

Logică și structuri discrete

Mulțimi

Marius Minea

marius@cs.upt.ro

<http://www.cs.upt.ro/~marius/curs/lsd/>

13 octombrie 2014

Ce sunt mulțimile?

Mulțimea e un concept matematic *fundamental*. Am putea spune:

O mulțime e o *colecție* de obiecte numite *elementele* mulțimii.

... dar definiția dată e *informală*: ca să fie riguroasă, ar trebui să definim precis ce e o *colecție*.

Două noțiuni distincte: *element* și *mulțime*

$x \in S$: elementul x *aparține* mulțimii S

$x \notin S$: elementul x *nu aparține* mulțimii S

Spre deosebire de liste:

Elementele unei mulțimi *nu* sunt ordonate

Un element *nu* apare de mai multe ori

(Dar: există noțiunea de *multiset*: fiecare element e caracterizat prin numărul de apariții)

Noțiunea formală de mulțime e datorată lui Georg Cantor (1879).

Vom discuta pe scurt și despre formalizarea ei.

Moduri de definire

1. Prin *enumerarea* elementelor:

$$A = \{a, b, c\}, \quad D = \{1, 2, 3, 6\} = \text{mulțimea divizorilor lui } 6$$

Elementele mulțimii se scriu între acolade, separate prin virgulă.

2. Printr-o *proprietate* caracteristică

$$S = \{x \mid x \text{ are proprietatea } P(x)\}$$

$$D(n) = \{d \in \mathbb{N} \mid n \bmod d = 0\} \text{ (mulțimea divizorilor lui } n)$$

Știm: mulțimea numerelor naturale \mathbb{N} , întregi \mathbb{Z} , raționale \mathbb{Q} , reale \mathbb{R} , ...

Submulțimi

A e o *submulțime* a lui B :

$A \subseteq B$ dacă fiecare element al lui A e și un element al lui B .

A e o *submulțime proprie* a lui B : $A \subset B$

dacă $A \subseteq B$ și există cel puțin un element $x \in B$ așa încât $x \notin A$.

Obs. \in e o relație între un *element* și o mulțime.

\subseteq (și \subset) sunt relații între *două mulțimi*.

Obs. Ca să demonstrăm $A \not\subseteq B$ e suficient să găsim un element $x \in A$ pentru care $x \notin B$.

Dacă $A \subseteq B$ și $B \subseteq A$, atunci $A = B$ (mulțimile sunt egale)

asa putem demonstra egalitatea unor mulțimi definite prin proprietățile lor

Operații de bază

Reuniunea a două mulțimi:

$$A \cup B = \{x \mid x \in A \text{ sau } x \in B\}$$

Intersecția a două mulțimi:

$$A \cap B = \{x \mid x \in A \text{ și } x \in B\}$$

Diferența a două mulțimi:

$$A \setminus B = \{x \mid x \in A \text{ și } x \notin B\}$$

Uzual, discutăm într-un *context*: avem un *univers* (de discurs) U al tuturor elementelor la care ne-am putea referi.

Complementul unei mulțimi (în raport cu universul U):

$$A^c = \{x \in U \mid x \notin A\} = U \setminus A$$

(uneori notat și \bar{A})

Pot fi reprezentate prin *diagrame Venn*

Mulțimile, fundament al matematicii

Practic toată matematica poate fi formalizată în teoria mulțimilor (sau în logică, de care e strâns legată, după cum vom vedea).

Exemplu: o *pereche* (deși e ordonată!) poate fi definită ca:

$$(a, b) = \{\{a\}, \{a, b\}\} \quad (\text{definiția lui Kuratowski})$$

cum putem extrage pe a și b fiind dată perechea (a, b) ?

Numerele naturale au fost formalizate de Peano:

0 e un număr natural

dacă n e un număr natural, $S(n)$ e un număr natural

(funcția succesori S e injectivă, și $S(n) \neq 0$ pentru orice n)

Putem să (re)definim, folosind mulțimi:

$$0 \stackrel{\text{def}}{=} \emptyset$$

$$S(n) \stackrel{\text{def}}{=} n \cup \{n\}$$

Paradoxul lui Russell

De obicei, o mulțime nu se conține pe ea însăși ca element: $X \notin X$.

