TEMA 1. ALGORITMOS Y NÚMEROS

1. ALGORITMOS

Un tema central en computación es el diseño de un proceso para llevar una tarea. En cada casa, la respuesta tiene la forma de una sucesión precisa de pasos conocida como un algoritmo.

Los algoritmos deben aportar salidas correctas y efectivas en un número finito de pasos y en un tiempo finito, garantizando así que termina tras su ejecución. Sucesión claramente definida y no ambigua, diseñada para la resolución general de un problema concreto teniendo en cuenta sus posibles variantes.

1.1. PROPIEDADES DE LOS ALGORITMOS

→ Entrada (input): un algoritmo tiene valores de entrada que son elementos de un conjunto especificado.

→ Salida (output): para cada conjunto de valores de entrada, un algoritmo produce valores de salida de un conjunto especificado. Los valores de salida son la solución del problema.

→ Definición: los pasos de un algoritmo deben definirse con precisión.

→ Corrección: un algoritmo debe producir salidas correctas para cada conjunto de valores de entrada.

→ Duración finita: un algoritmo debe producir la salida deseada tras un número finito (aunque quizás grande) de pasos para cualquier conjunto de valores de entrada.

→ Efectividad[1]: debe ser posible realizar cada paso del algoritmo con exactitud en un intervalo finito de tiempo.

→ Generalidad: el procedimiento debería ser aplicable a todos los problemas de la forma deseada, no solo para un conjunto particular de datos de entrada.

1.2. ALGORITMOS DE BÚSQUEDA

Un problema de búsqueda general puede describirse de la siguiente manera: localizar un elemento x en una lista de elementos distintos a_0, a_1, a_2,…,a_n, o determinar que no está en la lista. La solución a este problema de búsqueda es la ubicación del elemento en la lista que es igual a x, es decir, la solución es i si $x = a_i$, o es $False$ si x no está en la lista.

1.2.1. BÚSQUEDA LINEAL O SECUENCIAL

El algoritmo de búsqueda lineal comienza por comparar x y a_0. Si $x = a_0$, la solución es la localización de a_0, es decir, 0. De no ser así, este proceso continúa comparando x sucesivamente con cada término de la lista hasta que encuentre una coincidencia. Si se ha recorrido toda la lista sin localizar x, la solución es $False$.

1.2.2. BÚSQUEDA BINARIA

Este algoritmo se puede utilizar cuando la lista tiene los términos en orden creciente de tamaño siendo $a_0 < a_1 < a_2 < \dots < a_n$. Se procede comparando el elemento que se quiere localizar, x, con el termino central de la lista. La lista se divide entonces en dos sublistas más pequeñas. La búsqueda continúa restringiéndose a la sublista apropiada basándose en la comparación entre el elemento central de la misma.

FUNCIÓN FLOOR	FUNCIÓN CEILING
$\lfloor\ \rfloor: \mathbb{R} \to \mathbb{Z}$	$\lceil\ \rceil: \mathbb{R} \to \mathbb{Z}$
$x \mapsto \lfloor x \rfloor$, donde $\lfloor x \rfloor$ es el mayor entero $z\ /\ z \leq x$	$x \mapsto \lceil x \rceil$, donde $\lceil x \rceil$ es el menor entero $z\ /\ z \geq x$
EJEMPLO: $\lfloor 2.3 \rfloor = 2$	EJEMPLO: $\lceil 2.3 \rceil = 3$

[1] Efectividad ≠ eficiencia. Un algoritmo puede ser efectivo, pero no eficiente (ejecutarse en tiempo polinómico).

1.3. ALGORITMOS VORACES

Muchos algoritmos están diseñados para resolver problemas de optimización. Su objetivo problemas es encontrar una solución para el problema dado que o bien minimice o maximice el valor de algún parámetro.

Los algoritmos voraces, codiciosos o "*greedy*" encuentran una solución factible de una manera sencilla seleccionando la mejor opción en cada paso (solución local) en lugar de considerar toda la secuencia global de pasos que podría conducir una solución óptima. Es necesario determinar si finalmente, el algoritmo aporta o no una solución eficiente.

1.4. OTROS TIPOS DE ALGORITMOS

→ Algoritmos de ordenación (de burbuja, por selección, inserción, mezcla o de forma rápida).

→ Algoritmos de fuerza bruta (técnicas de enumeración, búsqueda exhaustiva).

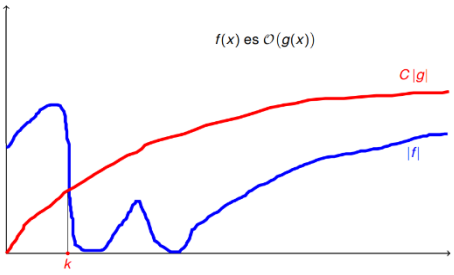
→ Algoritmos de divide y vencerás.

→ Algoritmos de transforma y vencerás (reformulación).

1.5. PROBLEMAS INDECIDIBLES

Alan Turing mostró que existen problemas matemáticos bien definidos para los cuales no hay ningún algoritmo. Hay muchos problemas, destacando el problema de la parada ("*halting problem*").

Este problema concluye que no existe ningún método general que permita predecir, una vez que un ordenador ha empezado un cálculo, si dicho cálculo terminará en una respuesta.



1.6. NOTACIÓN BIG-O

Sean f y g dos funciones tales que $f, g: \mathbb{Z} \to \mathbb{R}$, se dice que $f(x)$ es $O(g(x))$ si existen 2 constantes positivas C y k (testigos) de forma que:

$$|f(x)| \leq C|g(x)| \quad si\ x > k$$

TEOREMA

Sean $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio de grado n, entonces, $f(x)$ es $0(x^n)$

TEOREMA

Sean $f_1(x)$ es $O(g_1(x))$ y $f_2(x)$ es $O(g_2(x))$, entonces $(f_1 + f_2)(x)$ es $0(\max\{|g_1(x)|, |g_2(x)|\})$

COROLARIO

Si $f_1(x)$ y $f_2(x)$ son $O(g(x))$, entonces $(f_1 + f_2)(x)$ es $O(g(x))$

TEOREMA

Sean $f_1(x)$ es $O(g_1(x))$ y $f_2(x)$ es $O(g_2(x))$, entonces $(f_1 \cdot f_2)(x)$ es $0(g_1(x) \cdot g_2(x))$

TEOREMA (propiedad transitiva)

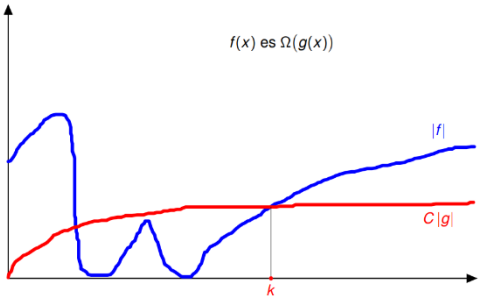
Si $f(x)$ es $O(g(x))$ y $g(x)$ es $O(h(x))$, entonces, $f(x)$ es $0(h(x))$

TEOREMA

Si $f(x)$ es $O(g(x))$, entonces $a \cdot f(x)$ es $O(g(x))$, para cualquier constante a

$$1 \to \log n \to \sqrt{n} \to n \cdot \log n \to n^2 \to 2^n \to n^n \to n!$$

1.7. NOTACIÓN BIG-Ω



Sean f y g dos funciones tales que $f, g: \mathbb{Z} \to \mathbb{R}$, se dice que $f(x)$ es $\Omega(g(x))$ si existen 2 constantes positivas C y k de forma que:

$$|f(x)| \geq C|g(x)| \quad si\ x > k$$

Asimismo, $f(x)$ es $\Omega(g(x))$ si y solo si $g(x)$ es $O(f(x))$.

1.8. NOTACIÓN BIG-Θ

Sean f y g dos funciones tales que $f, g: \mathbb{Z} \to \mathbb{R}$, se dice que $f(x)$ es $\Omega(g(x))$ si:

$$f(x) \text{ es } O(g(x)) \quad \text{y} \quad f(x) \text{ es } \Omega(g(x))$$

1.9. COMPLEJIDAD EN TIEMPO

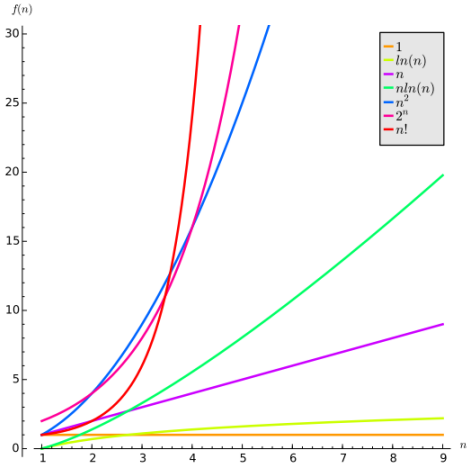
Un análisis del tiempo requerido para resolver un problema de un tamaño particular está relacionado con la complejidad en tiempo de un algoritmo. La complejidad en tiempo de un algoritmo se puede expresar en términos del número de operaciones usadas por el algoritmo; estas pueden ser: comparación de enteros, adición de enteros, multiplicación de enteros, o cualquier otra operación básica.

→ Complejidad en el peor caso: El comportamiento del algoritmo en el peor caso significa el mayor número de operaciones que hace falta para resolver el problema dado utilizando para unos datos de entrada un determinado tamaño. Los análisis del peor caso nos dicen cuántas operaciones tiene que realizar los algoritmos para garantizar una solución

→ Complejidad en el caso promedio: Se considera el número promedio (valor medio o esperado) de operaciones realizadas por el algoritmo. Se tiene en cuenta la probabilidad de los datos de entrada que se manejan.

→ Complejidad en el mejor caso: Se tiene en cuenta el menor número posible de operaciones ejecutadas por el algoritmo.

