4 Booleovy algebry

4.1 Definice

Definice 4.1 Nechť $(X, \preceq)$ je svaz s nejmenším prvkem 0 a největším prvkem 1. *Komplement* prvku $x \in X$ je každý prvek y, pro který platí

$$x \vee y = 1, \quad x \wedge y = 0.$$

Představu o pojmu komplement poskytuje svaz podmnožin libovolné množiny A, kde komplementem množiny $B \subset A$ je prostě množinový doplněk $A \setminus B$. (Je totiž jasné, že sjednocením množiny B a jejího doplňku je celá množina A, zatímco jejich průnik je prázdný.)

V tomto případě je komplement určen jednoznačně. Obecně tomu tak být nemusí, ale v případech, o které se budeme zajímat, platí, že komplement libovolného prvku je nejvýše jeden:

Tvrzení 4.2 *Je-li $(X, \preceq)$ distributivní svaz s 0 a 1, potom každý prvek $x \in X$ má nejvýše jeden komplement.*

Důkaz. Nechť $x \in X$ má komplementy y a y'. Podívejme se na prvek

$$p := y \wedge (x \vee y').$$

Na jednu stranu je $x \vee y' = 1$, a tedy $p = y$. Na druhou stranu z distributivity máme $p = (y \wedge x) \vee (y \wedge y') = 0 \vee (y \wedge y') = y \wedge y'$. Zkrátka a dobře $y = y \wedge y'$, což podle tvrzení **??** znamená, že $y \preceq y'$. Zcela symetrickým způsobem ale dostaneme $y' \preceq y$, takže $y = y'$ a důkaz je u konce. $\square$

Svazům s 0 a 1, kde každý prvek má nějaký komplement, se říká *komplementární* svazy.

Definice 4.3 *Booleova algebra* je distributivní komplementární svaz s prvky 0 a 1. Používá se také pojmu *Booleův svaz.*

V Booleově algebře má tedy každý prvek x právě jeden komplement, který se značí $\bar{x}$.

U Booleových algeber je rovněž často přijímána konvence, které se přidržíme i my, totiž značit operaci suprema jako $+$ a operaci infima jako $\cdot$ (přičemž tečka se stejně jako u běžného součinu obvykle vynechává). Přepíšeme-li tedy například definici komplementu v tomto novém značení, dostaneme $x + \bar{x} = 1$ a $x\bar{x} = 0$. Zákony distributivity v novém hávu vypadají takto:

- $x(y + z) = (x \cdot y) + (x \cdot z)$,
- $x + (y \cdot z) = (x + y) \cdot (x + z)$.

První z nich vypadá jako 'stará známá' distributivita u číselných operací, prosté roznásobení závorky. Druhá rovnost, která neplatí o nic méně, ale u čísel žádnou obdobu nemá.

Cvičení 4.4 Ukažte, že následující uspořádané množiny nejsou Booleovy algebry:

(a) $\{1, 2, 3, 4, 12\}$ s uspořádáním daným dělitelností,

(b) svaz dělitelů čísla 90.

4.2 Booleovské počítání

Věta 4.5 (De Morganovy zákony) *V Booleově algebře A platí pro každé $x, y \in A$:*

(a) $\overline{x+y} = \bar{x} \cdot \bar{y}$,

(b) $\overline{xy} = \bar{x} + \bar{y}$.

Důkaz. Dokažme část (a), tedy že prvek $\bar{x} \cdot \bar{y}$ je komplementem prvku $x + y$. Nejprve je třeba ukázat, že $(x+y)+(\bar{x} \cdot \bar{y}) = 1$. K tomu použijeme distributivitu. Ta nám říká, že $p := (x + y) + (\bar{x} \cdot \bar{y}) = (x + y + \bar{x}) \cdot (x + y + \bar{y})$. Z definice komplementu ale je $x + \bar{x} = 1$, a tedy i $x + \bar{x} + y = 1$. Podobně i druhá závorka je rovna jedné, takže $p = 1 \cdot 1 = 1$.

