Matemáticas Discretas

Funciones y Cardinalidad

Nicolás Alvarado
nfalvarado@mat.uc.cl

Bernardo Barías
bjbarias@uc.cl

Sebastián Bugedo
bugedo@uc.cl

Gabriel Diéguez
gsdieguez@ing.puc.cl

Departamento de Ciencia de la Computación
Escuela de Ingeniería
Pontificia Universidad Católica de Chile

11 de octubre de 2023

Objetivos

1. Formular enunciados formales en notación matemática usando lógica, conjuntos, relaciones, funciones, cardinalidad, y otras herramientas, desarrollando definiciones y teoremas al respecto, así como demostrar o refutar estos enunciados, usando variadas técnicas.

Contenidos

1. Introducción
2. Funciones
3. Cardinalidad
   - Conjuntos finitos
   - Conjuntos infinitos

¿Funciones... de nuevo?

Introducción

¿Por qué queremos funciones en Ciencia de la Computación?

- Calcular $\longrightarrow$ métodos
- Modelar $\longrightarrow$ simulación
- Estructuras de datos y algoritmos $\longrightarrow$ hashing, map reduce, ordenamiento
- Encriptar $\longrightarrow$ MD5, SHA-1
- Contar

Introducción

¿Por qué queremos funciones en Ciencia de la Computación?

- Calcular $\longrightarrow$ métodos
- Modelar $\longrightarrow$ simulación
- Estructuras de datos y algoritmos $\longrightarrow$ hashing, map reduce, ordenamiento
- Encriptar $\longrightarrow$ MD5, SHA-1
- **¡Contar o indexar!**

Formalizaremos el concepto y lo aplicaremos.

Definición

Sea f una relación binaria de A en B; es decir, $f \subseteq A \times B$.
Diremos que f es una **función** de A en B si dado cualquier elemento $a \in A$, si existe un elemento en $b \in B$ tal que afb, este es único:

$$afb \wedge afc \Rightarrow b = c$$

Si afb, escribimos $b = f(a)$.

- b es la *imagen* de a.
- a es la *preimagen* de b.

Notación: $f : A \to B$

Funciones

Una función $f : A \to B$ se dice **total** si todo elemento en A tiene imagen.

- Es decir, si para todo $a \in A$ existe $b \in B$ tal que $b = f(a)$.
- Una función que no sea total se dice **parcial**.
- De ahora en adelante, toda función será total a menos que se diga lo contrario.

Funciones

Ejemplos

Las siguientes relaciones son todas funciones de $\mathbb{N}_4$ en $\mathbb{N}_4$:

$$f_1 = \{(0,0),(1,1),(2,2),(3,3)\}$$
$$f_2 = \{(0,1),(1,1),(2,1),(3,1)\}$$
$$f_3 = \{(0,3),(1,2),(2,1),(3,0)\}$$

¿Cuántas funciones $f : \mathbb{N}_4 \to \mathbb{N}_4$ podemos construir?

Respuesta: $4^4 = 256$.

Funciones

También podemos definir funciones mediante expresiones que nos den el valor de $f(x)$.

Ejemplos

Las siguientes son definiciones para funciones de $\mathbb{R}$ en $\mathbb{R}$:

$$\forall x \in \mathbb{R}, f_1(x) = x^2 + 1$$
$$\forall x \in \mathbb{R}, f_2(x) = \lfloor x + \sqrt{x} \rfloor$$
$$\forall x \in \mathbb{R}, f_3(x) = 0$$
$$\forall x \in \mathbb{R}, f_4(x) = \begin{cases} 1 & x \geq 0 \\ -1 & x < 0 \end{cases}$$

Ejemplos

Dado un conjunto A cualquiera, las siguientes son definiciones para funciones de A en $\mathcal{P}(A)$:

$$\forall a \in A, f_1(a) = \{a\}$$
$$\forall a \in A, f_2(a) = A \setminus \{a\}$$
$$\forall a \in A, f_3(a) = \varnothing$$

Funciones

Definición

Diremos que una función $f : A \to B$ es:

1. **Inyectiva** (o 1-1) si para cada par de elementos $x, y \in A$ se tiene que $f(x) = f(y) \Rightarrow x = y$. Es decir, no existen dos elementos distintos en A con la misma imagen.

