uc3m | Universidad Carlos III de Madrid

ESCUELA POLITÉCNICA 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 2020–2021

Grupo de Modelización, Simulación Numérica y Matemática Industrial

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

v1.1: Junio 2019

Aviso importante

Estas notas son sólamente 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

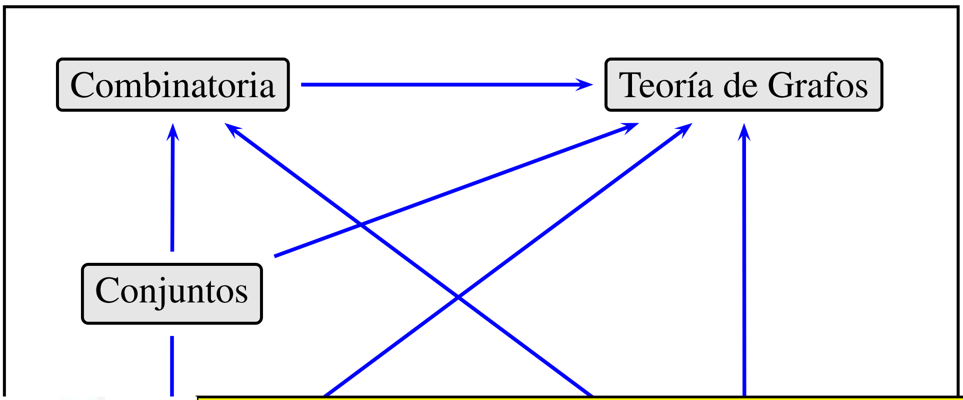
Curso 2019–2020

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.
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** X *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, $x \notin X$.*

El orden de los elementos de un conjunto es irrelevante, así como el número de veces

aquel que contiene todos los elementos de la clase que estemos 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:

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

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

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

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

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:
  - Números enteros: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.
  - Números racionales: $\mathbb{Q} = \left\{ \frac{p}{q} \colon p, q \in \mathbb{Z}, q \neq 0 \right\}$. 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 (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 Dom(f) y al conjunto Y se le denomina **codominio** de f. La **imagen** de la función f es el conjunto*

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

- 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 $f\colon X \to Y$, 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** $f^{-1}\colon Y \to X$ a través de la regla (bien definida)

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

Dadas dos funciones $f\colon X \to Y$, $g\colon Y \to Z$, es posible definir una nueva función $g \circ f\colon X \to Z$ 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.

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*

... nulo $a \in \mathbb{Z}$ se divide a sí mismo: $a = a \cdot 1$ $(q = 1)$.

Algoritmo de divisibilidad

Teorema 12 (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*

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

- 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 $\lceil x \rceil \geq x$.

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 <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 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 <u>menor número natural</u> m tal que $a \mid m$ y $b \mid m$.*

$1 \leq i < j \leq n.$

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

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**

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

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

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 $f : A \to B$.

Definición 23
Un conjunto que tiene un número finito de elementos o cuyo cardinal es igual al de $\mathbb{N}$ se denomina numerable.

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)

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 $A_1, A_2, \ldots, A_m$ son conjuntos finitos y disjuntos dos a dos, se tiene que:*

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

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* $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1.$

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*

$$\binom{n}{n_1, n_2, \ldots, n_k} \equiv \frac{n!}{n_1! n_2! \cdots n_k!}, \quad \text{con} \quad \sum^{k} n_i = n.$$

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.*

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

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

Números combinatorios: triángulo de Pascal

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

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

$$a \searrow \quad \swarrow b$$
$$a+b$$

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)

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

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*

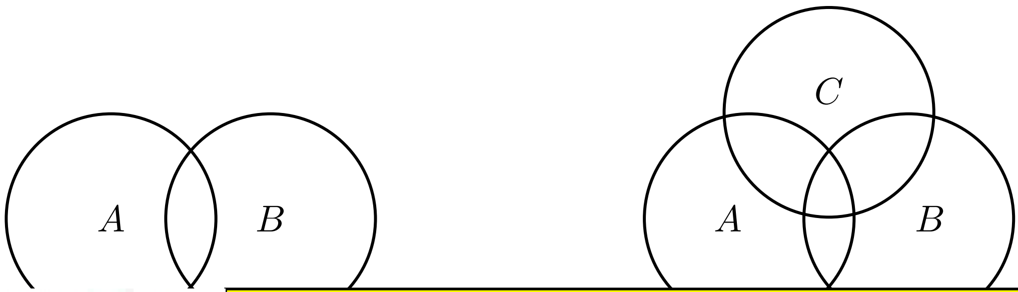
$$\binom{m+n}{k} \; = \; \sum_{q=0}^{k} \binom{m}{k-q}\binom{n}{q}\,.$$

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

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:

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

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.

