

Capitolul 1

Funcții booleene

Scopul acestui capitol îl constituie familiarizarea cititorului cu o clasă particulară de funcții – **clasa funcțiilor booleene**. Aceste funcții, deși au o mulțime de definiție (un **domeniu**) și o mulțime de valori (un **codomeniu**) aparent simple, au proprietăți locale și globale foarte utile. Teoria dezvoltată pentru ele constituie de fapt **baza** conceptuală și concretă a **semanticii** logicii propoziționale în sens clasic (și nu numai). Schimbând semnificația simbolurilor 0 și 1 din **cifră** în **valoare de adevăr** (**fals**, respectiv **adevărat**), a operațiilor $+$ și $-$, etc., din **adunare** (de exemplu, *adunarea în mulțimea numerelor naturale* sau *adunarea modulo 2*) și **opus**, în **disjuncție**, respectiv **negație** (ca operații cu valori de adevăr), etc., multe rezultate din logică pot fi ulterior deduse printr-o simplă „traducere”. Anumite noțiuni și proprietăți specifice funcțiilor booleene nu sunt direct și neapărat necesare în studiul logicii formale, astfel încât subiectul nu este tratat în detaliu.

Vom introduce - cât mai succint și la un nivel informal - și alte noțiuni, notații sau rezultate necesare pentru îmbunătățirea înțelegerii majoritatea de *natură algebrică* ([DID]) sau de *informatică elementară* ([SOR]). În primul rând, chiar din manualele de matematică de liceu sunt bine cunoscute cel puțin două modalități de a *prezenta* o mulțime:

- **Prin enumerarea elementelor sale.** $N = \{0, 1, 2, \dots\}$ este mulțimea numerelor naturale.

- **Prin specificarea unei proprietăți caracteristice.** $A = \{x \in \mathbf{R} \mid x^2 + 9x - 8 = 0\}$, este mulțimea rădăcinilor reale ale unei ecuații polinomiale de gradul al II-lea.

Mai există o modalitate de specificare, care, fără a fi fost tratată în mod explicit, a fost totuși suficient de des utilizată (în ideea constructivistă, [CAZ2], [RIC]). Aceasta poate fi descrisă pe scurt astfel: ***A este cea mai mică mulțime care conține elementele ... și care este închisă la operațiile ...***. De exemplu, dacă notăm cu 0 *cel mai mic (primul)* număr natural și, pentru fiecare n , număr natural, cu $S(n)$ *succesorul său imediat*, mulțimea \mathbf{N} poate fi definită (în ideea de mai sus) **constructiv** sau **structural** (ea este de fapt o *mulțime bine-ordonată*, [ȚIP]), astfel:

Baza. $0 \in \mathbf{N}$ (*zero* este număr natural).

Pas constructiv (structural). Dacă $n \in \mathbf{N}$, atunci $S(n) \in \mathbf{N}$ (dacă n este număr natural, atunci *succesorul său imediat* este număr natural).

Nimic altceva nu mai este număr natural.

Prin urmare, \mathbf{N} este o mulțime care conține (*inițial*) elementul numit 0. Se introduc apoi *elemente noi folosind elemente „vechi”* (*deja existente în mulțime*) și *simbolul (operatorial) S*. Procesul continuă *cât timp este posibil* (în cazul de mai sus, el *continuă „la infinit”*). Pentru ca \mathbf{N} să fie într-adevăr cea mai mică mulțime construită în felul descris, am adăugat, în plus față de **Bază** și **Pasul constructiv**, condiția **nimic altceva nu mai este număr natural** (în cele ce urmează, ultimul text va fi implicit presupus a fi prezent).

Soluția adoptată pentru această a treia cale de descriere a unei mulțimi are avantajul de a avea și o caracteristică de natură (semi)algoritmică. Acceptăm astfel **paradigma imperativă** propusă de D. Knuth ([KNU]), $Algoritm = Date + Operații$. Mai exact, un **algoritm (imperativ)** reprezintă o secvență finită de pași (instrucțiuni), care descriu operații precise asupra unor informații (date) inițiale (de intrare) sau intermediare (de lucru, temporare), în vederea obținerii unor informații (rezultate) finale (de ieșire). Pașii **se execută** (operațiile se efectuează în mod concret) în ordinea scrierii lor în secvență. Un algoritm **calculează o funcție** sau **rezolvă o problemă** ([CRO], [SOR]). Intuitiv, datele de intrare reprezintă elemente din domeniul de definiție al funcției de calculat (sau *informațiile inițiale* din realitatea în care își are originea problema pe care vrem să o rezolvăm), iar datele de ieșire sunt elemente din codomeniul funcției (respectiv, *soluțiile* problemei). Un algoritm **se termină** pentru toate intrările admise, prin urmare **există întotdeauna un ultim pas**, a cărui execuție marchează de obicei și obținerea rezultatelor de ieșire. Din motive tehnice, vom lua uneori în considerare și *algoritmi care nu se termină pentru toate intrările*, pe care-i vom numi **semialgoritmi (proceduri)**. Un (semi)algoritm poate fi descris sub mai multe forme, printre care se numără și **pseudocodul** (limbaj intermediar între limbajul natural și un limbaj de programare comercial). Astfel, definiția constructivă a lui **N** poate deveni, în *limbaj algoritmic* (pseudocod, [IVA]):

Intrare: -.

Ieșire: N.

Metodă:

Pas 1: $N := \{0\}$.

Pas 2: **Cât_timp** (*este posibil*) **execută**

Pas 3: Alege $n \in N$.

Pas 4: $N := N \cup \{S(n)\}$.

Sf_Cât_timp.

Desigur că în cele de mai sus 0 putea fi introdus „din exterior”, adică în **Intrare**. Înafara *instrucțiunii de ciclare cu un număr necunoscut de pași* (**Cât_timp** (<condiție>) **execută** <corp> **Sf_Cât_timp**) și a celei de *asignare* (<variabilă> := <valoare>), în descrierea algoritmilor imperativi vom mai folosi *selecția* (**Dacă** (<condiție>) **atunci** <corp> **altfel** <corp> **Sf_Dacă**) și *instrucțiunea de ciclare cu un număr cunoscut de pași* (**Pentru** <variabilă> = <valoare inițială>, <indice>, <valoare finală> **execută** <corp> **Sf_Pentru**). Câteodată vom întrebuința și varianta **Repetă** <corp> **Până_când** (<condiție>) **Sf_Repetă** pentru o instrucțiune de ciclare. Presupunând că semnificația intuitivă a instrucțiunilor de mai sus este cunoscută de către cititor, vom mai face precizări și completări pe parcursul lucrării legate de conceptul de algoritm, cum ar fi prezentarea pe scurt a conceptelor de **corectitudine**, **complexitate**, **tratabilitate**. Orice manual de introducere în programarea imperativă poate fi folositor celor care nu stăpânesc asemenea noțiuni (de exemplu, [COR], [AHO],

[LUC]). Revenind la definițiile constructive – care „ascund” și ideea de **recursivitate** în programare - ele au și alte avantaje. *Un prim* avantaj este acela că se poate folosi aceeași metodă pentru a introduce alte definiții, care sunt legate de mulțimea respectivă în totalitatea ei. Putem da astfel o definiție constructivă (recursivă) a adunării numerelor naturale, *pe care o vom folosi de altfel în Capitolul 5*, după cum urmează.

Baza: $x + 0 = x$, pentru fiecare $x \in \mathbf{N}$ (a aduna 0 la orice număr natural înseamnă a-l lăsa neschimbat).

Pas constructiv: $x + S(y) = S(x + y)$, pentru fiecare $x, y \in \mathbf{N}$ (dacă știm să calculăm $x + y$ și cunoaștem succesorul imediat al numărului natural y , atunci știm să calculăm și suma $x + S(y)$; mai exact, aceasta coincide cu succesorul imediat al numărului care reprezintă suma $x + y$).

