

Grado en Ingeniería Informática
2018-2019

Apuntes
Matemática Discreta

Jorge Rodríguez Fraile¹



Esta obra se encuentra sujeta a la licencia Creative Commons
Reconocimiento - No Comercial - Sin Obra Derivada

¹Universidad: 100405951@alumnos.uc3m.es | Personal: jrf1616@gmail.com

ÍNDICE GENERAL

| | |
|-----------------|----------|
| I Teoría | 3 |
|-----------------|----------|

Parte I

Teoría

Transparencias de Matemática Discreta

Grado en Ingeniería en Informática

Doble Grado en Ingeniería en Informática y
Administración de Empresas

Curso 2018–2019

Grupo de Modelización, Simulación Numérica y Matemática Industrial

*Universidad Carlos III de Madrid
Avda. de la Universidad, 30
28911 Leganés*

v1.0: Enero 2019

Aviso importante

Estas notas son sólomente un **guión orientativo** o ayuda para seguir el curso de Matemática Discreta. En ningún caso pretenden sustituir la bibliografía básica e imprescindible que todo alumno debe de consultar para adquirir los conocimientos requeridos en el programa de la asignatura. Esta bibliografía la podéis encontrar en la Guía de la asignatura (disponible en Aula Global) o en la correspondiente Ficha Reina.

Matemática Discreta

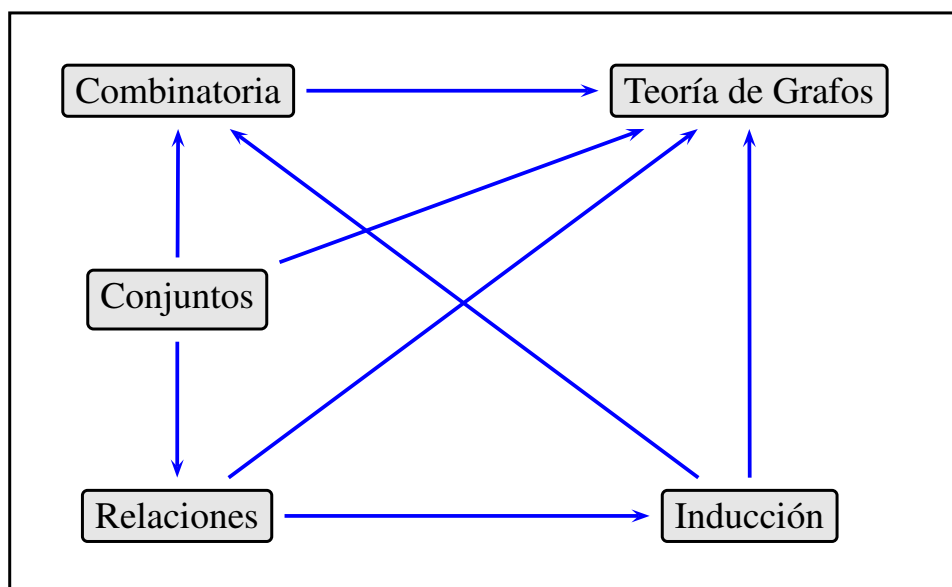
Curso 2018–2019

Grado en Ingeniería en Informática
Doble Grado en Ingeniería en Informática y Administración de Empresas

Universidad Carlos III de Madrid

DM– p. 1/141

Relaciones entre temas



DM– p. 2/141

Tema 1: Conjuntos y funciones

1. Teoría elemental de conjuntos:

- Definiciones y operaciones.
- Los números naturales.

2. Funciones:

- Definiciones y operaciones.
- Tipos de funciones.

3. Divisibilidad de enteros:

- Teorema de la divisibilidad.
- Máximo común divisor y mínimo común múltiplo.
- Números primos. Teorema fundamental de la aritmética.

DM– p. 3/141

Teoría de conjuntos elemental

Definición 1

Un **conjunto** X es una colección bien definida de objetos (denominados **elementos** del conjunto):

$$X = \{x_1, x_2, x_3, \dots\}.$$

Dado un conjunto X y un cierto objeto x una y sólo una de las siguientes afirmaciones debe ser cierta:

- o bien $x \in X$, es decir el objeto x pertenece al conjunto X ,
- o bien no pertenece, $x \notin X$.

El orden de los elementos de un conjunto es irrelevante, así como el número de veces que aparece un elemento dado en el conjunto.

Definición 2

Dos conjuntos son iguales si y sólo si tienen los mismos elementos.

Definición 3

El **conjunto vacío** \emptyset es aquél que no tiene elementos: $\emptyset = \{ \}$. El **conjunto universal** S es aquel que contiene todos los elementos de la clase que estemos considerando.

DM– p. 4/141

¿Cómo definir un conjunto?

- **Por extensión:** en el caso de que sea posible enumerar todos los elementos de un conjunto:

$$X = \{1, 2, 3, 4, 5, 6\}.$$

- **Por comprensión:** en el caso de que su definición se realice atendiendo a la propiedad común que poseen todos los elementos del conjunto:

$$Y = \{y: y \text{ es una provincia de Andalucía}\}.$$

- **Notación “mixta”:**

$$Z = \{1, 2\} \cup \{x: x \in [4, 5]\}.$$

- Podemos definir un conjunto utilizando otro ya conocido a través de alguna regla de formación:

$$C = \{n^3: n \in \mathbb{N}\} = \{m \in \mathbb{N}: \exists k \in \mathbb{N} \text{ tal que } m = k^3\}.$$

- Los diagramas de Venn son una representación muy útil de un conjunto.

DM– p. 5/141

Subconjuntos

Definición 4

*A es un **subconjunto** de B ($A \subseteq B$) si todo elemento de A está en B. Si existen elementos de B que no están en A, entonces A es un **subconjunto propio** de B ($A \subset B$).*

- Todo conjunto A satisface $A \subseteq A \subseteq S$.
- El conjunto vacío \emptyset satisface la propiedad $\emptyset \subseteq A$ para cualquier conjunto A.

Definición 5

*El **conjunto de las partes del conjunto** A (que se denota con el símbolo $\mathcal{P}(A)$) es el conjunto de todos los subconjuntos de A:*

$$\mathcal{P}(A) = \{B: B \subseteq A\}.$$

DM– p. 6/141

Operaciones con conjuntos

Dados dos conjuntos A y B podemos definir las siguientes operaciones:

- **Unión:** $A \cup B = \{x: (x \in B) \vee (x \in A)\}.$
- **Intersección:** $A \cap B = \{x: (x \in B) \wedge (x \in A)\}.$
- **Conjunto complementario:** $\overline{A} = \{x: x \notin A\}$ y además satisface que $\overline{(\overline{A})} = A.$
- **Diferencia:** $A \setminus B = \{x: (x \in A) \wedge (x \notin B)\}.$
- **Diferencia simétrica:** $A \triangle B = \{x: (x \in A \cup B) \wedge (x \notin A \cap B)\}.$

Algunas propiedades:

- **Leyes distributivas**
 - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$
 - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$
- **Leyes de De Morgan**
 - $\overline{A \cup B} = \overline{A} \cap \overline{B}.$
 - $\overline{A \cap B} = \overline{A} \cup \overline{B}.$
- $A \triangle B = (A \setminus B) \cup (B \setminus A).$

DM- p. 7/141

Producto cartesiano

Definición 6

Dados dos conjuntos X e Y , el **producto cartesiano** $X \times Y$ se define como el conjunto de los **pares ordenados**:

$$X \times Y = \{(x, y): (x \in X) \wedge (y \in Y)\}.$$

Observación: No es lo mismo usar $\{ \}$ ó $()$. En concreto $\{1, 2\}$ denota un conjunto y por tanto $\{1, 2\} = \{2, 1\}$. Sin embargo $(1, 2)$ es un par ordenado y por tanto $(1, 2) \neq (2, 1)$.

Definición 7

Dos conjuntos A y B son **disjuntos** si $A \cap B = \emptyset$.

DM- p. 8/141

Los números naturales

Definición 8

El conjunto de los números naturales \mathbb{N} se define mediante las condiciones siguientes:

- (1) $1 \in \mathbb{N}$.
- (2) Si $n \in \mathbb{N}$, entonces el número $n + 1$ (denominado el sucesor de n) también pertenece a \mathbb{N} .
- (3) Todo $n \in \mathbb{N}$ distinto de 1 es el sucesor de algún número en \mathbb{N} .
- (4) Todo subconjunto no vacío de \mathbb{N} tiene un elemento mínimo (*Principio de buena ordenación*).

- Notar que $0 \notin \mathbb{N}$.
- Los enteros no negativos se definen como $\mathbb{Z}_+ = \{0\} \cup \mathbb{N}$.
- Informalmente podemos definir los siguientes conjuntos de números:
 - Números enteros: $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.
 - Números racionales: $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$. En realidad, cada número racional $\frac{p}{q}$ se puede representar de infinitas maneras: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \dots$.

DM– p. 9/141

Funciones

Definición 9 (Spivak)

Una **función** $f \subset X \times Y$ de un conjunto X en un conjunto Y es un subconjunto del producto cartesiano $X \times Y$ tal que para cualquier $x \in X$, f contiene exactamente un par de la forma (x, y) . Al conjunto X se le denomina **dominio** de la función f ó $\text{Dom}(f)$ y al conjunto Y se le denomina **codominio** de f . La **imagen** de la función f es el conjunto

$$\text{Im}(f) = \{y : \exists x \in X \text{ tal que } (x, y) \in f\}.$$

- Dados dos conjuntos X e Y , una función es un objeto que a cada elemento $x \in X$ le asigna un único elemento $y \in Y$ al que se suele denominar $y = f(x)$. Habitualmente las funciones se denotan mediante $f : X \rightarrow Y$.
- Cuando no hay duda acerca de los conjuntos X e Y , la notación se suele reducir a expresiones del tipo $x \rightarrow f(x)$ ó $y = f(x)$.

DM– p. 10/141

Tipos de funciones

Definición 10

Dada una función $f: X \rightarrow Y$, decimos que

- f es **inyectiva** si $x_1 \neq x_2$ implica $f(x_1) \neq f(x_2)$.
- f es **sobreyectiva** si para cada $y \in Y$ existe al menos un $x \in X$ tal que $y = f(x)$.
- f es **biyectiva** si es inyectiva y sobreyectiva.

Si $f: X \rightarrow Y$ es una biyección, podemos definir su **función inversa** $f^{-1}: Y \rightarrow X$ a través de la regla (bien definida)

$$f^{-1}(y) = x \Leftrightarrow y = f(x).$$

Dadas dos funciones $f: X \rightarrow Y$, $g: Y \rightarrow Z$, es posible definir una nueva función $g \circ f: X \rightarrow Z$ mediante la expresión:

$$(g \circ f)(x) = g(f(x)).$$

La función $g \circ f$ es la **composición** de las funciones f y g .

DM– p. 11/141

Divisibilidad de enteros

El conjunto de los enteros \mathbb{Z} es *cerrado* bajo las operaciones de suma, diferencia y producto. Es decir, para todo $a, b \in \mathbb{Z}$, $a \pm b \in \mathbb{Z}$ y $a \cdot b \in \mathbb{Z}$. Además satisfacen que

- 0 es el elemento neutro de la suma: $a + 0 = a$ para todo $a \in \mathbb{Z}$.
- 1 es el elemento neutro del producto: $a \cdot 1 = a$ para todo $a \in \mathbb{Z}$.
- Para todo $a \in \mathbb{Z}$, existe un único elemento inverso $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.

Sin embargo, el cociente de los enteros puede no ser entero. Por ello debemos definir con cuidado cuándo un número entero divide a otro.

Definición 11

Dados dos enteros $a \neq 0$ y b , se dice de a **divide a b** si existe un entero $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Cuando a divide a b , se dice que a es un **factor** o **divisor** de b y que b es un **múltiplo** de a . Si a divide a b , lo denotamos por $a \mid b$ y si a no divide a b , por $a \nmid b$.

Observaciones:

- Cualquier entero no nulo $a \in \mathbb{Z}$ divide a 0: $0 = a \cdot 0$ ($q = 0$).
- 1 divide a cualquier entero $a \in \mathbb{Z}$: $a = 1 \cdot a$ ($q = a$).
- Cualquier entero no nulo $a \in \mathbb{Z}$ se divide a sí mismo: $a = a \cdot 1$ ($q = 1$).

DM– p. 12/141

Algoritmo de divisibilidad

Teorema 12 (Algoritmo de divisibilidad) Sean a y $b \neq 0$ dos enteros, entonces existe un único par de enteros q y r tales que

$$a = q \cdot b + r \quad \text{con} \quad 0 \leq r < |b|.$$

- Los números a y b se denominan respectivamente **dividendo** y **divisor**.
- El número r se denomina **resto de la división**: $r = a \bmod b$.
- El número q se denomina **cociente de la división**:

$$q = a \operatorname{div} b = \begin{cases} \lfloor a/b \rfloor & \text{si } b > 0, \\ \lceil a/b \rceil & \text{si } b < 0, \end{cases}$$

donde

- La función **suelo** asigna a cada número real x el **mayor** entero tal que $\lfloor x \rfloor \leq x$.
- La función **techo** asigna a cada número real x el **menor** entero tal que $\lceil x \rceil \geq x$.

DM– p. 13/141

Máximo común divisor

Definición 13

Dados dos enteros a, b no simultáneamente nulos, se denomina **máximo común divisor** de a y b [denotado por $\operatorname{mcd}(a, b)$] al mayor entero d tal que $d \mid a$ y $d \mid b$.

Observación: El caso $a = b = 0$ hay que excluirlo porque cualquier número divide al 0.

Teorema 14 El máximo común divisor de dos números enteros es único.

Definición 15

Dados dos números a, b enteros no nulos, se define el **mínimo común múltiplo** de a y b [y se denota por $\operatorname{mcm}(a, b)$] al menor número natural m tal que $a \mid m$ y $b \mid m$.

Teorema 16 Si a, b son dos números naturales, entonces

$$\operatorname{mcd}(a, b) \cdot \operatorname{mcm}(a, b) = a \cdot b.$$

Definición 17

Dos números a y b son **coprimos** (o **primos entre sí** o **primos relativos**) si $\operatorname{mcd}(a, b) = 1$.

Los enteros a_1, \dots, a_n son coprimos dos a dos si $\operatorname{mcd}(a_i, a_j) = 1$ para todo $1 \leq i < j \leq n$.

DM– p. 14/141

Teorema fundamental de la aritmética

Definición 18

Un número natural $p > 1$ se denomina **primo** si los únicos divisores naturales de p son 1 y p . Un natural $p > 1$ que no sea primo se denomina **compuesto**.

Observación: El número natural 1 **no** es primo. El primer primo es el número 2 y todos los demás primos son naturales impares (3, 5, 7, 11, ...).

Teorema 19 (Euclides) *Existen infinitos números primos.*

Los números primos son muy importantes porque constituyen los “bloques” fundamentales con que construir los demás naturales:

Teorema 20 (Teorema fundamental de la aritmética) *Todo número natural $n > 1$ se puede descomponer de manera única en factores primos*

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \dots \cdot p_k^{n_k},$$

donde los p_i son primos distintos entre sí y escritos en orden creciente y los exponentes n_i son números naturales.

DM– p. 15/141

Tema 2: Combinatoria elemental I

Definición 21

Sea S un conjunto. Si hay $n \in \mathbb{N}$ elementos distintos en S , decimos que S es un **conjunto finito** y que n es **el cardinal** de S (y lo denotamos por $|S|$).

Definición 22

Dos conjuntos A y B tienen el mismo cardinal si y sólo si existe una función **biyectiva** $f: A \rightarrow B$.

Definición 23

Un conjunto que tiene un número finito de elementos o cuyo cardinal es igual al de \mathbb{N} se denomina **numerable**.

El **objetivo de la combinatoria** es encontrar el cardinal de ciertos conjuntos finitos.

