Índex

Lògica proposicional

Proposicions

- Sentència que pot ser (o ser considerada) certa (1 ó V) o falsa (0 ó F).
- S'indica per minúscules.

Exemple

Són proposicions:

- Avui plou (p = "avui plou")
- $\sqrt{2}$ no és un nombre racional ($p = [\sqrt{2} \notin \mathbb{Q}]$)

No són proposicions:

- Quina hora és?
- Un nombre racional

Connectors

Forma de composar proposicions a partir d'altres:

- Negació: $\neg p$
  "no p" o "p és fals": cert quan p és fals
- Conjunció: $p \wedge q$
  "p i q": cert quan p i q són tots dos certs
- Disjunció: $p \vee q$
  "p o q": cert quan almenys un de p i q són certs
- Disjunció exclusiva: $p \oplus q$
  "o bé p o bé q": cert quan un i només un de p i q són certs
- Implicació: $p \rightarrow q$
  "p implica q" o "p és condició suficient per a q" o "q és condició necessària per a p": només es fals quan p és cert i q és fals
- Doble implicació: $p \leftrightarrow q$
  "p si, i només, q" o "p és condició necessària i suficient per a q": cert quan p i q són certs o falsos alhora

Exemple

"Si avui és diumenge i no plou, aniré al futbol" $= (p \wedge \neg q) \to r$.

- $p =$ "avui és diumenge"
- $q =$ "avui plou"
- $r =$ "aniré al futbol"

Situacions:

- Avui és diumenge, no plou i vaig al futbol: $p = \mathrm{V}, q = \mathrm{F}, r = \mathrm{V}$.
  $(p \wedge \neg q) \to r = (\mathrm{V} \wedge \neg \mathrm{F}) \to \mathrm{V} = \mathrm{V} \to \mathrm{V} = \mathrm{V}$.
- Avui és dissabte, plou i vaig al futbol: $p = \mathrm{F}, q = \mathrm{V}, r = \mathrm{V}$.
  $(p \wedge \neg q) \to r = (\mathrm{F} \wedge \neg \mathrm{V}) \to \mathrm{V} = \mathrm{F} \to \mathrm{V} = \mathrm{V}$.
- Avui és dijous, no plou i no vaig al futbol: $p = \mathrm{F}, q = \mathrm{F}, r = \mathrm{F}$.
  $(p \wedge \neg q) \to r = (\mathrm{F} \wedge \neg \mathrm{F}) \to \mathrm{F} = \mathrm{F} \to \mathrm{F} = \mathrm{V}$.
- Avui és diumenge, no plou i no vaig al futbol: $p = \mathrm{V}, q = \mathrm{F}, r = \mathrm{F}$.
  $(p \wedge \neg q) \to r = (\mathrm{V} \wedge \neg \mathrm{F}) \to \mathrm{F} = \mathrm{V} \to \mathrm{F} = \mathrm{F}$.

Ordres de precedència

l'ordre de major a menor precedència entre ells és:

- $\neg$
- $\wedge, \vee$
- $\to$
- $\leftrightarrow$

Exemple

La proposició $\neg p \vee q \to r$ s'ha de llegir com $((\neg p) \vee q) \to r$.

Taules de veritat

Forma d'expressar el valor de veritat d'una proposició: Posar cada possible valor en una taula.
Si hi ha n proposicions atòmiques, hi ha 2^n files

Exemple

p	$\neg p$
0	1
1	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Exemple

$(p \wedge q) \vee r \leftrightarrow s$

p	q	r	s	$(p \wedge q)$	$(p \wedge q) \vee r$	$(p \wedge q) \vee r \leftrightarrow s$
0	0	0	0	0	0	1
0	0	0	1	0	0	0
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	0	0
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	0	1
1	0	0	1	0	0	0
1	0	1	0	0	1	0
1	0	1	1	0	1	1
1	1	0	0	1	1	0
1	1	0	1	1	1	1
1	1	1	0	1	1	0
1	1	1	1	1	1	1

Equivalència

Dues proposicions són *equivalents* si (equiv.):

- Prenen els mateixos valors de veritat per a tota assignació
- Tenen la mateixa taula de veritat

S'indica per $p \iff q$

Exemple

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

Tautologia i contradicció

- *Tautologia*: Proposició que pren sempre el valor V
- *Contradicció*: Proposició que pren sempre el valor F

Exemple

- $p \vee \neg p$ és tautologia
- $p \wedge \neg p$ és contradicció

Observació

p i q són equivalents si, i només si, $p \leftrightarrow q$ és tautologia.