1.9.1. COMPLEJIDAD DE LOS ALGORITMOS



COMPLEJIDAD	TERMINOLOGÍA
$\Theta(1)$	Complejidad constante
$\Theta(\log n)$	Complejidad logarítmica
$\Theta(n)$	Complejidad lineal
$\Theta(n \log n)$	Complejidad cuasi-lineal (log-lineal)
$\Theta(n^b), b > 1$	Complejidad polinómica
$\Theta(b^n), b > 1$	Complejidad exponencial
$\Theta(n!)$	Complejidad factorial

Complejidad en el peor de los casos:

→ Algoritmo de encontrar el máximo: complejidad lineal.
→ Búsqueda lineal: complejidad lineal.
→ Búsqueda binaria: complejidad logarítmica.
→ Ordenación de burbuja: complejidad cuadrática.
→ Ordenación por selección: complejidad cuadrática.
→ Ordenación por inserción: complejidad cuadrática.
→ Ordenación por mezcla "Merge sort": complejidad cuasi-lineal.
→ Ordenación rápida "Quick sort": complejidad cuadrática (en el caso promedio: cuasi-lineal)

1.9.2. COMPLEJIDAD DE LOS PROBLEMAS

→ Problema resoluble: un problema se dice que es resoluble si puede resolverse por un algoritmo.

› Problema tratable: un problema que es resoluble utilizando un algoritmo con complejidad polinómica en el peor caso.

› Problema intratable: un problema que no se puede resolver utilizando un algoritmo con complejidad polinómica.

→ Problema irresoluble: un problema para el cual se puede probar que no existen algoritmos que puedan resolverlo.

→ Clase P: un problema es resoluble por un algoritmo que lo ejecuta en tiempo polinómico. Los problemas tratables pertenecen a la clase P.

→ Clase NP: un problema puede ser comprobado en tiempo polinómico si la solución probable es realmente una solución.

› NP-completos: problemas NP en los cuales no se sabe si las soluciones pueden obtenerse o no en tiempo polinómico. Si uno de estos problemas se puede resolver por un algoritmo con complejidad polinómica en el peor de los casos, entonces todos los problemas en la clase NP también se pueden resolver en tiempo polinómico

2. NÚMEROS

2.1. DIVISIÓN

Sean a y b números enteros donde $a \neq 0$, a divide a b ($a|b$) si existe un entero c tal que $b = a \cdot c$ (a es un factor de b; b es múltiplo de a).

TEOREMA

Sean a, b y $c \ \epsilon \mathbb{Z}$; $a \neq 0$. Entonces:

→ Si $a|b$ y $a|c \Rightarrow a|(b + c)$
→ Si $a|b \Rightarrow a|(b \cdot n)$ siendo $n \in \mathbb{Z}$
→ Si $a|b$ y $b|c \Rightarrow a|c$ (propiedad transitiva)

COROLARIO

Sean a, b y $c \ \epsilon \mathbb{Z}$; $a \neq 0$; tal que $a|b$ y $b|c \Rightarrow a|(mb + nc)$ siendo $m, n \in \mathbb{Z}$.

2.1.1. ALGORITMO DE LA DIVISIÓN

Sea $a \in \mathbb{Z}$ y d un entero positivo, entonces existen q y r enteros únicos, con $0 \leq r < d$ tales que:

$$a = d \cdot q + r; r = a \ mod \ b; q = \left\lfloor \frac{a}{b} \right\rfloor$$

2.2. NÚMEROS PRIMOS

Sea un número $\mathbb{Z}$ positivo > 1, se dice que p es un número primo si los únicos factores (divisores) positivos de p son 1 y p. Existen infinitos números primos. Podemos formar números primos llamados Primos de Mersenne con la ecuación $2^p - 1$ con p siendo un número primo (tiene un error al no formar el 11).

Un número positivo que no sea primo, se dice compuesto. Si n es un número compuesto, entonces n tiene un divisor primo $\leq \sqrt{n}$.

EJEMPLO: $\sqrt{641} \cong 25.32 \ \Rightarrow \ 641$ solo podría ser divisible por números ≤ 25.32

Todo entero > 1 se puede descomponer (factorizar) de manera única como un primo o producto de números primos donde los factores primos se describen en orden no decreciente.

El 1 y el -1 son lo que se llama 'unidad': a es una unidad si existe un b (inverso multiplicativo de a) tal que $a \cdot b = 1$.

2.3. MÁXIMO COMÚN DIVISOR

Sean a y b números enteros positivos y al menos uno de ellos $\neq 0$, el mayor entero d tal que $d|a$ y $d|b$ se llama máximo común divisor de a y b ($gcd(a,b)$).

Dos enteros a y b se dicen primos entre sí ('relativamente primos') si $gcd(a,b) = 1$.

EJEMPLO: 17 y 22 son primos entre sí.

Se dice que $a_1, a_2, \ldots, a_n$ números enteros son primos entre sí si $gcd(a_i, a_j) = 1; i \neq j$.

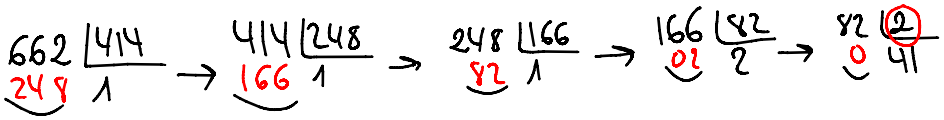
EJEMPLO: $4, 9, 11$ y 65 son primos entre sí.

2.3.1. CÁLCULO MEDIANTE EL ALGORITMO DE EUCLIDES / O(log(x))

→ Lema: Sean a y b dos números donde $a > b \Rightarrow gcd(a,b) = gcd(b,r)$
Sea d un divisor de a y $b \Rightarrow d|d$ y $d|r$
Sea d un divisor de b y $r \Rightarrow d|a$ y $d|r$

EJEMPLO:

$$gdc(662, 414) = gdc(414, 248) = gdc(248, 166) = gdc(166, 82) = 2$$



TEOREMA DE BÉZOUT

Sean a y b enteros positivos, entonces existe un s y $t \in \mathbb{Z}$ tales que $gcd(a,b) = s \cdot a + t \cdot b$ (identidad de Bézout), siendo estos los coeficientes de Bézout.

EJEMPLO:

$$gdc(662, 414) = 2 = s \cdot 662 + t \cdot 414$$

$$\begin{aligned} 2 &= 166 - 2 \cdot 82 \\ 82 &= 248 - 1 \cdot 166 \\ 166 &= 414 - 1 \cdot 248 \\ 248 &= 662 - 1 \cdot 414 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 2 &= 166 - 2 \cdot (248 - 166) = 3 \cdot 166 - 2 \cdot 248 = \\ &= 3 \cdot (414 - 248) - 2 \cdot 248 = 3 \cdot 414 - 5 \cdot 248 = \\ &= 3 \cdot 414 - 5 \cdot (662 - 414) = \boxed{8 \cdot 414 - 5 \cdot 662} \end{aligned}$$

→ Lema: Si a, b y c son enteros positivos tal que $gcd(a,b) = 1$ y $a|(b \cdot c) \Rightarrow a|c$

→ Lema: Si p es primo y $p|a_1, a_2, \ldots, a_n$, donde a_i son enteros, entonces: $p|a_i$ para algún i.

2.4. MÍNIMO COMÚN MÚLTIPLO

Sean a y b números enteros positivos y al menos uno de ellos $\neq 0$, el menor entero m tal que $m = \dot{a}$ y $m = \dot{b}$ se llama mínimo común múltiplo de a y b ($lcm(a,b)$).

2.4.1. CÁLCULO MEDIANTE EL ALGORITMO DE EUCLIDES / O(log(x))

$$lcm(a,b) = \frac{a \cdot b}{\gcd(a,b)} \Rightarrow lcm(a,b) \cdot gcd(a,b) = a \cdot b$$

$$\left.\begin{array}{l} a = p_1^{\alpha_1}, \dots, p_s^{\alpha_s} \\ b = p_1^{\beta_1}, \dots, p_s^{\beta_s} \end{array}\right\} \Rightarrow \begin{array}{l} lcm(a,b) = p_1^{max\{\alpha_1+\beta_1\}}, \dots, p_s^{\max\{\alpha_s+\beta_s\}} \\ gcd(a,b) = p_1^{min\{\alpha_1+\beta_1\}}, \dots, p_s^{\min\{\alpha_s+\beta_s\}} \end{array}$$

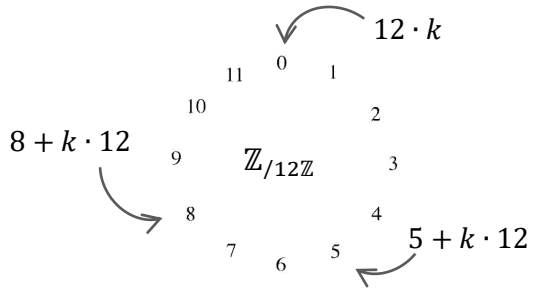
$$a \cdot b = p_1^{\alpha_1+\beta_1}, \dots, p_s^{\alpha_s+\beta_s} \qquad lcm(a,b) \cdot gcd(a,b) = p_1^{\alpha_1+\beta_1}, \dots, p_s^{\alpha_s+\beta_s}$$

2.5. ARITMÉTICA MODULAR

Sean a y b enteros, m entero positivo, diremos que a es congruente con b módulo m ($a \equiv b\ (mod\ m)$) si $m|(a-b)$.

EJEMPLO:

$$\left.\begin{array}{l} a = -243 \\ b = 9 \\ m = 12 \end{array}\right\} \quad -243 - 9 = -252\ ;\ 12 \mid -252\ S\acute{I} \Rightarrow -243 \equiv 9\ (mod\ 12)$$



Sean a y b enteros, m entero positivo: $a \equiv b\ (mod\ m) \Leftrightarrow a\ mod\ m = m\ mod\ b$. Sucede también:

$$m \cdot k = a - b = (qm + r) - (q'm + r') = (q - q')m + (r - r') \Rightarrow a - b = (q - q')m$$

TEOREMA

Sean a, b, c y d enteros, m entero positivo. Si:

$$a \equiv b\ (mod\ m) \qquad a + c \equiv b + d\ (mod\ m)$$

$$a \equiv b\ (mod\ m) \qquad a \cdot c \equiv b \cdot d\ (mod\ m)$$

COROLARIO

Sean a y b enteros, m entero positivo. Entonces:

$$(a + b)(mod\ m) = [(a\ mod\ m) + (b\ mod\ m)]\ (mod\ m)$$

$$(a \cdot b)(mod\ m) = [(a\ mod\ m) \cdot (b\ mod\ m)]\ (mod\ m)$$

$a \equiv b \Leftrightarrow \exists k \epsilon \mathbb{Z}\ ;\ a = b + km$ donde $k = q - q'$.