Ve druhé polovině důkazu části (a) musíme ukázat, že prvek $q := (x+y)\cdot(\bar{x}\cdot\bar{y})$ je roven nule. Argument je podobný: z distributivity $q = [x \cdot (\bar{x} \cdot \bar{y})] + [y \cdot (\bar{x} \cdot \bar{y})]$, a protože $x\bar{x} = y\bar{y} = 0$, jsou obě hranaté závorky nulové a $q = 0 + 0 = 0$.

Část (b) se dokazuje symetricky. □

Pravidla počítání v Booleových algebrách shrnuje následující věta:

Věta 4.6 *Pro libovolné prvky a, b, c Booleovy algebry B platí:*

(1) $a + a = a$,

(2) $a + b = b + a$ *(komutativita)*,

(3) $a + (b + c) = (a + b) + c$ *(asociativita)*,

(4) $a + (ab) = a$,

(5) $a(b + c) = (ab) + (ac)$ *(distributivita)*,

(6) $a + 0 = a$,

(7) $a \cdot 0 = 0$,

(8) $\bar{1} = 0$,

(9) $a + \bar{a} = 1$,

(10) $\bar{\bar{a}} = a$,

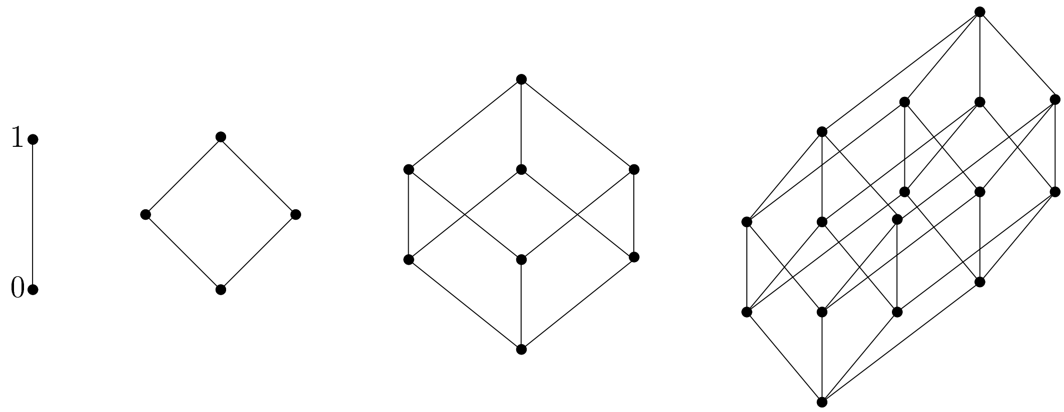
(11) $\overline{a+b} = \bar{a} \cdot \bar{b}$ *(De Morganovy zákony),*

a rovněž ***duální formy*** *všech těchto tvrzení (ve kterých zaměníme symboly* $+$ *a* $\cdot$ *a symboly* 0 *a* 1*).*

Důkaz. Většinu těchto tvrzení jsme již dokázali nebo plynou přímo z definic. Část (10) plyne z toho, že definice komplementu je symetrická: je-li $\bar{x}$ komplementem prvku x, je také x komplementem prvku $\bar{x}$, a tedy $x = \bar{\bar{x}}$. □

Důležitým příkladem Booleových algeber jsou již zmíněné svazy všech podmnožin. Víme, že soubor všech podmnožin množiny X (spolu s uspořádáním inkluzí) tvoří svaz. Je to dokonce svaz distributivní (proč?), a na začátku kapitoly jsme zjistili, že je i komplementární. Jedná se tedy o Booleovu algebru.

Podívejme se pro malá n podrobněji na Booleovu algebru tvořenou všemi podmnožinami množiny $\{1, \ldots, n\}$. Tato algebra má 2^n prvků a proto ji budeme značit $\mathcal{B}_{2^n}$. Obr. 1 ukazuje Hasseovy diagramy Booleových algeber $\mathcal{B}_{2^n}$ pro $n \leq 4$. ***** popisky u prvků $\mathcal{B}_{2^n}$, záměna prvků 1? *****



Obrázek 1: Booleovy algebry $\mathcal{B}_2$, $\mathcal{B}_4$, $\mathcal{B}_8$ a $\mathcal{B}_{16}$.

