Tema 1: Introducción. Demostración matemática. Métodos de demostración

David de Frutos Escrig
versión original elaborada por
María Inés Fernández Camacho

MATEMÁTICA DISCRETA Y LÓGICA MATEMÁTICA
(Ingeniería Informática - Ciencias Matemáticas)
UCM Curso 18/19

Demostración matemática: Argumento que establece la verdad de una proposición/enunciado.

Argumento: A partir de unas afirmaciones que se dan por **ciertas**, se deduce mediante ciertas **reglas de razonamiento** aceptadas, una proposición más compleja.

Herramientas: Axiomas, definiciones, términos primitivos (definidos implícitamente mediante acuerdos y postulados), reglas de inferencia, resultados previos conocidos ...

Def:

Una **proposición** *es una afirmación (declaración) que o bien es cierta o bien es falsa (pero no ambas).*

Ejemplos:

- Proposiciones:
  - París es la capital de Francia
  - 8 es un número primo
  - 9 no es un número primo
  - $(2 < 3)$ y 5 es primo
  - Todos los números naturales son pares
  - Algunos mamíferos leen
- Oraciones que no son proposiciones:
  - ¡Cállate!
  - ¿Qué hay en la bolsa?
  - 4 - 2
  - x es par

Clases de proposiciones:

- Proposiciones sobre individuos:
  - París es la capital de Francia
  - 8 es un número primo
  - 9 no es un número primo
  - $(2 < 3\ )$ y 5 es primo
  - $6 = 2 * 3$
- Proposiciones sobre colectivos:
  - Todos los números naturales son pares
  - Algunos mamíferos leen
  - Para cada números natural hay otro más grande
  - Si x es par, puede escribirse como $2 * y$

- **Proposiciones atómicas:** No se pueden descomponer en otras más simples. Se les denota con letras minúsculas, p,q, r, s, ... con o sin subíndices (símbolos proposicionales).

Mario compró un coche	p
Luisa saludó a Mario	q
Luisa conoce a Mario	r

- **Proposiciones compuestas:** Construidas por cuantificación de predicados y/o combinando otras más simples mediante conectivas lógicas: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.
  - Conectiva unaria: $\neg$ (negación).
  - Conectivas binarias: $\wedge$(conjunción), $\vee$(disyunción), $\rightarrow$ (condicional o implicación) y $\leftrightarrow$ (bicondicional o biimplicación).

Mario compró un coche y Luisa saludó a Mario	$(p \wedge q)$
Luisa no saludó a Mario	$\neg q$
Mario compró un coche y Luisa no saludó a Mario aunque le conoce	$((p \wedge \neg q) \wedge r)$

- **Fórmulas:** cualquier enunciado formalizado ya sea simple o compuesto
  - Se les denota con letras griegas $\varphi, \psi, \chi, \ldots$ con o sin subíndices.
  - En las fórmulas condicionales $(\varphi_1 \to \varphi_2)$ a φ_1 se le llama **antecedente** y a φ_2**consecuente**.
- A la verdad o falsedad de una fórmula se la llama su **valor veritativo**
  - **0** denota **falso**
  - **1** denota **cierto**
- **Constantes lógicas:**
  - Sirven para representar respectivamente un enunciado que siempre es cierto o que siempre es falso.
    - $\perp$ (falsedad)
    - $\top$ (certeza)
  - **EJ:** $\begin{array}{ll} (0=0) & \top \\ (0=1) & \perp \end{array}$

Principales conectivas lógicas

Nombre	Notación	Significado
Negación	$\neg\varphi$	"no φ"
Conjunción	$(\varphi_1 \wedge \varphi_2)$	" φ_1 y φ_2 "
Disyunción	$(\varphi_1 \vee \varphi_2)$	" φ_1 o φ_2"
Implicación	$(\varphi_1 \to \varphi_2)$	"si φ_1 entonces φ_2 " ' φ_2 si φ_1" " φ_2 siempre que φ_1" " φ_1 sólo si φ_2 " " φ_1 es condición suficiente para φ_2 " " φ_2 es condición necesaria para φ_1 "
Bicondicional	$(\varphi_1 \leftrightarrow \varphi_2)$	" φ_1 si y sólo si φ_2" " φ_1 es condición necesaria y suficiente para φ_2"

- **Tabla de verdad** de una proposición compuesta mediante conectivas: da los valores veritativos de la proposición para todas las asignaciones posibles a sus argumentos.

