uc3m | Universidad Carlos III de Madrid

Grado en Ingeniería Informática

2018-2019

Apuntes

Matemática Discreta

Jorge Rodríguez Fraile[1]

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

ÍNDICE GENERAL

Parte I

Teoría

Tema 1: Conjuntos y funciones

Teoria de Conjuntos.

- Conjunto: Colección desordenada de objetos bien ~~definimidos~~ definidos, denominados elementos. $A=\{1,2,3\}=\{2,3,1\}$ Un conjunto contiene a sus elementos.
  Si S es un conjunto y x un elemento del mismo $\Rightarrow x \in S$ x pertenece a S
  Si x no pertenece a S, $x \notin S$
- Relación de pertenencia, se da entre un conjunto y sus elementos
- Relación de igualdad de conjuntos, si y solo si tienen los mismos elementos.
  $A=\{1,3,5\}=B=\{5,1,3\}$ $C=\{4,7,6\}=D=\{4,4,6,7,7\}$ $A=B$ $C=D$ $A\neq C$
- Formas de describir un conjunto:
  Por extensión: Cuando es posible enumerar o listar todos sus elementos.
  $V=\{a,e,i,o,u\}$ $W=\{2, \text{Madrid}, a\}$
  Por compresión: Cuando se usa una propiedad comun para enumerar todos sus elementos. $D=\{x / x=2y,\ y\in\mathbb{R}\}$
  Mixta, empleando los dos.
- Propiedades: Para dos conjuntos dados A y B
  Reflexiva $A=A$
  Simetrica $A=B$, $B=A$
  Transitiva $A=B$, $B=C \Rightarrow A=C$
- Conjunto Universal (U): Conjunto que contiene todos los objetos o elementos. bajo consideración
- Conjunto vacio ($\emptyset$): Conjunto que no posee elemento alguno. $\emptyset=\{\}$
  Los diagramas de Venn, representan los elementos de los conjuntos y son muy utiles 
- Subconjunto: Si todo elemento de A pertenece a B, A contenido o incluido en B
  A es un subconjunto de B. $A\subseteq B$ $\emptyset\subseteq A,\ \forall A$
  Si se cumple son conjuntos comparables.
- Subconjunto propio: Si $A\subseteq B$ y, además, existen elementos de B que no pertenecen a A. Inclusión estricta de A en B $A\subset B$
  B contiene a A estrictamente
  A está contenida estrictamente en B
- Propiedades de la inclusión:
  Reflexiva: $A\subseteq A$
  Antisimetrica $A\subseteq B$ y $B\subseteq A \Rightarrow A=B$
  Transitiva $A\subseteq B$ y $B\subseteq C \Rightarrow A\subseteq C$
- Cardinal: Siendo A un conjunto finito formado por n elementos distintos, el cardinal de A, $|A|=n$, será igual a n. $|\emptyset|=0$

- Conjunto de las partes del conjunto A: Es el conjunto formado por todos sus subconjuntos. Se indica por $P(A)$.

  $A=\{a,b\}$ $P(A)=\{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ $|P(A)|=2^2=4$

  $|X|=n$ $|P(x)|=2^n$

- Operaciones con Conjuntos:

  Unión: $A\cup B$ Conjunto que contiene aquellos elementos de A o de B o de ambos.

  Intersección: $A\cap B$ Conjunto formado por todos los elementos que pertenecen simultaneamente a A y a B. <u>Disjunto</u>: Intersección vacia $A\cap B=\emptyset$

  Complemento: $\bar{A}$ Conjunto formado por todos los elementos de U que no pertenecen a A. $\bar{A}=\{x/x\notin A\}$

  Diferencia: $\underset{A-B}{A\setminus B}$ Conjunto formado por los elementos de A que no pertenecen a B.

  $A\setminus B=\{x/(x\in A)\wedge(x\in B)\}$ $\underline{A\setminus B=A\cap\bar{B}}$ $\underline{U-A=\bar{A}}$

  Diferencia simétrica: $A\Delta B$ ó $\underset{\text{Suma booleana}}{A\oplus B}$ Conjunto definido por todos los elementos de A que no estan en B o todos los de B que no estan en A.

  $A\Delta B=\{x/(x\in A\cup B)\wedge(x\notin A\cap B)\}$

- Propiedades:

  Leyes de De Morgan: $\underline{\overline{A\cup B}=\bar{A}\cap\bar{B}}$ $\underline{\overline{A\cap B}=\bar{A}\cup\bar{B}}$

  $\underline{A\Delta B=(A\setminus B)\cup(B\setminus A)}$

  Conmutativa: $A\cup B=B\cup A$ $A\cap B=B\cap A$

  Asociativa: $A\cup(B\cup C)=(A\cup B)\cup C$ $A\cap(B\cap C)=(A\cap B)\cap C$

  Absorción: $A\cup U=U$ $A\cap\emptyset=\emptyset$ $\underline{A\cup(A\cap B)=A}$ $\underline{A\cap(A\cup B)=A}$

  Idempotencia: $A\cup A=A$ $A\cap A=A$

  Neutralidad: $A\cup\emptyset=A$ $A\cap U=A$

  Distributiva: $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ $\underline{A\cap(B\cup C)=(A\cap B)\cup(A\cap C)}$

- Producto cartesiano, de A y B: Conjunto de todos los pares cuya primera componente sea un elemento de A y la segunda un elemento de B. Se representa por $A\times B$. $A\times B=\{(a,b)/(a\in A)\wedge(b\in B)\}$

  $(a,b)=(a',b')$ $a=a'$ $b=b'$ pares iguales

  $(a,b)\neq(b,a)$ pares reciprocos, pero no iguales.

  $A\times A=A^2$ cuadrado cartesiano.

  Ej: $A=\{1,2,3\}$ $B=\{a,b\}$

  $A\times B=\{(1,a),(2,a),(3,a),(1,b),(2,b),(3,b)\}$

- Conjunto de los números naturales ($\mathbb{N}$):

  Si $n \in \mathbb{N}$, entonces $n+1 \in \mathbb{N}$ (El sucesor de n)

  Todo $n \in \mathbb{N}$ distinto de 1 es sucesor de otro número de $\mathbb{N}$

  $0 \notin \mathbb{N}$

  Principio de buena ordenación: Todo subconjunto no vacío de $\mathbb{N}$ tiene un elemento mínimo.
- Conjunto de los números enteros: $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$
- Conjunto de los números racionales: $\mathbb{Q} = \{p/q \,/\, p, q \in \mathbb{R}, q \neq 0\}$

Metodos para demostrar igualdades:

Por propiedades y definiciones.

Tiene que cumplir $\subseteq$ y $\supseteq$

Por Tablas de verdad.

$\#A$ Cardinal de A. número de elementos.

Función: $f \subset A \times B$ Es un subconjunto del producto cartesiano $A \times B$ tal que para $\forall x \in A$, f contenga un par de la forma (x, y).

A es el dominio de la aplicación y el B recibe el nombre de codominio

$Dom(f) = A$ $\quad Im(f) = \{y \,/\, \exists x \in A \text{ tal que } (x,y) \in f\}$

Es una transformación que no tiene porqué ser lineal, pero todo elemento del conjunto de entrada tiene un unico elemento de salida.

Tipos de funciones:

Inyectiva: Si para cada elemento $b \in B$, existe, como mucho, un elemento $a \in A$ tal que $f: a \to b$ $\quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

Sobreyectiva: Si cada elemento $b \in B$ es la imagen de al menos un elemento $a \in A$. Es decir, rango $A \subseteq B$

Biyectiva: Si es inyectiva y sobreyectiva.

Inversa: $f^{-1}: b \to a$ es la inversa de otra biyectiva $f: a \to b$

Asigna a un elemento $b \in B$ un unico elemento $a \in A$.

$f(x) = 2x+1 \quad f^{-1}(x) = \dfrac{x-1}{2} \qquad x = 2y+1 \,;\; x-1 = 2y \,;\; y = \frac{x-1}{2}$

Composición: $f: A \to B \quad g: B \to C \quad f \circ g: A \to C$

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

Techo: $f(x) = \lceil x \rceil$

Suelo: $f(x) = \lfloor x \rfloor$

Divisibilidad de enteros:

Multiplo: Producto de un número entero a. Siendo r un valor entero, cualquiera.

