Inducción matemática y Principio del buen orden

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

5 de mayo de 2020

Tabla de contenidos

A lo largo del curso aceptaremos los siguientes conjuntos con sus propiedades:

1. Número naturales $\mathbb{N} = \{1, 2, \ldots\}$.
2. Números enteros $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$, es decir: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
3. Números racionales $\mathbb{Q} = \left\{ \frac{a}{b} \,/\, a \in \mathbb{Z}, b \in \mathbb{Z}^* \right\}$ donde $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$.
4. Números reales $\mathbb{R}$.

Sumatorias y productorias

Si $a_1, a_2, \ldots, a_n$ son números reales, entonces los símbolos $\sum$ (sumatoria) y $\prod$ (productoria) se definen como sigue:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n \quad \text{y} \quad \prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n.$$

Ejemplos:

$$\sum_{j=2}^{5} \frac{1}{2j} = \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10}, \quad \text{y}$$

$$\prod_{i=1}^{n} \frac{i+1}{i} = \left(\frac{2}{1}\right)\left(\frac{3}{2}\right)\ldots\left(\frac{n+1}{n}\right) = n+1.$$

Tabla de contenidos

Definición 1

Diremos que un subconjunto $S \subset \mathbb{R}$ posee un **menor elemento** *si existe $s \in S$ tal que $s \leq x$ para todo $x \in S$. En tal caso diremos que s es el* **menor elemento** *de S.*

Definición 2

Diremos que un subconjunto $H \subset \mathbb{R}$ es **bien ordenado** *si todo subconjunto no vacío de H posee un menor elemento.*

Principio del buen orden

El conjunto $\mathbb{N} \subset \mathbb{R}$ es bien ordenado, es decir, cualquier subconjunto $S \subset \mathbb{N}$ y $S \neq \emptyset$ posee un menor elemento.

Ejemplo:

En un torneo cada jugador juega con cada uno de los otros jugadores exactamente una vez, y cada juego entrega un ganador y un perdedor. Decimos que los jugadores $p_1, p_2, \ldots, p_m$ forma un **ciclo** de largo m si p_1 le gana a p_2, p_2 le gana a p_3, ..., p_{m-1} le gana a p_m y p_m le gana a p_1.

Use el principio del buen orden para demostrar que si hay un ciclo $p_1, p_2, \ldots, p_m$ $(m \geq 3)$ en un torneo, entonces hay un ciclo de largo 3.

Solución:

Por contradicción. Asuma que no hay ciclo de largo 3.

El conjunto:
$S = \{n \in \mathbb{N} \,/ \text{existen jugadores} \quad p_1, \ldots p_n \quad \text{que forman un ciclo}\}$
es no vacío ya que por hipótesis existe $m \geq 3$ tal que $p_1, \ldots p_m$ es un ciclo, entonces $m \in S$.

Por el Principio del Buen Orden, existe $k \in S$ que es su menor elemento y $p_1, p_2, \ldots, p_k$ es un ciclo de largo k.

Considere jugadores p_1, p_2 y p_3. Entonces p_1 le ganó a p_3, de lo contrario habría un ciclo de largo 3.

Pero entonces, $p_1, p_3, \ldots, p_{k-1}$ es también un ciclo, esta vez de largo $k-1$ lo cual es una contradicción.

Ejemplo: Algoritmo de la división

Para $a, b \in \mathbb{Z}$ con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ tales que:

$$a = bq + r, \quad 0 \leq r < b.$$

Solución:
Defina el conjunto: $S = \{a - bx \,/\, x \in \mathbb{N},\ a - bx \geq 0\}$.
Observe que para $x = -|a|$ entonces
$a - bx = a + |a|b \geq a + |a| \geq 0$ entonces $x = -|a| \in S$.
Luego: $S \neq \emptyset$ y $S \subset \mathbb{N}$, entonces por el principio del buen orden existe un elemento mínimo $r \in S$ de la forma $r = a - bq$ para algún $q \in \mathbb{Z}$.
Por definición $r \geq 0$.

Ejemplo: Algoritmo de la división (cont.)

Veamos también que $r < b$. En efecto, si $r \geq b$ entonces $r - b \geq 0 \Rightarrow a - bq - b \geq 0$, es decir:

$$0 \leq r - b = a - (q + 1)b$$

es decir, $r - b$ sería un elemento de S menor que el elemento mínimo r, lo cual es una contradicción.
Lo anterior prueba la existencia.
Ahora vamos a probar la unicidad:
Supongamos que a tiene dos representaciones, es decir, existen $q, q' \in \mathbb{Z}$ y $r, r' \in \mathbb{Z}$ tal que:

$$qb + r = a = q'b + r', \quad 0 \leq r, r' < b,$$

Ejemplo: Algoritmo de la división (cont.)

luego: $0 \leq r < b$ y $-b < -r' \leq 0$ entonces $-b < r - r' < b$ y por tanto:$|r - r'| < b$.
A partir de las expresiones para " a " resulta:

$$b > |r - r'| = b|q' - q| \Rightarrow |q' - q| < 1$$

donde en $\mathbb{Z}$ la única posibilidad es $q' - q = 0$, es decir, $q = q'$ y así $r = r'$

Tabla de contenidos

Principio de inducción simple

Sea X un subconjunto de los números naturales tal que:
a. $1 \in X$.
b. Si dado $n \in X$ implica que $n + 1 \in X$.

Entonces X es el conjunto de los números naturales, es decir, $X = \mathbb{N}$.

Demostración:
Por contradicción. Asuma que el conjunto X satisface **(a)** y **(b)** pero $X \neq \mathbb{N}$. Entonces existe al menos un $n \in \mathbb{N}$ pero $n \notin X$.

Entonces el conjunto $S = \{n \in \mathbb{N} \,/\, n \notin X\}$ es no vacío y $S \subset \mathbb{N}$.

Entonces por el principio del buen orden existe $n_0 \in S$ que es el menor elemento de S.

Como X cumple **(a)**, es decir, $1 \in X$, entonces $n_0 > 1$ y desde que n_0 es el menor elemento de S entonces $n_0 - 1 \in X$.

Como X cumple **(b)** implica que $(n_0 - 1) + 1 = n_0 \in X$ lo cual es una contradicción.

Sean $\{P_n\}$ con $n \in \mathbb{N}$, un conjunto de propiedades cuya certeza queremos probar. Si:
1. La propiedad es cierta para $n = n_0$.
2. Si la propiedad es cierta para $n = k$ también lo es para $n = k + 1$.

Entonces la propiedad es cierta para $n \geq n_0$.

Ejemplo: Demuestre por inducción que todo número mayor o igual que 8 puede escribirse como una suma de treses (3) y cincos (5).

Solución:

El caso base de la inducción es $n = 8$, así se tiene: $8 = 5 + 3$.
Por tanto, la propiedad es cierta para $n = 8$.
Supongamos que la propiedad se cumple para un cierto número k, es decir, k se puede poner como suma de treses y cincos. Esto quiere decir que existen a y b enteros mayores o iguales que 0 tales que:

$$k = 3a + 5b.$$

Siendo esto cierto, ¿se puede poner $k + 1$ como suma de treses y cincos?. Distinguiremos dos casos: $b > 0$ y $b = 0$.
Si $b > 0$, en la descomposición de k tenemos por lo menos un 5 y podremos poner:

$$k = 3a + 5(b - 1) + 5,$$

Solución: (cont.)

por tanto: $k + 1 = 3a + 5(b - 1) + 6 = 3(a + 2) + 5(b - 1)$.
Si $b = 0$, tenemos que k es múltiplo de 3, es decir, $k = 3a$.
Pero como $k \geq 8$, entonces $k = 9, 12, 15, \ldots$, lo que quiere decir que $a \leq 3$, de esta forma se tiene:

$$k = 3(a - 3) + 9$$

y en consecuencia: $k + 1 = 3(a - 3) + 10 = 3(a - 3) + 2(5)$.
Por tanto, si k cumple la propiedad también la cumple $k + 1$.
Puesto que la base de la inducción está probada para $n = 8$, podemos concluir que todo número mayor o igual que 8 se puede expresar como suma de treses y cincos.

Principio de inducción fuerte

Una propiedad $P(n)$ que cumple:

a. $P(1)$ es cierto, y
b. para todo número natural n se cumple $P(j)$ para todo $j = 1, \ldots, n$ entonces $P(n+1)$ se sigue cumpliendo.

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

Observaciones:

1. La inducción fuerte da mayor flexibilidad para probar algo respecto a la inducción simple.
2. En la inducción fuerte se puede usar cualquier hipótesis inductiva previa.

Demostración del Principio de inducción fuerte

Defina el conjunto $X = \{n \in \mathbb{N} \,/\, P(n) \quad \text{es verdadero}\}$. Demostremos que $X = \mathbb{N}$.

Considere el conjunto $Y = \mathbb{N} \backslash X$. Afirmamos que $Y = \emptyset$. Caso contrario, tenemos $Y \neq \emptyset$ e $Y \subset \mathbb{N}$, entonces por el principio del buen orden, existe un mínimo elemento $p \in Y$. Note que $p \notin X$

Entonces, para todo $n \in \mathbb{N}$ tal que $n < p$ se cumple que $n \in X$, esto es para $n = 1, 2, \ldots, p-1$ se tiene que $P(n)$ es verdadero.

De la parte **(b)** del principio de inducción fuerte se tiene que $P(p)$ es verdadero, es decir $p \in X$, lo cual es una contradicción.

Ejemplo:

La **sucesión de Fibonacci** $\{F_n\}_{n=1}^{\infty}$ es definida por $F_1 = 1$, $F_2 = 1$ y $F_n = F_{n-1} + F_{n-2}$ para todo $n \in \mathbb{N}$.

Demuestre que $F_n = \dfrac{1}{\sqrt{5}}\left[\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n\right]$.

Solución
Usaremos el principio de inducción fuerte.
Definimos

$$S = \left\{ n \in \mathbb{N} \,/\, F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]\right\}.$$

Luego:

Ejemplo: (cont.)

- Para $n = 1$:
  $F_1 = \dfrac{1}{\sqrt{5}}\left[\left(\dfrac{1+\sqrt{5}}{2}\right) - \left(\dfrac{1-\sqrt{5}}{2}\right)\right] = \dfrac{1}{\sqrt{5}}\left[\dfrac{2\sqrt{5}}{2}\right] = 1.$
- Sea $n \in \mathbb{N}$ tal que $1, 2, \ldots, n-1, n \in S$.

Demostremos que $n+1 \in S$:
Sabemos que $F_{n+1} = F_n + F_{n-1}$ y como $n-1, n \in S$ entonces:

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

$$F_{n-1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right]$$

Ejemplo: (cont.)

Observe:

$$\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} = \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left[\frac{1+\sqrt{5}}{2} + 1\right]$$

$$\left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} = \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left[\frac{1-\sqrt{5}}{2} + 1\right]$$

además:

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+\sqrt{5}}{2} + 1 \quad \text{y} \quad \left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{1-\sqrt{5}}{2} + 1$$

Ejemplo: (cont.)

Por tanto, reemplazando en F_{n+1} resulta:

$$\begin{aligned} F_{n+1} &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2} + 1\right) \\ &- \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2} + 1\right) \\ \Rightarrow F_{n+1} &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}\right)^2 \\ &- \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2}\right)^2 \end{aligned}$$

Ejemplo: (cont.)

simplificando:

$$F_{n+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

ordenando:

$$F_{n+1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right],$$

así $n+1 \in S$ y del principio de inducción fuerte concluimos que $S = \mathbb{N}$.

Sea $P(n)$ una propiedad que depende del parámetro $n \in \mathbb{N}$ y suponga que:

a. $P(n_0)$ es verdadero para un cierto $n_0 \in \mathbb{N}$.
b. Siempre que $P(k)$ es verdadero y que $P(m)$ es verdadero para cualquier $n_0 < m < k$ se tendrá que $P(k+1)$ es verdadero.

Entonces la afirmación $P(n)$ es verdadero para todo $n \in \mathbb{N}$ y $n > n_0$.

Ejemplo:

Demuestre usando inducción fuerte que todo entero $n > 1$ puede ser escrito como un producto de números primos (¿Puede usarse el primer principio de inducción?).

Solución:
Considere la propiedad:

$$P(n) = \{n \in \mathbb{N} \,/\, n \quad \text{puede ser escrito como producto de números primos}\}$$

- Caso base: $n_0 = 2$ y observe que $P(n_0)$ es verdadero.
- Hipótesis inductiva: Considere $k+1 \in \mathbb{N}$ y asuma por hipótesis inductiva que todo $P(j)$ es verdadero para todo $j \in [2, k]$ y $j \in \mathbb{N}$. Esto significa que j puede ser escrito como un producto de primos para todo $j \in [2, k]$.

Ejemplo: (cont.)

Demostremos que $P(k+1)$ es verdadero. Tenemos dos casos:

- Si $k+1$ es primo, entonces $P(k+1)$ es verdadero.
- Si $k+1$ no es primo: en este caso existen dos enteros $r, s \in [2, k]$ tal que $k+1 = rs$. Por hipótesis inductiva, r y s pueden ser escritos como producto de primos.

Así podemos concluir que $k+1$ puede ser escrito como producto de primos.
En conclusión, $P(n)$ es verdadero para todo $n \geq n_0$ y $n \in \mathbb{N}$.

Sean $b \in \mathbb{N}$ y j un entero positivo. Entonces, una propiedad $P(n)$ se se cumple para todo $n \in \mathbb{N}$ y $n \geq b$ si:

a. $P(b), P(b+1), \ldots, P(b+j)$ son verdaderas, y
b. para todo $k \geq b+j$, si $P(l)$ es verdadero para cada $l \in [b, k]$ entonces $P(k+1)$ es verdadero.

Ejemplo:

Demuestre que cualquier cantidad entera positiva mayor o igual a 12 pesos puede ser pagada usando sólo monedas de 4 y 5 pesos.

Solución:
El conjunto

$$P(k) = \{k \in \mathbb{N} \,/\, k \quad \text{pesos puede pagarse con monedas sólo de 4 y 5 pesos}\}$$

Para el caso inductivo, observe que esto es cierto para los casos: $j = 12, 13, 14, 15$.
Nuestra hipótesis inductiva indica que la propiedad $P(j)$ es verdadera para todo $j \in [12, k]$ donde $j \in \mathbb{N}$ y k es un entero mayor o igual a 15.

Ejemplo: (cont.)

Queremos demostrar que $P(k+1)$ sea verdadera, es decir, $k+1$ pesos puede ser pagada sólo con monedas de 4 y 5 pesos.

Dado que $k \geq 15$, por hipótesis inductiva, la propiedad es cierta para $k-3$.

Es decir, $k-3$ pesos puede ser pagada sólo con monedas de 4 y 5 pesos. Por tanto, si agregamos una moneda más de 4 pesos obtenemos la cantidad $k+1$, la cual viene repartida en monedas sólo de 4 y 5 pesos.

Tabla de contenidos

Tanto el Principio del buen orden como los principios de inducción son axiomas acerca de los naturales $\mathbb{N}$, es decir, no pueden demostrarse sino que son parte de la definición de $\mathbb{N}$.
Resulta sorprendente el siguiente resultado:

Teorema 1

Las siguientes proposiciones son equivalentes sobre $\mathbb{N}$:

1. *Principio del buen orden.*
2. *Principio de inducción fuerte.*
3. *Principio de inducción.*

Hemos demostrado el Principio de inducción matemática y el principio de inducción fuerte usando como hipótesis el Principio del buen orden.

Demostremos ahora el Principio del buen orden usando como hipótesis el Principio de inducción matemática.

Demostración:

Sea $X \subset \mathbb{N}$ y $X \neq \emptyset$. Supongamos que X no tiene elemento mínimo, es decir:

$$\forall\, m \in X \quad \exists n \in A \quad \text{tal que} \quad m \geq n$$

Si $1 \in X$ entonces $1 < n$ para todo $n \in X$, lo cual no puede ocurrir porque X no tiene menor elemento, entonces $1 \notin X$.
Sea $Y = \mathbb{N} \backslash X$, entonces $1 \in Y$. Sea $k \in \mathbb{N}$ tal que $1, 2, 3, \ldots, k \in Y$. Entonces, $k+1 \in B$ de lo contrario, $k+1$ sería el primer elemento de X, lo cual no ocurre pues X no tiene elemento mínimo.
Por tanto, por el principio de inducción se tiene que $Y = \mathbb{N}$ y como $Y = \mathbb{N} \backslash X$ entonces $X = \emptyset$ lo cual es una contradicción.
Por lo tanto, X debe tener un elemento mínimo.

CONJUNTOS-RELACIONES-FUNCIONES

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

30/03/2020

Tabla de contenidos

Un **conjunto** está formado de objetos que son llamados elementos del conjunto.

La relación básica entre un conjunto y un objeto es la **relación de pertenencia.**

Cuando un objeto x es uno de los elementos de un conjunto A, decimos que x **pertenece** a A y se denota por $x \in A$.

Caso contrario, cuando un objeto x no es uno de los elementos de un conjunto A, decimos que x **no pertenece** a A y se denota por $x \notin A$.

El método más frecuente de definir un conjunto es por medio de una propiedad común y exclusiva de sus elementos.

Siendo más preciso, partiendo de una propiedad P definimos el conjunto A del modo que sigue:

Si un objeto x satisface la propiedad P entonces $x \in A$, y si x no satisface P entonces $x \notin A$

lo anterior se expresa: $A = \{x \,/\, x \quad \text{satisface la propiedad} \quad P\}$.

En ocasiones, la propiedad P se refiere a elementos de un cierto conjunto universal U, en cuyo caso:

$$A = \{x \in U \,/\, x \quad \text{satisface la propiedad} \quad P\}$$

Ejemplos:

1. $\mathbb{N} = \{1, 2, \ldots, \}, \mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$, etc.
2. Definamos: U: conjunto de todos los triángulos. Sea la propiedad P: Es un triángulo rectángulo. Luego: $A = \{x \in U \,/\, x \quad \text{satisface la propiedad} \quad P\}$ = Conjunto de todos los triángulos rectángulos.
3. En cálculo se trabajan con conjuntos de la forma:

$$\begin{aligned} [a, b] &= \{x \in \mathbb{R} \,/\, a \leq x \leq b\} \\ [a, b\rangle &= \{x \in \mathbb{R} \,/\, a \leq x < b\} \\ \langle a, b] &= \{x \in \mathbb{R} \,/\, a < x \leq b\} \\ \langle a, b\rangle &= \{x \in \mathbb{R} \,/\, a < x < b\} \end{aligned}$$

Definition 1 (Conjunto vacío)

Denotado por $\emptyset$, es definido así:

Para todo x se cumple que $x \notin \emptyset$

Ejemplo: $\emptyset = \{x \in \mathbb{N} \,/\, 1 < x < 2\}$.

Definition 2 (Inclusión)

A es subconjunto de B cuando todo elemento de A es elemento de B. Se denota por $A \subset B$ y se lee " A está contenido en B ".

Ejemplo: Sean X conjunto de todos los cuadrados e Y conjunto de todos los rectángulos, entonces $X \subset Y$.

Observación: $A \subset B$ no excluye la posibilidad que $A = B$. En el caso que $A \subset B$ y $A \neq B$ se dice que A es un subconjunto propio de B.

Propiedades de la inclusión:

Se cumple:

1. Es reflexiva: $A \subset A$ para todo conjunto A.
2. Antisimétrica: Si $A \subset B$ y $B \subset A$ entonces $A = B$.
3. Transitiva: Si $A \subset B$ y $B \subset C$ entonces $A \subset C$.

Definition 3 (Conjunto de partes)

Dado un conjunto A, se denota por $\mathcal{P}(A)$ al conjunto cuyos elementos son los subconjuntos de A.

Observación: $\mathcal{P}(A)$ nunca es vacío porque $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$.
Ejemplo: Si $A = \{1, 2, 3\}$ entonces
$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Operaciones entre conjuntos

Definition 4 (Unión)

Denotado por $A \cup B$ y está formado por los elementos de A con los elementos de B, es decir:

$$A \cup B = \{x \,/\, x \in A \quad \vee \quad x \in B\}.$$

Definition 5 (Intersección)

Denotado por $A \cup B$ y está formado por los elementos comunes de A y de B, es decir:

$$A \cap B = \{x \,/\, x \in A \quad \wedge \quad x \in B\}.$$

Observación: En el caso que A y B no tienen elementos comunes, entonces $A \cap B = \emptyset$.

Operaciones entre conjuntos

Definition 6 (Diferencia)

Denotado por $A - B$ y está formado por los elementos de A que no pertenecen a B, es decir:

$$A - B = \{x \,/\, x \in A \quad \vee \quad x \notin B\}.$$

Definition 7 (Complemento)

Si $B \subset A$ entonces $A - B$ se llama el **complemento** *de B en relación a A. Esto se denota $C_A B$.*

Observación: Es usual tener un conjunto universal U, en este caso, el complemento de A es denotado por CA o A^c. Por tanto, $x \in A^c \Leftrightarrow x \notin A$.

Propiedades de conjuntos

Con la **unión:**

1. $A \cup \emptyset = A$.
2. $A \cup A = A$.
3. $A \cup B = B \cup A$.
4. $(A \cup B) \cup C = A \cup (B \cup C)$.
5. $A \cup B = A \Leftrightarrow B \subset A$.
6. $A \subset B, A' \subset B' \Rightarrow (A \cup A') \subset (B \cup B')$.
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Con la **intersección:**

1. $A \cap \emptyset = A$.
2. $A \cap A = A$.
3. $A \cap B = B \cap A$.
4. $(A \cap B) \cap C = A \cap (B \cap C)$.
5. $A \cap B = A \Leftrightarrow A \subset B$.
6. $A \subset B, A' \subset B' \Rightarrow (A \cap A') \subset (B \cap B')$.
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Propiedades de conjuntos

Con el **complemento:**
Sean A, B subconjuntos de un conjunto universal U, luego:

1. $(A^c)^c = A$.
2. $A \subset B \Leftrightarrow B^c \subset A^c$.
3. $A = \emptyset \Leftrightarrow A^c = U$.
4. $(A \cup B)^c = A^c \cap B^c$.
5. $(A \cap B)^c = A^c \cup B^c$.

Tamaño de un conjunto

Sea A un conjunto. Si A tiene exactamente n elementos distintos, donde $n \in \mathbb{N}$, decimos que A es un **conjunto finito** y n es la **cardinalidad** de A. La cardinalidad de A es denotada por $|A|$.

Un conjunto A es **infinito** cuando no es finito.

Producto cartesiano:

El **producto cartesiano** de dos conjuntos A y B es el conjunto $A \times B$ definido por:

$$A \times B = \{(a, b) \,/\, a \in A \quad \wedge \quad b \in B\}.$$

Cuando $A = B$ se tiene el producto cartesiano $A^2 = A \times A$. El subconjunto $\Delta \subset A \times A$ definido por:

$$\Delta = \{(a, a) \,/\, a \in A\}$$

es llamado **diagonal** de A^2.

El **producto cartesiano** de los conjuntos $A_1, A_2, \ldots, A_n$ denotado por $A_1 \times A_2 \times \ldots \times A_n$, es definido por:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \,/\, a_i \in A_i \quad \text{para} \quad i = 1, 2, \ldots, n\}.$$

Tabla de contenidos

Un subconjunto R del producto cartesiano $A \times B$ es llamado **una relación** del conjunto A en el conjunto B. Es decir, los elementos de R son pares ordenados (a, b) donde el primer elemento $a \in A$ y el segundo elemento $b \in B$.

Ejemplo 1:
Sea $A = \{a, b, c, d, e\}$ y $B = \{0, 1, 2, 3, 4\}$ entonces:

$$A \times B = \left\{ \begin{array}{l} (a,0),(a,1),(a,2),(a,3),(a,4), \\ (b,0),(b,1),(b,2),(b,3),(b,4), \\ (c,0),(c,1),(c,2),(c,3),(c,4), \\ (d,0),(d,1),(d,2),(d,3),(d,4), \\ (e,0),(e,1),(e,2),(e,3),(e,4) \end{array} \right\}$$

$R = \{(a,0),(a,1),(a,3),(b,1),(b,2),(c,0),(c,3)\} \subset A \times B$, así R es una relación de A en B.

El ejemplo anterior ilustra que una relación R no contiene un par (x, y) para todo elemento de $x \in A$.

Una relación de A en sí mismo es llamado **una relación** en A.

Un par ordenado $(a, b) \in R$ es denotado por aRb.

Ejemplo 2: Del Ejemplo 1, calcule los pares (a, b) de la relación R sobre A donde $aRb \Leftrightarrow a \leq b$.

$$R = \left\{ \begin{array}{l} (0,0),(0,1),(0,2),(0,3), \\ (1,1),(1,2),(1,3), \\ (2,2),(2,3),(3,3) \end{array} \right\}$$

Definition 8

Si R es una relación de A en B y S una relación de B en C, la **composición** *de R con S denotada por $R \circ S$ es una relación de A en C definida por:*

$$R \circ S = \{(x, y) \,/\, \exists z \in B \quad \text{tal que} \quad (x, z) \in R \quad y \quad (y, z) \in S\}.$$

Definition 9 (Relación inversa R^{-1}.)

Sea R una relación de A en B. Definimos la relación inversa R^{-1} de B en A como sigue: $R^{-1} = \{(b, a) \in B \times A \,/\, (a, b) \in R\}$.
De forma equivalente:

$$\text{para todo} \quad a \in A \quad y \quad b \in B : (b, a) \in R^{-1} \Leftrightarrow (a, b) \in R.$$

Sea R una relación sobre un conjunto A.

Definition 10

R es llamada **Reflexiva** *si y sólo si para todo $a \in A$: aRa.*

Definition 11

R es llamada **Simétrica** *si y sólo si para todo $a, b \in A$: si aRb entonces bRa.*

Definition 12

R es llamada **Transitiva** *si y sólo si para todo $a, b, c \in A$: Si aRb y bRc entonces aRc.*

Definition 13

R es llamada **Antisimétrica** *si y sólo si para todo $a, b \in A$: Si aRb y bRa entonces aRb.*

Ejemplo:

Defina una relación R sobre $\mathbb{R}$ como sigue: para todo número real a, b :

$$aRb \quad \Leftarrow \quad a = b.$$

¿R es reflexiva?. ¿R es simétrica?. ¿R es transitiva?.

Ejemplo:

Defina una relación T sobre $\mathbb{Z}$ como sigue: Para todos los enteros $m, n \in \mathbb{Z}$:

$$mTn \quad \Leftrightarrow \quad 3|(m-n).$$

Esta relación es llamada **congruencia módulo 3**.
¿T es reflexiva?. ¿T es simétrica?. ¿T es transitiva?.

Tabla de contenidos

Función:

Una función f de un conjunto X hacia un conjunto Y denotado por $f : X \to Y$, es una relación de X en Y que satisface dos propiedades:

1. Todo elemento en X está relacionado con algún elemento de Y.
2. Ningún elemento en X está relacionado con más de un elemento de Y.

Es decir, cualquier elemento $x \in X$ está relacionado con un único elemento $y \in Y$ por la relación f y decimos que f envía x hacia y o que f mapea x en y y se denota $f : x \to y$. El único elemento $y \in Y$ para el cual f envía x es denotado por $f(x)$, es decir: $y = f(x)$.

Definiciones:

Sea f una función de X en Y.

1. El conjunto X es llamado el **dominio** de f.
2. El conjunto de valores de f es llamado el **rango** de f o la **imagen** de X bajo f, es denotado por:
$$\text{rango de } f = \{y \in Y \,/\, y = f(x) \quad \text{para algún} \quad x \in X\}.$$
3. Dado un elemento $y \in Y$, pueden existir elementos $x \in X$ tal que y es su imagen, es decir $f(x) = y$, entonces x es llamado una **preimagen** de y o una **imagen inversa** de y. El conjunto de todas las imágenes inversas de y es llamado **la imagen inversa** de y, es decir:
$$\text{la imagen inversa de} \quad y = \{x \in X \,/\, f(x) = y\}.$$

Definiciones:

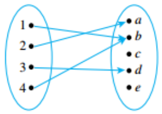
Sea $f : X \to Y$ una función, $A \subset X$ y $C \subset Y$, entonces:

1. La **imagen** de A se define por:
$$f(A) = \{y \in Y \,/\, y = f(x) \quad \text{para algún} \quad x \in A\}.$$
2. La **imagen inversa** de C se define por:
$$f^{-1}(C) = \{x \in X \,/\, f(x) \in C\}.$$

Ejemplo:

The Action of a Function on Subsets of a Set

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$, and define $F: X \to Y$ by the following arrow diagram:



Let $A = \{1, 4\}$, $C = \{a, b\}$, and $D = \{c, e\}$. Find $F(A)$, $F(X)$, $F^{-1}(C)$, and $F^{-1}(D)$.

Solution

$$F(A) = \{b\} \quad F(X) = \{a, b, d\} \quad F^{-1}(C) = \{1, 2, 4\} \quad F^{-1}(D) = \varnothing$$

Propiedades:

Dada una función $f : A \to B$.

Para las **imágenes**:
Sean X e Y subconjuntos de A. Se cumplen:

1. $f(X \cup Y) = f(X) \cup f(Y)$.
2. $f(X \cap Y) \subset f(X) \cap f(Y)$.
3. Si $X \subset Y$ entonces $f(X) \subset f(Y)$.
4. $f(\emptyset) = \emptyset$.

Para las **imágenes inversas o pre-imágenes**:
Sean Y y Z subconjuntos de B. Se cumplen:

1. $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$.
2. $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$.
3. $f^{-1}(Y^c) = (f^{-1}(Y))^c$.
4. Si $Y \subset Z$ entonces $f^{-1}(Y) \subset f^{-1}(Z)$.
5. $f^{-1}(B) = A$.
6. $f^{-1}(\emptyset) = \emptyset$.

Sea $f : X \to Y$ una función.

Definition 14 (Función inyectiva)
*f es llamada **inyectiva** cuando para cualesquiera $x, y \in X$ tal que $f(x) = f(y)$ implica que $x = y$.*

Definition 15 (Función sobreyectiva)
*f es llamada **sobreyectiva** cuando para todo $y \in Y$ existe por lo menos un $x \in X$ tal que $f(x) = y$.*

Definition 16 (Función biyectiva)
*f es llamada **biyectiva** cuando es **inyectiva** y **sobreyectiva**.*

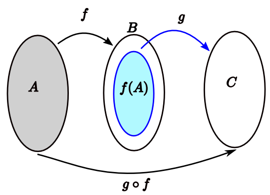
Ejemplo:

Sean A, B conjuntos. Definimos $\mathcal{F}(A, B) = \{f : A \to B \,/\, f \quad \text{es una función}\}$. Sean A, B, C, D conjuntos. Suponga que existe funciones biyectivas $f : A \to C$ y $g : B \to D$, entonces demuestre que existe una función biyectiva entre $\mathcal{F}(A, B)$ y $\mathcal{F}(C, D)$.

Composición de funciones

Sean $f : A \to B$ y $g : B \to C$ funciones tales que el **dominio** de g es igual al **rango** (o contradominio) de f. Definimos la **función compuesta** $g \circ f : A \to C$ que consiste en evaluar primero f y luego aplicar g, es decir:

$$(g \circ f)(x) := g(f(x)) \quad \text{para todo} \quad x \in A.$$



Propiedades:

Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones tales que está bien definido la composición de funciones. Se cumple:

1. La composición de funciones es asociativa, es decir: $(h \circ g) \circ f = h \circ (g \circ f)$.
2. Si f y g son funciones inyectivas entonces $g \circ f$ es inyectiva.
3. Si f y g son funciones sobreyectivas entonces $g \circ f$ es sobreyectiva.
4. La composición de dos biyecciones es otra biyección.

Sean $f : A \to B$, $g : B \to A$ funciones ($dom(g) = B$).

Definition 17 (Función Inversa a derecha)

Si $g \circ f = id_A : A \to A$, es decir, $(g \circ f)(x) = g(f(x)) = x$ para todo $x \in A$, entonces g es llamada ***inversa a izquierda*** *de f.*

Definition 18 (Función Inversa a izquierda)

Si $f \circ g = id_B : B \to B$, es decir, $(f \circ g)(y) = f(g(y)) = y$ para todo $y \in B$, entonces g es llamada ***inversa a derecha*** *de f.*

Definition 19 (Función inversa)

Si $g \circ f = id_A$ y $f \circ g = id_B$ (es decir, g es inversa a izquierda y a derecha de f), entonces g es llamada ***función inversa*** *de f y es denotada por $f^{-1} := g$.*

Ejemplo:

Sea $\mathbb{N} = \{1, 2, 3, \ldots\}$ el conjunto de los números naturales. Definamos $s : \mathbb{N} \to \mathbb{N}$ como $s(n) = n + 1$, la cual es llamada **función shift**. Demuestre que s no tiene inversa a la derecha pero tiene infinitas funciones inversas a la izquierda.

Solución:

- Por contradicción: Suponga que s admite una inversa a derecha " r ". Luego: $s(r(1)) = 1$ entonces $1 + r(1) = 1$ esto es $r(1) = 0 \notin \mathbb{N}$. Entonces s no admite inversa a derecha.
- Defina l sobre el conjunto $\{2, 3, \ldots, \} \subset \mathbb{N}$ del modo siguiente: $l(n) = n - 1$. Esto permite crear una infinidad de funciones $\{l_i\}$ y cada uno de ellos cumple $l_i(s(n)) = (n + 1) - 1 = n$ para todo $n \in \{2, 3, \ldots\}$. Así l_i es una inversa a izquierda de s para todo $i = 2, 3, \ldots$.

Propiedades:

1. Una función $f : A \to B$ posee inversa a izquierda si y solamente si f es inyectiva.
2. Una función $f : A \to B$ posee inversa a derecha si y solamente si f es sobreyectiva.
3. Una función $f : A \to B$ tiene inversa si y sólo si es una biyección.
4. Cuando existe la función inversa, ésta es única.
5. Si $f : A \to B$ y $g : B \to A$ son biyecciones, entonces es claro que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Relación de Equivalencia y Orden

Ronald Mas,
Angel Ramirez

2 de junio de 2021

Contenido

Relación de equivalencia

Dado el conjunto $A \neq \emptyset$. Una relación $\sim$ definida sobre A decimos que es una **relación de equivalencia** si cumple las siguientes propiedades:

i) Reflexiva
Si para todo $a \in A$ se tiene $(a, a) \in \sim$.

ii) Simétrica
Si $(a, b) \in \sim$ entonces $(b, a) \in \sim$.

iii) Transitiva
Si $(a, b) \in \sim$ y $(b, c) \in \sim$ entonces $(a, c) \in \sim$.

Notaciones:

- Escribimos $a \sim b$ en vez de $(a, b) \in \sim$.
- Usamos $R, \sim, \equiv, etc$ para denotar a un relación de equivalencia.

Relación de equivalencia

Dado el conjunto $A \neq \emptyset$. Una relación $\sim$ definida sobre A decimos que es una **relación de equivalencia** si cumple las siguientes propiedades:

i) Reflexiva
Si para todo $a \in A$ se tiene $(a, a) \in \sim$.

ii) Simétrica
Si $(a, b) \in \sim$ entonces $(b, a) \in \sim$.

iii) Transitiva
Si $(a, b) \in \sim$ y $(b, c) \in \sim$ entonces $(a, c) \in \sim$.

Notaciones:

- Escribimos $a \sim b$ en vez de $(a, b) \in \sim$.
- Usamos $R, \sim, \equiv, etc$ para denotar a un relación de equivalencia.

Relación de equivalencia

Dado el conjunto $A \neq \emptyset$. Una relación $\sim$ definida sobre A decimos que es una **relación de equivalencia** si cumple las siguientes propiedades:

i) Reflexiva
Si para todo $a \in A$ se tiene $(a, a) \in \sim$.

ii) Simétrica
Si $(a, b) \in \sim$ entonces $(b, a) \in \sim$.

iii) Transitiva
Si $(a, b) \in \sim$ y $(b, c) \in \sim$ entonces $(a, c) \in \sim$.

Notaciones:

- Escribimos $a \sim b$ en vez de $(a, b) \in \sim$.
- Usamos $R, \sim, \equiv, etc$ para denotar a un relación de equivalencia.

Ejemplo 1

Para $A = \mathbb{Z}$ se define la relación $\sim$ sobre A como:

$$x \sim y \leftrightarrow x + y \text{ es un número par.}$$

En efecto:

- Reflexiva: $x + x = 2x$, para todo $x \in \mathbb{Z}$. ✓
- Simétrica: Si $x + y = 2k$ para algún $k \in \mathbb{Z}$ entonces $y + x = 2k$ para algún $k \in \mathbb{Z}$. ✓
- Transitiva: Si $x + y = 2k$ y $y + z = 2r$ para algunos $k, r \in \mathbb{Z}$ entonces $x + z = 2k + 2r - 2y$ es par.✓

Por tanto $\sim$ es una relación de equivalencia.

Ejemplo 1

Para $A = \mathbb{Z}$ se define la relación $\sim$ sobre A como:

$$x \sim y \leftrightarrow x + y \text{ es un número par.}$$

En efecto:

- Reflexiva: $x + x = 2x$, para todo $x \in \mathbb{Z}$. ✓
- Simétrica: Si $x + y = 2k$ para algún $k \in \mathbb{Z}$ entonces $y + x = 2k$ para algún $k \in \mathbb{Z}$. ✓
- Transitiva: Si $x + y = 2k$ y $y + z = 2r$ para algunos $k, r \in \mathbb{Z}$ entonces $x + z = 2k + 2r - 2y$ es par.✓

Por tanto $\sim$ es una relación de equivalencia.

Ejemplo 2

Para $A = M_{2\times2}(\mathbb{Z})$ se define la relación $\sim$ sobre A como:

$$A \sim B \leftrightarrow det(A - B) = 0$$

En efecto

- Reflexiva: $det(A - A) = 0$, para todo $A \in M_{2\times2}(\mathbb{Z})$.✓
- Simétrica: Si $det(A - B) = 0$ entonces $det(B - A) = (-1)^2.det(A - B) = 0$.✓
- Transitiva: Si $det(A - B) = 0$ y $det(B - C) = 0$ entonces $det(A - C) = 0$. ×
Considera: $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix}$ y $C = \begin{bmatrix} 7 & 8 \\ 5 & 9 \end{bmatrix}$.

Por tanto $\sim$ no es una relación de equivalencia.

Ejemplo 2

Para $A = M_{2\times2}(\mathbb{Z})$ se define la relación $\sim$ sobre A como:

$$A \sim B \leftrightarrow det(A - B) = 0$$

En efecto

- Reflexiva: $det(A - A) = 0$, para todo $A \in M_{2\times2}(\mathbb{Z})$.✓
- Simétrica: Si $det(A - B) = 0$ entonces $det(B - A) = (-1)^2.det(A - B) = 0$.✓
- Transitiva: Si $det(A - B) = 0$ y $det(B - C) = 0$ entonces $det(A - C) = 0$. ×
Considera: $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix}$ y $C = \begin{bmatrix} 7 & 8 \\ 5 & 9 \end{bmatrix}$.

Por tanto $\sim$ no es una relación de equivalencia.

Clase de equivalencia y conjunto cociente

Definición

Sea R una relación de equivalencia definida sobre el conjunto $A \neq \emptyset$, definamos la clase de equivalencia de $a \in A$ como:

$$R[a] = \{b \in A : bRa\}.$$

Definición

Sea R una relación de equivalencia definida sobre el conjunto $A \neq \emptyset$, definamos el conjunto cociente

$$\frac{A}{R} = \{R[a] : a \in A\}$$

Observaciones:

- Usamos $R[x], [x], \overline{x}, etc$ para denotar la clase de equivalencia de x.
- La relación de equivalencia tiene la propiedad de particionar el conjunto A.

Clase de equivalencia y conjunto cociente

Definición

Sea R una relación de equivalencia definida sobre el conjunto $A \neq \emptyset$, definamos la clase de equivalencia de $a \in A$ como:

$$R[a] = \{b \in A : bRa\}.$$

Definición

Sea R una relación de equivalencia definida sobre el conjunto $A \neq \emptyset$, definamos el conjunto cociente

$$\frac{A}{R} = \{R[a] : a \in A\}$$

Observaciones:

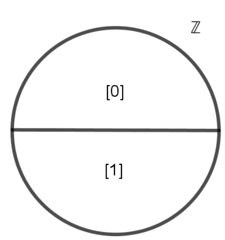
- Usamos $R[x], [x], \overline{x}, etc$ para denotar la clase de equivalencia de x.
- La relación de equivalencia tiene la propiedad de particionar el conjunto A.

Ejemplo

Ejemplo: Del ejemplo 1) se tiene que:

- $[0] = [\pm 2] = [\pm 4] = \cdots$
- $[\pm 1] = [\pm 3] = [\pm 5] = \cdots$

Luego se tiene: $\frac{\mathbb{Z}}{\sim} = \{[0], [1]\}$
Es decir se tiene:



Propiedades

Para toda relación R en X con $X \neq \emptyset$, se tiene:

1) $R[x] \neq \emptyset$, para todo $x \in X$.
2) Para todo par de elementos $x, y \in X$ se cumple:

$$R[x] = R[y] \text{ o } R[x] \cap R[y] = \emptyset.$$

3) Si R y S son relaciones de equivalencia sobre X y $R[x] = S[x], \forall x \in X$ entonces $R = S$.

Prueba:

1) Como R es reflexiva se tiene que $x \in R[x]$, $\forall x \in X$, luego $R[x]$ es no nulo.

Continua Prueba:

2) Sean $x, y \in X$ se presenta dos casos:
   a) Si $x\,R\,y$, entonces veamos que $R[x] \subseteq R[y]$. Sea $z \in R[x]$ entonces $x\,R\,z$, por ser R simétrica $z\,R\,x$, luego por ser R transistiva $z\,R\,y$, de donde se concluye que $z \in R[y]$. La otra inclusión es similar.
   b) Si x no esta relacionado con y, supomgamos que $R[x] \cap R[y] \neq \emptyset$ entonces existe $z \in X$ tal que $x\,R\,z$ y $y\,R\,z$, luego por ser R simétrica y transitiva se tiene $x\,R\,y$ lo cual es una contradicción.
3) Sea $(x, y) \in R$ entonces $y \in R[x] = S[x]$ entonces $(x, y) \in S$. La otra inclusión es similar.

Relación de orden parcial

Dado el conjunto $A \neq \emptyset$ y una relación $\preceq$ definida sobre A. Decimos que $\preceq$ es una **relación de orden parcial** si cumple las siguientes propiedades:

i) Reflexiva
   Si para todo $a \in A$ se tiene $(a, a) \in \preceq$.
ii) Antisimétrica
   Si $(a, b) \in \preceq$ y $(b, a) \in \preceq$ entonces $a = b$.
iii) Transitiva
   Si $(a, b) \in \preceq$ y $(b, c) \in \preceq$ entonces $(a, c) \in \preceq$.

Notaciones:

- Escribimos $a \preceq b$ en vez de $(a, b) \in \preceq$.
- Usamos las letras $R, \preceq, \prec, etc$ para denotar a un relación de orden.

Relación de orden parcial

Dado el conjunto $A \neq \emptyset$ y una relación $\preceq$ definida sobre A. Decimos que $\preceq$ es una **relación de orden parcial** si cumple las siguientes propiedades:

i) Reflexiva
   Si para todo $a \in A$ se tiene $(a, a) \in \preceq$.
ii) Antisimétrica
   Si $(a, b) \in \preceq$ y $(b, a) \in \preceq$ entonces $a = b$.
iii) Transitiva
   Si $(a, b) \in \preceq$ y $(b, c) \in \preceq$ entonces $(a, c) \in \preceq$.

Notaciones:

- Escribimos $a \preceq b$ en vez de $(a, b) \in \preceq$.
- Usamos las letras $R, \preceq, \prec, etc$ para denotar a un relación de orden.

Relación de orden total o lineal

Decimos que $\preceq$ es una **relación de orden total o lineal** si cumple:

i) $\preceq$ es una relación de orden parcial.
ii) Para todo $a, b \in A$ se tiene que $(a, b) \in \preceq$ o $(b, a) \in \preceq$

Observación:

- Los elementos de A que cumplan la propiedad $ii)$ se denominan **elementos comparables** caso contrario serán elementos no comparables.