φ	$\neg\varphi$
0	1
1	0

TABLA: Tabla de verdad para $\neg\varphi$

$\neg\varphi$ es falso cuando φ es cierto
$\neg\varphi$ es cierto cuando φ es falso
Afirmar $\neg\varphi$ equivale a afirmar que
"**no** φ es cierto" o que "φ no tiene lugar"
EJ: **p** : Nieva , $\neg$ **p**: **NO** nieva

φ_1	φ_2	$(\varphi_1 \wedge \varphi_2)$	$(\varphi_1 \vee \varphi_2)$	$(\varphi_1 \to \varphi_2)$	$(\varphi_1 \leftrightarrow \varphi_2)$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

TABLA: Tablas de verdad de las principales conectivas binarias.

Si dos fórmulas φ y ψ expresan lógicamente lo mismo se dice que son lógicamente equivalentes, y se escribe $\varphi \sim \psi$.

φ_1	φ_2	$\neg\varphi_1$	$(\varphi_1 \to \varphi_2)$	$(\neg\varphi_1 \vee \varphi_2)$	$((\varphi_1 \to \varphi_2) \leftrightarrow (\neg\varphi_1 \vee \varphi_2))$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	0	1	1	1

TABLA: $(\varphi_1 \to \varphi_2) \sim (\neg\varphi_1 \vee \varphi_2)$

DEF:

- *El* **recíproco** *de una proposición condicional* $(\varphi_1 \to \varphi_2)$ *es la proposición* $(\varphi_2 \to \varphi_1)$.
- *El* **contrarrecíproco** *de una proposición condicional* $(\varphi_1 \to \varphi_2)$ *es la proposición* $(\neg\varphi_2 \to \neg\varphi_1)$.
- *La* **inversa** *de una proposición condicional* $(\varphi_1 \to \varphi_2)$ *es la proposición* $(\neg\varphi_1 \to \neg\varphi_2)$.

- $(\varphi_1 \to \varphi_2) \sim (\neg\varphi_2 \to \neg\varphi_1)$ pero $(\varphi_1 \to \varphi_2) \not\sim (\neg\varphi_1 \to \neg\varphi_2)$.

- $(p \to q) \sim (\neg q \to \neg\, p)$ pero $(p \to q) \not\sim (\neg p \to \neg\, q)$.

- **Ej:** Si $\underbrace{\text{Jaime es de Barcelona}}_{p}$ entonces $\underbrace{\text{Jaime es español}}_{q}$ $\quad (p \to q)$

  Su **recíproco** es:

  Si $\underbrace{\text{Jaime es español}}_{q}$ entonces $\underbrace{\text{Jaime es de Barcelona}}_{p}$ $\quad (q \to p)$

  Su **contrarrecíproco** es:

  Si $\underbrace{\text{Jaime no es español}}_{\neg q}$ entonces $\underbrace{\text{Jaime no es de Barcelona}}_{\neg\, p}$ $\quad (\neg\, q \to \neg\, p)$

  Su **inversa** es:

  Si $\underbrace{\text{Jaime no es de Barcelona}}_{\neg q}$ entonces $\underbrace{\text{Jaime no es español}}_{\neg\, q}$ $\quad (\neg\, p \to \neg\, q)$

Lenguaje matemático: proposiciones sobre colectivos

Con frecuencia nuestros razonamientos cotidianos aluden a elementos de un colectivo no como individuos, sino precisamente como elementos de dicho colectivo.

- **Dominio o universo de discurso:** Colectivo de individuos sobre los que hablamos.
  Ej: x es par **Dominio:** $\mathbb{N}$
- **Constantes:** nombres propios de individuos
  Ej: 8, Paco, María
- **Variables:** denotan valores cualesquiera del universo. Representan individuos anónimos, generales.
  Notación x, y, ...