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* $\gamma\colon E \to \{\{a, b\}\colon a, b \in V\}$.

- 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.*

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

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

Definición 51
Los vértices de grado 1 se denominan **terminales***. Los vértices de grado 0 se denominan*

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.*

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.

Grafos complementarios y subgrafos. Representación de un grafo

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* $F \subseteq E$.

Definición 61
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 *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.

Isomorfismos

Importante: No confundir un grafo con su representación gráfica.

Definición 62
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**.

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

Caminos en un grafo

Definición 63
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 64
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 los extremos v_0 y v_ℓ) se denomina **camino elemental**. *Un camino elemental cerrado es un* **ciclo**.

Número de caminos entre dos vértices

Teorema 65 *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 66 *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 67
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 68
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 no los vértices con los que es incidente) obtenemos un grafo con más componentes conexas que* G.

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.

Árboles

Definición 69
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 70

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

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

Teorema 72 *Todo árbol con al menos dos vértices tiene al menos dos vértices de grado uno.*

Propiedades de los árboles

Definición 73
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 74 *Todo grafo obtenido por este procedimiento es un árbol y todo árbol se puede construir de este modo.*

Teorema 75 *Todo árbol de n vértices tiene $n - 1$ aristas.*

Grafos planares

Definición 77
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 78
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 79 (Kuratowsky, 1930) *Un grafo es planar si y sólo si no contiene como subgrafo a ninguna subdivisión de K_5 ni de $K_{3,3}$.*

Grafos planares y grafos duales

Teorema 80 (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 81
Dado un grafo $G = (V, E)$ plano, su **grafo dual** *$G^\star = (V^\star, E^\star)$ se define de la siguiente*

Algunos corolarios sobre planaridad

Definición 82
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. El grado de la región* r *lo denotaremos por* d_r.

Teorema 83 *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 84 *Si* G *es un grafo simple, conexo y planar con* $|V| \geq 3$*, entonces* $|E| \leq 3|V| - 6$.

Corolario 85 *Si* G *es un grafo simple, conexo y planar con* $|V| \geq 3$ *y no tiene ciclos de longitud* 3*, entonces* $|E| \leq 2|V| - 4$.

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.

Árbol generador de peso mínimo

Definición 86
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 87
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 88
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 89
Un **algoritmo voraz** *es aquel que en cada paso toma la elección óptima.*

Algoritmo de Prim, 1957

Algoritmo 90 (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:

Algoritmo de Kruskal, 1957

Algoritmo 92 (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 $(i = 1, \ldots, n-1)$ puede no ser única.
- En cada paso, T_i es un bosque $(1 \leq i \leq n-1)$.

Teorema 93 *Dado un grafo conexo ponderado $G = (V, E, \omega)$, el algoritmo de Kruskal produce un árbol generador mínimo de G.*

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 94 *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.*

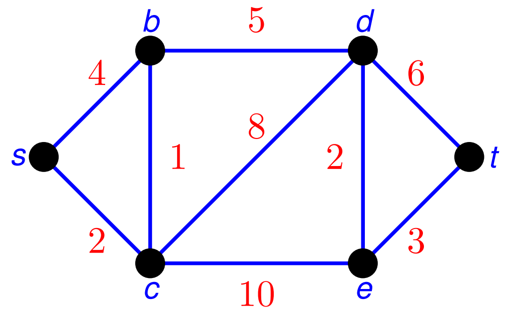
Idea:

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 $\boxed{(\delta_j, P_j)}$

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 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 $\delta_v + \omega_{v,j}$:

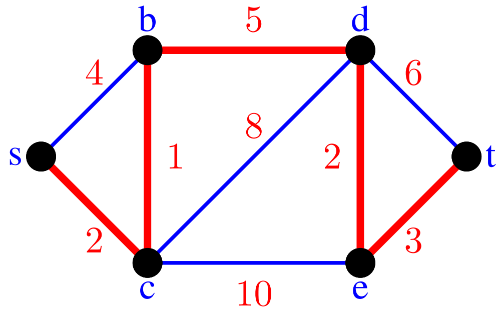
- Si $\delta_v + \omega_{v,j} < \delta_j$, cambiamos (δ_j, P_j) por $(\delta_v + \omega_{v,j}, v)$.
- Si $\delta_v + \omega_{v,j} \geq \delta_j$, no hacemos nada.

