

# Teorema de Cantor y aplicaciones

Clase 15

IIC 1253

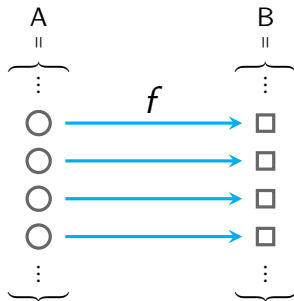
Prof. Cristian Riveros

# Recordatorio: Cardinalidad

Sea  $A$  y  $B$  dos conjuntos.

## Definición

$A$  y  $B$  son **equinumerosos** si existe una biyección  $f : A \rightarrow B$ .



Si  $A$  es **equinumeroso** con  $B$  lo anotaremos como  $|A| = |B|$ .

# Recordatorio: Cardinalidad

## Proposición

La relación  $|\cdot| = |\cdot|$  es una **relación de equivalencia**, esto es:

1. refleja.
2. simétrica.
3. transitiva.

Por lo tanto, podemos tomar las clases de equivalencia de  $|\cdot| = |\cdot|$ .

## Definición

Para un conjunto  $A$ , denotaremos por  $|A|$  su **clase de equivalencia** según la relación  $|\cdot| = |\cdot|$ .

# Recordatorio: Conjuntos numerables

## Definición

Decimos que un conjunto  $A$  es **numerable** si:  $|A| = |\mathbb{N}|$ .

## Proposición

$A$  es **numerable** si, y solo si, existe una secuencia infinita:

$$a_0, a_1, a_2, a_3, \dots, a_n, a_{n+1}, \dots$$

1.  $a_i \in A$  para todo  $i \in \mathbb{N}$ .
2.  $a_i \neq a_j$  para todo  $i \neq j$ .
3. para todo  $a \in A$ , existe un  $i \in \mathbb{N}$  tal que  $a = a_i$ .

$A$  es numerable si, y solo si,  
todos sus elementos se pueden poner en una **lista infinita**.

# Outline

Teorema de Cantor

Aplicaciones: Algoritmos

Aplicaciones: Números

# ¿son todos los conjuntos numerables?

¿es  $\mathbb{R}$  numerable?

Teorema

$\mathbb{R}$  **NO** es numerable.

Demostración

- Demostraremos que el intervalo  $(0,1)$  de  $\mathbb{R}$  **NO** es numerable.
- Por **contradicción**, supongamos que  $(0,1)$  es numerable.
- Entonces existe una **lista infinita** del los reales en  $(0,1)$ , donde cada elemento aparece una vez y solo una vez.

¿son todos los conjuntos numerables?

### Demostración que $\mathbb{R}$ NO es numerable

Reales	Representación decimal							
$r_0$	0.	$d_{00}$	$d_{01}$	$d_{02}$	$d_{03}$	$d_{04}$	$d_{05}$	$\dots$
$r_1$	0.	$d_{10}$	$d_{11}$	$d_{12}$	$d_{13}$	$d_{14}$	$d_{15}$	$\dots$
$r_2$	0.	$d_{20}$	$d_{21}$	$d_{22}$	$d_{23}$	$d_{24}$	$d_{25}$	$\dots$
$r_3$	0.	$d_{30}$	$d_{31}$	$d_{32}$	$d_{33}$	$d_{34}$	$d_{35}$	$\dots$
$r_4$	0.	$d_{40}$	$d_{41}$	$d_{42}$	$d_{43}$	$d_{44}$	$d_{45}$	$\dots$
$r_5$	0.	$d_{50}$	$d_{51}$	$d_{52}$	$d_{53}$	$d_{54}$	$d_{55}$	$\dots$
$\vdots$					$\vdots$			$\ddots$

¿son todos los conjuntos numerables?