2. **Sobreyectiva** (o sobre) si cada elemento $b \in B$ tiene preimagen. Es decir, para todo $b \in B$ existe $a \in A$ tal que $b = f(a)$.

3. **Biyectiva** si es inyectiva y sobreyectiva a la vez.

Ejercicio

Determine qué propiedades cumplen o no cumplen las siguientes funciones:

1. $f : A \to \mathcal{P}(A)$, $\forall a \in A, f(a) = \{a\}$
2. $f : A \to \mathcal{P}(A)$, $\forall a \in A, f(a) = \varnothing$
3. $f : \mathbb{N} \to \mathbb{N}_4$, $\forall n \in \mathbb{N}, f(n) = n \text{ mod } 4$
4. $f : \mathbb{N}_4 \to \mathbb{N}_4$, $\forall n \in \mathbb{N}_4, f(n) = (n + 2) \text{ mod } 4$

1. es inyectiva y no sobreyectiva.
2. ni inyectiva ni sobreyectiva.
3. es sobreyectiva y no inyectiva.
4. es inyectiva, sobreyectiva y biyectiva.

Paréntesis: relaciones y funciones como conjuntos

- Recordemos que las relaciones (y por lo tanto las funciones) son conjuntos (de pares ordenados).
- Esto significa que podemos usar las operaciones de conjuntos.
    - Unión
    - Intersección
    - Complemento
    - ...
- Existen también operaciones exclusivas para relaciones (y funciones).

Definición

Dada una relación R de A en B, la **relación inversa** de R es una relación de B en A definida como

$$R^{-1} = \{(b, a) \in B \times A \mid aRb\}$$

Definición

Dada una función f de A en B, diremos que f es **invertible** si su relación inversa f^{-1} es una función de B en A.

Paréntesis: relaciones y funciones como conjuntos

Definición

Dadas relaciones R de A en B y S de B en C, la **composición** de R y S es una relación de A en C definida como

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B \text{ tal que } aRb \wedge bSc\}$$

Proposición

Dadas funciones f de A en B y g de B en C, la **composición** $g \circ f$ es una función de A en C.

Ejercicio

Demuestre la proposición.

Paréntesis: relaciones y funciones como conjuntos

Proposición

Dadas funciones f de A en B y g de B en C, la **composición** $g \circ f$ es una función de A en C.

1. $g \circ f$ es función: supongamos que

$$(g \circ f)(x) = z_1 \text{ y } (g \circ f)(x) = z_2, \text{ con } x \in A, z_1, z_2 \in C.$$

Por definición de composición:

$$g(f(x)) = z_1 \text{ y } g(f(x)) = z_2, \text{ con } x \in A, z_1, z_2 \in C.$$

Como f es función, existe un único $y \in B$ tal que $y = f(x)$, y luego

$$g(y) = z_1 \text{ y } g(y) = z_2, \text{ con } x \in A, y \in B, z_1, z_2 \in C$$

y como g también es función, $z_1 = z_2$. Concluimos que $g \circ f$ es función.

Paréntesis: relaciones y funciones como conjuntos

Proposición

Dadas funciones f de A en B y g de B en C, la **composición** $g \circ f$ es una función de A en C.

2. $g \circ f$ es total: sea $x \in A$.
   Como f es función total, $\exists y \in B$ tal que $(x, y) \in f$.
   Similarmente, como g es función total, $\exists z \in C$ tal que $(y, z) \in g$.
   Luego, $(x, z) \in g \circ f$.
   Como para cada $x \in A$ existe $z \in C$ tal que $z = (g \circ f)(x)$, $g \circ f$ es total.

Teorema

Si $f : A \to B$ es biyectiva, entonces la relación inversa f^{-1} es una función biyectiva de B en A.

Ejercicio

Demuestre el teorema.

Corolario

Si f es biyectiva, entonces es invertible.

Funciones

Teorema

Si $f : A \to B$ es biyectiva, entonces la relación inversa f^{-1} es una función biyectiva de B en A.

1. Función: supongamos que $yf^{-1}x_1$ e $yf^{-1}x_2$, con $y \in B$ y $x_1, x_2 \in A$. Por definición de relación inversa, esto significa que $x_1 f y$ y $x_2 f y$. Como f es inyectiva, $x_1 = x_2$, y por lo tanto f^{-1} es función.
2. Total: como f es sobre, para todo $y \in B$ existe $x \in A$ tal que $y = f(x)$. Luego, para todo $y \in B$ existe $x \in A$ tal que $x = f^{-1}(y)$, y por lo tanto f^{-1} es total.

