Grado en Ingeniería Informática
Fundamentos matemáticos para la informática
Curso 2009-10

Introducción a la lógica matemática

Lógica es la disciplina que se ocupa de los métodos de razonamiento, suministrando reglas y técnicas que nos permiten decidir si una argumentación , una deducción, es correcta o no. Es la base de todo razonamiento matemático y tiene numerosas aplicaciones en las ciencias de la computación (construcción, escritura y verificación de programas, diseño de circuitos de ordenador, ...), en las ciencias físicas y naturales, en las ciencia sociales y en la vida diaria.

1. Proposiciones

1.1. Definiciones.

Definición. Una *proposición* es una oración declarativa que es verdadera o falsa, pero no ambas cosas a la vez.

Ejemplos. Son proposiciones:

- El río Miño pasa por Ourense.
- $1 - 100 = 99$.
- La suma de dos números positivos es un número positivo.

No son proposiciones:

- ¿Qué hora es?
- Escuchadme
- $x + 2 = 5$

Denotaremos las proposiciones por las letras minúsculas **p, q, r, s, t, u, ...**

Ejemplos.

- p: El río Miño pasa por Ourense
- q: $1 - 100 = 99$

Valor de verdad. El *valor de verdad de una proposición* es *verdadero* si la proposición es verdadera (V) y es *falso* si la proposición es falsa (F).

Ejemplos.

- p es V
- q es F

Lógica proposicional. El área de la lógica que se ocupa de las proposiciones y de las reglas para el cálculo de sus valores de verdad se llama *lógica proposicional o cálculo proposicional.*

Operadores lógicos. Un *operador lógico* es un elemento verbal o escrito que permite formar una proposición (llamada *fórmula* o *proposición molecular* o *proposición compuesta*) a partir de otras (llamadas *proposiciones* o *proposiciones atómicas* o *proposiciones simples*).

Ejemplos.

- Pareces cansado o enfermo.
- Está lloviendo y hace mucho viento.
- No te escucho.
- O vienes al laboratorio regularmente o tienes que realizar una prueba práctica.
- Si no entiendo, pregunto.
- Comeré si, y sólo si, tengo hambre.

Los operadores lógicos más importantes son:

Nombre	Notación	Se lee
Disyunción u O inclusivo	$\vee$	o
Conjunción	$\wedge$	y
Negación	$\neg$	no
O exclusivo	$\oplus$	o ... o ...
Implicación	$\rightarrow$	si ... entonces ...
Bicondicional o doble implicación	$\leftrightarrow$	... si, y sólo si, ...

Ejercicios. Expresa las proposiciones compuestas anteriores utilizando proposiciones simples y conectores lógicos.

1.2. Tablas de verdad. Una *tabla de verdad* de una proposición compuesta es una tabla que da los valores de verdad (V ó F) de la proposición en función de los valores de verdad (V ó F) de sus proposiciones componentes atómicas. A continuación describimos las tablas de verdad de los operadores lógicos.

Negación ($\neg$). Si p es una proposición, entonces $\neg p$ (se lee "no p") es la proposición "no se cumple p".

p	$\neg p$
V	F
F	V

Ejemplos.

- p: Hoy es lunes, $\neg p$: Hoy no es lunes
- p: 2+5 =7, $\neg p$: $2 + 5 \neq 7$

Conjunción ($\wedge$). Si p y q son dos proposiciones, entonces $p \wedge q$ (se lee "p y q") es la proposición "se cumplen p y q".

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo. p: Hoy es lunes, q: Hoy Llueve, $p \wedge q$: Hoy es lunes y llueve

La proposición $p \wedge q$ sólo es verdadera los lunes con lluvia.

Disyunción ($\vee$). Si p y q son dos proposiciones, entonces $p \vee q$ (se lee "p o q") es la proposición "se cumple p o se cumple q o ambas".

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo. $p \vee q$: Hoy es lunes u hoy llueve.

La proposición $p \vee q$ sólo es falsa los días que ni son lunes ni llueve.

O exclusivo ($\oplus$). Si p y q son dos proposiciones, entonces $p \oplus q$ (se lee "o p o q") es la proposición "se cumple p o se cumple q, pero no ambas".

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

Ejemplo. $p \oplus q$: U hoy es lunes u hoy llueve.

La proposición $p \oplus q$ sólo es falsa los días que ni son lunes ni llueve y los lunes que llueve.

Implicación ($\rightarrow$). Si p y q son dos proposiciones, entonces $p \rightarrow q$ (se lee "si p, entonces q", "p es suficiente para q", "p implica q", "q es necesaria para p" o "q se deduce de p") es la proposición "si p es verdadera, entonces q también". A p se le llama *hipótesis*, *condición suficiente* o *premisa* y a q *conclusión*, *condición necesaria*, *tesis* o *consecuencia*.

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Ejemplo. p: Hace frío, q: Enciendo la calefacción, $p \rightarrow q$: Si hace frío, enciendo la calefacción.

La proposición $p \rightarrow q$ sólo es falsa si hace frío y no enciendo la calefacción.

Recíproca y contra-recíproca. La implicación $q \rightarrow p$ se llama *recíproca* de $p \rightarrow q$ y la *contra-recíproca* de $p \rightarrow q$ es $\neg q \rightarrow \neg p$.

p	q	$q \rightarrow p$
V	V	V
V	F	V
F	V	F
F	F	V

p	q	$\neg q \rightarrow \neg p$
V	V	V
V	F	F
F	V	V
F	F	V

En la Sección 2 veremos que una implicación y su contra-recíproca son equivalentes.

Ejemplo. $q \rightarrow p$: Si enciendo la calefacción, entonces hace frío

La proposición $q \rightarrow p$ sólo es falsa si enciendo la calefacción y no hace frío.

$\neg q \rightarrow \neg p$: Si no enciendo la calefacción, entonces no hace frío.

La proposición $\neg q \to \neg p$ sólo es falsa si hace frío y no enciendo la calefacción.

Doble implicación ($\leftrightarrow$). Si p y q son dos proposiciones, entonces $p \leftrightarrow q$ (se lee "p si, y sólo si, q", "p es necesario y suficiente para q" o "si p, entonces q, y recíprocamente") es la proposición "se cumple p si, y sólo si, se cumple q".

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo. p: Supero la prueba, q: Estudio, $p \leftrightarrow q$: Supero la prueba si, y sólo si, estudio.

Observación. Combinando operadores lógicos, paréntesis y proposiciones moleculares es posible formar otras proposiciones compuestas y determinar sus valores de verdad utilizando las tablas de verdad.

Ejemplo. $(p \to q) \wedge (q \to p)$

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

1.3. Tautologías, contradicciones y contingencias. Una proposición molecular que siempre es verdadera independientemente de los valores de verdad de las fórmulas atómicas que la componen es una *tautología*; si siempres es falsa, se llama *contradicción.* Y si no es ni tautología ni contradicción se llama *contingencia.*

La tabla de verdad de una tautología únicamente tiene valores verdaderos en su última columna, la de una contradicción valores falsos, y la de una contingencia valores falsos y verdaderos.

Ejemplo.

- $p \vee \neg p$ es una tautología.

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

- $p \wedge \neg p$ es una contradicción.

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

- $p \rightarrow q$ es una contingencia.

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Otras tautologías. Las siguientes implicaciones son tautologías y se usarán en la demostración de resultados en matemáticas y ciencias de la computación (véase la Sección 4).

- $(p \wedge q) \rightarrow p$
- $p \rightarrow (p \vee q)$
- $\neg p \rightarrow (p \rightarrow q)$
- $(p \wedge (p \rightarrow q)) \rightarrow q$
- $\neg(p \rightarrow q) \rightarrow p$
- $(\neg p \wedge (p \vee q)) \rightarrow q$
- $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
- $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Ejercicio. Realizar las tablas de verdad de las anteriores tautologías.