- **Predicados:** Enunciados sobre individuos.
  - Monádicos : Propiedades de un individuo. Forma general de un enunciado atributivo, i.e. que atribuye una propiedad a un sujeto.
    (P(x) es un predicado con respecto al dominio D, si para cada x en el dominio, P(x) es una proposición).
    Notación P(x),Q(y), ...
    Ej: P(x): x es par , M(x): x es mamífero,...
    Un ejemplo de P(x) es un valor para el que P(x) es cierto . Un contraejemplo de P(x) es un valor para el que P(x) es falso . 2 es un ejemplo de P(x): x es par, porque P(2) es cierta y 3 es un contraejemplo, pues P(3) es falsa.
  - Poliádicos : Relaciones entre individuos.
    Ej: H(x,y): x e y son hermanos,...
    "Paco y María son hermanos" se formalizaría H(Paco, María)
- **Funciones**: Descripción de un individuo en función de otro(s)
  Ej: x + y , abs(-5), 3 + 2, pred(suc(x)),...

- **Cuantificadores** : Definen predicados sobre un colectivo que indican la frecuencia con que ocurre un predicado sobre individuos de ese colectivo.

  * Cuantificador universal : Indica que algo es cierto para todos los individuos del universo de discurso. Símbolo $\forall$

Def:

Dado un predicado $P(x)$ sobre un dominio D , $\forall\ x\ P(x)$ es una proposición que afirma que $P(x)$ es cierta para todos los posibles valores de x en el dominio D.

Se lee “ Para todo x (en D) se cumple P(x) ”, “Todo x (de D) cumple P(x)”, “Cada x (de D) cumple P(x)”, “Para cada x (en D) se cumple P(x)”

- **Ej:** Dado P(x): x es par , $D = \mathbb{N}$

  $\forall$ x P(x) es una proposición que afirma que todos los números naturales son pares,

  y por lo tanto es falsa (En particular P(3) es un contraejemplo, y no sirve de nada que para algunos otros valores, por ejemplo 2, se tenga P(2)).

- **Ej:** Observad que para P'(x):$\neg$ P(x) , $D = \mathbb{N}$ (o sea x es impar)

  $\forall$ x P'(x) (o sea $\forall$ x $\neg$ P(x)) también es falsa, **¿Por qué?**

*Cuantificador existencial : Indica que algo es cierto para algún(os) individuos del universo de discurso Símbolo $\exists$

Def:

Dado un predicado P(x) sobre un dominio D , $\exists$ x P(x) es una proposición que afirma que P(x) es cierta para al menos un valor de la variable x en el dominio D.

Se lee "Existe un x en D tal que P(x)" ," Existe un x en D tal que se cumple P(x)", "Para algún x, P"

Ejemplos:

- Dado $P(x)$: $x + 2 = 7$, $D = \mathbb{Z}$

  $\exists\, x\ P(x)$ es una proposición que es cierta, ya que $x = 5$ es un ejemplo de $P(x)$

- Dado $Q(x)$: $2x = 7$, $D = \mathbb{Z}$

  $\exists\, x\ Q(x)$ es una proposición que es falsa, ya que no hay ningún entero que cumpla $Q(x)$

- Dado $Q(x)$: $2x = 7$, $D = \mathbb{Q}$

  $\exists\, x\ Q(x)$ es una proposición que es cierta, ya que $x = \frac{7}{2}$ es un ejemplo de $Q(x)$

Ejemplos:

- "Todos los que leen disfrutan" se formaliza así:
  $\forall$ x (L(x) $\to$ Ds(x)) siendo
  D = seres vivos
  Ámbito del cuantificador: Si x lee entonces x disfruta
  L(x): x lee
  Ds(x) : x disfruta

- "Algunos mamíferos leen " se formaliza así:
  $\exists$ x (M(x) $\wedge$ L(x)) siendo
  D = seres vivos
  Ámbito del cuantificador: x es mamífero y x lee
  L(x): x lee
  M(x) : x es mamífero

- Los cuantificadores existencial y universal en general no conmutan, es decir, en general $\forall$ x $\exists$ y P(x,y) $\not\sim$ $\exists$ y $\forall$ x P(x,y)

  Ej: P(x,y): "x e y son amigos"
  D = Personas
  $\forall$ x $\exists$ y P(x,y) significa "Toda persona tiene un amigo".
  $\exists$ y $\forall$ x P(x,y) significa "Existe una persona (al menos una) que es amiga de todos".

