Unidad VI: Funciones y Cardinalidad

Conjuntos no enumerables

Clase 18 - Matemáticas Discretas (IIC1253)

Prof. Miguel Romero

¿Existen conjuntos no enumerables?

Teorema:

$\mathbb{R}$ **no** es enumerable.

- Como $\mathbb{R} \approx (0,1)$ entonces basta probar que $(0,1)$ no es enumerable.
  - No existe biyección $f : \mathbb{N} \to (0,1)$.

- Cada real $r \in (0,1)$ se puede representar con una **secuencia infinita** de dígitos entre $\{0, \ldots, 9\}$.
  - Esto es la representación decimal de r.

$$r = 0.\ d_0\ d_1\ d_2\ d_3\ \cdots$$

Ejemplos:

$$\frac{1}{2} = 0.\ 5\ 0\ 0\ 0\ 0\ \cdots \qquad \frac{1}{3} = 0.\ 3\ 3\ 3\ 3\ 3\ \cdots \qquad \frac{1}{4} = 0.\ 2\ 5\ 0\ 0\ 0\ \cdots$$

$$\frac{\pi}{4} = 0.\ 7\ 8\ 5\ 3\ 9\ \cdots \qquad \frac{e}{4} = 0.\ 6\ 7\ 9\ 5\ 7\ \cdots$$

- Algunos reales en $(0,1)$ tienen dos posibles representaciones decimales. Por ejemplo:

$$\frac{1}{4} = 0.\ 2\ 5\ 0\ 0\ 0\ \cdots\ =\ 0.\ 2\ 4\ 9\ 9\ 9\ \cdots$$

  - En este caso escogemos la representación que termina con 0's.

Por contradicción, supongamos que existe una biyección $f : \mathbb{N} \to (0,1)$.

Luego, existe una enumeración $(r_i)_{i \in \mathbb{N}}$ de $(0,1)$:

- La secuencia no tiene repeticiones.
- **Todos** los reales en $(0,1)$ aparecen en la secuencia.

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}	$\cdots$
$\vdots$					$\vdots$			$\ddots$

$\mathbb{R}$ no es enumerable

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}	$\cdots$
$\vdots$					$\vdots$			$\ddots$

Para cada $i \geq 0$, definamos:

$$e_i = \begin{cases} 4 & d_{ii} \neq 4 \\ 5 & d_{ii} = 4 \end{cases}$$

Defina el número real $s = 0.\ e_0\ e_1\ e_2\ e_3\ \ldots$

¿Puede aparecer s en la lista $r_0, r_1, r_2, \ldots$?

Para cada $i \geq 0$, definamos:

$$e_i = \begin{cases} 4 & d_{ii} \neq 4 \\ 5 & d_{ii} = 4 \end{cases}$$

Defina el número real $s = 0.\ e_0\ e_1\ e_2\ e_3\ \ldots$

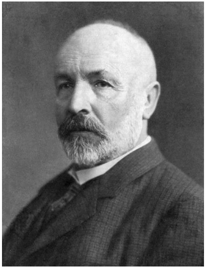
Tenemos que:

- $s \neq r_0$ ya que difieren en el 0-ésimo dígito.
- $s \neq r_1$ ya que difieren en el 1-ésimo dígito.
- $\ldots$

Para cada $i \geq 0$, tenemos $s \neq r_i$ ya que difieren en el i-ésimo dígito.

Encontramos un real $s \in (0, 1)$ que **no** aparece en la enumeración $(r_i)_{i \in \mathbb{N}}$.

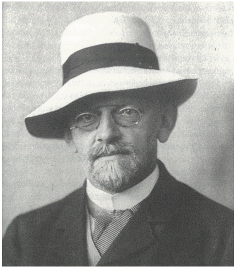
Esto es una contradicción.



Georg Cantor (1845 - 1918)

Teorema (de Cantor):

Para todo conjunto A, se cumple que $A \prec \mathcal{P}(A)$.



David Hilbert (1862 - 1943)

Hilbert (1926):

"*No one shall expel us from the paradise that Cantor has created for us.*"

- Si A es finito, el teorema se cumple. (¿por qué?)
- Asumiremos que A es infinito.
- Demostraremos que **no** existe una biyección de A en $\mathcal{P}(A)$.
- Demostraremos primero el caso de $A = \mathbb{N}$, y luego el caso general.

Por contradicción, suponga que existe una biyección $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

Considere la siguiente tabla:

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

Cada fila i, representa al conjunto $f(i)$.

- La coordenada (i,j) de la tabla es igual a 1 si y sólo si $j \in f(i)$.

Como f es biyección, **cada** conjunto $S \in \mathcal{P}(\mathbb{N})$ es una fila en la tabla.

Considere la diagonal de la tabla:

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

Conjunto diagonal D:

$$1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad \cdots$$

En general:

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

Teorema de Cantor: demostración

Considere la diagonal de la tabla:

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

Conjunto complemento de la diagonal $\overline{D}$:

$$0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad \cdots$$

En general:

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

¿Puede aparecer $\overline{D}$ en alguna fila?

