Tema 2: Conjunts i Relacions (bloc 2)

Relacions

Definició

Una *relació n-ària R* entre els conjunts $A_1, \ldots, A_n$ és qualsevol subconjunt

$$R \subseteq A_1 \times \ldots \times A_n.$$

Les més freqüents són les relacions entre dos conjunts:

Definició

Una *relació binària* R entre dos conjunts A i B és un subconjunt

$$R \subseteq A \times B.$$

Dit d'una altra manera, R pot veure's com el graf d'una correspondència de A en B.

Notació:

Si R es una relació entre A i B, el fet que un parell ordenat (a, b) estiga en R sol denotar-se aRb. Així mateix, el fet contrari, és a dir, $(a, b) \notin R$, sol denotar-se $a \not R b$.

Exemples

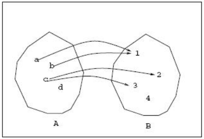
- Si $A = \{1, 2, 3, 4\}$ i $B = \{a, b, c, d\}$ podem definir la següent relació binària entre els conjunts A i B:
$$R = \{(1, b), (1, c), (2, a), (3, a), (3, b)\} \subseteq A \times B.$$
Així, doncs, $1Rb$, $1Rc$, $2Ra$, $3Ra$, $3Rb$, i $4\not R x \ \ \forall\, x \in B$.

- Si $A = B = \mathbb{N}$, podem definir la següent relació binària R entre A i B:
$$aRb \Leftrightarrow a \text{ divideix } b$$
És a dir:
$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ divideix } b\}.$$
Normalment, la condició «a divideix b» s'escriu $a \mid b$.
En aquest cas es té, per exemple, que $3R6$ (o també $(3, 6) \in R$) i que $7\not R 15$ (o també $(7, 15) \notin R$)).

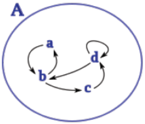
Notació: Quan R siga una relació binària entre A i A direm simplement que «R és una relació binària en A».

Representacions gràfiques

- Siguen $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$ i la relació $R = \{(a, 1), (b, 1), (c, 2), (c, 3)\}$. Veient R com una correspondència entre A i B podem representar-la gràficament amb un diagrama sagital:



- En el cas de relacions binàries en un mateix conjunt, si aquest és finit, es mès adequat representar-les mitjançant *grafs dirigits (o digrafs)*:



  - Els elements del conjunt es representen en un diagrama de Venn.
  - Si a està relacionat amb b, es dibuixa una fletxa orientada de a a b.
  - Si un element està relacionat amb ell mateix, es dibuixa una fletxa que uneix el punt amb si mateix (anomenada *bucle*).

Representació matricial d'una relació binària

Una relació binària admet una representació matricial sempre que els conjunts entre els quals s'estableix la relació siguen finits.

Definició

Si $A = \{a_1, \ldots, a_m\}$ i $B = \{b_1, \ldots, b_p\}$, aleshores la matriu associada a R és la matriu booleana (formada només per uns i zeros) amb m files i p columnes

$$M_R = \begin{pmatrix} r_{11} & \cdots & r_{1p} \\ \vdots & \vdots & \vdots \\ r_{m1} & \cdots & r_{mp} \end{pmatrix} \text{ donada per } r_{ij} = \begin{cases} 1 & \text{si} \quad a_i R b_j \\ 0 & \text{si} \quad a_i \not R\, b_j \end{cases}$$

Exemple:

Si entre els conjunts $A = \{2, 3, 5\}$ y $B = \{4, 6, 9, 10\}$ es defineix la relació

$$R := \{(2,4), (2,6), (2,10), (3,6), (3,9), (5,10)\} \subseteq A \times B$$

(és a dir, aRb si i només si $a \mid b$), aleshores la matriu associada a R és

$$M_R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Operacions amb relacions

Com que una relació és un subconjunt de $A_1 \times A_2 \times \cdots \times A_n$, donades dues relacions R i S entre els mateixos conjunts podem definir, de manera òbvia, les operacions $R \cup S$, $R \cap S$, R^c i $R \setminus S$.
A més, els conceptes i operacions que vejerem per a correspondències poden reinterpretar-se amb la notació de parells ordenats per a relacions binàries:

- $\mathrm{Dom}\, R = \{a \in A \mid \exists b \in B, (a, b) \in R\}$.
- $\mathrm{Im}\, R = \{b \in B \mid \exists a \in A, (a, b) \in R\}$.
- Si R és una relació binària entre A i B, la relació inversa de R és $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$ (que és una relació entre B i A).
- Si R és una relació binària entre A i B, i S és una relació binària entre B i C, la composició $S \circ R$ és la següent relació entre A i C:

$$S \circ R = \{(a, c) \in A \times C \mid \exists\, b \in B \text{ amb } (a, b) \in R \text{ i } (b, c) \in S\}.$$

1. Conceptes bàsics
2. Relacions binàries en un conjunt
3. Relacions d'ordre
4. Relacions d'equivalència

Propietats d'una relació binària en un conjunt

D'entre les diverses propietats que pot (o no) tenir una relació binària R en un conjunt A, les més interessants són les següents:

- Una relació R en un conjunt A és *reflexiva* si tot element de A està relacionat amb ell mateix:

  $$aRa, \ \forall a \in A.$$

  . Equivalentment, $\Delta \subseteq R$, on $\Delta = \{(a, a) \mid a \in A\}$ és la relació d'igualtat en el conjunt A.