Se llaman divisores de cero a un $a \neq 0$ y $b \neq 0$ tales que $a \cdot b \equiv 0\ (mod\ m)$.

2.6. INVERSO MULTIPLICATIVO

Sea a un número del módulo m, existe b tal que $a \cdot b \equiv 1(\mathrm{mod}\, m)$, si a y m son primos entre sí. El número b se denomina inverso multiplicativo, $a^{-1} \equiv b$.

En $\mathbb{Z}_{/m\mathbb{Z}}$, a es una unidad (tiene inverso multiplicativo) $\Leftrightarrow gcd(a,m) = 1$, es decir, a es primo con m.

TEOREMA DE EULER (1)

¿Cuántas unidades hay en $\mathbb{Z}_{/m\mathbb{Z}}$?

Si p es un número primo $\begin{cases} \phi(p) = p-1 \\ \phi(p^k) = p^{k-1}(p-1) \\ \phi(n) = \phi(p_1^{k_1}, \dots, p_s^{k_s}) = \phi(p_1^{k_1}) \cdot \dots \cdot \phi(p_s^{k_s}) \end{cases}$

EJEMPLO:

$\mathbb{Z}_{/8\mathbb{Z}} \rightarrow 8 = 2^3 \rightarrow$ Hay $\phi(2^3) = 2^{3-1}(2-1) = 4$ unidades.

$\mathbb{Z}_{/12\mathbb{Z}} \rightarrow 12 = 2^2 \cdot 3 \rightarrow$ Hay $\phi(2^3, 3) = 2^{3-1}(2-1) \cdot 3^{1-1}(3-1) = 4$ unidades.

TEOREMA (el pequeño Teorema de Fermat)

Si p es un número primo y $p \nmid a$. Entonces:

$$a^{p-1} \equiv 1\ (mod\ p)$$

COROLARIO

Si p es un número primo, para cualquier a:

$$a^p \equiv a\ (mod\ p) \quad \begin{cases} p|a \Rightarrow a \equiv 0\ (mod\ p) \\ p \nmid a \Rightarrow a \cdot a^{p-1} \equiv 1 \cdot a (mod\ p) \end{cases}$$

TEOREMA EULER (2)

Si $gcm(a,m) = 1$, entonces:

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\, p)$$

2.7. RESOLUCIÓN DE CONGRUENCIAS LINEALES

En $\mathbb{Z}_{/m\mathbb{Z}}$, siendo $ax \equiv b(\mathrm{mod}\, m)$, pueden suceder tres situaciones al intentar hallar x:

- $\rightarrow$ $d = gcd(a,m)$; $d \nmid b \Rightarrow$ La ecuación no tiene soluciones.
  EJEMPLO: $2x \equiv 3\ (mod\ 6)$ no tiene soluciones porque $2 \nmid 3$.
- $\rightarrow$ $d = gcd(a,m)$; $d \mid b \Rightarrow$ La ecuación tiene exactamente d soluciones.
  EJEMPLO: $2x \equiv 4\ (mod\ 6)$ tiene soluciones porque $2 \mid 4 = 2$. Entonces: $x = 2$ y $x = 5$.
- $\rightarrow$ $d = gcd(a,m) = 1 \Rightarrow$ Caso particular: a es una unidad de $mod\ m$; aplicar el *Teorema de Bézout.*
  EJEMPLO: $252x \equiv 473\ (mod\ 6)$, $252^{-1} \equiv 110$. Entonces $x = 473 \cdot 110 \equiv 253(mod\ 523)$.

Las soluciones de la ecuación $ax \equiv b(mod\, m)$ son $x_0 + k \cdot \frac{m}{d}$, donde k es un número entero comprendido entre 0 y $d-1$ y x_0 es la única solución de $\frac{a}{d}x \equiv \frac{b}{d}\left(mod\ \frac{m}{d}\right)$.

TEOREMA CHINO DE LOS RESTOS

Sean $m_1, m_2,\ldots,m_k$ primos relativos entre sí y sean $a_1, a_2,\ldots,a_k$ números enteros arbitrarios, sucede que:

$$\begin{cases} x \equiv a_1(mod\, m_1) \\ x \equiv a_2(mod\, m_2) \\ \ldots \\ x \equiv a_k(mod\, m_k) \end{cases} \Rightarrow \text{Tiene única solución en módulo } m, \text{ donde } m = m_1 \cdot m_2 \cdot \ldots \cdot m_k. \quad 0 \le x \le m$$

$$x = a_1 \cdot \frac{m}{m_1} \cdot \left[\frac{m}{m_1}\right]_{m_1}^{-1} + a_2 \cdot \frac{m}{m_2} \cdot \left[\frac{m}{m_2}\right]_{m_2}^{-1} + \cdots + a_k \cdot \frac{m}{m_k} \cdot \left[\frac{m}{m_k}\right]_{m_k}^{-1}$$

EJEMPLO:

$$\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ \ 7) \end{cases} \Rightarrow \quad x = 2 \cdot 35 \cdot [35]_3^{-1} + 3 \cdot 21 \cdot [21]_5^{-1} + 2 \cdot 15 \cdot [15]_7^{-1} =$$

$$x = 2 \cdot 35 \ \cdot 2 + 3 \cdot 21 \ \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv \boxed{23\ (mod\ 105)}$$

O infinitas soluciones: $23 + \lambda \cdot 105\ ,\ \lambda \in \mathbb{Z}$

2.8. CRITERIOS DE DIVISIBILIDAD

→ Criterio del 2: acaba en cifra par.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0\ (mod\ 2)$$

→ Criterio del 3: la suma de sus cifras es múltiplo de 3.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0\ (mod\ 3)$$

→ Criterio del 4: la suma de sus cifras son múltiplo de 4.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_1 \cdot 10 + a_0 \equiv a_1 a_0\ (mod\ 4)$$

→ Criterio del 5: el último dígito es 0 o 5.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0\ (mod\ 5)$$

→ Criterio del 7:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv \ldots - a_3 + 2a_2 + 3a_1 + a_0\ (mod\ 7)$$

$10^1 \equiv 3\ (mod\ 7)$
$10^2 \equiv 3 \cdot 3 \equiv 2\ (mod\ 7)$
$10^3 = 2 \cdot 3 = -1\ (mod\ 7)$
…

→ Criterio del 8: las tres últimas cifras son múltiplo de 8.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_2 a_1 a_0\ (mod\ 8)$$

→ Criterio del 9: la suma de sus cifras es múltiplo de 9.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + a_2 + a_1 + a_0\ (mod\ 9)$$

→ Criterio del 11: la suma de sus cifras pares (empezando por el 0) menos sus cifras impares es múltiplo de 11.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0\ (mod\ 11)$$

$10^1 \equiv -1\ (mod\ 11)$
$10^2 \equiv -1 \cdot (-1) \equiv 1\ (mod\ 11)$
$10^3 \equiv 1 \cdot (-1) \equiv -1\ (mod\ 11)$
…

2.9. ALGORITMO DE EXPONENCIACIÓN BINARIA

$b^e = b \cdot b \cdot b \cdot b \cdot \ldots$; e veces.
$e = 2^k + 2^n + \cdots + 2^s$
$b^e = b^{2^k} \cdot b^{2^n} \cdot \ldots \cdot b^{2^s}$

EJEMPLO:

$7^{51} = 7 \cdot 7 \cdot 7 \cdot 7 \cdot \ldots$; 51 veces
$51 = 32 + 16 + 2 + 1 = 2^5 + 2^4 + 2^1 + 2^0 \equiv (110011)_2$

$$\left.\begin{array}{l} 7 \\ 7^2 \\ 7^2 \cdot 7^2 = 7^4 = 7^{2^2} \\ 7^4 \cdot 7^4 = 7^8 = 7^{2^3} \\ 7^8 \cdot 7^8 = 7^{16} = 7^{2^4} \\ 7^{16} \cdot 7^{16} = 7^{32} = 7^{2^5} \end{array}\right\} \quad 7^{51} = 7^{32} \cdot 7^{16} \cdot 7^2 \cdot 7^1$$

2.10. CRIPTOGRAFÍA (RSA)

1) Escogemos dos primos muy grandes: p y q.
2) Calculamos $n = p \cdot q$
3) Al conocer p y q, se pueden elegir dos números e y d tal que para todo m:

$$(m^e)^d = m \ (mod\ n)$$

   → Escogemos e con inverso multiplicativo módulo $\phi(n) = (p-1) \cdot (p+1)$.
   → Escogemos d como el inverso de e módulo $\phi(n)$, es decir, $d \cdot e \equiv 1 \ (mod\ \phi(n))$

4) Ciframos el mensaje:

$$E(m) \equiv m^e (mod\ n)$$

5) Desciframos el mensaje:

$$E(m)^d = (m^e)^d \equiv m (mod\ n)$$

TEMA 2. COMBINATORIA

1. PRINCIPIOS BÁSICOS DE CONTEO

1.1. PRINCIPIO DE ADICIÓN

Sean A y B conjuntos disjuntos ($A \cap B = \emptyset$), entonces: $|A \cup B| = |A| + |B|$.

Si un suceso A puede ocurrir m veces distintas y otro suceso B puede ocurrir de k maneras diferentes, y ambos sucesos no pueden ocurrir simultáneamente, entonces el suceso "A o B" puede ocurrir de $m + k$ maneras.

