Matemáticas Discretas

Demostraciones

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

6 de septiembre 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.
2. Modelar formalmente un problema usando lógica, conjuntos, relaciones, y las propiedades necesarias, y demostrar propiedades al respecto de su modelo.

Contenidos

¿Qué es una demostración?

Definición

Una **demostración** es un **argumento válido** para establecer la verdad de una **afirmación matemática**.

Afirmaciones matemáticas

¿Qué tipos de afirmaciones matemáticas conocemos?

- Definición
- Axioma
- Teorema
- Proposición
- Lema
- Corolario
- Conjetura
- Problema abierto

Afirmaciones matemáticas

Definición

Una **afirmación matemática** es una sentencia sobre objetos matemáticos que puede ser verdadera o falsa.

Observación

Todo predicado o fórmula es una afirmación matemática.

Ejemplos

- Todo número natural cumple que si es par, entonces su sucesor es impar.
- Existe un número natural tal que todo número es mayor a él.

Axiomas

¿Qué es un axioma?

Definición

Un **axioma** es una afirmación matemática que se considera evidente y se acepta sin requerir demostración previa.

¿Qué axiomas conocemos?

Axiomas

Geometría Euclidiana

- Dados dos puntos se puede trazar una línea que los une.
- Cualquier segmento puede prolongarse de manera continua en cualquier sentido.
- Se puede trazar una circunferencia con centro en cualquier punto y de cualquier radio.
- Todos los ángulos rectos son congruentes.
- Si una recta, al cortar a otras dos, forma ángulos internos menores a dos ángulos rectos, esas dos rectas prolongadas indefinidamente se cortan del lado en el que están los ángulos menores que dos rectos.

Axiomas

Axiomatización de Peano

- $0 \in \mathbb{N}$
- $\forall x(x = x)$
- $\forall x \forall y(x = y \rightarrow y = x)$
- $\forall x \forall y \forall z(x = y \wedge y = z \rightarrow x = z)$
- $\forall x \forall y(x = y \wedge y \in \mathbb{N} \rightarrow x \in \mathbb{N})$
- $\forall x(x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N})$
- $\forall x \forall y(x = y \leftrightarrow S(x) = S(y))$
- $\neg(\exists x(S(x) = 0))$

Teoremas

¿Qué es un teorema?

Definición

Un **teorema** es una afirmación matemática verdadera y demostrable.

Ejemplos

- Teorema de Pitágoras.
- Teorema fundamental del cálculo.
- Teorema fundamental del álgebra.
- Teorema fundamental de la aritmética.

Teoremas

Definición

Un **lema** es un resultado menor cuyo fin es ayudar en la demostración de un teorema.

Definición

Una **proposición** es un resultado interesante, pero de menor importancia que un teorema.

Definición

Un **corolario** es una afirmación matemática cuya demostración se deriva casi directamente de un teorema.

Conjeturas

¿Qué es una conjetura?

Definición

Una conjetura es una afirmación matemática que se cree que es verdad pero **NO** se ha demostrado.

Ejemplo

- *"Todo número par mayor a 2 puede ser expresado como suma de dos primos"*

  Conjetura de Goldbach

- $\forall x \forall y \forall z \forall n (n > 2 \rightarrow x^n + y^n \neq z^n)$

  (ex) Conjetura de Fermat

Problemas abiertos

¿Qué es un problema abierto?

Definición

Un **problema abierto** es una afirmación matemática la cual no se sabe si es verdadera o falsa, y para la cual todavía no se conoce una solución o demostración.

¿Cuál es el problema abierto más importante en ciencia de la computación?

¿Cuál es el problema abierto más importante en ciencia de la computación?

$$\mathrm{P} \stackrel{?}{=} \mathrm{NP}$$

"If the solution to a problem can be quickly verified by a computer, can the computer also solve that problem quickly?"

Wikipedia.

¿Cuál es el problema abierto más importante en ciencia de la computación?

$$\mathrm{P} \stackrel{?}{=} \mathrm{NP}$$

"Aside from being an important problem in computational theory, a proof either way would have profound implications for mathematics, cryptography, algorithm research, artificial intelligence, game theory, multimedia processing, philosophy, economics and many other fields"

Wikipedia.

¿Qué es una demostración?

Definición

Una **demostración** es un **argumento válido** para establecer la verdad de una **afirmación matemática**.

