Fonaments Matemàtics (primera part)

Mercè Mora, José Luis Ruiz

Juliol 2017

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Lògica i raonament

El mètode deductiu

- Les teories científiques es presenten, una vegada elaborades, de manera deductiva: a partir d'uns quants principis bàsics es poden derivar les demés veritats, mitjançant raonament lògic.
- La lògica desenvolupa i proporciona mètodes i tècniques que ens permeten distingir els arguments correctes dels incorrectes.

Exemple d'argument lògic

Un dels arguments lògics correctes més usats és el *Modus Ponens*:

Exemple de Modus Ponens

1. Si la mesura d'un angle és més petita que 90°, llavors l'angle és agut.
2. L'angle A mesura 60°.
3. L'angle A és agut.

- (1) i (2) són les *premises* o *hipòtesis* de l'argument;
- (3) és la *conclusió* o *tesi*.
- Si les premises són certes, llavors la conclusió també ho és.

Proposicions

- Oracions susceptibles de ser vertaderes o falses (però no les dues coses alhora).
- Valors de veritat: una proposició pren el valor 1 si és certa i 0 si és falsa.
- Les proposicions poden ser simples o compostes.
- Una proposició composta està formada per proposicions simples unides mitjançant *connectives*: *no*, *i*, *o*, *si…llavors…*, *si i només si*.

Exemples

Són proposicions: "Avui plou"; "El quadrat de 2 és 5".
No són proposicions: "$x > 2$"; "Has llegit aquest llibre?".

Càlcul proposicional

- Els raonaments lògics són vàlids en virtut de la seva forma.
- Per a concentrar-nos en la forma, treballem amb un llenguatge buit de contingut (llenguatge formal).
- No treballem amb proposicions reals sinó amb símbols o lletres proposicionals, purament formals, buits de significat.

Llenguatge del càlcul proposicional

Proposicions simples

Les proposicions simples o atòmiques es representen per lletres: p, q, r, ..., que anomenem *lletres proposicionals*.

Proposicions compostes o *fórmules proposicionals*

Les proposicions compostes o no atòmiques es formen amb les connectives lògiques.

Connectives lògiques

Negació: $\neg$

Equival a *no* en llenguatge natural.
$\neg p$ és una proposició certa si p és falsa, i falsa si p és certa.

Conjunció: $\wedge$

Equival a *i* en llenguatge natural.
$p \wedge q$ és una proposició certa si p i q són certes, i falsa si alguna de les dues és falsa.

Disjunció: $\vee$

Equival a *o* (inclusiu) en llenguatge natural.
$p \vee q$ és una proposició certa si p és certa o si q és certa, i falsa si p i q són falses.

Connectives lògiques

Condicional: $\rightarrow$

Equival a *Si*..., *llavors*... en llenguatge natural.
$p \rightarrow q$ és una proposició certa si p és falsa o q és certa, i és falsa si p és certa i q és falsa.

Bicondicional: $\leftrightarrow$

Equival a ... *si, i només si,* ... en llenguatge natural.
$p \leftrightarrow q$ és una proposició certa si les dues són certes o les dues són falses, i és falsa si una és certa i l'altra falsa.

Fórmules del càlcul proposicional formal

Les fórmules proposicionals són successions de símbols generades mitjançant l'aplicació un nombre finit de vegades de les regles següents:

1. Tota lletra proposicional és una fórmula.
2. Si α és una fórmula, llavors $\neg\alpha$ és una fórmula.
3. Si α, β són fórmules, llavors $(\alpha \vee \beta)$, $(\alpha \wedge \beta)$, $(\alpha \rightarrow \beta)$ i $(\alpha \leftrightarrow \beta)$ són fórmules.

Subfórmula d'una fórmula proposicional

Les subfórmules d'una fórmula φ són totes les fórmules generades per les regles següents:

1. Si φ és una lletra proposicional, l'única subfórmula de φ és ella mateixa.
2. Si $\varphi = \neg\alpha$, les subfórmules de φ són φ més les subfórmules de α.
3. Si $*$ és una connectiva binària i $\varphi = \alpha * \beta$, les subfórmules de φ són φ més les subfórmules de α més les subfórmules de β.

Exemple

Les subfórmules de $\neg p \to (q \vee r)$ són:

$$\neg p \to (q \vee r), \quad \neg p, \quad q \vee r, \quad p, \quad q, \quad r$$

Les taules de veritat donen el valor de veritat d'una fórmula proposicional en funció dels valors de veritat de les lletres proposicionals.

