Matemática Discreta

Clase 6: Técnicas de demostración

Federico Olmedo y Alejandro Hevia
Departamento de Ciencias de la Computación
Universidad de Chile

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

- Un teorema es un resultado matemático importante, cuya demostración es generalmente compleja y por lo tanto se organiza alrededor de algunos resultados intermedios.

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

- Un teorema es un resultado matemático importante, cuya demostración es generalmente compleja y por lo tanto se organiza alrededor de algunos resultados intermedios.
- Un lema o proposición es un resultado intermedio, que sirve para probar un teorema de mayor relevancia.

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

- Un teorema es un resultado matemático importante, cuya demostración es generalmente compleja y por lo tanto se organiza alrededor de algunos resultados intermedios.
- Un lema o proposición es un resultado intermedio, que sirve para probar un teorema de mayor relevancia.
- Un corolario es un resultado que sigue inmediatamente de un teorema.

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

- Un teorema es un resultado matemático importante, cuya demostración es generalmente compleja y por lo tanto se organiza alrededor de algunos resultados intermedios.
- Un lema o proposición es un resultado intermedio, que sirve para probar un teorema de mayor relevancia.
- Un corolario es un resultado que sigue inmediatamente de un teorema.

¿Qué es una conjetura?

Nomenclatura

¿Qué diferencia hay entre teorema, lema, proposición y corolario?

- Un teorema es un resultado matemático importante, cuya demostración es generalmente compleja y por lo tanto se organiza alrededor de algunos resultados intermedios.
- Un lema o proposición es un resultado intermedio, que sirve para probar un teorema de mayor relevancia.
- Un corolario es un resultado que sigue inmediatamente de un teorema.

¿Qué es una conjetura?

- Una conjetura es una proposición que se cree firmemente verdadera, pero que no se ha podido demostrar.

Enunciado de teoremas

Enunciado de teoremas

- Un teorema generalmente establece que todos los elementos de un dominio dado tienen cierta propiedad

Enunciado de teoremas

- Un teorema generalmente establece que todos los elementos de un dominio dado tienen cierta propiedad
- Sin embargo, el cuantificador universal muchas veces no queda explícito en el enunciado

Enunciado de teoremas

- Un teorema generalmente establece que todos los elementos de un dominio dado tienen cierta propiedad
- Sin embargo, el cuantificador universal muchas veces no queda explícito en el enunciado

Ejemplo: Un número compuesto admite una única descomposición en factores primos.

Enunciado de teoremas

- Un teorema generalmente establece que todos los elementos de un dominio dado tienen cierta propiedad
- Sin embargo, el cuantificador universal muchas veces no queda explícito en el enunciado

Ejemplo: Un número compuesto admite una única descomposición en factores primos.

> *Para todo número entero n, si n es compuesto, n admite una única descomposición en factores primos.*

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \to q$.

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \rightarrow q$.
- Para probar dicha implicación podemos seguir diversas estrategias:

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \rightarrow q$.
- Para probar dicha implicación podemos seguir diversas estrategias:
    - prueba directa

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \to q$.
- Para probar dicha implicación podemos seguir diversas estrategias:
  - prueba directa
  - prueba por contraposición (o contrarecíproco)

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \to q$.
- Para probar dicha implicación podemos seguir diversas estrategias:
  - prueba directa
  - prueba por contraposición (o contrarecíproco)
  - prueba por análisis de casos

Metodos de demostración

Gran parte de los teoremas tienen la forma

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

donde P representa la(s) hipótesis y Q el resultado a probar.