Definición

Sea $(X, \preceq)$ un conjunto ordenado, decimos que un elemento $x \in X$ es un predecesor inmediato del elemento $y \in X$ si:

- *$x \prec y$.*
- *No existe $t \in X$ tal que $x \prec t \prec y$.*

Denotamos la relación de un predecesor inmediato como $\lhd$.

Relación de orden total o lineal

Decimos que $\preceq$ es una **relación de orden total o lineal** si cumple:

i) $\preceq$ es una relación de orden parcial.
ii) Para todo $a, b \in A$ se tiene que $(a, b) \in \preceq$ o $(b, a) \in \preceq$

Observación:

- Los elementos de A que cumplan la propiedad $ii)$ se denominan **elementos comparables** caso contrario serán elementos no comparables.

Definición

Sea $(X, \preceq)$ un conjunto ordenado, decimos que un elemento $x \in X$ es un predecesor inmediato del elemento $y \in X$ si:

- *$x \prec y$.*
- *No existe $t \in X$ tal que $x \prec t \prec y$.*

Denotamos la relación de un predecesor inmediato como $\lhd$.

Proposición

Sea $(X, \preceq)$ un conjunto ordenado finito. Entonces para todo $x, y \in X$, se tiene que $x \prec y$ si y sólo si existen elementos $\{x_i\}_{i=1}^{k} \subset X$ tal que

$$x \lhd x_1 \lhd \cdots \lhd x_k \lhd y$$

Demostración.

Para $k = 0$ se tiene que $x \lhd y$.
La ida queda como tarea, veamos la vuelta:
Si $x \lhd x_1 \lhd \cdots \lhd x_k \lhd y$ entonces $x \preceq x_1 \preceq \cdots \preceq x_k \preceq y$ y por la transitividad de $\preceq$ se tiene que $x \preceq y$. □

Ejemplo

Para $A = \mathbb{N}$ definamos la relación $|$ sobre A como:

$$a|b \leftrightarrow \text{existe } k \in \mathbb{N} \text{ tal que } b = ak.$$

- Reflexiva: $a|a$, $\forall a \in A$.✓
- Antisimétrica: Si $a|b$ y $b|a$ entonces existen $r, s \in \mathbb{N}$ tal que $b = ra$ y $a = sb$, luego $sb = a = sra$. Al simplificar a se tiene $sr = 1$ lo que implica que $s = r = 1$, por tanto $a = b$.✓
- Transitiva: Si $a|b$ y $b|c$ entonces existen $r, s \in \mathbb{N}$ tal que $b = ra$ y $c = sb$, luego $c = sra$, por tanto $a|c$.✓

Decimos que $|$ es una relación de orden parcial pero no total ya que existen elementos no comparables como por ejemplo 2 y 3.

Ordenamientos parcial y lineal

Ronald Mas
Angel Ramirez

12 de junio de 2020

Contenido

Elementos minimales y maximales

Definición

Sea $(X, \preceq)$ un conjunto ordenado.

1) Un elemento $a \in X$ se dice que es elemento minimal de $(X, \preceq)$ si no existe $x \in X$ tal que $x \prec a$.
2) Un elemento $a \in X$ se dice que es elemento maximal de $(X, \preceq)$ si no existe $x \in X$ tal que $x \succ a$.

Definición

Sea $(X, \preceq)$ un conjunto ordenado.

1) Un elemento $a \in X$ se dice que es el elemento mínimo de $(X, \preceq)$ si $a \preceq x$, $\forall x \in X$.
2) Un elemento $a \in X$ se dice que es el elemento máximo de $(X, \preceq)$ si $x \preceq a$, $\forall x \in X$.

Diagrama de Hasse

Es una representación gráfica simplificada de un conjunto ordenado finito.
Ejemplo: En el Ejemplo 1) el elemento minimal y maximal coinciden con el elemento mínimo y máximo respectivamente. En el ejemplo 2) el elemento minimal coincide con el elemento mínimo y no posee elemento máximo.

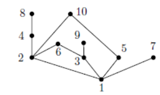
1) Diagrama de Hasse del conjunto linealmente ordenado

$$(A, \leq) = (\{1, 2, \cdots, 7\}, \leq):$$

Elemento minimal:1
Elemento maximal:7

2) Diagrama de Hasse del conjunto parcialmente ordenado

$$(B, |) = (\{1, 2, \cdots, 10\}, |):$$

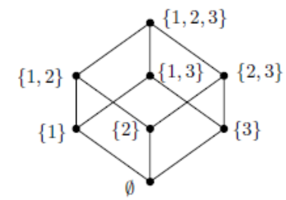


Elemento minimal:1
Elemento maximales:6,7,8,9,10

Más ejemplos

3) Diagrama de Hasse del conjunto parcialmente ordenado

$$(C, \subseteq) = (\{1, 2, 3\}, \subseteq)$$



Elemento minimal:$\emptyset$
Elemento maximal: $\{1, 2, 3\}$

Teorema

Todo conjunto parcialmente ordenado $(X, \preceq)$ posee al menos un elemento minimal.

Prueba:
Sea $x_0 \in X$. Si x_0 es minimal no hay nada que probar, caso contrario existe $x_1 \prec x_0$, luego si x_1 es minimal no hay nada que probar, caso contrario existe $x_2 \prec x_1$. Luego como X es finito, al proceder una cantidad finita de veces se tiene el resultado deseado.

Teorema

Sea $(X, \preceq)$ un conjunto finito parcialmente ordenado. Entonces existe un ordenamiento lineal $\leq$ en X tal que $x \preceq y$ implica que $x \leq y$.

Ordenamiento por inclusión

Definición

Sean $(X, \preceq)$ y $(X', \preceq')$ dos conjuntos ordenados. Una aplicación $f : X \to X'$ es llamada un **encaje** de $(X, \preceq)$ en $(X', \preceq')$ si cumple las siguientes propiedades:

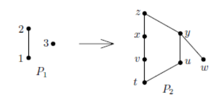
1) f es una aplicación inyectiva.
2) $f(x) \preceq' f(y)$ si y sólo si $x \preceq y$.

Observaciones:

- Si f es un encaje y también sobreyectiva entonces f e un isomorfismo.
- Un encaje f significa que una parte de $(X', \preceq')$, es decir la parte $\{f(x) : x \in X\}$ se parece a $(X, \preceq)$.

Ejemplo

Ejemplo: Sean los siguientes diagramas de Hasse de dos conjuntos ordenados.



Son ejemplos de encajes:

$$\begin{array}{cccc} f: & P_1 & \to & P_2 \\ & 1 & \mapsto & v \\ & 2 & \mapsto & x \\ & 3 & \mapsto & y \\ f': & P_1 & \to & P_2 \\ & 1 & \mapsto & t \\ & 2 & \mapsto & x \\ & 3 & \mapsto & w \end{array}$$

No son ejemplos de encajes:

$$\begin{array}{cccc} g: & P_1 & \to & P_2 \\ & 1 & \mapsto & t \\ & 2 & \mapsto & v \\ & 3 & \mapsto & y \\ g' & P_1 & \to & P_2 \\ & 1 & \mapsto & x \\ & 2 & \mapsto & w \\ & 3 & \mapsto & u \end{array}$$

Teorema

Para todo conjunto ordenado $(X, \preceq)$ existe un encaje en $(2^X, \subseteq)$.

Prueba:
Definamos:

$$\begin{array}{cccc} f: & X & \to & 2^X \\ & x & \mapsto & f(x) = \{y \in X : y \preceq x\}. \end{array}$$

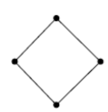
Veamos que f es un encaje

1) Si $f(x) = f(y)$, entonces por ser $\preceq$ reflexiva se tiene que $x \in f(x)$ y $y \in f(Y)$, luego $x \preceq y$ y $y \preceq x$ y por ser $\preceq$ antisimétrica se tiene $x = y$. Por tanto f es inyectiva.
2)
   - Veamos que, si $x \preceq y$ entonces $f(x) \subseteq f(y)$:
     Sea $z \in f(x)$ entonces $z \preceq x$ y por transitividad de $\preceq$ se tiene que $z \preceq y$, luego $z \in f(y)$.
   - Veamos que, si $f(x) \subseteq f(y)$ entonces $x \preceq y$:
     Como $f(x) \subseteq f(y)$ entonces $x \in f(y)$ y por tanto $x \preceq y$.

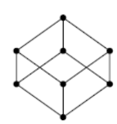
Diagrama de Hasse de $(2^X, \subseteq)$

En particular, para $X = \{1, 2, ..., n\}$ el conjunto ordenado $(2^X, \subseteq)$ se denotan por B_n. Veamos los diagramas de Hasse de B_1, B_2, B_3.

B_1



B_2



B_3

Una aplicación de adicionar propiedades a dichos conjuntos es el estudio del Álgebra de Boole.

Independencia sobre un conjunto ordenado

En adelante usemos P para denotar un conjunto finito parcialmente ordenado $(X, \preceq)$.

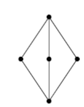
Definición

Un conjunto $A \subseteq X$ es llamado **independiente** en P si cualquier par de elementos distintos de A son incomparables.

Denotamos:

$$\alpha(P) = max\{|A| : A \text{ es indenpendiente en } P\}.$$

Ejemplo: Para los conjuntos parcialmente ordenados



P_1

P_2

se tiene que $\alpha(P_1) = 3$ y $\alpha(P_2) = 4$.

Definición

Un conjunto $A \subseteq X$ es llamado una cadena en P si cualquier par de elementos son comparables.

Denotamos:

$$w(P) = max\{k \in \mathbb{Z}_{\geq 0} : \ k = \text{número de elementos de la cadena P}\}$$

Ejemplo: Para los conjuntos parcialmente ordenados del ejemplo anterior se tiene que $w(P_1) = 3$ y $w(P_2) = 2$.

Teorema

Para conjunto finito ordenado $P = (X, \preceq)$ se cumple que:

$$\alpha(P) \cdot w(P) \geq |X|.$$

CONTEO COMBINATORIO - PERMUTACIONES - COMBINACIONES.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

10 de junio de 2020

Tabla de contenidos

Proposición 1

Sea N un conjunto de n elementos (pudiendo ser vacío, es decir, $n = 0$) y sea M un conjunto de m elementos ($m \geq 1$). Entonces, el número de todas las posibles funciones $f : N \to M$ es m^n.

Demostración:

- Caso $n = 0$:
  En este caso $f : N \to M$ donde $N = \emptyset$. Por definición de función, f debe ser un conjunto de pares ordenados $(x, y) \in N \times M$ tal que $x \in N$ e $y \in M$. Desde que $N = \emptyset$ entonces f no puede posiblemente contener elementos y por tanto la única posibilidad es que f sea vacío.
  Por otra parte, $f = \emptyset$ satisface la definición de función, la cual dice que para cada $x \in N$ algo debe ser verdad, pero no existen $x \in N$, entonces, existe exactamente 1 función $f : \emptyset \to M$.
  Esto prueba la fórmula $m^n = 1$ para $n = 0$ y cualquier $m \geq 1$.

- Caso $n \in \mathbb{N}$:
  - Para $n = 1$: como existen m valores distintos en el conjunto de llegada, entonces exactamente hay m funciones. Así se cumple $m^n = m$ para $n = 1$ y todo $m \geq 1$.
  - Hipótesis inductiva: Dado $n_0 \in \mathbb{N}$, existen m^n funciones cuando N tiene n elementos y M tiene m elementos para todo $n \leq n_0$.
  - Veamos que se cumple para $n_0 + 1$.
    Elijamos $a \in N$ arbitrario y lo mantenemos fijo. Considere la función $f : N \to M$ tal que $f(a) \in M$ y la función $f' : N \backslash \{a\} \to M$. Dado $a \in N$ fijo, existen m formas distintas de elegir $f(a) \in M$. Para elegir f', tenemos que $N \backslash \{a\}$ tiene n_0 elementos y M tiene m elementos, entonces por la hipótesis inductiva existen m^{n_0} funciones $f' : N \backslash \{a\} \to M$. Como cada elección de $f(a)$ puede ser combinada con cualquier de f' entonces el número total de posibilidades para f es igual a $m \times m^{n_0} = m^{n_0+1}$.

Proposición 2

Cualquier conjunto de $n \in \mathbb{N} \cup \{0\}$ elementos tiene 2^n subconjuntos.

Demostración:
Analizamos por caso:

- Para $|X| = 0$: Entonces $|X| = \emptyset$ y así existe un único subconjunto $\emptyset$ y así $2^{|X|} = 1$.
- Para $|X| \in \mathbb{N}$ procedemos por inducción sobre $|X|$.
  1. Para $|X| = 1$ entonces existen dos subconjuntos, los cuales son $\emptyset$ y el propio X, por tanto se cumple $2^{|X|} = 2^1 = 2$.
  2. Hipótesis inductiva: dado $n \in \mathbb{N}$ tal que $|X| = n$ se cumple que el número de subconjuntos es 2^n.

3. Veamos que se cumple para conjuntos X tal que $|X| = n + 1$:
   Sea $a \in X$ un elemento fijo pero arbitrario. Ahora, dividamos los subconjuntos de X en dos familias $\mathcal{F}_1 = \{A \subset X \,/\, a \notin A\}$ y $\mathcal{F}_2 = \{A \subset X \,/\, a \in A\}$.

   Todo $A \in \mathcal{F}_1$ cumple que $A \subset X \backslash \{a\}$ y donde $|X \backslash \{a\}| = n$ y por la hipótesis inductiva se tienen 2^n subconjuntos.

   Para todo $A \in \mathcal{F}_2$ considere $A' = A \backslash \{a\} \subset X \backslash \{a\}$ y así $A' \in \mathcal{F}_1$. Viceversa, cada $A' \in \mathcal{F}_1$ se obtiene exactamente de un conjunto $A \in \mathcal{F}_2$ de la forma $A = A' \cup \{a\}$.

   Es decir, existe una biyección entre los elementos de $\mathcal{F}_1$ y $\mathcal{F}_2$, por tanto, el número de subconjuntos de $\mathcal{F}_2$ también es 2^n.

   Por tanto, el número total de subconjuntos es $2^n + 2^n = 2^{n+1}$.

Proposición 3

Sea $n \in \mathbb{N}$. Cada conjunto de n elementos tiene exactamente 2^{n-1} subconjuntos de tamaño impar y 2^{n-1} de tamaño par.

Demostración:
Considere $a \in X$ fijo pero arbitrario. Defina la siguiente función:

$$\begin{array}{rccl} F: & X \backslash \{a\} & \to & Y = \{A' \subset X \,/\, |A'| \ \text{es un número impar}\} \\ & A & \mapsto & F(A) := \begin{cases} A & \text{si} \ \ |A| \ \ \text{es impar} \\ A \cup \{a\} & \text{si} \ \ |A| \ \ \text{es par} \end{cases} \end{array}$$

Observe que F es un biyección y que $|X \backslash \{a\}| = n - 1$, luego, por la Proposición 2 se tiene que el número de subconjuntos de $X \backslash \{a\}$ es 2^{n-1} y debido a que F es biyectiva conluimos que $|Y| = 2^{n-1}$.
De forma análoga se procede para determinar el número de subconjuntos de cardinalidad par. O también se puede calcular como $|X| - |Y| = 2^n - 2^{n-1} = 2^{n-1}$.

Proposición 4

Dados $n, m \in \mathbb{N} \cup \{0\}$, existen $m(m-1)\ldots(m-n+1) = \prod_{i=0}^{n-1}(m-i)$ funciones inyectivas de un conjunto de n elementos a un conjunto de m elementos.

Demostración:

1. Para $n = 0$, la función vacía es inyectiva y así exactamente existe una función inyectiva, aceptando el hecho que el valor de un producto vacío es definido como 1.
2. Procedemos por inducción:
   a) Para $n = 1$ tenemos m funciones inyectivas.
   b) Observe que no existen funciones inyectivas cuando $n > m$ cumpliéndose la fórmula debido a que aparece el factor cero en el producto.

- Por tanto, consideremos un conjunto N con n elementos y $n \geq 1$ y un conjunto M con m elementos tal que $m \geq n$. Fijemos $a \in N$ y elijamos $f(a) \in M$ arbitrariamente, para esto tenemos m formas distintas. Resta elegir una función inyectiva del conjunto $N \backslash \{a\}$ hacia el conjunto $M \backslash \{f(a)\}$. Por la hipótesis inductiva, existen $(m-1)(m-2)\ldots(m-n+1)$ formas distintas de elecciones siguiente. Por tanto, tenemos $m(m-1)(m-2)\ldots(m-n+1)$ funciones inyectivas $f: N \to M$.

Tabla de contenidos

Definición 1

Sea X un conjunto finito. Una función **biyectiva** $f: X \to X$ *es llamada* **permutación**.

Ejemplo:
Sea $X = \{a, b, c, d\}$. Un ejemplo de permutación es $P: X \to X$ donde $P(a) = b, p(b) = d, p(c) = c, p(d) = a$. P es usual denotarse por:

$$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$$

Es frecuente trabajar con permutaciones en $X = \{1, 2, 3, \ldots, n\}$. Con la convención que la primera fila esté en orden creciente, luego podemos considerar la notación:

$$P = \begin{pmatrix} 2 & 3 & 4 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Según la Proposición 8 el número de permutaciones de n elementos es:

$$n(n-1)(n-2)\ldots 2 \times 1.$$

$$n! = n(n-1)(n-2)\ldots 2 \times 1.$$

En particular para $n = 0$ se define $0! = 1$.

De forma equivalente, una **permutación** de un conjunto de objetos distintos es un **arreglo ordenado** de estos objetos. También estamos interesados en arreglos ordenados de algunos de los elementos de un conjunto. Un arreglo ordenado de r elementos de un conjunto es llamada una **r-permutación**.

Ejemplo:

Sea $S = \{a, b, c\}$. El arreglo ordenado c, a, b es una permutación de S. El arreglo ordenado c, b es una 2-permutación de S.

Todas las 2-permutaciones de S son los arreglos ordenados $\{a, b\}, \{a, c\}, \{b, a\}, \{b, c\}, \{c, a\}$ y $\{c, b\}$. Es decir, existen seis 2-permutaciones de este conjunto con 3 elementos.

Teorema 1

Si n es un entero positivo y r es un entero tal que $1 \leq r \leq n$, entonces existen

$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1)$$

r-permutaciones de un conjunto con n elementos distintos.

Demostración: Usaremos la regla del producto. El primer elemento de la permutación puede ser elegido en n forma distintas porque el conjunto tiene n elementos. Del mismo modo, existen $n-1$ formas distintas de elegir el segundo elemento de la permutación, porque existen $n-1$ elementos en el conjunto después de haber elegido el primero. Similarmente, existen $n-2$ formas para elegir el tercer elemento y así sucesivamente, hasta que quedan exactamente $n-(r-1) = n-r+1$ modos de elegir el $r-$ésimo elemento. Por

tanto, usando la regla del producto, se concluye que existen $n(n-1)(n-2)\ldots(n-r+1)$ $r-$permutaciones del conjunto.

Tabla de contenidos

Coeficientes binomiales

Definición 2

Sea $n \geq k$ enteros no negativos. Definimos el **coeficiente binomial** *al siguiente valor:*

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k(k-1)\ldots 2 \times 1} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}$$

Es mucho más conocida la fórmula: $\binom{n}{k} \frac{n!}{k!(n-k)!}$.

Entre las ventajas de la forma dada en la definición, se tiene:

- Computacional, realiza menos operaciones.
- Resultados intermedios más pequeños.
- Tiene sentido para todo $n \in \mathbb{R}$.
- Permite definir $\binom{n}{k}$ para $n < k$ en cuyo caso $\binom{n}{k} = 0$.

Definición 3

Sea X un conjunto y k un enterno no negativo. El símbolo $\binom{X}{k}$ denota el conjunto de todos los subconjuntos de k elementos de conjunto X.

Ejemplo:
Sea $X = \{a, b, c\}$ entonces: $\binom{X}{2} = \{\{a, b\}, \{b, c\}, \{a, c\}\}$.

Observación: El símbolo $\binom{X}{k}$ tiene dos significados, dependiendo si X es un número o un conjunto.

1. Si X es un número natural, entonces $\binom{X}{k}$ denota el número de todos los subconjuntos de k elementos de un conjunto de X elementos.
2. Si X es un conjunto, entonces $\binom{X}{k}$ denota el conjunto de todos los subconjuntos de k elementos del conjunto X.

Proposición 5

Para cualquier conjunto finito X, el número de todos los subconjuntos de k elementos es igual a $\binom{|X|}{k}$.

En símbolos:

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}$$

Demostración:
Sea $r = |X|$. Vamos a contar las $k-$ *tuplas* ordenadas de elementos de X(sin repeticiones de elementos) de dos formas distintas.

1. El número de las $k-$ tuplas ordenadas es $n(n-1)\ldots(n-k+1)$ (usando la Proposición 8).

2. De un subconjunto M de k elementos (es decir, $M \in \binom{X}{k}$), podemos crear $k!$ $k-$tuplas ordenadas distintas y cada $k-$tupla se obtiene de exactamente un subconjunto M de k elementos.

por tanto, de **(1)** y **(2)**:

$$n(n-1)\ldots(n-k+1) = k!\left|\binom{X}{k}\right|$$

Propiedades:

Teorema 2

Para todo $n \geq 1$ y $0 \leq k \leq n$ se cumple:

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

Teorema 3

Si n y k son números enteros no negativos tales que $0 \leq k \leq n$, entonces:

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

Demostración Teorema 3

Sea A un conjunto con n elementos y B un conjunto con un sólo elemento, por ejemplo $B = \{b\}$ tal que $b \notin A$, es decir, $A \cap B = \emptyset$. Por tanto, si $C = A \cup B$ se tiene que $|C| = n + 1$.

Sea P el conjunto formado por todos los subconjuntos de C con k elementos, es decir:

$$P = \{X \subset C \,/\, |X| = k\},$$

por tanto, se tienen dos opciones para los k elementos que forman X:

- Los k elementos de X son del conjunto A, es decir:

$$Q = \{X \subset A \,/\, |X| = k\}.$$

Demostración Teorema 3 (cont.)

- O también, $k-1$ son elementos de A y b es el elemento que falta, es decir:

$$R = \{X = D \cup B \,/\, , D \subset A, |D| = k-1\}.$$

Además $P = Q \cup R$ donde $Q \cap R = \emptyset$. Por tanto:

$$|P| = |R| + |Q|,$$

pero:

$$\begin{aligned} |P| &= \binom{n+1}{k} \\ |Q| &= \binom{n}{k} \\ |R| &= \binom{n}{k-1} \end{aligned}$$

de esta forma se obtiene:

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

Ejemplo clásico usando el coeficiente binomial

Sea m un entero no negativo. ¿Cuántas formas existen para expresar m como suma de r enteros no negativos? (el orden de los sumandos es importante).
Por ejemplo, para $m = 3$ y $r = 2$ se tienen las siguientes formas:

$$\begin{aligned} 3 &= 0 + 3 \\ &= 1 + 2 \\ &= 2 + 1 \\ &= 3 + 0 \end{aligned}$$

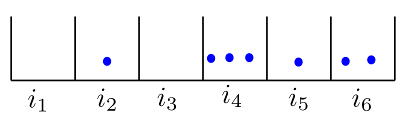
Mas explícitamente: queremos encontrar r sumandos $(i_1, i_2, \ldots, i_r)$ de enteros no negativos que satisfacen la ecuación:

$$i_1 + i_2 + \ldots + i_r = m. \qquad (1)$$

La respuesta a este problema es $\binom{m+r-1}{r-1}$.

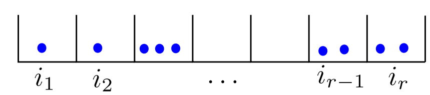
Solución:

Imaginemos cada sumando i_r como una caja, es decir, tenemos r cajas.
Queremos repartir m objetos en las r cajas (asumimos que cada caja puede guardar los m objetos de ser necesario.)
Observe que cada posible distribución da una solución a la Ecuación 1.
Para quedar mas claro, considere el siguiente ejemplo para $m = 7$y $r = 6$.
Una solución es $7 = 0 + 1 + 0 + 3 + 1 + 2$ y la distribución correspondiente es:

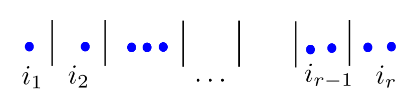


Solución (Cont.)

Por lo tanto, la solución buscada a la ecuación 1 es equivalente al número de distribuciones de los m objetos en las r cajas.
El gráfico para el caso general de una solución de la ecuación 1 es:



Para realizar el conteo de las soluciones de la ecuación 1 consideramos la siguiente figura:



Solución (Cont.)

Donde debemos tener en cuenta:

1. Cada $i_n\,(n = 1, \ldots, r)$ denota el número de posiciones a ser ocupadas por los objetos.
2. Cada barra de separación cuenta una posición más.
3. Entre las posiciones de los objetos y barras tenemos en total $m + r - 1$ posiciones.
4. Observe que cada distribución de las $r - 1$ barras separando los objetos nos da una solución para la ecuación 1.

Por tanto, elegir una distribución de los objetos significa seleccionar la posición de las barras de separación entre los objetos.
En otras palabras, tenemos en total $m + r - 1$ objetos (entre los objetos a repartir y las barras) arregladas en fila y queremos determinar cuales posiciones serán ocupadas por los objetos a repartirse y las barras. Esto corresponde a seleccionar un subconjunto de $r - 1$ posiciones de un total de $m + r - 1$

Ejemplo:

Contar el número de soluciones enteras a

$$x_1 + x_2 + x_3 + x_4 = 10, \quad x_1 \geq -2, x_2 \geq 0, x_3 \geq 0, x_4 \geq 0.$$

Ejemplo:

Contar el número de soluciones enteras a

$$x_1 + x_2 + x_3 + x_4 = 10, \quad x_1 \geq 3, x_2 \geq 0, x_3 \geq -4, x_4 \geq 0.$$

Ejemplo:

Un estudiante tiene que responder siete preguntas de cuestionario de 10. ¿de cuántas maneras puede hacer su elección si:

1. no hay restricciones?
2. debe responder a las dos primeras preguntas?
3. debe responder, como mínimo, a tres preguntas de las cinco primeras?

Solución:

Supongamos que las diez preguntas son:
$p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}$ y elegimos un grupo cualquiera de siete de ellas, por ejemplo: $p_1, p_3, p_5, p_7, p_8, p_9, p_{10}$. Es claro que si cambiamos el orden entre ellas el grupo elegido es el mismo, sin embargo si cambiamos alguna o algunas preguntas, el grupo es distinto, por tanto, los grupos de siete preguntas serán combinaciones de orden siete elegidas entre las 10 del cuestionario.

1. Al no haber ningún tipo de restricciones la elección podrá hacerse de:
$$\binom{10}{7} = 120$$
formas distintas.

Solución: (cont.)

2. Si el estudiante debe responder a las dos primeras preguntas, hallamos todos los grupos distintos de cinco preguntas que pueden elegirse entre las ocho restantes y a cada uno de ellos le añadimos las dos primeras. Por tanto, la elección puede hacerse de:
$$\binom{8}{5} = 56$$
formas distintas.

Solución: (cont.)

3. El estudiante debe responder como mínimo, a tres preguntas de entre las cinco primeras.
Hallamos todos los grupos distintos de k preguntas, con $k = 3, 4$ o 5 que pueden elegirse entre las cinco primeras y para cada uno de ellos elegimos $7 - k$ preguntas entre las cinco restantes. El número total de formas distintas de hacer la elección será, por tanto:
$$\sum_{k=3}^{5} \binom{5}{k}\binom{5}{7-k} = 110.$$

Teorema Binomial

Teorema 4

Para cualquier entero n no negativo se cumple:
$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

En particular, el teorema anterior para $x = 1$ resulta:
$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$$

COEFICIENTES BINOMIALES. ESTIMACIONES DE LA FUNCIÓN FACTORIAL

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

14 de junio de 2020

Tabla de contenidos

Teorema Binomial

Teorema 1

Para cualquier entero n no negativo se cumple:

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

En particular, el teorema anterior para $x = 1$ resulta:

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$$

Proposición 1

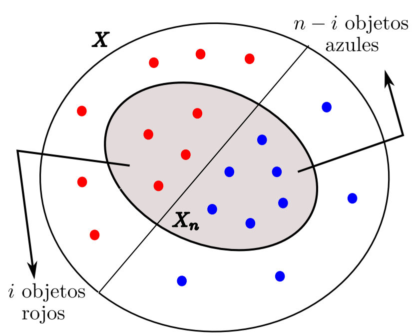
$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$$

Demostración:
Observe que:

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$$

y que esta suma representa el número de subconjuntos de n elementos de un conjunto que tiene $2n$ elementos (probando así la proposición).
Considere un conjunto X tal que $|X| = 2n$, de los cuales n elementos son de color rojo y los n restantes son de color azul. Para elegir un subconjunto $X_n \subset X$ de n elementos, ahora significa elegir

subconjuntos de i elementos de color rojo y subconjuntos de $n-i$ elementos de color azul, donde $i = 0, 1, \ldots, n$.



Para un i dado, existen $\binom{n}{i}$ posibilidades para elegir subconjuntos de objetos rojos, independientemente se tienen $\binom{n}{n-i}$ posibilidades para elegir subconjuntos de objetos azules. En total, el número de subconjuntos de n elementos de X pueden ser seleccionados de $\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$ modos distintos.

Ejemplo:
Calcule $\sum_{j=1}^{n} j\binom{n}{j} 3^{j-1}$.
Del Teorema Binomial tenemos:
$\frac{d}{dx}(1+x)^n = n(1+x)^{n-1} = \sum_{j=1}^{n} j\binom{n}{j} x^{j-1}$ y evaluando en $x = 3$
resulta:

$$\sum_{j=1}^{n} j\binom{n}{j} 3^{j-1} = n4^{n-1}.$$

Tabla de contenidos

¿Cómo ordenar elementos de un conjunto cuando uno de sus elementos se repite? Ejemplo: cara

Consideremos cara $\equiv$ cara para "*diferenciar*" las letras " **a** " una de la otra en la palabra " **cara**". Veamos ahora las formas **distintas** de ordenar las letras:

cara	caar	cara	caar	craa	craa	raac	rcaa
raca	raca	raac	rcaa	acra	acar	arca	arac
aacr	aarc	acra	acar	arca	arac	aacr	aarc

Vemos que 2 ordenaciones de cara da lugar a la misma ordenación de las letras (resultado de intercambiar a por a). Por tanto, las letras de cara pueden ser ordenadas de $\frac{24}{2} = 12$ formas distintas.

Caso general:

Proposición 2

Supongamos que tenemos una lista de n objetos de r tipos diferentes. Del tipo 1 hay un total de n_1 objetos, todos ellos indistinguibles. Del tipo 2 hay n_2 objetos y así sucesivamente hasta el tipo r del cual hay n_r objetos. Entonces, el número total de ordenaciones de estos objetos es:

$$\frac{n!}{n_1!\, n_2! \ldots n_r!}$$

Demotración:

Para situar los n objetos, situamos en primer lugar los n_1 objetos del tipo 1. Para esto, únicamente hay que elegir el lugar en van a situarse estos objetos, y eso puede hacerse de $\binom{n}{n_1}$ formas.
Una vez hecho esto, situamos los n_2 objetos del tipo 2. Ahora tenemos únicamente $n - n_1$ lugares disponibles, luego, podemos colocarlos de $\binom{n-n_1}{n_2}$ formas.
Razonando de esta forma sucesivamente, el número total de ordenaciones es:

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\ldots\binom{n-n_1-\ldots-n_{r-1}}{n_r} = \frac{n!}{n_1!\, n_2! \ldots n_r!}$$

El problema de repartir objetos distinguibles en cajas distinguibles es una aplicación de la Proposición 2. Supongamos que tenemos n objetos y queremos repartirlos en r cajas de forma que en la primera caja haya n_1 objetos, en la caja 2 hay n_2 objetos y así sucesivamente hasta la $r-$ésima caja en la que debe haber n_r objetos.
El número de formas viene dado por:

$$\underbrace{\binom{n}{n_1}}_{Caja\,1}\underbrace{\binom{n-n_1}{n_2}}_{Caja\,2}\cdots\underbrace{\binom{n-n_1-\ldots-n_{r-1}}{n_r}}_{Caja\,r}=\frac{n!}{n_1!\,n_2!\,\ldots\,n_r!}$$

Sea $n\in\mathbb{N}$, $n_1,n_2,\ldots,n_r\in\mathbb{N}$ tales que $n_1+n_2+\ldots+n_r=n$. Se define el **coeficiente multinomial** como:

$$\binom{n}{n_1,n_2,\ldots,n_r}=\frac{n!}{n_1!\,n_2!\,\ldots\,n_r!}$$

Lema 1

Sea $n\in\mathbb{N}$, $n_1,n_2,\ldots,n_r$ tal que $n_1+n_2+\ldots+n_r=n+1$. Entonces:

$$\sum_{k=1}^{r}\binom{n}{n1,n_2,\ldots,n_k-1,\ldots,n_r}=\binom{n+1}{n_1,n_2,\ldots,n_r}$$

Si para algún i entre 1 y r se tiene $n_i=0$ entonces el sumando para $k=i$ también vale cero.

Demostración:

$$\binom{n}{n_1-1,n_2,\ldots,n_r}+\ldots+\binom{n}{n_1,n_2,\ldots,n_r-1}=$$

$$\frac{n!}{(n_1-1)!\,n_2!\,\ldots\,n_r!}+\ldots+\frac{n!}{n_1!\,n_2!\,\ldots\,(n_r-1)!}=$$

$$\frac{n!\,n_1}{n_1!\,n_2!\,\ldots\,n_r!}+\ldots+\frac{n!\,n_r}{n_1!\,n_2!\,\ldots\,n_r!}=$$

$$=\frac{n!}{n_1!\,n_2!\,\ldots\,n_r!}(n_1+\ldots+n_r)=\frac{(n+1)!}{n_1!\,n_2!\,\ldots\,n_r!}=\binom{n+1}{n_1,n_2,\ldots,n_r}$$

Teorema 2 (Teorema multinomial)

Para cada $n\in\mathbb{N}$ se cumple:

$$(x_1+x_2+\ldots+x_r)^n=\sum_{n_1+\ldots+n_r=n}\binom{n}{n_1,n_2,\ldots,n_r}x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r}$$

Demostración:

Inducción sobre n:

1. Caso base: $n=1$:

$$(x_1+x_2+\ldots+x_r)^1=x_1+x_2+\ldots+x_r,$$

pues las únicas formas de expresar 1 como suma de r sumandos es: $1+0+\ldots+0$ (da lugar al sumando x_1), $0+1+\ldots+0$ (da lugar al sumando x_2) y así sucesivamente.

2. Hipótesis de inducción: El teorema es válido para n.

Demostración: (cont.)

3. Demostremos para $n+1$:
Denote $a=(x_1+x_2+\ldots+x_r)^n$, luego:

$$(x_1+x_2+\ldots+x_r)^{n+1}=(x_1+\ldots+x_r)^n(x_1+\ldots+x_r)=a(x_1+\ldots+x_r)$$

Ahora, dados $n_1,n_2,\ldots,n_r\in\mathbb{N}$ tal que $n_1+n_2+\ldots+n_r=n+1$, el coeficiente de:

$$x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r}\quad\text{en}\quad(x_1+\ldots+x_r)^{n+1}$$

se obtiene sumando los coeficientes de:

$$x_1^{n_1-1}x_2^{n_2}\ldots x_r^{n_r},\,x_1^{n_1}x_2^{n_2-1}\ldots x_r^{n_r},\ldots,x_1^{n_1}x_2^{n_2}\ldots x_r^{n_r-1}$$

que aparecen en el desarrollo de " a ".

Demostración: (cont.)

Por la hipótesis inductiva, estos coeficientes valen:

$$\binom{n}{n_1-1,n_2,\ldots,n_r},\binom{n}{n_1,n_2-1,\ldots,n_r},\ldots,\binom{n}{n_1,n_2,\ldots,n_r-1}$$

y su suma se calcula usando el Lema 1, lo cual resulta en:

$$\binom{n+1}{n_1,n_2,\ldots,n_r}$$

Ejemplos:

1. Demuestre que $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$.
2. Determine el coeficiente de x^8 en el desarrollo de $(1+x^2-x^3)^9$.
3. Calcule $S=\displaystyle\sum_{k=0}^{n-1}(-1)^k\binom{n-1}{k}5^{2n-2k}2^{2k-2}6^{k+2}$.

Resolución:

Veamos 3:

$$\begin{aligned}S&=\sum_{k=0}^{n-1}(-1)^k\binom{n-1}{k}(5^2)^{n-k}[(2^2)(6)]^k(2^{-2})(6^2)\\&=25\frac{36}{4}\sum_{k=0}^{n-1}(-1)^k\binom{n-1}{k}25^{n-1-k}(24^k)\\&=25(9)(25-24)^{n-1}=225.\end{aligned}$$

Tabla de contenidos

Primeras estimaciones

Observe que:

$$n! \;\leq\; \prod_{i=1}^{n} i \;\leq\; \prod_{i=1}^{n} n \;=\; n^n$$

$$n! \;=\; \prod_{i=2}^{n} i \;\geq\; \prod_{i=2}^{n} 2 \;=\; 2^{n-1}$$

por tanto se tiene la siguiente estimación:

$$2^{n-1} \leq n! \leq n^n$$

¿$n!$ está más cerca de 2^{n-1} o de n^n?

Tenemos dos casos:

1. n par: Entonces $\frac{n}{2}$ elementos de $\{1, 2, \ldots, n\}$ son a lo más $\frac{n}{2}$ y $\frac{n}{2}$ son mayores que $\frac{n}{2}$. Luego:

$$n! \geq \prod_{i=\frac{n}{2}+1}^{n} i \geq \prod_{i=\frac{n}{2}+1}^{n} \frac{n}{2} = \left(\frac{n}{2}\right)^{\frac{n}{2}} = \left(\sqrt{\frac{n}{2}}\right)^n$$

por otro lado:

$$n! \leq \left(\prod_{i=1}^{\frac{n}{2}} \frac{n}{2}\right)\left(\prod_{i=\frac{n}{2}+1}^{n} n\right) = \frac{n^n}{2^{n/2}}.$$

¿$n!$ está más cerca de 2^{n-1} o de n^n? (cont.)

2. n impar: Demuestre que:

$$\left(\sqrt{\frac{n}{2}}\right)^n < n! \leq \frac{n^n}{2^{n/2}}$$

para todo $n \geq 3$

Teorema 3

Para todo $n \in \mathbb{N}$: $n^{\frac{n}{2}} \leq n! \leq \left(\frac{n+1}{2}\right)^n.$

Demostración:
La idea es conectar cada $i = 1, 2, \ldots, n$ con $n+1-i$ y estimar cada producto $i(n+1-i)$ superiormente e inferiormente.
Para cada $i = 1, 2, \ldots, n$ se tiene que $n+1-i = n, n-1, \ldots, 2, 1$; así el producto:

$$\prod_{i=1}^{n} i(n+1-i)$$

contiene cada factor $j = 1, 2, \ldots, n$ exactamente 2 veces, así se obtiene $(n!)^2$, por tanto:

$$(n!)^2 = \prod_{i=1}^{n} \sqrt{i(n+1-i)}$$

Eligiendo $a = i$ y $b = n+1-i$ y sabiendo que $\frac{a+b}{2} \geq \sqrt{ab}$ para todo $a, b \geq 0$; se obtiene:

$$\sqrt{i(n+1-i)} \leq \frac{(i+n+1-i)}{2} = \frac{n+1}{2},$$

así:

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leq \prod_{i=1}^{n} \left(\frac{n+1}{2}\right) = \left(\frac{n+1}{2}\right)^n$$

Para probar la cota inferior, basta mostrar que $i(n+1-i) \geq n$ para todo $i = 1, 2, \ldots, n$.
Para $2 \leq i \leq n-1$ tenemos el producto de dos números y observe:

- El más grande siendo al menos $n/2$,
- El más pequeño siendo al menos 2,

por tanto:

$$i(n+1-i) \geq \frac{n}{2}(2) = n \quad \forall i$$

entonces:

$$n! \geq \sqrt{n^n} = n^{n/2}.$$

Teorema 4

Para todo $n \in \mathbb{N}$ se cumple: $e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$

Demostración:
Probemos la cota superior, es decir: $n! \leq en\left(\frac{n}{e}\right)^n$.
Procedemos por inducción:

1. Caso base: $n = 1$, se verifica fácilmente: $1 \leq 1$.
2. Hipótesis de inducción: Supongamos válida la cota para $n-1$, es decir:

$$(n-1)! \leq e(n-1)\left(\frac{n-1}{e}\right)^{n-1}$$

3. Veamos que se cumple para n:

$$n! \;=\; n(n-1)! \leq n\left[e(n-1)\left(\frac{n-1}{e}\right)^{n-1}\right]$$

$$n! \;\leq\; \underbrace{ne\frac{(n-1)^n}{e^{n-1}}\frac{e\,n^n}{e\,n^n}}_{=}$$

$$\leq\; \left[en\left(\frac{n}{e}\right)^n\right]\underbrace{\left[\left(\frac{n-1}{n}\right)^n e\right]}_{(*)}$$

resta mostrar que $(*)$ es menor que 1. En efecto:

$$(*) = \left(\frac{n-1}{n}\right)^n e = e\left(1 - \frac{1}{n}\right)^n \leq e\left(e^{-1/n}\right)^n = ee^{-1} = 1$$

Probar la cota inferior queda como ejercicio.

Teorema 5 (Fórmula de Stirling)

Para $n \in \mathbb{N}$ se define $f(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ y se cumple:

$$\lim_{n\to\infty} \frac{f(n)}{n!} = 1$$

La demostración queda como ejercicio.

Estimaciones de los Coefcientes Binomiales

Ronald Mas,
Angel Ramirez

24 de junio de 2020

Contenido

Introducción

Empecemos estudiando una estimación rápida del coeficiente binomial:

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}$$

Como $\frac{n-i}{k-i} \leq n$, $\forall i \in \{0, 1, \cdots, \ddots k-1\}$ entonces:

$$\binom{n}{k} \leq n^k.$$

Por otro lado, para $n \geq k > i \geq 0$ se tiene que $\frac{n-i}{k-i} \geq \frac{n}{k}$ y por tanto:

$$\binom{n}{k} \geq \left(\frac{n}{k}\right)^k.$$

Teorema

Para cada $n \geq 1$ y k entero con $1 \leq k \leq n$, se tiene que:

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Prueba:
Para todo $x \in \mathbb{R}$ se tiene:

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (1+x)^n.$$

En particular para $x \in]0, 1[$ y $k \in [1, n]$ se tiene:

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{k}x^k \leq (1+x)^n.$$

Continua prueba

Al dividir por x^k se tiene:

$$\frac{1}{x^k}\binom{n}{0} + \frac{1}{x^{k-1}}\binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Entonces:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Luego al tomar $x = \frac{k}{n}$ se tiene:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

Por otro lado, como $1 + u \leq e^u$, $\forall u \in \mathbb{R}$, para $u = \frac{k}{n}$ se tiene:

$$\left(1 + \frac{k}{n}\right)^n \leq (e^{k/n})^n = e^k.$$

Por lo tanto se tiene el resultado deseado.