- $\forall$ x $\exists$ y (x $<$ y) en D = $\mathbb{R}$ significa
  "Para todo número real existe otro número real mayor que él".

  Su negación es:
  $\neg\forall$ x $\exists$ y (x $<$ y) $\sim$ $\exists$ x $\forall$ y $\neg$(x $<$ y) que significa
  "Existe un número real mayor o igual que cualquier otro ".

ARGUMENTACIÓN LÓGICA

- Premisas y conclusión

Mario compró un coche Luisa saludó a Mario	Pepe lleva sombrero Juan contrató a Pepe
∴ Luisa saludó a uno que compró un coche (A1)	∴ Juan contrató a uno que lleva sombrero (A2)

- (A1) y (A2) son razonamientos válidos.

(A3)

Alguien lleva bufanda
Pedro pagó a alguien

∴ Pedro pagó a uno que lleva bufanda

- (A3) no es un razonamiento lógicamente válido.

Argumentaciones con igual forma "superficial" en lenguaje natural pueden diferir en su validez lógica.

La validez lógica de una argumentación no depende sólo de la verdad o falsedad de sus premisas, sino **de la relación entre la hipotética verdad de las premisas y la verdad de la conclusión.**

Argumentación lógica

$$\text{Premisas}\left\{\begin{array}{l}\varphi_1\\ \varphi_2\\ \vdots\\ \varphi_n\end{array}\right.$$

$$\text{Conclusión}\quad \therefore \psi$$

Una argumentación es lógicamente válida si la verdad de las premisas conlleva necesariamente la verdad de la conclusión (i.e. si no podemos concebir circunstancias que hagan verdaderas las premisas y falsa la conclusión)

- Si un argumento es lógicamente válido, se dice que la conclusión se deduce lógicamente de las premisas, lo cual es cierto si y sólo si $((\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n) \to \psi)$ es siempre verdad (tautología).
- **Reglas de inferencia**: razonamientos lógicamente válidos sencillos. Cada regla de inferencia tiene su origen en una implicación lógica.

Regla de inferencia Modus Tollens ("Modo que negando niega")

$$\begin{array}{c} (\varphi_1 \to \varphi_2) \\ \neg\varphi_2 \\ \hline \therefore \neg\varphi_1 \end{array}$$

Si camino entonces me canso
No me canso

∴ No camino

Implicación lógica relacionada: $(\ ((\varphi_1 \to \varphi_2) \wedge \neg\varphi_2) \to \neg\varphi_1)$

φ_1	φ_2	$(\varphi_1 \to \varphi_2)$	$\neg\varphi_2$	$\neg\varphi_1$	$((\varphi_1 \to \varphi_2) \wedge \neg\varphi_2\ )$	$(\ ((\varphi_1 \to \varphi_2) \wedge\neg\varphi_2\ ) \to \neg\varphi_1)$
0	0	1	1	1	1	1
0	1	1	0	1	0	1
1	0	0	1	0	0	1
1	1	1	0	0	0	1

Regla de inferencia Silogismo disyuntivo

$$\frac{\begin{array}{c}(\varphi_1 \vee \varphi_2)\\ \neg\varphi_1\end{array}}{\therefore\ \varphi_2}$$

$$\frac{\begin{array}{c}\text{Camino o cojo el autobús}\\ \text{No camino}\end{array}}{\therefore\ \text{Cojo el autobús}}$$

Implicación lógica relacionada: $(\ ((\varphi_1 \vee \varphi_2)\ \wedge\neg\varphi_1\ ) \to \varphi_2)$

φ_1	φ_2	$(\varphi_1 \vee \varphi_2)$	$\neg\varphi_1$	$((\varphi_1 \vee \varphi_2)\ \wedge\neg\varphi_1\ )$	$(\ ((\varphi_1 \vee \varphi_2)\ \wedge\neg\varphi_1\ ) \to \varphi_2)$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	0	0	1