***** tabulky operací v $\mathcal{B}_4$, $\mathcal{B}_8$ *****
***** definovat $\prec$, dva pohledy na BA *****

4.3 Stoneova věta o reprezentaci

Definice 4.7 *Atom* Booleovy algebry $(\mathcal{A}, \preceq)$ je libovolný prvek $a \in \mathcal{A}$ takový, že jediným prvkem $z \in \mathcal{A}$, pro který platí $z \prec a$, je prvek $z = 0$. Množinu všech atomů Booleovy algebry $\mathcal{A}$ značíme $\mathrm{At}(\mathcal{A})$.

Všimněme si, že ekvivalentně by šlo atomy definovat jako prvky, jejichž bezprostředním předchůdcem je prvek 0. Snadno se nahlédne, že každá *konečná*

Booleova algebra obsahuje aspoň jeden atom: platí dokonce následující silnější tvrzení.

Pozorování 4.8 *Pro každý prvek $x \neq 0$ Booleovy algebry $\mathcal{A}$ existuje atom $a \in \mathrm{At}(\mathcal{A})$ takový, že $a \preceq x$.*

Důkaz. Není-li x atom, zvolme nějakého jeho bezprostředního předchůdce $x_1 \neq 0$. Není-li ani x_1 atom, zvolme jeho bezprostředního předchůdce $x_2 \neq 0$. Iterací tohoto postupu musíme po konečném počtu kroků narazit na nějaký atom a, a pro ten jistě platí $a \preceq x$. □

Na druhou stranu existují *nekonečné* Booleovy algebry, které neobsahují ani jeden atom.

Příklad 4.9 * atomy v $2^{a,b,c}$, ve svazu dělitelů 30.**

Definice 4.10 *Isomorfismus* uspořádaných množin $(X_1, \preceq_1)$ a $(X_2, \preceq_2)$ je bijekce $f : X_1 \to X_2$ taková, že pro každé $x, y \in X_1$ platí $x \preceq_1 y$ právě když $f(x) \preceq_2 f(y)$. Tyto uspořádané množiny jsou *isomorfní* (psáno $(X_1, \preceq_1) \simeq (X_2, \preceq_2)$), pokud mezi nimi existuje isomorfismus.

> **Cvičení 4.11** Ukažte, že jsou-li dvě Booleovy algebry isomorfní (jako uspořádané množiny), pak příslušný isomorfismus zachovává i operace suprema, infima a komplementu, tedy například
>
> $$f(x + y) = f(x) + f(y)$$
>
> (kde se ovšem symbol + na každé straně rovnice vztahuje k jiné Booleově algebře!)

Definice 4.12 Nechť $B = \{ a_1, \ldots, a_k \}$ je množina prvků svazu $(X, \preceq)$, který má prvky 0 a 1. Je-li $k > 1$, definujme *supremum množiny* B jako

$$\sup B = \Big(\ldots ((a_1 \vee a_2) \vee a_3) \vee \ldots \Big) \vee a_k.$$

Dále definujme $\sup \emptyset = 0$, $\sup \{ a \} = a$.

> **Cvičení 4.13** Ukažte v situaci definice 4.12, že
>
> (1) $\sup B$ je nejmenší horní závora množiny B, tj. nejmenší prvek $x \in X$ s vlastností $a_i \preceq x$ pro každé i,
>
> (2) ve vzorci pro $\sup B$ tedy nezáleží na pořadí prvků $a_1, \ldots, a_k$ ani na jejich uzávorkování (a má tak smysl psát $\sup B = a_1 \vee \ldots \vee a_k$).

Věta 4.14 (Stoneova věta) *Konečná Booleova algebra $(\mathcal{A}, \preceq)$ je isomorfní s Booleovou algebrou $(\mathbf{2}^{\mathrm{At}(\mathcal{A})}, \subseteq)$.*

Důkaz. Zkonstruujeme isomorfismus mezi uspořádanými množinami $(\mathcal{A}, \preceq)$ a $(\mathbf{2}^{\mathrm{At}(\mathcal{A})}, \subseteq)$. Konkrétně pro $x \in \mathcal{A}$ nechť

$$x^* = \{\, a \in \mathrm{At}(\mathcal{A}) \mid a \preceq x \,\}.$$

Zobrazení $x \mapsto x^*$ přiřazuje každému prvku $x \in \mathcal{A}$ množinu atomů algebry $\mathcal{A}$. Potřebujeme ukázat, že se jedná o bijekci mezi $\mathcal{A}$ a $\mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a že platí $x \preceq y$, právě když $x^* \subseteq y^*$. Důkaz rozdělíme do čtyř částí.