Un al doilea – și cel mai important – avantaj este posibilitatea folosirii în demonstrații a **principiului inducției structurale**:

*Fie A o mulțime definită constructiv, $A' \hat{=} A$ mulțimea **elementelor inițiale** (definite prin pasul **Baza** al definiției) și P o afirmație care trebuie demonstrată pentru toate elementele lui A . Acceptăm că $P(a)$ este adevărată pentru fiecare $a \hat{=} A$ dacă și numai dacă:*

1. (Baza.) *Arătăm că $P(a)$ este adevărată pentru fiecare $a \hat{=} A'$.*

2. (Pas inductiv.) *Fie orice $b \hat{=} A$, element nou obținut din elementele deja construite a_1, a_2, \dots, a_n , cu ajutorul operatorului f (vom conveni să*

scriem acest lucru prin $b = f(a_1, a_2, \dots, a_n)$, deși relația dintre elementele vechi și cele noi nu este întotdeauna de natură funcțională) și presupunem că este adevărată $P(a_i)$ pentru fiecare $a_i \in \{1, 2, \dots, n\}$. Arătăm că este adevărată $P(b)$.

Observație. Principiul inducției matematice (naturale) așa cum este el cunoscut din matematica de liceu, este un caz particular al principiului inducției structurale (după cum se observă imediat). Folosim cuvântul *principiu* în loc de *teoremă* (care trebuie să aibă și o *demonstrație* aferentă) deoarece în cele de mai sus doar *stipulăm* că formulele $(\forall n)P(n)$ și respectiv $P(0) \wedge (\forall n)(P(n) \text{ implică } P(n+1))$ sunt *tare echivalente* (în sensul care va fi precizat în **Capitolul 2**). În cele de mai sus, $P(0)$ poate fi înlocuit și cu orice $P(k)$, k – număr natural fixat, deoarece și submulțimea lui \mathbf{N} , $\{k, k + 1, \dots\}$ este *bine-ordonată*; în acest caz, locul lui $(\forall n)$ este luat de $(\forall n \geq k)$. Echivalența amintită, deși *adevărată în anumite situații („structuri”) particulare, nu este adevărată în sensul general al logicii formale*. Forme particulare ale principiului inducției structurale sunt și **metoda aserțiunilor invariante** ([DIJ]), folosită pentru demonstrarea *corectitudinii algoritmilor imperativi*, sau **metoda inducției asupra unei demonstrații** ([WIN]), folosită pentru demonstrarea unor teoreme de tip „corectitudine și completitudine”. ■

Noțiunile de axiomă, teoremă, regulă de inferență, demonstrație, raționament, sunt utilizate în acest capitol la modul informal/descriptiv, ele urmând a fi precizate în capitolele următoare.

§1. Algebre booleene

Se presupun cunoscute noțiunile și notațiile de bază din matematica de liceu. În plus, submulțimea lui \mathbf{N} , $\{1, 2, \dots, n\}$ se va nota și cu $[n]$, iar pentru indicarea unui element al unui produs cartezian (numit și *tuplu* sau *n-uplu* în cazul în care numărul n de componente este cunoscut) se vor folosi parantezele ascuțite, nu cele rotunde (exceptând cazul în care este vorba de aplicarea unei funcții unui tuplu).

Notăm cu \mathbf{B} mulțimea $\{0, 1\}$ și cu $\mathbf{FB}^{(n)} = \{f \mid f : \mathbf{B}^n \rightarrow \mathbf{B}\}$, \mathbf{B}^n reprezentând *produsul cartezian* al lui \mathbf{B} cu el însuși, luat de $n \in \mathbf{N}$ ori ($\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \dots \times \mathbf{B}$). $\mathbf{FB}^{(0)}$ va coincide cu \mathbf{B} , prin convenție. Vom pune deci:

$$\begin{cases} \mathbf{FB} = \bigcup_{n \geq 0} \mathbf{FB}^n \\ \mathbf{FB}^{(0)} = \mathbf{B} \end{cases}$$


Observație. $\text{card}(\mathbf{FB}^n) = 2^{2^n}$. Cardinalul unei mulțimi \mathbf{A} va mai fi notat, atunci când nu există confuzii și cu $|\mathbf{A}|$. Mai mult, dacă atât domeniul cât și codomeniul unei funcții sunt mulțimi finite, funcția poate fi dată tabelar. O asemenea tabelă de definiție va fi numită încă de pe acum **tabelă de adevăr**, deși semnificația acestui termen poate

crea anumite confuzii de moment. În cazul unei funcții $f \in \text{FB}^{(n)}$ (operație n -ară), tabela de definiție va fi de forma:

x_1	x_2	...	x_n	$f(x_1, x_2, \dots, x_n)$
0	0		0	$f(0, 0, \dots, 0)$
0	0	...	1	$f(0, 0, \dots, 1)$
...
1	1	1	1	$f(1, 1, \dots, 1)$

■

Se mai observă că am folosit o *ordine standard* pe \mathbf{B}^n , de unde se poate deriva o ordine standard pentru valorile din codomeniul funcției. Acest lucru face posibilă o reprezentare a funcțiilor booleene ca numere în baza 2 și (desigur) ca numere în baza 10.

 **Întrebare.** Puteți justifica egalitatea $\text{card}(\text{FB}^n) = 2^{2^n}$? ■


Indicăm câteva funcții importante din FB. După cum am precizat deja, în $\text{FB}^{(0)}$ avem doar *constantele* corespunzătoare, elemente ale lui \mathbf{B} (prin convenție, acestea sunt *funcții de 0 variabile*).


• Pentru $n = 1$, cele 4 funcții de o variabilă (operații 1-are sau *unare*) sunt c_0 (funcția *identică 0*), c_1 (funcția *identică 1*), 1_B (*identitatea*) și \neg (*negația, opusul*), date prin:

x	c_0	c_1	1_B	$-$
0	0	1	0	1
1	0	1	1	0

• Pentru $n = 2$, din totalul celor 16 funcții de două variabile posibile (operații 2-are; *binare*), câteva dintre cele mai importante sunt: $+$ (*suma*, sau *adunarea booleană* sau *disjuncția*), \cdot (*produsul boolean* sau *conjunția*), \oplus (*suma modulo 2* sau *disjuncția exclusivă*) și $|$ (*anticonjuncția* sau *operația lui Sheffer*):

x	y	$x + y$	$x \cdot y$	$x \dot{\vee} y$	$x y$
0	0	0	0	0	1
0	1	1	0	1	1
1	0	1	0	1	1
1	1	1	1	0	0

 **Întrebare.** Câte funcții sunt în $FB^{(3)}$? Puteți da vreun exemplu de asemenea funcție, care să aibă și o „semnificație cunoscută”? ■

 **Întrebare.** Puteți descoperi singuri metoda „standard” de construcție a liniilor unui tabel ca cel de mai sus (ordinea standard pe B^n)? ■

Observație. Funcțiile binare \cdot , $+$ și funcția unară $-$, pot fi privite ca *legi de compoziție interne* pe mulțimea B . Astfel, într-un mod cu totul

similar cu cazurile cunoscute ale *grupului*, *inelului* sau *corpului*, tuplul $B = \langle \mathbf{B}, \bullet, +, ^- \rangle$ formează o *algebră booleană*, sau *algebră Boole* (după numele matematicianului G. Boole, 1815 – 1864). ■

Definiția 1.1. Se numește **algebră booleană** un 4-uplu \mathcal{M} , $\mathcal{M} = \langle \mathbf{M}, \perp, \nabla, \sim \rangle$, format din orice mulțime nevidă \mathbf{M} (*suportul* algebrei) două operații binare $\perp, \nabla : \mathbf{M} \times \mathbf{M} \rightarrow \mathbf{M}$ și o operație unară $\sim : \mathbf{M} \rightarrow \mathbf{M}$, care satisfac condițiile (*legile*):

