Algebraické štruktúry I

- **algebraické štruktúry**
- **grupa**
- **základné vlastnosti grupy**
- **morfizmy**
- **Boolova algebra**

Binárne operácie

Teória algebraických štruktúr študuje všeobecné vlastnosti systémov, ktoré obsahujú množinu (alebo množiny) elementov, nad ktorým je obvykle definovaná binárna operácia (alebo operácie).

Definícia. ***Binárna operácia*** na množine X je predpis (funkcia)

$$f : X \times X \to X$$

ktorá dvom elementom $x, y \in X$ jednoznačne priradí element

$z = x * y = f(x, y) \in X$

$$\forall x \forall y \exists ! z \left(z = x * y = f(x, y) \right)$$

Definícia. Usporiadaná dvojica $(X, *)$ obsahujúca množinu X a binárnu operáciu $*$ nad touto množinou sa nazýva ***algebraická štruktúra***.

Príklady

(1) Algebraická štruktúra $(\mathbb{Z},+)$ obsahuje množina celých čísel $\mathbb{Z}$ a binárnu operáciu súčet nad touto množinou. Podobným spôsobom môžeme definovať ďalšie dve algebraické štruktúry $(\mathbb{Z},-)$ a $(\mathbb{Z},\times)$, ktoré sú založené na binárnych operáciách rozdiel resp. súčin.

(2) Nech $X=\mathcal{P}(A)$ je potenčná množina pre množinu A. Operácia zjednotenia a prieniku priradí dvom podmnožinám z A nejakú podmnožinu z A

$$\cup:\mathcal{P}(A)\times\mathcal{P}(A)\rightarrow\mathcal{P}(A)$$

$$\cap:\mathcal{P}(A)\times\mathcal{P}(A)\rightarrow\mathcal{P}(A)$$

Potom existujú dve jednoduché algebraické štruktúry $(X,\cup)$ a $(X,\cap)$.

Multiplikačná tabuľka

Binárna operácia $'*'$ môže byť špecifikovaná pomocou multiplikačnej tabuľky (ktorá sa v anglosaskej literatúre nazýva Caleyho tabuľka). Napríklad pre $X=\{a,b,c,d\}$ táto tabuľka má tvar

$*$	a	b	c	d
a	a	b	c	d
b	d	c	a	b
c	c	b	a	a
d	d	b	c	a

Definícia.

(1) Binárna operácia $*$ sa nazýva ***asociatívna*** na množine X vtedy a len vtedy, ak pre každé $x, y, z \in X$

$$(x * y) * z = x * (y * z)$$

(2) Binárna operácia $*$ sa nazýva ***komutatívna*** na množine X vtedy a len vtedy, ak pre každé $x, y \in X$

$$x * y = y * x$$

(3) Element $e \in X$ sa nazýva ***jednotkový*** vzhľadom k binárnej operácii $*$ na množine X vtedy a len vtedy, ak pre každé $x \in X$

$$x * e = e * x = x$$

(4) Element $y \in X$ sa nazýva ***inverzný*** vzhľadom k elementu $x \in X$ a k binárnej operácii $*$ na množine X vtedy a len vtedy, ak

$$y * x = x * y = e$$

Inverzný element y často značíme symbolom x^{-1}, aby sme zdôraznili je vzťah k elementu x.

Príklady

(1) Pre algebraickú štruktúru $(\mathbb{Z},+)$ jednotkový element je nula, pre každé celé číslo $x \in \mathbb{Z}$ platí podmienka

$$0 + x = x + 0 = x$$

Pre dané celé číslo $x \in \mathbb{Z}$ existuje inverzný element $(-x) \in \mathbb{Z}$, ktorý spĺňa podmienku

$$(-x) + x = x + (-x) = 0$$

(2) Pre algebraickú štruktúru $(\mathbb{Z},\times)$ jednotkový element je číslo jedna, pre každé celé číslo $x \in \mathbb{Z}$ platí

$$x \times 1 = 1 \times x = x$$

Môžeme si položiť otázku, či každý element $x \in \mathbb{Z}$ má inverzný element? Napríklad, položme $x = 5$, potom inverzný element y vzhľadom k tomuto prvku je taký, čo vyhovuje podmienke

$$5 \times y = y \times 5 = 1$$

Táto podmienka nemá riešenie v množine celých čísel, $\neg\exists\left(y \in \mathbb{Z}\right)\left(5 \times y = y \times 5 = 1\right)$. Preto, v rámci algebraického systému $(\mathbb{Z},\times)$ nemá zmysel hovoriť o inverznom elemente vzhľadom k binárnej operácii ´súčin´.

(3) Študujme algebraickú štruktúru $\left(\mathcal{P}(A),\cap,\cup\right)$, definovaný pre potenčnú množinu s dvoma binárnymi operáciami ´prienik´ a ´zjednotenie´. Jednotkový a inverzný element pre tento algebraický systém musíme zaviesť separátne pre operáciu zjednotenia resp. prieniku. Každá z týchto operácií má svoj jednotkový element, pre každé $x \in \mathcal{P}(A)$

$$x \cap A = A \cap x = x$$
$$x \cup \emptyset = \emptyset \cup x = x$$

To znamená, že pre binárnu operáciu prieniku (zjednotenia) ako jednotkový element je množina A (prázdna množina $\emptyset$). Komplement $\overline{x} = A - x \in \mathcal{P}(A)$ nie je inverzný element vzhľadom k podmnožine $x \in \mathcal{P}(A)$

$$x \cup \overline{x} = \overline{x} \cup x = A$$
$$x \cap \overline{x} = \overline{x} \cap x = \emptyset$$

pretože na pravých stranách nemáme jednotkové elementy pre dané binárne operácie.

Veta. Nech $*$ je binárna operácia na množine X. Ak existuje jednotkový element $x * e = e * x = x$, pre každé $x \in X$, potom tento jednotkový element existuje jednoznačne.

Predpokladajme, že existujú dva jednotkové elementy $e_1, e_2 \in X$, potom súčasne platí

$$e_1 * e_2 = e_2 * e_1 = e_1$$
$$e_2 * e_1 = e_1 * e_2 = e_2,$$

preto musí platiť $e_1 = e_2$

Veta. Nech $*$ je binárna operácia na množine X, ktorá má jednotkový element $e \in X$. Ak pre každý element $x \in X$ existuje inverzný element, $x * x^{-1} = x^{-1} * x = e$, potom tento inverzný element existuje jednoznačne.

Predpokladajme, že x má dva inverzné elementy u a v

$$x * u = u * x = e$$

$$x * v = v * x = e$$

Potom

$$u = u * e = u * \left(x * v \right) = \left(u * x \right) * v = e * v = v$$

Poznamenajme, že dôkaz jednoznačnosti inverzného elementu kľúčovú úlohu hrala podmienka asociatívnosti súčinu $*$, ak tento súčin nie je asociatívny, potom nevieme zabezpečiť túto jednoznačnosť inverzného elementu.