Funciones

Teorema

Si $f : A \to B$ es biyectiva, entonces la relación inversa f^{-1} es una función biyectiva de B en A.

3. Inyectiva: supongamos que $f^{-1}(y_1) = f^{-1}(y_2) = x$, con $y_1, y_2 \in B$ y $x \in A$. Por definición de relación inversa, esto significa que $f(x) = y_1$ y $f(x) = y_2$. Como f es función, $y_1 = y_2$, y por lo tanto f^{-1} es inyectiva.
4. Sobre: como f es total, para todo $x \in A$ existe $y \in B$ tal que $y = f(x)$. Luego, para todo $x \in A$ existe $y \in B$ tal que $x = f^{-1}(y)$, y por lo tanto f^{-1} es sobre.

Teorema

Dadas dos funciones $f : A \to B$ y $g : B \to C$:

1. Si f y g son inyectivas, entonces $g \circ f$ también lo es.
2. Si f y g son sobreyectivas, entonces $g \circ f$ también lo es.

Ejercicio

Demuestre el teorema.

Corolario

Si f y g son biyectivas, entonces $g \circ f$ también lo es.

Teorema

Dadas dos funciones $f : A \to B$ y $g : B \to C$:

1. Si f y g son inyectivas, entonces $g \circ f$ también lo es.
2. Si f y g son sobreyectivas, entonces $g \circ f$ también lo es.

1. Supongamos que $(g \circ f)(x_1) = (g \circ f)(x_2)$, con $x_1, x_2 \in A$. Por definición de composición, $g(f(x_1)) = g(f(x_2))$. Como g es inyectiva, se tiene que $f(x_1) = f(x_2)$, y como f también es inyectiva, $x_1 = x_2$. Por lo tanto, $g \circ f$ es inyectiva.
2. Sea $z \in C$. Como g es sobre, sabemos que existe $y \in B$ tal que $z = g(y)$. Similarmente, como f es sobre, sabemos que existe $x \in A$ tal que $y = f(x)$. Entonces, tenemos que $z = g(y) = g(f(x)) = (g \circ f)(x)$, y por lo tanto para cada $z \in C$ existe $x \in A$ tal que $z = (g \circ f)(x)$. Concluimos que $g \circ f$ es sobre.

Una aplicación muy importante de las funciones es que nos permiten razonar sobre el tamaño de los conjuntos. Una propiedad interesante sobre los conjuntos finitos es la siguiente:

Principio del palomar

Se tienen m palomas y n palomares, con $m > n$. Entonces, si se reparten las m palomas en los n palomares, necesariamente existirá un palomar con más de una paloma.

Principio del palomar (matemático)

Si se tiene una función $f : \mathbb{N}_m \to \mathbb{N}_n$ con $m > n$, la función f no puede ser inyectiva. Es decir, necesariamente existirán $x, y \in \mathbb{N}_m$ tales que $x \neq y$, pero $f(x) = f(y)$.

Principio del palomar (para sobreyectividad)

Si se tiene una función $f : \mathbb{N}_m \to \mathbb{N}_n$ con $m < n$, la función f no puede ser sobreyectiva.

Corolario

La única forma en que una función $f : \mathbb{N}_m \to \mathbb{N}_n$ sea biyectiva es que $m = n$.

Ejemplo

Si en una sala hay 8 personas, entonces este año necesariamente dos de ellas celebrarán su cumpleaños el mismo día de la semana.

Las 8 personas las podemos modelar como el conjunto $P = \{0, \ldots, 7\}$ y los días de la semana como el conjunto $S = 0, \ldots, 6$. El día de la semana que se celebra el cumpleaños de cada una resulta ser una función de P en S, por el principio de los cajones, esta función no puede ser inyectiva, luego al menos dos personas distintas celebrarán su cumpleaños el mismo día de la semana.

Queremos resolver el problema de determinar el tamaño de un conjunto.

- Es decir, la cantidad de elementos que contiene.
- ¿Cómo lo hacemos?