- | | |
|--|---|
| 1) $x \perp y = y \perp x$ | <i>comutativitate</i> (a lui \perp) |
| 2) $(x \perp y) \perp z = x \perp (y \perp z)$ | <i>asociativitate</i> (a lui \perp) |
| 3) $x \perp (y \nabla z) = (x \perp y) \nabla (x \perp z)$ | <i>distributivitate</i> (a lui \perp față de ∇) |
| 4) $(x \perp y) \nabla y = y$ | <i>absorbție</i> |
| 5) $(x \perp (\sim x)) \nabla y = y$ | <i>legea contradicției</i> |
| și respectiv | |
| 1') $x \nabla y = y \nabla x$ | <i>comutativitate</i> (a lui ∇) |
| 2') $(x \nabla y) \nabla z = x \nabla (y \nabla z)$ | <i>asociativitate</i> (a lui ∇) |
| 3') $x \nabla (y \perp z) = (x \nabla y) \perp (x \nabla z)$ | <i>distributivitate</i> (a lui ∇ față de \perp) |
| 4') $(x \nabla y) \perp y = y$ | <i>absorbție</i> |
| 5') $(x \nabla (\sim x)) \perp y = y$ | <i>legea tautologiei</i> |

■


Legile (numite impropriu și *axiome*) de mai sus nu reprezintă identități, ele trebuind să fie înțelese ca niște *ecuații satisfăcute pentru toate valorile variabilelor* x, y, z , care sunt *nume generice* pentru elemente oarecare din \mathbf{M} . Fiecare dintre cei doi membri reprezintă de fapt (expresiile unor) funcții booleene (numărul de argumente fiind dat de numărul de nume de variabile distincte care apar în întreaga ecuație). *Egalitatea înseamnă prin urmare egalitatea de funcții*. Mai mult, vom admite fără demonstrație, că **ecuațiile reprezintă scheme de axiome**, adică legile anterioare – precum și cele „derivate” care vor urma – sunt adevărate și dacă înlocuim (textual) orice apariție a unei funcții (subexpresii) prin altă funcție (subexpresie). O asemenea **Teoremă de substituție** va fi demonstrată în capitolul următor, în contextul logicii formale.

În general, considerând *afirmații* (notate generic cu A) *peste o mulțime* \mathbf{M} (*suport al unei algebre booleene*), care depind doar de variabile cu valori în \mathbf{M} și folosesc doar operațiile amintite, afirmații care sunt reprezentate fie prin axiome (**Baza** definiției structurale), fie obținute din axiome printr-un anumit *raționament utilizând reguli de inferență* (**Pasul constructiv**: cu ajutorul regulilor se obțin afirmații noi, numite și *teoreme*, din afirmații vechi), putem defini **dualele** lor, A^δ , în felul următor: A^δ *se obține din* A *prin înlocuirea simultană (textuală) a tuturor aparițiilor lui* \wedge *cu* \tilde{N} *și a tuturor aparițiilor lui* \tilde{N} *cu* \wedge .

Putem extinde conceptul și notația anterioară la *obiecte* oarecare (afirmații, dar și elemente din \mathbf{M} , funcții peste \mathbf{M} , texte, etc.). Astfel, în

B, 1 este dualul lui 0 (evident și reciproc, *relația de dualitate fiind o relație simetrică*), duala sumei este produsul, duala unei funcții oarecare se obține prin dualizarea *întregii* *tabele de adevăr*, etc. Într-o algebră booleană oarecare M , **se poate arăta** (demonstrația formală nefiind esențială pentru scopul acestei lucrări) că există un (unic) element în M (notat 0) care satisface în plus ecuația $x \perp (\tilde{x}) = 0$, precum și un (unic) element $1 \in M$, care este dualul lui 0 , satisfăcând $x \vee (\tilde{x}) = 1$ (0 fiind desigur distinct de 1). Mai mult, relația de dualitate este și *idempotentă* (avem $(o^\delta)^\delta = o$, pentru fiecare obiect o), existând și obiecte *autoduale*, adică obiecte care satisfac $o^\delta = o$ (de exemplu, funcțiile 1_B , \neg și $f \in FB^{(3)}$, dată prin $f(x, y, z) = x \oplus y \oplus z$, sunt autoduale). Fiecare axiomă i din **Definiția 1.1**, $i \in [5]$ are astfel duala sa, notată acolo prin i'). Mai mult, înlocuind într-un raționament prin care se obține o teoremă A , orice axiomă cu duala ei, vom găsi un raționament (dual), prin care se obține (*deduce, demonstrează*) afirmația A^δ . Este justificat atunci să adoptăm **principiul dualității pentru B** (care, la o privire atentă, este și el un caz particular al principiului inducției structurale). De fapt, pentru fiecare *text (secvență finită de caractere grafice)* se poate afla dualul său, după schema sugerată anterior. Admitem deci fără demonstrație formală că:

N.B. O afirmație booleană A este adevărată dacă și numai dacă duala sa A^δ este adevărată.

 **Întrebare.** Puteți arăta că funcția $f(x, y, z) = x \dot{\wedge} y \dot{\wedge} z$ este autoduală ? ■

Teorema 1.1. Tuplul $B = \langle \mathbf{B}, \bullet, +, - \rangle$ este o algebră booleană și pentru fiecare $x \in \mathbf{B}$ avem $x \bullet (\bar{x}) = 0$ și $x + (\bar{x}) = 1$.

Demonstrație. Conform principiului dualității, este suficient să arătăm că sunt adevărate doar axiomele 1) – 5) și $x \bullet (\bar{x}) = 0$ (în cazul nostru, \perp este înlocuit de \bullet iar ∇ de către $+$). Vom privi atât membrul stâng cât și membrul drept al ecuațiilor ca expresiile unor funcții și vom folosi tabelele de adevăr pentru reprezentarea acestora. Datorită simplității calculelor, dintre axiome vom arăta doar validitatea lui 4). Avem:

x	y	$x \bullet y$	$(x \bullet y) + y$	y
0	0	0	0	0
0	1	0	1	1
1	0	0	0	0
1	1	1	1	1

și respectiv:

x	\bar{x}	$x \bullet (\bar{x})$
0	1	0
1	0	0

Adevărul axiomei 4) rezultă din primul tabel prin compararea penultimei coloane (care este membrul stâng al ecuației) cu ultima

coloană (membrul drept), linie cu linie. Se observă imediat că acestea coincid, adică funcțiile date de expresiile respective sunt egale (*două funcții sunt egale dacă au același domeniu și codomeniu și valorile lor coincid pe fiecare valoare a argumentului*). Similar pentru $x \bullet (\bar{x}) = 0$ și cel de-al doilea tabel, cu observația că nu am mai explicitat coloana care reprezintă membrul drept (și care este de fapt expresia funcției c_0).

■

O algebră booleană cunoscută este dată de *mulțimea părților (submulțimilor)* unei mulțimi oarecare V , notată 2^V , împreună cu *intersecția, reuniunea și complementara față de V* , $V = \langle 2^V, \cap, \cup, C_V \rangle$.

Observație. Conceptul de algebră booleană este prezent în matematică prin mai multe definiții, nu toate echivalente în orice context ([BIR]). Să menționăm faptul că o definiție echivalentă cu **Definiția 1.1** este:

O *algebră booleană* este o *latice* $M = \langle M, \perp, \nabla \rangle$ care satisface condițiile suplimentare:

- Există (măcar) un *prim element*, $0 \in M$, astfel încât $x \nabla 0 = x$.
- Există (măcar) un *ultim element*, $1 \in M$, astfel încât $x \perp 1 = x$.
- Operația \perp este *distributivă* față de operația ∇ .
- Pentru fiecare $x \in M$, există un element $\bar{x} \in M$ (numit și *complementul* lui x), astfel încât $x \nabla \bar{x} = 1$ și $x \perp \bar{x} = 0$.