Si $A_1, A_2, \dots, A_n$ conjuntos finitos distintos dos a dos, $Ai \cap A_j = \emptyset; (i \neq j)$, entonces $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.

1.2. PRINCIPIO DE LA DIFERENCIA

Si U es el universo, entonces $|U| = |A| + |\bar{A}| \Rightarrow |A| = |U| - |\bar{A}|$

1.3. PRINCIPIO DE LA MULTIPLICACIÓN

Si una tarea puede dividirse en 2 subtareas consecutivas de manera que hay n formas distintas de realizar la primera subtarea y, para cada una de ellas, hay k formas de realizar la segunda subtarea, entonces hay $n \cdot k$ formas distintas de completar la tarea.

1.4. PRINCIPIO DE LA BIYECCIÓN

Sean A y B dos conjuntos finitos y sea $f: A \to B$ biyectiva, entonces $|A| = |B|$

1.5. PRINCIPIO DEL PALOMAR

Si tenemos $n + 1$ "palomas" y n "nidales", entones al menos 2 "palomas" tienen que estar en el mismo "nidal".

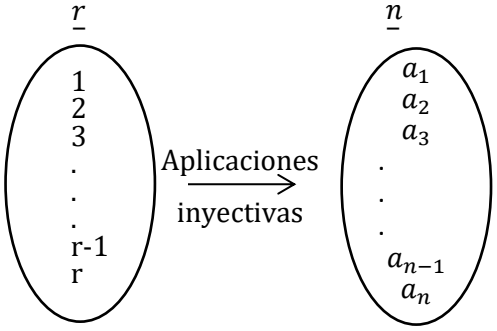
Si tenemos n "palomas" y k "nidales", entonces al menos alguna caja contiene por lo menos $\left\lceil \frac{n}{k} \right\rceil$.

2. SELECCIONES

En las variaciones influye el orden, pero en las combinaciones no.

2.1. SELECCIONES ORDENADAS SIN REPETICIONES

Sea $A = \{a_1, a_2, \dots, a_n\}$ un conjunto finito de n elementos y r un número natural tal que $r \leq n$, una variación de orden r de los n elementos es una lista o selección ordenada de r elementos distintos de A.



POSIBILIDADES:
$1 \rightarrow n$ posiciones posibles
$2 \rightarrow n - 1$ posiciones posibles
$3 \rightarrow n - 2$ posiciones posibles
.
.
.
$r - 1 \rightarrow n - (r - 2)$ posiciones posibles
$r \rightarrow n - (r - 1)$ posiciones posibles

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

EJEMPLO:

En el conjunto A de 3 elementos, ¿cuántos grupos de 2 se pueden formar?

$A = \{a, b, c\}$; $n = 3$ y $r = 2$

$V(3,2) = \frac{3!}{(3-2)!} = \frac{3 \cdot 2}{1} = 6$; donde los grupos son $[a, b], [a, c], [b, a], [b, c], [c, a], [c, b]$.

2.1.1. PERMUTACIONES

Un caso particular es cuando $r = n$, lo que hace que la aplicación sea biyectiva.

$$P(n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

EJEMPLO:

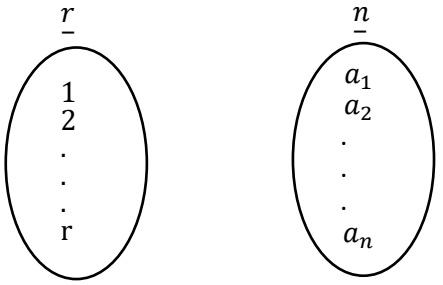
En el conjunto A de 3 elementos, ¿cuántos grupos de 3 se pueden formar?

$A = \{a, b, c\}$; $n = 3$ y $r = 3$

$P(3) = 3! = 6$; donde los grupos son $[a, b, c], [a, c, b], [b, a, c], [b, c, a], [c, b, a], [c, a, b]$.

2.2. SELECCIONES ORDENADAS CON REPETICIONES

Sea $A = \{a_1, a_2, \dots, a_n\}$ un conjunto finito de n elementos y r un número natural cualquiera, una variación de orden r con repetición de los n elementos de A es una lista o selección ordenada de n elementos no necesariamente distintos del conjunto A.



POSIBILIDADES:
$1 \rightarrow n$ posiciones posibles
$2 \rightarrow n$ posiciones posibles
.
.
.
$r \rightarrow n$ posiciones posibles

$$VR(n, r) = n \cdot n \cdot n \cdot \dots \cdot n;\ r\ veces = n^r$$

EJEMPLO:

En el conjunto A de 3 elementos, ¿cuántos grupos de 2 se pueden formar?

$A = \{a, b, c\}$; $n = 3$ y $r = 2$

$VR(3,2) = 3^2 = 9$; donde los grupos son $[a, a], [b, b], [c, c], [a, b], [a, c], [b, a], [b, c], [c, a], [c, b]$.

2.3. SELECCIONES NO ORDENADAS SIN REPETICIONES

Sea $A = \{a_1, a_2, \dots, a_n\}$ un conjunto finito de n elementos y r un número natural tal que $r \leq n$, una combinación de orden r de los n elementos de A es un subconjunto (selección no ordenada) de r elementos distintos de A.

$$C(n, r) \cdot r! = V(n, r)$$

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

EJEMPLO:

¿Cuántas cadenas de 8 bits hay que tengan exactamente 3 ceros?

$$C(8,3) = \binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \cdot 7 \cdot 6 \cdot 5!}{3! \cdot 5!} = 56$$

2.4. SELECCIONES NO ORDENADAS CON REPETICIONES

Sea $A = \{a_1, a_2, \dots, a_n\}$ un conjunto finito de n elementos y r un número natural, una combinación con repetición de orden r de los n elementos de A es una selección no ordenada de r elementos no necesariamente distintos de A.

$$CR(n,r) = \binom{n-1+r}{r}$$

EJEMPLO:

Habiendo 4 sabores de helado, al comprar 10, ¿cuántas combinaciones de helados se pueden hacer?

$Sabores = \{F, N, C, V\}$; $n = 4$ y $r = 10$

$$CR(4,10) = \binom{13}{10} = \frac{13!}{3!\,10!} = \frac{13 \cdot 12 \cdot 11 \cdot 10!}{3 \cdot 2 \cdot 10!} = 286$$

2.4.1. PERMUTACIONES CON REPETICIÓN

Si disponemos de r tipos distintos de objetos con la condición de que los objetos de un mismo tipo son iguales entre sí y diferentes de otros tipos, las distintas ordenaciones que se puedan hacer con los n objetos se llaman permutaciones con repetición de n objetos con $n_1, n_2, \dots, n_r$ repeticiones.

$$PR(n; n_1, n_2, \dots, n_r) = \frac{n!}{n_1!\, n_2! \dots n_r!}$$

EJEMPLO:

¿Cuántas palabras (con o sin sentido) puedes realizar con la palabra C A S A C A ?

$$\begin{cases} 2 \text{ letras de tipo C} \\ 3 \text{ letras de tipo A} \\ 1 \text{ letra de tipo S} \end{cases}$$

$$PR(6; 3,2,1) = \frac{6!}{3!2!1!} = \frac{6 \cdot 5 \cdot 4 \cdot 3!}{3! \cdot 2} = 60$$

2.5. TABLAS RESUMEN

Selecciones de n elementos de orden r	Ordenadas	No ordenadas
Sin repetición	$V(n,r) = \frac{n!}{(n-r)!}$	$C(n,r) = \binom{n}{r} = \frac{n!}{r!\,(n-r)!}$
Con repetición	$VR(n,r) = n^r$	$CR(n,r) = \binom{n-1+r}{r} = \frac{(n-1+r)!}{r!\,(n-1)!}$

Distribuir r objectos en n cajas distintas	Sin restricción	Cajas no vacías (al menos 1 objeto)	A lo sumo 1 objecto
Objetos diferentes	Aplicaciones $VR(n,r) = n^r$	Aplicación sobreyectiva	Aplicación inyectiva $V(n,r) = \frac{n!}{(n-r)!}$
Objetos iguales	$CR(n,r) = \binom{n-1+r}{r}$	$CR(n,r-n) = \binom{r-1}{r-n} = \binom{r-1}{n-1}$	$C(n,r) = \binom{n}{r}$
		$r \geq n$	$r \leq n$

3. COEFICIENTES BINOMIALES Y MULTINOMIALES

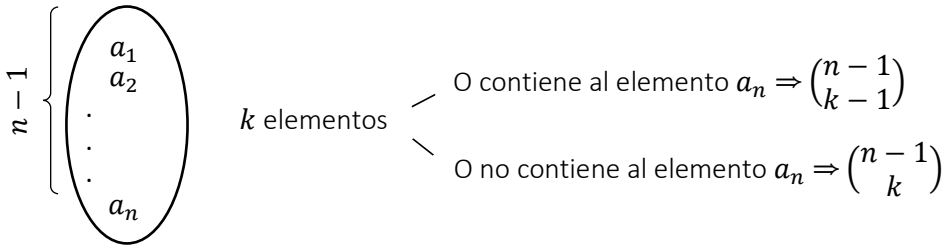
→ Binomio Newton: $(x+y)^2 = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k}$

→ Multinomio Leitnitz: $(x_1 + x_2 + \cdots + x_n)^n = \sum_{n_1+n_l+\cdots+n_k} \binom{n}{n_1 n_2 \ldots n_k} x^{n_1} x^{n_2} \ldots x_k^{n_k}$

3.1. FÓRMULA (IDENTIDAD) PASCAL

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

El número de subconjuntos de k elementos que hay en un conjunto de n elementos.



3.2. TRIÁNGULO DE PASCAL

$n = 0 \rightarrow \quad \binom{0}{0} = 1$

$n = 1 \rightarrow \quad \binom{1}{0} = 1 \quad \binom{1}{1} = 1$

$\backslash + /$

$n = 2 \rightarrow \quad \binom{2}{0} = 1 \quad \binom{2}{1} = 2 \quad \binom{2}{2} = 1$

$n = 3 \rightarrow \quad \binom{3}{0} = 1 \quad \binom{3}{1} = 3 \quad \binom{3}{2} = 3 \quad \binom{3}{3} = 1$

$n = 4 \rightarrow \quad \binom{4}{0} = 1 \quad \binom{4}{1} = 4 \quad \binom{4}{2} = 6 \quad \binom{4}{3} = 4 \quad \binom{4}{4} = 1$

...