Ejemplo

¿Cuántos elementos tiene el conjunto $A = \{a, b, c, d, e, f\}$?

Simplemente contamos... tiene 6.

Cardinalidad

Ejemplo

¿Cuántos elementos tiene el conjunto $A = \{a, b, c, d, e, f\}$?

$$\begin{aligned} a &\to 1 \\ b &\to 2 \\ c &\to 3 \\ d &\to 4 \\ e &\to 5 \\ f &\to 6 \end{aligned}$$

Estamos estableciendo una *correspondencia* entre los elementos de A y los números naturales. . .

Definición

Sean A y B dos conjuntos cualesquiera. Diremos que A es **equinumeroso** con B (o que A tiene el mismo tamaño que B) si existe una función biyectiva $f : A \to B$. Lo denotamos como

$$A \approx B$$

A y B tienen el mismo tamaño si los elementos de A se pueden poner en correspondencia con los de B.

Notemos que $\approx$ es una relación sobre conjuntos.

Teorema

La relación $\approx$ es una relación de equivalencia.

Ejercicio

Demuestre el teorema.

Teorema

La relación $\approx$ es una relación de equivalencia.

Demostración:

- Refleja: Para todo conjunto A existe $f : A \to A$ tal que $f(a) = a$, $\forall a \in A$ es una función biyectiva, por lo que $A \approx A$.
- Simétrica: Sea A, B conjuntos tal que $A \approx B \Rightarrow$ existe $f : A \to B$ biyectiva, entonces la función $f^{-1} : B \to A$ es biyectiva y por lo tanto $B \approx A$.
- Transitiva: Sea A, B, C conjuntos tal que $A \approx B$ y $B \approx C \Rightarrow$ existen $f : A \to B$ y $g : B \to C$ biyectivas, luego $f \circ g : A \to C$ es una función biyectiva, por lo que $A \approx C$.

Cardinalidad

Podemos usar conceptos de las relaciones de equivalencia para hablar sobre el tamaño de los conjuntos.

- ¿Por ejemplo?
- Podemos tomar las clases de equivalencia inducidas por $\approx$.

Definición

La **cardinalidad** de un conjunto A es su clase de equivalencia bajo $\approx$:

$$|A| = [A]_{\approx}$$

Cardinalidad

Ejemplo

¿Cuál es la cardinalidad del conjunto $A = \{a, b, c, d, e, f\}$?

Es fácil notar que $A \approx \{0, 1, 2, 3, 4, 5\}$.

- Entonces, $|A| = [A]_{\approx} = [\{0, 1, 2, 3, 4, 5\}]_{\approx}$.
- Pero nosotros le pusimos un nombre al último conjunto...

$$|A| = [6]_{\approx}$$

Formalizaremos esto y simplificaremos la notación.

Cardinalidad de conjuntos finitos

Definición

Diremos que A es un conjunto **finito** si $A \approx n$, para algún $n \in \mathbb{N}$. Es decir, si existe una función biyectiva $f : A \to n = \{0, \ldots, n-1\}$.

En tal caso, se tiene que $|A| = [n]_{\approx}$.

- Por simplicidad, diremos que $|A| = n$.
- También podremos decir que A tiene n elementos.

Cardinalidad de conjuntos finitos

Ejemplo

¿Cuál es la cardinalidad del conjunto $A = \{a, b, c, d, e, f\}$?

- $|A| = 6$
- A tiene 6 elementos.

Cardinalidad de conjuntos finitos

Lema

Sean A y B dos conjuntos finitos tales que $A \cap B = \varnothing$. Entonces, $|A \cup B| = |A| + |B|$.

Ejercicio

Demuestre el lema.

Cardinalidad

Lema

Sean A y B dos conjuntos finitos tales que $A \cap B = \varnothing$. Entonces, $|A \cup B| = |A| + |B|$.

Demostración:

Supongamos que $|A| = n$ y que $|B| = m$. Sabemos entonces que $A \approx \{0, \ldots, n-1\}$ y que $B \approx \{0, \ldots, m-1\}$, luego existen funciones biyectivas $f : A \to \{0, \ldots, n-1\}$ y $g : B \to \{0, \ldots, m-1\}$. Sea $h : A \cup B \to \{0, \ldots, n, n+1, \ldots, n+m-1\}$ tal que

$$h(x) = \begin{cases} f(x) & x \in A \\ n + g(x) & x \in B \end{cases}$$

Primero se debe notar que h está bien definida como función ya que no existe un x que pertenezca simultáneamente a A y B.