Proposición

Para todo $m \geq 1$ se tiene:

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}.$$

Prueba:
Definamos el número P como:

$$P = \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2m-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot (2m)},$$

luego al reescribir P se tiene:

$$P = \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2m-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot (2m)} \cdot \frac{2\cdot 4\cdot \ldots \cdot (2m)}{2\cdot 4\cdot \ldots \cdot (2m)} = \frac{(2m)!}{2^{2m}(m!)^2},$$

Continua prueba

Entonces

$$P = \frac{1}{2^{2m}}\binom{2m}{m}.$$

Como $\left(1 - \frac{1}{(2i)^2}\right) < 1$, $\forall i \in \{1, 2, \ldots, m\}$ entonces:

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right)\cdots\left(1 - \frac{1}{(2m)^2}\right) < 1.$$

Luego

$$\left(\frac{1\cdot 3}{2^2}\right)\left(\frac{3\cdot 5}{4^2}\right)\cdots\left(\frac{(2m-1)\cdot(2m+1)}{(2m)^2}\right) = (2m+1)P^2.$$

Continua prueba

Entonces $(2m+1)P^2 < 1$, por tanto $P \leq \frac{1}{\sqrt{2m}}$.
Veamos la otra desigualdad, como $\left(1 - \frac{1}{(2i-1)^2}\right) < 1. \forall i \in \{2, 3, \ldots, m\}$ se tiene:

$$\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots\left(1 - \frac{1}{(2m-1)^2}\right) < 1.$$

Luego

$$\left(\frac{2\cdot 4}{3^2}\right)\left(\frac{4\cdot 6}{5^2}\right)\cdots\left(\frac{(2m-2)\cdot(2m)}{(2m-1)^2}\right) = \frac{1}{2(2m)P^2}.$$

Por tanto:

$$P \geq \frac{1}{2\sqrt{m}}.$$

Estimación usando una relación de equivalencia

Definamos la relación $\sim$ sobre el conjunto $A = \{f(n) : f \text{ es una sucesión de números reales}\}$ como

$$f(n) \sim g(n) \text{ si y sólo si } \lim_{n\to+\infty} \frac{f(n)}{g(n)} = 1$$

Veamos que dicha relación es de equivalencia:

1) Reflexiva: $\lim_{n\to+\infty} \frac{f(n)}{f(n)} = 1$.
2) Simétrica: Si $\lim_{n\to+\infty} \frac{f(n)}{g(n)} = 1$ entonces $\lim_{n\to+\infty} \frac{g(n)}{f(n)} = 1$.
3) Transitiva: $\lim_{n\to+\infty} \frac{f(n)}{g(n)} = 1$ y $\lim_{n\to+\infty} \frac{g(n)}{h(n)} = 1$ entonces

$$\lim_{n\to+\infty} \frac{f(n)}{g(n)} \cdot \lim_{n\to+\infty} \frac{g(n)}{h(n)} = \lim_{n\to+\infty} [\frac{f(n)}{g(n)} \cdot \frac{g(n)}{h(n)}] = \lim_{n\to+\infty} \frac{f(n)}{h(n)} = 1$$

Fórmula de Stirling

$$n! \sim \frac{n^n}{e^n}\sqrt{2\pi n}.$$

Ejemplo:

- Para $n = 10$ se tiene:

$$10! = 3628800 \text{ y } \frac{10^{10}}{e^{10}}\sqrt{20\pi} = 3598695,61\ldots$$

Luego $\frac{10!}{\frac{10^{10}}{e^{10}}\sqrt{20\pi}} = 1,00836536$

- Para $n = 12$ se tiene:

$$10! = 479001600 \text{ y } \frac{12^{12}}{e^{12}}\sqrt{24\pi} = 475687486,2\ldots$$

Luego $\frac{12!}{\frac{12^{12}}{e^{12}}\sqrt{24\pi}} = 1,006967$

Estimación del coeficiente binomial usando Stirling

Como caso particular se podría hallar una estimación del coeficiente binomial:

$$\binom{2m}{m} = \frac{(2m)!}{(m!)^2}$$

$$\binom{2m}{m} \sim \frac{(2m)^{2m}/e^{2m}\sqrt{2\pi(2m)}}{(m^m/e^m)^2(2\pi m)} = \frac{2^{2m}}{\sqrt{\pi m}}.$$

Teorema

Sea $\pi(n)$ el número de primos naturales que no exceden al número n. Entonces:

$$\pi(n) \sim \frac{n}{ln(n)}.$$

Ejemplo:

- Para $n = 1000$ se tiene:

$$\pi(1000) = 168 \text{ y } \frac{1000}{ln1000} = 144,7648.$$

Luego $\frac{\pi(1000)}{\frac{1000}{ln1000}} = 1,16050311.$

- Para $n = 10000$ se tiene:

$$\pi(10000) = 1229 \text{ y } \frac{10000}{ln10000} = 1085,7362.$$

Luego $\frac{\pi(10000)}{\frac{10000}{ln10000}} = 1,13195084.$

Principio del Palomar

Principio del Palomar

Si se colocan n objetos en k casillas con $n, k \in \mathbb{N}$ entonces existe una casilla que contiene $[\![\frac{n-1}{k}]\!] + 1$ o más objetos.

Prueba:

Procedamos por contradicción, supongamos que en cada casilla podemos colocar a lo más $[\![\frac{n-1}{k}]\!]$ objetos. Como:

$$[\![\frac{n-1}{k}]\!] < \frac{n}{k}$$

entonces el número total de objetos es a lo más

$$k \cdot [\![\frac{n-1}{k}]\!] < k\left(\frac{n}{k}\right) = n$$

lo que contradice que el número total de objetos sea n.

Consecuencias del Principio del Palomar

Consecuencias

- Si m objetos se distribuyen en k conjuntos y $n > mk$ entonces al menos $m + 1$ objetos se encuentran en un mismo conjunto.
- Si $k + 1$ ó más objetos se colocan en k casillas existe al menos una casilla que contiene dos o más objetos.

Ejemplo:

1) En un grupo de 13 personas existen al menos dos que cumplen años en el mismo mes.
2) Al seleccionar 6 números naturales cualesquiera, se puede asegurar que siempre hay al menos dos de ellos cuya diferencia es múltiplo de 5.
3) En un grupo de 6 personas siempre hay 3 que se conocen entre ellas o 3 que no se conocen entre sí.

Estimaciones de los Coefcientes Binomiales

Ronald Mas,
Angel Ramirez

22 de junio de 2020

Contenido

Resultados Previos

Proposición

Si $A \subset B$ entonces $| B - A |=| B | - | A |$.

Prueba:

Si $A \subset B$ entonces $B = A \cup (B - A)$. Como $A \cap (B - A) = \emptyset$ entonces $| B |=| A \cup (B - A) |=| A | + | B - A |$ que concluye la prueba.

Proposición

Si A, B y C son conjuntos finitos disjuntos dos a dos se cumple que:

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

Prueba:

Como $A \cap (B \cup C) = (A \cap B) \cup (A \cap C) = \emptyset \cup \emptyset = \emptyset$. Luego

$$\begin{aligned} | A \cup B \cup C | &= | A \cup (B \cup C) | \\ &= | A | + | B \cup C | \\ &= | A | + | B | + | C | \end{aligned}$$

Principio de Inclusión-exclusión

Teorema

Para toda sucesión $A_1, A_2, \cdots, A_n$ de conjuntos finitos se cumple que:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\cdots,n\}}{k}} |\bigcap_{i \in I} A_i|.$$

Prueba:

Procedamos por inducción:

1) Para $n = 2$ se tiene que:
Como $A_1 \cup A_2 = [A_1 - (A_1 \cap A_2)] \cup [A_2 - (A_1 \cap A_2)] \cup [A_1 \cap A_2]$.
Por lo resultados previos se tiene que:

$$\begin{aligned} |A_1 \cup A_2| &= |A_1 - (A_1 \cap A_2)| + |A_2 - (A_1 \cup A_2)| + |A_1 \cap A_2| \\ &= |A_1| - |A_1 \cap A_2| + |A_2| - |A_1 \cap A_2| + |A_1 \cap A_2 \\ &= |A_1| + |A_2| - |A_1 \cap A_2|. \end{aligned}$$

2) Supongamos que se cumple para $n - 1$

$$\begin{aligned} |\bigcup_{i=1}^{n} A_i| &= |\bigcup_{i=1}^{n-1} (A_i) \cup A_n| \\ &= |\bigcup_{i=1}^{n-1} A_i| + |A_n| - |(\bigcup_{i=1}^{n-1} A_i) \cap A_n| \\ &= |\bigcup_{i=1}^{n-1} A_i| + |A_n| - |(\bigcup_{i=1}^{n-1} (A_i \cap A_n)| \end{aligned}$$

Usando la hipotesis de inducción a $|\bigcup_{i=1}^{n-1} A_i|$ y $|\bigcup_{i=1}^{n-1} A'_i|$ con $A'_i = A_i \cap A_n$.

Continua la prueba

$$\begin{aligned} &= \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\cdots,n-1\}}{k}} |\bigcap_{i \in I} A_i| \right) + |A_n| \\ &- \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\cdots,n-1\}}{k}} |\bigcap_{i \in I \cup \{n\}} A_i| \right). \end{aligned}$$

Luego en la primera suma agregamos con los signos apropiados el tamaño de las intersecciones que no incluyan a An y en la segunda suma el tamaño de las intersecciones que incluyan a An aparecidas. Luego esto concluiria la prueba.

Ejemplo:

Para un número natural el valor de $\varphi(n)$ llamado **Indicador de Euler o función de Euler** es definido como la cantidad de números $m \leq n$ y que son coprimos con n Es decir:

$$\varphi(n) = |\{m \in \mathbb{N} : \ MCD(n, m) = 1\}|.$$

Por ejemplo, si: $n = p_1^{\alpha_1} p_2^{\alpha_2}$, luego

$$\begin{aligned} \varphi(n) &= n - |A_1 \cup A_2| \\ &= n - |A_1| - |A_2| + |A_1 \cap A_2| \\ &= n - \tfrac{n}{p_1} - \tfrac{n}{p_2} + \tfrac{n}{p_1 p_2} \\ &= n \left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right). \end{aligned}$$

Fórmula del Indicador

Sea $n \in \mathbb{N}$ entonces por el teorema fundamental de la aritmética se tiene

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

con $p_1, \cdots, p_r$ primos distintos y $\alpha_i \in \mathbb{N}$.

Teorema

Para $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ se tiene:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Álgebra de Boole

Definición

Un álgebra de Boole también llamada un álgebra Booleana es un conjunto B junto con dos operaciones:

$$\begin{aligned} + : \ B \times B &\longrightarrow B \\ (a, b) &\longmapsto a + b \end{aligned} \qquad \begin{aligned} \cdot : \ B \times B &\longrightarrow B \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

que cumplen los siguientes axiomas:

1) $a + b = b + a$ y $a \cdot b = b \cdot a$.
2) $(a + b) + c = a + (b + c)$ y $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3) $a + (b \cdot c) = (a + b) \cdot (a + c)$ y $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
4) Existen elementos 0 y 1 en B tal que $a + 0 = a$ y $a \cdot 1 = a$.
5) Para cada $a \in B$ existe un elemento en B denotado por $\overline{a}$ llamado el complemento de a tal que $a + \overline{a} = 1$ y $a \cdot \overline{a} = 0$.

Teorema

Sea B un álgebra de Boole, se cumple:

1) *El complemento $\overline{a}$ de $a \in B$ es único.*
2) *Los elementos 0 y 1 son únicos.*
3) $\overline{(\overline{a})} = a$, $\forall a \in B$.
4) *Para cada $a \in B$ se cumple que $a + a = a$ y $a \cdot a = a$.*
5) *Para cada $a, b \in B$ se cumple que $a + 1 = 1$ y $a \cdot 0 = 0$.*
6) *Para cada $a, b \in B$ se cumple que $\overline{a + b} = \overline{a} \cdot \overline{b}$ y $\overline{a \cdot b} = \overline{a} + \overline{b}$.*

Prueba del teorema

Prueba:

1) Supongamos que $a \in B$ posee otro complemento, es decir existe $x \in B$ tal que $a + x = 1$ y $a \cdot x = 0$. Entonces:

$$\begin{aligned} x &= x \cdot 1 \\ &= x \cdot (a + \overline{a}) \\ &= x \cdot a + x \cdot \overline{a} \\ &= a \cdot x + x \cdot \overline{a} \\ &= 0 + x \cdot \overline{a} \\ &= a \cdot \overline{a} + x \cdot \overline{a} \\ &= \overline{a} \cdot a + \overline{a} \cdot x \\ &= \overline{a} \cdot (a + x) \\ &= \overline{a} \cdot 1 \\ &= \overline{a}. \end{aligned}$$

Continuación de la prueba

3) $$\begin{aligned} \overline{a} + a &= a + \overline{a} \\ &= 1 \end{aligned} \quad \text{y}$$

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

Como a satisface las condiciones para ser el complemento de a se tiene que $\overline{(\overline{a})} = a$.

4) Sea $a \in B$ entonces:

$$\begin{aligned} a &= a + 0 \\ &= a + (a \cdot \overline{a}) \\ &= (a + a) \cdot (a + \overline{a}) \\ &= (a + a) \cdot 1 \\ &= a + a. \end{aligned}$$

Dado $B=\{0,1\}$, sea $B^n=\{(x_1,\cdots,x_n): \ x_i\in B \text{ con } 1\leq i\leq n\}$, definamos una función booleana como:

$$\begin{array}{rccc} f: & B^n & \longrightarrow & B \\ & (x_1,\cdots,x_n) & \longmapsto & f(x_1,\cdots,x_n) \end{array}$$

Observaciones:

a) La variable $x\in B$ se denomina **variable booleana**.

b) En el lenguaje de las maquinas el 0 significa apagado y el 1 encendido.

Ejemplos:

Ejemplo 1:
Encuentre los valores que toma la función booleana dado por $F(x,y,z)=xy+\overline{z}$.
Solución:

x	y	z	F(x,y,z)
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

Ejemplo 2:
Encontrar la función booleana de una cámara fotográfica que tiene 3 sensores y toma la foto si.

i) El sensor luz esta prendido (1) y el sensor distancia Apagado (0);

ii) El sensor sonrisa Prendido(1) y el sensor luz apagado (0)

Solución:
Sean las variables:
x:El sensor de luz
y:El sensor de sonrisa
z:El sensor de distancia

Continua Ejemplo 2

x	y	z	F(x,y,z)
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

Por tanto la función booleana es:

$$F(x,y,z)=xy\overline{z}+x\overline{y}\,\overline{z}+\overline{x}yz+\overline{x}y\overline{z}.$$

GRAFOS. ISOMORFISMO. SUBGRAFOS. CAMINOS. CICLOS.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

19 de junio de 2020

Tabla de contenidos

Definición 1

*Un **grafo** G es un par ordenado (V,E) donde V es algún conjunto y E es un conjunto de subconjuntos de 2 puntos de V. Los elementos del conjunto V son llamados **vértices** del grafo G y los elementos de E son llamados **Aristas** del grafo G.*

Ejemplo:
Sea $V=\{\text{personas en una fiesta}\}$ y
$E=\{(x,y)\in V\times V \,/\, x \quad \text{conoce a} \quad y\}$.

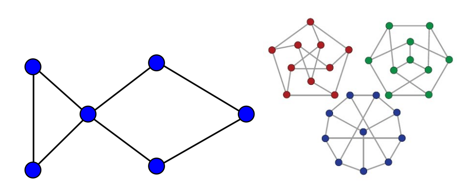
Observaciones

1. Consideraremos grafos con conjunto de vértices V finito.
2. $G=(V,E)$ denota un grafo con conjunto de vértices V y aristas E.
3. $V(G)$ denota el conjunto de vértices de un grafo G.
4. $E(G)$ denota el conjunto de aristas de un grafo G.
5. $\binom{V}{2}$ es el conjunto de todos los subconjuntos de 2 elementos de V, por tanto, podemos también decir que un grafo es un par (V,E) donde $E\subset\binom{V}{2}$.
6. Si $\{u,v\}$ es una arista de algún grafo G, decimos que u y v son adyacentes en G o que u es un vecino de v (o viceversa).

Representación de un grafo

Los grafos son usualmente representados en el plano como sigue:

1. Los vértices del grafo son representados por puntos.
2. Las aristas son representadas por rectas (o arcos) que unen un par de puntos.



Observaciones:

1. El rol de graficar un grafo es auxiliar.
2. En un computador no se representa un grafo por un gráfico.
3. Hay otros modos de representarlos, por ejemplo, el grafo $G = (V, E)$ donde:

$$\begin{aligned} V &= \{a, b, c, e, f, g\} \\ E &= \{\{a, f\}, \{a, g\}, \{g, f\}, \{g, b\}, \{g, c\}, \\ &\quad \{f, b\}, \{f, c\}, \{b, c\}, \{b, e\}, \{c, e\}\} \end{aligned}$$

representa el grafo mostrado en la Figura 1.

Observaciones: (cont.)

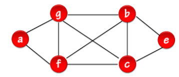


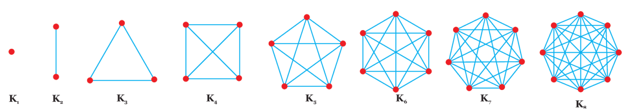
Figura 1: Representación gráfica del grafo G

4. Al graficar un grafo, visualmente las aristas deben de cruzarse lo menos posible. Los cruces pueden provocar errores como en esquemas de circuitos eléctricos u otras situaciones. Esto motiva el estudio de **grafos planares**.
5. Graficar grafos es una ayuda importante en la teoría de grafos. Dibujar grafos tanto como sea posible, ayuda a un mejor análisis. Muchas nociones son motivadas por el gráfico y dibujarlas pueden hacer las cosas más intuitivas.

Tabla de contenidos

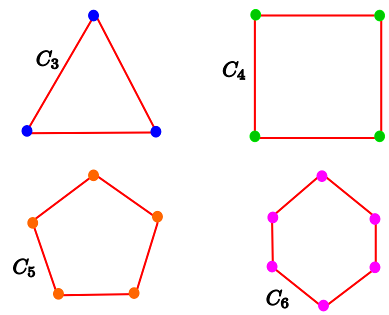
Grafo completo K_n

$K_n = (V, E)$ donde $V = \{1, 2, \ldots, n\}$ y $E = \binom{V}{2}$



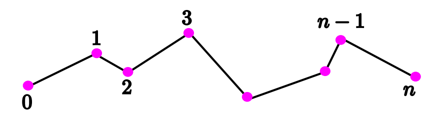
Ciclo C_n

$C_n = (V, E)$ donde $V = \{1, 2, \ldots, n\}$ y
$E = \{\{i, i+1\} \,/\, i = 1, 2, \ldots, n-1\} \cup \{n, 1\}$.



Ruta (Path) P_n

$P_n = (V, E)$ donde $V = \{0, 1, \ldots, n\}$ y
$E = \{\{i-1, i\} \,/\, i = 1, 2, \ldots, n\}$.



Un path P_n también es llamado **camino simple**.

Grafo bipartito $K_{n,m}$

$K_{n,m} = (V, E)$ donde $V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\}$ y
$E = \{\{u_i, v_j\} \,/\, i = 1, \ldots, n; j = 1, \ldots, m\}$.

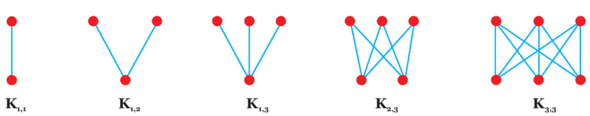


Tabla de contenidos

Dos grafos G y G' son considerados **idénticos** (o iguales) si ellos tienen el mismo conjunto de vértices y el mismo conjunto de aristas, es decir, $G = G' \Leftrightarrow V(G) = V(G')$ y $E(G) = E(G')$. Pero muchos grafos difieren solamente por el nombre de sus vértices y aristas pero tienen la misma estructura.

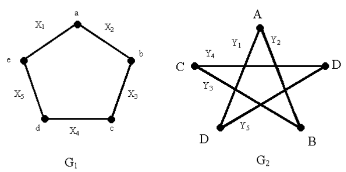
Definición 2

Dos grafos $G = (V, E)$ y $G' = (V', E')$ son llamados **isomorfos** *si existe una biyección $f : V \to V'$ tal que:*

$$\{x, y\} \in E \Leftrightarrow \{f(x), f(y)\} \in E' \quad \forall x, y \in V, x \neq y.$$

Tal f es llamado **isomorfismo** *entre los grafos G y G'. Dos grafos isomorfos es denotado por $G \cong G'$.*

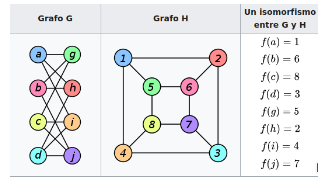
Ejemplo: Grafos Isomorfos



Un isomorfismo para los grafos anteriores G_1 y G_2 está definido por:

$$f(a) = A, \quad f(b) = B, \quad f(c) = C, \quad f(d) = D, \quad f(e) = E$$

Ejemplo: Grafos Isomorfos



Ejemplo

Dado un grafo $G = (V, E)$ definimos el **complemento** de G al grafo $G^c = (V, E^c)$ donde $e \in E^c \Leftrightarrow e \notin E$. Decimos que un grafo G es autocomplementario si G es isofomorfo a G^c. Demuestre que si G es **autocomplementario** entonces $n \equiv 0$ o $1 \, mod \, 4$, donde $n = |V(G)|$. **Solución**:

Como $G \cong G^c$ entonces deben tener el mismo número de aristas y además la suma de sus números de aristas deben ser igual al número de aristas del grafo completo. Por tanto, el número de aristas de G y G^c debe ser:

$$\frac{1}{2}\binom{n}{2} = \frac{1}{2}\left(\frac{n!}{(n-2)!2!}\right) = \frac{n(n-1)}{4}.$$

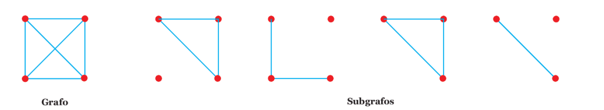
Ejemplo (cont.)

Claramente este número de aristas debe ser un entero. Así, $n(n-1)$ debe ser divisible por 4. Desde que n y $n-1$ no pueden ser ambos divisibles por 2, debemos tener que n o $n-1$ es divisible por 4. Por tanto, esto es la condición $n \equiv 0$ o $1 \, mod \, 4$.

Tabla de contenidos

Definición 3

Sean G y G' grafos. Decimos que G es un **subgrafo** *de G' si $V(G) \subset V(G')$ y $E(G) \subset E(G')$.*



Definición 4

Decimos que G es un **subgrafo inducido** *de G' si $V(G) \subset V(G')$ y $E(G) = E(G') \cap \binom{V(G)}{2}$.*

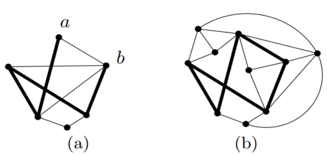


Figura 2: **(a)** Ejemplo de subgrafo. **(b)** Ejemplo de subgrafo inducido.

Ejemplo:

Determine si K_4 es un subgrafo de $K_{4,4}$. Si su respuesta es afirmativa, entonces grafique. Caso contrario, justifique.

Demostración:
Afirmamos que K_4 no es un subgrafo de $K_{4,4}$. Procedemos a demostrarlo. Sean X e Y las dos partes de $K_{4,4}$. Para cada subgrafo H de $K_{4,4}$ con 4 vértices, alguno de sus vértices están en X y los otros están en Y. Así tenemos los siguientes casos:

1. $V(H) \in X$ o $V(H) \subset Y$. Entonces H no debe tener aristas porque un grafo bipartito no tiene aristas cuyos ambos extremos están en X (respectivamente en Y). Así, H no es K_4.
2. Tres vértices de H están en X y uno está en Y(o viceversa). Entonces a lo más uno de los vértices en H tiene grado a lo más 3 y el resto de los vértices tienen grado a lo más 1. Pero, la secuencia de grados de K_4 es (3,3,3,3). Así, H no es K_4 en

Camino en un grafo

Un subgrafo de un grafo G isormorfo a algún camino P_t es llamado un **camino simple (path)** en el grafo G. Un **camino simple** en un grafo G puede ser entendido como una secuencia:

$$(v_0, e_1, v_1, \ldots, e_t, v_t),$$

donde $v_0, v_1, \ldots, v_t$ son vértices distintos del grafo G para cada $i = 1, 2, \ldots, t$ y además $e_i = \{v_{i-1}, v_i\} \in E(G)$.
También decimos que el camino $(v_0, e_1, v_1, \ldots, e_t, v_t)$ es un **camino simple desde** v_0 **hasta** v_t de **longitud** t.
En el caso que $t = 0$, es decir, un camino de longitud cero consiste de un **único vértice**.

Ejemplo de camino

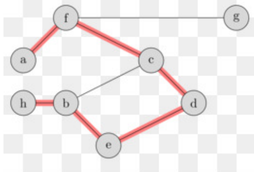


Figura 3: $P_6 = \{a, \{a, f\}, f, \{f, c\}, c, \{c, d\}, d, \{d, e\}, e, \{e, b\}, b, \{b, h\}, h\}$.

Ciclo en un grafo

Un subgrafo de G que es isomorfo a algún ciclo C_t $(t \geq 3)$ es llamado **un ciclo** en el grafo G. También es llamado **circuito**. Un ciclo en un grafo G puede ser entendido como una secuencia:

$$(v_0, e_1, v_1, e_2, \ldots, e_{t-1}, v_{t-1}, e_t, v_0)$$

(observe que los puntos inicial y final **coinciden**), donde $v_0, v_1, \ldots, v_{t-1}$ son pares de vértices distintos del grafo G y $e_i = \{v_{i-1}, v_i\} \in E(G)$ para $i = 1, 2, \ldots, t-1$ y además $e_t = \{v_{t-1}, v_0\} \in E(G)$. El número $t \geq 3$ es llamado **longitud** del ciclo.

Ejemplo de ciclo

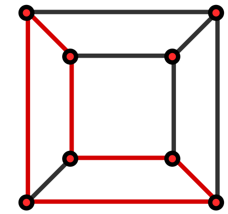


Figura 4: C_6.

Ejemplo de ciclo

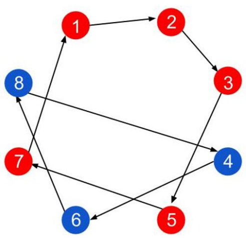


Figura 5: C_3 y C_5.

Tabla de contenidos

Grafos conexos

Decimos que un grafo G es conexo si para cualquier par de vértices $x, y \in V(G)$ se tiene que G contiene un **camino simple** desde x a y.

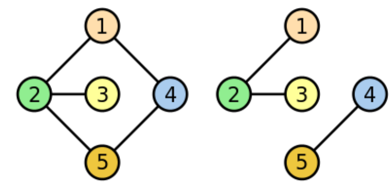


Figura 6: Grafo conexo (Izquierda). Grafo no conexo (Derecha).

Camino (WALK)

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

$$(v_0, e_1, v_1, e_2, \ldots, e_t, v_t)$$

es llamado **un camino** en G (o **camino de longitud** t **desde** v_0 **hasta** v_t) si se cumple que $e_i = \{v_{i-1}, v_i\} \in E$ para todo $i = 1, \ldots, t$.

En un **camino** algunos vértices y aristas pueden **repetirse**, mientras que un **camino simple** está prohibido que se repiten vértices y aristas.

Ejemplo de camino

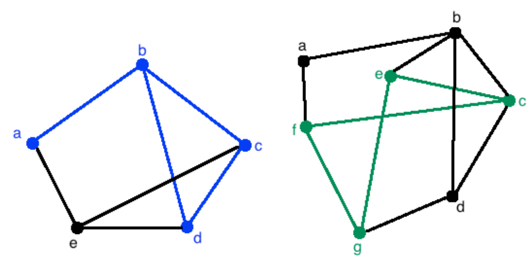


Figura 7: Camino en un grafo

Componentes de un grafo

Definimos una relación $\sim$ sobre el conjunto $V(G)$ del modo siguiente, dados $x, y \in V(G)$:

$$x \sim y \Leftrightarrow \text{existe un camino desde} \quad x \quad \text{hasta} \quad y \quad \text{en} \quad G$$

Verifique que $\sim$ es una relación de equivalencia.
Sea $V = V_1 \cup V_2 \cup \ldots \cup V_k$ la partición en $V(G)$ generada por la relación de equivalencia $\sim$. Los subgrafos de G inducidos por los conjuntos V_i son llamados **componentes** del grafo G.

Teorema 1

Cada componente de cualquier grafo es conexa. Un grafo es conexo si y sólo si tiene una única componente.

Demostración:
De la definición de componente se tiene que ésta es conexa.
Por otro lado, si un grafo es conexo entonces es claro que tiene una única componente.
Por otra parte, para cualquier par de vértices x, y en la misma componente de un grafo G pueden ser unidos por un camino.
Cualquier camino de x a y de longitud más corta posible debe ser un camino simple.

DISTANCIA EN GRAFOS. MATRIZ DE ADYACENCIA. SECUENCIA DE GRADOS.

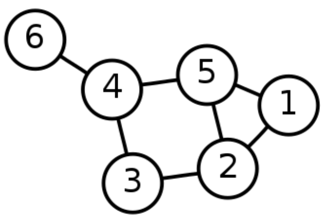
Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

19 de junio de 2020

Tabla de contenidos

Sea $G = (V, E)$ un **grafo conexo**. Definimos la **distancia** entre dos vértices $v, v' \in V(G)$, denotado por $d_G(v, v')$, como la longitud del camino simple más corto desde v hasta v' en G.



Observe que $d_G : V(G) \times V(G) \to \mathbb{R}$ es una función llamada **función distancia** o **métrica** del grafo G. Esta métrica tiene las siguientes propiedades:

1. $d_G(v, v') \geq 0$ para todo $v, v' \in V(G)$.
2. $d_G(v, v') = 0$ si y sólo si $v = v'$.
3. Simetría: $d_G(v, v') = d_G(v', v)$ para cualquier par $v, v' \in V(G)$.
4. Desigualdad triangular: $d_G(v, v'') \leq d_G(v, v') + d_G(v', v'')$ para todo $v, v', v'' \in V(G)$.

Una función $d : V(G) \times V(G) \to \mathbb{R}$ que satisfacen las propiedades 1–4 es llamada **métrica** sobre el conjunto $V(G)$. El par $(V(G), d)$ es llamado **espacio métrico**.

La función distancia d_G cumple además las siguientes propiedades:

1. $d_G(v, v')$ es un enetro no negativo para cualquier $v, v' \in V(G)$.
2. Si $d_G(v, v'') > 1$ entonces existe un vértice $v' \neq v''$ y $v \neq v'$ tal que $d_G(v, v') + d_G(v', v'') = d_G(v, v'')$.

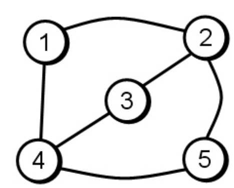
Tabla de contenidos

Definición 1

Sea $G = (V, E)$ un grafo con n vértices. Denote los vértices por $v_1, v_2, \ldots, v_n$ (en algún orden arbitrario). La **matriz de adyacencia** *de G, con respecto a la numeración realizada en los vértices, es una matriz $n \times n$ definida por la siguiente regla:*

$$a_{ij} = \begin{cases} 1, & si \quad \{v_i, v_j\} \in E, \\ 0 & en\ otro\ caso \end{cases}$$

Ejemplo:



M	1	2	3	4	5
1	0	1	0	1	0
2	1	0	1	0	1
3	0	1	0	1	0
4	1	0	1	0	1
5	0	1	0	1	0

Figura 1: Matriz de adyacencia

Proposición 1

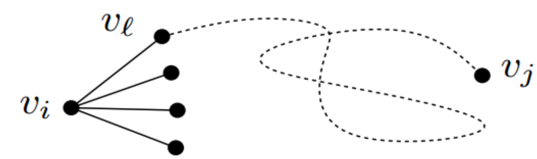
Sea $G = (V, E)$ un grafo con vértices $V = \{v_1, v_2, \ldots, v_n\}$ y sea $A = A_G$ su respectiva matriz de adyacencia. A^k denota la potencia $k-$ésima de la matriz A. $a_{ij}^{(k)}$ denota el elemento de la matriz A^k en la posición (i, j). Entonces, $a_{ij}^{(k)}$ es el número de caminos de longitud exactamente k desde el vértice v_i hasta el vértice v_j en el grafo G.

Demostración:

Procedemos por inducción.

1. Un camino de longitud 1 entre dos vértices significa exactamente que estos vértices están unidos por una arista, y de aquí para $k = 1$ la proposición sólo reformula la definición de la matriz de adyacencia.
2. Sea $k > 1$, y sean v_i, v_j dos vértices arbitrarios (posiblemente idénticos). Cualquier camino de longitud k de v_i hacia v_j consiste de una arista desde v_i a algún vecino v_l y de camino de longitud $k-1$ desde v_l hasta v_j:

Demostración: (cont.)



Demostración: (cont.)

Por hipótesis de inducción, el número de caminos de longitud $k-1$ desde v_l hasta v_j es $a_{lj}^{(k-1)}$. De aquí el número de caminos de longitud k desde v_i hacia v_j es:

$$\sum_{\{v_i, v_l\} \in E(G)} a_{lj}^{(k-1)} = \sum_{l=1}^{n} a_{il} a_{lj}^{(k-1)}$$

Pero esto es exactamente el elemento en la posición (i, j) en el producto de las matrices A y A^{k-1}, es decir: $a_{ij}^{(k)}$.

Corolario 1

La distancia de cualquier dos vértices v_i y v_j satisface:

$$d_G(v_i, v_j) = \min\{k \geq 0 \,/\, a_{ij}^{(k)} \neq 0\}.$$

Tabla de contenidos

Definición 2 (Grado de un vértice)

Sea G un grafo y sea v un vértice de G. El número de aristas de G que contienen el vértice v es denotado por el símbolo $deg_G(v)$. Este número es llamado **grado** *de v en el grafo G.*

Definición 3 (Secuencia de grado)

Denotando los vértices de G por $v_1, v_2, \ldots, v_n$ (en algún orden elegido arbitrariamente). La secuencia

$$(deg_G(v_1), deg_G(v_2), \ldots, deg_G(v_n))$$

es llamado **secuencia de grado** *del grafo G o* **score** *de G.*

Observaciones:

1. No haremos distinción entre dos scores si uno de ellos se puede obtener a partir del otro al reordenar sus términos.
2. Por convención, escribiremos los scores en orden no decreciente, es decir, el primer valor será el más pequeño.
3. Dos grafos isomorfos tienen el mismo score, así, dos grafos con score diferente son necesariamente no isomorfos.
4. Por otro lado, grafos con el mismo score no son necesariamente isomorfos. Analice los siguientes grafos:

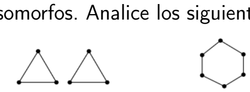


Figura 2: Score: (2,2,2,2,2,2). Grafo no conexo (Izquierda). Grafo conexo (Derecha).

Ejemplo:

Determine si K_4 es un subgrafo de $K_{4,4}$. Si su respuesta es afirmativa, entonces grafique. Caso contrario, justifique.

Demostración:

Ejemplo: (cont.)

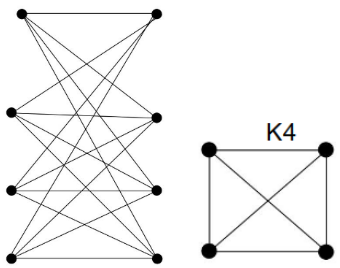


Figura 3: $K_{4,4}$ a la izquierda.

Ejemplo: (cont.)

Afirmamos que K_4 no es un subgrafo de $K_{4,4}$. Procedemos a demostrarlo. Sean X e Y las dos partes de $K_{4,4}$. Para cada subgrafo H de $K_{4,4}$ con 4 vértices, alguno de sus vértices están en X y los otros están en Y. Así tenemos los siguientes casos:

1. $V(H) \in X$ o $V(H) \subset Y$. Entonces H no debe tener aristas porque un grafo bipartito no tiene aristas cuyos ambos extremos están en X (respectivamente en Y). Así, H no es K_4.
2. Tres vértices de H están en X y uno está en Y(o viceversa). Entonces a lo más uno de los vértices en H tiene grado a lo más 3 y el resto de los vértices tienen grado a lo más 1. Pero, la secuencia de grados de K_4 es (3,3,3,3). Así, H no es K_4 en este caso.

Ejemplo: (cont.)

3. Dos vértices de H están en X y los otros dos están en Y. Entonces el máximo grado de un vértice en H es 2, y así H no es K_4.

Desde que hemos considerado todos los subgrafos posibles de $K_{4,4}$ con 4 vértices y ninguno de ellos puede ser K_4, entonces K_4 no es un subgrafo de $K_{4,4}$.

Proposición 2

Para cada grafo $G = (V, E)$ se cumple:

$$\sum_{v \in V} deg_G(v) = 2|E|.$$

Demostración:
El grado de un vértice v es el número de aristas que contienen a v. Cada arista contiene 2 vértices, y de aquí sumando sobre todos los grados se obtiene el doble del número de aristas.

Corolario 2 (Lema de Handshake)

En cualquier grafo, el número de vértices de grado impar es par.

Teorema 1 (Teorema del score)

Sea $D = (d_1, d_2, \ldots, d_n)$ una secuencia de números naturales $n > 1$. Suponga que $d_1 \leq d_2 \leq \ldots \leq d_n$ y sea el símbolo D' que denota a la secuencia $(d_1', \ldots, d_{n-1}')$ donde:

$$d_i' = \begin{cases} d_i, & para \quad i < n - d_n \\ d_i - 1, & para \quad i \geq n - d_n \end{cases}$$

Por ejemplo, para $D = (1, 1, 2, 2, 2, 3, 3)$, tenemos $D' = (1, 1, 2, 1, 1, 2)$. Entonces D es el score de un grafo si y sólo si D' es el score de un grafo.

Grafos Eurelianos

Ronald Mas,
Angel Ramirez

8 de julio de 2020

Contenido

Introducción

Empecemos estudiando el problema más antiguo que usa dibujo de grafos:
Problema: Dibujar un grafo $G = (V, E)$ con una sola linea cerrada sin levantar el lapiz del papel y pasar por cada arista solo una vez.
En términos matemáticos se puede formalizar como: Encontrar un camino cerrado

$$(v_0, e_1, v_1, \cdots, e_m, v_0)$$

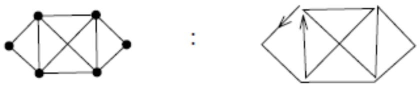
conteniendo todos lo vértices y todas las aristas exactamente una vez (los vértices pueden repetirse).

Definición
Definamos el recorrido cerrado Eureliano en G como el camino

$$(v_0, e_1, v_1, e_2, \cdots, e_{m-1}, v_{m-1}, e_m, v_0).$$

Definición
Un grafo que posee un recorrido cerrado Eureliano es llamado **Grafo Eureliano**.

Ejemplo: El dibujo muestra un grafo eureliano



con recorrido Eureliano:

$$(v_0, e_1, v_1, e_2, v_2, e_3, v_3, e_4, v_4, e_5, v_5, e_6, v_6, e_7, v_7, e_8, v_8, e_9, v_9, e_{10}, v_0),$$

donde $v_6 = v_3$, $v_7 = v_0$, $v_8 = v_5$ y $v_9 = v_2$.

Caracterización de grafos Eurelianos

Teorema
Un grafo $G = (V, E)$ es Eureliano si y sólo si este es conexo y cada vértice posee grado par.

Prueba:
Veamos la vuelta, definamos el recorrido en G como un camino en el que ninguna arista se repite (vértices se pueden repetir). Sea el recorrido

$$T = (v_0, e_1, v_1, e_2, \cdots, e_{m-1}, v_{m-1}, e_m, v_0).$$

en G de mayor longitud posible. Afirmación:

i) $v_0 = v_m$ y
ii) $\{e_i : i = 1, 2, \cdots, m\} = E$

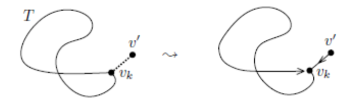
Continua prueba:

En efecto:

i) Si $v_0 \neq v_m$ entonces el vértice v_0 incidente a un número impar de aristas del recorrido T, pero como $deg_G(v_0)$ es par entonces existe una arista $e \in E(G)$ no contenido en T, por tanto T puede ser extendido con esta arista, lo que contradice la maximalidad de la longitud de T.
ii) Si $V(T) \neq V(G)$ y como G conexo entonces existe $e = \{v_k, v'\} \in E(G)$ tal que $v_k \in V(T)$ pero $v' \notin V(T)$. Luego existe un recorrido:

$$T' = (v', e, v_k, e_{k+1}, v_{k+1}, \cdots v_{m-1}, e_m, v_0, e_1, v_1, e_2, \cdots, e_k, v_k).$$

con longitud $m + 1$ lo que contradice la maximalidad de m.

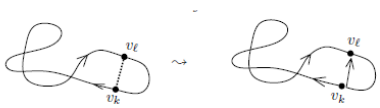


Continua prueba:

Si $V(T) = V(G)$ y $E(T) \neq E(G)$, sea $e \in E(G) \backslash E(T)$ con $e = \{v_k, v_l\}$.
Procedamos de modo similar como el caso anterior, al considerar un nuevo recorrido:

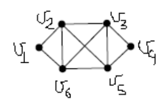
$$T' = (v_k, e_{k+1}, v_{k+1}, \cdots v_{m-1}, e_m, v_0, e_1, v_1, e_2, \cdots, e_k, v_k, e, v_l)$$

llegamos a una contradicción.



Lema
Si un grafo $G = (V, E)$ posee todos sus vértices de grado par entonces el conjunto $E(G)$ puede ser particionado en conjuntos disjuntos $E_1, E_2, \cdots, E_k$ tal que cada E_i es el conjunto de aristas de un ciclo.

Ejemplo: Dado el grafo Eureliano



se tiene la partición para $E(G)$ en:

$$\begin{aligned} E_1 &= \{\{v_1, v_2\}, \{v_2, v_6\}, \{v_1, v_6\}\} \\ E_2 &= \{\{v_2, v_3\}, \{v_3, v_5\}, \{v_2, v_5\}\} \\ E_3 &= \{\{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_3, v_6\}\} \end{aligned}$$

Grados Eurelianos dirigidos

Definición
Un grafo dirigido G es un par (V, E), donde $E \subset V \times V$. Los pares ordenados $(x, y) \in E$ son llamados aristas dirigidas.

Observación:

- Si $e = (x, y)$ diremos que la arista viene de x a y.

Definición
Definamos el recorrido dirigido en un grafo dirigido $G = (V, E)$ como la secuencia:

$$(v_0, e_1, v_1, e_2, \cdots, e_m, v_m)$$

tal que $e_i = (v_{i-1}, v_i) \in E \; \forall i \in \{1, 2, \cdots, m\}$ con $e_i \neq e_j$ si $i \neq j$.

Observación:

- Un grafo dirigido (V, E) es **Eureliano** si este posee un recorrido dirigido cerrado conteniendo todos los vértices y pasando cada arista dirigida exactamente una vez.

Consecuencias

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

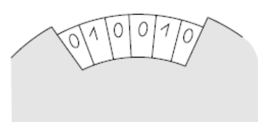
- Denotamos $deg_G^+(v)$ como el número de aristas dirigidas que terminan en v.
- Denotamos $deg_G^-(v)$ como el número de aristas dirigidas que se originan en v.
- Cada grafo dirigido $G = (V, E)$ puede ser asignado un grafo no dirigido $sym(G) = (V, \overline{E})$ donde

$$\overline{E} = \{\{x, y\} : (x, y) \in E \text{ o } (y, x) \in E\}.$$

El grafo $sym(G)$ es llamado la **simetrización** del grafo G.

Proposición
Un grafo dirigido es Eureliano si y sólo si su simetrización es conexo y $deg_G^+(v) = deg_G^-(v)$, $\forall v \in V(G)$.

Aplicación:
Una rueda tiene una secuencia de n dígitos 0 y 1 escritos a lo largo de su circunferencia. Podemos leer k dígitos consecutivos a través de un espacio:



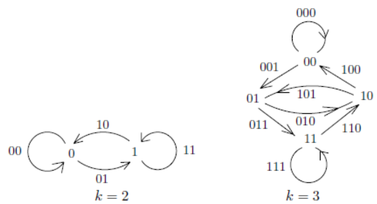
Continua la aplicación

La secuencia de n dígitos debe ser tal que la posición de la rueda siempre se puede detectar desde los k dígitos en la ranura, no importa cómo se gire la rueda. Analicemos el siguiente problema
Problema: Encuentre una secuencia cíclica de dígitos 0 y 1 de mayor longitud tal que no coincidan dos k-uplas de dígitos consecutivos (aquí una secuencia cíclica significa colocar los dígitos en la alrededor de un círculo).

Proposición

Sea $\ell(k)$ el número máximo posible de dígitos en tal secuencia para un k dado. Para cada $k \geq 1$ se tiene que $\ell(k) = 2^k$.