O *latice* (și aici sunt mai multe accepțiuni matematice ale termenului și câteva definiții echivalente pentru o aceeași accepțiune) este un triplet $M = \langle \mathbf{M}, \perp, \nabla \rangle$, în care ambele operații satisfac proprietățile de *idempotență*, *comutativitate*, *asociativitate* și *absorbție*. În plus, în orice latice (deci și în orice algebră booleană), se poate defini o *relație de ordine parțială* (relație binară, reflexivă, tranzitivă și antisimetrică), prin: $x \leq y$ dacă și numai dacă $x = x \perp y$ (sau, dual, $y = x \nabla y$). Datorită acestui fapt, o latice se mai definește și ca fiind o *mulțime parțial ordonată* (*poset*) în care toate submulțimile finite, nevide, admit măcar o *cea mai mică margine superioară* (*l.u.b.*, \bigvee) și o *cea mai mare margine inferioară* (*g.l. b.*, \bigwedge). ■

§2. Teoreme de reprezentare și forme normale pentru funcțiile booleene

Într-o algebră booleană (în particular, în B) sunt valabile și alte teoreme. Ele pot fi demonstrate fie utilizând tabelele de adevăr, fie construind un raționament, adică pornind de la axiome (și/sau de la alte teoreme, demonstrate anterior) și utilizând anumite reguli de inferență. Sumarizăm câteva dintre ele în tabelul următor (teoremele sunt notate cu 6) – 13) iar dualele lor respectiv cu 6') – 13'); am neglijat uneori, de exemplu în 13) și 13'), scrierea lui \bullet).

6) $\overline{\overline{x}} = x$	6') $\overline{\overline{x}} = x$
7) $x \bullet \overline{x} = 0$	7') $x + \overline{x} = 1$
8) $x \bullet x = x$	8') $x + x = x$
9) $x \bullet 0 = 0$	9') $x + 1 = 1$
10) $x \bullet 1 = x$	10') $x + 0 = x$
11) $x_1 \bullet x_2 \bullet \dots \bullet x_n = 0$ dacă și numai dacă există $i \in [n]$ astfel încât $x_i = 0$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)	11') $x_1 + x_2 + \dots + x_n = 1$ dacă și numai dacă există $i \in [n]$ astfel încât $x_i = 1$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)
12) $x_1 \bullet x_2 \bullet \dots \bullet x_n = 1$ dacă și numai dacă pentru fiecare $i \in [n]$ avem $x_i = 1$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)	12') $x_1 + x_2 + \dots + x_n = 0$ dacă și numai dacă pentru fiecare $i \in [n]$ avem $x_i = 0$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)
13) $\overline{x_1 \bullet x_2 \bullet \dots \bullet x_n} = \overline{x_1} + \overline{x_2} + \dots + \overline{x_n}$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)	13') $\overline{x_1 + x_2 + \dots + x_n} = \overline{x_1} \bullet \overline{x_2} \bullet \dots \bullet \overline{x_n}$ (oricare ar fi $n \geq 2$ și oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$)

Tabelul 1.1.

Din tabel se observă că afirmația 6) este autoduală și acesta putea fi completat cu generalizarea la $n \geq 3$ elemente a asociativității,

comutativității, distributivității, precum și cu alte teoreme, etc. Afirmatiile 13) și 13') se mai numesc *legile lui deMorgan*.

Exercițiul 1.1. Să se demonstreze adevărul afirmațiilor care urmează folosind atât tabelele de adevăr cât și raționamente, implicând axiome (sau alte afirmații, demonstrate în prealabil) și reguli de inferență (deducție, demonstrație), cunoscute din matematica de liceu (de exemplu, cele legate de faptul că *egalitatea* este o *relație de echivalență*, adică este *reflexivă, simetrică și tranzitivă*):

- a) 11) din tabelul anterior.
- b) $x \bullet (x + y) = x$.
- c) $x + x \bullet y = x$.
- d) $x + \bar{x} \bullet y = x + y$.
- e) $\bar{x} + x \bullet y = \bar{x} + y$.
- f) $x \bullet (\bar{x} + y) = x \bullet y$.
- g) $\bar{x} \bullet (x + y) = \bar{x} \bullet y$.

Rezolvare. Vom lăsa aplicarea metodei care utilizează tabelele de adevăr pe seama cititorului. De asemenea, vom presupune deja demonstrate celelalte afirmații din **Tabelul 1.1**.

a) Procedăm prin inducție matematică, afirmația de demonstrat fiind $(\forall n \in \mathbf{N})(n \geq 2 \text{ implică } P(n))$, unde:

$P(n)$: $(\forall x_1, x_2, \dots, x_n \in \mathbf{B})(x_1 \bullet x_2 \bullet \dots \bullet x_n = 0 \text{ dacă și numai dacă } (\exists i \in [n])(x_i = 0))$.

Baza. $n = 2$. Se folosesc 9) și 10) din **Tabelul 1.1**.

Pas inductiv. Să presupunem că pentru (orice) $k \geq 2$ și oricare elemente $x_1, x_2, \dots, x_k \in \mathbf{B}$ avem:

$x_1 \bullet x_2 \bullet \dots \bullet x_k = 0$ atunci și numai atunci când există $i \in [k]$ astfel încât $x_i = 0$.

Să presupunem faptul că este adevărată $P(k)$ și să arătăm că $P(k + 1)$ este adevărată. Fie orice element din \mathbf{B} , notat x_{k+1} și să notăm $y = x_1 \bullet x_2 \bullet \dots \bullet x_k$. Atunci avem de demonstrat că este adevărată afirmația $y \bullet x_{k+1} = 0$ dacă și numai dacă există $i \in [k + 1]$ astfel încât $x_i = 0$, ceea ce este echivalent cu a arăta că:

$y \bullet x_{k+1} = 0$ dacă și numai dacă există $i \in [k]$ astfel încât $x_i = 0$ sau $x_{k+1} = 0$.

Aplicând acum ipoteza inductivă, rezultă că mai trebuie să arătăm că:

$y \bullet x_{k+1} = 0$ dacă și numai dacă $y = 0$ sau $x_{k+1} = 0$.

Ultima afirmație este însă adevărată din cele deja demonstrate ($P(2)$ este adevărată).

b) $x \bullet (x + y) = x$. Pornim cu membrul stâng și folosind axioma 3) (distributivitate) găsim $x \bullet (x + y) = x \bullet x + x \bullet y$. Folosim acum 8) din **Tabelul 1.1**, distributivitatea și faptul că egalitatea este o relație tranzitivă, pentru a obține $x \bullet (x + y) = x \bullet (1 + y)$. Din comutativitate și 9') (**Tabelul 1.1**), se deduce că $x \bullet (x + y) = x \bullet 1$. Ceea ce trebuia arătat urmează acum imediat, prin aplicarea lui 10) (**Tabelul 1.1**).

c) $x + x \bullet y = x$. Rezultă din ultima parte a demonstrației anterioare.

d) $x + \bar{x} \bullet y = x + y$. Pornim cu membrul stâng al egalității și îl înlocuim pe x cu $x + x \bullet y$, ceea ce putem face folosind punctul anterior și faptul că egalitatea este o relație simetrică. Găsim $x + \bar{x} \bullet y = x + x \bullet y + \bar{x} \bullet y$.