Príklad

Budeme študovať binárnu operáciu $*$ nad množinou $X=\{a,b,c,d\}$, ktorá je určená multiplikatívnou tabuľkou

$*$	a	b	c	d
a	a	b	c	d
b	d	c	a	a
c	c	b	a	d
d	d	b	c	a

Takto definovaná binárna operácia nie je asociatívna.

$$b*(c*d)=b*d=a$$

$$(b*c)*d=a*d=d$$

to znamená, že pre tento konkrétny výber troch elementov z množiny X sme dokázali

$$b*(c*d)\neq(b*c)*d$$

t. j. binárna operácia nie je asociatívna.

Pologrupy, monoidy a grupy

Budeme študovať jednoduché algebraické štruktúry $(G,*)$, kde G je množina a $*$ je binárna operácia nad touto množinou. Jedna z najjednoduchších takýchto algebraických štruktúr je pologrupa.

Definícia. Nech G je neprázdna množina a $*$ je binárna operácia nad touto množinou. Algebraická štruktúra $(G,*)$ sa nazýva ***pologrupa*** vtedy a len vtedy, ak binárna operácia $*$ je asociatívna

$$(\forall x,y,z \in G)\big((x*y)*z = x*(y*z)\big)$$

Ak binárna operácia $*$ je aj komutatívna, potom algebraická štruktúra sa nazýva ***komutatívna pologrupa*** (alebo ***Abelova pologrupa***).

Príklady

(1) Algebraické štruktúry $(\mathbb{N},+)$, $(\mathbb{N},\times)$ sú komutatívne pologrupy. Binárne operácie súčtu a súčinu nad množnou celých čísel $\mathbb{N}$ sú asociatívne a komutatívne.

Tieto dve algebraické štruktúry môžeme zovšeobecniť na množinu $\mathbb{R}$ reálnych čísiel, potom štruktúry $(\mathbb{R},+)$, $(\mathbb{R},\times)$ sú taktiež komutatívne pologrupy.

(2) Nech $A=\{a,b,c,...\}$ je konečná množina symbolov našej abecedy. Reťazce dĺžky n obsahujúce znaky tejto množiny tvoria n-násobný karteziánsky produkt A^n. Množina $A^*=\{\varepsilon\}\cup A_1\cup A_2\cup ...$, získame množinu, ktorá obsahuje všetky možné reťazce nad A, včítane prázdneho reťazca ε. Binárna operácia „spojenia“ (konkatenácie) dvoch reťazcov $\alpha,\beta\in A^*$ vytvorí nový reťazec $\gamma=(\alpha+\beta)\in A^*$. Táto binárna operácia je asociatívna a nekomutatívna. Algebraická štruktúra $(A^*,+)$ je nekomutatívna pologrupa.

(3) Pre množinu $A=\{a,b,c\}$ definujme binárnu operáciu pomocou multiplikačnej tabuľky

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Táto multiplikačná tabuľka je symetrická, z čoho plynie skutočnosť, že binárna operácia je komutatívna. Dôkaz asociatívnosti binárnej operácie je netriviálna záležitosť, pre všetky možné usporiadané trojice s opakovaním musíme dokázať, že platí zákon asociatívnosti

$$\forall(x,y,z\in A)\big(x*(y*z)=(x*y)*z\big)$$

Dá sa ukázať, že operácia $*$ je asociatívna. Potom, algebraická štruktúra $(A,*)$ je komutatívna pologrupa.

Definícia. Pologrupa $(A,*)$ sa nazýva ***monoid*** vtedy a len vtedy, ak má jednotkový element.

Príklady

(1) Algebraická štruktúra $(\mathbb{N}_+,\times)$, kde množina $\mathbb{N}_+$ obsahuje kladné celé čísla je monoid, existuje jednotkový prvok ´1´, ktorý zachováva súčin $x*1=1*x=x$. Podobná algebraická štruktúra $(\mathbb{N}_+,+)$, ktorá je pologrupou, nie je monoid, pre operáciu súčet neexistuje v rámci množiny $\mathbb{N}_+$ jednotkový prvok ´0´ (pretože $0\notin\mathbb{N}_+$), ktorý zachováva súčet $x+0=0+x=x$.

(2) Nech $(A^*,+)$ je nekomutatívna pologrupa reťazcov nad abecedou A, pričom táto množina obsahuje aj prázdny znak ε. Táto algebraická štruktúra má jednotkový element ε, ktorý je neutrálny vzhľadom k binárnej operácii spojenia reťazcov

$$\forall\left(x\in A^*\right)\left(\varepsilon+x=x+\varepsilon=x\right)$$

Algebraická štruktúra $(A^*,+)$ je monoid.

(4) Nech $(X,\cup)$ a $(X,\cap)$, kde $X=\mathcal{P}(A)$, sú algebraické štruktúry. Obe tieto štruktúry sú pologrupy, pretože množinové operácie zjednotenia a prieniku sú asociatívne. Tieto štruktúry tvoria monoidy, pretože prvá (druhá) štruktúra má jednotkový element prázdnu množinu $\varnothing$ (množinu A)

$$\forall\big(X\in\mathcal{P}(A)\big)\big(\varnothing\cup X=X\cup\varnothing=X\big)$$

$$\forall\big(X\in\mathcal{P}(A)\big)\big(A\cap X=X\cap A=X\big)$$

Mnohé algebraické štruktúry, ktoré sú monoidy, majú ešte dodatočnú vlastnosť, ku každému prvku z množiny existuje inverzný element. Potom takýto monoid sa nazýva grupa. Algebraické štruktúry tohto typu našli široké uplatnenie nielen v mnohých oblastiach matematiky a informatiky, ale aj vo fyzike, chémii a pod.

Definícia. Monoid $(G,*)$ sa nazýva ***grupa*** vtedy a len vtedy, ak ku každému elementu $x \in G$ existuje inverzný element $x^{-1} \in G$. Platí teda, že algebraická štruktúra $(G,*)$ je ***grupa*** vtedy a len vtedy, ak sú splnené tieto tri podmienky:

(1) binárna operácia $*$ je asociatívna,

(2) existuje jednotkový element $e \in G$,

(3) pre každé $x \in G$ existuje inverzný element $x^{-1} \in G$.

Mohutnosť množiny G sa nazýva rád grupy $(G,*)$, označuje sa $|G|$.

Príklady

(1) Algebraická štruktúra $(\mathbb{Z},+)$, kde $\mathbb{Z}$ je množina celých čísel, je komutatívna grupa. Binárna operácia súčet $'+'$ je asociatívna a komutatívna, číslo $0\in\mathbb{Z}$ má charakter neutrálneho prvku vzhľadom k operácii $'+'$, $0+x=x+0=x$, pre každé číslo x ; podobne, pre každé číslo $x\in\mathbb{Z}$ existuje ′inverzné′ číslo $(-x)\in\mathbb{Z}$ také, že $(-x)+x=x+(-x)=0$.