Lleis lògiques

- Lleis d'identitat:
  $p \wedge \text{V} \iff p$
  $p \vee \text{F} \iff p$
- Lleis de dominació:
  $p \wedge \text{F} \iff \text{F}$
  $p \vee \text{V} \iff \text{V}$
- Lleis d'idempotència:
  $p \wedge p \iff p$
  $p \vee p \iff p$
- Llei de doble negació:
  $\neg(\neg p) \iff p$
- Lleis commutatives:
  $p \wedge q \iff q \wedge p$
  $p \vee q \iff q \vee p$
- Lleis associatives:
  $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$
  $p \vee (q \vee r) \iff (p \vee q) \vee r$
- Lleis de De Morgan:
  $\neg(p \wedge q) \iff \neg p \vee \neg q$
  $\neg(p \vee q) \iff \neg p \wedge \neg q$
- Lleis de la tautologia i la contradicció
  $p \vee \neg p \iff \text{V}$
  $p \wedge \neg p \iff \text{F}$
- Llei de la implicació:
  $p \to q \iff \neg p \vee q \iff \neg(p \wedge \neg q)$

Exemple

- Interpretació de llei de De Morgan:
  "És fals que avui sigui diumenge i plogui": estarem dient la veritat exactament quan o bé no és diumenge, o bé no plou, o bé totes dues coses.
- Interpretació de la llei de la implicació:
  "Si avui és diumenge, aleshores aniré a passejar": la única forma possible en que el que diem és fals és que sigui diumenge i no anem a passejar. Dit d'altre forma, estarem dient una veritat exactament quan no sigui diumenge o quan vagi a passejar.

Lògica de primer ordre

Variables i predicats

- Estenem la lògica proposicional: el valor de veritat de la proposició depèn d'altres objectes
- *Forma proposicional*: *Predicats* que estableixen propietats que depenen de *variables*
- S'indica per: $P(x)$, $Q(x, y)$,...

Exemple

"n és un nombre parell" $= Q(n)$

- Variable: n
- Predicat: $Q(n)$

Observació

Quan s'assigna a una variable un valor concret, el predicat esdevé una proposició

Quantificador universal

- Objectiu: Expressar que el predicat $P(x)$ pren sempre el valor cert per a qualsevol assignació a la variable x (dins un univers Ω)
- Notació:

$$(\forall x \in \Omega)P(x) \quad \text{o} \quad \forall x[P(x)] \quad \text{o} \quad \forall x : P(x).$$

- Ull: El resultat és una proposició

Exemple

- Tot nombre és parell: $P(n) =$"n és parell"

$$\forall n : P(n)$$

és una proposició (falsa)

Quantificador existencial

- Objectiu: Expressar que el predicat $P(x)$ pren el valor cert per a alguna assignació a la variable x (dins un univers Ω)
- Notació:

$$(\exists x \in \Omega)P(x) \quad \text{o} \quad \exists x[P(x)] \quad \text{o} \quad \exists x : P(x).$$

- Ull: El resultat és una proposició

Exemple

- Hi ha algun nombre parell: $P(n) =$"n és parell"

$$\exists n : P(n)$$

és una proposició (certa)

Quantificador existencial amb unicitat

- Objectiu: Expressar que el predicat $P(x)$ pren el valor cert per a una (i només una) assignació a la variable x (dins un univers Ω)
- Notació:

$$(\exists! x \in \Omega)P(x) \quad \text{o} \quad \exists! x[P(x)] \quad \text{o} \quad \exists! x : P(x).$$

- Ull: El resultat és una proposició

Exemple

- Hi ha un únic nombre parell: $P(n) =$"n és parell"

$$\exists! n : P(n)$$

és una proposició (falsa)

Observació

Es pot posar en termes dels altres: $\exists! x : P(x)$ és equivalent a: $(\exists x : P(x)) \wedge (\forall x, y : P(x) \wedge P(y) \to x = y)$

Exemple amb múltiples variables

$P(x,y) =$ "$x + y = 0$": Forma prop. amb 2 variables
Composant universals i existencials en un ordre...

