ESCUELA POLITÈCNICA SUPERIOR
UNIVERSIDAD CARLOS III DE MADRID

Transparencias de Matemática Discreta

Grado en Ingeniería en Informática

Doble Grado en Ingeniería en Informática y Administración de Empresas

Curso 2013–2014

Grupo de Modelización, Simulación Numérica y Matemática Industrial

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

v1.0: Septiembre 2013

Matemática Discreta

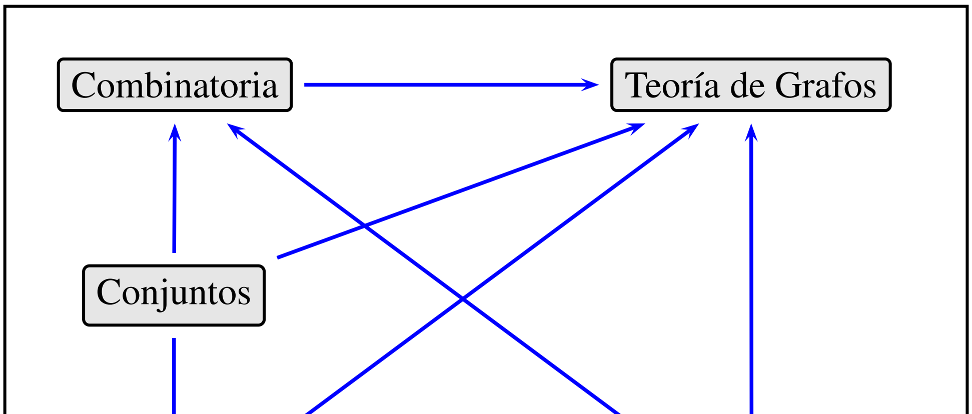
Curso 2013–2014

Grado en Ingeniería en Informática

Doble Grado en Ingeniería en Informática y Administración de Empresas

Universidad Carlos III de Madrid

Relaciones entre temas



Tema 1: Conjuntos y funciones

1. Teoría elemental de conjuntos:
   - Definiciones y operaciones.
   - Los números naturales.
2. Funciones:
   - Definiciones y operaciones.
   - Tipos de funciones.
   - Cardinal de un conjunto.
3. Divisibilidad de enteros:
   - Teorema de la divisibilidad.
   - Máximo común divisor y mínimo común múltiplo.
   - Números primos. Teorema fundamental de la aritmética.

Teoría de conjuntos elemental

Definición 1
Un **conjunto** A *es una colección bien definida de objetos (denominados* **elementos** *del conjunto):*

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

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, $x \notin X$.*

Los conjuntos no poseen una ordenación privilegiada de sus elementos ni admiten elementos múltiples.

considerando.

¿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:

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

- Notación "mixta":

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

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

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

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:*

Operaciones con conjuntos

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

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

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 Morgan
  - $\overline{A \cup B} \ = \ \overline{A} \cap \overline{B}$.
  - $\overline{A \cap B} \ = \ \overline{A} \cup \overline{B}$.
- $A \triangle B \ = \ (A \setminus B) \cup (B \setminus A)$.

Producto cartesiano

Definición 6
Dados dos conjuntos X e Y, el **producto cartesiano** $X \times Y$ *se define como el conjuntos de los* **pares ordenados***:*

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

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

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 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:
  - $\mathbb{N} = \{1, 2, 3, \ldots\}$.
  - Números enteros: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.
  - 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: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$.

Funciones

Definición 9
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 Dom(f). La* **imagen** *de la función f es el conjunto*

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

- 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 $f \colon X \to Y$.

Tipos de funciones

Definición 10
Dada una función $f: X \to Y$, 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 $f : X \to Y$ es una biyección, podemos definir su **función inversa** $f^{-1}: Y \to X$ a través de la regla (bien definida)

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

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

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

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

Cardinal de un conjunto

Definición 11
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 12
Dos conjuntos A y B tienen el mismo cardinal si y sólo si existe una correspondencia biyectiva de A a B.

Definición 13
Un conjunto que tiene un número finito de elementos o cuyo cardinal es igual al de $\mathbb{N}$ se denomina numerable.

Divisivilidad 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 14
Dados dos enteros $a \neq 0$ y b, se dice de $\boldsymbol{a}$ **divide a** $\boldsymbol{b}$ *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 $\boldsymbol{a \mid b}$ y si a no divide a b, por $\boldsymbol{a \nmid b}$.*

Observaciones:

- Cualquier entero $a \in \mathbb{Z}$ 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: $a = a \cdot 1$.

Algoritmo de divisibilidad

Teorema 15 (Algoritmo de divisibilidad) *Sean a y $b \neq 0$ dos enteros, entonces existe un* <u>**único**</u> *par de enteros q y r tales que*

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

- 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**:

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

Máximo común divisor

Definición 16
Dados dos enteros $a, b \neq 0$, se denomina **máximo común divisor** *de a y b [denotado por $\mathrm{mcd}(a,b)$] al <u>mayor</u> 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 17 *El máximo común divisor de dos números enteros es único.*

Definición 18
Dados dos números a, b enteros no nulos, se define el **mínimo común múltiplo** *de a y b [y se denota por $\mathrm{mcm}(a,b)$] al <u>menor número natural</u> m tal que $a \mid m$ y $b \mid m$.*

Teorema fundamental de la aritmética

Definición 19
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 $(3, 5, 7, 11, \ldots)$.

Teorema 20 (Euclides) *Existen infinitos números primos.*

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

son números naturales.

Máximo común divisor (2)

Una vez conocida la descomposición en factores primos de dos números es muy fácil calcular su máximo común divisor y su mínimo común múltiplo:

Teorema 22 *Si $a, b \in \mathbb{N}$ se factorizan de la forma*

$$\begin{aligned} a &= p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}, \\ b &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}, \end{aligned}$$

con $n_i, m_i \geq 0$ y donde todos los factores primos de a y b aparecen en ambas factorizaciones, se cumple que:

$$\begin{aligned} \operatorname{mcd}(a,b) &= p_1^{\text{mín}(n_1,m_1)} \cdot p_2^{\text{mín}(n_2,m_2)} \cdots p_k^{\text{mín}(n_k,m_k)}, \\ \operatorname{mcm}(a,b) &= p_1^{\text{máx}(n_1,m_1)} \cdot p_2^{\text{máx}(n_2,m_2)} \cdots p_k^{\text{máx}(n_k,m_k)}. \end{aligned}$$

Números coprimos

Es importante no confundir el concepto de número primo con el de números coprimos o primos entre sí:

Definición 23
Dos números a y b son **coprimos** *(o* **primos entre sí** *o* **primos relativos***) si $\operatorname{mcd}(a,b) = 1$.*
Se dice que un conjunto de enteros $\{a_1, \cdots, a_n\}$ es un conjunto de números coprimos si $\operatorname{mcd}(a_1, a_2, \ldots, a_n) = 1$.

Tema 2: 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.
5. Otros patrones de recuento.

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:*

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

Proposición 26 (Principio de la suma v3) *Si una tarea se puede hacer de [illegible] formas y una*

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 $A_1, A_2, \ldots, A_m$ son conjuntos finitos, entonces se tiene que:*

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

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.*

Ordenaciones de un conjunto

Definición 30
Si $n \in \mathbb{N}$, se define el **factorial de n** *como* $\quad n! \;=\; n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1.$

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*

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

Subconjuntos ordenados

Proposición 33 (Variaciones de r objetos tomados de entre n) *Dado un conjunto de n elementos diferentes podemos extraer*

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

subconjuntos ordenados de r elementos.

Observación: $V(n,n) = n!$ si defino $0! = 1$.