Cardinalidad

Continuación:

- Sobreyectividad: Sea $k \in \{0, \ldots, n, n+1, \ldots, n+m-1\}$, lo demostraremos por casos. Si $k < n$ entonces dado que f es sobreyectiva en $\{0, \ldots, n+1\}$ sabemos que existe un $x \in A$ tal que $k = f(x) = h(x)$. Si $n \leq k < n+m$ entonces dado que g es sobreyectiva en $\{0, \ldots, m-1\}$ sabemos que existe en $x \in B$ tal que $g(x) = k - n$ y por lo tanto $k = n + g(x) = h(x)$, finalmente h es sobreyectiva en $k \in \{0, \ldots, n, n+1, \ldots, n+m-1\}$.
- Inyectividad: Otra vez por casos, si $h(x) = h(y) < n$ entonces necesariamente $h(x) = f(x) = h(y) = f(y)$ de donde se concluye que $f(x) = f(y)$ y dado que f es inyectiva obtenemos que $x = y$. Si en cambio $n \leq h(x) = h(y) < n+m$, sabemos que $h(x) = n + g(x) = h(y) = n + g(y)$ de donde se concluye que $g(x) = g(y)$ y dado que g es inyectiva obtenemos que $x = y$, finalmente h es inyectiva.

Cardinalidad de conjuntos finitos

Teorema

Sea A un conjunto finito. Entonces, se cumple que $|\mathcal{P}(A)| = 2^{|A|}$.

Esto implica que si A es un conjunto finito, entonces su cardinalidad es **estrictamente menor** que la de su conjunto potencia.

Ejercicio

Demuestre el teorema.

Cardinalidad de conjuntos finitos

Teorema

Sea A un conjunto finito. Entonces, se cumple que $|\mathcal{P}(A)| = 2^{|A|}$.

Demostración:

Por inducción en la cardinalidad de A.

BI: Si $|A| = 0$ entonces $A = \varnothing \Rightarrow \mathcal{P}(A) = \{\varnothing\} \approx \{0\}$ por lo tanto $|\mathcal{P}(A)| = 1 = 2^0 = 2^{|A|}$.

HI: Supongamos que para cualquier conjunto A tal que $|A| = n$ se cumple que $|\mathcal{P}(A)| = 2^n = 2^{|A|}$

TI: Sea A un conjunto tal que $|A| = n + 1$, y sea $B = A - \{a\}$, con a un elemento arbitrario de A. El conjunto B cumple con $|B| = n$, por lo que $|\mathcal{P}(B)| = 2^n$. ¿Cómo podemos a partir de $\mathcal{P}(B)$ formar $\mathcal{P}(A)$? Si nos damos cuenta en $\mathcal{P}(B)$ están todos los subconjuntos de B, es decir, todos los subconjuntos de A que no contienen al elemento a.

Continuación:
Si llamamos $\mathcal{S}$ al conjunto

$$\mathcal{S} = \{X \mid X \subseteq A \wedge a \in X\}$$

Es decir $\mathcal{S}$ está formado por todos los subconjuntos de A que contienen a a, no es difícil notar que $\mathcal{S} \cap \mathcal{P}(B) = \varnothing$ y que $\mathcal{P}(A) = \mathcal{S} \cup \mathcal{P}(B)$. Ahora, la siguiente función $f : \mathcal{P}(B) \to \mathcal{S}$ tal que $f(X) = X \cup \{a\}$, es una función biyectiva de $\mathcal{P}(B)$ en $\mathcal{S}$, por lo que concluímos que $\mathcal{P}(B) \approx \mathcal{S}$ y por lo tanto $|\mathcal{P}(B)| = |\mathcal{S}|$. Luego, dado que $\mathcal{S} \cap \mathcal{P}(B) = \varnothing$ y que $\mathcal{P}(A) = \mathcal{P}(B) \cup \mathcal{A}$ y usando el lema anterior concluímos que $|\mathcal{P}(A)| = |\mathcal{P}(B) \cup A| = |\mathcal{P}(B)| + |A| = |\mathcal{P}(B)| + |\mathcal{P}(B)| = 2^n + 2^n = 2^{n+1} = 2^{|A|}$.

