16 (c) no muestra direcciones.

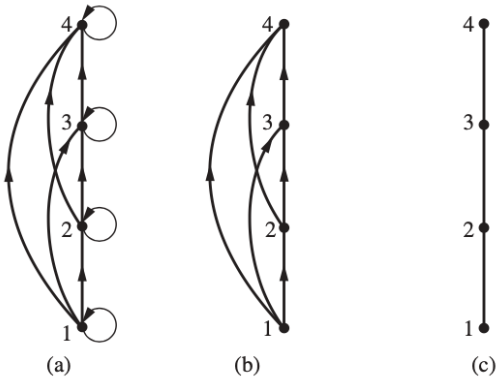


Figura 2.16: Construcción del diagrama de Hasse para $(\{1, 2, 3, 4\}, \leq)$.

En general, podemos representar un poset finito $(S, \preccurlyeq)$ usando este procedimiento: Comience con el grafo dirigido para esta relación. Debido a que un ordenamiento parcial es reflexivo, un bucle (a, a) está presente en cada vértice a. Elimine estos bucles.

A continuación, elimine todas las aristas que deban estar en el orden parcial debido a la presencia de otras aristas y transitividad. Es decir, elimine todas las aristas (x, y) para las que hay un elemento $z \in S$ tal que $x \prec z$ y $z \prec y$.

Finalmente, ordene cada arista de modo que su vértice inicial esté debajo de su vértice terminal. Elimine todas las flechas en las aristas dirigidas, porque todos las aristas apuntan "hacia arriba" hacia su vértice terminal.

Estos pasos están bien definidos y sólo es necesario realizar un número finito de pasos para un poset finito. Cuando se han dado todos los pasos, el diagrama resultante contiene información suficiente para encontrar el orden parcial, como explicaremos más adelante.

El diagrama resultante se llama **diagrama de Hasse** de $(S, \preccurlyeq)$, y recibe su nombre del matemático alemán del siglo XX Helmut Hasse, que hizo un uso extensivo de ellos.

Sea $(S, \preccurlyeq)$ un poset. Decimos que un elemento $y \in S$ **cubre** un elemento $x \in S$ si $x \prec y$ y no hay ningún elemento $z \in S$ tal que $x \prec z \prec y$. El conjunto de pares (x, y) tal que y cubre x se llama la **relación de cobertura** de $(S, \preccurlyeq)$.

De la descripción del diagrama de Hasse de un poset, vemos que las aristas en el diagrama de Hasse de $(S, \preccurlyeq)$ son aristas apuntando hacia arriba que corresponden a los pares en la relación de cobertura de $(S, \preccurlyeq)$.

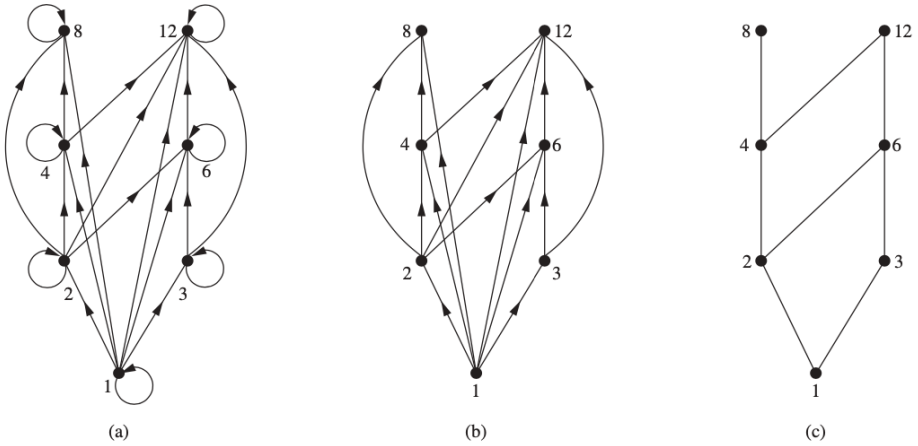


Figura 2.17: Construcción del diagrama de Hasse para $(\{1, 2, 3, 4, 6, 8, 12\}, |)$.

Además, podemos recuperar un poset de su relación de cobertura, porque es la cerradura transitiva y reflexiva de su relación de cobertura. Esto nos dice que podemos construir un ordenamiento parcial a partir de su diagrama de Hasse.

Ejemplo 2.5.12 Dibuje el diagrama de Hasse que representa el orden parcial $\{(a, b)|a \text{ divide } b\}$ sobre $\{1, 2, 3, 4, 6, 8, 12\}$.

Solución: Comience con el digrafo para este orden parcial, como se muestra en la Figura 2.17 (a). Retire todos los bucles, como se muestra en la Figura 2.17 (b). Luego elimine todas las aristas implicadas por la propiedad transitiva. Estas son $(1, 4)$, $(1, 6)$, $(1, 8)$, $(1, 12)$, $(2, 8)$, $(2, 12)$ y $(3, 12)$. Organice todas las aristas para que apunten hacia arriba y elimine todas las flechas para obtener el diagrama de Hasse. El diagrama de Hasse resultante se muestra en la Figura 2.17 (c).

□

Ejemplo 2.5.13 Dibuje el diagrama de Hasse para el orden parcial $\{(A, B)|A \subseteq B\}$ sobre el conjunto potencia $\mathscr{P}(S)$, donde $S = \{a, b, c\}$.

Solución: El diagrama de Hasse para este ordenamiento parcial se obtiene a partir del digrafo asociado eliminando todos los bucles y todos las aristas que se producen por la transitividad, a saber, $(\emptyset, \{a, b\})$, $(\emptyset, \{a, c\})$, $(\emptyset, \{b, c\})$, $(\emptyset, \{a, b, c\})$, $(\{a\}, \{a, b, c\})$, $(\{b\}, \{a, b, c\})$ y $(\{c\}, \{a, b, c\})$. Finalmente, todas las aristas apuntan hacia arriba y las flechas se eliminan. El

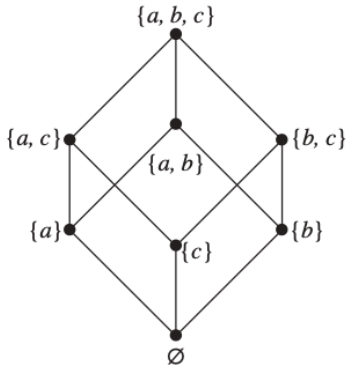


Figura 2.18: El diagrama de Hasse para $(\mathscr{P}(\{a, b, c\}), \subseteq)$.

diagrama de Hasse resultante se ilustra en la Figura 2.18.

□

2.5.4. Elementos Maximales y Minimales

Los elementos de los posets que tienen ciertas propiedades extremas son importantes para muchas aplicaciones. Un elemento de un poset se llama maximal si no es menor que cualquier elemento del poset. Es decir, a es **maximal** en el poset $(S, \preccurlyeq)$ si no hay $b \in S$ tal que $a \prec b$.

De manera similar, un elemento de un poset se llama minimal si no es mayor que cualquier elemento del poset. Es decir, a es **minimal** si no hay ningún elemento $b \in S$ tal que $b \prec a$. Los elementos maximales y minimales son fáciles de detectar mediante un diagrama de Hasse, son los elementos "superiores" e "inferiores" del diagrama.

Ejemplo 2.5.14 ¿Qué elementos del poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ son maximales y cuáles son minimales?

Solución: El diagrama de Hasse en la Figura 2.19 para este poset muestra que los elementos maximales son 12, 20 y 25, los elementos minimales son 2 y 5. Como muestra este ejemplo, un poset puede tener más de un elemento maximal y más de un elemento minimal. □

A veces hay un elemento en un poset que es mayor que cualquier otro elemento. Tal elemento se llama el elemento más grande (mayor). Es decir,

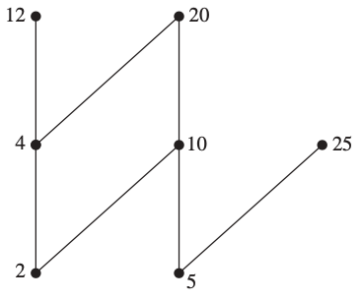


Figura 2.19: El diagrama de Hasse para $(\{2, 4, 5, 10, 12, 20, 25\}, |)$.

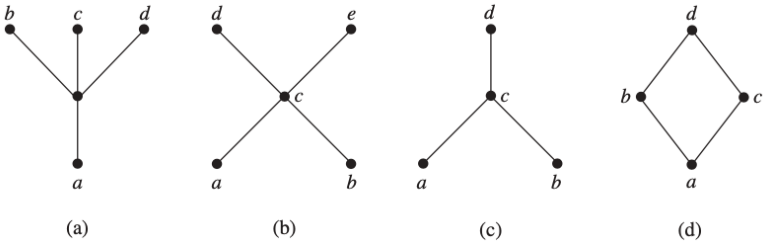


Figura 2.20: Diagramas de Hasse para el Ejemplo 2.5.15.

a es el **elemento más grande** (**mayor**) del poset $(S, \preccurlyeq)$ si $b \preccurlyeq a$ para todo $b \in S$. El elemento más grande es único cuando existe.

Del mismo modo, un elemento se denomina elemento más pequeño (menor) si es menor que todos los demás elementos del poset. Es decir, a es el **elemento más pequeño** (**menor**) de $(S, \preccurlyeq)$ si $a \preccurlyeq b$ para todo $b \in S$. El elemento más pequeño es único cuando existe.

Ejemplo 2.5.15 Determine si los posets representados por cada uno de los diagramas de Hasse en la Figura 2.20 tienen un elemento mayor y un elemento menor.

Solución: El elemento menor del poset con diagrama de Hasse (a) es a, este poset no tiene elemento mayor. El poset con diagrama de Hasse (b) no tiene ni un elemento menor ni uno mayor. El poset con diagrama de Hasse (c) no tiene ningún elemento menor, su elemento mayor es d. El poset con diagrama de Hasse (d) tiene el elemento menor a y el elemento mayor d.

□

Ejemplo 2.5.16 Sea S un conjunto. Determine si hay un elemento mayor

y un elemento menor en el poset $(\mathscr{P}(S), \subseteq)$.

Solución: El elemento menor es el conjunto vacío, porque $\emptyset \subseteq T$ para cualquier subconjunto T de S. El conjunto S es el elemento más grande en este conjunto, porque $T \subseteq S$ siempre que T es un subconjunto de S.

□

Ejemplo 2.5.17 ¿Hay un elemento mayor y un elemento menor en el poset $(\mathbb{Z}^+, |)$?

Solución: El número entero 1 es el elemento menor porque $1|n$ siempre que n es un número entero positivo. Debido a que no hay un número entero que sea divisible por todos los números enteros positivos, no hay ningún elemento mayor. □

A veces es posible encontrar un elemento que sea mayor o igual que todos los elementos de un subconjunto A de un poset $(S, \preccurlyeq)$. Si u es un elemento de S tal que $a \preccurlyeq u$ para todos los elementos $a \in A$, entonces u se llama una **cota superior** de A.

Asimismo, puede haber un elemento menor o igual que todos los elementos en A. Si l es un elemento de S tal que $l \preccurlyeq a$ para todos los elementos $a \in A$, entonces l se llama una **cota inferior** de A.

Ejemplo 2.5.18 Encuentre las cotas inferior y superior de los subconjuntos $\{a, b, c\}$, $\{j, h\}$ y $\{a, c, d, f\}$ en el poset con el diagrama de Hasse que se muestra en la Figura 2.21.

Solución: Las cotas superiores de $\{a, b, c\}$ son e, f, j y h, y su única cota inferior es a. No existen cotas superiores de $\{j, h\}$ y sus cotas inferiores son a, b, c, d, e y f. Las cotas superiores de $\{a, c, d, f\}$ son f, h y j y su cota inferior es a.

□

El elemento x se llama la **cota superior mínima** del subconjunto A si x es una cota superior que es menor que cualquier otra cota superior de A. Debido a que solo hay uno de estos elementos, si existe, tiene sentido llamar a este elemento la cota superior mínima. Es decir, x es la cota superior mínima de A si $a \preccurlyeq x$ siempre que $a \in A$, y $x \preccurlyeq z$ siempre que z es una cota superior de A.

De manera similar, el elemento y se llama la **cota inferior máxima** de A si y es una cota inferior de A y $z \preccurlyeq y$ siempre que z es una cota inferior de A. La cota inferior máxima de A es única si existe. La cota inferior máxima

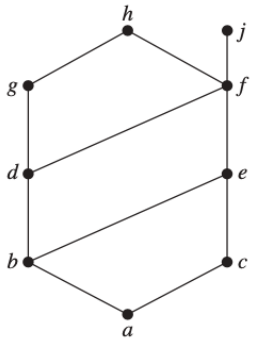


Figura 2.21: Diagrama de Hasse para el Ejemplo 2.5.18.

y la cota superior mínima de un subconjunto A se indican mediante glb(A) y lub(A), respectivamente.

Ejemplo 2.5.19 Encuentre la cota inferior máxima y la cota superior mínima de $\{b, d, g\}$, si existen, en el poset que se muestra en la Figura 2.21.

Solución: Las cotas superiores de $\{b, d, g\}$ son g y h. Como $g \prec h$, g es la cota superior mínima. Las cotas inferiores de $\{b, d, g\}$ son a y b. Debido a que $a \prec b$, b es la cota inferior máxima. □

Ejemplo 2.5.20 Encuentre la cota inferior máxima y la cota superior mínima de los conjuntos $\{3, 9, 12\}$ y $\{1, 2, 4, 5, 10\}$, si existen, en el poset $(\mathbb{Z}^+, |)$.

Solución: Un número entero es una cota inferior de $\{3, 9, 12\}$ si 3, 9 y 12 son divisibles por este número entero. Los únicos números enteros son 1 y 3. Como $1|3$, 3 es cota inferior máxima de $\{3, 9, 12\}$. La única cota inferior para el conjunto $\{1, 2, 4, 5, 10\}$ con respecto a $|$ es el elemento 1. Por lo tanto, 1 es la cota inferior máxima para $\{1, 2, 4, 5, 10\}$.

Un número entero es una cota superior para $\{3, 9, 12\}$ si y sólo si es divisible entre 3, 9 y 12. Los números enteros con esta propiedad son los divisibles por el mínimo común múltiplo de 3, 9 y 12, que es 36. Por tanto, 36 es la cota superior mínima de $\{3, 9, 12\}$.

Un entero positivo es una cota superior para el conjunto $\{1, 2, 4, 5, 10\}$ si y sólo si es divisible por 1, 2, 4, 5 y 10. Los enteros con esta propiedad son aquellos enteros divisibles por el mínimo común múltiplo de estos enteros, que es 20. Por tanto, 20 es la cota superior mínima de $\{1, 2, 4, 5, 10\}$. □

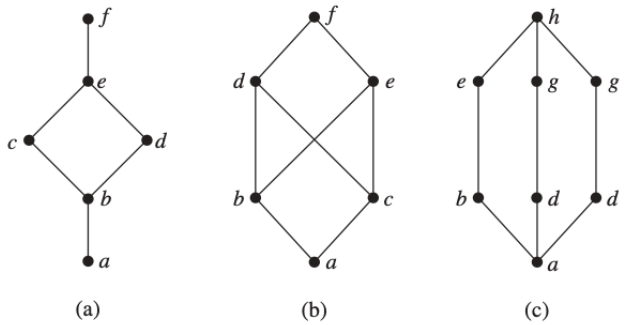


Figura 2.22: Diagrama de Hasse para el Ejemplo 2.5.21.

2.5.5. Retículos

Un conjunto parcialmente ordenado en el que cada par de elementos tiene tanto una cota superior mínima como una cota inferior máxima se llama **retículo**. Los retículos tienen muchas propiedades especiales. Además, los retículos se utilizan en muchas aplicaciones diferentes, como modelos de flujo de información, y desempeñan un papel importante en el álgebra booleana.

Ejemplo 2.5.21 Determine si los posets representados por cada uno de los diagramas de Hasse en la Figura 2.22 son retículos.

Solución: Los posets representados por los diagramas de Hasse en (a) y (c) son retículos porque en cada poset cada par de elementos tiene una cota superior mínima y una cota inferior máxima, como el lector debe verificar.

Por otro lado, el poset con el diagrama de Hasse que se muestra en (b) no es un retículo, porque los elementos b y c no tienen cota superior mínima. Para ver esto, tenga en cuenta que cada uno de los elementos d, e y f es una cota superior, pero ninguno de estos tres elementos precede a los otros dos con respecto al orden de este poset. □

Ejemplo 2.5.22 ¿Es el poset $(\mathbb{Z}^+, |)$ un retículo?

Solución: Sean a y b dos números enteros positivos. La cota superior mínima y la cota inferior máxima de estos dos números enteros son el mínimo común múltiplo y el máximo común divisor de estos números enteros, respectivamente, como el lector debe verificar. De ello se deduce que este poset es un retículo. □

Ejemplo 2.5.23 Determina si los posets $(\{1,2,3,4,5\},|)$ y $(\{1,2,4,8,16\},|)$ son retículos.

Solución: Debido a que 2 y 3 no tienen cotas superiores en $(\{1,2,3,4,5\},|)$, ciertamente no tienen una cota superior mínima. Por tanto, el primer poset no es un retículo.

Cada dos elementos del segundo conjunto tienen una cota superior mínima y una cota inferior máxima. La cota superior mínima de dos elementos en este conjunto es el más grande de los elementos y la cota inferior máxima de dos elementos es el más pequeño de los elementos, como el lector debe verificar. Por tanto, este segundo poset es un retículo. □

Ejemplo 2.5.24 Determina si $(\mathscr{P}(S),\subseteq)$ es un retículo donde S es un conjunto.

Solución: Sean A y B dos subconjuntos de S. La cota superior mínima y la cota inferior máxima de A y B son $A\cup B$ y $A\cap B$, respectivamente, como puede mostrar el lector. Por tanto, $(\mathscr{P}(S),\subseteq)$ es un retículo. □

Ejemplo 2.5.25 El modelo de retículo del flujo de información En muchos entornos, el flujo de información de una persona o programa de computadora a otro está restringido mediante autorizaciones de seguridad. Podemos utilizar un modelo de retículo para representar diferentes políticas de flujo de información.

Por ejemplo, una política de flujo de información común es la política de seguridad multinivel utilizada en los sistemas gubernamentales y militares. Cada información se asigna a una clase de seguridad y cada clase de seguridad está representada por un par (A,C) donde A es un nivel de autoridad y C es una categoría. Las personas y los programas de computadora pueden acceder a la información de un conjunto restringido específico de clases de seguridad.

Los niveles de autoridad típicos utilizados en el gobierno de los Estados Unidos son sin clasificar (0), confidencial (1), secreto (2) y ultrasecreto (3). Se dice que la información está clasificada si es confidencial, secreta o ultrasecreta.

Las categorías utilizadas en las clases de seguridad son los subconjuntos de un conjunto de todos los compartimentos relevantes para un área de interés particular. Cada compartimento representa un área temática particular. Por ejemplo, si el conjunto de compartimentos es $\{espías, topos, agentes\ dobles\}$, entonces hay ocho categorías diferentes, una para cada uno de los ocho subconjuntos del conjunto de compartimentos, como $\{espías, topos\}$.

Podemos ordenar las clases de seguridad especificando que $(A_1, C_1) \preccurlyeq (A_2, C_2)$ si y solo si $A_1 \leq A_2$ y $C_1 \subseteq C_2$. Se permite que la información fluya de la clase de seguridad (A_1, C_1) a la clase de seguridad (A_2, C_2) si y sólo si $(A_1, C_1) \preccurlyeq (A_2, C_2)$.

Por ejemplo, se permite que la información fluya de la clase de seguridad

$$(secreto, \{espías, topos\})$$

a la clase de seguridad

$$(ultrasecreto, \{espías, topos, agentes\ dobles\}),$$

mientras que la información no puede fluir de la clase de seguridad

$$(ultrasecreto, \{espías, topos\})$$

en cualquiera de las clases de seguridad

$$(secreto, \{espías, topos, agentes\ dobles\})$$

o

$$(ultrasecreto, \{espías\}).$$

Dejamos que el lector muestre que el conjunto de todas las clases de seguridad con el orden definido en este ejemplo forma un retículo.

□

2.5.6. Ejercicios

1. ¿Cuáles de estas relaciones sobre $\{0, 1, 2, 3\}$ son órdenes parciales? Determine las propiedades, de un orden parcial, de las que carecen las que no lo son.

   a) $(0, 0), (1, 1), (2, 2), (3, 3)$.

   b) $(0, 0), (1, 1), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)$.

   c) $(0, 0), (1, 1), (1, 2), (2, 2), (3, 3)$.

   d) $(0, 0), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)$.

   e) $(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)$.

2. ¿Cuáles de estos son posets?

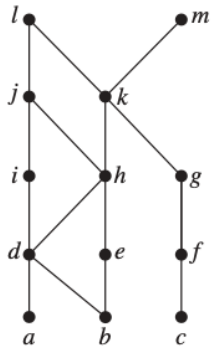


Figura 2.23: Diagrama de Hasse para el Ejercicio 5.

a) $(\mathbb{Z}, =)$. *b*) $(\mathbb{Z}, \neq)$. *c*) $(\mathbb{Z}, \geq)$. *d*) $(\mathbb{Z}, \nmid)$.

3. Encuentre el orden lexicografo de estas cadenas de letras minúsculas en inglés:

   a) *quack, quick, quicksilver, quicksand, quacking.*

   b) *open, opener, opera, operand, opened.*

   c) *zoo, zero, zoom, zoology, zoological.*

4. Dibuje un diagrama de Hasse para la divisibilidad sobre cada uno de los siguientes conjuntos:

   a) $\{1, 2, 3, 4, 5, 6\}$ *c*) $\{2, 3, 5, 10, 11, 15, 25\}$

   b) $\{3, 5, 7, 11, 13, 16, 17\}$ *d*) $\{1, 3, 9, 27, 81, 243\}$

5. Dado el diagrama de Hasse de la Figura 2.23, realice lo siguiente:

   a) Encuentre los elementos maximales.

   b) Encuentre los elementos minimales.

   c) ¿Existe un elemento mayor?

   d) ¿Existe un elemento menor?

   e) Encuentre todas las cotas superiores de $\{a, b, c\}$.

   f) Encuentre la mínima cota superior de $\{a, b, c\}$, si existe.

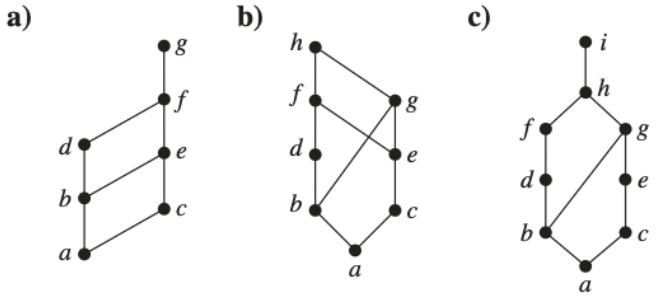


Figura 2.24: Diagrama de Hasse para el Ejercicio 8.

g) Encuentre todas las cotas inferiores de $\{f, g, h\}$.

h) Encuentre la máxima cota inferior de $\{f, g, h\}$, si existe.

6. Sea (S, R) un poset. Muestre que (S, R^{-1}) también es un poset, donde R^{-1} es la inversa de R. El poset (S, R^{-1}) se llama **dual** de (S, R).

7. Sea $(S, \preccurlyeq)$ un poset, demuestre que si existe el(la):

   a) elemento mayor, entonces es único.

   b) elemento menor, entonces es único.

   c) mínima cota superior, entonces es única.

   d) máxima cota inferior, entonces es única.

8. Determine si son retículos los posets cuyos diagramas de Hasse están dados en la Figura 2.24.

2.6. Funciones

2.6.1. Introducción

En muchos casos asignamos a cada elemento de un conjunto un elemento particular de un segundo conjunto (que puede ser el mismo que el primero).

Por ejemplo, suponga que a cada estudiante de una clase de matemáticas discretas se le asigna una calificación con letras del conjunto {A, B, C, D, F}. Y supongamos que las calificaciones son A para Adams, C para Chou, B para Goodfriend, A para Rodríguez y F para Stevens. Esta asignación de calificaciones se ilustra en la Figura 2.25.

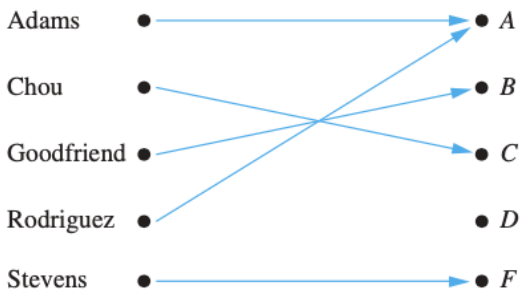


Figura 2.25: Asignación de calificaciones en un curso de matemáticas discretas.

Esta asignación es un ejemplo de función. El concepto de función es extremadamente importante en matemáticas y ciencias de la computación. Por ejemplo, en matemáticas discretas, las funciones se utilizan en la definición de estructuras discretas como secuencias y cadenas.

Las funciones también se utilizan para representar el tiempo que tarda una computadora en resolver problemas de un tamaño determinado. Muchos programas y subrutinas de computadora están diseñados para calcular valores de funciones.

Las funciones recursivas, que son funciones definidas en términos de sí mismas, se utilizan ampliamente en ciencias de la computación.

Esta sección revisa los conceptos básicos que involucran funciones necesarias en matemáticas discretas.

Definición 2.6.1 Sean A y B conjuntos no vacíos. Una función f de A a B es una asignación de exactamente un elemento de B a cada elemento de A. Escribimos $f(a) = b$ si b es el único elemento de B asignado por la función f al elemento a de A. Si f es una función de A a B, escribimos $f : A \to B$.

Observación 2.6.1 En ocasiones, las funciones también se denominan asignaciones, mapeos o transformaciones.

□

Las funciones se especifican de muchas formas diferentes. A veces declaramos explícitamente las asignaciones, como en la Figura 2.25. A menudo damos una fórmula, como $f(x) = x+1$, para definir una función. Otras veces usamos un programa de computadora para especificar una función.

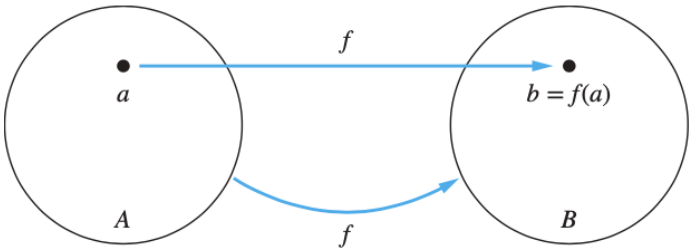


Figura 2.26: La función f mapea A en B.

Una función $f : A \to B$ también se puede definir en términos de una relación de A a B. Recuerde de la sección 2.1 que una relación de A a B es sólo un subconjunto de $A \times B$. Una relación de A a B que contiene uno y sólo un par ordenado (a, b) para cada elemento $a \in A$ define una función f de A a B. Esta función está definida por la asignación $f(a) = b$, donde (a, b) es el par ordenado único en la relación que tiene a a como primer elemento.

Definición 2.6.2 Si f es una función de A a B, decimos que A es el *dominio* de f y B es el *codominio* de f. Si $f(a) = b$, decimos que b es la *imagen* de a y a es una *preimagen* de b. El *rango*, o *imagen*, de f es el conjunto de todas las imágenes de elementos de A. Además, si f es una función de A a B, decimos que f *mapea* A en B.

La figura 2.26 representa una función de A a B.

Observación 2.6.2 Tenga en cuenta que el codominio de una función de A a B es el conjunto de todos los valores posibles de dicha función (es decir, todos los elementos de B), y el rango es el conjunto de todos los valores de $f(a)$ para $a \in A$, y siempre es un subconjunto del codominio. Es decir, el codominio es el conjunto de posibles valores de la función y el rango es el conjunto de todos los elementos del codominio que son el valor de f para al menos un elemento del dominio.

□

Cuando definimos una función especificamos su dominio, su codominio y el mapeo de elementos del dominio a elementos en el codominio. Dos funciones son iguales cuando tienen el mismo dominio, tienen el mismo codominio y asignan cada elemento de su dominio común al mismo elemento en su codominio común.

Tenga en cuenta que si cambiamos el dominio o el codominio de una función, obtenemos una función diferente. Si cambiamos el mapeo de elementos, también obtenemos una función diferente.

Los ejemplos 2.6.1 a 2.6.5 proporcionan ejemplos de funciones. En cada caso, describimos el dominio, el codominio, el rango y la asignación de valores a los elementos del dominio.

Ejemplo 2.6.1 ¿Cuáles son el dominio, codominio y rango de la función que asigna calificaciones a los estudiantes descrita en el primer párrafo de la introducción de esta sección?

Solución: Sea G la función que asigna una calificación a un estudiante en nuestra clase de matemáticas discretas. Tenga en cuenta que $G(Adams) = A$, por ejemplo. El dominio de G es el conjunto

$$\{Adams, Chou, Goodfriend, Rodríguez, Stevens\}$$

y el codominio es el conjunto $\{A, B, C, D, F\}$. El rango de G es el conjunto $\{A, B, C, F\}$, porque cada calificación excepto D se asignó a algún estudiante. □

Ejemplo 2.6.2 Sea R la relación que tiene los siguientes pares ordenados

$$(Abdul, 22), (Brenda, 24), (Carla, 21), (Desire, 22), (Eddie, 24), (Felicia, 22).$$

Cada par consta de un estudiante de posgrado y la edad de este estudiante. Especifique una función determinada por esta relación.

Solución: Si f es una función especificada por R, entonces $f(Abdul) = 22$, $f(Brenda) = 24$, $f(Carla) = 21$, $f(Desire) = 22$, $f(Eddie) = 24$ y $f(Felicia) = 22$. [Aquí, $f(x)$ es la edad de x, donde x es un estudiante.] Para el dominio, tomamos el conjunto

$$\{Abdul, Brenda, Carla, Desire, Eddie, Felicia\}.$$

También necesitamos especificar un codominio, que debe contener todas las edades posibles de los estudiantes. Debido a que es muy probable que todos los estudiantes tengan menos de 100 años, podemos tomar el conjunto de números enteros positivos menores de 100 como codominio.

(Tenga en cuenta que podríamos elegir un codominio diferente, como el conjunto de todos los enteros positivos o el conjunto de enteros positivos entre

10 y 90, pero eso cambiaría la función. El uso de este codominio también nos permitirá extender la función agregando después nombres y edades de más estudiantes.)

El rango de la función que hemos especificado es el conjunto de diferentes edades de estos estudiantes, que es el conjunto $\{21, 22, 24\}$. □

Ejemplo 2.6.3 Sea f la función que asigna los dos últimos bits de una cadena de bits de longitud 2 o mayor a esa cadena. Por ejemplo, $f(11010) = 10$. Entonces, el dominio de f es el conjunto de todas las cadenas de bits de longitud 2 o mayor, y tanto el codominio como el rango son el conjunto $\{00, 01, 10, 11\}$. □

Ejemplo 2.6.4 Sea $f : \mathbb{Z} \to \mathbb{Z}$ que asigna el cuadrado de un número entero a este número entero. Entonces, $f(x) = x^2$, donde el dominio de f es el conjunto de todos los enteros, el codominio de f es el conjunto de todos los enteros y el rango de f es el conjunto de todos los enteros que son cuadrados perfectos, es decir, $\{0, 1, 4, 9, \ldots\}$. □

Ejemplo 2.6.5 El dominio y codominio de funciones se especifican a menudo en lenguajes de programación. Por ejemplo, la declaración de Java

int **floor**(float real) {...}

y la declaración de función de C++

int **floor**(float x) {...}

ambos nos dicen que el dominio de la función floor es el conjunto de números reales (representados por números de punto flotante) y su codominio es el conjunto de números enteros. □

Una función se llama de **valor real** si su codominio es el conjunto de números reales, y se llama de **valor entero** si su codominio es el conjunto de números enteros. Se pueden sumar y multiplicar dos funciones de valor real o dos funciones de valor entero con el mismo dominio.

Definición 2.6.3 Sean f_1 y f_2 funciones de A a $\mathbb{R}$. Entonces $f_1 + f_2$ y $f_1 f_2$ también son funciones de A a $\mathbb{R}$ definidas para todo $x \in A$ por

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

Tenga en cuenta que las funciones $f_1 + f_2$ y $f_1 f_2$ se han definido especificando sus valores en x en términos de los valores de f_1 y f_2 en x.

Ejemplo 2.6.6 Sean f_1 y f_2 funciones de $\mathbb{R}$ a $\mathbb{R}$ tales que $f_1(x) = x^2$ y $f_2(x) = x - x^2$. ¿Cuáles son las funciones $f_1 + f_2$ y $f_1 f_2$?

Solución: De la definición de la suma y el producto de funciones, se deduce que

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

y

$$(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4.$$

□

Cuando f es una función de A a B, también se puede definir la imagen de un subconjunto de A.

Definición 2.6.4 Sea f una función de A a B y sea S un subconjunto de A. La imagen de S bajo la función f es el subconjunto de B que consta de las imágenes de los elementos de S. Denotamos la imagen de S por $f(S)$, entonces

$$f(S) = \{t | \exists s \in S(t = f(s))\}.$$

También usamos la abreviatura $\{f(s) | s \in S\}$ para denotar este conjunto.

Observación 2.6.3 La notación $f(S)$ para la imagen del conjunto S bajo la función f es potencialmente ambigua. Aquí, $f(S)$ denota un conjunto, y no el valor de la función f para el conjunto S.

□

Ejemplo 2.6.7 Sean $A = \{a, b, c, d, e\}$ y $B = \{1, 2, 3, 4\}$ con $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$ y $f(e) = 1$. La imagen del subconjunto $S = \{b, c, d\}$ es el conjunto $f(S) = \{1, 4\}$. □

2.6.2. Funciones Uno a Uno y Sobre

Algunas funciones nunca asignan el mismo valor a dos elementos diferentes del dominio. Se dice que estas funciones son uno a uno.

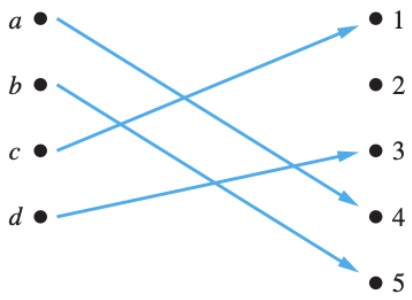


Figura 2.27: Una función uno a uno.

Definición 2.6.5 Se dice que una función f es *uno a uno*, o una *inyección*, si y sólo si $f(a) = f(b)$ implica que $a = b$ para todo a y b en el dominio de f. Se dice que una función es *inyectiva* si es uno a uno.

Tenga en cuenta que una función f es uno a uno si y sólo si $f(a) \neq f(b)$ siempre que $a \neq b$. Esta forma de expresar que f es uno a uno se obtiene tomando la contrapositiva de la implicación en la Definición 2.6.5.

Observación 2.6.4 Podemos expresar que f es uno a uno usando cuantificadores como $\forall a \forall b(f(a) = f(b) \rightarrow a = b)$ o equivalentemente $\forall a \forall b(a \neq b \rightarrow f(a) \neq f(b))$, donde el universo de discurso es el dominio de la función. □

Ilustramos este concepto dando ejemplos de funciones que son uno a uno y otras funciones que no son uno a uno.

Ejemplo 2.6.8 Determine si la función f de $\{a, b, c, d\}$ a $\{1, 2, 3, 4, 5\}$ con $f(a) = 4$, $f(b) = 5$, $f(c) = 1$ y $f(d) = 3$ es uno a uno.

Solución: La función f es uno a uno porque f toma diferentes valores en los cuatro elementos de su dominio. Esto se ilustra en la Figura 2.27. □

Ejemplo 2.6.9 Determine si la función $f(x) = x^2$ del conjunto de números enteros al conjunto de números enteros es uno a uno.

Solución: La función $f(x) = x^2$ no es uno a uno porque, por ejemplo, $f(1) = f(-1) = 1$, pero $1 \neq -1$. □

Observación 2.6.5 La función $f(x) = x^2$ con dominio $\mathbb{Z}^+$ es uno a uno. (Vea la explicación en el Ejemplo 2.6.12 para ver por qué). Esta es una función diferente de la función en el Ejemplo 2.6.9 debido a la diferencia en sus dominios.

□

Ejemplo 2.6.10 Determina si la función $f(x) = x+1$ del conjunto de números reales a sí mismo es uno a uno.

Solución: Suponga que x y y son números reales con $f(x) = f(y)$, de modo que $x + 1 = y + 1$. Esto significa que $x = y$. Por tanto, $f(x) = x + 1$ es una función uno a uno de $\mathbb{R}$ a $\mathbb{R}$. □

Ejemplo 2.6.11 Suponga que a cada trabajador de un grupo de empleados se le asigna un trabajo de un conjunto de trabajos posibles, cada uno de los cuales debe realizarlo un solo trabajador. En esta situación, la función f que asigna un trabajo a cada trabajador es uno a uno. Para ver esto, observe que si x y y son dos trabajadores diferentes, entonces $f(x) \neq f(y)$ porque los dos trabajadores x y y deben tener diferentes trabajos. □

A continuación, damos algunas condiciones que garantizan que una función sea uno a uno.

Definición 2.6.6 Una función f cuyo dominio y codominio son subconjuntos del conjunto de números reales se llama creciente si $f(x) \leq f(y)$, y estrictamente creciente si $f(x) < f(y)$, siempre que $x < y$ y x y y están en el dominio de f. De manera similar, f se llama decreciente si $f(x) \geq f(y)$, y estrictamente decreciente si $f(x) > f(y)$, siempre que $x < y$, x y y están en el dominio de f. (La palabra estrictamente en esta definición indica una desigualdad estricta).

Observación 2.6.6 Una función f es creciente si $\forall x \forall y(x < y \rightarrow f(x) \leq f(y))$, estrictamente creciente si $\forall x \forall y(x < y \rightarrow f(x) < f(y))$, decreciente si $\forall x \forall y(x < y \rightarrow f(x) \geq f(y))$, y estrictamente decreciente si $\forall x \forall y(x < y \rightarrow f(x) > f(y))$, donde el universo de discurso es el dominio de f.

□

Ejemplo 2.6.12 La función $f(x) = x^2$ de $\mathbb{R}^+$ a $\mathbb{R}^+$ es estrictamente creciente. Para ver esto, suponga que x y y son números reales positivos con

$x < y$. Al multiplicar ambos lados de esta desigualdad por x da $x^2 < xy$. De manera similar, multiplicar ambos lados por y da $xy < y^2$. Por tanto, $f(x) = x^2 < xy < y^2 = f(y)$.

Sin embargo, la función $f(x) = x^2$ de $\mathbb{R}$ al conjunto de números reales no negativos no es estrictamente creciente porque $-1 < 0$, pero $f(-1) = (-1)^2 = 1$ no es menor que $f(0) = 0^2 = 0$. □

A partir de estas definiciones, se puede demostrar que una función que es estrictamente creciente o estrictamente decreciente debe ser uno a uno. Sin embargo, una función que crece, pero no crece estrictamente, o decrece, pero no decrece estrictamente, no es uno a uno.

Para algunas funciones, el rango y el codominio son iguales. Es decir, cada miembro del codominio es la imagen de algún elemento del dominio. Las funciones con esta propiedad se llaman funciones **sobre**.

Definición 2.6.7 Una función f de A a B se llama *sobre*, o una *sobreyección*, si y sólo si para cada elemento $b \in B$ hay un elemento $a \in A$ con $f(a) = b$. Una función f se llama *sobreyectiva* si es sobre.

Observación 2.6.7 Una función f es sobre si $\forall y \exists x(f(x) = y)$, donde el dominio de x es el dominio de la función y el dominio de y es el codominio de la función.

□

Ahora damos ejemplos de funciones sobre y funciones que no son sobre.

Ejemplo 2.6.13 Sea f la función de $\{a, b, c, d\}$ a $\{1, 2, 3\}$ definida por $f(a) = 3$, $f(b) = 2$, $f(c) = 1$ y $f(d) = 3$. ¿Es f una función sobre?

Solución: Debido a que los tres elementos del codominio son imágenes de elementos en el dominio, vemos que f es sobre. Esto se ilustra en la Figura 2.28. Tenga en cuenta que si el codominio fuera $\{1, 2, 3, 4\}$, entonces f no sería sobre.

□

Ejemplo 2.6.14 ¿Es sobre la función $f(x) = x^2$ del conjunto de enteros al conjunto de enteros?

Solución: La función f no es sobre porque no hay un número entero x con $x^2 = -1$, por ejemplo. □

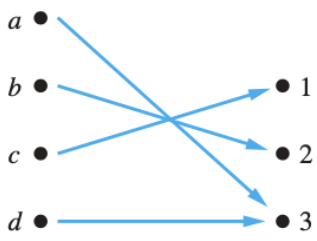


Figura 2.28: Una función sobre.

Ejemplo 2.6.15 ¿Es sobre la función $f(x) = x + 1$ del conjunto de enteros al conjunto de enteros?

Solución: Esta función es sobre, porque para cada entero y hay un entero x tal que $f(x) = y$. Para ver esto, tenga en cuenta que $f(x) = y$ si y sólo si $x + 1 = y$, lo cual se cumple si y sólo si $x = y - 1$. (Tenga en cuenta que $y - 1$ también es un número entero, por lo que está en el dominio de f.)

□

Ejemplo 2.6.16 Considere la función f del Ejemplo 2.6.11 que asigna trabajos a los trabajadores. La función f es sobre si para cada trabajo hay un trabajador asignado a este trabajo. La función f no es sobre si hay al menos un trabajo que no tiene ningún trabajador asignado.

□

Definición 2.6.8 La función f es una *correspondencia uno a uno*, o una *biyección*, si es tanto uno a uno como sobre. También decimos que tal función es *biyectiva*.

Los ejemplos 2.6.17 y 2.6.18 ilustran el concepto de biyección.

Ejemplo 2.6.17 Sea f la función de $\{a, b, c, d\}$ a $\{1, 2, 3, 4\}$ con $f(a) = 4$, $f(b) = 2$, $f(c) = 1$ y $f(d) = 3$. ¿Es una biyección?

Solución: La función f es uno a uno y sobre. Es uno a uno porque no se asigna el mismo valor de función a dos valores en el dominio. Es sobre porque los cuatro elementos del codominio son imágenes de elementos del dominio. Por tanto, f es una biyección. □

La Figura 2.29 muestra cuatro funciones donde la primera es uno a uno pero no sobre, la segunda es sobre pero no uno a uno, la tercera es tanto uno

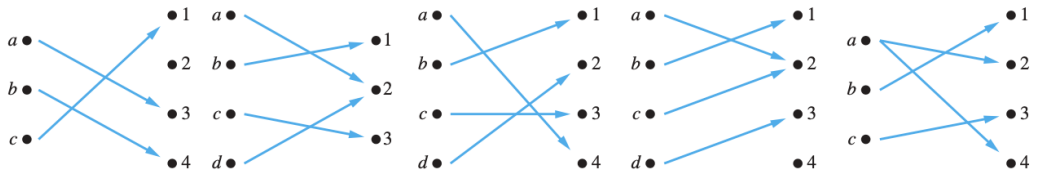


Figura 2.29: Ejemplos de diferentes tipos de correspondencias.

a uno como sobre, y la cuarta no es ni uno a uno ni sobre. La quinta correspondencia en la Figura 2.29 no es una función, porque envía un elemento a dos elementos diferentes.