DM– p. 16/141

Combinatoria elemental I

1. **Regla de la suma:** si $A \cap B = \emptyset$, $|A \cup B| = |A| + |B|$.
2. **Regla del producto:** $|A \times B| = |A| \cdot |B|$.
 - Ordenaciones.
 - Subconjuntos ordenados.
 - Subconjuntos.
3. **Principio de inclusión–exclusión:** $|A \cup B| = |A| + |B| - |A \cap B|$.
4. **Principio del palomar.** (Ver las hojas de problemas)

DM– p. 17/141

Principio de la suma

Proposición 24 (Principio de la suma v1) Si A y B son dos conjuntos finitos y disjuntos $A \cap B = \emptyset$, entonces

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

Proposición 25 (Principio de la suma v2) Si A_1, A_2, \dots, A_m son conjuntos finitos y disjuntos dos a dos, se tiene que:

$$|A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \dots + |A_m| = \sum_{j=1}^m |A_j|.$$

Proposición 26 (Principio de la suma v3) Si una tarea se puede hacer de n_1 formas y una segunda tarea se puede hacer de n_2 formas y ambas tareas son incompatibles, entonces hay $n_1 + n_2$ formas de realizar una de las dos tareas.

DM– p. 18/141

Principio del producto

Proposición 27 (Principio del producto v1) Si A y B son dos conjuntos finitos, entonces

$$|A \times B| = |A| \cdot |B|.$$

Proposición 28 (Principio del producto v2) Si A_1, A_2, \dots, A_m son conjuntos finitos, entonces se tiene que:

$$|A_1 \times A_2 \times \dots \times A_m| = |A_1| \cdot |A_2| \cdots |A_m| = \prod_{k=1}^m |A_k|.$$

Proposición 29 (Principio del producto v3) Supongamos que una tarea se puede dividir en dos tareas consecutivas. Si hay n_1 maneras posibles de realizar la primera y n_2 formas de hacer la segunda tarea después de que la primera haya sido realizada, entonces hay $n_1 n_2$ formas de completar la tarea.

DM– p. 19/141

Ordenaciones de un conjunto

Definición 30

Si $n \in \mathbb{N}$, se define el **factorial de n** como $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.

Proposición 31 (Permutaciones de n objetos) n objetos *diferentes* se pueden ordenar de $n!$ maneras distintas.

Proposición 32 (Permutaciones con repetición) El número de maneras distintas de ordenar n objetos clasificados en k *grupos de objetos idénticos entre sí* (con n_1 elementos el primero, n_2 elementos el segundo, etc) es

$$\binom{n}{n_1, n_2, \dots, n_k} \equiv \frac{n!}{n_1! n_2! \cdots n_k!}, \quad \text{con} \quad \sum_{i=1}^k n_i = n.$$

DM– p. 20/141

Subconjuntos ordenados

Proposición 33 Dado un conjunto de n elementos diferentes podemos extraer

$$n(n-1)(n-2)\dots(n-r+1) = \frac{n!}{(n-r)!}$$

subconjuntos ordenados de r elementos.

Observación: Si $r = n$, la primera fórmula implica que hay $n!$ subconjuntos ordenados de n elementos (= permutaciones de n elementos). Para que la segunda fórmula tenga sentido, se define $0! = 1$.

Proposición 34 Dado un conjunto de n elementos diferentes, podemos extraer n^r subconjuntos ordenados de r elementos si permitimos repeticiones.

DM– p. 21/141

Subconjuntos

Proposición 35 El número de subconjuntos distintos que contengan r elementos que pueden extraerse de un conjunto de n elementos diferentes es

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Definición 36 (Números combinatorios)

Para todo $n, r \in \mathbb{Z}_+$ tales que $0 \leq r \leq n$ definimos el **número combinatorio** $\binom{n}{r}$ como

$$\binom{n}{r} = \frac{n!}{r!(n-r)!},$$

donde por convenio se define $0! = 1$.

DM– p. 22/141

Números combinatorios: triángulo de Pascal



Teorema 37 (Simetría)

$$\binom{n}{r} = \binom{n}{n-r} = \frac{n!}{r!(n-r)!}, \quad n \geq 0, \quad 0 \leq r \leq n.$$

Teorema 38 (Identidad de Pascal)

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}, \quad n \geq 0, \quad 0 < r \leq n.$$

DM– p. 23/141

Números combinatorios: binomio de Newton

Teorema 39 (Teorema del binomio de Newton)

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}, \quad n \geq 0.$$

Corolario 40

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k, \quad n \geq 0.$$

Corolario 41 Para todo $n \geq 0$,

$$\sum_{k=0}^n \binom{n}{k} = 2^n,$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

DM– p. 24/141

Números combinatorios

Corolario 42 Dado un conjunto A finito, entonces

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Teorema 43 (Identidad de Vandermonde) Para todo $n, m \geq 0$ y $0 \leq k \leq m + n$ se cumple que

$$\binom{m+n}{k} = \sum_{q=0}^k \binom{m}{k-q} \binom{n}{q}.$$

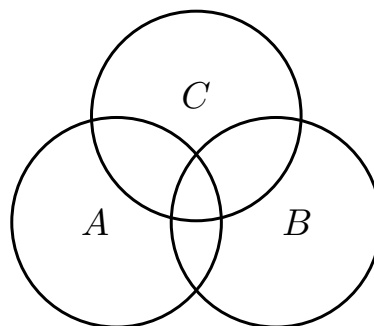
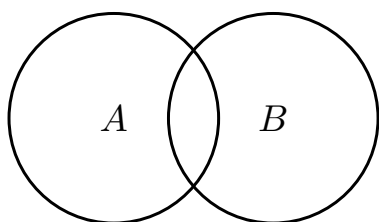
Observación: $\binom{n}{k} = 0$ siempre que $k < 0$ ó $k > n$.

DM– p. 25/141

Principio de inclusión-exclusión

Proposición 44 (Principio de inclusión-exclusión v1)

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



Proposición 45 (Principio de inclusión-exclusión v2)

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

DM– p. 26/141

Principio de inclusión-exclusión (2)

Proposición 46 (Principio de inclusión exclusión v3)

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots \\ &+ (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

Proposición 47 (Principio de inclusión exclusión v4) Sean $A_i \subset S$ con $1 \leq i \leq n$. Entonces

$$\begin{aligned} |\overline{A_1 \cup A_2 \cup \dots \cup A_n}| &= |\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}| \\ &= |S| - |A_1 \cup A_2 \cup \dots \cup A_n|. \end{aligned}$$

Notas:

- $\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n} = \{x : x \notin A_1, x \notin A_2, \dots, x \notin A_n\}$.
- $\overline{A} = S \setminus A \Rightarrow |\overline{A}| = |S| - |A|$.

DM– p. 27/141

Tema 3: Teoría de grafos I

1. Grafos no dirigidos:

- Notación y definiciones básicas.
- Representación de grafos.
- Isomorfismo.
- Caminos en grafos.
- Árboles.
- Grafos planos.

2. Algoritmos en teoría de grafos.

3. Problemas combinatorios en grafos.

DM– p. 28/141

Grafos no dirigidos

Definición 48

Un **pseudografo** $G = (V, E, \gamma)$ está compuesto por un conjunto no vacío de **vértices** V , un conjunto de **aristas** E y una función $\gamma: E \rightarrow \{\{a, b\}: a, b \in V\}$.

- La función γ codifica las conexiones entre los vértices.
- Si $e \in E$ satisface que $\gamma(e) = \{u, v\}$ con $u \neq v$, entonces u y v son **adyacentes o vecinos** y e es **incidente** a u y v .
- Si existen $e_1, e_2 \in E$ distintas tales que $\gamma(e_1) = \gamma(e_2)$, el pseudografo tiene **aristas múltiples**.
- Si existe $e \in E$ tal que $\gamma(e) = \{v, v\} = \{v\}$, entonces e es un **bucle** o (“loop”) incidente a v .
- Si no se dice lo contrario, se asumirá que $G = (V, E)$ es no dirigido.

Definición 49

Un **multigrafo** $G = (V, E, \gamma)$ es un pseudografo en el que se permite que haya **aristas múltiples**; pero no bucles. Un **grafo simple** $G = (V, E, \gamma)$ es un pseudografo en el que no se permite que haya aristas múltiples ni bucles.

DM– p. 29/141

Más definiciones

Definición 50

El **grado o valencia** de un vértice v de un grafo G es el número de aristas incidentes con él, exceptuando los bucles, cada uno de los cuales contribuye con dos unidades al grado del vértice. El grado del vértice $v \in V$ se denota por $d(v)$ (o por $\deg(v)$).

Nota: dado un vértice $v \in V$, su grado $d(v)$ es igual a

$$d(v) = |\{\{v, y\} \in E: y \neq v\}| + 2 \times \text{Número de bucles}.$$

Definición 51

Los vértices de grado 1 se denominan **terminales**. Los vértices de grado 0 se denominan **aislados**. Un grafo sin aristas se denomina **trivial**.

Definición 52

Un grafo es **regular** si todos sus vértices tienen el mismo grado.

DM– p. 30/141

El teorema del apretón de manos

Teorema 53 (Teorema del apretón de manos) *La suma de los grados de los vértices de un grafo $G = (V, E)$ es dos veces el número de aristas. Es decir:*

$$\sum_{i \in V} d(i) = 2|E|.$$

Corolario 54 *En todo grafo G la suma de los grados de sus vértices es par.*

Teorema 55 *El número de vértices de grado impar en un grafo G es par.*

Corolario 56 *En todo grafo G con número impar de vértices hay un número impar de vértices de grado par.*

DM– p. 31/141

Más definiciones

Definición 57

Un grafo $G = (V, E)$ es **bipartito** si V se puede dividir en dos conjuntos no vacíos y disjuntos V_1 y V_2 , de manera que cada arista $e \in E$ conecta un vértice de V_1 con otro de V_2 y viceversa.

Familias sencillas de grafos:

- Grafo completo de n vértices K_n .
- Camino P_n de n vértices.
- Ciclo C_n de n vértices.
- Rueda de $n + 1$ vértices W_n .
- Grafo bipartito completo de n y m vértices $K_{n,m}$.
- El grafo n -cubo Q_n es aquel que cada vértice representa una cadena de bits de longitud n . Dos vértices son adyacentes si y sólo si sus correspondientes cadenas de bits difieren exactamente en un bit.

DM– p. 32/141

Grafos complementarios y subgrafos

Definición 58

El **grafo complementario** $\overline{G} = (V, \overline{E})$ de un grafo **simple** $G = (V, E)$ es aquel formado por el mismo conjunto de vértices y tal que dos vértices son adyacentes en \overline{G} si y sólo si no son adyacentes en G .

Definición 59

Un grafo $H = (W, F)$ es un **subgrafo** de $G = (V, E)$ si $W \subseteq V$ y $F \subseteq E$.

Definición 60

Dado un grafo $G = (V, E)$, un **subgrafo generador** de G es todo aquel subgrafo $H = (V, F)$ con $F \subseteq E$.

DM– p. 33/141

Representación numérica de un grafo

Definición 61

Sea $G = (V, E)$ un grafo. Consideremos una ordenación $v_1, v_2, \dots, v_{|V|}$ de los vértices de G . La **matriz de adyacencia** de G asociada a dicha ordenación es la matriz $|V| \times |V|$ cuyas entradas A_{ij} cuentan el número de aristas que unen v_i con v_j .

Definición 62

Sea $G = (V, E)$ un grafo. Consideremos una ordenación $v_1, v_2, \dots, v_{|V|}$ de los vértices de G y una ordenación $e_1, e_2, \dots, e_{|E|}$ de las aristas de G . La **matriz de incidencia** de G asociada a dichas ordenaciones es la matriz $|V| \times |E|$ con entradas

$$I_{ij} = \begin{cases} 0 & \text{si } e_j \text{ no es incidente con } v_i \\ 1 & \text{si } e_j \text{ es incidente con } v_i \end{cases}$$

DM– p. 34/141

Isomorfismos

Importante: No confundir un grafo con su representación gráfica.

Definición 63

Dos grafos simples $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son **isomorfos** si y sólo si existe una función biyectiva $f: V_1 \rightarrow V_2$ con la siguiente propiedad: a y b son adyacentes en G_1 si y sólo si $f(a)$ y $f(b)$ son adyacentes en G_2 . Dicha función f se denomina **isomorfismo**.

Nota: dados dos grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$, entonces

1. Si $|V_1| \neq |V_2|$, entonces G_1 y G_2 **no** son isomorfos.
2. Si $|E_1| \neq |E_2|$, entonces G_1 y G_2 **no** son isomorfos.
3. Si S_i es la secuencia de grados de G_i y $S_1 \neq S_2$, entonces G_1 y G_2 **no** son isomorfos.
4. Otros métodos ...

Nota: G_1 y G_2 son isomorfos si existe una aplicación lineal invertible (permutación) $\pi: V_1 \rightarrow V_2$ tal que $A_2 = P^{-1} \cdot A_1 \cdot P$. Hay $|V_1|! = |V_2|!$ de estas aplicaciones.

DM– p. 35/141

Camino en un grafo

Definición 64

Un **camino** en un grafo $G = (V, E)$ es una secuencia alternada de vértices y aristas de la forma $v_0, \{v_0, v_1\}, v_1, \{v_1, v_2\}, v_2, \dots, v_{\ell-1}, \{v_{\ell-1}, v_\ell\}, v_\ell$. La **longitud** del camino es igual al número de aristas ℓ que lo componen. Existe una dirección implícita en todo camino: v_0 es el **vértice inicial** y v_ℓ , el **vértice final**.

Definición 65

Un camino en el que todas las aristas son distintas se denomina **camino simple**. Un **circuito** es un camino simple cerrado ($v_0 = v_\ell$).

Un camino simple en el que todos los vértices v_0, v_1, \dots, v_ℓ son distintos (excepto quizás los extremos v_0 y v_ℓ) se denomina **camino elemental**. Un camino elemental cerrado es un **ciclo**.

DM– p. 36/141

Número de caminos entre dos vértices

Teorema 66 Sea un grafo G con matriz de adyacencia A con respecto al orden $\{v_1, v_2, \dots, v_{|V|}\}$. El número de caminos orientados diferentes de longitud $n \geq 1$ que empiezan en v_i y acaban en v_j está dado por la entrada (i, j) de la matriz A^n .

Corolario 67 Sea G un grafo **simple** con matriz de adyacencia A , entonces

- $A_{ii}^2 = d(i)$ para todo $1 \leq i \leq |V|$.
- $\text{tr } A^2 = 2|E|$.
- $\text{tr } A^3 = 6 \times \text{Número de triángulos no orientados en } G$.

DM– p. 37/141

Grafos conexos

Definición 68

Un grafo es **conexo** si cada par de vértices $v, w \in V$ pueden ser conectados por un **camino elemental**. Un grafo no conexo está formado por la unión de varios subgrafos conexos y desconectados entre sí que se denominan **componentes conexas** del grafo.

Nota: Si dos vértices de un grafo se pueden conectar por un camino, entonces existe al menos un **camino elemental** que los une. Los caminos elementales que unen dos vértices son los caminos de menor longitud.

Definición 69

Un **punto de articulación o de corte** de un grafo G es un vértice tal que si lo eliminamos (junto con todas las aristas que le son incidentes) obtenemos un subgrafo con más componentes conexas que G .

Un **punto de articulación o de corte** de un grafo G es una arista tal que si la eliminamos (pero no los vértices con los que es incidente) obtenemos un grafo con más componentes conexas que G .

DM– p. 38/141

Tema 4: Teoría de grafos II

1. Grafos no dirigidos:

- Notación y definiciones básicas.
- Representación de grafos.
- Isomorfismo.
- Caminos en grafos.
- Árboles.
- Grafos planos.

2. Algoritmos en teoría de grafos.

3. Problemas combinatorios en grafos.

DM– p. 39/141

Árboles

Definición 70

Un **árbol** es un grafo simple y conexo que no contiene ciclos. Un **bosque** es un grafo simple que no contiene ciclos. Cada componente conexa de un bosque es un árbol.