$b = a \cdot r$ b es multiplo de a $b = \dot{a}$

Divisor: Siendo, $b = a \cdot r$, b un multiplo de a. Tambien a es divisor de b.

$a = b/r$ $r = b/a$

Cociente exacto:

- a divide a b: Siendo $a \neq 0$ y b dos enteros, y r un entero que cumpla $b = a \cdot r$. Se indica $a|b$ y si a no divide a b $a \nmid b$
- Algoritmo de divisibilidad: Si D y d son números enteros, con $d \neq 0$, entonces existen dos enteros únicos q y r tales que:

$D = dq + r$ y $0 \leq r < |d|$ D dividendo d divisor

El entero q recibe el nombre de cociente, y el r de resto.

$$q = \begin{cases} \lfloor a/b \rfloor & \text{si } b > 0 \\ \lceil a/b \rceil & \text{si } b < 0 \end{cases} \qquad qd \leq D < (q+1)d$$

Divisor comun: Sean a y b números enteros, d un entero no nulo.

Si $d|a$ y $d|b$, se dice que d es divisor comun de a y de b.

- Máximo común divisor: Sean a y b enteros no nulos. El divisor comun d mayor de a y b es el máximo comun divisor, $mcd(a,b) = d$.

Ej: $2|12$ $2|36$, $3|12$ $3|36$, $12|12$ $12|36 \Rightarrow mcd(12,36) = 12$

- Coprimos o primos relativos: Lo son dos números enteros a y b tal que el maximo comun divisor sea 1, $mcd(a,b) = 1$
- Mínimo comun multiplo: Es el menor multiplo comun distinto de 0 de dos enteros a y b no nulos. $mcm(a,b) = l$

Siendo a y b dos enteros. $mcd(a,b) \cdot mcm(a,b) = a \cdot b$

- Primo: Dado un entero $p \in \mathbb{N}$, $p > 1$, cuando no admite más divisores en $\mathbb{N}$ que el 1 y el propio p. Ej: 2, 3, 5, 7, ... Existen infinitos primos.
- Compuesto: Aquel que no es primo.
- Teorema fundamental de la aritmetica: Todo número natural $m > 1$ se puede descomponer de manera unica en factores primos.

$m = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots$ p_i números primos diferentes

$63 = 3^2 \cdot 7$ n_i número de veces que se repite el primo.

Matemática Discreta T (3) 5/02/2019

$0! = 1 \quad 1! = 1$

Tema 2: Combinatoria elemental.

Combinatoria: Contar los elementos de un conjunto ≡ Calcular el cardinal de un conjunto.

$A = \{a, b, c, d, e\}$ $|A| = 5$ 5 elementos → Cardinal 5

$A' = \{1, 2, 3, 4, 5\}$ Biyección $f: A \to A'$

Dos conjuntos tienen el mismo cardinal se puede establecer una relación biyectiva entre sus elementos. Para conjuntos finitos.

Regla del producto "y": Conjuntos cuyos elementos se pueden construir de forma secuencial. No depende el uno del otro (sus resultados) Pag. 275

Nº de 5 cifras con los dígitos $\{1,2,3\}$

$\boxed{|A \times B| = |A| \cdot |B|}$ $3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = \boxed{3^5}$

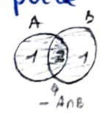
Regla de la suma "o": Suponemos que A y B son dos sucesos disjuntos ($A \cap B = \emptyset$). Si el suceso A se puede realizar de m maneras y el B de n, entonces el suceso A o el B se podrá realizar de m+n maneras distintas. Útil para unir conjuntos tras particionarlos.

Nº pares en $A = \{2, 7, 8, 14\}$ y $B\{1, 2, 3\}$

$\boxed{|A \cup B| = |A| + |B|}$ $3 + 1 = \boxed{4}$

Paso al complementario: Para hallar un cardinal complejo, hacer el opuesto y restarselo al conjunto universal.
$|A| = |U| - |B|$ Pares del 0-12 $|A| = 13 -$ impares $= 13 - 6 = 7$ pares

Principio de inclusión - exclusión: Si los dos conjuntos no son disjuntos, nos puede llevar a contar alguno dos veces. Si $A \cap B \neq 0 \Rightarrow \boxed{|A \cup B| = |A| + |B| - |A \cap B|}$



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

Tener en cuenta si son listas o subconjuntos y si hay repetición
Mirar ejercicio 2.6, tipo repetición elementos en lo que combinamos huecos

Patrones elementales de recuento:

Permutaciones (ordenaciones): Dado un cierto conjunto (con n-elementos), ¿cuantas secuencias (cadenas, filas) de longitud maxima (n) podemos formar.

Formar grupos tomando todos los elementos

$\boxed{P_n = n!}$ $A = \{1, 2, 3\}$ $P_3 = 3! = 6$ 123 132 213 231 312 321

Permutaciones con repetición: Teniendo m elementos, entre los que hay α iguales, β iguales de otro tipo y así sucesivamente. ¿Cuantas secuencias?

$$\boxed{P_m^{\alpha, \beta, \dots} = \frac{m!}{\alpha! \, \beta! \dots}} \qquad m = \alpha + \beta + \dots$$

□, □, ☒ $\frac{3!}{2! \, 1!} = 3$ ☒□□ □☒□ □□☒ Son iguales y forman uno u otro es igual.

Variaciones (Subconjuntos ordenados): k listas (listas de orden k) con m símbolos ($\{1, 2, \dots, m\}$) de un conjunto dado.

$$\boxed{V_{m,k} = \frac{m!}{(m-k)!}} = m(m-1)(m-2)\dots(m-k+1)$$

Regla del producto

25 atletas // listas de atletas que pisan podio
3 posiciones // $V_{25,3} = \frac{25!}{22!} = 25 \cdot 24 \cdot 23 = 13.800$

Variaciones con repetición: k listas que pueden formarse con los m elementos de un conjunto dado. Permitiendose la repetición en la secuencia:

$\boxed{VR_{m,k} = m^k}$ Mediante la regla del producto.

Combinaciones (subconjuntos): Sea un conjunto formado por m elementos distintos, una combinación es cada grupo formado por n elementos tomados de los m, no influye el orden ($\{1,2\} = \{2,1\}$) de colocación, se toman como distintos si difiere en algún elemento.

$$\boxed{C_{m,n} = \binom{m}{n} = \frac{m!}{n! \, (m-n)!}}$$

Lema del Saludo: Para un número par ó impar de elementos (personas), siempre hay un número par de relaciones (saludo)

$$\begin{array}{c|ccc|c} & 1,2 & 1,3 & 2,3 & \\ \hline 1 & 1 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 3 & 0 & 1 & 1 & 2 \\ \hline & 2 & 2 & 2 & \end{array}$$

Simetría: $\boxed{\binom{n}{k}=\binom{n}{n-k}}$ $\quad \frac{n!}{k!(n-k)!}=\frac{n!}{(n-k)!\,k!}$ $\quad n\geq 0$, $0\leq k\leq n$

Identidad de Pascal:

$$\boxed{\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}} \quad \text{Iguales} \quad \binom{n+1}{k}=\binom{n}{k-1}+\binom{n}{k}$$

Triangulo de Pascal $\boxed{\binom{n}{r}\ \begin{matrix}\text{fila}\\ \text{columna}\end{matrix}}$

$$\begin{array}{ccccccc} & & & 1\binom{0}{0} & & & \\ & & 1\binom{1}{0} & & 1\binom{1}{1} & & \\ & 1\binom{2}{0} & & 2\binom{2}{1} & & 1\binom{2}{2} & \\ 1\binom{3}{0} & & 3\binom{3}{1} & & 3\binom{3}{2} & & 1\binom{3}{3} \end{array}$$

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

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

Obs: $\binom{n}{k}=0$ Si $k<0$, Si $k>n$

Th. Binomio de Newton: $n\geq 0$

$$\boxed{(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}} \quad (a+b=n,\ x^a\cdot y^b)$$

$$\boxed{(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k}$$

$$\boxed{(x+y+z)^n=\sum_{a,b,c\geq 0,\ a+b+c=n}\binom{n}{a,b,c}x^a\cdot y^b\cdot z^c}$$

Debe cumplir imprescindible por $\binom{n}{a,b,c}$ que $a+b+c=n$ para $\frac{n!}{a!\,b!\,c!}$, sino será 0

Corolario: Para todo $n\geq 0$

$$\boxed{\sum_{k=0}^{n}\binom{n}{k}=2^n} \qquad \sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$$

Identidad de Vandermonde.