Suponga que f es una función de un conjunto A en sí mismo. Si A es finito, entonces f es uno a uno si y sólo si es sobre. Este no es necesariamente el caso si A es infinito.

Ejemplo 2.6.18 Sea A un conjunto. La función identidad sobre A es la función $\iota_A : A \to A$, donde $\iota_A(x) = x$ para todo $x \in A$. En otras palabras, la función identidad ι_A es la función que asigna cada elemento a sí mismo. La función ι_A es uno a uno y sobre, por lo que es una biyección. (Tenga en cuenta que ι es la letra griega iota). □

Para referencia futura, resumimos lo que debe mostrarse para establecer si una función es uno a uno y si es sobre. Es instructivo revisar los ejemplos 2.6.8-2.6.17 a la luz de este resumen.

Suponga que $f : A \to B$.
Demostrar que f es inyectiva Muestre que si $f(x) = f(y)$ para $x, y \in A$ arbitrario, entonces $x = y$.
Demostrar que f no es inyectiva Encuentre elementos particulares $x, y \in A$ tales que $x \neq y$ y $f(x) = f(y)$.
Demostrar que f es sobre Considere un elemento arbitrario $y \in B$ y encuentre un elemento $x \in A$ tal que $f(x) = y$.
Demostrar que f no es sobre Encuentre un $y \in B$ particular tal que $f(x) \neq y$ para todo $x \in A$.

2.6.3. Funciones Inversas y Composiciones de Funciones

Considere ahora una correspondencia uno a uno f del conjunto A al conjunto B. Dado que f es una función sobre, cada elemento de B es la

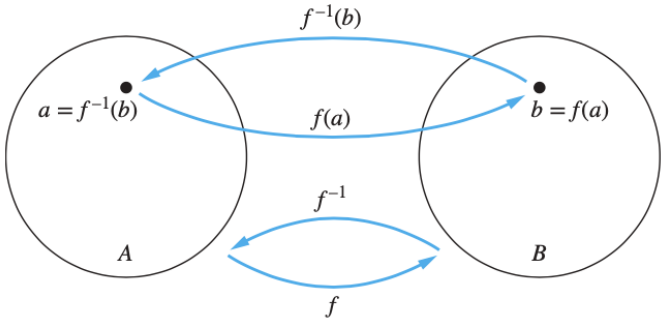


Figura 2.30: La función f^{-1} es la inversa de la función f.

imagen de algún elemento en A. Además, debido a que f también es una función uno a uno, cada elemento de B es la imagen de un elemento único de A. En consecuencia, podemos definir una nueva función de B a A que invierte la correspondencia dada por f. Esto conduce a la Definición 2.6.9.

Definición 2.6.9 Sea f una correspondencia uno a uno del conjunto A al conjunto B. La *función inversa* de f es la función que asigna a un elemento b perteneciente a B el elemento único a en A tal que $f(a) = b$. La función inversa de f se denota por f^{-1}. Por tanto, $f^{-1}(b) = a$ cuando $f(a) = b$.

Observación 2.6.8 Asegúrese de no confundir la función f^{-1} con la función $1/f$, que es la función que asigna a cada x en el dominio el valor $1/f(x)$. Observe que este último tiene sentido sólo cuando $f(x)$ es un número real distinto de cero.

□

La Figura 2.30 ilustra el concepto de función inversa.

Si una función f no es una correspondencia uno a uno, no podemos definir una función inversa de f. Cuando f no es una correspondencia uno a uno, o no es uno a uno o no es sobre. Si f no es uno a uno, algún elemento b en el codominio es la imagen de más de un elemento en el dominio.

Si f no es sobre, para algún elemento b en el codominio, no existe ningún elemento a en el dominio para el cual $f(a) = b$. En consecuencia, si f no es una correspondencia uno a uno, no podemos asignar a cada elemento b en el codominio un elemento único a en el dominio tal que $f(a) = b$ (porque para algunos b hay más de un a o ningún a).

Una correspondencia uno a uno se llama **invertible** porque podemos definir una inversa de esta función. Una función **no es invertible** si no es una correspondencia uno a uno, porque la inversa de dicha función no existe.

Ejemplo 2.6.19 Sea f la función de $\{a, b, c\}$ a $\{1, 2, 3\}$ tal que $f(a) = 2$, $f(b) = 3$ y $f(c) = 1$. ¿Es invertible f y si lo es, ¿cuál es su inversa?

Solución: La función f es invertible porque es una correspondencia uno a uno. La función inversa f^{-1} invierte la correspondencia dada por f, entonces $f^{-1}(1) = c$, $f^{-1}(2) = a$, y $f^{-1}(3) = b$.

□

Ejemplo 2.6.20 Sea $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(x) = x + 1$. ¿Es invertible f, y si lo es, cuál es su inversa?

Solución: La función f tiene una inversa porque es una correspondencia uno a uno, como se muestra en los Ejemplos 2.6.10 y 2.6.15. Para invertir la correspondencia, suponga que y es la imagen de x, de modo que $y = x + 1$. Entonces $x = y - 1$. Esto significa que $y - 1$ es el elemento único de $\mathbb{Z}$ que es enviado a y por f. En consecuencia, $f^{-1}(y) = y - 1$. □

Ejemplo 2.6.21 Sea f la función de $\mathbb{R}$ a $\mathbb{R}$ con $f(x) = x^2$. ¿Es invertible f?

Solución: Como $f(-2) = f(2) = 4$, f no es uno a uno. Si se definiera una función inversa, tendría que asignar dos elementos a 4, violando la Definición 2.6.1. Por tanto, f no es invertible. (Tenga en cuenta que también podemos mostrar que f no es invertible porque no es sobre).

□

A veces podemos restringir el dominio o el codominio de una función, o ambos, para obtener una función invertible, como lo ilustra el Ejemplo 22.

Ejemplo 2.6.22 Demuestre que si restringimos la función $f(x) = x^2$ en el Ejemplo 2.6.21 a una función del conjunto de todos los números reales no negativos al conjunto de todos los números reales no negativos, entonces f es invertible.

Solución: La función $f(x) = x^2$ del conjunto de números reales no negativos al conjunto de números reales no negativos es uno a uno. Para ver esto, tenga en cuenta que si $f(x) = f(y)$, entonces $x^2 = y^2$, entonces $x^2 - y^2 = (x + y)(x - y) = 0$. Esto significa que $x + y = 0$ o $x - y = 0$, entonces $x = -y$ o $x = y$. Debido a que tanto x como y no son negativos, debemos tener $x = y$. Entonces, esta función es uno a uno.

Además, $f(x) = x^2$ es sobre cuando el codominio es el conjunto de todos los números reales no negativos, porque cada número real no negativo tiene una raíz cuadrada.

Es decir, si y es un número real no negativo, existe un número real no negativo x tal que $x = \sqrt{y}$, lo que significa que $x^2 = y$. Debido a que la función $f(x) = x^2$ del conjunto de números reales no negativos al conjunto de números reales no negativos es uno a uno y sobre, es invertible. Su inversa está dada por la regla $f^{-1}(y) = \sqrt{y}$.

□

Definición 2.6.10 Sea g una función del conjunto A al conjunto B y sea f una función del conjunto B al conjunto C. La *composición* de las funciones f y g, denotada para todo $a \in A$ por $f \circ g$, es la función de A a C definida por

$$(f \circ g)(a) = f(g(a)).$$

En otras palabras, $f \circ g$ es la función que asigna al elemento a de A el elemento asignado por f a $g(a)$. El dominio de $f \circ g$ es el dominio de g. El rango de $f \circ g$ es la imagen del rango de g con respecto a la función f.

Es decir, para encontrar $(f \circ g)(a)$ primero aplicamos la función g a a para obtener $g(a)$ y luego aplicamos la función f al resultado $g(a)$ para obtener $(f \circ g)(a) = f(g(a))$.

Tenga en cuenta que la composición $f \circ g$ no se puede definir a menos que el rango de g sea un subconjunto del dominio de f. En la Figura 2.31 se muestra la composición de funciones.

Ejemplo 2.6.23 Sea g la función del conjunto $\{a, b, c\}$ a sí mismo tal que $g(a) = b$, $g(b) = c$, y $g(c) = a$. Sea f la función del conjunto $\{a, b, c\}$ al conjunto $\{1, 2, 3\}$ tal que $f(a) = 3$, $f(b) = 2$, y $f(c) = 1$. ¿Cuál es la composición de f y g, y cuál es la composición de g y f?

Solución: La composición $f \circ g$ está definida por $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$ y $(f \circ g)(c) = f(g(c)) = f(a) = 3$. Tenga en cuenta que $g \circ f$ no está definida, porque el rango de f no es un subconjunto del dominio de g.

□

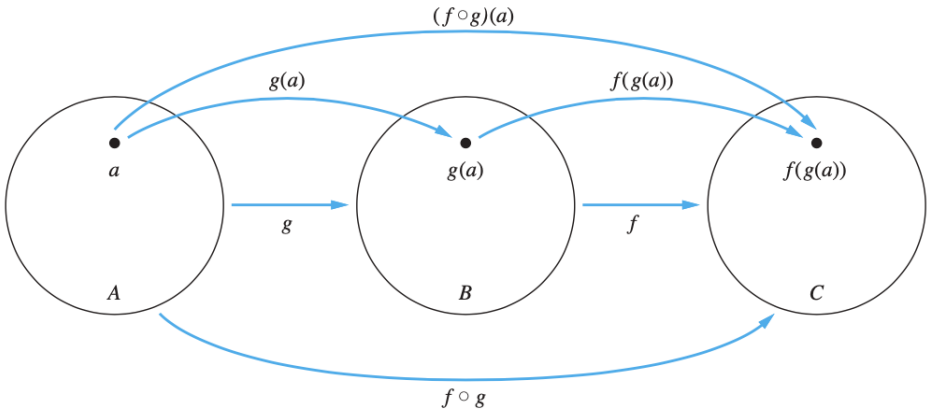


Figura 2.31: La composición de las funciones f y g.

Ejemplo 2.6.24 Sean f y g las funciones del conjunto de enteros al conjunto de enteros definido por $f(x) = 2x+3$ y $g(x) = 3x+2$. ¿Cuál es la composición de f y g? ¿Cuál es la composición de g y f?

Solución: Se definen las composiciones $f \circ g$ y $g \circ f$. Así,

$$(f \circ g)(x) = f(g(x)) = f(3x+2) = 2(3x+2)+3 = 6x+7$$

y

$$(g \circ f)(x) = g(f(x)) = g(2x+3) = 3(2x+3)+2 = 6x+11.$$

□

Observación 2.6.9 Tenga en cuenta que aunque $f \circ g$ y $g \circ f$ se definen para las funciones f y g en el Ejemplo 2.6.24, $f \circ g$ y $g \circ f$ no son iguales. En otras palabras, la ley conmutativa no se cumple para la composición de funciones.

□

Ejemplo 2.6.25 Sean f y g las funciones definidas por $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ con $f(x) = x^2$ y $g : \mathbb{R}^+ \cup \{0\} \to \mathbb{R}$ con $g(x) = \sqrt{x}$ (donde $\sqrt{x}$ es la raíz cuadrada no negativa de x). ¿Cuál es la función $(f \circ g)(x)$?

Solución: El dominio de $(f \circ g)(x) = f(g(x))$ es el dominio de g, que es $\mathbb{R}^+ \cup \{0\}$, el conjunto de números reales no negativos. Si x es un número real no negativo, tenemos $(f \circ g)(x) = f(g(x)) = f(\sqrt{x}) = \sqrt{x}^2 = x$. El rango de $f \circ g$ es la imagen del rango de g con respecto a la función f. Este es el

conjunto $\mathbb{R}^+ \cup \{0\}$, el conjunto de números reales no negativos. Resumiendo, $f \circ g : \mathbb{R}^+ \cup \{0\} \to \mathbb{R}^+ \cup \{0\}$ y $f(g(x)) = x$ para todo x.

□

Cuando se forma la composición de una función y su inversa, en cualquier orden, se obtiene una función identidad. Para ver esto, suponga que f es una correspondencia uno a uno del conjunto A al conjunto B. Entonces la función inversa f^{-1} existe y es una correspondencia uno a uno de B a A. La función inversa invierte la correspondencia de la función original, entonces $f^{-1}(b) = a$ cuando $f(a) = b$, y $f(a) = b$ cuando $f^{-1}(b) = a$. Por eso,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

y

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$$

En consecuencia, $f^{-1} \circ f = \iota_A$ y $f \circ f^{-1} = \iota_B$, donde ι_A y ι_B son las funciones identidad de los conjuntos A y B, respectivamente. Es decir, $(f^{-1})^{-1} = f$.

2.6.4. Gráficas de funciones

Podemos asociar un conjunto de pares en $A \times B$ a cada función de A a B. Este conjunto de pares se denomina **gráfica** de la función y, a menudo, se muestra gráficamente para ayudar a comprender el comportamiento de la función.

Definición 2.6.11 Sea f una función del conjunto A al conjunto B. La *gráfica* de la función f es el conjunto de pares ordenados $\{(a, b)|a \in A \text{ y } f(a) = b\}$.

De la definición, la gráfica de una función f de A a B es el subconjunto de $A \times B$ que contiene los pares ordenados con la segunda entrada igual al elemento de B asignado por f a la primera entrada. Además, observe que la gráfica de una función f de A a B es la misma que la relación de A a B determinada por la función f, como se describe en la Sección 2.6.1.

Ejemplo 2.6.26 Muestre la gráfica de la función $f(n) = 2n+1$ del conjunto de enteros al conjunto de enteros.

Solución: La gráfica de f es el conjunto de pares ordenados de la forma $(n, 2n+1)$, donde n es un número entero. Esta gráfica se muestra en la Figura 2.32.

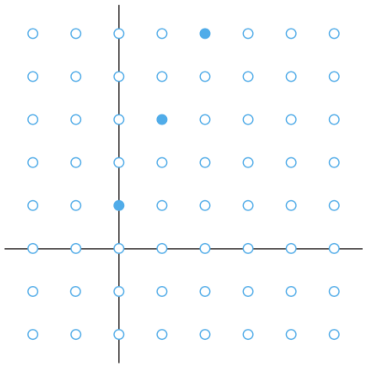


Figura 2.32: La gráfica de $f(n) = 2n + 1$ de $\mathbb{Z}$ a $\mathbb{Z}$.

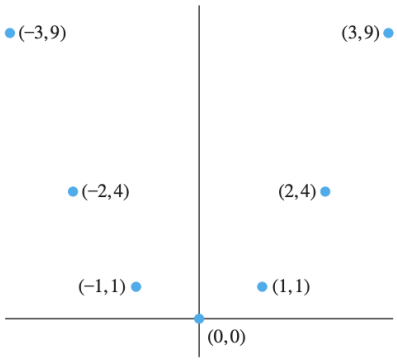


Figura 2.33: La gráfica de $f(x) = x^2$ de $\mathbb{Z}$ a $\mathbb{Z}$.

□

Ejemplo 2.6.27 Muestre la gráfica de la función $f(x) = x^2$ del conjunto de enteros al conjunto de enteros.

Solución: La gráfica de f es el conjunto de pares ordenados de la forma $(x, f(x)) = (x, x^2)$, donde x es un número entero. Esta gráfica se muestra en la Figura 2.33. □

2.6.5. Algunas Funciones Importantes

A continuación, presentamos dos funciones importantes en matemáticas discretas, a saber, las funciones **piso** y **techo**.

Sea x un número real. La función piso redondea x hacia abajo al número

entero más cercano menor o igual a x, y la función techo redondea x hacia arriba al número entero más cercano mayor o igual a x.

Estas funciones se utilizan a menudo cuando se cuentan objetos. Desempeñan un papel importante en el análisis del número de pasos utilizados por los procedimientos para resolver problemas de un tamaño particular.

Definición 2.6.12 La *función piso* asigna al número real x el entero más grande que es menor o igual que x. El valor de la función piso en x se denota por $\lfloor x \rfloor$. La *función techo* asigna al número real x el entero más pequeño que es mayor o igual que x. El valor de la función techo en x se denota por $\lceil x \rceil$.

Ejemplo 2.6.28 Estos son algunos valores de las funciones piso y techo:

$$\lfloor \frac{1}{2} \rfloor = 0, \lceil \frac{1}{2} \rceil = 1, \lfloor -\frac{1}{2} \rfloor = -1, \lceil -\frac{1}{2} \rceil = 0,$$
$$\lfloor 3.1 \rfloor = 3, \lceil 3.1 \rceil = 4, \lfloor 7 \rfloor = 7, \lceil 7 \rceil = 7.$$

□

Mostramos las gráficas de las funciones piso y techo en la Figura 2.34. En la Figura 2.34 (a) mostramos la gráfica de la función piso $\lfloor x \rfloor$. Tenga en cuenta que esta función tiene el mismo valor en todo el intervalo $[n, n+1)$, a saber, n, y luego salta a $n+1$ cuando $x = n+1$.

En la Figura 2.34 (b) mostramos la gráfica de la función techo $\lceil x \rceil$. Tenga en cuenta que esta función tiene el mismo valor en todo el intervalo $(n, n+1]$, es decir, $n+1$, y luego salta a $n+2$ cuando x es un poco mayor que $n+1$. Las funciones piso y techo son útiles en una amplia variedad de aplicaciones, incluidas las que implican almacenamiento y transmisión de datos. Considere los ejemplos 2.6.29 y 2.6.30, típicos de cálculos básicos realizados cuando se estudian problemas de comunicaciones de datos y bases de datos.

Ejemplo 2.6.29 Los datos almacenados en un disco de computadora o transmitidos a través de una red de datos generalmente se representan como una cadena de bytes. Cada byte se compone de 8 bits. ¿Cuántos bytes se requieren para codificar 100 bits de datos?

Solución: Para determinar el número de bytes necesarios, determinamos el número entero más pequeño que sea al menos tan grande como el cociente cuando 100 se divide por 8, el número de bits en un byte. En consecuencia, se requieren $\lceil 100/8 \rceil = \lceil 12.5 \rceil = 13$ bytes. □

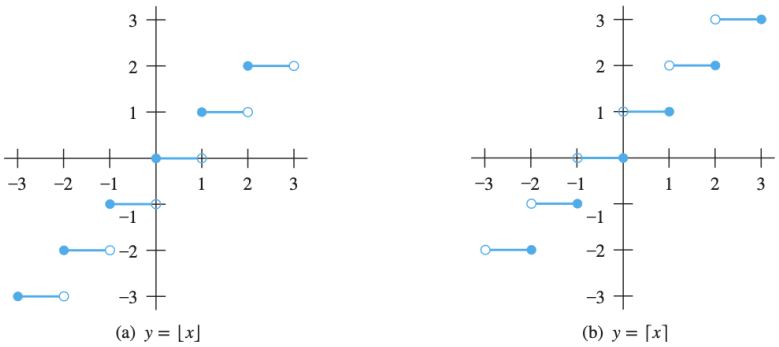


Figura 2.34: Las gráficas de las funciones (a) piso y (b) techo.

Ejemplo 2.6.30 En el modo de transferencia asincrónica (ATM) (un protocolo de comunicaciones utilizado en redes troncales), los datos se organizan en celdas de 53 bytes. ¿Cuántas celdas ATM se pueden transmitir en 1 minuto a través de una conexión que transmite datos a una velocidad de 500 kilobits por segundo?

Solución: En 1 minuto, esta conexión puede transmitir $500,000 \cdot 60 = 30,000,000$ bits. Cada celda ATM tiene una longitud de 53 bytes, lo que significa que tiene una longitud de $53 \cdot 8 = 424$ bits.

Para determinar el número de celdas que se pueden transmitir en 1 minuto, determinamos el número entero más grande que no exceda el cociente cuando 30,000,000 se divide por 424. En consecuencia, $\lfloor 30,000,000/424 \rfloor = 70,754$ celdas ATM se pueden transmitir en 1 minuto sobre una conexión de 500 kilobits por segundo.

□

La Tabla 2.1, donde x denota un número real, muestra algunas propiedades simples pero importantes de las funciones piso y techo. Debido a que estas funciones aparecen con tanta frecuencia en las matemáticas discretas, es útil examinar estas identidades.

Cada propiedad de esta tabla se puede establecer utilizando las definiciones de las funciones piso y techo. Las propiedades (1a), (1b), (1c) y (1d) se derivan directamente de estas definiciones.

Por ejemplo, (1a) establece que $\lfloor x \rfloor = n$ si y sólo si el número entero n es menor o igual que x y $n + 1$ es mayor que x. Esto es precisamente lo que significa que n sea el mayor número entero que no exceda x, que es la definición de $\lfloor x \rfloor = n$.

Las propiedades (1b), (1c) y (1d) se pueden establecer de manera similar. Demostraremos la propiedad (4a) usando una prueba directa.

(1a)	$\lfloor x \rfloor = n$ if and only if $n \leq x < n+1$
(1b)	$\lceil x \rceil = n$ if and only if $n-1 < x \leq n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x-1 < n \leq x$
(1d)	$\lceil x \rceil = n$ if and only if $x \leq n < x+1$
(2)	$x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x+n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x+n \rceil = \lceil x \rceil + n$

Tabla 2.1: Propiedades útiles de las funciones piso y techo ($n \in \mathbb{N}$ y $x \in \mathbb{R}$).

Demostración: Suponga que $\lfloor x \rfloor = m$, donde m es un número entero positivo. Por la propiedad (1a), se deduce que $m \leq x < m+1$. Sumando n a las tres cantidades en esta cadena de dos desigualdades muestra que $m+n \leq x+n < m+n+1$. Usando la propiedad (1a) nuevamente, vemos que $\lfloor x+n \rfloor = m+n = \lfloor x \rfloor + n$. Esto completa la prueba. Las pruebas de las otras propiedades se dejan como ejercicios.

■

Las funciones piso y techo disfrutan de muchas otras propiedades útiles además de las que se muestran en la Tabla 2.1. También hay muchas afirmaciones sobre estas funciones que pueden parecer correctas, pero en realidad no lo son. Consideraremos declaraciones sobre las funciones piso y techo en los Ejemplos 2.6.31 y 2.6.32.

Un enfoque útil para considerar declaraciones sobre la función piso es hacer $x = n + \epsilon$, donde $n = \lfloor x \rfloor$ es un número entero, y ϵ, la parte fraccionaria de x, satisface la desigualdad $0 \leq \epsilon < 1$. De manera similar, cuando considerando declaraciones sobre la función de techo, es útil escribir $x = n - \epsilon$, donde $n = \lceil x \rceil$ es un número entero y $0 \leq \epsilon < 1$.

Ejemplo 2.6.31 Demuestre que si x es un número real, entonces $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Solución: Para probar esta afirmación, tomamos $x = n + \epsilon$, donde n es un número entero y $0 \leq \epsilon < 1$. Hay dos casos a considerar, dependiendo de

si ϵ es menor, mayor o igual que $\frac{1}{2}$. (La razón por la que elegimos estos dos casos se aclarará en la prueba).

Primero consideramos el caso cuando $0 \leq \epsilon < \frac{1}{2}$. En este caso, $2x = 2n+2\epsilon$ y $\lfloor 2x \rfloor = 2n$ porque $0 \leq 2\epsilon < 1$. De manera similar, $x + \frac{1}{2} = n + (\frac{1}{2} + \epsilon)$, entonces $\lfloor x + \frac{1}{2} \rfloor = n$, porque $0 < \frac{1}{2} + \epsilon < 1$. En consecuencia, $\lfloor 2x \rfloor = 2n$ y $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + n = 2n$.

A continuación, consideramos el caso cuando $\frac{1}{2} \leq \epsilon < 1$. En este caso, $2x = 2n + 2\epsilon = (2n + 1) + (2\epsilon - 1)$. Como $0 \leq 2\epsilon - 1 < 1$, se deduce que $\lfloor 2x \rfloor = 2n + 1$. Como $\lfloor x + \frac{1}{2} \rfloor = \lfloor n + (\frac{1}{2} + \epsilon) \rfloor = \lfloor n + 1 + (\epsilon - \frac{1}{2}) \rfloor$ y $0 \leq \epsilon - \frac{1}{2} < 1$, se deduce que $\lfloor x + \frac{1}{2} \rfloor = n + 1$. En consecuencia, $\lfloor 2x \rfloor = 2n + 1$ y $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + (n + 1) = 2n + 1$. Con esto concluye la prueba.

□

Ejemplo 2.6.32 Demuestre o refute que $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ para todos los números reales x y y.

Solución: Aunque esta afirmación puede parecer razonable, es falsa. Un contraejemplo lo proporcionan $x = \frac{1}{2}$ y $y = \frac{1}{2}$. Con estos valores encontramos que $\lceil x + y \rceil = \lceil \frac{1}{2} + \frac{1}{2} \rceil = \lceil 1 \rceil = 1$, pero $\lceil x \rceil + \lceil y \rceil = \lceil \frac{1}{2} \rceil + \lceil \frac{1}{2} \rceil = 1 + 1 = 2$.

□

Sea n un número entero positivo y sea b un número real positivo fijo. La función $f_b(n) = b^n$ está definida por

$$f_b(n) = b^n = b \cdot b \cdot b \cdot \cdots \cdot b,$$

donde hay n factores de b multiplicados juntos en el lado derecho de la ecuación.

Podemos definir la función $f_b(x) = b^x$ para todos los números reales x usando técnicas de cálculo. La función $f_b(x) = b^x$ se llama **función exponencial en base *b***. No vamos a discutir cómo encontrar los valores de funciones exponenciales en base b cuando x no es un número entero.

En el Teorema 2.6.1 se dan dos de las propiedades importantes que satisfacen las funciones exponenciales. Las pruebas de estas y otras propiedades relacionadas se pueden encontrar en los textos de cálculo.

Teorema 2.6.1 Sea b un número real positivo y x y y números reales. Entonces

1. $b^{x+y} = b^x b^y$, y

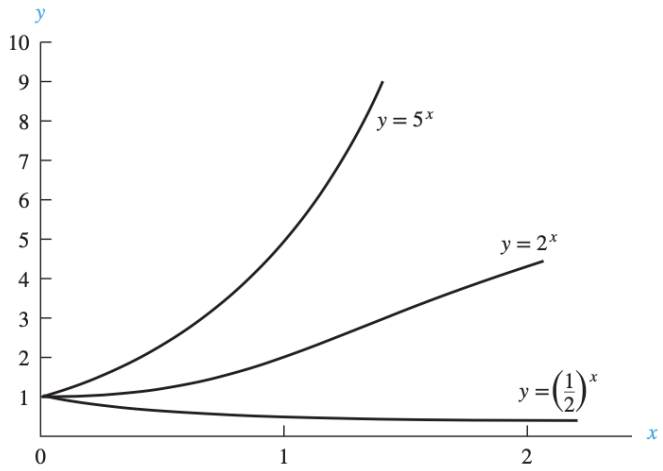


Figura 2.35: Gráficas de las funciones exponenciales en bases $\frac{1}{2}$, 2 y 5.

2. $(b^x)^y = b^{xy}$.

■

Mostramos las gráficas de algunas funciones exponenciales en la Figura 2.35.

Suponga que b es un número real con $b > 1$. Entonces la función exponencial b^x es estrictamente creciente (un hecho que se muestra en el cálculo). Es una correspondencia uno a uno del conjunto de números reales al conjunto de números reales no negativos. Por lo tanto, esta función tiene una inversa $\log_b x$, llamada la **función logarítmica en base *b***. En otras palabras, si b es un número real mayor que 1 y x es un número real positivo, entonces

$$b^{\log_b x} = x.$$

El valor de esta función en x se llama **logaritmo de *x* en base *b***.
De la definición se deduce que

$$\log_b b^x = x.$$

Damos varias propiedades importantes de los logaritmos en el Teorema 2.6.2.

Teorema 2.6.2 Sea b un número real mayor que 1. Entonces

1. $\log_b(xy) = \log_b x + \log_b y$ siempre que x y y sean números reales positivos, y

2. $\log_b(x^y) = y \log_b x$ siempre que x es un número real positivo y y es un número real.

Demostración: Debido a que $\log_b(xy)$ es el único número real con $b^{\log_b(xy)} = xy$, para probar la parte 1 basta con mostrar que $b^{\log_b x + \log_b y} = xy$. Según la parte 1 del Teorema 2.6.1, tenemos

$$b^{\log_b x + \log_b y} = b^{\log_b x} b^{\log_b y} = xy.$$

Para probar la parte 2, basta con mostrar que $b^{y \log_b x} = x^y$. Según la parte 2 del Teorema 2.6.1, tenemos que

$$b^{y \log_b x} = (b^{\log_b x})^y = x^y.$$

■

El siguiente teorema relaciona los logaritmos con dos bases diferentes.

Teorema 2.6.3 CAMBIO DE FÓRMULA BASE PARA LOGARITMOS Sean a y b números reales mayores que 1 y sea x un número real positivo. Entonces

$$\log_a x = \log_b x / \log_b a.$$

Demostración: Para probar este resultado, basta con mostrar que

$$b^{\log_a x \cdot \log_b a} = x.$$

Según la parte 2 del Teorema 2.6.1, tenemos

$$b^{\log_a x \cdot \log_b a} = (b^{\log_b a})^{\log_a x} = a^{\log_a x} = x.$$

Esto completa la prueba. ■

En estas notas, la notación $\log x$ se usará para denotar el logaritmo en base 2 de x, porque 2 es la base que usualmente usaremos para los logaritmos. Denotaremos logaritmos en base b, donde b es cualquier número real mayor que 1, por $\log_b x$ y el logaritmo natural por $\ln x$.

La gráfica de la función $f(x) = \log x$ se muestra en la Figura 2.36. A partir del Teorema 2.6.3, cuando se usa una base b distinta de 2, se obtiene una función que es un múltiplo constante de la función $\log x$, a saber, $(1/\log b) \log x$.

Otra función que usaremos es la **función factorial** $f : \mathbb{N} \to \mathbb{Z}^+$, denotada por $f(n) = n!$. El valor de $f(n) = n!$ es el producto de los primeros n números enteros positivos, por lo que $f(n) = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$ [y $f(0) = 0! = 1$].

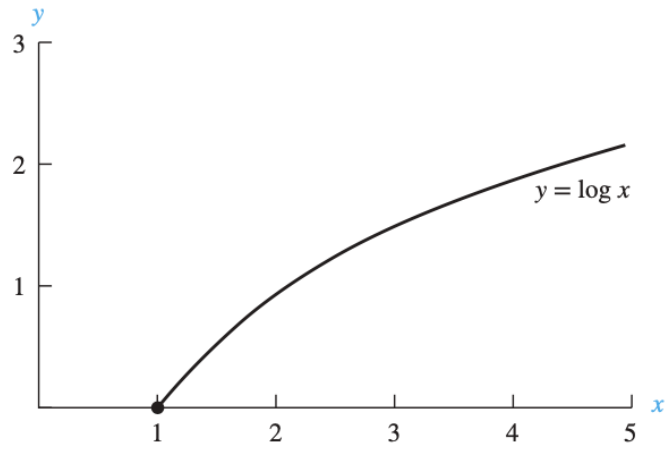


Figura 2.36: La gráfica de $f(x) = \log x$.

Ejemplo 2.6.33 Tenemos que $f(1) = 1! = 1$, $f(2) = 2! = 1 \cdot 2 = 2$, $f(6) = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$, y $f(20) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 = 2,432,902,008,176,640,000$.

□

El Ejemplo 2.6.33 ilustra que la función factorial crece extremadamente rápido a medida que crece n.

2.6.6. Funciones Parciales

Un programa diseñado para evaluar una función puede no producir el valor correcto de la función para todos los elementos en el dominio de esta función. Por ejemplo, un programa puede no producir un valor correcto porque la evaluación de la función puede conducir a un bucle infinito o un desbordamiento.

De manera similar, en matemáticas abstractas, a menudo queremos discutir funciones que están definidas solo para un subconjunto de los números reales, como $1/x$, $\sqrt{x}$ y $\arcsin(x)$.

También, queremos usar nociones como la función "el hijo más joven", el cual está indefinido si una pareja no tiene hijos, o "la hora del amanecer" que está indefinida por algunos días en el Círculo Ártico. Para estudiar dichas situaciones, usamos el concepto de función parcial.

Definición 2.6.13 Una *función parcial* f de un conjunto A a un conjunto B es una asignación a cada elemento a en un subconjunto de A, llamado *dominio de definición* de f, de un elemento único b en B. Los conjuntos A y B se llaman dominio y codominio de f, respectivamente. Decimos que f no está definida para los elementos de A que no están en el dominio de definición de f. Cuando el dominio de definición de f es igual a A, decimos que f es una *función total*.

Observación 2.6.10 Escribimos $f : A \to B$ para denotar que f es una función parcial de A a B. Note que esta es la misma notación que se usa para las funciones. El contexto en el que se usa la notación determina si f es una función parcial o una función total.

□

Ejemplo 2.6.34 La función $f : \mathbb{Z} \to \mathbb{R}$ donde $f(n) = \sqrt{n}$ es una función parcial de $\mathbb{Z}$ a $\mathbb{R}$ donde el dominio de definición es el conjunto de enteros no negativos. Tenga en cuenta que f no está definida para números enteros negativos. □

2.6.7. Ejercicios

1. Determine si cada una de estas funciones de $\{a, b, c, d\}$ a sí mismo es uno a uno.

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

2. Determine si cada una de estas funciones de $\mathbb{Z}$ a $\mathbb{Z}$ es uno a uno.

   a) $f(n) = n - 1.$
   b) $f(n) = n^2 + 1.$
   c) $f(n) = n^3.$
   d) $f(n) = \lceil n/2 \rceil.$

3. Determine si $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ es sobre cuando

a) $f(m, n) = 2m - n$.
b) $f(m, n) = m^2 - n^2$.
c) $f(m, n) = m + n + 1$.
d) $f(m, n) = m^2 - 4$.

4. Determine si cada una de estas funciones es una biyección de $\mathbb{R}$ a $\mathbb{R}$.

   a) $f(x) = -3x + 4$.
   b) $f(x) = 2x + 1$.
   c) $f(x) = -3x^2 + 7$.
   d) $f(x) = x^2 + 1$.

5. Encuentre $f \circ g$ y $g \circ f$, donde $f(x) = x^2 + 1$ y $g(x) = x + 2$, son funciones de $\mathbb{R}$ a $\mathbb{R}$.

6. Suponga que g es una función de A a B y f es una función de B a C.

   a) Demuestre que si tanto f como g son funciones uno a uno, entonces $f \circ g$ también es uno a uno.
   b) Demuestre que si tanto f como g son funciones sobre, entonces $f \circ g$ también es sobre.

7. Suponga que g es una función de A a B y f es una función de B a C. Pruebe cada una de estas afirmaciones.

   a) Si $f \circ g$ es sobre, entonces f debe ser sobre.
   b) Si $f \circ g$ es uno a uno, entonces g debe ser uno a uno.

Capítulo 3

Teoría de Números

La parte de las matemáticas dedicada al estudio del conjunto de números enteros y sus propiedades se conoce como teoría de números. En este capítulo desarrollaremos algunos de los conceptos importantes de la teoría de números, incluidos muchos de los que se utilizan en ciencias de la computación.

Primero presentaremos la noción de divisibilidad de números enteros, que usamos para introducir aritmética modular o de reloj. La aritmética modular opera con los restos de números enteros cuando se dividen por un número entero positivo fijo, llamado módulo. Demostraremos muchos resultados importantes sobre la aritmética modular que utilizaremos ampliamente en este capítulo.

Discutiremos los números primos, los enteros positivos que tienen sólo a 1 y ellos mismos como divisores positivos. Demostraremos que hay infinitos números primos; la demostración que damos se considera una de las más hermosas de las matemáticas.

Introduciremos el concepto de máximo común divisor y estudiaremos el algoritmo euclidiano para calcularlos.

Este algoritmo se describió por primera vez hace miles de años. Introduciremos el teorema fundamental de la aritmética, un resultado clave que nos dice que cada entero positivo tiene una factorización única en números primos.

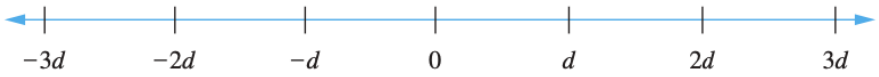


Figura 3.1: Enteros divisibles por el entero positivo d.

3.1. Divisibilidad y Aritmética Modular

3.1.1. Introducción

Las ideas que desarrollaremos en esta sección se basan en la noción de divisibilidad. La división de un número entero por un número entero positivo produce un cociente y un resto. Trabajar con estos restos conduce a la aritmética modular, que juega un papel importante en matemáticas y que se utiliza en todas las ciencias de la computación.

3.1.2. Division

Cuando un número entero se divide por un segundo número entero distinto de cero, el cociente puede ser o no un número entero. Por ejemplo, $12/3 = 4$ es un número entero, mientras que $11/4 = 2.75$ no lo es. Esto conduce a la Definición 3.1.1.

Definición 3.1.1 Si a y b son números enteros con $a \neq 0$, decimos que a *divide* a b si hay un número entero c tal que $b = ac$ (o de forma equivalente, si $\frac{b}{a}$ es un número entero). Cuando a divide a b, decimos que a es un *factor* o *divisor* de b, y que b es un múltiplo de a. La notación $a|b$ denota que a divide a b. Escribimos $a \not| b$ cuando a no divide a b.

Observación 3.1.1 Podemos expresar $a|b$ usando cuantificadores como $\exists c(ac = b)$, donde el universo de discurso es el conjunto de números enteros.

□

En la Figura 3.1, una recta numérica indica qué enteros son divisibles por el entero positivo d.

Ejemplo 3.1.1 Determine si $3|7$ y si $3|12$.

Solución: Vemos que $3 \not| 7$, porque $7/3$ no es un número entero. Por otro lado, $3|12$ porque $12/3 = 4$.

□

Ejemplo 3.1.2 Sean n y d enteros positivos. ¿Cuántos números enteros positivos que no exceden a n son divisibles por d?

Solución: Los enteros positivos divisibles por d son todos los enteros de la forma dk, donde k es un entero positivo.

Así, el número de enteros positivos divisibles por d que no exceden a n es igual al número de enteros k con $0 < dk \leq n$, o con $0 < k \leq n/d$.

Por lo tanto, hay $\lfloor n/d \rfloor$ enteros positivos que no exceden a n y son divisibles por d.

□

Algunas de las propiedades básicas de divisibilidad de números enteros se dan en el Teorema 3.1.1.

Teorema 3.1.1 Sean a, b y c números enteros, donde $a \neq 0$. Entonces

(I) si $a|b$ y $a|c$, entonces $a|(b + c)$;

(II) si $a|b$, entonces $a|bc$ para todos los enteros c;

(III) si $a|b$ y $b|c$, entonces $a|c$.

Demostración: Daremos una prueba directa de (I). Suponga que $a|b$ y $a|c$. Entonces, de la definición de divisibilidad, se deduce que hay números enteros s y t con $b = as$ y $c = at$. Por tanto, $b + c = as + at = a(s + t)$.

Por ello, a divide $b + c$. Esto establece la parte (I) del teorema. Las demostraciones de las partes (II) y (III) se dejan como ejercicios para el lector.

■

El teorema 3.1.1 tiene esta consecuencia útil.

Corolario 3.1.1 Si a, b y c son números enteros, donde $a \neq 0$, tal que $a|b$ y $a|c$, entonces $a|mb + nc$ siempre que m y n sean números enteros.

Demostración: Daremos una prueba directa. Por la parte (II) del Teorema 3.1.1 vemos que $a|mb$ y $a|nc$ siempre que m y n son números enteros. Por la parte (I) del Teorema 3.1.1 se deduce que $a|mb + nc$.

■

3.1.3. El Algoritmo de División

Cuando un número entero se divide por un número entero positivo, hay un cociente y un residuo (o resto), como muestra el algoritmo de división.

Teorema 3.1.2 EL ALGORITMO DE DIVISIÓN Sea a un número entero y d un entero positivo. Entonces hay enteros únicos q y r, con $0 \leq r < d$, tales que $a = dq + r$. ■

Observación 3.1.2 El teorema 3.1.2 no es realmente un algoritmo. (¿Por qué no?) Sin embargo, usaremos su nombre tradicional.

□

Definición 3.1.2 En la igualdad dada en el algoritmo de división, d se llama *divisor*, a se llama *dividendo*, q se llama *cociente* y r se llama *residuo (resto)*. Esta notación se usa para expresar, respectivamente, el cociente y el residuo:

$$q = a \text{ div } d, \qquad\qquad r = a \bmod d.$$

Observación 3.1.3 Tenga en cuenta que tanto a div d como a mod d para un d fijo son funciones en el conjunto de números enteros. Además, cuando a es un número entero y d es un número entero positivo, tenemos a div $d = \lfloor a/d \rfloor$ y $a \bmod d = a - d\lfloor a/d \rfloor$.

□

Los ejemplos 3.1.3 y 3.1.4 ilustran el algoritmo de división.

Ejemplo 3.1.3 ¿Cuáles son el cociente y el resto cuando 101 se divide entre 11?

Solución: Tenemos que

$$101 = 11 \cdot 9 + 2.$$

Por lo tanto, el cociente cuando 101 se divide entre 11 es $9 = 101$ div 11, y el resto es $2 = 101 \bmod 11$.

□

Ejemplo 3.1.4 ¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución: Tenemos

$$-11 = 3(-4) + 1.$$

Por lo tanto, el cociente cuando -11 se divide por 3 es $-4 = -11 \text{ div } 3$, y el residuo es $1 = -11 \bmod 3$. Tenga en cuenta que el resto no puede ser negativo. En consecuencia, el resto no es -2, aunque $-11 = 3(-3)-2$, porque $r = -2$ no satisface $0 \leq r < 3$.

□

Tenga en cuenta que el entero a es divisible por el entero d si y sólo si el resto es cero cuando a se divide por d.

3.1.4. Aritmética Modular

En algunas situaciones, solo nos preocupamos por el resto de un número entero cuando se divide por algún número entero positivo especificado. Por ejemplo, cuando preguntamos qué hora será (en un reloj de 24 horas) dentro de 50 horas, solo nos preocupamos por el resto cuando 50 más la hora actual se divide por 24.

Debido a que a menudo solo nos interesan los restos, tenemos notaciones especiales para ellos. Ya hemos introducido la notación $a \bmod m$ para representar el resto cuando un entero a se divide por el entero positivo m. Introducimos ahora una notación diferente, pero relacionada, que indica que dos enteros tienen el mismo resto cuando se dividen por el entero positivo m.

Definición 3.1.3 Si a y b son números enteros y m es un número entero positivo, entonces a es *congruente con b módulo m* si m divide a $a - b$. Usamos la notación $a \equiv b (\bmod m)$ para indicar que a es congruente con b módulo m. Decimos que $a \equiv b (\bmod m)$ es una **congruencia** y que m es su **módulo**. Si a y b no son congruentes módulo m, escribimos $a \not\equiv b (\bmod m)$.