Conjunto complemento de la diagonal $\overline{D}$:

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

El conjunto $\overline{D}$ no aparece en **ninguna** fila $f(i)$ de la tabla !!

Para cada $i \in \mathbb{N}$, se cumple que $\overline{D} \neq f(i)$:

$$\begin{array}{ccc} i \in f(i) & \Longrightarrow & i \notin \overline{D} \\ i \notin f(i) & \Longrightarrow & i \in \overline{D} \end{array}$$

Es decir, tenemos:

$$\big(i \in f(i) \ \text{ y } \ i \notin \overline{D}\big) \ \text{ o } \ \big(i \notin f(i) \ \text{ y } \ i \in \overline{D}\big)$$

Esto contradice que $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ es biyección.

¿Cómo aplicamos este argumento para un A arbitrario?

Por contradicción, suponga que existe una biyección $f : A \to \mathcal{P}(A)$.

- Ya no podemos visualizar f como una tabla, ya que A podría ser no enumerable. (piense por ejemplo en $A = \mathbb{R}$.)

Pero aún podemos definir el conjunto complemento de la diagonal $\overline{D}$:

$$\overline{D} = \{a \in A \mid a \notin f(a)\} \quad \in \quad \mathcal{P}(A)$$

Para cada $a \in A$, se cumple que $\overline{D} \neq f(a)$:

$$\begin{array}{ccc} a \in f(a) & \Longrightarrow & a \notin \overline{D} \\ a \notin f(a) & \Longrightarrow & a \in \overline{D} \end{array}$$

Es decir, tenemos: $\left(a \in f(a) \ \text{ y } \ a \notin \overline{D}\right) \ \text{ o } \ \left(a \notin f(a) \ \text{ y } \ a \in \overline{D}\right)$

Esto nos dice que $\overline{D} \in \mathcal{P}(A)$ **no** tiene preimagen con respecto a f.

- En otras palabras, la función f **no** es sobreyectiva.

Esto contradice que $f : A \to \mathcal{P}(A)$ es biyección.

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \cdots$$

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

¿Dónde se ubica la cardinalidad de los reales $\mathbb{R}$?

Teorema:

$\mathbb{R} \approx \mathcal{P}(\mathbb{N})$.

Como $\mathbb{R} \approx (0,1)$, basta demostrar que $(0,1) \approx \mathcal{P}(\mathbb{N})$.

Veamos que $(0,1) \preceq \mathcal{P}(\mathbb{N})$.

Defina $f : (0,1) \to \mathcal{P}(\mathbb{N})$ como sigue.

Para cada $r \in (0,1)$ cuya representación decimal es

$$r = 0.\ d_0\ d_1\ d_2\ d_3\ \cdots$$

definimos $f(r)$ como

$$f(r) = \{d_i \cdot 10^i \mid i \in \mathbb{N}\}$$

Ejercicio: Demuestre que f es una función inyectiva.

Como $\mathbb{R} \approx (0,1)$, basta demostrar que $(0,1) \approx \mathcal{P}(\mathbb{N})$.

Veamos que $\mathcal{P}(\mathbb{N}) \preceq (0,1)$.

Defina $g : \mathcal{P}(\mathbb{N}) \to (0,1)$ como sigue.

Para cada $A \subseteq \mathbb{N}$, definimos

$$f(A) = 0.\ 1\ d_0\ d_1\ d_2\ d_3\ \cdots$$

donde para cada $i \in \mathbb{N}$:

$$d_i = \begin{cases} 1 & i \in A \\ 0 & i \notin A \end{cases}$$

Ejercicio: Demuestre que g es una función inyectiva.

Una propiedad muy útil:

Proposición:

Si A **no** es enumerable y $B \subseteq A$ es enumerable,
entonces $A \setminus B$ **no** es enumerable.

Demostración:

Por contradicción, suponga que $A \setminus B$ es enumerable.

Recuerde que la unión de dos conjuntos enumerables es enumerable.

Obtenemos que $(A \setminus B) \cup B = A$ es enumerable. Contradicción.

Los **números irracionales** son los números reales que **no** son racionales, es decir, que **no** se pueden escribir como una fracción $\frac{p}{q}$, donde $p, q \in \mathbb{Z}$.

- Denotamos por $\mathbb{I}$ al conjunto de los números irracionales.
- Por definición, se tiene que $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.
- Ejemplos: $\sqrt{2}$, π, e, ...

Como $\mathbb{R}$ no es enumerable, $\mathbb{Q}$ es enumerable, y por la proposición anterior, obtenemos:

Corolario:

$\mathbb{I}$ no es enumerable.

Los **números irracionales** son los números reales que **no** son racionales, es decir, que **no** se pueden escribir como una fracción $\frac{p}{q}$, donde $p, q \in \mathbb{Z}$.