Ejemplo: Para $k = 2$, se puede encontrar un recorrido $00, 01, 11, 10$ y la correspondiente secuencia cíclica es 0011 y para $k = 3$ se tiene el recorrido $000, 001, 011, 111, 110, 101, 010, 100$ y la correspondiente secuencia cíclica es 00011101 como muestra el grafo dirigido siguiente:



Grafos 2-conexo

Ronald Mas,
Angel Ramirez

10 de julio de 2020

Contenido

2-Conectividad

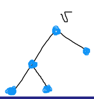
Definición

Un grafo G se llama k-vértice conexo si tiene como mínimo $k+1$ vértices y permanece conexo después de suprimir cualquier conjunto de $k-1$ vértices.

Observaciones:

- Diremos que un grafo G es 2-conexo en vez de decir que un grafo G es 2-vértice conexo.
- Es decir, un grafo G se llama 2-conexo si tiene como mínimo 3 vértices y al suprimir cualquier vértice se tiene un grafo conexo.
- Un grafo 2- conexo es también conexo.

Ejemplo: El siguiente grafo no es 2-conexo ya que el suprimir el vértice v se genera un grafo no conexo.



Operaciones en grafos

Definición

Sea $G = (V, E)$ un grafo. Definamos algunas operaciones en grafos:

1) Eliminación de una arista:

$$G - e = (V, E \setminus \{e\}),$$

donde $e \in E(G)$.

2) Adición de una nueva arista:

$$G + \overline{e} = (V, E \cup \{\overline{e}\}),$$

donde $\overline{e} \in \binom{V}{2} \setminus E$.

Continua las Operaciones en grafos

Definición

3) Eliminación de un vértice:

$$G - v = (V \setminus \{v\}, \{e \in E : \ v \notin e\}),$$

donde $v \in V(G)$ (al eliminar el vértice se eliminan también todas las aristas que lo contienen).

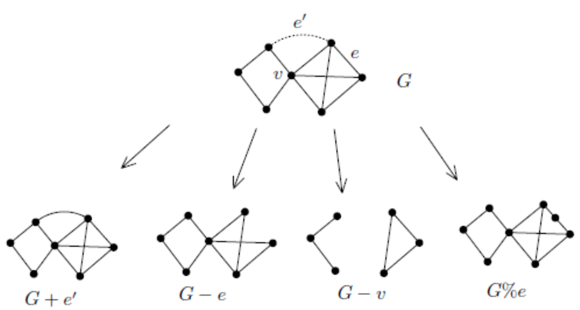
4) Subdivisión de una arista:

$$G\,\%e = (V \cup \{z\}, (E \setminus \{\{x, y\}\}) \cup \{\{x, z\}, \{z, y\}\})$$

donde $e = \{x, y\} \in E(G)$ y $z \notin V(G)$ es un nuevo vértice (se coloca un nuevo vértice z en la arista $\{x, y\}$).

Ejemplos:

Dado un grafo $G = (V, E)$ veamos algunas operaciones:



Teorema

Un grafo G es 2-conexo si y sólo si para cualquier par de vértices de G existe un ciclo en G conteniendo estos dos vértices.

Prueba:

$\Leftarrow$) Como cualquier par de vértices $v, v' \in V(G)$ pertenecen a un ciclo en común entonces existen dos caminos que no contienen vértices comunes excepto los vértices finales y así v y v' no caen en distintos componentes al eliminar un solo vértice.

$\Rightarrow$) Ejercicio.

Proposición

Un grafo G es 2-conexo si y sólo si cualquier subdivisión de G es 2-conexo.

Prueba:

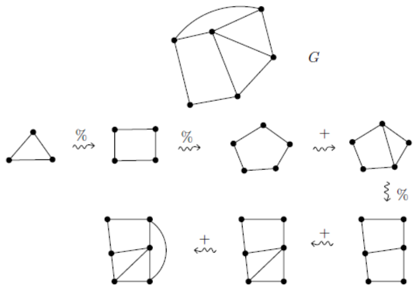
Es suficiente probar que, para todo $e \in E(G)$, G es 2-conexo si y sólo si $G\,\%e$ es 2-conexo. Veamos sólo la vuelta, si $v \in V(G)$ entonces $G - v$ es conexo si y sólo si $(G\,\%e) - v$ es conexo, por tanto si $G\,\%$ es 2-conexo entonces G también es 2-conexo.

Caracterización de grafos 2-conexo

Teorema

Un grafo G es 2-conexo si y sólo si este puede ser creado de un triángulo (K_3) por una secuencia de subdivisiones y adición de aristas.

Ejemplo: Veamos como generar el grafo G.



Grafos libres de triángulos

Sea G un grafo simple con $\mid V(G) \mid= n$, si $\mid E(G) \mid= k$ entonces

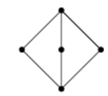
$$0 \leq k \leq \binom{n}{2}.$$

Es bien sabido que todo grafo simple con n vértices es isomorfo a K_n, analicemos la siguiente interrogante:
¿ Cuántas aristas como máximo puede tener un grafo simple G con n vértices libre de triángulos?

Casos particulares

Sea $T(n)$ el número máximo de aristas que puede tener un grafo G libre de triángulos con n vértices. Luego se tiene que:

- $T(1) = 0$.
- $T(2) = 1$.
- $T(3) = 2$.
- $T(4) = 4$, $(G \simeq C_4)$.
- $T(5) = 6$. En efecto como muestra el dibujo:



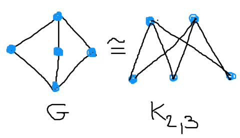
Teorema

Para todo número natural n se tiene que $T(n) = [\![\frac{n^2}{4}]\!]$.

Teorema

Para todo número natural n cada grafo libre de triángulo con la máxima cantidad de aristas es isomorfo a el grafo $K_{a,b}$ con $a = [\![\frac{n}{2}]\!]$ y $b = n - [\![\frac{n}{2}]\!]$

Ejemplo: Para un grafo $G = (V, E)$ libre de triángulos con $\mid V(G) \mid= n = 5$ se tiene que $a = 2$ y $b = 3$, por tanto:



Teorema

Sea $G = (V, E)$ un grafo libre de triángulos. Entonces existe una partición de V en dos subconjuntos X y Y tal que para todo vértice $x \in V$ se tiene que $deg_G(x) \leq deg_{K_{|X|,|Y|}}(x)$.

Este teorema permite probar de manera rápida que

$$T(n) = [\![\frac{n^2}{4}]\!].$$

En efecto, si $\mid X \mid= a$ y $\mid Y \mid= b$ se tiene por el teorema anterior que:

$$\mid E(G) \mid\leq\mid E(K_{a,b}) \mid$$

con $a + b = n$, luego como deseamos maximizar $a.b$ se tiene:
$a.b = a(n - a) = -a^2 + an$, es decir el máximo valor del producto e obtiene cuando $a = \frac{n}{2}$. Luego

$$\mid E(G) \mid\leq \frac{n^2}{4}.$$

Por tanto $T(n) = [\![\frac{n^2}{4}]\!]$.

ÁRBOLES.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

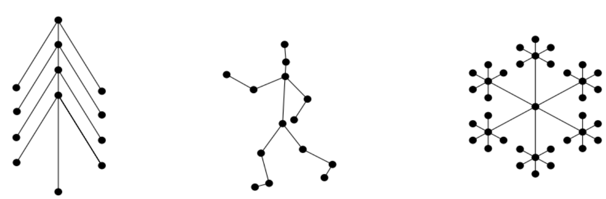
[1]Universidad Nacional de Ingeniería, Lima, Perú

6 de julio de 2020

Tabla de contenidos

Definición 1

*Un **árbol** es un grafo conexo que no contiene ciclos.*



Caracterización de árboles

Teorema 1

Las siguientes condiciones son equivalentes para grafo $G = (V, E)$:

1. *G es un árbol.*
2. **(Unicidad de camino simple).** *Para todo par de vértices $x, y \in V$ existe un único camino simple que los une.*
3. **(Mínimo grafo conexo).** *El grafo G es conexo y si borramos cualquiera de sus aristas resulta un grafo disconexo.*
4. **(Máximo grafo sin ciclos).** *El grafo G no tiene ciclos, y cualquier grafo que se obtiene de G aumentando una arista (es decir, un grafo de la forma $G + e$ donde $e \in \binom{V}{2} \setminus \{E\}$) tiene un ciclo.*
5. **(Fórmula de Euler).** *G es conexo y además $|V| = |E| + 1$.*

Antes de demostrar el teorema anterior, vamos a dar una definición previa y auxiliarnos de dos lemas que se dan a continuación.

Definición 2

Un vértice de G de grado uno es llamado **vértice final** *o también que es una* **hoja** *de G.*

Lemma 1

Cada árbol con al menos 2 vértices contiene al menos 2 vértices finales.

Lemma 2

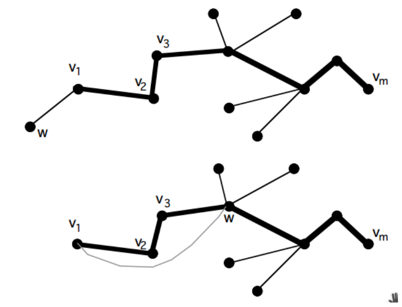
Las siguientes proposiciones son equivalentes para un grafo G y su vértice final v:

1. *G es un árbol.*
2. *$G - \{v\}$ es un árbol.*

Demostración del Lema 1

Sea $P = (v_0, e_1, v_1, \dots, e_t, v_t)$ un camino simple de máxima longitud en un árbol $T = (V, E)$. Desde que el árbol tiene al menos dos hojas, entonces la longitud de P es al menos 1, por tanto $v_0 \neq v_t$.
Afirmamos que v_0 y v_t son hojas.
Procedamos por contradicción:
Si, por ejemplo, v_0 no es una hoja, entonces existe una arista $e = \{v_0, v\}$ que contiene a v_0 y diferente de la primera arista $e_1 = \{v_0, t_t\}$ del camino simple P. Entonces o v es uno de los vértices de P, es decir $v = v_i$ $i \geq 2$ (en este caso, la arista e junto con la porción de P de v_0 a v_t forman un ciclo) $v \in \{v_0, \dots, v_t\}$ en cuyo caso estamos extendiendo P al añadir una arista e. En ambos casos se observa que llegamos a una contradicción.

Demostración del Lema 1 (cont.)



Demostración del Lema 2

- ($\Rightarrow$): Sean $x, y \in G \backslash \{v\}$. Desde que G es conexo entonces x e y están unidos por un camino simple en G. Este camino no puede contener un vértice de grado 1 diferente de x e y, y así no contiene a v. Por tanto, el camino simple está contenido en $G \backslash \{v\}$, es decir, $G \backslash \{v\}$ es conexo. Además, como G no contiene ciclos, entonces $G \backslash \{v\}$ tampoco tiene ciclos, y así, $G \backslash \{v\}$ es un árbol.
- ($\Leftarrow$): Al retornar la hoja v no se crea ciclo. G es conexo: Sean x, y vértices de G distintos de v. De la hipótesis x e y están unidos por un camino simple en G. Y un camino de v hacia cualquier otro vértice x se obtiene considerando el vecino $v' \in G \backslash \{v\}$, que está unido a x mediante un camino en $G \backslash \{v\}$ y luego extendemos este camino añadiendo la arista $\{v', v\}$.

Demostración del Teorema 1

- Veamos que $(i) \Leftrightarrow (ii)$. Sea G un grafo tal que existe un único camino simple entre cualquier par de vértices de G, esto implica que G es conexo. Afirmamos que G no tiene ciclos. Si G tiene un ciclo, digamos entre los vértices u y v, entonces existen dos caminos simples distintos que unen a u y v, lo cual es una contradicción. Por tanto, G es conexo y sin ciclos, entonces es un árbol.
Inversamente, sea G un árbol. Desde que G es conexo, existe al menos un camino simple entre cualquier par de vértices en G. Falta demostrar la unicidad del camino simple. Considere dos caminos simples entre dos vértices u y v de G. La unión de estos dos caminos forman un ciclo lo cual contradice el hecho de que G es un árbol.

Demostración del Teorema 1 (cont.)

- Veamos que $(iii) \Rightarrow (i)$. Como G es un grafo mínimo conexo entonces no tiene ciclos. Por tanto es un árbol.
Veamos que $(i) \Rightarrow (iii)$. Sea G un árbol, entonces G no tiene ciclos y así, si borramos cualquier arista de G se obtiene un grafo disconexo. Por tanto, G es un grafo mínimo conexo.

Demostración del Teorema 1 (cont.)

- Veamos que $(i) \Rightarrow (iv)$. Dados dos vértices u, v en G, como G es conexo entonces existe un camino simple en G que une a u y v. Si agregamos la arista $\{u, v\}$ se obtiene un ciclo, contradiciendo el hecho de que G es un árbol.
- Veamos que $(iv) \Rightarrow (i)$. Resta probar que G es conexo. Sean $x, y \in V(G)$, luego, o ellos están unidos por una arista o el grafo $G + \{x, y\}$ contiene un ciclo, y removiendo la arista $\{x, y\}$ de este ciclo se obtiene un camino simple desde x a y en G.

Demostración del Teorema 1 (cont.)

- Veamos que $(i) \Rightarrow (v)$. Usamos inducción sobre $|V| = n$. El resultado es directo para $n = 1$. Asumamos que es verdad para árboles con cantidad de vértices menores a n. Considere el árbol G con n vértices y sea e una arista con extremos u y v. Si eliminamos la arista e se obtiene exactamente dos componentes conexas en G, digamos G_1 y G_2, observe que estas componentes no contienen ciclos, así cada componente es un árbol. Sean n_1 y n_2 el número de vértices en G_1 y G_2 respectivamente, es decir, $n_1 + n_2 = n$. Observe que $n_1 < n$ y $n_2 < n$, así, por hipótesis de inducción. el número de aristas en G_1 y G_2 son respectivamente $n_1 - 1$ y $n_2 - 1$. Por tanto, el número de aristas en G es:

$$|E| = n_1 - 1 + n_2 - 1 + 1 = (n_1 + n_2) - 1 = n - 1 \Rightarrow |V| = n = |E| + 1.$$

Demostración del Teorema 1 (cont.)

Veamos que $(v) \Rightarrow (i)$. Usamos inducción sobre $|V|$. Hipótesis inductiva: Todo grafo G conexo con $|V| = n - 1$ vértices tal que $|V| = |E| + 1$ es un árbol. Veamos para un grafo conexo G con $|V| = n + 1$ vértices y $|V| = n = |E| + 1$. Como $n \geq 2$ entonces $|V| = |E| + 1 \geq 2$.
Por teorema de la suma de los grados se obtiene:

$$\sum_{v \in V(G)} deg_G(v) = 2|E| = 2(|V| - 1) = 2|V| - 2$$

Si $deg_G(v) > 2$ para todo $v \in V(G)$ entonces $\sum_{v \in V(G)} deg_G(v) > 2|V|$ contradiciendo el resultado anterior.
Por tanto $deg_G(v) \leq 2$.

Demostración del Teorema 1 (cont.)

Como G es conexo entonces $deg_G(v) \geq 1$ y así $1 \leq deg_G(v) \leq 2$.
Si $deg_G(v) = 2$ para todo $v \in V(G)$ se llega a una contradicción. Por tanto, debe existe al menos un vértice $v \in V(G)$ tal que $deg_G(v) = 1$, es decir, una hoja de G.
Considerando el grafo $G' = G \backslash \{v\}$ es otra vez conexo tal que $|V(G')| = n - 1$ y además $|V(G')| = |E(G')| + 1$, entonces por la hipótesis inductiva G' es un árbol y por el Lema 2 se concluye que G es un árbol.

Tabla de contenidos

Definición 3 (Árbol con raíz)

Es un par (T, r) donde T es un árbol y $r \in V(T)$ es un vértice distinguido de T llamado **raíz**. *Si $\{x, y\} \in E(T)$ es una arista y el vértice x está en el único camino simple que une y a la raíz, decimos que x* **es padre** *de y (en el árbol con raíz) e y es llamado* **hijo** *de x.*

Definición 4 (Árbol plantado)

Es un **árbol con raíz** (T, r) *mas un gráfico de T en el plano. En el gráfico, la* **raíz** *es señalada mediante una flecha apuntando hacia abajo y los hijos de cada vértice son ubicados arriba del vértice respectivo.*

Isomorfismos

Definición 5

Una función $f : V(T) \to V(T')$ es un **isomorfismo de árboles** *T y T' si f es una biyección que satisface $\{x, y\} \in E(T)$ si sólo si $\{f(x), f(y)\} \in E(T')$. Este isomorfismo es denotado por $T \cong T'$.*

Definición 6

Un **isomorfismo de árboles con raíz** *(T, r) y (T', r') es un isomorfismo f de los árboles T y T' y que además se cumple $f(r) = r'$. Este isomorfismo es denotado por $T \cong' T'$.*

Definición 7

Un **isomorfismo de árboles plantados** *es un isomorfismo de árboles con raíz que preservan el orden de izquierda a derecha de los hijos de cada vértice. Este isomorfismo es denotado por $T \cong'' T'$.*

Representación gráfica. Ejemplo 1

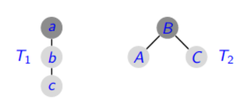


Figura 1: Isomorfos como grafos.

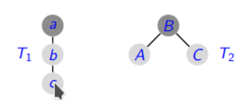
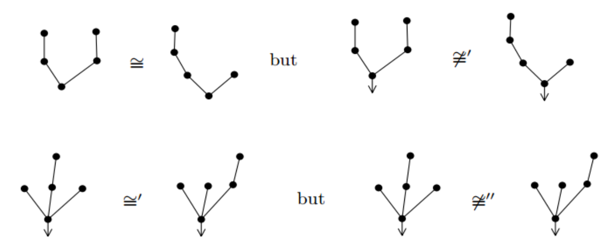


Figura 2: No son isomorfos como árboles con raíz.

Representación gráfica. Ejemplo 2

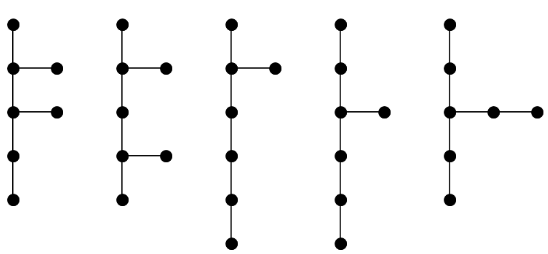


La definición de **árboles plantados** es más restrictiva y por tanto hace más fácil su codificación.

Ejemplo:

Draw all possible 7-vertex trees with maximun degree 3.

Solución:
La secuencia de grados pueden ser (3,3,2,1,1,1,1) o (3,2,2,2,1,1,1).
Por tanto, los árboles pueden ser:



CODIFICACIÓN DE ÁRBOLES.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

6 de julio de 2020

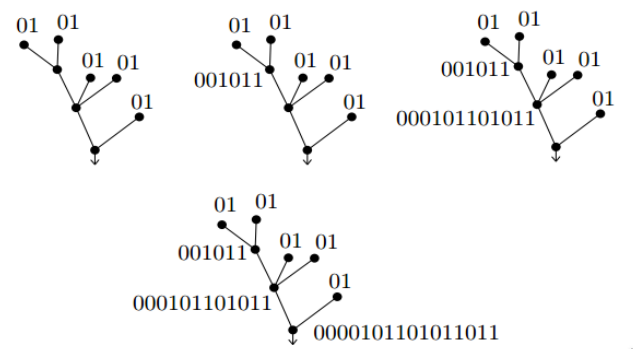
Tabla de contenidos

Codificación de árboles plantados

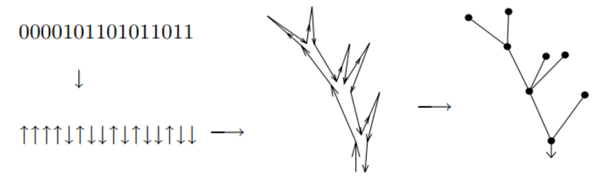
Se sigue los siguientes pasos:

1. Cada vértice distinto de la raíz se le asigna el código 01.
2. Sea v un vértice con hijos $v_1, v_2, \ldots, v_t$ (escritos en el orden de izquierda a derecha). Si A_i es el código del hijo v_i entonces el vértice v recibe el código $0A_1A_2\ldots A_t1$.

Codificación de árboles plantados (cont.)



Decodificando códigos



Codificando árboles con raíz

Para árboles con raíz (T, r) se tiene un código similar usando el método para árboles plantados, para esto cambiamos la segunda regla para árboles plantados por la siguiente regla:

2) Suponga que cada hijo w de un vértice v le sido asignado el código $A(w)$. Denotemos los hijos de v mediante $w_1, w_2, \ldots, w_t$ y además $A(w_1) \leq A(w_2) \leq \ldots A(w_t)$. Luego, el vértice v recibe el código: $0A_1A_2\ldots A_t1$, donde $A_i = A(w_i)$

¿Qué significa $A \leq B$ en el código anterior?

Para dos secuencias A y B se entiende por $A \leq B$ que A es menor o igual que B en algún ordenamiento lineal fijo de todas las secuencias finitas de ceros y unos. Por definición, podemos usar el llamado **ordenamiento lexicográfico**. Dos secuencias distintas $A = (a_1, a_2, \ldots, a_n)$ y $B = (b_1, b_2, \ldots, b_m)$ son comparados como sigue:

1. Si A es un segmento inicial de B entonces $A < B$. Si B es un segmento inicial de A entonces $B < A$. Por ejemplo: $0010 < 00100$ y $0 < 0111$.
2. En otro caso, sea j el menor índice tal que $a_j \neq b_j$. Entonces, si $a_j < b_j$ decimos que $A < B$, y si $a_j > b_j$ entonces decimos que $A > B$. Por ejemplo: $011 < 1$ y $10011 < 10110$.

Excentricidad de un vértice

Para un vértice v de un grafo, el símbolo $ex_G(v)$ denota el máximo de las distancias de v hacia los otros vértices.
El número $ex_G(v)$ es llamado **excentricidad** del vértice v en el grafo G. Se puede entender que los vértices con excentricidad grande permanecen sobre la periferie de G.

Centro de un grafo

$C(G)$ denota el conjunto de todos los vértices de G con **excentricidad mínima**. El conjunto $C(G)$ es llamado el **centro** de G.
El ejemplo de un ciclo (así como muchos otros grafos) muestra que algunas veces el centro puede coincidir con todo el conjunto de vértices.

Para árboles tenemos el siguiente resultado:

Proposición 1

Para cualquier árbol T, $C(T)$ tiene al menos 2 vértices. Si $C(T)$ consiste de dos vértices x e y entonces $\{x, y\}$ es una arista.

Demostración: Describimos a continuación un procedimiento para determinar el centro de un árbol. Sea $T(V, E)$ un árbol dado. Si T tiene a lo más 2 vértices, entonces su centro coincide con el conjunto de vértices y la proposición se cumple. En otro caso, sea $T' = (V', E')$ el árbol que se obtiene de T después de remover todas sus hojas, es decir:

$$V' = \{x \in V \,/\, deg_T(x) > 1\},$$

$$E' = \{\{x, y\} \in E \,/\, deg_T(x) > 1 \quad \text{y} \quad deg_T(y) > 1\}$$

Observe que $V(T') \neq \emptyset$, desde que no todos los vértices de T pueden ser hojas. Además, para cualquier vértice v, los vértices más distantes de v son necesariamente las hojas, y por tanto, para cada $v \in V'$ se obtiene:

$$ex_T(v) = ex_{T'}(v) + 1.$$

En particular, se obtiene $C(T') = C(T)$. Si T' tiene por lo menos 3 vértices, repetimos la construcción descrita, en otro caso, hemos encontrado el centro de T.

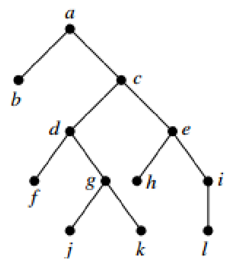
Código de un árbol

1. Si el centro de T es un único vértice, entonces definimos el código de T como el código del árbol con raíz (T, v).
2. Si el centro de T consiste de una arista $e = \{x_1, x_2\}$, consideramos el grafo $T - e$. Este grafo tiene exactamente dos componentes T_1 y T_2; la notación es elegida de tal modo que $x_i \in V(T_i)$. Considere: la letra A denota el código del árbol con raíz (T_1, x_1) y la letra B denota el código del árbol con raíz (T_2, x_2). Si $A \leq B$ según el **ordenamiento lexicográfico**, el árbol T es codificado por el código del árbol con raíz (T, x_1) y para $A \geq B$ su código es el código de (T, x_2).

Lo descrito permite codificar un árbol.

Ejemplo:

Find every vertex that is a center in the given tree:



Ejemplo:

A tree T has 17 nodes and the degree of each node is either 1 or 4. After Alice added some edges to this graph, it has an Eulerian circuit. At least how many edges did she add?

Solution:
Let k be the number of nodes with degree 4. The tree has 16 edges, so the sum of the degrees is

$$\sum_{v \in V} deg_T(v) = 4k + (17 - k) = 32.$$

We get that $k = 5$. The tree has nodes with odd degree. By adding 6 edges, Alice can achieve that every degree of the graph is even, thus it contains an Eulerian circuit.

Ejemplo:

a) How many nonisomorphic unrooted trees are there with 4 vertices?
b) How many nonisomorphic rooted trees are there with 4 vertices?

Solution:

a) There are 2 non isomorphic unrooted trees with 4 vertices: the 4 chain and the tree with one trivalent vertex and three pendant vertices.
b) There are 4 non isomorphic rooted trees with 4 vertices, since we can pick a root in two distinct ways from each of the two trees in **(a)**.

Ejemplo:

Prove that every tree with at least two vertices is a bipartite graph.

Solution:
Choose a root for the treee T. Then, let X consist of the vertices of even level, and let Y be the vertices of odd level. Then, T is bipartite on X and Y.

Árbol de expansión de un grafo

Ronald Mas,
Angel Ramirez

20 de julio de 2020

Contenido

Árbol de expansión de un grafo

Definición

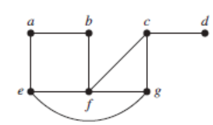
Sea $G = (V, E)$ un grafo. Un árbol arbitrario de la forma $T = (V, E')$, donde $E' \subseteq E$ es llamado un árbol de expansión del grafo G. Es decir un árbol de expansión es un subgrafo de G que es un árbol y contiene todos los vértices de G.

Observaciones:

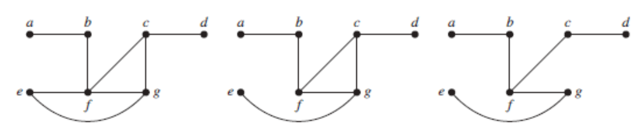
- Si G es un grafo no conexo entonces no existe un árbol de expansión para G.
- Todo grafo G conexo posee un árbol de expansión.

Ejemplo

Sea el grafo simple $G = (V, E)$:



El dibujo muestra un árbol de expansión que resulta al suprimir ciertas aristas del grafo G:



Aristas suprimidas: $\{a, e\}$ $\{e, f\}$ $\{c, g\}$

Algoritmo:(Árbol de expansión)

Algoritmo:(Árbol de expansión) Sea $G = (V, E)$ un grafo con $|V(G)| = n$, $|E(G)| = m$ y secuencia de grados $(e_1, e_2, \cdots, e_m)$. El algoritmo construye sucesivamente conjuntos de aristas $E_0, E_1, \cdots \subseteq E$. Sea $E_0 = \emptyset$, si el conjunto E_{i-1} fue encontrado entonces el conjunto E_i es calculado como:

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\} & \text{, si el grafo } (V, E_{i-1} \cup \{e_i\}) \text{ no tiene ciclos} \\ E_{i-1} & \text{caso contrario} \end{cases}$$

El algoritmo se detiene si E_i posee $n-1$ aristas o $i = m$. Es decir todas las aristas del grafo G han sido considerados. Denotemos por E_t el conjunto para los cuáles el algoritmo se detiene y sea $T = (V, E_t)$.

Proposición

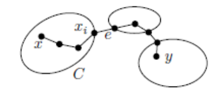
1) *Si el algoritmo anterior produce un árbol T con $n-1$ aristas entonces T es un árbol de expansión de G.*
2) *Si el algoritmo anterior produce un árbol T que tiene $k < n-1$ aristas entonces G es un grafo disconexo con $n-k$ componentes.*

Prueba:

1) Según la forma en que los conjuntos E_i fueron creados, el grafo G no tiene ciclos, si $k = |E(T)| = n-1$ entonces T es un árbol y por tanto éste es un árbol de expansión del grafo G.
2) Si $k < n-1$ entonces T es un grafo disconexo tal que cada componente es un árbol (éste es llamado un bosque). Veamos que el conjunto de vértices de las componentes del grafo T coincide con el conjunto de vértices de las componentes del grafo G.

Continua prueba:

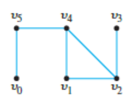
Procedamos por contradicción, supongamos que no es cierto y sean x y y vértices que pertenecen a la misma componente de G pero en distintas componentes de T, denotemos por C la componente de T conteniendo al vértice x y sea el camino $(x = x_0, e_1, x_1, e_2, \cdots, e_l, x_l = y)$ de x hacia y en el grafo G, como muestra la figura:



Sea i el último índice tal que x_i este contenido en la componente C, entonces $i < l$ y por tanto $x_{i+1} \notin C$. La arista $e = \{x_i, x_{i+1}\}$ por tanto no pertenece al grafo T, así éste tuvo que formar un ciclo con algunas de las aristas seleccionadas en T en alguna etapa del algoritmo. Por tanto el grafo $T + e$ también contiene un ciclo, pero esto es imposible ya que e conecta dos componentes distintas de T.

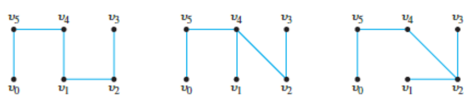
Ejemplo

Sea el grafo $G = (V, E)$:



G

Los árboles de expansión del grafo G son:



Árboles de expansión de G

EL problema del árbol de expansión mínima

Introducción:
Imagine un mapa de su región favorita de campo con unos 30 o 40 pueblos. Algunos pares de aldeas están conectadas por caminos de grava. La municipalidad decide modernizar algunas de estas carreteras adecuadas para la conducción rápida de automóviles, pero quiere invertir la menor cantidad de dinero posible con la condición de que sea posible viajar entre dos pueblos a lo largo de una carretera. De esta manera se consigue un problema fundamental llamado árbol de expansión mínimal. Esta sección está dedicada a su solución.

Definición

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

1) Para cada arista $e \in E(G)$ asignemos un número real no negativo $w(e)$ llamado el peso de la arista e
2) El grafo G junto con una función de peso $w : E \to \mathbb{R}$ es llamada una red o malla.

Observaciones:

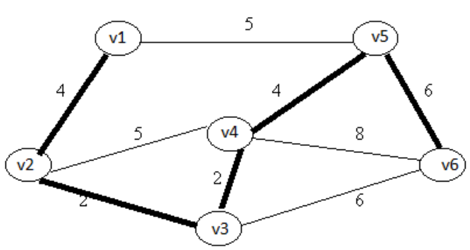
- El problema a tratar se reformula matemáticamente, dado un grafo $G = (V, E)$ con función peso no negativa w en las aristas, encontrar un subgrafo conexo de expansión (V', E') tal que la suma

$$w(E') = \sum_{e \in E'} w(e)$$

posea el mínimo valor posible.

Ejemplo

La siguiente red muestra un árbol de expansión mínima T que con $V(T) = \{v_1, v_2, v_3, v_4, v_5\}$ y $E(T) = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}\}$



Es decir $w(T) = 4 + 2 + 2 + 4 + 6 = 18$.

Árbol de expansión de un grafo

Ronald Mas,
Angel Ramirez

11 de junio de 2021

Contenido

Algoritmo de Kruskal

La entrada es un grafo conexo $G = (V, E)$ con función de peso w para las aristas. Sea las aristas $e_1, e_1, \cdots, e_m$ tal que:

$$w(e_1) \leq w(e_2) \leq \cdots \leq w(e_n).$$

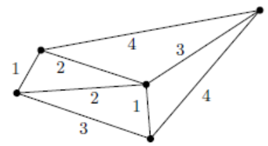
Para el ordenamiento de aristas ejecutar el algoritmo de expansión:

1) Se crea un bosque B (un conjunto de árboles), donde cada vértice del grafo es un árbol separado.
2) Se crea un conjunto C que contenga a todas las aristas del grafo.
3) Mientras C es no vacío, suprimir una arista de peso mínimo de C.
4) Si esa arista conecta dos árboles diferentes se añade al bosque, combinando los dos árboles en un solo árbol.
5) En caso contrario, se desecha la arista.

Al acabar el algoritmo, el bosque tiene un solo componente, el cual forma un árbol de expansión mínimo del grafo.

Ejemplo

Dada la siguiente red o malla:



Una posible ejecución del algoritmo de Kruskal se muestra en el siguiente diagrama:

Proposición

El algoritmo de Kruskal resuelve el problema de árbol expansión mínima.

Prueba:
Sea T un árbol de expansión encontrado por el algoritmo y sea $\check{T}$ otro árbol de expansión del grafo $G = (V, E)$. Por demostrar que $w(E(T)) \leq w(E(\check{T}))$. Denotemos las aristas de T por $e'_1, e'_2, \cdots, e'_{n-1}$ tal que $w(e'_1) \leq w(e'_2) \leq \cdots \leq w(e'_{n-1})$ (la arista $e_i = e_j$ para algún j). De igual modo, sea $\check{e}_1, \cdots, \check{e}_{n-1}$ las aristas de $\check{T}$ ordenados en orden creciente por pesos. Vamos a probar que para $i = 1, \cdots, n-1$ se tiene que:

$$w(e'_i) \leq w(\check{e}_i).$$

Esto prueba que T es un árbol de expansión mínima, procedamos por contradicción supongamos que la desigualdad anterior no se cumple, entonces $w(e'_i) > w(\check{e}_i)$.

Continua prueba

Al considerar los conjuntos

$$\begin{aligned} E' &= \{e'_1, e'_2, \cdots, e'_{i-1}\}, \\ \check{E} &= \{\check{e}_1, \check{e}_2, \cdots, \check{e}_i\}. \end{aligned}$$

Los grafos (V, E') y $(V, \check{E})$ no contienen ciclos y $|E'| = i-1$, $|\check{E}| = i$. Para llegar a una contradicción es suficiente probar que existe una arista $e \in \check{E}$ tal que el grafo $(V, E' \cup \{e\})$ no contiene ciclos, así obtenemos que $w(e) \leq w(\check{e}_i) < w(e'_i)$ y esto significa que al elegir la arista e en el algoritmo nosotros cometimos un error, pero no hay necesidad de eliminar la arista e ya que podemos seleccionar a e'_i en su reemplazo. Por tanto, es suficiente probar que, si $E', E \subseteq \binom{V}{2}$ son dos conjuntos de aristas tal que el grafo $(V, \check{E})$ no tiene ciclos y $|E'| < |\check{E}|$, entonces alguna arista $e \in \check{E}$ conecta vértices de componentes distintas del grafo V, E'.

Continua prueba

Esto se puede hacer mediante un simple argumento de conteo. Sea $V_1, \cdots V_s$ los conjuntos de vértices de las componentes del grafo (V, E'), luego se tiene que:

$$|E' \cap \binom{V_j}{2}| \geq |V_j| - 1,$$

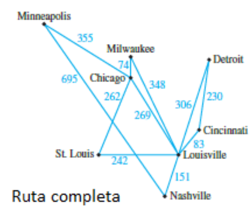
y al sumar estas desigualdades sobre j se tiene que $E' \geq n - s$. Por otro lado, como $\check{E}$ no tiene ciclos, se tiene:

$$|\check{E} \cap \binom{V_j}{2}| \leq |V_j| - 1,$$

y por lo tanto a lo más $n - s$ aristas de $\check{E}$ estan contenidos en alguna de las componentes V_j, pero como asumimos que $|\check{E}| > |E'|$, existiría una arista $e \in \check{E}$ que pertenece a dos componentes distintas.

El camino mas corto

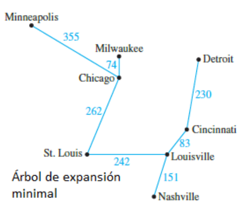
Aunque los árboles producidos por el algoritmo de Kruskal tiene el menor peso posible total en comparación con todos los demás árboles de expansión para los grafos dados, no siempre muestra la distancia más corta entre dos puntos en el grafo. Por ejemplo la siguiente red muestra la ruta completa de viajes entre ciudades con sus respectivas distancias en millas



Ruta completa

Continua

Se puede probar que al aplicacar del algoritmo de Kruskal en la red anterior se tiene el siguiente árbol de expansión minimal:



Árbol de expansión minimal

De acuerdo con el sistema de ruta completo, se puede volar directamente de Nashville a Minneapolis por una distancia de 695 millas, mientras que si usa el árbol de expansión mínimal la única forma de volar desde Nashville a Minneapolis es pasando por Louisville, St. Louis y Chicago, lo que da distancia total de 151+242+262+355=1 010 millas.

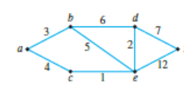
Algoritmo de Dijkstra

ALGORITHM 1 Dijkstra's Algorithm.

procedure *Dijkstra*(G: weighted connected simple graph, with all weights positive)
{G has vertices $a = v_0, v_1, \ldots, v_n = z$ and lengths $w(v_i, v_j)$ where $w(v_i, v_j) = \infty$ if $\{v_i, v_j\}$ is not an edge in G}
for $i := 1$ **to** n
    $L(v_i) := \infty$
$L(a) := 0$
$S := \emptyset$
{the labels are now initialized so that the label of a is 0 and all other labels are ∞, and S is the empty set}
while $z \notin S$
    $u :=$ a vertex not in S with $L(u)$ minimal
    $S := S \cup \{u\}$
    for all vertices v not in S
        if $L(u) + w(u, v) < L(v)$ **then** $L(v) := L(u) + w(u, v)$
        {this adds a vertex to S with minimal label and updates the labels of vertices not in S}
return $L(z)$ {$L(z) =$ length of a shortest path from a to z}

Ejemplo:

Dada la red



Veamos los pasos en la ejecución del algoritmo de Dijkstra para hallar la ruta más corta de a hacia z.

Step	$V(T)$	$E(T)$	F	$L(a)$	$L(b)$	$L(c)$	$L(d)$	$L(e)$	$L(z)$
0	$\{a\}$	$\emptyset$	$\{a\}$	0	∞	∞	∞	∞	∞
1	$\{a\}$	$\emptyset$	$\{b, c\}$	0	3	4	∞	∞	∞
2	$\{a, b\}$	$\{\{a, b\}\}$	$\{c, d, e\}$	0	3	4	9	8	∞
3	$\{a, b, c\}$	$\{\{a, b\}, \{a, c\}\}$	$\{d, e\}$	0	3	4	9	5	∞
4	$\{a, b, c, e\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}\}$	$\{d, z\}$	0	3	4	7	5	17
5	$\{a, b, c, e, d\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}\}$	$\{z\}$	0	3	4	7	5	14
6	$\{a, b, c, e, d, z\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}, \{e, z\}\}$							

GRAFOS PLANARES.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

29 de julio de 2020

Tabla de contenidos

Definición 1 (Arco)

Es un subconjunto α del plano de la forma

$$\alpha = \gamma([0,1]) = \{\gamma(x) \,/\, x \in [0,1]\},$$

donde $\gamma : [0,1] \to \mathbb{R}^2$ es una función continua inyectiva definida en el intervalo cerrado $[0,1]$ sobr el plano. Los puntos $\gamma(0)$ y $\gamma(1)$ son llamados **extremos** *del arco α.*

Dibujo de un grafo

Definición 2

Por **dibujo** *de un grafo $G = (V, E)$ se debe entender lo siguiente: a todo vértice $v \in V(G)$ le corresponde un punto $b(v)$ del plano, y a toda arista $e = \{v, v'\} \in E(G)$ le corresponde un arco $\alpha(e)$ en el plano con* **extremos** *$b(v)$ y $b(v')$. Asumimos que el mapeo b es inyectivo (es decir, a diferentes vértices le corresponden distintos puntos en el plano), y ningún punto de la forma $b(v)$ está sobre cualquier arco $\alpha(e)$ a menos que sea un extremo del arco. Un grafo junto con algún dibujo es llamado* **grafo topológico**.

Un dibujo de un grafo G en el cual dos arcos cualesquiera correspondientes a arcos distintos o no tienen intersección o sólo comparten un extremo es llamado **dibujo planar**. Un grafo G es **planar** si tiene al menos un **dibujo planar**.

Caras de un grafo planar

Definición 3 (Conjunto conexo)

Decimos que un conjunto $A \subset \mathbb{R}^2$ es **conexo** *si para cualquier par de puntos $x, y \in A$ existe un arco $\alpha \subset A$ con extremos x e y).*

Sea $G = (V, E)$ un grafo topológico planar, es decir, un grafo planar junto con dibujo en el plano. Considere el conjunto de todos los puntos en el plano que no están en los arcos del dibujo. Este conjunto consiste de un número finito de regiones conexas. Estas regiones son llamadas **caras** del grafo topológico planar.
La región que se extiende hasta el infinito, tal como F_1 en la Figura 1, es llamada **cara exterior** (o **cara ilimitada**) del dibujo y todas las otras caras son llamadas **caras internas** (o **caras limitadas**.)

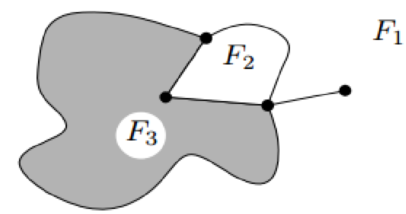
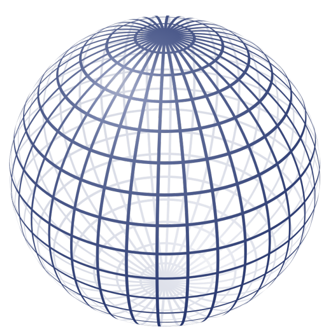


Figura 1: Caras de un grafo planar

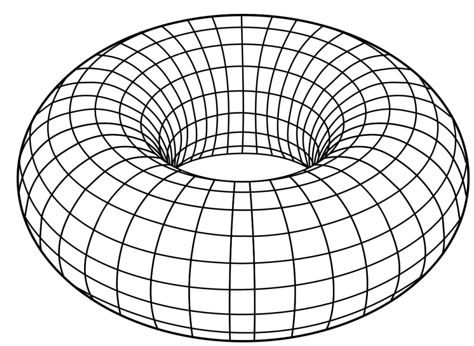
Dibujos sobre otras superficies

Un grafo puede ser también dibujado sobre otras superficies además del plano. A continuación se muestran algunas otras superficies.

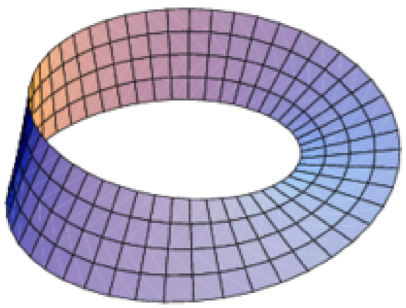
Superficie esférica



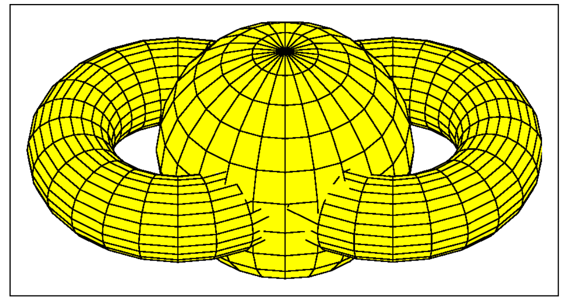
Superficie del toro



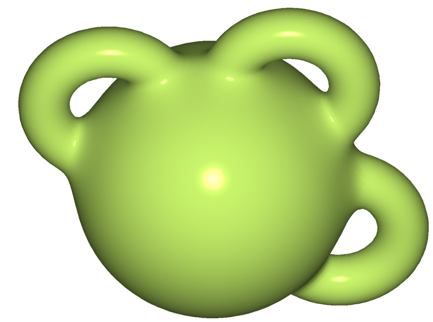
Superficie de la cinta de Mobius



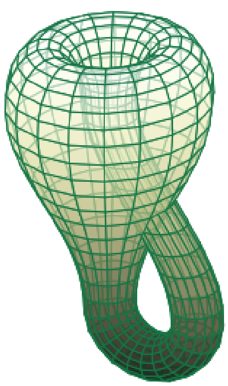
Esfera con dos asas



Esfera con tres asas



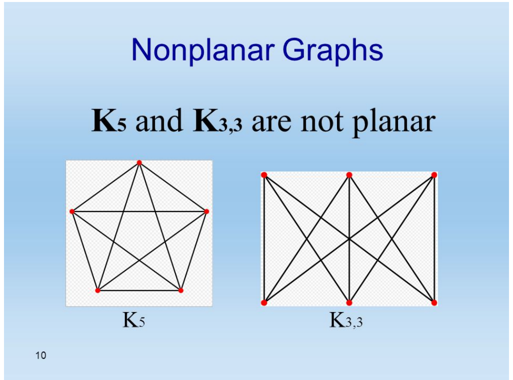
Botella de Klein



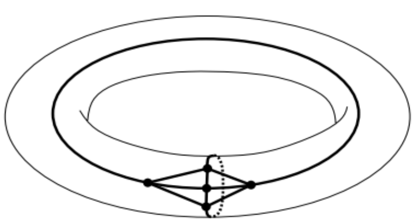
Observaciones

- Los grafos pueden ser clasificados según la superficie donde puedan ser graficados.
- Los grafos K_5 y $K_{3,3}$ no son planares.
- K_5 puede ser dibujado en el toro.