Proposición 34 (Variaciones con repetición) *Dado un conjunto de n elementos diferentes, podemos extraer n^r subconjuntos ordenados de r elementos si permitimos repeticiones.*

Subconjuntos

Proposición 35 (Combinaciones de r elementos tomados de entre n) *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 $0 \le r \le n$ definimos el número combinatorio $\binom{n}{r}$ como

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

Números combinatorios: triángulo de Pascal

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

$$\binom{n}{r} \equiv \binom{\text{fila}}{\text{columna}}$$

$$
\begin{tikzcd}
a \arrow[dr] & & b \arrow[dl] \\
 & a+b &
\end{tikzcd}
$$

Teorema 37

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

Teorema 38 (Identidad de Pascal)

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

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* $n \geq 0$,

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*

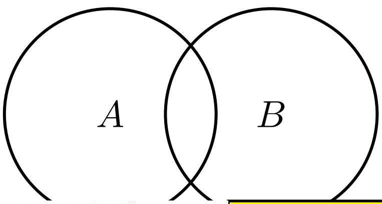
$$\binom{m+n}{k} \;=\; \sum_{q=0}^{k} \binom{m}{k-q}\binom{n}{q}\,.$$

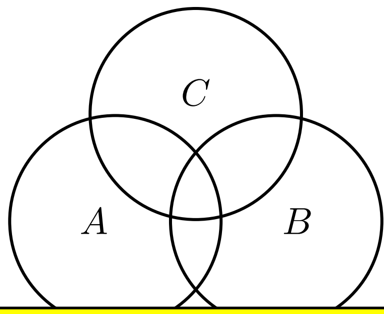
Observación: $\binom{n}{k} = 0$ para todo $n, k \in \mathbb{Z}_+$ tales que $k > n$.

Principio de inclusión-exclusión

Proposición 44 (Principio de inclusión-exclusión v1)

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





Principio de inclusión-exclusión (2)

Proposición 46 (Principio de inclusión exclusión v3)

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

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

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

Notas:

- $\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n} = \{x \mid x \notin A_1 \,, x \notin A_2 \,, \ldots \,, x \notin A_n\}$.
- $\overline{A} = S \setminus A \;\Rightarrow\; |\overline{A}| = |S| - |A|$.

Principio del palomar

Proposición 48 (Principio del palomar v1) *Si $k+1$ ó más objetos se colocan en k cajas, existe al menos una caja que contiene dos o más objetos.*

Proposición 49 (Principio del palomar generalizado) *Si se colocan N objetos en k cajas, existe al menos una caja con al menos $\lceil N/k \rceil$ objetos.*

Tema 3: Teoría de grafos I

1. Nociones generales:
   - Notación y definiciones básicas.
   - Representación de grafos.
   - Isomorfismo.
   - Caminos en grafos.
   - Árboles.
   - Grafos planos.
   - Grafos dirigidos.
2. Algoritmos en teoría de grafos.
3. Problemas combinatorios en grafos.

Grafos no orientados: definición v1

Definición 50
Un **grafo simple** $G = (V, E)$ *está compuesto por un conjunto no vacío de* **vértices** V *y un conjunto de* **aristas** E*, que es un conjunto de pares de elementos distintos de* V*.*

Si la arista e une los vértices $u, v \in V$, diremos que u y v son **adyacentes o vecinos** y que la arista e es **incidente** con u y v.

Definición 51
Un **multigrafo** $G = (V, E)$ *está compuesto por un conjunto no vacío de* **vértices** V*, un conjunto de* **aristas** E *en el que se permite que haya* **aristas múltiples** *(que son aquellas que conectan el mismo par de vértices).*

Grafos no orientados: definición v2

Definición 53
Un **pseudografo** $G = (V, E, \gamma)$ *está compuesto por un conjunto no vacío de* **vértices** V*, un conjunto de* **aristas** E*, y una función* γ *que asigna a cada arista un par no ordenado de vértices de* V *(*γ *codifica las conexiones entre los vértices).*

Si la arista e une los vértices $u, v \in V$, (es decir, si $\gamma(e) = \{u, v\}$) diremos que u y v son adyacentes o vecinos y que la arista e es incidente con u y v.
Si existen dos aristas distintas e_1, e_2 tales que $\gamma(e_1) = \gamma(e_2)$ diremos que el pseudografo tiene aristas múltiples.

Definición 54
Un **grafo simple** $G = (V, E, \gamma)$ *es un pseudografo en el que no se permite que haya aristas múltiples ni bucles.*
Un **multigrafo** $G = (V, E, \gamma)$ *es un pseudografo en el que se permite que haya aristas múltiples pero no bucles.*

Definiciones

Definición 55
El número de aristas incidentes con un vértice v *de un grafo* G *se denomina* **grado** *o* **valencia** *de* v *y se denota por* $d(v)$.

Definición 56
Los vértices de grado 1 *se denominan* **terminales**. *Los vértices de grado* 0 *se denominan* **aislados**. *Un grafo sin aristas se denomina* **trivial**.

Definición 57
Un grafo es **regular** *si todos sus vértices tienen el mismo grado.*

El teorema del *apretón de manos*

Teorema 58 *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 59 *En todo grafo G la suma de los grados de sus vértices es par.*

Teorema 60 *El número de vértices de grado impar en un grafo G es par.*

Corolario 61 *En todo grafo G con número impar de vértices hay un número impar de vértices de grado par.*

Más definiciones

Definición 62
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 y ciclo C_n de n vértices.
- Rueda de $n+1$ vértices W_n.
- Grafo bipartito completo de n y m vértices $K_{n,m}$.

Grafos complementarios y subgrafos

Definición 63
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 adyacendes en* G*.*

Definición 64
Un grafo $H = (W, F)$ *es un* **subgrafo** *de* $G = (V, E)$ *si* $W \subseteq V$ *y* $F \subseteq E$*.*

Definición 65
Dado un grafo $G = (V, E)$*, un* **subgrafo generador** *de* G *es todo aquel subgrafo* $H = (V, F)$ *con* $F \subseteq E$*.*

Representación numérica de un grafo

Definición 66
Sea $G = (V, E)$ *un grafo. Consideremos una ordenación* $v_1, v_2, \ldots, v_{|V|}$ *de los vértices de* G*. La* **matriz de adyacencia** *de* G <u>*asociada a dicha ordenación*</u> *es la matriz* $|V| \times |V|$ *cuyas entradas* A_{ij} *cuentan el número de aristas que unen* v_i *con* v_j*.*

Definición 67
Sea $G = (V, E)$ *un grafo. Consideremos una ordenación* $v_1, v_2, \ldots, v_{|V|}$ *de los vértices de* G *y una ordenación* $e_1, e_2, \ldots, e_{|E|}$ *de las aristas de* G*. La* **matriz de incidencia** *de* G <u>*asociada a dichas ordenaciones*</u> *es la matriz* $|V| \times |E|$ *con entradas*

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

Isomorfismos

Importante: No confundir un grafo con su representación gráfica.

Definición 68
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* $f : V_1 \to V_2$ *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**.

Caminos en un grafo

Definición 69
Un **camino** *en un grafo* $G = (V, E)$ *es una secuencia alternada de vértices y aristas de la forma* $v_0, \{v_0, v_1\}, v_1, \{v_1, v_2\}, v_2, \ldots, v_{\ell-1}, \{v_{\ell-1}, v_\ell\}, v_\ell$*. 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 70
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 $v_0, v_1, \ldots, v_\ell$ *son distintos (excepto quizás*

Número de caminos entre dos vértices

Teorema 71 *Sea un grafo G con matriz de adyacencia A con respecto al orden $\{v_1, v_2, \ldots, v_{|V|}\}$. 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 72 *Sea G un grafo simple con matriz de adyacencia A, entonces*

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

Grafos conexos

Definición 73
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 un camino elemental que los une.