### Demostración que $\mathbb{R}$ NO es numerable

Reales	Representación decimal						
$r_0$	0.	$d_{00}$	$d_{01}$	$d_{02}$	$d_{03}$	$d_{04}$	$d_{05} \dots$
$r_1$	0.	$d_{10}$	$d_{11}$	$d_{12}$	$d_{13}$	$d_{14}$	$d_{15} \dots$
$r_2$	0.	$d_{20}$	$d_{21}$	$d_{22}$	$d_{23}$	$d_{24}$	$d_{25} \dots$
$r_3$	0.	$d_{30}$	$d_{31}$	$d_{32}$	$d_{33}$	$d_{34}$	$d_{35} \dots$
$r_4$	0.	$d_{40}$	$d_{41}$	$d_{42}$	$d_{43}$	$d_{44}$	$d_{45} \dots$
$r_5$	0.	$d_{50}$	$d_{51}$	$d_{52}$	$d_{53}$	$d_{54}$	$d_{55} \dots$
$\vdots$					$\vdots$		$\ddots$

- Para cada  $i \geq 0$ , definamos: 
$$d_i = \begin{cases} d_{ii} + 1 & d_{ii} < 9 \\ 0 & d_{ii} = 9 \end{cases}$$
- Defina el número real:  $r = 0.d_0d_1d_2d_3d_4d_5d_6\dots$

¿aparece  $r$  en la lista?



¿son todos los conjuntos numerables?

### Demostración que $\mathbb{R}$ NO es numerable

- Para cada  $i \geq 0$ , definamos:  $d_i = \begin{cases} d_{ii} + 1 & d_{ii} < 9 \\ 0 & d_{ii} = 9 \end{cases}$ .
- Defina el número real:  $r = 0.d_0d_1d_2d_3d_4d_5d_6\dots$

¿aparece  $r$  en la lista?

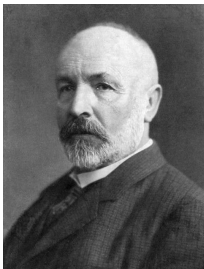
Veamos:

- $r = r_0?$  ✗
- $r = r_1?$  ✗
- $\dots$
- $r = r_n?$  NO, porque el  $n$ -ésimo dígito de  $r$  es distinto al de  $r_n$ :

$$d_n \neq d_{nn}$$

→← **CONTRADICCIÓN** →←

# Argumento de diagonalización de Cantor

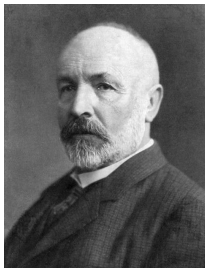


Georg Cantor  
(1845 - 1918)

*"I see it, but I don't believe it!"*

Carta de Cantor a Dedekind.

# Argumento de diagonalización de Cantor



Georg Cantor  
(1845 - 1918)

Técnica inventada por **Georg Cantor** para demostrar que no existe una biyección entre  $A$  y su conjunto potencia:

$$2^A = \{S \mid S \subseteq A\}$$

# Argumento de diagonalización de Cantor

Sea  $A$  un conjunto no vacío.

## Teorema de Cantor

**NO** existe una **biyección** entre  $A$  y el conjunto potencia  $2^A$ .

### Demostración

■ Si  $A$  es finito, el teorema se cumple.

¿por qué?

■ Supongamos que  $A$  es infinito.

Para hacer mas “**pedagógica**” la demostración:

1. Demostraremos que NO existe una biyección de  $\mathbb{N}$  a  $2^{\mathbb{N}}$ .
2. Demostraremos que NO existe una biyección de  $A$  a  $2^A$ .

# Diagonalización entre $\mathbb{N}$ y $2^{\mathbb{N}}$

Suponga (**por contradicción**) una biyección  $f$  entre  $\mathbb{N}$  y  $2^{\mathbb{N}}$ .