Nota: los árboles pueden tener raíz, que no es más que un vértice que es especial. A no ser que se diga lo contrario, los árboles serán sin raíz.

Teorema 71

- (a) El grafo simple G es un árbol si y sólo si es conexo y al borrar cualquier arista se obtiene un grafo desconexo.
- (b) El grafo simple G es un árbol si y sólo si no contiene ciclos y al añadir cualquier arista se crea un ciclo.

Teorema 72 Un grafo $G = (V, E)$ es un árbol si y sólo si existe un **único** camino elemental entre cualquier par de vértices.

Teorema 73 Todo árbol con al menos dos vértices tiene al menos dos vértices de grado uno.

DM– p. 40/141

Propiedades de los árboles

Definición 74

Procedimiento para hacer crecer un árbol:

1. Comenzar con $G = (\{r\}, \emptyset)$, donde r es el vértice raíz.
2. Dado $G = (V, E)$, añadir un nuevo vértice u y una nueva arista $\{u, v\}$ donde $v \in V$.

Teorema 75 Todo grafo obtenido por este procedimiento es un árbol y todo árbol se puede construir de este modo.

Teorema 76 Todo árbol de n vértices tiene $n - 1$ aristas.

Teorema 77 Si G es un grafo de n vértices, entonces las siguientes afirmaciones son equivalentes:

1. G es un árbol.
2. G es conexo y tiene $n - 1$ aristas.
3. G tiene $n - 1$ aristas y no tiene ciclos.

DM– p. 41/141

Grafos planares

Definición 78

Un grafo es **planar** si puede ser dibujado en el plano sin que sus aristas se crucen. Una representación de un grafo planar en la que las aristas no se crucen se denomina **grafo plano**.

Definición 79

Insertar un nuevo vértice en una arista de un grafo se denomina **subdividir** dicha arista. La subdivisión de una o más aristas de un grafo G da lugar a una **subdivisión** de G .

Teorema 80 (Kuratowsky, 1930) Un grafo es planar si y sólo si no contiene como subgrafo a ninguna subdivisión de K_5 ni de $K_{3,3}$.

DM– p. 42/141

Grafos planares y grafos duales

Teorema 81 (Fórmula de Euler, 1752) Un grafo $G = (V, E)$ *plano y conexo* divide al plano en R regiones de manera que

$$|V| - |E| + R = 2.$$

Un grafo G *plano* (aunque no necesariamente conexo) divide al plano en R regiones tales que

$$|V| - |E| + R = 1 + \text{Número de componentes conexas de } G.$$

Definición 82

Dado un grafo $G = (V, E)$ plano, su **grafo dual** $G^* = (V^*, E^*)$ se define de la siguiente manera: a cada región f de G le corresponde un vértice dual $f^* \in V^*$ y por cada arista $e \in E$ existe una arista dual $e^* \in E^*$. Si la arista original e es la intersección de dos regiones f, h de G (siendo posible que $f = h$), entonces la correspondiente arista dual e^* es incidente a los vértices duales $f^*, h^* \in V^*$.

- Notar que $(G^*)^* = G$.

DM– p. 43/141

Algunos corolarios sobre planaridad

Definición 83

El **grado de una región** r de un grafo plano se define como el grado del vértice correspondiente $r \in V^*$ en el grafo dual. El grado de la región r lo denotaremos por d_r .

Teorema 84 En un grafo plano y conexo G se cumple que

$$2|E| = \sum_{r \in R} d_r,$$

donde R es el conjunto de regiones del plano definidas por G .

Corolario 85 Si G es un grafo simple, conexo y planar con $|V| \geq 3$, entonces $|E| \leq 3|V| - 6$.

Corolario 86 Si G es un grafo simple, conexo y planar con $|V| \geq 3$ y no tiene ciclos de longitud 3, entonces $|E| \leq 2|V| - 4$.

DM– p. 44/141

Tema 5: Teoría de grafos III

1. Grafos no dirigidos.
2. Grafos dirigidos.
3. Algoritmos en teoría de grafos:
 - Árbol generador de peso mínimo: algoritmos de Prim y Kruskal.
 - Camino de longitud mínima: algoritmo de Dijkstra.
 - Coloraciones de grafos.
 - Grafos eulerianos y hamiltonianos. Algoritmo de Fleury.
4. Problemas combinatorios en grafos.

DM– p. 45/141

Árbol generador de peso mínimo

Definición 87

Un **árbol generador o recubridor** de un grafo *conexo* G es un árbol que contiene todos los vértices de G y es subgrafo de G .

Definición 88

Un **grafo ponderado** $G = (V, E, \omega)$ es un grafo en el que a cada arista $e \in E$ se le asocia un peso $\omega(e) \in \mathbb{R}$.

Definición 89

Un **árbol generador de peso mínimo** de un grafo conexo ponderado es un árbol generador tal que la suma de los pesos de sus aristas es la más pequeña posible.

Problema 1

Encontrar un árbol generador de peso mínimo del grafo ponderado $G = (V, E, \omega)$.

Nota: El número de árboles con n vértices crece muy rápidamente con n .

Definición 90

Un **algoritmo voraz** es aquel que en cada paso toma la elección óptima.

DM– p. 46/141

Algoritmo de Prim, 1957

Algoritmo 91 (Algoritmo de Prim)

procedure *Prim*(G : grafo ponderado conexo con n vértices)

$T_1 = (V_1, E_1)$ donde $E_1 = \{e_1\}$, $e_1 = \{x_0, x_1\}$ es una arista con peso mínimo ω_{\min}
y $V_1 = \{x_0, x_1\}$.

for $i = 1$ **to** $n - 2$

begin

$e_{i+1} = \{x_i, x_{i+1}\}$ arista de peso mínimo incidente con un vértice x_j de
 $T_i = (V_i, E_i)$ y que no forme un ciclo si se le añade a T_i

$T_{i+1} = (V_i \cup \{x_{i+1}\}, E_i \cup \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$

end

Notas:

- La arista e_i ($i = 1, \dots, n - 1$) puede no ser única.
- El árbol generador de peso mínimo puede no ser único.
- En cada paso, T_i es un árbol ($1 \leq i \leq n - 1$).

Teorema 92 Dado un grafo conexo ponderado $G = (V, E, \omega)$, el algoritmo de Prim produce un árbol generador mínimo de G . Su complejidad computacional es $O(|E| + |V| \log |V|)$.

DM– p. 47/141

Algoritmo de Kruskal, 1957

Algoritmo 93 (Algoritmo de Kruskal)

procedure *Kruskal*(G : grafo ponderado conexo con n vértices)

$T_0 = (V, E_0)$ con $E_0 = \emptyset$

for $i = 1$ **to** $n - 1$

begin

$e_i =$ arista de peso mínimo que no forme un ciclo si se le añade a $T_{i-1} = (V, E_{i-1})$

$T_i = (V, E_{i-1} \cup \{e_i\}) = (V, E_i)$

end

Notas:

- La arista e_i ($i = 1, \dots, n - 1$) puede no ser única.
- En cada paso, T_i es un bosque ($1 \leq i \leq n - 1$).

Teorema 94 Dado un grafo conexo ponderado $G = (V, E, \omega)$, el algoritmo de Kruskal produce un árbol generador mínimo de G . Su complejidad computacional es $O(|E| \log |V|)$.

DM– p. 48/141

Problema del camino mínimo: algoritmo de Dijkstra, 1959

Problema 2

Encontrar el camino de longitud mínima que une un vértice inicial s y un vértice final t en un grafo $G = (V, E, \omega)$ **conexo, simple y ponderado con todos los pesos positivos** ($\omega_e > 0$ para toda arista $e \in E$).

Teorema 95 El algoritmo de Dijkstra encuentra la longitud del camino más corto entre dos vértices de un grafo $G = (V, E, \omega)$ conexo, simple y ponderado con todos los pesos positivos. Su complejidad computacional es $O(|V|^2)$.

Idea:

En cada iteración a cada vértice j se le asignan dos etiquetas que pueden ser o bien temporales (δ_j, P_j) o bien permanentes $\boxed{(\delta_j, P_j)}$.

- La etiqueta δ_j es una estimación de la longitud del camino mínimo desde el vértice inicial s hasta el vértice j .
- La etiqueta P_j es una estimación del predecesor del vértice j en dicho camino.

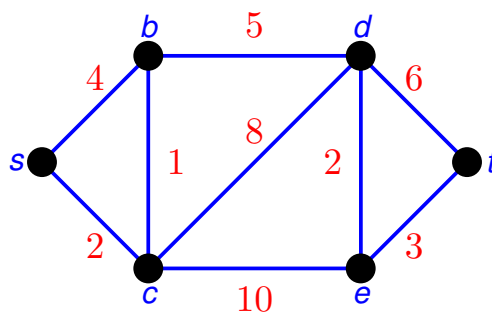
Denotaremos $\omega_{ij} > 0$ al peso de la arista $\{i, j\} \in E$.

DM– p. 49/141

El algoritmo de Dijkstra

Problema 3

Calcular el camino de menor longitud entre s y t en el siguiente grafo:



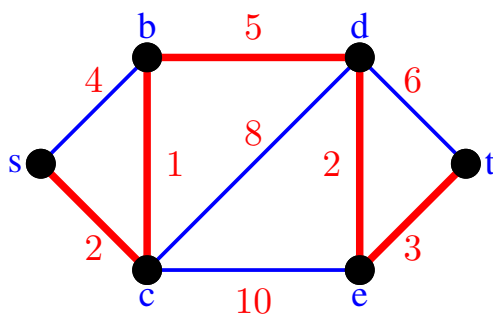
DM– p. 50/141

El algoritmo de Dijkstra (2)

- (1) **Paso inicial:** Marcamos el origen s con la etiqueta permanente $(0, s)$.
El resto de los vértices $j \in V$ ($j \neq s$) se marcan con etiquetas temporales:
 - Si $\{j, s\} \in E$, se le asigna la etiqueta $(\omega_{s,j}, s)$.
 - Si $\{j, s\} \notin E$, se le asigna la etiqueta $(\infty, -)$.
- (2) Sea $v \in V$ el último vértice que se ha vuelto permanente. Examinamos cada vértice temporal j comparando δ_j con el valor de $\delta_v + \omega_{v,j}$:
 - Si $\delta_v + \omega_{v,j} < \delta_j$, cambiamos (δ_j, P_j) por $(\delta_v + \omega_{v,j}, v)$.
 - Si $\delta_v + \omega_{v,j} \geq \delta_j$, no hacemos nada.
- (3) De entre todos los vértices temporales j elegimos el que tenga el estimador δ_j más pequeño ($= \delta_{\min}$).
 - Si $\delta_{\min} = \infty$, el algoritmo termina: no hay camino entre s y t .
 - Si $\delta_{\min} < \infty$, marcamos dicho vértice con la etiqueta permanente (δ_{\min}, P_j) .
- (4) Si t es el vértice cuya etiqueta (δ_t, P_t) se ha hecho permanente, el algoritmo termina. La longitud del camino más corto entre s y t es δ_t y dicho camino se obtiene siguiendo las etiquetas permanentes en sentido contrario $t \rightarrow P_t \rightarrow \dots \rightarrow s$. Si no es t , volver al paso (2).

DM– p. 51/141

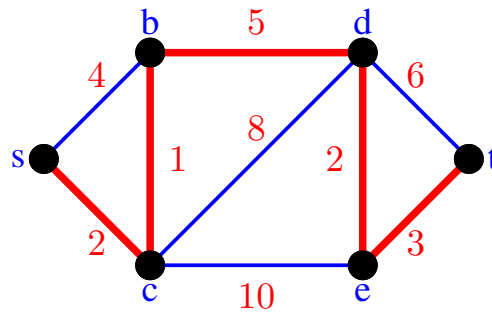
El algoritmo de Dijkstra: Ejemplo



| Vértice | Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 |
|---------|----------|-----------|-----------|-----------|-----------|-----------|
| s | $(0, s)$ | * | * | * | * | * |
| b | $(4, s)$ | $(3, c)$ | $(3, c)$ | * | * | * |
| c | $(2, s)$ | $(2, s)$ | * | * | * | * |
| d | ∞ | $(10, c)$ | $(8, b)$ | $(8, b)$ | * | * |
| e | ∞ | $(12, c)$ | $(12, c)$ | $(10, d)$ | $(10, d)$ | * |
| t | ∞ | ∞ | ∞ | $(14, d)$ | $(13, e)$ | $(13, e)$ |

DM– p. 52/141

El algoritmo de Dijkstra (2)



Observaciones:

- Si en un paso dado hay varias opciones, escogemos una cualquiera de ellas.
- El camino de longitud mínima entre dos vértices puede no ser único; pero el peso mínimo no depende de dicha elección.
- El resultado final del algoritmo de Dijkstra (una vez que todos los vértices tienen etiquetas permanentes) es un árbol generador T con raíz en s y tal que la distancia entre s y otro vértice j del grafo es la suma de los pesos del **único** camino elemental que une s y j en T .

DM– p. 53/141

Grafos orientados o dirigidos

Definición 96

Un **grafo dirigido** $G = (V, E)$ está compuesto por un conjunto no vacío de **vértices** V y un conjunto de **aristas** E , tal que cada arista $e \in E$ es un par ordenado de elementos $e = (x, y)$ con $x, y \in V$.

Definición 97

Si v es un vértice de un grafo dirigido G , entonces el **grado interno** $d_i(v)$ de v es el número de aristas que llegan a v y su **grado externo** $d_e(v)$ es el número de aristas que salen de v .

Proposición 98 En un grafo dirigido $G = (V, E)$ se cumple que:

$$\sum_{v \in V} d_i(v) = \sum_{v \in V} d_e(v) = |E|.$$

Definición 99

Sea $G = (V, E)$ un grafo dirigido. Consideremos una ordenación $v_1, v_2, \dots, v_{|V|}$ de los vértices de G . La **matriz de adyacencia** de G asociada a dicha ordenación es la matriz $|V| \times |V|$ cuyas entradas A_{ij} cuentan el número de aristas (v_i, v_j) que comienzan en v_i y acaban en v_j .

DM– p. 54/141

Grafos orientados o dirigidos (2)

Definición 100

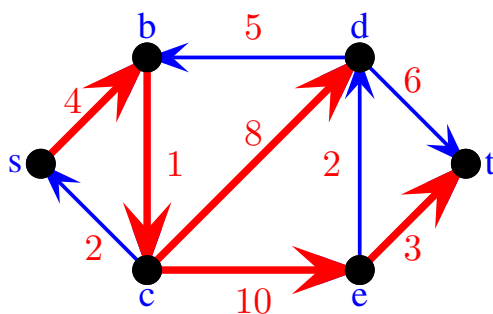
Un **camino** de longitud ℓ en un grafo dirigido $G = (V, E)$ es una sucesión de aristas de la forma $(v_0, v_1), (v_1, v_2), \dots, (v_{\ell-1}, v_\ell)$.

Las definiciones de camino elemental, camino simple, circuito y ciclo para grafos dirigidos son análogas a las de un grafo no dirigido (Tema 3).

También podemos definir grafos dirigidos ponderados $G = (V, E, \omega)$ de manera análoga.

DM– p. 55/141

El algoritmo de Dijkstra para grafos orientados



| Vértice | Paso 1 | Paso 2 | Paso 3 | Paso 4 | Paso 5 | Paso 6 |
|---------|----------|----------|-----------|-----------|-----------|-----------|
| s | $(0, s)$ | * | * | * | * | * |
| b | $(4, s)$ | $(4, s)$ | * | * | * | * |
| c | ∞ | $(5, b)$ | $(5, b)$ | * | * | * |
| d | ∞ | ∞ | $(13, c)$ | $(13, c)$ | * | * |
| e | ∞ | ∞ | $(15, c)$ | $(15, c)$ | $(15, c)$ | * |
| t | ∞ | ∞ | ∞ | $(19, d)$ | $(18, e)$ | $(18, e)$ |

DM– p. 56/141

Tema 6: Teoría de grafos IV

1. Grafos no dirigidos.
2. Algoritmos en teoría de grafos:
 - Árbol generador de peso mínimo: algoritmos de Prim y Kruskal.
 - Camino de longitud mínima: algoritmo de Dijkstra.
 - Coloraciones de grafos.
 - Grafos eulerianos y hamiltonianos. Algoritmo de Fleury.
3. Problemas combinatorios en grafos.