Aunque ambas notaciones $a \equiv b (\bmod m)$ y $a \bmod m = b$ incluyen "mod", representan conceptos fundamentalmente diferentes. El primero representa una relación en el conjunto de números enteros, mientras que el segundo representa una función. Sin embargo, la relación $a \equiv b (\bmod m)$ y la función mod m están estrechamente relacionadas, como se describe en el Teorema 3.1.3.

Teorema 3.1.3 Sean a y b números enteros y m un número entero positivo. Entonces $a \equiv b(\text{mod } m)$ si y sólo si $a \bmod m = b \bmod m$.

■

La demostración del Teorema 3.1.3 se deja como ejercicio. Recuerde que por la Definición 3.1.2 $a \bmod m$ y $b \bmod m$ son los residuos cuando a y b se dividen por m, respectivamente. En consecuencia, el Teorema 3.1.3 también dice que $a \equiv b(\text{mod } m)$ si y sólo si a y b tienen el mismo resto cuando se dividen por m.

Ejemplo 3.1.5 Determine si 17 es congruente con 5 módulo 6 y si 24 y 14 son congruentes módulo 6.

Solución: Como 6 divide a $17 - 5 = 12$, vemos que $17 \equiv 5(\text{mod } 6)$. Sin embargo, debido a que $24 - 14 = 10$ no es divisible entre 6, vemos que $24 \not\equiv 14(\text{mod } 6)$. □

El gran matemático alemán Karl Friedrich Gauss desarrolló el concepto de congruencias a finales del siglo XVIII. La noción de congruencias ha jugado un papel importante en el desarrollo de la teoría de números.

El Teorema 3.1.4 proporciona una forma útil de trabajar con congruencias.

Teorema 3.1.4 Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Prueba: Si $a \equiv b(\text{mod } m)$, por la definición de congruencia (Definición 3.1.3), sabemos que $m|(a - b)$. Esto significa que hay un entero k tal que $a - b = km$, de modo que $a = b + km$. Por el contrario, si hay un número entero k tal que $a = b + km$, entonces $km = a - b$. Por tanto, m divide a $a - b$, de modo que $a \equiv b(\text{mod } m)$. ■

El conjunto de todos los números enteros congruentes con un número entero módulo m se denomina la clase de congruencia de un módulo m. En el capítulo 2 mostramos que hay m clases de equivalencia disjuntas por pares módulo m y que la unión de estas clases de equivalencia es el conjunto de enteros.

El teorema 3.1.5 muestra que las sumas y multiplicaciones preservan las congruencias.

Teorema 3.1.5 Sea m un entero positivo. Si $a \equiv b(\text{mod } m)$ y $c \equiv d(\text{mod } m)$, entonces

$$a + c \equiv b + d(\text{mod } m)$$

y

$$ac \equiv bd(\text{mod } m).$$

Prueba: Haremos una prueba directa. Debido a que $a \equiv b(\text{mod } m)$ y $c \equiv d(\text{mod } m)$, según el Teorema 3.1.4 hay números enteros s y t con $b = a + sm$ y $d = c + tm$. Por lo tanto,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

y

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Por ello,

$$a + c \equiv b + d(\text{mod } m)$$

y

$$ac \equiv bd(\text{mod } m).$$

■

Ejemplo 3.1.6 Dado que $7 \equiv 2(\text{mod } 5)$ y $11 \equiv 1(\text{mod } 5)$, del Teorema 3.1.5 se sigue que

$$18 = 7 + 11 \equiv 2 + 1 = 3(\text{mod } 5)$$

y que

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2(\text{mod } 5).$$

□

Debemos tener cuidado al trabajar con congruencias. Algunas propiedades que podemos esperar que sean verdaderas no son válidas. Por ejemplo, si $ac \equiv bc(\text{mod } m)$, la congruencia $a \equiv b(\text{mod } m)$ puede ser falsa. De manera similar, si $a \equiv b(\text{mod } m)$ y $c \equiv d(\text{mod } m)$, la congruencia

$$a^c \equiv b^d(\text{mod } m)$$

puede ser falsa.

El corolario 3.1.2 muestra cómo encontrar los valores de la función mod m para la suma y el producto de dos enteros usando los valores de esta función en cada uno de estos enteros.

Corolario 3.1.2 Sea m un entero positivo y sean a y b enteros. Entonces

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

y

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Prueba: Por las definiciones de mod m y de congruencia módulo m, sabemos que $a \equiv (a \bmod m)(\bmod m)$ y $b \equiv (b \bmod m)(\bmod m)$. Por lo tanto, el Teorema 3.1.5 nos dice que

$$a + b \equiv (a \bmod m) + (b \bmod m)(\bmod m)$$

y

$$ab \equiv (a \bmod m)(b \bmod m)(\bmod m).$$

Las igualdades en este corolario se derivan de estas dos últimas congruencias del Teorema 3.1.3. ■

Ejemplo 3.1.7 Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución: Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$. Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$. Entonces, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$.

A continuación, tenga en cuenta que $8^4 = 4096$. Como $4096 = 178 \cdot 23 + 2$, tenemos $4096 \bmod 23 = 2$. Por lo tanto, $(19^3 \bmod 31)^4 \bmod 23 = 2$.

□

3.1.5. Aritmética Módulo m

Podemos definir operaciones aritméticas en $\mathbb{Z}_m$, el conjunto de enteros no negativos menores que m, es decir, el conjunto $\{0, 1, \ldots, m-1\}$. En particular, definimos la suma de estos números enteros, denotados por $+_m$ por

$$a +_m b = (a + b) \bmod m,$$

donde la suma en el lado derecho de esta ecuación es la suma ordinaria de enteros, y definimos la multiplicación de estos enteros, denotada por $\cdot_m$ por

$$a \cdot_m b = (a \cdot b) \bmod m,$$

donde la multiplicación del lado derecho de esta ecuación es la multiplicación ordinaria de números enteros. Las operaciones $+_m$ y $\cdot_m$ se llaman suma y multiplicación módulo m y cuando usamos estas operaciones, se dice que estamos haciendo **aritmética módulo m**.

Ejemplo 3.1.8 Use la definición de suma y multiplicación en $\mathbb{Z}_m$ para hallar $7 +_{11} 9$ y $7 \cdot_{11} 9$.

Solución: Usando la definición de suma módulo 11, encontramos que

$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$$

y

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$$

Por tanto, $7 +_{11} 9 = 5$ y $7 \cdot_{11} 9 = 8$. □

Las operaciones $+_m$ y $\cdot_m$ satisfacen muchas de las mismas propiedades de la suma y multiplicación ordinarias de números enteros. En particular, satisfacen estas propiedades:

Cerradura Si a y b pertenecen a $\mathbb{Z}_m$, entonces $a +_m b$ y $a \cdot_m b$ pertenecen a $\mathbb{Z}_m$.

Asociatividad Si a, b y c pertenecen a $\mathbb{Z}_m$, entonces $(a +_m b) +_m c = a +_m (b +_m c)$ y $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Conmutatividad Si a y b pertenecen a $\mathbb{Z}_m$, entonces $a +_m b = b +_m a$ y $a \cdot_m b = b \cdot_m a$.

Elementos identidad Los elementos 0 y 1 son los elementos identidad para la suma y la multiplicación módulo m, respectivamente. Es decir, si a pertenece a $\mathbb{Z}_m$, entonces $a +_m 0 = 0 +_m a = a$ y $a \cdot_m 1 = 1 \cdot_m a = a$.

Inversos aditivos Si $a \neq 0$ pertenece a $\mathbb{Z}_m$, entonces $m - a$ es un inverso aditivo de a módulo m y 0 es su propio inverso aditivo, es decir, $a +_m (m - a) = 0$ y $0 +_m 0 = 0$.

Distributividad Si a, b y c pertenecen a $\mathbb{Z}_m$, entonces $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ y $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Observación 3.1.4 Usaremos las notaciones $+$ y $\cdot$ para $+_m$ y $\cdot_m$, sin el subíndice m en el símbolo para el operador, siempre que trabajemos con $\mathbb{Z}_m$. □

3.1.6. Ejercicios

1. ¿17 divide a cada uno de estos números?

   a) 68 *b*) 84 *c*) 357 *d*) 1001

2. Demuestre las partes (II) y (III) del Teorema 3.1.1.

3. Demuestre que si a, b, c y d son enteros, con $a \neq 0$ y $b \neq 0$, tal que $a|c$ y $b|d$ entonces $ab|cd$.

4. ¿Cuál es el cociente y el residuo cuando

   a) 19 es dividido por 7?
   b) -111 es dividido por 11?
   c) 789 es dividido por 23?
   d) 0 es dividido por 19?
   e) -1 es dividido por 3r?
   f) 1001 es dividido por 13?
   g) 3 es dividido por 5?
   h) 4 es dividido por 1?

5. ¿Qué hora marcará un reloj de 12 horas

   a) 80 horas después de que marca las 11:00?
   b) 40 horas después de que marca las 12:00?
   c) 100 horas después de que marca las 6:00?

6. Decida si cada uno de estos números enteros es congruente con 3 módulo 7.

   a) 37 *b*) 66 *c*) -17 *d*) -67

7. Encuentre cada uno de los siguientes valores.

   a) $(19^2 \bmod 41) \bmod 9$
   b) $(32^3 \bmod 13)^2 \bmod 11$
   c) $(7^3 \bmod 23)^2 \bmod 31$
   d) $(21^2 \bmod 15)^3 \bmod 22$

8. Escriba las tablas de adición y multiplicación para $\mathbb{Z}_6$ (donde por adición y multiplicación queremos decir $+_6$ y $\cdot_6$).

3.2. Primos y Máximo Común Divisor

3.2.1. Introducción

En la sección 3.1 estudiamos el concepto de divisibilidad de números enteros. Un concepto importante basado en la divisibilidad es el de un número primo. Un primo es un número entero mayor que 1 que no es divisible por ningún entero positivo que no sea 1 y él mismo.

El estudio de los números primos se remonta a la antigüedad. Hace miles de años se sabía que hay infinitos números primos; la prueba de este hecho, que se encuentra en las obras de Euclides, es famosa por su elegancia y belleza.

Describiremos algunos de los resultados sobre números primos encontrados por matemáticos en los últimos 400 años. En particular, presentaremos un teorema importante, el teorema fundamental de la aritmética. Este teorema, que afirma que todo entero positivo puede escribirse de forma única como producto de números primos en orden no decreciente, tiene muchas consecuencias interesantes.

En esta sección también estudiaremos el máximo común divisor de dos enteros, así como el mínimo común múltiplo de dos enteros. Desarrollaremos un algoritmo importante para calcular los máximos divisores comunes, llamado algoritmo euclidiano.

3.2.2. Números Primos

Todo entero mayor que 1 es divisible por al menos dos enteros, porque un entero positivo es divisible por 1 y por sí mismo. Los números enteros positivos que tienen exactamente dos factores enteros positivos diferentes se denominan números **primos**.

Definición 3.2.1 Un entero p mayor que 1 se llama *primo* si los únicos factores positivos de p son 1 y p. Un número entero positivo que es mayor que 1 y no es primo se llama *compuesto*.

Observación 3.2.1 El número entero 1 no es primo porque sólo tiene un factor positivo. Tenga en cuenta también que un número entero n es compuesto si y sólo si existe un número entero a tal que $a|n$ y $1 < a < n$.

□

Ejemplo 3.2.1 El número entero 7 es primo porque sus únicos factores positivos son 1 y 7, mientras que el número entero 9 es compuesto porque es divisible por 3.

□

Los números primos son los componentes básicos de los números enteros positivos, como muestra el teorema fundamental de la aritmética.

Teorema 3.2.1 TEOREMA FUNDAMENTAL DE LA ARITMÉTICA Todo número entero mayor que 1 puede escribirse únicamente como un primo o como el producto de dos o más primos, donde los factores primos se escriben en orden de tamaño no decreciente. ■

El ejemplo 3.2.2 da algunas factorizaciones primas de números enteros.

Ejemplo 3.2.2

$$\begin{aligned} 100 &= 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2, \\ 641 &= 641, \\ 999 &= 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37, \\ 1024 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}. \end{aligned}$$

□

3.2.3. División por Ensayo

A menudo es importante mostrar que un número entero dado es primo. Por ejemplo, en criptología, los números primos grandes se utilizan en algunos métodos para hacer que los mensajes sean secretos. Un procedimiento para demostrar que un número entero es primo se basa en la siguiente observación.

Teorema 3.2.2 Si n es un entero compuesto, entonces n tiene un divisor primo menor o igual que $\sqrt{n}$.

Demostración: Si n es compuesto, por la definición de un entero compuesto, sabemos que tiene un factor a con $1 < a < n$. Por lo tanto, por la definición de un factor de un entero positivo, tenemos $n = ab$, donde b es un entero positivo mayor que 1.

Demostraremos que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$. Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es una contradicción. En consecuencia, $a \leq \sqrt{n}$

o $b \leq \sqrt{n}$. Debido a que tanto a como b son divisores de n, vemos que n tiene un divisor positivo que no excede a $\sqrt{n}$. Este divisor es primo o, por el teorema fundamental de la aritmética, tiene un divisor primo menor que él. En cualquier caso, n tiene un divisor primo menor o igual que $\sqrt{n}$.

■

Del teorema 3.2.2 se deduce que un número entero es primo si no es divisible por ningún primo menor o igual que su raíz cuadrada. Esto conduce al algoritmo de fuerza bruta conocido como **división por ensayo**. Para usar la división por ensayo, dividimos n por todos los primos que no excedan a $\sqrt{n}$ y concluimos que n es primo si no es divisible por ninguno de estos primos. En el Ejemplo 3.2.3 usamos la división por ensayo para mostrar que 101 es primo.

Ejemplo 3.2.3 Muestre que 101 es primo.

Solución: Los únicos números primos que no exceden a $\sqrt{101}$ son 2, 3, 5 y 7. Dado que 101 no es divisible entre 2, 3, 5 o 7 (el cociente de 101 y cada uno de estos números enteros no es un número entero), se sigue que 101 es primo.

□

Debido a que cada entero tiene una factorización prima, sería útil tener un procedimiento para encontrar esta factorización prima. Considere el problema de encontrar la factorización prima de n.

Comience por dividir n entre primos sucesivos, comenzando con el primo más pequeño, 2. Si n tiene un factor primo, entonces por el Teorema 3.2.2 se encontrará un factor primo p que no exceda a $\sqrt{n}$.

Así, si no se encuentra un factor primo que no exceda a $\sqrt{n}$, tenemos que n es primo. De otro modo si se encuentra un factor primo p, continue factorizando n/p. Tenga en cuenta que n/p no tiene factores primos menores que p.

Nuevamente, si n/p no tiene un factor primo mayor o igual a p y que no excede a su raíz cuadrada, entonces es primo. De lo contrario, si tiene un factor primo q, continúe factorizando $n/(pq)$. Este procedimiento se continúa hasta que la factorización se ha reducido a un primo. Este procedimiento se ilustra en el Ejemplo 3.2.4.

Ejemplo 3.2.4 Encuentre la factorización prima de 7007.

Solución: Para encontrar la factorización prima de 7007, primero realice divisiones de 7007 entre números primos sucesivos, comenzando con 2. Ninguno de los primos 2, 3 y 5 divide 7007. Sin embargo, 7 divide 7007, con $7007/7 = 1001$.

A continuación, divida 1001 entre primos sucesivos, comenzando con 7. Se ve inmediatamente que 7 también divide 1001, porque $1001/7 = 143$. Continúe dividiendo 143 entre primos sucesivos, comenzando con 7. Aunque 7 no divide 143, 11 divide 143 y $143/11 = 13$. Como 13 es primo, el procedimiento se completa.

De ello se deduce que $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. En consecuencia, la factorización prima de 7007 es $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

□

Los números primos se estudiaron en la antigüedad por razones filosóficas. Hoy en día, existen razones muy prácticas para su estudio. En particular, los números primos grandes juegan un papel crucial en la criptografía.

3.2.4. La Criba de Eratóstenes

Tenga en cuenta que los números enteros compuestos que no excedan 100 deben tener un factor primo que no exceda 10. Debido a que los únicos números primos menores que 10 son 2, 3, 5 y 7, los números primos que no exceden 100 son estos cuatro primos y los números enteros positivos mayores que 1 que no exceden a 100 que no son divisibles por 2, 3, 5, o 7.

La criba de Eratóstenes se usa para encontrar todos los números primos que no excedan un número entero positivo especificado. Por ejemplo, el siguiente procedimiento se usa para encontrar los números primos que no excedan 100. Comenzamos con la lista de todos los números enteros entre 1 y 100.

Para comenzar el proceso de cribado, se eliminan los números enteros que son divisibles por 2, distintos de 2. Debido a que 3 es el primer número entero mayor que 2 que queda, se eliminan todos los números enteros divisibles por 3 que no sean 3. Como 5 es el siguiente número entero que queda después de 3, se eliminan los números enteros divisibles por 5 que no sean 5. El siguiente número entero que queda es 7, por lo que se eliminan los números enteros divisibles por 7 que no sean 7.

Debido a que todos los números enteros compuestos que no excedan de 100 son divisibles entre 2, 3, 5 o 7, todos los números enteros restantes excepto

1 son primos. En la Tabla 3.1, los paneles muestran los números enteros eliminados en cada etapa, donde cada entero divisible por 2, distinto de 2, está subrayado en el primer panel, cada entero divisible por 3, distinto de 3, está subrayado en el segundo panel, cada el entero divisible por 5, distinto de 5, está subrayado en el tercer panel, y cada entero divisible por 7, distinto de 7, está subrayado en el cuarto panel.

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabla 3.1: La criba de Eratóstenes para los primos menores que 100.

Los números enteros no subrayados son los números primos que no superan 100. Concluimos que los números primos menores a 100 son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

LA INFINITUD DE PRIMOS Se sabe desde hace mucho tiempo que

hay infinitos números primos. Esto significa que siempre que $p_1, p_2, \ldots, p_n$ son los n primos más pequeños, sabemos que hay un primo mayor que no aparece en la lista.

Demostraremos este hecho usando una demostración dada por Euclides en su famoso texto de matemáticas, *Los Elementos*. Muchos matemáticos consideran que esta demostración simple, pero elegante, se encuentra entre las demostraciones más hermosas de las matemáticas.

Es la primera prueba presentada en el libro *Proofs from THE BOOK*, donde EL LIBRO se refiere a la colección imaginaria de pruebas perfectas que el legendario matemático Paul Erdős afirma que Dios mantiene. Por cierto, hay una gran cantidad de pruebas diferentes de que hay una infinidad de números primos, y se publican nuevas con una frecuencia sorprendente.

Teorema 3.2.3 Hay infinitos números primos.

Demostración: Probaremos este teorema usando una prueba por contradicción. Suponemos que sólo hay un número finito de primos, $p_1, p_2, \ldots, p_n$. Sea

$$Q = p_1 p_2 \cdots p_n + 1.$$

Según el teorema fundamental de la aritmética, Q es primo o puede escribirse como el producto de dos o más primos. Sin embargo, ninguno de los primos p_j divide a Q, porque si $p_j|Q$, entonces p_j divide $Q - p_1 p_2 \cdots p_n = 1$, por lo tanto, hay un primo que no está en la lista $p_1, p_2, \ldots, p_n$. Este primo o es Q, si es primo, o un factor primo de Q. Esto es una contradicción porque asumimos que hemos enumerado todos los números primos. En consecuencia, hay infinitos números primos.

■

Observación 3.2.2 ¡Tenga en cuenta que en esta demostración no declaramos que Q sea primo! Además, en esta prueba, hemos dado una prueba de existencia no constructiva de que dados n números primos, hay un primo que no está en esta lista. Para que esta demostración sea constructiva, habríamos tenido que dar explícitamente un primo que no esté en nuestra lista original de n primos.

□

Debido a que hay infinitos números primos, dado cualquier entero positivo hay primos mayores que este número entero. Hay una búsqueda en curso para descubrir números primos cada vez más grandes; durante casi todos los

últimos 300 años, el número primo más grande conocido ha sido un número entero de la forma especial $2^p - 1$, donde p también es primo. (Tenga en cuenta que $2^n - 1$ no puede ser primo cuando n no es primo.)

Estos números primos se llaman números primos de Mersenne, en honor al monje francés Marin Mersenne, que los estudió en el siglo XVII. La razón por la que el número primo más grande conocido suele ser un número primo de Mersenne es que existe una prueba extremadamente eficiente, conocida como prueba de Lucas-Lehmer, para determinar si $2^p - 1$ es primo. Además, actualmente no es posible probar tan rápido si son primos números que no sean de esta u otras formas especiales.

Ejemplo 3.2.5 Los números $2^2-1 = 3$, $2^3-1 = 7$, $2^5-1 = 31$ y $2^7-1 = 127$ son números primos de Mersenne, mientras que $2^{11} - 1 = 2047$ no es un número primo de Mersenne porque $2047 = 23 \cdot 89$.

□

3.2.5. Máximo Común Divisor y Mínimo Común Múltiplo

El número entero más grande que divide dos enteros se llama el **máximo común divisor** de estos números enteros.

Definición 3.2.2 Sean a y b enteros, no ambos cero. El entero más grande d tal que $d|a$ y $d|b$ se llama el *máximo común divisor* de a y b. El máximo común divisor de a y b se denota por $\text{mcd}(a, b)$.

El máximo común divisor de dos enteros, no ambos cero, existe porque el conjunto de divisores comunes de estos enteros no es vacío y es finito. Una forma de encontrar el máximo común divisor de dos enteros es encontrar todos los divisores comunes positivos de ambos enteros y luego tomar el mayor divisor. Esto se hace en los Ejemplos 3.2.6 y 3.2.7. Más adelante, se dará un método más eficiente para encontrar el máximo común divisor de dos enteros.

Ejemplo 3.2.6 ¿Cuál es el máximo común divisor de 24 y 36?

Solución: Los divisores comunes positivos de 24 y 36 son 1, 2, 3, 4, 6 y 12. Por lo tanto, $\text{mcd}(24, 36) = 12$. □

Ejemplo 3.2.7 ¿Cuál es el máximo común divisor de 17 y 22?

Solución: Los números enteros 17 y 22 no tienen divisores comunes positivos distintos de 1, de modo que $\text{mcd}(17, 22) = 1$. □

Debido a que a menudo es importante especificar que dos números enteros no tienen un divisor positivo común distinto de 1, tenemos la Definición 3.2.3.

Definición 3.2.3 Los números enteros a y b son *primos relativos* si su máximo común divisor es 1.

Ejemplo 3.2.8 Del ejemplo 3.2.7 se deduce que los números enteros 17 y 22 son primos relativos, porque $\text{mcd}(17, 22) = 1$. □

Debido a que a menudo necesitamos especificar que no hay dos números enteros en un conjunto de números enteros que tengan un divisor positivo común mayor que 1, hacemos la Definición 3.2.4.

Definición 3.2.4 Los enteros $a_1, a_2, \ldots, a_n$ son *primos relativos por pares* si $\text{mcd}(a_i, a_j) = 1$ siempre que $1 \leq i < j \leq n$.

Ejemplo 3.2.9 Determine si los números enteros 10, 17 y 21 son primos relativos por pares y si los números enteros 10, 19 y 24 son primos relativos por pares.

Solución: Como $\text{mcd}(10, 17) = 1$, $\text{mcd}(10, 21) = 1$ y $\text{mcd}(17, 21) = 1$, concluimos que 10, 17 y 21 son primos relativos por pares.

Como $\text{mcd}(10, 24) = 2 > 1$, vemos que 10, 19 y 24 no son primos relativos por pares.

□

Otra forma de encontrar el máximo común divisor de dos números enteros positivos es usar las factorizaciones primas de estos números enteros. Suponga que las factorizaciones primas de los enteros positivos a y b son

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

donde cada exponente es un número entero no negativo, y donde todos los números primos que ocurren en la factorización prima de a o b se incluyen en ambas factorizaciones, con exponentes cero si es necesario.

Entonces $\text{mcd}(a, b)$ viene dado por

$$\text{mcd}(a, b) = p_1^{\text{mín}(a_1,b_1)} p_2^{\text{mín}(a_2,b_2)} \cdots p_n^{\text{mín}(a_n,b_n)},$$

donde $\text{mín}(x, y)$ representa el mínimo de los dos números x y y.

Para demostrar que esta fórmula para $\text{mcd}(a, b)$ es válida, debemos mostrar que el número entero del lado derecho divide tanto a a como a b, y que ningún entero más grande lo hace.

Este número entero divide a a y a b, porque la potencia de cada primo en la factorización no excede la potencia de este primo ni en la factorización de a ni en la de b. Además, ningún número entero mayor puede dividir a y b, porque los exponentes de los números primos en esta factorización no se pueden aumentar y no se pueden incluir otros números primos.

Ejemplo 3.2.10 Debido a que las factorizaciones primas de 120 y 500 son $120 = 2^3 \cdot 3 \cdot 5$ y $500 = 2^2 \cdot 5^3$, el máximo común divisor es

$$\text{mcd}(120, 500) = 2^{\text{mín}(3,2)} 3^{\text{mín}(1,0)} 5^{\text{mín}(1,3)} = 2^2 3^0 5^1 = 20.$$

□

Las factorizaciones primas también se pueden usar para encontrar el **mínimo común múltiplo** de dos números enteros.

Definición 3.2.5 El *mínimo común múltiplo* de los enteros positivos a y b es el menor entero positivo que es divisible por a y b. El mínimo común múltiplo de a y b se denota mediante el $\text{mcm}(a, b)$.

El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b no está vacío (porque ab pertenece a este conjunto, por ejemplo), y cada conjunto no vacío de enteros positivos tiene un elemento mínimo (por la propiedad del buen orden). Suponga que las factorizaciones primas de a y b son las mismas que antes. Entonces el mínimo común múltiplo de a y b viene dado por

$$\text{mcm}(a, b) = p_1^{\text{máx}(a_1,b_1)} p_2^{\text{máx}(a_2,b_2)} \cdots p_n^{\text{máx}(a_n,b_n)},$$

donde $\text{máx}(x, y)$ denota el máximo de los dos números x y y. Esta fórmula es válida porque un múltiplo común de a y b tiene al menos $\text{máx}(a_i, b_i)$ factores de p_i en su factorización prima, y el mínimo común múltiplo no tiene otros factores primos además de los de a y b.

Ejemplo 3.2.11 ¿Cuál es el mínimo común múltiplo de $2^3 3^5 7^2$ y $2^4 3^3$?
Solución: Tenemos que

$$\text{mcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\text{máx}(3,4)} 3^{\text{máx}(5,3)} 7^{\text{máx}(2,0)} = 2^4 3^5 7^2.$$

□

El teorema 3.2.4 da la relación entre el máximo común divisor y el mínimo común múltiplo de dos números enteros. Se puede probar usando las fórmulas que hemos derivado para estas cantidades. La demostración de este teorema se deja como ejercicio.

Teorema 3.2.4 Sean a y b enteros positivos. Entonces

$$ab = \text{mcd}(a, b) \cdot \text{mcm}(a, b).$$

■

3.2.6. El Algoritmo de Euclides

Calcular el máximo común divisor de dos números enteros directamente a partir de las factorizaciones primas de estos números enteros es ineficaz. La razón es que lleva mucho tiempo encontrar las factorizaciones primas.

Daremos un método más eficiente para encontrar el máximo común divisor, llamado algoritmo euclidiano. Este algoritmo se conoce desde la antigüedad. Lleva el nombre del antiguo matemático griego Euclides, quien incluyó una descripción de este algoritmo en su libro *Los elementos*.

Antes de describir el algoritmo euclidiano, mostraremos cómo se usa para encontrar $\text{mcd}(91, 287)$. Primero, divida 287, el mayor de los dos enteros, por 91, el menor, para obtener

$$287 = 91 \cdot 3 + 14.$$

Cualquier divisor de 91 y 287 también debe ser un divisor de $287 - 91 \cdot 3 = 14$. Además, cualquier divisor de 91 y 14 también debe ser un divisor de $287 = 91 \cdot 3 + 14$. Por lo tanto, el máximo común divisor de 91 y 287 es el mismo que el máximo común divisor de 91 y 14. Esto significa que el problema de encontrar $\text{mcd}(91, 287)$ se ha reducido al problema de encontrar $\text{mcd}(91, 14)$.

Luego, divida 91 entre 14 para obtener

$$91 = 14 \cdot 6 + 7.$$

Debido a que cualquier divisor común de 91 y 14 también divide $91 - 14 \cdot 6 = 7$ y cualquier divisor común de 14 y 7 divide 91, se deduce que $\text{mcd}(91, 14) = \text{mcd}(14, 7)$.

Continúe dividiendo 14 entre 7, para obtener

$$14 = 7 \cdot 2.$$

Como 7 divide 14, se deduce que $\text{mcd}(14, 7) = 7$. Además, dado que

$$\text{mcd}(287, 91) = \text{mcd}(91, 14) = \text{mcd}(14, 7) = 7,$$

el problema original se ha resuelto.

Ahora describimos cómo funciona el algoritmo euclidiano en general. Usaremos divisiones sucesivas para reducir el problema de encontrar el máximo común divisor de dos enteros positivos al mismo problema con enteros más pequeños, hasta que uno de los enteros sea cero.

El algoritmo euclidiano se basa en el siguiente resultado sobre el máximo común divisor y el algoritmo de división.

Lema 3.2.1 Sea $a = bq + r$, donde a, b, q y r son números enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración: Si podemos demostrar que los divisores comunes de a y b son los mismos que los divisores comunes de b y r, habremos demostrado que $\text{mcd}(a, b) = \text{mcd}(b, r)$, porque ambos pares deben tener el mismo máximo común divisor.

Entonces, suponga que d divide a a y b. Así, se deduce que d también divide $a - bq = r$ (del Teorema 3.1.1). Por tanto, cualquier divisor común de a y b es también divisor común de b y r.

Asimismo, suponga que d divide a b y r. Entonces d también divide $bq + r = a$. Por tanto, cualquier divisor común de b y r es también un divisor común de a y b.

En consecuencia, $\text{mcd}(a, b) = \text{mcd}(b, r)$.

■

Suponga que a y b son números enteros positivos con $a \geq b$. Sea $r_0 = a$ y $r_1 = b$. Cuando aplicamos sucesivamente el algoritmo de división, obtenemos

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_1 + r_3 & 0 \leq r_3 < r_2, \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n \end{aligned}$$

Finalmente, se produce un resto de cero en esta secuencia de divisiones sucesivas, porque la secuencia de restos $a = r_0 > r_1 > r_2 > \cdots \geq 0$ no puede contener más de a términos. Además, del Lema 3.2.1 se sigue que

$$\begin{aligned} \text{mcd}(a, b) &= \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \cdots = \text{mcd}(r_{n-2}, r_{n-1}) \\ &= \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, 0) = r_n. \end{aligned}$$

Por tanto, el máximo común divisor es el último resto distinto de cero en la secuencia de divisiones.

Ejemplo 3.2.12 Encuentre el máximo común divisor de 414 y 662 usando el algoritmo euclidiano.

Solución: Los usos sucesivos del algoritmo de división dan:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41. \end{aligned}$$

Por lo tanto, $\text{mcd}(414, 662) = 2$, porque 2 es el último resto distinto de cero. Podemos resumir estos pasos en forma de tabla. □

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	2	41	0

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return x{gcd(a, b) is x}
```

Algoritmo 2: Algoritmo Euclideano para calcular $\text{mcd}(a, b)$.

El algoritmo euclidiano se expresa en pseudocódigo en el Algoritmo 2.

En el algoritmo 2, los valores iniciales de x y y son a y b, respectivamente. En cada etapa del procedimiento, x se reemplaza por y, y y se reemplaza por x mod y, que es el resto cuando x se divide por y. Este proceso se repite siempre que $y \neq 0$. El algoritmo termina cuando $y = 0$, y el valor de x en ese punto, el último resto distinto de cero en el procedimiento, es el máximo común divisor de a y b.

3.2.7. Ejercicios

1. Determine si cada uno de estos números enteros es primo.

   a) 19 *b*) 93 *c*) 107 *d*) 27 *e*) 101 *f*) 113

2. Encuentre la factorización prima de cada uno de estos números enteros.

   a) 39 *b*) 81 *c*) 101 *d*) 143 *e*) 289 *f*) 899

3. ¿Qué números enteros positivos menores que 12 son primos relativos a 12?

4. Determine si los números enteros de cada uno de estos conjuntos son primos relativos por pares.

   a) 11, 15, 19
   b) 14, 15, 21
   c) 12, 17, 31, 37
   d) 7, 8, 9, 11

5. ¿Cuáles son los máximos comunes divisores de estos pares de números enteros?

   a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$
   b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
   c) $23^{31}, 23^{17}$
   d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
   e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
   f) $1111, 0$

6. ¿Cuál es el mínimo común múltiplo de cada par en el ejercicio 5?

7. Encuentre $\text{mcd}(1000, 625)$ y $\text{mcm}(1000, 625)$ y verifique que

$$\text{mcd}(1000, 625) \cdot \text{mcm}(1000, 625) = 1000 \cdot 625.$$

8. Utilice el algoritmo euclidiano para encontrar

   a) $\text{mcd}(12, 18)$
   b) $\text{mcd}(111, 201)$
   c) $\text{mcd}(1001, 1331)$
   d) $\text{mcd}(12345, 54321)$
   e) $\text{mcd}(1000, 5040)$
   f) $\text{mcd}(9888, 6060)$

Capítulo 4

Combinatoria

La combinatoria, el estudio de la disposición de objetos, es una parte importante de las matemáticas discretas. Este tema se estudió ya en el siglo XVII, cuando surgieron cuestiones de combinación en el estudio de los juegos de azar. La enumeración, el conteo de objetos con ciertas propiedades, es una parte importante de la combinatoria. Debemos contar objetos para resolver muchos tipos diferentes de problemas.

Por ejemplo, el conteo se usa para determinar la complejidad de los algoritmos. También es necesario contar para determinar si hay suficientes números de teléfono o direcciones de protocolo de Internet para satisfacer la demanda. Recientemente, ha jugado un papel clave en biología matemática, especialmente en la secuenciación del ADN. Además, las técnicas de conteo se utilizan ampliamente cuando se calculan las probabilidades de eventos.

Las reglas básicas de conteo, que estudiaremos en la sección **??**, pueden resolver una gran variedad de problemas. Por ejemplo, podemos usar estas reglas para enumerar los diferentes números de teléfono posibles en los Estados Unidos, las contraseñas permitidas en un sistema informático y los diferentes órdenes en los que pueden terminar los corredores en una carrera.

Otra herramienta combinatoria importante es el principio del casillero, que estudiaremos en la Sección **??**. Esto establece que cuando los objetos se colocan en cajas y hay más objetos que cajas, entonces hay una caja que contiene al menos dos objetos.

Por ejemplo, podemos usar este principio para mostrar que entre un grupo de 15 o más estudiantes, al menos 3 nacieron el mismo día de la semana. Podemos formular muchos problemas de conteo en términos de arreglos ordenados o desordenados de los objetos de un conjunto con o sin repeticiones.

Estos arreglos, llamados permutaciones y combinaciones, se utilizan en muchos problemas de conteo. Por ejemplo, supongamos que se invita a un banquete a los 100 primeros clasificados en un examen competitivo realizado por 2000 estudiantes. Podemos contar los posibles conjuntos de 100 alumnos que serán invitados, así como las formas en las que se pueden otorgar los 10 primeros premios.

Otro problema de la combinatoria implica generar todas las combinaciones de un tipo específico. Esto suele ser importante en las simulaciones por computadora. Idearemos algoritmos para generar combinaciones de varios tipos.

4.1. Los Fundamentos del Conteo

4.1.1. Introducción

Suponga que una contraseña en un sistema de computadora consta de seis, siete u ocho caracteres. Cada uno de estos caracteres debe ser un dígito o una letra del alfabeto. Cada contraseña debe contener al menos un dígito. ¿Cuántas contraseñas de este tipo existen? En esta sección se presentarán las técnicas necesarias para responder esta pregunta y una amplia variedad de otros problemas de conteo.

Los problemas de conteo surgen a lo largo de las matemáticas y las ciencias de la computación. Por ejemplo, debemos contar los resultados exitosos de los experimentos y todos los resultados posibles de estos experimentos para determinar las probabilidades de eventos discretos.

Necesitamos contar el número de operaciones utilizadas por un algoritmo para estudiar su complejidad en tiempo. Introduciremos las técnicas básicas de conteo en esta sección. Estos métodos sirven como base para casi todas las técnicas de conteo.

4.1.2. Principios Básicos de Conteo

Primero presentamos dos principios básicos de conteo, la **regla del producto** y la **regla de la suma**. Luego, mostraremos cómo se pueden usar para resolver muchos problemas de conteo diferentes.

La regla del producto se aplica cuando un procedimiento se compone de tareas separadas.

LA REGLA DEL PRODUCTO Suponga que un procedimiento se puede dividir en una secuencia de dos tareas. Si hay n_1 formas de realizar la primera tarea y para cada una de estas formas de realizar la primera tarea, hay n_2 formas de realizar la segunda tarea, entonces hay $n_1 n_2$ formas de realizar el procedimiento.

Los ejemplos del 4.1.1 al 4.1.10 muestran cómo se usa la regla del producto.

Ejemplo 4.1.1 Una empresa nueva con sólo dos empleados, Sánchez y Patel, alquila un piso de un edificio con 12 oficinas. ¿De cuántas formas hay para asignar diferentes oficinas a estos dos empleados?

Solución: El procedimiento de asignación de oficinas a estos dos empleados consiste en asignar una oficina a Sánchez, que se puede hacer de 12 formas, luego asignarle una oficina a Patel diferente a la asignada a Sánchez, que se puede hacer de 11 formas. Según la regla del producto, hay $12 \cdot 11 = 132$ formas de asignar oficinas a estos dos empleados.

□

Ejemplo 4.1.2 Las sillas de un auditorio deben etiquetarse con una letra mayúscula en inglés seguida de un número entero positivo que no exceda 100. ¿Cuál es la mayor cantidad de sillas que se pueden etiquetar de manera diferente?

Solución: El procedimiento de etiquetado de una silla consta de dos tareas, a saber, asignar al asiento una de las 26 letras mayúsculas en inglés y luego asignarle uno de los 100 números enteros posibles. La regla del producto muestra que hay $26 \cdot 100 = 2600$ formas diferentes de etiquetar una silla. Por lo tanto, la mayor cantidad de sillas que se pueden etiquetar de manera diferente es 2600.

□

Ejemplo 4.1.3 Hay 32 computadoras en un centro de datos en la nube. Cada una de estas computadoras tiene 24 puertos. ¿Cuántos puertos de computadora diferentes hay en este centro de datos?

Solución: El procedimiento para elegir un puerto consta de dos tareas, primero elegir una computadora y luego elegir un puerto en esta computadora. Debido a que hay 32 formas de elegir la computadora y 24 formas de elegir el puerto sin importar qué computadora se haya seleccionado, la regla del producto muestra que hay $32 \cdot 24 = 768$ puertos.

□

A menudo resulta útil una versión ampliada de la regla del producto. Supongamos que un procedimiento se lleva a cabo realizando las tareas $T_1, T_2, \ldots, T_m$ en secuencia. Si cada tarea $T_i, i = 1, 2, \ldots, m$ se puede realizar de n_i maneras, independientemente de cómo se hayan realizado las tareas anteriores, entonces hay $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ formas de realizar el procedimiento. Esta versión de la regla del producto se puede demostrar por inducción matemática de la regla del producto para dos tareas

Ejemplo 4.1.4 ¿Cuántas cadenas de bits diferentes de longitud siete hay?

Solución: Cada uno de los siete bits se puede elegir de dos maneras, porque cada bit es 0 o 1. Por lo tanto, la regla del producto muestra que hay un total de $2^7 = 128$ cadenas de bits diferentes de longitud siete.

□

Ejemplo 4.1.5 ¿Cuántas placas de matrícula diferentes se pueden hacer si cada placa contiene una secuencia de tres letras en inglés mayúsculas seguidas de tres dígitos (y no se prohíbe ninguna secuencia de letras, incluso si son obscenas)?

Solución: Hay 26 opciones para cada una de las tres letras mayúsculas en inglés y 10 opciones para cada uno de los tres dígitos. Por lo tanto, según el producto, hay un total de $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17,576,000$ posibles placas de matrícula.

□

Ejemplo 4.1.6 Contando funciones ¿Cuántas funciones hay de un conjunto con m elementos a un conjunto con n elementos?

Solución: Una función corresponde a la elección de uno de los n elementos del codominio para cada uno de los m elementos del dominio. Por lo tanto, según la regla del producto, hay $n \cdot n \cdot \cdots \cdot n = n^m$ funciones de un conjunto con m elementos a uno con n elementos. Por ejemplo, hay $5^3 = 125$ funciones diferentes de un conjunto con tres elementos a un conjunto con cinco elementos.

□

Ejemplo 4.1.7 Contando funciones uno a uno ¿Cuántas funciones uno a uno hay de un conjunto con m elementos a uno con n elementos?

Solución: En primer lugar, observe que cuando $m > n$ no hay funciones uno a uno de un conjunto con m elementos a un conjunto con n elementos.

Ahora sea $m \leq n$. Suponga que los elementos del dominio son $a_1, a_2, \ldots, a_m$. Hay n formas de elegir el valor de la función en a_1. Debido a que la función es uno a uno, el valor de la función en a_2 se puede elegir de $n-1$ formas (porque el valor usado para a_1 no se puede usar nuevamente).

En general, el valor de la función en a_k se puede elegir de $n-k+1$ formas. Por la regla del producto, hay $n(n-1)(n-2)\cdots(n-m+1)$ funciones uno a uno de un conjunto con m elementos a uno con n elementos.

Por ejemplo, hay $5 \cdot 4 \cdot 3 = 60$ funciones uno a uno de un conjunto con tres elementos a un conjunto con cinco elementos.

□

Ejemplo 4.1.8 El plan de numeración telefónica El plan de numeración de América del Norte (NANP) especifica el formato de los números de teléfono en los EE. UU., Canadá y muchas otras partes de América del Norte.

Un número de teléfono en este plan consta de 10 dígitos, que se dividen en un código de área de tres dígitos, un código de oficina de tres dígitos y un código de estación de cuatro dígitos. Debido a consideraciones de señalización, existen ciertas restricciones en algunos de estos dígitos.

Para especificar el formato permitido, sea X que denota un dígito que pueda tomar cualquiera de los valores del 0 al 9, N denota un dígito que pueda tomar cualquiera de los valores del 2 al 9, y Y denota un dígito que debe ser un 0 o un 1.

Se discutirán dos planes de numeración, que se denominarán plan antiguo y plan nuevo. El plan anterior, en uso en la década de 1960, ha sido reemplazado por el nuevo plan, pero el rápido crecimiento reciente en la demanda de nuevos números para teléfonos móviles y dispositivos eventualmente hará que incluso este nuevo plan sea obsoleto.

En este ejemplo, las letras utilizadas para representar dígitos sigue las convenciones del Plan de Numeración de América del Norte. Como se mostrará, el nuevo plan permite el uso de más números. En el plan anterior, los formatos del código de área, código de oficina y código de estación son NYX, NNX y XXXX, respectivamente, por lo que los números de teléfono tenían el formato NYX-NNX-XXXX.

En el nuevo plan, los formatos de estos códigos son NXX, NXX y XXXX, respectivamente, por lo que los números de teléfono tienen la forma NXX-NXX-XXXX. ¿Cuántos números de teléfono diferentes de América del Norte son posibles con el plan anterior y con el nuevo plan?