1.4. Ejercicios.

(1) ¿Cuáles de estas frases son proposiciones? ¿Cuál es el valor de verdad de aquellas que son proposiciones?
- Lugo es la capital de Galicia
- Madrid es la capital de España
- $2 + 3 = 5$
- $5 + 7 = 10$
- $x + 2 = 11$
- Responde a esta pregunta
- $x + y = y + x$ para todo par de números reales x e y.

(2) ¿Cuál es la negación de cada uno de estos enunciados?
- Hoy es jueves
- No hay polución en Ourense
- $2 + 1 = 3$
- El verano de Ourense es cálido y soleado.

(3) Sean p y q los enunciados: p: Compré un billete de lotería esta semana, q: gané el bote de un millón de euros del viernes. Expresa cada una de las siguientes fórmulas en lenguaje natural: $\neg p$, $p \vee q$, $p \rightarrow q$, $p \wedge q$, $p \leftrightarrow q$, $\neg p \rightarrow \neg q$, $\neg p \wedge \neg q$, $\neg p \vee (p \wedge q)$

(4) Sean p y q los enunciados: p: Conduces a más de 100 km por hora, q: Te multan por exceso de velocidad. Escribe los enunciados siguientes usando p y q y conectivos lógicos.
- No conduces a más de 100 km por hora
- Conduces a más de 100 km por hora, pero no te multan por exceso de velocidad
- Te multarán por exceso de velocidad si conduces a más de 100 km por hora
- Si no conduces a más de 100 km por hora no te multarán por exceso de velocidad
- Conducir a más de 100 km por hora es suficiente para que te multen por exceso de velocidad
- Te multan por exceso de velocidad pero no conduces a más de 100 km por hora
- Siempre que te multan por exceso de velocidad conduces a más de 100 km por hora.

(5) Determina si cada proposición es verdadera o falsa.
- $5 < 9$ y $9 < 7$.
- No es cierto que ($5 < 9$ y $9 < 7$).
- $5 < 9$ o no es cierto que ($9 < 7$) y ($5 < 7$).

(6) Determina si estas bicondicionales son verdaderas o falsas.
- $2 + 2 = 4$ si, y sólo si, $1 + 1 = 2$
- $1 + 1 = 2$ si, y sólo si, $2 + 3 = 4$
- Es invierno si, y sólo si, no es primavera, verano u otoño
- $1 + 1 = 3$ si, y sólo si, los cerdos vuelan
- $0 > 1$ si, y sólo si, $2 > 1$

(7) Determina si estas implicaciones son verdaderas o falsas.
- Si $1 + 1 = 2$, entonces $2 + 2 = 5$
- Si $1 + 1 = 3$, entonces $2 + 2 = 4$
- Si $1 + 1 = 3$, entonces $2 + 2 = 5$
- $1 + 1 = 3$ si los cerdos vuelan
- Los cerdos vuelan si $1 + 1 = 3$
- Si $1 + 1 = 2$, entonces los cerdos vuelan
- Si $2 + 2 = 4$, entonces $1 + 2 = 3$

(8) Determina el valor de verdad de la recíproca y contra-recíproca de cada una de las implicaciones del ejercicio anterior.

(9) Escribe cada uno de estos enunciados de la forma "si p, entonces q".

- Es necesario lavar el coche del jefe para ascender
- Viento del sur implica deshielo en primavera
- Una condición suficiente para que la garantía sea válida es que hayas comprado el ordenador hace menos de un año
- A Guillermo siempre se le pilla cuando hace trampas
- Puedes acceder a la página web si pagas una cuota de suscripción
- Ser elegido es consecuencia de conocer a la gente adecuada
- Carol se marea siempre que monta en una barca

(10) Escribe cada uno de estos enunciados de la forma "p si , y sólo si, q".
- Si hace calor fuera, te compras un cucurucho de helado, y si te compras un cucurucho de helado, hace calor fuera
- Para ganar el concurso es necesario y suficiente tener el número ganador
- Ascenderás sólo si tienes contactos, y tienes contactos sólo si asciendes
- Si ves televisión, tu mente se empobrecerá, y recíprocamente
- El tren llega con retraso exactamente aquellos días que tengo que tomarlo

(11) Enuncia la recíproca y la contra-recíproca de cada una de estas implicaciones.
- Si llueve esta noche, me quedaré en casa.
- Voy a la playa siempre que el día amanezca soleado.
- Cuando me acuesto tarde es necesario que duerma hasta mediodía.

(12) Construye las tablas de verdad para cada una de estas fórmulas.

$(p \vee \neg q) \rightarrow q$

$(p \vee q) \rightarrow (p \wedge q)$

$(p \vee q) \rightarrow (p \oplus q)$

$(p \vee q) \oplus (p \wedge q)$

$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$

$(p \wedge q) \vee r$

$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

$(p \rightarrow q) \rightarrow (q \rightarrow p)$

$(p \oplus q) \rightarrow (p \wedge q)$

$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$

$(p \oplus q) \rightarrow (p \oplus \neg q)$

$(p \wedge q) \vee \neg r$

(13) Una antigua leyenda siciliana dice que el barbero de una remota ciudad, a la que sólo se puede llegar a través de un peligroso camino de montaña, afeita a aquellas personas y sólo a aquellas personas, que no se afeitan a sí mismas. ¿Puede existir tal barbero?

(14) Expresa las siguientes especificaciones del sistema utilizando las proposiciones p: "El mensaje es revisado para buscar algún

virus", y q:"El mensaje fue enviado desde un sistema desconocido ", junto con conectivos lógicos.

- "El mensaje se revisa para buscar algún virus siempre que haya sido enviado desde un sistema desconocido"
- "El mensaje fue enviado desde un sistema desconocido, pero no se revisó para buscar ningún virus"
- "Es necesario revisar el mensaje para buscar algún virus siempre que haya sido enviado desde un sistema desconocido"
- "Cuando el mensaje no sea enviado desde un sistema desconocido no se revisa para buscar ningún virus"

(15) Demostrar que cada una de estas implicaciones es una tautología.

- $(p \wedge q) \to (p \to q)$
- $\neg(p \to q) \to \neg q$
- $[(p \vee q) \wedge (p \to r) \wedge (q \to r)] \to r$

2. Equivalencias lógicas

2.1. Definiciones.

Fórmulas lógicamente equivalentes. Dos fórmulas p y q son *lógicamente equivalentes* si $p \leftrightarrow q$ es una tautología. Es decir, p y q son simultáneamente verdaderas o falsas. Se denota $p \equiv q$.

Ejemplo. Las fórmulas $p \to q$ y $\neg p \vee q$ son lógicamente equivalentes, *i. e.*, $p \to q \equiv \neg p \vee q$.

p	q	$p \to q$	$\neg p$	$\neg p \vee q$
V	V	V	F	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

2.2. Equivalencias lógicas relativas a $\neg$, $\vee$ y $\wedge$. Sean p, q y r proposiciones.

- Identidad: $p \wedge V \equiv p$, $p \vee F \equiv p$
- Dominación: $p \vee V \equiv V$, $p \wedge F \equiv F$
- Idempotentes: $p \vee p \equiv p$, $p \wedge p \equiv p$
- Doble negación: $\neg(\neg p) \equiv p$
- Conmutativas: $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$
- Absorción: $p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$
- Asociativas: $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

- Distributivas: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- De Morgan: $\neg(p \vee q) \equiv \neg p \wedge \neg q$, $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Ejercicio. Demostrar las equivalencias anteriores.