(2) Algebraická štruktúra $(\mathbb{R}_+,\times)$, kde $\mathbb{R}_+=(0,\infty)$ a použitá binárna operácie je štandardný súčin, je komutatívna grupa. Binárna operácia je asociatívna a komutatívna, existuje neutrálny prvok $1\in\mathbb{R}_+$, $1\times x=x\times 1=x$, pre každý prvok x, a taktiež ku každému x existuje inverzný prvok $x^{-1}=1/x$, pre ktorý platí $x\times(1/x)=(1/x)\times x=1$.

Veta. Ak algebraická štruktúra $(G,*)$ je grupa, potom existuje „krátenie“ zľava a zprava, pre každé $a,x,y \in G$ platí

(a) krátenie zľava

$$a*x = a*y \Rightarrow x = y$$

(b) krátenie sprava

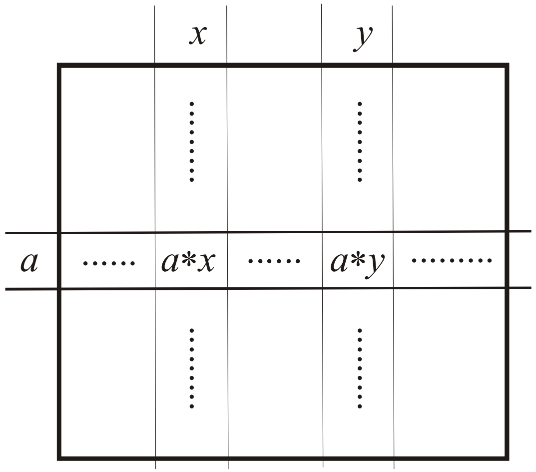
$$x*a = y*a \Rightarrow x = y.$$

Veta. Ak algebraická štruktúra $(G,*)$ je grupa, potom pre ľubovolné $a,b \in G$ platí

(a) rovnica $a*x = b$ má jednoznačné riešenie $x = a^{-1}*b$,

(b) rovnica $x*a = b$ má jednoznačné riešenie $x = b*a^{-1}$.

Veta. Ak algebraická štruktúra $(G,*)$ je grupa, potom v multiplikačnej tabuľke binárnej operácie $*$ sa v každom riadku alebo stĺpci vyskytuje každý element z G práve len raz.



Predpokladajme, že $a*x=a*y$, potom $x=y$, čo je však v spore, že stĺpce sú rôzne. Dôkaz pre stĺpce je podobný.

Definícia. Hovoríme, že algebraická štruktúra $(H,*)$ je ***podgrupa*** grupy $(G,*)$ vtedy a len vtedy, ak $H \subseteq G$ a $(H,*)$ je grupa, čo budeme zapisovať $(H,*) \subseteq (G,*)$.

- Ak $(H,*) \subseteq (G,*)$, potom obe štruktúry sú grupy a obe binárne operácie sú rovnaké.
- Každá grupa má aspoň dve triviálne podgrupy. Prvá je s množinou $H = \{e\}$ a druhá s množinou $H = G$, všetky ostatné podgrupy (ak existujú) nazývame netriviálne.

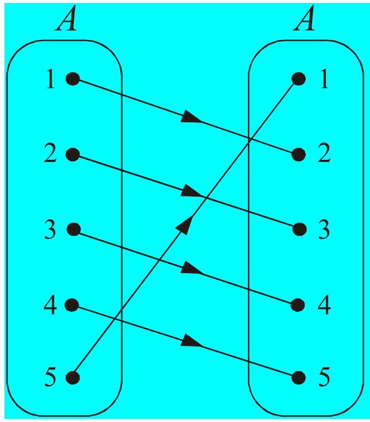
Veta (Lagrangeova). Nech $(H,*) \subseteq (G,*)$, potom rád množiny $|G|$ je deliteľný rádom podmnožiny $|H|$, alebo existuje také kladné celé číslo k, že $|G| = k|H|$

$$\left((H,*) \subseteq (G,*)\right) \Rightarrow \exists k\left(|G| = k|H|\right)$$

Grupa permutácií

Nech S_n je množina tvorená všetkými permutáciami n objektov. Permutácie sú špecifikované ako 1-1-značné zobrazenie $P : A \rightarrow A$, ktoré každému objektu $i \in A$ priradí objekt $p_i \in A$, pričom z podmienky 1-1-značnosti vyplýva podmienka $\forall\left(i, j \in A\right)\left(i \neq j \Rightarrow p_i \neq p_j\right)$, permutáciu P vyjadríme formulou

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \Leftrightarrow P = \begin{pmatrix} p_1 & p_2 & \dots & p_n \end{pmatrix}$$



$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\left|S_n\right| = n!$$

Binárna operácia $*$ zobrazuje z dvoch permutácií novú permutácie

$$*: S_n \times S_n \to S_n$$

$$\begin{aligned}
P'' = P * P' &= \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} * \begin{pmatrix} 1 & 2 & \dots & n \\ p'_1 & p'_2 & \dots & p'_n \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} * \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ p''_1 & p''_2 & \dots & p''_n \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & \dots & n \\ p''_1 & p''_2 & \dots & p''_n \end{pmatrix}
\end{aligned}$$

Súčin dvoch permutácií môžeme interpretovať ako kompozíciu dvoch zobrazení P a P'.

Znázornenie súčinu dvoch permutácií $(3 \quad 2 \quad 1) * (2 \quad 1 \quad 3)$.

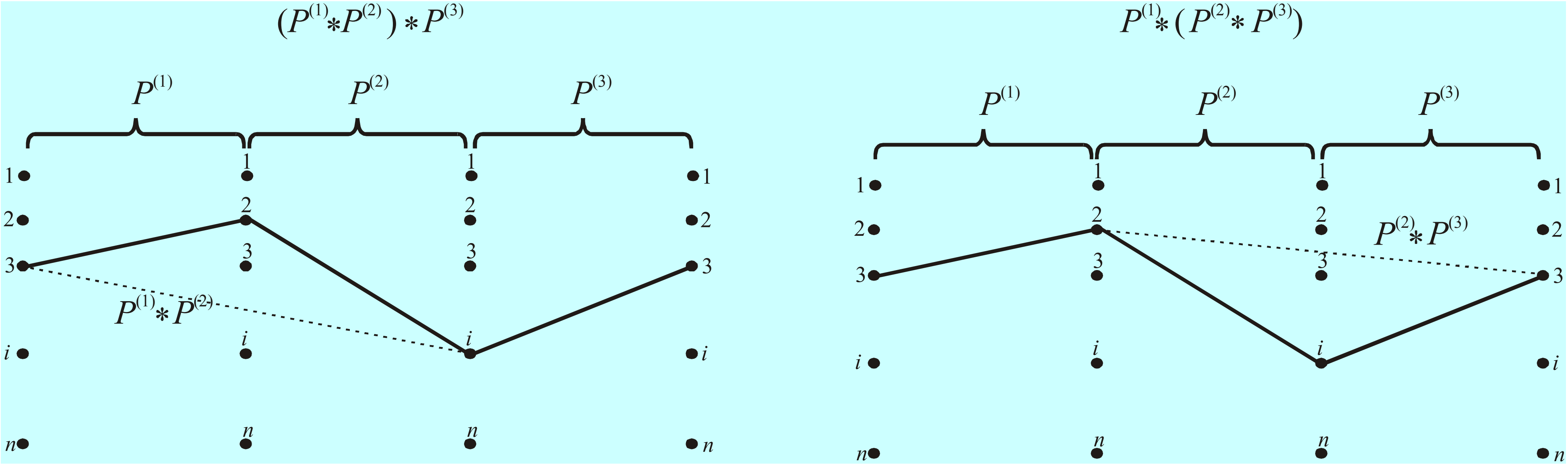
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Súčin dvoch permutácií musí byť asociatívnou operáciou, pre súčin ľubovolných troch permutácií P_1, P_2, P_3 platí

$$P_1 * \left(P_2 * P_3\right) = \left(P_1 * P_2\right) * P_3$$



Inverzná permutácia je zostrojená jednoduchou inverziou tabuľlky špecifikujúcej permutáciu

$$P = \begin{pmatrix} 1 & 2 & \dots & n \\ p_1 & p_2 & \dots & p_n \end{pmatrix} \Rightarrow P^{-1} = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Príklad