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

$n,m\geq 0$ $\quad 0\leq k\leq m+n$

Cuantas listas con m ~~el~~ y n elementos de longitud k se pueden forma. Ej: Comite de m-mujeres y h-hombres, cuantos subcomites de r miembros

$$\binom{m+h}{r}=\sum_{k=0}^{r}\binom{m}{k}\cdot\binom{n}{k-k}$$

Mediante la regla del producto, los m primeros q veces y los n k-q veces, pero sumando, ~~que~~ puede haber más de uno que del otro o incluso ninguno.

Principio del palomar de Dirichlet:

1º Principio: Si $k+1$ o más objetos se colocan en k cajas, existe al menos un caja que contiene dos o más objetos. Si no se cumpliese sería una contradicción. Como poco 2 en uno

2º Principio: Si N objetos se colocan en k cajas existen al menos una caja que contiene $\lceil N/k \rceil$ objetos.

Tema 3: Grafos I

- Grafo (G): Está formado por dos conjuntos, el conjunto V de vertices o nodos, por lo general no vacio y el otro E ó A formado por las aristas o lados que estan constituidos por pares no ordenados de vertices ($\{v_1, v_2\}$) distintos.

G(V,E)

- Bucle: Cuando una arista está asociada a dos vertices identicos
- Aristas paralelas: Dos aristas lo son cuando son incidentes con los mismos vertices.
- Grafo simple: Un grafo que no tiene bucles, ni aristas paralelas.
- Grafo: Permite bucles, pero no aristas paralelas.
- Multigrafo: Si para $a, b \in V$ y $a \neq b$, existen dos o mas aristas. Permite bucles y aristas paralelas.

No dirigido

Dirigido

$|E| = \binom{|V|}{2}$

$|E| = \frac{V(V-1)}{2}$

Grafo completo

- Subgrafo: Se eligen algunos vertices y aristas del grafo original.
- Grafo complementario: Tiene los vertices del original, pero las aristas que no tiene el otro. G $\overline{G}$
- Subgrafo inducido: Al escoger un par de vertices debe mantener la arista. si tenía
- Subgrafo abarcador, generadores o recubridores: Tiene todos los vertices, pero no todas las aristas.
- Adyacencia o vecindad: Cuando dos vertices estan unidos por una arista.

Incidencia → $d(v) = 2$

- Grado o valencia (gra(v) $d(v)$): Número de aristas incidentes con un vertice V.
  - Vertice grado 0 → Aislado.
  - Vertice grado 1 → Terminal.
- Grafo regular: Si todos los vertices tienen el mismo grado.
- Teorema del apretón de manos: La suma de los grados de todos los vertices es el doble del número de aristas. $\boxed{\sum_{i \in V}^{N} d(i) = 2|E|}$
  - En un grafo o multigrafo, el número total de vertices de grado impar es par.
  - En todo grafo G, la suma de los grados de sus vertices es par.
  - En todo grafo G, con un número impar de vertices hay un numero impar de vertices de grado par.
- Grafo 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 vertice de V_1 con otro de V_2.

Para comprobar si no lo son: que contenga al K_3 como subgrafo o ciclo impar. Lo es si Árbol

- Sucesión de grados: lista de los grados de los vertices de un grafo ordenados de menor a mayor. El nº de elementos son los vertices. No todas las secuencias son validas (no corresponden a un grafo).

  Debe cumplir el Lema del apreton de manos.

Ej: 2, 2, 3, 3, 4
nº par de vertices de grados impares
la suma de los grados es par

- Familias de grafos:

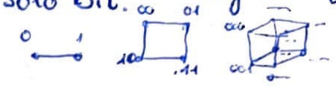
$K_n \to$ Grafo completo: Tienen todos los vertices el grado maximo posible $(n-1)$ 

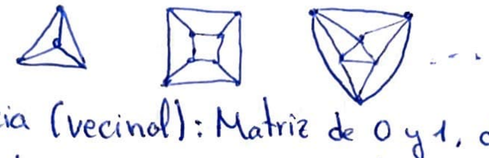
$L_n \to$ Grafo lineal: Dos vertices terminales y el resto con grado dos.

$C_n \to$ Grafo circular: Todos los vertices tienen grado dos. 

$K_{n,m} \to$ Grafo bipartito completo: n y m vertices. 

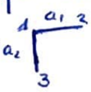
$W_n \to$ Grafo rueda: Tienen grados tres excepto uno que es el maximo posible. 

$Q_n \to$ Grafo cubo: Los vertices tienen etiquetas binarias, hay 2^n vertices de longitud n.
Son adyacentes los que varian en un solo bit. hay $n2^{n-1}$ aristas.
Todos son regulares y bipartitos. 

- Grafos platónicos:  . . .

- Matriz de adyacencia (vecinal): Matriz de 0 y 1, de tamano $|V| \times |V|$.
Los 1 son las aristas, y aparecen en sus vertices.
Diagonal de un grafo simple es 0 y simetrica 

$$\begin{array}{c|ccc} & V_1 & V_2 & V_3 \\ \hline V_1 & 0 & 1 & 1 \\ V_2 & 1 & 0 & 0 \\ V_3 & 1 & 0 & 0 \end{array}$$

- Matriz de incidencia: Cuenta los vertices que conectan cada arista, tamaño $|E| \times |V|$
Un 1 en los extremos de la arista. 

$$\begin{array}{c|ccc} & V_1 & V_2 & V_3 \\ \hline a_1 & 1 & 1 & 0 \\ a_2 & 1 & 0 & 1 \end{array}$$

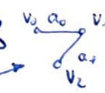
- Grafos isomorfos: Si tienen el mismo número de vertices y aristas, la misma sucesión de grados y difieren en el etiquetado. Estos sirven para demostrar la no isometria, pero para demostrar la isometria ademas debe cumplirse $\boxed{AP = PB}$ Siendo A y B las matrices adyacentes y P la matriz permutación. (Matriz identidad con filas permutadas)

En la biyección de los vert. o aris

Mirar cual cambia y intercambiar filas

- Si se puede establecer una biyección entre las aristas y otra entre los vertices.

También Hamiltoniano, Euleriano, Cromatico, grados vecinos

- Camino: Secuencia alterna de vertices y aristas (o solo vertices) $\{V_0, a_0, V_1, a_1, V_2\}$ 

- Longitud: Número de aristas que componen un camino (2)

Camino simple: Se permite la repetición de vertices, pero no de aristas.
- abierto: el vertice final e inicial distintos $V_1 \neq V_n$
- cerrado: el vertice final e inicial es el mismo $V_1 = V_n$

Camino elemental: No se permite la repetición de vertices ni aristas.

Circuito: Camino simple cerrado (Se permite repetir vertice, no arista)

Ciclo: Camino elemental cerrado (No se repiten aristas, ni vertices excepto inicial y final)

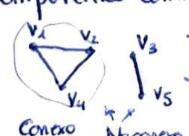
- Número de caminos de longitud l: Vienen dados por las entradas i,j de la matriz de adyacencia elevada a la longitud. M^l $\begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 5 & x & \cdot \end{pmatrix}$ 5 caminos de V_3 a V_2, x caminos de V_3 a V_3

Traza de M^2 es $2|A|$ Traza de M^3 es $3!\cdot$ nº de triangulos no orientados.