(3) De entre todos los vértices temporales j elegimos el que tenga el estimador δ_j

... las etiquetas permanentes en sentido contrario

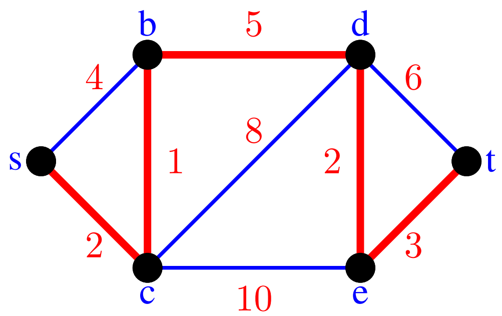
$t \to P_t \to \cdots \to s$. Si no es t, volver al paso (2).

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	∞	∞	∞	$(14, d)$	$(13, e)$	$\boxed{(13, e)}$

El algoritmo de Dijkstra (2)



Observaciones:

- Si en un paso dado hay varias opciones, escogemos una cualquiera de ellas.

Grafos orientados o dirigidos

Definición 95
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 96
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 97 *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 98
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* (v_i, v_j) *que comienzan en* v_i *y acaban en* v_j.

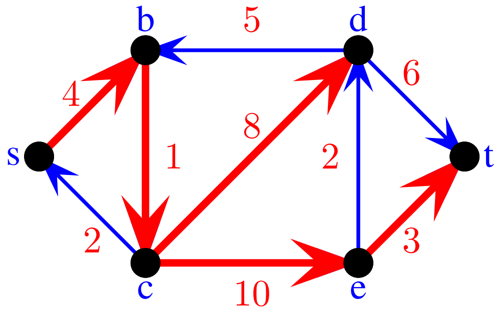
Grafos orientados o dirigidos (2)

Definición 99
Un **camino** *de longitud* ℓ *en un grafo dirigido* $G = (V, E)$ *es una sucesión de aristas de la forma* $(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell)$.

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

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

El algoritmo de Dijkstra para grafos orientados



Vértice	Paso 1	Paso 2	Paso 3	Paso 4	Paso 5	Paso 6
s	$\boxed{(0,s)}$	$\star$	$\star$	$\star$	$\star$	$\star$
b	$(4,s)$	$\boxed{(4,s)}$	$\star$	$\star$	$\star$	$\star$
c	∞	$(5,b)$	$\boxed{(5,b)}$	$\star$	$\star$	$\star$
d	∞	∞	$(13,c)$	$\boxed{(13,c)}$	$\star$	$\star$
e	∞	∞	$(15,c)$	$(15,c)$	$\boxed{(15,c)}$	$\star$
t	∞	∞	∞	$(19,d)$	$(18,e)$	$\boxed{(18,e)}$

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.

Coloraciones propias de un grafo

Definición 100
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 como mínimo para poder colorear G?

Definición 101
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 102 *Decidir si los vértices de un grafo arbitrario G se pueden colorear propiamente con $k \geq 3$ colores es un problema difícil.*

Algoritmo voraz para colorear un grafo

Algoritmo 103 (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
  $S_i = \{q\colon c(v_k) = q$ *, para todo v_k vecino de v_i con $k < i$*$\}$
  $c(v_i) = \min(\overline{S_i} \cap \mathbb{N}) =$ *el color más pequeño que no está en S_i*
end

Notas:

Algunos teoremas

Teorema 104 *Si G es un grafo con grado máximo k, entonces $\chi(G) \leq k+1$.*

Teorema 105 (Brooks, 1941) *Si G es un grafo no completo, conexo y con grado máximo $k \geq 3$, entonces $\chi(G) \leq k$.*

Proposición 106 *Un grafo G es bipartito si y sólo si $\chi(G) = 2$.*

Teorema 107 *Un grafo es bipartito si y sólo si no contiene ciclos de longitud impar.*