Ejemplo. Demostrar: $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$

$$\begin{aligned} \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q)) \\ &\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) \\ &\equiv \neg p \wedge (p \vee \neg q) \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\ &\equiv F \vee (\neg p \wedge \neg q) \\ &\equiv (\neg p \wedge \neg q) \end{aligned}$$

2.3. Equivalencias lógicas relativas a implicaciones. Sean p, q y r proposiciones.

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $\neg(p \to q) \equiv p \wedge \neg q$
- $p \vee q \equiv \neg p \to q$
- $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
- $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$
- $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
- $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Ejercicio. Demostrar las equivalencias anteriores.

2.4. Equivalencias lógicas relativas a dobles implicaciones. Sean p y q proposiciones.

- $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
- $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
- $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
- $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$
- $\neg(p \leftrightarrow q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

Ejercicio. Demostrar las equivalencias anteriores.

2.5. Ejercicios.

(1) Demuestra que $p \to (q \to r)$ y $(p \to q) \to r$ no son equivalentes.
(2) Demuestra que $\neg(p \oplus q) \equiv p \leftrightarrow q$
(3) Demuestra que $\neg(p \leftrightarrow q) \not\equiv (p \leftrightarrow q)$
(4) Demuestra que $\neg p \to (q \to r) \equiv q \to (p \vee r)$

(5) La siguiente frase se ha tomado de una especificación de un sistema de telefonía: "Si la base de datos del directorio está abierta, el monitor se pone en estado cerrado si el sistema no está en estado inicial ". Encuentra una especificación equivalente, más fácil de entender, que incluya disyunciones o negaciones, pero no implicaciones.

3. Predicados y cuantificadores

La afirmación $x + 2 = 5$ no es una proposición, ya que el hecho de que sea verdadera o falsa depende del valor de x. Sin embargo, muchas afirmaciones en matemáticas y en computación son de este tipo.

3.1. Predicados. Una sentencia P que alude a una o varias variables $X_1, X_2, \ldots, X_n$ se llama *predicado* o *función proposicional* y se denota $P(X_1, X_2, \ldots, X_n)$.

Ejemplos.

- $P(X) : X > 3$, donde X representa a cualquier número real.
- $Q(X, Y) : X + Y = 5$, donde X e Y representan a dos números reales cualesquiera.

Universo del predicado. Todo predicado $P(X)$ se puede considerar como una aplicación P que asocia una proposición $P(x)$ a cada elemento x de un cierto conjunto llamado *universo del predicado* o *dominio del predicado.*

Ejemplos.

- El universo de P es el conjunto de los números reales $\mathbb{R}$
- El universo de Q es el conjunto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Valor de verdad de un predicado. El valor de verdad de un predicado puede variar ya que depende de la selección de las variables $X_1, X_2, \ldots, X_n$. Cuando las variables de una función proposicional tomen valores concretos el resultado será una proposición verdadera o falsa.

Ejemplos.

- $P(4)$ es verdadera y $P(2)$ es falsa.
- $Q(0, 5)$ es verdadera, $Q(-1, 6)$ es verdadera y $Q(0, \frac{1}{2})$ es falsa.

A partir de ahora y, para simplificar, consideraremos predicados $P(X)$ que dependen únicamente de una variable X.

Operadores lógicos y predicados. Al igual que las proposiciones, los predicados que se apoyan en un mismo universo pueden combinarse mediante operadores lógicos. Por ejemplo:

- El predicado $\neg P(X)$ que asocia a cada elemento x del dominio de P la negación de la proposición $P(x)$, *i. e.*, $\neg P(x)$.
- El predicado $(P \vee Q)(X)$ que asocia a cada elemento x del dominio de P y de Q la conjunción de las proposiciones $P(x)$ y $Q(x)$, *i. e.*, $P(x) \vee Q(x)$.
- El predicado $(P \wedge Q)(X)$ que asocia a cada elemento x del dominio de P y de Q la disyunción de las proposiciones $P(x)$ y $Q(x)$, *i. e.*, $P(x) \wedge Q(x)$.

Ejemplos. Sean P y Q los siguientes predicados con dominio el conjunto de los números naturales:

$$P(X) : X \text{ es un número par}$$
$$Q(X) : X \text{ es el cuadrado de un número natural}$$

- $\neg P(X) : X$ no es un número par
- $(P \vee Q)(X) : X$ es par o es el cuadrado de un número natural.
- $(P \wedge Q)(X) : X$ es par y es el cuadrado de un número natural

3.2. Cuantificadores. Cuando a todas las variables de una proposición proposicional se le han asignado valores, la sentencia resultante se convierte en una proposición con un determinado valor de verdad (V ó F). Pero hay otra forma importante de conseguir una proposición a partir de un predicado: la cuantificación.

Sea $P(X)$ un predicado en la variable X.

Cuantificación universal. La *cuantificación universal* de $P(X)$ es la proposición "$P(x)$ es verdadera para todo los valores x del dominio".

Se denota $\forall x\, P(x)$ y se lee "para todo x $P(x)$", "para cada x $P(x)$" o "para cualquier x $P(x)$". Y para especificar el universo U del predicado escribimos $\forall x$ en U, $P(x)$ $(\forall x \in U,\, P(x))$

El símbolo $\forall$ se llama *cuantificador universal*.

Ejemplos.

- $\forall x \in \mathbb{N},\, P(x)$: todo número natural es par

- $\forall x \in \mathbb{N}, Q(x)$: todo número natural es el cuadrado de un número natural

Valores de verdad de la cuantificación universal. Para mostrar que una proposición de la forma $\forall x\, P(x)$ es falsa, sólo necesitamos encontrar un valor x del dominio para el cual $P(x)$ sea falsa. Este valor x se llama *contraejemplo* de la sentencia $\forall x\, P(x)$. Y para mostrar que $\forall x\, P(x)$ es verdadera hay que probar que $P(x)$ es verdadera para todos los valores x en el dominio.

Ejemplos.

- $\forall x \in \mathbb{N}, P(x)$ es falsa ya que el número 3 es natural y no es par.
- $\forall x \in \mathbb{N}, Q(x)$ es falsa ya que el número 3 es natural y no es el cuadrado de un número natural.

Ejercicio. Determina el valor de verdad de $\forall x \in \mathbb{R}, x > 1 \Rightarrow x+1 > 1$.

Cuantificación existencial. La *cuantificación existencial* de $P(X)$ es la proposición "existe un elemento x en el dominio tal que $P(x)$ es verdadera".

Se denota $\exists x\, P(x)$ y se lee "hay un x tal que $P(x)$", "hay al menos un x tal que $P(x)$" o "para algún x $P(x)$". Y para especificar el universo U del predicado escribimos $\exists x$ en U, $P(x)$ ($\exists x \in U$, $P(x)$)

El símbolo $\exists$ se llama *cuantificador existencial*.

Ejemplos.

- $\exists x \in \mathbb{N}, P(x)$: existe (al menos) un número natural que es par
- $\exists x \in \mathbb{N}, Q(x)$: existe (al menos) un número natural que es el cuadrado de un número natural

Valores de verdad de la cuantificación existencial. Para mostrar que una proposición de la forma $\exists x\, P(x)$ es falsa, hay que mostrar que $P(x)$ es falsa para todos los valores x del dominio; y para mostrar que es verdadera hay que encontrar un valor x en el dominio para el cual $P(x)$ sea verdadera.

Ejemplos.