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Tautologies i contradiccions

Tautologia

Fórmula proposicional que és certa per a qualsevol valor de veritat que prenguin les lletres proposicionals de què consta.

Contradicció

Fórmula proposicional que és falsa per a qualsevol valor de veritat que prenguin les lletres proposicionals de què consta.

Exemples

Tautologia: $p \vee \neg p$ (principi del tercer exclòs).
Contradicció: $p \wedge \neg p$.

Tautologies i contradiccions: propietats

- La negació d'una tautologia és una contradicció.
- La negació d'una contradicció és una tautologia.
- No tota fórmula proposicional és tautologia o contradicció.

Algunes tautologies importants

Siguin α, β i γ fórmules proposicionals.

1. Principi del tercer exclòs: $\alpha \vee \neg\alpha$.
2. Principi de la no contradicció: $\neg(\alpha \wedge \neg\alpha)$.
3. Addició: $\alpha \to (\alpha \vee \beta)$.
4. Simplificació: $(\alpha \wedge \beta) \to \alpha$.
5. Modus Ponens: $((\alpha \to \beta) \wedge \alpha) \to \beta$.
6. Modus Tollens: $((\alpha \to \beta) \wedge \neg\beta) \to \neg\alpha$.
7. Sil·logisme disjuntiu: $((\alpha \vee \beta) \wedge \neg\alpha) \to \beta$.
8. Sil·logisme hipotètic: $((\alpha \to \beta) \wedge (\beta \to \gamma)) \to (\alpha \to \gamma)$.

Equivalència lògica

- Dues fórmules proposicionals α, β són *lògicament equivalents* si tenen la mateixa taula de veritat.
- Dues fórmules α i β són equivalents si $\alpha \leftrightarrow \beta$ és una tautologia.

Notació: $\alpha \equiv \beta$.

Exemples

- Si τ és una tautologia i α és una proposició, llavors $(\tau \to \alpha) \equiv \alpha$.
- En particular: $(\alpha \vee \neg\alpha) \to \beta \equiv \beta$.

Algunes equivalències importants

Siguin α, β i γ fórmules proposicionals.

Commutatives	$\alpha \wedge \beta \equiv \beta \wedge \alpha, \quad \alpha \vee \beta \equiv \beta \vee \alpha$
Associatives	$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$ $\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$
Distributives	$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ $\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
Doble negació	$\neg(\neg\alpha) \equiv \alpha$
Lleis de De Morgan	$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta, \quad \neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$
$\rightarrow$ en funció de $\neg$, $\vee$	$\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$
Negació del condicional	$\neg(\alpha \rightarrow \beta) \equiv \alpha \wedge \neg\beta$
Contrarrecíproc	$\alpha \rightarrow \beta \equiv \neg\beta \rightarrow \neg\alpha$
‘O’ a l’antecedent	$(\alpha \vee \beta) \rightarrow \gamma \equiv (\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)$
‘O’ en el consequent	$\alpha \rightarrow (\beta \vee \gamma) \equiv (\alpha \wedge \neg\beta) \rightarrow \gamma$

Recíproc i contrarrecíproc

Proposició contrarrecíproca

- La proposició *contrarrecíproca* de $p \to q$ és $\neg q \to \neg p$.
- Un condicional i la seva forma contrarrecíproca són equivalents.

Proposició recíproca

- La proposició *recíproca* de $p \to q$ és $q \to p$.
- Un condicional $p \to q$ i el condicional recíproc $q \to p$ NO són equivalents.

Predicats i univers de discurs

- Un *predicat* és una afirmació que depèn d'una o més variables.
  Notació: $P(x)$, $P(x, y)$, etc.
- Un *univers de discurs* és un conjunt U no buit de valors que poden prendre les variables d'un predicat.
- Si $P(x)$ és un predicat amb univers de discurs U i $a \in U$, llavors $P(a)$ és una proposició.

Quantificadors

- Quantificador universal $\forall$: que la proposició $\forall x\, P(x)$ sigui certa significa que "per a tot x de U, $P(x)$ és una proposició certa".
- Quantificador existencial $\exists$: que la proposició $\exists x\, P(x)$ sigui certa significa que "existeix x de U tal que $P(x)$ és certa".