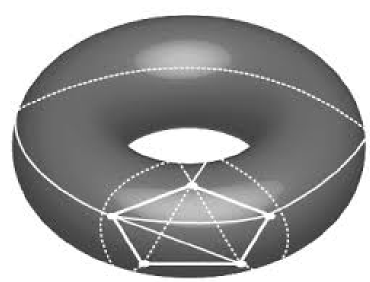
$K_{3,3}$ y K_5 no son planares.



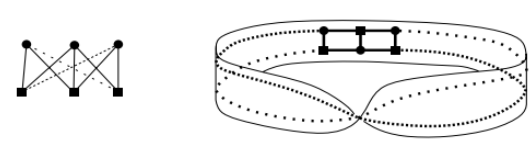
K_5 sobre el Toro



K_5 sobre el Toro



$K_{3,3}$ sobre la banda de Mobius



Proposición 1

Cualquier grafo puede ser dibujado sin intersección de aristas sobre una esfera con suficiente número de asas.

Idea de la demostración:
Dibujamos el grafo $G = (V, E)$ sobre la esfera, posiblemente con aristas intersectándose. Sean $e_1, e_2, \ldots, e_n$ las aristas que se intersectan con otra arista. Para cada arista e_i, añadimos una asa que sirve como puente para que la arista evite las otras aristas, de modo que las asas son disjuntas y así las aristas dibujadas sobre las asas no se intersectan más.
Desde que tenemos un número finito de aristas, es fácil determinar tales asas.

La idea de la demostración anterior motiva la siguiente definición.

Definición 4 (Género de un grafo planar)

El menor número de asas que deben ser añadidas a la esfera de modo que el grafo G pueda ser dibujado sobre la superficie resultante sin intersección de aristas es llamado **género** *del grafo G.*

Tabla de contenidos

Teorema de curva de Jordan

Definición 5

Una **curva de Jordan** *es una curva cerrada sin autointersecciones. Más formalmente, una* **curva de Jordan** *es definida como un arco cuyos extremos coinciden, es decir, una imagen continua del intervalo $[0, 1]$ bajo una función f inyectiva excepto en la igualdad $f(0) = f(1)$.*

Teorema 1

Cualquier curva de Jordan k divide al plano en exactamente dos regiones conexas, la parte **interior** *y* **exterior** *de k, y k es la frontera de ambas regiones. (Ambas partes serán llamadas* **las regiones de** *k).*

Proposición 2

K_5 es no planar.

Demostración:
Procedamos por contradicción. Sean b_1, b_2, b_3, b_4, b_5 los puntos correspondientes a los vértices de K_5 en algún dibujo planar. Los arcos que conectan a los puntos b_i y b_j serán denotados por $\alpha(i, j)$. Desde que b_1, b_2 y b_3 son vértices de un ciclo en el grafo K_5, los arcos $\alpha_{1,2}, \alpha_{2,3}$ y $\alpha_{3,1}$ forman una curva de Jordan k. De aquí, los puntos b_4 y b_5 o ambos están dentro o ambos están afuera de k, de otra forma, el arco $\alpha(4, 5)$ intersectaría a la curva k. Supongamos primero que b_4 está en el interior de k, como en la Figura 2.

Representación gráfica. Ejemplo 2

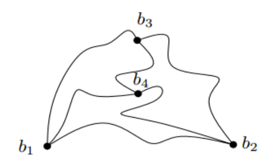


Figura 2: b_4 en el interior de la curva de Jordan

Entonces, b_5 está dentro de la curva formada por los arcos:

$$\begin{array}{lcl} \alpha(1,4), \alpha(2,4) & \text{y} & \alpha(1,2), \quad \text{o} \\ \alpha(2,3), \alpha(3,4) & \text{y} & \alpha(2,4), \quad \text{o} \\ \alpha(1,3), \alpha(3,4) & \text{y} & \alpha(1,4). \end{array}$$

Sin embargo, en el primer caso, el arco $\alpha(3, 5)$ intersecta a la curva de Jordan formada por los arcos

$$\alpha(1,4), \alpha(2,4) \quad \text{y} \quad \alpha(1,2).$$

Similarmente en los dos casos restantes.
Si los puntos b_4 y b_5 están en el exterior de k, se procede de forma análoga.

Caras y ciclos en grafos 2-conexos

Si $e_1, e_2, \ldots, e_n$ son las aristas de un ciclo en un grafo topológico planar G, entonces los arcos $\alpha(e_1), \ldots, \alpha(e_n)$ forman una curva de Jordan. Por el teorema de la curva de Jordan, se tiene que cada cara de G está en el interior o en el exterior de esta curva. Por brevedad, llamaremos a esta curva de Jordan **un ciclo** de G (así, un ciclo de G puede ahora significar o un ciclo en el sentido de grafo, es decir, un subgrafo de G, o la curva de Jordan correspondiente al ciclo de G en algún dibujo de G).

Proposición 3

Sea G un grafo planar 2-vértice conexo. Entonces toda cara en cualquier dibujo de G es una región de algún ciclo de G.

Teorema 2

Un grafo G es planar si y solamente si no tiene subgrafos isomórficos a una subdivisión de $K_{3,3}$ o a una subdivisión de K_5.

CARACTERÍSTICA DE EULER Y COLORACIÓN DE MAPAS.

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

2 de agosto de 2020

Tabla de contenidos

Fórmula de Euler

Teorema 1

Sea $G = (V, E)$ un grafo planar conexo y sea f el número de caras de algún dibujo de G. Se cumple:

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

En particular, el número de caras no depende del dibujo.

Demostración:
Se procede por inducción sobre el número de aristas del grafo G.
Si $E = \emptyset$ entonces $|V| = 1$ y $|f| = 1$, observándose que la fórmula de Euler se cumple.
Si $|E| \geq 1$, se presentan los siguientes casos:

Fórmula de Euler (cont.)

1. El grafo G no tiene ciclos. Entonces G es un árbol y así $|V| = |E| + 1$ y al mismo tiempo $f = 1$ desde que un dibujo planar de un árbol tiene solamente una cara (no limitada).
2. Alguna arista $e \in E$ está contenida en un ciclo. En este caso el grafo $G - e$ es conexo. Por tanto, por hipótesis inductiva, la fórmula de Euler se cumple (al considerar el grafo que se obtiene de G al remover la arista e). La arista e el dibujo considerado de G es adyacente a dos caras distintas F y F', por el teorema de la curva de Jordan. De aquí, ambos (el número de caras y el número de aristas) se incrementan en 1 al añadir e al dibujo, mientras que el número de vértices no varía. De aquí, la fórmula de Euler se sigue cumpliendo.

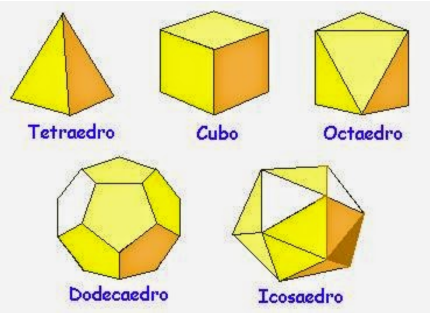
Definición 1

*Un **poliedro regular** es un cuerpo convexo tridimensional limitado por un número finito de caras. Todas las caras deben ser copias congruentes del mismo polígono convexo regular y el mismo número de caras deben intersectarse en cada vértice del cuerpo.*

Una razón del gran interés para el estudio de los poliedros regulares es su excepcionalidad. Existen solamente 5 tipos de poliedros regulares:

1. El tetraedro regular.
2. El cubo.
3. El octaedro.
4. El dodecaedro.
5. El icosaedro.

Poliedros regulares



Proposición 1

Sea G un grafo topológico planar en el cual cada vértice tiene grado d y cada cara es adyacente a k vértices, para algunos enteros $d \geq 3$ y $k \geq 3$. Entonces G es isomorfo a uno de los grafos mostrados la Figura 1

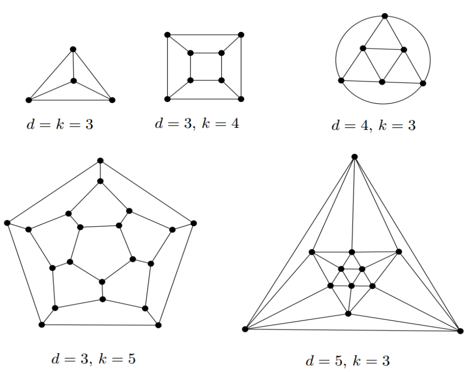


Figura 1: Grafos de los sólidos platónicos

Demostración de la Proposición 1

Sea el grafo $G = (V, E)$ tal que $|V| = n$, $|E| = m$ y el número de caras es f. Del lema de Handshaking se tiene que:

$$\sum_{v \in V} deg_G(v) = 2|E|$$

en nuestro caso implica que $dn = 2m$.
Análogamente se obtiene: $2m = kf$.
Nosotros contamos dos veces el número de los pares ordenados (e, F), donde F es una cara de G y e es una arista que está en la frontera de F. Cada arista contribuye a 2 de tales pares (como cada cara es limitada por un ciclo) y cada cara k pares.

Demostración de la Proposición 1 (cont.)

Luego, expresamos n y f en términos de m usando las relaciones anteriores para sustituirlas en la fórmula de Euler:

$$2 = n - m + f = \frac{2m}{d} - m + \frac{2m}{k}.$$

Sumando y dividiendo por $2m$, resulta:

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{2} + \frac{1}{m}.$$

De esta última ecuación, conocidos d y k, los otros parámetros n, m y f pueden ser determinados de forma única. Es claro que $\text{mín}(d, k) = 3$, en otro caso $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$.

Demostración de la Proposición 1 (cont.)

Para $d = 3$ obtenemos:

$$\frac{1}{k} - \frac{1}{6} = \frac{1}{m} > 0$$

y esto implica $k \in \{3, 4, 5\}$.
Similarmente para $k = 3$ se deduce que $d \in \{3, 4, 5\}$. De aquí una de las siguientes posibilidades deben ocurrir:

d	k	n	m	f
3	3	4	6	4
3	4	8	12	6
3	5	20	30	12
4	3	6	12	8
5	3	12	30	20

Demostración de la Proposición 1 (cont.)

De la tabla anterior es fácil observar que en cada uno de los casos el grafo está completamente determinado por los valores de d, k, n, m y f y así es isomorfo a uno de los grafos de la Figura 1.
Una propiedad muy importante de grafos planares es que ellos pueden solamente tener relativamente pocas aristas: un grafo planar con n vértices tiene $O(n)$ aristas. Una formulación más precisa lo da el siguiente el siguiente resultado.

Proposición 2

Se cumple:

1. *Sea $G = (V, E)$ un grafo planar con al menos 3 vértices. Entonces $|E| \leq 3|V| - 6$. Más aún, la igualdad se cumple para cualquier grafo planar maximal, es decir, un grafo planar tal que añadiendo cualquier nueva arista (sin variar el número de vértices) se obtiene un grafo noplanar.*
2. *Si además, el grafo planar considerado contiene un triángulo (es decir, tiene a K_3 como subgrafo) y tiene al menos 3 vértices, entonces $|E| \leq 2|V| - 4$.*

El siguiente resultado nos da más información acerca de los posibles scores de grafos planares.

Proposición 3

Sea $G = (V, E)$ un grafo planar 2-conexo con al menos 3 vértices. Sea n_i el número de sus vértices de grado i, y sea f_i el número de caras (en algún dibujo planar fijo) limitados por ciclos de longitud i. Entonces se cumple:

$$\sum_{i \geq 1} (6 - i) n_i = 12 + 2 \sum_{j \geq 3} (j - 3) f_j$$

o que es lo mismo:

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \ldots = 12 + 2f_4 + 4f_5 + 6f_6 + \ldots$$

De la proposición anterior se observa que $5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 \geq 12$, así todo grafo planar con al menos 3 vértices contiene al menos 3 vértices de grado no mayor que 5.

Demostración de la Proposición 3

Observe que:

$$|V| = \sum_i n_i, \quad f = \sum_i f_i.$$

Reemplazando estas expresiones en la fórmula de Euler, se obtiene:

$$2|E| = 2(|V| + f - 2) = \sum_i 2n_i + \sum_j 2f_j - 4.$$

Por conteo similar se obtiene las siguientes relaciones:

$$\sum_i i n_i = 2|E| = \sum_j j f_j.$$

Demostración de la Proposición 3 (cont.)

De ambas expresiones para $2|E|$, obtenemos las siguientes igualdades:

$$\sum_j (j - 2) f_j + 4 = \sum_i 2n_i, \quad \sum_j 2f_j = \sum_i (i - 2) n_i + 4.$$

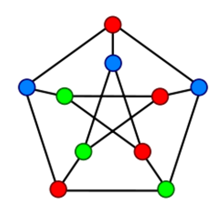
Si multiplicamos a la primera de estas igualdades por 2 para luego sustraerle la segunda, resulta:

$$\sum_i (6 - i) n_i - 4 = 2 \sum_j (j - 3) f_j + 8.$$

Tabla de contenidos

Definición 2

Sea $G = (V, E)$ un grafo, y sea k un número natural. Una función $c : V \to \{1, 2, \ldots, k\}$ es llamado una **coloración** *del grafo G si $c(x) \neq c(y)$ para todo $\{x, y\} \in E$. El* **número cromático** *de G denotado por $\chi(G)$, es el mínimo k tal que existe un coloración $c : V(G) \to \{1, 2, \ldots, k\}$.*



Observaciones:

¿Qué podemos decir de $\chi(G)$ en un grafo G cualquiera?
Lo primero, que si G tiene aristas, entonces $\chi(G)$ está siempre comprendido entre 2 y el número de vértices del grafo, en efecto:

1. Por un lado, $\chi(G) \leq |V(G)|$ para todo grafo G, porque una coloración que siempre es válida (aunque, desde luego, poco efectiva) es asignar a cada vértice un color distinto.
2. Por otro lado, si el grafo contiene al menos una arista, entonces necesitaremos dos colores como mínimo. Es decir, si $|E(G)| \geq 1$ entonces $\chi(G) \geq 2$.

Propiedades

1. Si G contiene a G' como subgrafo, entonces $\chi(G) \geq \chi(G')$.
2. Si G tiene k componentes conexas $G_1, G_2, \ldots, G_k$ que tienen números cromáticos $\chi(G_1), \chi(G_2), \ldots, \chi(G_k)$ respectivamente, entonces $\chi(G) = \max_{1 \leq i \leq k}\{\chi(G_i)\}$.
3. Si G y G' son isomorfos, entonces $\chi(G) = \chi(G')$.

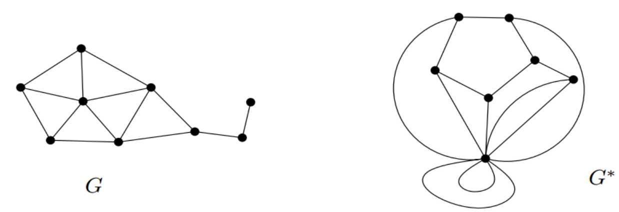
Ejemplo:

¿Cuál es el número cromático del grafo bipartito completo $K_{m,n}$ donde m y n son enteros positivos?
Solución: El número de colores necesarios puede observarse que depende de m y n. Pero observe que solamente dos colores son necesarios, porque $K_{m,n}$ es un grafo bipartito. De aquí, $\chi(K_{m,n}) = 2$. Esto significa que podemos colorear el conjunto de m vértices con un color y el conjunto de n vértices con un segundo color. Observe que las aristas conectan solamente un vértice del conjunto de m vértices y un vértice del conjunto de n vértices, con vértices no adyacentes tienen el mismo color.

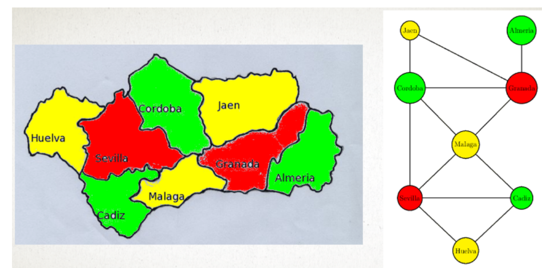
Definición 3 (Grafo dual)

Sea G un grafo topológico planar, es decir, un grafo planar (V, E) con un dibujo planar asociado. Sea $\mathcal{F}$ de conjunto de caras de G. Definimos un grafo, posiblemente con lazos y múltiples aristas, de la forma $(\mathcal{F}, E, \epsilon)$, donde ϵ es definido por $\epsilon(e) = \{F_i, F_j\}$ siempre que la arista e es una frontera común de las caras F_i y $F_j j$ (también permitimos $F_i = F_j$), en el caso cuando la misma cara pertenece a ambos lados de una arista dada). Este grafo $(\mathcal{F}, E, e)$ es llamado el **dual** *(geométrico) de G, y es denotado por G^*.*

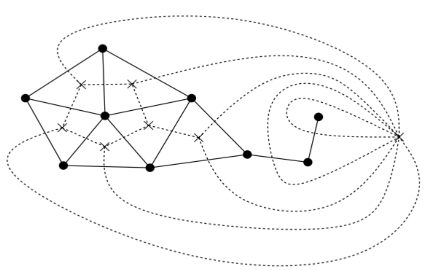
Ejemplo grafo dual



Ejemplo grafo dual



El grafo dual G^* puede ser dibujado junto con el dibujo del grafo G. Elija un punto b_F dentro de cada cara F de G y para cada arista e de G dibujamos un arco cruzando e y conectando los puntos b_F y $b_{F'}$, donde F y F' son las caras adyacentes a la arista e. Este arco permanece completamente en las caras F y F'. De este modo, se obtiene el dibujo planar de G^*.



¿$\chi(G) \leq 4$ para cualquier grafo planar G?

Teorema 2

Si G es un grafo planar, simple y conexo, entonces $\chi(G) \leq 4$.

Se tiene el siguiente resultado:

Proposición 4

Cualquier grafo planar satisface $\chi(G) \geq 5$.

Números cromáticos conocidos

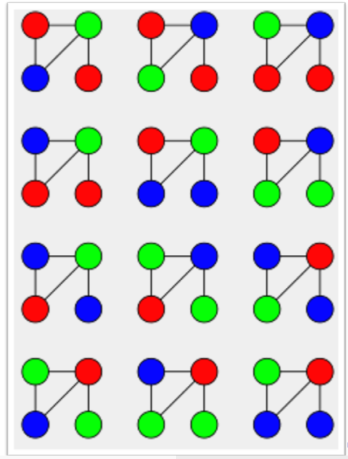
1. Grafo completo K_n: $\chi(K_n) = n$.
2. Grafo lineal (camino) L_n: $\chi(L_n) = 2$.
3. Grafo vacío N_n: $\chi(N_n) = 1$.
4. Ciclo C_n (n par): $\chi(C_n) = 2$.
5. Ciclo C_n (n impar): $\chi(C_n) = 3$.
6. Grafo bipartito G: $\chi(G) = 2$.
7. Grafo bipartito completo $K_{n,m}$: $\chi(K_{n,m}) = 2$.

Polinomio cromático

No sólo interesa saber si se puede colorear un grafo con k colores, sino también de cuántas maneras se puede colorear.
Como queremos contar y calcular, considere un grafo G y para cada entero $k \geq 1$ definimos:

$$P_G(k) = \#\{\text{coloraciones distintas de } G \text{ usando los colores de la colección } \{1, \ldots, k\}\}$$

teniendo en cuenta cuenta que no es necesario usarlos todos.
Observe que P_G es una función de k, que resulta ser un polinomio en k, que llamaremos el **polinomio cromático** de G.



El polinomio cromático se pregunta cuántas coloraciones, y el número cromático si hay alguna, así que cuál es el número cromático debe de quedar recogido dentro del propio polinomio cromático. En efecto:

1. Con menos de $\chi(G)$ colores no podemos colorear el grafo, así que $P_G(k) = 0$ si $k < \chi(G)$.
2. Pero con exactamente $\chi(G)$ colores se puede colorear el grafo de al menos una forma, por tanto, $P_G(\chi(G)) \geq 1$.
3. De un cierto grafo G ya conocemos $P_G(k)$, el número de coloraciones distintas con k colores. Supongamos que ahora en nuestra paleta de colores disponemos de algunos colores más, digamos $k' > k$. ¿Cuántas coloraciones podremos formar con esos k' colores?. Lo que es seguro, es que las que ya teníamos con k colores, seguiremos teniéndolas ahora y seguramente algunas más. Por tanto:

$$\text{si} \quad k < k' \Rightarrow P_G(k) \leq P_G(k')$$

Resumiendo las tres observaciones anteriores, deducimos que:

$$\begin{array}{lll} \text{Si} \quad k \geq \chi(G) & \Rightarrow & P_G(k) \geq 1, \\ \text{Si} \quad k < \chi(G) & \Rightarrow & P_G(k) = 0 \end{array}$$

Así, que si tuviéramos la expresión del polinomio cromático, podríamos obtener el valor del número cromático como el **menor valor entero** de k en el que $P_G(k)$ no se anula.

Polinomios cromáticos de algunos grafos

1. Triángulo K_3: $P_G(k) = k(k-1)(k-2)$.
2. Grafo completo K_n: $P_G(k) = k(k-1)(k-2)\ldots(k-n+1)$.
3. Árbol con n vértices: $P_G(k) = k(k-1)^{n-1}$.
4. Ciclo C_n: $P_G(k) = (k-1)^n + (-1)^n(k-1)$.

Ejemplo: Polinomio cromático del grafo lineal L_n

Para empezar, considere el grafo lineal con tres vértices L_3. Con 0 o con 1 color no se puede colorear, así que $P_{L_3}(0) = 0$ y $P_{L_3}(1) = 0$. ¿Y para que número de colores k general? Intentemos contar las coloraciones directamente. Tendremos k posible colores para el vértice v_1, una vez coloreado, tendremos $k-1$ colores disponibles para v_2, porque está prohibido utilizar el color que hayamos asignado al vértice v_1. Finalmente, para v_3 también hay un color prohibido, el utilizado para v_2, así que utilizando la regla del producto:

$$P_{L_3}(k) = k(k-1)(k-1) = k(k-1)^2.$$

Un argumento análogo nos permite concluir que, para el grafo lineal con n vértices L_n, se cumple:

$$P_{L_n}(k) = k(k-1)^{n-1}$$

Por tanto, $\chi(L_n) = 2$, como ya sabíamos.

Aritmética de los Enteros

Ronald Mas,
Angel Ramirez

12 de agosto de 2020

Contenido

Introducción

El conjunto de los números enteros $\mathbb{Z}$ posee una estructura que nos permite hablar de factorización única, divisibilidad, múltiplos (ideales). Es más de acuerdo al número de sus divisores se puede definir los números primos. El siguiente cuadro muestra las bondades que posee $\mathbb{Z}$:

	Suma	Producto
Clausura	✓	✓
Neutro	✓	✓
Inverso	✓	X
Asociatividad	✓	✓

Los únicos elementos que poseen inverso multiplicativo son el -1 y 1. Es más, se cumple la propiedad distributiva y que carece de elementos divisores de 0. Existen otros conjunto con las mismas características de $\mathbb{Z}$, estos reciben el nombre de **dominio de factorización única**.

Teorema (Teorema de Representación Base)

Sea $b > 1$ un número entero. Entonces para cada $n \in \mathbb{N}$ existe una sucesión de números enteros no negativos $\{a_i\}_{i=0}^{m}$ tal que:

$$n = \sum_{i=0}^{m} a_i b^i$$

con $0 \leq a_i < b$, $\forall j \in \{0, 1, \cdots, m\}$ y $a_m \neq 0$.
Es más esta representación es única y es llamada **la representación de n en base b**.

Prueba:
Procedamos por inducción fuerte sobre n:

1) Para $n = 1$ se tiene que $a_0 = 1$, luego $n = a_0$.

Continuación de la prueba

2) Supongamos que todo número entero menor que n se puede representar en base b, luego por el algoritmo de Euclides existen únicos q, r enteros tal que

$$n = qb + r, \text{ con } 0 \leq r < b.$$

Por hipotesis de inducción sobre $q < n$ se tiene que:

$$q = \sum_{i=0}^{m} a'_i b^i$$

para alguna sucesión $\{a'_i\}_{i=0}^{m}$ con $0 \leq a'_i < b$. Luego

$$n = (\sum_{i=0}^{m} a'_i b^i)b + r = \sum_{i=0}^{m} a'_i b^{i+1} + r$$

Por tanto, al considerar $a_0 = r$ y $a_{i+1} = a'_i$ se tiene el resultado deseado.

Máximo común divisor y mínimo común múltiplo

Definición

Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, decimos que a divide a b si existe $c \in \mathbb{Z}$ tal que $b = ac$. En adelante a divide a b se denota como $a \mid b$.

Definición

Dados $a, b \in \mathbb{Z}$ no nulos, decimos que $d \in \mathbb{Z}^+$ es el máximo común divisor de a y b:

1) $d \mid a$ y $d \mid b$.
2) Si existe $d' \in \mathbb{Z}$ tal que $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$.

En adelante denotamos $d = MCD(A, B)$.

Observación:

- Si existe el MCD de a y b este es único.

Teorema (Existencia del MCD)

Si $a, b \in \mathbb{Z}$ no nulos entonces existe $MCD(a, b)$ y $MCD(a, b) = m_0 a + n_0 b$ para algunos $m_0, n_0 \in \mathbb{Z}$.

Prueba:
Sea

$$I = \{ma + nb : \ m, n \in \mathbb{Z}\}$$

- **Afirmación 1**: $I \neq \emptyset$.
  En efecto, $a = 1.a + 0.b$ y $b = 0.a + 1.b$ de aquí se tiene que $a, b \in I$ entonces $-x = ((-m)a + (-n)b) \in \mathbb{Z}$, por tanto $I \cap \mathbb{Z}^+ \neq \emptyset$.
  Luego por el principio de buen orden existe $d \in I \cap \mathbb{Z}^+$ tal que $d \leq x$, $\forall x \in I \cap \mathbb{Z}^+$ entonces existen $m_0, n_0 \in \mathbb{Z}$ tal que $d = (m_0 a + n_0 b)$ con $0 < d \leq x$, $\forall x \in I \cap \mathbb{Z}^+$.

Continua la prueba

- **Afirmación 2**: $d = MCD(a, b)$.
  1) Si $x = (ma + nb) \in I$, por el algoritmo de la división existen únicos $q, r \in \mathbb{Z}$ tales que $x = dq + r$ con $0 \leq r < d$ entonces $ma + nb = (m_0 a + n_0 b)q + r$ de donde se concluye que $r = ((m - m_0 q)a) + ((n - n_0 q)b) \in I$.
     Como $r \in I$ con $r \geq 0$ entonces $r = 0$ (caso contrario se contradice la minimalidad de d). Por lo tanto $x = dq$, así $d \mid x$, $\forall x \in I$. Luego en particular $d \mid a$ y $d \mid b$.
  2) Si $d' \mid a$ y $d' \mid b$ entonces $d' \mid (m_0 a + n_0 b)$, es decir $d' \mid d$.

Definición

Sean $a, b \in \mathbb{Z}$ no nulos, decimos que a y b son primos relativos si $MCD(a, b) = 1$.

Definición

Sea $p \in \mathbb{Z}$, decimos que p es un número primo si posee exactamente 4 divisores enteros que son: ± 1 y $\pm p$.

Observaciones:

1) La cantidad de números primos en $\mathbb{Z}$ es infinito.
   Prueba:
   Es suficiente probar que la cantidad de números primos en $\mathbb{N}$ es infinita. Procedamos por contradicción, supongamos que la cantidad sea finita y este dada por el conjunto:

$$P = \{p_1, p_2, \cdots, p_k \,; \text{tal que } p_1 \leq p_2 \leq \cdots p_k\}$$

   Luego el elemento p_k es el máximo elemento que pertenece a P.
   Por otro lado, $m = p_1.p_2 \cdots .p_k + 1 \in P$ ya que no es divisible por ningún elemento de P, pero $p_k < m$. Ello contradice la maximalidad de p_k.

Continua las observaciones

2) Sea $p \in \mathbb{Z}^+$ un número primo, se cumple:
   1. Si $p = 4k + 1$ con $k \in \mathbb{N}$ entonces p se puede expresar como suma de dos cuadrados.
   2. Si $p = 4k + 3$ con $k \in \mathbb{N}$ entonces p no se puede expresar como suma de dos cuadrados.

Prueba:
2. Todo número cuadrado perfecto al dividirlo entre 4 deja residuo 0 o 1, luego la suma de dos cuadrados perfectos dejan como residuo de dividir entre 4 a 0, 1 o 2. Por ello ningún primo de la forma $4k + 3$ con $k \in \mathbb{N}$ se puede expresar como suma de dos cuadrados.

A pesar de no ser objeto de estudio en el curso, la última observación juega un papel importante en el estudio de los números primos en los enteros gaussianos $\mathbb{Z}(i) = \{a + bi : \ a, b \in \mathbb{Z}\}$ ya que permite establecer que números primos en $\mathbb{Z}$ dejan de serlo en $\mathbb{Z}(i)$. Por ejemplo 5 es un número primo en $\mathbb{Z}$ pero no lo es $\mathbb{Z}(i)$ ya que $5 = (1 - 2i)(1 + 2i)$.

Lema (1)

Sean $a, b, c \in \mathbb{Z}$ no nulos. Si $a \mid bc$ y $MCD(a, b) = 1$ entonces $a \mid c$.

Prueba:
Como $MCD(a, b) = 1$ entonces existen $r, s \in \mathbb{Z}$ tal que $ra + sb = 1$ entonces $rac + sbc = c$ y como $a \mid bc$ se tiene que $a \mid c$.

Lema (2)

Si $a \in \mathbb{Z}$ y $p \in \mathbb{Z}$ es un número primo entonces $p \mid a$ o $MCD(a, p) = 1$.

Prueba:
Si $p \mid a$ no hay nada que probar. Supongamos que $p \nmid a$ y sea $d = MCD(a, p)$ entonces $d \mid p$ y $d \mid a$. Luego $d = 1$ (termina la prueba) o $d = p$, si $d = p$ entonces $p \mid a$, ello es un contradicción.

Lema (3)

Sean $a, b \in \mathbb{Z}$ no nulos y $p \in \mathbb{Z}$ primo. Si $p \mid ab$ entonces $p \mid a$ o $p \mid b$.

Prueba:
Si $p \mid a$, termina la prueba. Supongamos que $p \nmid a$ entonces por el lema anterior $MCD(a, p) = 1$ y como $p \mid ab$, se tiene por el lema (1) que $p \mid b$.

Teorema (Teorema Fundamental de la Aritmética)

Todo número $n \in \mathbb{Z}$ no nulo puede ser escrito de forma única como:

$$n = \mu p_1 p_2 \cdots p_k$$

donde $\mu \in \{-1, 1\}$ y $p_1 \leq p_2 \cdots \leq p_k$ son números primos enteros positivos (no necesariamente distintos).

1) **Existencia**:
Es suficiente probar para $n \in \mathbb{N}$ $(\mu = 1)$, procedamos por inducción.
- Si $n = 1$ se tiene que $n = \mu p_1 p_2 \cdots p_k$ con $\mu = 1$ y $k = 0$.
- Supongamos que todo entero m con $1 \leq m < n$ puede ser escrito coo producto de primos. Si n es primo la prueba termina, caso contrario existen $d, d' \in \mathbb{Z}$ tal que $n = dd'$ con $1 < d, d' < n$. Luego por hipotesis inductiva se tiene:

$$\begin{array}{lll} d = q_1 q_2 \cdots q_r & \text{con} & q_1 \leq q_2 \leq \cdots \leq q_r \text{ primos positivos y} \\ d' = q'_1 q'_2 \cdots q'_s & \text{con} & q'_1 \leq q'_2 \leq \cdots \leq q'_s \text{ primos positivos.} \end{array}$$

Al reemplazar y ordenar si fuese necesario los primos $q_1, q_2, \cdots, q_r, q'_1, q'_2, \cdots q'_s$ se tiene el resultado deseado con $k = r + s$.

2) **Unicidad:**
Supongamos que

$$n = \mu p_1 p_2 \cdots p_k = \mu' p'_1 p'_2 \cdots p'_s \text{ con}$$

$p_1 \leq p_2 \leq \cdots \leq p_k$ y $p'_1 \leq p'_2 \leq \cdots \leq p'_s$ primos positivos entonces $\mu = \mu'$ y $p_1 p_2 \cdots p_k = p'_1 p'_2 \cdots p'_s$, faltaría probar que $k = s$ y que $p_i = p'_i$, $\forall i \in \{1, 2, \cdots, k\}$. Procedamos por inducción sobre k.
- Si $k = 1$ entonces $p_1 = p'_1 p'_2 \cdots p'_s$, luego $p'_s \mid p_1$, por tanto $p'_s = p_1$ (s=1 y $p'_1 = p_1$).
- Supongamos que para r factores primos positivos con $1 \leq r < k$ se cumple la unicidad. Luego como:

$$\begin{array}{lll} p_1 \mid p'_j & \text{para algún } j \text{ tal que} 1 \leq j \leq s & \text{entonces } p_1 = p'_j \\ p'_1 \mid p_i & \text{para algún } i \text{ tal que} 1 \leq i \leq k & \text{entonces } p'_1 = p_i \end{array}$$

y $p_1 \leq p_2 \leq \cdots \leq p_k$ y $p'_1 \leq p'_2 \leq \cdots \leq p'_s$ se tiene que $p_1 = p'_1$. Entonces $p_2 p_3 \cdots p_k = p'_2 p'_3 \cdots p'_s$ y hipotesis inductiva aplicada a $r = k - 1$ se tiene que $k - 1 = s - 1$ y $p_2 = p'_2, p_3 = p'_3, \cdots, p_k = p'_k$. Por tanto $k = s$ y $p_i = p'_i$, $\forall i \in \{1, 2, \cdots, k\}$.

Aritmética Modular

Ronald Mas,
Angel Ramirez

14 de agosto de 2020

Contenido

Teorema (Teorema chino del resto)

Sean $n_1, n_2, \cdots, n_k \in \mathbb{N}$, k números naturales con $k > 1$ tal que:

$$MCD(n_i, n_j) = 1, \ \forall i \neq j$$

y $r_i \in \mathbb{Z}$, donde $i \leq k$ son arbitrarios. Entonces existen enteros x_i, donde $1 \leq i \leq k$ tal que:

$$n_1 x_1 + r_1 = n_2 x_2 + r_2 = \cdots = n_k x_k + r_k. \tag{1}$$

Prueba:
Procedamos por inducción sobre k. Si $k = 2$, se tiene $MCD(n_1, n_2) = 1$ entonces existen $z_1, z_2 \in \mathbb{Z}$ tal que $n_1 z_1 + n_2 z_2 = 1$. Luego la ecuación $n_1 x - n_2 y = r_2 - r_1$ tiene solución, la cuál es $(x_1, x_2) = (z_1(r_2 - r_1), z_2(r_1 - r_2))$. Supongamos que el resultado es cierto para $k \geq 2$, veamos para $k + 1$.
Sean $n_1, n_2, \cdots, n_{k+1} \in \mathbb{N}$ números primos relativos dos a dos y $r_1, r_2, \cdots, r_{k+1} \in \mathbb{Z}$ elegidos arbitrariamente.

Continua la prueba

Por hipotesis de inducción, existen enteros $x_1, x_2, \cdots, x_k \in \mathbb{Z}$ que satisfacen la ecuación (1). Como los n_i con $1 \leq i \leq k$ son primos relativos dos a dos entonces $n_1 n_2 \cdots n_k$ y n_{k+1} son primos relativos también, es decir $MCD(n_1 n_2 \cdots n_k, n_{k+1}) = 1$, luego existen $X, Y \in \mathbb{Z}$ tal que $n_1 n_2 \cdots n_k X - n_{k+1} Y = r_{k+1} - n_1 x_1 - r_1$.
Al considerar

$$X_j = \frac{n_1 n_2 \cdots n_k X}{n_j} + x_j \in \mathbb{Z} \ \forall 1 \leq j \leq k \text{ y } X_{k+1} = Y,$$

se tiene $n_1 X_1 + r_1 = n_2 X_2 + r_2 = \cdots = n_{k+1} X_{k+1} + r_{k+1}$.

Los Enteros Módulo n

Sea $n \in \mathbb{Z}^+$, $n \geq 2$ se define la relación $\equiv_n$ sobre $\mathbb{Z}$ como:

$$a \equiv_n b \text{ si y sólo si } n \mid (a - b).$$

Es bien sabido que dicha relación es de equivalencia. Por tanto, la clase de a y el conjunto cociente son respectivamente:

$$\overline{a} = \{a + kn : \ k \in \mathbb{Z}\} \text{ y}$$

$$\mathbb{Z}_n := \frac{\mathbb{Z}}{\equiv_n} = \{\overline{a} : \ a \in \mathbb{Z}\}$$

Proposición

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} \text{ y } \mid \mathbb{Z}_n \mid = n.$$

Prueba: Si $x \in \mathbb{Z}_n$ entonces $x = \overline{a}$ con $a \in \mathbb{Z}$, luego por el algoritmo de la división existen $q, r \in \mathbb{Z}$ tal que $a = qn + r$, $0 \leq r < n$, es decir existe $r \in \mathbb{Z}$, $0 \leq r < n$ tal que $a \equiv_n r$ entonces $x = \overline{a} = \overline{r}$. Luego $x \in \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, es decir:

$$\mathbb{Z}_n \subseteq \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Por tanto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Por otro lado veamos que $\mid \mathbb{Z}_n \mid = n$, supongamos que existen $i, j \in \mathbb{Z}$ tal que $0 \leq i < j < n$ y $\overline{i} = \overline{j}$ entonces $j - i = n\alpha$, $\alpha \in \mathbb{Z}$ y como $0 < j$ y $i < n$ se tiene que $0 < n\alpha < n$ entonces $0 < \alpha < 1$ con $\alpha \in \mathbb{Z}$, lo cuál es una contradicción.

Proposición

Sean $\overline{a}, \overline{a'}, \overline{b}, \overline{b'} \in \mathbb{Z}_n$. Si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ entonces

$$\overline{a + b} = \overline{a' + b'} \text{ y } \overline{ab} = \overline{a'b'}.$$

Prueba:
Como $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ entonces $n \mid (a - a')$ y $n \mid (b - b')$. Luego, como $(a + b) - (a' + b') = (a - a') + (b - b')$ se tiene que $n \mid [(a + b) - (a' + b')]$, así $\overline{a + b} = \overline{a' + b'}$. Por otro lado, como $ab - a'b' = (a - a')b + a'(b - b')$ se tiene que $n \mid (ab - a'b')$, así $\overline{ab} = \overline{a'b'}$.

Definición

En $\mathbb{Z}_n$ definamos las operaciones:

$$\overline{a} \oplus \overline{b} = \overline{a + b} \text{ y } \overline{a} \odot \overline{b} = \overline{ab}$$

La proposición anterior nos garantiza la buena definición de estas operaciones. Por abuso de notación $\oplus$ y $\odot$las denotamos por $+$ y .

Teorema

Las operaciones en $\mathbb{Z}_n$ satisfacen las siguientes propiedades:

1) $\overline{x}+(\overline{y}+\overline{z})=(\overline{x}+\overline{y})+\overline{z},\ \forall\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_n$.
2) $\exists\overline{0}\in\mathbb{Z}_n:\ \overline{x}+\overline{0}=\overline{0}+\overline{x}=\overline{x},\ \forall\overline{x}\in\mathbb{Z}_n$.
3) $\forall\overline{x}\in\mathbb{Z}_n,\ \exists(\overline{-x})\in\mathbb{Z}_n:\ \overline{x}+(\overline{-x})=(\overline{-x})+\overline{x}=\overline{0}$.
4) $\overline{x}+\overline{y}=\overline{y}+\overline{x},\ \forall\overline{x},\overline{y}\in\mathbb{Z}_n$.
5) $(\overline{x}\,\overline{y})\overline{z}=\overline{x}(\overline{y}\,\overline{z}),\ \forall\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_n$.
6) $\exists\overline{1}\in\mathbb{Z}_n$: $\overline{x}\overline{1}=\overline{1}\overline{x}=\overline{x},\ \forall\overline{x}\in\mathbb{Z}_n$.
7) $\overline{x}\,\overline{y}=\overline{y}\,\overline{x},\ \forall\overline{x},\overline{y}\in\mathbb{Z}_n$.
8) $\overline{x}(\overline{y}+\overline{z})=\overline{x}\,\overline{y}+\overline{x}\,\overline{z},\ \forall\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_n$.

Prueba:

2) $\overline{0}=\{0+kn:\ k\in\mathbb{Z}\}=\{kn:\ k\in\mathbb{Z}\}=\{0,\pm n,\pm 2n,\cdots\}$ y es claro que:
$$\overline{x}+\overline{0}=\overline{x+0}=\overline{x},\ \overline{0}+\overline{x}=\overline{0+x}=\overline{x},\ \forall\overline{x}\in\mathbb{Z}_n.$$
3) $\overline{x}+(\overline{-x})=\overline{x+(-x)}=\overline{0}$ y $(\overline{-x})+\overline{x}=\overline{(-x)+x}=\overline{0},\ \forall\overline{x}\in\mathbb{Z}_n$.
8) $\overline{x}(\overline{y}+\overline{z})=\overline{x}(\overline{y+z})=\overline{x(y+z)}=\overline{xy}+\overline{xz}=\overline{x}\,\overline{y}+\overline{x}\,\overline{z},\ \forall\overline{x},\overline{y},\overline{z}\in\mathbb{Z}_n$.

Proposición

En $\mathbb{Z}_n$ se cumple que:

1) *Si $\overline{x}\neq\overline{0}$ y $\overline{y}\neq\overline{0}$ entonces $\overline{x}\,\overline{y}\neq\overline{0}$ si y sólo si n es primo.*
2) *Si n es un número primo, para cada $\overline{x}\in\mathbb{Z}_n-\{\overline{0}\}$, existe $\overline{y}\in\mathbb{Z}_n$ tal que $\overline{x}\,\overline{y}=\overline{y}\,\overline{x}=\overline{1}$.*

Prueba:

2) Sea $\overline{x}\in\mathbb{Z}_n$ con $\overline{x}\neq\overline{0}$ entonces $MCD(p,x)=1$, por tanto existen $r,s\in\mathbb{Z}$ tal que $pr+xs=1$, luego $\overline{x}\,\overline{s}=\overline{1}$. Por lo tanto $\exists\overline{y}=\overline{s}\in\mathbb{Z}_n$ tal que $\overline{x}\,\overline{y}=\overline{1}$.

Continua prueba

1) $\Rightarrow$) Si $d\mid n$ entonces $n=db$ con $b\in\mathbb{Z}$, así $\overline{db}=\overline{0}$ entonces $\overline{d}=\overline{0}$ o $\overline{b}=\overline{0}$, analicemos ambos casos:
   - Si $\overline{d}=\overline{0}$ entonces $n\mid d$, y como $d\mid n$ se tiene que $d=\pm n$.
   - Si $\overline{b}=\overline{0}$ entonces $n\mid b$, es decir $b=n\beta$ con $\beta\in\mathbb{Z}$, luego como $n=db$ entonces $n=dn\beta$, así $1=d\beta$, por ello $d=\pm 1$. Por tanto n es primo.