- $\exists x \in \mathbb{N}, P(x)$ es verdadera ya que el número 2 es natural y par

- $\exists x \in \mathbb{N}$, $Q(x)$ es verdadera ya que el número 4 es natural y $4 = 2^2$

Ejercicio. Determina el valor de verdad de $\exists x \in \mathbb{R}$, $\frac{1}{x^2+1} > 1$

Cuantificadores anidados. Cuando un predicado depende de varias variables se pueden utilizar cuantificadores (universal y/o existencial) para cada una de las variables. Si $P(X, Y)$ es un predicado se presentan las siguientes situaciones:

- $\forall x\, \forall y\, P(x, y)$: "para todo par x, y $P(x, y)$ es verdadera"
- $\exists x\, \exists y\, P(x, y)$: "existe un par x, y para el cual $P(x, y)$ es verdadera"
- $\forall x\, \exists y\, P(x, y)$: "para todo x hay un y para el cual $P(x, y)$ es verdadera"
- $\exists x\, \forall y\, P(x, y)$: "existe un x para el cual $P(x, y)$ es verdadera para todo y"

Para cada una de las variables se puede especificar el universo.

Ejemplos. Supongamos que el dominio de las variables reales x e y consiste en todos los números reales

- $\forall x \in \mathbb{R}$, $\forall y \in \mathbb{R}$, $(x + y = y + x)$: la suma de dos números reales es conmutativa
- $\exists x \in \mathbb{R}$, $\forall y \in \mathbb{R}$, $(x + y = y)$: existencia del elemento neutro para la suma (x es el 0)
- $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $(x + y = y + x = 0)$: existencia del elemento opuesto para la suma (y es $-x$)
- $\exists x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $(x \cdot y = \frac{x}{y} = -1)$

Ejercicio. Determinar el valor de verdad de cada una de las proposiciones anteriores.

Ejercicio. Expresar la proposición "existe (al menos) un número natural que es el cuadrado de un número natural" utilizando dos variables.

Conmutatividad de los cuantificadores anidados.

- $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y) \equiv \forall (x, y) P(x, y)$
- $\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y) \equiv \exists (x, y) P(x, y)$
- Cuidado!: $\exists y \forall x P(x, y) \not\equiv \forall x \exists y P(x, y)$

Ejemplo. Sea $P(X,Y)$ la sentencia "$X+Y=0$", con universo el conjunto de los números reales.

- $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, P(x,y)$: hay un número real y tal que para todo número real x se verifica que $x+y=0$. Esta sentencia es falsa.
- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, P(x,y)$: para todo número real x existe un número real y tal que $x+y=0$. Esta sentencia es verdadera (y sería $-x$).

3.3. Álgebra de predicados. El *álgebra de predicados* se ocupa de las reglas que relacionan los cuantificadores entre sí y con los conectores lógicos.

Negación.

- $\neg(\forall x,\ P(x)) \equiv \exists x,\ \neg P(x)$
- $\neg(\exists x,\ P(x)) \equiv \forall x,\ \neg P(x)$

Ejemplos. Sea $P(X)$ el predicado "X ha cursado una asignatura de francés" con universo todos los alumnos de 1º de la E.S.E.I.

- $\neg(\forall x,\ P(x))$: hay al menos un alumno que no ha cursado una asignatura de francés
- $\neg(\exists x,\ P(x))$: ningún alumno ha cursado una asignatura de francés.

Ejercicios. Negar las siguientes proposiciones:

- $\exists x \in \mathbb{R},\ \frac{1}{x^2+1} > 1$
- $\forall x \in \mathbb{R},\ x^2 > x$

Disyunción.

- $\exists x(P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x))$
- Cuidado!: $\forall x(P(x) \vee Q(x)) \not\equiv (\forall x P(x)) \vee (\forall x Q(x))$

Ejemplos. Consideremos los siguientes predicados con universo el alfabeto:

$$P(X) : X \text{ es una vocal}$$
$$Q(X) : X \text{ es una consonante}$$

- $\forall x(P(x) \vee Q(x))$: Toda letra es vocal o consonante
- $(\forall x P(x)) \vee (\forall x Q(x))$: Todas las letras son vocales o todas las letras son consonantes.

Conjunción.

- $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$
- Cuidado!: $\exists x(P(x) \wedge Q(x)) \not\equiv (\exists x P(x)) \wedge (\exists x Q(x))$

Ejemplos.

- $\exists x(P(x) \wedge Q(x))$: Existe una letra que es vocal y consonante.
- $(\exists x P(x)) \wedge (\exists x Q(x))$: Existe una letra que es vocal y existe una letra que es consonante.

Existencia única. La *unicidad* de la cuantificación existencial de $P(X)$ es la proposición "existe un único elemento x en el dominio tal que $P(x)$ es verdadera".

Se denota $\exists^{\bullet} x\, P(x)$ o $\exists! x\, P(x)$ y se lee "hay un único x tal que $P(x)$".

- $\exists^{\bullet} x P(x) \equiv \exists x P(x) \wedge [\forall y \forall z (P(y) \wedge P(z)) \rightarrow (y = z)]$

Ejemplos. Sea $P(X) = X + X = 0$ con dominio el conjunto de los números reales

- $\exists^{\bullet} x \in \mathbb{R},\ P(x)$: existe un único número real x tal que $x+x = 0$. La sentencia es verdadera y x sería el número 0.

Implicaciones.

- $\exists x(P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \exists x Q(x)$
- $\exists x P(x) \rightarrow \forall x Q(x) \equiv \forall x(P(x) \rightarrow Q(x))$

Tautologías. Son tautologías:

- $(\forall x P(x)) \vee (\forall x Q(x)) \rightarrow \forall x(P(x) \vee Q(x))$
- $\exists x(P(x) \wedge Q(x)) \rightarrow \exists x P(x) \wedge \exists x Q(x)$

3.4. Ejercicios.

(1) Denotemos por $P(X)$ la sentencia la palabra X contine la letra a. ¿Cuáles son los valores de verdad siguientes?
   - P(naranja)
   - P(limón)
   - P(verdadero)
   - P(falsa)

(2) Sea $N(X)$ la sentencia "X ha visitado Alemania", donde el dominio de X consiste en todos los estudiantes de tu clase. Expresa cada una de estas cuantificaciones en lenguaje natural:
   - $\exists x\, N(x)$
   - $\forall x\, N(x)$
   - $\neg\exists x\, N(x)$
   - $\exists x\, \neg N(x)$
   - $\neg\forall x\, N(x)$
   - $\forall x\, \neg N(x)$

(3) Traduce estas sentencias a lenguaje natural donde $C(X)$ es "X es un cómico" y $F(X)$ es "X es divertido" y el dominio consiste en todas las personas.
- $\forall x\,(C(x) \to F(x))$
- $\exists x\,(C(x) \to F(x))$
- $\forall x\,(C(x) \wedge F(x))$
- $\exists x\,(C(x) \wedge F(x))$

(4) Sea $C(X)$ la sentencia "X tiene un gato", $D(X)$ "X tiene un perro", y $F(X)$ "X tiene un hámster". Expresa cada una de las siguientes sentencias en términos de $C(X)$, $D(X)$ y $F(X)$, cuantificadores y conectivos lógicos. El dominio para los cuantificadores consiste en todos los estudiantes de tu clase.
- Un estudiante de tu clase tiene un gato, un perro y un hámster.
- Todos los estudiantes de tu clase tienen un gato, un perro o un hámster.
- Algún estudiante de tu clase tiene un gato y un hámster, pero no un perro.
- Ningún estudiante de tu clase tiene un gato, un perro y un hámster.
- Para cada uno de los tres animales, gatos, perros y hámsters, hay un estudiante de tu clase que tiene uno de esos animales como mascota.