```
k := 0
for i_1 := 1 to n_1
   for i_2 := 1 to n_2
          .
          .
          .
      for i_m := 1 to n_m
          k := k + 1
```

Figura 4.1: Código para el Ejemplo 4.1.9.

Solución: según la regla del producto, hay $8 \cdot 2 \cdot 10 = 160$ códigos de área con formato NYX y $8 \cdot 10 \cdot 10 = 800$ códigos de área con formato NXX.

De manera similar, según la regla del producto, hay $8 \cdot 8 \cdot 10 = 640$ códigos de oficina con formato NNX. La regla del producto también muestra que hay $10 \cdot 10 \cdot 10 \cdot 10 = 10,000$ códigos de estación con formato XXXX.

En consecuencia, aplicando la regla del producto nuevamente, se deduce que bajo el plan anterior hay

$$160 \cdot 640 \cdot 10,000 = 1,024,000,000$$

diferentes números disponibles en Norteamérica.

Bajo el nuevo plan, hay

$$800 \cdot 800 \cdot 10,000 = 6,400,000,000$$

diferentes números disponibles.

□

Ejemplo 4.1.9 ¿Cuál es el valor de k después de que se haya ejecutado el código de la Figura 4.1, donde $n_1, n_2, \ldots, n_m$ son números enteros positivos?

Solución: El valor inicial de k es cero. Cada vez que se atraviesa el bucle anidado, se agrega 1 a k. Sea T_i la tarea de atravesar el $i-$ésimo bucle. Entonces, el número de veces que se atraviesa el bucle es el número de formas de realizar las tareas $T_1, T_2, \ldots, T_m$.

El número de formas de realizar la tarea $T_j, j = 1, 2, \ldots, m$, es n_j, porque el $j-$ésimo bucle se recorre una vez por cada entero i_j con $1 \leq i_j \leq n_j$. Por la regla del producto, se deduce que el bucle anidado se atraviesa $n_1 n_2 \cdots n_m$ veces. Por tanto, el valor final de k es $n_1 n_2 \cdots n_m$.

□

Ejemplo 4.1.10 Conteo de subconjuntos de un conjunto finito Utilice la regla del producto para mostrar que el número de subconjuntos diferentes de un conjunto finito S es $2^{|S|}$.

Solución: Suponga que $S = \{a_1, a_2, \ldots, a_k\}$, así $|S| = k$. Considere que cada $a_i, 1 \leq i \leq k$ puede estar o no en en algún subconjunto de S, por lo tanto tenemos que el número de subconjuntos de S es $\overbrace{2 \cdot 2 \cdot \ \cdots \ \cdot 2}^{k-\text{veces}} = 2^k$. □

La regla del producto a menudo se expresa en términos de conjuntos de esta manera: si $A_1, A_2, \ldots, A_m$ son conjuntos finitos, entonces el número de elementos en el producto cartesiano de estos conjuntos es el producto del número de elementos en cada conjunto. Para relacionar esto con la regla del producto, observe que la tarea de elegir un elemento en el producto cartesiano $A_1 \times A_2 \times \cdots \times A_m$ se realiza eligiendo un elemento en A_1, un elemento en $A_2, \ldots$, y un elemento en A_m. Por la regla del producto se sigue que

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \ \cdots \ \cdot |A_m|.$$

Ejemplo 4.1.11 ADN y genomas La información hereditaria de un organismo vivo se codifica utilizando ácido desoxirribonucleico (ADN) o, en ciertos virus, ácido ribonucleico (ARN). El ADN y el ARN son moléculas extremadamente complejas, con diferentes moléculas que interactúan en una amplia variedad de formas para permitir el proceso de la vida. Para nuestros propósitos, damos sólo la descripción más breve de cómo el ADN y el ARN codifican la información genética.

Las moléculas de ADN constan de dos hebras que constan de bloques conocidos como nucleótidos. Cada nucleótido contiene subcomponentes llamados bases, cada uno de los cuales es adenina (A), citosina (C), guanina (G) o timina (T). Las dos hebras de ADN se mantienen unidas por enlaces de hidrógeno que conectan diferentes bases, el enlace A se conecta sólo con T y el enlace C se conecta sólo con G.

A diferencia del ADN, el ARN es monocatenario y el uracilo (U) reemplaza a la timina como base. Entonces, en el ADN los posibles pares de bases son A-T y C-G, mientras que en el ARN son A-U y C-G. El ADN de una criatura viviente consta de múltiples piezas de ADN que forman cromosomas separados. Un gen es un segmento de una molécula de ADN que codifica una proteína en particular. La totalidad de la información genética de un organismo se denomina genoma.

Las secuencias de bases en el ADN y el ARN codifican largas cadenas de proteínas llamadas aminoácidos. Hay 22 aminoácidos esenciales para los seres humanos. Podemos ver rápidamente que se necesita una secuencia de al menos tres bases para codificar estos 22 aminoácidos diferentes.

En primer lugar, tenga en cuenta que debido a que hay cuatro posibilidades para cada base en el ADN, A, C, G y T, según la regla del producto hay $4^2 = 16 < 22$ secuencias diferentes de dos bases. Sin embargo, hay $4^3 = 64$ secuencias diferentes de tres bases, que proporcionan suficientes secuencias diferentes para codificar los 22 aminoácidos diferentes (incluso después de tener en cuenta que varias secuencias diferentes de tres bases codifican el mismo aminoácido).

El ADN de seres vivos simples como las algas y las bacterias tiene entre 10^5 y 10^7 enlaces, donde cada enlace es una de las cuatro bases posibles. Los organismos más complejos, como insectos, aves y mamíferos, tienen entre 10^8 y 10^{10} enlaces en su ADN. Entonces, según la regla del producto, hay al menos 4^{10^5} secuencias diferentes de bases en el ADN de organismos simples y al menos 4^{10^8} secuencias diferentes de bases en el ADN de organismos más complejos.

Ambos son números increíblemente enormes, lo que ayuda a explicar por qué existe una variabilidad tan tremenda entre los organismos vivos. En las últimas décadas se han desarrollado técnicas para determinar el genoma de diferentes organismos. El primer paso es localizar cada gen en el ADN de un organismo.

La siguiente tarea, llamada secuenciación de genes, es la determinación de la secuencia de enlaces en cada gen. (La secuencia específica de enlaces en estos genes depende del representante individual particular de una especie cuyo ADN se analiza). Por ejemplo, el genoma humano incluye aproximadamente 23.000 genes, cada uno con 1.000 enlaces o más.

Las técnicas de secuenciación de genes aprovechan muchos algoritmos desarrollados recientemente y se basan en numerosas ideas nuevas en combinatoria. Muchos matemáticos e informáticos trabajan en problemas relacionados con los genomas, participando en los campos de rápida evolución de la bioinformática y la biología computacional.

□

Ahora introducimos la regla de la suma.

LA REGLA DE LA SUMA Si una tarea se puede realizar de una de n_1 formas o de una de n_2 formas, donde ninguna del conjunto de n_1 formas es igual que ninguna del conjunto de n_2 formas, entonces hay $n_1 + n_2$ formas de realizar la tarea.

El ejemplo 4.1.12 ilustra como se usa la regla de la suma.

Ejemplo 4.1.12 Suponga que se elige a un miembro de la facultad de matemáticas o un estudiante que se especializa en matemáticas como representante de un comité universitario.

¿Cuántas opciones diferentes hay para este representante si hay 37 miembros de la facultad de matemáticas y 83 especialistas en matemáticas y nadie es a la vez miembro de la facultad y estudiante?

Solución: Hay 37 formas de elegir a un miembro de la facultad de matemáticas y 83 formas de elegir a un estudiante que se especializa en matemáticas.

Elegir a un miembro de la facultad de matemáticas nunca es lo mismo que elegir a un estudiante que se especializa en matemáticas porque nadie es a la vez miembro de la facultad y estudiante. Por la regla de la suma se deduce que hay $37 + 83 = 120$ formas posibles de elegir este representante. □

Podemos extender la regla de la suma a más de dos tareas. Suponga que una tarea se puede realizar de una de n_1 formas, de una de n_2 formas, ..., o de una de n_m formas, donde ninguna de las n_i formas de realizar la tarea es igual a ninguna de las del conjunto de n_j formas, para todos los pares i y j con $1 \leq i < j \leq m$. Entonces, el número de formas de realizar la tarea es $n_1 + n_2 + \cdots + n_m$. Esta versión ampliada de la regla de la suma suele ser útil para contar problemas, como muestran los ejemplos 4.1.13 y 4.1.14.

Ejemplo 4.1.13 Un estudiante puede elegir un proyecto de computadora de una de tres listas. Las tres listas contienen 23, 15 y 19 proyectos posibles, respectivamente. Ningún proyecto está en más de una lista. ¿Cuántos proyectos posibles hay para elegir?

Solución: el estudiante puede elegir un proyecto seleccionando un proyecto de la primera lista, la segunda lista o la tercera lista. Debido a que ningún proyecto está en más de una lista, según la regla de la suma hay $23+15+19 = 57$ formas de elegir un proyecto. □