- Conexión y Componentes conexas: Si dados dos vertices cualesquiera existe un camino (elemental) que los una (conecta)

G es conexo si contiene un arbol generador.

$$\begin{array}{c|ccc|cc} V_1 & 0 & 1 & 1 & 0 & 0 \\ V_2 & 1 & 0 & 1 & 0 & 0 \\ V_4 & 1 & 1 & 0 & 0 & 0 \\ \hline V_3 & 0 & 0 & 0 & 0 & 1 \\ V_5 & 0 & 0 & 0 & 1 & 0 \end{array}$$



- Si G es simple y conexo $|A(G)| \leq |V(G)| - 1$
- Si alguna entrada de la matriz $\tilde{M} = I + M + M^2 + \dots + M^{n-1}$ es nula el grafo no es conexo. Por el contrario si no hay ninguna nula es conexo

Los grafos no conexos son la unión de dos subgrafos conexos que estan desconectados, llamadas componentes conexas. Un puente es una arista que si la eliminamos convierte a G en no conexa (aumentan las componentes conexas)
Un punto de articulacion o de corte: Vertice que si lo eliminamos junto a las aristas (que lo unen)

Tema 4: Grafos II

Árboles: Grafo simple, conexo y sin ciclos.

Si y solo si es conexo y al borrar cualquier arista pasa a ser disconexo.

Si y solo si no contiene ciclos y al añadir una arista se crea un ciclo.

Si y solo si existe un unico camino elemental entre cualquier par de vertices.

Un arbol cumple $\boxed{|E|=|V|-1}$ $\boxed{\sum_{i=0}^{|V|} d(v_i)=2|V|-2}$

- Raiz: Vertice arbitrario, unico en el arbol.
- Hojas: Vertices terminales ($d(v)=1$) de un arbol, incluso puede ser la raiz.

Minimo nº de hojas es 2 —— Maximo nº de hojas $n-1$

- Bosque: Grafo simple sin ciclos, sus componentes conexas son arboles.
- Arbol generador: Grafo generador que tiene forma de arbol, pasa de un grafo a un arbol eliminando aristas (sin ciclos y conexo)

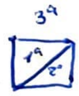
Teorema: Un grafo G es conexo si contiene un arbol generador.

Grafo planar: Grafo que puede ser dibujado en el plano sin que sus aristas se cruzen.

- Kuratowsky: Un grafo es planar si y solo si no contiene como subgrafo a ninguna subdivisión de K_5 ni de $K_{3,3}$
- Formula de Euler: Un grafo plano simple divide al plano en R regiones tal que:

Si es conexo: $\boxed{|V|-|E|+R=2}$

Si no es conexo: $\boxed{|V|-|E|+R=1+\text{nº de componentes conexas}}$



$4-5+R=2;\ R=3$

Corolarios para demostrar que un grafo no es planar:

Si G es plano, simple y conexo con $|V|\geq 3 \Rightarrow \boxed{|E|\leq 3|V|-6}$

Si G es simple, conexo, plano, con $|V|\geq 3$ y sin ciclos de longitud 3 $\Rightarrow \boxed{|E|\leq 2|V|-4}$

Dualidad: Un grafo dual G^* de un grafo planar G consiste en, por cada región en G hay un vertice en G^* y dos vertices estan unidos por tantas aristas como fronteras entre esas regiones.

Grado de una región: Grado del vertice de esa región en el grafo dual.

$$\sum_{i=0}^{|R|} d(R_i)=2|E|$$

Subdivisión: Remplazar una arista por un vertice conectado a los vertices a los que estaba unida la arista.

Homeomorfos: Grafo obtenido mediante la subdivisión.

26/02/2019

Tema 5: Grafos III

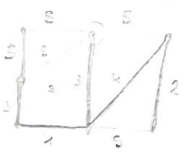
- Grafo ponderado: Es un grafo en el que a cada arista $e \in E$ se le asocia un peso $w(e) \in \mathbb{R}$. El peso es un real. $G(V,E,w)$
- Arbol generador minimal: En un grafo conexo ponderado, es el árbol generador tal que la suma de los pesos de las aristas sea la más pequeña posible.
- Algoritmo voraz: Es aquel que en cada paso coge la elección optima.
- Algoritmo de busqueda de arboles generadores:

Algoritmo de busqueda a lo ancho: Se elige un vertice y se avanza por todos los vertices vecinos, sin formar ciclos, y se repite, se avanza de nuevo por todas a la vez. Hasta que $|E|$ sea el esperado $|E| = |V| - 1$

Algoritmo de busqueda profundidad: Se elige un vertice y se avanza por ese todo lo posible, sin ciclos, y si no se puede se retrocede un vertice. Hasta $|E|$ sea el esperado.

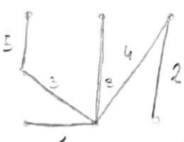
Algoritmo de busqueda de arboles generadores minimales:

Grafos con muchas aristas → Algoritmo de Prim: Se elige un vertice, se coge la arista de menor peso incidente en nuestros vertices, sin formar ciclos, se repite el proceso de coger la de menor peso entre todas las incidentes con los vertices. Hasta que $|E| = |V| - 1$. No es unico, pero su peso total no cambia.



Peso: 18

Algoritmo de Krustal: Se elige la arista de menor peso, se vuelve a coger la siguiente de menor peso y se comprueba que no forme ciclos, se repite hasta que $|E| = |V| - 1$ y haya una unica componente conexa



Peso: 14

Algoritmo de Dijkstra: Determina el camino más corto (mínimo peso) entre un nodo origen hacia los demás nodos en un grafo ponderado.

1° Marcamos el origen con una etiqueta permanente $\boxed{(0, V_1)}$ y el resto con una temporal, si está conectada con el origen $(3, V_2)$ (peso) y si no $(\infty, -)$

2° Elegimos el de menor grado de los anteriores y lo convertimos en permanente, a los que ya han sido permanente en blanco (*), y se ponen las etiquetas temporales de los vecinos del permanente, pero son el resultado de la suma del peso del permanente y la del vertice temporal con el permanente (arista que une el temporal y el permanente), si este es menor que el valor que tenia antes.

3° Repetir el 2° hasta que no haya más temporales. El camino más corto se ve mirando las etiquetas permanentes en sentido contrario. Se va de letra en letra de los permanentes

$\boxed{3,B}$ ← Despues iriamos a la que esté en B

	Paso 1	Paso 2	Paso 3	Paso 4
A	$\boxed{(0,A)}$	*	*	
B	(3,A) →	$\boxed{(3,A)}$	*	
C	∞	(8,B)	(11,D) $5+3<\infty$	$\boxed{(11,D)}$
D	(7,A)	(7,A) →	$\boxed{(7,A)}$ $7<23$	

	A	B	C	D	
A	x	3	∞	7	P1
B	3	x	5	20	P2
C	∞	5	x	4	
D	7	20	4	x	P3

Tema 6: Grafos IV

Coloración de un grafo: Asignar un color a cada vertice (sin restricciones)

Coloración propia de un grafo: Asignar un color a cada vertice, pero sin que vertices adyacentes tenga el mismo color.

Es una funcion $C: V \to C(V)$ tal que $C(u) \neq C(v)$ si forman una arista $\{u,v\}$
↳ color de la paleta's

Cuello: Ciclo de menor longitud.

Número cromatico ($X(G)$): Es el mínimo número de colores posibles para colorear un grafo G (propia)

Maximo y minimo → Si tiene alguna arista $2 \leq X(G) \leq |V|$ Si no $X(G)=1$

Si G tiene grado maximo $k \to X(G) \leq k+1$

Si G es bipartito $\to X(G)=2$ ← Si G es un arbol.

Si G' y G → $X(G') \leq X(G)$

Si G no completo, conexo y grado maximo $k \geq 3 \to X(G) \leq k$

Teorema de los cuatro colores. Appel y Haken: Todo grafo G planar cumple $X(G) \leq 4$ $P_G(4)>0$

Algoritmo voraz para colorear un grafo:

1. Ordenamos los vertices $\{V_1, V_2, \dots\}$
2. Asignamos a V_1 el color $C(V_1)=a$.
3. A los vecinos de V_1 un segundo color b
4. Si es vecino de V_1 o V_2, no utilizaran esos.
5. Repetir mirando no asignar el color del adyacente y sea la menor cantidad.

Grafos eulerianos. (Tienen que ser Conexos)

Circuito euleriano: Circuito que contiene todas las aristas del grafo. Grafo euleriano

Si y solo si todos los vertices tienen grado par. Si es dirigido lo es si y solo si grado int = y grado ext

Camino euleriano: Camino abierto que contiene todas las aristas.