(5) Sea $Q(X)$ la sentencia $X + 1 > 2X$. Si el dominio consiste en todos los enteros, ¿cuáles son los valores de verdad?
- $Q(0)$
- $\exists x\, Q(x)$
- $\forall x\, \neg Q(x)$
- $Q(-1)$
- $\forall x\, Q(x)$
- $Q(1)$
- $\exists x\, \neg Q(x)$

(6) Halla un contraejemplo, si es posible, a estas sentencias universalmente cuantificadas.
- $\forall x \in \mathbb{Z},\ (x^2 \geq x)$
- $\forall x \in \mathbb{Z},\ (x = 1)$
- $\forall x \in \mathbb{Z},\ (x > 0 \vee x < 0)$

(7) ¿Cuáles son los valores de verdad?
- $\exists! x \in \mathbb{Z},\ (x > 1)$
- $\exists! x \in \mathbb{Z},\ (x + 3 = 2x)$
- $\exists! x \in \mathbb{Z},\ (x^2 = 1)$
- $\exists! x \in \mathbb{Z},\ (x = x + 1)$

(8) Determina el valor de verdad de las siguientes proposiciones. El universo de las variables x e y es $\mathbb{R}$.
- Para cada x, $(x^2 > x)$
- $\forall x,\ (x > 1 \Rightarrow x^2 > x)$
- $\forall x,\ \forall y,\ x^2 < y + 1$
- $\exists x,\ \forall y,\ x^2 < y + 1$
- Para alguna x, $(x^2 > x)$
- $\exists x,\ (x > 1 \Rightarrow x^2 > x)$
- $\forall x,\ \exists y,\ x^2 < y + 1$
- $\exists x,\ \exists y,\ x^2 < y + 1$
- $\forall x,\ \forall y,\ (x < y \Rightarrow x^2 < y^2)$.
- $\forall x,\ \exists y,\ (x < y \Rightarrow x^2 < y^2)$.
- $\exists x,\ \forall y,\ (x < y \Rightarrow x^2 < y^2)$.

- $\exists x$, $\exists y$, $(x < y \Rightarrow x^2 < y^2)$.

(9) Escribe la negación de cada una de las proposiciones del ejercicio anterior.

(10) Traduce estas especificaciones de sistema a lenguaje natural, donde $F(p)$ es "La impresora p está fuera de servicio", $B(p)$ es "La impresora p está ocupada", $L(j)$ es "El trabajo de impresión j se ha perdido" y $Q(j)$ es "El trabajo de impresión está en cola".
- $\exists p\,(F(p) \wedge B(p)) \to \exists j\,L(j)$
- $\forall p\,B(p) \to \exists j\,Q(j)$
- $\exists j\,(Q(j) \wedge L(j)) \to \exists p\,F(p)$
- $(\forall p\,B(p) \wedge \forall j\,Q(j)) \to \exists j\,L(j)$

(11) Sea $Q(X, Y)$ la sentencia "X ha enviado un correo electrónico a Y", donde el dominio tanto para X como para Y consiste en todos los estudiantes de tu clase. Expresa cada una de estas cuantificaciones en lenguaje natural.
- $\exists x\,\exists y\,P(x, y)$
- $\forall x\,\exists y\,P(x, y)$
- $\forall y\,\exists x\,P(x, y)$
- $\exists x\,\forall y\,P(x, y)$
- $\exists y\,\forall x\,P(x, y)$
- $\forall x\,\forall y\,P(x, y)$

(12) Sea $F(X, Y)$ la sentencia "X puede engañar a Y", donde el dominio tanto para X como para Y consiste en todas las personas del mundo. Utiliza cuantificadores para expresar cada una de las siguientes sentencias.
- Todo el mundo puede engañar a Juan
- María puede engañar a todo el mundo
- Todo el mundo puede engañar a alguien
- No hay nadie que pueda engañar a todo el mundo
- Todo el mundo puede ser engañado por alguien
- Nadie puede engañar a Juan y a María
- Paula puede engañar exactamente a dos personas
- Hay exactamente una persona a quien todo el mundo puede engañar
- Nadie puede engañarse a sí mismo

(13) Determina el valor de verdad de cada una de estas sentencias.
- $\forall n \in \mathbb{Z}$, $\exists m \in \mathbb{Z}$, $(n^2 < m)$
- $\forall n \in \mathbb{Z}$, $\exists m \in \mathbb{Z}$, $(n + m = 0)$
- $\exists n \in \mathbb{Z}$, $\exists m \in \mathbb{Z}$, $(n^2 + m^2 = 5)$
- $\exists n \in \mathbb{Z}$, $\forall m \in \mathbb{Z}$, $(n < m^2)$
- $\exists n \in \mathbb{Z}$, $\forall m \in \mathbb{Z}$, $(nm = m)$

4. Razonamiento deductivo

4.1. Reglas de inferencia. Los argumentos basados en tautologías son métodos de razonamiento universalmente correctos. Son las *reglas de inferencia.* Las reglas de inferencia se basan en tautologías de la forma

$$\text{Hipótesis } 1 \wedge \text{Hipótesis } 2 \wedge \ldots \rightarrow \text{Conclusión}$$

Usaremos la siguiente notación para las reglas de inferencia:

$$\begin{array}{c} \text{Hipótesis 1} \\ \text{Hipótesis 2} \\ \ldots \\ \hline \therefore \text{Conclusión} \end{array}$$

El símbolo $\therefore$ se lee "por lo tanto", "luego", etc.

Regla	Tautología	Nombre
$\begin{array}{c} p \\ \hline \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	adición
$\begin{array}{c} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \rightarrow p$	simplificación
$\begin{array}{c} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow p \wedge q$	conjunción
$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	modus ponens
$\begin{array}{c} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	modus tollens
$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	silogismo hipotético
$\begin{array}{c} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$((p \vee q) \wedge (\neg p)) \rightarrow q$	silogismo disyuntivo
$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	ley de resolución
$\begin{array}{c} p \leftrightarrow q \\ \hline \therefore (p \rightarrow q) \wedge (q \rightarrow p) \end{array}$	$(p \leftrightarrow q) \rightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$	
$\begin{array}{c} p \rightarrow q \\ q \rightarrow p \\ \hline \therefore p \leftrightarrow q \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow p)) \rightarrow (p \leftrightarrow q)$	
$\begin{array}{c} p \rightarrow q \\ \hline \therefore \neg q \rightarrow \neg p \end{array}$	$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$	

Ejemplos. Determinar en qué regla de inferencia se basan los siguientes argumentos:

- Si hace frío, enciendo la calefacción. Hace frío, luego enciendo la calefacción.
- Hace frío. Por tanto, hace frío o llueve.
- Hace frío y llueve. Por tanto, llueve.
- Hace frío. Llueve. Por tanto, hace frío y llueve.
- Si hace frío, enciendo la calefacción. Si enciendo la calefacción, el consumo de electricidad aumenta. Si hace frío, el consumo de electricidad aumenta.
- Si hace frío, enciendo la calefacción. No enciendo la calefacción, luego no hace frío.
- Llueve o hace frío. No hace frío. Por lo tanto, llueve.
- Voy al cine o voy a la piscina. No voy al cine o voy a la playa. Por lo tanto, voy a la piscina o voy a la playa
- Bebo si, y sólo si, tengo sed. Por lo tanto, si bebo, tengo sed y si tengo sed, bebo.
- Si bebo, tengo sed y si tengo sed, bebo. Por lo tanto, bebo si, y sólo si, tengo sed.

Reglas de inferencia para sentencias cuantificadas. Si $P(X)$ es un predicado y c un elemento en el universo de P, se cumplen las siguientes reglas de inferencia.

Regla	Nombre
$\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$	particularización universal
$\dfrac{P(c),\ c \text{ arbitrario}}{\therefore\ \forall x\, P(x)}$	generalización universal
$\dfrac{\exists x\, P(x)}{\therefore\ P(c), \text{ para algún elemento } c}$	particularización existencial
$\dfrac{P(c), \text{ para algún elemento } c}{\therefore\ \exists x\, P(x)}$	generalización existencial

Estas reglas de inferencia se usan con frecuencia en los argumentos matemáticos, muchas veces sin mencionarlas explícitamente.