Cardinalidad de conjuntos infinitos

Nuestro problema es un poco fácil cuando el conjunto es finito.

- ¿Qué pasa cuando es infinito?
- Ya no podemos contar...
- ...pero sí podemos establecer una correspondencia como la que mostramos.
- ¿Cómo? ¡Con funciones!

Cardinalidad de conjuntos infinitos

Ejemplo

Sea $\mathbb{P} = \{2k \mid k \in \mathbb{N}\}$ el conjunto de los números naturales pares. ¿Cuál conjunto es más grande, $\mathbb{N}$ o $\mathbb{P}$?

Podemos tomar $f : \mathbb{N} \to \mathbb{P}$ dada por $f(n) = 2n$, la cual es claramente biyectiva, y entonces $|\mathbb{P}| = |\mathbb{N}|$.

Definición

Un conjunto A se dice **enumerable** si $|A| = |\mathbb{N}|$.

Ejercicio

Demuestre que $\mathbb{Z}$ es enumerable.

Podemos tomar $f : \mathbb{N} \to \mathbb{Z}$ dada por

$$f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ -(\frac{n+1}{2}) & \text{si } n \text{ es impar} \end{cases}$$

la cual es claramente biyectiva (se deja como ejercicio), y entonces $|\mathbb{Z}| = |\mathbb{N}|$.

Cardinalidad de conjuntos infinitos

Un teorema útil (sobre todo para el caso infinito):

Teorema (Schröder-Bernstein)

$A \approx B$ si y sólo si existen funciones inyectivas $f : A \to B$ y $g : B \to A$.

Ejercicio

Demuestre que $A = \{2^i \cdot 3^j \mid i, j \in \mathbb{N}\}$ es enumerable.

Tomamos las siguientes funciones:

- $f : A \to \mathbb{N}$ dada por $f(x) = x$, la cual es claramente inyectiva.
- $g : \mathbb{N} \to A$ dada por $g(x) = 2^x \cdot 3^x = 6^x$.
  $g(x) = g(x) \Rightarrow 6^x = 6^y \Rightarrow x = y$, y por lo tanto es inyectiva.

Por teorema de Schröder-Bernstein, concluimos que $|A| = |\mathbb{N}|$.

Cardinalidad de conjuntos infinitos

La siguiente definición nos permite caracterizar a los conjuntos enumerables de una manera muy práctica.

Definición

Un conjunto A es enumerable si y sólo si todos sus elementos se pueden poner en una lista infinita; es decir, si existe una sucesión infinita

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

tal que *todos* los elementos de A aparecen en la sucesión *una única vez* cada uno.

¿Cómo se justifica esta definición?

- ¿Cuál es la biyección?

La biyección está dada por los índices de cada elemento del conjunto en la lista: $f : A \to \mathbb{N}$ con $f(a_i) = i$.

Cardinalidad de conjuntos infinitos

Ejercicio

Demuestre que:

- $\mathbb{N} \times \mathbb{N}$ es enumerable.
- $\mathbb{N}^n$ es enumerable.
- $\mathbb{Q}$ es enumerable.

¿Por qué esta definición es *práctica*?

- Piense en un computador.

Ejercicio

¿Cuál es la cantidad de programas válidamente escritos en { INSERTE SU LENGUAJE FAVORITO AQUÍ }?

Ejercicio

Demuestre que:

- $\mathbb{N} \times \mathbb{N}$ es enumerable.
- $\mathbb{Q}$ es enumerable.

Solución: Apuntes Jorge Pérez, Sección 1.6.2, Teorema 1.6.5, página 52.

Ejercicio

Demuestre que $\mathbb{N}^n$ es enumerable.

Por inducción sobre n:

BI: La base es $n = 2$, demostrado anteriormente.

HI: Supongamos que $\mathbb{N}^n$ es enumerable, con $n \geq 2$.

TI: PD: $\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N}$ es enumerable.
Como por HI sabemos que $\mathbb{N}^n$ es enumerable, existe una lista $(a_0, a_1, \ldots, a_i, \ldots)$ que contiene a todas las tuplas de $\mathbb{N}^n$ exactamente una vez cada una. Luego, de manera similar a la demostración de $\mathbb{N} \times \mathbb{N}$, ponemos las tuplas de $\mathbb{N}^n \times \mathbb{N}$ en una matriz, la cual recorremos por las diagonales, que son los pares en que el índice de la primera componente en la lista de $\mathbb{N}^n$ más la segunda componente suman k.