- Denotamos por $\mathbb{I}$ al conjunto de los números irracionales.
- Por definición, se tiene que $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.
- Ejemplos: $\sqrt{2}$, π, e, $\ldots$

Como $\mathbb{R}$ no es enumerable, $\mathbb{Q}$ es enumerable, y por la proposición anterior, obtenemos:

Corolario:

$\mathbb{I}$ no es enumerable.

Un número real r es **algebraico** si existe un polinomio $p(x)$ tal que:

- $p(x)$ no es nulo, es decir, existe $s \in \mathbb{R}$ tal que $p(s) \neq 0$.
- los coeficientes de $p(x)$ son números enteros.
- $p(r) = 0$.

Ejemplos:

- Cada número racional en $\mathbb{Q}$ es algebraico.
- $\sqrt{2}$ es algebraico.

Un número real r es **trascendente** si no es algebraico.

¿Existen números trascendentes? SI!

- $\pi, e, \ldots$

Un argumento simple para probar existencia de números trascendentes:

- El conjunto de los polinomios $p(x)$ con coeficientes enteros es enumerable. (¿por qué?)
- El conjunto de números algebraicos es enumerable. (¿por qué?)
- Como $\mathbb{R}$ **no** es enumerable, el conjunto de números trascendentes **no** es enumerable.
    - Existe **infinitos** números trascendentes.

Consecuencias: problemas no decidibles

Una **propiedad** P sobre $\mathbb{N}$ es un subconjunto de $\mathbb{N}$.

Ejemplos:

- $\text{PAR} = \{n \in \mathbb{N} \mid n \text{ es par}\}$.
- $\text{PRIMO} = \{n \in \mathbb{N} \mid n \text{ es primo}\}$.
- $\text{REP} = \{n \in \mathbb{N} \mid \text{la representación binaria de } n \text{ tiene más 0's que 1's}\}$.

Definición (informal):

Una propiedad P sobre $\mathbb{N}$ es **decidible** si existe un programa en Python tal que:

- Recibe como entrada un natural $n \in \mathbb{N}$.
- Retorna **SI**, en caso de que $n \in P$. Retorna **NO**, en el caso contrario.

Ejemplos:

- $\text{PAR}, \text{PRIMO}, \text{REP}$ son decidibles.

¿Existen propiedades no decidibles?

- El conjunto de propiedades decidibles sobre $\mathbb{N}$ es enumerable. (¿por qué?)
- El conjunto de propiedades sobre $\mathbb{N}$ no es enumerable.
  - Este conjunto es exactamente $\mathcal{P}(\mathbb{N})$.
- Concluimos que existen propiedades no decidibles.
  - De hecho, una cantidad infinita no enumerable.

Existen **muchos** problemas que no se pueden resolver con un algoritmo!

Hay una cantidad **infinita** de **infinitos**.

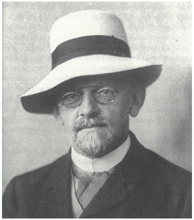
$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \cdots$$

¿Existe algún infinito entre $\mathbb{N}$ y $\mathcal{P}(\mathbb{N})$?

- ¿Existe un conjunto A tal que $\mathbb{N} \prec A \prec \mathcal{P}(\mathbb{N})$?

Hipótesis del continuo:

No existe ningún conjunto A tal que $\mathbb{N} \prec A \prec \mathcal{P}(\mathbb{N})$.

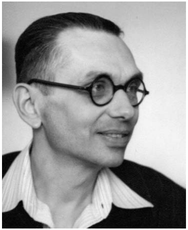


David Hilbert
(1862 - 1943)

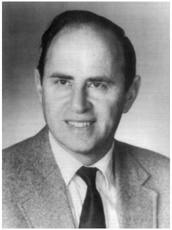
Uno de los 23 problemas de Hilbert propuestos en 1900.

Hipótesis del continuo:

No existe ningún conjunto A tal que $\mathbb{N} < A < \mathcal{P}(\mathbb{N})$.



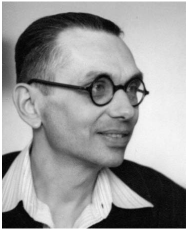
Kurt Gödel
(1906 - 1978)



Paul Cohen
(1934 - 2007)

Con los axiomas de teoría de conjuntos (Zermelo-Fraenkel):

Gödel (1940): **NO** se puede demostrar que la hipótesis es **falsa**.
Cohen (1963): **NO** se puede demostrar que la hipótesis es **verdadera**.



Kurt Gödel
(1906 - 1978)

Lo anterior es un caso particular de un fenómeno más general, demostrado por Gödel en 1930:

Teorema de incompletitud de Gödel (informal):

Para cada conjunto de axiomas en lógica de predicados (suficientemente poderoso), existen oraciones φ tal que φ y $\neg\varphi$ **no** son consecuencia de los axiomas.