Exemples

- El quadrat de tot nombre real és no negatiu:

$$\forall x\,(x \in \mathbb{R} \to x^2 \geq 0)$$

- Existeix un nombre enter tal que el seu quadrat és 2:

$$\exists x\,(x \in \mathbb{Z} \land x^2 = 2)$$

- Si $U = \{a, b, c\}$, llavors:
  $\forall x\, P(x)$ equival a $P(a) \land P(b) \land P(c)$.
- Si $U = \{a, b, c\}$, llavors:
  $\exists x\, P(x)$ equival a $P(a) \lor P(b) \lor P(c)$.

Propietats dels quantificadors

Negació dels quantificadors

- $\neg\forall x\, P(x)$ és equivalent a $\exists x\, \neg P(x)$.
- $\neg\exists x\, P(x)$ és equivalent a $\forall x\, \neg P(x)$.

Commutativitat dels quantificadors

- $\forall x \forall y\, P(x, y) \equiv \forall y \forall x\, P(x, y)$
- $\exists x \exists y\, P(x, y) \equiv \exists y \exists x\, P(x, y)$
- $\forall x \exists y\, P(x, y)$ i $\exists y \forall x\, P(x, y)$ NO són equivalents.

Altres propietats

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

Axioma

Proposició que assumim certa en una teoria determinada.

Teorema

Afirmació que es pot provar que és certa en una teoria determinada.

Demostració

Argument lògic correcte per a provar un teorema. S'utilitzen regles d'inferència que es deriven de tautologies.

Regles d’inferència

Regles d’inferència més usades

- Addició: de p certa, deduïm que $p \vee q$ és certa.
- Simplificació: de $p \wedge q$ certa, deduïm que p és certa.
- Modus ponens: de $p \rightarrow q$ i p certes, deduïm que q és certa.
- Modus tollens: de $p \rightarrow q$ i $\neg q$ certes, deduïm $\neg p$ certa.
- Sil·logisme disjuntiu: de $p \vee q$ i $\neg p$ certes, deduïm q certa.
- Sil·logisme hipotètic: de $p \rightarrow q$ i $q \rightarrow r$ certes, deduïm $p \rightarrow r$ certa.

Errors més freqüents (fal·làcies)

- De $p \rightarrow q$ i q certes, NO es pot deduir que p sigui certa.
- De $p \rightarrow q$ i $\neg p$ certes, NO es pot deduir que $\neg q$ sigui certa.

La implicació $p \Rightarrow q$

- $p \Rightarrow q$ és una afirmació que significa que si p és certa, llavors q també ho ha de ser.
- Dir que p implica q és dir que el condicional $p \to q$ és vertader.
- Que $p \Rightarrow q$ no és veritat (s'escriu $p \not\Rightarrow q$ i es llegeix "p no implica q") vol dir que es pot donar al mateix temps que p sigui certa i q falsa.
- $p \Leftrightarrow q$ significa que $p \Rightarrow q$ i que $q \Rightarrow p$.
- En matemàtiques, el tipus d'argumentació que usem per a justificar que p implica q és la demostració.

Demostració de $p \Rightarrow q$

Prova directa

- Es tracta d'exhibir un raonament vàlid per a arribar a q certa partint del fet que p és certa.
- p és la *hipòtesi* i q és la *tesi*.

Contrarrecíproc

- És equivalent a demostrar $\neg q \Rightarrow \neg p$.
- $\neg q$ és la *hipòtesi* i $\neg p$ és la *tesi*.

Reducció a l'absurd

- Es tracta d'arribar a una contradicció a partir de $p \wedge \neg q$.
- $p \wedge \neg q$ és la *hipòtesi*.

Més mètodes de demostració

Com demostrar una conjunció

Demostrar $p \Rightarrow (q \wedge r)$ equival a demostrar $p \Rightarrow q$ i $p \Rightarrow r$.

Com demostrar una disjunció

Demostrar $p \Rightarrow (q \vee r)$ equival a demostrar $(p \wedge \neg q) \Rightarrow r$.

Demostració per casos

Demostrar $(p_1 \vee p_2 \vee \cdots \vee p_r) \Rightarrow q$ és equivalent a demostrar $p_1 \Rightarrow q$ i $p_2 \Rightarrow q$ i $\ldots$ i $p_r \Rightarrow q$.

Equivalència de dues proposicions

Demostrar $p \Leftrightarrow q$ equival a demostrar $p \Rightarrow q$ i $q \Rightarrow p$.

