

## Inducción matemática y Principio del buen orden

### Profesores del curso:

Ronald Mass<sup>1</sup>

Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



5 de mayo de 2020

## Tabla de contenidos

- ① Números y Notaciones
- ② Principio del buen orden
- ③ Principio de inducción matemática
- ④ PIM y PBO

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

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

Periodo 2020-1	Profesores del curso	Periodo 2020-1	Profesores del curso	Periodo 2020-1	Profesores del curso
Números y Notaciones ○○○	Principio del buen orden ○○○○○○○	Números y Notaciones ○○○	Principio del buen orden ○○○○○○○	Números y Notaciones ○○○	Principio del buen orden ○○○○○○○

## Sumatorias y productorias

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

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

### Ejemplos:

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

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

## Tabla de contenidos

- ① Números y Notaciones
- ② Principio del buen orden
- ③ Principio de inducción matemática
- ④ PIM y PBO

### 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.

Periodo 2020-1	Profesores del curso	Periodo 2020-1	Profesores del curso	Periodo 2020-1	Profesores del curso
Números y Notaciones ○○○	Principio del buen orden ○○○○○○○	Números y Notaciones ○○○	Principio del buen orden ○○○○○○○	Números y Notaciones ○○○	Principio del buen orden ○○○○○○○

## 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  $p_1, p_2, \dots, p_m$  forma un **ciclo** de largo  $m$  si  $p_1$  le gana a  $p_2$ ,  $p_2$  le gana a  $p_3, \dots, p_{m-1}$  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  $p_1, p_2, \dots, p_m$  ( $m \geq 3$ ) en un torneo, entonces hay un ciclo de largo 3.

## Solución:

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

El conjunto:

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

Por el Principio del Buen Orden, existe  $k \in S$  que es su menor elemento y  $p_1, p_2, \dots, p_k$  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,  $p_1, p_3, \dots, p_{k-1}$  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  $r = r'$

Periodo 2020-1 Profesores del curso

## Tabla de contenidos

1 Números y Notaciones

2 Principio del buen orden

3 Principio de inducción matemática

- Primer principio de inducción
- Principio de inducción matemática generalizado
- Segundo principio de inducción
- Variante del principio de inducción fuerte 1
- Variante del principio de inducción fuerte 2

4 PIM y PBO

Periodo 2020-1 Profesores del curso

## Principio de inducción simple

Sea  $X$  un subconjunto de los números naturales tal que:

- $1 \in X$ .
- 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.

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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 podemos poner:

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

Periodo 2020-1 Profesores del curso

## 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  $k = 9, 12, 15, \dots$ , 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.

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## Segundo principio de inducción

## 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  $j = 1, \dots, n$  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.

### Ejemplo: (cont.)

- Para  $n = 1$ :  

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

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.)

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  $S = \mathbb{N}$ .

## Segundo principio de inducción

## Demostración del Principio de inducción fuerte

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

Demostremos que  $X = \mathbb{N}$ .

Considere el conjunto  $Y = \mathbb{N} \setminus X$ . 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  $n = 1, 2, \dots, p-1$  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: (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:

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

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 verdadera para todo  $n \in \mathbb{N}$  y  $n > n_0$ .

## Segundo principio de inducción

## 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  $n \in \mathbb{N}$ .

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

**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.)

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

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

## Ejemplo:

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

**Solución:**

Considere la propiedad:

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

- 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  $j \in [2, k]$ .

Variante del principio de inducción fuerte 1

## Ejemplo: (cont.)

Demostraremos 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 cumple para todo  $n \in \mathbb{N}$  y  $n \geq b$  si:

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

Variante del principio de inducción fuerte 2

## 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

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

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.

Periodo 2020-1 Profesores del curso

Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO

Variante del principio de inducción fuerte 2

## 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

- 1 Números y Notaciones
- 2 Principio del buen orden
- 3 Principio de inducción matemática
- 4 PIM y PBO

Periodo 2020-1 Profesores del curso

Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO Números y Notaciones Principio del buen orden Principio de inducción matemática PIM y PBO

Conjuntos Relaciones Funciones

## Demostración:

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

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

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  $Y = \mathbb{N} \setminus X$ , entonces  $1 \in Y$ . Sea  $k \in \mathbb{N}$  tal que  $1, 2, 3, \dots, k \in Y$ . 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  $Y = \mathbb{N} \setminus X$  entonces  $X = \emptyset$  lo cual es una contradicción. Por lo tanto,  $X$  debe tener un elemento mínimo.

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.

## CONJUNTOS-RELACIONES-FUNCIONES

Profesores del curso:

Ronald Mass <sup>1</sup>  
Ángel Ramírez <sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



30/03/2020

**Conjuntos**

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

## Tabla de contenidos

- 1 Conjuntos
- 2 Relaciones
- 3 Funciones

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:  $A = \{x / x \text{ satisface la propiedad } P\}$ .

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

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

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## Ejemplos:

①  $\mathbb{N} = \{1, 2, \dots\}, \mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$ , etc.

② Definamos:  $U$ : conjunto de todos los triángulos. Sea la propiedad  $P$ : Es un triángulo rectángulo. Luego:  $A = \{x \in U / x \text{ satisface la propiedad } P\} = \text{Conjunto de todos los triángulos rectángulos.}$

③ En cálculo se trabajan con conjuntos de la forma:

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

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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  $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ .

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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:

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

Definition 5 (Intersección)

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

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

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

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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:

$$A - B = \{x / x \in A \wedge x \notin B\}.$$

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  $C_A$  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  $A \cap \emptyset = \emptyset$ .
- 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  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ .

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

**Conjuntos**

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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.

### Tabla de contenidos

- 1 Conjuntos
- 2 Relaciones
  - Tipos de relaciones
- 3 Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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:

$$A \times B = \{(a, 0), (a, 1), (a, 2), (a, 3), (a, 4), (b, 0), (b, 1), (b, 2), (b, 3), (b, 4), (c, 0), (c, 1), (c, 2), (c, 3), (c, 4), (d, 0), (d, 1), (d, 2), (d, 3), (d, 4), (e, 0), (e, 1), (e, 2), (e, 3), (e, 4)\}$$

$R = \{(a, 0), (a, 1), (a, 3), (b, 1), (b, 2), (c, 0), (c, 3)\} \subset A \times B$ , 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  $aRb \Leftrightarrow a \leq b$ .

$$R = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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:

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

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:

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

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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  $aRb$ .

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

Conjuntos

Relaciones  
○○○○

Funciones

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

$aRb \Leftrightarrow a = b$ .

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

Ejemplo:

**Ejemplo:**

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

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

Esta relación es llamada **congruencia módulo 3**.

¿ $T$  es reflexiva?. ¿ $T$  es simétrica?. ¿ $T$  es transitiva?.

**Tabla de contenidos**

- 1 Conjuntos
- 2 Relaciones
- 3 Funciones

**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:

$$\text{rango de } f = \{y \in Y / y = f(x) \text{ para algún } x \in X\}.$$

- 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:

$$\text{la imagen inversa de } y = \{x \in X / f(x) = y\}.$$

**Propiedades:**

Dada una función  $f : A \rightarrow B$ .

**Para las imágenes 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  $f^{-1}(\emptyset) = \emptyset$ .

**Definiciones:**

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

- ① La **imagen** de  $A$  se define por:

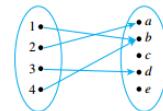
$$f(A) = \{y \in Y / y = f(x) \text{ para algún } x \in A\}.$$

- 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  $F : X \rightarrow Y$  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**

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

**Ejemplo:**

Sean  $A, B$  conjuntos. Definimos

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

Conjuntos Relaciones Funciones Conjuntos Relaciones Funciones Conjuntos Relaciones Funciones

## Composición de funciones

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

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

Propiedades:

Sean  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  y  $h : C \rightarrow D$  funciones tales que está bien definida 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  $f : A \rightarrow B$ ,  $g : B \rightarrow A$  funciones (dom( $g$ ) =  $B$ ). Si  $g \circ f = id_A : A \rightarrow A$ , es decir,  $(g \circ f)(x) = g(f(x)) = x$  para todo  $x \in A$ , entonces  $g$  es llamada **inversa a derecha** de  $f$ .

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

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  $\mathbb{N} = \{1, 2, 3, \dots\}$  el conjunto de los números naturales. Definamos  $s : \mathbb{N} \rightarrow \mathbb{N}$  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  $\{2, 3, \dots\} \subset \mathbb{N}$  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  $n \in \{2, 3, \dots\}$ . Así  $l_i$  es una inversa a izquierda de  $s$  para todo  $i = 2, 3, \dots$

## Relación de Equivalencia y Orden

Ronald Mas, Angel Ramirez 2 de junio de 2021

## 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.

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.

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  $R, \sim, \equiv, \text{etc}$  para denotar a un relación de equivalencia.

## Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 3 / 13 Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 4 / 13 Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 4 / 13 Ejemplo 2

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.

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.

Para  $A = M_{2 \times 2}(\mathbb{Z})$  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  $A \in M_{2 \times 2}(\mathbb{Z})$ . ✓
- Simétrica: Si  $\det(A - B) = 0$  entonces  $\det(B - A) = (-1)^2 \cdot \det(A - B) = 0$ . ✓
- Transitiva: Si  $\det(A - B) = 0$  y  $\det(B - C) = 0$  entonces  $\det(A - C) = 0$ . ✗

$$\text{Considera: } A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix} \text{ y } C = \begin{bmatrix} 7 & 8 \\ 5 & 9 \end{bmatrix}.$$

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

## Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 5 / 13 Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 5 / 13 Ronald Mas, Angel Ramirez Relación de Equivalencia y Orden 2 de junio de 2021 6 / 13 Clase de equivalencia y conjunto cociente

## Ejemplo 2

Para  $A = M_{2 \times 2}(\mathbb{Z})$  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  $A \in M_{2 \times 2}(\mathbb{Z})$ . ✓
- Simétrica: Si  $\det(A - B) = 0$  entonces  $\det(B - A) = (-1)^2 \cdot \det(A - B) = 0$ . ✓
- Transitiva: Si  $\det(A - B) = 0$  y  $\det(B - C) = 0$  entonces  $\det(A - C) = 0$ . ✗

$$\text{Considera: } A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix} \text{ y } C = \begin{bmatrix} 7 & 8 \\ 5 & 9 \end{bmatrix}.$$

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

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

## Observaciones:

- Usamos  $R[x], [x], \bar{x}$ , 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

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

## Observaciones:

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

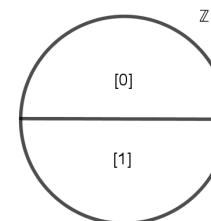
## Ejemplo

**Ejemplo:** Del ejemplo 1) se tiene que:

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

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

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.

## Relación de orden parcial

## Relación de orden parcial

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  $R$  transitiva  $z R y$ , de donde se concluye que  $z \in R[y]$ . La otra inclusión es similar.
- b) Si  $x$  no está relacionado con  $y$ , supongamos 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.

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:

- Reflexiva  
Si para todo  $a \in A$  se tiene  $(a, a) \in \preceq$ .
- Antisimétrica  
Si  $(a, b) \in \preceq$  y  $(b, a) \in \preceq$  entonces  $a = b$ .
- 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  $R, \preceq, \prec, \text{etc}$  para denotar a un relación de orden.

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:

- Reflexiva  
Si para todo  $a \in A$  se tiene  $(a, a) \in \preceq$ .
- Antisimétrica  
Si  $(a, b) \in \preceq$  y  $(b, a) \in \preceq$  entonces  $a = b$ .
- 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  $R, \preceq, \prec, \text{etc}$  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 cumplen 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  $\triangleleft$ .

## 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 cumplen 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  $\triangleleft$ .