Folosind comutativitatea și distributivitatea, rezultă că trebuie să arătăm $x + y \cdot (x + \bar{x}) = x + y$. Aplicăm acum 7') și apoi 10) (**Tabelul 1.1**), pentru a obține ceea ce se cere.

e) $\bar{x} + x \cdot y = \bar{x} + y$. În relația precedentă se înlocuiesc toate aparițiile lui x cu \bar{x} și se folosește apoi 6).

f) $x \cdot (\bar{x} + y) = x \cdot y$. Se folosesc - în ordine - distributivitatea, afirmația 7) (**Tabelul 1.1**), comutativitatea și 10') (**Tabelul 1.1**).

g) $\bar{x} \cdot (x + y) = \bar{x} \cdot y$. Din nou, se înlocuiesc simultan toate aparițiile lui x cu \bar{x} în relația precedentă și se aplică 6). ■

Să trecem în revistă și câteva rezultate importante din teoria generală a funcțiilor booleene, pregătind un suport abstract adecvat pentru capitolele următoare. *O primă parte* dintre enunțuri vor fi reluate pe parcursul lucrării, într-un alt cadru. *O a doua parte* este prezentată mai detaliat în alte cursuri (cum ar fi **Arhitecturi și sisteme de operare**). În sfârșit, *a treia parte* necesită cunoștințe suplimentare (din acest motiv, unele demonstrații vor fi omise).

O clasă de proprietăți interesante se referă la o metodă generală de reprezentare „standard” a funcțiilor din FB. Începând cu teorema următoare introducem notațiile $x^1 = x$ și $x^0 = \bar{x}$ (*în sensul că „puterea” 1 atașată unei expresii o lasă neschimbată, iar „puterea” 0 îi „adaugă” o bară*). Să remarcăm că indicii superiori precedenți nu se supun principiului dualității (de exemplu, nu este adevărat că $(x^1 = x)^\delta$ coincide cu $(x^0 = x)$).

Teorema 1.2 ([CAZ1], de descompunere, în sumă de „termeni”).

Pentru fiecare $n \in \mathbf{N}^*$, $f \in \mathbf{FB}^{(n)}$ și fiecare $k \in [n]$, avem:

$$f(x_1, x_2, \dots, x_n) = \sum_{a_1, a_2, \dots, a_k \in \mathbf{B}} x_1^{a_1} \cdot x_2^{a_2} \cdot \dots \cdot x_k^{a_k} \cdot f(a_1, a_2, \dots, a_k, x_{k+1}, \dots, x_n)$$

oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$.

Demonstrație. Dacă $x_i, a_i \in \mathbf{B}$ atunci, direct din notațiile de mai sus, rezultă că:

$$(*) \quad (x^0)^a = (x^a)^0 \text{ precum și } x^a = 1 \text{ dacă și numai dacă } x = a.$$

Folosind 12) (**Tabelul 1.1**), rezultă imediat că, în condițiile teoremei,

$$x_1^{a_1} \cdot x_2^{a_2} \cdot \dots \cdot x_k^{a_k} = 1 \text{ dacă și numai dacă } x_i = a_i \text{ pentru fiecare } i \in [k].$$

Fie acum elementele $a_1, a_2, \dots, a_n \in \mathbf{B}$, oarecare, fixate. Conform (*), în suma

$$\sum_{a_1, a_2, \dots, a_k \in \mathbf{B}} a_1^{a_1} \cdot a_2^{a_2} \cdot \dots \cdot a_k^{a_k} \cdot f(a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_n)$$

unul și numai unul dintre factorii $a_1^{a_1} \cdot a_2^{a_2} \cdot \dots \cdot a_k^{a_k}$ va fi egal cu 1, adică cel pentru care $a_i = a_i$, pentru fiecare $i \in [k]$. Datorită comutativității și legilor 10), 9) și 10') (**Tabelul 1.1**), rezultă că suma este egală exact cu $f(a_1, a_2, \dots, a_n)$. ■

Este adevărată și *teorema duală* (de descompunere, în produs de „factori”), ambele rezultate fiind folosite pentru demonstrarea existenței formelor normale pentru funcțiile booleene. În enunțul teoremei duale, înafara înlocuirii lui + cu • și a lui Σ cu Π , numele

$\alpha_1, \alpha_2, \dots, \alpha_k$ (ca argumente ale lui f) se înlocuiesc cu aceleași elemente, dar barate.


Definiția 1.2. Fie $n \in \mathbf{N}^*$ și $x_1, x_2, \dots, x_n \in \mathbf{B}$ variabile (booleene) distincte (putem nota mulțimea acestora cu $X = \{x_1, x_2, \dots, x_n\}$, ideea fiind însă că lucrăm cu o listă, adică cu o colecție *ordonată* de elemente distincte). Se numește *termen (n-ar, peste X)* orice produs (uneori, operatorul de produs este omis, sau supradimensionat) $t = x_{i_1}^{a_1} \cdot x_{i_2}^{a_2} \cdot \dots \cdot x_{i_k}^{a_k}$, unde $0 \leq k \leq n$, $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbf{B}$ și $1 \leq i_1 < i_2 < \dots < i_k \leq n$. ■

În definiția precedentă, termenul generat pentru $k=0$ este 1 (prin convenție). Pentru $k = n$ obținem așa-numiții *termeni maximali (maxtermeni)*, adică *acei termeni în care fiecare dintre variabilele considerate apare o dată și numai o dată (barată sau nebarată), în ordinea precizată*.


Observație. Între mulțimea termenilor n -ari t (peste X) și mulțimea n -uplelor peste $\{0, 1, 2\}$ (aceasta „coincide” de fapt cu mulțimea $\{f \mid f : [n] \rightarrow \{0, 1, 2\}\}$) se poate stabili o corespondență biunivocă g , dată de $g(t) = \langle e_1, e_2, \dots, e_n \rangle$, unde, pentru fiecare $i \in [n]$, avem $e_i = 0$ dacă x_i apare barată în t , $e_i = 1$ dacă x_i apare nebarată în t și $e_i = 2$ în rest (x_i nu apare în t). Mulțimea termenilor n -ari considerați va avea atunci 3^n elemente. Raționând similar pentru cazul maxtermenilor n -ari (în acest caz, nu este posibil ca vreo variabilă considerată să nu apară),


rezultă că există 2^n maxtermeni n -ari distincți (indiferent de numele celor n variabile diferite fixate prin X). ■

Considerațiile de natură combinatorială sunt practic indispensabile în vederea obținerii unor rezultate convenabile.

 **Întrebare.** Puteți rescrie atât teorema de descompunere cu termeni cât și teorema de descompunere cu factori pentru cazul $n = 2$ și $k = 1$? ■

Exemplu. Dacă luăm $n = 2$ și notăm x_1 cu x și x_2 cu y , atunci cei $3^2 = 9$ termeni sunt: $x, y, \bar{x}, \bar{y}, x \cdot y, \bar{x} \cdot y, x \cdot \bar{y}, \bar{x} \cdot \bar{y}, 1$. Cei $2^2 = 4$ maxtermeni sunt: $x \cdot y, \bar{x} \cdot y, x \cdot \bar{y}, \bar{x} \cdot \bar{y}$. ■

 **Întrebare.** Sunt adevărate afirmațiile făcute în precedenta **Observație**? Justificați răspunsul. ■

 **Întrebare.** Fie $X = \{x, y, z, t\}$. Este $\bar{x} \cdot z \cdot t$ un maxtermen (peste X) ? ■

Definiția 1.3. Se numește *formă normală disjunctivă* (n -ară, $n \in \mathbb{N}^*$), sau **(n-)FND** pe scurt, orice sumă (finită) de termeni n -ari distincți. Se numește *formă normală disjunctivă perfectă* (n -ară, $n \in \mathbb{N}^*$), sau **(n-)FNDP** pe scurt, orice sumă de maxtermeni n -ari distincți. ■

Orice **FND** se poate reprezenta și grafic, ca un *arbore* ([KNU], [LUC]). Datorită comutativității adunării putem face abstracție de ordinea (max)termenilor dintr-o sumă, *mai exact, considerând oricare două sume care diferă doar prin ordinea termenilor, le vom privi ca fiind identice*. Vor exista astfel $C_{3^n}^k$ forme normale disjunctive n-are având k termeni, $0 \leq k \leq 3^n$ (prin convenție, pentru $k = 0$, unica formă care este acceptată și este și perfectă, se notează tot cu 0). În consecință, numărul total al n-**FND** – urilor va fi:

$$C_{3^n}^0 + C_{3^n}^1 + \dots + C_{3^n}^k + \dots + C_{3^n}^{3^n} = 2^{3^n}.$$

Analog, numărul total al n-**FNDP** – urilor va fi:

$$C_{2^n}^0 + C_{2^n}^1 + \dots + C_{2^n}^k + \dots + C_{2^n}^{2^n} = 2^{2^n}.$$

Teorema 1.3 ([CAZ1]). Orice funcție booleană se poate „reprezenta” în mod unic ca o **FNDP**.