Ejercicio:
Demuestra la corrección de las siguientes reglas de inferencia:

Simplificación

$$\frac{(\varphi_1 \wedge \varphi_2)}{\therefore \varphi_1}$$

Modus Ponens

$$\frac{\begin{array}{c}(\varphi_1 \to \varphi_2)\\ \varphi_1\end{array}}{\therefore \varphi_2}$$

Conjunción

$$\frac{\begin{array}{c}\varphi_1\\ \varphi_2\end{array}}{\therefore (\varphi_1 \wedge \varphi_2)}$$

Reglas de inferencia para fórmulas cuantificadas:

- Particularización universal:
  Si $\forall\ x\ P(x)$ es cierta **entonces** $P(a)$ es cierta para cada elemento particular a del dominio.
- Particularización existencial:
  Si $\exists\ x\ P(x)$ es cierta **entonces** podemos concluir que hay un elemento en el dominio, al que llamamos a, para el que $P(a)$ es cierta.
  Aquí a no es un elemento arbitrario del dominio, sino un valor concreto para el que $P(a)$ es cierta.
- Generalización universal:
  Si demostramos $P(x)$ para un elemento genérico (arbitrario) del dominio, **entonces** podemos concluir que $\forall\ x\ P(x)$.
  (Por genérico o arbitrario nos referimos a un elemento para el que no podemos hacer más suposiciones que su pertenencia al dominio)
- Generalización existencial:
  Si $P(a)$ es cierta para un elemento específico (particular o concreto) a del dominio **entonces** podemos concluir que $\exists\ x\ P(x)$ es cierta.

Demostración directa

Partiendo de las premisas (hipótesis), que se asumen ciertas, se utilizan reglas de inferencia, axiomas , definiciones y otros teoremas ya demostrados, para concluir que la tesis debe ser también cierta.

Ejemplo:

Cojo el autobús o camino	$(p \vee q)$	donde:
Si camino entonces me canso	$(q \rightarrow r)$	p: Cojo el autobús
No me canso	$\neg r$	q: Camino
$\therefore$ Cojo el autobús	$\therefore p$	r: Me canso

Demostración directa paso a paso :

1)	$(q \rightarrow r)$	premisa
2)	$\neg r$	premisa
3)	$\neg q$	1),2) y Modus Tollens
4)	$(p \vee q)$	premisa
5)	$\therefore p$	4),3) y Silogismo disyuntivo

Ejemplo:

Lenguaje natural	Lógica de predicados
Algunos mamíferos leen	$\exists\, x\ (M(x) \wedge L(x))$
Todos los que leen disfrutan	$\forall\, x\ (L(x) \rightarrow Ds(x))$
$\therefore$ Algunos mamíferos disfrutan	$\therefore \exists\, x\ (M(x) \wedge Ds(x))$

donde:
Universo de discurso: Seres vivos
$L(x)$: x lee
$Ds(x)$: x disfruta
$M(x)$: x es mamífero

1)	$\exists\, x\ (M(x) \wedge L(x))$	premisa
2)	$(M(a) \wedge L(a))$	particularización existencial de 1) para un ser vivo concreto al que llamo a
3)	$\forall\, x\ (L(x) \rightarrow Ds(x))$	premisa
4)	$((L(a) \rightarrow Ds(a))$	particularización universal de 3)
5)	$(L(a) \wedge M(a))$	2), conmutatividad de $\wedge$
6)	$L(a)$	5), simplificación
7)	$Ds(a)$	4), 6) y Modus ponens
8)	$M(a)$	2), simplificación
9)	$(M(a) \wedge Ds(a))$	8), 7) y conjunción
10)	$\exists\, x\ (M(x) \wedge Ds(x))$	generalización existencial de 9)

Ej.: Demuestra que el cuadrado de un número natural impar es impar.

1. **Conocido**:

Def:

Un número natural n es par si existe un número natural k tal que $n = 2k$ y es impar si existe un número natural k tal que $n = 2k + 1$

Prop: Todo número natural es o bien par o bien impar.

Aritmética elemental y propiedades de cierre de las operaciones (suma y producto) en $\mathbb{N}$.