Definición 74
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* **puente** *de un grafo G es una arista tal que si la eliminamos (pero*

Tema 4: Teoría de grafos II

1. Nociones generales:
   - Notación y definiciones básicas.
   - Representación de grafos.
   - Isomorfismo.
   - Caminos en grafos.
   - Árboles.
   - Grafos planos.
   - Grafos dirigidos.
2. Algoritmos en teoría de grafos.
3. Problemas combinatorios en grafos.

Árboles

Definición 75
*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.*

Teorema 76

(a) *El grafo G es un árbol si y sólo si es conexo y al borrar cualquier arista se obtiene un grafo disconexo.*

(b) *El grafo G es un árbol si y sólo si no contiene ciclos y al añadir cualquier arista se crea un ciclo.*

Teorema 77 *Un grafo $G = (V, E)$ es un árbol si y sólo si existe un único camino elemental*

Propiedades de los árboles

Definición 79
Procedimiento para hacer crecer un árbol:

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

Teorema 80 *Todo grafo obtenido por este procedimiento es un árbol y todo árbol se puede construir de este modo.*

Teorema 81 *Todo árbol de n vértices tiene $n - 1$ aristas.*

Teorema 82 *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.*

Grafos planares

Definición 83
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**.

Teorema 84 (Kuratowsky, 1930) *Un grafo es planar si y sólo si no contiene como subgrafo a ninguna subdivisión de K_5 ni de $K_{3,3}$.*

Definición 85
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.*

Grafos planares y grafos duales

Teorema 86 (Fórmula de Euler, 1752) *Un grafo $G = (V, E)$ plano y conexo divide al plano en R regiones de manera que*

$$|V| - |E| + R \;=\; 2\,.$$

Definición 87
Dado un grafo $G = (V, E)$ plano, podemos construir su **grafo dual** $G^\star = (V^\star, E^\star)$ *de la siguiente manera: introducimos un vértice del grafo dual $r \in V^\star$ por cada región r en la que G divide al plano. Los vértices $r_1, r_2 \in V^\star$ tienen tantas aristas incidentes $e \in E^\star$ como aristas comparten las regiones r_1, r_2 definidas por el grafo G.*

Definición 88
El **grado de una región** r *de un grafo plano se define como el grado del vértice correspondiente $r \in V^\star$ en el grafo dual.*

Teorema 89 *En un grafo plano y conexo se cumple que*

$$2|E| \;=\; \textit{Suma de los grados de las regiones}\,.$$

Algunos corolarios

Corolario 90 *Si G es un grafo simple, conexo y plano con $|V| \geq 3$, entonces $|E| \leq 3|V| - 6$.*

Corolario 91 *Si G es un grafo simple, conexo y plano con $|V| \geq 3$ y no tiene ciclos de longitud 3, entonces $|E| \leq 2|V| - 4$.*

Grafos orientados o dirigidos

Definición 92
Un **grafo dirigido** $G = (V, E)$ *está compuesto por un conjunto no vacío de* **vértices** V *y un conjunto de* **aristas** E*, que es un conjunto* ordenado *de pares de elementos distintos de* V.

Definición 93
El **grado interno** *de un vértice* v *de un grafo dirigido* G *es el número de aristas que llegan a* v. *El* **grado externo** *de un vértice* v *de un grafo dirigido* G *es el número de aristas que salen de* v.

Proposición 94 *En un grafo dirigido* $G = (V, E)$ *la suma de los grados internos de los vértices es igual a la suma de los grados externos.*

Definición 95
Sea $G = (V, E)$ *un grafo dirigido. Consideremos una ordenación* $v_1, v_2, \ldots, v_{|V|}$ *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 comienzan en* v_i *y acaban en* v_j.

Caminos en un grafo dirigido

Definición 96
Un **camino** *en un grafo dirigido* $G = (V, E)$ *es una sucesión de aristas de la forma* $(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell)$.

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

Tema 5: Teoría de grafos III

1. Nociones generales.
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.

Árbol generador de peso mínimo

Definición 97
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 98
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 99
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.*

quel que en cada paso toma la elección óptima.

Algoritmo de Prim, 1957

Algoritmo 101 (Algoritmo de Prim)

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

T = *arista con peso mínimo*

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

begin

  e = *arista de peso mínimo incidente con un vértice de* T

   y que no forme un ciclo si se le añade a T

  $T = T$ *con la arista* e *añadida*

end

Notas:

- La arista e puede no ser única.
- El árbol generador de peso mínimo puede no ser único.
- El resultado es un árbol con n vértices, luego tiene que tener $n - 1$ aristas.

Teorema 102 *Dado un grafo conexo ponderado $G = (V, E)$, el algoritmo de Prim produce un árbol generador mínimo de G. Su complejidad computacional es $O(|E| + |V| \log |V|)$.*

Algoritmo de Kruskal, 1957

Algoritmo 103 (Algoritmo de Kruskal)

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

T = *grafo vacío*

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

begin

  e = *arista de peso mínimo que no forme un ciclo si se le añade a* T

  $T = T$ *con la arista* e *añadida*

end

Notas:

- La arista e puede no ser única.

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 ($\omega_i > 0$ para todo $i \in E$).

Teorema 105 *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 $O(|V|^2)$.*

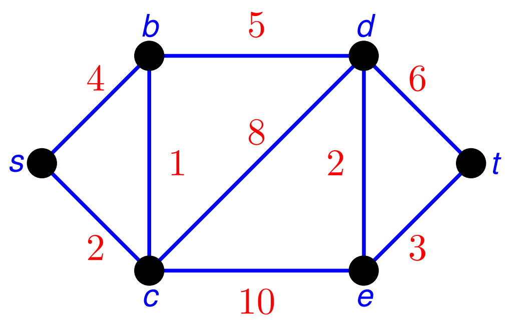
Idea:
En cada iteración a cada vértice j se le asignan dos etiquetas que pueden ser o bien temporales (δ_j, P_j) o bien permanentes $\boxed{(\delta_j, P_j)}$.

- La etiqueta δ_j es una estimación de la longitud del camino mínimo desde el vértice inicial s hasta el vértice actual 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 $\{i, j\} \in E$.

El algoritmo de Dijkstra

Problema 3
Calcular el camino de menor longitud entre s y t en el siguiente grafo:



El algoritmo de Dijkstra (2)

(1) Paso inicial: Marcamos el origen s con la etiqueta permanente $\boxed{(0, s)}$.
El resto de los vértices $j \in V$ $(j \neq s)$ se marcan temporalmente:

- Si $\{j, s\} \in E$, se marca con $(\omega_{s,j}, s)$.
- Si $\{j, s\} \notin E$, se marca con $(\infty, -)$.

(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 $\boxed{\delta_v} + \omega_{v,j}$.

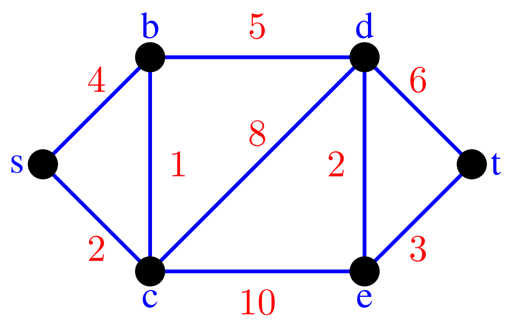
- Si $\boxed{\delta_v} + \omega_{v,j} < \delta_j$, cambiamos (δ_j, P_j) por $(\boxed{\delta_v} + \omega_{v,j}, v)$.
- Si $\boxed{\delta_v} + \omega_{v,j} \geq \delta_j$, no hacemos nada.

(3) De entre todos los vértices temporales j examinados, elegimos aquél cuya δ_j sea mínima δ_{min}.