4. PRINCIPIO DE INCLUSIÓN-EXCLUSION

Para dos conjuntos: $|A \cup B| = |A| + |B| - |A \cap B|$

Para tres conjuntos: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Para n conjuntos: $|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^{n}|A_i| - \sum_{1\le i<j\le n}|A_i \cap A_j| + \sum_{1\le i<j<k\le n}|A_i \cap A_j \cap A_k| + \cdots + (-1)^n \sum_{i=1}^{n}|A_i \cap A_i \cap \hat{A}_i \cap \dots \cap A_n| + (-1)^{n+1}|A_i \cap A_i \cap \hat{A}_i \cap \dots \cap A_n|$

* $\hat{A}_i$ significa que no aparece, así: $|A \cup B \cup C| = \cdots - |A \cap B \cap \hat{C}| - |A \cap \hat{B} \cap C| - |\hat{A} \cap B \cap C| + \cdots$

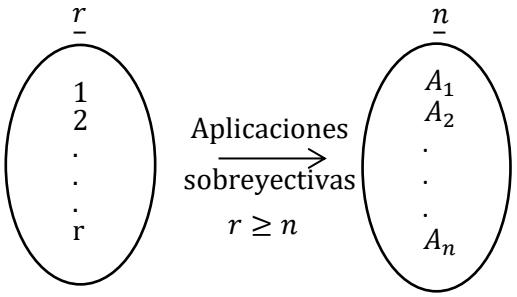
EJEMPLO:

¿Cuántos números enteros positivos, $1 \le x \le 100$, que son múltiplos de 4 o múltiplos de 6?

A = "múltiplos de 4"
B = "múltiplos de 6"
$\Big\}\ |A \cup B| = |A| + |B| - |A \cap B| = 25 + 16 - 8 = 33$

$|A| = \left\lfloor \frac{100}{4} \right\rfloor = 25$; $|B| = \left\lfloor \frac{100}{6} \right\rfloor = 16$; $|A \cap B| = \left\lfloor \frac{100}{12} \right\rfloor = 8$

4.1. APLICACIONES SOBREYECTIVAS



$A_i = \{f / la\ caja\ A_i\ no\ sea\ imagen\ (esté\ vacía)\}$

Aplicaciones sobreyectivas = todas las aplicaciones – aplicaciones que no sean sobreyectivas

Todas las aplicaciones se calculan aplicando variaciones con repetición y las aplicaciones que no sean sobreyectivas se calculan aplicando PIE.

$$|T| - |A_1 \cup A_2 \cup \dots \cup A_n|$$

$|T| = n^r$

$|A_1| = (n-1)^r$

$|A_1 \cap A_2| = (n-2)^r$

$|A_1 \cup A_2 \cup \dots \cup A_i| = (n-i)^r$

$|A_1 \cup A_2 \cup \dots \cup A_n| = 0$

TEOREMA

El número de aplicaciones sobreyectivas que hay entre $\underline{r} \to \underline{n}$, $r \ge n$, es:

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

EJEMPLO:

Distribuir 6 objetos diferentes en 4 cajas diferentes de forma que ninguna caja quede vacía.

$$6\sum_{k=0}^{4} (-1)^k \binom{4}{k} (4-k)^6 = \binom{4}{0}4^6 - \binom{4}{1}3^6 + \binom{4}{2}2^6 - \binom{4}{3}1^6 + \binom{4}{4}0^6$$

TEMA 3. RECURSIVIDAD

1. INTRODUCCIÓN

Una sucesión en S es una aplicación $\mathbb{N} \to S$. La recursión consiste en definir un "objeto" en términos de sí mismo.

EJEMPLO: $7, 17, 27, 37, \ldots \quad \Rightarrow \quad S_n = 7 + n \cdot 10$

Una función recursiva de una sucesión específica uno o más términos iniciales y una regla para determinar términos siguientes en función de los precedentes (relación de recurrencia).

Una relación de recurrencia para la sucesión $\{a_n\}$ es una ecuación (fórmula) que expresa a_n en términos de uno o más términos anteriores de la sucesión $a_0, a_1, \ldots, a_{n-1}$. Una sucesión se llama solución de una relación de recurrencia si sus términos satisfacen la propia relación de recurrencia, dando una fórmula explícita para el cálculo del término n-ésimo.

2. RELACIÓN DE RECURRENCIA LINEAL HOMOGÉNEA

Se llama relación de recurrencia lineal homogénea con coeficientes constantes (RRLHCC) de orden k a una expresión de la forma:

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k}$$

Donde c_i son constantes y $c_k \neq 0$.

Hay tantas condiciones iniciales como el orden RRLHCC.

2.1. ECUACIÓN CARACTERÍSTICA

Partiendo de la relación de recurrencia:

$$a_n = \{r^n\} \quad \Rightarrow \quad r^n = c_1 \cdot r^{n-1} + c_2 \cdot r^{n-2} + \cdots + c_k \cdot r^{n-k}$$

Dividimos por r^{n-k}:

$$r^k = c_1 \cdot r^{k-1} + c_2 \cdot r^{k-2} + \cdots + c_k \quad \Rightarrow \quad \boxed{r^k - c_1 \cdot r^{k-1} - c_2 \cdot r^{k-2} - \cdots - c_k = 0}$$

2.2. RESOLCUCIÓN DE RRLHCC

TEOREMA RAÍCES CARACTERÍSTICAS DISTINTAS

Sea $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k}$ una RRLHCC de orden k y sus raíces características son $r_1, r_2, \ldots, r_k$. Entonces, las soluciones de RR vienen dadas por:

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_n r_k^n$$

TEOREMA RAÍCES CARACTERÍSTICAS REPETIDAS

Sea $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k}$ una RRLHCC de orden k y sus raíces características son $r_1, r_2, \ldots, r_S$ de multiplicidades $m_1, m_2, \ldots, m_S$ respectivamente. Entonces, las soluciones de RR vienen dadas por:

$$a_n = \left(\alpha_{10} + \alpha_{11} n + \cdots + \alpha_{m_1 - 1} n^{m_1 - 1}\right) r_1^n + \cdots + \left(\alpha_{s0} + \alpha_{s1} n + \cdots + \alpha_{m_s - 1} n^{m_s - 1}\right) r_s^n$$

EJEMPLO: Raíces características distintas en RRLHCC

$$a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3} \qquad \begin{cases} a_0 = 8 \\ a_1 = 6 \\ a_2 = 26 \end{cases}$$

ES UNA RRLHCC $\Rightarrow$ EC. CARACTERÍSTICA:

$$r^n = -r^{n-1} + 4r^{n-2} + 4 \cdot r^{n-3} \Rightarrow r^3 = -r^2 + 4r + 4$$

$$r^3 + r^2 - 4r - 4 = 0 \Rightarrow \begin{cases} r_1 = -1 \\ r_2 = 2 \\ r_3 = -2 \end{cases}$$

LAS SOLUCIONES SON:

$$a_0 \to 8 = \alpha_1 (-1)^0 + \alpha_2 (2)^0 + \alpha_3 (-2)^0 \Rightarrow 8 = \alpha_1 + \alpha_2 + \alpha_3$$

$$a_1 \to 6 = \alpha_1 (-1)^1 + \alpha_2 (2)^1 + \alpha_3 (-2)^1 \Rightarrow 6 = -\alpha_1 + 2\alpha_2 - 2\alpha_3$$

$$a_2 \to 26 = \alpha_1 (-1)^2 + \alpha_2 (2)^2 + \alpha_3 (-2)^2 \Rightarrow 26 = \alpha_1 + 4\alpha_2 + 4\alpha_3$$

TRAS RESOLVER

$$\begin{cases} \alpha_1 = 2 \\ \alpha_2 = 5 \\ \alpha_3 = 1 \end{cases}$$

EJEMPLO: Raíces características iguales en RRLHCC

$$a_n = 8a_{n-2} - 16a_{n-4} \qquad \begin{cases} a_0 = 1 \\ a_1 = 4 \\ a_2 = 28 \\ a_3 = 32 \end{cases}$$

ES UNA RRLHCC $\Rightarrow$ EC. CARACTERÍSTICA:

$$r^n = 8 \cdot r^{n-2} - 16 r^{n-4} \Rightarrow r^4 = 8r^2 - 16$$

$$r^4 - 8r^2 + 16 = 0 \Rightarrow \begin{cases} r_1 = 2 \\ r_2 = 2 \end{cases} \; r_1 = 2 \text{ multiplicidad } 2$$

$$\begin{cases} r_3 = -2 \\ r_4 = -2 \end{cases} \; r_2 = -2 \text{ multiplicidad } 2$$

LAS SOLUCIONES SON:

$$a_0 \to 1 = (\alpha_{10} + \alpha_{11} \cdot 0) 2^0 + (\alpha_{20} + \alpha_{21} \cdot 0)(-2)^0 \Rightarrow 1 = \alpha_1 + \alpha_3$$

$$a_1 \to 4 = (\alpha_{10} + \alpha_{11} \cdot 1) 2 + (\alpha_{20} + \alpha_{21} \cdot 1)(-2) \Rightarrow 4 = 2\alpha_{10} + 2\alpha_{11} - 2\alpha_{20} - 2\alpha_{21}$$

$$a_2 \to 28 = (\alpha_{10} + \alpha_{11} \cdot 2) 2^2 + (\alpha_{20} + \alpha_{21} \cdot 2)(-2)^2 \Rightarrow 28 = 4\alpha_{10} + 8\alpha_{11} + 4\alpha_{20} + 8\alpha_{21}$$

$$a_3 \to 32 = (\alpha_{10} + \alpha_{12} \cdot 3) 2^3 + (\alpha_{20} + \alpha_{21} \cdot 2)(-2)^2 \Rightarrow 32 = 8\alpha_{10} + 24\alpha_{11} - 8\alpha_{20} - 24\alpha_{21}$$

TRAS RESOLVER $\Rightarrow$

$$\begin{cases} \alpha_{10} = 1 \\ \alpha_{11} = 2 \\ \alpha_{20} = 0 \\ \alpha_{21} = 1 \end{cases}$$

3. RELACIÓN DE RECURRENCIA LINEAL NO HOMOGÉNEA

Se llama relación de recurrencia lineal no homogénea con coeficientes constantes (RRLnHCC) de orden k a una expresión de la forma:

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k} + L(n)$$

Donde c_i son constantes, $c_k \neq 0$ y $L(n)$ es la parte no homogénea.