## 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

$$x \triangleleft x_1 \triangleleft \cdots \triangleleft x_k \triangleleft y$$

## Demostración.

Para  $k = 0$  se tiene que  $x \triangleleft y$ .  
La idea queda como tarea, veamos la vuelta:

Si  $x \triangleleft x_1 \triangleleft \cdots \triangleleft x_k \triangleleft y$  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  $sra = 1$  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

## Contenido

- ① Elementos minimales y maximales
- ② Diagrama de Hasse
- ③ Ordenamiento lineal
- ④ Ordenamiento por inclusión parcial y total

12 de junio de 2020

Ronald Mas  
Angel Ramirez

**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

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

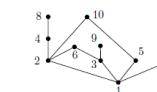


Elemento minimal: 1

Elemento maximal: 7

2) Diagrama de Hasse del conjunto parcialmente ordenado

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



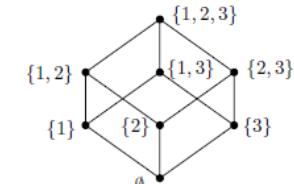
Elemento minimal: 1

Elemento maximal: 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  $x \leq y$ .

**Diagrama de Hasse****Definición**

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

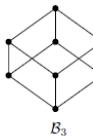
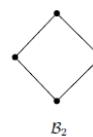
- 1)  $f$  es una aplicación inyectiva.
- 2)  $f(x) \preceq' f(y)$  si y sólo si  $x \preceq y$ .

**Observaciones:**

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

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

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

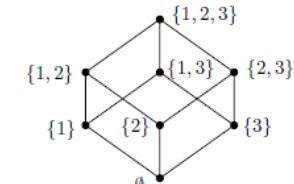


Una aplicación de adicionar propiedades a dichos conjuntos es el estudio del Álgebra de Boole.

**Más ejemplos**

3) Diagrama de Hasse del conjunto parcialmente ordenado

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



Elemento minimal:  $\emptyset$

Elemento maximal: {1, 2, 3}

**Independencia sobre un conjunto ordenado**

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

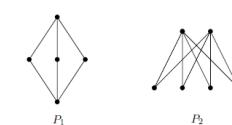
**Definición**

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

Denotamos:

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

**Ejemplo:** Para los conjuntos parcialmente ordenados



## 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:

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

## 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  $f : N \rightarrow M$  es  $m^n$ .

### Demostración:

#### • Caso $n = 0$ :

En este caso  $f : N \rightarrow M$  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  $f : \emptyset \rightarrow M$ .

Esto prueba la fórmula  $m^0 = 1$  para  $n = 0$  y cualquier  $m \geq 1$ .

② Veámos 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  $A \subset X \setminus \{a\}$  y donde  $|X \setminus \{a\}| = n$  y por la hipótesis inductiva se tienen  $2^n$  subconjuntos.

Para todo  $A \in \mathcal{F}_2$  considere  $A' = A \setminus \{a\} \subset X \setminus \{a\}$  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  $2^n + 2^n = 2^{n+1}$ .

## CONTEO COMBINATORIO - PERMUTACIONES - COMBINACIONES.

Profesores del curso:

Ronald Mass <sup>1</sup>

Ángel Ramírez <sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



10 de junio de 2020



### • 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  $m^1 = m$  para  $n = 1$  y todo  $m \geq 1$ .

• Hipótesis inductiva: Dado  $n_0 \in \mathbb{N}$ , existen  $m^{n_0}$  funciones cuando  $N$  tiene  $n$  elementos y  $M$  tiene  $m$  elementos para todo  $n \leq n_0$ .

• Veámos que se cumple para  $n_0 + 1$ .

Elijamos  $a \in N$  arbitrario y lo mantengamos fijo. Considera la función  $f : N \rightarrow M$  tal que  $f(a) \in M$  y la función  $f' : N \setminus \{a\} \rightarrow M$ . Dado  $a \in N$  fijo, existen  $m$  formas distintas de elegir  $f(a) \in M$ . Para elegir  $f'$ , tenemos que  $N \setminus \{a\}$  tiene  $n_0$  elementos y  $M$  tiene  $m$  elementos, entonces por la hipótesis inductiva existen  $m^{n_0}$  funciones  $f' : N \setminus \{a\} \rightarrow M$ . 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 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:

$$F : X \setminus \{a\} \rightarrow Y = \{A' \subset X / |A'| \text{ es un número impar}\}$$

$$A \mapsto F(A) := \begin{cases} A & \text{si } |A| \text{ es impar} \\ A \cup \{a\} & \text{si } |A| \text{ es par} \end{cases}$$

Observe que  $F$  es un biyección y que  $|X \setminus \{a\}| = n - 1$ , luego, por la Proposición 2 se tiene que el número de subconjuntos de  $X \setminus \{a\}$  es  $2^{n-1}$  y debido a que  $F$  es biyectiva concluimos 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 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  $2^n$ .



## Proposición 4

Dados  $n, m \in \mathbb{N} \cup \{0\}$ , existen  $m(m-1)\dots(m-n+1) = \prod_{i=0}^{n-1}(m-i)$  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:

③ Para  $n = 1$  tenemos  $m$  funciones inyectivas.

④ Observe que no existen funciones inyectivas cuando  $n > m$  cumpliéndose la fórmula debido a que aparece el factor cero en el producto.



CONTEO COMBINATORIO  
oooooooo●PERMUTACIONES  
ooooooCOMBINACIONES  
ooooooooooooooooooooCONTEO COMBINATORIO  
ooooooooPERMUTACIONES  
ooooooooCOMBINACIONES  
ooooooooooooooooooooCONTEO COMBINATORIO  
ooooooooPERMUTACIONES  
○●○○○COMBINACIONES  
oooooooooooooooooooo

## Tabla de contenidos

- 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  $N \setminus \{a\}$  hacia el conjunto  $M \setminus \{f(a)\}$ . Por la hipótesis inductiva, existen  $(m-1)(m-2)\dots(m-n+1)$  formas distintas de elecciones siguiente. Por tanto, tenemos  $m(m-1)(m-2)\dots(m-n+1)$  funciones inyectivas  $f : N \rightarrow M$ .

- 1 CONTEO COMBINATORIO
- 2 PERMUTACIONES
- 3 COMBINACIONES

### Definición 1

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

#### Ejemplo:

Sea  $X = \{a, b, c, d\}$ . Un ejemplo de permutación es  $P : X \rightarrow X$  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  $X = \{1, 2, 3, \dots, n\}$ . Con la convención que la primera fila esté en orden creciente, luego podemos considerar la notación:

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

Periodo 2020-1 Profesores del curso

CONTEO COMBINATORIO  
ooooooooPERMUTACIONES  
○○●○○COMBINACIONES  
ooooooooooooooooooooCONTEO COMBINATORIO  
oooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
○○○●○COMBINACIONES  
ooooooooooooooooooooCONTEO COMBINATORIO  
oooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
○○○○●COMBINACIONES  
oooooooooooooooooooo

## Ejemplo:

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

$$n(n-1)(n-2)\dots2 \times 1.$$

$$n! = n(n-1)(n-2)\dots2 \times 1.$$

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**.

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.

Periodo 2020-1 Profesores del curso

CONTEO COMBINATORIO  
ooooooooPERMUTACIONES  
○○●○○COMBINACIONES  
oooooooooooooooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
○○○●○COMBINACIONES  
●oooooooooooooooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
○○○○●COMBINACIONES  
oooooooooooooooooooo

## Tabla de contenidos

- 1 CONTEO COMBINATORIO
- 2 PERMUTACIONES
- 3 COMBINACIONES

### Definición 2

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

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots2 \times 1} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}$$

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  $\binom{n}{k} = 0$ .

Periodo 2020-1 Profesores del curso

CONTEO COMBINATORIO  
ooooooooPERMUTACIONES  
ooooooCOMBINACIONES  
oooooooooooooooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
●ooooooooooooCOMBINACIONES  
oooooooooooooooooooo

Periodo 2020-1 Profesores del curso

PERMUTACIONES  
○●○○○COMBINACIONES  
oooooooooooooooooooo

### Definición 3

Sea  $X$  un conjunto y  $k$  un entero 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  $X$ .

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

### 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:

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

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

### 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:

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

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

$$i_1 + i_2 + \dots + i_r = m. \quad (1)$$

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

Periodo 2020-1 Profesores del curso

### Solución:

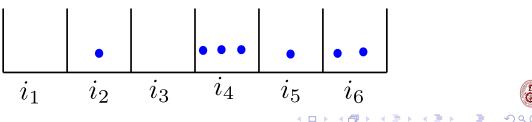
Imaginemos cada sumando  $i_r$  como una caja, es decir, tenemos  $r$  cajas.

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 más 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:



Periodo 2020-1 Profesores del curso

- ① De un subconjunto  $M$  de  $k$  elementos (es decir,  $M \in \binom{X}{k}$ ), podemos crear  $k!$   $k$ -tuplas ordenadas distintas y cada  $k$ -tuple se obtiene de exactamente un subconjunto  $M$  de  $k$  elementos.

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

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

Periodo 2020-1 Profesores del curso

### 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:

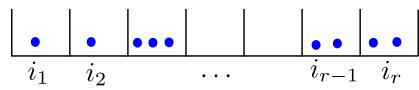
$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Periodo 2020-1 Profesores del curso

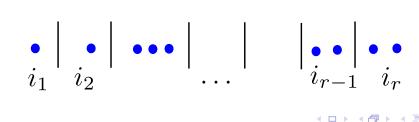
### Solución (Cont.)

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:



Periodo 2020-1 Profesores del curso

## Solución (Cont.)

Donde debemos tener en cuenta:

- ① Cada  $i_n$  ( $n = 1, \dots, r$ ) 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) arreglados 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  $m + r - 1$ .

Periodo 2020-1 Profesores del curso

## 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

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

Periodo 2020-1 Profesores del curso



CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

## 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.

Periodo 2020-1 Profesores del curso



CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

COEFICIENTE BINOMIAL  
ooooooo

COEFICIENTE MULTINOMIAL  
oooooooooooo

ESTIMACIÓN FUNCIÓN FACTORIAL  
oooooooooooo

## Solución: (cont.)

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:

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

Periodo 2020-1 Profesores del curso



CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

CONTEO COMBINATORIO  
oooooooooooo

PERMUTACIONES  
oooooooooooo

COMBINACIONES  
oooooooooooooooooooo

## COEFICIENTES BINOMIALES. ESTIMACIONES DE LA FUNCIÓN FACTORIAL

Profesores del curso:

Ronald Mass <sup>1</sup>

Ángel Ramírez <sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



14 de junio de 2020

## Tabla de contenidos

## 1 COEFICIENTE BINOMIAL

## 2 COEFICIENTE MULTINOMIAL

## 3 ESTIMACIÓN FUNCIÓN FACTORIAL

## Teorema Binomial

## Teorema 1

Para cualquier entero  $n$  no negativo se cumple:

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

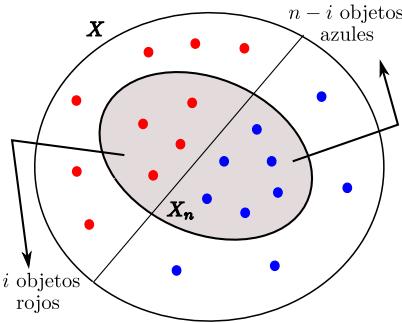
En particular, el teorema anterior para  $x = 1$  resulta:

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

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

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



Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

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:

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

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:

$$\sum_{j=1}^n j \binom{n}{j} 3^{j-1} = n 4^{n-1}.$$

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

## 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:

$$\frac{n!}{n_1! n_2! \dots n_r!}$$

## 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).

Consideré 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

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
•○○○○COEFICIENTE MULTINOMIAL  
●○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

## Tabla de contenidos

## 1 COEFICIENTE BINOMIAL

## 2 COEFICIENTE MULTINOMIAL

## 3 ESTIMACIÓN FUNCIÓN FACTORIAL

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

## 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:

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

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

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
○○○○○COEFICIENTE MULTINOMIAL  
○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

Periodo 2020-1 Profesores del curso

COEFICIENTE BINOMIAL  
•○○○○COEFICIENTE MULTINOMIAL  
●○○○○○○○○○○○○ESTIMACIÓN FUNCIÓN FACTORIAL  
○○○○○○○○○○○○

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:

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

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

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

### Lema 1

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

Entonces:

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

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

### Demostración:

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

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

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

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

### Demostración:

Inducción sobre  $n$ :

① Caso base:  $n = 1$ :

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

pues las únicas formas de expresar 1 como suma de  $r$  sumandos es:  $1 + 0 + \cdots + 0$  (da lugar al sumando  $x_1$ ),  $0 + 1 + \cdots + 0$  (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  $a = (x_1 + x_2 + \cdots + x_r)^n$ , luego:

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

Ahora, dados  $n_1, n_2, \dots, n_r \in \mathbb{N}$  tal que

$n_1 + n_2 + \cdots + n_r = n + 1$ , el coeficiente de:

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

se obtiene sumando los coeficientes de:

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

que aparecen en el desarrollo de "a".