Ejemplos. Determinar en qué regla de inferencia se basan los siguientes argumentos:

- Todos los alumnos de matemática discreta están matriculados en ingeniería informática. María es una alumna de matemática discreta. Entonces María está matriculada en ingeniería informática.
- Un estudiante de esta clase no ha leído el libro. Luego, alguien no ha leído el libro.

4.2. Razonamientos válidos y falacias.

Razonamientos válidos. Un argumento $P_1 \wedge P_2 \wedge \ldots \wedge P_n \to Q$ es *válido* si siempre que $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ sean todas verdaderas, entonces Q también sea verdadera. Observa que no decimos que la conclusión Q sea verdadera; sino que si se garantizan las hipótesis, entonces se tiene garantizada la conlusión. Un argumento es válido debido a su foma, no a su contenido.

Para evitar razonamientos incorrectos, se debe mostrar en cada paso cómo se llega de un razonamiento a otro, razonando explícitamente cada paso que se ha dado.

Ejemplos. Determinar si los siguientes argumentos son válidos:

- $\begin{array}{c} \text{p} \to \text{q} \\ \underline{\quad \text{p} \quad} \\ \therefore \text{q} \end{array}$
- Fumar es saludable. Si fumar es saludable, entonces los cigarrillos son recetados por los médicos. Entonces los cigarrillos son recetados por los médicos.
- Si bajan los impuestos, entonces se elevan los ingresos. Los ingresos se elevan. Entonces bajan los impuestos.
- Si $2 = 3$, entonces me comí el sombrero. $2 = 3$. Entonces me comí el sombrero.
- Si fumar es saludable, entonces los cigarrillos son recetados por los médicos. Fumar no es saludable. Entonces los cigarrillos no son recetados por los médicos
- Si $2 = 3$, entonces me comí el sombrero. Me comí el sombrero. Entonces $2 = 3$.

Falacias. Las *falacias* son una forma de razonamiento incorrecto basadas en contingencias.

Algunas falacias frecuentes son:

- Falacia de afirmar la conclusión: $[(p \to q) \wedge q] \to p$
- Falacia de negar la hipótesis: $[(p \to q) \wedge \neg p] \to \neg q$

Ejemplos.

- El segundo ejemplo es la falacia de afirmar la conclusión
- El tercer ejemplo es la falacia de negar la hipótesis

Ejercicio. Estudiar la validez del siguiente argumento: "Condición suficiente para que yo apruebe es que yo sepa o que el profesor no sea justo. Yo no se y el profesor no es justo. Por lo tanto, suspendo."

4.3. Ejercicios.

(1) ¿Qué reglas de inferencia se han usado en los siguientes argumentos?
   - Los canguros viven en Australia y son marsupiales. Por lo tanto, los canguros son marsupiales.
   - Estamos a más de 40ºC hoy o la polución es peligrosa. Estamos a menos de 40º hoy. Por tanto, la polución es peligrosa.
   - Linda es una excelente nadadora. Si Linda es una excelente nadadora, entonces puede trabajar como salvavidas. Por tanto, Linda puede trabajar como salvavidas.
   - Susana trabajará en una compañía de informática este verano. Por tanto, este verano Susana trabajará en una compañía de informática o deambulará por la playa.
   - Si trabajo toda la noche, podré resolver todos los problemas. Si puedo resolver todos los problemas, entonces entenderé la asignatura. Por tanto, si trabajo toda la noche, entonces entenderé la asignatura.

(2) Para cada uno de estos conjuntos de premisas, ¿qué conclusión o conclusiones se pueden deducir? Explica las reglas de inferencia utilizadas para obtener cada conclusión a partir de las premisas.
   - Si me tomo el día libre, bien llueve o bien nieva. Me tomé el martes o el jueves libre. Hizo sol el martes. No nevó el jueves.

- Si ceno comidas picantes, entonces tengo sueños extraños. Tengo sueños extraños si truena por la noche. No he tenido sueños extraños.
- Soy inteligente o afortunado. No soy afortunado. Si soy afortunado, me tocará la lotería.
- Todo estudiante de ingeniería informática tiene un ordenador. Marcos no tiene un ordenador. Ana tiene un ordenador
- Lo que es bueno para las empresas, lo es para tu país. Lo que es bueno para tu país es bueno para ti. Lo que es bueno para las empresas es que comas compulsivamente.
- Todos los roedores roen su comida. Los ratones son roedores. Los conejos no roen la comida. Los murciélagos no son roedores.

(3) Para cada uno de estos argumentos determina si es válido y explica por qué.
- Todos los estudiantes de la clase entienden lógica. Xavier es un estudiante de la clase. Por tanto, Xavier entiende lógica
- Todos los estudiantes de ingeniería informática cursan matemática discreta. Natacha cursa matemática discreta. Por tanto Natacha es estudiante de ingeniería informática.
- A todos los loros les gusta la fruta. Mi pájaro no es un loro. Por tanto, a mi pájaro no le gusta la fruta.
- Los que comen vegetales todos los días están sanos. Ana no está sana. Por tanto Ana no come vegetales todos los días.

(4) Para cada uno de estos argumentos determina si es válido y explica por qué.
- $$\begin{array}{c} p \to q \\ \neg p \\ \hline \therefore q \end{array}$$
- $$\begin{array}{c} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$
- $$\begin{array}{c} p \wedge \neg p \\ \hline \therefore q \end{array}$$
- $$\begin{array}{c} p \to (q \to r) \\ q \to (p \to r) \\ \hline \therefore (p \vee q) \to r \end{array}$$
- $$\begin{array}{c} (p \to q) \wedge (r \to s) \\ p \vee r \\ \hline \therefore q \vee s \end{array}$$

5. Métodos de demostración

5.1. Definiciones. Un sistema matemático consta de axiomas, definiciones y términos no definidos. Se suponen verdaderos los axiomas; las definiciones se utilizan para crear conceptos nuevos en términos de los ya existentes; algunos términos no se definen de forma explícita, sino que se definen de forma implícita mediante axiomas. Dentro de un sistema matemático es posible deducir teoremas.

Teoremas. Un *teorema* es una sentencia que se puede verificar que es verdadera (*i.e.* su valor de verdad es verdadero). El enunciado de un teorema puede ser de la forma:

- $p \to q$ (recordemos que p es la *hipótesis* y q la *conclusión*)
- $p \leftrightarrow q$
- $\exists x\, P(x)$
- $\forall x\, P(x)$

Ejemplos.

- Si $3n + 2$ es impar, entonces n es impar.
- El entero n impar si, y sólo si, n^2 es un entero impar.
- Existen dos números irracionales x e y tales que x^y es racional
- $\forall n$ con n un número natural positivo, se verifica que $n < 2^n$.

Tipos de teoremas.

- Una *proposición* es un teorema de menor importancia en el discurso. Cuando tenemos varios resultados y, queremos resaltar la importancia de uno de elllos, se llama teorema y los otros proposiciones.
- Un *lema* es un teorema sencillo utilizado en la demostración de otros teoremas.
- Un *corolario* es una proposición que se puede establecer directamente a partir de un teorema que ya ha sido demostrado.

Demostración. Una *demostración* de un teorema es un argumento formado por una secuencia de sentencias, mediante el cual se prueba que el teorema es verdadero. La demostración de un teorema debe comenzar con las hipótesis y, mediante axiomas o postulados y teoremas demostrados previamente, se derivan sentencias nuevas, justificando cada paso por alguna regla de inferencia, hasta llegar a la conclusión. Las *reglas de inferencia* se usan para deducir conclusiones a partir de otras afirmaciones y son las que enlazan los pasos de una demostración.