3.1. RESOLUCION DE RRLNHCC

Si $a_n^{(p)}$ es una solución particular de la RRLnHCC y $a_n^{(h)}$ es una solución de la parte homogénea, entonces $a_n = a_n^{(h)} + a_n^{(p)}$ es una solución de la RRLnHCC y, además, todas las soluciones son de esta forma.

TEOREMA SOLUCIONES PARTICULARES

Dada una RRLnHCC $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k} + L(n)$ con $L(n) = (p_0 + p_1 n + \cdots + p_t n^t)s^n$ siendo p_i y s constantes.

1) Si s no es raíz de la ecuación característica de la RRH asociada, entonces la RRLnHCC admite como solución particular:
$$a_n^{(p)} = (\beta_0 + \beta_1 + \cdots + \beta_t n^t)s^n$$
2) Si s es raíz de la ecuación característica de la RRH asociada, entonces la RRLnHCC admite como solución particular:
$$a_n^{(p)} = (\beta_0 + \beta_{1^n} + \cdots + \beta + n^+)s^n \cdot n^m$$

En ambos casos, $\beta_0, \beta_1, \beta_t$ son números y m es la multiplicidad de la raíz s.

EJEMPLO: s no es raíz de la ecuación característica en RRLnHCC

$a_n = 2a_{n-1} - a_{n-2} + 2^n$ $\begin{cases} a_0 = 5 \\ a_1 = 3 \end{cases}$

parte homogénea | parte no homogénea.

1) Hallamos la ec. característica asociada a la parte homogénea:

$r^2 = 2r - 1 \Rightarrow r^2 - 2r + 1 = 0 \rightarrow \begin{cases} r_1 = 1 \\ r_2 = 1 \end{cases}$ $r = 1$ multiplicidad 2

2) Hallamos las soluciones de la parte particular (2 no es raíz de la ec. característica):

$a_n^{(p)} = B_0 2^n$

3) Sustituimos en la ec. principal:

$B_0 2^n = 2B_0 2^{n-1} - B_0 2^{n-2} + 4 \cdot 2^n$

$4B_0 2^n = 4B_0 2^n - B_0 \cdot 2^n + 4 \cdot 2^n$

$4B_0 2^n = (3B_0 + 4)2^n$

$B_0 = 4$ → SOLUCIÓN PARTICULAR: $a_n^{(p)} = 4 \cdot 2^n$

4) Hallamos las soluciones de la parte particular

$a_n^{(h)} = (\alpha_0 + \alpha_1 n) \cdot 1^n$

$a_n = a_n^{(h)} + a_n^{(p)} \Rightarrow a_n = \alpha_0 + \alpha_1 n + 4 \cdot 2^n$

$a_0 \to 5 = \alpha_0 + 4 \Rightarrow \boxed{\alpha_0 = 1}$

$a_1 \to 3 = \alpha_0 + \alpha_1 + 8 \Rightarrow \boxed{\alpha_1 = -6}$

5) La relación de recurrencia:

$$\boxed{a_n = 1 - 6n + 4 \cdot 2^n}$$

EJEMPLO: *s* es raíz de la ec. característica en RRLnHCC

$a_n = \underbrace{3a_{n-1} - 2a_{n-2}}_{\text{parte homogénea}} + \underbrace{n \cdot 2^n}_{\text{parte no homogénea}}$

1) Hallamos la ec. característica asociada a la parte homogénea:

$r^2 = 3r - 2 \Rightarrow r^2 - 3r + 2 = 0 \to r_1 = 2, \; r_2 = 1$

3) Hallamos las soluciones de la parte particular (2 es raíz)

$a_n^{(p)} = (\beta_0 + \beta_1 n) n \cdot 2^n$

4) Sustituimos en la ec. principal:

$(\beta_0 + \beta_1 n) n \cdot 2^n = 3(\beta_0 + \beta_1 (n-1))(n-1) 2^{n-1} - 2(\beta_0 + \beta_1 (n-2))(n-2) 2^{n-2} + n 2^n$

TRAS RESOLVER $\Rightarrow \boxed{\beta_0 = -1 \; ; \; \beta_1 = 1}$

SOLUCIÓN PARTICULAR: $a_n^{(p)} = (n-1) n 2^n$

4) Hallamos las soluciones de la parte homogénea:

$a_n^{(h)} = \alpha_1 2^n + \alpha_2$

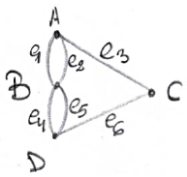
$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 2^n + \alpha_2 + (n-1) \cdot n \cdot 2^n$

SE APLICARÍAN LAS CONDICIONES INICIALES.

TEMA 4. GRAFOS

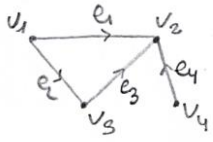
1. CONCEPTOS

Un grafo es un par $G = (V, E)$, donde V es un conjunto finito "no vacío" de elementos llamados vértices (nodos) y E es un conjunto de elementos llamados ejes (aristas).



Si los ejes son "pares no ordenados" de vértices de V, se trata de un grafo no dirigido o grafo. $e_3 = \{A, C\} = \{C, A\}$

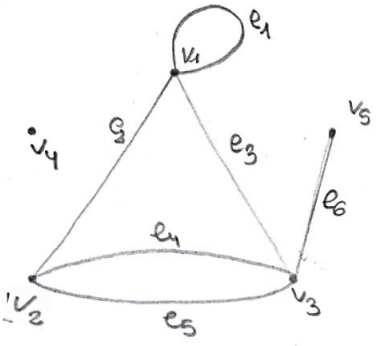
Si los ejes son pares ordenados de vértices de V, se trata de un grafo dirigido o digrafo. $e_3 = (v_1, v_2) \neq (v_2, v_1)$



El cardinal de los vértices se llama orden de un grafo y el cardinal de los ejes, tamaño del grafo.

Un vértice que no está conectado a ningún otro vértice se llama vértice aislado (v_4). Un vértice con un único eje, se llama hoja (v_5).

Si un par de vértices están conectados por más de un eje, esos ejes se llaman ejes paralelos o múltiples (e_4, e_5).



Un par de vértices se dicen adyacentes si existe un eje que los conecte.

Se dice que un eje e índice en dos vértices u, v si e conecta a u y v. En este caso, u y v son los extremos del eje.

El grado de un vértice v, $\delta(v)$, es el número de ejes incidentes en él. La sucesión de grados de G, $\{\delta(v)\}_{v \in V}$, es la sucesión de los grados de los vértices de G.

→ <u>Lema (Apretón de manos)</u>: la suma de los grados de los vértices es 2 veces el número de ejes.

$$\sum_{v} \delta(v) = 2|E|$$

→ <u>Corolario</u>: el número de vértices de grao impar es par.

$$\sum_{v_{par}} \delta(v) + \sum_{v_{impar}} \delta(v) = 2|E|$$

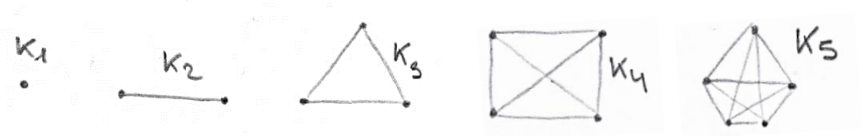
Un vértice que conecta el mismo vértice se llama lazo (e_1). El lazo cuenta dos veces en el grado del vértice.

Un grafo se dice simple si no tiene lazos ni ejes múltiples. Si un grafo es simple: $0 \leq \delta(v) \leq |V| - 1$

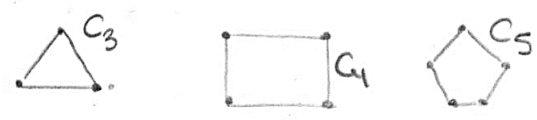
Si un grafo es simple y todos los vértices tiene el mismo grado, r, se llama un grafo r-regular.