Un argumento válido es una secuencia de argumentos que puede estar compuesta por:

- Axiomas
- Hipótesis (si existen)
- Afirmaciones previamente demostradas

Cada argumento en la secuencia de argumentos está conectado con el anterior por una regla de inferencia.
El último paso de la secuencia establece la verdad de la afirmación.
Se parece a algo que ya vimos, ¿no?

¿Qué **NO** es una demostración?

- Una secuencia de símbolos
- Una secuencia disconexa de argumentos

IMPORTANTE

La secuencia de argumentos debe ser lo más **clara**, **precisa** y **completa** posible. La demostración debe **convencer** al lector u oyente sin dejarle ninguna duda sobre la correctitud de la demostración.

¿Cómo encontramos una secuencia de argumentos para demostrar un teorema?

- Experiencia
- Intuición
- Creatividad
- Perseverancia
- **Métodos de demostración**

Supongamos que tenemos una afirmación como la siguiente:

$$\forall x(P(x) \to Q(x))$$

¿Qué métodos de demostración podemos ocupar?

Métodos de demostración

$$\forall x(P(x) \rightarrow Q(x))$$

- Directa
- Contrapositivo
- Contradicción
- Por análisis de casos
- Otros tipos de demostración

Veremos cada una de las distintas metodologías.

Demostración directa

También se conoce del latin *modus ponendo ponens* ("la forma en que se afirma afirmando"). Por demostrar:

$$\forall x(P(x) \to Q(x))$$

Método directo

Suponemos que $P(n)$ es verdadero para un n arbitrario y demostramos que $Q(n)$ también es verdadero.

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si n es impar, entonces n^2 es impar.

Demostración directa

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si n es impar, entonces n^2 es impar.

Sea $n \in \mathbb{N}$. Suponemos que n es impar, y entonces es de la forma $n = 2k + 1$ con $k \in \mathbb{N}$:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2k' + 1 \end{aligned}$$

Finalmente, como los naturales son cerrados bajo multiplicación y suma es claro que k' también es natural y n^2 es impar.

Contrapositivo

También se conoce del latin *modus tollendo tollens* ("el camino que niega al negar"). Por demostrar:

$$\forall x(P(x) \to Q(x))$$

Método por contrapositivo

Suponemos que $Q(n)$ es falso para un n arbitrario y demostramos que $P(n)$ también es falso.

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si $3n + 2$ es impar, entonces n es impar.

Demostración por contrapositivo

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si $3n + 2$ es impar, entonces n es impar.

Sea $n \in \mathbb{N}$. Supongamos que n no es impar, y por lo tanto es par. Luego, n es de la forma $n = 2k$ con $k \in \mathbb{N}$:

$$
\begin{aligned}
n &= 2k \\
3n &= 6k && \text{(Multiplicamos por 3)} \\
3n + 2 &= 6k + 2 && \text{(Sumamos 2)} \\
3n + 2 &= 2(3k + 1) \\
3n + 2 &= 2k'
\end{aligned}
$$

Como los naturales son cerrados bajo multiplicación y suma es claro que k' también es natural y $3n + 2$ es par. Finalmente, por contrapositivo concluimos que si $3n + 2$ es impar, entonces n es impar.

Demostración por contradicción

"Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

A mathematician's apology (G. H. Hardy).

Demostración por contradicción

Por demostrar:

$$\forall x(P(x) \to Q(x))$$

Método por contradicción

Suponemos que existe un n tal que $P(n)$ es verdadero y $Q(n)$ es falso e inferimos una contradicción.

¿A qué se parece?

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Demostración por contradicción

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Por contradicción suponemos que $\sqrt{2}$ es racional, y entonces puede escribirse de la forma $\sqrt{2} = \frac{a}{b}$ con $a, b \in \mathbb{Z}$ sin factores en común y $b \neq 0$. Notemos que al no tener factores en común, no pueden ser ambos pares. Desarrollando la igualdad:

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \qquad \text{(Elevamos al cuadrado)} \\ a^2 &= 2b^2 \end{aligned}$$

Entonces, a^2 es par y por teorema anterior a también es par: $a = 2k$.

Demostración por contradicción

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Entonces, a^2 es par y por teorema anterior a también es par: $a = 2k$.
Reemplazando en la igualdad anterior:

$$\begin{aligned} a^2 &= 2b^2 \\ (2k)^2 &= 2b^2 \\ 4k^2 &= 2b^2 \\ b^2 &= 2k^2 \end{aligned}$$

Entonces, b^2 es par, y por teorema anterior b también es par. Esto es una contradicción, ya que entre a y b alguno debe ser un número impar. Concluimos entonces que $\sqrt{2}$ no puede ser racional, y por lo tanto es irracional.