5.2. Métodos de demostración. Los métodos de demostración son importantes no sólo porque se usan para demostrar teoremas matemáticos, sino por sus muchas aplicaciones en ciencias de la computación (verificación de que un programa de ordenador es correcto, seguridad de los sistemas operativos, inferencias en inteligencia artificial, consistencia de las especificaciones de un sistema, ...). A continuación mostramos algunas técnicas de demostración de teoremas.

Consideremos un teorema de la forma "Si se cumple p, entonces se cumple q":

Teorema : $\mathbf{p} \to \mathbf{q}$ (puede ocurrir que $\mathbf{p} \leftrightarrow \mathbf{p_1} \wedge \mathbf{p_2} \wedge \ldots \wedge \mathbf{p_n}$)

Demostraciones directas. Suponemos que p es verdadera y se utilizan las reglas de inferencia, axiomas y teoremas ya demostrados para demostrar que q también es verdadera.

Ejemplos. Demostrar la proposición "Si n es un entero impar, entonces n^2 es un entero impar."
Demostración.

$$n \text{ es impar } \Rightarrow n = 2k+1, \text{ para algún número entero } k \Rightarrow$$
$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1 \Rightarrow n^2 \text{ es impar}$$

Observación. Un corolario de este resultado sería "Si n es un entero tal que n^2 es par, entonces n es par"

Demostraciones indirectas: paso al contra-recíproco. Como $(p \to q) \leftrightarrow (\neg q \to \neg p)$, el teorema se puede demostrar viendo que el contra-recíproco es verdadero. A su vez, este se puede probar directamente o mediante otra técnica.

Ejemplos. Demostrar la proposición "Si $3n+2$ es un entero impar, entonces n es un entero impar."
Demostración. Por paso al contra-recíproco veamos que si n es un entero par, entonces $3n+2$ es un entero par.

$$n \text{ es par } \Rightarrow n = 2k, \text{ para algún número entero } k \Rightarrow$$
$$3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) \Rightarrow 3n+2 \text{ es par}$$

Demostración por contradicción: reducción al absurdo. Se basa en la tautología $p \to q \leftrightarrow [(p \wedge \neg q) \to F]$, *i.e.* $p \to q \equiv (p \wedge \neg q) \to F$. Para probar que $p \to q$ supongamos que $\neg q$ es verdadera (*i.e.* q es falsa) y que p es verdadera. Basta ver que $p \wedge \neg q$ implica una contradicción (F).

Explicación: en efecto, si $p \wedge \neg q$ implica una contradicción (*i.e.* $p \wedge \neg q \to F$ es verdadera), entonces o p es falsa o $\neg q$ es falsa. Con lo cual, como p es verdadera, $\neg q$ es falsa y, por lo tanto q es verdadera.

Ejemplo.

$$Teorema : \sqrt{2} \text{ es irracional}$$

Demostración. Por reducción al absurdo, supongamos que $\sqrt{2}$ es racional, *i.e.*

$$\sqrt{2} = \frac{p}{q}, \quad \text{con } p \text{ y } q \neq 0 \text{ números enteros sin factores comunes} \Rightarrow$$

$$2 = (\frac{p}{q})^2 = \frac{p^2}{q^2} \Leftrightarrow p^2 = 2q^2 \Rightarrow p^2 \text{ es par } \Rightarrow p \text{ es par } \Rightarrow$$

$$p = 2n, \text{con } n \text{ un número entero } \underset{p^2=2q^2}{\Rightarrow} 4n^2 = 2q^2 \Leftrightarrow 2n^2 = q^2 \Rightarrow$$

$$q^2 \text{ es par } \Rightarrow q \text{ es par } \Rightarrow$$

contradicción, ya que p y q no tienen factores comunes.

Demostración vacua. Supongamos que p es falsa, entonces $p \to q$ es verdadera.

Ejemplo. Sea n un número entero. Si $P(n)$ es la proposición "Si $n > 1$ es impar, entonces $n^2 > n$", demuestra que la proposición $P(0)$ es verdadera.

Demostración. La proposición $P(0)$ es la implicación "Si $0 > 1$ es impar, entonces $0^2 > 0$". Como la hipótesis es falsa, la implicación es automáticamente verdadera.

Demostración trivial. Supongamos que q es verdadera, entonces $p \to q$ es verdadera.

Ejemplo. Sea n un número entero. Si $P(n)$ es la proposición "Si a y b son enteros positivos, entonces $a^n \geq b^n$", demuestra que la proposición $P(0)$ es verdadera.

Demostración. La proposición $P(0)$ es la implicación "Si a y b son enteros positivos, entonces $a^0 \geq b^0$". Como $a^0 = b^0 = 1$, la conclusión de $P(0)$ es verdadera (y no se ha usado la hipótesis).

Demostración por casos. Supongamos que $p \leftrightarrow p_1 \vee p_2 \vee \ldots \vee p_n$, *i.e.*, queremos probar

$$\textbf{Teorema}: \mathbf{p_1 \vee p_2 \vee \ldots \vee p_n \rightarrow q}$$

Se puede utilizar la tautología

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

y, por lo tanto, probar que $p_1 \rightarrow q$, $p_2 \rightarrow q$, … y $p_n \rightarrow q$.

Ejemplo. Demuestra que si x e y son números reales, entonces $|xy| = |x||y|$.

Demostración.

- Si x e y son positivos, xy es positivo y, por lo tanto $|xy| = xy = |x||y|$, ya que $x = |x|$ e $y = |y|$
- Si x e y son negativos, xy es positivo y, por lo tanto $|xy| = xy = (-x) \cdot (-y) = |x||y|$, ya que $-x = |x|$ y $-y = |y|$
- Si x es positivo e y es negativo, xy es negativo y, por lo tanto $|xy| = -xy = x \cdot (-y) = |x||y|$, ya que $x = |x|$ y $-y = |y|$
- Si x es negativo e y es positivo, xy es negativo y, por lo tanto $|xy| = -xy = (-x) \cdot y = |x||y|$, ya que $-x = |x|$ e $y = |y|$

Demostración por equivalencia. Para demostrar un teorema de la forma

$$\textbf{Teorema}: \mathbf{p \leftrightarrow q}$$

se puede usar la tautología

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

y, por lo tanto, probar que $p \rightarrow q$ y $q \rightarrow p$.

Ejemplo. Demuestra que "El entero n impar si, y sólo si, n^2 es un entero impar".

Demostración.

"$\Rightarrow$" Esta implicación se ha probado en un ejemplo anterior.

"$\Leftarrow$" Por paso al contra-recíproco, probemos que si n es un entero par entonces n^2 es par.

$$n \text{ par } \Rightarrow n = 2k \text{ para algún entero } k \Rightarrow$$
$$n^2 = (2k)^2 = 4k^2 \Rightarrow n^2 \text{ es par}$$

Demostración de varias equivalencias. Para demostrar un teorema de la forma

$$\textbf{Teorema} : \mathbf{p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n}$$

se emplea la tautología

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_n \to p_1)]$$

y, por lo tanto, probar que $p_1 \to p_2$, $p_2 \to p_3$, $\ldots$ y $p_n \to p_1$.

Ejemplos. Muestra que las siguientes sentencias son equivalentes:

(1) n es un entero par
(2) $n - 1$ es un entero impar
(3) n^2 es un entero par

Demostración.