2. **Formalizamos lo que nos piden demostrar:**

Universo de discurso: $\mathbb{N}$
I(n): n es impar
Q(n) : n^2 es impar
Nos piden demostrar que $\forall n\ (I(n) \rightarrow Q(n))$

3. **Vemos que $(I(n) \rightarrow Q(n))$ y aplicamos la regla de infer. de generalización universal.**

1)	$I(n)$	premisa
2)	$\exists\, k \in \mathbb{N}\ (n = 2k + 1)$	1) y def. de impar
3)	$\exists\, k \in \mathbb{N}\ (n^2 = (2k + 1)^2)$	2) y aritmética elemental
4)	$\exists\, k \in \mathbb{N}\ (n^2 = 4k^2 + 4k + 1)$	3) y aritmética elemental
5)	$\exists\, k \in \mathbb{N}\ (n^2 = 2(2k^2 + 2k) + 1)$	4) y aritmética elemental
6)	$(n^2 = 2(2k_1^2 + 2k_1) + 1)$	para un cierto $k_1 \in \mathbb{N}$ por particularización existencial de 5)
7)	$\forall\, k \in \mathbb{N}\ ((2k^2 + 2k) \in \mathbb{N})$	$\mathbb{N}$ es cerrado bajo $+$ y $\times$
8)	$(n^2 = 2k_2 + 1)$ con $k_2 = 2k_1^2 + 2k_1 \in \mathbb{N}$	6) y particularización universal de 7)
9)	$\exists\, k \in \mathbb{N}\ (n^2 = 2k + 1)$	generalización existencial de 8)
10)	$Q(n)$	def. de impar

Luego queda probado $(I(n) \rightarrow Q(n))$ y por tanto $\forall n\ (I(n) \rightarrow Q(n))$, por generalización universal.

Demostración por contrarrecíproco o indirecta

Como $(p \rightarrow q) \sim (\neg q \rightarrow \neg\, p)$ este tipo de demostración consiste en demostrar el contrarrecíproco de la implicación postulada.

Ej.: Demuestra que $\forall\ n \in \mathbb{N}\ (n^2 \text{ par} \rightarrow n \text{ par})$

Sean $P(n)$: n^2 par y $Q(n)$: n par

Para demostrar $(P(n) \rightarrow Q(n))$ pasamos al contrarrecíproco $(\neg\, Q(n) \rightarrow \neg\, P(n))$ pero $\neg\, Q(n) \sim$ n no es par $\sim$ n impar por definición de $\neg$ y el hecho de que los números naturales o bien son pares o bien son impares.

Análogamente $\neg P(n) \sim n^2$ impar

Luego lo que tenemos que demostrar es que $\forall\ n \in \mathbb{N}\ (n \text{ impar} \rightarrow n^2 \text{ impar})$, que es justo lo que acabamos de demostrar en el ejemplo anterior.

Demostración por reducción al absurdo o por contradicción

Se basa en que $(p \to q) \sim ((p \wedge \neg q) \to \perp)$
Este tipo de demostración consiste en suponer la hipótesis y la negación de la conclusión y demostrar que de ello se concluye una contradicción.

Ej.: Demuestra que $\forall\ n \in \mathbb{N}\ (n^2 \text{ par} \to n \text{ par})$ por reducción al absurdo

Sean $P(n)$: n^2 par y $Q(n)$: n par
Suponemos ciertos $P(n)$ y $\neg Q(n)$, pero $\neg\ Q(n) \sim n$ impar y ya hemos demostrado que $\forall\ n \in \mathbb{N}\ (n \text{ impar} \to n^2 \text{ impar})$, lo que nos lleva a $\neg P(n)$, contradiciendo la suposición de que se tiene $P(n)$, completando la demostración.

Demostración por contraejemplo

Se trata de demostrar que cierto enunciado que se refiere a un conjunto M de elementos no es cierto, mostrando un elemento del conjunto M que no lo cumple.

Ej.: ¿ $\forall\, k \in \mathbb{R} \quad ((2k^2 + 2k \in \mathbb{N}) \to (k \in \mathbb{N}))$?

Contraejemplo: $k = -2$