Teorema de Cantor

Clase 19

IIC 1253

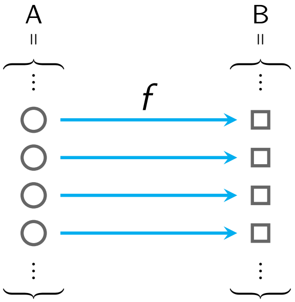
Prof. Cristian Riveros

Recordatorio: Cardinalidad

Sea A y B dos conjuntos.

Definición

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



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

A es **numerable** si tiene la misma cardinalidad que un subconjunto de $\mathbb{N}$.

$$\exists S \subseteq \mathbb{N}.\ \ |A| = |S|.$$

Proposición

A es **numerable** si, y solo si, existe una secuencia (finita o infinita) en A:

$$a_0, a_1, a_2, a_3, \ldots$$

1. $a_i \neq a_j$ para todo $i \neq j$, y
2. 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**.

Outline

Outline

¿son todos los conjuntos numerables?

Teorema

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

Demostración

- Demostraremos que el intervalo $(0, 1)$ de $\mathbb{R}$ NO es numerable.
- Por **contradicción**, suponemos 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}	$\cdots$
r_1	0.	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	$\cdots$
r_2	0.	d_{20}	d_{21}	d_{22}	d_{23}	d_{24}	d_{25}	$\cdots$
r_3	0.	d_{30}	d_{31}	d_{32}	d_{33}	d_{34}	d_{35}	$\cdots$
r_4	0.	d_{40}	d_{41}	d_{42}	d_{43}	d_{44}	d_{45}	$\cdots$
r_5	0.	d_{50}	d_{51}	d_{52}	d_{53}	d_{54}	d_{55}	$\cdots$
$\vdots$					$\vdots$			$\ddots$

¿son todos los conjuntos numerables?

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

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

- 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: $r = 0.d_0 d_1 d_2 d_3 d_4 d_5 d_6 \ldots$

¿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: $r = 0.d_0 d_1 d_2 d_3 d_4 d_5 d_6 \ldots$

¿aparece r en la lista?

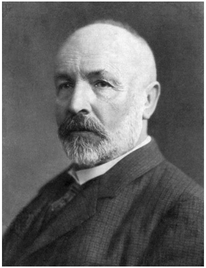
Veamos:

- $r = r_0$? ✕
- $r = r_1$? ✕
- ...
- $r = r_n$? NO, porque el n-esimo digito de r es distinto al de r_n:

$$d_n \neq d_{nn}$$

→← **CONTRADICCIÓN** →←

Argumento de diagonalización de Cantor

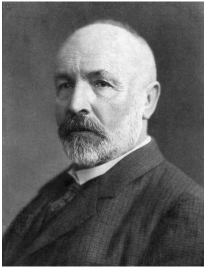


Georg Cantor
(1845 - 1918)

"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 primero que NO existe una biyección de $\mathbb{N}$ a $2^{\mathbb{N}}$.
2. Demostraremos después 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:

$$
\begin{array}{c|ccccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\
\hline
f(0) & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \\
f(1) & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & \\
f(2) & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \\
f(3) & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & \\
f(4) & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & \cdots \\
f(5) & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & \\
f(6) & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \\
f(7) & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & \\
\vdots & & & & & \vdots & & & & \ddots
\end{array}
$$

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	$\cdots$
$f(0)$	$\boxed{1}$	1	0	1	0	0	1	1	
$f(1)$	0	$\boxed{0}$	1	1	1	0	0	1	
$f(2)$	1	1	$\boxed{1}$	1	0	0	0	0	
$f(3)$	1	0	1	$\boxed{0}$	0	1	0	1	
$f(4)$	0	0	1	1	$\boxed{0}$	0	1	0	$\cdots$
$f(5)$	1	1	0	1	0	$\boxed{1}$	1	1	
$f(6)$	1	0	0	0	0	0	$\boxed{1}$	0	
$f(7)$	1	0	0	1	0	1	1	$\boxed{1}$	
$\vdots$					$\vdots$				$\ddots$

- El conjunto de la **diagonal** es igual a $D = \{i \in \mathbb{N} \mid i \in f(i)\} \in 2^{\mathbb{N}}$.
- El **complemento** de la diagonal es $\bar{D} = \{i \in \mathbb{N} \mid i \notin f(i)\} \in 2^{\mathbb{N}}$.