“(1) $\Rightarrow$ (2)”

$$\begin{aligned} &n \text{ par } \Rightarrow n = 2k \text{ para algún entero } k \Rightarrow \\ &n - 1 = 2k - 1 = 2(k-1) + 1 \Rightarrow n - 1 \text{ impar} \end{aligned}$$

“(2) $\Rightarrow$ (3)”

$$\begin{aligned} &n - 1 \text{ impar } \Rightarrow n - 1 = 2k + 1 \text{ para algún entero } k \Rightarrow \\ &n = 2k + 2 = 2(k+1) \Rightarrow n^2 = [2(k+1)]^2 = 4(k+1)^2 \Rightarrow \\ &n^2 \text{ par} \end{aligned}$$

“(3) $\Rightarrow$ (1)” Por paso al contra-recíproco, basta probar que si n es impar entonces n^2 es impar. Y esta implicación ya ha sido probada en un ejemplo anterior.

Demostraciones de existencia. Para demostrar un teorema de la forma

$$\textbf{Teorema} : \exists \mathbf{x}\, \mathbf{P}(\mathbf{x})$$

hay dos formas

- Demostración constructiva: encontrar un elemento a tal que $P(a)$ es verdadera
- Demostración no constructiva: por ejemplo, por reducción al absurdo, *i.e.*, mostrando que $\neg(\exists x\, P(x))$ implica una contradicción.

Ejemplos.

(1) Demuestra que "Hay un entero positivo que se puede poner de dos formas diferentes como suma de cubos de enteros positivos"

Demostración. Tras muchos cálculos se encuentra que $1729 = 10^3 + 9^3 = 12^3 + 1^3$

(2) Demuestra que "Existen dos números irracionales x e y tales que x^y es racional"

Demostración. Por un ejemplo anterior sabemos que $\sqrt{2}$ es irracional. Si $\sqrt{2}^{\sqrt{2}}$ es racional, ya estaría. En caso contrario, $\sqrt{2}^{\sqrt{2}}$ es irracional y tomando $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ resulta que:

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$$

Demostraciones de unicidad. Para demostrar un teorema de la forma

$$\textbf{Teorema}: \exists!\mathbf{x}\,\mathbf{P}(\mathbf{x})$$

debemos realizar dos pasos:

(1) Demostrar la existencia (ver "Demostraciones de existencia")
(2) Demostrar la unicidad: para ello hay que mostrar que si $y \neq x$ entonces no se cumple $P(y)$

Es decir:

$$(\exists x\, P(x)) \wedge (\forall y\,(y \neq x \to \neg P(y)))$$

Ejemplo. Muestra que "Todo número entero tiene un único elemento opuesto"

Demostración.

Existencia: Si p es un número entero $-p$ es su opuesto ya que $p + (-p) = 0$

Unicidad: Supongamos que existe un número entero $r \neq -p$ tal que $p + r = 0$. Entonces

$$p + r = 0 = p + (-p) \Rightarrow p + r - p = -p \Rightarrow r = -p$$

Contraejemplos. Si creemos que una sentencia de la forma $\forall x,\ P(x)$ es falsa, o bien no conseguimos encontrar una demostración, buscamos un contraejemplo.

Ejemplo. Muestra que la afirmación "Todo entero positivo es la suma de los cuadrados de tres enteros" es falsa.

El número 7 es un contraejemplo ya que no se puede escribir como suma de los cuadrados de tres enteros. En efecto, sólo podrían considerarse los cuadrados que no excedan de 7, que son 0, 1 y 4. Y utilizando estos tres cuadrados nunca se obtiene el 7.

Inducción matemática. La inducción matemática se emplea para probar teoremas de la forma

$$\mathbf{Teorema}: \forall \mathbf{n}\, \mathbf{P}(\mathbf{n})$$

donde el dominio es el conjunto de los números enteros n tales que $n \geq n_0$ para un número entero n_0 fijo.

La inducción matemática se basa en la tautología

$$[P(n_0) \wedge \forall k\, (P(k) \rightarrow P(k+1))] \rightarrow \forall n\, P(n)$$

En toda demostracción por inducción se deben realizar los siguientes pasos:

- Paso base: Se demuestra que $P(n_0)$ es verdadera.
- Paso de inducción: Se demuestra que $P(k) \rightarrow P(k+1)$ es una tautología, $\forall k \geq n_0$. Es decir, hay que probar que si $P(k)$ es verdadera, entonces $P(k+1)$ también.

Ejemplo. Demuestra que "$\forall n$ con n un número natural positivo, se verifica que $n < 2^n$."

- *Paso base:* $n_0 = 1$. La afirmación $1 < 2$ es trivial
- *Paso de inducción:* supongamos que la afirmación es cierta para $k > 1$ y probémosla para $k + 1$.

  $$k < 2^k \Rightarrow 2k < 2 \cdot 2^k = 2^{k+1}$$

  Por otra parte

  $$1 < k \Rightarrow k + 1 < k + k = 2k$$

  Combinando las dos desigualdades se obtiene que

  $$k + 1 < 2k < 2^k + 1 \Rightarrow k + 1 < 2^{k+1}$$

5.3. Ejercicios.

(1) Demuestra que si n es un entero y $n^3 + 5$ es impar, entonces n es par usando:
  - una demostración directa
  - una demostración indirecta
  - una demostración por reducción al absurdo

(2) Demuestra que el producto de dos números racionales es racional
(3) Muestra que se cumple, o que no, que el producto de dos números irracionales es irracional.
(4) Demuestra que estas tres sentencias son equivalentes, donde a y b son números reales.
- a es menor que b
- el valor medio de a y b es mayor que a
- el valor medio de a y b es menor que b

(5) ¿Es correcto este razonamiento para encontrar las soluciones de la ecuación $\sqrt{2x^2-1}=x$?
  (a) Se da $\sqrt{2x^2-1}=x$
  (b) $2x^2-1=x^2$, elevando al cuadrado ambos términos de (a)
  (c) $x^2-1=0$, restando x^2 a ambos lados de (b)
  (d) $(x-1)(x+1)=0$, factorizando la parte izquierda de (c)
  (e) $x=1$ o $x=-1$, ya que si $ab=0$ implica que bien $a=0$ o bien $b=0$.

(6) Obtén una fórmula para la suma de los n primeros positivos pares.
(7) Usa la inducción matemática para probar la fórmula obtenida en el ejercicio anterior.
(8) Usa la inducción matemática para demostrar que

$$3+3\cdot 5+3\cdot 5^2+\ldots+3\cdot 5^n=\frac{3(5^{n+1}-1)}{4}$$

para todo entero no negativo n

(9) Encuentra el fallo en esta "demostración":

Teorema: Para todo entero positivo n, $\sum_{i=1}^{n} i=\frac{(n+\frac{1}{2})^2}{2}$
- *Paso base:* La fórmula es cierta para $n_0=1$
- *Paso de inducción:* Supongamos que $\sum_{i=1}^{k} i=\frac{(k+\frac{1}{2})^2}{2}$. Entonces, $\sum_{i=1}^{k+1} i=(\sum_{i=1}^{k} i)+(k+1)$. Por hipótesis de inducción, $\sum_{i=1}^{k+1} i=\frac{(k+\frac{1}{2})^2}{2}+(k+1)=\frac{k^2+k+\frac{1}{4}}{2}+k+1=\frac{k^2+3k+\frac{9}{4}}{2}=\frac{(k+\frac{3}{2})^2}{2}=\frac{[(k+1)+\frac{1}{2}]^2}{2}$, lo que completa el paso de inducción.

MARTA PÉREZ RODRÍGUEZ, DEPARTAMENTO DE MATEMÁTICAS, ESCOLA SUPERIOR DE ENXENERÍA INFORMÁTICA, UNIVERSIDADE DE VIGO - CAMPUS OURENSE, E-32004 OURENSE, SPAIN

E-mail address: `martapr@uvigo.es, http://webs.uvigo.es/martapr`