Teorema CSB y aplicaciones

Clase 16

IIC 1253

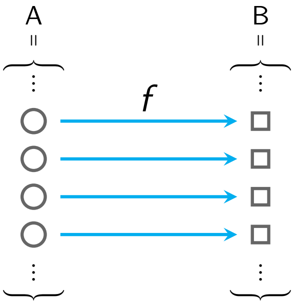
Prof. Cristian Riveros

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

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

Proposición

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

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

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**.

Recordatorio: Conjuntos numerables y no-numerables

Sabemos que...

- Los conjuntos $\mathbb{P}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{N} \times \mathbb{N}$ son numerables.
- Los conjuntos $\mathbb{R}$ y $2^{\mathbb{N}}$ son no-numerables.

Teorema de Cantor

Para todo conjunto no vacío A,
NO existe una **biyección** entre A y el conjunto potencia 2^A.

Outline

Funciones y cardinalidad

Sea A y B dos conjuntos no vacíos.

Definición

Decimos que B es **al menos tan numeroso** como A:

$$|A| \leq |B|$$

si existe una función **inyectiva** $f : A \to B$.

¿qué tipo de relación es $|\cdot| \leq |\cdot|$?

Teorema de Cantor–Schröder–Bernstein

Sea A y B dos conjuntos no vacíos.

Teorema (Cantor–Schröder–Bernstein)

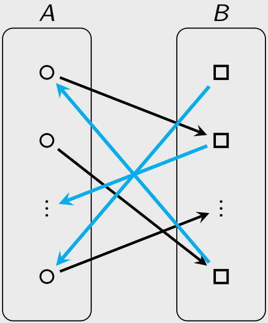
Si existen funciones **inyectivas** $f : A \to B$ y $g : B \to A$, entonces existe una función **biyectiva** $h : A \to B$.

En otras palabras, $|A| = |B|$ si, y solo si, $|A| \leq |B|$ y $|B| \leq |A|$

Teorema de Cantor–Schröder–Bernstein

Demostración

Sea A, B conjuntos no vacíos y $f : A \to B$, $g : B \to A$ funciones **inyectivas**. *Sin perdida de generalidad*, suponga que A y B son **disjuntos** ($A \cap B = \varnothing$).

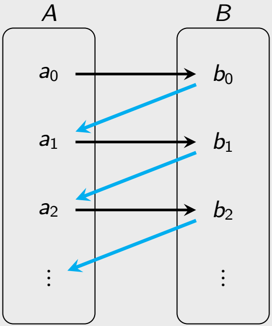


¿cómo hacemos una biyección desde A hasta B?

Teorema de Cantor–Schröder–Bernstein

Demostración

Sea A, B conjuntos no vacíos y $f : A \to B$, $g : B \to A$ funciones **inyectivas**.
Sin perdida de generalidad, suponga que A y B son **disjuntos** ($A \cap B = \varnothing$).



Teorema de Cantor–Schröder–Bernstein

Demostración

Sea A, B conjuntos no vacíos y $f : A \to B$, $g : B \to A$ funciones **inyectivas**.
Sin perdida de generalidad, suponga que A y B son **disjuntos** ($A \cap B = \varnothing$).

Caso 1:
$$\begin{tikzcd} a_0 \arrow[r, "f"] & b_0 \arrow[r, "g"] & a_1 \arrow[r, "f"] & \cdots \arrow[r, "g"] & a_k \arrow[r, "f"] & b_k \arrow[lllll, bend left, "g"] \end{tikzcd}$$

Caso 2: $\cdots \xrightarrow{g} a_0 \xrightarrow{f} b_0 \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} \cdots$

Caso 3: $a_0 \xrightarrow{f} b_0 \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} \cdots$

Caso 4: $b_0 \xrightarrow{g} a_0 \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} \cdots$

Teorema de Cantor–Schröder–Bernstein

Demostración

Para $a \in A$, sea $C_a \subseteq A \cup B$ "todos los elementos **alcanzables** desde a":

$$
\begin{aligned}
C_a = \Big\{ x \in A \cup B \;\Big|\; \exists i \geq 0.\quad & x = (f \circ g)^i(a) && \vee \\
& x = (f \circ g)^i \circ f(a) && \vee \\
& x = (g^{-1} \circ f^{-1})^i(a) && \vee \\
& x = (g^{-1} \circ f^{-1})^i \circ g^{-1}(a) && \Big\}
\end{aligned}
$$

donde $(f \circ g)^i$ es la función $f \circ g$ aplicada i-veces (con $(f \circ g)^0(a) = a$).