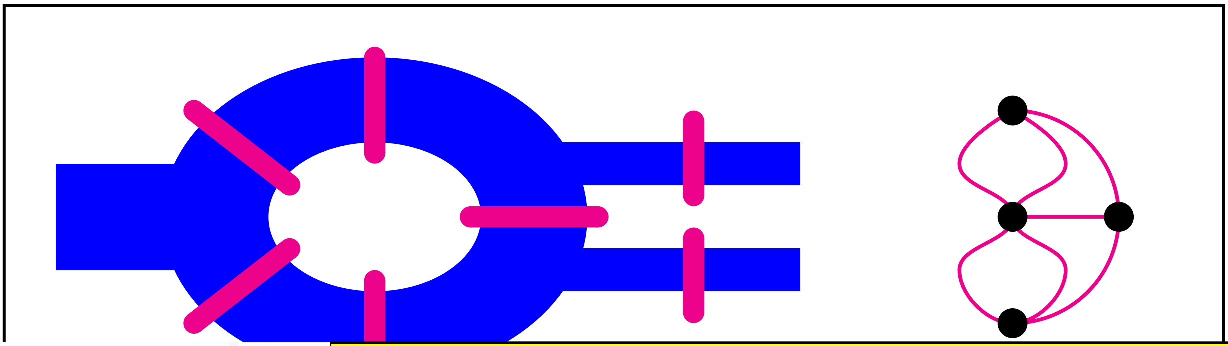
Corolario 108 *Todos los árboles son bipartitos*

Teorema 109 (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 (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?



Grafos eulerianos

Definición 110
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 111 *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 $C_0 = (v_0)$ 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 $C_i = (v_0, e_1, v_1, \ldots, e_i, v_i)$ al que le corresponde el grafo $G_i = (V_i, E_i) \subseteq G_0$.

- Si existe una única arista $e_{i+1} = \{v_i, w\} \in E_i = E \setminus \{e_1, e_2, \ldots, e_i\}$:
  - $C_{i+1} = (v_0, e_1, v_1, \ldots, e_i, v_i, e_{i+1}, w)$.
  - $G_{i+1} = (V_i \setminus \{v_i\}, E_i \setminus \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$.
- Si hay varias aristas incidentes en E_i con v_i: elegimos cualquiera de ellas con

Grafos hamiltonianos

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

Definición 112
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 difícil.

Teorema 113 (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 $n \geq 5$.

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 114 (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 115 *Si hay que repartir r objetos iguales en n grupos (distintos) pudiendo quedar grupos vacíos, entonces existen*

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

repartos distintos.

Patrones de conteo: particiones de un conjunto

Definición 116
Sea un conjunto finito S con $|S| = n$ elementos. Una **partición** *de S de tipo $(n_1, n_2, \ldots, n_k)$ con $n_i \in \mathbb{N}$ 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 117 *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 $(m, m, \ldots, m)$

donde r_k es el número de partes con k elementos.

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.

Relaciones de recurrencia

Definición 119
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*

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

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

Definición 120
El **orden de una relación de recurrencia** *es la diferencia entre los subíndices máximo y*

Solución de una relación de recurrencia lineal homogénea

Teorema 121 (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.

Solución de una relación de recurrencia lineal homogénea

Teorema 122 (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* $n \geq 1$*:*

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

Solución de una relación de recurrencia lineal homogénea

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

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

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

- 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:

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

- 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.

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:

$$\sum^{r} \left[\sum^{k_i} K^{(j)} \quad j-1 \right] \quad n \quad \geq 1$$

Solución de una relación de recurrencia lineal no homogénea

Teorema 123 (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 y $(a_1, \ldots, a_k)$ dados. La función $t_n : \mathbb{N} \to \mathbb{R}$ 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

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

y una solución particular cualquiera de la ecuación completa.

Solución de una relación de recurrencia lineal no homogénea

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

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

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

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

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

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

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.

Función generatriz

Definición 125
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 $\left(\binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k}, 0, 0, \ldots\right)$.

- $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ es la f.g. de $(1, 1, \frac{1}{2!}, \frac{1}{3!}, \ldots)$.

Maniobras básicas con funciones generatrices

- $(1, 2, 3, \ldots)$ 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 $G(x) = x^k F(x)$.

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* $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$.