```
k := 0
for i_1 := 1 to n_1
    k := k + 1
for i_2 := 1 to n_2
    k := k + 1
        .
        .
        .
for i_m := 1 to n_m
    k := k + 1
```

Figura 4.2: Código para el Ejemplo 4.1.14.

Ejemplo 4.1.14 ¿Cuál es el valor de k después de que se haya ejecutado el código de la Figura 4.2, donde $n_1, n_2, \ldots, n_m$ son números enteros positivos?

Solución: El valor inicial de k es cero. Este bloque de código se compone de m bucles diferentes. Cada vez que se atraviesa un bucle, se agrega 1 a k. Para determinar el valor de k después de que se haya ejecutado este código, necesitamos determinar cuántas veces atravesamos un bucle.

Tenga en cuenta que hay n_i formas de atravesar el $i-$ésimo bucle. Debido a que sólo atravesamos un bucle a la vez, la regla de la suma muestra que el valor final de k, que es el número de formas de atravesar los m bucles, es $n_1 + n_2 + \cdots + n_m$.

□

La regla de la suma puede expresarse en términos de conjuntos como: Si $A_1, A_2, \ldots, A_m$ son conjuntos finitos disjuntos por pares, entonces el número de elementos en la unión de estos conjuntos es la suma del número de elementos en los conjuntos.

Para relacionar esto con nuestra afirmación de la regla de la suma, tenga en cuenta que hay $|A_i|$ formas de elegir un elemento de A_i para $i = 1, 2, \ldots, m$. Debido a que los conjuntos son disjuntos por pares, cuando seleccionamos un elemento de uno de los conjuntos A_i, no seleccionamos un elemento de un conjunto diferente A_j.

En consecuencia, por la regla de la suma, debido a que no podemos seleccionar un elemento de dos de estos conjuntos al mismo tiempo, el número de formas de elegir un elemento de uno de los conjuntos, que es el número

de elementos en la unión, es

$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|$ cuando $A_i \cap A_j = \emptyset$ para todo i, j.

Esta igualdad se aplica solo cuando los conjuntos en cuestión son disjuntos por pares. La situación es mucho más complicada cuando estos conjuntos tienen elementos en común.

4.1.3. Problemas de Conteo más Complejos

Muchos problemas de conteo no se pueden resolver usando solo la regla de la suma o solo la regla del producto. Sin embargo, muchos problemas de conteo complicados se pueden resolver usando estas dos reglas en combinación. Comenzamos contando el número de nombres de variables en el lenguaje de programación BASIC. Luego contaremos el número de contraseñas válidas sujetas a un conjunto particular de restricciones.

Ejemplo 4.1.15 En una versión del lenguaje de programación BASIC, el nombre de una variable es una cadena de uno o dos caracteres alfanuméricos, donde no se distinguen mayúsculas y minúsculas. (Un carácter alfanumérico es una de las 26 letras inglesas o uno de los 10 dígitos).

Además, el nombre de una variable debe comenzar con una letra y debe ser diferente de las cinco cadenas de dos caracteres que están reservadas para el uso de programación. ¿Cuántos nombres de variables diferentes hay en esta versión de BASIC?

Solución: Sea V el número de diferentes nombres de variables en esta versión de BASIC. Sea V_1 el número de éstas que tienen un carácter de largo y V_2 el número de éstas que tienen dos caracteres de largo. Luego, por la regla de la suma, $V = V_1 + V_2$. Tenga en cuenta que $V_1 = 26$, porque un nombre de variable de un carácter debe ser una letra. Además, según la regla del producto, hay $26 \cdot 36$ cadenas de longitud dos que comienzan con una letra y terminan con un carácter alfanumérico. Sin embargo, cinco de estos están excluidos, por lo que $V_2 = 26 \cdot 36 - 5 = 931$. Por lo tanto, hay $V = V_1 + V_2 = 26 + 931 = 957$ nombres diferentes para las variables en esta versión de BASIC.

□

Ejemplo 4.1.16 Cada usuario de un sistema informático tiene una contraseña, que tiene de seis a ocho caracteres, donde cada carácter es una letra

mayúscula o un dígito. Cada contraseña debe contener al menos un dígito. ¿Cuántas contraseñas posibles hay?

Solución: Sea P el número total de contraseñas posibles y P_6, P_7 y P_8 denoten el número de contraseñas posibles de longitud 6, 7 y 8, respectivamente. Por la regla de la suma, $P = P_6 + P_7 + P_8$. Ahora encontraremos P_6, P_7 y P_8

. Encontrar P_6 directamente es difícil. Para encontrar P_6, es más fácil encontrar el número de cadenas de letras mayúsculas y dígitos de seis caracteres, incluidas las que no tienen dígitos, y restar de esto el número de cadenas sin dígitos. Según la regla del producto, el número de cadenas de seis caracteres es 366 y el número de cadenas sin dígitos es 266. Por lo tanto,

$$P_6 = 36^6 - 26^6 = 2,176,782,336 - 308,915,776 = 1,867,866,560.$$

Del mismo modo, tenemos

$$P_7 = 36^7 - 26^7 = 78,364,164,096 - 8,031,810,176 = 70,332,353,920$$

y

$$P_8 = 36^8 - 26^8 = 2,821,109,907,456 - 208,827,064,576 = 2,612,282,842,880.$$

Como consecuencia,

$$P = P_6 + P_7 + P_8 = 2,684,483,063,360.$$

□

Ejemplo 4.1.17 Contar direcciones de Internet En Internet, que se compone de redes físicas interconectadas de computadoras, a cada computadora (o más precisamente, a cada conexión de red de una computadora) se le asigna una dirección de Internet. En la versión 4 del Protocolo de Internet (IPv4), todavía en uso hoy, una dirección es una cadena de 32 bits. Comienza con un número de red (netid). El netid va seguido de un número de host (hostid), que identifica a una computadora como miembro de una red en particular.

Se utilizan tres formas de direcciones, con diferentes números de bits utilizados para netids y hostids. Las direcciones de clase A, utilizadas para las redes más grandes, constan de 0, seguido de un netid de 7 bits y un hostid de 24 bits. Las direcciones de clase B, utilizadas para redes de tamaño medio, constan de 10, seguidas de un netid de 14 bits y un hostid de 16 bits. Las

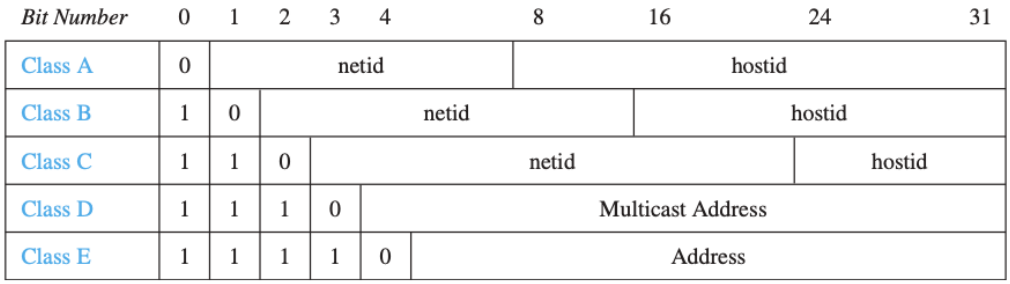


Figura 4.3: Direcciones de Internet (IPv4).

direcciones de clase C, utilizadas para las redes más pequeñas, constan de 110, seguidas de un netid de 21 bits y un hostid de 8 bits.

Existen varias restricciones en las direcciones debido a usos especiales: 1111111 no está disponible como netid de una red de Clase A, y los hostid que consisten en todos los 0 y todos los 1 no están disponibles para su uso en ninguna red. Una computadora en Internet tiene una dirección de Clase A, Clase B o Clase C. (Además de las direcciones de Clase A, B y C, también hay direcciones de Clase D, reservadas para su uso en multidifusión cuando se direccionan varias computadoras a la vez, que constan de 1110 seguidas de 28 bits y direcciones de Clase E, reservadas para uso futuro , que consta de 11110 seguido de 27 bits.

Ni las direcciones de clase D ni de clase E se asignan como dirección IPv4 de una computadora en Internet.) La Figura 4.3 ilustra el direccionamiento IPv4. (Las limitaciones en la cantidad de redes de Clase A y Clase B han hecho que el direccionamiento IPv4 sea inadecuado; IPv6, una nueva versión de IP, utiliza direcciones de 128 bits para resolver este problema). ¿Cuántas direcciones IPv4 diferentes están disponibles para computadoras en Internet?

Solución: Sea x el número de direcciones disponibles para computadoras en Internet y sean x_A, x_B y x_C que denotan el número de direcciones Clase A, Clase B y Clase C disponibles, respectivamente. Por la regla de la suma, $x = x_A + x_B + x_C$.

Para encontrar x_A, tenga en cuenta que hay $2^7 - 1 = 127$ netids Clase A, recordando que el netid 1111111 no está disponible. Para cada netid, hay $2^{24} - 2 = 16,777,214$ hostids, recordando que los hostids que consisten en todos los 0 y todos los 1 no están disponibles. En consecuencia, $x_A = 127 \cdot 16,777,214 = 2,130,706,178$.

Para encontrar x_B y x_C, tenga en cuenta que hay $2^{14} = 16,384$ netids Clase B y $2^{21} = 2,097,152$ netids Clase C. Para cada netid de Clase B, hay $2^{16} - 2 = 65,534$ hostids, y para cada netid de Clase C, hay $2^8 - 2 = 254$ hostids, recordando que en cada red los hostids que consisten en todos los 0 y todos los 1 no están disponibles. En consecuencia, $x_B = 1,073,709,056$ y $x_C = 532,676,608$.

Concluimos que el número total de direcciones IPv4 disponibles es

$$\begin{aligned} x &= x_A + x_B + x_C \\ &= 2,130,706,178 + 1,073,709,056 + 532,676,608 \\ &= 3,737,091,842. \end{aligned}$$

□

4.1.4. La Regla de la Resta (Inclusión-Exclusión para Dos Conjuntos)

Suponga que una tarea se puede realizar de dos formas, pero algunas de las formas de hacerlo son comunes a ambas. En esta situación, no podemos usar la regla de la suma para contar el número de formas de realizar la tarea.

Si sumamos el número de formas de realizar las tareas de estas dos formas, obtenemos un recuento excesivo del número total de formas de hacerlo, porque las formas de realizar la tarea que son comunes a las dos formas se cuentan dos veces.

Para contar correctamente el número de formas de hacer las dos tareas, debemos restar el número de formas que se cuentan dos veces. Esto nos lleva a una importante regla de conteo.

> LA REGLA DE LA RESTA Si una tarea se puede realizar de n_1 formas o de n_2 formas, entonces el número de formas de realizar la tarea es $n_1 + n_2$ menos el número de formas de realizar la tarea que es común a las dos formas diferentes.

La regla de la resta también se conoce como el principio de inclusión-exclusión, especialmente cuando se usa para contar el número de elementos en la unión de dos conjuntos. Suponga que A_1 y A_2 son conjuntos. Luego, hay $|A_1|$ formas de seleccionar un elemento de A_1 y $|A_2|$ formas de seleccionar un elemento de A_2.

El número de formas de seleccionar un elemento de A_1 o de A_2, es decir, el número de formas de seleccionar un elemento de su unión, es la suma del

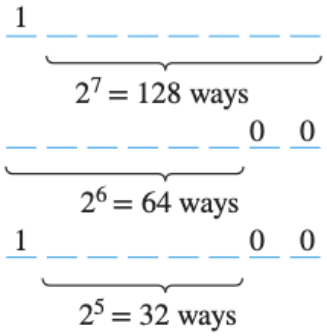


Figura 4.4: Cadenas de 8 bits que empiezan con 1 o terminan con 00.

número de formas de seleccionar un elemento de A_1 y el número de formas de seleccionar un elemento de A_2, menos el número de formas de seleccionar un elemento que está tanto en A_1 como en A_2.

Porque hay $|A_1 \cup A_2|$ formas de seleccionar un elemento en A_1 o en A_2, y $|A_1 \cap A_2|$ formas de seleccionar un elemento común a ambos conjuntos, tenemos

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Ésta es la fórmula dada en la Sección 1.8 para el número de elementos en la unión de dos conjuntos.

El ejemplo 4.1.18 ilustra cómo podemos resolver problemas de conteo usando el principio de la resta.

Ejemplo 4.1.18 ¿Cuántas cadenas de bits de longitud ocho comienzan con 1 o terminan con 00?

Solución: La Figura 4.4 ilustra los tres problemas de conteo que debemos resolver antes de poder aplicar el principio de inclusión-exclusión.

Podemos construir una cadena de bits de longitud ocho que comience con el bit 1 o que termine con los dos bits 00, construyendo una cadena de bits de longitud ocho que comience con el bit 1 o construyendo una cadena de bits de longitud ocho que termine con la dos bits 00.

Podemos construir una cadena de bits de longitud ocho que comience con 1 en $2^7 = 128$ formas. Esto sigue la regla del producto, porque el primer bit se puede elegir de una sola manera y cada uno de los otros siete bits se puede elegir de dos maneras.

De manera similar, podemos construir una cadena de bits de longitud ocho que termine con los dos bits 00, de $2^6 = 64$ formas. Esto sigue la regla del producto, porque cada uno de los primeros seis bits se puede elegir de dos maneras y los dos últimos bits se pueden elegir de una sola manera.

Algunas de las formas de construir una cadena de bits de longitud ocho que comience con un 1 son las mismas que las formas de construir una cadena de bits de longitud ocho que termine con los dos bits 00. Hay $2^5 = 32$ formas de construir dicha cadena.

Esto sigue la regla del producto, porque el primer bit se puede elegir de una sola manera, cada uno del segundo al sexto bits se puede elegir de dos maneras, y los dos últimos bits se pueden elegir de una manera.

En consecuencia, el número de cadenas de bits de longitud ocho que comienzan con 1 o terminan con 00, que es igual al número de formas de construir una cadena de bits de longitud ocho que comienza con 1 o que termina con 00, es igual a $128 + 64 - 32 = 160$.

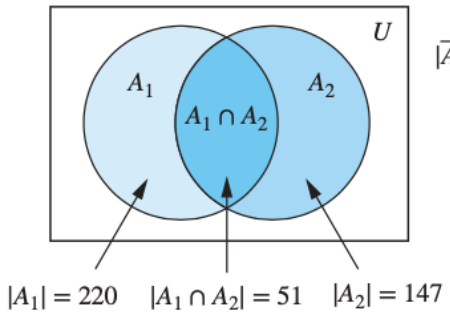
□

Ejemplo 4.1.19 Una empresa de informática recibe 350 solicitudes de graduados universitarios para un trabajo que planifica una línea de nuevos servidores web. Suponga que 220 de estos solicitantes se especializaron en ciencias de la computación, 147 se especializaron en negocios y 51 se especializaron tanto en ciencias de la computación como en negocios. ¿Cuántos de estos solicitantes no se especializaron en ciencias de la computación ni en negocios?

Solución: Para encontrar el número de estos solicitantes que no se especializaron ni en ciencias de la computación ni en negocios, podemos restar el número de estudiantes que se especializaron en ciencias de la computación o en negocios (o ambos) del número total de solicitantes. Sea A_1 el conjunto de estudiantes que se especializaron en ciencias de la computación y A_2 el conjunto de estudiantes que se especializaron en negocios. Entonces $A_1 \cup A_2$ es el conjunto de estudiantes que se especializaron en ciencias de la computación o negocios (o ambos), y $A_1 \cap A_2$ es el conjunto de estudiantes que se especializaron tanto en ciencias de la computación como en negocios. Por la regla de la resta, el número de estudiantes que se especializaron en ciencias de la computación o en negocios (o ambos) es igual a

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316.$$

Concluimos que $350 - 316 = 34$ de los solicitantes no se especializaron en ciencias de la computación ni en negocios. En la Figura 4.5 se muestra un



$$\begin{aligned}|\overline{A_1 \cup A_2}| &= |U| - |A_1 \cup A_2| \\ &= |U| - (|A_1| + |A_2| - |A_1 \cap A_2|) \\ &= 350 - (220 + 147 - 51) \\ &= 350 - 316 \\ &= 34\end{aligned}$$

Figura 4.5: Solicitantes que no se especializaron en ciencias de la computación ni en negocios.

diagrama de Venn para este ejemplo.

□

4.1.5. La Regla de la División

Hemos introducido las reglas del producto, la suma y la resta para contar. Quizás se pregunte si también existe una regla de la división para contar. De hecho, existe una regla de este tipo, que puede ser útil para resolver ciertos tipos de problemas de enumeración.

> LA REGLA DE LA DIVISIÓN Hay n/d formas de hacer una tarea si se puede hacer usando un procedimiento que se puede llevar a cabo de n formas, y para todas las formas w, exactamente d de las n formas corresponden a la forma w.

Podemos reformular la regla de división en términos de conjuntos: "Si el conjunto finito A es la unión de n subconjuntos disjuntos por pares, cada uno con d elementos, entonces $n = |A|/d$".

También podemos formular la regla de división en términos de funciones: "Si f es una función de A a B donde A y B son conjuntos finitos, y que para cada valor $y \in B$ hay exactamente d valores $x \in A$ tales que $f(x) = y$ (en cuyo caso, decimos que f es d-a-uno), entonces $|B| = |A|/d$".

Observación 4.1.1 La regla de división resulta útil cuando parece que una tarea se puede realizar de n formas diferentes, pero resulta que para cada forma de realizar la tarea, existen d formas equivalentes de realizarla. En

estas circunstancias, podemos concluir que existen n/d formas desiguales de realizar la tarea.

□

Ilustramos el uso de la regla de división para contar con dos ejemplos.

Ejemplo 4.1.20 Suponga que se ha desarrollado un sistema automatizado que cuenta las patas de las vacas en un pastizal. Suponga que este sistema ha determinado que en el pastizal de un agricultor hay exactamente 572 patas. ¿Cuántas vacas hay en este pasto, asumiendo que cada vaca tiene cuatro patas y que no hay otros animales presentes?

Solución: Sea n el número de patas de vaca contadas en un pastizal. Debido a que cada vaca tiene cuatro patas, según la regla de división sabemos que el pastizal contiene $n/4$ vacas. En consecuencia, el pastizal con 572 patas de vaca tiene $572/4 = 143$ vacas en él.

□

Ejemplo 4.1.21 ¿De cuántas formas diferentes hay de sentar a cuatro personas alrededor de una mesa circular, donde dos asientos se consideran iguales cuando cada persona tiene el mismo vecino de la izquierda y el mismo vecino de la derecha?

Solución: Seleccionamos arbitrariamente un asiento en la mesa y lo etiquetamos asiento 1. Numeramos el resto de los asientos en orden numérico, avanzando en el sentido de las agujas del reloj alrededor de la mesa.

Tenga en cuenta que hay cuatro formas de seleccionar a la persona para el asiento 1, tres formas de seleccionar a la persona para el asiento 2, dos formas de seleccionar a la persona para el asiento 3 y una forma de seleccionar a la persona para el asiento 4.

Por lo tanto, hay $4! = 24$ formas de ordenar las cuatro personas indicadas para estos asientos. Sin embargo, cada una de las cuatro opciones para el asiento 1 conduce a la misma disposición, ya que distinguimos dos disposiciones sólo cuando una de las personas tiene un vecino inmediato a la izquierda o derecha diferente.

Debido a que hay cuatro formas de elegir a la persona para el asiento 1, según la regla de división hay $24/4 = 6$ disposiciones de asientos diferentes de cuatro personas alrededor de la mesa circular.

□

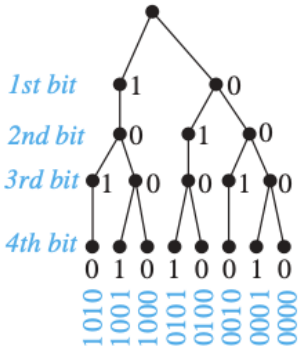


Figura 4.6: Cadenas de longitud cuatro sin dos unos consecutivos.

4.1.6. Diagramas de Árbol

Los problemas de conteo se pueden resolver usando diagramas de árbol. Un árbol consta de una raíz, varias ramas que salen de la raíz y posibles ramas adicionales que salen de los extremos de otras ramas.

Para usar árboles en el conteo, usamos una rama para representar cada opción posible. Representamos los posibles resultados por las hojas, que son los puntos finales de las ramas que no tienen otras ramas comenzando en ellas.

Tenga en cuenta que cuando se usa un diagrama de árbol para resolver un problema de conteo, el número de opciones de qué rama seguir para llegar a una hoja puede variar como en el Ejemplo 4.1.22.

Ejemplo 4.1.22 ¿Cuántas cadenas de bits de longitud cuatro no tienen dos unos consecutivos?

Solución: El diagrama de árbol de la Figura 4.6 muestra todas las cadenas de bits de longitud cuatro sin dos unos consecutivos. Vemos que hay ocho cadenas de bits de longitud cuatro sin dos unos consecutivos.

□

Ejemplo 4.1.23 Un desempate entre dos equipos consta de un máximo de cinco juegos. El primer equipo que gane tres juegos gana el desempate. ¿De cuántas formas diferentes puede ocurrir el desempate?

Solución: El diagrama de árbol de la Figura 4.7 muestra todas las formas en que puede continuar la eliminatoria, y se muestra el ganador de cada juego. Vemos que hay 20 formas diferentes de que ocurra la eliminatoria. □

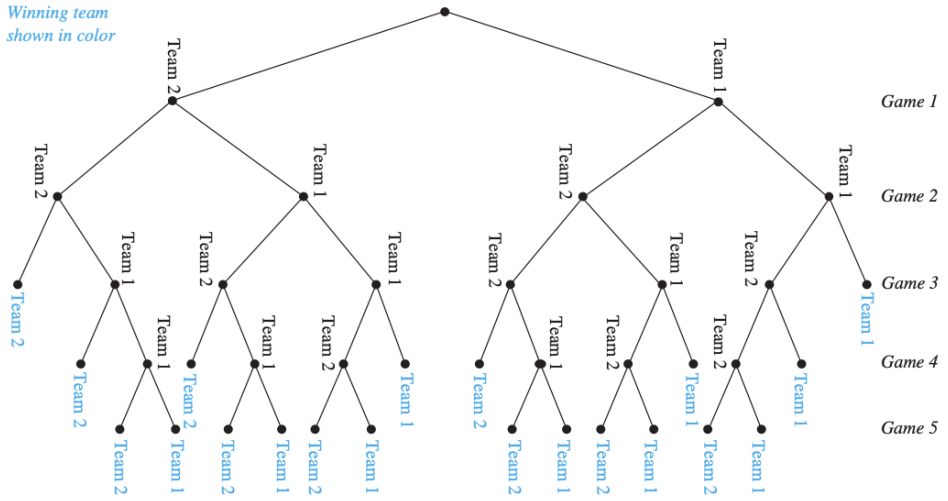


Figura 4.7: Los mejores tres juegos de una eliminatoria a cinco juegos.

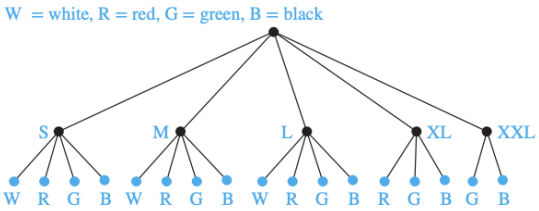


Figura 4.8: Conteo de variedades de camisetas.

Ejemplo 4.1.24 Suponga que las camisetas "I Love New Jersey" vienen en cinco tamaños diferentes: S, M, L, XL y XXL. Además, suponga que cada tamaño viene en cuatro colores, blanco, rojo, verde y negro, excepto XL, que viene solo en rojo, verde y negro, y XXL, que viene solo en verde y negro. ¿Cuántas camisetas diferentes tiene que tener una tienda de souvenirs para tener al menos una de cada talla y color disponibles de la camiseta?

Solución: el diagrama de árbol de la Figura 4.8 muestra todos los pares de tamaños y colores posibles. De ello se deduce que el propietario de la tienda de souvenirs debe tener en stock 17 camisetas diferentes. □

4.1.7. Ejercicios

1. Una marca particular de camisa viene en 12 colores, tiene una versión masculina y una femenina, y viene en tres tallas para cada sexo. ¿Cuántos tipos diferentes de esta camisa se fabrican?

2. Seis aerolíneas diferentes vuelan desde Nueva York a Denver y siete vuelan desde Denver a San Francisco. ¿Cuántos pares diferentes de aerolíneas puede elegir para reservar un viaje de Nueva York a San Francisco vía Denver, cuando elige una aerolínea para el vuelo a Denver y una aerolínea para el vuelo de continuación a San Francisco?

3. Hay cuatro rutas de automóviles principales de Boston a Detroit y seis de Detroit a Los Ángeles. ¿Cuántas rutas de automóviles importantes hay de Boston a Los Ángeles a través de Detroit?

4. ¿Cuántas iniciales de tres letras diferentes pueden tener las personas?

5. ¿Cuántas iniciales de tres letras diferentes sin ninguna de las letras repetidas puede tener la gente?

6. ¿Cuántas iniciales de tres letras diferentes hay que comienzan con una A?

7. ¿Cuántas cadenas de bits de longitud ocho hay?

8. ¿Cuántas cadenas de bits de longitud diez comienzan y terminan con un 1?

9. En una gran universidad, 434 estudiantes de primer año, 883 estudiantes de segundo año y 43 estudiantes de tercer año están inscritos en un curso de introducción a los algoritmos. ¿Cuántas secciones de este curso deben programarse para acomodar a todos estos estudiantes si cada sección contiene 34 estudiantes?

10. ¿Cuántas cadenas de bits de longitud siete comienzan con dos ceros o terminan con tres unos?

11. Determine el número de partidos jugados en un torneo de eliminación simple con n jugadores, donde para cada juego entre dos jugadores el ganador continúa, pero el perdedor es eliminado.

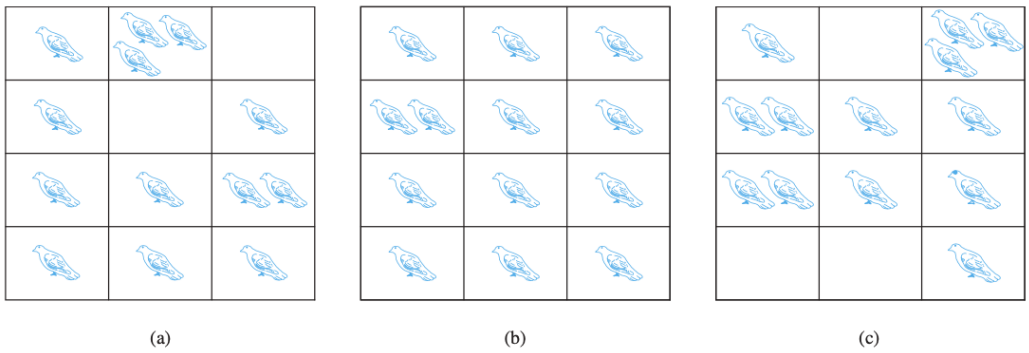


Figura 4.9: Hay más palomas que casilleros.

4.2. El Principio del Casillero

4.2.1. Introducción

Suponga que una bandada de 20 palomas vuela en un conjunto de 19 casilleros para posarse. Debido a que hay 20 palomas pero sólo 19 casilleros, al menos uno de estos 19 casilleros debe tener al menos dos palomas.

Para ver por qué esto es cierto, tenga en cuenta que si cada casillero tuviera como máximo una paloma, se podrían acomodar como máximo 19 palomas, una por casillero.

Esto ilustra un principio general llamado principio de casillero, que establece que si hay más palomas que casilleros, entonces debe haber al menos un casillero con al menos dos palomas en él (ver Figura 4.9). Este principio es extremadamente útil; se aplica a mucho más que palomas y casilleros.

Teorema 4.2.1 EL PRINCIPIO DEL CASILLERO Si k es un número entero positivo y $k+1$ o más objetos se colocan en k cajas, entonces hay al menos una caja que contiene dos o más de los objetos.

Demostración: Demostramos el principio del casillero usando una prueba por contraposición. Suponga que ninguna de las k cajas contiene más de un objeto. Entonces, el número total de objetos sería como máximo k. Esto es una contradicción, porque hay al menos $k+1$ objetos.

■

Ilustraremos la utilidad del principio del casillero. Primero mostramos que puede usarse para demostrar un corolario útil sobre las funciones.

Corolario 4.2.1 Una función f de un conjunto con $k+1$ o más elementos a un conjunto con k elementos no es uno a uno.

Demostración: Suponga que para cada elemento y en el codominio de f tenemos una caja que contiene todos los elementos x del dominio de f tales que $f(x) = y$. Debido a que el dominio contiene $k+1$ o más elementos y el codominio contiene solo k elementos, el principio de casillero nos dice que una de estas cajas contiene dos o más elementos x del dominio. Esto significa que f no puede ser uno a uno.

■

Los ejemplos del 4.2.1 al 4.2.3 muestran cómo se utiliza el principio del casillero.

Ejemplo 4.2.1 Entre cualquier grupo de 367 personas, debe haber al menos dos con el mismo cumpleaños, porque sólo hay 366 cumpleaños posibles.

□

Ejemplo 4.2.2 En cualquier grupo de 27 palabras en inglés, debe haber al menos dos que comiencen con la misma letra, porque hay 26 letras en el alfabeto inglés.

□

Ejemplo 4.2.3 ¿Cuántos estudiantes debe haber en una clase para garantizar que al menos dos estudiantes reciban la misma calificación en el examen final, si el examen se califica en una escala de 0 a 100 puntos?

Solución: Hay 101 posibles calificaciones en el examen final. El principio del casillero muestra que entre 102 estudiantes debe haber al menos 2 estudiantes con la misma calificación.

□

El principio del casillero es una herramienta útil en muchas pruebas, incluidas las pruebas de resultados sorprendentes, como la que se da en el Ejemplo 4.2.4.

Ejemplo 4.2.4 Demuestre que para cada entero n hay un múltiplo de n que sólo tiene 0 y 1 en su expansión decimal.

Solución:: Sea n un número entero positivo. Considere los $n+1$ enteros $1, 11, 111, \ldots, 11\ldots1$ (donde el último entero en esta lista es el entero con $n+1$ 1s en su expansión decimal).

Tenga en cuenta que hay n residuos posibles cuando un número entero se divide por n. Debido a que hay $n+1$ números enteros en esta lista, por el principio del casillero debe haber dos con el mismo resto cuando se divide por n. El mayor de estos enteros menos el menor es un múltiplo de n, que tiene una expansión decimal que consta completamente de 0 y 1.

□

4.2.2. El Principio Generalizado del Casillero

El principio del casillero establece que debe haber al menos dos objetos en la misma caja cuando hay más objetos que cajas. Sin embargo, se puede decir aún más cuando el número de objetos excede un múltiplo del número de cajas. Por ejemplo, entre cualquier conjunto de 21 dígitos decimales debe haber 3 que sean iguales. Esto se debe a que cuando 21 objetos se distribuyen en 10 cajas, una caja debe tener más de 2 objetos.

Teorema 4.2.2 EL PRINCIPIO GENERALIZADO DEL CASILLERO Si N objetos se colocan en k cajas, entonces hay al menos una caja que contiene al menos $\lceil N/k \rceil$ objetos.

Demostración: Usaremos una prueba por contraposición. Suponga que ninguna de las cajas contiene más de $\lceil N/k \rceil - 1$ objetos. Entonces, el número total de objetos es como máximo

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k}+1\right)-1\right) = N$$

donde se ha utilizado la desigualdad $\lceil N/k \rceil < (N/k)+1$. Por tanto, el número total de objetos es menor que N. Esto completa la demostración por contraposición.

■

Un tipo de problema común pide el número mínimo de objetos de modo que al menos r de estos objetos debe estar en una de las k cajas, cuando estos objetos se distribuyen entre las cajas. Si tenemos N objetos, el principio generalizado del casillero nos dice que debe haber al menos r objetos en una de las cajas siempre que $\lceil N/k \rceil \geq r$.

El número entero más pequeño N con $N/k > r-1$, es decir, $N = k(r-1)+1$, es el número entero más pequeño que satisface la desigualdad $\lceil N/k \rceil \geq r$. ¿Podría ser suficiente un valor menor de N? La respuesta es no, porque si

tuviéramos $k(r-1)$ objetos, podríamos poner $r-1$ de ellos en cada una de las k cajas y ninguna caja tendría al menos r objetos.

Al pensar en problemas de este tipo, es útil considerar cómo puede evitar tener al menos r objetos en una de las cajas a medida que agrega objetos sucesivos. Para evitar agregar un objeto r-ésimo a cualquier caja, eventualmente terminará con $r-1$ objetos en cada caja. No hay forma de agregar el siguiente objeto sin poner un objeto r-ésimo en esa caja.

Los ejemplos del 4.2.5 al 4.2.8 ilustran cómo se aplica el principio generalizado del casillero.

Ejemplo 4.2.5 Entre 100 personas hay al menos $\lceil 100/12 \rceil = 9$ que nacieron en el mismo mes.

□

Ejemplo 4.2.6 ¿Cuál es el número mínimo de estudiantes requeridos en una clase de matemáticas discretas para asegurarse de que al menos seis recibirán la misma calificación, si hay cinco calificaciones posibles, A, B, C, D y F?

Solución: El número mínimo de estudiantes necesario para garantizar que al menos seis estudiantes reciban la misma calificación es el número entero más pequeño N tal que $\lceil N/5 \rceil = 6$.

El número entero más pequeño es $N = 5 \cdot 5 + 1 = 26$. Si se tienen sólo 25 estudiantes, es posible que haya cinco que hayan recibido cada calificación, de modo que no haya seis estudiantes que hayan recibido la misma calificación.

Por lo tanto, 26 es el número mínimo de estudiantes necesarios para garantizar que al menos seis estudiantes reciban la misma calificación.

□

Ejemplo 4.2.7

1. ¿Cuántas cartas deben seleccionarse de una baraja estándar de 52 cartas para garantizar que se seleccionen al menos tres cartas de la misma figura?

2. ¿Cuántos deben seleccionarse de una baraja estándar de 52 cartas para garantizar que se seleccionen al menos tres corazones?

Solución:

1. Suponga que hay cuatro casillas, una para cada figura, y cuando se seleccionan las cartas, se colocan en la casilla reservada para las cartas de esa figura. Usando el principio generalizado del casillero, vemos que si se seleccionan N cartas, hay al menos una caja que contiene al menos $\lceil N/4 \rceil$ cartas.

   En consecuencia, sabemos que se seleccionan al menos tres cartas de una figura si $\lceil N/4 \rceil \geq 3$. El número entero más pequeño N tal que $\lceil N/4 \rceil \geq 3$ es $N = 4 \cdot 2 + 1 = 9$, entonces nueve cartas son suficientes.

   Tenga en cuenta que si se seleccionan ocho cartas, es posible tener dos cartas de cada figura, por lo que se necesitan más de ocho cartas. En consecuencia, se deben seleccionar nueve cartas para garantizar que se elijan al menos tres cartas de una misma figura.

   Una buena forma de pensar en esto es tener en cuenta que después de elegir la octava carta, no hay forma de evitar tener una tercera carta de alguna figura.

2. No utilizamos el principio generalizado del casillero para responder a esta pregunta, porque queremos asegurarnos de que haya tres corazones, no solo tres cartas de una figura.

   Tenga en cuenta que, en el peor de los casos, podemos seleccionar todos los tréboles, diamantes y espadas, 39 cartas en total, antes de seleccionar un solo corazón. Las siguientes tres cartas serán todas de corazones, por lo que es posible que debamos seleccionar 42 cartas para obtener tres corazones.

□

Ejemplo 4.2.8 ¿Cuál es la menor cantidad de códigos de área necesarios para garantizar que a los 25 millones de teléfonos de un estado se les puedan asignar números de teléfono distintos de 10 dígitos? (Suponga que los números de teléfono tienen el formato NXX-NXX-XXXX, donde los primeros tres dígitos forman el código de área, N representa un dígito del 2 al 9 inclusive, y X representa cualquier dígito).

Solución: Hay ocho millones de números de teléfono diferentes con el formato NXX-XXXX. Por lo tanto, según el principio generalizado del casillero, entre 25 millones de teléfonos, al menos $\lceil 25,000,000/8,000,000 \rceil = 4$ de ellos

deben tener números de teléfono idénticos. Por lo tanto, se requieren al menos cuatro códigos de área para garantizar que todos los números de 10 dígitos sean diferentes.

□

El ejemplo 4.2.9, aunque no es una aplicación del principio generalizado del casillero, hace uso de principios similares.

Ejemplo 4.2.9 Suponga que un laboratorio de ciencias de la computación tiene 15 estaciones de trabajo y 10 servidores. Se puede utilizar un cable para conectar directamente una estación de trabajo a un servidor.

Para cada servidor, solo una conexión directa a ese servidor puede estar activa en cualquier momento. Queremos garantizar que en cualquier momento cualquier conjunto de 10 o menos estaciones de trabajo pueda acceder simultáneamente a diferentes servidores a través de conexiones directas.

Aunque podríamos hacer esto conectando cada estación de trabajo directamente a cada servidor (usando 150 conexiones), ¿cuál es la cantidad mínima de conexiones directas necesarias para lograr este objetivo?

Solución: Supongamos que etiquetamos las estaciones de trabajo $W_1, W_2, \ldots, W_{15}$ y los servidores $S_1, S_2, \ldots, S_{10}$. Primero, nos gustaría encontrar una manera de que haya menos de 150 conexiones directas entre estaciones de trabajo y servidores para lograr nuestro objetivo.

Un enfoque prometedor es conectar directamente W_k a S_k para $k = 1, 2, \ldots, 10$ y luego conectar cada uno de $W_{11}, W_{12}, W_{13}, W_{14}$ y W_{15} a los 10 servidores. Esto nos da un total de $10 + 5 \cdot 10 = 60$ conexiones directas.

Necesitamos determinar si con esta configuración cualquier conjunto de 10 o menos estaciones de trabajo puede acceder simultáneamente a diferentes servidores. Observamos que si la estación de trabajo W_j está incluida con $1 \leq j \leq 10$, puede acceder al servidor S_j, y para cada estación de trabajo W_k con $k \geq 11$ incluida, debe haber una estación de trabajo W_j correspondiente con $1 \leq j \leq 10$ no incluida, por lo que W_k puede acceder al servidor S_j.

Esto se debe a que hay al menos tantos servidores disponibles S_j como estaciones de trabajo W_j con $1 \leq j \leq 10$ no incluidas. Por lo tanto, cualquier conjunto de 10 o menos estaciones de trabajo puede acceder simultáneamente a diferentes servidores.

Pero, ¿podemos utilizar menos de 60 conexiones directas? Suponga que hay menos de 60 conexiones directas entre estaciones de trabajo y servidores. Entonces, algún servidor se conectaría a un máximo de $\lfloor 59/10 \rfloor = 5$ estacio-

nes de trabajo. Si todos los servidores estuvieran conectados a al menos seis estaciones de trabajo, habría al menos 6 x 10 = 60 conexiones directas.

Esto significa que los nueve servidores restantes no son suficientes para que las otras 10 o más estaciones de trabajo accedan simultáneamente a diferentes servidores. En consecuencia, se necesitan al menos 60 conexiones directas. De ello se deduce que 60 es la respuesta.

□

4.2.3. Ejercicios

1. ¿Cuántos números deben seleccionarse del conjunto $\{1, 2, 3, 4, 5, 6\}$ para garantizar que al menos un par de estos números sumen 7?

2. Muestre que en un grupo de 10 personas (donde dos personas son amigos o enemigos), hay tres amigos mutuos o cuatro enemigos mutuos, y hay tres enemigos mutuos o cuatro amigos mutuos.

3. Muestre que hay al menos seis personas en California (población: 39 millones) con las mismas tres iniciales que nacieron el mismo día del año (pero no necesariamente en el mismo año). Suponga que todos tienen tres iniciales.

4. Hay 38 períodos de tiempo diferentes durante los cuales se pueden programar las clases en una universidad. Si hay 677 cursos diferentes, ¿cuántas salones diferentes se necesitarán?

5. Una red de computadoras consta de seis computadoras. Cada computadora está conectada directamente al menos a una de las otras computadoras. Muestre que hay al menos dos computadoras en la red que están conectadas directamente a la misma cantidad de otras computadoras.

6. Hay 51 casas en una calle. Cada casa tiene una dirección entre 1000 y 1099, inclusive. Muestre que al menos dos casas tienen direcciones que son números enteros consecutivos.

4.3. Permutaciones y Combinaciones

4.3.1. Introducción

Muchos problemas de conteo se pueden resolver encontrando el número de formas de organizar un número específico de elementos distintos de un conjunto de un tamaño particular, donde el orden de estos elementos es importante.

Muchos otros problemas de conteo se pueden resolver encontrando el número de formas de seleccionar un número particular de elementos de un conjunto de un tamaño particular, donde el orden de los elementos seleccionados no importa.

Por ejemplo, ¿de cuántas formas podemos seleccionar a tres estudiantes de un grupo de cinco estudiantes para que hagan fila para tomarse una foto? ¿Cuántos comités diferentes de tres estudiantes se pueden formar a partir de un grupo de cuatro estudiantes? En esta sección desarrollaremos métodos para responder preguntas como estas.

4.3.2. Permutaciones

Comenzamos resolviendo la primera pregunta planteada en la introducción de esta sección, así como las preguntas relacionadas.

Ejemplo 4.3.1 ¿De cuántas formas podemos seleccionar a tres estudiantes de un grupo de cinco estudiantes para que hagan fila para tomar una foto? ¿De cuántas formas podemos organizar a los cinco estudiantes en una línea para una foto?

Solución: Primero, tenga en cuenta que el orden en el que seleccionamos a los estudiantes es importante. Hay cinco formas para seleccionar al primer alumno que se sitúe al principio de la fila. Una vez que se ha seleccionado a este estudiante, hay cuatro formas de seleccionar al segundo estudiante en la línea. Después de seleccionar al primer y segundo alumno, hay tres formas de seleccionar al tercer alumno de la línea. Según la regla del producto, hay $5 \cdot 4 \cdot 3 = 60$ formas de seleccionar a tres estudiantes de un grupo de cinco estudiantes para que hagan fila para tomar una foto.

Para organizar a los cinco estudiantes en una línea para una foto, seleccionamos al primer estudiante de cinco formas, al segundo de cuatro formas, al tercero de tres formas, al cuarto de dos formas y al quinto de una forma.

En consecuencia, hay $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ formas de organizar a los cinco estudiantes en una línea para una foto.

□

El ejemplo 4.3.1 ilustra cómo se pueden contar las disposiciones ordenadas de distintos objetos. Esto conduce a cierta terminología.

Una **permutación** de un conjunto de objetos distintos es una disposición ordenada de estos objetos. También nos interesan los arreglos ordenados de algunos de los elementos de un conjunto. Un arreglo ordenado de r elementos de un conjunto se llama **permutación-r**.

Ejemplo 4.3.2 Sea $S = \{1, 2, 3\}$. La disposición ordenada 3, 1, 2 es una permutación de S. La disposición ordenada 3, 2 es una permutación-2 de S.
□

El número de permutaciones-r de un conjunto con n elementos se denota por $P(n, r)$. Podemos encontrar $P(n, r)$ usando la regla del producto.

Ejemplo 4.3.3 Sea $S = \{a, b, c\}$. ¿Cuáles son las permutaciones-2 de S?

Solución: Las permutaciones-2 de S son las disposiciones ordenadas

$$a, b; a, c; b, a; b, c; c, a; c, b.$$

En consecuencia, hay seis permutaciones-2 de este conjunto con tres elementos. Siempre hay seis permutaciones-2 de un conjunto con tres elementos.

Hay tres formas de elegir el primer elemento del arreglo. Hay dos formas de elegir el segundo elemento del arreglo, porque debe ser diferente del primer elemento. Por tanto, según la regla del producto, vemos que $P(3, 2) = 3 \cdot 2 = 6$.

□

Ahora usamos la regla del producto para encontrar una fórmula para $P(n, r)$ siempre que n y r son números enteros positivos con $1 \leq r \leq n$.

Teorema 4.3.1 Si n es un número entero positivo y r es un número entero con $1 \leq r \leq n$, entonces hay

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

permutaciones-r de un conjunto con n elementos distintos.

Demostración: Usaremos la regla del producto para demostrar que esta fórmula es correcta. El primer elemento de la permutación se puede elegir de n formas porque hay n elementos en el conjunto. Hay $n-1$ formas de elegir el segundo elemento de la permutación, porque quedan $n-1$ elementos en el conjunto después de usar el elemento elegido para la primera posición. De manera similar, hay $n-2$ formas de elegir el tercer elemento, y así sucesivamente, hasta que existan exactamente $n-(r-1) = n-r+1$ formas de elegir el r-ésimo elemento. En consecuencia, según la regla del producto, hay

$$n(n-1)(n-2)\cdots(n-r+1)$$

permutaciones-r del conjunto.

■

Tenga en cuenta que $P(n,0) = 1$ siempre que n es un número entero no negativo porque hay exactamente una forma de ordenar cero elementos. Es decir, hay exactamente una lista sin elementos, a saber, la lista vacía.

Enunciamos ahora un corolario útil del teorema 4.3.1.

Corolario 4.3.1 Si n y r son números enteros con $0 \leq r \leq n$, entonces

$$P(n,r) = \frac{n!}{(n-r)!}$$

.

Demostración: Cuando n y r son números enteros con $1 \leq r \leq n$, entonces por el Teorema 4.3.1 tenemos que

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}.$$

Ya que $\frac{n!}{(n-0)!} = \frac{n!}{(n)!} = 1$ siempre que n es un entero no negativo, vemos que la fórmula

$$P(n,r) = \frac{n!}{(n-r)!}$$

también se cumple cuando $r = 0$.

■

Por el teorema 4.3.1 sabemos que si n es un número entero positivo, entonces $P(n,n) = n!$. Ilustraremos este resultado con algunos ejemplos.

Ejemplo 4.3.4 ¿Cuántas formas hay de seleccionar un ganador del primer premio, un ganador del segundo premio y un ganador del tercer premio de entre 100 personas diferentes que participaron en un concurso?

Solución: Debido a que importa qué persona gana qué premio, el número de formas de elegir a los tres ganadores del premio es el número de selecciones ordenadas de tres elementos de un conjunto de 100 elementos, es decir, el número de permutaciones-3 de un conjunto de 100 elementos. En consecuencia, la respuesta es

$$P(100, 3) = 100 \cdot 99 \cdot 98 = 970,200.$$

□

Ejemplo 4.3.5 Suponga que hay ocho corredores en una carrera. El ganador recibe una medalla de oro, el que finaliza en segundo lugar recibe una medalla de plata y el que finaliza en tercer lugar recibe una medalla de bronce. ¿De cuántas formas diferentes hay de otorgar estas medallas, si todos los posibles resultados de la carrera pueden ocurrir y no hay empates?

Solución: El número de formas diferentes de otorgar las medallas es el número de permutaciones-3 de un conjunto con ocho elementos. Por lo tanto, hay $P(8, 3) = 8 \cdot 7 \cdot 6 = 336$ formas posibles de otorgar las medallas.

□

Ejemplo 4.3.6 Suponga que una vendedora tiene que visitar ocho ciudades diferentes. Debe comenzar su viaje en una ciudad especificada, pero puede visitar las otras siete ciudades en el orden que desee. ¿Cuántos posibles órdenes puede utilizar la vendedora para visitar estas ciudades?

Solución: El número de caminos posibles entre las ciudades es el número de permutaciones de siete elementos, porque la primera ciudad está determinada, pero los siete restantes pueden ordenarse arbitrariamente. En consecuencia, hay $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ maneras para que la vendedora elija su recorrido. Si, por ejemplo, la vendedora desea encontrar el camino entre las ciudades con una distancia mínima y calcula la distancia total para cada camino posible, ¡debe considerar un total de 5040 caminos!

□

Ejemplo 4.3.7 ¿Cuántas permutaciones de las letras $ABCDEFGH$ contienen la cadena ABC?

Solución: Debido a que las letras ABC deben aparecer como un bloque, podemos encontrar la respuesta al encontrar el número de permutaciones de seis objetos, a saber, el bloque ABC y las letras individuales *D, E, F, G* y *H*. Porque estos seis objetos pueden aparecer en cualquier orden, hay $6! = 720$ permutaciones de las letras $ABCDEFGH$ en las que ABC aparece como un bloque.

□

4.3.3. Combinaciones

Ahora centramos nuestra atención en contar selecciones desordenadas de objetos. Comenzamos resolviendo una pregunta planteada en la introducción a esta sección del capítulo.

Ejemplo 4.3.8 ¿Cuántos comités diferentes de tres estudiantes se pueden formar a partir de un grupo de cuatro estudiantes?

Solución: Para responder a esta pregunta, solo necesitamos encontrar el número de subconjuntos con tres elementos del conjunto que contiene a los cuatro estudiantes. Vemos que hay cuatro de esos subconjuntos, uno para cada uno de los cuatro estudiantes, porque elegir tres estudiantes es lo mismo que elegir uno de los cuatro estudiantes para dejarlo fuera del grupo. Esto significa que hay cuatro formas de elegir a los tres estudiantes para el comité, donde el orden en el que se eligen estos estudiantes no importa.

□

El ejemplo 4.3.8 ilustra que muchos problemas de conteo se pueden resolver encontrando el número de subconjuntos de un tamaño particular de un conjunto con n elementos, donde n es un número entero positivo.

Una **combinación-r** de elementos de un conjunto es una selección desordenada de r elementos del conjunto. Por tanto, una combinación-r es simplemente un subconjunto con r elementos del conjunto del dominio del problema.

Ejemplo 4.3.9 Sea S el conjunto $\{1, 2, 3, 4\}$. Entonces $\{1, 3, 4\}$ es una combinación-3 de S. Tenga en cuenta que $\{4, 1, 3\}$ es la misma combinación-3 que $\{1, 3, 4\}$, porque el orden en el que los elementos de un conjunto se enumeran no importa.

□

El número de combinaciones-r de un conjunto con n elementos distintos se denota por $C(n, r)$. Tenga en cuenta que $C(n, r)$ también se denota por $\binom{n}{r}$ y se denomina coeficiente binomial.

Ejemplo 4.3.10 Vemos que $C(4, 2) = 6$, porque las combinaciones-2 de $\{a, b, c, d\}$ son los seis subconjuntos $\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}$ y $\{c, d\}$. □

Podemos determinar el número de combinaciones-r de un conjunto con n elementos usando la fórmula para el número de permutaciones-r de un conjunto. Para hacer esto, tenga en cuenta que las permutaciones-r de un conjunto se pueden obtener primero formando combinaciones-r y luego ordenando los elementos en estas combinaciones. La demostración del Teorema 4.3.2, que da el valor de $C(n, r)$, se basa en esta observación.

Teorema 4.3.2 El número de combinaciones-r de un conjunto con n elementos, donde n es un número entero no negativo y r es un número entero con $0 \leq r \leq n$, es igual a

$$C(n, r) = \frac{n!}{r!(n - r)!}.$$

Demostración: Las permutaciones-r $P(n, r)$ del conjunto se pueden obtener formando las combinaciones-r $C(n, r)$ del conjunto, y luego ordenando los elementos en cada combinación-r, lo cual se puede hacer en $P(r, r)$ formas. En consecuencia, por la regla del producto,

$$P(n, r) = C(n, r) \cdot P(r, r).$$

Esto implica que

$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!/(n - r)!}{r!/(r - r)!} = \frac{n!}{r!(n - r)!}.$$

También podemos usar la regla de la división para construir una demostración de este teorema. Debido a que el orden de los elementos en una combinación no importa y hay $P(r, r)$ formas de ordenar r elementos en una combinación-r de n elementos, cada una de las $C(n, r)$ combinaciones-r de un conjunto con n elementos corresponde exactamente a $P(r, r)$ permutaciones-r. Por lo tanto, según la regla de división, $C(n, r) = P(n, r)/P(r, r)$, que implica como antes que $C(n, r) = \frac{n!}{r!(n-r)!}$.

■

La fórmula del Teorema 4.3.2, aunque explícita, no es útil cuando $C(n, r)$ se calcula para valores grandes de n y r. Las razones son que es práctico calcular valores exactos de factoriales exactamente sólo para valores enteros pequeños, y cuando se usa aritmética de punto flotante, la fórmula del Teorema 4.3.2 puede producir un valor que no es un número entero.

Al calcular $C(n, r)$, primero tenga en cuenta que cuando cancelamos $(n - r)!$ del numerador y denominador de la expresión para $C(n, r)$ en el Teorema 4.3.2, obtenemos

$$C(n, r) = \frac{n!}{r!(n-r)!} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}.$$

En consecuencia, para calcular $C(n, r)$ puede cancelar todos los términos en el factorial más grande en el denominador del numerador y el denominador, luego multiplicar todos los términos que no se cancelan en el numerador y finalmente dividir por el factorial más pequeño en el denominador.

Al hacer este cálculo a mano, en lugar de hacerlo por máquina, también vale la pena factorizar factores comunes en el numerador $n(n-1)\cdots(n-r+1)$ y en el denominador $r!$. Tenga en cuenta que se pueden usar muchos programas computacionales para encontrar $C(n, r)$. [Estas funciones pueden llamarse $choose(n, k)$ o $binom(n, k)$.]

El ejemplo 4.3.11 ilustra cómo se calcula $C(n, k)$ cuando k es relativamente pequeño en comparación con n y cuando k está cerca de n. También ilustra una identidad clave que disfrutan los números $C(n, k)$.

Ejemplo 4.3.11 ¿Cuántas manos de póquer de cinco cartas se pueden repartir con una baraja estándar de 52 cartas? Además, ¿cuántas formas hay de seleccionar 47 cartas de una baraja estándar de 52 cartas?

Solución: Debido a que el orden en el que se reparten las cinco cartas de una baraja de 52 cartas no importa, hay

$$C(52, 5) = \frac{52!}{5!47!}$$

diferentes manos de cinco cartas que se pueden repartir. Para calcular el valor de $C(52, 5)$, primero divida el numerador y el denominador entre 47!. para obtener

$$C(52, 5) = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}.$$

Esta expresión se puede simplificar dividiendo primero el factor 5 en el denominador por el factor 50 en el numerador para obtener un factor 10 en el numerador.

Luego dividiendo el factor 4 en el denominador por el factor 48 en el numerador para obtener un factor de 12 en el numerador.

Posteriormente dividiendo el factor 3 en el denominador por el factor 51 en el numerador para obtener un factor de 17 en el numerador.

Finalmente, dividiendo el factor 2 en el denominador por el factor 52 en el numerador para obtener un factor de 26 en el numerador. Encontramos que

$$C(52,5) = 26 \cdot 17 \cdot 10 \cdot 49 \cdot 12 = 2,598,960.$$

En consecuencia, hay $2,598,960$ manos de póquer diferentes de cinco cartas que se pueden repartir con una baraja estándar de 52 cartas.

Tenga en cuenta que hay

$$C(52,47) = \frac{52!}{47!5!}$$

diferentes formas de seleccionar 47 cartas de una baraja estándar de 52 cartas. No necesitamos calcular este valor porque $C(52,47) = C(52,5)$. (Sólo el orden de los factores 5! y 47! es diferente en los denominadores de las fórmulas para estas cantidades.) De ello se deduce que también hay $2,598,960$ formas diferentes de seleccionar 47 cartas de una baraja estándar de 52 cartas.

□

En el ejemplo 4.3.11 observamos que $C(52,5) = C(52,47)$. Esto no es sorprendente porque seleccionar cinco cartas de 52 es lo mismo que seleccionar las 47 que dejamos fuera. La identidad $C(52,5) = C(52,47)$ es un caso especial de la identidad útil para el número de combinaciones-r de un conjunto, dada en el Corolario 4.3.2.

Corolario 4.3.2 Sean n y r números enteros no negativos con $r \leq n$. Entonces $C(n,r) = C(n,n-r)$.

Demostración: Del Teorema 4.3.2 se sigue que

$$C(n,r) = \frac{n!}{r!(n-r)!}$$

y

$$C(n,n-r) = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!}.$$

Así, $C(n, r) = C(n, n - r)$.

■

También podemos probar el Corolario 4.3.2 sin depender de la manipulación algebraica. En su lugar, podemos usar una prueba combinatoria. Describimos este importante tipo de prueba en la Definición 4.3.1.

Definición 4.3.1 Una *prueba combinatoria* de una identidad es una prueba que usa argumentos de conteo para probar que ambos lados de la identidad cuentan los mismos objetos pero de diferentes maneras o una prueba que se basa en mostrar que existe una biyección entre los conjuntos de objetos contados por los dos lados de la identidad. Estos dos tipos de pruebas se denominan *pruebas de conteo doble* y *pruebas biyectivas*, respectivamente.

Muchas identidades que involucran coeficientes binomiales pueden probarse usando demostraciones combinatorias. Ahora mostramos cómo demostrar el Corolario 4.3.2 usando una prueba combinatoria. Proporcionaremos una prueba de doble conteo y una prueba biyectiva, ambas basadas en la misma idea básica.

Demostración: Usaremos una prueba biyectiva para mostrar que $C(n, r) = C(n, n - r)$ para todos los enteros n y r con $0 \leq r \leq n$.

Suponga que S es un conjunto con n elementos. La función que mapea un subconjunto A de S a $\overline{A}$ es una biyección entre subconjuntos de S con r elementos y subconjuntos con $n - r$ elementos (como el lector debería verificar). La identidad $C(n, r) = C(n, n - r)$ se sigue porque cuando hay una biyección entre dos conjuntos finitos, los dos conjuntos deben tener el mismo número de elementos.

Alternativamente, podemos reformular este argumento como una prueba de doble conteo. Por definición, el número de subconjuntos de S con r elementos es igual a $C(n, r)$. Pero cada subconjunto A de S también se determina especificando qué elementos no están en A, así están en $\overline{A}$. Dado que el complemento de un subconjunto de S con r elementos tiene $n - r$ elementos, también hay $C(n, n - r)$ subconjuntos de S con r elementos. De ello se deduce que $C(n, r) = C(n, n - r)$.

■

Ejemplo 4.3.12 ¿Cuántas formas hay de seleccionar a cinco jugadores de un equipo de tenis de 10 miembros para hacer un viaje a un partido en otra

escuela?

Solución: La respuesta viene dada por el número de combinaciones-5 de un conjunto con 10 elementos. Según el teorema 4.3.2, el número de tales combinaciones es

$$C(10,5) = \frac{10!}{5!5!} = 252.$$

□

Ejemplo 4.3.13 Un grupo de 30 personas han sido entrenadas como astronautas para ir a la primera misión a Marte. ¿De cuántas formas hay de seleccionar una tripulación de seis personas para esta misión (suponiendo que todos los miembros de la tripulación tengan el mismo trabajo)?

Solución: El número de formas de seleccionar un equipo de seis de un grupo de 30 personas es el número de combinaciones-6 de un conjunto con 30 elementos, porque el orden en el que se eligen estas personas no importa. Según el teorema 4.3.2, el número de tales combinaciones es

$$C(30,6) = \frac{30!}{6!24!} = \frac{30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 593,775.$$

□

Ejemplo 4.3.14 ¿Cuántas cadenas de bits de longitud n contienen exactamente r 1s?

Solución: Las posiciones de r 1s en una cadena de bits de longitud n forman una combinación-r del conjunto $\{1,2,3,...,n\}$. Por lo tanto, hay $C(n,r)$ cadenas de bits de longitud n que contienen exactamente r 1s.

□

Ejemplo 4.3.15 Suponga que hay 9 profesores en el departamento de matemáticas y 11 en el departamento de ciencias de la computación. ¿Cuántas formas hay de seleccionar un comité para desarrollar un curso de matemáticas discretas en una escuela si el comité está formado por tres miembros de la facultad del departamento de matemáticas y cuatro del departamento de ciencias de la computación?

Solución: Según la regla del producto, la respuesta es el producto del número de combinaciones-3 de un conjunto con nueve elementos y el número de combinaciones-4 de un conjunto con 11 elementos. Según el Teorema 4.3.2, el número de formas de seleccionar el comité es

$$C(9,3) \cdot C(11,4) = \frac{9!}{3!6!} \cdot \frac{11!}{4!7!} = 84 \cdot 330 = 27,720.$$

□

4.3.4. Ejercicios

1. Calcule el valor de cada una de estas cantidades.

   a) $P(6,3)$ *c*) $P(8,1)$ *e*) $P(8,8)$
   b) $P(6,5)$ *d*) $P(8,5)$ *f*) $P(10,9)$

2. Calcule el valor de cada una de estas cantidades.

   a) $C(5,1)$ *c*) $C(8,4)$ *e*) $C(8,0)$
   b) $C(5,3)$ *d*) $C(8,8)$ *f*) $C(12,6)$

3. ¿En cuántos órdenes diferentes pueden terminar una carrera cinco corredores si no se permiten empates?

4. ¿Cuántas cadenas de bits de longitud 10 contienen

   a) exactamente tres 1s? *c*) al menos tres 1s?
   b) a lo más tres 1s? *d*) un número igual de 0s y 1s?

5. ¿Cuántas maneras hay para que cuatro hombres y cinco mujeres que están haciendo fila

   a) todos los hombres queden juntos? *b*) todas las mujeres queden juntas?

6. ¿Cuántas permutaciones de las letras $ABCDEFG$ contienen

   a) las cadenas BA y GF? *c*) las cadenas ABC y CDE?
   b) las cadenas ABC y DE? *d*) las cadenas CBA y BED?

7. ¿Cuántas formas hay para que termine una carrera de tres caballos si es posible empatar? [Nota: dos o tres caballos pueden empatar.]

4.4. Permutaciones y Combinaciones Generalizadas

4.4.1. Introducción

En muchos problemas de conteo, los elementos pueden usarse repetidamente. Por ejemplo, una letra o un dígito se puede usar más de una vez en una placa. Cuando se seleccionan una docena de rosquillas, cada variedad se puede elegir repetidamente.

Esto contrasta con los problemas de conteo discutidos anteriormente en el capítulo donde sólo consideramos permutaciones y combinaciones en las que cada elemento podría usarse como máximo una vez. En esta sección mostraremos cómo resolver problemas de conteo donde los elementos se pueden usar más de una vez.

Además, algunos problemas de conteo involucran elementos indistinguibles. Por ejemplo, para contar el número de formas en que se pueden reorganizar las letras de la palabra *SUCCESS*, se debe considerar la ubicación de letras idénticas.

Esto contrasta con los problemas de conteo discutidos anteriormente donde todos los elementos se consideraban distinguibles. En esta sección describiremos cómo resolver problemas de conteo en los que algunos elementos son indistinguibles.

4.4.2. Permutaciones con Repetición

El conteo de permutaciones cuando se permite la repetición de elementos se puede hacer fácilmente usando la regla del producto, como muestra el Ejemplo 4.4.1.

Ejemplo 4.4.1 ¿Cuántas cadenas de longitud r se pueden formar a partir de las letras mayúsculas del alfabeto inglés?

Solución: Según la regla del producto, debido a que hay 26 letras mayúsculas en inglés, y debido a que cada letra se puede usar repetidamente, vemos que hay 26^r cadenas de letras mayúsculas en inglés de longitud r.

□

El número de permutaciones-r de un conjunto con n elementos cuando se permite la repetición se da en el Teorema 4.4.1.

Teorema 4.4.1 El número de permutaciones-r de un conjunto de n objetos cuando se permite repetir objetos es n^r.

Demostración: Hay n formas de seleccionar un elemento del conjunto para cada una de las r posiciones en la permutación-r cuando se permite la repetición, porque para cada opción están disponibles todos los n objetos.

Por lo tanto, según la regla del producto, hay n^r permutaciones-r cuando se permite la repetición.

■

4.4.3. Combinaciones con Repetición

Considere estos ejemplos de combinaciones donde se permiten elementos repetidos.

Ejemplo 4.4.2 ¿Cuántas formas hay de seleccionar cuatro piezas de fruta de un cuenco que contiene manzanas, naranjas y peras si el orden en el que se seleccionan las piezas no importa, solo importa el tipo de fruta y no la pieza individual y por lo menos hay cuatro piezas de cada tipo de fruta en el tazón?

Solución: Para resolver este problema enumeramos todas las formas posibles de seleccionar la fruta. Hay 15 formas:

4 manzanas	4 naranjas	4 peras
3 manzanas, 1 naranja	3 manzanas, 1 pera	3 naranjas, 1 manzana
3 manzanas, 1 pera	3 peras, 1 manzana	3 peras, 1 naranja
2 manzanas, 2 naranjas	2 manzanas, 2 peras	2 naranjas, 2 peras
2 manzanas, 1 naranja, 1 pera	2 naranjas, 1 manzana, 1 pera	2 peras, 1 manzana, 1 naranja

La solución es el número de combinaciones-4 con repetición tomadas de un conjunto de tres elementos, {manzana, naranja, pera}.

□

Para resolver problemas de conteo más complejos de este tipo, necesitamos un método general para contar las combinaciones-r con repetición

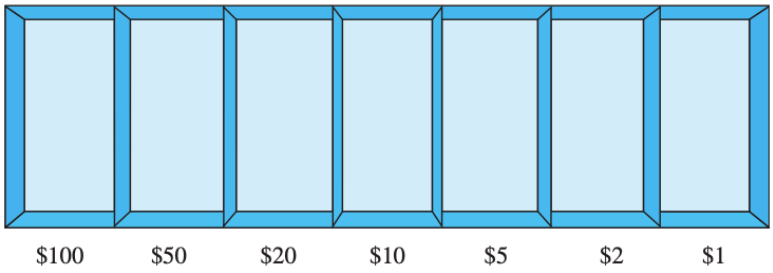


Figura 4.10: Caja de efectivo con siete tipos de billetes.

tomadas de un conjunto de n elementos. En el ejemplo 4.4.3 ilustraremos dicho método.

Ejemplo 4.4.3 ¿Cuántas formas hay de seleccionar cinco billetes de una caja de efectivo que contiene billetes de $1, billetes de $2, billetes de $5, billetes de $10, billetes de $20, billetes de $50 y billetes de $100? Suponga que el orden en el que se eligen los billetes no importa, que los billetes de cada denominación son indistinguibles y que hay al menos cinco billetes de cada tipo.

Solución: Debido a que el orden en que se seleccionan los billetes no importa y se pueden seleccionar siete tipos diferentes de billetes hasta cinco veces, este problema implica contar combinaciones-5 con repetición tomadas de un conjunto de siete elementos. Enumerar todas las posibilidades sería tedioso, porque hay una gran cantidad de soluciones. En su lugar, ilustraremos el uso de una técnica para contar combinaciones con repetición.

Suponga que una caja de efectivo tiene siete compartimentos, uno para cada tipo de billete, como se ilustra en la Figura 4.10. Estos compartimentos están separados por seis divisores, como se muestra en la imagen. La elección de cinco billetes corresponde a colocar cinco marcadores en los compartimentos que contienen diferentes tipos de billetes. La Figura 4.11 ilustra esta correspondencia para tres formas diferentes de seleccionar cinco billetes, donde los seis divisores están representados por barras y los cinco billetes por estrellas.

El número de formas de seleccionar cinco billetes corresponde al número de formas de organizar seis barras y cinco estrellas seguidas con un total de 11 posiciones. En consecuencia, el número de formas de seleccionar los cinco billetes es el número de formas de seleccionar las posiciones de las cinco estrellas de las 11 posiciones. Esto corresponde al número de selecciones

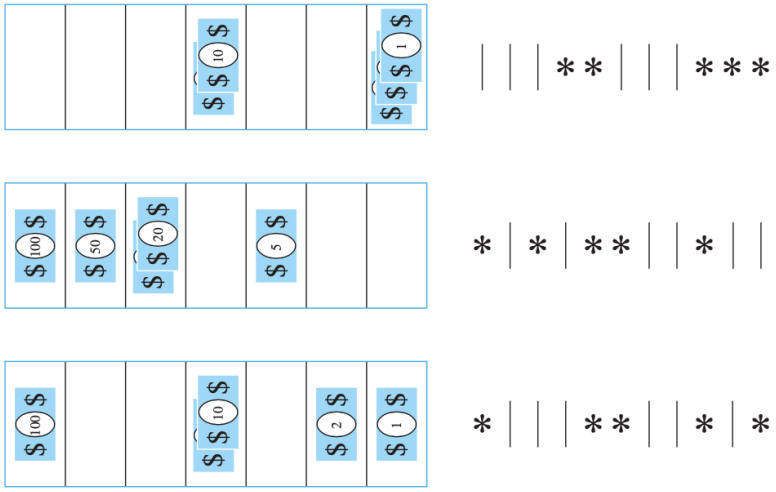


Figura 4.11: Ejemplos de formas de seleccionar cinco billetes.

desordenadas de 5 objetos de un conjunto de 11 objetos, que se pueden hacer en $C(11, 5)$ formas. En consecuencia, hay

$$C(11, 5) = \frac{11!}{5!6!} = 462$$

formas de elegir cinco billetes de la caja de efectivo con siete tipos de billetes. □

El Teorema 4.4.2 generaliza esta discusión.

Teorema 4.4.2 Hay $C(n+r-1, r) = C(n+r-1, n-1)$ combinaciones-r de un conjunto con n elementos cuando se permite la repetición de elementos.

Demostración: Cada combinación-r de un conjunto con n elementos cuando se permite la repetición puede ser representada por una lista de $n-1$ barras y r estrellas. Las $n-1$ barras se utilizan para marcar n celdas diferentes, con la i-ésima celda que contiene una estrella por cada vez que el i-ésimo elemento del conjunto ocurre en la combinación.

Por ejemplo, una combinación-6 de un conjunto con cuatro elementos se representa con tres barras y seis estrellas. Aquí

$$**|*|\ \ |***$$

representa la combinación que contiene exactamente dos del primer elemento, uno del segundo elemento, ninguno del tercer elemento y tres del cuarto elemento del conjunto.

Como hemos visto, cada lista diferente que contiene $n-1$ barras y r estrellas corresponde a una combinación-r del conjunto con n elementos, cuando se permite la repetición.

El número de dichas listas es $C(n-1+r, r)$, porque cada lista corresponde a una elección de las r posiciones para colocar las r estrellas de las $n-1+r$ posiciones que contienen r estrellas y $n-1$ barras.

El número de dichas listas también es igual a $C(n-1+r, n-1)$, porque cada lista corresponde a una elección de las $n-1$ posiciones para colocar las $n-1$ barras.

■

Los ejemplos del 4.4.4 al 4.4.6 muestran cómo se aplica el Teorema 4.4.2.

Ejemplo 4.4.4 Suponga que una tienda de galletas tiene cuatro tipos diferentes de galletas. ¿De cuántas formas diferentes se pueden elegir seis galletas? Suponga que sólo importa el tipo de galleta, y no las galletas individuales o el orden en que se eligen.

Solución: El número de formas de elegir seis galletas es el número de combinaciones-6 de un conjunto con cuatro elementos. Del Teorema 4.4.2 esto es igual a $C(4+6-1, 6) = C(9, 6)$. Porque

$$C(9,6) = C(9,3) = \frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3} = 84,$$

hay 84 formas diferentes de elegir las seis galletas.

□

El teorema 4.4.2 también se puede usar para encontrar el número de soluciones de ciertas ecuaciones lineales donde las variables son números enteros sujetos a restricciones. Esto se ilustra en el ejemplo 4.4.5

Ejemplo 4.4.5 ¿Cuántas soluciones tiene la ecuación

$$x_1 + x_2 + x_3 = 11,$$

donde x_1, x_2 y x_3 son números enteros no negativos?

Solución: Para contar el número de soluciones, observamos que una solución corresponde a una forma de seleccionar 11 elementos de un conjunto

con tres elementos de modo que se elijan x_1 elementos del tipo uno, x_2 elementos del tipo dos y x_3 elementos del tipo tres. Por lo tanto, el número de soluciones es igual al número de combinaciones-11 con repetición tomadas de un conjunto con tres elementos. Del Teorema 4.4.2 se deduce que existen

$$C(3 + 11 - 1, 11) = C(13, 11) = C(13, 2) = \frac{13 \cdot 12}{1 \cdot 2} = 78$$

soluciones.

El número de soluciones de esta ecuación también se puede encontrar cuando las variables están sujetas a restricciones. Por ejemplo, podemos encontrar el número de soluciones donde las variables son números enteros con $x_1 \geq 1, x_2 \geq 2$ y $x_3 \geq 3$. Una solución a la ecuación sujeta a estas restricciones corresponde a una selección de 11 elementos con x_1 elementos del tipo uno, x_2 elementos del tipo dos y x_3 elementos del tipo tres, donde, además, hay al menos un elemento del tipo uno, dos elementos del tipo dos y tres elementos del tipo tres. Por tanto, una solución corresponde a la elección de un elemento del tipo uno, dos del tipo dos y tres del tipo tres, junto con la elección de cinco elementos adicionales de cualquier tipo. Por el teorema 4.4.2 esto se puede hacer en

$$C(3 + 5 - 1, 5) = C(7, 5) = C(7, 2) = \frac{7 \cdot 6}{1 \cdot 2} = 21$$

maneras. Por lo tanto, hay 21 soluciones de la ecuación sujetas a las restricciones dadas.

□

Ejemplo 4.4.6 ¿Cuál es el valor de k después de que se haya ejecutado el pseudocódigo de la Figura 4.12?

Solución: Tenga en cuenta que el valor inicial de k es 0 y que 1 se suma a k cada vez que el bucle anidado se atraviesa con una secuencia de enteros $i_1, i_2, \ldots, i_m$ tal que

$$1 \leq i_m, i_{m-1} \leq \cdots \leq i_1 \leq n.$$

El número de tales secuencias de enteros es el número de formas de elegir m enteros de $\{1, 2, \ldots, n\}$, con la repetición permitida.

Para ver esto, tenga en cuenta que una vez que se ha seleccionado dicha secuencia, si ordenamos los enteros en la secuencia en orden no decreciente,