DM– p. 57/141

Coloraciones propias de un grafo

Definición 101

Una **coloración propia** (con q colores) de un grafo $G = (V, E)$ es una función $c : V \rightarrow \{1, 2, \dots, q\}$ tal que $c(u) \neq c(w)$ siempre que u y w sean adyacentes.

- Dado un grafo $G = (V, E)$ el número total de coloraciones (propias y no propias) con q colores es $q^{|V|}$.
- En todo lo que sigue consideraremos sólo **coloraciones propias**.
- **Dos preguntas difíciles:**
 1. ¿Cuántas coloraciones con q colores $P_G(q)$ se pueden conseguir sobre G ?
 2. ¿Cuántos colores q necesito como mínimo para poder colorear G ?

Definición 102

El **número cromático** $\chi(G)$ de un grafo G es el menor entero q tal que existe una coloración de G con q colores; es decir, $P_G(q) > 0$ para todo $q \geq \chi(G) \in \mathbb{N}$.

Proposición 103 Decidir si los vértices de un grafo arbitrario G se pueden colorear propiamente con $k \geq 3$ colores es un problema NP-completo.

DM– p. 58/141

Algoritmo voraz para colorear un grafo

Algoritmo 104 (Algoritmo voraz)

procedure (G : grafo simple conexo con n vértices)

Ordenamos los vértices de $V: (v_1, v_2, \dots, v_n)$

$c(v_1) = 1$

for $i = 2$ **to** n

begin

$S_i = \{q: c(v_k) = q, \text{ para todo } v_k \text{ vecino de } v_i \text{ con } k < i\}$

$c(v_i) = \min(\overline{S_i} \cap \mathbb{N}) = \text{el color más pequeño que no está en } S_i$

end

Notas:

- No calculamos $\chi(G)$, sino una cota superior (muy) dependiente de la ordenación usada.
- Para calcular $\chi(G)$ habría que considerar las $n!$ ordenaciones posibles de los n vértices de G (tiempo exponencial).

DM– p. 59/141

Algunos teoremas

Teorema 105 Si G es un grafo con grado máximo k , entonces $\chi(G) \leq k + 1$.

Teorema 106 (Brooks, 1941) Si G es un grafo no completo, conexo y con grado máximo $k \geq 3$, entonces $\chi(G) \leq k$.

Proposición 107 Un grafo G es bipartito si y sólo si $\chi(G) = 2$.

Teorema 108 Un grafo es bipartito si y sólo si no contiene ciclos de longitud impar.

Corolario 109 Todos los árboles son bipartitos

Teorema 110 (El teorema de los cuatro colores, Appel y Haken, 1976) $P_G(4) > 0$ para todo grafo planar G .

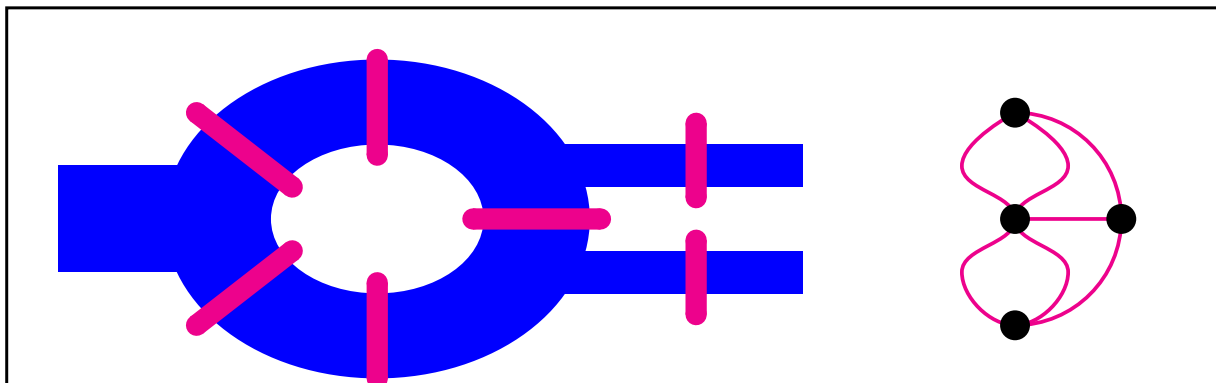
- La prueba original fue *asistida* por ordenador (¡más de 1200 horas de CPU!).
- No existe aún una prueba analítica.
- No existe un teorema de los tres colores: existen grafos planares con número cromático $\chi(G) = 4$: e.g. K_4 .

DM– p. 60/141

Grafos eulerianos

Problema 4 (Euler)

En la ciudad de Königsberg (Kaliningrado) hay un río y siete puentes. ¿Es posible dar una vuelta y cruzar cada puente una sola vez?



Problema 5

Dado un grafo $G = (V, E)$, ¿existe un circuito que contenga cada arista $e \in E$? [Al ser circuito debe contener cada arista una sola vez].

DM– p. 61/141

Grafos eulerianos

Definición 111

Un **circuito euleriano** es un circuito que contiene a todas las aristas del grafo. Un grafo que admite un circuito euleriano se denomina **grafo euleriano**.

Un **camino euleriano** es un camino simple y abierto que contiene todas las aristas del grafo. Un grafo no euleriano que admite un camino euleriano se denomina **grafo semi-euleriano**.

Teorema 112 Un grafo conexo es euleriano si y sólo si todos sus vértices tienen grado par.

Un grafo conexo es semi-euleriano si y sólo si contiene exactamente dos vértices de grado impar.

Un grafo dirigido conexo es euleriano si y solo si para cualquier vértice el grado interno coincide con el grado externo.

Luego, el [problema de los puentes de Königsberg](#) **no** tiene solución: el grafo correspondiente no es ni euleriano ni semi-euleriano.

DM– p. 62/141

Algoritmo de Fleury

Sea $G = (V, E)$ un grafo conexo con todos los vértices de grado par:

- (1) **Paso inicial:** Escogemos un vértice v_0 como origen del circuito $C_0 = (v_0)$ y definimos $G_0 = (V_0, E_0) = G$. El algoritmo hace crecer secuencialmente el circuito C_0 mientras que va eliminando elementos de G_0 .
- (2) **Extensión del circuito:** Sea el circuito $C_i = (v_0, e_1, v_1, \dots, e_i, v_i)$ al que le corresponde el grafo $G_i = (V_i, E_i) \subseteq G_0$.
 - Si existe una única arista $e_{i+1} = \{v_i, w\} \in E_i = E \setminus \{e_1, e_2, \dots, e_i\}$:
 - $C_{i+1} = (v_0, e_1, v_1, \dots, e_i, v_i, e_{i+1}, w)$.
 - $G_{i+1} = (V_i \setminus \{v_i\}, E_i \setminus \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$.
 - Si hay varias aristas incidentes en E_i con v_i : elegimos cualquiera de ellas con la condición que **no sea puente**. Si escogemos $e_{i+1} = \{v_i, w\} \in E_i$:
 - $C_{i+1} = (v_0, e_1, v_1, \dots, e_i, v_i, e_{i+1}, w)$.
 - $G_{i+1} = (V_i, E_i \setminus \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$.
- (3) Repetimos el Paso (2) $|E|$ veces hasta que $G_{|E|} = (\emptyset, \emptyset)$; $C_{|E|}$ es el circuito euleriano buscado.

DM– p. 63/141

Grafos hamiltonianos

Problema 6

¿Es posible encontrar un ciclo en G tal que pase por todos los vértices (una sola vez)?

Definición 113

Un **ciclo hamiltoniano** es un ciclo que contiene a todos los vértice del grafo. Un grafo que admite un ciclo hamiltoniano se denomina **grafo hamiltoniano**.

Un **camino hamiltoniano** es un camino elemental y abierto que contiene todos los vértices del grafo. Un grafo no hamiltoniano que admite un camino hamiltoniano se denomina **grafo semi-hamiltoniano**.

El problema de decidir si un grafo es hamiltoniano o no es NP-completo.

Teorema 114 (Dirac, 1950) Si G es un grafo simple con $n \geq 3$ vértices y cada vértice tiene un grado $\geq n/2$, entonces G es hamiltoniano.

Nota: No todos los grafos hamiltonianos satisfacen la condición anterior: e.g. C_n con $n \geq 5$.

DM– p. 64/141

Tema 7: Combinatoria elemental II

1. **Regla de la suma:** si $A \cap B = \emptyset$, $|A \cup B| = |A| + |B|$.
2. **Regla del producto:** $|A \times B| = |A| \cdot |B|$.
3. **Principio de inclusión–exclusión:** $|A \cup B| = |A| + |B| - |A \cap B|$.
4. **Principio del palomar.**
5. **Otros patrones de recuento:**
 - Repartos.
 - Particiones.

DM– p. 65/141

Patrones de conteo: repartos

Proposición 115 (Repartos) Si hay que repartir r objetos iguales en n grupos (distintos) y todos los grupos deben de contar con algún objeto, entonces existen

$$\binom{r-1}{n-1}$$

repartos distintos.

Proposición 116 Si hay que repartir r objetos iguales en n grupos (distintos) pudiendo quedar grupos vacíos, entonces existen

$$\binom{n+r-1}{r}$$

repartos distintos.

DM– p. 66/141

Patrones de conteo: particiones de un conjunto

Definición 117

Sea un conjunto finito S que contiene n elementos. Una **partición** de S de tipo (n_1, n_2, \dots, n_k) es el conjunto $\{S_i\}_{i=1}^k$ donde los conjuntos S_i satisfacen: (1) $|S_i| = n_i$ para todo $1 \leq i \leq k$, (2) son disjuntos entre sí: $S_i \cap S_j = \emptyset$ para todo $i \neq j$ y (3) su unión es S (luego $\sum_{i=1}^k n_i = n$).

Proposición 118 Sea un conjunto S de $m \cdot n$ elementos. Entonces existen

$$\frac{(m \cdot n)!}{(m!)^n n!}$$

particiones distintas de S en n conjuntos S_i de tipo (m, m, \dots, m) .

Proposición 119 El número de particiones de un conjunto de m elementos del tipo (m_1, m_2, \dots, m_n) es

$$\binom{m}{m_1, m_2, \dots, m_n} \prod_{k \geq 1} \frac{1}{r_k!},$$

donde r_k es el número de partes con k elementos.

DM– p. 67/141

Tema 8: Combinatoria. Métodos avanzados.

1. Relaciones de recurrencia:

- Definiciones.
- Solución de relaciones de recurrencia lineales homogéneas.
- Solución de relaciones de recurrencia lineales no homogéneas.

2. Funciones generatrices.

DM– p. 68/141

Relaciones de recurrencia

Definición 120

Una **relación de recurrencia** para la secuencia $(a_n)_{n \in \mathbb{N}}$ es una ecuación que expresa a_n en función de uno o más de los términos anteriores; es decir, una ecuación del tipo

$$F(n; a_n, a_{n-1}, a_{n-2}, \dots, a_{n-k}) = 0,$$

con k fijo y válida para todo $n \geq k + 1$. Las **condiciones iniciales** son los términos (a_1, \dots, a_k) .

Definición 121

El **orden de una relación de recurrencia** es la diferencia entre los subíndices máximo y mínimo de los términos a_k que aparecen en la ecuación. Una relación de recurrencia de orden k es **lineal** si lo es en $a_n, a_{n-1}, \dots, a_{n-k}$. En cualquier otro caso, se dice que es **no lineal**. Una relación de recurrencia es **homogénea** si la secuencia $a_n = a_{n-1} = \dots = a_{n-k} = 0$ es una solución de la relación. En caso contrario, la relación es **no homogénea**.

DM– p. 69/141

Solución de una relación de recurrencia lineal homogénea

Teorema 122 (Solución ecuaciones de recurrencia de orden 1 homogéneas)

Supongamos que la secuencia $(a_n)_{n \in \mathbb{N}}$ verifica la relación de recurrencia

$$a_n = A a_{n-1}, \quad n \geq 2,$$

con A real y a_1 dado. Entonces la solución de la ecuación de recurrencia es

$$a_n = a_1 A^{n-1}, \quad n \geq 1.$$

Observación: en este curso sólo vamos a considerar ecuaciones de recurrencia lineales con coeficientes constantes.

DM– p. 70/141

Solución de una relación de recurrencia lineal homogénea

Teorema 123 (Solución ecuaciones de recurrencia tipo Fibonacci homogéneas)

Supongamos que la secuencia $(a_n)_{n \in \mathbb{N}}$ verifica la relación de recurrencia

$$a_n = A a_{n-1} + B a_{n-2}, \quad n \geq 3,$$

con A, B reales y (a_1, a_2) dados. Si la **ecuación característica** asociada a dicha recurrencia es

$$x^2 = A x + B$$

y tiene raíces α y β , entonces la solución de la ecuación de recurrencia es para todo $n \geq 1$:

$$a_n = \begin{cases} K_1 \alpha^n + K_2 \beta^n & \text{si } \alpha \neq \beta, \\ (K_1 + n K_2) \alpha^n & \text{si } \alpha = \beta, \end{cases}$$

donde las constantes K_1 y K_2 se determinan a partir de las condiciones iniciales (a_1, a_2) .

DM– p. 71/141

Solución de una relación de recurrencia lineal homogénea

- Supongamos que la secuencia $(a_n)_{n \in \mathbb{N}}$ verifica la relación de recurrencia lineal

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}, \quad n \geq k+1,$$

con c_1, c_2, \dots, c_k reales. Se suponen conocidas las k condiciones iniciales (a_1, a_2, \dots, a_k) .

- Si buscamos una solución de la forma

$$a_n = K_i x^n,$$

entonces la amplitud se cancela y la variable x debe satisfacer la **ecuación característica**:

$$x^k = c_1 x^{k-1} + c_2 x^{k-2} + \dots + c_k.$$

- Si a_n y b_n son soluciones de la recurrencia, entonces cualquier combinación lineal $\alpha a_n + \beta b_n$ será solución de la misma.

DM– p. 72/141

Solución de una relación de recurrencia lineal homogénea (2)

- A cada raíz **distinta** x_i de la ecuación característica le corresponde una solución $a_n^{(i)}$ cuya forma depende de la multiplicidad de x_i :
 - Si la raíz x_i es simple, entonces $a_n^{(i)} = K_i x_i^n$.
 - Si la raíz x_i es doble, entonces $a_n^{(i)} = (K_i + K'_i n) x_i^n$.
 - Si la raíz x_i es triple, entonces $a_n^{(i)} = (K_i + K'_i n + K''_i n^2) x_i^n$, etc.
- Si la ecuación característica tiene r raíces distintas x_i con multiplicidades k_i (tales que $\sum_{i=1}^r k_i = k$), entonces la solución general es del tipo:

$$a_n = \sum_{i=1}^r \left[\sum_{j=1}^{k_i} K_i^{(j)} n^{j-1} \right] x_i^n, \quad n \geq 1,$$

donde las k constantes $K_i^{(j)}$ se determinan a partir de las k condiciones iniciales.

DM– p. 73/141

Solución de una relación de recurrencia lineal no homogénea

Teorema 124 (Solución ecuaciones de recurrencia no homogéneas) Supongamos que la secuencia $(a_n)_{n \in \mathbb{N}}$ verifica la relación de recurrencia lineal

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + t_n, \quad n \geq k+1,$$

con c_1, c_2, \dots, c_k reales y (a_1, \dots, a_k) dados. La función $t_n: \mathbb{N} \rightarrow \mathbb{R}$ es una cierta función **conocida** de n . Entonces la solución general de la ecuación no homogénea es la suma de la solución general de la ecuación homogénea

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}, \quad n \geq k+1$$

y una solución particular cualquiera de la ecuación completa.