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 $f_1 = 1 + x + x^2 + x^3 + \ldots = \frac{1}{1-x}$.
   - La función generatriz de colocar 2's es $f_2 = 1 + x^2 + x^4 + x^6 + \ldots = \frac{1}{1-x^2}$.
   - $\vdots$
   - La función generatriz de colocar el natural $p \geq 1$ es

$k=1$

Procedimiento práctico

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

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

Ejemplo: la ecuación de Fibonacci

2. Manipular las sumas para que queden en función de F y de las condiciones iniciales:
   - $\sum_{n=2}^{\infty} a_n\, x^n = F - a_0 - a_1\, x = F - x.$
   - $\sum_{n=2}^{\infty} a_{n-1}\, x^n = x \sum_{n=2}^{\infty} a_{n-1}\, x^{n-1} = x \sum_{m=1}^{\infty} a_m\, x^m = x(F - a_0) = x\, F.$
   - $\sum_{n=2}^{\infty} a_{n-2}\, x^n = x^2 \sum_{n=2}^{\infty} a_{n-2}\, x^{n-2} = x^2 \sum_{m=0}^{\infty} a_m\, x^m = x^2\, F.$

   La ecuación de recurrencia se transforma en la ecuación

$$F - x \;=\; x\, F + x^2\, F\,.$$

3. Resolvemos esta ecuación para F:

$$F(x) \;=\; \frac{x}{1 - x - x^2} \;=\; \sum_{n=0}^{\infty} a_n\, x^n\,.$$

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 todos los coeficientes mediante un poco de álgebra:

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

Teorema del binomio generalizado

Teorema 126 *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

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

Tema 10: Teoría de grafos V

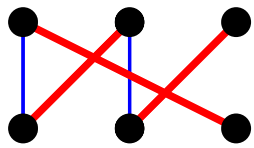
1. Grafos no dirigidos.
2. Algoritmos en teoría de grafos.
3. Problemas combinatorios en grafos:
   - Emparejamiento en grafos.
   - Coloraciones propias en grafos.

Emparejamientos en grafos

Definición 127
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 128 *Si G es un grafo bipartito y regular con grado $d \geq 1$, entonces G contiene un emparejamiento perfecto.*

Coloraciones propias: polinomio cromático

Definición 129
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.

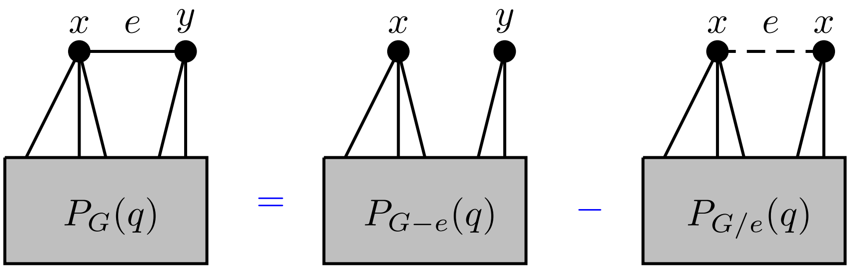
Teorema 130 *Si $G = (V, E)$ es un grafo simple, $P_G(q)$ es un polinomio en q.*

La demostración se basa en:

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

al contraer la arista e (identificando los vértices x e y y eliminando posibles multiaristas).

Demostración del Teorema de contracción-borrado



Teorema 132 *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 133 *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*

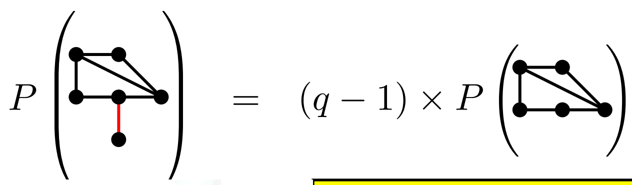
$$P_G(q) = \frac{P_{G_1}(q) \times P_{G_2}(q)}{P_{K_n}(q)}.$$

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

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:



$\chi(G) = 3.$

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 134
Una **relación binaria** $\mathcal{R}$ *del conjunto* V *al conjunto* W *es un subconjunto del producto cartesiano* $V \times W$*:*

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

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

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

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

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

Relaciones binarias en un conjunto

Definición 135
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:*

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

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

$$\mathit{Im}\,\mathcal{R} \;=\; \{w \in V \colon (v,w) \in \mathcal{R} \quad \textit{para algún}\; v \in V\}\,.$$

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

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):

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

Operaciones con relaciones

Definición 136
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 137
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

Definición 138
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 139 *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:*