Demostración por análisis de casos

Por demostrar:

$$\forall x(P(x) \to Q(x))$$

Dividimos el dominio de la interpretación $\mathcal{I}$ con que trabajamos en una cantidad finita de casos $C_1, ..., C_n$, tal que:

$$\mathcal{I}(dom) = \bigcup_{i=1}^{n} C_i$$

Método por casos

Para cada subdominio $C_1, \ldots, C_n$ demostramos que:

$$\forall x(P(x) \to Q(x))$$

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \geq n$.

Demostración por análisis de casos

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \geq n$.

Sea $n \in \mathbb{Z}$. Tenemos 3 casos:

1. $n = 0$: es claro que se cumple la propiedad.
2. $n > 0$: como $n \in \mathbb{Z}$ tenemos que $n \geq 1$.
   Si multiplicamos por n a ambos lados, obtenemos que $n^2 \geq n$.
3. $n < 0$: si multiplicamos por n (negativo) a ambos lados:
   $n^2 > 0 \Rightarrow n^2 > n \Rightarrow n^2 \geq n$.

Ya que no existen más casos, concluimos que la propiedad se cumple para todo $n \in \mathbb{Z}$. $\square$

Otros tipos de demostración

- Demostración por doble-implicación
- Demostración por contra-ejemplo
- Demostración existencial

Demostración por doble implicación

Por demostrar:

$$\forall x(P(x) \leftrightarrow Q(x))$$

Demostración por doble implicación

Se deben demostrar ambas direcciones por separado. En términos formales:

$$\forall x(P(x) \rightarrow Q(x)) \land \forall x(Q(x) \rightarrow P(x))$$

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que n es impar si y sólo si n^2 es impar.

Demostración por doble implicación

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que n es impar si y sólo si n^2 es impar.

($\Rightarrow$) Lo demostramos en un ejercicio anterior.

($\Leftarrow$) Por contrapositivo, suponemos que n es par y por ende de la forma $n = 2k$ con $k \in \mathbb{N}$:

$$\begin{aligned} n &= 2k \\ n^2 &= 4k^2 \\ &= 2 \cdot (2k^2) \end{aligned}$$

Entonces, n^2 es par y por contrapositivo se cumple que si n^2 es impar entonces n es impar.

Dado que mostramos ambas direcciones, concluimos que la doble implicancia es cierta. $\square$

Demostración por contra-ejemplo

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que $P(n)$ es falso.

Ejercicio

Un natural $n \in \mathbb{N}$ se dice un **cuadrado perfecto** si existe un $k \in \mathbb{N}$ tal que $n = k^2$. Demuestre que es falso que todo número natural es suma de dos cuadrados perfectos.

Demostración por contra-ejemplo

Ejercicio

Un natural $n \in \mathbb{N}$ se dice un **cuadrado perfecto** si existe un $k \in \mathbb{N}$ tal que $n = k^2$. Demuestre que es falso que todo número natural es suma de dos cuadrados perfectos.

Probamos con los primeros números naturales:

$$\begin{aligned} 0 &= 0^2 + 0^2 \\ 1 &= 0^2 + 1^2 \\ 2 &= 1^2 + 1^2 \\ 3 &\neq 1^2 + 1^2 \\ &\neq 2^2 + 1^2 \end{aligned}$$

Por lo tanto, 3 no es la suma de dos cuadrados perfectos.

Demostración existencial

Por demostrar:

$$\exists x(P(x))$$

Método por existencia

Debemos demostrar que existe un elemento n tal que $P(n)$ es verdadero. (Nótese que NO es estrictamente necesario mostrar n explícitamente.)

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Demostración existencial

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

1. Si $\sqrt{2}^{\sqrt{2}}$ es **racional**, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.
2. Si $\sqrt{2}^{\sqrt{2}}$ es **irracional**, entonces considere $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$:

$$\begin{aligned} \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} &= \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} \\ &= \sqrt{2}^{2} \\ &= 2 \end{aligned}$$

Por lo tanto, a^b es racional. $\square$

¿Cuál método de demostración ocupar?

¡No existe un método infalible para demostrar!

- Probar con distintos métodos.
- Ganar intuición intentando con casos o ejemplos más sencillos.
- Revisar demostraciones similares.
- Sean creativos.

Matemáticas Discretas

Demostraciones

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

6 de septiembre de 2023