### Ejemplos:

Por la hipótesis inductiva, estos coeficientes valen:

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

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

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

### Resolución:

Veamos 3:

$$\text{① Demuestre que } \sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

② Determine el coeficiente de  $x^8$  en el desarrollo de  $(1 + x^2 - x^3)^9$ .

$$\text{③ Calcule } S = \sum_{k=0}^{n-1} (-1)^k \binom{n-1}{k} 5^{2n-2k} 2^{2k-2} 6^{k+2}.$$

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

## Tabla de contenidos

1 COEFICIENTE BINOMIAL

2 COEFICIENTE MULTINOMIAL

3 ESTIMACIÓN FUNCIÓN FACTORIAL

## 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  $\{1, 2, \dots, n\}$  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

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

## Demostración:

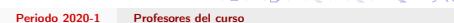
La idea es conectar cada  $i = 1, 2, \dots, n$  con  $n+1-i$  y estimar cada producto  $i(n+1-i)$  superiormente e inferiormente.

Para cada  $i = 1, 2, \dots, n$  se tiene que  $n+1-i = n, n-1, \dots, 2, 1$ ; así el producto:

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

contiene cada factor  $j = 1, 2, \dots, n$  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  $i = 1, 2, \dots, n$ .

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,

COEFICIENTE BINOMIAL  
ooooCOEFICIENTE MULTINOMIAL  
ooooooooooooESTIMACIÓN FUNCIÓN FACTORIAL  
○○●ooooooooCOEFICIENTE BINOMIAL  
ooooCOEFICIENTE MULTINOMIAL  
ooooooooooooESTIMACIÓN FUNCIÓN FACTORIAL  
○○●ooooooooCOEFICIENTE BINOMIAL  
ooooCOEFICIENTE MULTINOMIAL  
ooooooooooooESTIMACIÓN FUNCIÓN FACTORIAL  
○○●oooooooo③ Veamos que se cumple para  $n$ :

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

$$\begin{aligned} n! &\leq \underbrace{ne \frac{(n-1)^n}{e^{n-1}}}_{=} \frac{e n^n}{e^{n-1}} \\ &\leq \left[ en \left( \frac{n}{e} \right)^n \right] \underbrace{\left[ \left( \frac{n-1}{n} \right)^n e \right]}_{(*)} \end{aligned}$$

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

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

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

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

## Demostración:

Probaremos 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:

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



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:

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

La demostración queda como ejercicio.

## Estimaciones de los Coeficientes Binomiales

Ronald Mas,  
Angel Ramirez

24 de junio de 2020

### Contenido

- ① Estimaciones de los Coeficientes Binomiales
- ② Fórmula de Stirling
- ③ Principio del Palomar

Periodo 2020-1 Profesores del curso

Ronald Jesús Mas Huamán

Estimaciones de los Coeficientes Binomiales

24 de junio de 2020

1 / 14

Ronald Jesús Mas Huamán

Estimaciones de los Coeficientes Binomiales

24 de junio de 2020

2 / 14

## Introducción

Empecemos estudiando una estimación rápida del coeficiente binomial:

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots2\cdot1} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}$$

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

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

Ronald Jesús Mas Huamán

Estimaciones de los Coeficientes Binomiales

24 de junio de 2020

3 / 14

### 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

Entonces

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

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

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

## 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:

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

luego al reescribir  $P$  se tiene:

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

## 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:

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

Por lo tanto se tiene el resultado deseado.

## Continua prueba

Entonces  $(2m+1)P^2 < 1$ , por tanto  $P \leq \frac{1}{\sqrt{2m}}$ .

Veamos la otra desigualdad, como

$$\left(1 - \frac{1}{(2i-1)^2}\right) < 1, \forall i \in \{2, 3, \dots, m\}$$

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

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:

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

Definamos la relación  $\sim$  sobre el conjunto

$A = \{f(n) : f \text{ es una sucesión de números reales}\}$  como

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

Veámos que dicha relación es de equivalencia:

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

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

### Fórmula de Stirling

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

#### Ejemplo:

- Para  $n = 10$  se tiene:

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

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

- Para  $n = 12$  se tiene:

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

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

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:

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

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

- Para  $n = 10000$  se tiene:

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

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

### 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  $\lceil \frac{n-1}{k} \rceil + 1$  o más objetos.

#### Prueba:

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

$$\lceil \frac{n-1}{k} \rceil < \frac{n}{k}$$

entonces el número total de objetos es a lo más

$$k \cdot \lceil \frac{n-1}{k} \rceil < k \left( \frac{n}{k} \right) = n$$

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

### Estimaciones de los Coeficientes Binomiales

Ronald Mas,  
Angel Ramirez

22 de junio de 2020

#### Contenido

- ① Principio de inclusión y exclusión
- ② Álgebra de Boole
- ③ Funciones booleanas

### Resultados Previos

#### Proposición

$|A \subset B| \text{ entonces } |B - A| = |B| - |A|$ .

#### 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

$|A, B \text{ y } C \text{ son conjuntos finitos disjuntos dos a dos se cumple que:}$

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

#### Prueba:

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

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

**Teorema**

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

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

**Prueba:**

Procedamos por inducción:

- 1) Para  $n = 2$  se tiene que:

$$\text{Como } A_1 \cup A_2 = [A_1 - (A_1 \cap A_2)] \cup [A_2 - (A_1 \cap A_2)] \cup [A_1 \cap A_2].$$

Por lo resultados previos se tiene que:

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

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

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

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

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

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

**Ejemplo:****Fórmula del Indicador**

Para un número natural el valor de  $\varphi(n)$  llamado **Indicador de Euler o función de Euler** es definido como la cantidad de números  $m \leq n$  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

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

**Álgebra de Boole****Definición**

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

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

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  $\bar{a}$  llamado el complemento de  $a$  tal que  $a + \bar{a} = 1$  y  $a \cdot \bar{a} = 0$ .

**Prueba del teorema****Continuación de la prueba****Teorema**

Sea  $B$  un álgebra de Boole, se cumple:

- 1) El complemento  $\bar{a}$  de  $a \in B$  es único.
- 2) Los elementos 0 y 1 son únicos.
- 3)  $(\bar{\bar{a}}) = a$ ,  $\forall a \in B$ .
- 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  $\bar{a + b} = \bar{a} \cdot \bar{b}$  y  $\bar{a \cdot b} = \bar{a} + \bar{b}$ .

**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:

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

$$\begin{aligned} 3) \quad \bar{a} + a &= a + \bar{a} \\ &= 1 \quad \text{y} \\ \bar{a} \cdot a &= a \cdot \bar{a} \\ &= 0 \end{aligned}$$

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

- 4) Sea  $a \in B$  entonces:

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

**Definición**

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

$$\begin{array}{ccc} f : & B^n & \longrightarrow B \\ & (x_1, \dots, x_n) & \mapsto f(x_1, \dots, x_n) \end{array}$$

**Observaciones:**

- a) La variable  $x \in B$  se denomina **variable booleana**.
- b) En el lenguaje de las máquinas el 0 significa apagado y el 1 encendido.

**Ejemplo 1:**

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

**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:

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

**GRAFOS. ISOMORFISMO. SUBGRAFOS. CAMINOS. CICLOS.****Profesores del curso:**

Ronald Mass<sup>1</sup>

Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



19 de junio de 2020

**Tabla de contenidos**

- 1 Grafos
- 2 Grafos importantes
- 3 Grafos Isomorfos
- 4 Subgrafos
- 5 Conexidad

**Observaciones****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  $G$ .

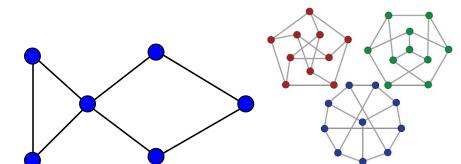
**Ejemplo:**

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

- 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).

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.



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

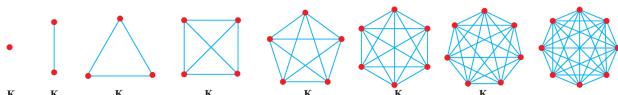
- 1 Grafos
- 2 Grafos importantes
- 3 Grafos Isomorfos
- 4 Subgrafos
- 5 Conexidad

Periodo 2020-1 Profesores del curso

Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooo Conexidad oooooo

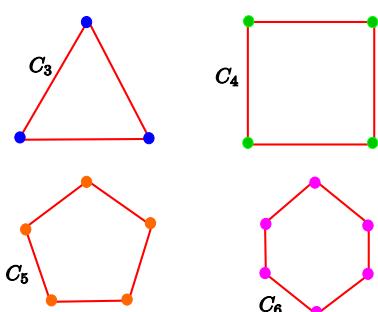
## Grafo completo $K_n$

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



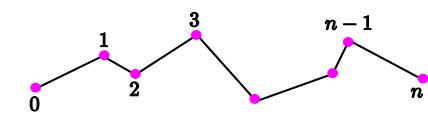
## Ciclo $C_n$

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



## Ruta (Path) $P_n$

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



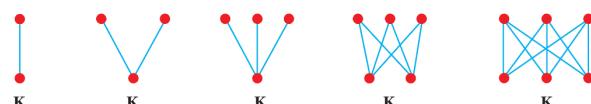
Un path  $P_n$  también es llamado **camino simple**.

Periodo 2020-1 Profesores del curso

Grafos oooooo Grafos importantes oooo● Grafos Isomorfos oooooo Subgrafos oooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooo Conexidad oooooo

## Grafo bipartito $K_{n,m}$

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



## Tabla de contenidos

- 1 Grafos
- 2 Grafos importantes
- 3 Grafos Isomorfos
- 4 Subgrafos
- 5 Conexidad

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.

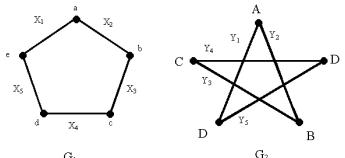
### Definición 2

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

Grafo G	Grafo H	Un isomorfismo entre G y H
		$f(a) = 1$ $f(b) = 6$ $f(c) = 8$ $f(d) = 3$ $f(e) = 5$ $f(f) = 2$ $f(g) = 4$ $f(h) = 7$

## 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 isomorfo a  $G^c$ . Demuestre que si  $G$  es **autocomplementario** entonces  $n \equiv 0$  o  $1 \bmod 4$ , 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:

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

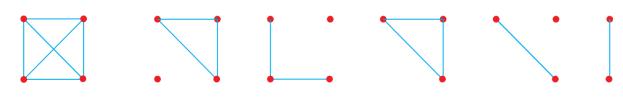
## Ejemplo (cont.)

## Tabla de contenidos

- 1 Grafos
- 2 Grafos importantes
- 3 Grafos Isomorfos
- 4 Subgrafos
- 5 Conexidad

## 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  $E(G) = E(G') \cap \binom{V(G)}{2}$ .

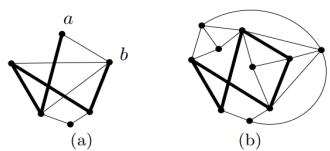


Figura 2: (a) Ejemplo de subgrafo. (b) Ejemplo de subgrafo inducido.

## Ejemplo:

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

### Demostración:

Afirmamos que  $K_4$  no es un subgrafo de  $K_{4,4}$ . Procedemos a demostrarlo. Sean  $X$  y  $Y$  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  $K_4$ .

## Camino en un grafo

Un subgrafo de un grafo  $G$  isomorfo 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:

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

donde  $v_0, v_1, \dots, v_t$  son vértices distintos del grafo  $G$  para cada  $i = 1, 2, \dots, t$  y además  $e_i = \{v_{i-1}, v_i\} \in E(G)$ .