Algunos hechos:

- $C_a = C_{a'}$ o $C_a \cap C_{a'} = \varnothing$ para todo $a, a' \in A$. (¿por qué?)
- el conjunto $\{C_a \mid a \in A\}$ forma una partición de $A \cup B$. (¿por qué?)
- $\{A \cap C_a, B \cap C_a\}$ es una partición de C_a. (¿por qué?)

Teorema de Cantor–Schröder–Bernstein

Demostración

PD: Para todo $a \in A$, existe una **biyección** $f_a : (A \cap C_a) \to (B \cap C_a)$.

Caso 1:

$$\begin{tikzcd} a_0 \arrow[r, "f"] & b_0 \arrow[r, "g"] & a_1 \arrow[r, "f"] & \cdots \arrow[r, "g"] & a_k \arrow[r, "f"] & b_k \arrow[lllll, bend left, "g"] \end{tikzcd}$$

$$f_a(a_i) = b_i \quad \text{para todo } a_i \in A \cap C_a$$

Caso 2:

$$\begin{tikzcd} \cdots \arrow[r, "g"] & a_0 \arrow[r, "f"] & b_0 \arrow[r, "g"] & a_1 \arrow[r, "f"] & b_1 \arrow[r, "g"] & \cdots \end{tikzcd}$$

$$f_a(a_i) = b_i \quad \text{para todo } a_i \in A \cap C_a$$

Teorema de Cantor–Schröder–Bernstein

Demostración

PD: Para todo $a \in A$, existe una **biyección** $f_a : (A \cap C_a) \to (B \cap C_a)$.

Caso 3: $\cdot a_0 \xrightarrow{f} b_0 \xrightarrow{g} a_1 \xrightarrow{f} b_1 \xrightarrow{g} \cdots$

$$f_a(a_i) = b_i \quad \text{para todo } a_i \in A \cap C_a$$

Caso 4: $b_0 \xrightarrow{g} a_0 \xrightarrow{f} b_1 \xrightarrow{g} a_1 \xrightarrow{f} \cdots$

$$f_a(a_i) = g^{-1}(a_i) = b_i \quad \text{para todo } a_i \in A \cap C_a$$

Teorema de Cantor–Schröder–Bernstein

Demostración

Por lo tanto, como:

- $\{C_a \mid a \in A\}$ forma una partición de $A \cup B$ y
- para todo $a \in A$, existe una **biyección** $f_a : (A \cap C_a) \to (B \cap C_a)$

entonces:

$$(h : A \to B) \;=\; \bigcup_{a \in A} f_a$$

es una biyección de A en B. $\square$

Outline

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 $f : \mathbb{N} \to \mathbb{N}$ 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:

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

Ejemplo

Sea $\textsc{Primo} : \mathbb{N} \to \{0,1\}$ 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 $P : \mathcal{I} \rightarrow \{0, 1\}$ 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:

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

Solución a los problemas de decisión

Ejemplo

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

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

Una **solución** para el problema de decisión $\textsc{Primo}$ 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 con 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: $P : \{0,1\}^* \rightarrow \{0,1\}$.

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

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

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

$$\mathcal{P} = \left\{ L_P \subseteq \{0,1\}^* \mid P : \{0,1\}^* \rightarrow \{0,1\} \right\}$$

¿a qué equivale $\mathcal{P}$?

¿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

Números reales y nombres

Podemos asociar nombres a los reales:

$$
\begin{aligned}
1 &= \text{uno} \\
2 &= \text{dos} \\
&\vdots \\
1234 &= \text{mil docientos treinta y cuatro} \\
&\vdots \\
3.1415\ldots &= \pi \\
2.7182\ldots &= e \\
&\vdots
\end{aligned}
$$

¿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): π

¿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.