Zostrojte multiplikačnú tabuľku permutácií troch objektov. Jednotlivé permutácie označíme takto

$$P_1 = (123),\ P_2 = (231),\ P_3 = (312),$$

$$P_4 = (132),\ P_5 = (321),\ P_6 = (213)$$

Potom multiplikačná tabuľka pre tieto permutácie má tvar

$*$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_5	P_6	P_4
P_3	P_3	P_1	P_2	P_6	P_4	P_5
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_4	P_6	P_2	P_1	P_3
P_6	P_6	P_5	P_4	P_3	P_2	P_1

Morfizmy

Definícia. Hovoríme, že medzi grupami $(G,*)$ a $(G',\circ)$ existuje ***izomorfimus*** (alebo, že grupy sú ***izomorfné***), čo značíme $(G,*)\cong(G',\circ)$, vtedy a len vtedy, ak existuje 1-1-značné zobrazenie $f:G\to G'$, ktoré

$$\forall(x,y\in G)\big(f(x*y)=f(x)\circ f(y)\big)$$

Príklad

Uvažujme dve grupy $(\mathbb{R},+)$ a grupu $(\mathbb{R}_+,\times)$, kde $\mathbb{R}_+=(0,\infty)$. Dokážte, že funkcia $f(x)=2^x$ definuje izomorfizmus medzi týmito dvoma grupami, $(\mathbb{R},+)\cong(\mathbb{R}_+,\times)$. Funkcia $f(x)=2^x$ je monotónne rastúca, čiže je aj 1-1-značná. Funkcia má zaujímavú vlastnosť, $(\forall x,y\in\mathbb{R})\,f(x+y)=f(x)\cdot f(y)$, pomocou ktorej sa jednoducho zostrojí izomorfizmus medzi grupami, $f:\mathbb{R}\to\mathbb{R}_+$.

Veta. Ak $f: G \to G'$ je izomorfizmus medzi grupami $(G,*)$ a $(G',\circ)$, potom

(1) Ak e je jednotkový element v grupe $(G,*)$, potom $f(e)$ je jednotkový element v grupe $(G',\circ)$.

(2) Grupa $(G,*)$ je komutatívna vtedy a len vtedy, ak $(G',\circ)$ je komutatívna grupa.

(3) Ak x^{-1} je inverzný element vzhľadom k elementu x v grupe $(G,*)$, potom $f(x^{-1})$ je inverzný element vzhľadom k elementu $f(x)$ v grupe $(G',\circ)$.

(4) Inverzné zobrazenie $f^{-1}: G' \to G$ definuje izomorfizmus z grupy $(G',\circ)$ do grupy $(G,*)$.

(5) Ak $(H,*)$ je podgrupa grupy $(G,*)$, potom $(H',\circ)$, kde $H' = \{f(x); x \in H\}$, je podgrupa grupy $(G',\circ)$ a $(H,*) \cong (H',\circ)$.

Príklad

Dokážte, že ak $A=\{a,b\}$, potom monoidy $(\mathcal{P}(A),\cup)$ a $(\mathcal{P}(A),\cap)$ sú izomorfné. Multiplikatívne tabuľky pre tieto monoidy sú

$\cup$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

$\cap$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\{a\}$	$\varnothing$	$\{a\}$	$\varnothing$	$\{a\}$
$\{b\}$	$\varnothing$	$\varnothing$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$

1-1-značná funkcia $f:\mathcal{P}(A)\to\mathcal{P}(A)$, ktorá zobrazuje prvú tabuľku na druhú má tvar

$$f(\varnothing)=\{a,b\},\ f(\{a\})=\{a\},\ f(\{b\})=\{b\},\ f(\{a,b\})=\varnothing$$

Potom medzi monoidami $(\mathcal{P}(A),\cup)$ a $(\mathcal{P}(A),\cap)$ existuje izomorfizmus.

Definícia. Hovoríme, že medzi grupami $(G,*)$ a $(G',\circ)$ existuje ***morfizmus*** vtedy a len vtedy, ak existuje zobrazenie $f:G\to G'$, ktoré

$$\forall(x,y\in G)\big(f(x*y)=f(x)\circ f(y)\big)$$

Ak medzi dvoma algebraickými štruktúrami existuje izomorfizmus, potom tieto štruktúry sú „skoro totožné“. Ak odstránime podmienku 1-1-značnosti funkcie $f:G\to G'$, potom táto „skoro totožnosť“ sa stráca, druhá algebraická štruktúra $(G',\circ)$ stráca niektoré detaily prvej štruktúry.

Veta 2.10. Ak $f: G \to G'$ je ***morfizmus*** medzi grupami $(G,*)$ a $(G',\circ)$, potom

(1) Ak e je jednotkový element v grupe $(G,*)$, potom $f(e)$ je jednotkový element v grupe $(G',\circ)$.

(2) Grupa $(G,*)$ je komutatívna vtedy a len vtedy, ak $(G',\circ)$ je komutatívna grupa.

(3) Ak x^{-1} je inverzný element vzhľadom k elementu x v grupe $(G,*)$, potom $f(x^{-1})$ je inverzný element vzhľadom k elementu $f(x)$ v grupe $(G',\circ)$.

Príklad

Uvažujme množinu $A=\{a,b,c\}$, množina A^* obsahuje všetky možné reťazce (včítane prázdneho reťazca ε). Algebraická štruktúra $\left(A^*,*\right)$, kde binárna operácia $*$ reprezentuje spájanie reťazcov, je monoid (existuje jednotkový element reprezentovaný prázdnym reťazcom ε). Nech existuje funkcia $f : A^* \to \mathbb{N}$, kde $\mathbb{N}$ je množina nezáporných celých čísel, táto funkcia je definovaná takto

$$f\left(x\right)=\text{dĺžka reťazca } x$$

Ukážte, že toto zobrazenie f je morfizmus z $\left(A^*,*\right)$ na $\left(\mathbb{N},+\right)$.