DM– p. 74/141

Solución de una relación de recurrencia lineal no homogénea

Teorema 125 (Solución ecuaciones lineales no homogéneas) Supongamos que la secuencia $(a_n)_{n \in \mathbb{N}}$ verifica la relación de recurrencia lineal

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + t_n, \quad n \geq k+1,$$

con c_1, c_2, \dots, c_k reales y (a_1, a_2, \dots, a_k) dados. La función $t_n: \mathbb{N} \rightarrow \mathbb{R}$ toma la forma:

$$t_n = s^n [b_0 + b_1 n + \dots + b_t n^t],$$

con b_0, b_1, \dots, b_t, s reales. Si s **no es raíz** de la ecuación característica de la relación de recurrencia homogénea asociada, entonces existe una solución particular de la forma

$$a_{n,p} = s^n [p_0 + p_1 n + \dots + p_t n^t].$$

Si s **es una raíz con multiplicidad m** de esta ecuación característica, entonces existe una solución particular de la forma

$$a_{n,p} = n^m \cdot s^n [p_0 + p_1 n + \dots + p_t n^t].$$

- La solución particular $a_{n,p}$ **no** tiene parámetros libres: hay una única elección de los coeficientes $\{p_k\}_{k=1}^t$ tal que $a_{n,p}$ sea realmente una solución de la recurrencia.

DM– p. 75/141

Tema 9: Combinatoria. Métodos avanzados.

1. Relaciones de recurrencia.
2. Funciones generatrices:
 - Definición.
 - Codificación eficiente de problemas combinatorios.
 - Solución de relaciones de recurrencia usando funciones generatrices.

DM– p. 76/141

Función generatriz

Definición 126

La **función generatriz** asociada a la sucesión $(a_0, a_1, a_2, \dots, a_n, \dots)$ se define como la serie formal de potencias siguiente:

$$F(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots = \sum_{n=0}^{\infty} a_n x^n.$$

- $(1+x)^k = \sum_{n=0}^k \binom{k}{n} x^n$ es la f.g. de $\left(\binom{k}{0}, \binom{k}{1}, \dots, \binom{k}{k}, 0, 0, \dots\right)$.
- $1 + x + x^2 + \dots + x^{k-1} = \sum_{n=0}^{k-1} x^n = \frac{1-x^k}{1-x}$ es la f.g. de $(\underbrace{1, 1, \dots, 1}_k, 0, 0, \dots)$.
- $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots = \sum_{n=0}^{\infty} x^n$ es la f.g. de $(1, 1, 1, \dots)$.
- $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ es la f.g. de $(1, 1, \frac{1}{2!}, \frac{1}{3!}, \dots)$.

DM– p. 77/141

Maniobras básicas con funciones generatrices

- $(1, 2, 3, \dots)$ tiene como f.g. a

$$\sum_{n=0}^{\infty} (n+1)x^n = \frac{d}{dx} \sum_{n=0}^{\infty} x^{n+1} = \frac{d}{dx} \frac{x}{1-x} = \frac{1}{(1-x)^2}.$$
- Si $F(x) = \sum_{n=0}^{\infty} a_n x^n$ y $G(x) = \sum_{n=0}^{\infty} b_n x^n$, entonces

$$(F+G)(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$
- Si F es la f.g. de la secuencia (a_n) , entonces la f.g. de la secuencia $(\underbrace{0, 0, \dots, 0}_k, a_0, a_1, \dots)$ es $G(x) = x^k F(x)$.

DM– p. 78/141

Particiones de un natural

Problema 7

Calcular cuántas particiones distintas hay del número $N \in \mathbb{N}$. Por ejemplo, si $N = 4$, hay 5 particiones $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$.

- El principio de la suma nos permite calcular la función generatriz de colocar en la partición el natural k :
 - La función generatriz de colocar 1's es $f_1 = 1 + x + x^2 + x^3 + \dots = \frac{1}{1-x}$.
 - La función generatriz de colocar 2's es $f_2 = 1 + x^2 + x^4 + x^6 + \dots = \frac{1}{1-x^2}$.
 - \vdots
 - La función generatriz de colocar el natural $p \geq 1$ es $f_p = 1 + x^p + x^{2p} + x^{3p} + \dots = \frac{1}{1-x^p}$.
- Como escribir una partición es un proceso secuencial, la función generatriz que codifica el Problema 7 viene dada por el principio del producto:

$$f(x) = \prod_{k=1}^{\infty} f_k(x) = \prod_{k=1}^{\infty} \frac{1}{1-x^k} = 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + \dots$$

DM– p. 79/141

Procedimiento práctico

- Codificación de un problema:**
 - Usando el principio de la suma, el principio del producto y otras operaciones, calcular la función generatriz F .
 - Haciendo el desarrollo de Taylor de F alrededor del origen obtenemos los coeficientes a_n .
- Resolver una ecuación de recurrencia:**
 - Reescribir la relación de recurrencia para a_n en términos de una ecuación que sólo involucre a la función generatriz F .
 - Resolver la ecuación anterior y obtener la forma explícita de F .
 - Haciendo el desarrollo de Taylor de F alrededor del origen obtenemos los coeficientes a_n .

DM– p. 80/141

Ejemplo: la ecuación de Fibonacci

Queremos resolver la ecuación

$$a_n = a_{n-1} + a_{n-2}, \quad n \geq 2, \quad a_0 = 0, \quad a_1 = 1,$$

mediante la función generatriz

$$F(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \sum_{n=2}^{\infty} a_n x^n.$$

Algoritmo:

1. Multiplicar la ecuación de recurrencia por x^n y sumar sobre todos los valores de n para los que esta ecuación es válida (en nuestro caso $n \geq 2$):

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n.$$

DM- p. 81/141

Ejemplo: la ecuación de Fibonacci

2. Manipular las sumas para que queden en función de F y de las condiciones iniciales:

- $\sum_{n=2}^{\infty} a_n x^n = F - a_0 - a_1 x = F - x.$
- $\sum_{n=2}^{\infty} a_{n-1} x^n = x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} = x \sum_{m=1}^{\infty} a_m x^m = x(F - a_0) = xF.$
- $\sum_{n=2}^{\infty} a_{n-2} x^n = x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} = x^2 \sum_{m=0}^{\infty} a_m x^m = x^2 F.$

La ecuación de recurrencia se transforma en la ecuación

$$F - x = xF + x^2 F.$$

3. Resolvemos esta ecuación para F :

$$F(x) = \frac{x}{1 - x - x^2}.$$

DM- p. 82/141

Ejemplo: la ecuación de Fibonacci

4. Desarrollamos F en serie de Taylor y leemos el coeficiente de x^n :

$$F(x) = \frac{x}{1-x-x^2} = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \dots$$

Podemos obtener todos los coeficientes mediante un poco de álgebra:

$$\begin{aligned} F(x) &= \frac{\alpha}{x + (1 + \sqrt{5})/2} + \frac{\beta}{x + (1 - \sqrt{5})/2} \\ &= \frac{1}{\sqrt{5}} \left[\frac{1}{1 - x(1 + \sqrt{5})/2} - \frac{1}{1 - x(1 - \sqrt{5})/2} \right] \\ &= \sum_{n=0}^{\infty} \frac{x^n}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]. \\ F_n &= \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]. \end{aligned}$$

DM– p. 83/141

Teorema del binomio generalizado

Teorema 127 Sea $k \in \mathbb{N}$, entonces tenemos formalmente que

$$\frac{1}{(1+x)^k} = \sum_{n=0}^{\infty} \binom{-k}{n} x^n,$$

donde para todo $n \geq 0$ el coeficiente binomial se define como

$$\binom{-k}{n} = \frac{-k(-k-1)(-k-2)\dots(-k-n+1)}{n!} = (-1)^n \binom{n+k-1}{n}.$$

DM– p. 84/141

Tema 10: Teoría de grafos V

1. Grafos no dirigidos.
2. Algoritmos en teoría de grafos.
3. Problemas combinatorios en grafos:
 - Emparejamiento en grafos.
 - Coloraciones propias en grafos.

DM– p. 85/141

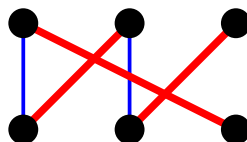
Emparejamientos en grafos

Definición 128

Un **emparejamiento completo o perfecto** de un grafo simple con $2n$ vértices es un subgrafo generador formado por n aristas disjuntas.

Notas:

- Todos los vértices de G pertenecen al subgrafo.
- Cada vértice de G sólo tiene una arista incidente perteneciente al subgrafo.
- En grafos **bipartitos** es menos difícil:



Teorema 129 Si G es un grafo **bipartito** y regular con grado $d \geq 1$, entonces G contiene un emparejamiento perfecto.

DM– p. 86/141

Coloraciones propias: polinomio cromático

Definición 130

Sea $G = (V, E)$ un grafo simple y sea $q \geq 2$ un número natural. El **polinomio cromático** P_G es un polinomio tal que $P_G(q)$ nos dice el número de coloraciones propias con $q \in \mathbb{N}$ colores que admite el grafo G .

Teorema 131 Si $G = (V, E)$ es un grafo simple, $P_G(q)$ es un polinomio en q .

La demostración se basa en:

- Si $G = (\{v\}, \emptyset)$, $P_G(q) = q$.
- Se cumple el teorema de contracción-borrado:

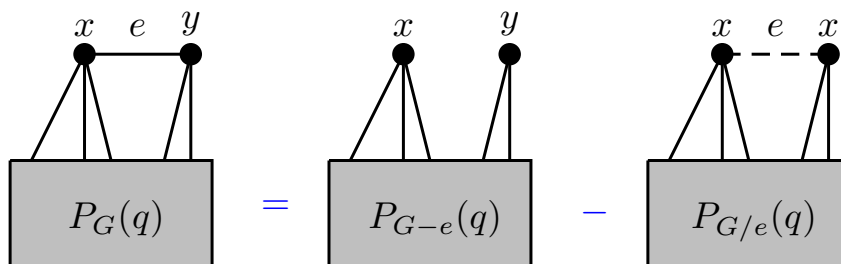
Teorema 132 (Teorema de contracción-borrado) Si $G = (V, E)$ es un grafo simple y $e = \{x, y\} \in E$ con $x, y \in V$, entonces

$$P_G(q) = P_{G-e}(q) - P_{G/e}(q),$$

donde $G - e$ es el grafo que se obtiene al borrar la arista e y G/e es el grafo que se obtiene al contraer la arista e (identificando los vértices x e y y eliminando posibles multiaristas).

DM- p. 87/141

Demostración del Teorema de contracción-borrado



Teorema 133 Si G es un grafo no conexo con $k \geq 1$ componentes conexas G_j , entonces

$$P_G(q) = \prod_{j=1}^k P_{G_j}(q).$$

Teorema 134 Si G es un grafo que se puede dividir en dos partes G_1 y G_2 cuya intersección es K_n para algún $n \geq 1$, entonces

$$P_G(q) = \frac{P_{G_1}(q) \times P_{G_2}(q)}{P_{K_n}(q)}.$$

1. Si $G = K_n$, entonces $P_{K_n}(q) = q(q-1) \dots (q-n+1)$.
2. Si G es un árbol de n vértices T_n , entonces $P_{T_n}(q) = q(q-1)^{n-1}$.

DM- p. 88/141

Ejemplo

Problema 8

En el congreso Lattice'06 hay seis conferencias de una hora programadas para el día inaugural $\{c_1, c_2, \dots, c_6\}$. Entre la audiencia hay quienes quieren escuchar los pares de conferencias $\{c_1, c_2\}$, $\{c_1, c_4\}$, $\{c_3, c_5\}$, $\{c_2, c_6\}$, $\{c_4, c_5\}$, $\{c_5, c_6\}$ y $\{c_1, c_6\}$. ¿Cuál es el número mínimo de horas necesarias para poder dar todas las conferencias sin solaparse?

Aplicación recursiva del teorema de contracción borrado:

$$P \left(\begin{array}{c} \bullet \\ \bullet \quad \bullet \\ \bullet \quad \bullet \\ \bullet \end{array} \right) = (q-1) \times P \left(\begin{array}{c} \bullet \\ \bullet \quad \bullet \\ \bullet \quad \bullet \\ \bullet \end{array} \right)$$

$$P \left(\begin{array}{c} \bullet \\ \bullet \quad \bullet \\ \bullet \quad \bullet \\ \bullet \end{array} \right) = P \left(\begin{array}{c} \bullet \\ \bullet \quad \bullet \\ \bullet \quad \bullet \\ \bullet \end{array} \right) - P \left(\begin{array}{c} \bullet \\ \bullet \quad \bullet \\ \bullet \quad \bullet \\ \bullet \end{array} \right) = (q-2)P_{C_4}(q)$$

$$P_G(q) = (q-1)(q-2)P_{C_4}(q) \quad [P_{C_4}(q) = q(q-1)(q^2-3q+3)]$$

$$= q(q-1)^2(q-2)(q^2-3q+3).$$

$$\chi(G) = 3.$$

DM-p. 89/141

Tema 11. Relaciones binarias. Relaciones de equivalencia

1. Relaciones binarias:

- Definición.
- Representación gráfica de una relación.
- Operaciones definidas sobre relaciones.
- Propiedades.

2. Relaciones de equivalencia:

- Clases de equivalencia.
- Conjunto cociente.

3. Relaciones de orden.

4. Retículos y álgebras de Boole.

DM-p. 90/141

Relaciones binarias entre dos conjuntos

Definición 135

Una **relación binaria** \mathcal{R} del conjunto V al conjunto W es un subconjunto del producto cartesiano $V \times W$:

$$V \times W = \{(v, w) : (v \in V) \wedge (w \in W)\}.$$

Luego $\mathcal{R} \subseteq V \times W$. El **dominio** de \mathcal{R} es:

$$\text{Dom } \mathcal{R} = \{v \in V : (v, w) \in \mathcal{R} \text{ para algún } w \in W\}.$$

y la **imagen** de \mathcal{R} es:

$$\text{Im } \mathcal{R} = \{w \in W : (v, w) \in \mathcal{R} \text{ para algún } v \in V\}.$$

Notación: Si $(v, w) \in \mathcal{R}$, lo escribiremos $v\mathcal{R}w$.

DM– p. 91/141

Relaciones binarias en un conjunto

Definición 136

Una **relación binaria** \mathcal{R} sobre un conjunto V es un subconjunto del producto cartesiano $V \times V$. Luego $\mathcal{R} \subseteq V \times V$. El **dominio** de \mathcal{R} es:

$$\text{Dom } \mathcal{R} = \{v \in V : (v, w) \in \mathcal{R} \text{ para algún } w \in V\}$$

y la **imagen** de \mathcal{R} es:

$$\text{Im } \mathcal{R} = \{w \in V : (v, w) \in \mathcal{R} \text{ para algún } v \in V\}.$$

Observación importante: una función $f: A \rightarrow B$ es una relación entre los conjuntos A y B tal que a cada elemento $x \in \text{Dom}(f)$ le corresponde un único elemento de B (i.e., $f(x)$).

DM– p. 92/141

Representación gráfica de una relación

- Representación cartesiana.
- Representación con diagramas de Venn.
- Matriz de adyacencia de \mathcal{R} :
Sean $V = \{v_1, v_2, \dots, v_{|V|}\}$ y $W = \{w_1, w_2, \dots, w_{|W|}\}$. La entrada (i, j) de $A_{\mathcal{R}}$ es 1 si $v_i \mathcal{R} w_j$ y es 0 en caso contrario.
- Grafo orientado $G_{\mathcal{R}}$ asociado a \mathcal{R} :
Los vértices del grafo son los elementos del conjunto V sobre el que está definida la relación \mathcal{R} . El conjunto de aristas (dirigidas) es el conjunto de pares (ordenados):

$$E = \{(v_i, v_j) \in V \times V : v_i \mathcal{R} v_j\}.$$

DM– p. 93/141

Operaciones con relaciones

Definición 137

Dada la relación \mathcal{R} sobre V , se define su **relación inversa** \mathcal{R}^{-1} como la relación en V definida como $(v_1, v_2) \in \mathcal{R}^{-1} \Leftrightarrow (v_2, v_1) \in \mathcal{R}$ ó bien como $v_1 \mathcal{R}^{-1} v_2 \Leftrightarrow v_2 \mathcal{R} v_1$.