Caracterizăm toate aceste mulțimi:

$$R = \{X \mid X \notin X\}$$

Mulțimea R se conține pe ea însăși sau nu?

dacă $R \in R$, pentru a satisface condiția de definiție, avem $R \notin R$.

dacă $R \notin R$, atunci cum R satisface condiția, avem $R \in R$

paradox!

Reformulare similară: “paradoxul bărbierului”:

Bărbierul bărbierește exact oamenii care nu se bărbieresc singuri.

Bărbierul se bărbierește pe el însuși sau nu ?

Paradoxul a pus probleme serioase formalizării logicii matematice

Poate fi evitat în mai multe feluri:

de exemplu, oricând definim o mulțime printr-o proprietate, trebuie să specificăm universul din care își poate lua elementele:

$$R = \{X \mid X \subseteq U \text{ și } X \notin X\}$$

Axiome despre mulțimi

O *axiomă* e o propoziție presupusă adevărată.
E un punct de plecare pentru un raționament.

Exemple de axiome în teoria mulțimilor (există mai multe *sisteme axiomatice*, ex. sistemul *Zermelo-Fraenkel*)

Axioma mulțimii vide (existență):

Există o mulțime care nu are niciun element

Axioma extensivității:

Două mulțimi sunt egale dacă și numai dacă au aceleași elemente (dacă fiecare element al lui A e și un element al lui B , și reciproc)

...

Axiome ale teoriei mulțimilor (cont.)

Axioma regularității (a fundației)

Orice mulțime nevidă are un element $x \in A$ disjunct de ea: $x \cap A = \emptyset$

Implică faptul că nu există un șir infinit $A_0, A_1, \dots, A_n \dots$ astfel încât

$$A_0 \ni A_1 \ni \dots \ni A_n \ni \dots$$

(rezultă și că nicio mulțime nu se poate avea ca element, $X \notin X$, altfel ar exista un astfel de șir)

Intuitiv, spune că orice mulțime e formată din elemente (posibil mulțimi) mai simple, care la rândul lor conțin elemente mai simple, până ajungem la elemente fundamentale

\Rightarrow elimină paradoxul lui Russell

Algebra Booleană a mulțimilor

Noțiune datorată matematicianului George Boole (sec. 19)
Operațiile unei algebre Boolene (aici \cup și \cap) satisfac legile:

Comutativitate: $A \cup B = B \cup A$ $A \cap B = B \cap A$

Asociativitate: $(A \cup B) \cup C = A \cup (B \cup C)$ și
 $(A \cap B) \cap C = A \cap (B \cap C)$

Distributivitate: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ și
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Identitate: există două valori (aici \emptyset și U) astfel ca:
 $A \cup \emptyset = A$ $A \cap U = A$

Complement: orice A are un complement A^c (sau \bar{A}) astfel ca:
 $A \cup A^c = U$ $A \cap A^c = \emptyset$

Algebra Booleană a mulțimilor (cont.)

Alte proprietăți (pot fi deduse din cele de mai sus):

Idempotență: $A \cup A = A$ $A \cap A = A$

Absorbție: $A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$

Dublu complement: $(A^c)^c = A$

Complemente elementelor identitate: $\emptyset^c = U$ $U^c = \emptyset$

Limită universală: $A \cup U = U$ $A \cap \emptyset = \emptyset$

Legile lui de Morgan:

$$(A \cup B)^c = A^c \cap B^c \quad (A \cap B)^c = A^c \cup B^c$$

Partiție a unei mulțimi

O *partiție* a unei mulțimi A e o colecție de mulțimi P_1, P_2, \dots astfel încât:

- ▶ mulțimile P_1, P_2, \dots sunt nevide și mutual disjuncte, adică $P_i \cap P_j = \emptyset$, pentru orice $i \neq j$
- ▶ A e reuniunea tuturor mulțimilor P_i : $A = \bigcup_i P_i$

Dacă \mathcal{A} e o colecție de mulțimi, definim

$$\bigcup_{A \in \mathcal{A}} A = \{x \mid x \in A_i \text{ cu } A_i \in \mathcal{A}\}$$

În particular, notăm $\bigcup_{i=1}^n A_i = A_1 \cup \dots \cup A_n$ și

$$\bigcup_{i \in \mathbb{N}} A_i = A_0 \cup \dots \cup A_n \cup \dots \quad (\text{reuniune infinită de mulțimi})$$

La fel pentru intersecție.