2. ALGUNOS TIPOS DE GRAFOS SIMPLES

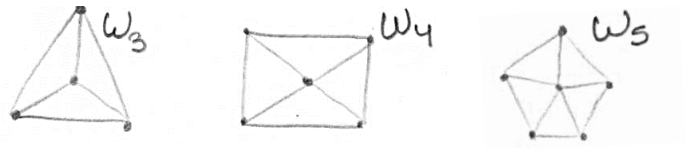
→ Grafo completo de n vértices: K_n



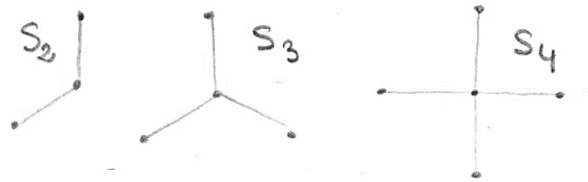
→ Ciclo de orden n, $n \geq 3$: C_n



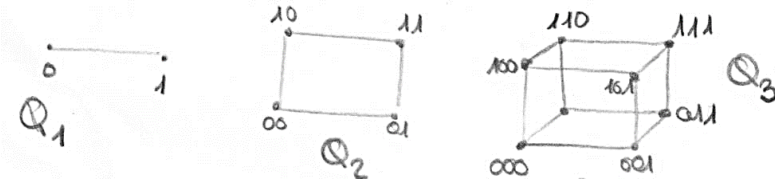
→ Ruedas (Wheel), $n \geq 3$: W_n



→ Estrella (Star): S_n



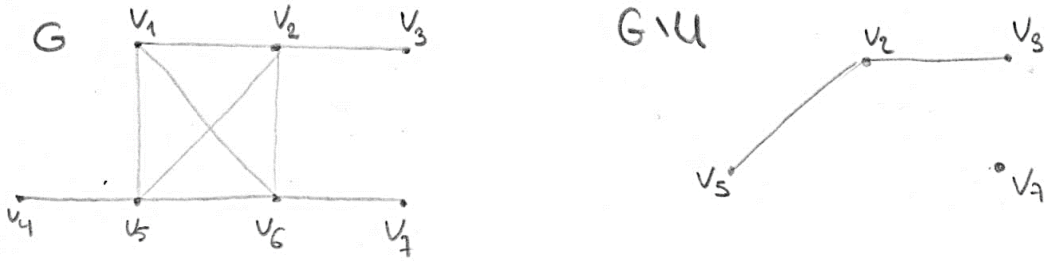
→ N-cubo, $n \geq 1$: Q_n



3. SUBGRAFOS

Sea $G = (V, E)$ un grafo. Si $G' = (V', E')$ es otro grafo donde $V' \subset V$ y $E' \subset E$, se dice que G' es un subgrafo de G.

Sea $G = (V, E)$ un grafo, $U \subset V$ donde $U \neq \emptyset$ y sea $G \setminus U$ un subgrafo de G que se detiene al eliminar los vértices de U del grafo G (y os ejes que coinciden en los vértices de U). Donde $U = \{v_1, v_4, v_6\}$:

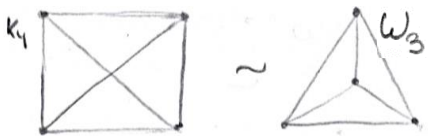


4. GRAFOS ISOMORFOS

Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos, se dice que G y G' son isomorfos si existen dos aplicaciones biyectivas $\varphi; V \to V'$ y $\psi; E \to E'$, tal que:

$$e = \{v_i, v_j\} \in E \Leftrightarrow \psi(e) = \{\varphi(v_i), \varphi(v_j)\} \in E'$$

EJEMPLO: K_4 y W_3 son isomorfos.

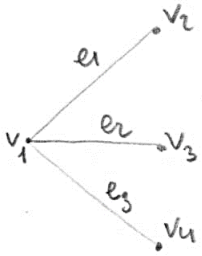


Para conservar el isomorfismo, hay ciertas propiedades invariantes. Así lo son el orden, tamaño y la sucesión de grados.

5. REPRESENTACIÓN ESQUEMATIZADA

5.1. TABLAS DE ADYACENCIA

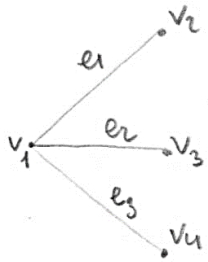
Sea $G = (V, E)$ un grafo. La tabla de adyacencia del grafo es una tabla que da una lista de los vértices y los vértices adyacentes con el mismo.



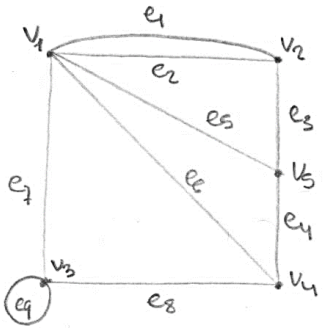
$\boldsymbol{v}$	$\boldsymbol{v}$ adyacentes
$\boldsymbol{v_1}$	v_2, v_3, v_4
$\boldsymbol{v_2}$	v_1
$\boldsymbol{v_3}$	v_1
$\boldsymbol{v_4}$	v_1

5.2. MATRIZ DE ADYACENCIA

Sea $G = (V, E)$ un grafo tal que $|V| = n$ donde $V = \{v_1, v_2, \dots, v_n\}$. La matriz de adyacencia del grafo es una matriz cuadrada de orden n, $A = (a_{ij})$, siendo a_{ij} el número de ejes que conectan el vértice v_i con v_j.



$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$



$$A = \begin{pmatrix} 0 & 2 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

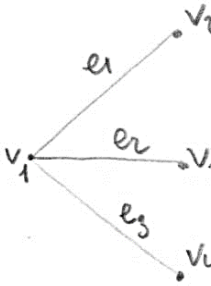
La matriz de adyacencia es una matriz simétrica. Se cumple que:

$$2a_{ii} + \sum_{i \neq j} a_{ij} = \delta(v_i)$$

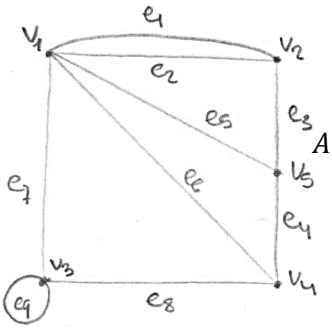
Si G es un grafo simple, entonces la matriz de adyacencia es una matriz binaria (solo tiene 0 y 1). Además, en la diagonal todos los elementos son 0.

5.3. MATRIZ DE INCIDENCIA

Sea $G = (V, E)$ un grafo tal que $|V| = n$ donde $V = \{v_1, v_2, \dots, v_n\}$ y $|E| = m$ donde $E = \{e_1, e_2, \dots, e_m\}$. La matriz de incidencia del grafo es una matriz $n \times m$, $B = (b_{ij})$, siendo $b_{ij} = 1$ si v_i incide con el eje e_j o $b_{ij} = 0$ en otro caso.



$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Siempre es una matriz binaria.

6. PROPIEDADES

6.1. CONECTIVIDAD

Sea $G = (V, E)$ un grafo.

Un camino o trayectoria de un vértice v a otro vértice w es una secuencia de ejes (no necesariamente distintos) de G de la forma: $e_1 = \{v, v_1\}, e_2 = \{v_1, v_2\}, \cdots, e_n = \{v_n, w\}$, donde v es el vértice inicial y w el vértice final.

El número de ejes es la longitud del camino.

Un camino donde $v = w$ se dice camino cerrado (ciclo, circuito).

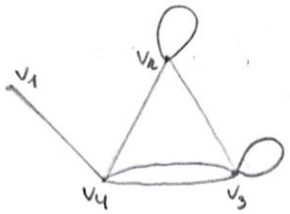
Un camino en el que todos los ejes sean distintos se llama camino simple.

TEOREMA

Sea $G = (V, E)$ un grafo tal que $|V| = n$ y sea A su matriz adyacente con respecto a $V = \{v_1, v_2, \dots, v_n\}$. El número de caminos de longitud k que hay entre el vértice v_i y el vértice v_j es la entrada (i, j) de la matriz A^k.

EJEMPLO: ¿Cuantos caminos hay de longitud 3 entre v_4 y v_1 en la siguiente figura?

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 2 & 0 \end{pmatrix}; \quad A^3 = A \cdot A \cdot A = \begin{pmatrix} 0 & 3 & 3 & 6 \\ 3 & 10 & 13 & 12 \\ 3 & 13 & 16 & 18 \\ 6 & 12 & 18 & 9 \end{pmatrix}$$



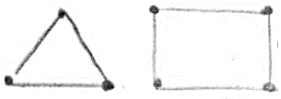
Buscando la posición $(4, 1)$ encontramos que hay 6 caminos posibles.

Se dice que 2 vértices v y w de un grafo G están conectados si $v = w$ o existe un camino que los une.

Un grafo G es conexo si todos los vértices están unidos por un camino. En caso contrario, se dice disconexo (no conexo).

Una componente conexa es un subgrafo conexo maximal (que no está contenido en otro grafo conexo).

Un grafo es conexo si, y solo si, tiene una única componente conexa.



G es disconexo.
Tiene 2 componentes conexas

G' es disconexo.
Tiene 3 componentes conexas

TEOREMA

Sea un grafo G de orden n ($|V| = n$) y sea A su matriz de adyacencia. G es conexa si, y solo si, todas las entradas no diagonales de la matriz $A + A^2 + \cdots + A^{n-1}$ son no nulas.

7. GRAFO BIPARTITO

Sea $G = (V, E)$ un grafo en el que $V = V_1 \cup V_2$ disjunto ($V_1 \cap V_2 = \emptyset$) tal que no haya ejes que incidan en dos vértices de V_1 ni en dos vértices de V_2, entonces G es bipartito.

Si un grafo es bipartito, se puede obtener la partición (V_1, V_2) de la siguiente manera:

$$V_1 = \{w \in V \,/\, d(w,v) = par\} \text{ y } V_2 = \{w' \in V \,/\, d(w',v) = impar\}$$

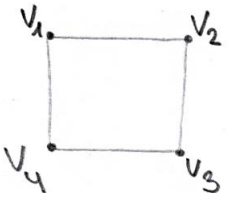
siendo d la longitud del camino más corto entre los dos vértices y v, w, w' siendo vértices cualesquiera.

TEOREMA

Un grafo es bipartito si, y solo si, todos sus ciclos tienen longitud par. De haber al menos un ciclo de longitud impar, no podrá ser bipartito.

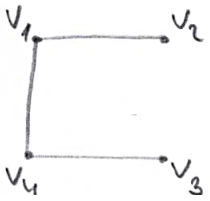
7.1. GRAFO BIPARTITO COMPLETO

Un grafo bipartito se dice completo si todo vértice de V_1 está conectado con todo vértice de V_2 (y recíprocamente).



Bipartito completo

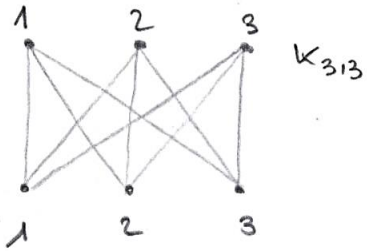
$V_1 = \{v_1, v_3\}$ y $V_2 = \{v_2, v_4\}$



Bipartito no completo

$V_1 = \{v_1, v_3\}$ y $V_2 = \{v_2, v_4\}$

Los grafos bipartitos completos se denominan como $K_{n,m}$ siendo $|V_1| = n$ y $|V_2| = m$. De esta forma, el orden del grafo es $|V| = n + m$ y el tamaño, $|E| = n \cdot m$.