- $\exists x : P(x,y)$: Forma proposicional amb 1 variable (y)
  = "existeix un invers respecte la suma de y"
- $\forall y : \exists x : P(x,y)$: Proposició
  = "tot element té un invers respecte la suma" (cert)

...i en un altre ordre

- $\forall y : P(x,y)$: Forma proposicional amb 1 variable (x)
  = "tot element sumat a x dóna 0"
- $\exists x : \forall y : P(x,y)$: Proposició
  = "hi ha un element que sumis el que li sumis, sempre dóna 0" (fals)

"Moraleja": L'ordre és important

Cas finit

Si l'univers és finit (# finit d'eleccions per a la variable):

$$\forall x : P(x) \iff P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

$$\exists x : P(x) \iff P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

Cas d'univers buit

- Tot quantificador universal és cert
- Tot quantificador existencial és fals

Exemple

- Tots els meus vaixells són a vela (cert, no tinc vaixells)
- Algun dels meus vaixells és a vela (fals, no tinc vaixells)

Negació de quantificadors

- La negació d'un universal és un existencial (i viceversa)
- Negació d'universal:

$$\neg(\forall x : P(x)) \iff \exists x : \neg P(x)$$

- Negació d'existencial:

$$\neg(\exists x : P(x)) \iff \forall x : \neg P(x)$$

Exemple

- És fals que tot nombre sigui parell, ja que existeix almenys un nombre senar (1)
- És fals que hi hagi un nombre més gran que qualsevol altre, ja que per a tot nombre, podem considerar el resultat de sumar-li 1

Raonament matemàtic i demostracions

Lemes, proposicions, teoremes...

Coneixement matemàtic estructurat en:

- Conceptes que es suposen certs: definicions i axiomes
- Mètode per deduir nous resultats: demostracions
- Resultats demostrats: lemes, proposicions, teoremes, corol·laris

Regles d'inferència

- Expressen matemàticament el concepte de "deduir resultats a partir d'altres"
- Per exemple ("modus ponens"):
  - Suposem cert: "si plou em mullo" i "està plovent"
  - Puc deduir: "em mullo"
  - Això s'expressa matemàticament com:

$$\begin{array}{rl} & p \to q \\ & p \\ \hline \therefore & q \end{array}$$

  - Equivalentment, dient que

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

  és una tautologia

Regles d'inferència habituals

- Addició:
$$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$$
- Simplificació:
$$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$$
- Conjunció:
$$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$$
- Modus ponens:
$$\begin{array}{rl} & p \to q \\ & p \\ \hline \therefore & q \end{array}$$
- Modus tollens:
$$\begin{array}{rl} & p \to q \\ & \neg q \\ \hline \therefore & \neg p \end{array}$$
- Sil·logisme hipotètic:
$$\begin{array}{rl} & p \to q \\ & q \to r \\ \hline \therefore & p \to r \end{array}$$
- Sil·logisme disjuntiu:
$$\begin{array}{rl} & p \vee q \\ & \neg q \\ \hline \therefore & p \end{array}$$

Exemple

- Suposem cert: “si avui és diumenge, aniré al futbol”
  - Si és diumenge, puc deduir que vaig al futbol (Modus Ponens)
  - Si no vaig al futbol, puc deduir que no és diumenge (Modus Tollens)
- Suposem cert: “tinc gana o tinc set”
  - Si no tinc set, puc deduir que tinc gana (sil·logisme disjuntiu)

Regles d’inferència en lògica de primer ordre

- Particularització universal:

$$\begin{array}{rl} & \forall x P(x) \\ \hline \therefore & P(c) \text{ per a } c \text{ arbitrari} \end{array}$$

- Generalització universal:

$$\begin{array}{rl} & P(c) \text{ per a } c \text{ arbitrari} \\ \hline \therefore & \forall x P(x) \end{array}$$

- Particularització existencial:

$$\begin{array}{rl} & \exists x P(x) \\ \hline \therefore & P(c) \text{ per a algun } c \end{array}$$

- Generalització existencial:

$$\begin{array}{rl} & P(c) \text{ per a algun } c \\ \hline \therefore & \exists x P(x) \end{array}$$

Demostracions

- Successió de regles d’inferència aplicades a unes hipòtesis per obtenir un resultat
- Diferents estratègies:
  - Demostració directa
  - Demostració per contrarecíproc
  - Demostració per reducció a l’absurd
  - etc.