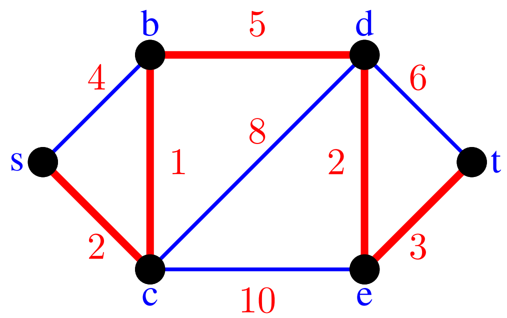
- Si $\delta_{\text{min}} = \infty$ el algoritmo termina: no hay camino entre s y t.
- Si $\delta_{\text{min}} < \infty$, marcamos dicho vértice con etiqueta permanente.
  (Esta estimación sólo puede empeorar porque $\omega_{ij} > 0$).

(4) Si el vértice marcado es t, el algoritmo termina: el camino más corto entre s y t se obtiene siguiendo las etiquetas permanentes.
Si no es t, volver al paso (2).

El algoritmo de Dijkstra: Ejemplo



El algoritmo de Dijkstra: Ejemplo



Vértice	Paso 1	Paso 2	Paso 3	Paso 4	Paso 5	Paso 6
s	$\boxed{(0, s)}$	$\star$	$\star$	$\star$	$\star$	$\star$
b	$(4, s)$	$(3, c)$	$\boxed{(3, c)}$	$\star$	$\star$	$\star$
c	$(2, s)$	$\boxed{(2, s)}$	$\star$	$\star$	$\star$	$\star$
d	∞	$(10, c)$	$(8, b)$	$\boxed{(8, b)}$	$\star$	$\star$
e	∞	$(12, c)$	$(12, c)$	$(10, d)$	$\boxed{(10, d)}$	$\star$
t	∞	∞	∞	$(14, d)$	$(13, e)$	$\boxed{(13, e)}$

Tema 6: Teoría de grafos IV

1. Nociones generales.
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.

Coloraciones propias de un grafo

Definición 106
Una **coloración propia** *(con q colores) de un grafo $G = (V, E)$ es una función $c : V \to \{1, 2, \ldots, q\}$ 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 cómo mínimo para poder colorear G?

Definición 107
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 108 *Decidir si los vértices de un grafo arbitrario G se pueden colorear propiamente con $k \geq 3$ colores es un problema NP–completo.*

Algoritmo voraz para colorear un grafo

Algoritmo 109 (Algoritmo voraz)
procedure *(G: grafo simple conexo con n vértices)*
Ordenamos los vértices de V: $\{v_1, v_2, \ldots, v_n\}$
$c(v_1) = 1$
for $i = 2$ **to** n
begin
  $S_i = \{q \mid c(v_k) = q$ *, para todo v_k vecino de v_i con $k < i$*$\}$
  $c(v_i) =$ *color más pequeño que no esté en S_i*
end

Notas:

Algunos teoremas

Teorema 110 *Si G es un grafo con grado máximo k, entonces $\chi(G) \leq k+1$.*

Teorema 111 (Brooks, 1941) *Si G es un grafo no completo, conexo y con grado máximo $k \geq 3$, entonces $\chi(G) \leq k$.*

Proposición 112 *Un grafo G es bipartito si y sólo si $\chi(G) = 2$.*

Teorema 113 *Un grafo es bipartito si y sólo si no contiene ciclos de longitud impar.*

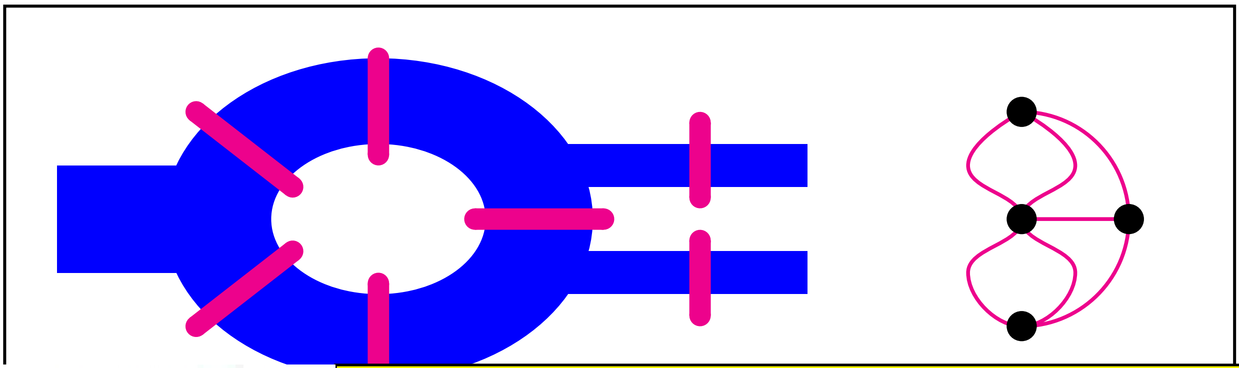
Corolario 114 *Todos los árboles son bipartitos*

Teorema 115 (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.

Grafos eulerianos

Problema 4
En la ciudad de Königsberg (Kaliningrado) hay un río y siete puentes. ¿Es posible dar una vuelta y cruzar cada puente una sola vez?



Grafos eulerianos

Definición 116
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 117 *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.

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 $C_0 = \{v_0\}$.

(2) Extensión del circuito: Sea el circuito $C_i = \{v_0, e_1, v_1, \ldots, e_i, v_i\}$ donde $v_i \in V$ y $e_i \in E$.

- Si existe una única arista $e_{i+1} = \{v_i, w\} \in E \setminus \{e_1, e_2, \ldots, e_i\}$:
  - $C_i \to C_{i+1} = \{v_0, e_1, v_1, \ldots, e_i, v_i, e_{i+1}, w\}$
  - $V \to V \setminus \{v_i\}$
  - $E \to E \setminus \{e_{i+1}\}$
- Si hay varias aristas incidentes con v_i: elegimos cualquiera de ellas con la condición que **no** sea **puente**. Si escogemos

Grafos hamiltonianos

Problema 6
¿Es posible encontrar un ciclo en G tal que pase por todos los vértices (una sola vez)?

Definición 118
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 119 (Dirac, 1950) *Si G es un grafo simple con n vértices y cada vértice tiene un grado $\geq n/2$, entonces G es hamiltoniano.*

El problema del viajante

Problema 7
Un viajante tiene que cubrir n ciudades interconectadas todas entre sí. Su objetivo es salir de su casa, visitarlas todas una sola vez y volver a su casa al finalizar de manera que la distancia recorrida sea mínima.

Este problema consiste en encontrar entre todos los ciclos hamiltonianos del grafo ponderado $K_n = (V_n, E_n, \omega)$ uno C que minimice la función

$$E(C) = \sum_{e \in V(C)} \omega_e \, .$$

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.

Patrones de conteo: repartos

Proposición 120 (Repartos) *Si hay que repartir r objetos iguales en n grupos y todos los grupos deben de contar con algún objeto, entonces existen*

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

repartos distintos.

Proposición 121 *Si hay que repartir r objetos iguales en n grupos, entonces existen*

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

Patrones de conteo: particiones de un conjunto

Proposición 122 *Sea un conjunto S de $m \cdot n$ elementos. Entonces S puede romperse en n conjuntos de m elementos de*

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

maneras distintas.

Proposición 123 *El número de particiones de un conjunto de m elementos del tipo $(m_1, m_2, \ldots, m_n)$ con $\sum_k m_k = m$ es*

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

donde r_k es el número de partes con k elementos.

Tema 8: Combinatoria. Métodos avanzados.

1. Relaciones de recurrencia:
   - Relaciones de recurrencia.
   - Solución de relaciones de recurrencia lineales homogeneas.
   - Solución de relaciones de recurrencia lineales no homogeneas.
2. Funciones generatrices.

Relaciones de recurrencia

Definición 124
Una **relación de recurrencia** *para la secuencia* $\{a_n\}_{n=0}^{\infty}$ *es una ecuación que expresa* a_n *en función de uno o más de los términos anteriores; es decir, una ecuación del tipo*

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

con k *fijo y válida para todo* $n \geq k$*. Las condiciones iniciales son los términos* $\{a_0, a_1, \ldots, a_{k-1}\}$.