Demonstrație. Fie fixate $n \in \mathbf{N}^*$, $f \in \mathbf{FB}^{(n)}$ și $X = \{x_1, x_2, \dots, x_n\}$. Aplicând **Teorema de descompunere** cu termeni pentru f și $k = n$, găsim că f se poate scrie sub forma:

$$f(x_1, x_2, \dots, x_n) = \sum_{a_1, a_2, \dots, a_n \in \mathbf{B}} x_1^{a_1} \cdot x_2^{a_2} \cdot \dots \cdot x_n^{a_n} \cdot f(a_1, a_2, \dots, a_n)$$

oricare ar fi valorile lui x_1, x_2, \dots, x_n din \mathbf{B} și prin urmare avem:

$$f(x_1, x_2, \dots, x_n) = \sum_{a_1, a_2, \dots, a_n \in \mathbf{B}} x_1^{a_1} \cdot x_2^{a_2} \cdot \dots \cdot x_n^{a_n},$$

oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$, $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{B}$, astfel încât $f(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$, ceea ce înseamnă exact o reprezentare a lui f ca o n -**FNDP**. Unicitatea reprezentării provine din faptul că mulțimea n -**FNDP**-urilor și mulțimea $\mathbf{FB}^{(n)}$ au același cardinal (adică număr de elemente). Mai spunem că expresia din membrul drept al reprezentării este (o) **FND(P)** pentru f . ■

Prin dualizare se obțin noțiunile de **(n-)factor peste X** (orice sumă de n variabile din X , acestea apărând barate sau nu), **maxfactor (n-ar, peste X)** – un (n) -factor în care apar toate variabilele, **formă normală conjunctivă (n-ară)** ((n -)**FNC**, adică orice produs de factori distincți), **formă normală conjunctivă (n-ară) perfectă** ((n -)**FNCP**, adică orice produs de maxfactori distincți). Nu uităm că se aplică asociativitatea generalizată și comutativitatea, peste tot, atât pentru sumă cât și pentru produs, astfel încât **două sume (produse) nu vor fi considerate distincte dacă diferă doar prin ordinea componentelor**. Aplicând principiul dualității, rezultă că este adevărată și duala **Teoremei 1.3**, adică:

Teorema 1.4. Fie orice $n \in \mathbf{N}^*$, orice $f \in \mathbf{FB}^{(n)}$ și oricare nume distincte de variabile x_1, x_2, \dots, x_n . Atunci f se poate reprezenta în mod unic ca o **FNCP** peste $X = \{x_1, x_2, \dots, x_n\}$, sub forma:

$$f(x_1, x_2, \dots, x_n) = \prod_{a_1, a_2, \dots, a_n \in \mathbf{B}} (x_1^{a_1} + x_2^{a_2} + \dots + x_n^{a_n}),$$

oricare ar fi $x_1, x_2, \dots, x_n \in \mathbf{B}$, $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbf{B}$, astfel încât $f(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) = 0$. ■

§3. Clase speciale de funcții booleene

Deși rezultatele teoretice anterioare sunt încurajatoare (funcțiile booleene, date tabelar, pot fi reprezentate și prin *expresii standard*, cum ar fi **FNDP**, **FNCP**; acestea sunt *unice* dacă se folosesc anumite convenții; se pot *construi* „*algoritmice*”, conform **Teoremei 1.3** și **Teoremei 1.4**, etc.), s-ar putea ca din punct de vedere practic să nu fie chiar convenabile. Astfel, ne-am putea pune problema găsirii *celei mai „scurte”* forme normale, funcție de o anumită *măsură* fixată. Există numeroase „măsuri candidat” pentru o **FND** sau **FNC**, suficient de simple (vom nota orice asemenea formă prin φ): lungimea ca text (număr de caractere grafice conținute, poate chiar excluzând parantezele); numărul de operatori folosiți (poate chiar exceptând *negația*); numărul de nivele din arborele atașat; numărul de termeni (factori); numărul de componente „elementare” ale unui termen (factor); **numărul total de apariții ale variabilelor** (**apariția unei aceleiași variabile pe poziții diferite se numără distinct**), etc. Considerând ultima măsură (pe care o vom nota cu $n(\varphi)$), putem numi *formă normală disjunctivă minimală* (**FNDM**) pentru $f \in \mathbf{FB}$, orice **FND** φ' astfel încât:

$$n(\varphi') = \min \{n(\varphi) \mid \varphi \text{ este FND pentru } f\}.$$

Dată o funcție booleană $f \in \mathbf{FB}$, se poate pune **problema determinării tuturor FNDM pentru f**, sau a uneia *standard* (ceea ce este posibil

deoarece – reamintim - pentru fiecare număr natural n numărul funcțiilor booleene n -are este 2^{2^n} iar numărul formelor disjunctive n -are este 2^{3^n}). **Problema anterioară este rezolvabilă cu ajutorul algoritmului lui W. Quine** ([CAZ1]). Algoritmul lui Quine intră sub incidența principiului dualității, astfel încât făcând modificările de rigoare el poate determina și toate *formele normale conjunctive minimale (FNCM)* pentru orice funcție booleană.

O problemă similară, prin rezolvarea căreia s-ar putea reduce în anumite cazuri timpul de procesare a unor texte (expresii, formule, etc.), este **găsirea unui număr minim de operații booleene convenabile**, cu ajutorul cărora să se „reprezinte” **orice** funcție booleană.

Definiția 1.4. Clasa funcțiilor booleene *elementare* este:

$$\mathbf{E} = \{ i_p^n \mid n \in \mathbf{N}^*, 1 \leq p \leq n, i_p^n : \mathbf{B}^n \rightarrow \mathbf{B},$$

$$i_p^n(x_1, x_2, \dots, x_p, \dots, x_n) = x_p \}.$$

Fie $n \in \mathbf{N}^*$, t un număr natural, $f, h_1, h_2, \dots, h_t \in \mathbf{FB}^{(n)}$ și $g \in \mathbf{FB}^{(t)}$. Spunem că f se obține din g, h_1, h_2, \dots, h_t prin **superpoziție** dacă pentru fiecare $x = \langle x_1, x_2, \dots, x_n \rangle$ avem:

$$f(x) = g(h_1(x), h_2(x), \dots, h_t(x)).$$

Fie $M \subseteq \mathbf{FB}$. Se numește *M-șir* orice *secvență (listă) finită* f_0, f_1, \dots, f_r de funcții booleene în care fiecare f_i este fie din $\mathbf{E} \cup M$ fie se obține prin superpoziție din alte funcții, aflate în aceeași listă dar înaintea lui f_i . ■

Funcțiile i_p^n se mai numesc și *proiecții*. Pentru superpoziție vom utiliza notația $f = \text{SUP}(g, h_1, h_2, \dots, h_t)$, iar \overline{M} va denota *mulțimea funcțiilor care apar ca elemente în M-șiruri*. Pentru fiecare M dat, \overline{M} va fi practic o mulțime definită constructiv, în care $E \cup M$ constituie mulțimea funcțiilor de bază iar operatorul de superpoziție este singura modalitate de a se obține funcții noi din funcții vechi. Prin urmare, \overline{M} este cea mai mică mulțime care conține proiecțiile, elementele lui M și este închisă la superpoziție. Algebric vorbind, se mai spune că \overline{M} este închiderea prin superpoziție a mulțimii $E \cup M$. M se va numi închisă dacă coincide cu închiderea sa.