- R es *simètrica* si sempre que a està relacionat amb b, aleshores b también està relacionat amb a:

  $$aRb \Rightarrow bRa, \ \forall a, b \in A,$$

  o equivalentement, $R = R^{-1}$.

Propietats d'una relació binària en un conjunt

- R és *antisimètrica* si no és possible que a estiga relacionat amb b i que b estiga relacionat amb a si $a \neq b$:

$$a \neq b \wedge aRb \Rightarrow b \not{R} a, \quad \forall a, b \in A,$$

o equivalentement,

$$aRb \wedge bRa \Rightarrow a = b, \quad \forall a, b \in A.$$

Açò equival també a que $R \cap R^{-1} \subseteq \Delta$.

- R es *transitiva* si sempre que a està relacionat amb b i b amb c, aleshores a està relacionat també amb c:

$$aRb \wedge bRc \Rightarrow aRc, \quad \forall a, b, c \in A,$$

o equivalentement, $R \circ R \subseteq R$.

Interpretació matricial de les propietats

Si R és una relació binària en un conjunt finit A y M_R és la matriu associada, aleshores:

- R és reflexiva $\iff$ M_R té un 1 en totes les posicions de la diagonal principal.
- R és simètrica $\iff$ $M_R = {M_R}^t$ (es a dir, si M_R és una matriu simètrica).
- R és antisimétrica $\iff$ no existeixen fora de la diagonal dos posicions simétricas els valors de les quals siguen 1 simultàniament.

No ens detindrem en la interpretació matricial de la propietat transitiva (per a això es necessita conèixer l'operació *"producte booleà"* de matrius booleanes i la seva relació amb la composició de relacions). Si esteu interessats, podeu consultar-ho en el capítol 13 del llibre de Robert Fuster.

Definició

Una relació R en un conjunt A és d'ordre si és reflexiva, antisimètrica i transitiva.

Exemples (de relacions de'ordre):

1. la inclusió entre conjunts,
2. la desigualdad entre nombres,
3. la relación de divisibilitat entre nombres naturals.

Notació: Si R és una relació d'ordre i aRb solem dir que «a és anterior a b» o que «b és posterior a a». A vegades, es sol representar la relació amb el símbol $\preceq$

Definició

Una relació d'ordre R es diu que és *d'ordre total* si

$$\forall x, y \in A, \quad (xRy) \vee (yRx).$$

Diagrames de Hasse

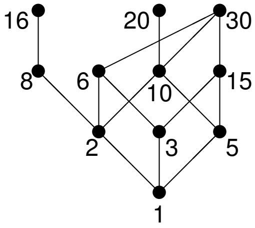
Si en un conjunt *finit* A tenim definida una relació R, podem representar-la gràficament per un diagrama sagital. Aquest diagrama pot «simplificar-se» *quan R és una relació d'ordre* de la següent manera:

- S'eliminen els bucles que indiquen que se satisfà la propietat reflexiva.
- S'eliminen les fletxes que poden deduir-se de la propietat transitiva, és a dir, sempre que aRb i bRc, s'elimina la fletxa corresponent a aRc (perquè es dedueix de les altres dues).
- Finalment, es dibuixa el diagrama escrivint els elements de forma «ascendent», substituint les fletxes per segments. És a dir, si aRb, se situa a per baix de b i es dibuixa un segment ascendent des de a fins a b.

El diagrama resultant s'anomena diagrama de Hasse.
Observem que un element a és anterior a un altre b si existeix un camí ascendent de a a b. A més, cal recordar que tot element és anterior a si mateix (por la propietat reflexiva).

Exemple: relació de divisibilitat

Siga $A = \{1, 2, 3, 5, 6, 8, 10, 15, 16, 20, 30\}$ i considerem en A la relació de divisibilitat (representada per $|$). El diagrama de Hasse d'aquesta relació ve representat per la figura següent:



Observem que 2 està relacionat amb 30, ja que existeix almenys un camí ascendent. En canvi, 2 i 15 no ho estan, per no existir un camí ascendent entre aquests nombres.

Elements notables d'un conjunt ordenat

Siga A un conjunt dotat d'una relació d'ordre $\preceq$.