Definición 125
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}, $\ldots$, a_{n-k}*. En cualquier otro caso, se dice que es* **no lineal**.

Solución de una relación de recurrencia lineal homogenea

Teorema 126 (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_1 *dado. Entonces la solución de la ecuación de recurrencia es*

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

Solución de una relación de recurrencia lineal homogenea

Teorema 127 (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_1 *y* 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*

$$a_n \;=\; \begin{cases} K_1\,\alpha^n + K_2\,\beta^n & \text{si } \alpha \neq \beta \\ (K_1 + nK_2)\,\alpha^n & \text{si } \alpha = \beta \end{cases}$$

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

Solución de una relación de recurrencia lineal homogenea

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

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

  con $c_1, c_2, \ldots, c_k$ reales. Se suponen conocidas las k condicions iniciales a_i con $i = 1, \ldots, k$.
- 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:

Solución de una relación de recurrencia lineal homogenea (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:

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

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

Solución de una relación de recurrencia lineal no homogenea

Teorema 128 (Solución ecuaciones de recurrencia no homogéneas) *Supongamos que la secuencia $\{a_n\}_{n\in\mathbb{N}}$ verifica la relación de recurrencia lineal*

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

con $c_1, c_2, \ldots, c_k$ reales, $a_1, \ldots, a_k$ dados y donde t_n 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

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

y una solución particular cualquiera de la ecuación completa.

Solución de una relación de recurrencia lineal no homogenea

Teorema 129 (Solución ecuaciones lineales no homogéneas) *Supongamos que la secuencia $\{a_n\}_{n\in\mathbb{N}}$ verifica la relación de recurrencia lineal*

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

con $c_1, c_2, \ldots, c_k$ reales y

$$t_n = s^n \left[b_0 + b_1 n + \ldots + b_t n^t\right] ,$$

con $b_0, b_1, \ldots, b_t$ y 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

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

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

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

Tema 9: Combinatoria. Métodos avanzados.

1. Relaciones de recurrencia.
2. Funciones generatrices.
   - Funciones generatrices.
   - Solución de relaciones de recurrencia usando funciones generatrices.

Función generatriz

Definición 130

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

$$F(x) \;=\; a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots \;=\; \sum_{n=0}^{\infty} a_n\, x^n\,.$$

- $(1+x)^k = \sum_{n=0}^{k} \binom{k}{n} x^n$ es la f.g. de $\left\{\binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k}, 0, 0, \ldots\right\}$.
- $1 + x + x^2 + \ldots + x^{k-1} = \sum_{n=0}^{k-1} x^n = \dfrac{1-x^k}{1-x}$ es la f.g. de $\{\underbrace{1, 1, \ldots, 1}_{k}, 0, 0, \ldots\}$.
- $\dfrac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots = \sum_{n=0}^{\infty} x^n$ es la f.g. de $\{1, 1, 1, \ldots\}$.

Función generatriz

- $\{1, 2, 3, \ldots\}$ 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 $\{\underbrace{0, 0, \ldots, 0}_{k}, a_0, a_1, \ldots\}$ es $G(x) = x^k F(x)$.

Ejemplo: la ecuación de Fibonacci

Queremos resolver la ecuación

$$a_n = a_{n-1} + a_{n-2}, \quad n \geq 3, \quad a_1 = 1, \quad a_2 = 1$$

mediante la función generatriz

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

Algoritmo:

1. Escribir la fórmula general para a_n válida para todo $n \in \mathbb{Z}$ asumiendo que $a_0, a_{-1}, a_{-2}, \ldots = 0$:

$$a_n = a_{n-1} + a_{n-2} + I[n = 1], \quad n \in \mathbb{Z},$$

donde $I[A]$ es la función indicatriz del suceso A

$$I[A] = \begin{cases} 1 & \text{si } A \text{ es verdadero} \\ 0 & \text{si } A \text{ es falso} \end{cases}$$

Ejemplo: la ecuación de Fibonacci

2. Multiplicar por x^n y sumar sobre todo $n \in \mathbb{Z}$:

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

Manipulamos la sumas para que sólo aparezca F:

$$F(x) - x = \sum_{n=-\infty}^{\infty} x^n (a_{n-1} + a_{n-2})$$

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

$$1 - x - x^2$$

Ejemplo: la ecuación de Fibonacci

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

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

Podemos obtener los coeficientes mediante un poco de álgebra:

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

Teorema del binomio generalizado

Teorema 131 *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

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

Tema 10: Teoría de grafos V

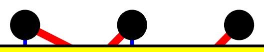
1. Nociones generales.
2. Algoritmos en teoría de grafos:
3. Problemas combinatorios en grafos:
   - Emparejamiento en grafos.
   - Coloraciones propias en grafos.

Emparejamientos en grafos

Definición 132
Un **emparejamiento completo o perfecto** *de un grafo 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:



Coloraciones propias: polinomio cromático

Definición 134
Sea $G = (V, E)$ un grafo simple y sea $q \geq 2$ un número entero. El polinomio cromático P_G es un polinomio tal que $P_G(q)$ nos dice el número de coloraciones propias con q colores que admite el grafo G.

P_G es un polinomio en q ya que

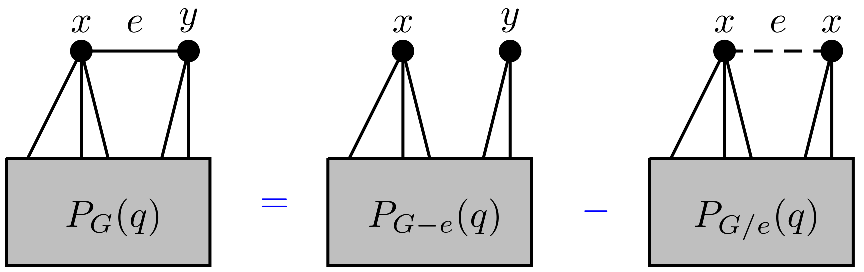
- Si $G = (\{v\}, \emptyset)$, $P_G(q) = q$.
- Se cumple el teorema de contracción-borrado:

Teorema 135 (Teorema de contracción-borrado) *Si $G = (V, E)$ es un grafo simple y $e = xy \in E$ 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 $e = xy$ y G/e es el grafo que se obtiene al contraer la arista $e = xy$ (identificando los vértices x e y y eliminando posibles multi-aristas).

Demostración del Teorema de contracción-borrado



■

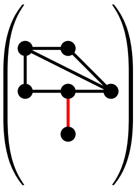
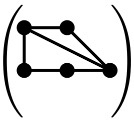
Teorema 136 *Si G es un grafo no conexo con dos componentes conexas G_1 y G_2, entonces $P_G(q) = P_{G_1}(q) \times P_{G_2}(q)$.*

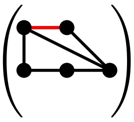
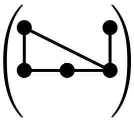
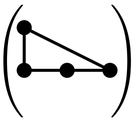
Ejemplo

Problema 8

En el congreso Lattice'06 hay seis conferencias de una hora programadas para el día inaugural $\{c_1, c_2, \ldots, c_6\}$*. 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  $= (q-1) \times P$ 

P  $= P$  $- \; P$  $= (q-2)P_{C_4}(q)$

$$\begin{aligned} P_G(q) &= (q-1)(q-2)P_{C_4}(q) \quad [P_{C_4}(q) = q(q-1)(q^2-3q+3)] \\ &= q(q-1)^2(q-2)(q^2-3q+3)\,. \\ \chi(G) &= 3\,. \end{aligned}$$

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.