También decimos que el camino  $(v_0, e_1, v_1, \dots, e_t, v_t)$  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

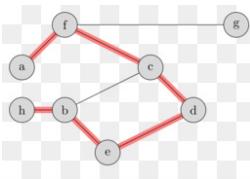


Figura 3:  
 $P_6 = \{a, \{a, f\}, f, \{f, c\}, c, \{c, d\}, d, \{d, e\}, e, \{e, b\}, b, \{b, h\}, h\}$ .

## 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 **círculo**. Un ciclo en un grafo  $G$  puede ser entendido como una secuencia:

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

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

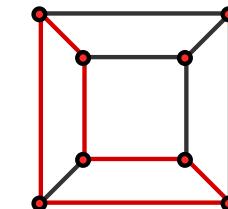


Figura 4:  $C_6$ .

## Ejemplo de ciclo

Periodo 2020-1 Profesores del curso

Grafos oooooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo

## Ejemplo de ciclo

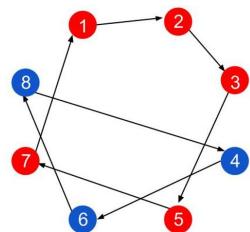


Figura 5:  $C_3$  y  $C_5$ .

## Tabla de contenidos

- 1 Grafos
- 2 Grafos importantes
- 3 Grafos Isomorfos
- 4 Subgrafos
- 5 Conexidad

## 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  $y$ .

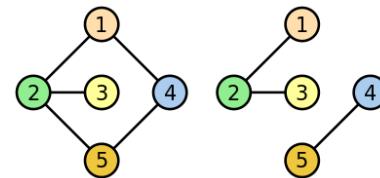


Figura 6: Grafo conexo (Izquierda). Grafo no conexo (Derecha).

Periodo 2020-1 Profesores del curso

Grafos oooooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo Grafos oooooo Grafos importantes oooo Grafos Isomorfos oooooo Subgrafos oooooooooooo Conexidad oooooo

## Camino (WALK)

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

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

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  $i = 1, \dots, t$ .

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

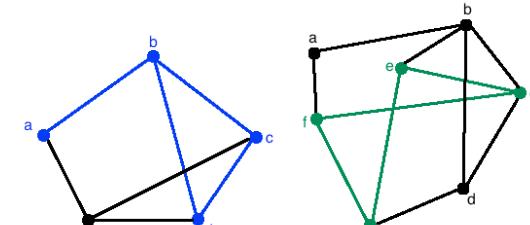


Figura 7: Camino en un grafo

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

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

Verifique que  $\sim$  es una relación de equivalencia.

Sea  $V = V_1 \cup V_2 \cup \dots \cup V_k$  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 <sup>1</sup>

Ángel Ramírez <sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



19 de junio de 2020

## Tabla de contenidos

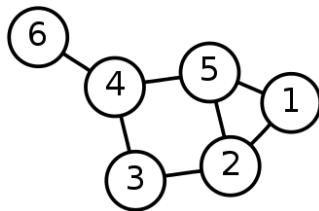
1 Distancia en grafos

2 Matriz de adyacencia

3 Score de un grafo

Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso		
Distancia en grafos ●ooo	Matriz de adyacencia ●oooooooooooo	Score de un grafo oooooooooooo	Distancia en grafos ●ooo	Matriz de adyacencia oooooooooooo	Score de un grafo oooooooooooo	Distancia en grafos ●ooo	Matriz de adyacencia oooooooooooo	Score de un grafo oooooooooooo

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  $d_G : V(G) \times V(G) \rightarrow \mathbb{R}$  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  $d : V(G) \times V(G) \rightarrow \mathbb{R}$  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 entero 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

Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso		
Distancia en grafos ●ooo	Matriz de adyacencia ●oooooooooooo	Score de un grafo oooooooooooo	Distancia en grafos ●ooo	Matriz de adyacencia oooooooooooo	Score de un grafo oooooooooooo	Distancia en grafos ●ooo	Matriz de adyacencia ●oooooooooooo	Score de un grafo oooooooooooo

## Ejemplo:

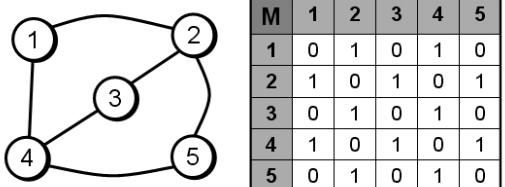


Figura 1: Matriz de adyacencia

Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso			Periodo 2020-1 Profesores del curso		
-------------------------------------	--	--	-------------------------------------	--	--	-------------------------------------	--	--

## Demostración:

### Proposición 1

Sea  $G = (V, E)$  un grafo con vértices  $V = \{v_1, v_2, \dots, v_n\}$  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  $G$ .

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  $v_j$ :



### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

Matriz de adyacencia  
oooo●●●○

Score de un grafo  
oooooooooo

### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

### Periodo 2020-1 Profesores del curso

### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

Matriz de adyacencia  
oooo●●●●●

Score de un grafo  
oooooooooo

## 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

1 Distancia en grafos

2 Matriz de adyacencia

3 Score de un grafo

### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

Matriz de adyacencia  
oooo●●●●●

Score de un grafo  
oooooooooo

### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

### Periodo 2020-1 Profesores del curso

### Periodo 2020-1 Profesores del curso

Distancia en grafos  
oooo

Matriz de adyacencia  
oooo●●●●●

Score de un grafo  
oooooooooo

## 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:



### 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  $v_1, v_2, \dots, v_n$  (en algún orden elegido arbitrariamente). La secuencia

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

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

## Ejemplo:

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

### Demostración:

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

## Ejemplo: (cont.)

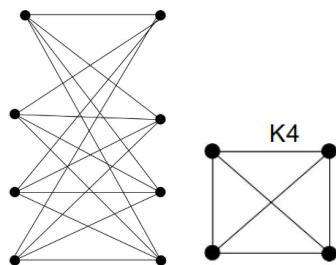


Figura 3:  $K_{4,4}$  a la izquierda.

## 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  $K_{4,4}$ .

Periodo 2020-1 Profesores del curso



Distancia en grafos

Matriz de adyacencia  
oooooooooooo

Score de un grafo  
oooooooooooo

Distancia en grafos  
oooo

Periodo 2020-1 Profesores del curso



Matriz de adyacencia  
oooooooooooo

Score de un grafo  
oooooooooooo

Distancia en grafos  
oooo

Periodo 2020-1 Profesores del curso



Matriz de adyacencia  
oooooooooooo

Score de un grafo  
oooooooooooo

## 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  $D = (d_1, d_2, \dots, d_n)$  una secuencia de números naturales  $n > 1$ . Suponga que  $d_1 \leq d_2 \leq \dots \leq d_n$  y sea el símbolo  $D'$  que denota a la secuencia  $(d'_1, \dots, d'_{n-1})$  donde:

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

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.

Periodo 2020-1 Profesores del curso



Periodo 2020-1 Profesores del curso



Periodo 2020-1 Profesores del curso



## Grafos Eurelianoss

Ronald Mas,  
Angel Ramirez

8 de julio de 2020

### Contenido

- ① Grafos Eurelianoss
- ② Grafos Eurelianoss dirigidos
- ③ Principio del Palomar

## 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

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

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

## Definición

Definamos el recorrido cerrado Eureliano en  $G$  como el camino

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

## 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  $v_9 = v_2$ .

Ronald Jesús Mas Huamán Grafos Eurelianos 8 de julio de 2020 4 / 13

## Continua prueba:

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

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

llegamos a una contradicción.



## 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  $\text{sym}(G) = (V, \bar{E})$  donde

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

El grafo  $\text{sym}(G)$  es llamado la **simetrización** del grafo  $G$ .

## Caracterización de grafos Eureelianos

### 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

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

en  $G$  de mayor longitud posible. Afirmación:

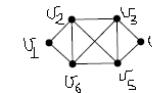
- $v_0 = v_m$  y
- $\{e_i : i = 1, 2, \dots, m\} = E$

Ronald Jesús Mas Huamán Grafos Eurelianos 8 de julio de 2020 5 / 13

### 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  $E_1, E_2, \dots, E_k$  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:

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

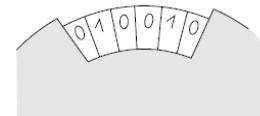
## Continua prueba:

### 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:



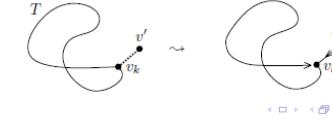
## Continua prueba:

En efecto:

- Si  $v_0 \neq v_m$  entonces el vértice  $v_0$  incidente a un número impar de aristas del recorrido  $T$ , pero como  $\text{deg}_G(v_0)$  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  $T$ .
- 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:

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

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



## Grados Eureelianos 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:

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

tal que  $e_i = (v_{i-1}, v_i) \in E \forall i \in \{1, 2, \dots, m\}$  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 contenido todos los vértices y pasando cada arista dirigida exactamente una vez.

Ronald Jesús Mas Huamán Grafos Eurelianos 8 de julio de 2020 9 / 13

## Continua la aplicación

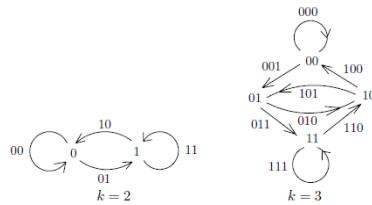
La secuencia de  $n$  dígitos debe ser tal que la posición de la rueda siempre se puede detectar desde los  $k$  dígitos en la ranura, no importa cómo se gire la rueda. Analicemos el siguiente problema

**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

- ① Grafos 2-conexo
- ② Operaciones en grafos
- ③ Grafos libre de triángulos

## 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:

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

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

## 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).

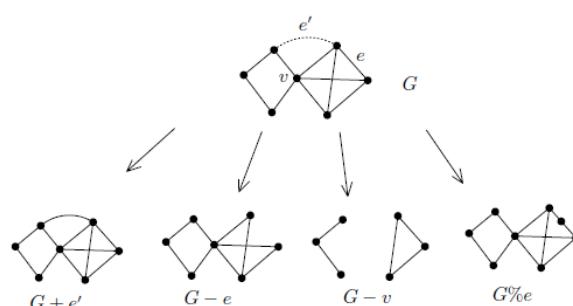
- 4) Subdivisión de una arista:

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

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  $G$  contenido estos dos vértices.

### Prueba:

$\Rightarrow$ ) 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.

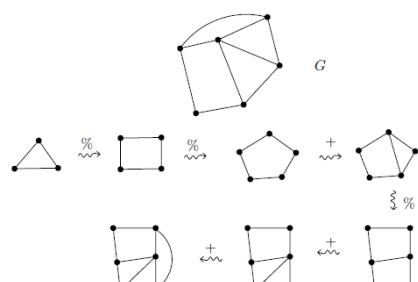
### Prueba:

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  $G \% e$  es 2-conexo entonces  $G$  también es 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  $G$ .



Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

9 / 13

10 / 13

10 / 13

11 / 13

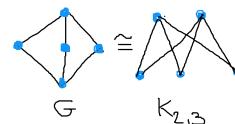
**Teorema**

Para todo número natural  $n$  se tiene que  $T(n) = \left\lfloor \frac{n^2}{4} \right\rfloor$ .

**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  $a = \left\lfloor \frac{n}{2} \right\rfloor$  y  $b = n - \left\lfloor \frac{n}{2} \right\rfloor$ .

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



Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

Ronald Jesús Mas Huamán

Grafos Eureelianos

10 de julio de 2020

12 / 13

13 / 13

## Tabla de contenidos

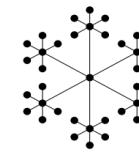
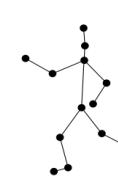
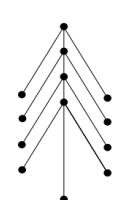
1 Árboles

2 Isomorfismo de árboles

3 Codificando árboles

**Definición 1**

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



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

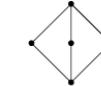
$$0 \leq k \leq \binom{n}{2}.$$

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?

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:

Árboles  
ooooooooooooIsomorfismo de árboles  
ooooooCodificando árboles  
oooooooooooo**ÁRBOLES.**

Profesores del curso:

Ronald Mass <sup>1</sup>Ángel Ramírez <sup>1</sup><sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú

6 de julio de 2020

**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 desconexo.
- 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.