Cardinalul unei mulțimi

Cardinalul (cardinalitatea) unei mulțimi A e numărul de elemente al mulțimii. Îl notăm $|A|$.

Putem avea mulțimi *finite* sau *infinite*

Dacă A e o mulțime finită și P_1, \dots, P_N o partiție a ei, atunci

$$|A| = |P_1| + \dots + |P_n|$$

Cardinalul uniunii / intersecției / diferenței

Pentru mulțimi *finite*:

Legea reuniunii:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Legea diferenței:

$$|A \setminus B| = |A| - |A \cap B|$$

Putem demonstra considerând cele 2x2 cazuri posibile:

$A \cap B$, $A \cap B^c$, $A^c \cap B$ și $A^c \cap B^c$ formează o *partiție* a universului

$$A = (A \cap B) \cup (A \cap B^c) \text{ (partiție)} \Rightarrow |A| = |A \cap B| + |A \cap B^c|$$

$$\text{La fel, } |B| = |A \cap B| + |A^c \cap B|$$

$$\text{și } |A \cup B| = |A \cap B| + |A \cap B^c| + |A^c \cap B|$$

de unde, combinând, rezultă egalitățile de mai sus.

Principiul includerii și excluderii

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Mai general,

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n|$$

Demonstrație: prin inducție după n

Tupluri și produsul cartezian

Un *n-tuplu* e un șir de n elemente (x_1, x_2, \dots, x_n)
(nu neapărat distincte, iar ordinea elementelor contează).

Cazuri particulare: *pereche* (a, b) , *triplet* (x, y, z) , etc.

Produsul cartezian a două mulțimi e mulțimea perechilor

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Exemplu: mulțimea numerelor complexe poate fi văzută ca produs cartezian $\mathbb{R} \times \mathbb{R}$ (putem găsi o *bijecție* între ele)

Produsul cartezian a n mulțimi e mulțimea *n-tuplilor*

$$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) \mid x_i \in A_i, 1 \leq i \leq n\}$$

Dacă mulțimile sunt finite, atunci

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n|$$

Mulțimea submulțimilor

Mulțimea submulțimilor (engl. power set) a unei mulțimi S , notată $\mathcal{P}(S)$ (uneori 2^S):

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}$$

Exemplu, pentru $S = \{a, b, c\}$, avem

$$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Dacă S e finită, atunci $|\mathcal{P}(S)| = 2^{|S|}$

Există o bijecție între $\mathcal{P}(S)$ și mulțimea funcțiilor $f : S \rightarrow \{0, 1\}$ dacă $f(x) = 1$, x aparține submulțimii, altfel nu.
numărul funcțiilor e $|\{0, 1\}|^{|S|} = 2^{|S|}$

Mulțimi numărabile și nenumărabile

O mulțime e *numărabilă* dacă are cardinalul egal cu cardinalul unei submulțimi a numerelor naturale. Altfel spus, formal:

O mulțime S e *numărabilă* dacă există o funcție injectivă $f : S \rightarrow \mathbb{N}$

Orice mulțime finită e numărabilă: $|A| = n \Rightarrow A = \{a_1, a_2, \dots, a_n\}$
(indicii reprezintă corespondența cu $\{1, 2, \dots, n\}$)

Dar nu orice mulțime numărabilă e finită (evident, \mathbb{N} e numărabilă)
(în definiție, alegem f funcția identitate).

\mathbb{Z} e numărabilă: putem enumera: $0, -1, 1, -2, 2, \dots$

$f(x) = 2x$, pentru $x \geq 0$, $f(x) = -2x - 1$ pentru $x < 0$

Definiție echivalentă: S e numărabilă dacă e fie finită, fie există o bijecție între S și \mathbb{N} (e infinit numărabilă).