- Se parte considerando un x arbitrario
- Y la demostración se vuelve una implicación de la forma $p \rightarrow q$.
- Para probar dicha implicación podemos seguir diversas estrategias:
  - prueba directa
  - prueba por contraposición (o contrarecíproco)
  - prueba por análisis de casos
  - prueba por contradicción (o reducción al absurdo)

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Demostraciones directas

Una demostración directa de $p \to q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Sean n un numero impar arbitrario;

Demostraciones directas

Una demostración directa de $p \to q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Sean n un numero impar arbitrario;
- $n = 2k + 1$ para algún entero k

Demostraciones directas

Una demostración directa de $p \to q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Sean n un numero impar arbitrario;
- $n = 2k + 1$ para algún entero k
- Luego $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$,

Demostraciones directas

Una demostración directa de $p \to q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Sean n un numero impar arbitrario;
- $n = 2k + 1$ para algún entero k
- Luego $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$,
- o equivalentemente, $n^2 = 2(2k^2 + 2k) + 1$;

Demostraciones directas

Una demostración directa de $p \to q$ se construye derivando q a partir de p. Sólo nos tenemos que enfocar en el caso en el que p es verdadero.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Sean n un numero impar arbitrario;
- $n = 2k + 1$ para algún entero k
- Luego $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$,
- o equivalentemente, $n^2 = 2(2k^2 + 2k) + 1$;
- Por lo tanto n^2 es impar.

Demostraciones directas

Ejercicio: Demuestre directamente que si m, n, p son enteros y $(m + n)$ y $(n + p)$ son enteros pares, entonces $m + p$ también es un entero par.

Ejercicio: Demuestre directamente que si m y n son cuadrados perfectos, entonces mn es también cuadrado perfecto[1].

[1] Un natural a es un cuadrado perfecto sii existe otro natural b tal que $a = b^2$.

Demostraciones por contraposición

Muchas veces es difícil encontrar una demostración directa de un resultado.

Demostraciones por contraposición

Muchas veces es difícil encontrar una demostración directa de un resultado.

Ejercicio: Trate de demostrar directamente que si n es un entero y $3n + 2$ es impar, entonces n es impar.

Demostraciones por contraposición

Muchas veces es difícil encontrar una demostración directa de un resultado.

Ejercicio: Trate de demostrar directamente que si n es un entero y $3n+2$ es impar, entonces n es impar.

Las demostración por contraposición se basan en la equivalencia

$$p \to q \ \equiv \ \neg q \to \neg p \ .$$

En vez de probar $p \to q$ probamos (de manera directa) $\neg q \to \neg p$.

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n+2$ es impar, entonces n es impar.

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n + 2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n + 2$ es par.

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n + 2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n + 2$ es par.

- Sean n un numero par arbitrario;

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n+2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n+2$ es par.

- Sean n un numero par arbitrario;
- $n = 2k$ para algún entero k

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n+2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n+2$ es par.

- Sean n un numero par arbitrario;
- $n = 2k$ para algún entero k
- Luego $3n + 2 = 3(2k) + 2$,

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n+2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n+2$ es par.

- Sean n un numero par arbitrario;
- $n = 2k$ para algún entero k
- Luego $3n+2 = 3(2k)+2$,
- o equivalentemente, $3n+2 = 2(3k+1)$;

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n+2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n+2$ es par.

- Sean n un numero par arbitrario;
- $n = 2k$ para algún entero k
- Luego $3n+2 = 3(2k)+2$,
- o equivalentemente, $3n+2 = 2(3k+1)$;
- Por lo tanto $3n+2$ es par.

Demostraciones por contraposición

Ejemplo: Demuestre por contraposición que si n es un entero y $3n + 2$ es impar, entonces n es impar.

Tengo que probar (de manera directa) que si n es par entones $3n + 2$ es par.

- Sean n un numero par arbitrario;
- $n = 2k$ para algún entero k
- Luego $3n + 2 = 3(2k) + 2$,
- o equivalentemente, $3n + 2 = 2(3k + 1)$;
- Por lo tanto $3n + 2$ es par.

Ejercicio*: Demuestre por contraposición que si $n = ab$, donde ambos a y b son reales positivos, entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q) \ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q)\ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Ejemplo: Probar que para todo entero n, si $3 \nmid n$ entonces $3 \mid n^2 - 1$.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q) \ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Ejemplo: Probar que para todo entero n, si $3 \nmid n$ entonces $3 \mid n^2 - 1$.

Si $3 \nmid n$ hay dos posibilidades: $n = 3k + 1$ o $n = 3k + 2$ para algún entero k.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q) \ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Ejemplo: Probar que para todo entero n, si $3 \nmid n$ entonces $3 \mid n^2 - 1$.