Periodo 2020-1 Profesores del curso



Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

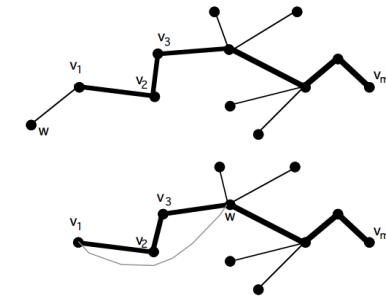
### Demostración del Lema 1

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  $e_1 = \{v_0, t_1\}$  del camino simple  $P$ . Entonces  $v$  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 2

- ( $\Rightarrow$ ): Sean  $x, y \in G \setminus \{v\}$ . 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  $G \setminus \{v\}$ , es decir,  $G \setminus \{v\}$  es conexo. Además, como  $G$  no contiene ciclos, entonces  $G \setminus \{v\}$  tampoco tiene ciclos, y así,  $G \setminus \{v\}$  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  $v' \in G \setminus \{v\}$ , que está unido a  $x$  mediante un camino en  $G \setminus \{v\}$  y luego extendemos este camino añadiendo la arista  $\{v', v\}$ .

Periodo 2020-1 Profesores del curso



Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Periodo 2020-1 Profesores del curso



Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

### 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  $G$ .

Periodo 2020-1 Profesores del curso



Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Periodo 2020-1 Profesores del curso

### Demostración del Teorema 1 (cont.)

- 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, digámoslo 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.

Periodo 2020-1 Profesores del curso



Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

Árboles  
oooooooooooo

Isomorfismo de árboles  
oooooo

Codificando árboles  
oooooooooooo

### 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  $n$ . Consideré 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  $G$ , digámoslas  $G_1$  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:

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

Periodo 2020-1 Profesores del curso

### 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

$$\sum_{v \in V(G)} \deg_G(v) > 2|V| \text{ contradic平iendo el resultado anterior.}$$

Por tanto  $\deg_G(v) \leq 2$ .

Periodo 2020-1 Profesores del curso



## 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 existir al menos un vértice  $v \in V(G)$  tal que  $\deg_G(v) = 1$ , es decir, una hoja de  $G$ .

Considerando el grafo  $G' = G \setminus \{v\}$  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

### 1 Árboles

### 2 Isomorfismo de árboles

### 3 Codificando árboles

### 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  $f : V(T) \rightarrow V(T')$  es un isomorfismo de árboles  $T$  y  $T'$  si  $f$  es una biyección que satisface  $\{x, y\} \in E(T)$  si y 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  $T \cong^r T'$ .

### 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

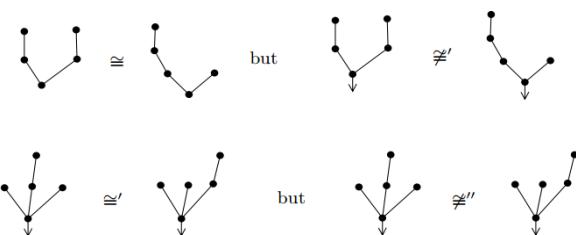


Figura 1: Isomorfos como grafos.



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.

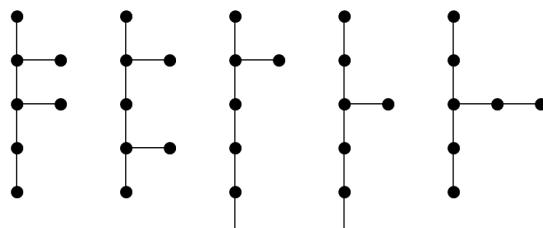
## Ejemplo:

Draw all possible 7-vertex trees with maximum 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<sup>1</sup>

Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



6 de julio de 2020

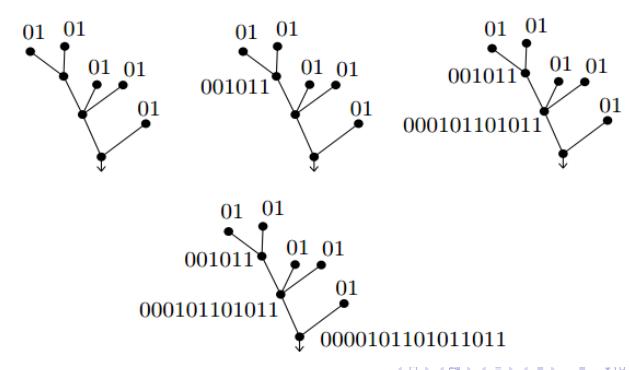
## Tabla de contenidos

### 1 Codificando árboles

## 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  $v_1, v_2, \dots, v_t$  (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  $0A_1A_2\dots A_t1$ .



Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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 ha sido asignado el código  $A(w)$ . Denotemos los hijos de  $v$  mediante  $w_1, w_2, \dots, w_t$  y además  $A(w_1) \leq A(w_2) \leq \dots A(w_t)$ . Luego, el vértice  $v$  recibe el código:  $0A_1A_2\dots A_t1$ , 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  $A = (a_1, a_2, \dots, a_n)$  y  $B = (b_1, b_2, \dots, b_m)$  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  $10011 < 10110$ .

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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:

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

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

## Excentricidad de un vértice

Para un vértice  $v$  de un grafo, el símbolo  $\text{ex}_G(v)$  denota el máximo de las distancias de  $v$  hacia los otros vértices.

El número  $\text{ex}_G(v)$  es llamado **excentricidad** del vértice  $v$  en el grafo  $G$ . Se puede entender que los vértices con excentricidad grande permanecen sobre la periferie de  $G$ .

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:

$$\text{ex}_T(v) = \text{ex}_{T'}(v) + 1.$$

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  $T$ .

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## Código de un árbol

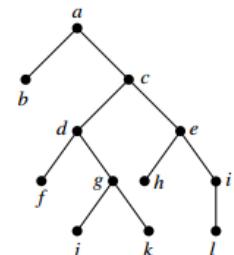
- ① Si el centro de  $T$  es un único vértice, entonces definimos el código de  $T$  como el código del árbol con raíz  $(T, v)$ .
- ② Si el centro de  $T$  consiste de una arista  $e = \{x_1, x_2\}$ , consideramos el grafo  $T - e$ . Este grafo tiene exactamente dos componentes  $T_1$  y  $T_2$ ; la notación es elegida de tal modo que  $x_i \in V(T_i)$ . Considera: 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?

### Solución:

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.



## Árbol de expansión de un grafo

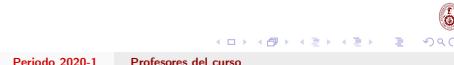
Ronald Mas,  
Angel Ramirez

20 de julio de 2020



### Solución:

- ④ There are 2 non isomorphic unrooted trees with 4 vertices: the 4 chain and the tree with one trivalent vertex and three pendant vertices.
- ⑤ 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).



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

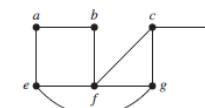
### Solución:

Choose a root for the tree  $T$ . 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  $Y$ .

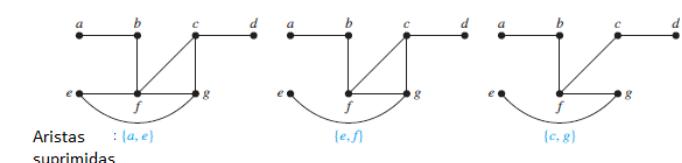


## Ejemplo

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



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



### Contenido

- ① Árbol de expansión de un grafo
- ② Noción de árbol de expansión mínima

### 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.

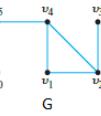
**Algoritmo:(Árbol de expansión)** Sea  $G = (V, E)$  un grafo con  $|V(G)| = n$ ,  $|E(G)| = m$  y secuencia de grados  $(e_1, e_2, \dots, e_m)$ . El algoritmo construye sucesivamente conjuntos de aristas  $E_0, E_1, \dots \subseteq E$ . Sea  $E_0 = \emptyset$ , si el conjunto  $E_{i-1}$  fue encontrado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

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

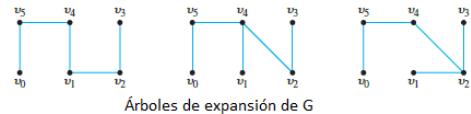
El algoritmo se detiene si  $E_i$  posee  $n - 1$  aristas o  $i = m$ . Es decir todas las aristas del grafo  $G$  han sido considerados. Denotemos por  $E_t$  el conjunto para los cuales el algoritmo se detiene y sea  $T = (V, E_t)$ .

## Ejemplo

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



Los árboles de expansión del grafo  $G$  son:



Árboles de expansión de G

## EL problema del árbol de expansión mínima

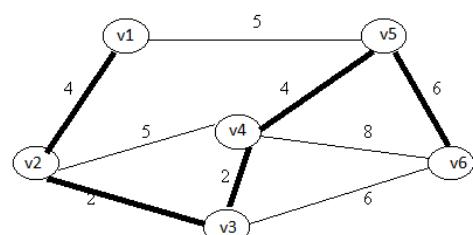
### Introducción:

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 mínimo. Esta sección está dedicada a su solución.



## 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  $w(T) = 4 + 2 + 4 + 5 + 5 = 18$ .

### Proposición

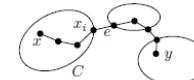
- 1) Si el algoritmo anterior produce un árbol  $T$  con  $n - 1$  aristas entonces  $T$  es un árbol de expansión de  $G$ .
- 2) Si el algoritmo anterior produce un árbol  $T$  que tiene  $k < n - 1$  aristas entonces  $G$  es un grafo desconexo con  $n - k$  componentes.

### 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 desconexo 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  $(x = x_0, e_1, x_1, e_2, \dots, e_l, x_l = y)$  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  $T$ .

## 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  $w : E \rightarrow \mathbb{R}$  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.

## Árbol de expansión de un grafo

Ronald Mas,  
Angel Ramirez

11 de junio de 2021

### Contenido

- ① Algoritmo de Kruskal
- ② Algoritmo de Dijkstra

## Algoritmo de Kruskal

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

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

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.

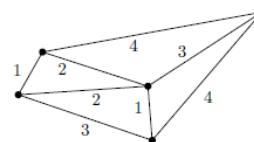
Al acabar el algoritmo, el bosque tiene un solo componente, el cual forma un árbol de expansión mínimo del grafo.

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 3 / 11

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 4 / 11

## 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  $\tilde{T}$  otro árbol de expansión del grafo  $G = (V, E)$ . Por demostrar que  $w(E(T)) \leq w(E(\tilde{T}))$ . Denotemos las aristas de  $T$  por  $e'_1, e'_2, \dots, e'_{n-1}$  tal que  $w(e'_1) \leq w(e'_2) \leq \dots \leq w(e'_{n-1})$  (la arista  $e_i = e_j$  para algún  $j$ ). De igual modo, sea  $\check{e}_1, \dots, \check{e}_{n-1}$  las aristas de  $\tilde{T}$  ordenados en orden creciente por pesos. Vamos a probar que para  $i = 1, \dots, n-1$  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  $w(e'_i) > w(\check{e}_i)$ .

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 5 / 11

## Continua prueba

Al considerar los conjuntos

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

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  $V, E'$ .

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 6 / 11

## Continua prueba

Esto se puede hacer mediante un simple argumento de conteo. Sea  $V_1, \dots, V_s$  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:

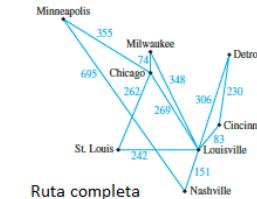
$$|\check{E} \cap \binom{V_j}{2}| \leq |V_j| - 1,$$

y por lo tanto a lo más  $n - s$  aristas de  $\check{E}$  están 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.