```
k := 0
for i_1 := 1 to n
    for i_2 := 1 to i_1
        .
        .
        .
        for i_m := 1 to i_{m-1}
            k := k + 1
```

Figura 4.12: Pseudocódigo para el Ejemplo 4.4.6.

esto define de forma única una asignación de $i_m, i_{m-1}, \ldots, i_1$. A la inversa, cada asignación de este tipo corresponde a un conjunto desordenado único. Por lo tanto, del Teorema 4.4.2, se deduce que $k = C(n+m-1, m)$ después de que se haya ejecutado este código.

□

Las fórmulas para el número de selecciones ordenadas y no ordenadas de r elementos, elegidos con y sin repetición de un conjunto con n elementos, se muestran en la Tabla 4.1.

Type	*Repetition Allowed?*	*Formula*
r-permutations	No	$\frac{n!}{(n-r)!}$
r-combinations	No	$\frac{n!}{r!\,(n-r)!}$
r-permutations	Yes	n^r
r-combinations	Yes	$\frac{(n+r-1)!}{r!\,(n-1)!}$

Tabla 4.1: Combinaciones y permutaciones con y sin repetición.

4.4.4. Permutaciones con Objetos Indistinguibles

Algunos elementos pueden ser indistinguibles en los problemas de conteo. Cuando este sea el caso, se debe tener cuidado de no contar las cosas más de

una vez. Considere el ejemplo 4.4.7.

Ejemplo 4.4.7 ¿Cuántas cadenas diferentes se pueden formar reordenando las letras de la palabra *SUCCESS*?

Solución: Debido a que algunas de las letras de *SUCCESS* son las mismas, la respuesta no está dada por el número de permutaciones de siete letras. Esta palabra contiene tres S, dos C, una U y una E. Para determinar el número de cadenas diferentes que se pueden formar reordenando las letras, primero tenga en cuenta que las tres S se pueden colocar entre las siete posiciones en $C(7,3)$ diferentes formas, dejando cuatro posiciones libres. Luego, las dos C se pueden colocar en $C(4,2)$ formas, dejando dos posiciones libres. La U se puede colocar en $C(2,1)$ formas, dejando solo una posición libre. Por lo tanto, E se puede colocar en la forma $C(1,1)$. En consecuencia, a partir de la regla del producto, el número de cadenas diferentes que se pueden hacer es

$$\begin{aligned} C(7,3)C(4,2)C(2,1)C(1,1) &= \frac{7!}{3!4!} \cdot \frac{4!}{2!2!} \cdot \frac{2!}{1!1!} \cdot \frac{1!}{1!0!} \\ &= \frac{7!}{3!2!1!1!} \\ &= 420. \end{aligned}$$

□

Podemos demostrar el Teorema 4.4.3 usando el mismo tipo de razonamiento que en el ejemplo 4.4.7.

Teorema 4.4.3 El número de permutaciones diferentes de n objetos, donde hay n_1 objetos indistinguibles de tipo 1, n_2 objetos indistinguibles de tipo 2, ..., y n_k objetos indistinguibles de tipo k, es

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

Demostración: Para determinar el número de permutaciones, primero tenga en cuenta que los n_1 objetos de tipo uno se pueden colocar entre las n posiciones en $C(n, n_1)$ formas, dejando $n - n_1$ posiciones libres. Luego, los objetos de tipo dos se pueden colocar en $C(n - n_1, n_2)$ formas, dejando $n - n_1 - n_2$ posiciones libres. Continúe colocando los objetos de tipo tres, ..., tipo $k - 1$, hasta que en la última etapa, n_k objetos de tipo k se puedan

colocar en $C(n - n_1 - n_2 - \cdots - n_{k-1}, n_k)$ formas. Por tanto, según la regla del producto, el número total de diferentes permutaciones es

$$\begin{aligned} & C(n, n_1)C(n - n_1, n_2) \cdots C(n - n_1 - \cdots - n_{k-1}, n_k) \\ = & \frac{n!}{n_1!(n - n_1)!} \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \cdots \frac{(n - n_1 - \cdots - n_{k-1})!}{n_k!0!} \\ = & \frac{n!}{n_1!n_2! \cdots n_k!}. \end{aligned}$$

■

4.4.5. Ejercicios

1. ¿De cuántas formas diferentes se pueden seleccionar cinco elementos en orden de un conjunto con tres elementos cuando se permite la repetición?

2. ¿De cuántas formas diferentes se pueden seleccionar cinco elementos en orden de un conjunto con cinco elementos cuando se permite la repetición?

3. Todos los días, un estudiante elige al azar un sándwich para el almuerzo de entre una pila de sándwiches envueltos. Si hay seis tipos de sándwiches, ¿de cuántas formas diferentes hay para que el estudiante elija sándwiches para los siete días de la semana si el orden en el que se eligen los sándwiches es importante?

4. ¿Cuántas formas diferentes hay de elegir una docena de donas de las 21 variedades en una tienda de donas?

5. ¿Cuántas cadenas diferentes se pueden hacer a partir de las letras de MISSISSIPPI, usando todas las letras?

6. Un estudiante tiene tres mangos, dos papayas y dos kiwis. Si el estudiante come una pieza de fruta cada día, y sólo importa el tipo de fruta, ¿de cuántas formas diferentes se pueden consumir estas frutas?

7. ¿Cuántas formas hay de repartir manos de siete cartas a cada uno de cinco jugadores de una baraja estándar de 52 cartas?

Capítulo 5

Grafos

Los grafos son estructuras discretas que constan de vértices y aristas que conectan estos vértices. Hay diferentes tipos de grafos, dependiendo de si las aristas tienen direcciones, si varias aristas pueden conectar el mismo par de vértices y si se permiten ciclos. Los problemas en casi todas las disciplinas imaginables se pueden resolver utilizando modelos de grafos.

Daremos ejemplos para ilustrar cómo se utilizan los grafos como modelos en una variedad de áreas. Por ejemplo, mostraremos cómo se usan los grafos para representar la competencia de diferentes especies en un nicho ecológico, cómo se usan los grafos para representar quién influye en quién en una organización y cómo se usan los grafos para representar los resultados de los torneos de todos contra todos.

Describiremos cómo se pueden utilizar los grafos para modelar relaciones entre personas, colaboración entre investigadores, llamadas telefónicas entre números de teléfono y enlaces entre sitios web. Mostraremos cómo se pueden utilizar los grafos para modelar hojas de ruta y la asignación de trabajos a los empleados de una organización.

Usando modelos de grafos, podemos determinar si es posible caminar por todas las calles de una ciudad sin tener que recorrer una calle dos veces, y podemos encontrar la cantidad de colores necesarios para colorear las regiones de un mapa. Se pueden usar grafos para determinar si un circuito se puede implementar en una placa de circuito plana.

Podemos distinguir entre dos compuestos químicos con la misma fórmula molecular pero diferentes estructuras usando grafos. Podemos determinar si dos computadoras están conectadas por un enlace de comunicaciones usando modelos de grafos de redes de computadoras. Los grafos con pesos asignados a

sus aristas se pueden usar para resolver problemas como encontrar el camino más corto entre dos ciudades en una red de transporte.

También podemos utilizar grafos para programar exámenes y asignar canales a estaciones de televisión. Este capítulo introducirá los conceptos básicos de la teoría de grafos y presentará muchos modelos de grafos diferentes. Para resolver la amplia variedad de problemas que se pueden estudiar utilizando grafos, presentaremos muchos algoritmos de grafos diferentes. También estudiaremos la complejidad de estos algoritmos.

5.1. Grafos y Modelos de Grafos

Empezamos con la definición de un grafo.

Definición 5.1.1 Un grafo $G = (V, E)$ consta de V, un conjunto no vacío de *vértices* (o *nodos*) y E, un conjunto de *aristas*. Cada arista tiene uno o dos vértices asociados, llamados *puntos finales*. Se dice que una arista *conecta* sus puntos finales.

Observación 5.1.1 El conjunto de vértices V de un grafo G puede ser infinito. Un grafo con un conjunto de vértices infinito o un número infinito de aristas se llama **grafo infinito** y, en comparación, un grafo con un conjunto de vértices finito y un conjunto de aristas finito se llama **grafo finito**. En este libro, por lo general, consideraremos sólo grafo finitos.

□

Ahora suponga que una red está formada por centros de datos y enlaces de comunicación entre computadoras. Podemos representar la ubicación de cada centro de datos por un punto y cada enlace de comunicaciones por un segmento de línea, como se muestra en la Figura 5.1.

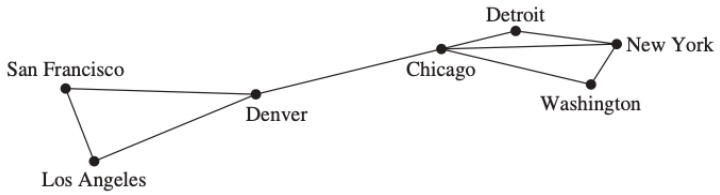


Figura 5.1: Una red de computadoras.

Esta red de computadoras se puede modelar mediante un grafo en el que los vértices del grafo representan los centros de datos y las aristas representan los enlaces de comunicación.

En general, visualizamos grafos usando puntos para representar vértices y segmentos de línea, posiblemente curvos, para representar aristas, donde los puntos finales de un segmento de línea que representa una arista son los puntos que representan los puntos finales de la arista.

Cuando dibujamos un grafo, generalmente tratamos de dibujar las aristas para que no se crucen. Sin embargo, esto no es necesario porque se puede usar cualquier representación que use puntos para representar vértices y cualquier forma de conexión entre vértices.

De hecho, hay algunos grafos que no se pueden dibujar en el plano sin que las aristas se crucen. El punto clave es que la forma en que dibujamos un grafo es arbitraria, siempre que se describan las conexiones correctas entre los vértices.

Tenga en cuenta que cada arista del grafo que representa esta red de computadoras conecta dos vértices diferentes. Es decir, ninguna arista conecta un vértice consigo mismo. Además, no hay dos aristas diferentes que conecten el mismo par de vértices.

Un grafo en el que cada arista conecta dos vértices diferentes y donde no hay dos aristas que conecten el mismo par de vértices se llama grafo simple. Tenga en cuenta que en un grafo simple, cada arista está asociado a un par de vértices desordenado, y ninguna otra arista está asociada a esta misma arista.

En consecuencia, cuando hay una arista de un grafo simple asociado a $\{u, v\}$, también podemos decir, sin posible confusión, que $\{u, v\}$ es una arista del grafo.

Una red de computadoras puede contener múltiples enlaces entre los centros de datos, como se muestra en la Figura 5.2.

Para modelar tales redes, necesitamos grafos que tengan más de una arista que conecte el mismo par de vértices. Los grafos que pueden tener múltiples aristas que conectan los mismos vértices se denominan **multigrafos**.

Cuando hay m aristas diferentes asociadas al mismo par desordenado de vértices $\{u, v\}$, también decimos que $\{u, v\}$ es una arista de multiplicidad m. Es decir, podemos pensar en este conjunto de aristas como m copias diferentes de una arista $\{u, v\}$.

A veces, un enlace de comunicaciones conecta un centro de datos consigo mismo, tal vez un circuito de retroalimentación con fines de diagnóstico. Tal

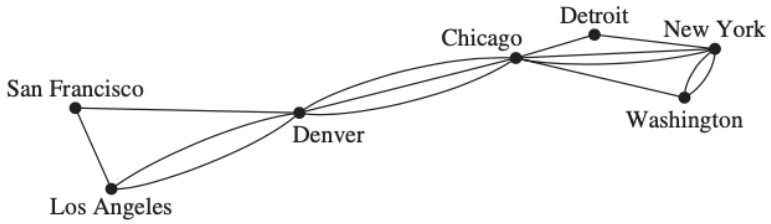


Figura 5.2: Una red de computadoras con enlaces múltiples entre los centros de datos.

red se ilustra en la Figura 5.3.

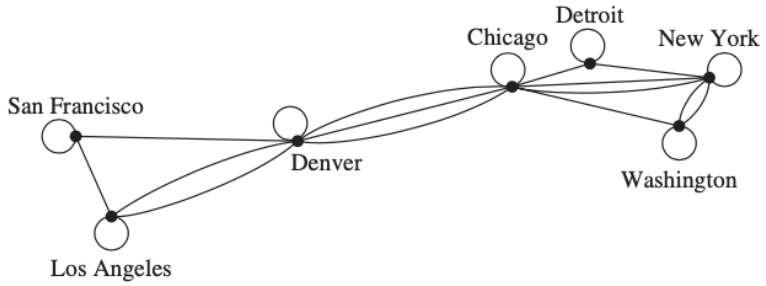


Figura 5.3: Una red de computadoras con enlaces de diagnóstico.

Para modelar esta red, necesitamos incluir aristas que conecten un vértice consigo mismo. Estas aristas se denominan **ciclos** y, a veces, incluso podemos tener más de un ciclo en un vértice.

Los grafos que pueden incluir ciclos y posiblemente varias aristas que conectan el mismo par de vértices a veces se denominan **pseudografos**.

Hasta ahora, los grafos que hemos introducido son **grafos no dirigidos**. También se dice que sus aristas **no están dirigidas**. Sin embargo, para construir un modelo de grafos, puede ser necesario asignar direcciones a las aristas de un grafo.

Por ejemplo, en una red de computadoras, algunos enlaces pueden operar en una sola dirección (tales enlaces se denominan líneas dúplex simples). Este puede ser el caso si se envía una gran cantidad de tráfico a algunos centros de datos, con poco o ningún tráfico en la dirección opuesta. Tal red se muestra en la Figura 5.4.

Para modelar una red de computadoras de este tipo, utilizamos un grafo

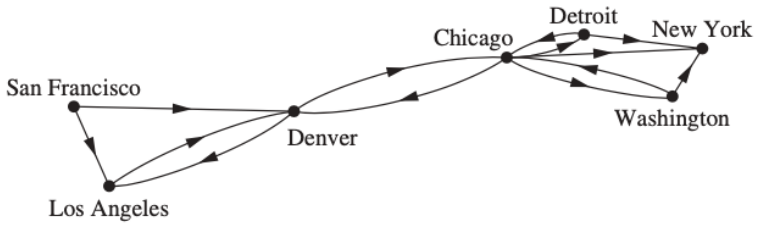


Figura 5.4: Una red de computadoras con enlaces de comunicación en un solo sentido.

dirigido. Cada arista de un grafo dirigido está asociada a un par ordenado. La definición de grafo dirigido que damos aquí es más general que la que enunciamos en el Capítulo 2, donde usamos grafos dirigidos para representar relaciones.

Definición 5.1.2 Un *grafo dirigido* (o *digrafo*) (V, E) consiste en un conjunto no vacío de vértices V y un conjunto de *aristas dirigidas* (o *arcos*) E. Cada arista dirigida está asociada con un par ordenado de vértices. Se dice que la arista dirigida asociada con el par ordenado (u, v) *comienza* en u y *termina* en v.

Cuando representamos un grafo dirigido con un dibujo lineal, usamos una flecha que apunta de u a v para indicar la dirección de una arista que comienza en u y termina en v. Un grafo dirigido puede contener ciclos y puede contener múltiples aristas dirigidas que comienzan y terminan en los mismos vértices.

Un grafo dirigido también puede contener aristas dirigidas que conectan los vértices u y v en ambas direcciones; es decir, cuando un digrafo contiene una arista de u a v, también puede contener una o más aristas de v a u. Tenga en cuenta que obtenemos un grafo dirigido cuando asignamos una dirección a cada arista en un grafo no dirigido.

Cuando un grafo dirigido no tiene ciclos y no tiene múltiples aristas dirigidas, se denomina **grafo dirigido simple**. Debido a que un grafo dirigido simple tiene como máximo una arista asociada a cada par ordenado de vértices (u, v), llamamos a (u, v) una arista si hay una arista asociada a él en el grafo.

En algunas redes de computadoras, pueden estar presentes múltiples en-

laces de comunicación entre dos centros de datos, como se ilustra en la Figura 5.5.

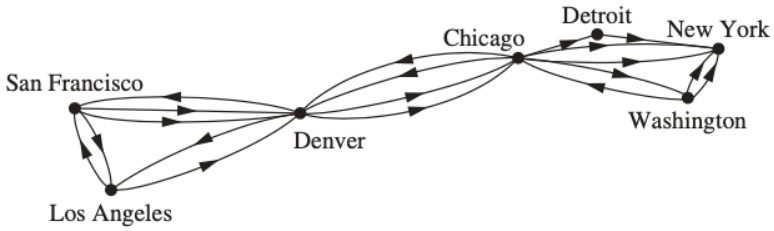


Figura 5.5: Una red de computadoras con múltiples enlaces de un solo sentido.

Los grafos dirigidos que pueden tener **múltiples aristas dirigidas** desde un vértice a un segundo vértice (posiblemente el mismo) se utilizan para modelar dichas redes. A estos grafos los llamamos **multigrafos dirigidos**. Cuando hay m aristas dirigidas, cada una asociada a un par ordenado de vértices (u, v), decimos que (u, v) es una arista de **multiplicidad** m.

Para algunos modelos, es posible que necesitemos un grafo en el que algunas aristas no estén dirigidas, mientras que otras sí. Un grafo con aristas tanto dirigidas como no dirigidas se llama **grafo mixto**. Por ejemplo, un grafo mixto podría usarse para modelar una red de computadoras que contiene enlaces que operan en ambas direcciones y otros enlaces que operan sólo en una dirección.

Esta terminología para los diversos tipos de grafos se resume en la Tabla 5.1. A veces usaremos el término grafo como un término general para describir grafos con aristas dirigidas o no dirigidas (o ambas), con o sin ciclos y con o sin múltiples aristas. En otras ocasiones, cuando el contexto sea claro, usaremos el término grafo para referirnos sólo a grafos no dirigidos.

Debido al interés relativamente moderno en la teoría de grafos, y debido a que tiene aplicaciones en una amplia variedad de disciplinas, se han introducido muchas terminologías diferentes de la teoría de grafos. El lector debe determinar cómo se utilizan esos términos cada vez que se encuentran.

La terminología utilizada por los matemáticos para describir los grafos se ha estandarizado cada vez más, pero la terminología utilizada para discutir los grafos cuando se utilizan en otras disciplinas sigue siendo bastante variada.

Aunque la terminología utilizada para describir los grafos puede variar, tres preguntas clave pueden ayudarnos a comprender la estructura de un grafo:

TABLE 1 Graph Terminology.

Type	*Edges*	*Multiple Edges Allowed?*	*Loops Allowed?*
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and undirected	Yes	Yes

Tabla 5.1: Terminología en Teoría de Grafos.

- ¿Las aristas del grafo no están dirigidas o están dirigidas (o ambas)?
- Si el grafo no está dirigido, ¿existen múltiples aristas que conectan el mismo par de vértices? Si el grafo está dirigido, ¿existen múltiples aristas dirigidas?
- ¿Hay ciclos?

Responder a estas preguntas nos ayuda a comprender los grafos. Es menos importante recordar la terminología particular utilizada.

5.1.1. Modelos de Grafos

Los grafos se utilizan en una amplia variedad de modelos. Comenzamos esta sección describiendo cómo construir modelos de grafos para redes de comunicaciones que enlazan centros de datos. Completaremos esta sección describiendo algunos modelos de grafos para algunas aplicaciones interesantes. Regresaremos a muchas de estas aplicaciones más adelante en este capítulo.

Introduciremos modelos de grafos adicionales en las secciones siguientes de este capítulo. Además, recuerde que los modelos de grafos dirigidos para algunas aplicaciones se introdujeron en el Capítulo 2. Cuando construimos un modelo basado en grafos, debemos asegurarnos de haber respondido correctamente las tres preguntas clave que planteamos sobre la estructura de un grafo.

REDES SOCIALES Los grafos se utilizan ampliamente para modelar estructuras sociales basadas en diferentes tipos de relaciones entre personas o grupos de personas. Estas estructuras sociales, y los grafos que las representan, se conocen como **redes sociales**.

En estos modelos de grafos, los individuos u organizaciones están representados por vértices; las relaciones entre individuos u organizaciones están representadas por aristas. El estudio de las redes sociales es un área multidisciplinaria extremadamente activa, y se han estudiado muchos tipos diferentes de relaciones entre personas a través de ellas. Aquí presentaremos algunas de las redes sociales más estudiadas.

Ejemplo 5.1.1 Grafos de conocidos y amistades Podemos usar un grafo simple para representar si dos personas se conocen, es decir, si se conocen o si son amigos (ya sea en el mundo real o en el mundo virtual a través de un sitio de redes sociales como Facebook).

Cada persona de un grupo particular de personas está representada por un vértice. Una arista no dirigida se usa para conectar a dos personas cuando estas personas se conocen entre sí, cuando nos preocupamos sólo por si son conocidos o si son amigos.

No se utilizan aristas múltiples y, por lo general, no se utilizan ciclos. (Si queremos incluir la noción de autoconocimiento, incluiríamos ciclos). En la Figura 5.6 se muestra un pequeño grafo de conocidos. ¡El grafo de conocidos de todas las personas del mundo tiene más de seis mil millones de vértices y probablemente más de un billón de aristas! Discutiremos este grafo más a fondo en la Sección **??**.

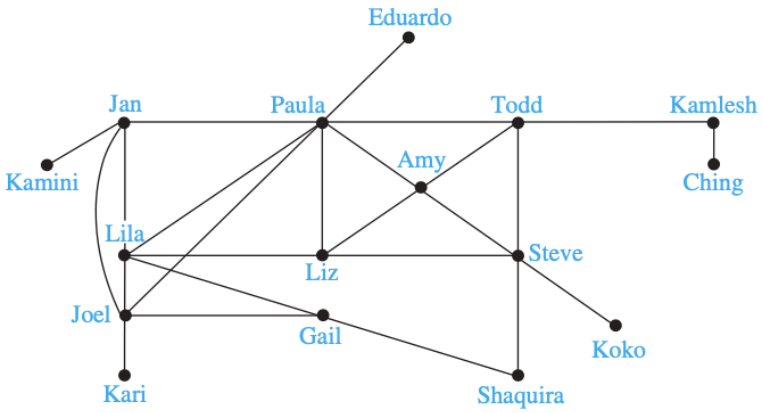


Figura 5.6: Un grafo de conocidos.

□

Ejemplo 5.1.2 Grafos de influencia En los estudios de comportamiento grupal se observa que determinadas personas pueden influir en el pensamiento de otras. Se puede utilizar un grafo dirigido llamado **grafo de influencia** para modelar este comportamiento.

Cada persona del grupo está representada por un vértice. Hay una arista dirigida desde el vértice a al vértice b cuando la persona representada por el vértice a puede influir en la persona representada por el vértice b. Este grafo no contiene ciclos y no contiene múltiples aristas dirigidas.

En la Figura 5.7 se muestra un ejemplo de un grafo de influencia para los miembros de un grupo. En el grupo modelado por este grafo de influencia, Deborah no puede ser influenciada, pero puede influir en Brian, Fred y Linda. Además, Yvonne y Brian pueden influirse mutuamente.

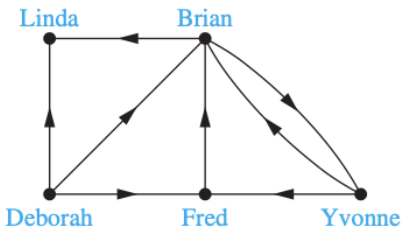


Figura 5.7: Un grafo de influencia.

□

Ejemplo 5.1.3 Grafos de colaboración Un **grafo de colaboración** se utiliza para modelar redes sociales donde dos personas están relacionadas trabajando juntas de una manera particular.

Los grafos de colaboración son grafos simples, ya que las aristas de estos grafos no están dirigidas y no hay múltiples aristas o ciclos. Los vértices en estos grafos representan personas; dos personas están conectadas por una arista no dirigida cuando las personas han colaborado. No hay ciclos ni aristas múltiples en estos grafos.

El **grafo de Hollywood** es un grafo de colaboración que representa a los actores por vértices y conecta a dos actores con una arista si han trabajado juntos en una película o programa de televisión. El grafo de Hollywood es un grafo enorme con más de 2,9 millones de vértices (a principios de 2018). Discutiremos algunos aspectos del grafo de Hollywood más adelante en la Sección **??**.

En un **grafo de colaboración académica**, los vértices representan a personas (quizás restringidos a miembros de una determinada comunidad académica) y las aristas vinculan a dos personas si han publicado un artículo de forma conjunta.

En 2004 se encontró que el grafo de colaboración para personas que han publicado artículos de investigación en matemáticas tiene más de 400,000 vértices y 675,000 aristas, y estos números han crecido considerablemente desde entonces.

Tendremos más que decir sobre este grafo en la Sección **??**. Los grafos de colaboración también se han utilizado en el deporte, donde se considera que dos deportistas profesionales han colaborado si alguna vez han jugado en el mismo equipo durante una temporada regular de su deporte.

□

REDES DE COMUNICACIÓN Podemos modelar diferentes redes de comunicaciones utilizando vértices para representar dispositivos y aristas para representar el tipo particular de enlaces de comunicaciones de interés. Ya hemos modelado una red de datos en la primera parte de esta sección.

Ejemplo 5.1.4 Grafos de llamadas Los grafos se pueden utilizar para modelar las llamadas telefónicas realizadas en una red, como una red telefónica de larga distancia. En particular, se puede utilizar un grafo múltiple dirigido para modelar llamadas en las que cada número de teléfono está representado por un vértice y cada llamada telefónica está representada por una arista dirigida.

La arista que representa una llamada comienza en el número de teléfono desde el que se realizó la llamada y termina en el número de teléfono al que se realizó la llamada. Necesitamos aristas dirigidas porque la dirección en la que se realiza la llamada es importante. Necesitamos múltiples aristas dirigidas porque queremos representar cada llamada realizada desde un número de teléfono particular a un segundo número.

En la Figura 5.8 (a) se muestra un pequeño grafo de llamadas telefónicas, que representa siete números de teléfono. Este grafo muestra, por ejemplo, que se han realizado tres llamadas del 732-555-1234 al 732-555-9876 y dos en la otra dirección, pero no se han realizado llamadas del 732-555-4444 a ninguno de los otros seis números excepto 732-555-0011.

Cuando sólo nos importa si ha habido una llamada que conecta dos números de teléfono, usamos un grafo no dirigido con una arista que conecta

números de teléfono cuando ha habido una llamada entre estos números. Esta versión del grafo de llamadas se muestra en la Figura 5.8 (b).

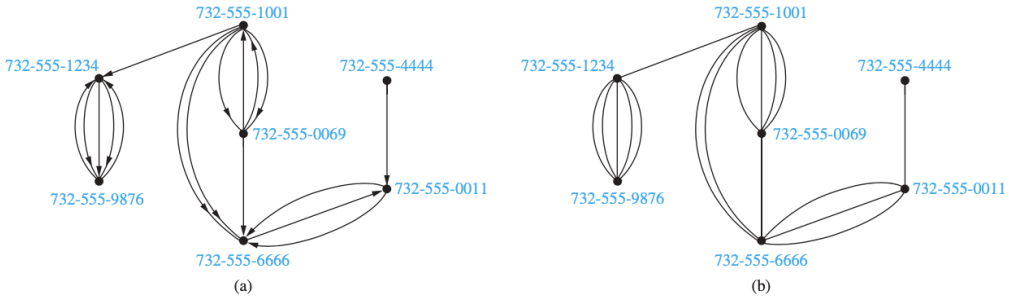


Figura 5.8: Grafos de llamadas. En (a) importa el origen y el destino de la llamada, en (b) sólo importa que hubo una llamada entre los números correspondientes.

Los grafos de llamadas que modelan las actividades de llamadas reales pueden ser enormes. Por ejemplo, un grafo de llamadas estudiado en AT&T, que modela llamadas durante 20 días, tiene alrededor de 290 millones de vértices y 4 mil millones de aristas. Discutiremos los grafos de llamadas con más detalle en la Sección **??**.

□

Ejemplo 5.1.5 El grafo de la Web La web se puede modelar como un grafo dirigido donde cada página web está representada por un vértice y donde una arista comienza en la página web a y termina en la página web b si hay un enlace en a apuntando a b.

Debido a que se crean nuevas páginas web y otras se eliminan en algún lugar de la web casi cada segundo, el grafo de la web cambia de forma casi continua. Mucha gente está estudiando las propiedades del grafo de la web para comprender mejor la naturaleza de la web. Regresaremos a los grafos de la web en la Sección **??**.

□

Ejemplo 5.1.6 Grafos de citas Los grafos se pueden utilizar para representar citas en diferentes tipos de documentos, incluidos artículos académicos, patentes y opiniones legales. En tales grafos, cada documento está representado por un vértice, y hay una arista de un documento a un segundo documento si el primer documento cita al segundo en su lista de citas.

En un artículo académico, la lista de citas es la bibliografía, o lista de referencias; en una patente, es la lista de patentes anteriores que se citan; y en una opinión legal es la lista de opiniones anteriores citadas. El grafo de citas es un grafo dirigido sin ciclos ni aristas múltiples.

□

APLICACIONES DE DISEÑO DE SOFTWARE Los modelos de grafos son herramientas útiles en el diseño de software. Describiremos brevemente dos de estos modelos aquí.

Ejemplo 5.1.7 Grafos de dependencias de módulos Una de las tareas más importantes en el diseño de software es cómo estructurar un programa en diferentes partes o módulos. Comprender cómo interactúan los diferentes módulos de un programa es esencial no sólo para el diseño del programa, sino también para la prueba y el mantenimiento del software resultante.

Un **grafo de dependencias de módulos** proporciona una herramienta útil para comprender cómo interactúan los diferentes módulos de un programa. En un grafo de dependencias de un programa, cada módulo está representado por un vértice. Hay una arista dirigida de un módulo a un segundo módulo si el segundo módulo depende del primero. En la Figura 5.9 se muestra un ejemplo de un grafo de dependencias del programa para un navegador web.

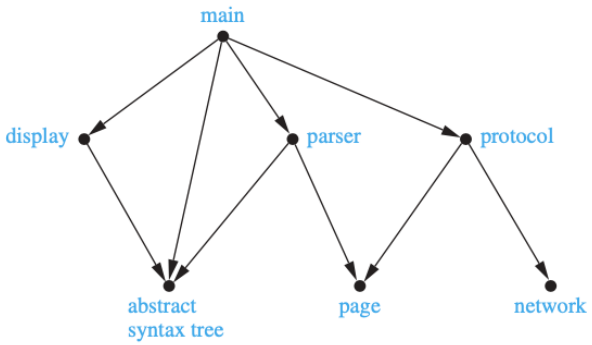


Figura 5.9: Un grafo de dependencias de módulos.

□

Ejemplo 5.1.8 Grafos de precedencia y procesamiento concurrente Los programas de computadora se pueden ejecutar más rápidamente ejecu-

tando ciertas instrucciones al mismo tiempo. Es importante no ejecutar una instrucción que requiera resultados de instrucciones aún no ejecutadas.

La dependencia de instrucciones sobre instrucciones anteriores se puede representar mediante un grafo dirigido. Cada instrucción está representada por un vértice, y hay una arista de una instrucción a una segunda instrucción si la segunda instrucción no se puede ejecutar antes que la primera instrucción. Este grafo resultante se llama **grafo de precedencia**.

Un programa de computadora y su grafo se muestran en la Figura 5.10. Por ejemplo, el grafo muestra que la instrucciones S_5 no se puede ejecutar antes de que se ejecuten las instrucciones S_1, S_2 y S_4.

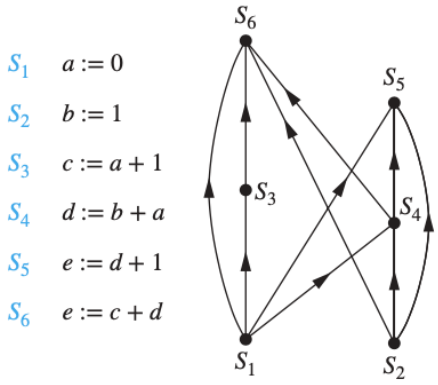


Figura 5.10: Un grafo de precedencias.

□

REDES DE TRANSPORTE Podemos usar grafos para modelar muchos tipos diferentes de redes de transporte, incluidas las redes de carreteras, aéreas y ferroviarias, así como las redes de envío.

Ejemplo 5.1.9 Rutas de aerolíneas Podemos modelar las redes de aerolíneas representando cada aeropuerto por un vértice.

Concretamente, podemos modelar todos los vuelos de una aerolínea en particular cada día usando una arista dirigida para representar cada vuelo, yendo desde el vértice que representa el aeropuerto de salida hasta el vértice que representa el aeropuerto de destino.

El grafo resultante generalmente será un multigrafo dirigido, ya que puede haber varios vuelos de un aeropuerto a otro aeropuerto durante el mismo día.

□

Ejemplo 5.1.10 Redes de carreteras Los grafos se pueden utilizar para modelar redes de carreteras. En tales modelos, los vértices representan intersecciones y las aristas representan carreteras. Cuando todas las carreteras son de dos vías y hay como máximo una carretera que conecta dos intersecciones, podemos usar un grafo simple no dirigido para modelar la red de carreteras.

Sin embargo, a menudo queremos modelar redes de carreteras cuando algunas son de un solo sentido y cuando puede haber más de una carretera entre dos intersecciones. Para construir tales modelos, usamos aristas no dirigidas para representar caminos de dos sentidos y usamos aristas dirigidas para representar caminos de un solo sentido.

Múltiples aristas no dirigidas representan múltiples caminos de dos vías que conectan las mismas dos intersecciones. Múltiples aristas dirigidas representan múltiples caminos de un solo sentido que comienzan en una intersección y terminan en una segunda intersección. Los ciclos representan caminos de ciclo.

Se necesitan grafos mixtos para modelar redes de carreteras que incluyan carreteras de un solo sentido y de dos sentidos.

□

REDES BIOLÓGICAS Muchos aspectos de las ciencias biológicas se pueden modelar utilizando grafos.

Ejemplo 5.1.11 Grafos de superposición de nichos en ecología Los grafos se utilizan en muchos modelos que involucran la interacción de diferentes especies de animales. Por ejemplo, la competencia entre especies en un ecosistema se puede modelar utilizando un grafo de superposición de nichos.

Cada especie está representada por un vértice. Una arista no dirigida conecta dos vértices si las dos especies representadas por estos vértices compiten (es decir, algunos de los recursos alimenticios que utilizan son los mismos).

Un grafo de superposición de nichos es un grafo simple porque no se necesitan ciclos ni aristas múltiples en este modelo. El grafo de la Figura 5.11 modela el ecosistema de un bosque. Vemos en este grafo que las ardillas y los mapaches compiten pero que los cuervos y las musarañas no lo hacen.

□

Ejemplo 5.1.12 Grafos de interacción de proteínas Una interacción de proteínas en una célula viva ocurre cuando dos o más proteínas en esa célula se unen para realizar una función biológica. Debido a que las interacciones

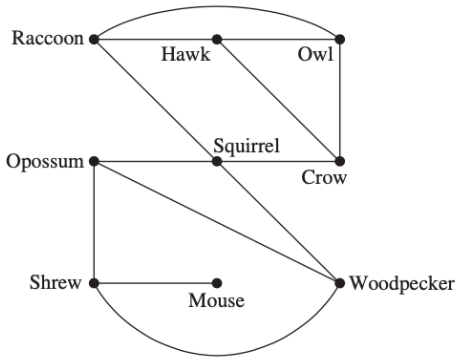


Figura 5.11: Un grafo de superposición de nichos.

de proteínas son cruciales para la mayoría de las funciones biológicas, muchos científicos trabajan para descubrir nuevas proteínas y comprender las interacciones entre proteínas.

Las interacciones de proteínas dentro de una célula se pueden modelar utilizando un grafo de interacción de proteínas (también llamado red de interacción proteína-proteína), un grafo no dirigido en el que cada proteína está representada por un vértice, con una arista que conecta los vértices que representan cada par de proteínas. que interactúan.

Es un problema difícil determinar las interacciones de proteínas genuinas en una célula, ya que los experimentos a menudo producen falsos positivos, que concluyen que dos proteínas interactúan cuando en realidad no lo hacen.

Los grafos de interacción de proteínas se pueden utilizar para deducir información biológica importante, por ejemplo, mediante la identificación de las proteínas más importantes para diversas funciones y la funcionalidad de proteínas recién descubiertas.

Debido a que hay miles de proteínas diferentes en una célula típica, el grafo de interacción de proteínas de una célula es extremadamente grande y complejo.

Por ejemplo, las células de levadura tienen más de 6.000 proteínas y se conocen más de 80.000 interacciones entre ellas, y las células humanas tienen más de 100.000 proteínas, con quizás hasta 1.000.000 de interacciones entre ellas.

Se agregan vértices y aristas adicionales a un grafo de interacción de proteínas cuando se descubren nuevas proteínas e interacciones entre proteínas. Debido a la complejidad de los grafos de interacción de proteínas, a menudo

se dividen en grafos más pequeños llamados módulos que representan grupos de proteínas que participan en una función particular de una célula.

La Figura 5.12 ilustra un módulo del grafo de interacción de proteínas descrito en [Bo04], que comprende el complejo de proteínas que degradan el ARN en células humanas. Para obtener más información sobre los grafos de interacción de proteínas, consulte [Bo04], [Ne10] y [Hu07].

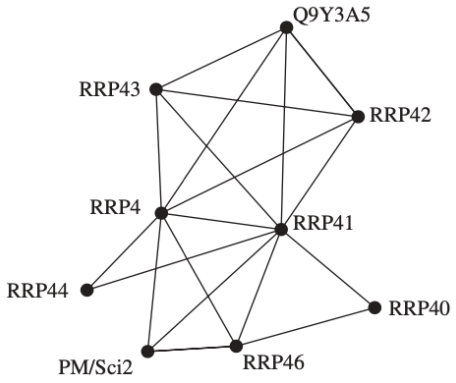


Figura 5.12: Un módulo de un grafo de interacción de proteinas.

□

Redes semánticas Los modelos de grafos se utilizan ampliamente en la comprensión del lenguaje natural y en la recuperación de información. La comprensión del lenguaje natural (NLU) consiste en lograr que las máquinas desensamblen y analicen el habla humana.

Su objetivo es permitir que las máquinas comprendan y se comuniquen como lo hacen los humanos. La recuperación de información (IR) trata de la obtención de información de una colección de fuentes basada en varios tipos de búsquedas. La comprensión del lenguaje natural es la tecnología habilitadora cuando conversamos con agentes automatizados de servicio al cliente.

Los avances en NLU son evidentes a medida que la comunicación entre humanos y máquinas mejora continuamente. Cuando hacemos búsquedas en la web, aprovechamos los muchos avances en la recuperación de información realizados en las últimas décadas.

En los modelos de grafos para aplicaciones NLU e IR, los vértices a menudo representan palabras, frases u oraciones, y las aristas representan conexiones relacionadas con el significado de estos objetos.

Ejemplo 5.1.13 En las **redes semánticas**, los vértices se utilizan para representar palabras y las aristas no dirigidas se utilizan para conectar los vértices cuando existe una relación semántica entre estas palabras.

Una relación semántica es una relación entre dos o más palabras que se basa en el significado de las palabras. Por ejemplo, podemos construir un grafo en el que los vértices representan sustantivos y dos vértices están conectados cuando tienen un significado similar. Otro ejemplo, los nombres de diferentes países tienen un significado similar, al igual que los nombres de diferentes verduras.

Para determinar qué sustantivos tienen un significado similar, se pueden examinar grandes volúmenes de texto. Se supone que los sustantivos en el texto que están separados por una conjunción (como "o" o "y") o una coma, o que aparecen en listas, tienen un significado similar. Por ejemplo, al examinar libros sobre agricultura, podemos determinar que los sustantivos que representan nombres de frutas, como aguacate, fruta del pan, guayaba, mango, papaya y guanábana, tienen un significado similar.

Los investigadores que adoptaron este enfoque utilizando el British National Corpus, una colección de textos en inglés con 100.000.000 de palabras, produjeron un grafo con cerca de 100.000 vértices, que representan sustantivos y 500.000 enlaces, conectando vértices que representan pares de palabras con significado similar.

La Figura 5.13 muestra un pequeño grafo donde los vértices representan sustantivos y las aristas conectan palabras con un significado similar. Este grafo se centra en la palabra mouse. El grafo ilustra que hay dos significados distintos para mouse. Puede referirse a un animal o puede referirse a hardware de computadora.

Cuando un programa de NLU encuentra la palabra mouse en una oración, puede ver qué palabras con un significado similar encajarían en la oración para ayudar a determinar si mouse se refiere a un animal o hardware de computadora en esa oración.

□

TORNEOS A continuación, damos algunos ejemplos que muestran cómo los grafos también se pueden utilizar para modelar diferentes tipos de torneos.

Ejemplo 5.1.14 Torneos Round-Robin Un torneo en el que cada equipo juega contra todos los demás equipos exactamente una vez y no se permiten empates se denomina torneo round-robin. Estos torneos se pueden mode-

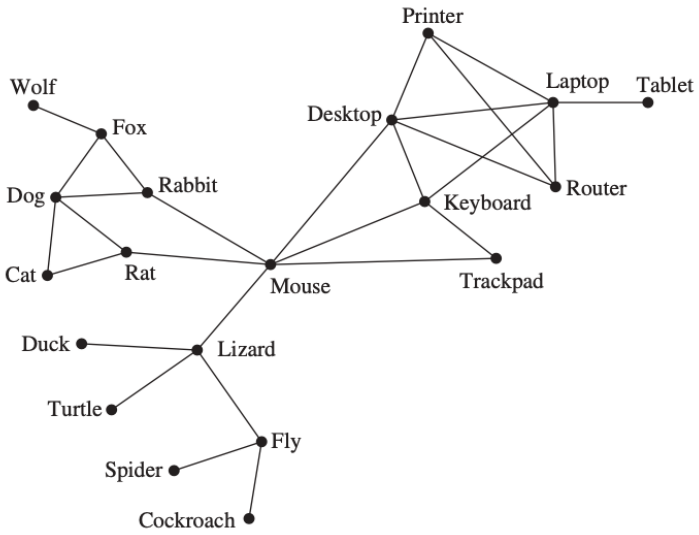