La relación inversa \mathcal{R}^{-1} existe siempre, al contrario que la función inversa f^{-1} (que sólo existe si f es biyectiva).

Definición 138

Dada la relación \mathcal{R} sobre V , se define su **relación complementaria** $\overline{\mathcal{R}}$ como la relación en V definida como $(v_1, v_2) \in \overline{\mathcal{R}} \Leftrightarrow (v_1, v_2) \notin \mathcal{R}$.

Las relaciones son subconjuntos del conjunto $V \times W$, luego podemos efectuar las mismas operaciones que con un conjunto cualquiera.

DM– p. 94/141

Composición de relaciones

Definición 139

Sea \mathcal{R} una relación de V en W y sea \mathcal{S} una relación de W en Y . La **relación compuesta** $\mathcal{S} \circ \mathcal{R}$ de V en Y es un subconjunto del producto cartesiano $V \times Y$ tal que $v(\mathcal{S} \circ \mathcal{R})y$ con $v \in V$ e $y \in Y$ si existe algún $w \in W$ tal que $v\mathcal{R}w$ y $w\mathcal{S}y$.

Proposición 140 Si $A_{\mathcal{R}}$ es la matriz de adyacencia de la relación \mathcal{R} de V en W y $A_{\mathcal{S}}$ es la matriz de adyacencia de la relación \mathcal{S} de W en Y , la matriz de adyacencia $A_{\mathcal{S} \circ \mathcal{R}}$ de la relación compuesta $\mathcal{S} \circ \mathcal{R}$ viene dada por:

$$A_{\mathcal{S} \circ \mathcal{R}} = A_{\mathcal{R}} \odot A_{\mathcal{S}},$$

donde el producto \odot es el **producto booleano** de matrices.

El uso de operaciones booleanas garantiza que $A_{\mathcal{S} \circ \mathcal{R}}$ sea una matriz de adyacencia asociada a una relación.

DM– p. 95/141

Propiedades de las relaciones sobre V

Definición 141

Una relación \mathcal{R} es **reflexiva** si para todo $v \in V$ se cumple que $v\mathcal{R}v$.

Definición 142

Una relación \mathcal{R} es **antirreflexiva** si para todo $v \in V$ se cumple que $v\overline{\mathcal{R}}v$.

Definición 143

Una relación \mathcal{R} es **simétrica** si $\mathcal{R} = \mathcal{R}^{-1}$, es decir, si $v\mathcal{R}w \Rightarrow w\mathcal{R}v$.

Definición 144

Una relación \mathcal{R} es **antisimétrica** si $(v_1\mathcal{R}v_2) \wedge (v_2\mathcal{R}v_1) \Rightarrow v_1 = v_2$.

DM– p. 96/141

Relaciones transitivas

Definición 145

Una relación \mathcal{R} es **transitiva** si $(v_1 \mathcal{R} v_2) \wedge (v_2 \mathcal{R} v_3) \Rightarrow v_1 \mathcal{R} v_3$.

Proposición 146 Una relación \mathcal{R} es transitiva si y sólo si $\mathcal{R}^n \subseteq \mathcal{R}$ para $n \in \mathbb{N}$. La **potencia de una relación** \mathcal{R}^n se define recursivamente como sigue:

$$\mathcal{R}^1 = \mathcal{R}, \quad \mathcal{R}^n = \mathcal{R} \circ \mathcal{R}^{n-1}.$$

Corolario 147 Una relación \mathcal{R} es transitiva si y sólo si para toda entrada no nula $(A_{\mathcal{R}^2})_{i,j} = 1$ de la matriz de adyacencia de \mathcal{R}^2 , la correspondiente entrada de la matriz de adyacencia de \mathcal{R} es también no nula $(A_{\mathcal{R}})_{i,j} = 1$.

DM– p. 97/141

Relaciones de equivalencia

Definición 148

Una relación \mathcal{R} sobre el conjunto V es una **relación de equivalencia** si es reflexiva, simétrica y transitiva.

Notación: Si \mathcal{R} es una relación de equivalencia, $a \mathcal{R} b$ se suele denotar por $a \equiv b \text{ (mód } \mathcal{R})$.

Definición 149

Sea \mathcal{R} una relación de equivalencia sobre V . El conjunto de todos los elementos relacionados con un cierto $v \in V$ se denomina **clase de equivalencia de v** y se denota por $[v]_{\mathcal{R}}$ ó simplemente por $[v]$. Luego

$$[v]_{\mathcal{R}} = \{w \in V : v \mathcal{R} w\}.$$

Cualquier elemento $w \in [v]_{\mathcal{R}}$ (en particular, v) se denomina **representante** de la clase de equivalencia $[v]_{\mathcal{R}}$.

DM– p. 98/141

Conjunto cociente

Teorema 150 Sea \mathcal{R} una relación de equivalencia sobre V . Entonces, dos

- (1) $[a]_{\mathcal{R}}$ es no vacía para todo $a \in V$.
- (2) Para cualquier par de elementos $a, b \in V$, o bien $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ (y $a\mathcal{R}b$) o bien $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.
- (3) Las clases de equivalencia determinan de manera única la relación de equivalencia.

Teorema 151 Sea \mathcal{R} una relación de equivalencia sobre V . Entonces las clases de equivalencia de \mathcal{R} constituyen una partición de V . Recíprocamente, dada una partición $\{V_1, V_2, \dots\}$ de V , existe una relación de equivalencia \mathcal{R} tal que sus clases de equivalencia son los conjuntos V_i .

Definición 152

Sea \mathcal{R} una relación de equivalencia sobre V . El conjunto de todas las clases de equivalencia de \mathcal{R} se denomina **conjunto cociente de V por \mathcal{R}** y se denota por V/\mathcal{R} :

$$V/\mathcal{R} = \{[v]_{\mathcal{R}} : v \in V\}.$$

DM– p. 99/141

Tema 12: Aritmética modular

1. **Aritmética entera:**

- División de enteros (recordatorio).
- Algoritmo de Euclides.
- Identidad de Bezout.
- Ecuaciones diofánticas lineales.

2. **Aritmética modular.**

- Congruencias lineales.
- Aritmética en \mathbb{Z}_p .
- La función de Euler. Teorema de Euler.

DM– p. 100/141

Aritmética entera: Recordatorio del tema 1

Definición 153

Dados dos enteros $a \neq 0$ y b , se dice de a **divide a b** si existe un entero $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Cuando a divide a b , se dice que a es un **factor** o **divisor** de b y que b es un **múltiplo** de a . Si a divide a b , lo denotamos por $a \mid b$ y si a no divide a b , por $a \nmid b$.

Observaciones:

- Cualquier entero no nulo $a \in \mathbb{Z}$ divide a 0: $0 = a \cdot 0$.
- 1 divide a cualquier entero $a \in \mathbb{Z}$: $a = 1 \cdot a$.
- Cualquier entero $a \in \mathbb{Z}$ se divide a sí mismo: $a = a \cdot 1$.

Teorema 154 (Algoritmo de divisibilidad) Si a y b son dos enteros con $b \neq 0$, entonces existe un único par de enteros q y r tales que

$$a = q \cdot b + r \quad \text{con} \quad 0 \leq r < |b|.$$

DM- p. 101/141

Propiedades de la división de enteros

Teorema 155 Sean $a, b, c \in \mathbb{Z}$.

1. Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.
2. Si $a \mid b$, entonces $a \mid (b \cdot c)$ para todo $c \in \mathbb{Z}$.
3. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
4. Si $c \neq 0$, entonces $a \mid b$ si y sólo si $(c \cdot a) \mid (c \cdot b)$.
5. Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.
6. Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.

Teorema 156 Si $a \mid b_i$ para $i = 1, \dots, N$, entonces $a \mid \sum_{i=1}^N u_i \cdot b_i$ para todo $u_i \in \mathbb{Z}$.

DM- p. 102/141

Máximo común divisor. Lema de Euclides (s III a.c.)

Definición 157

Dados dos enteros $a, b \neq 0$, se denomina **máximo común divisor** de a y b [denotado por $\text{mcd}(a, b)$] al mayor entero d tal que $d \mid a$ y $d \mid b$.

Observaciones:

- El caso $a = b = 0$ hay que excluirlo porque cualquier número divide al 0.
- $\text{mcd}(0, a) = |a|$ para todo entero no nulo a .

Teorema 158 El máximo común divisor de dos números enteros es único.

Lema 159 (Euclides) Sea $a = q \cdot b + r$, donde $a, b \neq 0$, q y r son enteros. Entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

DM- p. 103/141

Algoritmo de Euclides

Problema 9

Aplicar el Lema de Euclides de manera recursiva para calcular $\text{mcd}(662, 414)$.

$$\begin{aligned}a &= b \cdot q + r, \\662 &= 414 \cdot 1 + 248, \\414 &= 248 \cdot 1 + 166, \\248 &= 166 \cdot 1 + 82, \\166 &= 82 \cdot 2 + \boxed{2}, \\82 &= 2 \cdot 41 + 0.\end{aligned}$$

$$\begin{aligned}\text{mcd}(662, 414) &= \text{mcd}(414, 248) = \text{mcd}(248, 166) = \text{mcd}(166, 82) \\&= \text{mcd}(82, 2) = \boxed{2}.\end{aligned}$$

En general, $\text{mcd}(a, b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2) = \dots = \text{mcd}(r_{n-2}, r_{n-1})$, donde r_{n-1} es el último resto no nulo ($r_n = 0$). En el último paso:

$r_{n-2} = q_n \cdot r_{n-1} \Rightarrow r_{n-1} \mid r_{n-2}$. Por tanto, $\text{mcd}(r_{n-2}, r_{n-1}) = r_{n-1}$.

Teorema 160 En el Algoritmo de Euclides $\text{mcd}(a, b) = r_{n-1}$ (i.e., el último resto no nulo).

DM- p. 104/141

Identidad de Bezout

Teorema 161 (Identidad de Bezout, 1730-1783) Si a y b son enteros (no nulos simultáneamente), existen enteros u, w tales que

$$\text{mcd}(a, b) = a \cdot u + b \cdot w.$$

DEMOSTRACIÓN. Si escribimos los pasos del Algoritmo de Euclides

$$\begin{array}{llll} a = q_1 \cdot b + r_1 & \Rightarrow & r_1 = a - q_1 \cdot b & P_1 \\ b = q_2 \cdot r_1 + r_2 & \Rightarrow & r_2 = b - q_2 \cdot r_1 & P_2 \\ r_1 = q_3 \cdot r_2 + r_3 & \Rightarrow & r_3 = r_1 - q_3 \cdot r_2 & P_3 \\ \vdots & & \vdots & \\ r_{n-4} = q_{n-2} \cdot r_{n-3} + r_{n-2} & \Rightarrow & r_{n-2} = r_{n-4} - q_{n-2} \cdot r_{n-3} & P_{n-2} \\ r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1} & \Rightarrow & r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2} & P_{n-1} \\ r_{n-2} = q_n \cdot r_{n-1} + (r_n = 0) & \Rightarrow & r_{n-1} = \text{mcd}(a, b) & P_n \end{array}$$

Luego, $\text{mcd}(a, b) = r_{n-1} = \alpha_{n-1}r_{n-3} + \beta_{n-1}r_{n-2} = \alpha_{n-2}r_{n-4} + \beta_{n-2}r_{n-3} = \dots = \alpha_3r_1 + \beta_3r_2 = \alpha_2b + \beta_2r_1 = \alpha_1a + \beta_1b$.

DM- p. 105/141

Identidad de Bezout (2)

Importante: La identidad de Bezout **no** implica la unicidad de los enteros u y w .

Teorema 162 Sean dos números enteros a y b no nulos simultáneamente con $\text{mcd}(a, b) = d$. Un entero c puede ser escrito de la forma $a \cdot x + b \cdot y$ para algunos enteros x, y si y sólo si c es múltiplo de d . En particular, d es el menor natural de la forma $a \cdot x + b \cdot y$ con $x, y \in \mathbb{Z}$.

Corolario 163 Dos enteros a y b son coprimos si y sólo si existen enteros x, y tales que $a \cdot x + b \cdot y = 1$.

Corolario 164 Si $\text{mcd}(a, b) = d$, entonces:

1. $\text{mcd}(m \cdot a, m \cdot b) = m \cdot d$ para todo $m \in \mathbb{N}$.
2. $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Corolario 165 Si a, b son enteros primos entre sí, entonces:

1. Si $a \mid c$ y $b \mid c$, entonces $(a \cdot b) \mid c$.
2. Si $a \mid (b \cdot c)$, entonces $a \mid c$.

DM- p. 106/141

Mínimo común múltiplo

Definición 166

Dados dos números a, b enteros no nulos, se define el **mínimo común múltiplo** de a y b [y se denota por $\text{mcm}(a, b)$] al menor número natural m tal que $a \mid m$ y $b \mid m$.

Observación: Este número existe debido a que \mathbb{N} es un conjunto bien ordenado como veremos en el siguiente tema.

Teorema 167 Sean $a, b \in \mathbb{N}$ con $d = \text{mcd}(a, b)$ y $m = \text{mcm}(a, b)$. Entonces,

$$a \cdot b = d \cdot m.$$

Algunos resultados sobre números primos:

Teorema 168 Si $n > 1$ es un número compuesto si y sólo si n es divisible por algún número primo $p \leq \sqrt{n}$.

Lema 169 Sea p un número primo y $a, b \in \mathbb{Z}$. Entonces:

- (a) $p \mid a$ ó $p \nmid a$ y a son primos entre sí.
- (b) Si $p \mid (a \cdot b)$, entonces ó $p \mid a$ ó $p \mid b$.

DM- p. 107/141

Ecuaciones diofánticas lineales [Diophantos, s III]

Definición 170

Una **ecuación diofántica** es una ecuación de una o varias variables y de la que nos interesan sólo sus soluciones enteras.

Teorema 171 (Brahmagupta, s VII) La ecuación lineal

$$a \cdot x + b \cdot y = c,$$

con $a, b, c \in \mathbb{Z}$ (y a, b no nulos simultáneamente) admite soluciones enteras si y sólo si $d = \text{mcd}(a, b)$ divide a c , en cuyo caso existen infinitas soluciones enteras (x_k, y_k) con $k \in \mathbb{Z}$ dadas por

$$\begin{aligned}x_k &= u \cdot p + \frac{b \cdot k}{d}, \\y_k &= w \cdot p - \frac{a \cdot k}{d},\end{aligned}$$

donde $p = c/d \in \mathbb{Z}$ y u, w vienen dados por:

$$d = u \cdot a + w \cdot b.$$

DM- p. 108/141

Aritmética modular

La **aritmética modular** nos permite realizar operaciones algebraicas utilizando en vez de números sus respectivos restos respecto de una cantidad fija denominada **módulo** (el módulo es 12 ó 24 al contar horas en un reloj, 7 al contar días de la semana, etc).

Definición 172

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Entonces **a es congruente con b módulo m** si $m \mid (a - b)$. Esta relación se denota por $a \equiv b \pmod{m}$.

Proposición 173

1. $a \equiv b \pmod{m}$ si y sólo si $a \bmod m = b \bmod m$.
2. $a \equiv b \pmod{m}$ si y sólo si $a = b + k \cdot m$ para algún $k \in \mathbb{Z}$.

Teorema 174 La relación $\equiv \pmod{m}$ para cualquier natural m es una relación de equivalencia.

DM- p. 109/141

El conjunto cociente \mathbb{Z}_m

Las clases de equivalencia o de **congruencia** módulo m

$$[a]_m = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\} = \{a + mk : k \in \mathbb{Z}\}$$

constituyen una partición de \mathbb{Z} . Hay m clases de equivalencia distintas correspondientes a los m restos posibles al dividir un entero por m .