Cardinalidad de conjuntos infinitos

Ejercicio

Demuestre que $\mathbb{N}^n$ es enumerable.

TI: De esta manera, la lista sería algo como:

$$((a_0, 0), (a_0, 1), (a_1, 0), (a_0, 2), (a_1, 1), (a_2, 0), \ldots)$$

Concluimos entonces que $\mathbb{N}^n$ es enumerable para todo $n \in \mathbb{N}$.

Ejercicio

¿Cuál es la cantidad de programas válidamente escritos en { INSERTE SU LENGUAJE FAVORITO AQUÍ }?

Solución: Apuntes Jorge Pérez, Sección 1.6.2, páginas 52 y 53.

¿Existen conjuntos infinitos **no** enumerables?

Teorema (Cantor)

El intervalo real $(0,1) \subseteq \mathbb{R}$ es infinito pero no enumerable.

Ejercicio

Demuestre el teorema.

Cardinalidad de conjuntos infinitos

Teorema (Cantor)

El intervalo real $(0,1) \subseteq \mathbb{R}$ es infinito pero no enumerable.

Por contradicción, supongamos que $(0,1)$ es enumerable.

Entonces existe una lista infinita de los reales en $(0,1)$:

$$r_0, r_1, r_2, r_3, \ldots$$

donde cada real en $(0,1)$ aparece exactamente una vez.

Notemos que cada r_i es un número decimal de la forma

$$r_i = 0, d_{i0}d_{i1}d_{i2}d_{i3}\ldots, \text{ con } d_{ij} \in \{0,\ldots,9\}$$

Cardinalidad de conjuntos infinitos

Reales	Representación decimal						
r_0	$0,$	d_{00}	d_{01}	d_{02}	d_{03}	d_{04}	$\cdots$
r_1	$0,$	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	$\cdots$
r_2	$0,$	d_{20}	d_{21}	d_{22}	d_{23}	d_{24}	$\cdots$
r_3	$0,$	d_{30}	d_{31}	d_{32}	d_{33}	d_{34}	$\cdots$
r_4	$0,$	d_{40}	d_{41}	d_{42}	d_{43}	d_{44}	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Cardinalidad de conjuntos infinitos

Reales	Representación decimal						
r_0	$0,$	$\boxed{d_{00}}$	d_{01}	d_{02}	d_{03}	d_{04}	$\cdots$
r_1	$0,$	d_{10}	$\boxed{d_{11}}$	d_{12}	d_{13}	d_{14}	$\cdots$
r_2	$0,$	d_{20}	d_{21}	$\boxed{d_{22}}$	d_{23}	d_{24}	$\cdots$
r_3	$0,$	d_{30}	d_{31}	d_{32}	$\boxed{d_{33}}$	d_{34}	$\cdots$
r_4	$0,$	d_{40}	d_{41}	d_{42}	d_{43}	$\boxed{d_{44}}$	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Para cada $i \geq 0$, definimos $d_i = \begin{cases} d_{ii} + 1 & d_{ii} < 9 \\ 0 & d_{ii} = 9 \end{cases}$

Sea ahora el número real $r = 0, d_0 d_1 d_2 d_3 d_4 d_5 d_6 \ldots$

Cardinalidad de conjuntos infinitos

Para cada $i \geq 0$, definimos: $d_i = \begin{cases} d_{ii} + 1 & d_{ii} < 9 \\ 0 & d_{ii} = 9 \end{cases}$

Sea ahora 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?

- ¿$r = r_0$? No, porque difieren en el primer dígito decimal.
- ¿$r = r_1$? No, porque difieren en el segundo dígito decimal.
- $\ldots$
- ¿$r = r_i$? No, porque el i-ésimo digito de r es distinto al de r_i:

$$d_i \neq d_{ii}$$

Por lo tanto, r no aparece en la lista $\rightarrow\leftarrow$

Como $(0, 1)$ no puede ponerse en una lista, no es enumerable.