Figura 5.13: Una red semántica de sustantivos con un significado similar centrada en la palabra mouse.

lar utilizando grafos dirigidos donde cada equipo está representado por un vértice.

Tenga en cuenta que (a, b) es una arista si el equipo a vence al equipo b. Este grafo es un grafo dirigido simple, que no contiene ciclo ni aristas dirigidas múltiples (porque no hay dos equipos que jueguen entre sí más de una vez). Este modelo de grafo dirigido se presenta en la Figura 5.14. Vemos que el Equipo 1 está invicto en este torneo y el Equipo 3 no ha ganado.

□

Ejemplo 5.1.15 Torneos de eliminación simple Un torneo en el que cada participante es eliminado después de una derrota se denomina torneo de eliminación simple. Los torneos de eliminación simple se utilizan a menudo en los deportes, incluidos los campeonatos de tenis y el campeonato anual de baloncesto de la NCAA.

Podemos modelar un torneo de este tipo usando un vértice para representar cada juego y una arista dirigida para conectar un juego con el siguiente juego en el que jugó el ganador de este juego. El grafo en la Figura 5.15 representa los juegos jugados por los 16 equipos finalistas en el torneo femenil de baloncesto de la NCAA en el 2010.

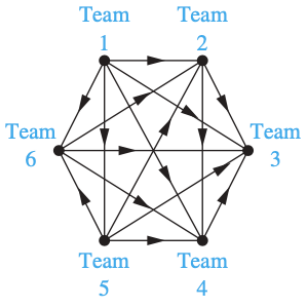


Figura 5.14: Un modelo de grafo de un torneo round-robin.

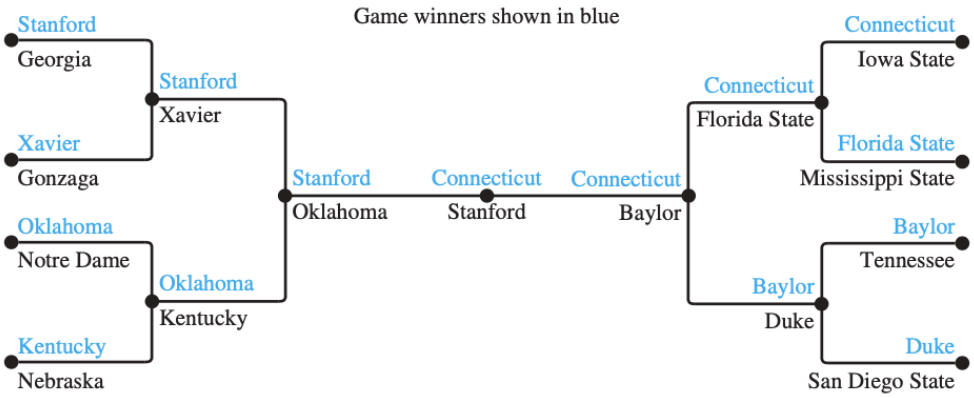


Figura 5.15: Un torneo de eliminación simple.

□

5.1.2. Ejercicios

1. Construya un grafo de influencia para los miembros de la junta de una empresa si el presidente puede influir en el director de investigación y desarrollo, el director de marketing y el director de operaciones; el Director de Investigación y Desarrollo puede influir en el Director de Operaciones; el director de marketing puede influir en el director de operaciones; y nadie puede influir ni ser influenciado por el Director Financiero.

2. La palabra manzana puede referirse a una planta, un alimento o una empresa de computadoras. Construya un grafo de palabras para estos sustantivos: manzana, fresa, lenovo, queso, chocolate, ibm, roble, microsoft, seto, hierba, pastel, quiche, hp, sidra, rosquilla, azalea, pino, dell, abeto, frambuesa. Conecte dos vértices por una arista no dirigida si los sustantivos que representan tienen un significado similar.

3. La palabra rock puede referirse a un tipo de música o a algo de una montaña. Construya un grafo de palabras para estos sustantivos: roca, piedra, jazz, piedra caliza, grava, folk, bachata, piedra pómez, granito, tango, klezmer, pizarra, pizarra, clásica, guijarros, arena, rap, mármol. Conecte dos vértices por una arista no dirigida si los sustantivos que representan tienen un significado similar.

4. ¿A qué otros equipos venció el Equipo 4 y qué equipos vencieron al Equipo 4 en el torneo round-robin representado por el grafo de la Figura 5.14?

5. En un torneo round-robin los Tigres vencieron a los Azulejos, los Tigres vencieron a los Cardenales, los Tigres vencieron a los Orioles, los Azulejos vencieron a los Cardenales, los Azulejos vencieron a los Orioles y los Cardenales vencieron a los Orioles. Modele este resultado con un grafo dirigido.

6. Construya el grafo de llamadas para un conjunto de siete números de teléfono 555-0011, 555-1221, 555-1333, 555-8888, 555-2222, 555-0091 y 555-1200 si hubo tres llamadas del 555-0011 al 555-8888 y dos llamadas

del 555-8888 al 555-0011, dos llamadas del 555-2222 al 555-0091, dos llamadas del 555-1221 a cada uno de los otros números y una llamada del 555-1333 a cada uno de los 555-0011, 555-1221 y 555-1200.

5.2. Terminología de Grafos y Tipos Especiales de Grafos

5.2.1. Introducción

Presentamos parte del vocabulario básico de la teoría de grafos en esta sección. Usaremos este vocabulario más adelante en este capítulo cuando resolvamos muchos tipos de problemas diferentes.

Uno de esos problemas implica determinar si un grafo se puede dibujar en el plano de modo que no se crucen dos de sus aristas. Otro ejemplo es decidir si hay una correspondencia uno a uno entre los vértices de dos grafos que produce una correspondencia uno a uno entre las aristas de los grafos.

También presentaremos varias familias importantes de grafos que se utilizan a menudo como ejemplos y en modelos. Se describirán varias aplicaciones importantes donde surgen estos tipos especiales de grafos.

5.2.2. Terminología Básica

Primero, damos algo de terminología que describe los vértices y aristas de grafos no dirigidos.

Definición 5.2.1 Dos vértices u y v en un grafo no dirigido G se llaman *adyacentes* (o *vecinos*) en G si u y v son puntos extremos de una arista e de G. Dicha arista e se llama *incidente* con los vértices u y v, también se dice que e *conecta* a u y v.

También encontraremos terminología útil para describir el conjunto de vértices adyacentes a un vértice particular de un grafo.

Definición 5.2.2 El conjunto de todos los vecinos de un vértice v de $G = (V, E)$, denotado por $N(v)$, se llama la *vecindad* de v. Si A es un subconjunto de V, denotamos por $N(A)$ el conjunto de todos los vértices en G que son adyacentes a al menos un vértice en A. Así, $N(A) = \bigcup_{v \in A} N(v)$.

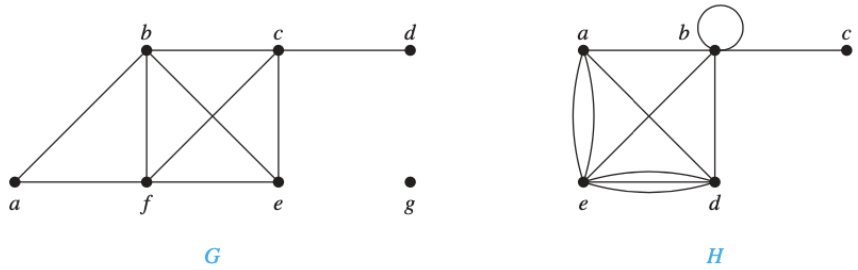


Figura 5.16: Los grafos no dirigidos G y H.

Para realizar un seguimiento de cuántas aristas inciden en un vértice, hacemos la siguiente definición.

Definición 5.2.3 El *grado de un vértice en un grafo no dirigido* es el número de aristas incidentes con él, excepto que un ciclo en un vértice contribuye dos veces al grado de ese vértice. El grado del vértice v se denota mediante $deg(v)$.

Ejemplo 5.2.1 ¿Cuáles son los grados y las vecindades de los vértices en los grafos G y H que se muestran en la Figura 5.16?

Solución: En G, $deg(a) = 2$, $deg(b) = deg(c) = deg(f) = 4$, $deg(d) = 1$, $deg(e) = 3$ y $deg(g) = 0$. Las vecindades de estos vértices son $N(a) = \{b, f\}$, $N(b) = \{a, c, e, f\}$, $N(c) = \{b, d, e, f\}$, $N(d) = \{c\}$, $N(e) = \{b, c, f\}$, $N(f) = \{a, b, c, e\}$ y $N(g) = \emptyset$. En H, $deg(a) = 4$, $deg(b) = deg(e) = 6$, $deg(c) = 1$ y $deg(d) = 5$. Las vecindades de estos vértices son $N(a) = \{b, d, e\}$, $N(b) = \{a, b, c, d, e\}$, $N(c) = \{b\}$, $N(d) = \{a, b, e\}$ y $N(e) = \{a, b, d\}$.

□

Un vértice de grado cero se llama **aislado**. De ello se deduce que un vértice aislado no es adyacente a ningún vértice. El vértice g del grafo G del Ejemplo 5.2.1 está aislado.

Un vértice es **colgante** si y sólo si tiene grado uno. En consecuencia, un vértice colgante es adyacente exactamente a otro vértice. El vértice d del grafo G del Ejemplo 5.2.1 es colgante. Examinar los grados de los vértices en un modelo de grafo puede proporcionar información útil sobre el modelo, como muestra el Ejemplo 5.2.2.

Ejemplo 5.2.2 ¿Qué representa el grado de un vértice en un grafo de superposición de nichos (presentado en el Ejemplo 5.1.11 en la Sección 5.1)? ¿Qué vértices de este grafo son colgantes y cuáles están aislados? Utilice el grafo de superposición de nichos que se muestra en la Figura 5.11 de la Sección 5.1) para interpretar sus respuestas.

Solución: Hay una arista entre dos vértices en un grafo de superposición de nichos si y sólo si las dos especies representadas por estos vértices compiten. Por lo tanto, el grado de un vértice en un grafo de superposición de nichos es el número de especies en el ecosistema que compiten con las especies representadas por este vértice.

Un vértice es colgante si la especie compite exactamente con otra especie en el ecosistema. Finalmente, el vértice que representa una especie se aísla si esta especie no compite con ninguna otra especie del ecosistema.

Por ejemplo, el grado del vértice que representa a la ardilla en el grafo de superposición de nichos en la Figura 5.11 en la Sección 5.1 es cuatro, porque la ardilla compite con otras cuatro especies: el cuervo, la zarigüeya, el mapache y el pájaro carpintero.

En este grafo de superposición de nichos, el ratón es la única especie representada por un vértice colgante, porque el ratón compite sólo con la musaraña y todas las demás especies compiten con al menos otras dos especies. No hay vértices aislados en este grafo de superposición de nichos porque cada especie en este ecosistema compite con al menos otra especie.

□

¿Qué obtenemos cuando sumamos los grados de todos los vértices de una grafo $G = (V, E)$? Cada arista contribuye con dos a la suma de los grados de los vértices porque una arista incide exactamente con dos vértices (posiblemente iguales).

Esto significa que la suma de los grados de los vértices es el doble del número de aristas. Tenemos el resultado en el Teorema 5.2.1, que a veces se denomina teorema del apretón de manos (y también se conoce a menudo como el lema del apretón de manos), debido a la analogía entre una arista que tiene dos extremos y un apretón de manos que involucra dos manos.

Teorema 5.2.1 EL TEOREMA DEL APRETÓN DE MANOS Sea $G = (V, E)$ un grafo no dirigida con m aristas. Entonces

$$2m = \sum_{v \in V} deg(v).$$

(Tenga en cuenta que esto se cumple incluso si están presentes múltiples aristas y ciclos).

■

Ejemplo 5.2.3 ¿Cuántas aristas hay en un grafo con 10 vértices cada uno de grado seis?

Solución: Debido a que la suma de los grados de los vértices es $6 \cdot 10 = 60$, se deduce que $2m = 60$ donde m es el número de aristas. Por lo tanto, $m = 30$.

□

El teorema 5.2.1 muestra que la suma de los grados de los vértices de una grafo no dirigido es par. Este simple hecho tiene muchas consecuencias, una de las cuales se da en el Teorema 5.2.2.

Teorema 5.2.2 Un grafo no dirigido tiene un número par de vértices de grado impar.

Demostración: Sean V_1 y V_2 el conjunto de vértices de grado par y el conjunto de vértices de grado impar, respectivamente, en un grafo no dirigido $G = (V, E)$ con m aristas.

$$2m = \sum_{v \in V} deg(v) = \sum_{v \in V_1} deg(v) + \sum_{v \in V_2} deg(v).$$

Debido a que $deg(v)$ es par para $v \in V_1$, el primer término en el lado derecho de la última igualdad es par.

Además, la suma de los dos términos en el lado derecho de la última igualdad es par, porque esta suma es $2m$. Por tanto, el segundo término de la suma también es par. Debido a que todos los términos de esta suma son impares, debe haber un número par de dichos términos. Por tanto, hay un número par de vértices de grado impar.

■

La terminología para grafos con aristas dirigidas refleja el hecho de que las aristas en los grafos dirigidos tienen direcciones.

Definición 5.2.4 Cuando (u, v) es una arista del grafo G con aristas dirigidas, se dice que u es *adyacente hacia* v y que v es *adyacente desde* u. El vértice u se llama *vértice inicial* de (u, v) y v se llama *vértice terminal* o *final* de (u, v). El vértice inicial y el vértice terminal de un ciclo son iguales.

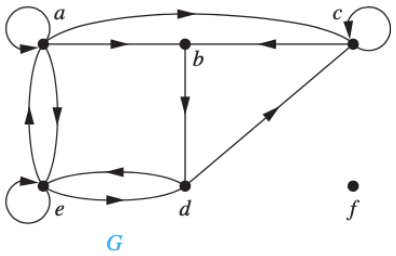


Figura 5.17: El grafo dirigido G para el ejemplo 5.2.4.

Debido a que las aristas en grafos con aristas dirigidas son pares ordenados, la definición del grado de un vértice se puede refinar para reflejar el número de aristas con este vértice como vértice inicial y como vértice terminal.

Definición 5.2.5 En un grafo con aristas dirigidas, el *grado de entrada de un vértice* v, denotado por $deg^-(v)$, es el número de aristas con v como su vértice terminal. El *grado de salida de* v, denotado por $deg^+(v)$, es el número de aristas con v como su vértice inicial. (Tenga en cuenta que un ciclo en un vértice aporta 1 tanto al grado de entrada como al de salida de este vértice).

Ejemplo 5.2.4 Encuentre el grado de entrada y salida de cada vértice en el grafo G con las aristas dirigidas que se muestran en la Figura 5.17.

Solución: Los grados de entrada en G son $deg^-(a) = 2$, $deg^-(b) = 2$, $deg^-(c) = 3$, $deg^-(d) = 2$, $deg^-(e) = 3$, y $deg^-(f) = 0$. Los grados de salida son $deg^+(a) = 4$, $deg^+(b) = 1$, $deg^+(c) = 2$, $deg^+(d) = 2$, $deg^+(e) = 3$ y $deg^+(f) = 0$.

□

Debido a que cada arista tiene un vértice inicial y un vértice terminal, la suma de los grados de entrada y la suma de los grados de salida de todos los vértices en un grafo con aristas dirigidas es la misma. Ambas sumas son el número de aristas en el grafo. Este resultado se expresa como el Teorema 5.2.3.

Teorema 5.2.3 Sea $G = (V, E)$ un grafo con aristas dirigidas. Entonces

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |V|.$$

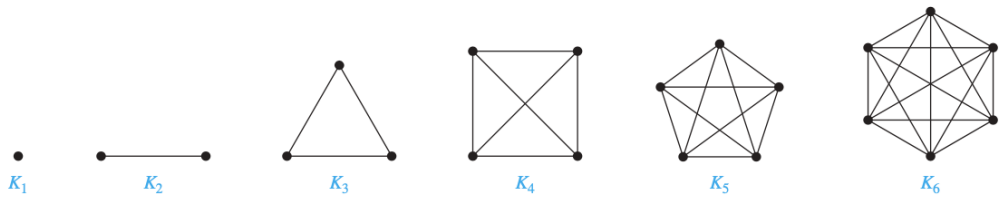


Figura 5.18: Los grafos K_n para $1 \leq n \leq 6$.

■

Hay muchas propiedades de un grafo con aristas dirigidas que no dependen de la dirección de sus aristas. En consecuencia, a menudo es útil ignorar estas direcciones. El grafo no dirigido que resulta de ignorar las direcciones de las aristas se denomina **grafo no dirigido subyacente**. Un grafo con aristas dirigidas y su grafo subyacente no dirigido tienen el mismo número de aristas.

5.2.3. Algunos Grafos Simples Especiales

Ahora presentaremos varias clases de grafos simples. Estos grafos se utilizan a menudo como ejemplos y surgen en muchas aplicaciones.

Ejemplo 5.2.5 Grafos completos Un **grafo completo sobre n vértices**, denotado por K_n, es un grafo simple que contiene exactamente una arista entre cada par de vértices distintos. Los grafos K_n, para $n = 1, 2, 3, 4, 5, 6$, se muestran en la Figura 5.18. Un grafo simple para el cual hay al menos un par de vértices distintos no conectados por una arista se llama **no completo**.

□

Ejemplo 5.2.6 Ciclos Un **ciclo** $C_n, n \geq 3$, consta de n vértices $v_1, v_2, \ldots, v_n$ y aristas $\{v_1, v_2\}$, $\{v_2, v_3\}, \ldots,$ $\{v_{n-1}, v_n\}$ y $\{v_n, v_1\}$. Los ciclos C_3, C_4, C_5 y C_6 se muestran en la Figura 5.19.

□

Ejemplo 5.2.7 Ruedas Obtenemos una **rueda** W_n cuando añadimos un vértice adicional a un ciclo C_n, para $n \geq 3$, y conectamos este nuevo vértice a cada uno de los n vértices de C_n, por nuevas aristas. Las ruedas W_3, W_4, W_5 y W_6 se muestran en la Figura 5.20.

□

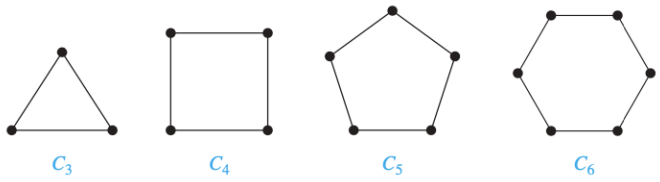


Figura 5.19: Los ciclos C_3, C_4, C_5 y C_6.

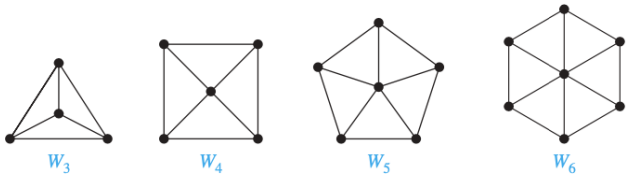


Figura 5.20: Las ruedas W_3, W_4, W_5 y W_6.

Ejemplo 5.2.8 ***n*-Cubos** Un **hipercubo *n*-dimensional**, o ***n*-cubo**, denotado por Q_n, es un grafo que tiene vértices que representan las cadenas de 2^n bits de longitud n. Dos vértices son adyacentes si y sólo si las cadenas de bits que representan difieren exactamente en la posición de un bit. Mostramos Q_1, Q_2 y Q_3 en la Figura 5.21.

Tenga en cuenta que puede construir el $(n+1)$-cubo Q_{n+1} a partir del n-cube Q_n haciendo dos copias de Q_n, anteponiendo las etiquetas en los vértices con un 0 en una copia de Q_n y con un 1 en la otra copia de Q_n, y agregando aristas que conectan dos vértices que tienen etiquetas que difieren solo en el primer bit.

En la Figura 5.21, Q_3 se construye a partir de Q_2 dibujando dos copias

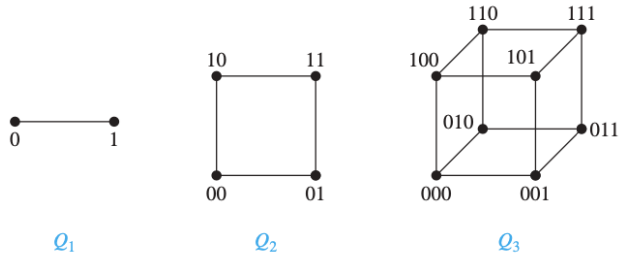


Figura 5.21: Los n-cubos Q_1, Q_2 y Q_3.

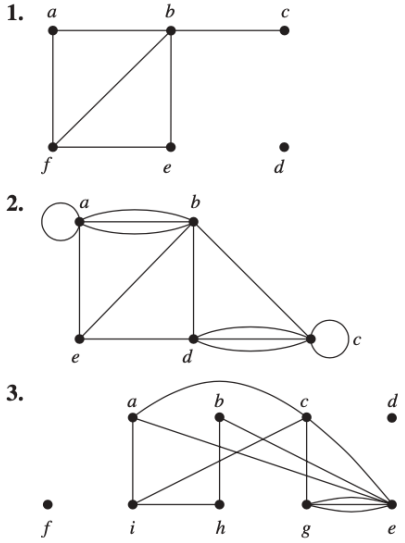


Figura 5.22: Grafos no dirigidos para los Ejercicios 1 y 2.

de Q_2 como las caras superior e inferior de Q_3, agregando 0 al comienzo de la etiqueta de cada vértice en la cara inferior y 1 al comienzo de la etiqueta de cada vértice en la cara superior.

(Aquí, por cara nos referimos a la cara de un cubo en un espacio tridimensional. Piense en dibujar el grafo Q_3 en un espacio tridimensional con copias de Q_2 como las caras superior e inferior de un cubo y luego dibujando en el plano la proyección de la representación resultante.)

□

5.2.4. Ejercicios

1. Para cada uno de los grafos no dirigidos en la Figura 5.22, encuentre el número de vértices, el número de aristas y el grado de cada vértice. Identifique todos los vértices aislados y colgantes.

2. Encuentra la suma de los grados de los vértices de cada grafo en la Figura 5.22 y verifica que sea igual al doble del número de aristas en el grafo.

3. Para cada uno de los multigrafos dirigidos en la Figura 5.23, determine el número de vértices y aristas, también encuentre el grado de entrada

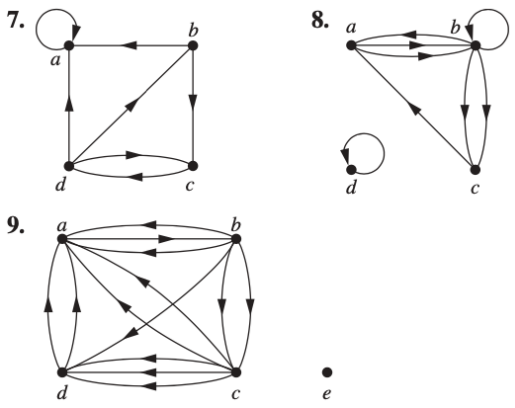


Figura 5.23: Multigrafos dirigidos para los Ejercicio 3 y 4.

y el grado de salida de cada vértice.

4. Para cada uno de los multigrafos dirigidos en la Figura 5.23, determine la suma de los grados de entrada de los vértices y la suma de los grados de salida de los vértices directamente. Demuestre que ambos son iguales al número de aristas en el grafo.

5. ¿Qué representa el grado de un vértice en el grafo de conocidos, donde los vértices representan a todas las personas del mundo? ¿Qué representa la vecindad de un vértice en este grafo? ¿Qué representan las vértices aisladas y colgantes en este grafo? En un estudio se estimó que el grado promedio de un vértice en este grafo es 1000. ¿Qué significa esto en términos del modelo?

6. ¿Qué representa el grado de un vértice en un grafo de colaboración académica? ¿Qué representa la vecindad de un vértice? ¿Qué representan los vértices aislados y colgantes?

7. ¿Qué representan el grado de entrada y el grado de salida de un vértice en un grafo dirigido que modela un torneo round-robin?

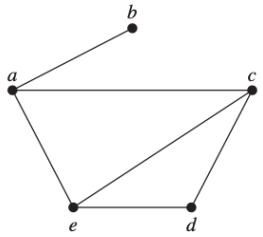


Figura 5.24: Grafo simple para el Ejemplo 5.3.1.

5.3. Representación de Grafos e Isomorfismo de Grafos

5.3.1. Introducción

Hay muchas formas útiles de representar grafos. Como veremos a lo largo de este capítulo, al trabajar con un grafo es útil poder elegir su representación más conveniente. En esta sección mostraremos cómo representar grafos de varias formas diferentes.

A veces, dos grafos tienen exactamente la misma forma, en el sentido de que existe una correspondencia uno a uno entre sus conjuntos de vértices que preservan las aristas. En tal caso, decimos que los dos grafos son isomorfos. Determinar si dos grafos son isomorfos es un problema importante de la teoría de grafos que estudiaremos en esta sección.

5.3.2. Representación de Grafos

Una forma de representar un grafo sin múltiples aristas es enumerar todas las aristas de este grafo. Otra forma de representar un grafo sin múltiples aristas es utilizar listas de adyacencias, que especifican los vértices adyacentes a cada vértice del grafo.

Ejemplo 5.3.1 Utilice listas de adyacencias para describir el grafo simple que se muestra en la Figura 5.24.

Solución: La Tabla 5.2 lista los vértices adyacentes a cada uno de los vértices del grafo.

□

Vertex	*Adjacent Vertices*
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

Tabla 5.2: Lista de adyacencia para el grafo de la Figura 5.24.

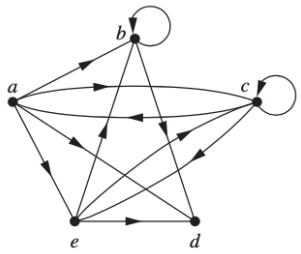


Figura 5.25: Grafo dirigido para el Ejemplo 5.3.2.

Ejemplo 5.3.2 Represente el grafo dirigido que se muestra en la Figura 5.25 listando todos los vértices que son los vértices terminales de las aristas que comienzan en cada vértice del grafo.

Solución: La Tabla 5.3 representa el grafo dirigido que se muestra en la Figura 5.25.

□

Initial Vertex	*Terminal Vertices*
a	b, c, d, e
b	b, d
c	a, c, e
d	
e	b, c, d

Tabla 5.3: Lista de adyacencia para el grafo de la Figura 5.25.

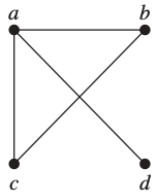


Figura 5.26: Grafo simple para el Ejemplo 5.3.3.

5.3.3. Matrices de Adyacencias

La realización de algoritmos para grafos utilizando la representación de grafos mediante listas de aristas o listas de adyacencias puede resultar engorrosa si hay muchas aristas en el grafo. Para simplificar el cálculo, los grafos se pueden representar mediante matrices.

Aquí se presentarán dos tipos de matrices comúnmente utilizadas para representar grafos. Uno se basa en la adyacencia de vértices y el otro se basa en la incidencia de vértices y aristas.

Suponga que $G = (V, E)$ es un grafo simple donde $|V| = n$. Suponga que los vértices de G se enumeran arbitrariamente como $v_1, v_2, \ldots, v_n$. La **matriz de adyacencias** $\boldsymbol{A}$ (o $\boldsymbol{A}_G$) de G, con respecto a esta lista de vértices, es la matriz $n \times n$ de ceros y unos con 1 como su (i, j)-ésima entrada cuando v_i y v_j son adyacentes, y 0 como su (i, j)-ésima entrada cuando no son adyacentes. En otras palabras, si su matriz de adyacencias es $\boldsymbol{A} = [a_{ij}]$, entonces

$$a_{ij} = \begin{cases} 1 & \text{si } \{v_i, v_j\} \text{ es una arista de } G, \\ 0 & \text{en otro caso.} \end{cases}$$

Ejemplo 5.3.3 Utilice una matriz de adyacencias para representar el grafo que se muestra en la Figura 5.26.

Solución: Ordenamos los vértices como a, b, c, d. La matriz que representa este grafo es

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

□

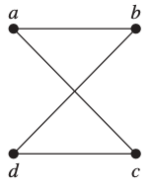


Figura 5.27: Un grafo para la matriz de adyacencias dada en el Ejemplo 5.3.4.

Ejemplo 5.3.4 Dibuje una grafo a partir de la matriz de adyacencias

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

con respecto al orden de los vértices a, b, c, d.

Solución: En la Figura 5.27 se muestra un grafo para esta matriz de adyacencias.

□

Tenga en cuenta que una matriz de adyacencias de un grafo se basa en el orden elegido para los vértices. Por lo tanto, puede haber tantos como $n!$ diferentes matrices de adyacencia para un grafo con n vértices, porque hay $n!$ diferentes ordenamientos de n vértices.

La matriz de adyacencias de un grafo simple es simétrica, es decir, $a_{ij} = a_{ji}$, porque ambas entradas son 1 cuando v_i y v_j son adyacentes, y ambas son 0 en caso contrario. Además, debido a que un grafo simple no tiene ciclos, cada entrada $a_{ii}, i = 1, 2, 3, \ldots, n$, es 0.

Las matrices de adyacencia también se pueden utilizar para representar grafos no dirigidos con ciclos y con múltiples aristas. Un ciclo en el vértice v_i está representado por un 1 en la posición (i, i)-ésima de la matriz de adyacencias.

Cuando existen múltiples aristas que conectan el mismo par de vértices v_i y v_j, o múltiples ciclos en el mismo vértice, la matriz de adyacencias ya no es una matriz cero-uno, porque la entrada (i, j)- ésima de esta matriz es igual al número de aristas asociadas a $\{v_i, v_j\}$. Todos los grafos no dirigidos, incluidos los multigrafos y los pseudógrafos, tienen matrices de adyacencia simétricas.

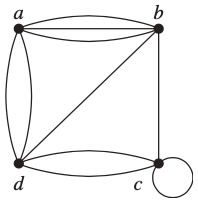


Figura 5.28: Un pseudografo para el Ejemplo 5.3.5.

Ejemplo 5.3.5 Utilice una matriz de adyacencias para representar el pseudógrafo que se muestra en la Figura 5.28.

Solución: La matriz de adyacencias usando el orden de los vértices a, b, c, d es

$$\begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{bmatrix}$$

□

Usamos matrices cero-uno en el Capítulo 2 para representar grafos dirigidos. La matriz para un grafo dirigido $G = (V, E)$ tiene un 1 en su (i, j)-ésima posición si hay una arista de v_i a v_j, donde $v_1, v_2, \ldots, v_n$ es una lista arbitraria de los vértices del grafo dirigido. En otras palabras, si $\boldsymbol{A} = [a_{ij}]$ es la matriz de adyacencias para el grafo dirigido con respecto a esta lista de vértices, entonces

$$a_{ij} = \begin{cases} 1 & \text{si } (v_i, v_j) \text{ es una arista de } G, \\ 0 & \text{en otro caso.} \end{cases}$$

La matriz de adyacencias para un grafo dirigido no tiene que ser simétrica, porque puede que no haya una arista de v_j a v_i cuando hay una arista de v_i a v_j.

Las matrices de adyacencia también se pueden utilizar para representar multigrafos dirigidos. Nuevamente, tales matrices no son matrices cero-uno cuando hay múltiples aristas en la misma dirección que conectan dos vértices. En la matriz de adyacencias de un multigraph dirigido, a_{ij} es igual al número de aristas que están asociadas a (v_i, v_j).

COMPROMISOS ENTRE LISTAS DE ADYACENCIAS Y MATRICES DE ADYACENCIAS Cuando un grafo simple contiene relativamente pocas aristas, es decir, cuando es **disperso**, generalmente es preferible

usar listas de adyacencias en lugar de una matriz de adyacencias para representar al grafo.

Por ejemplo, si cada vértice tiene un grado que no excede c, donde c es una constante mucho más pequeña que n, entonces cada lista de adyacencia contiene c o menos vértices. Por lo tanto, no hay más de cn elementos en todas estas listas de adyacencias. Por otro lado, la matriz de adyacencias del grafo tiene n^2 entradas.

Sin embargo, tenga en cuenta que la matriz de adyacencias de un grafo disperso es una **matriz dispersa**, es decir, una matriz con pocas entradas distintas de cero, y existen técnicas especiales para representar y calcular con matrices dispersas.

Ahora suponga que un grafo simple es **denso**, es decir, suponga que contiene muchas aristas, como un grafo que contiene más de la mitad de todas las aristas posibles. En este caso, el uso de una matriz de adyacencias para representar el grafo suele ser preferible al uso de listas de adyacencias.

Para ver por qué, comparamos la complejidad de determinar si la posible arista $\{v_i, v_j\}$ está presente. Usando una matriz de adyacencias, podemos determinar si esta arista está presente examinando la entrada (i, j)-ésima en la matriz. Esta entrada es 1 si el grafo contiene esta arista y es 0 en caso contrario.

En consecuencia, solo necesitamos hacer una comparación, a saber, comparar esta entrada con 0, para determinar si esta arista está presente. Por otro lado, cuando usamos listas de adyacencias para representar el grafo, necesitamos buscar en la lista de vértices adyacentes a v_i o v_j para determinar si esta arista está presente. Esto puede requerir $\Theta(|V|)$ comparaciones cuando hay muchas aristas presentes.

5.3.4. Matrices de Incidencias

Otra forma común de representar grafos es utilizando matrices de incidencias. Sea $G = (V, E)$ un grafo no dirigido. Suponga que $v_1, v_2, \ldots, v_n$ son los vértices y $e_1, e_2, \ldots, e_m$ son las aristas de G. Entonces la matriz de incidencias con respecto a este orden de V y E es la matriz de $n \times m$ $\boldsymbol{M} = [m_{ij}]$, donde

$$m_{ij} = \begin{cases} 1 & \text{cuando la arista } e_j \text{ es incidente con } v_i, \\ 0 & \text{en otro caso.} \end{cases}$$

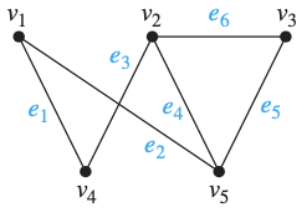


Figura 5.29: El grafo no dirigido para el Ejemplo 5.3.6.

Ejemplo 5.3.6 Represente el grafo que se muestra en la Figura 5.29 con una matriz de incidencias.

Solución: La matriz de incidencias es

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$

□

Las matrices de incidencia también se pueden utilizar para representar aristas múltiples y ciclos. Las aristas múltiples se representan en la matriz de incidencias utilizando columnas con entradas idénticas, porque estas aristas inciden con el mismo par de vértices. Los ciclos se representan mediante una columna con exactamente una entrada igual a 1, correspondiente al vértice que incide en este ciclo.

Ejemplo 5.3.7 Represente el pseudografo que se muestra en la Figura 5.30 utilizando una matriz de incidencias.

Solución: La matriz de incidencias de este pseudografo es

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

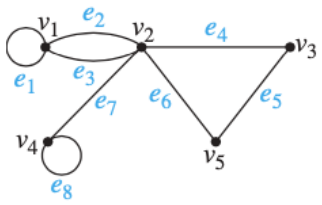


Figura 5.30: El pseudografo para el Ejemplo 5.3.7.

□

5.3.5. Isomorfismo de Grafos

A menudo necesitamos saber si es posible dibujar dos grafos de la misma manera. Es decir, ¿los grafos tienen la misma estructura cuando ignoramos las identidades de sus vértices? Por ejemplo, en química, los grafos se utilizan para modelar compuestos químicos (de una manera que describiremos más adelante).

Diferentes compuestos pueden tener la misma fórmula molecular pero pueden diferir en estructura. Dichos compuestos se pueden representar mediante grafos que no se pueden dibujar de la misma manera. Los grafos que representan compuestos previamente conocidos pueden usarse para determinar si un compuesto supuestamente nuevo se ha estudiado antes.

Existe una terminología útil para grafos con la misma estructura.

Definición 5.3.1 Los grafos simples $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son isomorfos si existe una función uno a uno y sobre f de V_1 a V_2 con la propiedad de que a y b son adyacentes en G_1 si y sólo si $f(a)$ y $f(b)$ son adyacentes en G_2, para todo a y b en V_1. Esta función f se llama *isomorfismo*[1]. Dos grafos simples que no son isomorfos se denominan *no isomorfos*.

En otras palabras, cuando dos grafos simples son isomorfos, existe una correspondencia uno a uno entre los vértices de los dos grafos que preserva la relación de adyacencia. El isomorfismo de grafos simples es una relación de equivalencia, como el lector puede verificar.

[1]La palabra *isomorfismo* proviene de las raíces griegas *isos* para "igual" y *morphe* para "forma".

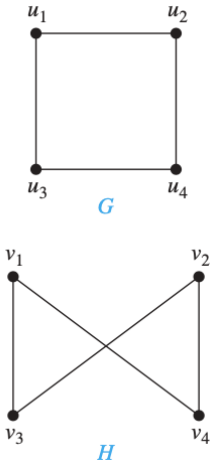


Figura 5.31: Los grafos G y H para el Ejemplo 5.3.8.

Ejemplo 5.3.8 Muestre que los grafos $G = (V, E)$ y $H = (W, F)$, que se muestran en la Figura 5.31, son isomorfos.

Solución: La función f con $f(u_1) = v_1$, $f(u_2) = v_4$, $f(u_3) = v_3$, y $f(u_4) = v_2$ es una correspondencia uno a uno entre V y W. Para ver que esta correspondencia conserva la adyacencia, observe que los vértices adyacentes en G son u_1 y u_2, u_1 y u_3, u_2 y u_4, y u_3 y u_4, y cada uno de los pares $f(u_1) = v_1$ y $f(u_2) = v_4$, $f(u_1) = v_1$ y $f(u_3) = v_3$, $f(u_2) = v_4$ y $f(u_4) = v_2$, y $f(u_3) = v_3$ y $f(u_4) = v_2$ consta de dos vértices adyacentes en H.

□

5.3.6. Determinando si dos grafos simples son isomorfos

A menudo es difícil determinar si dos grafos simples son isomorfos. Hay $n!$ posibles correspondencias uno a uno entre los conjuntos de vértices de dos grafos simples con n vértices. Probar cada una de estas correspondencias para ver si conserva la adyacencia y la no adyacencia no es práctico si n es grande.

A veces no es difícil demostrar que dos grafos no son isomorfos. En particular, podemos mostrar que dos grafos no son isomorfos si podemos encontrar una propiedad que sólo uno de los dos grafos tiene, pero que se conserva mediante isomorfismo.

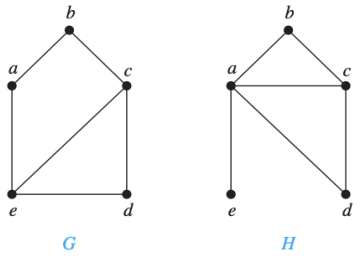


Figura 5.32: Los grafos G y H para el Ejemplo 5.3.9.

Una propiedad preservada por el isomorfismo de los grafos se denomina **invariante de grafos**. Por ejemplo, los grafos simples isomorfos deben tener el mismo número de vértices, porque existe una correspondencia uno a uno entre los conjuntos de vértices de los grafos.

Los grafos simples isomorfos también deben tener el mismo número de aristas, porque la correspondencia uno a uno entre vértices establece una correspondencia uno a uno entre aristas.

Además, los grados de los vértices en grafos simples isomorfos deben ser los mismos. Es decir, un vértice v de grado d en G debe corresponder a un vértice $f(v)$ de grado d en H, porque un vértice w en G es adyacente a v si y sólo si $f(v)$ y $f(w)$ son adyacente en H.

Ejemplo 5.3.9 Muestre que los grafos que se muestran en la Figura 5.32 no son isomorfos.

Solución: Tanto G como H tienen cinco vértices y seis aristas. Sin embargo, H tiene un vértice de grado uno, es decir, el vértice e, mientras que G no tiene vértices de grado uno. De ello se deduce que G y H no son isomorfos. □

El número de vértices, el número de aristas y el número de vértices de cada grado son todos invariantes bajo isomorfismo. Si alguna de estas cantidades difiere en dos grafos simples, estos grafos no pueden ser isomorfos.

Sin embargo, cuando estas invariantes son iguales, no significa necesariamente que los dos grafos sean isomorfos. Actualmente no se conocen conjuntos útiles de invariantes que puedan usarse para determinar si los grafos simples son isomorfos.

Ejemplo 5.3.10 Determine si los grafos que se muestran en la Figura 5.33 son isomorfos.

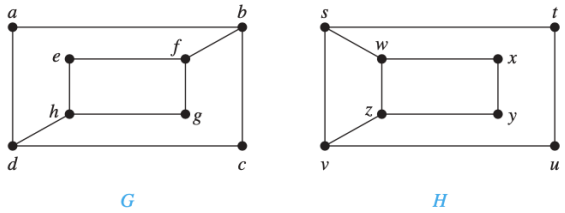


Figura 5.33: Los grafos G y H para el Ejemplo 5.3.10.

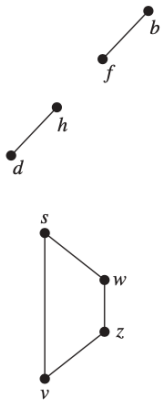


Figura 5.34: Los subgrafos de G y H formados por vértices de grado tres y las aristas que los conectan, para el Ejemplo 5.3.10.

Solución: Los grafos G y H tienen ocho vértices y 10 aristas. Ambos también tienen cuatro vértices de grado dos y cuatro de grado tres. Debido a que todas estas invariantes concuerdan, todavía es concebible que estos grafos sean isomorfos.

Sin embargo, G y H no son isomorfos. Para ver esto, tenga en cuenta que debido a que el $deg(a) = 2$ en G, a debe corresponder a t, u, x o y en H, porque estos son los vértices del grado dos en H. Sin embargo, cada uno de estos cuatro vértices en H es adyacente a otro vértice de grado dos en H, lo que no es cierto para a en G.

Otra forma de ver que G y H no son isomorfos es notar que los subgrafos de G y H formados por vértices de grado tres y las aristas que los conectan deben ser isomorfos si estos dos grafos son isomorfos (el lector debe verificar esto). Sin embargo, estos subgrafos, que se muestran en la Figura 5.34, no son isomorfos.

□

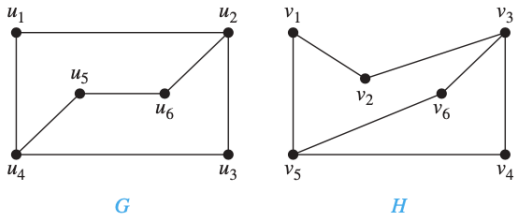


Figura 5.35: Los grafos G y H para el Ejemplo 5.3.11.

Para mostrar que una función f del conjunto de vértices de un grafo G al conjunto de vértices de un grafo H es un isomorfismo, debemos demostrar que f conserva la presencia y ausencia de aristas.

Una forma útil de hacer esto es utilizar matrices de adyacencia. En particular, para mostrar que f es un isomorfismo, podemos mostrar que la matriz de adyacencias de G es la misma que la matriz de adyacencias de H, cuando las filas y columnas están etiquetadas para corresponder a las imágenes bajo f de los vértices en G que son las etiquetas de estas filas y columnas en la matriz de adyacencias de G. Ilustramos cómo se hace esto en el Ejemplo 5.3.11.

Ejemplo 5.3.11 Determine si los grafos G y H que se muestran en la Figura 5.35 son isomorfos.

Solución: Tanto G como H tienen seis vértices y siete aristas. Ambos tienen cuatro vértices de grado dos y dos vértices de grado tres. También es fácil ver que los subgrafos de G y H que consisten en todos los vértices de grado dos y las aristas que los conectan son isomorfos (como el lector debe verificar). Dado que G y H concuerdan con respecto a estos invariantes, es razonable intentar encontrar un isomorfismo f.

Ahora definiremos una función f y luego determinaremos si es un isomorfismo. Debido a que $deg(u_1) = 2$ y debido a que u_1 no es adyacente a ningún otro vértice de grado dos, la imagen de u_1 debe ser v_4 o v_6, los únicos vértices de grado dos en H no adyacentes a un vértice de grado dos.

Establecemos arbitrariamente $f(u_1) = v_6$. [Si encontráramos que esta elección no condujo al isomorfismo, intentaríamos $f(u_1) = v_4$.] Como u_2 es adyacente a u_1, las posibles imágenes de u_2 son v_3 y v_5. Establecemos arbitrariamente $f(u_2) = v_3$.

Continuando de esta manera, usando la adyacencia de vértices y grados como guía, establecemos $f(u_3) = v_4$, $f(u_4) = v_5$, $f(u_5) = v_1$ y $f(u_6) = v_2$.

Ahora tenemos una correspondencia uno a uno entre el conjunto de vértices de G y el conjunto de vértices de H, a saber, $f(u_1) = v_6$, $f(u_2) = v_3$, $f(u_3) = v_4$, $f(u_4) = v_5$, $f(u_5) = v_1$, $f(u_6) = v_2$. Para ver si f conserva las aristas, examinamos la matriz de adyacencias de G,

$$\boldsymbol{A}_G = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{array} \begin{array}{c} \begin{array}{cccccc} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}.$$

y la matriz de adyacencias de H con las filas y columnas etiquetadas por las imágenes de los vértices correspondientes en G,