Teorema 1.5 ([CAZ1]). O mulțime $M \subseteq \text{FB}$ este închisă dacă și numai dacă conține funcțiile elementare și orice superpoziție de funcții din M se află în M.

Demonstrație. Este imediată din definiții, demonstrația reprezentând o aplicare directă a principiului inducției structurale. Astfel, este suficient să arătăm că, dată M, avem:

Baza. $E \subseteq M$ și $M \subseteq M$.

Pas inductiv. Pentru fiecare $n \in \mathbb{N}^*$, fiecare $t \in \mathbb{N}^*$, fiecare $g \in \text{FB}^{(t)}$, fiecare $h_1, h_2, \dots, h_t \in \text{FB}^{(n)}$, fiecare $f \in \text{FB}^{(n)}$, astfel încât $f = \text{SUP}(g, h_1, h_2, \dots, h_t)$, avem: Dacă $g, h_1, h_2, \dots, h_t \hat{I} M$, atunci $f \hat{I} M$. ■

Exemple imediate de mulțimi închise sunt \emptyset , E și FB. Se poate arăta și că următoarele mulțimi (infinite) sunt mulțimi închise (a se

consulta și exercițiile din finalul capitolului, împreună desigur cu rezolvările din **Anexă**):

- **T₀**: mulțimea funcțiilor booleene de oricâte argumente care *păstrează pe 0*, adică satisfac $f(0, 0, \dots, 0) = 0$.
- **T₁**: dual, mulțimea funcțiilor care *păstrează pe 1*, adică satisfac $f(1, 1, \dots, 1) = 1$.
- **Aut**: mulțimea funcțiilor *autoduale* ($f^\delta = f$). Să notăm ca o proprietate de caracterizare interesantă pentru această clasă de funcții și faptul că $f^\delta(x_1, x_2, \dots, x_n) = \overline{f(\overline{x}_1, \overline{x}_2, \dots, \overline{x}_n)}$. Acest lucru se obține imediat deoarece tabela de definiție pentru f^δ se obține din tabela pentru f , înlocuind simultan, peste tot, pe 0 cu 1 și pe 1 cu 0.
- **Mon**: mulțimea funcțiilor *monotone*. Pe **B** putem defini o relație de ordine „naturală”: $0 \leq 1$ (putem pune chiar $0 < 1$). Relația precedentă poate fi extinsă „pe componente” la orice produs cartezian. Să considerăm două n-uple $\alpha = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$ și $\beta = \langle \beta_1, \beta_2, \dots, \beta_n \rangle$, $\alpha_i, \beta_i \in \mathbf{B}$, $i \in [n]$. Vom spune că $\alpha \leq \beta$ dacă și numai dacă $\alpha_i \leq \beta_i$ pentru fiecare $i \in [n]$ (desigur că vom avea $\alpha < \beta$ dacă și numai dacă $\alpha \leq \beta$ și $\alpha \neq \beta$ adică α și β diferă prin măcar o componentă). O funcție $f \in \mathbf{FB}^{(n)}$ este monotonă dacă pentru fiecare $\alpha, \beta \in \mathbf{B}^n$, din $\alpha \leq \beta$ rezultă $f(\alpha) \leq f(\beta)$.
- **Lin**: mulțimea funcțiilor *liniare*. Se poate arăta mai întâi că tripletul $I = \langle \mathbf{B}, \oplus, \cdot \rangle$ este un inel comutativ cu unitatea 1, izomorf cu inelul claselor de resturi modulo 2 (cele două mulțimi suport și operațiile „corespondente” se pot

„identifica”). Urmează că *orice funcție booleană se poate reprezenta unic ca un polinom (eventual, de mai multe variabile) cu coeficienți în 1*. Fie astfel o funcție booleană f , despre care știm deja că se poate scrie ca o sumă (booleană) de termeni. Putem acum folosi egalitățile (se pot demonstra ușor, folosind tabelele de adevăr): $\bar{x} = x \oplus 1$ și $x + y = \overline{\bar{x} \cdot \bar{y}} = (x \oplus 1) \cdot (y \oplus 1) \oplus 1 = x \cdot y \oplus x \oplus y$, precum și proprietățile inelelor, pentru a observa că orice **FND** a lui f devine o sumă modulo 2 de termeni (care sunt produse de variabile distincte). Numărul acestor produse este 2^n , deci *numărul polinoamelor modulo 2 este 2^{2^n}* , același ca și numărul funcțiilor booleene n -are (de unde urmează *unicitatea* reprezentării). Spunem că o funcție $f \in \mathbf{FB}^{(n)}$ este liniară dacă reprezentarea sa (unică) sub formă de polinom modulo 2 are aspectul:

$$c_0 \oplus c_1 \cdot x_1 \oplus c_2 \cdot x_2 \oplus \dots \oplus c_n \cdot x_n, c_i \in \mathbf{B}, i \in [n].$$

Observație. Se poate arăta că toate mulțimile anterioare sunt nebanale, adică nu coincid nici cu \mathbf{FB} , nici cu \mathbf{E} , nici cu \emptyset . ■

Exemplu ([CAZ1]). Funcția $f(x, y, z) = x \cdot z + \bar{x} \cdot y \cdot \bar{z} + \bar{x} \cdot \bar{y} \cdot \bar{z}$ este liniară deoarece avem succesiv:

$$\begin{aligned} f(x, y, z) &= && \text{comutativitate, distributivitate} \\ &= x \cdot z + \bar{x} \cdot \bar{z} \cdot (y + \bar{y}) = && \text{știm că } y + \bar{y} = 1 \\ &= x \cdot z + \bar{x} \cdot \bar{z} = && \text{folosind } a + b = a \cdot b \oplus a \oplus b \\ &= x \cdot z \oplus \bar{x} \cdot \bar{z} \oplus x \cdot z \oplus \bar{x} \cdot \bar{z} = && \text{știm că } x \cdot z \oplus \bar{x} \cdot \bar{z} = 0 \end{aligned}$$

$$\begin{aligned}
&= x \cdot z \oplus \bar{x} \cdot \bar{z} = && \text{folosind } \bar{\bar{a}} = a \text{ \AA } 1 \\
&= x \cdot z \oplus (x \oplus 1)(z \oplus 1) = && \text{distributivitate} \\
&= x \cdot z \oplus x \cdot z \oplus x \oplus z \oplus 1 = && \text{folosind } a \text{ \AA } a = 0 \\
&= x \oplus z \oplus 1. \blacksquare
\end{aligned}$$

Definiția 1.5. O mulțime de funcții booleene este *completă* dacă închiderea sa coincide cu FB. O mulțime completă se numește *bază* dacă este *maximală* (adică nici o submulțime proprie a sa nu mai este completă). ■