Cardinalidad de conjuntos infinitos

El argumento anterior se llama **diagonalización**.

- ¿Por qué?
- Es clave para establecer muchos resultados en matemáticas y computación.
- ¿Qué nos dice el teorema anterior respecto a los programas en $\{$ INSERTE SU LENGUAJE FAVORITO AQUÍ $\}$?
- La enumerabilidad le pone una cota a las tareas que un computador puede realizar.

Cardinalidad de conjuntos infinitos

¿Qué otros conjuntos tienen la misma cardinalidad que $(0,1)$?

Teorema

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

Cardinalidad de conjuntos infinitos

Entonces, ¿dónde hay más elementos, en $\mathbb{N}$ o en $\mathbb{R}$?

Definición

Dados conjuntos A y B, diremos que $A \preceq B$ (A no es más grande que B) si existe una función inyectiva $f : A \to B$.

¿Es $\preceq$ una relación de orden?

Si $A \preceq B$, diremos que $|A| \leq |B|$.

Definición

Dados conjuntos A y B, diremos que $A \prec B$ (A es **menos numeroso** que B) si $A \preceq B$ pero $A \not\approx B$.

¿Cómo se define esta noción usando funciones?

- Existe función inyectiva $f : A \to B \ldots$
- $\ldots$ pero no existe función biyectiva $g : A \to B$.

Si $A \prec B$, diremos que $|A| < |B|$.

Cardinalidad de conjuntos infinitos

Ejemplo

$\mathbb{N}$ es menos numeroso que $\mathbb{R}$, y por lo tanto decimos que $|\mathbb{N}| < |\mathbb{R}|$.

¡Hay estrictamente **menos** números naturales que reales!

Corolario

$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Demostramos algo parecido para el caso finito. . .

Cardinalidad de conjuntos infinitos

Dado un conjunto A (no necesariamente finito):

Teorema (Cantor)

A es menos numeroso que su conjunto potencia ($|A| < |\mathcal{P}(A)|$).

Ejercicio

Demuestre el teorema.

Primero, es claro que $|A| \leq |\mathcal{P}(A)|$. Basta tomar

$$f : A \to \mathcal{P}(A) \text{ dada por } f(a) = \{a\}$$

la cual es claramente inyectiva.

Ahora mostraremos que no existe una función biyectiva entre A y $\mathcal{P}(A)$.

Por contradicción, supongamos que sí existe una biyección f entre A y $\mathcal{P}(A)$.

Diagonalización entre A y $\mathcal{P}(A)$

Considere el siguiente conjunto:

Definición (complemento de la diagonal)

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

Notemos que $\bar{D} \subseteq A$, y por lo tanto $\bar{D} \in \mathcal{P}(A)$. Luego, como f es biyectiva, debe existir $x \in A$ tal que $f(x) = \bar{D}$. Considere ahora los siguientes casos:

- Si $x \in f(x)$, entonces $x \in \bar{D}$ (porque $f(x) = \bar{D}$), pero por definición de $\bar{D}, x \notin f(x)$.
- Si $x \notin f(x)$, entonces $x \notin \bar{D}$ (porque $f(x) = \bar{D}$), pero por definición de $\bar{D}, x \in f(x)$.

Luego, $x \in f(x)$ si y sólo si $x \notin f(x)$, lo cual es una contradicción. Por lo tanto, no existe una biyección entre A y $\mathcal{P}(A)$.

Reflexiones finales

- ¿Cuántos "infinitos" existen?
- ¿Hay algún infinito entre $|\mathbb{N}|$ y $|\mathbb{R}|$?

- ¿Qué implica todo lo anterior para la computación?
  - ¿Qué cosas es capaz de hacer un computador?
  - ¿Qué cosas **no** es capaz de hacer?
  - ¿Existen problemas computacionales para los cuales no existan algoritmos que los resuelvan?
  - Respuesta: IIC2223 :)

Matemáticas Discretas

Funciones y Cardinalidad

Nicolás Alvarado
nfalvarado@mat.uc.cl

Bernardo Barías
bjbarias@uc.cl

Sebastián Bugedo
bugedo@uc.cl

Gabriel Diéguez
gsdieguez@ing.puc.cl

Departamento de Ciencia de la Computación
Escuela de Ingeniería
Pontificia Universidad Católica de Chile

11 de octubre de 2023