   $\Leftarrow$) Si n es primo y $\overline{a}\,\overline{b}=\overline{0}$ en $\mathbb{Z}_n$ entonces $n\mid ab$, luego $n\mid a$ o $n\mid b$, así se tiene que $\overline{a}=\overline{0}$ o $\overline{b}=\overline{0}$.

Observaciones:

- Por la parte 2) de la proposición anterior, se tiene que todo elemento dinstinto de $\overline{0}$ en $\mathbb{Z}_p$ con p primo posee inverso multiplicativo, en particular decimos que $\mathbb{Z}_p$ es un **cuerpo**.

Ejemplo 1:

Para $n=12$, se tiene que en $\mathbb{Z}_{12}$ la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
$\overline{0}$	$\overline{0}$	No tiene
$\overline{1}$	$\overline{11}$	$\overline{1}$
$\overline{2}$	$\overline{10}$	No tiene
$\overline{3}$	$\overline{9}$	No tiene
$\overline{4}$	$\overline{8}$	No tiene
$\overline{5}$	$\overline{7}$	$\overline{5}$
$\overline{6}$	$\overline{6}$	No tiene
$\overline{7}$	$\overline{5}$	$\overline{7}$
$\overline{8}$	$\overline{4}$	No tiene
$\overline{9}$	$\overline{3}$	No tiene
$\overline{10}$	$\overline{2}$	No tiene
$\overline{11}$	$\overline{1}$	$\overline{11}$

Ejemplo 2:

Para $n=13$, se tiene que en $\mathbb{Z}_{13}$ la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
$\overline{0}$	$\overline{0}$	No tiene
$\overline{1}$	$\overline{12}$	$\overline{1}$
$\overline{2}$	$\overline{11}$	$\overline{7}$
$\overline{3}$	$\overline{10}$	$\overline{9}$
$\overline{4}$	$\overline{9}$	$\overline{10}$
$\overline{5}$	$\overline{8}$	$\overline{8}$
$\overline{6}$	$\overline{7}$	$\overline{11}$
$\overline{7}$	$\overline{6}$	$\overline{2}$
$\overline{8}$	$\overline{5}$	$\overline{5}$
$\overline{9}$	$\overline{4}$	$\overline{3}$
$\overline{10}$	$\overline{3}$	$\overline{4}$
$\overline{11}$	$\overline{2}$	$\overline{6}$
$\overline{12}$	$\overline{1}$	$\overline{12}$

Teoría de números

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

15 de agosto de 2020

Tabla de contenidos

Pequeño Teorema de Fermat

Teorema 1

Si p es un primo y $n\in\mathbb{N}$ relativamente primo con p, entonces:
$$n^{p-1}\equiv 1\,(mod\ p)$$

Demostración:
Afirmamos que los números $n,2n,3n,\ldots,(p-1)n$ dejan todos ellos residuos distintos al dividirse entre p y, además, que ninguno de estos residuos es cero. En efecto, tomemos $0<i<j<p-1$. Sabemos que cuando p es primo se cumple que $[n]$ tiene inverso en $\mathbb{Z}_p$. Sea $[m]$ su inverso. Luego, si $[in]=[jn]$ entonces multiplicando por $[m]$ a ambos lados resulta:
$$[i]=[i(ab)]=[j(ab)]=[j]$$

Pequeño Teorema de Fermat (cont.)

pero como i, j están entre 1 y p, esto implica que $i = j$. Además, ninguno es cero pues si $[ia] = [0]$ entonces al multiplicar por $[m]$ se tiene que:

$$[i] = [i(ab)] = [0b] = [0]$$

lo que es una contradicción.
Así, usando la afirmación en la siguiente cadena módulo p, se tiene:

$$\begin{aligned}(p-1)!a^{p-1} &= (a)(2a)(3a)\ldots((p-1)a)\\ &= 1\cdot 2\cdot \ldots \cdot (p-1) = (p-1)!\end{aligned}$$

El número $(p-1)!$ no es divisible entre p, pues es producto de puros números menores que p, de modo que $mcd(p,(p-1)!) = 1$, así que tiene inverso módulo p, de modo que podemos cancelarlo

Pequeño Teorema de Fermat (cont.)

de la congruencia anterior multiplicando en ambos lados por su inverso. Así, obtenemos la igualdad:

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

Ejemplo:

Demuestre que $13|(2^{50} + 3^{50})$.
Demostración:
Por el pequeño teorema de Fermat:

$$\begin{aligned}2^{12} &\equiv 1\,(mod\,13)\\ 3^{12} &\equiv 1\,(mod\,13)\end{aligned}$$

Como $50 = 4(12) + 2$, entonces:

$$\begin{aligned}2^{50} &= 2^{4(12)+2} = (2^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 4 \equiv 4\,(mod\,13)\\ 3^{50} &= 3^{4(12)+2} = (3^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 9 \equiv 9\,(mod\,13)\end{aligned}$$

luego: $2^{50} + 3^{50} \equiv (4+9)\,(mod\,13) \equiv 0\,(mod\,13)$.

Tabla de contenidos

Proposición 1

Sea p un número primo. Los únicos elementos en $\mathbb{Z}_p$ que son inversos de sí mismos son $[1]$ y $[p-1]$.

Demostración: Claramente $[1]$ y $[p-1] = [-1]$ son inversos multiplicativos de sí mismos porque $1 \cdot 1 = (-1)\cdot(-1) = 1$. Ahora, si tenemos a tal que es inverso multiplicativo de sí mismo, tenemos que $[a^2] = [1]$ que por definición se tiene que $p|(a^2 - 1)$, pero $(a^2 - 1) = (a-1)(a+1)$. Cuando un primo divide a un producto, tiene que dividir a uno de los factores. Entonces p divide a $(a+1)$ o $(a-1)$ y obtenemos respectivamente que $[a] = [-1] = [p-1]$ o que $[a] = [1]$, que es lo que queríamos probar.

Teorema 2 (Teorema de Wilson)

Si p es un número primo, entonces $(p-1)! \equiv -1\,(mod\,p)$.

Demostración:
Si $p = 2$, el resultado es inmediato. Supongamos que $p \geq 3$. En $(p-1)!$ aparecen todos los números de 1 a $(p-1)$. Todos ellos son primos relativos con p, así que tienen inverso módulo p. Ese inverso también aparece en $(p-1)!$. Así podemos agrupar esos números en $(p-3)/2$ parejas de inversos multiplicativos, en donde por la proposición anterior sólo nos va a sobrar el 1 o -1. De esta forma:

$$(p-1)! \equiv (1)(-1)(1\cdot 1 \cdot \ldots \cdot 1) \equiv -1\,(mod\,p),$$

en donde en la expresión intermedia tenemos un 1, un -1 y $(p-3)/2$ unos, uno por cada pareja de inversos que se multiplicaron, finalizando así la prueba.

Ejemplo:

Determine el residuo que se obtiene al dividir $15! + 16! + 17!$ entre 17.
Resolución:
Notemos que 17 divide a 17!, así que $17! \equiv 0\,(mod\,17)$. Por el teorema de Wilson, $16! \equiv -1\,(mod\,17)$. Podemos multiplicar esta igualdad por -1, resultando:

$$15! = 15!(-1)(-1) \equiv 15!(16)(-1) = 16!(-1) \equiv (-1)(-1) \equiv 1$$

por tanto:

$$15! + 16! + 17! \equiv 1 + (-1) + 0 \equiv 0\,(mod\,17).$$

Tabla de contenidos

Funciones aritméticas

Funciones aritméticas son aquellas funciones cuyo dominio es $\mathbb{N}$ y cuyo rango es un subconjunto de $\mathbb{C}$. Una función aritmética f es llamada **multiplicativa** si:

$$f(mn) = f(m)f(n) \quad \text{para todo} \quad m,n \in \mathbb{N} \quad \text{tal que} \quad mcd(m,n) = 1.$$

f es llamada **completamente multiplicativa** si:

$$f(mn) = f(m)f(n) \quad \text{para todo} \quad m,n \in \mathbb{N}$$

Función de Euler

Para cualquier $n \in \mathbb{N}$ la **función de Euler**, también llamada **Euler's Totien**, $\phi(n)$ es definida como la cantidad de $m \in \mathbb{N}$ tal que $m < n$ y $mcd(m, n) = 1$. Es decir:

$$\phi(n) = |\{m \in \mathbb{N} \,/\, m < n \wedge mcd(m, n) = 1\}|.$$

Ejemplo:
Si p es primo, entonces cualquier $j \in \mathbb{N}$ con $j < p$ es relativamente primo a p, entonces $\phi(p) = p - 1$.

Sistema de residuos reducidos

Si $n \in \mathbb{N}$, entonces cualquier conjunto de $\phi(n)$ enteros no congruentes módulo n y relativamente primos a n, es llamado un **sistema de residuos reducido** módulo n.

Ejemplo:
El conjunto $\{1, 3, 7, 9\}$ es un sistema de residuos reducidos módulo 10 porque $\phi(10) = 4$, y cada elemento del conjunto es relativamente primo a 10, y ellos no son congruentes módulo 10.

Teorema 3

La función es Euler es multiplicativa, es decir, dados $m, n \in \mathbb{N}$ relativamente primos, entonces:

$$\phi(mn) = \phi(m)\phi(n).$$

Además, si $n = \prod_{j=1}^{k} p_j^{a_j}$ donde los p_j son primos distintos, entonces:

$$\phi(n) = \prod_{j=1}^{k}(p_j^{a_j} - p_j^{a_j-1}) = \prod_{j=1}^{k}\phi(p_j^{a_j}).$$

Teorema de Euler

Si $n \in \mathbb{N}$ y $m \in \mathbb{Z}$ tal que $mcd(m, n) = 1$, entonces:

$$m^{\phi(n)} \equiv 1 \,(mod\ n)$$

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática **Ciclo 2023-1**

Código: CM2H1

Examen Final de Matemática Discreta

Sección: A, B

Profesores: F. Jara, J. Palacios

Duración: 100 minutos.

---

1. Decir si los siguientes enunciados son verdaderos (V) o falsos (F). Justifique su respuesta.

   a) Si G es un árbol con 10 vértices y P_G es su polinomio cromático, entonces 1 es raíz de P_G de multiplicidad 9. (2.5 ptos)

   b) No existen enteros a, b tales que $2a^2 + b^2 = p$ para todo primo $p \equiv 5, 7 \mod 8$. (2.5 ptos)

2. Dado un entero impar m.

   a) Pruebe que para todo número natural $n \geq 3$, se cumple $m^{2^{n-2}} \equiv 1 \mod 2^n$. (3 ptos)

   b) Dado un numero natural $n \geq 1$. Deduzca que existe una raíz primitiva módulo 2^n solo en los casos $n = 1$ o $n = 2$. (2 pto)

3. Dada la función booleana F en las variables x, y, z que toman el valor cero o uno, tal que su valor sea uno cuando dos de sus valores x e y, no tomen simultáneamente el valor cero.

   a) Determine la tabla de verdad correspondiente. (1 pto)

   b) Exprese F en función de sus minitérminos. (2 ptos)

   c) Use el mapa de Karnaugh para simplificar la expresión encontrada en el ítem *a*). (2 ptos)

4. Construya una máquina de estado finito con salida[*] M sobre el alfabeto de entrada $I = \{a, b\}$ y alfabeto de salida $O = \{0, 1\}$, de modo que cada cadena de entrada tiene su cadena de salida formado por solo por ceros, salvo que contenga términos de la forma abb, que corresponden a términos de la forma 001 en la cadena de salida correspondiente. (3 ptos)

5. Teniendo en cuenta la pregunta anterior, proponga tres cadenas de entrada y escriba las cadenas de salida correspondientes. (2 ptos)

Solución:

[*]Una *máquina de estado finito con salida* es una tupla $M = (S, I, O, f, g, s_0)$, donde S es un conjunto finito de *estados*, I es un conjunto finito llamado *alfabeto de entrada*, O es un conjunto finito llamado *alfabeto de salida*, $f\colon S \times I \to S$ es una función llamada *función transición*, $g\colon S \times I \to O$ es una función llamada *función de salida* y $s_0 \in S$ es llamado *estado de inicio*. Se dice que $i_1 i_2 \cdots i_n$ es una *cadena de entrada* si $i_1, i_2, \cdots, i_n \in I$. Sea $s_j = f(s_{j-1}, i_j)$ para todo $j = 1, 2, \ldots, n$. Una *cadena de salida* es una cadena de la forma $\sigma_1 \sigma_2 \ldots \sigma_n$, donde $\sigma_j = g(s_{j-1}, i_j)$ para todo $j = 1, 2, \ldots, n$.

---

1. *a*) (V). Si G es un árbol con n vértices, entonces que $P_G(t) = t(t-1)^{n-1}$. Se prueba por inducción. Se cumple para $n = 2$, en este caso $G = K_2$. Supongamos que es cierto para arboles de $n-1$ vértices. Tomamos una hoja $v \in G$. Entonces $G - \{v\}$ es un árbol con $n-1$ vértices. Por hipótesis inductiva hay $t(t-1)^{n-2}$ formas de colorear $G - \{v\}$ con a lo más t colores. Como v es una hoja, hay $t-1$ formas de colorear v. Por tanto, hay $t(t-1)^{n-1}$ formas de colorear G con a lo más t colores.

   Luego si $n = 10$ entonces 1 es raíz de P_G de multiplicidad 9.

   b) (V) Supongamos lo contrario, i.e. existen enteros a, b tales que $2a^2 + b^2 = p$ para todo primo $p \equiv 5, 7 \mod 8$. Tenemos

$$(-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{2a^2}{p}\right) = \left(\frac{-b^2+p}{p}\right) = \left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

   Si $p \equiv 5 \mod 8$, de las igualdades tenemos $-1 = 1$; y si $p \equiv 7 \mod 8$, de las igualdades tenemos $1 = -1$, que es absurdo en ambos casos.

2. *a*) Por inducción sobre $n \geq 3$. Sea $m = 2k+1$, entonces

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \equiv 1 \mod 8$$

   Así es válido para $n = 3$. Asumamos que es válido para $n-1$, entonces

$$m^{2^{n-3}} \equiv 1 \mod 2^{n-1}$$

   Luego existe un entero r tal que $m^{2^{n-3}} = 1 + r2^{n-1}$. Elevando al cuadrado:

$$m^{2^{n-2}} = 1 + r2^n + r^2 2^{2(n-1)}$$

   De donde $m^{2^{n-2}} \equiv 1 \mod 2^n$.

   b) Tenemos $\varphi(2^n) = 2^{n-1}$. Si $n \geq 3$ del ítem anterior tenemos $m^{\varphi(2^n)/2} \equiv 1 \mod 2^n$, de donde $ord_{2^n}(m) \leq \varphi(2^n)/2 < \varphi(2^n)$, es decir que m no puede ser raíz primitiva. Resta los casos $n = 1$, $n = 2$. Tenemos que 1 es raíz primitiva módulo 2 y 3 es raíz primitiva módulo 4.

3. Tenemos

(a)

x	y	z	F
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

(b)

$$F(x;y;z) = \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}\bar{z} + x\bar{y}z + xy\bar{z} + xyz$$

(c)

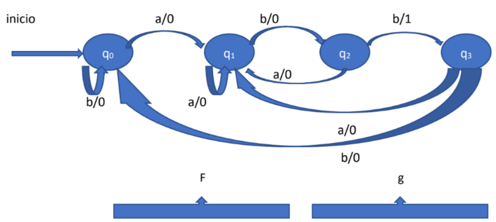
$x \setminus y$	xy	$x\bar{y}$	$\bar{x}\bar{y}$	$\bar{x}y$
z	1	1		1
$\bar{z}$	1	1		1

x y

Se forman dos grupos de cuatro cuadrados adyacentes: El primer grupo conserva invariable x y el segundo y.

$$F(x;y;z) = x + y$$

4. Definimos $M = (S, I, O, F, g, q_0)$, donde $S = \{q_0, q_1, q_2, q_3\}$, $I = \{a, b\}$, $O = \{0, 1\}$, F, g como muestra la figura:



	a	b	a	b
q_0	q_1	q_0	0	0
q_1	q_1	q_2	0	0
q_2	q_1	q_3	0	1
q_3	q_1	q_0	0	0

5. La cadena de entrada $abbaaabbabab$ da la cadena de salida 001000010000.

   La cadena de entrada $aaabaaa$ da la cadena de salida 0000000

   La cadena de entrada $abbabb$ da la cadena de salida 001001.

UNI, 10 de julio del 2023 **

**Hecho en LaTeX

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática **Ciclo 2023-1**

Código: CM2H1

Examen Parcial de Matemática Discreta

Sección: A, B

Profesores: J. Palacios, F. Jara

Duración: 100 minutos.

1. Sea D_n el conjunto de todos los divisores positivos de $n \in \mathbb{Z}^+$.

   a) ¿Es $(D_{40}; |)$ un conjunto parcialmente ordenado?. Donde:

   $$a\ R\ b \Longleftrightarrow a|b \quad (a \text{ divide a } b).$$

   (2 ptos)

   b) Teniendo en cuenta el ítem *a*). Realice el diagrama de Hasse. (2 ptos)

   c) Determine los maximales y minimales, máximo y mínimo el subconjunto.

   $$S = \langle 2; 4; 8; 20 \rangle.$$

   (1 pto)

2. En el contexto de comparación asintótica de funciones. Definimos

   $$T(n) = \Theta(f(n)) \quad \text{si y solo si}$$
   $$\exists (c_1; c_2; n_0) \in \mathbb{R}^+ \times \mathbb{R}^+ \times \mathbb{N}.$$

   Tal que $\forall n \geq n_0 : 0 \leq c_1 f(n) \leq T(n) \leq c_2 f(n)$.

   a) Describa en el plano XY el significado geométrico

   $$f(n) = \Theta(g(n))$$

   (2 ptos)

   b) Dado que $\frac{1}{2}n^2 - 3n = \Theta(n^2)$. Determine las constantes c_1, c_2 y n_0 tales que

   $$\forall n \geq n_0, c_1 n^2 \leq \frac{1}{2}n^2 - 3n \leq c_2 n^2$$

   (3 ptos)

3. Decir si los siguientes enunciados son verdaderos (V) o falsos (F). Justifique su respuesta.

   a) No existen grafos con infinitos vértices pero con un número finito de aristas. (2 ptos)

b) Todo árbol con n vértices tiene exactamente $n-1$ aristas. (3 ptos)

4. Sea G un grafo con n vértices y con matriz de adyacencia A.

   a) Pruebe que G es conexo, si y solo si, cada entrada (i,j) de A^m con $i \neq j$ es no nula para algún entero $m \geq 1$. (2 ptos)

   b) Deduzca que G es conexo si y solamente si $(A+I)^{n-1}$ no tiene entradas nulas. (3 ptos)

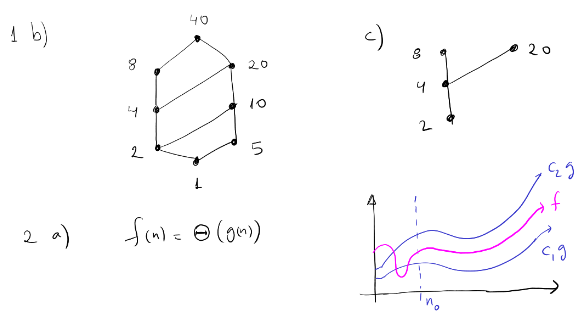
Solución:

1. a) Dado que $(\mathbb{Z}^+;|)$ es un conjunto parcialmente ordenado, por tanto $(D_{40};|)$ es también parcialmente ordenado.

   b) El diagrama de Hasse de $(D_{40};|)$ es mostrado en la figura inferior.

   c)

$$\begin{aligned}
&\text{Maximales } = \{8;20\}\\
&\text{Minimales } = \{2\}\\
&\text{No tiene máximo}\\
&\text{Mínimo } 2.
\end{aligned}$$



2.

   a) Se muestra en la figura superior.

   b) Dividiendo por n^2 a $c_1 n^2 \leq \frac{1}{2}n^2 - 3n \leq c_2 n^2$

$$c_1 \leq \frac{1}{2} - \frac{3}{n} \leq c_2.$$

   Ahora

$$\begin{aligned}
\forall n \geq 7; \quad 0 \leq \frac{1}{n} &\leq \frac{1}{7}\\
0 \geq -\frac{3}{n} &\geq \frac{-3}{7}\\
\frac{1}{2} \geq \frac{1}{2} - \frac{3}{n} &\geq \frac{1}{2} - \frac{3}{7}\\
\frac{1}{2} \geq \frac{1}{2} - \frac{3}{n} &\geq \frac{1}{14}
\end{aligned}$$

   Por tanto

$$\forall n \geq 7, \quad \frac{1}{c_1}n^2 \leq \frac{1}{2}n^2 - 3n \leq \frac{1}{2}n^2$$

   Existen $c_1 = \frac{1}{14}$ y $c_2 = \frac{1}{2}$.

3. a) (F). Si existen tales grafos, por ejemplo el grafo $G=(V,E)$ donde $V=\mathbb{N}$ y $E=\emptyset$.

   b) (V) Probemos por inducción. Para $n=2$, es cierto. Supongamos que el enunciado es cierto para $n \geq 2$. Sea G un grafo de $n+1$ vértices. Consideremos una hoja v de G i.e. un vértice de grado 1. Note que $G-v$ es un grafo con n vértices, y por hipótesis inductiva $G-v$ posee $n-1$ aristas. Supongamos que u es el vértice adyacente a v. Note que G es obtenido al añadir la arista $\{u,v\}$ a $G-v$. Por tanto G tiene $(n-1)+1=n$ aristas.

4. a) Supongamos que G tiene vértices $\{v_1, v_2, \ldots, v_n\}$. Por definición, el grafo G es conexo si cada par de vértices $v_i \neq v_j$ es conectado por un camino de longitud k para algún $k \geq 1$. Esta condición equivale a que la entrada (i,j) de A^k es no nula para algún $k \geq 1$. Si consideramos caminos simples podemos reducirnos a caso $1 \leq k \leq n-1$

   b) Consideremos el binomio de Newton:

$$(A+I)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A^k$$

   Luego, tomando la entrada (i,j), tenemos

$$\left((A+I)^{n-1}\right)_{i,j} = I_{i,j} + \sum_{k=1}^{n-1} \binom{n-1}{k} \left(A^k\right)_{i,j}$$

   donde $\binom{n-1}{k} \geq 1$ para todo $k \geq 1$. Luego, deducimos que $\left((A+I)^{n-1}\right)_{i,j} \geq 1$ si $i=j$; y si $i \neq j$, tenemos

$$\left((A+I)^{n-1}\right)_{i,j} > 0 \quad \Leftrightarrow \quad \left(A^k\right)_{i,j} > 0 \text{ para algún } k \in \{1,2,\ldots,n-1\}$$

   Finalmente se usa el ítem anterior para obtener la equivalencia deseada.

UNI, 15 de Mayo del 2023 *

*Hecho en LaTeX

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática **Ciclo 2023-1**

Código: CM2H1 EXAMEN SUSTITUTORIO DE MATEMÁTICA DISCRETA

Sección: A, B Profesores: F. Jara, J. Palacios

Duración: 100 minutos.

---

1. Sea D_n el conjunto de divisores positivos de un número natural n. En $(D_{10}, |) \times (D_{18}, |)$ se considera el orden lexicográfico.

   a) Halle las cotas inferiores, cotas superiores, ínfimo y supremo, si existen, del subconjunto $S = \{(2,2),(2,3)\}$ de $(D_{10}, |) \times (D_{18}, |)$. (2 ptos)

   b) Dibuje el diagrama de Hasse de $(D_{10}, |) \times (D_{18}, |)$. (2 ptos)

   c) Sea la función $f : (D_{10}, |) \times (D_{18}, |) \to (D_{180}, |)$ dada por $f(a, b) = ab$.
   ¿Es f biyectiva? (1 pto)

2. Pruebe que para todo entero $r \geq 2$, existe $n \in \mathbb{N}$ tal que todo grafo con al menos n vértices contiene a un subgrafo isomorfo al grafo completo K_r o a su complemento $\overline{K_r}$. Provea una demostración detallada. (5 ptos)

3. Dado un primo $p > 2$. Pruebe la igualdad

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1$$

(5 ptos)

4. Un motor F está controlado por tres interruptores x, y, z. Funciona cuando únicamente dos de los interruptores estén cerrados.

   a) Dado el álgebra de Boole $B = \{0, 1\}$. Deduzca la tabla de verdad de la función $F : B^3 \longrightarrow B$, y obtenga su expresión booleana en función de minitérminos. (2,5 ptos)

   b) Reduzca F y encuentre el circuito correspondiente con sus puertas lógicas. (2,5 ptos)

Solución:

1. *a)* El conjunto de cotas superiores de $S = \left\{(2,2),(2,3)\right\}$ es:

$$\left\{(2,6),(2,18),(10,1),(10,2),(10,3),(10,9),(10,18)\right\}$$

El conjunto de cotas inferiores de $S = \left\{(2,2),(2,3)\right\}$ es:

$$\left\{(2,1),(1,18),(1,9),(1,6),(1,3),(1,2),(1,1)\right\}$$

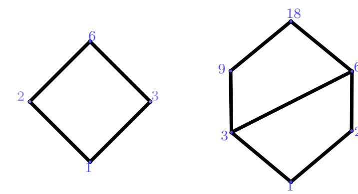
El supremo es

$$\text{mín}\left\{(2,6),(2,18),(10,1),(10,2),(10,3),(10,9),(10,18)\right\} = (2,6)$$

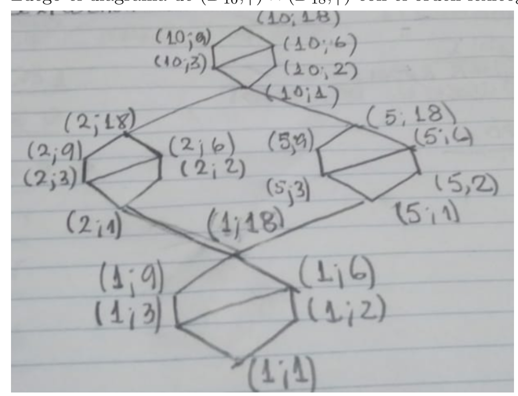
El ínfimo es

$$\text{máx}\left\{(2,1),(1,18),(1,9),(1,6),(1,3),(1,2),(1,1)\right\} = (2,1)$$

b) Tenemos $D_{10} = \{1, 2, 5, 10\}$ y $D_{18} = \{1, 2, 3, 6, 9, 18\}$. Sus diagramas de Hasse respectivos son:



Luego el diagrama de $(D_{10}, |) \times (D_{18}, |)$ con el orden lexicográfico es:



c) La función f no es inyectiva, pues $f(2,1) = f(1,2)$.

2. Sea $n = 2^{2r-3}$ y considere un grafo $G = (V, E)$ tal que $|V| \geq n$. Definimos inductivamente los subconjuntos $V_1, V_2, \cdots, V_{2r-2} \subset V$ y vértices $v_i \in V_i$ para todo $i = 1, 2, \ldots, 2r-2$ tales que:

   1) $|V_i| = 2^{2r-2-i}$ para todo $i = 1, 2, \ldots, 2r-2$.

   2) $V_i \subset V_{i-1} - \{v_{i-1}\}$ para todo $i = 1, 2, \ldots, 2r-2$.

3) v_{i-1} es adyacente, o bien a todos los vértices de V_i, o a ningún vértice de V_i, para todo $i = 2, 3, \ldots, 2r-2$.

En efecto, tomamos V_1 como cualquier subconjunto de V de cardinal $n = 2^{2r-3}$ y $v_1 \in V_1$ arbitrario. Observe que se cumple 1) y también 2) y 3) por vacuidad.

(HI) Supongamos que tenemos V_{i-1} y $v_{i-1} \in V_{i-1}$ satisfaciendo 1), 2) y 3). Tenemos

$$|V_{i-1} - \{v_{i-1}\}| = 2^{2r-2-(i-1)} - 1 = 2^{2r-1+i} - 1 > 2^{2r-2+i}$$

Sea W_i el subconjunto de $V_{i-1} - \{v_{i-1}\}$ de vértices adyacentes a v_{i-1}. Si $|W_i| \geq 2^{2r-2+i}$, entonces tomamos V_i como cualquier subconjunto de W_i de cardinal 2^{2r-2+i}.

Si $|W_i| < 2^{2r-2+i}$, entonces $|W_i| \leq 2^{2r-2+i} - 1$, luego

$$\Big|(V_{i-1} - \{v_{i-1}\}) - W_i\Big| = 2^{2r-1+i} - 1 - |W_i| \geq 2^{2r-1+i} - 1 - (2^{2r-2+i} - 1) = 2^{2r-2+i}$$

Luego tomamos V_i como cualquier subconjunto de $(V_{i-1} - \{v_{i-1}\}) - W_i$ de cardinal 2^{2r-2+i}. Note que ningún vértice de V_i es adyacente a v_{i-1}. Así tenemos la propiedad 3).

Finalmente tomando $v_i \in V_i$ arbitrario, se observa que V_i y $v_i \in V_i$ satisfacen 1), 2) y 3).

Afirmación: Entre los vértices $v_1, v_2, \ldots, v_{2r-3}$, existen $r-1$ vértices con una misma propiedad en 3).

En efecto, sea P_1 el conjunto de vértices v_{i-1} que son adyacentes a todos los vértices de V_i para $i = 2, 3, \ldots, 2r-2$, y sea P_2 el conjunto de vértices v_{i-1} no son adyacentes a ningún vértice de V_i para $i = 2, 3, \ldots, 2r-2$. Por el principio del palomar, P_1 o P_2 contiene al menos $r-1$ vértices. En cada caso, elegimos los $r-1$ vértices y lo añadimos el vértice v_{2r-2}, de modo que obtenemos un subgrafo inducido H de G con r vértices. Por construcción, se observa que en el primer caso, cada par de vértices de H está conectado, por tanto H es isomorfo a K_r; mientras que en el segundo caso, ningún par de vértices de H está conectado, de donde H es isomorfo a $\overline{K_r}$. Esto concluya la prueba.

3. Notemos que $U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \ldots, \overline{p-1}\}$. Tenemos

$$\begin{aligned}
\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x(x+1)}{p}\right) \\
&= \sum_{x \in U(\mathbb{Z}/p\mathbb{Z})} \left(\frac{x(x+1)}{p}\right) \\
&= \sum_{x \in U(\mathbb{Z}/p\mathbb{Z})} \left(\frac{x^2(1+1/x)}{p}\right) \\
&= \sum_{x \in U(\mathbb{Z}/p\mathbb{Z})} \left(\frac{1+1/x}{p}\right)
\end{aligned}$$

Se verifica sin dificultad que la función $U(\mathbb{Z}/p\mathbb{Z}) \to U(\mathbb{Z}/p\mathbb{Z})$ dada por $x \mapsto 1/x$ es biyectiva.

Luego

$$\begin{aligned}
\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) &= \sum_{x \in U(\mathbb{Z}/p\mathbb{Z})} \left(\frac{1+1/x}{p}\right) \\
&= \sum_{x \in U(\mathbb{Z}/p\mathbb{Z})} \left(\frac{1+x}{p}\right) \\
&= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1+x}{p}\right) - \left(\frac{1}{p}\right) \\
&= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) - 1 \\
&=
\end{aligned}$$

Como la cantidad de residuos cuadráticos modulo p y la cantidad de residuos no cuadráticos modulo p coinciden, tenemos $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) = 0$. Por tanto,

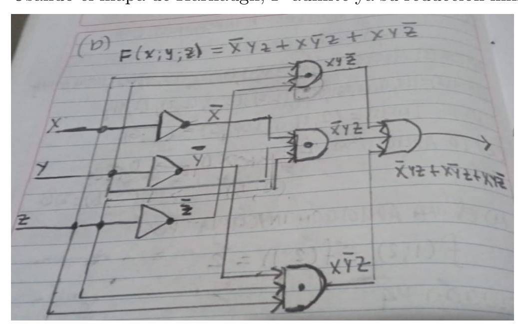
$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = 0 - 1 = -1\,.$$

4. La tabla de verdad es:

x	y	z	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

de donde $F(x, y, x) = \overline{x}yz + x\overline{y}z + xy\overline{z}$.

5. Usando el mapa de Karnaugh, F admite ya su reducción mínima. El circuito correspondiente es:



UNI, 24 de julio del 2023 *

*Hecho en LaTeX

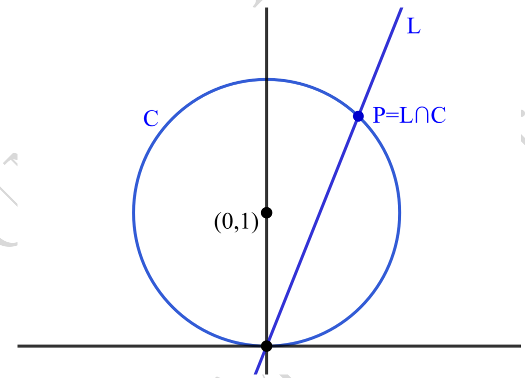
Matemática discreta
Solucionario Examen Parcial
20 de octubre de 2023

1. Para $X \subseteq \mathbb{R}^2 \setminus \{0\}$ no vacío considere la siguiente relación de equivalencia:

$$u \sim v \leftrightarrow \exists \lambda \in \mathbb{R} \setminus \{0\} \text{ tal que } u = \lambda v.$$

a) Cuando $X = \mathbb{R}^2 \setminus \{0\}$ pruebe que $X/\sim$ está en biyección una circunferencia. [2 pts]

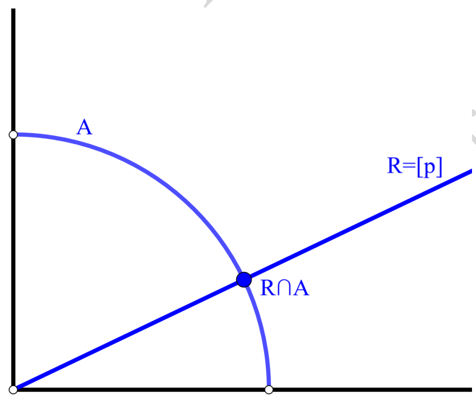
Solución. Notemos que las clases de equivalencia son rectas que pasan por el orígen a las que se le ha removido el origen,. Consideremos la circunsferencia C con centro en $(0,1)$ y radio uno. Cada clase, salvo la contenida en el eje x, corta a un único punto C.



Denotemos $E = \{(1,0)\}$. Definamos $F : \mathbb{R}^2/\sim \longrightarrow C$ como $F([u]) \in [u] \cap C$ si $[u] \neq E$ y $F(E) = O$. Claramente es una biyección. □

b) Dé un sistema de representates (s.d.r.) cuando $X = \mathbb{R}^2_+$. [2 pts]

Solución. Notemos que las clases de equivalncia son los rayos que parten del origen dentro del primer cuadrante. Si consideramos un arco A de circunsferenica (centrada en el origen) interseptado con el primer cuadrante, cara una de las clases va a cortar en un ˇnico punto a dicho arco, por tanto este sería un sistema de representantes.



$\square$

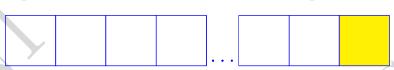
c) Cuando $X = \mathbb{N}^2$ pruebe que $\{(n, m) \in \mathbb{N}^2$ con n, m coprimos$\}$ es un s.d.r. [2 pts]

Solución. Llamemos $S = \{(n, m) \in \mathbb{N}^2$ con n, m coprimos$\}$. Notemos que en $\mathbb{N}^2$, $(n_1, m_1) \sim (n_2', m_2')$ si y solo sí $\dfrac{n_1}{m_1} = \dfrac{n_2'}{m_2'}$. Para un punto $(a, b) \in \mathbb{N}^2$ sabemos que $\dfrac{a}{b}$ se puede expresar de manera única como una fracción irreducible es decir $\dfrac{a}{b} = \dfrac{n}{m}$ con n, m coprimos y por tanto $(a, b) \sim (n, m) \in S$. Por la unicidad tenemos que S es un sistema de representantes. $\square$

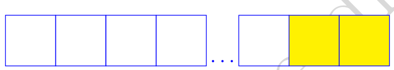
2. Considere un tablero $1 \times n$ el cual disponemos a llenar con fichas 1×1 y 1×2 (dominos) sin salirse, y F_k la secuencia de Fibonacci con $F_0 = F_1 = 1$. Pruebe que:

a) Hay F_n formas de llenar el tablero.

Solución. Sea T_n la cantidad de formas de llenar un tablero $1 \times n$, por ejemplo $T_1 = 1$ y $T_2 = 2$ ya que puede ser llenado por dos fichas 1×1 o con un solo dominó. Consideremos un tablero de $1 \times (n + 1)$, al ser llenado por nuestras fichas la útima casilla hay dos posibilidades: Es llenada por una ficha 1×1 o es llenada con un dominó. En el primer caso el resto del tablero puede ser llenado de T_n formas por defnición



En el segundo caso el resto del tablero puede ser llenado de T_{n-1} formas



Por tanto el total de formas de llenar al tablero es $T_{n+1} = T_n + T_{n-1}$ por tanto cumple la misma fórmula recursiva que los números de Fibonaccio por otro lado $T_1 = 1 = F_1$ y $T_2 = 2 = F_2$ por inducción fuerte obtenemos que para todo $n \in \mathbb{N} : T_n = F_n$. $\square$

b) Para todo $k \leq n/2$ el tablero se puede rellenar usando exactamente k dominos de $\dbinom{n-k}{k}$ formas.

Solución. Si un tablero $1 \times n$ al se llenado se usan k dominós, notamos que $2k \leq n$ y las $n - 2k$ casillas restantes se rellenan con fichas 1×1 en total usandose $n - k$ fichas. De estas $n - k$ fichas debemos escoger las posiciones de los k dominos y esto se puede hacer de $\dbinom{n-k}{k}$ formas. $\square$

c) Para todo $n \in \mathbb{N}$ se cumple $F_n = \displaystyle\sum_{0 \leq k \leq n/2} \binom{n-k}{k}$.

Solución. Consideremos X el conjunto de formas de llenar al tablero. Sea $\delta : X \longrightarrow \{0, 1, \ldots, \lfloor n/2 \rfloor\}$ la función que cuenta cuantos dominos se usaron. Por ejemplo $\delta(0) = 1$ ya que corresponde cuando se usan n fichas 1×1. Por la parte a) tenemos que $\#X = F_n$ y por la parte b) las fibras $\#\delta^{-1}(k) = \dbinom{n-k}{k}$. Como

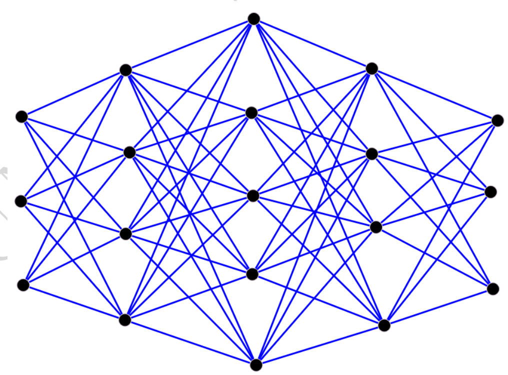
$$\#X = \sum_{0 \leq k \leq n/2} \#\delta^{-1}(k)$$

obtenemos el resultado. $\square$

3. Dado $\kappa = (k_0, k_1, \ldots, k_r) \in \mathbb{N}^{r+1}$ se define el grafo neuronal de tipo κ como el grafo con vértices $V = V_0 \cup V_1 \cup \ldots \cup V_r$ y aristas $A = \displaystyle\bigcup_{j=1}^{r} [V_{j-1}, V_j]$ donde los V_i, llamados capas, son disjuntos y $\#V_i = k_i$. Fijemos $\kappa = (k_0, k_1, \ldots, k_r)$ y $0 \leq i < j \leq r$.

a) Esboze un grafo neuronal de tipo $(3, 4, 5, 4, 3)$. [1 pt]

Solución. Considere el siguiente grafo siendo las capas las columnas verticale:



□

b) ¿Cuantos subgrafos de un grafo neuronal de tipo κ son caminos de longitud mínima conectando vértices de la capa i a la capa j? [2 pts]

Solución. Digamos que $j = i+\ell$, notamos que un camino de la capa i a la capa j tiene que pasar por aristas de capas $i, i+1, \ldots, i+\ell = j$ por tanto la longitud mínima debe ser $\ell = j-i$, por cada camino debemos escoger un vértice por cada una de las capas $i, i+1, \ldots, i+\ell$ esto se puede hacer de multiplicando la cantidad de vértices de cada una de estas capas, es decir hay $\kappa_i \cdot \kappa_{i+1} \cdots \kappa_{i+\ell}$ tales caminos. □

c) ¿Cuantos subgrafos de un grafo neuronal de tipo κ son ciclos de longitud mínima pasando por vértices de la capa i a la capa j? [2 pts]

Solución. Notamos que un ciclo de longitud mínima que pase por los vértices de las capas i y j debe estar formado por dos caminos que conecten un vértice de la capa i con uno de la capa j. Para el primer caminos hay $\kappa_i \cdot \kappa_{i+1} \cdots \kappa_{i+\ell}$ elecciones, para el segundo como ya teenmos fijos los extremos hay $(\kappa_{i+1}-1)\cdots(\kappa_{i+\ell-1}-1)$ per al hacer estas elecciones estamos contando cada ciclo dos veces por tanto el total de ciclos es

$$\frac{1}{2}\kappa_i\kappa_{i+1}(\kappa_{i+1}-1)\cdots\kappa_{j-1}(\kappa_{j-1}-1)\kappa_j$$

Otra forma de hacerlo, es notar que dicho ciclo de lontigud minima va a tomar un vértice de la capa i y de la capa j y dos vértices de las capas intermedias, se puede hacer de

$$\kappa_i\binom{\kappa_{i+1}}{2}\cdots\binom{\kappa_{j-1}}{2}\kappa_j$$

formas, más los vertices escogidos de las $\ell-1$ capas intermedias se puden conectar con $\ell-2$ pares de aristas mas esto se puede de 2 formas distintas

es decir debemos multiplicar por $2^{\ell-2}$ por tanto el total de formas es

$$2^{\ell-2}\kappa_i\binom{\kappa_{i+1}}{2}\cdots\binom{\kappa_{j-1}}{2}\kappa_j$$

Noten que ambas respuestas coinciden. □

d) Sea $\mu = (u_0, u_1, \ldots, u_r) \in \mathbb{N}^{r+1}$ con $u_i \leq k_i$ para todo $i \in \{0, \ldots, r\}$. ¿Cuantos subgrafos neuronales de tipo μ contiene uno de tipo κ? [1 pt]

Solución. Para formar estos subgrafos para $p \in \{0, 1, \ldots, r\}$ debemos escoger u_p vértices de los k_p de las capa p, es decir de $\binom{k_p}{u_p}$ formas. Por tanto el total de subgrafos de tipo μ es

$$\binom{k_0}{u_0}\binom{k_1}{u_1}\cdots\binom{k_r}{u_r}$$

□

4. Sea $d \in \mathbb{N}$ y A la matriz de adyacencia del grafo completo K_d.

a) Contando recorridos de longitud dos determine A^2. [2 pts]

Solución. Enumeremos los vértices $v_1, \ldots, v_d$. Si $A^2 = [a_{i,j}]$ sabemos que $a_{i,j}$ cuenta los 2−recorridos de v_i a v_j. De v_i a v_j dichos recorridos son de la forma $v_iv_kv_j$ con $k \notin \{i,j\}$ por tanto hay $d-2$. Por otro lado de v_i a v_i los recorridos son $v_iv_kv_i$ para $k \neq i$, por tanto hay $d-1$, esto es

$$a_{ij} = \begin{cases} d-1 & \text{si } i=j \\ d-2 & \text{para } i \neq j \end{cases}$$

. □

b) Pruebe por inducción que $A^{n+1} = (a_n + (-1)^n)A + a_nI$ y $a_{n+1} = (d-1)\big(a_n + (-1)^n\big)$. [3 pts]

Solución. Noten que A es la matriz con 0 en la diagonal y 1 en sus otras entradas. De la parte *a*) tenemos que $A^2 = (d-2)A + (d-1)I$ así con $a_1 = d-1$ se verifica la primera identidad para el caso $n=1$. Supongamos que $A^{n+1} = (a_n + (-1)^n)A + a_nI$, luego

$$A^{n+2} = AA^{n+1} = (a_n + (-1)^n)A^2 + a_nA = \big(a_n + (-1)^n\big)\big((d-2)A + (d-1)I\big) + a_nA$$

oten que la matriz identidad tiene coeficiente $\big(a_n + (-1)^n\big)(d-1)$ y el coeficiente de A es

$$(a_n + (-1)^n)(d-2) + a_n = (d-1)a_n + (-1)^n(d-2) = \big(a_n + (-1)^n\big)(d-1) - (-1)^n$$

es decir tomando $a_{n+1} = \big(a_n + (-1)^n\big)(d-1)$ tenemos que

$$A^{n+2} = \big(a_{n+1} + (-1)^{n+1}\big)A + a_{n+1}I$$

como se pedia probar. □

c) Para $d = 6$ determine a_4 y A^4. [1 pt]

Solución. Para $d = 6$ tenemos que $A^2 = 4A + 5I$ y $a_1 = 5$. De la relación recursiva $a_{n+1} = 5\big(a_n + (-1)^n\big)$ obtenemos $a_2 = 20$, $a_3 = 105$ y $a_4 = 521$. Por otro lado $A^4 = (a_3 - 1)A + a_3I$ es decir si $A^4 = [c_{ij}]$

$$c_{ij} = \begin{cases} 105 & \text{si } i=j \\ 104 & \text{para } i \neq j \end{cases}$$

□

5. **Pregunta Extra** (En caso la haga reemplaza a una de las anteriores)

Una permutación $\sigma \in S_n$ es llamada un desarreglo si $\forall k \leq n : \sigma(k) \neq k$. (Puebe interpretarse que se barajan n cartas enumeradas de 1 a n y $\sigma(k)$ es la numeración de k-esima carta).

a) Para $k \leq n$ denotamos $A_k = \{\sigma \in S_n / \, \sigma(k) = k\}$. Muestre que $\#A_k = (n-1)!$ [1 pt]

Solución. Como $\sigma(k) = k$, los valores restantes de sigma forman una permutación de $I_n \setminus \{k\}$ el cual tiene $n-1$ elementos por tanto hay $(n-1)!$ permutaciones. □

b) Para $k_1 < k_2 < \ldots < k_r \leq n$. Muestre que [2 pts]

$$\#(A_{k_1} \cap A_{k_2} \cap \ldots \cap A_{k_r}) = (n-r)!$$

Solución. Noten que $\sigma \in A_{k_1} \cap A_{k_2} \cap \ldots \cap A_{k_r}$ cuando $\sigma(k_1) = k_1, \sigma(k_2) = k_2, \ldots, \sigma(k_r) = k_r$ quedando $n-r$ valores de sigma los cuales forman una permutación de $I_n \setminus \{k_1, k_2, \ldots, k_r\}$ que al tener $n-r$ elementos, deben haber $(n-r)!$ de tales permutaciones. □

c) Explique como usar el principio de inclusion-exclusión para probar que el número de desarreglos en S_n cumple $D_n = \displaystyle\sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$. [3 pts]

Solución. Noten que el conjunto de desarreglos de S_n es el complemento de $A_1 \cup A_2 \cup \ldots \cup A_n$. Por el principio de inclusión exclusion tenemos

$$\#(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{J \in P^*(I_n)} (-1)^{\#J-1} \#(A_{j_1} \cap A_{j_2} \cap \ldots \cap A_{j_r})$$

agupandor los índices con el mismo número de elementos

$$\sum_{J \in P^*(I_n)} (-1)^{\#J-1} \#(A_{j_1} \cap A_{j_2} \cap \ldots \cap A_{j_r}) = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)!$$

Así la cantidad de desarreglos será

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

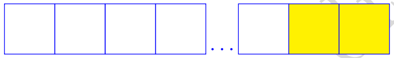
incorporando $n!$ como el termino $k=0$ obtenemos el resultado. □

Matemática discreta
Solucionario PC1
15 de septiembre 2023

1. Para $n \in \mathbb{N}, n \geq 2$ considere tableros $n \times n$. Se disponen de suficientes fichas 2×1 y 3×1 para colocar en el tablero llenando casillas consecutivas, ya sea vertical u horizontalmente. Pruebe que:

a) Para $2 \leq m \leq n$, toda franja de $m \times 1$ puede ser cubierta con las fichas mencionadas (pudiendo ser solo de un mismo tipo). [2 pts]

Solución. Para el caso de la franja de m casillas si $m = 2, 3$ basta colocar una ficha 2×1 y 3×1 respectivamente.
Fijemos $m \geq 3$, si asumimos cierto el resultado para franjas de k casillas con $2 \leq k \leq m$, veamos que podemos probarlo para una franja de $m+1$.
Para tal franja podemos colocar una ficha 2×1 al final faltando llenar una franja de $m-1$ casillas, lo que por hipótesis inductiva es posible llenar, por tanto podemos llenar la franja de $m+1$ casillas con las fichas mencionadas. Así por inducción fuerte siempre podemos llenar las franjas mencionadas.