Z definície funkcie f vyplýva, že platí

$$f\left(x*y\right)=f\left(x\right)+f\left(y\right)$$

t. j. dĺžka spojeného reťazca $x*y$ sa rovná súčtu dĺžok je zložiek x a y. Táto funkcia evidentne nie je 1-1-značná.

Boolova algebra

Elektronické obvody v počítačoch a v podobných zariadeniach sú charakterizované binárnymi vstupmi a výstupmi (rovnajúcimi sa 0 alebo 1), transformácia vstupu na výstupu sa uskutočňuje prostredníctvom elektronického obvodu, ktorý tvorí jadro tohto „transformačného“ zariadenia.

Všeobecná definícia ***Boolovej funkcie*** je

$$f:\{0,1\}^m \rightarrow \{0,1\}^n$$

Môžeme si položiť otázku, ako realizovať túto Boolovu funkciu, aby mala vopred špecifikované vlastnosti? Tento problém je realizovaný pomocou Boolovej algebry, ktorá pomocou premenných s 0-1 ohodnotením (t. j. binárnych) premenných a pomocou dvoch elementárnych algebraických operácií a jednej unárnej algebraickej operácie je schopná dostatočne všeobecne modelovať Boolove funkcie s vopred špecifikovanými vlastnosťami.

Boolova algebra má dva známe modely, prvým je výroková logika a druhým algebra teórie množín. Medzi zákonmi výrokovej logiky a formulami teórie množín existuje „dualizmus“

$$\neg(p \wedge q) \equiv (\neg p \vee \neg q) \Leftrightarrow \overline{A \cap B} = \bar{A} \cup \bar{B}$$
$$\neg(p \vee q) \equiv (\neg p \wedge \neg q) \Leftrightarrow \overline{A \cup B} = \bar{A} \cap \bar{B}$$

Vo všeobecnosti, dualizmus medzi výrokovou logikou a algebrou teórie množín môžeme zosumarizovať takto

výrokové premenné $p,q,r,\ldots \Leftrightarrow$ množiny $A,B,C,\ldots$

spojka negácie $\neg \Leftrightarrow$ operácia doplnku $\overline{}$

spojka konjunkcie $\wedge \Leftrightarrow$ operácia prieniku $\cap$

spojka disjunkcie $\vee \Leftrightarrow$ operácia zjednotenia $\cup$

spojka ekvivalentnosti $\equiv \Leftrightarrow$ relácia rovnosti $=$

Definícia. ***Boolova algebra*** je algebraická štruktúra špecifikovaná usporiadanou 6-ticou $\left(B,+,\cdot,\overline{},\mathbf{0},\mathbf{1}\right)$, kde $B=\{a,b,\ldots,x,y,\ldots\}$ je neprázdna množina prvkov (premenných Boolovej algebry), ktorá obsahuje dva špeciálne odlíšené prvky - konštanty $\mathbf{0},\mathbf{1}\in B$ a nad ktorou sú definované binárne operácie súčinu a súčtu

$$\cdot : B\times B\to B \text{ a } + : B\times B\to B$$

a unárna operácia komplementu

$$\overline{} : B\to B$$

ktoré vyhovujú týmto podmienkam

(1) komutatívnosť:

$$x\cdot y=y\cdot x \text{ a } x+y=y+x$$

(2) asociatívnosť:

$$\left(x\cdot y\right)\cdot z=x\cdot\left(y\cdot z\right) \text{ a } \left(x+y\right)+z=x+\left(y+z\right)$$

(3) distributívnosť:

$$x\cdot\left(y+z\right)=\left(x\cdot y\right)+\left(x\cdot z\right) \text{ a } x+\left(y\cdot z\right)=\left(x+y\right)\cdot\left(x+z\right)$$

(4) vlastnosť konštanty **0**:

$$x=x+\mathbf{0} \text{ a } x\cdot\overline{x}=\mathbf{0}$$

(5) vlastnosť konštanty **1** : $x=x\cdot\mathbf{1}$ a $x+\overline{x}=\mathbf{1}$

Príklad

Najjednoduchšia Boolova algebra (s veľkým významom v informatike a v logike) je založená na dvojprvkovej množine $B=\{0,1\}$. Binárne operácie súčinu, súčtu a unárna operácia komplementu sú pomocou multiplikačných tabuliek definované takto

$+$	0	1
0	0	1
1	1	1

$\llcorner$	0	1
0	0	0
1	0	1

b	$\bar{b}$
0	1
1	0

Jednoducho sa môžeme presvedčiť, že algebraická štruktúra $\left(B,+,\cdot,\overline{},\mathbf{0},\mathbf{1}\right)$ je Boolova algebra.

Príklad

Nech $B = \mathcal{P}(A)$, kde $A = \{a, b, c, ...\}$ je neprázdna množina. Operácie $\cdot$ a $+$ sú realizované pomocou množinových operácií $\cap$ resp. $\cup$, operácia komplementu je realizovaná ako množinový komplement vzhľadom k množine A, $\overline{x} = A - x$:

(a) binárne operácie sú asociatívne, komutatívne,

(b) medzi binárnymi operáciami platia distributívne zákony,

(c) prázdna množina $\emptyset$ má vlastnosti neutrálneho prvku pre operáciu $\cup$

$$(\forall X \in B)(X \cup \emptyset = \emptyset \cup X = X)$$

(d) množina A má vlastnosti neutrálneho prvku pre operáciu $\cap$

$$(\forall X \in B)(X \cap A = A \cap X = X)$$

(e) pre každé $X \in B$ existuje komplement $\overline{X} \in B$ taký, že

$$(\forall X \in B)(X \cap \overline{X} = \emptyset)$$

$$(\forall X \in B)(X \cup \overline{X} = A)$$

To znamená, algebraická štruktúra $\left(\mathcal{P}(A), \cup, \cap, {}^{-}, \emptyset, A\right)$ je Boolova algebra.

Príklad

Nech $B = \{p, q, r, ...\}$ je množina výrokových formúl, ktorá je uzavretá vzhľadom k binárnym operáciám konjunkcie ($\wedge$), disjunkcie ($\vee$) a k unárnej operácii negácie ($\neg$). Pre túto množinu je definovaná aj relácia ekvivalentnosti ´$\equiv$´, dve formuly sú ekvivalentné vtedy a len vtedy, ak majú rovnakú pravdivostnú interpretáciu (logicky ekvivalentné). Z množiny B vyberieme formulu kontradikciu (napr. $p \wedge \neg p$) a označíme ju symbolom 0; podobne formula tautológia (napr. $p \vee \neg p$) je označená symbolom 1. To znamená, že symboly **0** a **1** patria do množiny B. Pre každú formulu p platia tieto vzťahy

$$p \vee 0 = 0 \vee p = p \quad \text{a} \quad p \wedge 1 = 1 \wedge p = p$$

Pretože logické spojky konjunkcie a disjunkcie sú komutatívne a asociatívne, pre tieto operácie platia taktiež distributívne zákony, algebraická štruktúra $(B, \vee, \wedge, \neg, 0, 1)$ tvorí Boolovu algebru.