Relaciones binarias entre dos conjuntos

Definición 138
Una **relación binaria** $\mathcal{R}$ *del conjunto* V *al conjunto* W *es un subconjunto del producto cartesiano* $V \times W$*:*

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

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

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

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

$$\mathit{Imag}\,\mathcal{R} \;=\; \{w \in W \mid (v,w) \in \mathcal{R} \quad \text{para algún } v \in V\}\,.$$

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

Relaciones binarias en un conjunto

Definición 139
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:*

$$\mathit{Dom}\,\mathcal{R} \;=\; \{v \in V \mid (v,w) \in \mathcal{R} \quad \text{para algún } w \in V\}$$

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

$$\mathit{Imag}\,\mathcal{R} \;=\; \{w \in V \mid (v,w) \in \mathcal{R} \quad \text{para algún } v \in V\}\,.$$

Observación importante: una función $f\colon\, A \to B$ es una relación entre los conjuntos A

Representación gráfica de una relación

- Representación cartesiana.
- Representación con diagramas de Venn.
- Matriz de adyacencia de $\mathcal{R}$:
  Sean $V = \{v_1, v_2, \ldots, v_{|V|}\}$ y $W = \{w_1, w_2, \ldots, w_{|W|}\}$. 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):
  $$E = \{(v_i, v_j) \in V \times V \mid v_i \mathcal{R} v_j\}.$$

Operaciones con relaciones

Definición 140
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* $v_1 \mathcal{R}^{-1} v_2 \Leftrightarrow v_2 \mathcal{R} v_1$.

Definición 141
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.

Composición de relaciones

Proposición 143 *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.*

Propiedades de las relaciones sobre V

Definición 144
Una relación $\mathcal{R}$ es **reflexiva** *si para todo $v \in V$ se cumple que $v\mathcal{R}v$.*

Definición 145
Una relación $\mathcal{R}$ es **anti-reflexiva** *si para todo $v \in V$ se cumple que $v\overline{\mathcal{R}}v$.*

Definición 146
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 147
Una relación $\mathcal{R}$ es **anti-simétrica** *si $(v_1\mathcal{R}v_2) \wedge (v_2\mathcal{R}v_1) \;\Rightarrow\; v_1 = v_2$.*

Relaciones transitivas

Definición 148
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 149 *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:*

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

Corolario 150 *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 $(A_{\mathcal{R}})_{i,j} = 1$.*

Relaciones de equivalencia

Definición 151
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

$$a \equiv b \pmod{\mathcal{R}}.$$

Definición 152
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*

Conjunto cociente

Teorema 153 *Sea $\mathcal{R}$ una relación de equivalencia sobre V. Entonces dos clases de equivalencia de $\mathcal{R}$ o bien son iguales o bien son disjuntas. Es decir:*

(1) $[a] = [b] \;\Leftrightarrow\; a\mathcal{R}b$

(2) $[a] \neq [b] \;\Rightarrow\; [a] \cap [b] = \emptyset$

Teorema 154 *Sea $\mathcal{R}$ una relación de equivalencia sobre V. Entonces dicha relación determina una partición del conjunto V.*

Teorema 155 *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 $\{V_1, V_2, \ldots\}$ de V, existe una relación de equivalencia $\mathcal{R}$ tal que sus clases de equivalencia son los conjuntos V_i.*

Definición 156
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 A por $\mathcal{R}$** *y de denota por $V/\mathcal{R}$:*

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

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.

Aritmética entera: Recordatorio del tema 1

Definición 157
Dados dos enteros $a \neq 0$ y b, se dice de $\boldsymbol{a}$ **divide a** $\boldsymbol{b}$ *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* $\boldsymbol{a \mid b}$ *y si a no divide a b, por* $\boldsymbol{a \nmid b}$.

Observaciones:

- Cualquier entero $a \in \mathbb{Z}$ 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 158 (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*

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

Propiedades de la división de enteros

Teorema 159 *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 160 *Si $a \mid b_i$ para $i = 1, \ldots, N$, entonces $a \mid \sum^{N} y_i \cdot b_i$ para todo $y_i \in \mathbb{Z}$.*

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

Definición 161
Dados dos enteros $a, b \neq 0$, *se denomina* **máximo común divisor** *de* a *y* b *[denotado por* $\mathrm{mcd}(a,b)$*] al* *<u>mayor</u>* *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 162 *El máximo común divisor de dos números enteros es único.*

Lema 163 (Euclides) *Sea* $a = q \cdot b + r$, *donde* $a, b \neq 0$, q *y* r *son enteros. Entonces* $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r)$.

Algoritmo de Euclides

Problema 9
Aplicar el Lema de Euclides de manera recursiva para calcular $\mathrm{mcd}(662, 414)$.

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

$$\mathrm{mcd}(662, 414) = \mathrm{mcd}(414, 248) = \mathrm{mcd}(248, 166) = \mathrm{mcd}(166, 82)$$

Identidad de Bezout

Teorema 165 (Identidad de Bezout, 1730-1783) *Si a y b son enteros (no nulos simultaneamente), existen enteros u, w tales que*

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

PROOF. Si escribimos los pasos del Algoritmo de Euclides

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

Luego, $\operatorname{mcd}(a,b) = r_{n-1} = \alpha_{n-1}r_{n-3} + \beta_{n-1}r_{n-2} = \alpha_{n-2}r_{n-4} + \beta_{n-2}r_{n-3} = \ldots = \alpha_3 r_1 + \beta_3 r_2 = \alpha_2 b + \beta_2 r_1 = \alpha_1 a + \beta_1 b.$ ∎

Identidad de Bezout (2)

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

Teorema 166 *Sean dos números enteros a y b no nulos simultaneamente con $\operatorname{mcd}(a,b) = d$. 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 167 *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 168 *Si $\operatorname{mcd}(a,b) = d$, entonces:*

1. $\operatorname{mcd}(m\cdot a, m\cdot b) = m\cdot d$ *para todo $m \in \mathbb{N}$.*

Mínimo común múltiplo

Definición 170
Dados dos números a, b enteros no nulos, se define el **mínimo común múltiplo** *de a y b [y se denota por $\mathrm{mcm}(a, b)$] 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 171 *Sean $a, b \in \mathbb{N}$ con $d = \mathrm{mcd}(a, b)$ y $m = \mathrm{mcm}(a, b)$. Entonces,*

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

Lema 172 *Sea p un número primo y $a, b \in \mathbb{Z}$. Entonces:*

(a) $p \mid a$ ó p y a son primos entre sí.

(b) Si $p \mid (a \cdot b)$, entonces ó $p \mid a$ ó $p \mid b$.

Ecuaciones diofánticas lineales [Diophantos, s III]

Definición 173
Una **ecuación diofántica** *es una ecuación de una o varias variables y de la que nos interesan sólo sus soluciones enteras.*

Teorema 174 (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 $d = \mathrm{mcd}(a, b)$ divide a c, en cuyo caso existen infinitas soluciones enteras (x_k, y_k) con $k \in \mathbb{Z}$ dadas por

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 175
Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Entonces $\boldsymbol{a}$ **es congruente con** $\boldsymbol{b}$ **módulo** $\boldsymbol{m}$ *si* $m \mid (a - b)$.
Esta relación se denota por $a \equiv b \pmod{m}$.

Proposición 176

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

El conjunto cociente $\mathbb{Z}_m$

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

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

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

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

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

Aritmética modular

Teorema 179 *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 180 *Sean $m, k \in \mathbb{N}$. Si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$.*

Teorema 181 *Sea $m \in \mathbb{N}$ y sean $a, b, c \in \mathbb{Z}$. Si $a \cdot c \equiv b \cdot c \pmod{m}$ y $\mathrm{mcd}(c, m) = 1$, entonces $a \equiv b \pmod{m}$.*

Observación: 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.