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

Propiedades de las relaciones sobre V

Definición 140
Una relación $\mathcal{R}$ es **reflexiva** *si para todo $v \in V$ se cumple que $v\mathcal{R}v$.*

Definición 141
Una relación $\mathcal{R}$ es **antirreflexiva** *si para todo $v \in V$ se cumple que $v\overline{\mathcal{R}}v$.*

Definición 142
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 143
Una relación $\mathcal{R}$ es **antisimétrica** *si $(v_1\mathcal{R}v_2) \wedge (v_2\mathcal{R}v_1) \Rightarrow v_1 = v_2$.*

Relaciones transitivas

Definición 144
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 145 *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 146 *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 147
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 148
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 $[v]_{\mathcal{R}}$.*

Conjunto cociente

Teorema 149 *Sea $\mathcal{R}$ una relación de equivalencia sobre V. Entonces, dos*

(1) $[a]_{\mathcal{R}}$ en 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 150 *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.*

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 152
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 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: $a = a \cdot 1$.

Propiedades de la división de enteros

Teorema 154 *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 155 *Si $a \mid b_i$ para $i = 1, \ldots, N$, entonces $a \mid \sum_{i=1}^{N} u_i \cdot b_i$ para todo $u_i \in \mathbb{Z}$.*

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

Definición 156
Dados dos enteros $a, b \neq 0$, se denomina **máximo común divisor** *de a y b [denotado por $\mathrm{mcd}(a, b)$] 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.
- $\mathrm{mcd}(0, a) = |a|$ para todo entero no nulo a.

Teorema 157 *El máximo común divisor de dos números enteros es único.*

Algoritmo de Euclides

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

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

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

En general, $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r_1) = \mathrm{mcd}(r_1,r_2) = \ldots = \mathrm{mcd}(r_{n-2},r_{n-1})$, 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, $\mathrm{mcd}(r_{n-2},r_{n-1}) \;=\; r_{n-1}$.

Teorema 159 *En el Algoritmo de Euclides* $\mathrm{mcd}(a,b) = r_{n-1}$ *(i.e., el último resto no nulo).*

Identidad de Bezout

Teorema 160 (Identidad de Bezout, 1730-1783) *Si* a *y* b *son enteros (no nulos simultaneamente), existen enteros* u, w *tales que*
$$\mathrm{mcd}(a,b) \;=\; a\cdot u + b\cdot w\,.$$

DEMOSTRACIÓN. Si escribimos los pasos del Algoritmo de Euclides

$$\begin{array}{rclcrcll} a &=& q_1\cdot b + r_1 & \Rightarrow & r_1 &=& a - q_1\cdot b & P_1\\ b &=& q_2\cdot r_1 + r_2 & \Rightarrow & r_2 &=& b - q_2\cdot r_1 & P_2\\ r_1 &=& q_3\cdot r_2 + r_3 & \Rightarrow & r_3 &=& r_1 - q_3\cdot r_2 & P_3\\ &\vdots& & & &\vdots& & \end{array}$$

$\ldots = \alpha_3 r_1 + \beta_3 r_2 = \alpha_2 b + \beta_2 r_1 = \alpha_1 a + \beta_1 b.$

Identidad de Bezout (2)

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

Teorema 161 *Sean dos números enteros a y b no nulos simultáneamente con $\mathrm{mcd}(a,b)=d$. 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 162 *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 163 *Si $\mathrm{mcd}(a,b)=d$, entonces:*

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

Corolario 164 *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 $a\mid c$.*

Mínimo común múltiplo

Definición 165
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 166 *Sean $a,b\in\mathbb{N}$ con $d=\mathrm{mcd}(a,b)$ y $m=\mathrm{mcm}(a,b)$. Entonces,*

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

Algunos resultados sobre números primos:

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

Ecuaciones diofánticas lineales [Diophantos, s III]

Definición 169
Una **ecuación diofántica** *es una ecuación de una o varias variables y de la que nos interesan sólo sus soluciones enteras.*

Teorema 170 (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

$$x_k \;=\; u \cdot p + \frac{b \cdot k}{d}\,,$$
$$y_k \;=\; w \cdot p - \frac{a \cdot k}{d}\,,$$

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

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

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 171
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 172

1. $a \equiv b \pmod{m}$ *si y sólo si* $a \bmod m = b \bmod m$.