□

b) En general para $n \geq 3$ si escojemos una casilla cualquiera, el resto del tablero puede llenarse con las fichas mencionadas, de modo que no se salgan del tablero. (Sug. Proceda por inducción) [3 pts]

Solución. Para tableros 3×3 hay que cosniderar 3 casos: cuando se remueve una esquina, cuando se remueve la casilla central y cuando se remueve la casilla de en medio de un lado. Notar que cuando se remueve la casilla central el resto se puede llenar con 4 fichas 2×1. En los otros casos se puede rellenar con una ficha 2×1 y dos fichas 3×1.
Supongamos que es cierto para bloques $n \times n$, es decir que si quitamos una casilla podemos rellenar el resto con las ichas dadas. Para un tablero $(n+1) \times (n+1)$ al remover una casilla esta se va a encontrar en uno de los 4 subtableros $n \times n$ que admite nuestro tablero. Por inducción sabemos que podemos el subtablero $n \times n$ con las fichas dadas y por el item anterior tambien podemos llenar las dos ranjas restantes (una vertical $1 \times (n+1)$ y una horizontal $n \times 1$). En conclusion podemos llenar el tablero con la casilla removida.

Mate discreta UNI

El gráfico representa un tablero 11×11 cuando se remueve una ficha en el subtablero 10×10 superior izquierdo. y las dos franjas restantes. $\square$

2. Sea X un conjunto no vacío y 2^X el conjunto de funciones de X a $\{0,1\}$. Considere $\chi : P(X) \longrightarrow 2^X$ definida como $\chi(A) := \chi_A$ la función que vale 1 en puntos de A y 0 en puntos fuera de A. Pruebe que χ es una biyección. [4 pts]

Solución. $\chi : P(X) \to 2^X$ definida por $\chi(A) = \chi_A$.

- **Inyectividad:** Sean $A, B \subset X$ distintos, entonces $\exists c \in (A \setminus B) \sqcup (B \setminus A)$.
  En caso $c \in A \setminus B$: tenemos $\chi_A(c) = 1 \neq 0 = \chi_B$.
  En caso $c \in B \setminus A$: tenemos $\chi_B(c) = 1 \neq 0 = \chi_A$.
  En ambos casos $\chi_A \neq \chi_B$.
- **Sobreyectividad:** Sea $f : X \to \{0;1\}$, definimos $A_f := \{a \in X : f(a) = 1\}$.
  Afirmación: $\chi_{A_f} = f$. En efecto, si $x \in A_f$ entonces $\chi_{A_f}(x) = 1 = f(x)$; si $x \notin A_f$ entonces $\chi_{A_f}(x) = 0 = f(x)$.

$\square$

3. Pruebe que las siguientes afirmacionaciones para números naturales:

   a) Para $n > 1$ se tiene que $n^4 + n^2 + 1$ es compuesto. [2 pts]

Solución. Sea $n \in \mathbb{N}$ con $n > 1$, notemos que

$$(n^2+1+n)(n^2+1-n) = (n^2+1)^2 - n^2 = n^4 + n^2 + 1 \qquad (1)$$

Como $n \in \mathbb{N}$, entonces $n^2 + 1 + n \geq 3$, por otro lado $n \geq 2$, entonces

$$n^2 + 1 - n = \left(n - \frac{1}{2}\right)^2 + \frac{3}{4} \geq 3$$

luego la factorización en naturales (1) es no trivial (ningún factor es 1), por lo tanto $n^4 + n^2 + 1$ es compuesto. $\square$

   b) Si p y $q = p + 2$ son primos con $p > 3$ entonces $p + q$ es divisible por 12. [2 pts]

Solución. Sabemos que $p, q = p + 2 \in \mathcal{P}$ y $p > 3$, luego $p + q = p + (p+2) = 2p + 2$.
Afirmamos que p es impar. En efecto, si p es par entonces $p = 2$ y $q = 4$ no es primo, contradiciendo la parte de las hipótesis.
Ahora mostremos que $4 \mid 2p + 2$ y $3 \mid 2p+2$.

- $\underline{4 \mid 2p+2}$**:** Notemos que existe $k \in \mathbb{N}$ y $k \geq 3$ tal que $p = 2k - 1$, pues si $k = 1$ o $k = 2$ se sigue que $p = 1$ o $p = 3$ respectivamente. Por lo tanto $p + q = 2p + 2 = 2(2k-1) + 2 = 4k$.
- $\underline{3 \mid 2p+2}$**:** Afirmamos que $p = \mathring{3} + 2$. En efecto si $p = \mathring{3} + 1$, tenemos $q = p + 2 = (\mathring{3} + 1) + 2 = \mathring{3}$, luego $q \notin \mathcal{P}$, contradiciendo la hipótesis.
  Luego $p + q = 2p + 2 = 2(\mathring{3} + 1) + 2 = \mathring{3}$.

Finalmente $p + q = \overset{\circ}{mcm(4;3)} = \mathring{12}$. $\square$

4. Considere la relación en $\mathbb{R}$: $x \sim y$ si $x - y \in \mathbb{Z}$. Pruebe que:

   a) $\sim$ es una relación de equivalencia. [2 pts]

Solución.

- **Reflexiva:** Sea $x \in \mathbb{R}$, como $x - x = 0 \in \mathbb{Z}$ se tiene que $x \sim x$.
- **Simétrica:** Sean $x, y \in \mathbb{R}$ tales que $x \sim y$, entonces $x - y \in \mathbb{Z}$ y por tanto $y - x = -(x - y) \in \mathbb{Z}$, de donde $y \sim x$.
- **Transitiva:** Sean $x, y, z \in \mathbb{R}$ tales que $x \sim y$ e $y \sim z$, entonces $x - y, y - z \in \mathbb{Z}$ y por tanto $x - z = (x - y) + (y - z) \in \mathbb{Z}$, de donde $x \sim z$.

Concluímos que la relación dada $\sim$ es de equivalencia. $\square$

   b) $[0,1[$ es un sistema de representantes. [1 pt]

Solución. Denotemos $\widetilde{x} := \{y \in \mathbb{R} : y \sim x\}$ la clase de equivalencia de x, $\mathcal{C} := \{\widetilde{x} : x \in \mathbb{R}\}$ el conjunto de las clases de de equivalencia.
Definimos la "función":

$$\begin{array}{rccc} \varphi : & \mathcal{C} & \to & [0;1[\\ & \widetilde{x} & \mapsto & x - \lfloor x \rfloor \end{array}$$

veamos que está bien definida y es una biyección.

- **Buena definición:** Sean $x_1, x_2 \in \widetilde{x}$, veamos que $\varphi(\widetilde{x_1}) = \varphi(\widetilde{x_2})$. En efecto, tenemos $x - x_1, x - x_2 \in \mathbb{Z}$, luego $k = x_1 - x_2 \in \mathbb{Z}$ de donde

$$\varphi(\widetilde{x_1}) = x_1 - \lfloor x_1 \rfloor = x_2 + k - \lfloor x_2 + k \rfloor = x_2 - \lfloor x_2 \rfloor = \varphi(\widetilde{x_2}).$$

- **Biyectividad:** Dado $x \in [0;1[$ se tiene $\lfloor x \rfloor = 0$, de donde

$$\varphi(\widetilde{x}) = x - \lfloor x \rfloor = x,$$

luego φ es sobreyectiva.
Sea $x, y \in \mathbb{R}$, tales que $\varphi(\widetilde{x}) = \varphi(\widetilde{y})$ mostremos que $\widetilde{x} = \widetilde{y}$. En efecto, como $x - \lfloor x \rfloor = y - \lfloor y \rfloor$ se sigue $x - y = \lfloor x \rfloor - \lfloor y \rfloor \in \mathbb{Z}$, de donde $\widetilde{x} = \widetilde{y}$, luego φ es inyectiva.

□

c) El cociente $\mathbb{R}/\sim$ está en biyección con una circunferencia. [2 pts]

Solución. Recuerde que $\mathbb{R}/\sim = \{\widetilde{x} : x \in \mathbb{R}\}$. Denotamos $\mathcal{C}_1$ la circunferencia de radio 1. Notamos que la función $\psi : [0;1[\to \mathcal{C}_1$ definida por $\psi(t) = (\cos(2\pi t); \sin(2\pi t))$ es un biyección. □

5. **(Pregunta extra)** Prueba que hay infinitos primos de la forma múltiplos de 4 más 3. (*En caso la haga reemplaza alguna de las anteriores*)

Solución. Procediendo por reducción al absurdo.
Suponga $\mathcal{P}_3 = \{p \in \mathcal{P} : p = \mathring{4} + 3\}$ es finito, denote $N = \max_{p \in \mathcal{P}_3}\{p\}$. Considere

$$M := 3 + 4 \prod_{\substack{p \in \mathcal{P}\setminus\{3\} \\ p \le N}} p = 3 + \mathring{4} > N \tag{2}$$

Afirmación 1: $M \notin \mathcal{P}_3 \to \exists q \in \mathcal{P}_3, [q \mid M]$. En efecto, si todos los divisores de M fueran $\mathring{4} + 1$ entonces $M = \mathring{4} + 1$ contradiciendo la ecuación (2).
Afirmación 2: $\forall q \in \mathcal{P}_3, [q \nmid M]$. En efecto, en caso $q = 3$ la afirmación es cierta pues 3 no aparece en el producto de números primos en (2); caso contrario $q \in \mathcal{P}_3 \setminus \{3\}$ se tiene $q \in \mathcal{P}\setminus\{3\}$ con $q \le N$, es decir $q \mid \prod_{\substack{p \in \mathcal{P}\setminus\{3\} \\ p \le N}} p$, por lo tanto si $q \mid M$ entonces $q \mid 3 = M - \prod_{\substack{p \in \mathcal{P}\setminus\{3\} \\ p \le N}} p$, de donde $q = 3$ (absurdo).
De la afirmación 2 y la contrapuesta de la afirmación 2 se deduce que $M \in \mathcal{P}_3$ y $N < M < N$ (absurdo). □

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática
Ciclo 2023-I

Practica Calificada 1 de Matemática Discreta

1. Decir si las siguientes afirmaciones son verdaderas (V) o falsas (F). Justifique su respuesta. (4pts)
   (a) La unión de dos relaciones de equivalencia es una relación de equivalencia.
   (b) La composición[1] de dos relaciones de equivalencia es una relación de equivalencia.
   (c) La unión de dos ordenes parciales es un orden parcial.
   (d) La composición de dos ordenes parciales es un orden parcial.

2. Sea R una relación sobre $\mathbb{R}$. Dar un ejemplo con gráfica de cada uno de los siguientes: (6pts)
   (a) R reflexiva, pero no simétrica ni antisimetrica.
   (b) R simétrica, pero no reflexiva ni antisimetrica.
   (c) R antisimetrica, pero no reflexiva ni simétrica.

3. Se define la relación $\sim$ sobre el conjunto $A = \mathbb{Z} \times \mathbb{Z}^*$ como

$$(a,b) \sim (c,d) \text{ si y sólo si } a \times d = b \times c.$$

   Dicha relación $\sim$ es de equivalencia y permite construir los números racionales.
   Responda y justifique: (4pts)
   a) ¿Es cierto que $\mathbb{Q} = \{[(a,b)] : (a,b) \in \mathbb{Z} \times \mathbb{Z}^* : MCD(a,b) = 1\}$?.
   b) ¿Por que decimos que $\mathbb{Z} \subset \mathbb{Q}$?.

4. Sea $A = \{1, 2, 4, 6, 8\}$ y para $a, b \in A$ defina $a \preccurlyeq b$ si y sólo si a/b es un entero. (6pts)

[1] Si R y S son dos relaciones sobre un conjunto A, la *composición* $S \circ R$ se define como el conjunto de los pares $(x,z) \in A \times A$ tales que $(x,y) \in R$ y $(y,z) \in S$

Mate discreta UNI

a) Pruebe que $\preccurlyeq$ define un POSET en A.

b) Dibuje el diagrama de Hasse para $\preccurlyeq$.

c) Liste todos los elementos mínimo, máximo, minimal y maximal.

d) ¿Es un orden total?. Justifique la respuesta o dar un contraejemplo.

Solución:

1. (a) (F) Falla en la transitividad. Considere las relaciones de equivalencias sobre $\{1,2,3\}$: $R = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ y $S = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$. Note que $(1,2),(2,3) \in R \cup S$ pero $(1,3) \notin R \cup S$.

   (b) (F) Falla en la simetría. Considere las relaciones de equivalencias sobre $\{1,2,3\}$: $R = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$ y $S = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$. Note que $(1,3) \in S \circ R$ pero $(3,1) \notin S \circ R$.

   (c) (F) Falla en la transitividad. Considere las relaciones de orden sobre $\{1,2,3\}$: $R = \{(1,1),(2,2),(3,3),(1,2)\}$ y $S = \{(1,1),(2,2),(3,3),(2,3)\}$. Se tiene que $(1,2),(2,3) \in R \cup S$ pero $(1,3) \notin R \cup S$.

   (d) (F) Falla en la antisimetria. Considere las relaciones de orden sobre $\{1,2,3\}$: $R = \{(1,1),(2,2),(3,3),(1,2)\}$ y $S = \{(1,1),(2,2),(3,3),(2,1),(3,1),(3,2)\}$. Note que

   $$S \circ R = \{(1,1),(2,2),(3,3),(1,2),(2,1),(3,1),(3,2)\}$$

   Tenemos $(1,2),(2,1) \in S \cup R$ pero $1 \neq 2$.

2. (a) Un ejemplo de una relación R reflexiva, pero no simétrica ni antisimetrica se muestra en la Figura (1).

   (b) Un ejemplo de una relación R simétrica, pero no reflexiva ni antisimetrica. se muestra en la Figura (2).

   (c) Un ejemplo de una relación R antisimetrica, pero no reflexiva ni simétrica se muestra en la Figura (3).

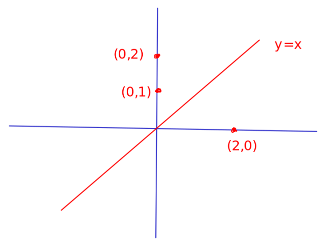


Figure 1:

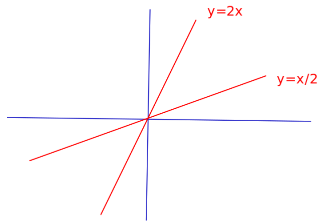


Figure 2:

3. a) Si es cierto, sea $[(a,b)]$ se presentan dos casos:
   - Si $MCD(a,b) = 1$ no habría nada que probar.
   - Si $MCD(a,b) > 1$ entonces existe $d = MCD(a,b) > 1$ tal que $a = d\alpha$ y $b = d\beta$ con α, β primos entre si. Como $(\alpha,\beta) \sim (a,b)$ entonces $[(a,b)] = [(\alpha,\beta)]$.

   b) El motivo es por que existe una copia de $\mathbb{Z}$ que esta en $\mathbb{Q}$ el cuál esta dado por
   $$\mathbb{Z}' = \{[(a,1)] : \ a \in \mathbb{Z}\}$$
   El significado de copia es un isomorfismo de $\mathbb{Z}'$ a $\mathbb{Z}$ dado por $[(a,1)] \mapsto a$

4. a)
   - Reflexiva
   $$a \preccurlyeq a \ \forall a \in A.$$
   - Simétrica
   Si $a \preccurlyeq b$ y $b \preccurlyeq a$ entonces $a = b$.

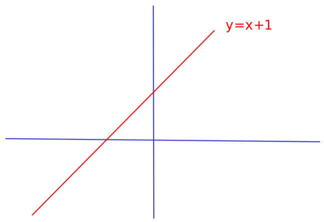
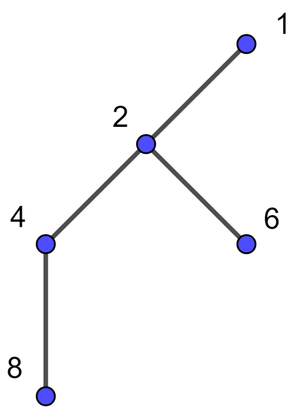


Figure 3:

- Transitiva
  Si $a \preccurlyeq b$ y $b \preccurlyeq c$ entonces $a = kb$ y $b = rc$ con k, r enteros luego $a = (kr)c$, es decir $a \preccurlyeq c$.

Por tanto $\preccurlyeq$ es una relación de orden parcial.



b)

c) Elementos mínimales: 6 y 8
Mínimo elemento: No existe
Elementos maximales: 1
Máximo elemento: 1

d) No es una relación de orden total ya que 6 y 8 son elementos no comparables.

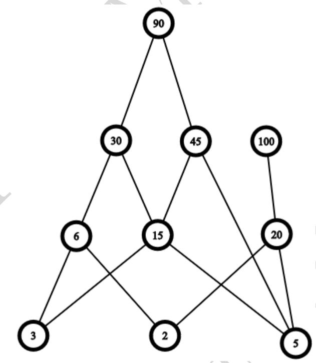
UNI, 10 de abril del 2023.

Matemática discreta
Solucionario PC2
29 de septiembre 2023

1. Considere $A = \{2, 3, 5, 6, 15, 20, 30, 45, 90, 100\}$ con el orden $a \prec b$ si $a \mid b$.

   a) Dé su diagrama de Hasse indicando solo las aristas que corresponden a vértices consecutivos. [1 pt]

   Solución.



□

   b) Determine si tiene mínimo, máximo, sus los elementos maximales y minimales. [1 pt]

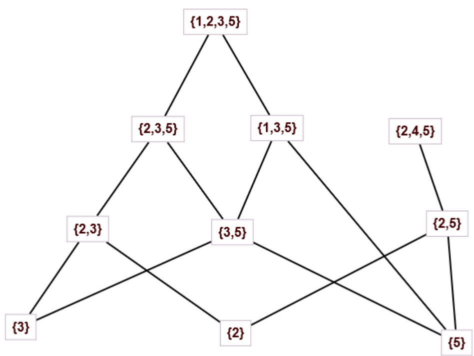
   Solución. Tiene dos maximales 90, 100 y tres minimales 2,3,5 en particular no tiene ni máximo ni mínimo. □

   c) Determine cuantas cadenas de longitud máxima hay en A. [1 pt]

   Solución. Notamos que la longitud máxima de las cadenas es 3 las cuales comienzan en un minimal y terminan en el maximal 90, de ellas tres comienzan en 3, una en 2 y dos 5 por tanto hay 6. Explicitamente:{3,6,30,90},{3,15,30,90},{3,15,45,90},{2,6,30,90},{5,15,30,90},{5,15,45,90}. □

   d) Determine si existe un subcojunto de $P(I_5)$ tal que ordenado con la inclusión es isomorfo a A. [2 pts]

Solución. Como $P(I_5)$ tiene máximo y mínimo para encontrar tal subconjunto, este no puede tener a $\varnothing$ ni a I_5 como elementos y como 2,3,5 estan en extremos de cadenas de longitud 4 solo les pueden corresponder unitarios digamos que les corresponden $\{2\},\{3\},\{5\}$ respectivamente. El siguiente grafo corresponde al ismorfismo buscado, haciendo corresponder cada vertivce con su respectivo del diagrama de Hasse.



Noten que escogemos que a 100 le corresponda $\{2,4,5\}$ para evitar que este contenido en $\{1,2,3,5\}$ y no haya una arista entre ambos nodos. Explicitamente el isomorfismo $f : A \longrightarrow P(I_5)$ viene dado por $f(n) = \{\text{divisores primos de } n\}$ para $n \leq 30$ y $f(45) = \{1,3,5\}, f(90) = \{1,2,3,5\}, f(100) = \{2,4,5\}$, $\square$

2. Sea X un conjunto de n elementos y $n \geq k$. Considere $P_k(X)$ el conjunto de particiones de X de k partes y $S_k(X) = \{f : X \longrightarrow I_k : \ f \text{ es sobreyectiva }\}$. Para $f \in S_k(X)$ defina $\psi(f)$ como el conjunto de fibras de f.

   a) Verifique que para $f \in S_k(X)$ se tiene que $\psi(f) \in P_k(X)$. [1 pt]

   Solución.
   Sea $f \in S_k(X)$, se tiene $f : X \to I_k$ sobreyectiva y luego las fibras de f son

   $$\psi(f) = \left\{ f^{-1}(\ell) : \ \ell \in \{1 \ldots, k\} \right\}$$

   lo que forma una partición de X con k partes pues son disjuntas, luego $\psi(f) \in P_k(X)$. $\square$

   b) Pruebe que función $\psi : S_k(X) \longrightarrow P_k(X)$ es sobreyectiva. [1.5 pts]

   Solución.
   Sea $\mathcal{A} = \{A_1, \ldots, A_k\} \in P_k(X)$. Definimos la 'función' $g : X \longrightarrow I_k$ como $g(x) = j$ si $x \in A_j$.
   Buena definición de g: Notemos que si $x \in A_i$ y $x \in A_j$ esto solo se puede si $i = j$ ya que $\mathcal{A}$ es una partición.
   Sobreyectividad de g: Como para cada $j \leq k$ tenemos que $A_j \neq \varnothing$ existe $a \in A_j$ y por tanto $g(a) = j$, así g es sobreyectiva, es decir $g \in S_k(X)$.
   Sobreyectividad de ψ:
   Afirmamos que $\psi(g) = \{A_1, \ldots, A_k\}$. Por definición $\psi(g) = \{g^{-1}(1), \ldots, g^{-1}(k)\}$. Por otro lado para $1 \leq j \leq k$ tenemos $g^{-1}(j) = A_j$ ya que $x \in A_j$ si y solo sí $g(x) = j$, equivalentemente $x \in g^{-1}(j)$. Como $\mathcal{A} = \{A_1, \ldots, A_k\} \in P_k(X)$ es una partición cualquiera, concluimos que ψ es sobreyectiva. $\square$

   c) Pruebe que las fibras de ψ tienen $k!$ elementos. [1.5 pts]

   Solución. Consideremos $\mathcal{A} = \{A_1, \ldots, A_k\} \in P_k(X)$ y $g : X \longrightarrow I_k$ como en el ítem anterior, es decir $g(x) = j$ si $x \in A_j$, así tenemos que $g \in \psi^{-1}(\mathcal{A})$.
   Consideremos B_k el conjunto de permutaciones de I_k, ciertamente por cada $\sigma \in B_k$ tenemos que $\sigma \circ g \in S_k(X)$ y $\psi(\sigma \circ g) = \psi(g) = \mathcal{A}$.
   Por otro lado si $\sigma \circ g = \sigma' \circ g$ entonces $\sigma = \sigma'$ (por ser g sobreyectiva), por tanto $k! = \#B_k \leq \#\psi^{-1}(\mathcal{A})$.
   Afirmamos que:

   $$\psi^{-1}(\mathcal{A}) = \{\sigma \circ g / \, \sigma \in S_k\}$$

   En efecto, tomemos $h \in \psi^{-1}(\mathcal{A})$ y consideremos $a_j \in A_j$. Como $h(a_1), h(a_2), \ldots h(a_k)$ son los números $1, 2, \ldots, k$ la función $\sigma : I_k \longrightarrow I_k$ definida como $\sigma(j) = h(a_j)$ es una biyección y por definición $\sigma \circ g(a_j) = h(a_j)$, lo cual implica que $\sigma \circ g = h$ ya que ambas uniones son constates en las partes de $\mathcal{A}$. De aquí concluimos que $k! = \#\psi^{-1}(\mathcal{A})$ $\square$

   d) Pruebe que $\#P_k(X) = \frac{1}{k!}\#S_k(X)$. [1 pt]

   Solución. Por la descomposición de fibras de ψ tenemos

   $$\begin{aligned} \#S_k(X) &= \textstyle\sum_{\mathcal{A} \in P_k(X)} \#\psi^{-1}(\mathcal{A}) \\ &= \textstyle\sum_{\mathcal{A} \in P_k(X)} k! \\ &= \#P_k(X) \cdot k! \end{aligned}$$

   concluímos despejando el términe $\#P_k(X)$. $\square$

3. Se tienen n galletas de chocolate y m de vainilla para distribuir en r niños.

   a) Si $r \leq n+m$ de cuantas maneras se pueden distribuir las galletas de modo que todo niño reciba al menos una galleta. [2 pts]

   Solución.
   Notemos que este conteo se puede modelar mediante separadores. Consideremos que colocamos en una linea horizontal las $m+n$ galletas por tanto queda $m+n-1$ espacios entre ellas Simbolizandolas con $*$ cada galleta tenemos:

   $$**$$

   En los $m+n-1$ colocamos $r-1$ separadores. Por ejemplo para repartir 60 galletas en 7 grupos colocamos 6 separadores:

   $$****|*********|**********|*****************|*******|*******$$

   En general estos separadores se pueden distribuir en $\binom{m+n-1}{r-1}$ formas dandonos todas las maneras de distribuir las $m+n$ galletas a r niños. $\square$

b) Si hay suficientes galletas ($2r \leq n$ y $r \leq m$) de cuantas maneras se pueden distribuir las galletas de modo que todo niño reciba al menos dos de chocolate y una de vainilla. [1.5 pts]

Solución. Como e el caso aterior para distribuir m galletas en r niños esto se puede hacer de $\binom{m-1}{r-1}$ formas de modo que todos tengan al menos una. Para distribuir n galletas en r niños de modo que tengan todos al menos 2, podemos pensar que primero le damos una cada uno quedando $n-r$ galletas por ditribuir a los r niños, lo cual es posible ya que $n-r \geq r$, y esto se puede hacer de $\binom{n-r-1}{r-1}$ formas. Al hacer las dos distribuciones de manera simultánea esto se puede hacer de $\binom{m-1}{r-1}\binom{n-r-1}{r-1}$ formas. □

c) Si hay 100 galletas de chocolate y 18 niños se puede garantizar que uno de los niños recibirá al menos 6 de chocolate? justifique su respuesta. [1,5 pts]

Solución.
Sí existe algún niño con al menos 6 galleta.
Suponga lo contrario, es decir todo niño recibe a lo más 5 galletas.
Luego la cantidad de galletas repartidas no excede $5 \times 18 = 90$ galletas, contradiciendo el hecho de haber repartido 100 galletas.
Otra forma: Usando la fórmula vista en clase el mínimo garantizado es

$$\left\lfloor \frac{100-1}{18} \right\rfloor + 1 = 6$$

□

4. Sea la proposición:
Para cualquier número real α y cualquier entero positivo N, existen enteros p y q tales que

$$1 \leq q \leq N \quad \text{y } |q\alpha - p| < \frac{1}{N}$$

Aplique el principio del palomar indicando claramente los n palomares y los más de n objetos a repartir para probar la proposición precedente. [5 pts]

Solución. Proceda con el principio del palomar:

- Palomares: $\left[\frac{k}{N}, \frac{k+1}{N}\right[$, $k \in \{0, \ldots, N-1\}$
- Palomas: $\{\ell\alpha - \lfloor \ell\alpha \rfloor : \ell \in \{1, \ldots, N+1\}\}$, donde $\lfloor x \rfloor$ es la parte entera de x.

Observe que dos puntos de un mismo palomar están a distancia inferior a $1/N$.
Luego tenemos $N+1$ palomas en N palomares, de donde $\exists i, j \in \{1, \ldots, N+1\}$ distintos, sin pérdida de generalidad podemos suponer $j < i$:

$$\left| i\alpha - \lfloor i\alpha \rfloor - (j\alpha - \lfloor j\alpha \rfloor) \right| = \left| \underbrace{(i-j)}_{q}\alpha + \underbrace{\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor}_{p} \right| < \frac{1}{N}$$

Basta escoger $q := i - j$ y $p := \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$. □

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE MATEMÁTICA
CICLO 2023-I

PRACTICA CALIFICADA 1 DE MATEMÁTICA DISCRETA

---

1. Demuestre que para todo $n \geq 1$ se cumple: (5 puntos)

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n.$$

2. Use el principio de inclusión-exclusión para determinar la cantidad de números telefónicos de 10 dígitos, usando los dígitos $\{1, 2, \ldots, 9\}$, tal que aparecen los números $1, 2$ y 3. El orden y la definición adecuada de los conjuntos será considerado en la calificación. (5 puntos)

3. Hallar el número de permutationes de las letras $ABCDEFGHI$ que contenga la cadena DEF. Justifique su procedimiento rigurosamente. (5 puntos)

4. Dado un numero real α y un entero $n \geq 1$. Probar que existe un numero racional p/q tal que $|\alpha - \frac{p}{q}| < \frac{1}{nq}$. Use el principio del palomar. (Sugerencia: use el hecho que $0 = \{0\alpha\}, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$ están en el intervalo $[0, 1\rangle$, donde $\{x\}$ denota la parte fraccionaria de x, por ejemplo $\{\pi\} = 3$) (5 puntos)

Solución:

1. a) Para probar la cota superior, la idea es analizar los pares i y $(n + +1 - i)$ para cada $i = 1, 2, \ldots, n$.
Observe que cuando $i = 1, 2, \ldots, n$ entonces $n + 1 - i$ toma los valores $n, n-1, \ldots, n$. Por tanto, el producto:

$$\prod_{i=1}^{n} i(n+1-i)$$

contiene el factor $j \in \{1, 2, \ldots, n\}$ exactamente dos veces y así, es exactamente igual a $(n!)^2$. Entonces tenemos:

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)}.$$

A partir de la desigualdad

$$\sqrt{ab} \leq \frac{a+b}{2} \quad \text{para todo} \quad a, b > 0,$$

elegimos $a = i$ y $b = n+1-i$ resultando:

$$\sqrt{i(n+1-i)} \leq \frac{i+(n+1-i)}{2} = \frac{n+1}{2},$$

y así, para $n!$ se obtiene:

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leq \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n,$$

lo cual prueba la cota superior.

b) Para probar la cota inferior es suficiente mostrar que $i(n+1-i) \geq n$ para todo $i = 1, 2, \ldots, n$. Para $i = 1$ e $i = n$ se tiene $i(n+1-i) = n$. Para todo $i = 2, 3, \ldots, n-1$ observe que el producto $i(n+1-i)$ contiene un factor por lo menos mayor que $n/2$ y el otro factor no menor que 2, por tanto, el producto $i(n+1-i) \geq n$ para todo i. Entonces:

$$n! \geq \sqrt{n^n} = n^{n/2},$$

lo cual prueba la cota inferior.

2. Definimos los conjuntos:

- A : conjunto de números telefónicos usando los dígitos $\{1, \ldots, 9\}$.
- A_1 : conjunto de números telefónicos en los cuales el 1 no aparece.
- A_2 : conjunto de números telefónicos en los cuales el 2 no aparece.
- A_3 : conjunto de números telefónicos en los cuales el 3 no aparece.

Por tanto, nos piden calcular:

$$|A \backslash (A_1 \cup A_2 \cup A_3)|. \tag{1}$$

Note que $|A| = 9^{10}$ y $|A_1| = |A_2| = |A_3| = 8^{10}$. Por otra parte, para $1 \leq i < j \leq 3$, se tiene que $|A_i \cap A_j| = 7^{10}$. También se tiene que $|A_1 \cap A_2 \cap A_3| = 6^{10}$. Entonces, usando el principio de inclusión-exclusión se obtiene lo establecido en el problema.

3. Note que el conjunto $\{A, B, C, D, E, F, G, H, I\}$ es biyectivo a $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Por tanto una permutación de $ABCDEFGHI$ se identifica con una permutación en $Sym(9)$. Luego, una permutación que contiene DEF se identifica con una permutacion σ de $Sym(9)$ tal que $\sigma(i) = 4, \sigma(i+1) = 5, \sigma(i+2) = 6$ para algún $i \in \{1, 2, 3, 4, 5, 6, 7\}$. Sea P_i el conjunto de permutationes con tal propiedad. No es dificil notar que cada P_i es biyectivo a $Sym(6)$ que tiene cardinal 6!. Entonces el conjunto de permutaciones deseadas es:

$$P = \bigcup_{i=1}^{7} P_i$$

Como la unión es disjunta, tenemos

$$|P| = \left|\bigcup_{i=1}^{7} P_i\right| = \sum_{i=1}^{7} |P_i| = \sum_{i=1}^{7} 6! = 7!\,.$$

La respuesta es 7!.

4. Particionamos el intervalo $[0, 1\rangle$ en n partes de igual longitud:

$$[0, 1/n\rangle, [1/n, 2/n\rangle, \ldots, [(n-1)/n, 1\rangle$$

Note que hay $n+1$ números $0 = \{0\alpha\}, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$ están en el intervalo $[0, 1\rangle$ en el intervalo $[0, 1\rangle$. Por el principio del palomar dos tales números deben estar en un mismo subintervalo, es decir existen dos enteros $m \geq 0$ y $q \geq 1$ tales que $\{m\alpha\}$ y $\{(m+q)\alpha\}$ están en un mismo subintervalo . Sea $p = q\alpha - \{q\alpha\}$.

Luego

$$|q\alpha - p| = |\{q\alpha\}| < 1/n$$

Finalmente, $|\alpha - p/q| = |\{q\alpha\}| < 1/nq$.

UNI, 23 de abril del 2023.

Matemática discreta
Solucionario PC3
13 de octubre de 2023

---

1. Probar que para $1 \leq k \leq n$ se cumple

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$

[5 pts]

Solución. □

2. Determine si las siguientes afirmaciones son ciertas, justifique su respuesta:

   a) Existe un grafo con secuencia de grados $(1, 2, 2, 3, 3, 4, 4)$. [1pt]

   Solución. Falso. No existe ya que la suma de la secuencia de grados siempre es par, igual al doble de las aristas. □

   b) El grafo C_5 es autocomplementario. [1pt]

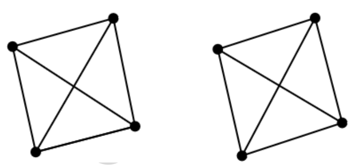
   Solución. Verdad. Ya que el grafo complementario es la estrella de 5 puntas formada por las diagonales del pentagono, la cual es isomorfa a C_5. □

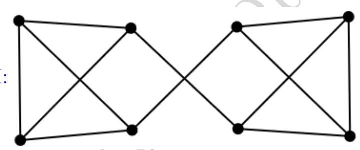
   c) Si un grafo es conexo entonces su complementario es conexo. [1pt]

   Solución. Falso. Por ejemplo considere el grao bipartito $K_{2,2}$ el cual es conexo pero su complemnetario tiene dos componentes, por tanto no es conexo. □

   d) Existen dos grafos de 8 vértices no isomorfos entre sí de modo que todos sus vértices tienen grado 3. [2pts]

   Solución. Verdad. Por ejemplo consideremos los siguientes grafos

G: 

H: 

   ambos tienen 8 vértices todos de grados 3 siembargo no pueden ser isomorfos ya que G es no conexo y H si lo es. □

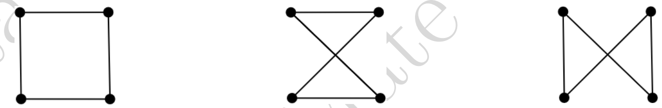
3. Considere el grafo completo de n-vértices K_n y $r \leq n$.

   a) ¿Cuántos subgrafos de K_n son isomorfos a un C_3? [0.5 pt]

   Solución. Notemos que los subgrafos de tipo C_3 de K_n están determinados por sus 3 vértices, así la cantidad de estos es la catidad de subconjuntos de 3 elementos de los vértices, es decir $\binom{n}{3}$. □

   b) ¿Cuántos subgrafos de K_n son isomorfos a un C_r? [2.5 pts]

   Solución. Primero veamos el caso $r = n$ es decir ¿Cuántos r-ciclos se pueden formar con r vértices? Llamemos a_r a esta cantidad. Por ejemplo $a_3 = 1$, $a_4 = 3$ ya que



   corresponden a los 4 ciclos de K_4. En general por cada r ciclo y un vértice adicional podemos formar $r+1$-ciclos por cada una de las r aristas cambiando esta arista por una par conectando a sus extremos con el nuevo vértice, siendo estos todos los posibles, es decir $a_{r+1} = ra_r$. De aquí podemos notar que $a_r = \frac{1}{2}(r-1)!$.
   En el caso general podemos escoger $\binom{n}{r}$ cojuntos de r-vérticies en K_n, para cada elección podemos formar a_r ciclos distintos, por tanto el total de r-ciclos es

$$\binom{n}{r}\frac{1}{2}(r-1)!$$

   . □

   c) ¿Cuántos subgrafos de K_n son isomorfos a un K_r? [0.5 pt]

   Solución. Para formar subgrafos isomorfos a K_r basta tomar r-vértices, esto de puede hacer de $\binom{n}{r}$ formas. □

   d) ¿Cuántos subgrafos de K_n son isomorfos a un $K_{r,s}$? donde $s \leq n - k$. [1.5 pt]

   Solución. Para formar grafos bipartitos tenemos que escoger 2 subcojuntos disjuntos de r y s vértices respectivamete, para el primero hay $\binom{n}{r}$ elecciones y para el segundo con los $n-r$ vértices restantes hay $\binom{n-r}{s}$ por tanto el total de formas es

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

   esto siempre y cuando $r \neq s$. Cuando $r = s$ estamos contando doble cada subgrafo, por tanto en este caso hay

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

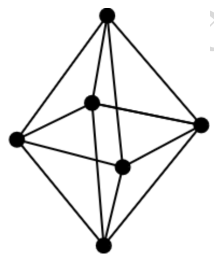
□

4. Dado un grafo $G = (V, A)$ se deie el grafo dual como $G' = (A, A')$ donde

$$A' = \{\{\alpha, \beta\} \in C_2(A) / \, \alpha \cap \beta \neq \varnothing\}$$

a) Para un grafo K_4 esboze su grafo dual K_4' y de su secuencia de grados. [2 pts]

Solución. Como K_4 tiene 6 aristas, K_4' tiene 6 vertices dos de ellos correspondiendo a las diagoales de K_4 las cuales se conectan con los otros 4 vértices de K_4'. Graficando podemos pensar en un octaedro siendo los vertices superior e inferior los que corresponden a las diagonales de K_4



Su secuencia de grados es $(4, 4, 4, 4, 4, 4)$. $\square$

b) Si G es conexo pruebe que G' es conexo. [3 pts]

Solución. Tomemos dos vértices α, β de G', queremos probar que hay un recorrido en G' que los conecta. Vistos como aristas de G tenemos que $\alpha = \{a_1, a_2\}$ y $\beta = \{b_1, b_2\}$. Si comparten un vertice en común por definición hay una arista entre α y β en G' y por tanto estan conectados. En caso no compartan un vértice en común, como G es conexo existe un camino que conecta a_1 con b_1, digamos $c_0 c_1 c_2 \dots c_n$ con $a_1 = c_0$ y $b_1 = c_n$ de modo que $\theta_i = \{c_{i-1}, c_i\}$ es arista de G. En G' tenemos que θ_1 esta conectada con α ya que comparten a a_1 y θ_n esta conectada con β ya que comparten a b_n, es más cada θ_i esta conectada con θ_{i+1} ya que comparte a c_i, por tanto $\theta_1 \theta_2 \dots \theta_n$ es un recorrido en G' que conecta α con β, es decir G' es conexo. $\square$

5. **Pregunta Extra** (en caso la haga reemplaza a una de las anteriores)
Para $n \in \mathbb{N}$ definimos $\tau(n) =$ la cantidad de divisores de n. Pruebe que: [5 pts]

$$\sum_{n \leq x} \tau(n) = \sum_{d \leq x} \left\lfloor \frac{x}{d} \right\rfloor = x \ln(x) + O(x)$$

Solución. $\square$

Matemática discreta
Solucionario PC3
13 de octubre de 2023

1. Probar que para $1 \leq k \leq n$ se cumple

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$

[5 pts]

Solución. Notemos que $\binom{n}{k} = \prod_{j=0}^{k-1} \frac{n-j}{k-j}$ y para $0 \leq j < k$ tenemos

$$\frac{n-j}{k-j} > \frac{n}{k} \iff k(n-j) > n(k-j) \iff nj < kj$$

por tanto $\binom{n}{k} = \prod_{j=0}^{k-1} \frac{n-j}{k-j} \geq \left(\frac{n}{k}\right)^k$.