Equivalència de vàries proposicions

Demostrar que les proposicions $p_1, p_2, \ldots, p_r$ són equivalents equival a demostrar $p_1 \Rightarrow p_2$, $p_2 \Rightarrow p_3$, $\ldots$, $p_{r-1} \Rightarrow p_r$, $p_r \Rightarrow p_1$.

Demostració de $\forall x\, P(x)$

- Fer una demostració genèrica de $P(x)$; és a dir, que sigui vàlida per a qualsevol valor de x.
- Reducció a l'absurd: arribar a contradicció a partir de $\exists\, x \neg P(x)$.

Demostració de $\exists x\, P(x)$

- Trobar un element concret c tal que la proposició $P(c)$ sigui certa.
- Reducció a l'absurd: arribar a contradicció a partir de $\forall x \neg\, P(x)$.

Propietats i observacions

- Demostrar $\neg\forall x\, P(x)$ és equivalent a demostrar $\exists x\, \neg P(x)$. En aquest cas, si c és tal que la proposició $P(c)$ és falsa, direm que c és un *contraexemple* de $\forall x\, P(x)$
- Demostrar $\neg\exists x\, P(x)$ és equivalent a demostrar $\forall x\, \neg P(x)$.

Principi d'inducció simple

Siguin $n_0 \in \mathbb{N}$ un nombre natural i $P(n)$ una propietat expressada en termes d'un nombre natural $n \geq n_0$. Si es compleixen les dues condicions següents:

1. **Cas base:** $P(n_0)$ és certa;
2. **Pas inductiu:** per a tot $n \geq n_0$, si $P(n)$ és certa, llavors $P(n+1)$ és certa;

aleshores la propietat $P(n)$ és certa per a tot $n \geq n_0$.

Principi d'inducció completa

Siguin $n_0 \in \mathbb{N}$ un nombre natural i $P(n)$ una propietat expressada en termes d'un nombre natural $n \geq n_0$. Si es compleixen les dues condicions següents:

1. **Cas base:** $P(n_0)$ és certa;
2. **Pas inductiu:** per a tot $n \geq n_0$, si $P(k)$ és certa per a tot $k \in \mathbb{N}$ tal que $n_0 \leq k \leq n$, llavors $P(n+1)$ és certa;

aleshores la propietat $P(n)$ és certa, per a tot $n \geq n_0$.

Conjunts i relacions

Conjunts i elements, relació de pertinença

Primera aproximació

Un conjunt és una col·lecció d'objectes diferents (els seus elements) però considerada com un tot, com una unitat, la qual pot també ser element d'algun altre conjunt.

Relació de pertinença

Notem $x \in A$ i $x \notin A$ per indicar que x és element del conjunt A i que x no és element de A, respectivament.
$x \in A$ també es pot llegir com "x pertany a A" i $x \notin A$ com "x no pertany a A".

Observacions

En un conjunt, no hi ha elements repetits i els elements no estan ordenats.

Principi d'extensionalitat

Un conjunt està determinat pels seus elements: els conjunts A i B són iguals si i només si tenen els mateixos elements. És a dir:

$$A = B \Leftrightarrow \forall x (x \in A \leftrightarrow x \in B).$$

Conseqüències del principi d'extensionalitat

- Dos conjunts diferents difereixen en, almenys, un element.
- No importa com definim un conjunt sinó quins són els seus elements.

Conjunt buit

És el conjunt que no té elements. Notació: $\emptyset = \{\}$.
Pel principi d'extensionalitat, és únic.

Descripció d'un conjunt

Els conjunts es poden denotar per extensió o per comprensió.

Descripció per extensió

Consisteix en anomenar tots els seus elements (*notació de llista*): $A = \{a_1, a_2, \ldots, a_n\}$.
No importa en quin ordre anomenem els seus elements ni si hi ha repeticions en l'enumeració.

En particular, $\emptyset = \{\}$.

Descripció per comprensió

Consisteix en donar una propietat φ que tinguin els elements del conjunt i només ells (*notació de predicat*). Denotarem aquest conjunt per $\{x : \varphi(x)\}$.
Si existeix, és únic, pel principi d'extensionalitat.

Subconjunts

- Un conjunt B és un subconjunt del conjunt A si i només si tot element de B és també element de A.
- Escrivim $B \subseteq A$ per indicar que B és un subconjunt de A. Així doncs:
$$B \subseteq A \Leftrightarrow \forall x\,(x \in B \rightarrow x \in A).$$
- Si B és un subconjunt de A, també diem que B està inclòs en A o que A conté B ($A \supseteq B$).
- Representem per $\not\subseteq$ la relació negada ($B \not\subseteq A$ vol dir que B no és subconjunt de A).