Demostració directa

Per demostrar $p \to q$: suposar p cert i obtenir q

Exemple

Si m i n són enters parells, aleshores $m + n$ és parell

- Com que m i n són parells, existeixen k i l enters amb $m = 2k$ i $n = 2l$
- Per propietats de la suma: $m + n = 2k + 2l = 2(k + l)$
- Com que $k + l$ és enter, $m + n$ és parell

Exemple (més formal)

Prenem la definició:

(1) $P(n)$ és el predicat "n és parell"

Acceptem els axiomes:

(2) $\forall x(P(x) \leftrightarrow \exists y[x = 2y])$ (definició de parell)

(3) $\forall x \forall y \forall z[x(y + z) = xy + xz]$ (propietat distributiva)

Aleshores, el resultat a provar és:

$$\forall x \forall y[P(x) \wedge P(y) \to P(x + y)]$$

(4) $P(m) \wedge P(n)$ (hipòtesi inicial)

(5) $P(m)$ (simplificació de (4))

(6) $P(m) \leftrightarrow \exists y[m = 2y]$ (particularització universal aplicada a (2))

(7) $\exists y[m = 2y]$ (modus ponens aplicat a (5) i (6))

(8) $m = 2k$ (particularització existencial aplicada a (7))

(5') $P(n)$ (simplificació de (4))

(6') $P(n) \leftrightarrow \exists y[n = 2y]$ (particularització universal aplicada a (2))

(7') $\exists y[n = 2y]$ (modus ponens aplicat a (5) i (6'))

(8') $n = 2l$ (particularització existencial aplicada a (7'))

(9) $2(k + l) = 2k + 2l$ (particularització universal aplicada a (3))

(10) $m + n = 2(k + l)$ (simple substitució)

(11) $\exists y[m + n = 2y]$ (generalització existencial aplicada a (10))

(12) $P(m + n) \leftrightarrow \exists y[m + n = 2y]$ (particularització universal aplicada a (2))

(13) $P(m + n)$ (modus ponens aplicat a (11) i (12))

(14) $P(m) \wedge P(n) \to P(m + n)$

(15) $\forall x \forall y[P(x) \wedge P(y) \to P(x + y)]$ (generalització universal aplicada a (14))

Demostració per contrarecíproc

- Es té l'equivalència lògica: $p \to q \iff \neg q \to \neg p$
- Demostrar per contrarecíproc $p \to q$ és provar $\neg q \to \neg p$

Exemple

Si n és un enter amb n^2 senar, aleshores n és senar

- Per contrarecíproc: Si n no és senar, aleshores n^2 no és senar
- És a dir: Si n és parell, aleshores n^2 és parell
- Suposem n parell, i.e. hi ha k amb $n = 2k$
- Ara tenim: $n^2 = 4k^2 = 2(2k^2)$ és parell

Demostració per reducció a l'absurd

- En general: Suposar el resultat fals i arribar a contradicció.
- Cas habitual: Es té l'equivalència lògica $p \to q \iff \neg(p \wedge \neg q)$
- Reducció a l'absurd: Suposar que p és cert i q és fals i arribar a contradicció.

Exemple

Si m i n són enters amb $n + n^2 + n^3 = m + m^2$, aleshores n és parell

- Suposem $n + n^2 + n^3 = m + m^2$ i que n és senar.
- Ara, $n + n^2 + n^3$ és senar (tots els sumands són senars)
- Per tant, $m + m^2$ és senar
- Si m és senar, $m + m^2$ és parell... contradicció!
- Si m és parell, $m + m^2$ és parell... contradicció!