Considere la siguiente la matriz:

	0	1	2	3	4	5	6	7	...
$f(0)$	1	1	0	1	0	0	1	1	
$f(1)$	0	0	1	1	1	0	0	1	
$f(2)$	1	1	1	1	0	0	0	0	
$f(3)$	1	0	1	0	0	1	0	1	
$f(4)$	0	0	1	1	0	0	1	0	...
$f(5)$	1	1	0	1	0	1	1	1	
$f(6)$	1	0	0	0	0	0	1	0	
$f(7)$	1	0	0	1	0	1	1	1	
$\vdots$					$\vdots$				$\ddots$

La coordenada  $(i, j)$  es igual a 1 ssi  $j \in f(i)$ .

Cada conjunto  $S \in 2^{\mathbb{N}}$  es una fila en la matriz

# Diagonalización entre $\mathbb{N}$ y $2^{\mathbb{N}}$

Ahora considere la diagonal de la matriz:

	0	1	2	3	4	5	6	7	...
$f(0)$	1	1	0	1	0	0	1	1	
$f(1)$	0	0	1	1	1	0	0	1	
$f(2)$	1	1	1	1	0	0	0	0	
$f(3)$	1	0	1	0	0	1	0	1	
$f(4)$	0	0	1	1	0	0	1	0	...
$f(5)$	1	1	0	1	0	1	1	1	
$f(6)$	1	0	0	0	0	0	1	0	
$f(7)$	1	0	0	1	0	1	1	1	
$\vdots$					$\vdots$				$\ddots$

- El conjunto de la **diagonal** es igual a  $D = \{i \in \mathbb{N} \mid i \in f(i)\}$ .
- El **complemento** de la diagonal es  $\bar{D} = \{i \in \mathbb{N} \mid i \notin f(i)\}$ .

¿aparece  $\bar{D}$  en alguna fila de la matriz?

# Diagonalización entre $\mathbb{N}$ y $2^{\mathbb{N}}$

Definición (complemento de la diagonal)

$$\bar{D} = \{i \in \mathbb{N} \mid i \notin f(i)\}$$

¿aparece  $\bar{D}$  en alguna fila de la matriz?

**NO**, debido a que  $\bar{D}$  difiere con  $f(x)$  para todo  $x \in \mathbb{N}$ .

$$x \in f(x) \quad \text{ssi} \quad x \notin \bar{D}$$

Por lo tanto, no existe una biyección entre  $\mathbb{N}$  y  $2^{\mathbb{N}}$ .



¿podemos ocupar el mismo argumento de la “diagonal” para cualquier conjunto  $A$ ?

# Diagonalización entre $A$ y $2^A$


Suponga (**por contradicción**) una biyección  $f$  entre  $A$  y  $2^A$ .

Definición (complemento de la diagonal)

$$\bar{D} = \{a \in A \mid a \notin f(a)\}$$

Suponga que existe  $x^* \in A$ , tal que  $f(x^*) = \bar{D}$ .

¿  $x^* \in f(x^*)$  ?    o    ¿  $x^* \notin f(x^*)$  ?

■ Si  $x^* \in f(x^*) \Rightarrow x^* \in \bar{D} \Rightarrow x^* \notin f(x^*)$  

■ Si  $x^* \notin f(x^*) \Rightarrow x^* \notin \bar{D} \Rightarrow x^* \in f(x^*)$  

Por lo tanto, NO existe una biyección entre  $A$  y  $2^A$ .





¿cuántos infinitos hay?

$$|\mathbb{N}| < |2^{\mathbb{N}}| = |\mathbb{R}| < |2^{2^{\mathbb{N}}}| < \dots$$

---

Notación:  $\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 < \dots$

Hay una cantidad **infinita** de distintos **infinitos**!!

¿hay algún conjunto que tenga una cardinalidad (infinitud) intermedia?

# ¿hay algún infinito entremedio?

## Hipótesis del continuo

No existe ningún conjunto  $A$  tal que:  $|\mathbb{N}| < |A| < |\mathbb{R}|$ .