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 7 / 11

## El camino mas corto

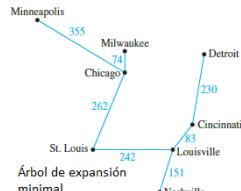
Aunque los árboles producidos por el algoritmo de Kruskal tiene el menor peso posible total en comparación con todos los demás árboles de expansión para los grafos dados, no siempre muestra la distancia más corta entre dos puntos en el grafo. Por ejemplo la siguiente red muestra la ruta completa de viajes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



Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 8 / 11

## Continua

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



De acuerdo con el sistema de ruta completa, se puede volar directamente de Nashville a Minneapolis por una distancia de 695 millas, mientras que si usa el árbol de expansión mínimo la única forma de volar desde Nashville a Minneapolis es pasando por Louisville, St. Louis y Chicago, lo que da distancia total de  $151 + 242 + 262 + 355 = 1010$  millas.

## Algoritmo de Dijkstra

### ALGORITHM 1 Dijkstra's Algorithm.

```

procedure Dijkstra(G: weighted connected simple graph, with
all weights positive)
  (G has vertices  $a = v_0, v_1, \dots, v_n = z$  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  $\infty$ , 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	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$
1	{a}	$\emptyset$		a	$\infty$	$\infty$	$\infty$	$\infty$	$\infty$
2	{a, b}	{(a, b)}		a	$\infty$	4	$\infty$	$\infty$	$\infty$
3	{a, b, c}	{(a, b), (a, c)}		a	4	9	8	$\infty$	$\infty$
4	{a, b, c, e}	{(a, b), (a, c), (c, e)}		a	4	9	5	$\infty$	$\infty$
5	{a, b, c, e, d}	{(a, b), (a, c), (c, e), (e, d)}		a	4	7	5	17	$\infty$
6	{a, b, c, e, d, z}	{(a, b), (a, c), (c, e), (e, d), (e, z)}		a	4	7	5	14	$\infty$

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 9 / 11

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 10 / 11

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 11 / 11

Ronald Jesús Mas Huamán Árbol de expansión de un grafo 11 de junio de 2021 11 / 11

## Tabla de contenidos

### GRAFOS PLANARES.

Profesores del curso:  
 Ronald Mass<sup>1</sup>  
 Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



29 de julio de 2020

#### 1 Grafos planares

#### 2 Ciclos en grafos planares

#### Definición 1 (Arco)

Es un subconjunto  $\alpha$  del plano de la forma

$$\alpha = \gamma([0, 1]) = \{\gamma(x) / x \in [0, 1]\},$$

donde  $\gamma : [0, 1] \rightarrow \mathbb{R}^2$  es una función continua inyectiva definida en el intervalo cerrado  $[0, 1]$  sobre el plano. Los puntos  $\gamma(0)$  y  $\gamma(1)$  son llamados extremos del arco  $\alpha$ .

### Periodo 2020-1 Profesores del curso

Grafos planares  
oooooooooooooooo

Ciclos en grafos planares  
oooooooo

Grafos planares  
oooooooooooooooooooo

Ciclos en grafos planares  
oooooooo

Grafos planares  
oooooooooooooooooooo

Ciclos en grafos planares  
oooooooo

### 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. Consideré 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**).

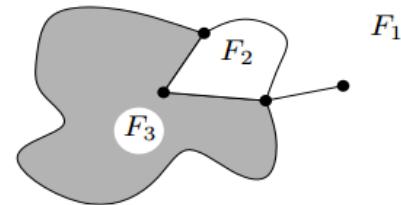


Figura 1: Caras de un grafo planar

### Periodo 2020-1 Profesores del curso

Grafos planares  
oooooooooooooooooooo

Ciclos en grafos planares  
oooooooo

Grafos planares  
oooooooooooooooooooo

Ciclos en grafos planares  
oooooooo

Grafos planares  
oooooooooooooooooooo

Ciclos en grafos planares  
oooooooo

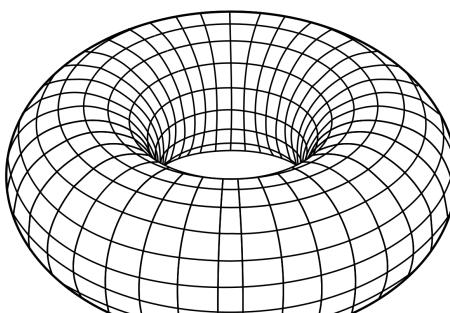
### Dibujos sobre otras superficies

Un grafo puede ser también dibujado sobre otras superficies además del plano. A continuación se muestran algunas otras superficies.

### Superficie esférica



### Superficie del toro



### Periodo 2020-1 Profesores del curso

Grafos planares  
oooooooooooooooo

Ciclos en grafos planares  
oooooooo

Grafos planares  
oooooooooooooooooooo

### Periodo 2020-1 Profesores del curso

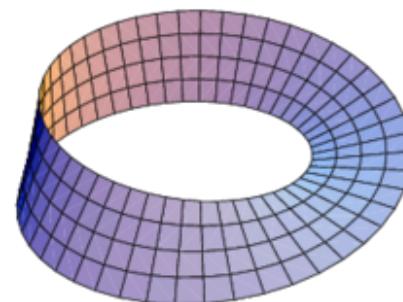
Grafos planares  
oooooooooooooooo

Grafos planares  
oooooooooooooooooooo

### Periodo 2020-1 Profesores del curso

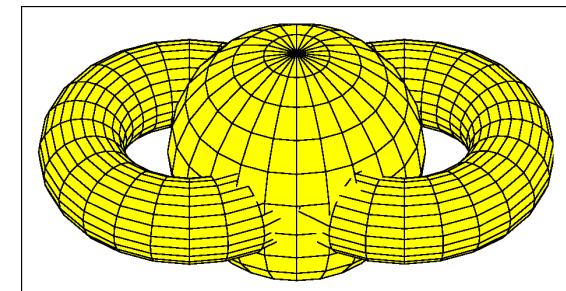
Grafos planares  
oooooooo

## Superficie de la cinta de Möbius



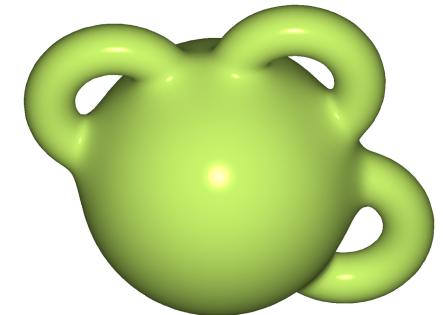
Periodo 2020-1 Profesores del curso

## Esfera con dos asas



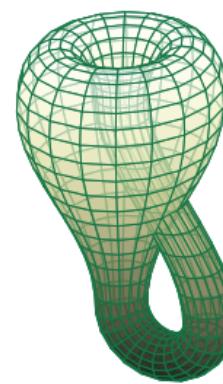
Periodo 2020-1 Profesores del curso

## Esfera con tres asas



Periodo 2020-1 Profesores del curso

## Botella de Klein



Periodo 2020-1 Profesores del curso

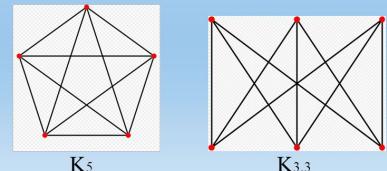
## Observaciones

- 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.

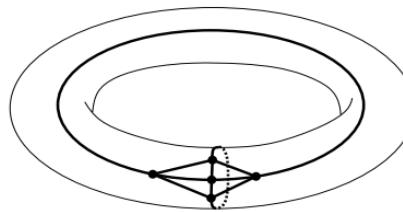
Periodo 2020-1 Profesores del curso

 $K_{3,3}$  y  $K_5$  no son planares.

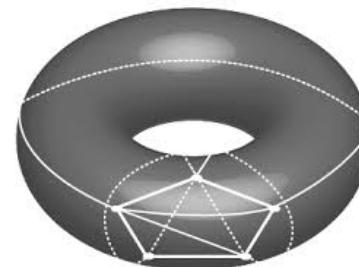
## Nonplanar Graphs

 $K_5$  and  $K_{3,3}$  are not planar

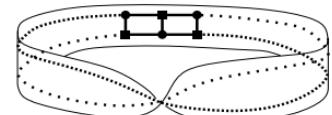
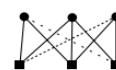
Periodo 2020-1 Profesores del curso

 $K_5$  sobre el Toro

Periodo 2020-1 Profesores del curso

 $K_5$  sobre el Toro

Periodo 2020-1 Profesores del curso

 $K_{3,3}$  sobre la banda de Möbius

Periodo 2020-1 Profesores del curso

## 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  $e_1, e_2, \dots, e_n$  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.



Periodo 2020-1 Profesores del curso

Ciclos en grafos planares  
oooooooooGrafos planares  
ooooooooooooooo

Periodo 2020-1 Profesores del curso

Ciclos en grafos planares  
oooooooooooo

Periodo 2020-1 Profesores del curso

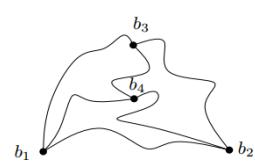
Ciclos en grafos planares  
oooooooooooo

## Proposición 1

$K_5$  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.

Figura 2:  $b_4$  en el interior de la curva de Jordan

## 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  $k$ ).



Periodo 2020-1 Profesores del curso

Ciclos en grafos planares  
oooooooooGrafos planares  
ooooooooooooooo

Periodo 2020-1 Profesores del curso

Ciclos en grafos planares  
ooooooooo

Periodo 2020-1 Profesores del curso

Ciclos en grafos planares  
oooooooooooo

Entonces,  $b_5$  está dentro de la curva formada por los arcos:

$$\begin{aligned} &\alpha(1, 4), \alpha(2, 4) \text{ y } \alpha(1, 2), \text{ o} \\ &\alpha(2, 3), \alpha(3, 4) \text{ y } \alpha(2, 4), \text{ o} \\ &\alpha(1, 3), \alpha(3, 4) \text{ y } \alpha(1, 4). \end{aligned}$$

Sin embargo, en el primer caso, el arco  $\alpha(3, 5)$  intersecta a la curva de Jordan formada por los arcos

$$\alpha(1, 4), \alpha(2, 4) \text{ y } \alpha(1, 2).$$

Similamente en los dos casos restantes.

Si los puntos  $b_4$  y  $b_5$  están en el exterior de  $k$ , se procede de forma análoga.



Periodo 2020-1 Profesores del curso



Periodo 2020-1 Profesores del curso



Periodo 2020-1 Profesores del curso

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  $G$ .

1 Grafos planares

2 Ciclos en grafos planares

## Caras y ciclos en grafos 2-conexos

Si  $e_1, e_2, \dots, e_n$  son las aristas de un ciclo en un grafo topológico planar  $G$ , entonces los arcos  $\alpha(e_1), \dots, \alpha(e_n)$  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<sup>1</sup>

Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



2 de agosto de 2020

## Tabla de contenidos

1 Fórmula de Euler  
● Sólidos platónicos

2 Coloración de mapas

## 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:

Periodo 2020-1 Profesores del curso

Coloración de mapas

Fórmula de Euler

Sólidos platónicos

Periodo 2020-1 Profesores del curso

Coloración de mapas

Fórmula de Euler

Sólidos platónicos

Periodo 2020-1 Profesores del curso

Coloración de mapas

## Fórmula de Euler (cont.)

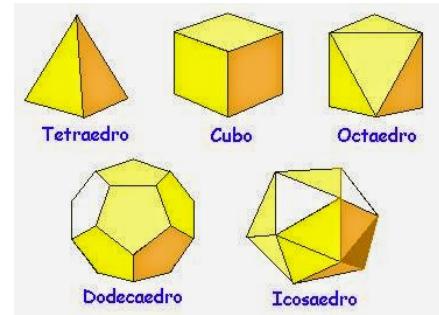
- 1 El grafo  $G$  no tiene ciclos. Entonces  $G$  es un árbol y así  $|V| = |E| + 1$  y al mismo tiempo  $f = 1$  desde que un dibujo planar de un árbol tiene solamente una cara (no limitada).
- 2 Alguna arista  $e \in E$  está contenida en un ciclo. En este caso el grafo  $G - e$  es conexo. Por tanto, 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.



Periodo 2020-1 Profesores del curso

Coloración de mapas

Fórmula de Euler

Sólidos platónicos

Periodo 2020-1 Profesores del curso

Coloración de mapas

Fórmula de Euler

Sólidos platónicos

Periodo 2020-1 Profesores del curso

Coloración de mapas

## 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

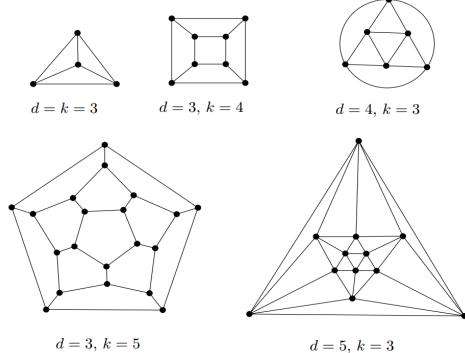


Figura 1: Grafos de los sólidos platónicos

## 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 diviendo 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  $\min(d, k) = 3$ , 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

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 resultado.

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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 no planar.
- 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  $f_j$  el número de caras (en algún dibujo planar fijo) limitados por ciclos de longitud  $j$ . 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:

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \dots = 12 + 2f_4 + 4f_5 + 6f_6 + \dots$$

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.