División modular: congruencias lineales

Definición 182
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

Congruencias lineales

Teorema 183 *Si $d = \mathrm{mcd}(a, m)$, 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, la solución general viene dada por

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

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

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

Corolario 184 *Si $\mathrm{mcd}(a, m) = 1$ las soluciones x de la congruencia lineal $a \cdot x \equiv b \pmod{m}$ constituyen una única clase de congruencia módulo m.*

Corolario 185 *Si $\mathrm{mcd}(a, m) = 1$ y $m > 1$, entonces existe un inverso de a módulo m. Dicho inverso es único módulo m.*

Aritmética en $\mathbb{Z}_m$

Los elementos de $\mathbb{Z}_m$ con $m \in \mathbb{N}$ son clases de equivalencia módulo m. Luego $x \in \mathbb{Z}_m$ representa que $x = [x]_m$.
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 $x \cdot y = y \cdot x$.

respecto del producto.

Aritmética en $\mathbb{Z}_m$ (2)

En $\mathbb{Z}$ no existe en general el inverso (multiplicativo) de un entero x:

$$y \text{ es el inverso multiplicativo de } x \;\Leftrightarrow\; x \cdot y \;=\; 1\,.$$

Sin embargo, 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 en $\mathbb{Z}_m$.

Definición 186
Un elemento $x \in \mathbb{Z}_m$ es un **divisor de cero** *si es no nulo y $x \cdot x \equiv 0 \pmod{m}$.*

Definición 187
Un elemento $x \in \mathbb{Z}_m$ es una **unidad módulo m** *si es inversible; es decir, si existe otro $s \in \mathbb{Z}_m$ tal que $x \cdot s \equiv 1 \pmod{m}$.*

Teorema 188 *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}.

Aritmética en $\mathbb{Z}_m$ (3)

Teorema 189 *Un elemento $r \in \mathbb{Z}_m$ es inversible si y sólo si r y m son primos entre sí.*

Definición 190
El conjunto de los elementos inversibles en $\mathbb{Z}_m$ se denotará por U_m.

Corolario 191 *Si p es primo, todo elemento de $\mathbb{Z}_p$ distinto de 0 es inversible.*

Notas:

- Si p es primo, entonces $(\mathbb{Z}_p, +, \cdot)$ es un **cuerpo** como $(\mathbb{R}, +, \cdot)$ ó $(\mathbb{Q}, +, \cdot)$.
- Si m es compuesto, entonces si p, q son tales que $p \cdot q = m$, se sigue la existencia

El teorema de Euler

Lema 193 *Si p es primo, $\phi(p) = p - 1$.*

Teorema 194 (Euler, 1790) *Si y es inversible en $\mathbb{Z}_m$ (es decir, si $\mathrm{mcd}(y, m) = 1$), entonces*

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

Corolario 195 (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 196 *Si p es primo, entonces para cualquier entero y se tiene que*

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

Teorema 197

1. *Si p es primo, entonces $\phi(p^k) = p^{k-1}(p-1)$ para todo $k \in \mathbb{N}$.*
2. *Si $\mathrm{mcd}(m, n) = 1$, entonces $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.*

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.

Relación de orden parcial

Definición 198
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 199
Un conjunto V equipado con una relación de orden $\preceq$ se denomina **conjunto parcialmente ordenado** $(V, \preceq)$ *(o poset).*

Definición 200
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***.*

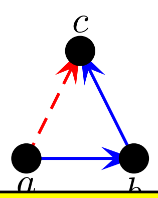
Definición 201
Un conjunto parcialmente ordenado $(V, \preceq)$ está **totalmente ordenado** *cuando cualquier par de elementos $a, b \in V$ son comparables. Se dice entonces que $(V, \preceq)$ es un conjunto* **totalmente ordenado** *(o* **cadena***).*

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:



Elementos extremales

Definición 202
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* $M = v$*. Es decir, no hay ningún elemento por encima de* M*.* $m \in V$ *es un* **elemento minimal** *si para todo* $v \in V$*,* $v \preceq m$ *implica que* $m = v$*. Es decir, no hay ningún elemento por debajo de* m*.*

Definición 203
Sea $(V, \preceq)$ *un conjunto parcialmente ordenado.* $M^\star \in V$ *es un* **elemento máximo** *si* $v \preceq M^\star$ *para todo* $v \in V$*. Es decir,* $M^\star$ *está encima de todos los elementos de* V*.* $m^\star \in V$ *es un* **elemento mínimo** *si* $m^\star \preceq v$ *para todo* $v \in V$*. Es decir,* $m^\star$ *está por debajo de todos los elementos de* V*.*

Nota: Los elementos extremales pueden no existir.

Teorema 204 *El elemento máximo* $M^\star$ *de un conjunto ordenado* A*, si existe, es único. Además todo elemento máximo es maximal.*

Elementos extremales (2)

Definición 205
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 mayor*(B)*.*
$u^\star \in V$ *es el* **supremo** *de* B *si es la menor de las cotas superiores:* $u^\star = \text{mín}(\textit{mayor}(B))$*.*

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

Nota: Los elementos extremales pueden no existir.

Orden total compatible con un orden parcial

Definición 206
Un orden total $\preceq_T$ es **compatible** *con el orden parcial $\preceq_P$ si para todo $v, w \in V$, $v \preceq_P w$ implica que $v \preceq_T w$.*

Algoritmo 207 (Ordenación topológica)
procedure *TotalOrder($(V, \preceq_P)$: conjunto finito parcialmente ordenado)*
$k = 1$
while $V \neq \emptyset$
begin
  v_k = *un elemento minimal de* $(V, \preceq_P)$
  $V \to V \setminus \{v_k\}$
  $k \to k + 1$
end

$v_1 \preceq_T v_2 \preceq_T \ldots \preceq_T v_n$ es un orden total compatible con $\preceq_P$

Conjunto bien ordenado

Definición 208
$(V, \preceq)$ es un **conjunto bien ordenado** *si $\preceq$ es un orden total y cualquier subconjunto no vacío de V tiene siempre un mínimo.*

Observación: 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 principio de inducción para los naturales

Definición 209 (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) $P(k+1)$ es cierta siempre que $P(k)$ sea cierta (para cualquier k arbitrario pero fijo).

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

Definición 210 (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) $P(k+1)$ es cierta siempre que $P(m)$ sea cierta para todo $m \leq k$ (con k arbitrario pero fijo).

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

Principio de inducción para conjuntos bien ordenados

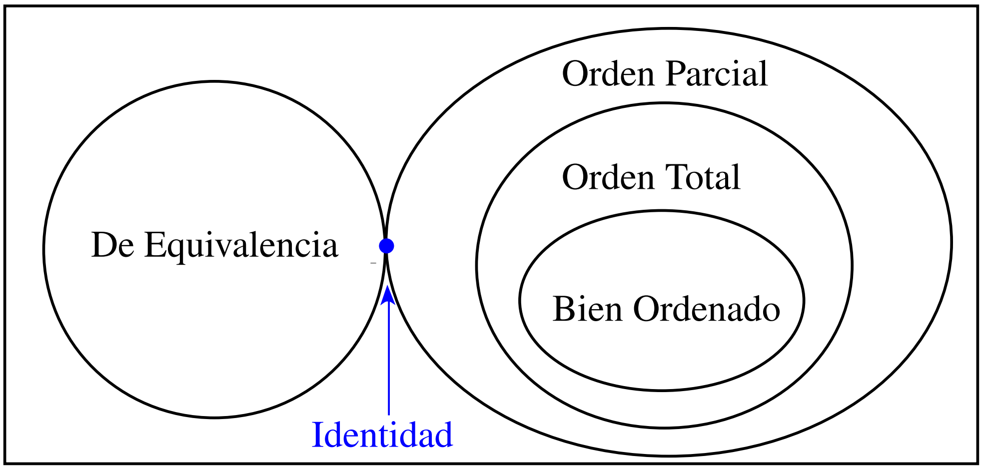
Proposición 211 (Principio de inducción para conjuntos bien ordenados) *Sea $(V, \preceq)$ un conjunto bien ordenado. Entonces, la propiedad P se cumple para todos los elementos de V si y sólo si se satisfacen las condiciones:*

1. *Paso base: $P(v_0)$ es verdadera para el mínimo de V.*
2. *Paso de inducción: si $P(w)$ es verdadera para todo $w \prec v$, entonces $P(v)$ es verdadera.*

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



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

Retículo

Definición 212
*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 $\inf(a, b) = \min(a, b)$.