Propietats

Si A, B i C són conjunts, llavors:

1. $A \subseteq A$.
2. Si $A \subseteq B$ i $B \subseteq C$, llavors $A \subseteq C$.
3. $A \subseteq B \wedge B \subseteq A \Leftrightarrow A = B$.
4. Per a tot conjunt A, $\emptyset \subseteq A$.

Observació

La propietat 3 és una reformulació del principi d'extensionalitat i és la que utilitzem habitualment per a demostrar que dos conjunts són iguals.

Inclusió estricta. Subconjunts propis

Subconjunt propi

Un conjunt B és un subconjunt propi del conjunt A si i només si B és un subconjunt de A i $B \neq A$.

Notació: $B \subset A$.

També diem que B està inclòs estrictament a A.

Propietats de la inclusió estricta $\subset$

Si A, B i C són conjunts, llavors:

1. $A \not\subset A$.
2. Si $B \subset A$, llavors $A \not\subset B$.
3. Si $A \subset B$ i $B \subset C$, llavors $A \subset C$.
4. Si $A \neq \emptyset$, llavors $\emptyset \subset A$.

Les notacions $\forall x \in B\ (\varphi)$ i $\exists x \in B\ (\varphi)$

- En matemàtiques, sovint treballem amb afirmacions del tipus $\forall x\,(x \in B \to \varphi)$ o del tipus $\exists x\,(x \in B \wedge \varphi)$, on φ és una propietat.
- Per simplicitat, aquestes afirmacions les solem escriure de la forma: $\forall x \in B\ (\varphi)$ o $\exists x \in B\ (\varphi)$.
- Aquestes notacions són compatibles amb la negació en el sentit següent:

$$\neg\forall x \in B\ (\varphi) \equiv \exists x \in B\ (\neg\varphi), \quad \neg\exists x \in B\ (\varphi) \equiv \forall x \in B\ (\neg\varphi).$$

El conjunt de les parts

Conjunt de les parts d'un conjunt A

És el conjunt que té per elements tots els subconjunts de A.

Notació: $\mathcal{P}(A)$.

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

Propietats

- Per definició: $X \in \mathcal{P}(A) \iff X \subseteq A$.
- En particular: $\emptyset \in \mathcal{P}(A)$ i $A \in \mathcal{P}(A)$, per a tot conjunt A.

Exemples

- $\mathcal{P}(\emptyset) = \{\emptyset\}$.
- Si $A = \{1, 2, 3\}$, llavors:

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}.$$

Nombres binomials

Siguin $n \in \mathbb{N}$ i $0 \leq k \leq n$.

Nombre binomial

Definim el nombre binomial $\binom{n}{k}$ com el nombre de subconjunts amb k elements d'un conjunt amb n elements.

Propietats

1. $\binom{n}{0} = 1$, $\binom{n}{n} = 1$.
2. $\binom{n}{1} = n$, $\binom{n}{n-1} = n$.
3. Simetria: $\binom{n}{k} = \binom{n}{n-k}$.
4. Recurrència: si $0 < k < n$, llavors $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
5. Càlcul directe: $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$.

Fórmula de Newton

Si $n \in \mathbb{N}$, llavors:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Conseqüències

1. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
2. Un conjunt amb n elements té 2^n subconjunts.
3. $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

Operacions amb conjunts

Siguin A, B conjunts.

Definicions

- **Unió de A i B:** és el conjunt que té per elements els objectes que pertanyen a A o a B. Notació: $A \cup B$.
$$A \cup B = \{x : x \in A \vee x \in B\}.$$
- **Intersecció de A i B:** és el conjunt que té per elements els objectes que pertanyen a A i a B. Notació: $A \cap B$.
$$A \cap B = \{x : x \in A \wedge x \in B\}.$$
- **Diferència de A i B:** és el conjunt que té per elements els objectes que pertanyen a A però no a B. Notació: $A - B$ o $A \setminus B$.
$$A - B = \{x : x \in A \wedge x \notin B\}.$$

Propietats de l'unió de conjunts

Propietats

1. $A \cup A = A$.
2. $A \cup B = B \cup A$.
3. $(A \cup B) \cup C = A \cup (B \cup C)$.
   Així podem escriure simplement: $A \cup B \cup C$.
4. $A \cup \emptyset = A$.
5. $A \subseteq A \cup B$, $B \subseteq A \cup B$.
6. $A \subseteq B \iff A \cup B = B$.
7. $A \cup B \subseteq C \iff A \subseteq C \land B \subseteq C$.