Vlastnosti Boolovej algebry

Ukážeme, že tento princíp duality je aplikovateľný aj pre Boolove algebry.

Postulujme nejakú formulu Boolovej algebry, duálnu formu dostaneme tak, že urobíme zámenu symbolov

$$\cdot \rightarrow +,\ + \rightarrow \cdot,\ \mathbf{0} \rightarrow \mathbf{1} \text{ a } \mathbf{1} \rightarrow \mathbf{0}$$

Uvažujme formulu Boolovej algebry, $\left(x+y\right)\cdot x\cdot \overline{y}=\mathbf{0}$, duálny tvar tejto formuly je $\left(x\cdot y\right)+x+\overline{y}=\mathbf{1}$.

Axiómy Boolovej algebry sú uvedené po dvojiciach duálnych formúl. To znamená, že ak v rámci Boolovej algebry odvodíme nejakú formulu, tak potom aj jej duálna forma je odvoditeľná pomocou postupu, ktorý je „duálny“ k postupu prvej formuly.

Veta (princíp duality). Každá veta Boolovej algebry je taktiež vetou aj v duálnej forme.

V Boolovej algebre neutrálne prvky **1** a **0** existujú jednoznačne, podobne, komplementárny prvok existuje jednoznačne.

Veta. Neutrálne prvky **1** a **0** existujú jednoznačne.

Veta. Pre každý prvok $x \in B$ existuje jednoznačne prvok $\overline{x} \in B$ taký, že $x \cdot \overline{x} = \mathbf{0}$ a $x + \overline{x} = \mathbf{1}$.

Veta. Nech $\left(B,+,\cdot,\bar{\ },\mathbf{0},\mathbf{1}\right)$ je Boolova algebra, potom platia tieto formule:

(1) Involutívnosť komplementu

$$(\forall x\in B)\left(\overline{\overline{x}}=x\right)$$

(2) Idempotentnosť

$$(\forall x\in B)(x\cdot x=x) \text{ a } (\forall x\in B)(x+x=x)$$

(3) De Morganove zákony

$$(\forall x,y\in B)\left(\overline{x+y}=\overline{x}\cdot\overline{y}\right) \text{ a } (\forall x,y\in B)\left(\overline{x\cdot y}=\overline{x}+\overline{y}\right)$$

(4) Nulitnosť

$$(\forall x\in B)(x+\mathbf{1}=\mathbf{1}) \text{ a } (\forall x\in B)(x\cdot\mathbf{0}=\mathbf{0})$$

(5) Absorpcia

$$(\forall x,y\in B)\big(x+(x\cdot y)=x\big) \text{ a } (\forall x\in B)\big(x\cdot(x+y)=x\big)$$

(6) Komplementy konštánt

$$\overline{\mathbf{0}}=\mathbf{1} \text{ a } \overline{\mathbf{1}}=\mathbf{0}$$

(7) Vlastnosti konštánt vzhľadom k binárnym operáciám

$$\mathbf{0}+\mathbf{0}=\mathbf{0},\mathbf{0}+\mathbf{1}=\mathbf{1},\mathbf{1}+\mathbf{0}=\mathbf{1},\mathbf{1}+\mathbf{1}=\mathbf{1} \text{ a } \mathbf{0}\cdot\mathbf{0}=\mathbf{0},\mathbf{0}\cdot\mathbf{1}=\mathbf{0},\mathbf{1}\cdot\mathbf{0}=\mathbf{0},\mathbf{1}\cdot\mathbf{1}=\mathbf{1}$$

Boolove funkcie

V úvode k tejto kapitole bola Boolova funkcia definovaná ako funkcia nad binárnymi premennými $\{0,1\}$. Tento pomerne zjednodušený pohľad na Boolovu funkciu bude teraz rozšírený tak, aby koncepcia Boolovej funkcie bola časťou Boolovej algebry.

Definícia. Nech $\left(B,+,\cdot,{}^{-},\mathbf{0},\mathbf{1}\right)$ je Boolova algebra. Potom,

(1) ***Boolova premenná*** je taká premenná, ktorá nadobúda hodnoty z množiny *B*,

(2) ***komplement premennej*** x, označený $\overline{x}$, je taká premenná, ktorej hodnota sa rovná komplementu hodnoty premennej x (t. j. ak $x=b\in B$, potom $\overline{x}=\overline{b}\in B$,

(3) ***literál*** je Boolova premenná x alebo jej komplement $\overline{x}$

$$x^e=\begin{cases} x & (pre\ e=1) \\ \overline{x} & (pre\ e=0) \end{cases}.$$

Definícia. Nech $\left(B,+,\cdot,{}^{-},\mathbf{0},\mathbf{1}\right)$ je Boolova algebra. Potom ***Boolova formula***, obsahujúca Boolove premenné $x_1,x_2,\ldots,x_n$, je definovaná takto:

(1) konštanty **0** a **1** sú Boolove formuly,

(2) Boolove premenné $x_1,x_2,\ldots,x_n$ sú Boolove formuly,

(3) ak X a Y sú Boolove formuly, potom aj výrazy $\left(X\cdot Y\right)$, $\left(X+Y\right)$, $\overline{X}$ a $\overline{Y}$ sú Boolove formuly.

Rastúca priorita operácií: (1) súčet, (2) súčin a (3) komplement. Napríklad, formulu $\left(\left(x\cdot y\right)+z\right)$ môžeme pomocou tejto konvencie vyjadriť v zjednodušenom tvare bez zátvoriek $x\cdot y+z$. Konečne, podobne ako v štandardnej algebre, budeme vynechávať znak súčinu, napríklad predchádzajúci ilustračný príklad má tvar $xy+z$.

Príklad

Zjednodušte formulu $\left(\left(x+y\right)\cdot\left(\overline{x}+\overline{y}\right)\right)$. Použitím distributívneho zákona a zákona nulitnosti

$$\left(\left(x+y\right)\cdot\left(\overline{x}+\overline{y}\right)\right)=\left(x\cdot\overline{x}\right)+\left(x\cdot\overline{y}\right)+\left(y\cdot\overline{x}\right)+\left(y\cdot\overline{y}\right)=\underbrace{x\overline{x}}_{\mathbf{0}}+x\overline{y}+y\overline{x}+\underbrace{y\overline{y}}_{\mathbf{0}}=x\overline{y}+\overline{x}y$$

Definícia. Dve Boolove formule sú ***ekvivalentné*** (alebo ***rovné***) vtedy a len vtedy, ak jedna formula je pomocou konečného počtu aplikácií axióm Boolovej algebry pretransformovaná na druhú formulu.

Podľa predošlého príkladu $\varphi_1=\left(x+y\right)\cdot\left(\overline{x}+\overline{y}\right)$ a $\varphi_2=x\overline{y}+\overline{x}y$ sú ekvivalentné, pretože druhú formulu získame z prvej použitím konečného počtu aplikácií axióm Boolovej algebry, potom $\varphi_1=\varphi_2$.

Definícia. Nech $\left(B,+,\cdot,^{-},\mathbf{0},\mathbf{1}\right)$ je Boolova algebra.