El conjunto cociente $\mathbb{Z}_m$

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

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

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

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

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

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

Aritmética modular

Teorema 175 *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 176 *Sean* $m, k \in \mathbb{N}$. *Si* $a \equiv b \pmod{m}$, *entonces* $a^k \equiv b^k \pmod{m}$.

Teorema 177 *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* $a \equiv b \pmod{m}$.

Observaciones:

División modular: congruencias lineales

Definición 178
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 $\mathbb{Z}_m$.

Congruencias lineales

Teorema 179 *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*

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

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

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. 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.

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 182
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 $x \not\equiv 0 \pmod{m}$.

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

Aritmética en $\mathbb{Z}_m$ (3)

Teorema 185 *Un elemento $r \in \mathbb{Z}_m$ es invertible si y sólo si r y m son primos entre sí.*

Corolario 186 *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 187
La **función ϕ de Euler** *$\phi \colon \mathbb{N} \to \mathbb{N}$ se define de manera que $\phi(m)$ es igual al número de elementos invertibles de $\mathbb{Z}_m$.*

Lema 188 *Si p es primo, $\phi(p) = p - 1$.*

El teorema de Euler

Teorema 189 (Euler, 1790) *Si y es invertible en $\mathbb{Z}_m$ (es decir, si $\mathrm{mcd}(y, m) = 1$), entonces*

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

Corolario 190 (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 191 *Si p es primo, entonces para cualquier entero y se tiene que*

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

$n_k \geq 1$, entonces $\phi(n) = n \cdot \prod_{k=1} (1 - 1/p_k)$.

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 193
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 194
Un conjunto V equipado con una relación de orden $\preceq$ se denomina **conjunto parcialmente ordenado** $(V, \preceq)$ *(o poset).*

Definición 195
Sea $(V, \preceq)$ un conjunto parcialmente ordenado. Dos elementos $a, b \in V$ son **comparables**

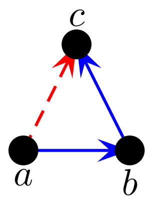
totalmente ordenado *(o* **cadena***).*

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:

   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.

Elementos extremales

Definición 197
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 198
Sea $(V, \preceq)$ un conjunto parcialmente ordenado. $M^\star \in V$ es un **elemento máximo** *si $v \preceq M^\star$ para todo $v \in V$. $m^\star \in V$ es un* **elemento mínimo** *si $m^\star \preceq v$ para todo $v \in V$. Es decir, en el diagrama de Hasse asociado a $(V, \preceq)$, $M^\star$ está encima de todos los elementos de V y $m^\star$ está por debajo de todos los elementos de V. Los elementos máximo y mínimo*

Elementos extremales (2)

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

Definición 200
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: $u^\star = \min($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: $d^\star = \max($minor$(B))$.*

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

Orden total compatible con un orden parcial

Definición 201
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 202 (Ordenación topológica)
procedure *TotalOrder($(V, \preceq_P)$: conjunto finito parcialmente ordenado)*
$k = 1$
while $V \neq \emptyset$
begin
  v_k = *un elemento minimal de* $(V, \preceq_P)$
  $V \to V \setminus \{v_k\}$

Conjunto bien ordenado

Definición 203
$(V, \preceq)$ *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.

El principio de inducción para los naturales

Definición 204 (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.

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

Principio de inducción para conjuntos bien ordenados

Proposición 206 (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:*

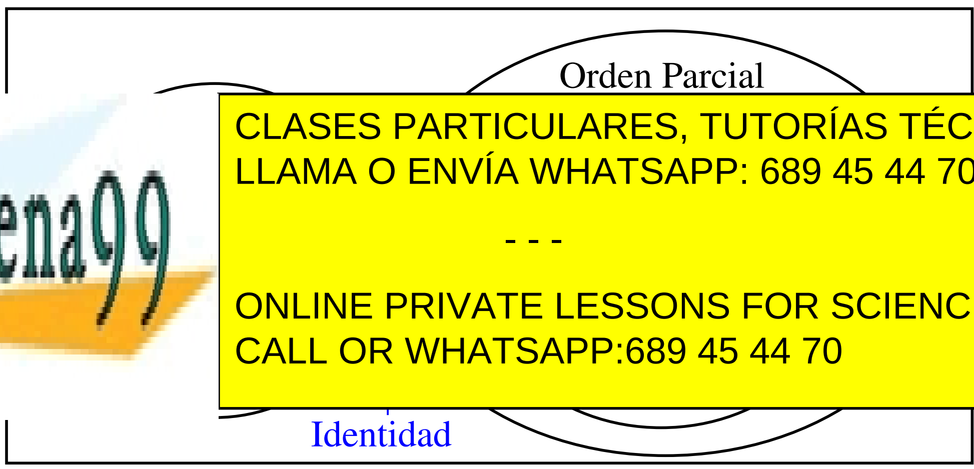
1. *Paso base: $P(v_0)$ es verdadera para $v_0 = \text{mín}(V)$.*
2. *Paso inductivo: sea w un elemento arbitrario pero fijo de V y sea v su sucesor. Entonces si $P(x)$ es verdadera para todo $v_0 \preceq x \preceq w$, entonces $P(v)$ es verdadera.*