Para la otra desigualdad partimos de $\binom{n}{k} = \frac{1}{k!} \prod_{j=0}^{k-1} (n-j) \leq \frac{n^k}{k!}$, así bastaría probar que $\frac{n^k}{k!} \leq \left(\frac{en}{k}\right)^k$ o equivalentemente que $k! \geq \left(\frac{k}{e}\right)^k$ para lo cual procedemos por inducción.

Para $k = 1$ es evidente, por otro lado si asumimos que $k! \geq \left(\frac{k}{e}\right)^k$ tenemos que

$$(k+1)! = (k+1)k! \geq (k+1)\left(\frac{k}{e}\right)^k$$

Afirmamos que $(k+1)\left(\frac{k}{e}\right)^k \geq \left(\frac{k+1}{e}\right)^{k+1}$. Claramente es equivalente a

$$\left(\frac{k}{e}\right)^k \geq \frac{(k+1)^k}{e^{k+1}} \iff e \geq \left(\frac{k+1}{k}\right)^k \iff e^{1/k} \geq 1 + \frac{1}{k}$$

siendo esta última desigualdad cierta ya que $e^x \geq 1 + x$ para cualquier $x \geq 0$. De la afirmación anterior sigue $(k+1)! \geq \left(\frac{k+1}{e}\right)^{k+1}$ como se quería demostrar. $\square$

2. Determine si las siguientes afirmaciones son ciertas, justifique su respuesta:

a) Existe un grafo con secuencia de grados $(1, 2, 2, 3, 3, 4, 4)$. [1pt]

Solución. Falso. No existe ya que la suma de la secuencia de grados siempre es par, igual al doble de las aristas. □

b) El grafo C_5 es autocomplementario. [1pt]

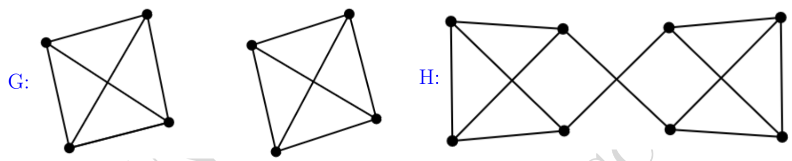
Solución. Verdad. Ya que el grafo complementario es la estrella de 5 puntas formada por las diagonales del pentagono, la cual es isomorfa a C_5. □

c) Si un grafo es conexo entonces su complementario es conexo. [1pt]

Solución. Falso. Por ejemplo considere el grao bipartito $K_{2,2}$ el cual es conexo pero su complemnetario tiene dos componentes, por tanto no es conexo. □

d) Existen dos grafos de 8 vértices no isomorfos entre sí de modo que todos sus vértices tienen grado 3. [2pts]

Solución. Verdad. Por ejemplo consideremos los siguientes grafos



ambos tienen 8 vértices todos de grados 3 siembargo no pueden ser isomorfos ya que G es no conexo y H si lo es. □

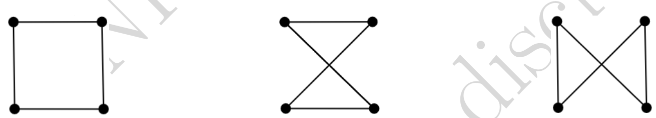
3. Considere el grafo completo de n-vértices K_n y $r \leq n$.

a) ¿Cuántos subgrafos de K_n son isomorfos a un C_3? [0.5 pt]

Solución. Notemos que los subgrafos de tipo C_3 de K_n están determinados por sus 3 vértices, así la cantidad de estos es la catidad de subconjuntos de 3 elementos de los vértices, es decir $\binom{n}{3}$. □

b) ¿Cuántos subgrafos de K_n son isomorfos a un C_r? [2.5 pts]

Solución. Primero veamos el caso $r = n$ es decir ¿Cuántos r-ciclos se pueden formar con r vértices? Llamemos a_r a esta cantidad. Por ejemplo $a_3 = 1$, $a_4 = 3$ ya que



corresponden a los 4 ciclos de K_4. En general por cada r ciclo y un vértice adicional podemos formar $r+1$-ciclos por cada una de las r aristas cambiando esta arista por una par conectando a sus extremos con el nuevo vértice, siendo estos todos los posibles, es decir $a_{r+1} = ra_r$. De aquí podemos notar que $a_r = \frac{1}{2}(r-1)!$.

En el caso general podemos escoger $\binom{n}{r}$ cojuntos de r-vérticies en K_n, para cada elección podemos formar a_r ciclos distintos, por tanto el total de r-ciclos es

$$\binom{n}{r}\frac{1}{2}(r-1)!$$

. □

c) ¿Cuántos subgrafos de K_n son isomorfos a un K_r? [0.5 pt]

Solución. Para formar subgrafos isomorfos a K_r basta tomar r-vértices, esto de puede hacer de $\binom{n}{r}$ formas. □

d) ¿Cuántos subgrafos de K_n son isomorfos a un $K_{r,s}$? donde $s \leq n-k$. [1.5 pt]

Solución. Para formar grafos bipartitos tenemos que escoger 2 subcojuntos disjuntos de r y s vértices respectivamete, para el primero hay $\binom{n}{r}$ elecciones y para el segundo con los $n-r$ vértices restantes hay $\binom{n-r}{s}$ por tanto el total de formas es

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

esto siempre y cuando $r \neq s$. Cuando $r = s$ estamos contando doble cada subgrafo, por tanto en este caso hay

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

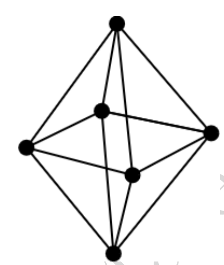
□

4. Dado un grafo $G = (V, A)$ se deie el grafo dual como $G' = (A, A')$ donde

$$A' = \{\{\alpha, \beta\} \in C_2(A) / \alpha \cap \beta \neq \varnothing\}$$

a) Para un grafo K_4 esboze su grafo dual K_4' y de su secuencia de grados. [2 pts]

Solución. Como K_4 tiene 6 aristas, K_4' tiene 6 vertices dos de ellos correspondiendo a las diagoales de K_4 las cuales se conectan con los otros 4 vértices de K_4'. Graficando podemos pensar en un octaedro siendo los vertices superior e inferior los que corresponden a las diagonales de K_4



Mate discreta UNI

Su secuencia de grados es $(4,4,4,4,4,4)$. $\square$

b) Si G es conexo pruebe que G' es conexo. [3 pts]

Solución. Tomemos dos vértices α, β de G', queremos probar que hay un recorrido en G' que los conecta. Vistos como aristas de G tenemos que $\alpha = \{a_1, a_2\}$ y $\beta = \{b_1, b_2\}$. Si comparten un vertice en común por definición hay una arista entre α y β en G' y por tanto estan conectados. En caso no compartan un vértice en común, como G es conexo existe un camino que conecta a_1 con b_1, digamos $c_0c_1c_2\dots c_n$ con $a_1 = c_0$ y $b_1 = c_n$ de modo que $\theta_i = \{c_{i-1}, c_i\}$ es arista de G. En G' tenemos que θ_1 esta conectada con α ya que comparten a a_1 y θ_n esta conectada con β ya que comparten a b_n, es más cada θ_i esta conectada con θ_{i+1} ya que comparte a c_i, por tanto $\theta_1\theta_2\dots\theta_n$ es un recorrido en G' que conecta α con β, es decir G' es conexo. $\square$

5. **Pregunta Extra** (en caso la haga reemplaza a una de las anteriores)
Para $n \in \mathbb{N}$ definimos $\tau(n) =$ la cantidad de divisores de n. Pruebe que: [5 pts]

$$\sum_{n\leq x} \tau(n) = \sum_{d\leq x} \left\lfloor \frac{x}{d} \right\rfloor = x\ln(x) + O(x)$$

Solución. Para la primera igualdad y $n \leq x$ consideremos

$$A_n = \{(x,y) \in \mathbb{N}^2 / \, xy = n\}$$

Así $\#A_n = \tau(n)$. Sea $A = \bigcup_{n\leq x} A_n$, como son disjuntos tenemos que $\#A = \sum_{n\leq x} \tau(n)$. Sea $p : A \longrightarrow \mathbb{N}$ la segunda proyección, es decir $p(x,y) = y$. Notamos que la imagen de p esta en $[1,x]$ y por la descomposición en fibras de p tenemos

$$\#A = \sum_{d\leq x} \#p^{-1}(d)$$

y $(a,d) \in p^{-1}(d) \iff ad \leq n \iff a \leq \frac{n}{d}$ por tanto $\#p^{-1}(d) = \left\lfloor \frac{n}{d} \right\rfloor$ y $\#A = \sum_{d\leq x} \left\lfloor \frac{x}{d} \right\rfloor$.
Para la segunda igualdad usaremos que: $\forall x \in \mathbb{R}$, $\lfloor x \rfloor = x - \{x\}$ donde $\{x\} \in [0;1[$.
Así tenemos

$$\sum_{d\leq x} \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d\leq x} \frac{x}{d} - \left\{ \frac{x}{d} \right\} = x \sum_{d\leq x} \frac{1}{d} - \sum_{d\leq x} \left\{ \frac{x}{d} \right\}$$

Claramente el segundo término en la última igualdad es $O(x)$, así que solo falta estimar el término $\sum_{d\leq x} f(d)$ con $f(x) = 1/x$

$$\sum_{d\leq x} f(d) = \frac{\lfloor x \rfloor}{x} + \ln(x) - \int_1^x \frac{\{x\}}{x^2}\, dx = \ln(x) + O(1)$$

$\square$

Mate discreta UNI

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática Ciclo 2023–I

PRACTICA CALIFICADA 3 DE MATEMÁTICA DISCRETA

1. Determine la veracidad de las siguientes proposiciones: (5 puntos)

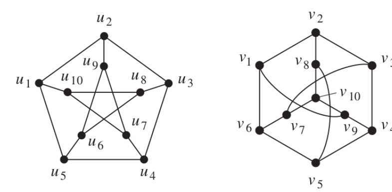
   a) Existe un grafo completo K_n para algún $n \in \mathbb{N}$ que contiene un subgrafo G que es isomorfo a G^c.

   b) Para todo $m, n \in \mathbb{N}$ se cumple que

$$K_m + K_n = K_{m+n}.$$

2. En caso exista, dibuje 6 árboles generadores no isomorfos del grafo de Petersen.
   Justifique su respuesta. (5 puntos)

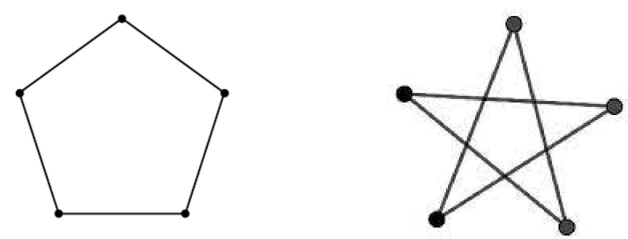
3. Determinar si los siguientes grafos son o no isomorfos. Justifique su respuesta. (5 pts)



4. Encontrar los autovalores de la matriz de adyacencia grafo completo K_n para todo $n \geq 2$. (5 puntos)

Solución:

1. a) Verdadero:
   Considere el grafo K_5 y los subgrafos que se muestran en la figura:

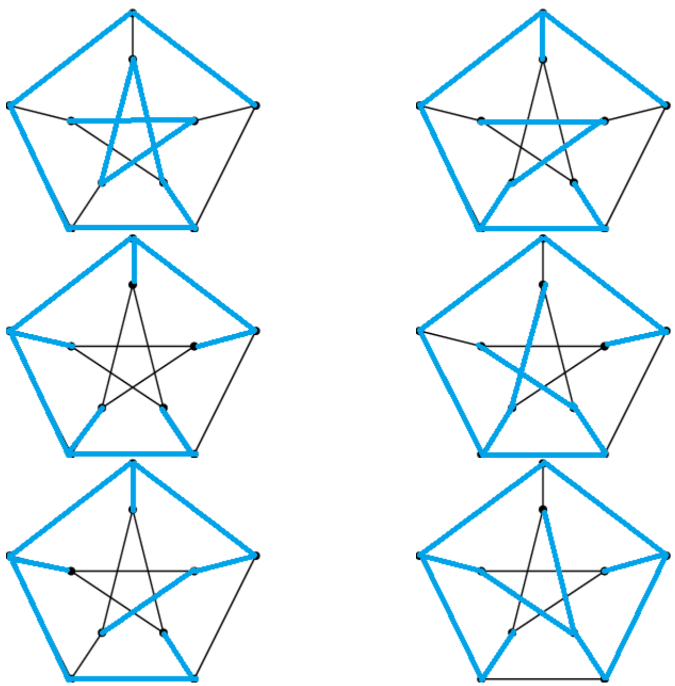


Es claro que son complementarios, faltaría sólo verificar que son isomorfos.

b) Falso:
Considere el caso de dos grafos iguales a K_2 la suma de ellos sería K_2.

2. Los siguientes árboles generadores no son isomorfos con secuencia de grados:

- (1,1,2,2,2,2,2,2,2,2)
- (1,1,1,1,2,2,2,2,3,3) hay dos grafos no isomorfos: un grafo con dos vértices de grado 3 vecinos y el otro grafo muestra dos vértices de grado 3 que no son isomorfos.
- (1,1,1,1,1,2,2,3,3,3) hay dos grafos no isomorfos: un grafo con tres vértices de grado 3 vecinos y el otro grafo muestra tres vértices de grado 3 que no son isomorfos.
- (1,1,1,2,2,2,2,2,2,3)



3. Considere la función $f\colon \{u_1, u_2, \ldots, u_{10}\} \to \{v_1, v_2, \ldots, v_{10}\}$ dada por

$$\begin{aligned} u_1 &\mapsto v_1 \\ u_2 &\mapsto v_2 \\ u_3 &\mapsto v_3 \\ u_4 &\mapsto v_4 \\ u_5 &\mapsto v_9 \\ u_6 &\mapsto v_{10} \\ u_7 &\mapsto v_5 \\ u_8 &\mapsto v_7 \\ u_9 &\mapsto v_8 \\ u_{10} &\mapsto v_6 \end{aligned}$$

Observe que f es una biyección que preserva aristas, es decir es un isomorfismo de grafos. Hay otros isomorfismos, por ejemplo la siguiente función:

$$\begin{aligned} u_1 &\mapsto v_1 \\ u_2 &\mapsto v_2 \\ u_3 &\mapsto v_3 \\ u_4 &\mapsto v_7 \\ u_5 &\mapsto v_6 \\ u_6 &\mapsto v_5 \\ u_7 &\mapsto v_{10} \\ u_8 &\mapsto v_4 \\ u_9 &\mapsto v_8 \\ u_{10} &\mapsto v_9 \end{aligned}$$

es también un isomorfismo de grafos.

4. Sea J la matriz $n \times n$ que tiene 1 en todas sus entradas. La matriz de adyacencia de K_n es $J - I$. Se verifica que el polinomio caracteristico de $J - I$ es

$$p(\lambda) = (\lambda + 1)^{n-1}(\lambda - n + 1),$$

de donde los autovalores pedidos son -1 y $n - 1$.

MATEMÁTICA DISCRETA
SOLUCIONARIO PC4
3 DE NOVIEMBRE 2023

1. Sea $G=(V,E)$ un grafo de al menos 2 vértices y A su matriz de adyacencia. Pruebe que:

   a) $tr(A^2)=2\#E$

   b) $tr(A^3)=6\#\Delta$ donde Δ es el conjunto de 3 ciclos de G.

Solución.

a) Consideremos $V=\{v_1,\dots,v_n\}$. $A=[a_{ij}]$ es una matriz $n\times n$ tenemos que si $A^2=[c_{ij}]$ sabemos que c_{ii} cuenta los recorridos de longitud 2 que comienzan y terminan en el vértice v_i, más esto es posible solo si se recorre una arista de ida y de vuelta por tanto c_{ii} cuenta los vertices vecinos a v_i es decir $c_{ii}=deg(v_i)$. Por el lema del handshake tenemos

$$2\#E=\sum_{i=1}^{n} deg(v_i)=\sum_{i=1}^{n} c_{ii}=tr(A^2)$$

b) Si $A^3=[t_{ij}]$ sabemos que t_{ii} cuenta los recorridos de longitud 3 que comienzan y terminan en el vértice v_i más esto es posible solo si recorre un triangulo de la forma $v_iv_jv_kv_i$ ya que $v_j\neq v_k$ (no consideramos lazos), más este trianfulo es recorrido dos veces $v_iv_kv_jv_i$ por tanto $t_{ii}=2\#\Delta_i$ dodne Δ_i es el conjunto triangulos que tienen a v_i como vértices.

$$tr(A^3)=\sum_{i=1}^{n} t_{ii}=2\sum_{i=1}^{n}\#\Delta_i$$

en la ultia suma cada triangulo es contado 3 veces por tanto $\sum_{i=1}^{n}\#\Delta_i=3\#\Delta$ coo se pedia deostrar.

□

2. Sea G un grafo conexo. La excentricidad de un vértice v se define como $e(v)=\max_{u\in V(G)} d(u,v)$. El radio del grafo $r(G)$ es mínimo valor de la excentricidad y los vértices centrales son los de exentricidad $r(G)$.

   a) Pruebe que la excentridad máxima es el diametro del grafo.

   b) Pruebe que $diam(G)\leq 2\,r(G)$.

   c) De un ejemplo de un grafo donde $diam(G)<2\,r(G)$.

   d) De un ejemplo de un árbol con 3 vértices centrales y 5 hojas.

Solución.

a) Sea m la excentricidad máxima, como $m=e(v)$ para algún vértice existe un vértice u tal que $m=d(u,v)$. Si cualquier otro par de vertices a,b tuviesemos $d(a,b)>m$ entonces $e(a)\geq m$ lo que contradice la maximalidad de m. Por tanto m es la ayor distancia posible entre dos vértices, es decir $m=diam(G)$.

b) Sean $u,v,w\in V$ con $d(u,v)=diam(G)$ y $e(w)=r(G)$. Por desigualdad triangular

$$d(u,v)\leq d(u,w)+d(w,v)\leq e(w)+e(w)=2r(G).$$

c) Consideremos un G un camino de longitud 3. La exetricidad de sus dos extremos es 3 y de los otros vértices es 2. Así su diámetro es 3 y su radio es 2.

d) Este caso no es posible, ya que un árbol tiene a lo más dos vértices centrales. Para ver esto consideremos un árbol G y γ un camino de longitud máxima m con extremos p y q. Si v esta en el centro de G es un árbol sabemos que hay un único camino que conecta a q con v y a p con v, as este define un camino que conecta p con q, por unicidad debe ser γ. En particular v es un vértice de γ y por ser central en G debe estar en el centro de γ, y por ser γ un camino su centro tiene a la más dos puntos.

□

3. Determine el máximo de árboles de órden 6 no isomorfos entre sí :

   a) Si solo tienen vértices de grado 1 y 2.

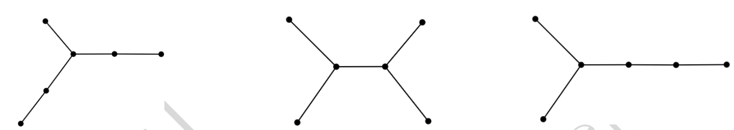
   b) Si tienen un vértice de grado 3.

   c) Si tienen un vértice de grado 4.

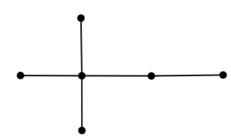
Solución.

a) Al tener vértices de grado 1 o 2 necesariamente es un camino, el máximo es 1.

b) Si v es un vértioce de grado 3, este tiene 3 vecinos faltaría conectarlos con 2 vértices restantes. Este se puede hacer conectando a 2 de los vecinos con los 2 restantes, conectando a uno de los vecinos con los dos restantes o conectando a uno de los vecinos con uno de los faltantes y a este con el último. Así obtenemos 3 grafos no isomorfos entre sí.



c) Si tiene un vértice de grado 4, con sus vecinos serían 5 vértices faltando uno el cual debe estar conectado con uno de estos vecinos. En este caso todos los arboles son isomorfos entre sí por tanto el máximo es 1.



□

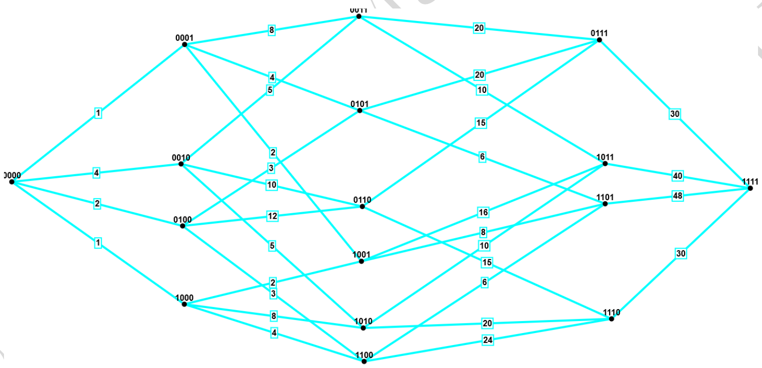
4. Considere el grafo cuyos vértices son cadenas $a_4a_3a_2a_1$ donde a_i son 0 o 1 y con arístas entre dos vértices cuando difieren en solo un término. Para definir el peso de una arista considere $p : V \longrightarrow \mathbb{N}$ como $p(a_4a_3a_2a_1) = 2^{a_1}3^{a_2}5^{a_3}2^{a_4}$ y $w : E \longrightarrow \mathbb{N}$ como $w(\alpha) = |p(u) - p(v)|$ cuando $\alpha = \{u, v\}$.

   a) Esboze el grafo indicando los pesos de las aristas.

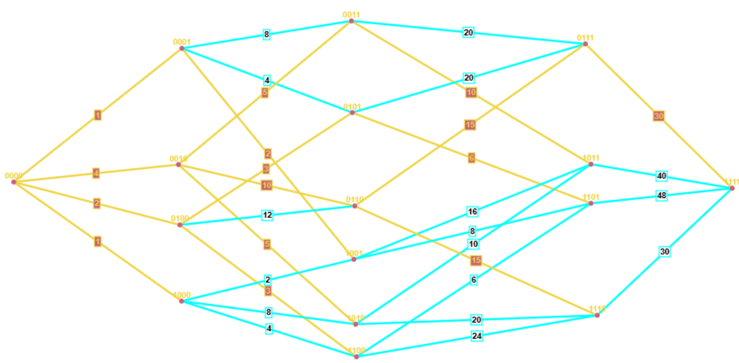
   b) Mediante el algoritmo de Druscal determine un arbol de expasión de peso mínimo.

Solución.

a) El grafo ponderado pedido es:



b) Un árbol de expansión mínima es



□

5. **Pregunta Extra** (en caso la haga reemplaza a una de las anteriores)

Sea $G = (V, E)$ un grafo con $V = \{v_1, \ldots, v_n\}$. Denotemos $i \to j$ cuando $i < j$ y $\{v_i, v_j\} \in E$. Se define $q : \mathbb{R}^n \longrightarrow \mathbb{R}$ como $q(x_1, \ldots, x_n) = \sum_{i \to j}(x_j - x_i)^2$. Si A es la matriz de adyacencia del grafo y $D = diag(\deg(v_1), \ldots, \deg(v_n))$ pruebe que:

$$q(x) = x(D - A)x^t$$

Solución. Considere I la matriz de incidecnia con signos, se vio en clase que la matriz de Laplace es

$$I \cdot I^t = D - A$$

Sea $Q(x) = x(D - A)x^t$, de lo anterior $Q(x) = (xI)(xI)^t = \|xI\|^2$, por tanto bastaría deterimar xI. Notemos que el vector xI tiene por componente j a xI_j donde I_j es la columna j de I, por otro lado la columna j de I componentes nulas salvo en los indices de los vértices que tiene por extremos a la arista j, digamos que sean los vertices $i < k$, siendo 1 y -1 respectivaente. Vectorialemente:

$$x \cdot I_j = (\ldots, x_i, \ldots, x_k, \ldots)\begin{pmatrix} \vdots \\ 1 \\ \vdots \\ -1 \\ \vdots \end{pmatrix} = x_i - x_k$$

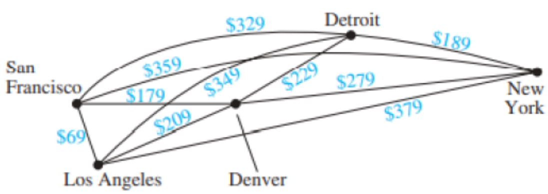
Sumando todas componentes obtenemos $Q(x) = q(x)$ como se pedía probar. □

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática   Ciclo 2023–I

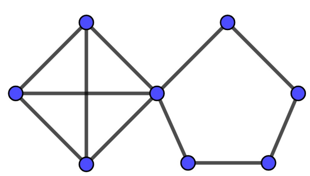
PRACTICA CALIFICADA 4 DE MATEMÁTICA DISCRETA

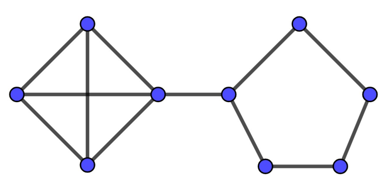
1. Pruebe que el grafo de Petersen no es planar. (5 puntos)
2. Pruebe que el polinomio cromático del grafo:
   (a) $P(K_n, t) = t(t-1)(t-2)\cdots(t-(n-1))$.
   (b) $P(C_n, t) = (t-1)^n + (-1)^n(t-1)$.

   (5 puntos)
3. Del siguiente grafo. (5 puntos)



   a) Encuentre una ruta con la menor tarifa aérea total que visite cada una de las ciudades. Justifique.
   b) Determine la matriz de Dijkstra.
   c) El subgrafo del precio más cómodo para viajar desde San Francisco hacia New York.
4. Determine el polinomio cromático en cada grafo: (5 puntos)

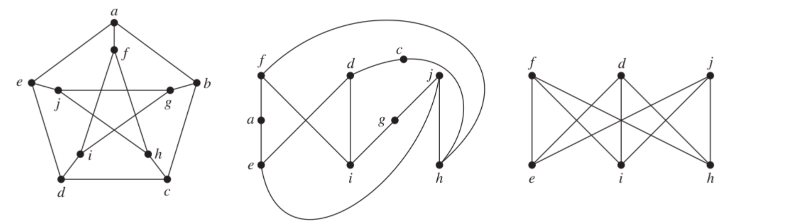

a)


b)

(Sugerencia use la Pregunta 2)

Solucion:

1. Por el teorema de Kuratowski, basta que el grafo de Petersen contenga un subgrafo homeomorfo a K_5 o $K_{3,3}$. En efecto, ocurre este ultimo caso:



2. (a) En el grafo completo K_n se cumple que $P(K_n, t)$ coincide con el cardinal de las funciones inyectivas $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, k\}$. De donde,
$$P(K_n, t) = t(t-1)(t-2)\cdots(t-(n-1))$$
   (b) Se usa inducción sobre n. Es cierto para $n = 3$. Supongamos que es cierto para $n-1$. Sea e una arista de C_n. Sean $C_n - e$ el grafo que resulta al eliminar la arista e y sea $C_n \dot{e}$ el grafo que resulta al contraer e. Observe que $C_n - e \cong L_n$ es el grafo lineal y $C_n \cdot e \cong C_{n-1}$.
   Como los vértices extremos de e no pueden ser coloreados con el mismo color se tiene que $P(C_n, t) = P(C_n - e, t) - P(C \cdot e, t)$. Por otro lado, L_n se puede colorear con dos colores, es mas $P(L_n, t) = t(t-1)^{n-1}$. Por hipótesis inductiva tenemos
$$\begin{aligned} P(C_n, t) &= P(C_n - e, t) - P(C \cdot e, t) \\ &= P(L_n, t) - P(C_{n-1}, t) \\ &= t(t-1)^{n-1} - (t-1)^{n-1} - (-1)^{n-1}(t-1) \\ &= (t-1)(t-1)^{n-1} + (-1)^n(t-1) \\ &= (t-1)^n + (-1)^n(t-1) \end{aligned}$$

3. a)

E(G)	Peso
e_1	69
e_2	179
e_3	189
e_4	229

El grafo que resulta del cuadra muestra la ruta con la menor tarifa.

b)

	San Francisco(SF)	Los Angeles(LA)	Denver(DV)	New York(NY)	Detroit(DT)	
SF	-	69 (SF)	179 (SF)	359 (SF)	329 (SF)	SF-LA
SF-LA	-	-	179 (SF)	359 (SF)	329 (SF)	SF-DV
SF-DV	-	-	-	359 (SF)	329 (SF)	SF-DT
SF-DT	-	-	-	359 (SF)	-	SF-NY

b)

c)

4. Sean k colores

a) El número de maneras diferentes de pintar C_5 es $P_{C_5}(k)$ donde el vértices común entre los grafos K_4 y C_5 se pueden pintar de k formas diferentes, luego se tiene que los otros vértices de K_4 se puede pintar de $(k-1)(k-2)(k-3)$, por tanto el prolinomio crómatico del grafo $K_3 \cup C_5$ esta dada por:

$$P(k) = \frac{P_{K_4} \cdot P_{C_5}}{k}$$

b) Sea $e = \{u, v\} \in E(G)$ la arista común entre K_4 y C_5. Como el vértice v se pudo pintar de k formas diferentes entonces u se puede pintar de $k-1$ formas diferentes, luego el siguiente vértice en K_4 también se puede pintar de $k-1$ formas diferentes y por último los demás vértices de $(k-2)(k-3)$, por tanto el prolinomio crómatico del grafo $K_3 \cup P_2 \cup C_5$ esta dada por:

$$P(k) = \frac{P_{K_4} \cdot P_{C_5}}{k}(k-1)$$

MATEMÁTICA DISCRETA
SOLUCIONARIO PC5
11 DE NOVIEMBRE 2023

1. Considere un poliedro convexo de n vértices con caras h caras hexagonales y p pentagonales sin ninguna otra cara) con la propiedad de que cada vértice adjacente a exactamente 3 caras. Pruebe que:

   a) El doble de las aristas es $5p + 6h$.

   b) El doble de las aristas es el triple de los vértices.

   c) La cantidad de petágonos es exactamente 12.

   d) Si adiciolamente pedimos que cada cara pentagonal es adyacente solo a caras hexagonales el mínimo de hexágonos necesarios es 20.

Solución.

a) El total de aristas de las caras pentagonales es $5p$ y de las hexagonales es $6h$. La suma de la cantidad de aristas de todas las caras es $5p + 6h$, más en esta suma cada arista es contada 2 veces ya que aparece en exactamente 2 caras contiguas, por es igual al doble de aristas.

b) Como cada vértice adjacente a exactamente 3 caras, en el concurren 3 aristas, es decir el grado de cada vértice es 3, en particular la suma de grados es doble de aristas debe coincidir con el triple de vértices.

c) Sea n la cantidad de vértices, a la cantidad de aristas y c la cantidad de caras. Así $c = p + h$, $2a = 5p + 6h$ y $3n = 2a$, por la relación de Euler

$$2 = n - a + c = \frac{2a}{3} - a + c = -\frac{1}{6}(5p + 6h) + p + h = \frac{p}{6}$$

por tanto $p = 12$.

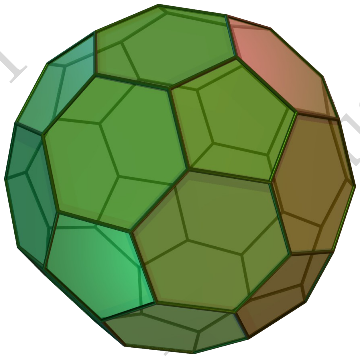
d) Sea r la cantidad de aristas comunes entre pentágonos y hexágonos y s la cantidad de aristas comunes entre dos hexágonos. Como el total de aristas es $r + s$

$$r + s = a = \frac{1}{2}(60 + 6h) = 30 + 3h$$

Como cada pentágono es adyacente solo a caras hexagonales teneos que $r = 5 \times 12 = 60$. Por otro lado como cada hexágono tiene a lo más 3 pentágonos vecinos, debe tener por lo menos 3 hexágonos vecinos. Por tanto si sumamos las arístas entre hexágonos $2s \geq 3h$

$$30 + 3h = r + s \geq 60 + \frac{3h}{2}$$

de ahí $h \geq 20$. Este es el mínimo ya que correponde a la configuracion de caras pentagonales y hexagonales de una pelota de fútbol.



$\square$

2. Sean $G_1 = (V_1, A_1)$ y $G_2 = (V_2, A_2)$ dos grafos con al menos una arista con polinomios cromáticos $p_1(x)$ y $p_2(x)$. Definimos $G_1 \cup G_2 = (V_1 \cup V_2, A_1 \cup A_2)$ Pruebe que:

   a) Si solo comparten un vértice $V_1 \cap V_2$ entonces $p_{G_1 \cup G_2}(x) = p_1(x)p_2(x)/x$
   b) Si no comparten vértices y tomamos dos vértices $v_i \in V_i$ para el grafo $G = G_1 \cup G_2 + \{v_1, v_2\}$ tenemos $p_G(x) = p_1(x)p_2(x)\left(1 - \frac{1}{x}\right)$.
   c) En el caso del grafo G del item b) se cumple $X(G) \leq \text{máx}\{X(G_1), X(G_2)\}$.

Solución.

a) Sea $v_1 V_1 \cap V_2$ el vértice común. Para $k\mathbb{N}$ notenos que por cada k-coloración de G_1 se fija el color de v, quedando por colorear G_2 con ese color de v fijado.
   Afirmamos que la cantidad de k-coloraciones para G_2 con el color de v fijado es $\dfrac{p_2(k)}{k}$.
   Para ver esto notemos que dados dos colores distintos, las cantidades de k-coloraciones de G_2 con v coloreado con el primer color y con v coloreado con el segundo color es la misma, ya que podeos establecer una biyección entre ambos conjutos cabiando el primer color con el segundo y viceversa. Si N es este número común de coloraciones, tendriaos que $kN = p_2(k)$ por tanto $N = \dfrac{p_2(k)}{k}$.
   Como por cada k-coloración de G_1 hay N k-coloraciones posibles para G_2, el total de k-coloraciones para G es
$$p_G(k) = p_1(k)N = \frac{1}{k}p_1(k)p_2(k)$$

b) Sea $\alpha = \{v_1, v_2\}$. Por la fórmula de eliminación-contracción tenemos que
$$p_G(x) = p_{G\setminus\alpha}(x) - p_{G/\alpha}(x).$$
   Como G_1 y G_2 no están conectados en $G \setminus \alpha$ tenemos que $p_{G\setminus\alpha}(x) = p_1(x)p_2(x)$, por otro lado G/α correponde al caso en que G_1 y G_2 compartan un único vértice, por la parte anterior tenemos que $p_{G/\alpha}(x) = \dfrac{1}{x}p_1(x)p_2(x)$. Restando ambos obteneos el resultado pedido.

c) Recordemos que para un grafo H su número cromático $X(H)$ es el primer natural en el cual su polinomio cromático no se anula, es más para $k \geq X(H)$, $p_H(k) > 0$. Si $m = X(G_i)$ es el mayor de ambos, en particular $m \geq 2$ (ya que tienen una arista) y como $p_G(x) = \frac{1}{x}p_1(x)p_2(x)(x-1)$, $p_G(m) > 0$ por tanto $m \geq X(G)$.

$\square$

3. Determine justificando su respuesta:

   a) Un sistema de representantes para las clases invertibles módulo 36.
   b) Usando el algoritmo de Euclides obtenga enteros a, b tal que $93a + 112b = 1$.
   c) La lista de números del 1 al 6 cuyas potencias generan $(\mathbb{Z}/7\mathbb{Z})^\times$.
   d) Si para $a, b \in \mathbb{N}$ es posible que $a^4 | b^3$ si $a \nmid b$.
   e) El menor k natural de manera que $7^k \equiv 1 \mod 25$

Solución.

a) Basta considerar números del 1 al 36 coprimos con 36, es decir impares y no múltiplos de 3. Explícitamente:
$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$$

b) Por divisionces sucesivas:
$$\begin{aligned} 112 &= 93 + 19 \\ 93 &= 5 \cdot 19 - 2 \\ 19 &= 9 \cdot 2 + 1 \end{aligned} \qquad \begin{aligned} 1 &= 19 - 9 \cdot 2 \\ &= 19 - 9(5 \cdot 19 - 93) = -44 \cdot 19 + 9 \cdot 93 \\ &= -44(112 - 93) + 9 \cdot 93 = -44 \cdot 112 + 53 \cdot 93 \end{aligned}$$

c) Como $(\mathbb{Z}/7\mathbb{Z})^\times$ tiene representantes 1,2,3,-3,-2,-1. Como $2^3 = 8 \equiv 1 \mod 7$ y $(-3)^3 = -27 \equiv 1 \mod 7$ descartamos a 2,-3 y támbien trivialmente a 1 y -1. Solo quedan 3 y -2, para verificarlo veamos sus potencias:

a	a^2	a^3	a^4	a^5	a^6
3	2	-1	-3	2	1
-2	-3	-1	2	3	1

   por tanto si generan a $(\mathbb{Z}/7\mathbb{Z})^\times$.

d) Si $a^4 \mid b^3$ los divisores primos de a van a ser divisores primos de b, si estos son $p_1, \ldots, p_r$ tenemos que $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $b = p_1^{\beta_1} \cdots p_r^{\beta_r} N$ donde N es coprimo con a. Como $a^4 \mid b^3$ tenemos $4\alpha_i \leq 3\beta_i$, luego $\alpha_i \leq \dfrac{3}{4}\beta_i < \beta_i$ más esto significa que $a \mid b$.

e) Como $7^2 = 49 \equiv -1 \mod 25$ tenemos que $7^4 \equiv 1 \mod 25$. 4 es el mínimo ya que $7^3 = 7 \cdot 7^2 \equiv -7 \mod 25$.

$\square$

4. Si $x^2 + y^2 = z^2$ en $\mathbb{Z}$, pruebe que:

   a) Al menos uno de los valores x, y, z es divisible por 3 .

   b) Al menos uno de los valores x, y, z es divisible por 5 .

   c) xyz es divisible por 4 .

   d) $xyz \equiv 0 (\text{mód} 60)$.

Solución.

a) Como todo número entero es congruente a 0,1,-1 módulo 3 notamos que todo cuadrado debe ser congruente a 0 o 1. En caso z no sea divisible por 3 tenemos que $z^2 \equiv 1 \mod 3$ esto fuerza a que o bien x o bien y sean divisibles por tres, que si ambos no lo son simultaneaente $x^2 + y^2 \equiv 2 \mod 3$ y por tanto no podría ser igual a z^2. Podemos concluir que en general al menos uno de ellos es divisible por 3. Esto lo podemos ver en la siguiente tabla de restos de $x^2 + y^2$ módulo 3:

+	0	1
0	0	1
1	1	2

b) Como todo número entero es congruente a $0, \pm 1, \pm 2$ módulo 5 notamos que todo cuadrado debe ser congruente a 0,1 o 4. La siguiente tabla corresponde los posibles restos que da $x^2 + y^2$ módulo 5:

+	0	1	4
0	0	1	4
1	1	2	0
4	4	0	3

En caso z no sea divisible por 5 tenemos 2 casos $z^2 \equiv 1$ o $4 \mod 5$ más en la tabla esto solo se da cuando x^2 o y^2 son 0 módulo 5 (primera fila y primera columna respectivamente).

c) Basta considerar 3 casos: Si x e y son pares no hay nada que probar. Si x e y son impares no se puede dar ya que en ese caso $x^2 + y^2 \equiv 2 \mod 4$ el cual no puede ser z^2. Finalmente uno es par y el otro impar, digamos x es par e y impar, tenemos que z es impar luego en este caso existen a, b, c enteros de modo que $x = 2a,\ y = 2b + 1,\ z = 2c + 1$. Luego como

$$(2c + 1)^2 = x^2 + y^2 = 4a^2 + (2b + 1)^2$$

simplificando obtenemos:

$$c(c + 1) = a^2 + b(b + 1)$$

Notamos que $c(c+1)$ y $b(b+1)$ siempre son pares por tanto a es par y $x = 2a$ es múltiplo de 4 por tanto xyz lo és.

$\square$

Universidad Nacional de Ingeniería
Facultad de Ciencias
Escuela Profesional de Matemática Ciclo 2022–II

PRACTICA CALIFICADA 5 DE MATEMÁTICA DISCRETA

---

1. Resolver la ecuación: (4 puntos)

$$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 1 \mod 8 \\ x &\equiv 4 \mod 9 \end{aligned}$$

2. Determine si los siguiente enunciados son verdaderos (V) o falsos (F). Justifique su respuesta. (6 puntos)

   (a) Existen raíces primitivas módulo n para todo entero $n \geq 25$.

   (b) La ecuación
   $$4x^4 \equiv 5 \mod 7$$
   tiene 4 soluciones distintas módulo 7.

3. Sean p y q números primos enteros positivos tales que (5 puntos)
$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \cdots - \frac{1}{230} + \frac{1}{231}$$
Encuentre un divisor primo de p con 3 cifras. Justifique su respuesta.

4. Pruebe que la ecuación (5 puntos)
$$(p - 1)! + 1 = p^m$$
no tiene solución para todo p número primo mayor que 5 y m entero positivo.

Solución:

1. Se usa el teorema chino del resto. La respuesta es $x \equiv 193 \mod 360$.

2. (a) (F). Por ejemplo no existen raíces primitivas modulo 30.

   (b) (F). La ecuación no tiene solución. Tenemos que $\phi(7) = 6$ y 3 es raíz primitiva módulo 7. Aplicando ind_3 a la ecuación, tenemos
   $$ind_3(4) + 4ind_3(x) \equiv ind_3(5) \mod 6$$
   Por otro lado, $ind_3(4) = 4$ y $ind_3(5) = 5$. Luego
   $$4 + 4ind_3(x) \equiv 5 \mod 6$$
   así
   $$4ind_3(x) \equiv 1 \mod 6$$
   de donde 4 es inversible módulo 6 que es un absurdo.

3.
$$\begin{aligned}\frac{p}{q} &= 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}-\cdots+\frac{1}{231}-2(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{230})\\ &= (\frac{1}{116}+\frac{1}{231})+(\frac{1}{117}+\frac{1}{230})+\cdots+(\frac{1}{173}+\frac{1}{174})\\ &= 347(\frac{1}{116\times 231}+\frac{1}{117\times 230}+\cdots+\frac{1}{173\times 174})\end{aligned}$$

Como 347 es un número primo entonces p posee como divisor a 347.

4. Para todo p número primo mayor que 5 se tiene

$$2<\frac{p-1}{2}<p-1$$

así,

$$(p-1)^2=2\frac{p-1}{2}(p-1)\mid(p-1)!.$$

Supongamos que existan p primo mayor que 5 y m entero positivo tal que

$$(p-1)!+1=p^m$$

se tiene que

$$(p-1)^2\mid(p^{m-1})$$

Al dividir ambos por $p-1$ se tiene

$$(p-1)\mid(p^{m-1}+p^{m-2}+\cdots+p+1).$$

Por otro lado, como $(p-1)\mid(p^k-1)$ entonces $p^k\equiv 1\,(mod\, p-1)$ para todo $k=0,1,2,\ldots$, esto quiere decir que

$$p^{m-1}+p^{m-2}+\cdots+p+1\equiv m\,(mod\, p-1)$$

por tanto $(p-1)\mid m$, así $m\geq p-1$. Es decir

$$p^m\geq p^{p-1}>(p-1)^{p-1}>(p-1)!,$$

por tanto $p^m>(p-1)!+1$, ello es una contradicción.