- Un element $m \in A$ és màxim si $\forall x \in A$, $x \preceq m$.
- Un element $m \in A$ és mínim si $\forall x \in A$, $m \preceq x$.
- Un element $m \in A$ és maximal si

  $$\forall x \in A \quad (m \preceq x \rightarrow m = x),$$

  és a dir, si no existeix cap element de A que siga posterior a m.
- Un element $m \in A$ és minimal si

  $$\forall x \in A \quad (x \preceq m \rightarrow m = x),$$

  és a dir, si no existeix cap element de A que siga anterior a m.

Nota: Si un conjunt ordenat té mínim, aquest és únic i és l'únic minimal. Anàlogament amb el màxim.

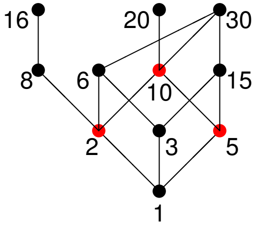
Elements notables d'un subconjunt d'un conjunt ordenat

Siga A un conjunt dotat d'una relació d'ordre $\preceq$, i siga B un subconjunt de A.

- Es diu que $a \in A$ és una cota superior o una *fita superior* de B si $\forall x \in B$, $x \preceq a$. Si B té cotes superiors, es diu que B està *acotat superiorment* o *fitat superiorment*.
- Es diu que $a \in A$ és una cota inferior o una *fita inferior* de B si $\forall x \in B$, $a \preceq x$. Si B té cotes inferiors, es diu que B està *acotat inferiorment* o *fitat inferiorment*.
- Es diu que $a \in A$ és el suprem de B ($\sup B$) si a és la mínima cota superior de B (és a dir, el mínim del conjunt de les cotes superiors de B).
- Es diu que $a \in A$ és l'ínfim de B ($\inf B$) si a és la màxima cota inferior de B (és a dir, el màxim del conjunt de les cotes inferiors de B).

Exemple

Tornem a l'exemple anterior:



Si considerem el subconjunt $B = \{2, 10, 5\}$, aleshores les cotes superiores de A són 10, 20 i 30, i el seu suprem és 10. La única cota inferior de B és 1 i, per tant, també és el seu ínfim. A més, el màxim de B es 10, B no té mínim, 10 és un maximal i els minimales de B són 2 i 5.

Definició

Una relació binària R en un conjunt A és d'equivalència si és reflexiva, simètrica i transitiva.

Com a exemples típics de relacions d'equivalència d'entre els estudiats anteriorment en aquesta assignatura, podem citar l'equivalència lògica, la igualtat de conjunts.

Definició

Si R és una relació d'equivalència, s'anomena classe d'equivalència de $a \in A$ respecte de R al conjunt

$$[a] = \bar{a} = [a]_R := \{x \in A \mid aRx\}.$$

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

$$A/R := \{[a] \mid a \in A\}.$$

Propietats

(1) Si R és una relació d'equivalència en un conjunt A, aleshores

$$aRb \Longleftrightarrow [a] = [b].$$

(2) El *conjunt quocient* defineix una *partició* del conjunt A.

Exemple: En el conjunt $A = \{1, 2, 3, 4, 5\}$ considerem la relación d'equivalència
$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 1), (2, 4), (4, 2)\}$.
Es comprova que

$$[1] = [3] = \{1, 3\}$$
$$[2] = [4] = \{2, 4\}$$
$$[5] = \{5\}$$

Així, el conjunt quocient és

$$A/R = \{[1], [2], [5]\}.$$

Exemple: relació de congruència

Donat un nombre enter positiu m definim, en el conjunt dels nombres enters $\mathbb{Z}$, la següent relació binària:

$$\forall a, b \in \mathbb{Z}, \qquad aRb \iff a - b \text{ és un múltiple de } m.$$

- R és una relació d'equivalència, anomenada *relació de congruència mòdul m*.
- El conjunt quocient $\mathbb{Z}/R$ el denotarem per $\mathbb{Z}_m$ i s'anomena «conjunt dels enters mòdul m».
- Si $\bar{a}$ és la classe d'equivalència del nombre enter a, aleshores
$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$$
- Per a aquesta relació binària en particular, en comptes de aRb s'escriu
$$a \equiv b \pmod{m}$$
i es llig «a és congruent amb b mòdul m».

Aplicacions dels enters mòdul m

- Digits de control
  - Nombres d'identificació personal (com el NIF)
  - Nombres d'identificació de llibres (com el ISBN)
  - Codis bancaris (com el número de compte bancari)
  - Codis de barra
- Seguritat en la transmissió de missatges (Criptologia)
  - Sistemes de clau privada
  - Sistemes de clau pública (com el RSA)
- Assignació de segments de memòria en un ordinador (Funcions hashing)