Propietats de la intersecció de conjunts

Propietats

1. $A \cap A = A$.
2. $A \cap B = B \cap A$.
3. $(A \cap B) \cap C = A \cap (B \cap C)$. Escrivim: $A \cap B \cap C$.
4. $A \cap \emptyset = \emptyset$.
5. $A \cap B \subseteq A$, $A \cap B \subseteq B$.
6. $A \subseteq B \iff A \cap B = A$.
7. $C \subseteq A \cap B \iff C \subseteq A \wedge C \subseteq B$.

Conjunts disjunts

Diem que A i B són disjunts si $A \cap B = \emptyset$.

Propitats de la diferència de conjunts

Propietats

1. $A - \emptyset = A$, $\emptyset - A = \emptyset$, $A - A = \emptyset$.
2. $A - B \subseteq A$.
3. $(A - B) \cap B = \emptyset$.
4. $A \subseteq B \iff A - B = \emptyset$.
5. $C \subseteq A - B \iff C \subseteq A \wedge C \cap B = \emptyset$.

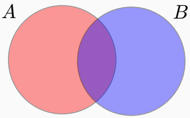
Propietats que relacionen l’unió i la intersecció

Propietats

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
3. $A \cap (A \cup B) = A$.
4. $A \cup (A \cap B) = A$.

Totes aquestes (i altres) propietats es poden visualitzar amb l’ajut dels diagrames de Venn. Per exemple:

$$A \cup B = (A - B) \cup (A \cap B) \cup (B - A).$$



Fixem un conjunt Ω ("univers del discurs") i considerem només subconjunts de Ω.

Complementari d'un subconjunt A de Ω

Si $A \subseteq \Omega$, definim el complementari o el complement de A respecte Ω com el conjunt de tots els elements de Ω que no pertanyen a A. Notació: A^c o $\overline{A}$.

$$A^c = \{x \in \Omega : x \notin A\} = \Omega - A.$$

Propitats de la complementació

Propietats

1. $\emptyset^c = \Omega$, $\Omega^c = \emptyset$.
2. $A^{cc} = A$.
3. $A \cap A^c = \emptyset$, $A \cup A^c = \Omega$.
4. $A \subseteq B \iff B^c \subseteq A^c$.
5. $A \cap B = \emptyset \iff A \subseteq B^c \iff B \subseteq A^c$.
6. $A \cup B = \Omega \iff A^c \subseteq B \iff B^c \subseteq A$.
7. $A - B = A \cap B^c$.
8. Lleis de De Morgan: $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$.

Pel principi d'extensionalitat, $\{x, y\} = \{y, x\}$. Volem un objecte *format* per x i y on l'ordre sigui *important*.

Parell ordenat

El *parell ordenat* de x i y és un objecte, que denotem per (x, y), que compleix que per a cada x, y, z, t:

$$(x, y) = (z, t) \iff x = z \wedge y = t.$$

x: primer component del parell;
y: segon component del parell.

n-pla ordenada

Definim la n-pla $(x_1, x_2, \ldots, x_n)$ amb la propietat:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff \forall i(x_i = y_i).$$

Propucte cartesià dels conjunts A i B

És el conjunt format per tots els parells ordenats (x, y) tals que $x \in A$ i $y \in B$. Notació: $A \times B$.

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

Propucte cartesià dels conjunts $A_1, \ldots, A_n$

Anàlogament, definim el producte cartesià:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, \forall i\}.$$

Propietats

1. $A \times \emptyset = \emptyset \times A = \emptyset$.
2. $A \times B = B \times A \iff A = B \vee A = \emptyset \vee B = \emptyset$.

Relacions

- A més dels objectes, també volem estudiar les relacions que hi ha entre ells; per exemple, i parlant de persones: la relació “ser pare de”, “ser veí de”, “ser més gran que”.
- Matemàticament, les relacions es poden modelar amb l’ajut del concepte de parell ordenat. Així, definim una relació com un conjunt de parells ordenats.
- Si R és una relació, s’escriu $a\,R\,b$ enlloc de $(a, b) \in R$ i es diu que a està relacionat amb b (per la relació R). Quan $(a, b) \notin R$, diem que a no està relacionat amb b. També escrivim: $a \not R\, b$.