Teorema 175 El conjunto cociente $\mathbb{Z}_m = \mathbb{Z} / \equiv \pmod{m}$ está dado por

$$\mathbb{Z}_m = \{[a]_m : 0 \leq a \leq m - 1\}.$$

Nota: Normalmente la notación para \mathbb{Z}_m se relaja:

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}.$$

DM- p. 110/141

Aritmética modular

Teorema 176 Sea $m \in \mathbb{N}$. Si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces:

- $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$.
- $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.

Corolario 177 Sean $m, k \in \mathbb{N}$. Si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$.

Teorema 178 Sea $m \in \mathbb{N}$ y sean $a, b, c \in \mathbb{Z}$. Si $a \cdot c \equiv b \cdot c \pmod{m}$ y $\text{mcd}(c, m) = 1$, entonces $a \equiv b \pmod{m}$.

Observaciones:

- Este teorema nos permite dividir a ambos lados del signo \equiv siempre y cuando el número por el que dividimos c y el módulo m sean primos entre sí.
- Si c y m no son coprimos, entonces el resultado correcto es: sea $m = p \cdot c$ con $p, c \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$. Si $a \cdot c \equiv b \cdot c \pmod{p \cdot c}$, entonces $a \equiv b \pmod{p}$.

DM- p. 111/141

División modular: congruencias lineales

Definición 179

Una congruencia de la forma

$$a \cdot x \equiv b \pmod{m},$$

donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina **congruencia lineal**.

Nota: Si existe una única solución de la congruencia lineal $a \cdot x \equiv 1 \pmod{m}$, entonces esto es equivalente a obtener un inverso multiplicativo de a módulo m .

Observación: Si x es una solución de una congruencia lineal y $x' \equiv x \pmod{m}$, entonces x' también es solución

$$a \cdot x' \equiv a \cdot x \pmod{m} \equiv b \pmod{m}.$$

Luego, las soluciones, si existen, forman clases de congruencia módulo m ; es decir, son elementos de \mathbb{Z}_m .

DM- p. 112/141

Congruencias lineales

Teorema 180 Si $d = \text{mcd}(a, m)$, entonces la congruencia lineal

$$a \cdot x \equiv b \pmod{m}$$

tiene solución si y sólo si $d \mid b$. En este caso y si x_0 es una solución particular de la congruencia lineal, la solución general viene dada por

$$x_k = x_0 + \frac{m \cdot k}{d}, \quad k \in \mathbb{Z}.$$

En particular, las soluciones forman d clases de congruencia módulo m con representantes

$$\left\{ x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{m(d-1)}{d} \right\}.$$

Corolario 181 Si $\text{mcd}(a, m) = 1$ las soluciones x de la congruencia lineal $a \cdot x \equiv b \pmod{m}$ constituyen una única clase de congruencia módulo m .

Corolario 182 Si $\text{mcd}(a, m) = 1$ y $m > 1$, entonces existe un inverso de a módulo m . Dicho inverso es único módulo m .

DM– p. 113/141

Aritmética en \mathbb{Z}_m

Los elementos de \mathbb{Z}_m con $m \in \mathbb{N}$ son clases de equivalencia módulo m . Por simplicidad, $x \in \mathbb{Z}_m$ representa que $x \in [x]_m$.

La **suma** y el **producto** en \mathbb{Z}_m se definen como

$$\begin{aligned} x + y &= [x]_m + [y]_m = [x + y]_m, \\ x \cdot y &= [x]_m \cdot [y]_m = [x \cdot y]_m, \end{aligned}$$

y verifican las propiedades usuales: para todo $x, y, z \in \mathbb{Z}_m$,

- Propiedad interna: $x + y \in \mathbb{Z}_m$ y $x \cdot y \in \mathbb{Z}_m$.
- Propiedades asociativas: $x + (y + z) = (x + y) + z$ y $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Propiedades conmutativas: $x + y = y + x$ y $x \cdot y = y \cdot x$.
- Propiedad distributiva: $x \cdot (y + z) = x \cdot y + x \cdot z$.
- Elemento neutro (suma): $\exists 0 \in \mathbb{Z}_m$ tal que $0 + x = x$, $\forall x \in \mathbb{Z}_m$.
- Elemento neutro (producto): $\exists 1 \in \mathbb{Z}_m$ tal que $1 \cdot x = x$, $\forall x \in \mathbb{Z}_m$.
- Elemento inverso (suma): $\forall x \in \mathbb{Z}_m$, $\exists -x \in \mathbb{Z}_m$ tal que $x + (-x) = 0$.

Importante: Son todas las propiedades de **cuerpo** (como $(\mathbb{R}, +, \cdot)$) excepto la existencia de inverso con respecto del producto.

DM– p. 114/141

Aritmética en \mathbb{Z}_m (2)

En \mathbb{Z} no existe en general el inverso (multiplicativo) de un entero x : y es el inverso multiplicativo de x si y sólo si $x \cdot y = 1$. Sin embargo, sí se verifican dos propiedades:

1. Propiedad cancelativa del producto: si $x \neq 0$ y $x \cdot y = x \cdot z$, entonces $y = z$.
2. Si $x \cdot y = 0$ entonces $x = 0$ ó $y = 0$.

Ninguna de las dos se cumple genéricamente en \mathbb{Z}_m .

Definición 183

Un elemento $x \not\equiv 0 \pmod{m}$ de \mathbb{Z}_m es un **divisor de cero** si existe un elemento $y \not\equiv 0 \pmod{m}$ tal que $x \cdot y \equiv 0 \pmod{m}$.

Nota: en algunos libros se elimina la condición $x \not\equiv 0 \pmod{m}$.

Definición 184

Un elemento $x \in \mathbb{Z}_m$ es una **unidad módulo m** si es invertible; es decir, si existe un $s \in \mathbb{Z}_m$ tal que $x \cdot s \equiv 1 \pmod{m}$.

Teorema 185 El inverso de una unidad módulo m es único.

Nota: Como el inverso de una unidad r módulo m es único, lo denotaremos por r^{-1} .

DM- p. 115/141

Aritmética en \mathbb{Z}_m (3)

Teorema 186 Un elemento $r \in \mathbb{Z}_m$ es invertible si y sólo si r y m son primos entre sí.

Corolario 187 Si p es primo, todo elemento de \mathbb{Z}_p distinto de 0 es invertible.

- Si p es primo, entonces $(\mathbb{Z}_p, +, \cdot)$ es un **cuerpo** como $(\mathbb{R}, +, \cdot)$ ó $(\mathbb{Q}, +, \cdot)$.
- Si $m = p \cdot q$ es compuesto, entonces se sigue la existencia de divisores de cero en \mathbb{Z}_m : $p \cdot q \equiv 0 \pmod{m}$ con $p, q \not\equiv 0 \pmod{m}$. En este caso, $(\mathbb{Z}_m, +, \cdot)$ es un **anillo con divisores de cero**.

Definición 188

La función ϕ de Euler $\phi: \mathbb{N} \rightarrow \mathbb{N}$ se define de manera que $\phi(m)$ es igual al número de elementos invertibles de \mathbb{Z}_m .

Lema 189 Si p es primo, $\phi(p) = p - 1$.

DM- p. 116/141

El teorema de Euler

Teorema 190 (Euler, 1790) Si y es invertible en \mathbb{Z}_m (es decir, si $\text{mcd}(y, m) = 1$), entonces

$$y^{\phi(m)} \equiv 1 \pmod{m}.$$

Corolario 191 (Teorema pequeño de Fermat) Si p es primo y si $y \not\equiv 0 \pmod{p}$, entonces

$$y^{p-1} \equiv 1 \pmod{p}.$$

Corolario 192 Si p es primo, entonces para cualquier entero y se tiene que

$$y^p \equiv y \pmod{p}.$$

Teorema 193

1. Si p es primo, entonces $\phi(p^k) = p^{k-1}(p-1)$ para todo $k \in \mathbb{N}$.
2. Si $\text{mcd}(m, n) = 1$, entonces $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
3. Si $n \geq 2$ tiene la siguiente descomposición en factores primos $n = \prod_{k=1}^r p_k^{n_k}$ con $n_k \geq 1$, entonces $\phi(n) = n \cdot \prod_{k=1}^r (1 - 1/p_k)$.

DM- p. 117/141

Tema 13. Relaciones de orden

1. Relaciones binarias.
2. Relaciones de equivalencia.
3. Relaciones de orden:
 - Conjuntos parcialmente ordenados.
 - Diagrama de Hasse.
 - Elementos maximales.
 - Conjuntos totalmente ordenados.
 - Conjuntos bien ordenados e inducción matemática.
4. Retículos y álgebras de Boole.

DM- p. 118/141

Relación de orden parcial

Definición 194

Una relación sobre un conjunto V se denomina **orden parcial** (o **relación de orden**) si es reflexiva, antisimétrica y transitiva.

Notación: Las relaciones de orden se suelen denotar por el símbolo \preceq .

Definición 195

Un conjunto V equipado con una relación de orden \preceq se denomina **conjunto parcialmente ordenado** (V, \preceq) (o **poset**).

Definición 196

Sea (V, \preceq) un conjunto parcialmente ordenado. Dos elementos $a, b \in V$ son **comparables** si ó bien $a \preceq b$ ó bien $b \preceq a$. Si no se verifican ninguna de estas condiciones, dichos elementos se denominan **no comparables**.

Definición 197

Un conjunto parcialmente ordenado (V, \preceq) está **totalmente ordenado** cuando cualquier par de elementos $a, b \in V$ son comparables. Se dice entonces que (V, \preceq) es un conjunto **totalmente ordenado** (o **cadena**).

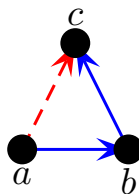
DM- p. 119/141

Diagramas de Hasse, 1926

El digrafo asociado a una relación de orden \preceq se puede simplificar eliminando las redundancias derivadas de las propiedades de orden

Algoritmo para obtener el diagrama de Hasse del orden parcial \preceq :

1. Como \preceq es reflexiva, hay un bucle en cada vértice. Eliminar todos los bucles.
2. La transitividad de \preceq se refleja en la posible existencia de subgrafos del tipo:



Si $a \preceq b$ y $b \preceq c$, eliminar la arista superflua asociada a $a \preceq c$.

3. Elegimos que todas las aristas apunten hacia arriba. Eliminar el sentido de las flechas.

DM- p. 120/141

Elementos extremales

Definición 198

Sea (V, \preceq) un conjunto parcialmente ordenado. $M \in V$ es un **elemento maximal** si para todo $v \in V$, $M \preceq v$ implica que $M = v$. $m \in V$ es un **elemento minimal** si para todo $v \in V$, $v \preceq m$ implica que $m = v$. Es decir, en el diagrama de Hasse asociado a (V, \preceq) , no hay ningún elemento por encima de M ni ningún elemento por debajo de m .

Definición 199

Sea (V, \preceq) un conjunto parcialmente ordenado. $M^* \in V$ es un **elemento máximo** si $v \preceq M^*$ para todo $v \in V$. $m^* \in V$ es un **elemento mínimo** si $m^* \preceq v$ para todo $v \in V$. Es decir, en el diagrama de Hasse asociado a (V, \preceq) , M^* está encima de todos los elementos de V y m^* está por debajo de todos los elementos de V . Los elementos máximo y mínimo de (V, \preceq) se denotan por $\text{máx}(V)$ y $\text{mín}(V)$ respectivamente.

Nota: Los elementos maximales, minimales, $\text{máx}(V)$ y/o $\text{mín}(V)$ de (V, \preceq) pueden no existir.

Teorema 200 El elemento máximo M^* de un conjunto parcialmente ordenado (A, \preceq) , si existe, es único. Además todo elemento máximo es maximal.

DM– p. 121/141

Elementos extremales (2)

Nota: los subconjuntos de un conjunto parcialmente ordenado (V, \preceq) heredan dicho orden \preceq .

Definición 201

Sea (V, \preceq) un conjunto parcialmente ordenado y $B \subset V$. $u \in V$ es una **cota superior o mayorante** de B si $b \preceq u$ para todo $b \in B$. El conjunto de las cotas superiores de B se denota $\text{mayor}(B)$.

$u^* \in V$ es el **supremo** de B si es la menor de las cotas superiores: $u^* = \text{mín}(\text{mayor}(B))$.

$d \in V$ es una **cota inferior o minorante** de B si $d \preceq b$ para todo $b \in B$. El conjunto de las cotas inferiores de B se denota $\text{minor}(B)$.

$d^* \in V$ es el **ínfimo** de B si es la mayor de las cotas inferiores: $d^* = \text{máx}(\text{minor}(B))$.

Nota: Puede ocurrir que $\text{mayor}(B) = \emptyset$, $\text{minor}(B) = \emptyset$ y/o que $\text{sup}(B)$ e $\text{ínf}(B)$ no existan.

DM– p. 122/141

Orden total compatible con un orden parcial

Definición 202

Un orden total (V, \preceq_T) es **compatible** con el orden parcial (V, \preceq_P) si para todo $v, w \in V$, $v \preceq_P w$ implica que $v \preceq_T w$.

Algoritmo 203 (Ordenación topológica)

procedure *TotalOrder*((V, \preceq_P) : conjunto finito parcialmente ordenado)

$k = 1$

while $V \neq \emptyset$

begin

$v_k =$ un elemento minimal de (V, \preceq_P)

$V \rightarrow V \setminus \{v_k\}$

$k \rightarrow k + 1$

end

$v_1 \preceq_T v_2 \preceq_T \dots \preceq_T v_n$ es un orden **total** compatible con (V, \preceq_P) .

DM- p. 123/141

Conjunto bien ordenado

Definición 204

(V, \preceq) es un **conjunto bien ordenado** si (V, \preceq) es un orden total y cualquier subconjunto no vacío de V tiene siempre un mínimo.

Observaciones:

- El conjunto de los números naturales con el orden habitual (\mathbb{N}, \leq) es un conjunto **bien ordenado**. Esta propiedad es equivalente al **principio de inducción**.
- El conjunto totalmente ordenado (\mathbb{Z}, \leq) no es un conjunto bien ordenado; pero como \mathbb{Z} es isomorfo a \mathbb{N} , podemos escoger otro orden \preceq tal que (\mathbb{Z}, \preceq) sea un conjunto bien ordenado.

DM- p. 124/141

El principio de inducción para los naturales

Definición 205 (El principio de inducción: versión débil)

Sea P una cierta propiedad que satisface las siguientes condiciones:

- (1) Paso base: $P(1)$ es cierta.
- (2) Paso inductivo: dado un natural k arbitrario pero fijo, si $P(k)$ es cierta, entonces $P(k + 1)$ es cierta.

Entonces $P(n)$ es cierta para todo $n \in \mathbb{N}$.

Observación: La hipótesis en el paso inductivo ($P(k)$ es cierta) se denomina **hipótesis de inducción**. Para realizar el paso inductivo, se asume la hipótesis de inducción y luego se usa ésta para probar que $P(k + 1)$ es cierta.

Definición 206 (El principio de inducción: versión fuerte)

Sea P una cierta propiedad que satisface las siguientes condiciones:

- (1) Paso base: $P(1)$ es cierta.
- (2) Paso inductivo: dado un natural k arbitrario pero fijo, si $P(m)$ es cierta para todo $1 \leq m \leq k$, entonces $P(k + 1)$ es cierta.

Entonces $P(n)$ es cierta para todo $n \in \mathbb{N}$.

DM– p. 125/141

Principio de inducción para conjuntos bien ordenados

Proposición 207 (Principio fuerte de inducción para conjuntos bien ordenados) Sea (V, \preceq) un conjunto bien ordenado y sea P una cierta propiedad que satisface las siguientes condiciones:

1. Paso base: $P(v_0)$ es verdadera para $v_0 = \min(V)$.
2. Paso inductivo: sea w un elemento arbitrario pero fijo de V y sea v su sucesor. Entonces si $P(x)$ es verdadera para todo $v_0 \preceq x \preceq w$, entonces $P(v)$ es verdadera.