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; de manera que supremo e ínfimo se intercambian.

Corolario 213 (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.

Propiedades de los retículos

Proposición 214 *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. $\sup(a, \text{ínf}(a, b)) = a \vee (a \wedge b) = a$ *[absorción]*

Por dualidad se obtiene:

Corolario 215 *Si $(A, \preceq)$ es un retículo, entonces para cualquier $a, b, c \in A$:*

1. $\text{ínf}(a, a) = a \wedge a = a$ *[idempotencia]*
2. $\text{ínf}(a, b) = a \wedge b = b \wedge a = \text{ínf}(b, a)$ *[conmutatividad]*
3. $\text{ínf}(a, \text{ínf}(b, c)) = a \wedge (b \wedge c) = (a \wedge b) \wedge c = \text{ínf}(\text{ínf}(a, b), c)$ *[asociatividad]*
4. $\text{ínf}(a, \sup(a, b)) = a \wedge (a \vee b) = a$ *[absorción]*

Propiedades de los retículos (2)

Proposición 216 *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. $\text{ínf}(a, b) = a \wedge b = a$

Proposición 217 (Propiedad isotónica) *Si $(A, \preceq)$ es un retículo, entonces para cualquier $a, b, c \in A$ se cumple que si $b \preceq c$, entonces*

1. $\sup(a, b) = a \vee b \preceq a \vee c = \sup(a, c)$
2. $\text{ínf}(a, b) = a \wedge b \preceq a \wedge c = \text{ínf}(a, c)$

Propiedades de los retículos (3)

Proposición 219 (Desigualdad modular) *Si* $(A, \preceq)$ *es un retículo, entonces para cualquier* $a, b, c \in A$ *las siguientes afirmaciones son equivalentes:*

1. $a \preceq c$
2. $\sup(a, \text{ínf}(b, c)) = a \vee (b \wedge c) \preceq (a \vee b) \wedge c = \text{ínf}(\sup(a, b), c)$

Los retículos como sistemas algebraicos

Definición 220
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.

Subretículos

Definición 221
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.

Retículos acotados

Definición 222
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 $a \in A$,
  - $\sup(a, 1) = a \vee 1 = 1$.
  - $\text{ínf}(a, 1) = a \wedge 1 = a$.
  - $\sup(a, 0) = a \vee 0 = a$.
  - $\text{ínf}(a, 0) = a \wedge 0 = 0$.
- La cota superior 1 es el elemento neutro de la operación $\wedge$: $a \wedge 1 = a$ y el cero de

está acotado: $1 = \sup(a_1, \ldots, a_n)$ y $0 = \inf(a_1, \ldots, a_n)$.

Retículos distributivos

Definición 223
Un retículo $(A, \preceq)$ *es un* **retículo distributivo** *si para todo* $a, b, v \in A$*,*

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

- Esto es algo más que la propiedad distributiva:

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

Retículos complementados

Definición 224
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 un elemento complementario de b, éste es un elemento complementario de a.
- Un elemento $a \in A$ puede no tener complementario o tener varios elementos complementarios.
- El único elemento complementario a 1 es 0 y viceversa.

Álgebra de Boole

Proposición 226 *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 $\overline{a}$.

Definición 227 (Definición 1)
Un **álgebra de Boole** *es un retículo $(A, \vee, \wedge, 0, 1)$ distributivo y complementado.*

Álgebra de Boole (2)

Definición 228 (Definición 2)
Si B es un conjunto no vacío que contiene al menos dos elementos distintos $0, 1$ y sobre el que definimos las siguientes operaciones:

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

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]*

Álgebra de Boole (3)

- 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 booleana $\cdot$ 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:

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

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

Álgebra de Boole (4)

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

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

dónde $B, C \subseteq A$.

- 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
  - $1 = A$

Propiedades de un álgebra de Boole

Proposición 229 *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 230
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 231 *El dual de un teorema en un álgebra de Boole es también un teorema.*

Definición 232
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 $+, \cdot, \overline{\ }$.*

Expresiones booleanas

Definición 233
Una **expresión booleana** *de n variables booleanas $x_1, \ldots, x_n$ es una cadena finita de símbolos formada recursivamente de la siguiente manera:*

1. *$0, x_1, \ldots, x_n, 1$ son expresiones booleanas.*
2. *Si E_1 y E_2 son expresiones booleanas, $E_1 + E_2$ y $E_1 \cdot E_2$ también lo son.*
3. *Si E es una expresión booleana, $\overline{E}$ también lo es.*

- Una expresión booleana de n variables $x_1, \ldots, x_n$ no tiene porqué contener cada una de las n variables x_i o sus complementarias $\overline{x}_i$.
- Una **literal** es una variable o su complementaria.

Funciones booleanas

Definición 234
Si $x_1, \ldots, x_n$ *son expresiones booleanas, una* **función booleana** *es una función* $f\colon \{x_1, \ldots, x_n\} \to \{0, 1\}$.

- Los valores de una función booleana $f\colon \{x_1, \ldots, x_n\} \to \{0, 1\}$ para los 2^n posibles valores de las variables x_i se suelen presentar en forma de **tablas de verdad** de la función f.

Definición 235
Un **mini-término** *de* n *variables booleanas es un producto booleano de las* n *literales en el que cada literal aparece exactamente una vez. Un* **maxi-término** *de* n *variables booleanas es una suma booleana de las* n *literales en las cuales cada literal aparece exactamente una vez. Cuando una función booleana se expresa como suma de mini-términos recibe el nombre de* **suma de expansión de productos** *y se dice que está en su* **forma normal disyuntiva**. *Cuando una función booleana se expresa como producto de maxi-términos recibe el nombre de* **producto de expansión de sumas** *y se dice que está en su* **forma normal conjuntiva**. *Una función booleana expresada en su formas normales conjuntiva o disyuntiva se dice que está en* **forma canónica**.

Funciones booleanas (2)

Dadas las variables booleanas a, b,

- Los posibles mini-términos son ab, $\overline{a}b$, $a\overline{b}$ y $\overline{a}\overline{b}$.
- Los posibles maxi-términos son $a + b$, $\overline{a} + b$, $a + \overline{b}$ y $\overline{a} + \overline{b}$.

Sea una función booleana $f\colon \{x_1, \ldots, x_n\} \to \{0, 1\}$. Dada su tabla de verdad

- Encontramos su forma normal disyuntiva buscando en la tabla de verdad aquellos valores de las variables para los cuales $f = 1$. La forma normal disyuntiva se obtiene sumando los mini-términos correspondientes a los literales de manera que las variables que toman el valor 1 se sustituyen por el literal x_i y las que toman el valor 0 se sustituyen por el literal $\overline{x}_i$.

Formas canónicas de una función booleana

Sea una función booleana $f\colon \{x,y,z\} \to \{0,1\}$ dada por la tabla de verdad:

x	y	z	$f(x,y,z)$
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

- Forma normal disyuntiva
  $f(x,y,z) = x\cdot y\cdot \overline{z} + x\cdot \overline{y}\cdot z + x\cdot \overline{y}\cdot \overline{z}$.
- Forma normal conjuntiva
  $f(x,y,z) = (\overline{x}+\overline{y}+\overline{z})\cdot(x+\overline{y}+\overline{z})\cdot(x+\overline{y}+z)\cdot(x+y+\overline{z})\cdot(x+y+z)$.
- Aplicación: diseño de puertas lógicas en ordenadores: puertas OR, AND y NOT.