Relacions en un conjunt

Relació en un conjunt A

Diem que R és una relació en A si $R \subseteq A \times A$.

Exemples

En qualsevol conjunt A es poden definir les relacions següents:

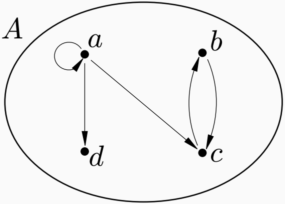
1. La relació identitat en A: $Id_A = \{(x, x) : x \in A\}$.
2. La relació nul·la en A: $R = \emptyset$.
3. La relació total en A: $R = A \times A$.

Diagrama d'una relació

Les relacions en un conjunt A es poden representar amb l'ajut de diagrames. Per exemple, la relació R següent:

$$A = \{a, b, c, d\}, \quad R = \{(a, a), (b, c), (c, b), (a, d), (a, c)\}$$

es pot representar amb:



Sigui R una relació definida sobre el conjunt (no buit) A.

Propietats que pot tenir una relació

- R és reflexiva si i només si $\forall x \in A\,(xRx)$.
- R és simètrica si i només si $\forall x, y \in A\,(xRy \to yRx)$.
- R és antisimètrica si i nomès si $\forall x, y \in A\,(xRy \land yRx \to x = y)$.
- R és transitiva si i només si $\forall x, y, z \in A(xRy \land yRz \to xRz)$.

Relacions d'ordre

R és una relacié d'ordre en A si és reflexiva, antisimètrica i transitiva.

Relacions d'equivalència

R és una relació d'equivalència en A si és reflexiva, simètrica i transitiva.

Particions d'un conjunt

Partició d'un conjunt $A \neq \emptyset$

És una família Π de subconjunts no buits de A disjunts dos a dos i tals que la seva unió és tot A. Formalment:
$\Pi = \{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ tal que:

1. $A_i \neq \emptyset$, per a cada $i \in I$;
2. $A_i \cap A_j = \emptyset$, si $i \neq j$;
3. $A = \bigcup_{i \in I} A_i$.

Els subconjunts A_i s'anomenen les *parts* o *blocs* de la partició.

Sigui $A \neq \emptyset$ un conjunt i R una relació d'equivalència en A.

Classe d'equivalència d'un element

Per a cada $x \in A$, definim la classe d'equivalència de x, que denotem per $[x]_R$, de la manera següent:

$$[x]_R = \{y \in A : yRx\}.$$

Escrivim també $[x]$ o $\overline{x}$, quan no hi ha risc de confusió.

Propietats

1. Per a cada $x \in A$, $x \in [x]$.
2. Per a cada $x, y \in A$, xRy si i només si $[x] = [y]$.
3. $A = \bigcup_{x \in A} [x]$.

Sigui $A \neq \emptyset$ un conjunt i R una relació d'equivalència en A.

Conjunt quocient

El conjunt format per totes les classes d'equivalència s'anomena conjunt quocient de A mòdul R i es representa per A/R:

$$A/R = \{[x]_R : x \in A\}.$$

Propietat

El conjunt quocient A/R és una partició de A.

Relacions d'equivalència i particions

- Tota relació d'equivalència definida en un conjunt A indueix una partició de A: el conjunt quocient A/R.
- Recíprocament, associada a tota partició Π de A, definim una relació R_Π en A:

$$xR_\Pi y \iff \exists B \in \Pi \ (x \in B \wedge y \in B).$$

- La relació R_Π és d'equivalència.

Propietat

1. Si R és una relació d'equivalència en A, llavors $R_{A/R} = R$.
2. Si Π és una partició de A, llavors $A/R_\Pi = \Pi$.

Aplicacions

Aplicacions, visió intuïtiva

Idea intuïtiva

És un algorisme o regla tal que donat un valor d'entrada determina un únic valor de sortida.

Com especificar una aplicació

Per a definir una aplicació cal especificar:

- La "regla" que converteix les entrades en sortides.
- El conjunt de totes les possibles entrades (el domini de la funció).
- El conjunt al qual pertanyen les sortides.

També s'utilitza la paraula 'funció' com a sinònim d'aplicació.

Definició d'aplicació

Definició

Una aplicació o funció del conjunt A en el conjunt B és una relació $f \subseteq A \times B$ que satisfà la propietat següent:

$$\text{per a cada } x \in A \text{ existeix un únic } y \in B \text{ tal que } (x, y) \in f.$$

Notacions

- Si f és una aplicació de A en B, escrivim $f : A \to B$.
- Si $x \in A$, denotem per $f(x)$ l'únic $y \in B$ tal que $(x, y) \in f$ i diem que $f(x)$ és la imatge de x per f.