Si y solo si contiene dos vertices de grado impar. Grafo Semieuleriano

Algoritmo de Fleury (Elimina las aristas recorridas)

1. Empezar en un vertice impar (para Semieuleriano), si no en cualquiera.
2. Si $d(x)=0$ se para // Si $d(x)=1$ Recorrer la unica // $d(x)>1$ Escogemos cualquiera que no sea un puente

⋮

n. Hasta $d(x)=0$ o A vacia (todas las aristas recorridas)

Grafos Hamiltoniano. (Conexo) Cuantas más aristas más probable que lo sea.

Ciclo hamiltoniano: Ciclo (sin repetir aristas ni vertices) que contiene todos los vertices del grafo. Grafo hamiltoniano $\geq n/2$

T. Dirac: Si para $n \geq 3$ vertices todos los grados son $\geq n/2$ → Si se cumple lo es, pero no sirve para los que no lo cumplen.

Camino hamiltoniano: Camino abierto que contiene todos los vertices, sin repetir aristas ni vertices. Grafo semihamiltoniano

Tema 7: Combinatoria básica II

12/09/2019

Repartos: Si tenemos r objetos indistinguibles que se quieren repartir en n grupos distinguibles:

- Con grupos vacios $\binom{r+n-1}{n-1}$ ó $\binom{r+n-1}{r} \Rightarrow \#\left\{\begin{matrix} x_1+\ldots x_n = r \\ x_i \geq 0 \end{matrix}\right\}$

Si son distinguibles: $\# = r^n$

- Con grupos con almenos 1 elemento $\binom{r-1}{n-1} \Rightarrow \#\left\{\begin{matrix} x_1+\ldots+x_n = r \\ x_i \geq 1 \end{matrix}\right\}$

Ecuación diofantica:

$x_1, x_2, \ldots, x_k \in \mathbb{Z}_+ . n \in \mathbb{N}$

$x_1 + x_2 + \ldots + x_k = n$

Si nos encontramos restricciones, debemos añadilas como condiciones a la ecuación. Si es una limitación por rango numerico, sustituimos restando o sumando hasta un caso conocido, si esta en un rango tantas prohibiciones como cotas superiores (y las bajas a 0) y hacer complementario.

Ejem: $\#\left\{\begin{matrix} x_1+x_2+x_3=9 \\ x_1 \geq 2, x_2 \geq 1, x_3 \geq 5 \end{matrix}\right\} = \begin{matrix} y_1 = x_1 - 2 \\ y_2 = x_2 - 1 \\ y_3 = x_3 - 5 \end{matrix}$

$= \#\left\{\begin{matrix} y_1+y_2+y_3 = 1 \\ y_i \geq 0 \end{matrix}\right\} = \binom{3+1-1}{3-1} = \binom{3}{2} ó \binom{3}{1}$

$\#\left\{\begin{matrix} x_1+x_2+x_3 = 20 \\ 6 \geq x_1 \geq 2, x_2 \geq 1, 5 \geq x_3 \geq 0 \end{matrix}\right\} = \#\left\{\begin{matrix} y_1+y_2+y_3 = 17 \\ 4 \geq y_1 \geq 0, y_2 \geq 0, 5 \geq y_3 \geq 0 \end{matrix}\right\} = |\text{Todos los } x_i \geq 0| - [|P_1 \cup P_2|] = \ldots$

P_1 P_2

todo $x \geq 0$ menos x_1 que es $x_1 \geq 7$ o por encima

$-[|P_1| + |P_2| - |P_1 \cap P_2|] = \ldots$

Multiconjuntos: Se permite la repetición de elementos, pero el orden no importa.

Con α y $\beta \Rightarrow$ Multiconjuntos de 3 elementos $\{\{\alpha\alpha\alpha\}, \{\alpha\beta\alpha\}, \{\beta\beta\beta\}, \{\beta,\beta,\alpha\}\}$

Partición: Distribuir elementos de un conjunto en subconjuntos tal que todos sean disjuntos.

- Sea A un conjunto con $A_1, A_2, \ldots, A_k$ particiones de A, lo son si $A_i \subseteq A \,/\, A_1 \cup A_2 \cup \ldots \cup A_k = A$
  $A_i \cap A_j = \emptyset . \forall i,j$

14 elementos en grupos de 4, 4, 3, 3

$$\frac{\binom{14}{4}\cdot\binom{10}{4}\cdot\binom{6}{3}\binom{3}{3}}{2! \cdot 2!} = \frac{14!}{(2!)^2(4!)^2(3!)^2}$$

14→10 10→6 6→3 3→1

Hay 2 grupos de 4 Hay 2 grupos de 3

Se calculan las conbinaciones de todos en el 1er grupo, luego los que quedarian en el 2º grupo, asi sucesivamente. hasta que no se pueda más.

Dividir lo anterior entre el factorial del número de veces que se repiten tamaños de grupos.

Tema 8: Relaciones de Recurrencia.

Relación de recurrencia para la sucesión $\{a_n\}_{n=0}^{\infty}$: Es una ecuación que expresa cierto termino en función de uno o más terminos anteriores.

Elementos:

- Termino enesimo. $a_n = a_{n-1} + a_{n-2}$
- Casos base (tantos como orden) $a_1 = 1$ $a_2 = 3$
- n para la que es valida $n \geq 1$

Orden: Es la diferencia entre el subindice maximo y el subindice mínimo.

$a_n = 7a_{n-4}$ Orden: $n-(n-4)=4$

Homogenea: Si no hay base, tendria la solución nula. Si: $a_n = 2a_{n-1}$ No: $a_n = a_{n-2}+5$

Coeficientes constantes: Lo que multiplica las a_n es constante.

Lineal: Si tiene la forma → $C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k}$ $\sqrt{a_n}$ | $\frac{1}{a_n}$ | a_n^2 → No

Solución ecuaciones de recurrencia de orden 1 homogeneas.

Tiene estructura de espacio vectorial y la dimensión es el orden.

De la forma → $a_n = C a_{n-1}$

Suponemos → $a_n = x^n \Rightarrow x^n = C x^{n-1} \overset{\text{Simpl.}}{\Rightarrow} x = C$ Ec. caracteristica.

Solución general (comb. lineal) → $a_n = A C^n$ ($A x^n$)

Solución concreta: sustituir caso base.

Solución ecuaciones de recurrencia de orden >1 (fibonacci) homogeneas.

Como el anterior, pero la ec. caracteristica puede tener tantas soluciones (x_1 x_2 x_n) como grado la ecuación.

Solución general (comb. lineal) → $a_n = Ax_1^n + Bx_2^n + \ldots$ ó $a_n = (A_1 + nA_2)x_2^n + Bx_3 \ldots$ Si x_1 y x_2 son iguales o solo ha 2 de 3

Solución concreta: Sustituir casos base y resolver la ecuación.

Solución ecuaciones de recurrencia no homogeneas.

Forma → $a_n = a_{n-1} + a_{n-2} \ldots + t^n$ t^n es una función que la hace no homogenea.

$a_n = a_{n,\text{homogenea}} + a_{n,\text{particular}}$ dividimos el problema.

$a_n = C2^n$ Solución $a_{n,h}$ como una normal homogenea ya sea de orden 1 o mayor. (Sin el termino no homogeneo)

$a_n = -1$ Solucion particular ($a_{n,p}$): Miramos que tipo de función es y suponemos un a_n (el menor, probamos y si no el siguiente mayor) Ejem: $a_n = An + C$ ó $a_n = A3^n$

Sustituimos en la ecuación completa y hallamos las constantes.

$a_n = -1 + C2^n$ Solución general: La suma de la solución homogenea con las constantes y el particular.

$a_1 = 1$

$a_n = 2^n - 1$ Solución particular (Concreta): Sustituir casos base y resolver.

27/03/2019

Tema 9: Funciones Generatrices.