$$\boldsymbol{A}_H = \begin{array}{c} \\ v_6 \\ v_3 \\ v_4 \\ v_5 \\ v_1 \\ v_2 \end{array} \begin{array}{c} \begin{array}{cccccc} v_6 & v_3 & v_4 & v_5 & v_1 & v_2 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}.$$

Como $\boldsymbol{A}_G = \boldsymbol{A}_H$, se deduce que f conserva las aristas. Concluimos que f es un isomorfismo, por lo que G y H son isomorfos. Tenga en cuenta que si f no hubiera sido un isomorfismo, no habríamos establecido que G y H no son isomorfos, porque otra correspondencia de los vértices en G y H puede ser un isomorfismo.

□

ALGORITMOS PARA EL ISOMORFISMO DE GRAFOS El mejor software práctico de propósito general para pruebas de isomorfismo, llamado NAUTY, se puede utilizar para determinar si dos grafos con hasta 100 vértices son isomorfos en menos de un segundo en una PC moderna.

El software NAUTY se puede descargar de Internet y experimentar con él. Existen algoritmos prácticos para determinar si dos grafos son isomorfos para grafos que están restringidos de varias formas, como cuando el grado máximo de los vértices es pequeño.

El problema de determinar si dos grafos son isomorfos es de especial interés porque es uno de los pocos problemas en NP que no se sabe si es tratable o NP-completo.

APLICACIONES DEL ISOMORFISMO DE GRAFOS Los isomorfismos de grafos, y funciones que son casi isomorfismos de grafos, surgen en aplicaciones de la teoría de grafos a la química y al diseño de circuitos electrónicos, y en otras áreas como la bioinformática y la visión por computadora.

Los químicos utilizan grafos múltiples, conocidos como grafos moleculares, para modelar compuestos químicos. En estos grafos, los vértices representan átomos y las aristas representan enlaces químicos entre estos átomos. Dos isómeros estructurales, moléculas con fórmulas moleculares idénticas pero con átomos unidos de manera diferente, tienen grafos moleculares no isomorfos.

Cuando se sintetiza un compuesto químico potencialmente nuevo, se verifica una base de datos de grafos moleculares para ver si el grafos molecular del compuesto es el mismo que uno ya conocido.

Los circuitos electrónicos se modelan mediante grafos en los que los vértices representan componentes y las aristas representan conexiones entre ellos. Los circuitos integrados modernos, conocidos como chips, son circuitos electrónicos miniaturizados, a menudo con millones de transistores y conexiones entre ellos.

Debido a la complejidad de los chips modernos, se utilizan herramientas de automatización para diseñarlos. El isomorfismo de grafos es la base para la verificación de que un diseño particular de un circuito producido por una herramienta automatizada corresponde al esquema original del diseño.

El isomorfismo de grafos también se puede utilizar para determinar si un chip de un proveedor incluye propiedad intelectual de otro proveedor. Esto se puede hacer buscando grandes subgrafos isomorfos en los grafos que modelan estos chips.

5.3.7. Ejercicios

1. Represente mediante una matriz de adyacencias cada uno de los grafos de la Figura 5.36.

2. Dibuje el grafo correspondiente a cada una de las siguientes matrices de adyacencias.

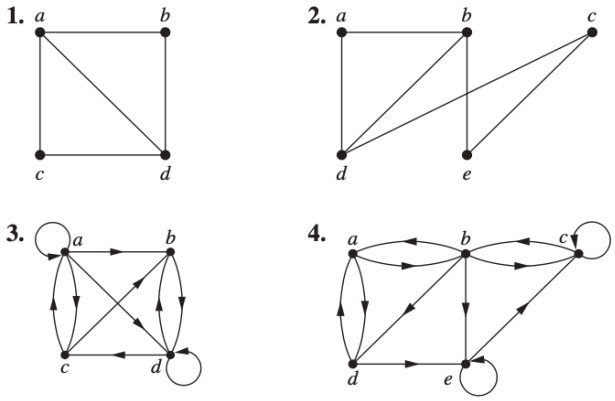


Figura 5.36: Grafos para el Ejercicio 1.

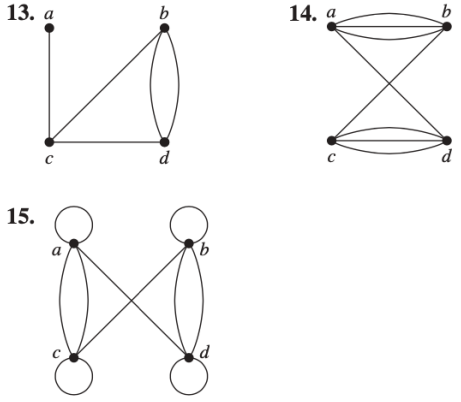


Figura 5.37: Grafos para el Ejercicio 3.

$$a)\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad b)\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad c)\ \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

3. Use una matriz de incidencias para representar cada grafo de la Figura 5.37.

4. Para cada par de grafos dados en la Figura 5.38 determine si son isomorfos. Demuestre un isomorfismo o proporcione un argumento riguroso de que no existe isomorfismo.

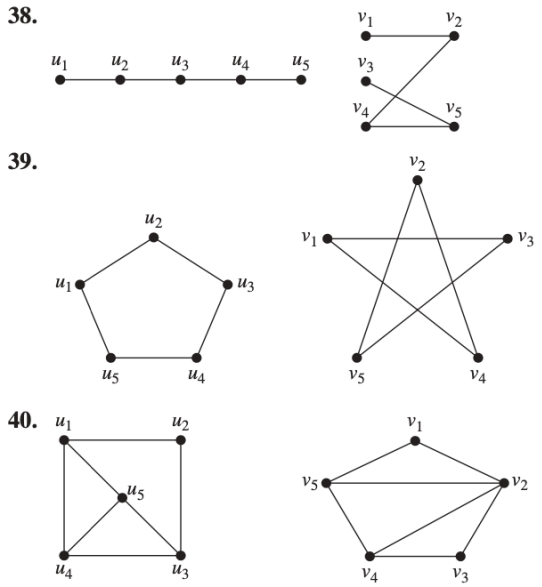


Figura 5.38: Grafos para el Ejercicio 4.

5.4. Conectividad en grafos

5.4.1. Introducción

Se pueden modelar muchos problemas con caminos formados viajando a lo largo de las aristas de los grafos. Por ejemplo, el problema de determinar si un mensaje se puede enviar entre dos computadoras usando enlaces intermedios se puede estudiar con un modelo de grafos.

Los problemas de planificación eficiente de rutas para la entrega de correo, recolección de basura, diagnósticos en redes de computadoras, etc. pueden resolverse utilizando modelos que involucran caminos en grafos.

5.4.2. Caminos

De manera informal, un camino es una secuencia de aristas que comienza en un vértice de un grafo y viaja de vértice a vértice a lo largo de las aristas del grafo. A medida que el camino viaja a lo largo de sus aristas, visita los vértices a lo largo de este camino, es decir, los puntos finales de estas aristas. En la Definición 5.4.1 se da una definición formal de caminos y terminología

relacionada.

Definición 5.4.1 Sea n un número entero no negativo y G un grafo no dirigido. Un *camino de longitud n* desde u hasta v en G es una secuencia de n aristas $e_1, \ldots, e_n$ de G para la cual existe una secuencia $x_0 = u, x_1, \ldots, x_{n-1}, x_n = v$ de vértices tales que e_i tiene, para $i = 1, \ldots, n$, los extremos x_{i-1} y x_i. Cuando el grafo es simple, denotamos este camino por su secuencia de vértices $x_0, x_1, \ldots, x_n$ (porque enumerar estos vértices determina de forma única el camino). El camino es un *circuito* si comienza y termina en el mismo vértice, es decir, si $u = v$, y tiene una longitud mayor que cero. Se dice que el camino o circuito *pasa por* los vértices $x_1, x_2, \ldots, x_{n-1}$ o *atraviesa* las aristas $e_1, e_2, \ldots, e_n$. Un camino o circuito es *simple* si no contiene la misma arista más de una vez.

En la Definición 5.4.2 formalizamos el concepto de camino en grafos dirigidos.

Definición 5.4.2 Sea n un número entero no negativo y G un grafo dirigido. Un *camino de longitud n* desde u hasta v en G es una secuencia de aristas $e_1, e_2, \ldots, e_n$ de G tal que e_1 está asociado con (x_0, x_1), e_2 está asociado con (x_1, x_2), y así sucesivamente, con e_n asociado con (x_{n-1}, x_n), donde $x_0 = u$ y $x_n = v$. Cuando no hay múltiples aristas en el grafo dirigido, este camino se denota por su secuencia de vértices $x_0, x_1, x_2, \ldots, x_n$. Un camino de longitud mayor que cero que comienza y termina en el mismo vértice se llama *circuito* o *ciclo*. Un camino o circuito se llama *simple* si no contiene la misma arista más de una vez.

5.4.3. Conectividad en grafos

¿Cuándo tiene una red de computadoras la propiedad de que cada par de computadoras puede compartir información, si los mensajes pueden enviarse a través de una o más computadoras intermedias? Cuando se usa un grafo para representar esta red de computadoras, donde los vértices representan las computadoras y las aristas representan los enlaces de comunicación, esta pregunta se convierte en: ¿Cuándo existe siempre un camino entre dos vértices en el grafo?

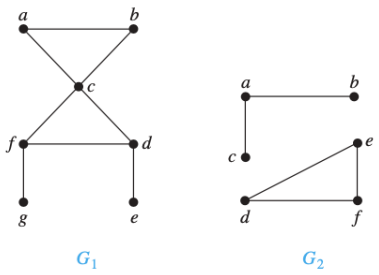


Figura 5.39: Los grafos G_1 y G_2 para el Ejemplo 5.4.1.

Definición 5.4.3 Un grafo no dirigido se llama *conectado* si hay un camino entre cada par de vértices distintos del grafo. Un grafo no dirigido que no está conectado se llama *desconectado*. Decimos que *desconectamos* un grafo cuando eliminamos vértices o aristas, o ambas, para producir un subgrafo desconectado.

Por lo tanto, dos computadoras cualesquiera en la red pueden comunicarse si y sólo si el grafo de esta red está conectado.

Ejemplo 5.4.1 El grafo G_1 en la Figura 5.39 está conectado, porque para cada par de vértices distintos hay un camino entre ellos (el lector debe verificar esto). Sin embargo, el grafo G_2 en la Figura 5.39 no está conectado. Por ejemplo, no hay un camino en G_2 entre los vértices a y d.

□

Teorema 5.4.1 Existe un camino simple entre cada par de vértices distintos de un grafo no dirigido conectado.

Demostración: Sean u y v dos vértices distintos del grafo no dirigido conectado $G = (V, E)$. Como G está conectado, hay al menos un camino entre u y v. Sea $x_0, x_1, \ldots, x_n$, donde $x_0 = u$ y $x_n = v$, la secuencia de vértices de un camino de menor longitud. Este camino de menor longitud es simple. Para ver esto, suponga que no es simple, entonces $x_i = x_j$ para algunos i y j con $0 \leq i < j$. Esto significa que hay un camino de u a v de menor longitud con secuencia de vértices $x_0, x_1, \ldots, x_{i-1}, x_j, \ldots, x_n$ obtenido al eliminar las aristas correspondientes a la secuencia de vértices $x_i, \ldots, x_{j-1}$.

■

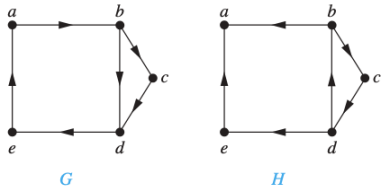


Figura 5.40: Los grafos G y H para el Ejemplo 5.4.2.

Hay dos nociones de conectividad en los gráficos dirigidos, dependiendo de si se consideran las direcciones de las aristas.

Definición 5.4.4 Un grafo dirigido está *fuertemente conectado* si hay un camino de a a b y de b a a siempre que a y b sean vértices en el grafo.

Para que un grafo dirigido esté fuertemente conectado, debe haber una secuencia de aristas dirigidas desde cualquier vértice en el grafo a cualquier otro vértice. Un grafo dirigido puede fallar al estar fuertemente conectado pero aún estar en "una pieza". La definición 5.4.5 hace que esta noción sea precisa.

Definición 5.4.5 Un grafo dirigido está *débilmente conectado* si hay un camino entre cada dos vértices en el grafo no dirigido subyacente.

Es decir, un grafo dirigido está débilmente conectado si y sólo si siempre hay un camino entre dos vértices cuando se ignoran las direcciones de las aristas. Claramente, cualquier grafo dirigido fuertemente conectado también está débilmente conectado.

Ejemplo 5.4.2 ¿Los grafos dirigidos G y H que se muestran en la Figura 5.40 están fuertemente conectados? ¿Están débilmente conectados?

Solución: G está fuertemente conectado porque hay un camino entre dos vértices cualesquiera en este grafo dirigido (el lector debe verificar esto). Por tanto, G también está débilmente conectado.

El grafo H no está fuertemente conectado. No hay un camino dirigido desde a hasta b en este grafo. Sin embargo, H está débilmente conectado, porque hay un camino entre dos vértices cualesquiera en el grafo no dirigido subyacente de H (el lector debe verificar esto).

□

5.5. Caminos Eulerianos y Hamiltonianos

5.5.1. Introducción

¿Podemos viajar a lo largo de las aristas de un grafo comenzando en un vértice y regresando a él atravesando cada arista del grafo exactamente una vez? De manera similar, ¿podemos viajar a lo largo de las aristas de un grafo comenzando en un vértice y regresando a él mientras visitamos cada vértice del grafo exactamente una vez?

Aunque estas preguntas parecen ser similares, la primera pregunta, que pregunta si un grafo tiene un circuito de Euler, se puede responder fácilmente simplemente examinando los grados de los vértices del grafo, mientras que la segunda pregunta, que pregunta si un grafo tiene un circuito de Hamilton es bastante difícil de resolver para la mayoría de los grafos.

En esta sección estudiaremos estas preguntas y discutiremos la dificultad de resolverlas. Aunque ambas preguntas tienen muchas aplicaciones prácticas en muchas áreas diferentes, ambas surgieron en viejos acertijos. Aprenderemos sobre estos viejos rompecabezas, así como sobre aplicaciones prácticas modernas.

5.5.2. Caminos y circuitos de Euler

La ciudad de Königsberg, Prusia (ahora llamada Kaliningrado y parte de la república rusa), estaba dividida en cuatro secciones por los brazos del río Pregel. Estas cuatro secciones incluían las dos regiones a orillas del Pregel, la isla Kneiphof y la región entre las dos ramas del Pregel.

En el siglo XVIII, siete puentes conectaban estas regiones[2]. La figura 5.41 muestra estas regiones y puentes. La gente del pueblo daba largos paseos por la ciudad los domingos. Se preguntaron si era posible comenzar en algún lugar de la ciudad, cruzar todos los puentes una vez sin cruzar ningún puente dos veces y regresar al punto de partida.

El matemático suizo Leonhard Euler resolvió este problema. Su solución, publicada en 1736, puede ser el primer uso de la teoría de grafos. Euler estu-

[2]Sólo cinco puentes conectan Kaliningrado en la actualidad. De estos, sólo quedan dos de la época de Euler.

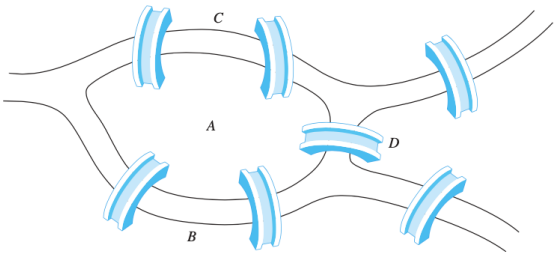


Figura 5.41: Los siete puentes de Königsberg.

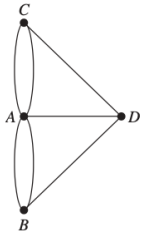


Figura 5.42: Multigrafo que modela la ciudad de Königsberg.

dió este problema usando el multigrafo obtenido cuando las cuatro regiones están representadas por vértices y los puentes por aristas. Este multigrafo se muestra en la Figura 5.42.

El problema de cruzar todos los puentes sin cruzar ningún puente más de una vez puede reformularse en términos de este modelo. La pregunta es: ¿Existe un circuito simple en este multigrafo que contenga todas las aristas?

Definición 5.5.1 Un *circuito de Euler* en un grafo G es un circuito simple que contiene todas las aristas de G. Un *camino de Euler* en G es un camino simple que contiene todos las aristas de G.

Los Ejemplos 5.5.1 y 5.5.2 ilustran el concepto de circuitos y caminos de Euler.

Ejemplo 5.5.1 ¿Cuál de los grafos no dirigidas de la Figura 5.43 tiene un circuito de Euler? De los que no lo tienen, ¿cuáles tienen un camino de Euler?

Solución: El grafo G_1 tiene un circuito de Euler, por ejemplo, a, e, c, d, e, b, a. Ninguno de los grafos G_2 o G_3 tiene un circuito de Euler (el

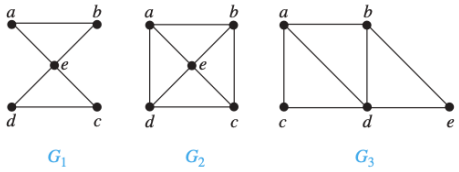


Figura 5.43: Los grafos no dirigidos para el Ejemplo 5.5.1.

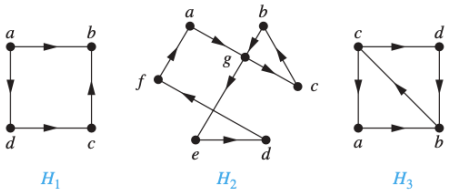


Figura 5.44: Los grafos dirigidos para el Ejemplo 5.5.2.

lector debe verificar esto). Sin embargo, G_3 tiene un camino de Euler, a saber, a, c, d, e, b, d, a, b. G_2 no tiene un camino de Euler (como el lector debe verificar).

□

Ejemplo 5.5.2 ¿Cuál de los grafos dirigidos de la Figura 5.44 tiene un circuito de Euler? De los que no lo tienen, ¿cuáles tienen un camino de Euler?

Solución: El grafo H_2 tiene un circuito de Euler, por ejemplo, a, g, c, b, g, e, d, f, a. Ni H_1 ni H_3 tienen un circuito de Euler (como el lector debe verificar). H_3 tiene un camino de Euler, a saber, c, a, b, c, d, b, pero H_1 no lo tiene (como el lector debería verificar).

□

CONDICIONES NECESARIAS Y SUFICIENTES PARA CIRCUITOS Y CAMINOS DE EULER Existen criterios simples para determinar si un multigrafo tiene un circuito de Euler o un camino de Euler. Euler los descubrió cuando resolvió el famoso problema del puente de Königsberg. Supondremos que todos los grafos discutidas en esta sección tienen un número finito de vértices y aristas.

¿Qué podemos decir si un multigrafo conectado tiene un circuito de Euler? Lo que podemos mostrar es que cada vértice debe tener un grado par. Para hacer esto, primero observe que un circuito de Euler comienza con un vértice a y continúa con una arista incidente con a, digamos $\{a, b\}$. La arista $\{a, b\}$

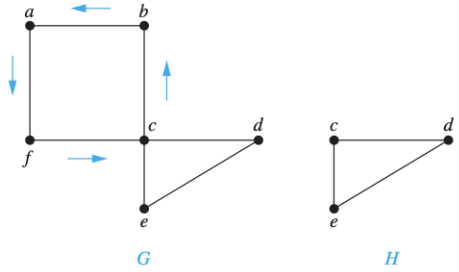


Figura 5.45: Construcción de un circuito de Euler en G.

contribuye con uno al $deg(a)$.

Cada vez que el circuito pasa por un vértice, contribuye con dos al grado del vértice, porque el circuito entra por una arista que incide en este vértice y sale por otra arista. Finalmente, el circuito termina donde comenzó, contribuyendo con uno al $deg(a)$. Por lo tanto, el deg(a) debe ser par, porque el circuito aporta uno cuando comienza, uno cuando termina y dos cada vez que pasa por a (si es que alguna vez lo hace).

Un vértice distinto de a tiene un grado par porque el circuito contribuye con dos a su grado cada vez que pasa por el vértice. Concluimos que si un grafo conectado tiene un circuito de Euler, entonces cada vértice debe tener un grado par.

¿Es también suficiente esta condición necesaria para la existencia de un circuito de Euler? Es decir, ¿debe existir un circuito de Euler en un multigrafo conectado si todos los vértices tienen un grado par? Esta cuestión puede resolverse afirmativamente con una construcción.

Suponga que G es un grafo múltiple conectado con al menos dos vértices y que el grado de cada vértice de G es par. Formaremos un circuito simple que comienza en un vértice arbitrario a de G, construyéndolo arista por arista.

Sea $x_0 = a$. Primero, elegimos arbitrariamente una arista $\{x_0, x_1\}$ incidente con a lo cual es posible porque G está conectado. Continuamos construyendo un camino simple $\{x_0, x_1\}$, $\{x_1, x_2\}, \ldots, \{x_{n-1}, x_n\}$, agregando sucesivamente las aristas una por una al camino hasta que no podamos agregar otra arista al camino.

Esto sucede cuando llegamos a un vértice para el que ya hemos incluido todas las aristas incidentes con ese vértice en el camino. Por ejemplo, en el grafo G de la Figura 5.45 comenzamos en a y elegimos sucesivamente las aristas $\{a, f\}$, $\{f, c\}$, $\{c, b\}$ y $\{b, a\}$.

El camino que hemos construido debe terminar porque el grafo tiene un número finito de aristas, por lo que tenemos la garantía de llegar eventualmente a un vértice para el que no hay aristas disponibles para agregar al camino.

El camino comienza en a con una arista de la forma $\{a, x\}$, y ahora mostramos que debe terminar en a con una arista de la forma $\{y, a\}$. Para ver que el camino debe terminar en a, tenga en cuenta que cada vez que el camino atraviesa un vértice con un grado par, usa sólo una arista para ingresar a este vértice, por lo que debido a que el grado debe ser al menos dos, al menos queda una arista para el camino para dejar el vértice.

Además, cada vez que entramos y salimos de un vértice de grado par, hay un número par de aristas incidentes con este vértice que aún no hemos utilizado en nuestro camino. En consecuencia, a medida que formamos el camino, cada vez que entramos en un vértice que no sea a, podemos dejarlo.

Esto significa que el camino sólo puede terminar en a. A continuación, tenga en cuenta que el camino que hemos construido puede usar todos las aristas del grafo, o puede que no lo haga si hemos regresado a a por última vez antes de usar todas las aristas.

Se ha construido un circuito de Euler si se han utilizado todas las aristas. De lo contrario, considere el subgrafo H obtenido de G al eliminar las aristas ya utilizados y los vértices que no son incidentes con las aristas restantes. Cuando eliminamos el circuito a, f, c, b, a del grafo de la Figura 5.45, obtenemos el subgrafo etiquetado como H.

Como G está conectado, H tiene al menos un vértice en común con el circuito que se ha eliminado. Sea w tal vértice. (En nuestro ejemplo, c es el vértice). Cada vértice en H tiene un grado par (porque en G todos los vértices tenían un grado par, y para cada vértice, los pares de aristas incidentes con este vértice se han eliminado para formar H).

Tenga en cuenta que es posible que H no esté conectado. Comenzando en w, construya un camino simple en H eligiendo aristas tanto como sea posible, como se hizo en G. Este camino debe terminar en w. Por ejemplo, en la Figura 5.45, c, d, e, c es un camino en H.

Luego, forme un circuito en G empalmando el circuito en H con el circuito original en G (esto se puede hacer porque w es uno de los vértices en este circuito). Cuando se hace esto en el grafo de la Figura 5.45, obtenemos el circuito a, f, c, d, e, c, b, a.

Continúe este proceso hasta que se hayan utilizado todas las aristas. (El proceso debe terminar porque solo hay un número finito de aristas en el

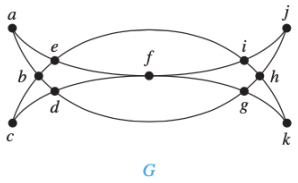


Figura 5.46: Las cimitarras de Mohammed.

grafo). Esto produce un circuito de Euler. La construcción muestra que si todos los vértices de un multígrafo conectado tienen grados pares, entonces el grafo tiene un circuito de Euler.

Resumimos estos resultados en el Teorema 5.5.1.

Teorema 5.5.1 Un multigrafo conectado con al menos dos vértices tiene un circuito de Euler si y sólo si cada uno de sus vértices tiene un grado par. ■

Ahora podemos resolver el problema del puente de Königsberg. Debido a que el multigrafo que representa estos puentes, que se muestra en la Figura 5.42, tiene cuatro vértices de grado impar, no tiene un circuito de Euler. No hay forma de comenzar en un punto dado, cruzar cada puente exactamente una vez y regresar al punto de partida.

El procedimiento constructivo para encontrar los circuitos de Euler dado en la discusión que precede al Teorema 5.5.1 se puede formalizar en un algoritmo. (Debido a que los circuitos en el procedimiento se eligen arbitrariamente, hay cierta ambigüedad. No nos molestaremos en eliminar esta ambigüedad especificando los pasos del procedimiento con mayor precisión.)

Dicho algoritmo para construir circuitos de Euler es eficiente para encontrar circuitos de Euler en un multigrafo G conectado con todos los vértices de grado par. El Ejemplo 5.5.3 muestra cómo los caminos y circuitos de Euler se pueden usar para resolver un tipo de rompecabezas.

Ejemplo 5.5.3 Muchos acertijos te piden que dibujes una imagen con un movimiento continuo sin levantar un lápiz para que ninguna parte de la imagen vuelva a aparecer. Podemos resolver estos acertijos utilizando circuitos y caminos de Euler. Por ejemplo, ¿se pueden dibujar las cimitarras de Mohammed, que se muestran en la Figura 5.46, de esta manera, donde el dibujo comienza y termina en el mismo punto?

Solución: Podemos resolver este problema porque el grafo G que se muestra en la Figura 5.46 tiene un circuito de Euler. Tiene tal circuito porque todos sus vértices tienen grado par.

Usaremos el algoritmo bosquejado para construir un circuito de Euler. Primero, formamos el circuito $a, b, d, c, b, e, i, f, e, a$. Obtenemos el subgrafo H eliminando las aristas en este circuito y todos los vértices que quedan aislados cuando se eliminan estas aristas.

Luego formamos el circuito $d, g, h, j, i, h, k, g, f, d$ en H. Después de formar este circuito, hemos usado todos las aristas en G. Al empalmar este nuevo circuito en el primer circuito en el lugar apropiado produce el circuito de Euler $a, b, d, g, h, j, i, h, k, g, f, d, c, b, e, i, f, e, a$.

Este circuito da una forma de dibujar las cimitarras sin levantar el lápiz o volver sobre parte de la imagen.

□

Ahora mostraremos que un multigrafo conectado tiene un camino de Euler (y no un circuito de Euler) si y sólo si tiene exactamente dos vértices de grado impar. Primero, suponga que un multigrafo conectado tiene un camino de Euler desde a hasta b, pero no un circuito de Euler.

La primer arista del camino aporta uno al grado de a. Se hace una contribución de dos al grado de a cada vez que el camino pasa por a. La última arista del camino aporta uno al grado de b. Cada vez que el camino pasa por b hay una contribución de dos a su grado.

En consecuencia, tanto a como b tienen un grado impar. Todos los demás vértices tienen un grado par, porque el camino aporta dos al grado de un vértice cada vez que lo atraviesa.

Ahora considere lo contrario. Suponga que un grafo tiene exactamente dos vértices de grado impar, digamos a y b. Considere el grafo más grande compuesto por el grafo original con la adición de una arista $\{a, b\}$. Cada vértice de este grafo más grande tiene un grado par, por lo que hay un circuito de Euler. La eliminación de la nueva arista produce un camino de Euler en el grafo original. El Teorema 5.5.2 resume estos resultados.

Teorema 5.5.2 Un multigrafo conectado tiene un camino de Euler pero no un circuito de Euler si y sólo si tiene exactamente dos vértices de grado impar.

■

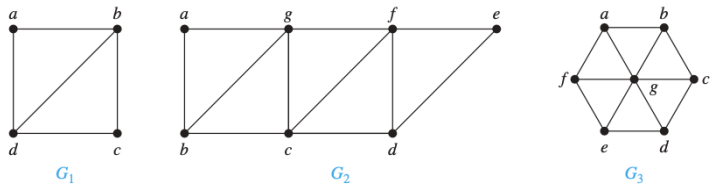


Figura 5.47: Tres grafos no dirigidos para el Ejemplo 5.5.4.

Ejemplo 5.5.4 ¿Cuáles de los grafos que se muestran en la Figura 5.47 tienen un camino de Euler?

Solución: G_1 contiene exactamente dos vértices de grado impar, a saber, b y d. Por lo tanto, tiene un camino de Euler que debe tener a b y d como puntos finales. Uno de esos caminos de Euler es d, a, b, c, d, b.

De manera similar, G_2 tiene exactamente dos vértices de grado impar, a saber, b y d. Por lo tanto, tiene un camino de Euler que debe tener a b y d como puntos finales. Uno de esos caminos de Euler es b, a, g, f, e, d, c, g, b, c, f, d.

G_3 no tiene camino de Euler porque tiene seis vértices de grado impar.

□

Volviendo a Königsberg del siglo XVIII, ¿es posible comenzar en algún punto de la ciudad, atravesar todos los puentes y terminar en algún otro punto de la ciudad? Esta pregunta se puede responder determinando si existe un camino de Euler en el multigrafo que representa los puentes en Königsberg. Debido a que hay cuatro vértices de grado impar en este multigrafo, no hay un camino de Euler, por lo que tal viaje es imposible.

APLICACIONES DE CAMINOS Y CIRCUITOS DE EULER Los caminos y circuitos de Euler se pueden utilizar para resolver muchos problemas prácticos. Por ejemplo, muchas aplicaciones requieren un camino o circuito que atraviese cada calle de un vecindario, cada camino en una red de transporte, cada conexión en una red de servicios públicos o cada enlace en una red de comunicaciones exactamente una vez.

Encontrar un camino o circuito de Euler en el grafo del modelo apropiado puede resolver estos problemas. Por ejemplo, si un cartero puede encontrar un camino de Euler en el grafo que representa las calles que el cartero necesita cubrir, este camino produce un camino que atraviesa cada calle del camino exactamente una vez.

Si no existe un camino de Euler, algunas calles deberán atravesarse más

de una vez. El problema de encontrar un circuito en un grafo con la menor cantidad de aristas que atraviesa cada arista al menos una vez se conoce como el *problema del cartero chino* en honor a Guan Meigu, quien lo planteó en 1962. Ver [MiRo91] para más información sobre la solución de el problema del cartero chino cuando no existe un camino de Euler.

Entre las otras áreas en las que se aplican los circuitos y caminos de Euler está en el diseño de circuitos, en la multidifusión de redes y en la biología molecular, donde los caminos de Euler se utilizan en la secuenciación del ADN.

5.5.3. Caminos y circuitos de Hamilton

Hemos desarrollado las condiciones necesarias y suficientes para la existencia de caminos y circuitos que contengan exactamente una vez cada arista de un multigrafo. ¿Podemos hacer lo mismo con caminos y circuitos simples que contienen exactamente una vez cada vértice del grafo?

Definición 5.5.2 Un camino simple en un grafo G que pasa por cada vértice exactamente una vez se llama *camino de Hamilton*, y un circuito simple en un grafo G que pasa por cada vértice exactamente una vez se llama *circuito de Hamilton*. Es decir, el camino simple x_0, $x_1, \ldots$, x_{n-1}, x_n en el grafo $G = (V, E)$ es un camino de Hamilton si $V = \{x_0, x_1, \ldots, x_{n-1}, x_n\}$ y $x_i \neq x_j$ para $0 \leq i < j \leq n$, y el circuito simple $x_0, x_1, \ldots, x_{n-1}, x_n, x_0$ (con $n > 0$) es un circuito de Hamilton si $x_0, x_1, \ldots, x_{n-1}, x_n$ es un camino de Hamilton.

Esta terminología proviene de un juego, llamado el *rompecabezas de Icosian*, inventado en 1857 por el matemático irlandés Sir William Rowan Hamilton. Consistía en un dodecaedro de madera [un poliedro con 12 pentágonos regulares como caras, como se muestra en la Figura 5.48 (a)], con una clavija en cada vértice del dodecaedro y una cuerda.

Los 20 vértices del dodecaedro fueron etiquetados con diferentes ciudades del mundo. El objetivo del rompecabezas era comenzar en una ciudad y viajar a lo largo de las aristas del dodecaedro, visitar cada una de las otras 19 ciudades exactamente una vez y terminar de regreso en la primera ciudad. El circuito recorrido se delimitó con la cuerda y las clavijas.

Debido a que el autor no puede proporcionar a cada lector un sólido de madera con clavijas y cuerda, consideraremos la pregunta equivalente: ¿Hay

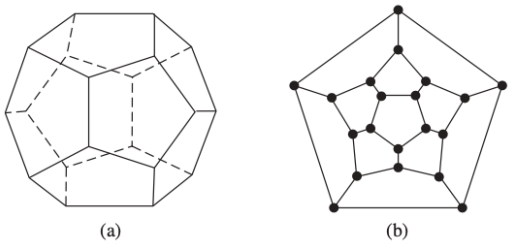


Figura 5.48: El rompecabezas de Hamilton"Un viaje alrededor del mundo".

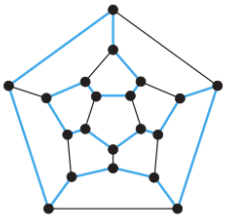


Figura 5.49: Una solución al rompecabezas de Hamilton "Un viaje alrededor del mundo".

un circuito en el grafo que se muestra en la Figura 5.48 (b) que pase por cada vértice exactamente una vez?

Esto resuelve el enigma porque este grafo es isomorfo al grafo que consta de los vértices y aristas del dodecaedro. En la Figura 5.49 se muestra una solución del rompecabezas de Hamilton.

Ejemplo 5.5.5 ¿Cuáles de las grafos simples de la Figura 5.50 tienen un circuito de Hamilton o, en caso contrario, un camino de Hamilton?

Solución: G_1 tiene un circuito de Hamilton: a, b, c, d, e, a.

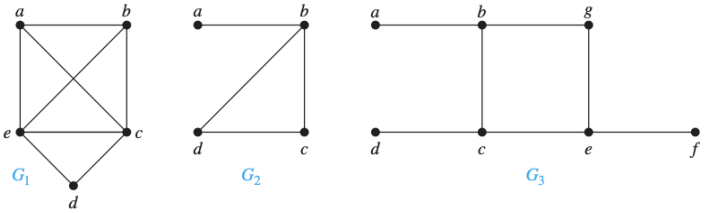


Figura 5.50: Tres grafos simples para el Ejemplo 5.5.5.

No hay un circuito de Hamilton en G_2 (esto se puede ver si se observa que cualquier circuito que contenga todos los vértices debe contener la arista $\{a, b\}$ dos veces), pero G_2 tiene un camino de Hamilton, a saber, a, b, c, d.

G_3 no tiene un circuito de Hamilton ni un camino de Hamilton, porque cualquier camino que contenga todos los vértices debe contener una de las aristas $\{a, b\}$, $\{e, f\}$ y $\{c, d\}$ más de una vez.

□

CONDICIONES PARA LA EXISTENCIA DE CIRCUITOS DE HAMILTON ¿Existe una forma sencilla de determinar si un grafo tiene un circuito o un camino de Hamilton? Al principio, podría parecer que debería haber una forma fácil de determinar esto, porque existe una forma sencilla de responder a la pregunta similar de si un grafo tiene un circuito de Euler.

Sorprendentemente, no se conocen criterios simples necesarios y suficientes para la existencia de circuitos de Hamilton. Sin embargo, se conocen muchos teoremas que dan condiciones suficientes para la existencia de circuitos de Hamilton. Además, se pueden usar ciertas propiedades para mostrar que un grafo no tiene un circuito de Hamilton.

Por ejemplo, un grafo con un vértice de grado uno no puede tener un circuito de Hamilton, porque en un circuito de Hamilton, cada vértice incide con dos aristas en el circuito. Además, si un vértice en el grafo tiene grado dos, entonces ambas aristas que inciden con este vértice deben ser parte de cualquier circuito de Hamilton.

También, tenga en cuenta que cuando se está construyendo un circuito de Hamilton y este circuito ha pasado por un vértice, entonces todas las aristas restantes que inciden en este vértice, distintos de los dos utilizados en el circuito, pueden eliminarse de la consideración. Aún más, un circuito de Hamilton no puede contener un circuito más pequeño dentro de él.

Ejemplo 5.5.6 Muestre que ninguno de los grafos que se muestran en la Figura 5.51 tiene un circuito de Hamilton.

Solución: No hay circuito de Hamilton en G porque G tiene un vértice de grado uno, es decir, e.

Ahora considere H. Dado que los grados de los vértices a, b, d y e son dos, cada arista incidente con estos vértices debe ser parte de cualquier circuito de Hamilton. Ahora es fácil ver que no puede existir ningún circuito de Hamilton en H, ya que cualquier circuito de Hamilton tendría que contener cuatro aristas incidentes con c, lo cual es imposible.

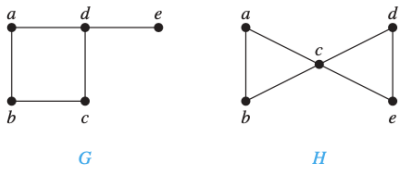


Figura 5.51: Dos grafos que no tienen un circuito de Hamilton.

□

Ejemplo 5.5.7 Demuestre que K_n tiene un circuito de Hamilton siempre que $n \geq 3$.

Solución: Podemos formar un circuito de Hamilton en K_n comenzando en cualquier vértice. Dicho circuito se puede construir visitando vértices en el orden que elijamos, siempre que la ruta comience y termine en el mismo vértice y se visite entre sí exactamente una vez. Esto es posible porque hay aristas en K_n entre dos vértices cualesquiera.

□

Aunque no se conocen condiciones útiles, necesarias y suficientes para la existencia de circuitos de Hamilton, se han encontrado bastantes condiciones suficientes. Tenga en cuenta que cuantas más aristas tenga un grafo, más probable será que tenga un circuito de Hamilton.

Además, agregar aristas (pero no vértices) a un grafo con un circuito de Hamilton produce un grafo con el mismo circuito de Hamilton. Entonces, a medida que agregamos aristas a un grafo, especialmente cuando nos aseguramos de agregar aristas a cada vértice, aumenta la probabilidad de que exista un circuito de Hamilton en este grafo.

En consecuencia, esperaríamos que hubiera condiciones suficientes para la existencia de circuitos de Hamilton que dependan de que los grados de los vértices sean suficientemente grandes. Enunciamos aquí dos de las condiciones suficientes más importantes. Estas condiciones fueron encontradas por Gabriel A. Dirac en 1952 y Øystein Ore en 1960.

Teorema 5.5.3 TEOREMA DE DIRAC Si G es un grafo simple con n vértices con $n \geq 3$ tal que el grado de cada vértice en G es al menos $n/2$, entonces G tiene un circuito de Hamilton.

■

Teorema 5.5.4 TEOREMA DE ORE Si G es un grafo simple con n vértices con $n \geq 3$ tal que $deg(u) + deg(v) \geq n$ para cada par de vértices no adyacentes u y v en G, entonces G tiene un circuito de Hamilton.

■

Tanto el teorema de Ore como el teorema de Dirac proporcionan condiciones suficientes para que un grafo simple conectado tenga un circuito de Hamilton. Sin embargo, estos teoremas no proporcionan las condiciones necesarias para la existencia de un circuito de Hamilton.

Por ejemplo, el grafo C_5 tiene un circuito de Hamilton pero no satisface las hipótesis del teorema de Ore ni del teorema de Dirac, como puede verificar el lector.

Los mejores algoritmos conocidos para encontrar un circuito de Hamilton en un grafo o determinar que no existe tal circuito tienen una complejidad de tiempo exponencial en el peor de los casos (en el número de vértices del grafo).

Encontrar un algoritmo que resuelva este problema con complejidad en tiempo polinomial en el peor de los casos sería un logro importante porque se ha demostrado que este problema es NP-completo. En consecuencia, la existencia de tal algoritmo implicaría que muchos otros problemas aparentemente intratables podrían resolverse utilizando algoritmos con complejidad de tiempo polinomial en el peor de los casos.

APLICACIONES DE CIRCUITOS DE HAMILTON Los caminos y circuitos de Hamilton se pueden utilizar para resolver problemas prácticos.

Por ejemplo, muchas aplicaciones requieren un camino o circuito que visite exactamente una vez cada intersección de carreteras en una ciudad, cada lugar donde las tuberías se cruzan en una red de servicios públicos o cada nodo en una red de comunicaciones.

Encontrar un camino o circuito de Hamilton en el modelo de grafo apropiado puede resolver estos problemas. El famoso problema del agente viajero o TSP (también conocido en la literatura antigua como el problema del vendedor ambulante) busca el camino más corto que un vendedor ambulante debe tomar para visitar un conjunto de ciudades.

Este problema se reduce a encontrar un circuito de Hamilton en un grafo completo de modo que el peso total de sus aristas sea lo más pequeño posible.

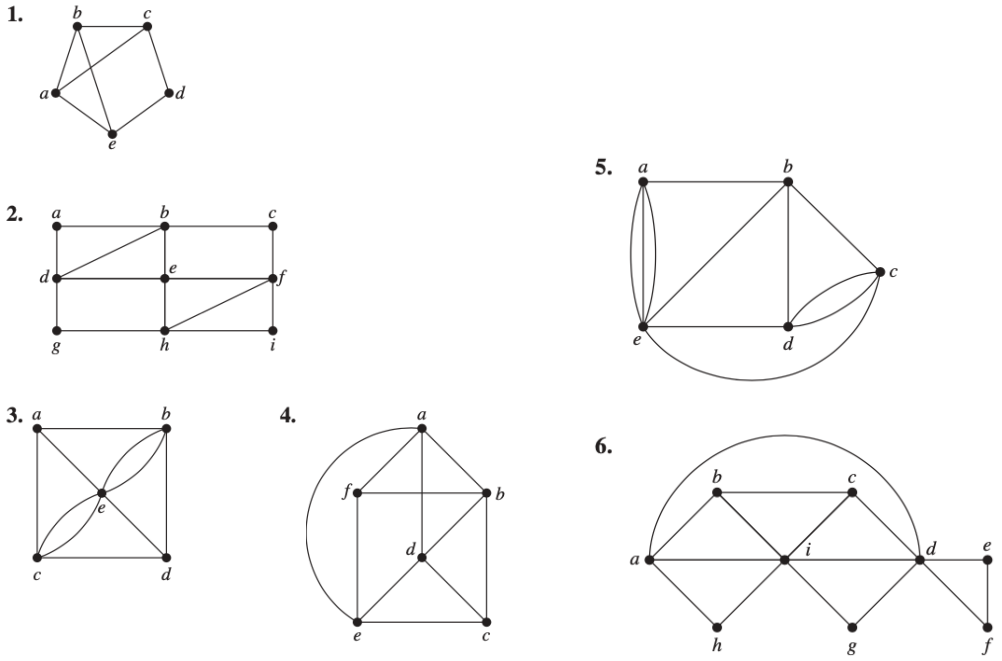


Figura 5.52: Grafos para el Ejercicio 1.

5.5.4. Ejercicios

1. Para cada uno de los grafos de la Figura 5.52 determine si tiene un circuito de Euler. Construya tal circuito cuando exista uno. Si no existe un circuito de Euler, determine si el grafo tiene un camino de Euler y construya dicho camino si existe.

2. Para cada uno de los grafos de la Figura 5.53 determine si tiene un circuito de Hamilton. Construya tal circuito cuando exista uno. Si no existe un circuito de Hamilton, determine si el grafo tiene un camino de Hamilton y construya dicho camino si existe.

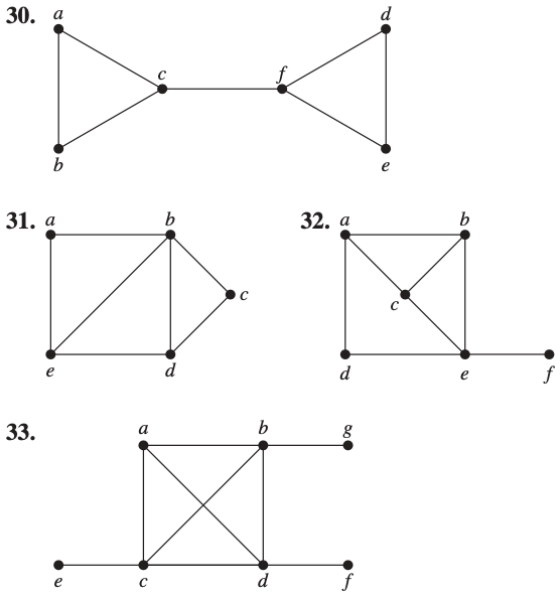


Figura 5.53: Grafos para el Ejercicio 2.