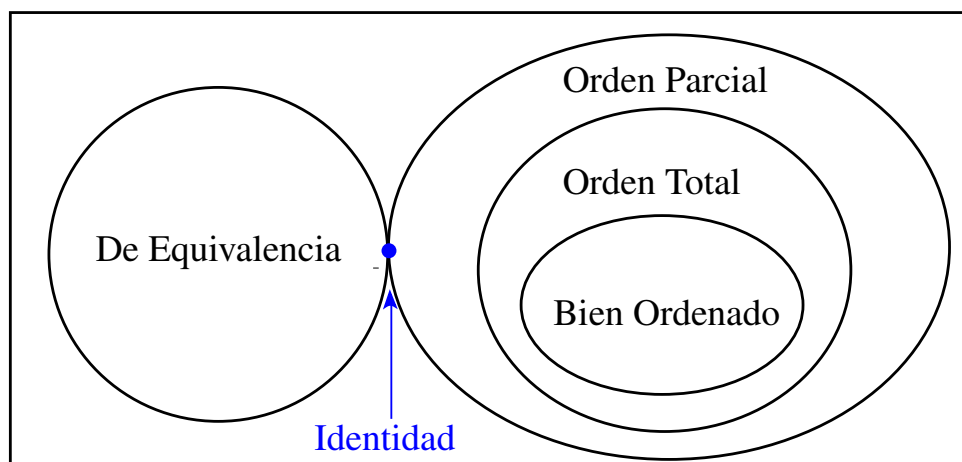
Entonces $P(v)$ es cierta para todo $v \in V$.

DM– p. 126/141

Resumen: Tipos de relaciones

| Relación | Reflexiva | Simétrica | Antisimétrica | Transitiva | |
|---------------|-----------|-----------|---------------|------------|--|
| Equivalencia | SI | SI | NO | SI | |
| Orden | SI | NO | SI | SI | |
| Orden Total | SI | NO | SI | SI | Todo par es comparable |
| Bien ordenado | SI | NO | SI | SI | Todo subconjunto no vacío tiene mínimo |

Relaciones



DM- p. 127/141

Tema 14. Retículos y álgebras de Boole

1. Relaciones binarias.
2. Relaciones de equivalencia.
3. Relaciones de orden.
4. Retículos y álgebras de Boole:
 - Definiciones y propiedades.
 - Retículos acotados.
 - Retículos distributivos.
 - Retículos complementados.
 - Álgebras de Boole

DM- p. 128/141

Retículo

Definición 208

Un **retículo** es un conjunto parcialmente ordenado (A, \preceq) en el que cada par de elementos tiene un supremo y un ínfimo.

- Si existen, tanto $\sup(a, b)$ como $\inf(a, b)$ son únicos.
- Si (A, \preceq) es un retículo, ambas operaciones se pueden considerar operadores binarios sobre A : si $a, b \in A$
 - Su supremo se denota por $\sup(a, b) = a \vee b \in A$.
 - Su ínfimo se denota por $\inf(a, b) = a \wedge b \in A$.
- No todos los conjuntos parcialmente ordenados son retículos.
- Un conjunto totalmente ordenado sí es un retículo con $\sup(a, b) = \max(a, b)$ e $\inf(a, b) = \min(a, b)$.

DM– p. 129/141

Dualidad

- Si (A, \preceq) es un conjunto parcialmente ordenado, (A, \succeq) lo es también. El diagrama de Hasse de (A, \succeq) se obtiene invirtiendo el de (A, \preceq) .
- Si (A, \preceq) es un retículo, entonces (A, \succeq) también lo es siempre que $\sup \leftrightarrow \inf$.

Corolario 209 (Principio de dualidad) *Cualquier enunciado referido a un retículo (A, \preceq) se mantiene válido si intercambiamos \preceq por \succeq , \sup por \inf y \vee por \wedge .*

- Los retículos (A, \preceq) y (A, \succeq) son duales entre sí.
- Las relaciones de orden \preceq y \succeq son duales entre sí.
- Las operaciones \vee y \wedge son duales entre sí.

DM– p. 130/141

Propiedades de los retículos

Proposición 210 Si (A, \preceq) es un retículo, entonces para cualquier $a, b, c \in A$:

1. $\sup(a, a) = a \vee a = a$ [idempotencia]
2. $\sup(a, b) = a \vee b = b \vee a = \sup(b, a)$ [conmutatividad]
3. $\sup(a, \sup(b, c)) = a \vee (b \vee c) = (a \vee b) \vee c = \sup(\sup(a, b), c)$ [asociatividad]
4. $\sup(a, \inf(a, b)) = a \vee (a \wedge b) = a$ [absorción]

Por dualidad se obtiene:

Corolario 211 Si (A, \preceq) es un retículo, entonces para cualquier $a, b, c \in A$:

1. $\inf(a, a) = a \wedge a = a$ [idempotencia]
2. $\inf(a, b) = a \wedge b = b \wedge a = \inf(b, a)$ [conmutatividad]
3. $\inf(a, \inf(b, c)) = a \wedge (b \wedge c) = (a \wedge b) \wedge c = \inf(\inf(a, b), c)$ [asociatividad]
4. $\inf(a, \sup(a, b)) = a \wedge (a \vee b) = a$ [absorción]

DM- p. 131/141

Propiedades de los retículos (2)

Proposición 212 Si (A, \preceq) es un retículo, entonces para cualquier $a, b \in A$ las siguientes afirmaciones son equivalentes:

1. $a \preceq b$
2. $\sup(a, b) = a \vee b = b$
3. $\inf(a, b) = a \wedge b = a$

Proposición 213 (Desigualdades distributivas) Si (A, \preceq) es un retículo, entonces para cualquier $a, b, c \in A$ se cumple que

1. $\inf(a, \sup(b, c)) = a \wedge (b \vee c) \succeq (a \wedge b) \vee (a \wedge c) = \sup(\inf(a, b), \inf(a, c))$
2. $\sup(a, \inf(b, c)) = a \vee (b \wedge c) \preceq (a \vee b) \wedge (a \vee c) = \inf(\sup(a, b), \sup(a, c))$

DM- p. 132/141

Los retículos como sistemas algebraicos

Definición 214

Un retículo es un sistema algebraico (A, \vee, \wedge) con dos operaciones binarias \vee y \wedge que satisfacen las leyes conmutativa, asociativa y de absorción.

- La ley de absorción implica la ley de idempotencia.
- Aunque no se asume la existencia de ninguna relación de orden en A , ésta se deduce de las propiedades de las operaciones \vee y \wedge . En particular, para todo $a, b \in A$,

$$a \preceq b \Leftrightarrow a \vee b = b.$$

- $a \preceq a$ ya que $a \vee a = a$ por idempotencia.
- Si $a \preceq b \Leftrightarrow a \vee b = b$. Si $b \preceq a \Leftrightarrow b \vee a = a$. Luego $a = b$.
- Si $a \preceq b \Leftrightarrow a \vee b = b$ y $b \preceq c \Leftrightarrow b \vee c = c$, entonces $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$. Luego $a \preceq c$.
- Luego \preceq es una relación de orden parcial y (A, \preceq) es un conjunto parcialmente ordenado.

DM- p. 133/141

Subretículos

Definición 215

Dado un retículo (A, \vee, \wedge) , un **subretículo** (M, \vee, \wedge) está formado por un subconjunto no vacío $M \subseteq A$ que es cerrado bajo las operaciones binarias \vee y \wedge .

- Todo retículo es subretículo de sí mismo.

DM- p. 134/141

Retículos acotados

Definición 216

Un retículo (A, \preceq) tiene una **cota inferior** denotada por 0 si $0 \preceq a$ para todo $a \in A$. De igual manera, un retículo tiene una **cota superior** denotada por 1 si $a \preceq 1$ para todo $a \in A$. Un retículo está **acotado** si tiene cotas superior e inferior.

- Las cotas 0 y 1 satisfacen las propiedades: para todo $a \in A$,
 - $\sup(a, 1) = a \vee 1 = 1$.
 - $\inf(a, 1) = a \wedge 1 = a$.
 - $\sup(a, 0) = a \vee 0 = a$.
 - $\inf(a, 0) = a \wedge 0 = 0$.
- La cota superior 1 es el elemento neutro de la operación \wedge : $a \wedge 1 = a$ y satisface que $a \vee 1 = 1$.
- La cota inferior 0 es el elemento neutro de la operación \vee : $a \vee 0 = a$ y satisface que $a \wedge 0 = 0$.
- En un retículo acotado podemos extender el principio de dualidad y considerar también el intercambio $0 \leftrightarrow 1$.
- Todo retículo finito A está acotado: $1 = \sup(A)$ y $0 = \inf(A)$.

DM- p. 135/141

Retículos distributivos

Definición 217

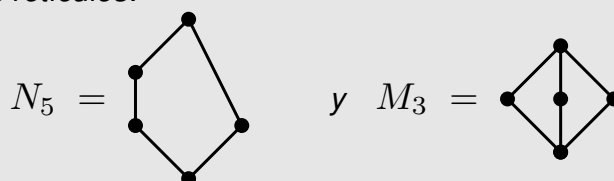
Un retículo (A, \preceq) es un **retículo distributivo** si para todo $a, b, c \in A$,

$$\begin{aligned} \inf(a, \sup(b, c)) &= a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) = \sup(\inf(a, b), \inf(a, c)) \\ \sup(a, \inf(b, c)) &= a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = \inf(\sup(a, b), \sup(a, c)) \end{aligned}$$

- Esto es algo más que la propiedad distributiva:

$$\begin{aligned} \inf(a, \sup(b, c)) &= a \wedge (b \vee c) \succeq (a \wedge b) \vee (a \wedge c) = \sup(\inf(a, b), \inf(a, c)) \\ \sup(a, \inf(b, c)) &= a \vee (b \wedge c) \preceq (a \vee b) \wedge (a \vee c) = \inf(\sup(a, b), \sup(a, c)) \end{aligned}$$

Teorema 218 Un retículo es distributivo si y sólo si **no** contiene un subretículo isomorfo a uno de estos dos retículos:



donde N_5 se denomina "retículo pentagonal" y M_3 se denomina "retículo diamante".

DM- p. 136/141

Retículos complementados

Definición 219

Si el retículo $(A, \vee, \wedge, 0, 1)$ es un retículo acotado y $a \in A$, entonces un **elemento complementario** de a es (si existe) un elemento $b \in A$ tal que $\sup(a, b) = a \vee b = 1$ e $\inf(a, b) = a \wedge b = 0$.

- Las cotas 0 y 1 son complementarios entre sí.
- Si a es complementario de b , b es complementario de a .
- Un elemento $a \in A$ puede no tener complementario o tener varios.
- El único elemento complementario a 1 es 0 y viceversa.

Definición 220

Un retículo $(A, \vee, \wedge, 0, 1)$ es **complementado** si cada elemento $a \in A$ tiene al menos un elemento complementario.

Proposición 221 En un retículo distributivo (A, \vee, \wedge) si un elemento $a \in A$ tiene un elemento complementario, éste es único.

- Luego si (A, \vee, \wedge) es un retículo distributivo y complementado, cada elemento $a \in A$ tiene un **único** elemento complementario, que denotaremos por \bar{a} .

DM– p. 137/141

Álgebra de Boole

Definición 222 (Definición 1)

Un **álgebra de Boole** es un retículo $(A, \vee, \wedge, \neg, 0, 1)$ acotado, distributivo y complementado.

Definición 223 (Definición 2)

Sea B un conjunto que contiene al menos dos elementos distintos 0, 1 y sobre el que definimos las siguientes operaciones:

- La operación binaria suma booleana $(a, b) \rightarrow a + b \in B$.
- La operación binaria producto booleano $(a, b) \rightarrow a \cdot b \in B$.
- La operación unitaria complementación $a \rightarrow \bar{a} \in B$.

Entonces B es un **álgebra de Boole** si se cumplen las siguientes propiedades para todo $a, b, c \in B$:

1. $a + 0 = a$ [elemento neutro respecto de la suma]
2. $a \cdot 1 = a$ [elemento neutro respecto del producto]
3. $a + b = b + a, a \cdot b = b \cdot a$ [conmutatividad]
4. $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [asociatividad]
5. $a + (b \cdot c) = (a + b) \cdot (a + c), a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ [propiedades distributivas]
6. $a + \bar{a} = 1, a \cdot \bar{a} = 0$ [leyes de complementos]

DM– p. 138/141

Álgebra de Boole sencilla

- Podemos eliminar el símbolo \cdot en el producto booleano $a \cdot b = ab$ siempre que no haya confusión.
- Los elementos $0, 1 \in A$ **no** tienen porqué ser iguales a los números $0, 1 \in \mathbb{Z}$.
- Las operaciones suma booleana $+$ y producto booleano \cdot en un álgebra de Boole no tienen porqué ser la suma y el producto de números reales.

El álgebra $(B, +, \cdot, \bar{}, 0, 1)$ formada por $B = \{0, 1\}$ con las operaciones suma, producto y complementación definidas sobre B como sigue:

$$\begin{aligned}1 \cdot 0 &= 0 \cdot 1 = 0 \cdot 0 = 0, \\1 \cdot 1 &= 1, \\1 + 1 &= 1 + 0 = 0 + 1 = 1, \\0 + 0 &= 0, \\\bar{1} &= 0, \\\bar{0} &= 1,\end{aligned}$$

es un álgebra de Boole y es la más simple que existe: **álgebra de Boole de dos elementos**.

DM- p. 139/141

Álgebras de Boole no triviales generales

Sea un conjunto no vacío A . Consideremos el conjunto de sus subconjuntos $\mathcal{P}(A)$ con la relación

$$B \preceq C \Leftrightarrow B \subseteq C,$$

donde $B, C \subseteq A$.

- El conjunto $(\mathcal{P}(A), \preceq)$ es un conjunto parcialmente ordenado.
- El conjunto $(\mathcal{P}(A), \preceq)$ es un retículo. Si $B, C \subseteq A$,
 - $\sup(B, C) = B \cup C \subseteq A$ ($\vee \Rightarrow \cup$).
 - $\inf(B, C) = B \cap C \subseteq A$ ($\wedge \Rightarrow \cap$).
- Los elementos neutros son
 - $1 = A$.
 - $0 = \emptyset$
- El conjunto $(\mathcal{P}(A), \cup, \cap, \emptyset, A)$ es un retículo distributivo.
- Cada $B \subseteq A$ tiene un complementario único $\bar{B} = A \setminus B \subseteq A$.
- El conjunto $(\mathcal{P}(A), \cup, \cap, \setminus, \emptyset, A)$ es un álgebra de Boole.
- Aplicación: teoría de la probabilidad.

DM- p. 140/141

Propiedades de un álgebra de Boole

Proposición 224 Si $(B, +, \cdot, \overline{}, 0, 1)$ es un álgebra de Boole, entonces para todo $a, b \in B$

1. *Leyes de idempotencia:* $a + a = a$ y $a \cdot a = a$.
2. *Leyes de dominancia:* $a + 1 = 1$ y $a \cdot 0 = 0$.
3. *Leyes de absorción:* $a \cdot (a + b) = a$ y $a + a \cdot b = a$.
4. *Leyes de De Morgan:* $\overline{(a + b)} = \overline{a} \cdot \overline{b}$ y $\overline{(a \cdot b)} = \overline{a} + \overline{b}$.
5. *Ley de involución:* $\overline{\overline{a}} = a$.
6. *Ley de cero y uno:* $\overline{1} = 0$ y $\overline{0} = 1$.

Definición 225

Dada un álgebra de Boole, el **enunciado dual** de uno dado es el que se obtiene al intercambiar las operaciones suma y producto y los elementos 0 y 1 en el enunciado original.

Proposición 226 El dual de un teorema en un álgebra de Boole es también un teorema.

Definición 227

Dada un álgebra de Boole $(B, +, \cdot, \overline{}, 0, 1)$, un subconjunto $C \subseteq B$ es una **subálgebra de Boole** si $0, 1 \in C$ y es cerrado respecto a las operaciones $+$, \cdot , $\overline{}$.