La función generatriz asociada a la sucesión $(a_0, a_1, \dots, a_n, \dots)$ $(a_k)_{k=0}^{\infty}$ se define como la serie formal de potencias siguiente: Son ctes constantes

$$\boxed{F(x) = a_0 + a_1 x + a_2 x^2 + \dots = \sum_{n=0} a_n x^n}$$

* $f(x) = e^x = \exp(x) \longleftrightarrow \left(\frac{1}{k!}\right)_{k=0}^{\infty}$ $\quad Coef_5[f(x)] = \frac{1}{5!}$ El coeficiente de x^5

* $f(x) = \frac{1}{1-x} = \sum_{k=0}^{\infty} x^k \longleftrightarrow (1)_{k=0}^{\infty}$ Infinitos 1's $\quad f(x) = \frac{1}{1-2x} \longleftrightarrow (2^k)_{k=0}^{\infty}$

* $f(x) = \frac{1-x^{p+1}}{1-x} = \sum_{k=0}^{p} x^k \longleftrightarrow (1)_{k=0}^{p}$ p 1's $\quad f(x) = \frac{1-x^3}{1-x} \longleftrightarrow (1)_{k=0}^{2} = (1,1,1,0,0\dots)$

* $f(x) = (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \longleftrightarrow \left[\binom{n}{k}\right]_{k=0}^{n}$ A partir de $n = k$ son 0's

Número combinatorio generalizado

$$\boxed{\binom{-\alpha}{k} = (-1)^k \binom{k+\alpha-1}{k}}$$

Ejem: $\binom{-2}{3} = \frac{(+2)(+3)(+4)}{3!}(+1)^3 = \frac{4\cdot3\cdot2}{3!} = \frac{4!}{3!\,1!} = \binom{4}{3} = \binom{4}{1}$ $\quad 3+2-1=4$, $\quad 4-3=1$

Propiedades (si son convergentes):

$$\sum (a_k + b_k) x^k = \sum a_k x^k + \sum b_k x^k$$

$$\sum \alpha a_k x^n = \alpha \sum a_k x^n$$

Maniobras basicas.

Desplazar hacia la derecha. $x^m f(x)$ (x^m unidades) $\quad (0,0,a_0,a_1,\dots) \longleftrightarrow x^2 f(x)$

Desplazar hacia la izquierda. $\frac{f(x) - (a_0 - a_1 x - \dots - a_{m-1}x^{m-1})}{x^m}$ m unidades, Los que no aparecen. $\quad (a_2, a_3, \dots) \longleftrightarrow \frac{f(x) - (a_0 - a_1 x)}{x^2}$

Si $k^p a_k$ Derivar todo y multiplicar por la variable tantas veces como sea p $\quad f(x) = (a_k)_{k=0}^{\infty} \quad x[f(x)x]' \longleftrightarrow (k^2 a_k)_{k=0}^{\infty}$

Ecuaciones de recurrencia.

1. Mirar el intervalo de validez para $\rightarrow \sum_{n=2}$ y meter ecuacion en el sumatorio.
2. Multiplico por x_n todos los terminos, tras separar sumas.
3. Sacar coeficientes y arreglar el sumatorio para llegar a $f(x)$ o similar.
4. Resolver la ecuación $f(x) = \bigcirc$ con $\frac{A}{\alpha - x} + \frac{B}{\beta - x}$
5. Sacar factor comun para llegar a la forma $\frac{A}{\alpha}\left(\frac{1}{1-\frac{x}{\alpha}}\right) + \frac{B}{\beta}\left(\frac{1}{1-\frac{x}{\beta}}\right)$
6. $a_n = \frac{A}{\alpha} \sum_{n=0} \left(\frac{x}{\alpha}\right)^n + \sum_{n=0} \frac{B}{\beta}\left(\frac{x}{\beta}\right)^n \Rightarrow \boxed{\frac{A}{\alpha}\underbrace{\left(\frac{1}{\alpha}\right)^n}_{coef} + \frac{B}{\beta}\underbrace{\left(\frac{1}{\beta}\right)^n}_{coef} = a_n}$

Repartos.

La función generatriz asociada al reparto, es el producto de las generatrices de cada una de las restricciones. Usar x y no $x_1, x_2 \ldots$ si no queremos saber las combi.

$0 \leq x \leq 2 \rightarrow 1 + x + x^2 \quad f(x) = f_1(x) \cdot f_2(x) \ldots = 1 + 3x + 5x^2 \ldots$

$\mathrm{Coef}_1[f(x)] = 3 \quad \mathrm{Coef}_2[f(x)] = 5$ Cogemos el coeficiente de la cantidad de elementos que manejamos. $x_1 + x_2 + x_3 = k$, k es el coeficiente.

Si la restricción es $0 \leq x$ en todas (n veces)

$$f(x) = f_1(x)^n = \left(\frac{1}{1+x}\right)^n = (1-x)^{-n} \quad \mathrm{Coef}_5[f(x)] = (-1)^5 \binom{-n}{5} = \binom{n+5-1}{5} = \binom{n+5-1}{n-1}$$

Se puede simplificar si la $f(x)$ tiene $x^3 f(x)$ que resta 3 unidades al coeficiente buscado en $f(x)$ o si $f(x) = (1-x^2)^{-3}$ podemos dividir el coeficiente entre dos (ya que va de por en par) 2 en 2

Tema 10: Polinomio Cromatico.

2/04/2019

Polinomio cromatico ($P_G(q)$): Indica cuantas coloraciones hay de un grafo G con q colores. Siendo q un número natural y $\boxed{q \geq 2}$.

Nº cromatico → Se puede colorear un grafo si: $\boxed{X(G) \leq q}$

el primer q que no anula el polinomio

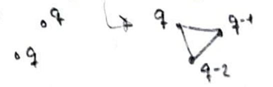
Dos grafos isometricos deben tener el mismo polinomio cromatico.

$q^n - a_{n-1} q^{n-1}$ Nos permite realizar recuentos de listas con restricciones y nos ayuda a organizar el principio de inclusión y exclusión.

n ← vertices

a_{n-1} ← Aristas

* La cota inferior → $P_{K_n}(q) = q(q-1)(q-2)\ldots(q-n+1)$
* La cota superior → $P_{N_n}(q) = q^n$ ← vacio, sin aristas



} A mayor número de aristas menor número de coloraciones.

* El polinomio cromatico de un grafo no conexo es: $P_G(q) = \prod_{i=1}^{\text{total componentes}} P_{G_i}(q)$

$P_{L_n}(q) = q(q-1)^{n-1}$ $\quad$ $P_{K_n}(q) = q(q-1)(q-2)\ldots = \frac{k!}{(k-n)!}$ $\quad$ $P_{C_n}(q) = (q-1)^n + (-1)^n (q-1)$

Los grafos bipartitos, como los arboles, tienen el mismo que una ~~lista~~ lineal (L_n)

* Algoritmo de contracción – borrado

$$P_G(q) = P_{G-e}(q) - P_{G/e}(q) =$$ El pol. del grafo sin una arista – El pol. con esos vectices contraidos.

Otro metodo es ver dos grafos unidos.

$$P_G(q) = \frac{P_{G_1}(q) \cdot P_{G_2}(q)}{P_{G_3}(q)} = \frac{\text{Grafo 1} \cdot \text{Grafo 2}}{\text{El que tienen en comun}} \quad \frac{q(q-1)^2(q-2)^2}{\cancel{q}} \quad \frac{q^2(q-1)^3(q-2)}{q^2} \quad \frac{q^2(q-1)^2(q-2)^2}{\cancel{q}(q-1)}$$

Hacemos el de q y luego con el otro ⋈ ↳ $q + (q-1)$

Recurrencia

$\rightarrow P_{C_{n-1}} - P_{C_{n-2}} \dots$

$\boxed{P_{C_n}(q)} = P_{L_n} - \boxed{P_{C_{n-1}}}$ $\quad a_n = t_n - a_{n-1} = q(q-1)^{n-1} - a_{n-1}$

Terminos de la recurrencia

Signos alternos
Sin termino independiente

Homogenea $a_n = -a_{n-1}$ $\quad x = -1$ $\quad x = A(-1)^n$

Particular $\tilde{a}_n = B(q-1)^n$ $\quad B(q-1) = q(q-1)^{n-1} - B(q-1)^{n-1}$; $\quad B = 1$

$a_n = A(-1)^n + 1(q-1)^n = (q-1)[-2q+5](-1)^n + (q-1)^{n-1}$

Emparejamientos perfectos.

Es un subgrafo generador de G en el que todos sus vertices tienen grado 1.

Debe G tener un $|V|$ par. y sus vertices como minimo grado 1. C_4 $\square \rightarrow$ || ó $=$
C_3 $\Delta \rightarrow$ /. No tiene.