Restricció d'una aplicació

Si $f : A \to B$ és una aplicació i $A_1 \subseteq A$, la restricció de f a A_1, que denotem per $f_{|A_1}$, és la funció $f_{|A_1} : A_1 \to B$ definida per $f_{|A_1}(x) = f(x)$, per a tot $x \in A_1$.

Igualtat d'aplicacions

Si $f, g : A \to B$ són aplicacions, llavors:

$$f = g \iff \forall a \in A \; (f(a) = g(a)).$$

L'aplicació identitat

L'aplicació identitat $I_A : A \to A$ està definida per: $I_A(x) = x$, per a tot $x \in A$.

Imatges i antiimatges

Sigui $f : A \to B$ una aplicació.

Imatge d'un conjunt per una aplicació

Si $X \subseteq A$, el conjunt imatge de X (o simplement la imatge de X) per f és el conjunt:

$$f[X] = \{f(x) : x \in X\} \subseteq B.$$

Antiimatge d'un conjunt per una aplicació

Si $Y \subseteq B$, el conjunt antiimatge de Y (o simplement la antiimatge de Y) per f és:

$$f^{-1}[Y] = \{x \in A : f(x) \in Y\} \subseteq A.$$

Aplicacions injectives, exhaustives i bijectives

Sigui $f : A \to B$ una aplicació.

Aplicació injectiva

f és injectiva si per a qualsevol $x, y \in A$, si $x \neq y$, llavors $f(x) \neq f(y)$.
Equivalentment: si per a qualsevol $x, y \in A$, si $f(x) = f(y)$, llavors $x = y$.

Aplicació exhaustiva

f és exhaustiva si per a qualsevol $y \in B$, existeix algun $x \in A$ tal que $y = f(x)$.

Aplicació bijectiva

f és bijectiva o una bijecció si és injectiva i exhaustiva alhora.

Composició d'aplicacions

Si $f : A \to B$ i $g : B \to C$ són aplicacions, la composició de f i g és l'aplicació $g \circ f : A \to C$ tal que $(g \circ f)(a) = g(f(a))$, per a tot $a \in A$.

Propietats de la composició

- És associativa: si $f : A \to B$, $g : B \to C$, $h : C \to D$, llavors $h \circ (g \circ f) = (h \circ g) \circ f$.
- En general, no és commutativa: si $f, g : A \to A$, en general no és cert $f \circ g = g \circ f$.
- Si $f : A \to B$, llavors $I_B \circ f = f = f \circ I_A$.

Composició: relació amb la injectivitat i exhaustivitat

Siguin $f : A \to B$, $g : B \to C$ aplicacions.

Propietats

- Si f i g són injectives, llavors $g \circ f$ és injectiva.
- Si $g \circ f$ és injectiva, llavors f és injectiva.
- Si f i g són exhaustives, llavors $g \circ f$ és exhaustiva.
- Si $g \circ f$ és exhaustiva, llavors g és exhaustiva.
- Si f i g són bijectives, llavors $g \circ f$ és bijectiva.
- Si $g \circ f$ és bijectiva, llavors f és injectiva i g és exhaustiva.

Aplicació inversa

Sigui $f : A \to B$ una aplicació bijectiva.
Donat un element $b \in B$:

- f exhaustiva $\Rightarrow$ existeix un $a \in A$ tal que $f(a) = b$;
- f és injectiva $\Rightarrow$ a és únic.

Definició d'aplicació inversa

Definim l'aplicació inversa $f^{-1} : B \to A$ de f com segueix:
donat $b \in B$, $f^{-1}(b)$ és l'únic element $a \in A$ tal que $f(a) = b$.

Aplicació inversa: propietats

Propietats

1. Si f és bijectiva, llavors f^{-1} és bijectiva i $(f^{-1})^{-1} = f$.
2. Si $f : A \to B$ i $g : B \to C$ són bijectives, llavors $g \circ f$ és bijectiva i $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
3. Si f és bijectiva, llavors $f \circ f^{-1} = I_B$, $f^{-1} \circ f = I_A$.
4. $f : A \to B$ és bijectiva si i només si existeix una aplicació $g : B \to A$ tal que $g \circ f = I_A$ i $f \circ g = I_B$. En tal cas, f i g són inverses una de l'altra.