David Hilbert  
(1862 - 1943)

Uno de los 23 problemas de Hilbert propuestos en 1900

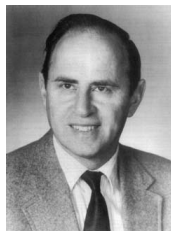
# ¿hay algún infinito entremedio?

## Hipótesis del continuo

No existe ningún conjunto  $A$  tal que:  $|\mathbb{N}| < |A| < |\mathbb{R}|$ .



Kurt Gödel  
(1906 - 1978)



Paul Cohen  
(1934 - 2007)

Con los axiomas de teoría de conjuntos (Zermelo–Fraenkel)

1940: **NO** se puede demostrar que la hipótesis es **falsa**.

1963: **NO** se puede demostrar que la hipótesis es **verdadera**.

# Outline

Teorema de Cantor

**Aplicaciones: Algoritmos**

Aplicaciones: Números

# Problemas de decisión

## Definición

Un **problema de decisión** esta compuesto por:

1. Un conjunto de **inputs** (llamados instancias).
  - Números, grafos, palabras, funciones, etc . . .
2. Una **pregunta** sobre los inputs que se responde con **SI** o **NO**

# Problemas de decisión

## Ejemplo

### NÚMEROS PRIMOS

---

Input: Un número  $N$

Pregunta: ¿es  $N$  primo?

### RELACIONES DE EQUIVALENCIA

---

Input: Una relación finita  $R \subseteq A \times A$

Pregunta: ¿es  $R$  una relación de equivalencia?

# Problemas de decisión

## Ejemplo

### MINIMIZACIÓN DE FUNCIONES

---

Input: Un función  $f : \mathbb{N} \rightarrow \mathbb{N}$  y un número  $c$

Pregunta: ¿es el mínimo de  $f$  mayor que  $c$ ?

### BUSQUEDA EN TEXTO

---

Input: Una página de texto  $T$  y una palabra  $w$

Pregunta: ¿Aparece  $w$  mencionada en  $T$ ?

# Problemas de decisión (definición formal)

Sea  $\mathcal{I}$  un conjunto de inputs (instancias).

## Definición

Un **problema de decisión** es una función:

$$P : \mathcal{I} \rightarrow \{0, 1\}$$

## Ejemplo

Sea  $\text{PRIMO} : \mathbb{N} \rightarrow \{0, 1\}$  tal que para todo  $n \in \mathbb{N}$ :

$$\text{PRIMO}(n) = 1 \quad \text{si, y solo si,} \quad n \text{ es un número primo.}$$

Por ejemplo:

- $\text{PRIMO}(49) = 0$
- $\text{PRIMO}(29) = 1$
- $\text{PRIMO}(997) = ?$



# Solución a los problemas de decisión

Considere su lenguaje de programación favorita (python?).

## Definición

Sea  $\mathcal{I}$  un conjunto de inputs y  $P : \mathcal{I} \rightarrow \{0, 1\}$  un problema de decisión.

- Una **solución** Program es un **programa en python** que recibe inputs en  $\mathcal{I}$  y retorna 0 o 1.
- Una solución Program es un **solución para el problema de decisión**  $P$  si para todo input  $X \in \mathcal{I}$  se cumple:

$P(X) = 1$  si, y solo si, al ejecutar Program con  $X$  retorna 1

# Solución a los problemas de decisión

## Ejemplo

Sea  $\text{PRIMO} : \mathbb{N} \rightarrow \{0, 1\}$  tal que para todo  $n \in \mathbb{N}$ :

$\text{PRIMO}(n) = 1$  si, y solo si,  $n$  es un número primo.

Una **solución** para el problema de decisión PRIMO es el siguiente:

```
import math
def is_prime(n):
    if n % 2 == 0 and n > 2:
        return 0
    for i in range(3, n):
        if n % i == 0:
            return 0
    return 1
```

# ¿cuántas soluciones/programas en python existen?

## Simplificación

Todo programa en python

lo podemos representar como una **palabra** de ceros y unos. (¿por qué?)