Numerele raționale sunt numărabile

$1/1$	$1/2$	$1/3$	$1/4$	\dots
$2/1$	$2/2$	$2/3$	$2/4$	\dots
$3/1$	$3/2$	$3/3$	$3/4$	\dots
\dots	\dots	\dots	\dots	\dots

Numărăm pe diagonale

(după valoare crescătoare a lui $m + n$, numărător + numitor):

$1/1, 1/2, 2/1, 1/3, 2/2, 3/3, \dots$

\Rightarrow Orice element va fi numărat

Exercițiu: care e numărul de ordine al lui m/n ?

Realii sunt nenumărabili

construcția diagonală a lui Cantor:

Reprezentăm numerele subunitare în baza 2: cifrele sunt 0 și 1

Exemplu:

$$0.01101\dots = 0 + 0 \cdot 2^{-1} + 1 \cdot 2^{-2} + 1 \cdot 2^{-3} + 1 \cdot 2^{-4} + 1 \cdot 2^{-5} + \dots$$

Presupunem prin reducere la absurd că realii din $[0, 1)$ ar fi numărabili

\Rightarrow am putea scrie realii subunitari într-un tabel, după numărul de ordine

$r_1 = 0.$	d_{11}	d_{12}	d_{13}	\dots	$0.1011101\dots$
$r_2 = 0.$	d_{21}	d_{22}	d_{23}	\dots	$0.0110010\dots$
$r_3 = 0.$	d_{31}	d_{32}	d_{33}	\dots	$0.1101101\dots$
\dots	\dots	\dots			

Construim un număr real $x = 0.d_1d_2d_3\dots$ cu următoarele cifre:

$d_i = 1 - d_{ii}$ (urmărind diagonala matricii, schimbăm $0 \leftrightarrow 1$)

Dar x diferă de toate numerele din tabel (diferă de r_i la poziția i)!

Deci *mulțimea realilor \mathbb{R} e nenumărabilă !*

Există oricâte infinituri

Teorema lui Cantor: *Nu există bijectie* de la X la $\mathcal{P}(X)$.

Să presupunem că ar exista o bijectie $f : X \rightarrow \mathcal{P}(X)$.

Formăm mulțimea:

$$Y = \{x \in X \mid x \notin f(x)\}$$

Cum $Y \in \mathcal{P}(X)$, și f e bijectie, există $y \in X$ cu $f(y) = Y$.

Dacă $y \in Y$, cum $Y = f(y)$ atunci $y \in f(y)$, și nu respectă condiția de construcție a lui Y , deci $y \notin Y$, contradicție.

Dacă $y \notin Y$, atunci $y \notin f(y)$ și satisface condiția pentru Y , deci $y \in Y$, contradicție.

Deci presupunerea e falsă, nu poate exista o bijectie.

Construcția seamănă cu cea din paradoxul lui Russell, dar cu alt scop: demonstrația prin *reducere la absurd*.

Deci $|\mathbb{N}|$, $|\mathcal{P}(\mathbb{N})|$, $|\mathcal{P}(\mathcal{P}(\mathbb{N}))|$, ... sunt infinități tot mai mari, incomparabile!

Calculabilitate și problema opririi programelor

engl. the *Halting Problem*: pusă de Alan Turing
mașina (automatul) lui Turing: model simplu, universal de calcul

Nu există algoritm (program) care acceptă un program arbitrar P și un set de date D și determină dacă programul P se va opri sau va rula la infinit pe datele de intrare D .

Presupunem că ar exista un astfel de program $CheckHalt(P, D)$.
Putem folosi textul lui P ca date pentru P : $CheckHalt(P, P)$.

Definim un nou program $Test(X)$ care are ca intrare un program X și are efect opus răspunsului $CheckHalt(X, X)$:

dacă $CheckHalt(X, X)$ scrie "halt", atunci **ciclează** la infinit
altfel (dacă $CheckHalt(X, X)$ scrie "ciclează"), **se oprește**

$Test(Test)$ se oprește? Putem întreba pe $CheckHalt(Test, Test)$.
Dar $Test(Test)$ e definit să facă invers de cum spune $CheckHalt$!
⇒ **contradicție**, deci nu poate exista $CheckHalt$!