Observație. Se arată relativ simplu că mulțimea $\{c_0, c_1, f, \cdot\}$, unde f este dată prin $f(x, y, z) = x \oplus y \oplus z$, este o bază. Mulțimea $\{\cdot, +, ^-\}$ este completă (ceea ce se arată direct, folosind definițiile), dar nu este bază pentru că atât $\{^-, \cdot\}$ cât și $\{^-, +\}$ sunt complete (acest lucru rezultă din legile lui deMorgan, care „ne spun” că disjuncția se exprimă cu ajutorul negației și conjuncției și dual, conjuncția se exprimă cu ajutorul negației și disjuncției). Poate surprinzător, $\{+, \cdot\}$ nu este completă, dar $\{|\}$ (care nu este inclusă în nici una dintre mulțimile $T_0, T_1, \text{Aut}, \text{Mon}, \text{Lin}$) este completă și desigur bază (ne bazăm pe egalitățile $\bar{x} = x | x$ și $x \cdot y = (x | y) | (x | y)$). Prin urmare, dacă ne reamintim de unul dintre scopurile enunțate (exprimarea tuturor funcțiilor booleene cu ajutorul unui număr minim de funcții), mulțimea $\{|\}$ ar fi **candidatul ideal**. Din păcate, operatorul lui Sheffer („|”) nu este prea „comod” (din punct de vedere al gândirii umane) astfel încât exprimările celorlalte funcții devin complicate și greu de reținut. Este

de dorit să se găsească o *cale de mijloc*, prin care să se păstreze într-adevăr cât mai *puține funcții într-o bază*, dar acestea să fie și *ușor de înțelese/manipulat*. ■

Acceptăm fără demonstrație (**Teorema 1.7** a fost însă deja demonstrată implicit, prin comentariile anterioare), următoarele rezultate ([CAZ1], această referință nefiind sursa primară):

Teorema 1.6 (E. L. Post). O mulțime de funcții booleene este completă dacă și numai dacă nu este inclusă în nici una dintre mulțimile **T₀**, **T₁**, **Aut**, **Mon**, **Lin**. ■

Teorema 1.7. Orice bază conține cel mult patru funcții și există baze compuse din una, două, trei și patru funcții. ■

Teorema 1.8. Orice mulțime închisă de funcții booleene fie este inclusă cel puțin în una dintre mulțimile **T₀**, **T₁**, **Aut**, **Mon**, **Lin**, fie coincide cu FB. ■

Teorema 1.9. Mulțimile **T₀**, **T₁**, **Aut**, **Mon**, **Lin** sunt *precomplete* (o mulțime M de funcții booleene este precompletă dacă pentru orice altă funcție $f \notin M$, mulțimea $M \cup \{f\}$ este completă). ■

E. L. Post a determinat chiar **toate** mulțimile închise de funcții booleene încă din anul 1941, cât și relațiile de incluziune între ele și anumite baze. Încă se fac cercetări în legătură cu extinderea rezultatelor

de acest tip la mulțimi de cardinal mai mare decât doi (cardinalul lui **B**). Importanța unor asemenea cercetări constă în speranța reducerii complexității unor algoritmi clasici și dezvoltării unor teorii similare, implementabile și care să fie valabile și pentru logicile neclasice multivaluate).

§4. Recapitulare și Index

Teoria funcțiilor booleene constituie *suportul pentru semantica logicii clasice*. Înțelegerea problematicii capitolelor următoare va fi astfel ușurată, anumite paragrafe (cum ar fi cel privind formele normale) fiind simple transpuneri într-un alt limbaj ale unor concepte și rezultate deja întâlnite. Principalele teme abordate au fost:

- Reprezentarea funcțiilor booleene. Funcții booleene particulare importante.
- Proprietățile globale ale clasei funcțiilor booleene. Principiul dualității. Algebre booleene.
- Forme normale pentru funcțiile booleene. Forme minimale.
- Mulțimi închise și (pre)complete de funcții booleene. Baze.

Deși ne-am bazat în principal pe cunoștințele de matematică de liceu, am fost nevoiți să abordăm tangențial – într-un mod intuitiv, pentru coerența materialului – subiecte colaterale cum ar fi cele privind algoritmi (imperativi), mulțimile definite structural (constructiv), sau principiul inducției structurale. Folosirea nediscreționară, în acest moment, de către cititor a unor termeni introduși doar informal (cum sunt, până acum: axiomă, teoremă, raționament, demonstrație, etc.)

poate fi dăunătoare, măbind confuziile care se fac în mod uzual între sintaxă și semantică sau între limbaj și metalimbaj.

Indexul (neexhaustiv) este:

definiția structurală (constructivă) a unei mulțimi, 8

algoritm (imperativ), 9

funcție calculată de un algoritm, 9

problemă rezolvată de un algoritm, 9

terminarea algoritmilor, semialgoritm, 10

pseudocod, 10

principiul inducției structurale, 11

funcții booleene, 13

tabele de adevăr, 13

algebre booleene, 15

afirmații și obiecte duale, 17

principiul dualității, 18

termen, maxtermen, 27

formă normală disjunctivă (perfectă), 28-29

factor, maxfactor, 30

formă normală conjunctivă (perfectă), 30

formă normală disjunctivă (conjunctivă) minimală, 31

funcții booleene elementare, 32

mulțime închisă de funcții booleene, 33

mulțime completă (precompletă) de funcții booleene, 36

bază de funcții, 36

Este poate bine să menționăm faptul că am preferat un **Index** în ordinea paginilor și nu în ordine alfabetică, tocmai pentru că insistăm asupra necesității parcurgerii secvențiale a materialului.

§5. Exerciții

1. Completați demonstrația **Teoremei 1.1**, adică arătați validitatea legilor 1), 2), 3), 5), 1') – 5') și $x + (\bar{x}) = 1$, utilizând tabelele de adevăr.
2. Arătați că $V = \langle 2^V, \cap, \cup, C_V \rangle$ este o algebră booleană, oricare ar fi mulțimea (nevidă) V . În plus, demonstrați că $\mathbf{0} = \emptyset$ și $\mathbf{1} = V$.
3. Arătați adevărul afirmațiilor rămase nedemonstrate din **Tabelul 1.1**.
4. Justificați egalitatea $\text{card}(\text{FB}^n) = 2^{2^n}$.
5. Fie mulțimea termenilor n -ari t , construiți peste mulțimea variabilelor booleene distincte (ordonate) $X = \{x_1, x_2, \dots, x_n\}$, precum și mulțimea n -uplurilor peste $\{0, 1, 2\}$. Arătați că există o funcție bijectivă g , care „identifică” aceste mulțimi, dată prin $g(t) = \langle e_1, e_2, \dots, e_n \rangle$, unde, pentru fiecare $i \in [n]$, avem $e_i = 0$ dacă x_i apare barată în t , $e_i = 1$ dacă x_i apare (nebarată) în t și $e_i = 2$ în rest (adică x_i nu apare în t). De asemenea, arătați că există (măcar) o corespondență bijectivă între mulțimea n -uplurilor peste $\{0, 1, 2\}$ și mulțimea de funcții $\{f \mid f : [n] \rightarrow \{0, 1, 2\}\}$. Deduceți că mulțimea termenilor n -ari

considerați va avea 3^n elemente și că vor exista 2^n maxtermeni n-ari distincți.

6. Să se găsească **FNDP** și **FNPC** pentru funcția definită prin tabelul:

x	y	z	f(x, y, z)
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

7. Justificați faptul că mulțimile **T₀**, **T₁**, **Aut**, **Mon**, **Lin** sunt infinite. Arătați că **T₀** este mulțime închisă.
8. Arătați că mulțimea $M = \{\bullet, +, ^-\}$ este o mulțime completă de funcții booleene.
9. Arătați că funcția booleană „+” este o funcție monotonă.
10. Arătați că $I = \langle \mathbf{B}, \oplus, \bullet \rangle$ este un inel comutativ cu unitatea **1** și că el este izomorf cu $R = \langle \mathbb{Z}_2, \oplus, \mathbf{U} \rangle$, inelul claselor de resturi modulo 2.
11. Arătați că funcția booleană $f(x, y, z) = x\bar{y} + y\bar{z}$ nu este liniară (acolo unde nu există confuzii, operatorul \bullet nu va fi scris explicit).