(1) ***Boolova funkcia*** premenných $x_1, x_2, \ldots, x_n$, pre danú, je funkcia $f : B^n \to B$, pričom $f\left(x_1, x_2, \ldots, x_n\right)$ je Boolova formula.

(2) Všetky Boolove formule, ktoré sú navzájom ekvivalentné, definujú rovnakú funkciu.

Z tejto definície vyplýva, že ekvivalentné Boolove formuly špecifikujú rovnakú Boolovu formulu. Napríklad, máme dve funkcie

$$f : B^2 \to B \qquad f\left(x_1, x_2\right) = x_1\left(\overline{x}_1 + x_2\right)$$
$$g : B^2 \to B \qquad g\left(x_1, x_2\right) = x_1 x_2$$

Použitím distribučného zákona ľahko dokážeme, že formuly sú ekvivalentné, $x_1\left(\overline{x}_1 + x_2\right) = x_1 x_2$, potom funkcie *f* a *g* sú rovnaké.

Definícia. ***Súčinová klauzula*** premenných $x_1, x_2, \ldots, x_n$ je Boolova formula, ktorá obsahuje súčin n literálov (t. j. premennú alebo jej komplement) pre každdú premennú.

Ako príklad súčinovej klauzuly premenných x_1, x_2, x_3 sú tieto formuly: $x_1 x_2 x_3$, $x_1 x_2 \overline{x}_3$, $x_1 \overline{x}_2 x_3$, $\overline{x}_1 x_2 x_3, \ldots,$ $\overline{x}_1 \overline{x}_2 \overline{x}_3$.

Ak použijeme formalizmus x^e, potom súčinovú klauzulu premenných $x_1, x_2, \ldots, x_n$, ktorá je špecifikovaná binárnym vektorom $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$, má tvar

$$l_{\boldsymbol{e}} = x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$$

Napríklad, pre $\boldsymbol{e} = (11011)$ súčinová klauzula má tvar

$$l_{(11011)} = x_1^1 x_2^1 x_3^0 x_4^1 x_5^1 = x_1 x_2 \overline{x}_3 x_4 x_5$$

Definícia. ***Súčtová klauzula*** premenných $x_1,x_2,\ldots,x_n$ je Boolova formula, ktorá obsahuje súčet n literálov (t. j. premennú alebo jej komplement) pre každú premennú.

Podobne ako pre súčinovú klauzulu, môžeme aj súčtovú klauzulu pre premenné $x_1,x_2,\ldots,x_n$ špecifikovať binárnym vektorom $x_1,x_2,\ldots,x_n$

$$L_{\boldsymbol{e}} = x_1^{1-e_1} + x_2^{1-e_2} + \ldots + x_n^{1-e_n}$$

Pre $\boldsymbol{e} = (10100)$ súčtová klauzula má tvar

$$L_{\boldsymbol{e}} = x_1^0 + x_2^1 + x_3^0 + x_4^1 + x_5^1 = \overline{x}_1 + x_2 + \overline{x}_3 + x_4 + x_5$$

Veta. Každá Boolova funkcia $f(x_1, x_2, ..., x_n)$, ktorá sa identicky nerovná nule, môže byť špecifikovaná ako suma súčinových klauzúl

$$\begin{aligned} f(x_1, x_2, ..., x_n) &= \sum_{\boldsymbol{e}} f(e_1, e_2, ..., e_n) x_1^{e_1} x_2^{e_2} ... x_n^{e_n} \\ &= \sum_{\boldsymbol{e}} f(e_1, e_2, ..., e_n) l_{(e_1, e_2, ..., e_n)} \\ &= \sum_{\boldsymbol{e}} f(\boldsymbol{e}) l_{\boldsymbol{e}} \end{aligned}$$

Naznačíme jednoduchý konštruktívny dôkaz. Boolova funkcia $f(x_1, x_2, ..., x_n)$ je vlastne špecifikovaná jej funkčnými hodnotami $f\left(e_1, e_2, ..., e_n\right)$ pre všetky hodnoty binárneho vektora $\boldsymbol{e} = \left(e_1, e_2, ..., e_n\right)$. Hovoríme, že funkcia f je špecifikovaná tabuľkou funkčných hodnôt, ktorá obsahuje 2^n riadkov

#	$\boldsymbol{e} = (e_1, e_2, ..., e_n)$	$l_{(e_1, e_2, ..., e_n)}$
1	(00........00)	**0**
2	(00........01)	**1**
....		
i	$(e_1^{(i)}, e_2^{(i)}, ..., e_n^{(i)})$	**1/0**
....		
2^n	(11........11)	**0**

Súčinová klauzula $l_{(e_1,e_2,...,e_n)}\left(x_1,x_2,...,x_n\right)=x_1^{e_1}x_2^{e_2}...x_n^{e_n}$ má zaujímavú vlastnosť, jej funkčná hodnota sa rovná **1** len pre $\left(x_1,x_2,...,x_n\right)=\left(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n\right)$, kde $\boldsymbol{e}_i\in\left\{\mathbf{0},\mathbf{1}\right\}$, pre všetky iné prípady funkčná hodnota je **0**

$$l_{(e_1,e_2,...,e_n)}\left(x_1,x_2,...,x_n\right)=\begin{cases}\mathbf{1} & \left(pre\left(x_1,x_2,...,x_n\right)=\left(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n\right)\right)\\ \mathbf{0} & \left(pre\left(x_1,x_2,...,x_n\right)\neq\left(\boldsymbol{e}_1,\boldsymbol{e}_2,...,\boldsymbol{e}_n\right)\right)\end{cases}$$

To znamená, že pre Boolovu funkciu sú dôležité len funkčné hodnoty **1**, funkčné hodnoty **0** nie sú podstatné pre náš konštruktívny dôkaz. Zostrojíme Boolovu formulu ako sumáciu týchto klauzúl (t. j. v DNF tvare)

$$F\left(x_1,x_2,...,x_n\right)=\sum_{\boldsymbol{e}}f\left(e_1,e_2,...,e_n\right)l_{(e_1,e_2,...,e_n)}$$

Boolove funkcie $f\left(x_1,x_2,...,x_n\right)$ a $F\left(x_1,x_2,...,x_n\right)$ sú ekvivalentné, t. j. majú rovnaké funkčné hodnoty pre rôzne hodnoty argumentov.