$K_6 = 5 \cdot 3 \cdot 1 = 15$ emparejamientos $\quad K_4 = 3 \cdot 1 = 3$ $\quad K_8 = 7 \cdot 5 \cdot 3 \cdot 1 = 105$

9/04/2019

Tema 11: Relaciones entre conjuntos.

Binaria: Sean A y B dos conjuntos (iguales o distintos) una relación R de A en B es un (cualquier) subconjunto del producto cartesiana. $(A \times B)$

Hay $P(A \times B) = 2^{|A| \cdot |B|}$ posibles subconjuntos. $\quad (a,b)$

Pares ordenados con la primera componente perteneciente a A y la sengunda a B

Metodos de representación:

- Matriz de adyacencia, si es A y B el mismo conjunto es cuadrada.
- Representación cartesiana:
- Diagrama de Venn
- Grafo dirigido y bipartito. si $A \times A$ tiene más sentido.

$A \times B$
(a, b)

Dominio: Conjunto de los elementos de A que tienen relación con alguno de B.

Codominio: Conjunto de los elementos de B que tienen relación con alguno de A.

Relación inversa (R^{-1}): $aRb \Leftrightarrow bR^{-1}a$ Tiene sentido cuando los conjuntos sean distintos

Relación complementaria ($\overline{R}$) $a\overline{R}b \Leftrightarrow a\not{R}b$ Si a no se relaciona con b.

Tiene sentidos cuando son el mismo conjunto. $aRb \cup a\overline{R} =$ Todas las relaciones.

Composición: Sean $\left\{ \begin{array}{l} R \text{ una relación } V \text{ en } W \\ S \text{ una relación } W \text{ en } Y \end{array} \right\} \Rightarrow S \circ R$ de V en Y

$a(S \circ R)c \Leftrightarrow \exists b \in W$ $\quad aRb$, bRc

La matriz de adyacencia será $|V| \times |Y|$ y se multiplica booleanamente

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

Propiedades (pueden verificarse o no):

Reflexividad: Si $\forall a \in A,\ aRa$ $\begin{pmatrix} 1 & - & - \\ - & 1 & - \\ - & - & 1 \end{pmatrix}$ No si $\exists a \in A\ a\overline{R}a$

Antireflexividad: Si $\forall a \in A,\ a\cancel{R}a = a\overline{R}a$ $\begin{pmatrix} 0 & - & - \\ - & 0 & - \\ - & - & 0 \end{pmatrix}$ No $\exists a \in A\ aRa$

Simetria: Si $(\forall a,b \in A)$, si $aRb \Rightarrow bRa$ $\begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \end{array}$ 1,3 3,3 2,1 1,2 No $\exists a,b \in A\ aRb \Rightarrow b\overline{R}a$

Antisimetria: Si $(\forall a,b \in A)$, si $(aRb \wedge bRa) \Rightarrow a=b$ $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ Solo si en el simetrico hay lo contrario excepto en la diagonal.

Si la matriz de R es igual que la de R^2 es transitiva $M_R = M_{R^2}$

Transitiva: Si $\forall a,b,c \in A$, si $(aRb \wedge bRc) \Rightarrow aRc$ $\begin{array}{c|ccc} & 1 & 2 & 3 \\ \hline 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 3 & 0 & 1 & 0 \end{array}$ No $\underset{1}{1R2} \wedge \underset{1}{2R3} \Rightarrow \underset{0}{1\cancel{R}3}$ niego No se cumple

Relaciones de equivalencia: Una relación es de equivalencia si cumple la propiedad reflexiva, simetria y transitiva. $a \equiv b\ (\text{mód } R)$ a equivale por equivalencia con b.

Clase de equivalencia: $a \in [a]$ Conjunto de todos los elementos relacionados con a.

$[a]_R = \{x \in A : aRx\}$ Buscar la relacion entre elementos ejem $[3] = \{3, 9, 27 \ldots\} = \{3^n : n \in \mathbb{N}\}$

Cada elemento de $[a]_R$ se llama representante.

Sean $a,b \in A$ con R de equivalencia. $[a]$ y $[b]$ $[a] \subseteq A$ $[b] \subseteq A$

$[a] \cap [b] \to \emptyset$ Disjuntos

$[a] \cap [b] \to \neq \emptyset \Rightarrow [a] = [b]$ por la simetria.

Conjunto cociente:

El conjunto de todas las clases de equivalencia de una relación de equivalencia R sobre V. $V/_R = \{[v]_R : v \in V\}$

Tema 12: Aritmética entera.

Divisibilidad: Si $a|b$ y $a|c \Rightarrow a|(b+c)$ $b = aq$ $c = ak$ $b+c = aq+ak = (q+k)a$

Tema 1 Si $a|b \Rightarrow ac|bc$ $\forall c \in \mathbb{Z}$

$\forall a,b \in \mathbb{Z}$, $b > a$ $\begin{cases} a|b & \exists q \in \mathbb{Z} : b = qa \\ a\nmid b & \exists q \in \mathbb{Z} : b = aq + r \quad 0 \leq r < |b| \end{cases}$

Teorema de Euclides (Hallar mcd) ← El comun más pequeño

Dada $a,b \in \mathbb{Z} \Rightarrow \exists q,r : a = bq + r$ $mcd(a,b) = mcd(b,r) \ldots = k$

$mcd(82,8) = mcd(8,2) = 2$ $82 = 8 \cdot 10 + 2$ $8 = 2 \cdot 4$ k el resto ultimo (no 0)

Identidad de Bezout:

Sean $a,b \in \mathbb{Z} : mcd(a,b) = d \Rightarrow \exists \alpha, \beta \in \mathbb{Z} : \alpha a + \beta b = d$

$a = bq_1 + r_1 \Rightarrow r_1 = a - bq_1$

$b = r_1 q_2 + r_2 \Rightarrow r_2 = b - r_1 q_2$

$\vdots \qquad \vdots$

$r_n = r_{n-1} q_n + r_n \Rightarrow r_n = r_{n-2} - r_{n-1} q_n$

$r_{n+1} = r_n q_{n-1}$

Se hace el teorema de euclides, y se van despejando los restos, dejando el ultimo (mcd) al otro lado y vamos sustituyendo los anteriores hasta llegar a la forma $\alpha a + \beta b = d$

$\text{mcd}(ac, bc) = dc$

Si $\text{mcd}(a,b) = d \Rightarrow \text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ Pasan a ser coprimos.

Mínimo comun multiplo: Los comunes y no comunes al mayor exponente.

Ecuaciónes diofanticas lineales: Donde x e y son enteros.

$ax + by = n \quad a, b, n \in \mathbb{Z}$

1° La ecuación tiene solución: Si y solo si $\text{mcd}(a,b) \mid n$. 1'5° Simplificamos. $\frac{a}{d}x + \frac{b}{d}y = \frac{n}{d}$

2° Hallamos una solución particular con Bezout. $ax_0 + by_0 = \text{mcd}(a,b) = d$

3° Y multiplicamos los x_0, y_0 y d por el número necesario para que sea n.

4° Restamos la anterior a la original. $a(x - x_0) = b(y_0 - y)$

5° Como hemos simplificado al principio, $a \nmid b$, pero si $a \mid (y_0 - y)$ entonces.

$ak = y_0 - y \quad \boxed{y = -ak + y_0} \quad bk = x - x_0 \quad \boxed{x = bk + x_0}$ Soluciones para $\forall k \in \mathbb{Z}$

Teorema: Si p es compuesto $\Leftrightarrow$ es divisible por un primo $\leq \sqrt{p}$

30/04/2019

Aritmética Modular (en $\mathbb{Z}_m$) $\quad \mathbb{Z}_m = \mathbb{Z}/\equiv$ Conjunto cociente de modulo m.

Relación de congruencia.

"Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$ se dice que a es congruente con b, modulo m".

$a \equiv b \pmod{m}$ si $m \mid (a - b)$"

Es una relación de equivalencia.