Demostracions existencials constructives

- Per a provar proposicions del tipus $\exists x : P(x)$
- Es construeix explícitament un c que compleix $P(c)$

Exemple

Per a tot natural n existeix un natural m amb $m > n$

- Sigui n qualsevol
- Consideram l'enter $m = n + 1$
- m compleix la propietat
- Per tant, existeix un element que ho compleix

Demostracions existencials no constructives

- Per a provar proposicions del tipus $\exists x : P(x)$
- Es demostra que existeix l'element sense construir-lo explícitament

Exemple

Si n és un enter positiu qualsevol, existeix un nombre primer p amb $p > n$

- Considerem l'enter $m = n! + 1$
- m és divisible per algun nombre primer p
- Però p no pot ser menor que n, ja que el residu de la divisió entre $m = n! + 1$ i p és zero, i tot enter $\leq n$ dóna residu 1
- Per tant, p compleix la propietat (tot i que no sabem construir-lo)

"Demostracions" per contraexemple

- Per a provar que resultats de la forma $\forall x : P(x)$ són falsos
- Trobar un contraexemple: c per al qual $P(c)$ és fals

Exemple

Tot enter positiu es pot escriure com a suma de 3 quadrats

- Considerem $n = 7$ i vegem que és fals
- Hauriem de tenir $7 = a^2 + b^2 + c^2$. Possibles a, b, c: $\{0, 1, 2\}$
- Fent totes les possibilitats mai surt 7

Dobles implicacions i equivalències

- Per a provar $p \leftrightarrow q$: Provar

$$p \to q \quad \text{i} \quad q \to p$$

- Per a provar $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_k$: Provar

$$p_1 \leftrightarrow p_2, \quad p_2 \leftrightarrow p_3, \quad \ldots \quad p_{k-1} \leftrightarrow p_k,$$

- Altra estratègia: Provar

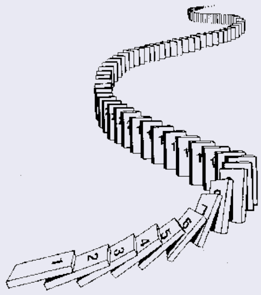
$$p_1 \to p_2, \quad p_2 \to p_3, \quad \ldots \quad p_{k-1} \to p_k, \quad p_k \to p_1,$$

Demostració per inducció matemàtica

Si certa propietat $P(n)$:

- És certa per a $n = 0$
- Suposant-la certa per a n, també és certa per a $n + 1$ (n arbitrari)

Aleshores és certa per a tot n



Principi d'inducció simple

Suposem que cert predicat $P(n)$ compleix:

- Cas inicial: $P(n_0)$ és cert.
- Pas d'inducció: Per a $n \geq n_0$ arbitrari, es té que $P(n) \to P(n + 1)$.

Aleshores, per a tot $n \geq n_0$ es té que $P(n)$ és cert.

Exemple

Per a tot $n \geq 1$ *es té que* $n < 2^n$

- Cas inicial: Per a $n = 1$, $1 < 2^1$: Cert
- Pas d'inducció: Suposant $n < 2^n$ provar que $n + 1 < 2^{n+1}$:

$$n + 1 \overset{(1)}{<} 2^n + 1 \overset{(2)}{<} 2^n + 2^n = 2^{n+1} : \qquad \text{Cert}$$

(1) Per hipòtesi d'inducció
(2) Ja que $1 < 2^n$

Principi d'inducció completa

Suposem que cert predicat $P(n)$ compleix:

- Cas inicial: $P(n_0)$ és cert.
- Pas d'inducció: Per a $n \geq n_0$ arbitrari, es té que $(P(n_0) \wedge \cdots \wedge P(n)) \to P(n + 1)$.

Aleshores, per a tot $n \geq n_0$ es té que $P(n)$ és cert.

Exemple

Tot natural > 1 *descompon en producte de primers*

- Cas inicial: Per a $n = 2$ es compleix (2 és primer)
- Pas d'inducció: Suposant-ho cert per a $n = 2, \ldots, n$, provar-ho per a $n + 1$:
  - Si $n + 1$ és primer, el resultat és cert
  - Si $n + 1$ no és primer, diguem $n + 1 = n_1 \cdot n_2$. Per hipòtesi d'inducció, n_1 i n_2 descomponen en producte de primers. Per tant, $n + 1$ també.