Príklad

Zostrojte Boolovu funkciu $f(x_1, x_2) = x_1 + x_2$ v tvare DNF. Podľa dokázanej vety tvar tejto funkcie je

$$f(x_1, x_2) = f(\mathbf{0},\mathbf{0})\overline{x}_1\overline{x}_2 + f(\mathbf{0},\mathbf{1})\overline{x}_1 x_2 + f(\mathbf{1},\mathbf{0}) x_1\overline{x}_2 + f(\mathbf{1},\mathbf{1}) x_1 x_2$$

kde jednotlivé funkčné hodnoty sú uvedené v tabuľke

#	e_1	e_2	$f(e_1,e_2)$
1	**0**	**0**	**0**
2	**0**	**1**	**1**
3	**1**	**0**	**1**
4	**1**	**1**	**1**

Potom funkcia *f* má ekvivalentný DNF tvar

$$F(x_1, x_2) = \cancel{\mathbf{0}\overline{x}_1\overline{x}_2} + \mathbf{1}\overline{x}_1 x_2 + \mathbf{1} x_1\overline{x}_2 + \mathbf{1} x_1 x_2 = \overline{x}_1 x_2 + x_1\overline{x}_2 + x_1 x_2$$

Veta. Každá Boolova funkcia $f\left(x_1,x_2,...,x_n\right)$, ktorá sa identicky nerovná jednotke, môže byť špecifikovaná ako súčin sumačných klauzúl

$$f\left(x_1,x_2,...,x_n\right)=\prod_{\boldsymbol{e}}\left(f\left(e_1,e_2,...,e_n\right)+x_1^{e_1}+x_2^{e_2}+...+x_n^{e_n}\right)$$

$$=\prod_{\boldsymbol{e}}\left(f\left(e_1,e_2,...,e_n\right)+L_{\left(1-e_1,1-e_2,...,1-e_n\right)}\right)$$

$$=\prod_{\boldsymbol{e}}\left(f\left(\boldsymbol{e}\right)+L_{\overline{\boldsymbol{e}}}\right)$$

Táto veta reprezentuje hlavný duálny výsledok tejto kapitoly, že každá Boolova funkcia môže byť jednoznačne vyjadrená ako súčin súčtových klauzúl (tento tvar sa nazýva vo výrokovej logike ***konjunktívna normálna forma***, skratka KNF).

Príklad

Vyjadrite $f(x_1,x_2)=x_1(x_1+x_2)$ v KNF tvare. Tabuľku funkčných hodnôt tejto Boolovej funkcie má tvar

#	e_1	e_2	e_1+e_2	$e_1(e_1+e_2)$
1	**0**	**0**	**0**	**0**
2	**0**	**1**	**1**	**0**
3	**1**	**0**	**1**	**1**
4	**1**	**1**	**1**	**1**

Použitím vety zostrojíme Boolovu funkciu, ktorá je ekvivalentná funkcii

$$f(x_1,x_2)=x_1(x_1+x_2)$$

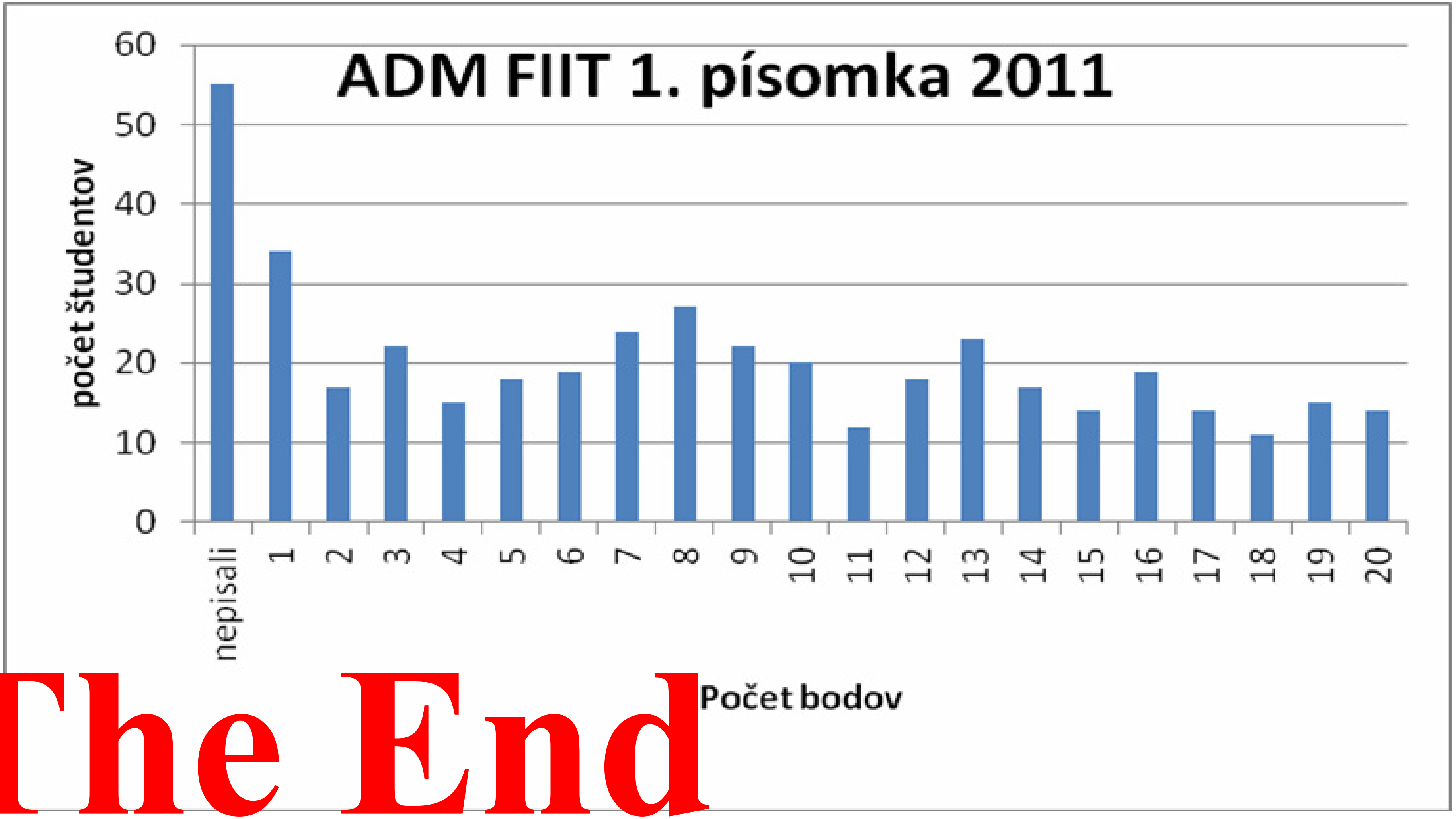
$$f(x_1,x_2)=$$

$$=\cancel{\left(\underbrace{f(\mathbf{0},\mathbf{0})}_{\mathbf{0}}+x_1+x_2\right)}\cdot\cancel{\left(\underbrace{f(\mathbf{0},\mathbf{1})}_{\mathbf{0}}+x_1+\bar{x}_2\right)}\cdot\underbrace{\left(\underbrace{f(\mathbf{1},\mathbf{0})}_{\mathbf{1}}+\bar{x}_1+x_2\right)}_{\mathbf{1}}\cdot\underbrace{\left(\underbrace{f(\mathbf{1},\mathbf{1})}_{\mathbf{1}}+\bar{x}_1+\bar{x}_2\right)}_{\mathbf{1}}$$

$$=(x_1+x_2)\cdot(x_1+\bar{x}_2)$$

"Nobody on the Internet knows I am a dog."
"Ninguém na Internet sabe que eu sou um cão."

Histogram výsledkov 1. písomky



The End