Hay tantas clases de equivalencia como restos (para m hay $0, 1, \dots, m-1$)

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \{[0]_5, [1]_5 \dots\}$

Sean $a, b, c, d \in \mathbb{Z}$ y $m \in \mathbb{N}$

$$\text{Si} \left\{ \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \right\} \Rightarrow \begin{array}{l} a - b = qm \\ c - d = q'm \end{array} \Rightarrow a + c - (b + d) = (q' + q)m$$

$$\boxed{(a+c) \equiv (b+d) \pmod{m}}$$

$\boxed{ac \equiv bd \pmod{m}}$

$\boxed{a^k \equiv b^k \pmod{m} \quad k \in \mathbb{N}}$

Cancelativa

$\text{mcd}(c, m) = 1 \quad \underline{ac} \equiv \underline{bc} \pmod{m} \Rightarrow \underline{a} \equiv \underline{b} \pmod{m}$

$\text{mcd}(c, m) \neq 1 \quad \underline{ac} \equiv \underline{bc} \pmod{\underline{pc}} \Rightarrow \underline{a} \equiv \underline{b} \pmod{\underline{p}}$

$m = pc$

Matemática Discreta T(10) 30/04/2019

Ecuaciones lineales de congruencia.

$ax \equiv b \pmod{m}$ Si se puede se simplifica con la cancelativa.

$ax + my = b$ Hay $mcd(a,m)=d$ soluciones. Debe b ser divisible con d $(d|b)$

Solo soluciones de x — Los valores de x están entre $0-(m-1)$, y si supera se resta m o suma si es negativo.

$x \equiv 0 \pmod{m}$

Cuidado para simplificado el válido es m original.

Sea p primo $(\mathbb{Z}_p)$ todos los elementos tienen inverso a excepción del 0

$(\mathbb{Z}_p, +, \cdot)$ Estructura de Cuerpo Conmutativo.

Sea m compuesto $(\mathbb{Z}_m, +, \cdot)$ Anillo conmutativo unitario.

Sea $m \in \mathbb{N}$ $(\mathbb{Z}_m)$

U_m = Conjunto de elementos invertibles (llamados unidades)

Números cuyo $mcd(m, x)=1$ Ejem: $U_4 = \{\bar{1}, \bar{3}\}$ $mcd(1,4)=1$ $mcd(3,4)=1$

$|U_m| = \varnothing(m)$ Cardinal del conjunto de unidades.

Teorema pequeño de Fermat — Si p es primo $\varnothing(p) = p-1$ $\quad \varnothing(5)=4$

Si m es compuesto $\varnothing(m) < m$ $\quad \varnothing(4)=2$

Si p ~~natural~~ primo $\varnothing(p^k) = p^{k-1}(p-1)$ $\quad \varnothing(8) = \varnothing(2^3) = 2^2 \cdot 1 = 4$

Si $mcd(m,n)=1$ $\varnothing(m \cdot n) = \varnothing(m)\varnothing(n)$

Teorema de Euler.

$y^{\varnothing(m)} \equiv 1 \pmod{m}$ $\quad \mathbb{Z}_4$ $U_4 = \{\bar{1}, \bar{3}\}$ $\quad 3^{\varnothing(4)} \equiv 1 \pmod 4$ $\quad 9 \equiv 1 \pmod 4$

Teorema chino del resto.

$x \equiv a \pmod c$

$x \equiv b \pmod d$

$x \equiv a \cdot d \cdot inv(a \cdot d) + b \cdot c \cdot (inv(b \cdot c)) \pmod{c \cdot d}$

Saber resto.

$2^{68} : 19 \quad 2^{\varnothing(19)} = 2^{18} \quad 2^{18} \equiv 1 \pmod{19} \quad (2^{18})^3 \cdot 2^{14} \equiv 2^{14} \pmod{19}$ $\quad 54+14=68$

$2^4 \equiv -3 \pmod{19}$ $\quad 16-(-3)=19$ $\quad (2^{18})^3 \cdot (2^4)^3 \cdot 2^2 \equiv (-3)^3 \cdot 2^2 \pmod{19} \quad 2^{68} \equiv -27 \cdot 4 \pmod{19}$

$-27 + 19 = -8 + 19 = 11$ $\quad -8 \cdot 4 = -32 + 19 + 19 = \boxed{6}$

$2^{68} \equiv 44 \pmod{19}$ $\quad 44-19=25-19=6$ $\quad 2^{68} \equiv 6 \pmod{19}$

El resto es 6

Inverso multiplicativo. (2^{68} en $\mathbb{Z}_{19}$)

1° Sean coprimos (2^{68} y 19, $mcd(2^{68}, 19)=1$) y única.

2° Hay que hallar $2^{68} x \equiv 1 \pmod{19}$

3° Por el teorema pequeño de Ferman $2^{18} \equiv 1 \pmod{19}$ $[y^{\varnothing(m)} \equiv 1 \pmod m]$

4° Descomponemos $68 = 18 \cdot 3 + 14$, con la $\varnothing(m)$ presente.

5° Para que sea $\equiv 1 \pmod{19}$, buscamos lo que le falta para serlo. $18-14=4$ completar la unidad de $\varnothing(19)$ $\quad X \equiv 2^4 \pmod{19}$ $\quad 16$

3° Hacer inv. 2^{68} y multiplicar por el 1 de $x \equiv 1 \pmod m$

4° Arreglar el valor

1° Hacer Bezout de 2^{68} y 18

2° El que acompaña a 2^{68} es el inverso

3.° Arreglar para el modulo ($\pm$ m

Relación de orden parcial ($\preceq$)

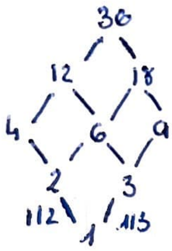
Relación reflexiva, antisimetrica y transitiva.

$(V, \preceq)$ Conjunto parcidmente ordenado o poset.

$a, b \in V$ son <u>comparables</u> si <u>$a \preceq b$ o bien $b \preceq a$</u>, si no no comparables.

Si $\forall a, b \in V$ son comparables, $(V, \preceq)$ esta <u>totalmente ordenado</u> o <u>cadena</u>

Diagrama de Hasse.



Para conjuntos parcial o totalmente ordenado.

Si hay una matriz se eligen los que tienen columna con + ceros. $\begin{pmatrix} - & 0 & - \\ - & 0 & - \\ - & 0 & - \\ - & 1 & - \end{pmatrix}$

Se relacionan en filas $\begin{array}{c|cccc} & a & b & & \\ \hline a & 1 & 1 & 0 & 0 \\ b & \vdots & \vdots & & \end{array}$ a – b

1° Hay bucles en cada vertice, pero se suprimen.

2° La transitividad se refleja sin ciclos. De $a \preceq b$ $b \preceq c$ se elimina $a \preceq c$

3.° Se eliminan los sentidos de las flechas, haciendo que apunten hacia arriba.

- Elemento Maximal, cuando no hay elementos por encima de este con los que se relacio
- Elemento Minimal, cuando no hay por debajo, no se relaciona.

- Elemento maximo, el maximal si es unico.
- Elemento minimo, el minimal si es unico.

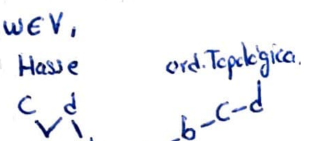
- Cota superior (Mayorante), elemento <u>del subconjunto</u> <u>o no</u> que están relacionados <u>con todos</u> los elementos del subconjunto <u>por debajo</u>.

- Cota inferior (Minorante), esta relacionado <u>por encima</u> con <u>todos</u> los elementos del subconjunto, este puede o no ser del subconjunto

- Supremo, el <u>mayor</u> de las cota superior. $\sup(B) = a$
- Infimo, el menor de las cota inferior. $\inf(B) = d$

Orden total ($\preceq_T$) es <u>Compatible</u> con el orden parcial $\preceq_p$ si para todo $v, w \in V$, $v \preceq_p w$ implica que $v \preceq_T w$.

Algoritmo de ordenación topológica, se van eligiendo los minimales.



Conjunto bien ordenado, $(V, \preceq)$ lo es si es de orden total y cualquier subconjunto no vacio de V tiene <u>siempre un minimo</u>. Como $\mathbb{N}$ el min = 1, no $\mathbb{R}$ el minimo es infinito.

Inducción, se puede hacer si es de un conjunto bien ordenado.

- Versión debil, caso base (minimo), – suponer el k cierto y demostrar $k+1$
- Versión fuerte, caso base (minimo), se quiere demostrar k y se hacen desde caso base hasta $k-1$