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

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 207
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 $\text{ínf}(a, b)$ 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 $\text{ínf}(a, b) = a \wedge b \in A$.
- No todos los conjuntos parcialmente ordenados son retículos.

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 $\sup \leftrightarrow \text{ínf}$.

Corolario 208 (Principio de dualidad) *Cualquier enunciado referido a un retículo $(A, \preceq)$ se mantiene válido si intercambiamos $\preceq$ por $\succeq$, $\sup$ por ínf 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.

Propiedades de los retículos

Proposición 209 *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 210 *Si $(A, \preceq)$ es un retículo, entonces para cualquier $a, b, c \in A$:*

1. $\text{ínf}(a, a) = a \wedge a = a$ *[idempotencia]*

Propiedades de los retículos (2)

Proposición 211 *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 212 (Desigualdades distributivas) *Si $(A, \preceq)$ es un retículo, entonces para cualquier $a, b, c \in A$ se cumple que*

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

Los retículos como sistemas algebraicos

Definición 213
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 214
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 215
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 $a \in A$,
  - $\sup(a, 1) = a \vee 1 = 1$.
  - $\text{ínf}(a, 1) = a \wedge 1 = a$.
  - $\sup(a, 0) = a \vee 0 = a$.
  - $\text{ínf}(a, 0) = a \wedge 0 = 0$.

- Todo retículo finito A está acotado: $1 = \sup(A)$ y $0 = \inf(A)$.

Retículos distributivos

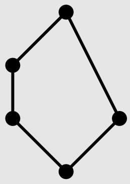
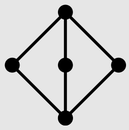
Definición 216
Un retículo $(A, \preceq)$ es un **retículo distributivo** *si para todo $a, b, c \in A$,*

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

- Esto es algo más que la propiedad distributiva:

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

Teorema 217 *Un retículo es distributivo si y sólo si* **no** *contiene un subretículo isomorfo a uno de estos dos retículos:*

$N_5 =$  *y* $M_3 =$ 

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

Retículos complementados

Definición 218
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 $\text{ínf}(a, b) = a \wedge b = 0$.*

- 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.

$a \in A$ tiene un **único** elemento complementario, que denotaremos por $\overline{a}$.

Álgebra de Boole

Definición 221 (Definición 1)
Un **álgebra de Boole** *es un retículo* $(A, \vee, \wedge, \overline{\ }, 0, 1)$ *acotado, distributivo y complementado.*

Definición 222 (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* $(a, b) \to a + b \in B$.
- *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]*
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. $a + \overline{a} = 1$, $a \cdot \overline{a} = 0$ *[leyes de complementos]*

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 booleana $\cdot$ en un álgebra de Boole no tienen porqué ser la suma y el producto de números reales.

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

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

elementos.

Álgebras de Boole no triviales generales

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

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

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 $B, C \subseteq A$,
  - $\sup(B, C) = B \cup C \subseteq A$ ($\vee \Rightarrow \cup$).
  - $\text{ínf}(B, C) = B \cap C \subseteq A$ ($\wedge \Rightarrow \cap$).
- 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 $\overline{B} = A \setminus B \subseteq A$.
- El conjunto $(\mathcal{P}(A), \cup, \cap, \setminus, \emptyset, A)$ es un álgebra de Boole.
- Aplicación: teoría de la probabilidad.

Propiedades de un álgebra de Boole

Proposición 223 *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 224

Boole *si* $0, 1 \in C$ *y es cerrado respecto a las operaciones* $+, \cdot, \overline{\ }$.