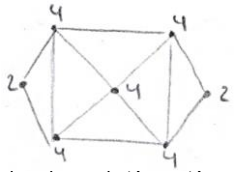
8. GRAFO EULERIANO

En un grafo G, se llama euleriano a un camino simple (no repite ejes) que contiene todos los ejes del grafo G. Se llama un circuito euleriano si es un camino euleriano cerrado.

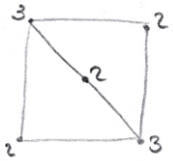
Un grafo se dice euleriano si tiene un circuito euleriano. Un grafo se dice semieuleriano (no es euleriano) si tiene un camino euleriano.

TEOREMA (EULER)

Un grafo conexo es euleriano si, y solo si, todos los vértices tienen grado par.



Un grafo conexo es semieuleriano si, y solo si, todos los vértices tienen grado par excepto dos de ellos.

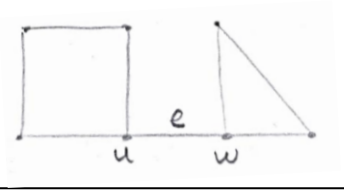


ALGORITMO DE FLEURY

Pasos para encontrar un circuito (camino) euleriano:

1) Se elige un vértice cualquiera.
2) Se recorren todos los ejes que forman un camino con las siguientes condiciones:
   - Cada eje se elimina una vez recorrido (de forma opcional, se eliminan todos los vértices que vayan quedando aislados).
   - Solo se selecciona un eje puente* (de separación) si no hay otra opción.

* Un eje puente (de separación) es un eje, $e = \{u, w\}$, que, al suprimirlo del grafo, el conjunto de vértices que están conectados con u es disjunto del conjunto de vértices que están conectados con w.



9. GRAFO HAMILTONIANO

Un camino hamiltoniano es un camino simple que contiene todos los vértices una única vez. Si el camino es cerrado, se dice un circuito hamiltoniano.

Un grafo es hamiltoniano si tiene un circuito hamiltoniano. Un grafo es semihamiltoniano (no es hamiltoniano) si contiene un camino hamiltoniano.

9.1. CONDICIONES SUFICIENTES

TEOREMA (DIRAC)

Sea $G = (V, E)$ un grafo simple y conexo con n vértices. Si $\delta(v) \geq \frac{n}{2}$ para todo vértice de V, entonces G es hamiltoniano.

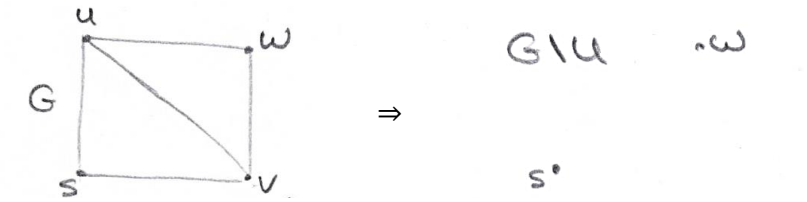
EJEMPLO: los grafos completos simples de n vértices (K_n).

TEOREMA (ORE)

Sea $G = (V, E)$ un grafo simple y conexo con n vértices, $n \geq 2$. Si $\delta(v) + \delta(u) \geq n$ para cualquier par de vértices no adyacentes, entonces G es hamiltoniano.

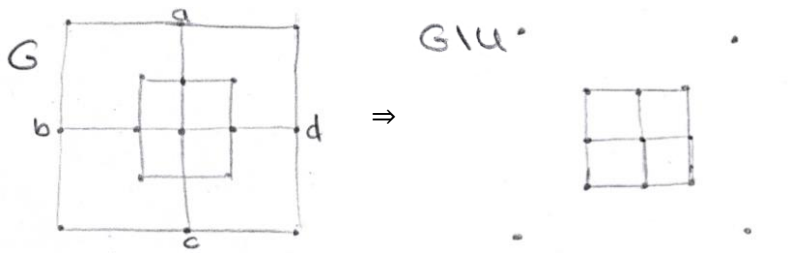
9.2. CONDICIÓN NECESARIA

Si $G = (V, E)$ es hamiltoniano, entonces para cada conjunto tal que $U \subset V$ y $U \neq \emptyset$, el grafo $G \setminus U$ tiene a lo sumo $|U|$ componentes conexas. Donde $U = \{u, v\}$ y luego $U = \{a, b, c, d\}$:



⇒ ⇒ 2 conexiones conexas ≤ $|U|$

Es hamiltoniano

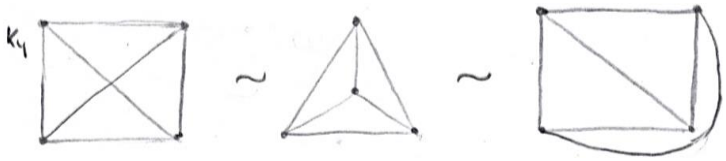


⇒ ⇒ 5 conexiones conexas ≥ $|U|$

No es hamiltoniano

10. GRAFO PLANO

Un grafo se dice plano si puede dibujarse en el plano de manera que ningún par de ejes se corten salvo en los vértices en los que inciden.



K_4 es plano

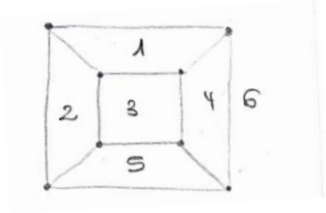
K_5 y $K_{3,3}$ no son planos

TEOREMA KURATOWSKI

Sea $G = (V, E)$ un grafo simple y conexo, G es plano si, y solo si, no contiene ningún subgrafo isomorfo por subdivisiones elementales* de K_5 o $K_{3,3}$.

* Las subdivisiones elementales se hacen tomando un eje y creando en el un vértice, dando lugar a 2 ejes.

Una representación plana de un grafo (mapa) divide al plano en caras o regiones.



FÓRMULA EULER PARA GRAFOS PLANOS

Sea $G = (V, E)$ un grafo simple, conexo y plano, entonces:

$$|C| + |V| = |E| + 2$$

donde C son las caras del plano.

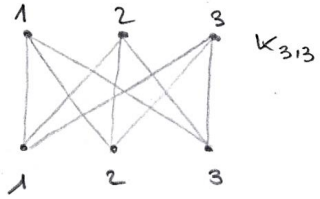
COROLARIO

Sea G un grafo simple, conexo y plano, entonces se cumplen tres condiciones necesarias:

- $\rightarrow$ Si $|V| \geq 3 \Rightarrow |E| \leq 3 \cdot |V| - 6$
- $\rightarrow$ G tiene un vértice de grado menor o igual que 5
- $\rightarrow$ Si $|V| \geq 3$ y no contiene ciclos de longitud 3, entonces $|E| \leq 2 \cdot |V| - 4$

EJEMPLO:

1. Demostración de que $K_{3,3}$ no es plano siguiendo la tercera condición necesaria:



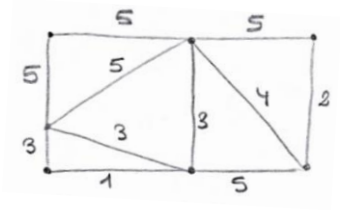
$|V| = 6 \geq 3$ y no tiene circuitos de longitud 3.
$|E| \leq 2 \cdot |V| - 4$
$9 \leq 2 \cdot 6 - 4 = 6 \Rightarrow$ NO

2. Demostración de que K_5 no es plano siguiendo la primera condición necesaria:

$|V| = 5 \geq 3$
$|E| \leq 3 \cdot |V| - 6$
$10 \leq 3 \cdot 5 - 6 = 9 \Rightarrow$ NO

11. GRAFOS PONDERADOS

Sea $G = (V, E)$ un grafo, se dice ponderando si existe una aplicación $\omega: E \to \mathbb{R}^+ \cup \{0\}$ tal que $e \to \omega(e)$ es el peso del eje.



→ Problema del viajante: encontrar el ciclo hamiltoniano de menos peso.
→ Algoritmo Dijktra: calcular el camino más corto entre los vértices.

12. ÁRBOLES

Un árbol es un grafo conexo y sin ciclos.

Sea $G = (V, E)$ un árbol, es equivalente decir:

→ En G cada par de vértices están conectados por un único camino simple.
→ G es conexo y todo eje es de separación.
→ G es conexo y $|V| = |E| + 1$
→ G no tiene ciclos y $|V| = |E| + 1$

12.1. ÁRBOLES GENERADORES

Sea G un grafo conexo, un árbol generador (recubridor, "spanning") de G es un árbol T que es un subgrafo de G y que contiene a todos los vértices de G.

Un árbol generador de peso minimal es un árbol generador en el que su peso es el menor entre todos los árboles generadores posibles del grafo.

ALGORITMO DE PRIM (1957)

Pasos para crear un árbol generador de peso minimal:

1. Se elige un vértice cualquiera del grafo, v. $T_0 = \{v\}$ es el primer árbol.
2. Se considera el conjunto de ejes que inciden en alguno de los vértices de T_i. De todos los ejes que inciden en T_i, se elige el de peso mínimo (que no forme el ciclo).
3. Se repite el paso 2 hasta que no se pueden añadir más ejes sin formar ciclo.

ALGORITMO DE KRUSKAL (1956)

Pasos para crear un árbol generador de peso minimal:

1. Se pone un contador en $i = 1$ y se elige un eje de peso mínimo, e_1.
2. Elegimos ejes $e_1, e_2, \dots, e_i$ con $1 \leq i \leq n - 2$, se toma el eje e_{i+1} de peso mínimo entre todos los ejes que quedan sin formar un ciclo con los ejes seleccionados.
3. Se repite el paso 2 hasta que no se puedan añadir ejes sin formar ciclo.