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

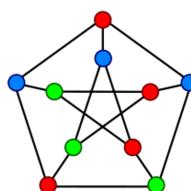
## Tabla de contenidos

1 Fórmula de Euler

2 Coloración de mapas

## Definición 2

Sea  $G = (V, E)$  un grafo, y sea  $k$  un número natural. Una función  $c : V \rightarrow \{1, 2, \dots, k\}$  es llamada 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  $c : V(G) \rightarrow \{1, 2, \dots, k\}$ .



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:

$$\sum_i (6 - i)n_i - 4 = 2 \sum_j (j - 3)f_j + 8.$$

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## 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  $G_1, G_2, \dots, G_k$  que tienen números cromáticos  $\chi(G_1), \chi(G_2), \dots, \chi(G_k)$  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.

Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●ooooooooooooFórmula de Euler  
ooooooooooooooo

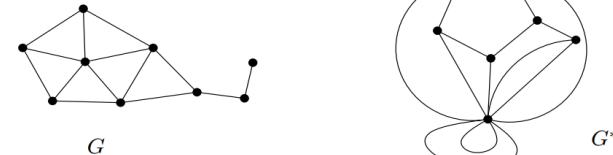
Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●ooooooooooooFórmula de Euler  
ooooooooooooooo

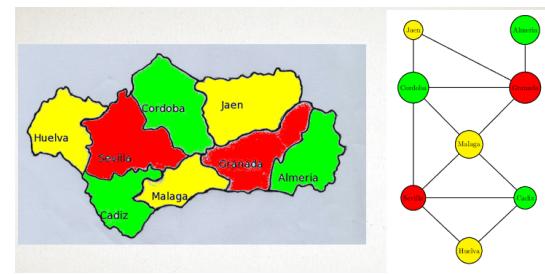
Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●ooooooooooooFórmula de Euler  
ooooooooooooooo

## Ejemplo grafo dual



## Ejemplo grafo dual



Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●ooooooooooooFórmula de Euler  
ooooooooooooooo

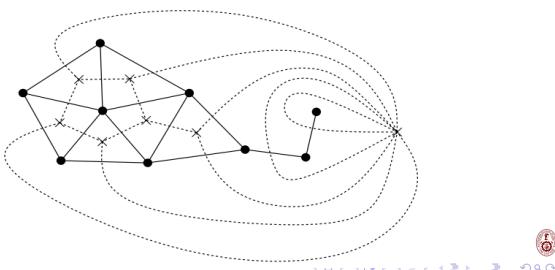
Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●ooooooooooooFórmula de Euler  
ooooooooooooooo

Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooo●oooooooooooo

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

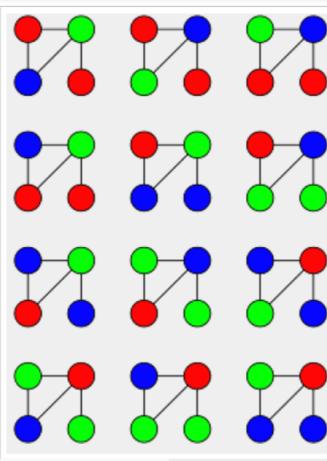
No sólo interesa saber si se puede colorear un grafo con  $k$  colores, sino también de cuántas maneras se puede colorear.

Como queremos contar y calcular, considere un grafo  $G$  y para cada entero  $k \geq 1$  definimos:

$$P_G(k) = \#\{\text{coloraciones distintas de } G \text{ usando los colores de la colección } \{1, \dots, k\}\}$$

teniendo en 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:

$$\text{Si } k < k' \Rightarrow P_G(k) \leq P_G(k')$$

Periodo 2020-1 Profesores del curso

Fórmula de Euler  
oooooooooooo

Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooooooooooo

## Polinomios cromáticos de algunos grafos

Resumiendo las tres observaciones anteriores, deducimos que:

$$\begin{aligned} \text{Si } k \geq \chi(G) &\Rightarrow P_G(k) \geq 1, \\ \text{Si } k < \chi(G) &\Rightarrow P_G(k) = 0 \end{aligned}$$

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.

- ① Triángulo  $K_3$ :  $P_G(k) = k(k-1)(k-2)$ .
- ② Grafo completo  $K_n$ :  $P_G(k) = k(k-1)(k-2)\dots(k-n+1)$ .
- 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 qué número de colores  $k$  general? Intentemos contar las coloraciones directamente. Tendremos  $k$  posibles 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.

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

Coloración de mapas  
oooooooooooooooo

## Aritmética de los Enteros

Ronald Mas,  
Angel Ramirez

12 de agosto de 2020

### Contenido

- ① Algoritmo de la división
- ② Mcd y Mcm
- ③ Teorema Fundamental de la Aritmética

## 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 conjuntos con las mismas características de  $\mathbb{Z}$ , estos reciben el nombre de **dominio de factorización única**.

## 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 hipótesis 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

$$n = \left( \sum_{i=0}^m a'_i b^i \right) b + r = \sum_{i=0}^m a'_i b^{i+1} + r$$

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  $a | b$ .

### 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)  $d | a$  y  $d | b$ .

2) Si existe  $d' \in \mathbb{Z}$  tal que  $d' | a$  y  $d' | b$  entonces  $d' | d$ .

En adelante denotamos  $d = MCD(A, B)$ .

### Observación:

- Si existe el MCD de  $a$  y  $b$  este es único.

## Continua la prueba

### Afirmación 2: $d = MCD(a, b)$ .

- 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  $ma + nb = (m_0a + n_0b)q + r$  de donde se concluye que  $r = ((m - m_0)a) + ((n - n_0q)b) \in I$ . 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  $d | x$ ,  $\forall x \in I$ . Luego en particular  $d | a$  y  $d | b$ .
- Si  $d' | a$  y  $d' | b$  entonces  $d' | (m_0a + n_0b)$ , es decir  $d' | d$ .

### 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:  $\pm 1$  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:

$$P = \{p_1, p_2, \dots, p_k\} \text{ ; tal que } p_1 \leq p_2 \leq \dots \leq p_k$$

Luego el elemento  $p_k$  es el máximo elemento que pertenece a  $P$ .

Por otro lado,  $m = p_1 \cdot p_2 \cdots p_k + 1 \in P$  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:

- Si  $p = 4k + 1$  con  $k \in \mathbb{N}$  entonces  $p$  se puede expresar como suma de dos cuadrados.
- Si  $p = 4k + 3$  con  $k \in \mathbb{N}$  entonces  $p$  no se puede expresar como suma de dos cuadrados.

#### Prueba:

- 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  $a | bc$  y  $MCD(a, b) = 1$  entonces  $a | c$ .

#### Prueba:

Como  $MCD(a, b) = 1$  entonces existen  $r, s \in \mathbb{Z}$  tal que  $ra + sb = 1$  entonces  $rac + sbc = c$  y como  $a | bc$  se tiene que  $a | c$ .

### Lema (2)

Si  $a \in \mathbb{Z}$  y  $p \in \mathbb{Z}$  es un número primo entonces  $p | a$  o  $MCD(a, p) = 1$ .

#### Prueba:

Si  $p | a$  no hay nada que probar. Supongamos que  $p \nmid a$  sea  $d = MCD(a, p)$  entonces  $d | p$  y  $d | a$ . Luego  $d = 1$  (termina la prueba) o  $d = p$ , si  $d = p$  entonces  $p | a$ , ello es un contradicción.

### Lema (3)

Sean  $a, b \in \mathbb{Z}$  no nulos y  $p \in \mathbb{Z}$  primo. Si  $p | ab$  entonces  $p | a$  o  $p | b$ .

#### Prueba:

Si  $p | a$ , termina la prueba. Supongamos que  $p \nmid a$  entonces por el lema anterior  $MCD(a, p) = 1$  y como  $p | ab$ , se tiene por el lema (1) que  $p | b$ .

## 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  $p_1 \leq p_2 \leq \cdots \leq p_k$  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 como 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 hipótesis inductiva se tiene:

$$\begin{aligned} d &= q_1 q_2 \cdots q_r \quad \text{con } q_1 \leq q_2 \leq \cdots \leq q_r \text{ primos positivos} \\ d' &= q'_1 q'_2 \cdots q'_s \quad \text{con } q'_1 \leq q'_2 \leq \cdots \leq q'_s \text{ primos positivos.} \end{aligned}$$

Al reemplazar y ordenar si fuese necesario los primos

$$q_1, q_2, \dots, q_r, q'_1, q'_2, \dots, q'_s \text{ se tiene el resultado deseado con } k = r + s.$$

### 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  $p_i = p'_i$ ,  $\forall i \in \{1, 2, \dots, k\}$ . 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:

$$\begin{aligned} p_1 \mid p'_j &\quad \text{para algún } j \text{ tal que } 1 \leq j \leq s \quad \text{entonces } p_1 = p'_j \\ p'_1 \mid p_i &\quad \text{para algún } i \text{ tal que } 1 \leq i \leq k \quad \text{entonces } p'_1 = p_i \end{aligned}$$

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 hipótesis inductiva aplicada a  $r = k - 1$  se tiene que  $k - 1 = s - 1$  y  $p_2 = p'_2, p_3 = p'_3, \dots, p_k = p'_k$ . Por tanto  $k = s$  y  $p_i = p'_i$ ,  $\forall i \in \{1, 2, \dots, k\}$ .

## Aritmética Modular

Ronald Mas,  
Angel Ramirez

14 de agosto de 2020

## Contenido

- 1 Teorema chino del resto
- 2 Los enteros módulo  $n$
- 3 Ejemplos

### Teorema (Teorema chino del resto)

Sean  $n_1, n_2, \dots, n_k \in \mathbb{N}$ ,  $k$  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:

$$n_1 x_1 + r_1 = n_2 x_2 + r_2 = \cdots = n_k x_k + r_k. \quad (1)$$

#### 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 cual es  $(x_1, x_2) = (z_1(r_2 - r_1), z_2(r_1 - r_2))$ . Supongamos que el resultado es cierto para  $k \geq 2$ , veámoslo para  $k + 1$ .

Sean  $n_1, n_2, \dots, n_{k+1} \in \mathbb{N}$  números primos relativos dos a dos y  $r_1, r_2, \dots, r_{k+1} \in \mathbb{Z}$  elegidos arbitrariamente.

## Continua la prueba

Por hipótesis de inducción, existen enteros  $x_1, x_2, \dots, x_k \in \mathbb{Z}$  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

$$X_j = \frac{n_1 n_2 \cdots n_k X}{n_j} + x_j \in \mathbb{Z} \quad \forall 1 \leq j \leq k \text{ y } X_{k+1} = Y,$$

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:

$$\bar{a} = \{a + kn : k \in \mathbb{Z}\} \text{ y}$$

$$\mathbb{Z}_n := \frac{\mathbb{Z}}{\equiv_n} = \{\bar{a} : a \in \mathbb{Z}\}$$

### Proposición

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\} \text{ y } |\mathbb{Z}_n| = n.$$

**Prueba:** Si  $x \in \mathbb{Z}_n$  entonces  $x = \bar{a}$  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  $x = \bar{a} = \bar{r}$ . Luego  $x \in \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ , es decir:

$$\mathbb{Z}_n \subseteq \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}.$$

Por tanto

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}.$$

Por otro lado veámos que  $|\mathbb{Z}_n| = n$ , supongamos que existen  $i, j \in \mathbb{Z}$  tal que  $0 \leq i < j < n$  y  $\bar{i} = \bar{j}$  entonces  $j - i = n\alpha$ ,  $\alpha \in \mathbb{Z}$  y como  $0 < j - i < n$  se tiene que  $0 < n\alpha < n$  entonces  $0 < \alpha < 1$  con  $\alpha \in \mathbb{Z}$ , lo cual es una contradicción.