Si $3 \nmid n$ hay dos posibilidades: $n = 3k + 1$ o $n = 3k + 2$ para algún entero k.

- Si $n = 3k + 1$ para algún entero k, tenemos que $n^2 = 3(3k^2 + 2k) + 1$ por lo que $3 \mid n^2 - 1$.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q)\ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Ejemplo: Probar que para todo entero n, si $3 \nmid n$ entonces $3 \mid n^2 - 1$.

Si $3 \nmid n$ hay dos posibilidades: $n = 3k + 1$ o $n = 3k + 2$ para algún entero k.

- Si $n = 3k + 1$ para algún entero k, tenemos que $n^2 = 3(3k^2 + 2k) + 1$ por lo que $3 \mid n^2 - 1$.
- Si $n = 3k + 2$ para algún entero k, tenemos similarmente que $n^2 = 3(3k^2 + 4k + 1) + 1$ por lo que $3 \mid n^2 - 1$.

Demostraciones por análisis casos

La demostración por casos se basa en la equivalencia

$$p_1 \vee \ldots \vee p_n \to q \quad \equiv \quad (p_1 \to q) \wedge \ldots \wedge (p_n \to q)\ .$$

Para probar que $p \to q$, hallamos $p_1, \ldots, p_n$ tal que $p \equiv p_1 \vee \ldots \vee p_n$ y probamos $p_1 \to q, \ldots, p_n \to q$.

Ejemplo: Probar que para todo entero n, si $3 \nmid n$ entonces $3 \mid n^2 - 1$.

Si $3 \nmid n$ hay dos posibilidades: $n = 3k + 1$ o $n = 3k + 2$ para algún entero k.

- Si $n = 3k + 1$ para algún entero k, tenemos que $n^2 = 3(3k^2 + 2k) + 1$ por lo que $3 \mid n^2 - 1$.
- Si $n = 3k + 2$ para algún entero k, tenemos similarmente que $n^2 = 3(3k^2 + 4k + 1) + 1$ por lo que $3 \mid n^2 - 1$.

Ejercicio: Demuestre por casos que $|xy| = |x||y|$.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \to \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \to \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo. Supongamos que existe un número racional r que es el menor de todos los racionales positivos.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo. Supongamos que existe un número racional r que es el menor de todos los racionales positivos. Luego $r/2$ es racional positivo,

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo. Supongamos que existe un número racional r que es el menor de todos los racionales positivos. Luego $r/2$ es racional positivo, y es menor que r.

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo. Supongamos que existe un número racional r que es el menor de todos los racionales positivos. Luego $r/2$ es racional positivo, y es menor que r. ¡Absurdo!

Demostraciones por contradicción

Las demostraciones por contradicción o reducción al absurdo se basan en la siguiente equivalencia

$$q \quad \equiv \quad \neg q \rightarrow \mathit{false} \ .$$

Para probar q, derivan una contradicción a partir de $\neg q$.

Ejercicio: Demuestre que no existe ningún número racional que sea el menor de todos los racionales (estrictamente) positivos.

La prueba procede por reducción al absurdo. Supongamos que existe un número racional r que es el menor de todos los racionales positivos. Luego $r/2$ es racional positivo, y es menor que r. ¡Absurdo! Por lo tanto, no existe un racional r que sea el menor de todos los racionales positivos.

Demostraciones por contradicción

Ejercicio*: Probar que si a y b son reales positivos, entonces $a + b \geq 2\sqrt{ab}$.

Demostraciones por contradicción

Ejercicio*: Probar que si a y b son reales positivos, entonces $a + b \geq 2\sqrt{ab}$.

Una proposición de la forma $p \to q$ también puede ser probada por contradicción. Basta derivar una contradicción a partir de $p \wedge \neg q$.

Demostraciones por contradicción

Ejercicio*: Probar que si a y b son reales positivos, entonces $a + b \geq 2\sqrt{ab}$.

Una proposición de la forma $p \rightarrow q$ también puede ser probada por contradicción. Basta derivar una contradicción a partir de $p \land \neg q$.

Ejercicio: Probar que para todo entero n, si n^2 es par, entonces n es par.