## Teorema

El conjunto de todas las **palabras**  $\{0, 1\}^*$  es **numerable**.

## Demostración (ejercicio)

Considere la siguiente lista infinita de  $\{0, 1\}^*$ :

$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, \dots$

## Corolario

La cantidad de **programas** en python es **numerable**.

# ¿cuántos problemas de decisión existen?

## Simplificación

Todo input como números, matrices, conjuntos, relaciones, etc, lo podemos representar con **palabras** de ceros y unos. (¿por qué?)

## Definición

Un **problema de decisión**  $P$  es una función:  $P : \{0,1\}^* \rightarrow \{0,1\}$ .

## Ejemplo

Sea  $\text{PRIMO} : \{0,1\}^* \rightarrow \{0,1\}$  tal que para todo  $n \in \mathbb{N}$ :

$\text{PRIMO}(\text{bin}(n)) = 1$  si, y solo si,  $n$  es un número primo.

- $\text{PRIMO}(00110001) = 0$
- $\text{PRIMO}(00011101) = 1$
- $\text{PRIMO}(0000001111100101) = 1$

# ¿cuántos problemas de decisión existen?

## Simplificación

Todo input como números, matrices, conjuntos, relaciones, etc, lo podemos representar con **palabras** de ceros y unos. (¿por qué?)

## Definición

Un **problema de decisión**  $P$  es una función:  $P : \{0,1\}^* \rightarrow \{0,1\}$ .

- Se define  $\mathcal{P}$  como el conjunto de todos los problemas de decisión:

$$\mathcal{P} = \{ P : \{0,1\}^* \rightarrow \{0,1\} \}$$

- Un problema de decisión  $P$  lo podemos representar como  $L_P \subseteq \{0,1\}^*$ :

$$L_P = \{ w \in \{0,1\}^* \mid P(w) = 1 \}$$

¿cuál es la relación entre  $\mathcal{P}$  y  $2^{\{0,1\}^*}$ ?

# ¿cuántos problemas de decisión existen?

## Teorema

El conjunto  $\mathcal{P}$  es NO numerable.

## Conclusión

Hay problemas de decisión que  
NO tienen una solución computacional (algoritmo).

¿cuál es un problema **sin solución** en computación?

# Outline

Teorema de Cantor

Aplicaciones: Algoritmos

Aplicaciones: Números

# Números reales y nombres

Podemos asociar nombres a los reales:

1	=	uno
2	=	dos
	⋮	
1234	=	mil docientos treinta y cuatro
	⋮	
3.1415 ...	=	$\pi$
2.7182 ...	=	$e$
	⋮	

¿podemos asociar un nombre a cada número real?



# Números algebraicos y trascendentes

## Definición

Un número  $a \in \mathbb{R}$  se dice **algebraico** si existe un polinomio (no nulo)  $p(x)$ :

1.  $p(x)$  tiene coeficientes en los enteros.
2.  $p(a) = 0$ .

## Ejemplo

- todos los números en  $\mathbb{Q}$ .
- $\sqrt{2}$ ,  $\sqrt[5]{17}$ , ...

## Definición

Un número  $a \in \mathbb{R}$  es **trascendente** si NO es algebraico.

¿existen números trascendentes?

# ¿existen números trascendentes?

Los matemáticos se demoraron en demostrar que existían números trascendentes, desde 1600 hasta:

- Liouville (1844):  $\sum_{i=1}^{\infty} 10^{-i!}$
- Hermite (1873):  $e$
- Lindemann (1882):  $\pi$

¿cómo demostramos que existen números trascendentes?

# ¿existen números trascendentes?

## Teorema

Los números algebraicos son numerables.

Demostración (ejercicio)

## Conclusión

Como  $\mathbb{R}$  es NO numerable,  
por lo tanto tienen que existir números trascendentes.