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

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

Definición (complemento de la diagonal)

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

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

NO, debido a que $\bar{D} \neq f(x)$ para todo $x \in \mathbb{N}$, ya que:

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

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

Por contradicción, suponga que existe 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 $x^* \in f(x^*) \quad \Rightarrow \quad x^* \in \bar{D} \quad \Rightarrow \quad x^* \notin f(x^*)$ ✗
- Si $x^* \notin f(x^*) \quad \Rightarrow \quad x^* \notin \bar{D} \quad \Rightarrow \quad x^* \in f(x^*)$ ✗

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

¿cuántos infinitos hay?

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

Notación: $\aleph_0 \quad < \quad \aleph_1 \quad < \quad \aleph_2 \quad < \quad \aleph_3 \quad < \quad \cdots$

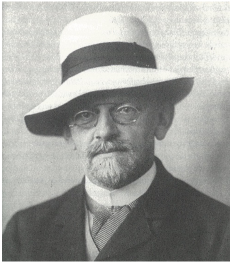
Hay una cantidad **infinita** de distintos **infinitos**!!

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

¿hay algún infinito entremedio?

Hipótesis del continuo

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



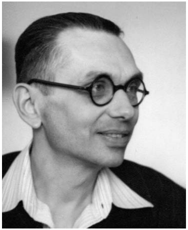
David Hilbert
(1862 - 1943)

Uno de los 23 problemas de Hilbert propuestos en 1900

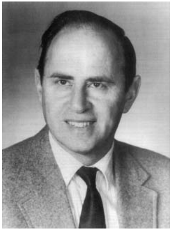
¿hay algún infinito entremedio?

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

Aplicación: Algoritmos

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?

BUSQUEDA EN TEXTO

Input:	Una documento de texto D y una palabra w
Pregunta:	¿Aparece w mencionada en D?

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 $\textsc{Primo} : \mathbb{N} \rightarrow \{0, 1\}$ tal que para todo $n \in \mathbb{N}$:

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

Por ejemplo:

- $\textsc{Primo}(49) = 0$
- $\textsc{Primo}(29) = 1$
- $\textsc{Primo}(997) = ?$

Solución a los problemas de decisión

Considere su lenguaje de programación favorita (python?).

Definición

Sea $\mathcal{I}$ un conjunto de inputs y $P : \mathcal{I} \to \{0, 1\}$ 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:

$$P(X) = 1 \quad \text{si, y solo si,} \quad \text{al ejecutar } \texttt{Program} \text{ con } X \text{ retorna } 1.$$

Solución a los problemas de decisión

Ejemplo

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

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

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 $\{0,1\}^*$:

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

Corolario

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

¿cuántos problemas de decisión existen?

Simplificación

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

Definición

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

Ejemplo

Sea $\textsc{Primo} : \{0,1\}^* \to \{0,1\}$ tal que para todo $n \in \mathbb{N}$:

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

- $\textsc{Primo}(00110001) = 0$
- $\textsc{Primo}(00011101) = 1$
- $\textsc{Primo}(0000001111100101) = 1$

¿cuántos problemas de decisión existen?

Simplificación

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

Definición

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

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

$$\mathcal{P} = \left\{ P : \{0,1\}^* \to \{0,1\} \right\}$$

Teorema

Los conjuntos $\mathcal{P}$ y $2^{\{0,1\}^*}$ son **equinumerosos**.

Demostración: ejercicio.

¿cuántos problemas de decisión existen?

Teorema

1. La cantidad de **programas en python** es numerable.
2. La cantidad de **problemas de decisión** es NO numerable.

(por el Teorema de Cantor)

Conclusión

Hay problemas de decisión que
NO tienen una solución computacional, esto es, **no tiene algoritmo**.

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