### Proposición

Sean  $\bar{a}, \bar{a}', \bar{b}, \bar{b}' \in \mathbb{Z}_n$ . Si  $\bar{a} = \bar{a}'$  y  $\bar{b} = \bar{b}'$  entonces

$$\bar{a} + \bar{b} = \bar{a}' + \bar{b}' \text{ y } \bar{a} \bar{b} = \bar{a}' \bar{b}'.$$

#### Prueba:

Como  $\bar{a} = \bar{a}'$  y  $\bar{b} = \bar{b}'$  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  $\bar{a} + \bar{b} = \bar{a}' + \bar{b}'$ . Por otro lado, como  $\bar{a} \bar{b} - \bar{a}' \bar{b}' = (a - a')b + a'(b - b')$  se tiene que  $n \mid (\bar{a} \bar{b} - \bar{a}' \bar{b}')$ , así  $\bar{a} \bar{b} = \bar{a}' \bar{b}'$ .

### Definición

En  $\mathbb{Z}_n$  definimos las operaciones:

$$\bar{a} \oplus \bar{b} = \bar{a} + \bar{b} \text{ y } \bar{a} \odot \bar{b} = \bar{a} \bar{b}$$

La proposición anterior nos garantiza la buena definición de estas operaciones. Por abuso de notación  $\oplus$  y  $\odot$  las denotamos por  $+$  y  $\cdot$ .

## Teorema

Las operaciones en  $\mathbb{Z}_n$  satisfacen las siguientes propiedades:

- 1)  $\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z}$ ,  $\forall \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$ .
- 2)  $\exists \bar{0} \in \mathbb{Z}_n : \bar{x} + \bar{0} = \bar{0} + \bar{x} = \bar{x}$ ,  $\forall \bar{x} \in \mathbb{Z}_n$ .
- 3)  $\forall \bar{x} \in \mathbb{Z}_n$ ,  $\exists (-\bar{x}) \in \mathbb{Z}_n$ :  $\bar{x} + (-\bar{x}) = (-\bar{x}) + \bar{x} = \bar{0}$ .
- 4)  $\bar{x} + \bar{y} = \bar{y} + \bar{x}$ ,  $\forall \bar{x}, \bar{y} \in \mathbb{Z}_n$ .
- 5)  $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$ ,  $\forall \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$ .
- 6)  $\exists \bar{1} \in \mathbb{Z}_n$ :  $\bar{x}\bar{1} = \bar{1}\bar{x} = \bar{x}$ ,  $\forall \bar{x} \in \mathbb{Z}_n$ .
- 7)  $\bar{x}\bar{y} = \bar{y}\bar{x}$ ,  $\forall \bar{x}, \bar{y} \in \mathbb{Z}_n$ .
- 8)  $\bar{x}(\bar{y} + \bar{z}) = \bar{x}\bar{y} + \bar{x}\bar{z}$ ,  $\forall \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$ .

## Prueba:

- 2)  $\bar{0} = \{0 + kn : k \in \mathbb{Z}\} = \{kn : k \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \dots\}$  y es claro que:

$$\bar{x} + \bar{0} = \bar{x} + \bar{0} = \bar{x}, \bar{0} + \bar{x} = \bar{0} + \bar{x} = \bar{x}, \forall \bar{x} \in \mathbb{Z}_n.$$

- 3)  $\bar{x} + (-\bar{x}) = \overline{x + (-x)} = \bar{0}$  y  $\overline{(-x)} + \bar{x} = \overline{(-x) + x} = \bar{0}$ ,  $\forall \bar{x} \in \mathbb{Z}_n$ .
- 8)  $\bar{x}(\bar{y} + \bar{z}) = \bar{x}(\bar{y} + \bar{z}) = \overline{x(y+z)} = \bar{x}\bar{y} + \bar{x}\bar{z} = \bar{x}\bar{y} + \bar{x}\bar{z}$ ,  $\forall \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$ .

## Proposición

En  $\mathbb{Z}_n$  se cumple que:

- 1) Si  $\bar{x} \neq \bar{0}$  y  $\bar{y} \neq \bar{0}$  entonces  $\bar{x}\bar{y} \neq \bar{0}$  si y sólo si  $n$  es primo.
- 2) Si  $n$  es un número primo, para cada  $\bar{x} \in \mathbb{Z}_n - \{\bar{0}\}$ , existe  $\bar{y} \in \mathbb{Z}_n$  tal que  $\bar{x}\bar{y} = \bar{y}\bar{x} = \bar{1}$ .

## Prueba:

- 2) Sea  $\bar{x} \in \mathbb{Z}_n$  con  $\bar{x} \neq \bar{0}$  entonces  $MCD(p, x) = 1$ , por tanto existen  $r, s \in \mathbb{Z}$  tal que  $pr + xs = 1$ , luego  $\bar{x}s = \bar{1}$ . Por lo tanto  $\exists \bar{y} = \bar{s} \in \mathbb{Z}_n$  tal que  $\bar{x}\bar{y} = \bar{1}$ .

Continua prueba

## Ejemplo 1:

Para  $n = 12$ , se tiene que en  $\mathbb{Z}_{12}$  la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
0	0	No tiene
1	11	1
2	10	No tiene
3	9	No tiene
4	8	No tiene
5	7	5
6	6	No tiene
7	5	7
8	4	No tiene
9	3	No tiene
10	2	No tiene
11	1	11

## Ejemplo 2:

Para  $n = 13$ , se tiene que en  $\mathbb{Z}_{13}$  la siguiente tabla:

	Inverso aditivo	Inverso multiplicativo
0	0	No tiene
1	12	1
2	11	7
3	10	9
4	9	10
5	8	8
6	7	11
7	6	2
8	5	5
9	4	3
10	3	4
11	2	6
12	1	12

Ronald Jesús Mas Huamán Aritmética Modular 14 de agosto de 2020 11 / 13 Ronald Jesús Mas Huamán Aritmética Modular 14 de agosto de 2020 12 / 13 Ronald Jesús Mas Huamán Aritmética Modular 14 de agosto de 2020 13 / 13

Pequeño Teorema de Fermat

Teorema de Wilson

Teorema de Euler

Pequeño Teorema de Fermat

Teorema de Wilson

Teorema de Euler

Pequeño Teorema de Fermat

Teorema de Wilson

Teorema de Euler

## Teoría de números

### Profesores del curso:

Ronald Mass<sup>1</sup>  
Ángel Ramírez<sup>1</sup>

<sup>1</sup>Universidad Nacional de Ingeniería, Lima, Perú



15 de agosto de 2020

## Tabla de contenidos

- 1 Pequeño Teorema de Fermat
- 2 Teorema de Wilson
- 3 Teorema de Euler

## Pequeño Teorema de Fermat

### Teorema 1

Si  $p$  es un primo y  $n \in \mathbb{N}$  relativamente primo con  $p$ , entonces:

$$n^{p-1} \equiv 1 \pmod{p}$$

### Demostración:

Afirmamos que los números  $n, 2n, 3n, \dots, (p-1)n$  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:

$$\begin{aligned} (p-1)!a^{p-1} &= (a)(2a)(3a) \dots ((p-1)a) \\ &= 1 \cdot 2 \cdot \dots \cdot (p-1) = (p-1)! \end{aligned}$$

El número  $(p-1)!$  no es divisible entre  $p$ , pues es producto de puros números menores que  $p$ , de modo que  $\text{mcd}(p, (p-1)!) = 1$ , así que tiene inverso módulo  $p$ , de modo que podemos cancelarlo

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
○○○○○

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

Pequeño Teorema de Fermat  
○○○○○

Periodo 2020-1 Profesores del curso

Teorema de Wilson  
○●○○○

Teorema de Euler  
○○○○○○

Pequeño Teorema de Fermat  
○○○○○

Periodo 2020-1 Profesores del curso

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

## Tabla de contenidos

- 1 Pequeño Teorema de Fermat
- 2 Teorema de Wilson
- 3 Teorema de Euler

## 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.

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
○○○○○

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

Pequeño Teorema de Fermat  
○○○○○

Periodo 2020-1 Profesores del curso

Teorema de Wilson  
○○○○○

Teorema de Euler  
○●○○○○

Periodo 2020-1 Profesores del curso

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

## Ejemplo:

Determine el residuo que se obtiene al dividir  $15! + 16! + 17!$  entre 17.

## Resolución:

Notemos que 17 divide a  $17!$ , así que  $17! \equiv 0 \pmod{17}$ . Por el teorema de Wilson,  $16! \equiv -1 \pmod{17}$ . Podemos multiplicar esta igualdad por -1, resultando:

$$15! = 15!(-1)(-1) \equiv 15!(16)(-1) = 16!(-1) \equiv (-1)(-1) \equiv 1$$

por tanto:

$$15! + 16! + 17! \equiv 1 + (-1) + 0 \equiv 0 \pmod{17}.$$

## Tabla de contenidos

- 1 Pequeño Teorema de Fermat

- 2 Teorema de Wilson

- 3 Teorema de Euler

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
○○○○○

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

Pequeño Teorema de Fermat  
○○○○○

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
○○○○○

## Ejemplo:

Demuestre que  $13|(2^{50} + 3^{50})$ .

## Demostración:

Por el pequeño teorema de Fermat:

$$\begin{aligned} 2^{12} &\equiv 1 \pmod{13} \\ 3^{12} &\equiv 1 \pmod{13} \end{aligned}$$

Como  $50 = 4(12) + 2$ , entonces:

$$\begin{aligned} 2^{50} &= 2^{4(12)+2} = (2^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 4 \equiv 4 \pmod{13} \\ 3^{50} &= 3^{4(12)+2} = (3^{12})^4 \cdot 3^2 \equiv 1^4 \cdot 9 \equiv 9 \pmod{13} \end{aligned}$$

Luego:  $2^{50} + 3^{50} \equiv (4 + 9) \pmod{13} \equiv 0 \pmod{13}$ .

## Teorema 2 (Teorema de Wilson)

Si  $p$  es un número primo, entonces  $(p-1)! \equiv -1 \pmod{p}$ .

## 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:

$$(p-1)! \equiv (1)(-1)(1 \cdot 1 \cdot \dots \cdot 1) \equiv -1 \pmod{p},$$

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.

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
○○○○○

Teorema de Wilson  
○○○○○

Teorema de Euler  
○○○○○○

## 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:

$$f(mn) = f(m)f(n) \quad \text{para todo } m, n \in \mathbb{N} \text{ tal que } \text{mcd}(m, n) = 1.$$

$f$  es llamada **completamente multiplicativa** si:

$$f(mn) = f(m)f(n) \quad \text{para todo } m, n \in \mathbb{N}$$

## Funció n de Euler

Para cualquier  $n \in \mathbb{N}$  la **función de Euler**, también llamada **Euler's Totient**,  $\phi(n)$  es definida como la cantidad de  $m \in \mathbb{N}$  tal que  $m < n$  y  $\text{mcd}(m, n) = 1$ . Es decir:

$$\phi(n) = |\{m \in \mathbb{N} / m < n \wedge \text{mcd}(m, n) = 1\}|.$$

### 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 reducidos** 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:

$$\phi(n) = \prod_{j=1}^k (p_j^{a_j} - p_j^{a_j-1}) = \prod_{j=1}^k \phi(p_j^{a_j}).$$

Periodo 2020-1 Profesores del curso

Pequeño Teorema de Fermat  
ooooooTeorema de Wilson  
oooooTeorema de Euler  
ooo●ooo

Periodo 2020-1 Profesores del curso

Periodo 2020-1 Profesores del curso

## Teorema de Euler

Si  $n \in \mathbb{N}$  y  $m \in \mathbb{Z}$  tal que  $\text{mcd}(m, n) = 1$ , entonces:

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

Periodo 2020-1 Profesores del curso