(1) Pokud $x \preceq y$, pak $x^* \subseteq y^*$.

Toto je nejlehčí část důkazu. Pro každé $a \in x^*$ platí $a \preceq x \preceq y$ a z tranzitivity je $a \in y^*$. Jinak řečeno, $x^* \subseteq y^*$.

(2) Pokud $x^* \subseteq y^*$, pak $x \preceq y$..

Nechť naopak $x \not\preceq y$. Podle lemmatu **??** musí být $xy \neq x$. Všimněme si, že

$$x = x \cdot 1 = x(y + \bar{y}) = xy + x\bar{y},$$

z čehož plyne, že $x\bar{y} \neq 0$. Najděme podle pozorování 4.8 atom $a \preceq x\bar{y}$. Z definice infima je $a \preceq x$ a tedy $a \in x^*$. Dále je $a \preceq \bar{y}$ a tím pádem nemůže být $a \preceq y$, protože bychom dostali $a \preceq y\bar{y} = 0$; a je však atom. Takže $a \notin y^*$. Atom a tedy dosvědčuje, že x^* není podmnožinou y^*. Tím je požadovaná implikace dokázána.

(3) Zobrazení $x \mapsto x^*$ je prosté.

Vezměme $x \neq y \in \mathcal{A}$. Z antisymetrie musí být buď $x \not\preceq y$ nebo $y \not\preceq x$; nechť platí první varianta. Podle obměny implikace v bodu (2) dostáváme, že x^* není podmnožinou y^*. Speciálně $x^* \neq y^*$ a tvrzení je dokázáno.

(4) Zobrazení $x \mapsto x^*$ je na.

Hledáme vzor libovolné množiny atomů $B = \{\, a_1, \ldots, a_k \,\} \subset \mathrm{At}(\mathcal{A})$, tedy takové $b \in \mathcal{A}$, že $b^* = B$. Dokážeme, že tuto vlastnost má prvek $b = \sup B$.

Pro každý atom $a_i \in B$ jistě platí, že $a_i \preceq b$. Otázkou je, zda tato nerovnost může platit i pro nějaký atom $c \notin B$. Dejme tomu, že ano, tedy $c \preceq b$. Rozepišme $\sup B$ s použitím symbolu $+$ a zjištění, že na závorkách nezáleží a můžeme je vynechat:

$$c \cdot b = c \cdot (a_1 + \ldots + a_k) = ca_1 + \ldots + ca_k = 0 + \ldots + 0 = 0,$$

přičemž předposlední rovnost vychází z faktu, že infimum dvou různých atomů je nutně 0. Dokázali jsme, že $c \cdot b \neq c$, a tedy $c \notin b^*$. Z toho již plyne, že $b^* = B$. Důkaz věty je proveden. $\square$

Důsledek 4.15 *Počet prvků konečné Booleovy algebry $\mathcal{A}$ je vždy mocnina čísla 2, konkrétně 2^m, kde $m = |\mathrm{At}(\mathcal{A})|$.* $\square$

Cvičení 4.16 Nechť $g : Y \to Z$ je bijekce mezi konečnými množinami. Zobrazení g indukuje zobrazení $\mathbf{2}^g : \mathbf{2}^Y \to \mathbf{2}^Z$, dané předpisem

$$\mathbf{2}^g(A) = \{\, g(a) \mid a \in A \,\}$$

pro libovolné $A \subseteq Y$. Ukažte, že $\mathbf{2}^g$ je isomorfismus Booleových algeber $(\mathbf{2}^Y, \subseteq)$ a $(\mathbf{2}^Z, \subseteq)$.

Cvičení 4.17 Ukažte, že jsou-li $g : X_1 \to X_2$ a $h : X_2 \to X_3$ isomorfismy uspořádaných množin $(X_1, \preceq_1)$ a $(X_2, \preceq_2)$, resp. $(X_2, \preceq_2)$ a $(X_3, \preceq_3)$, potom složení $h \circ g : X_1 \to X_3$ je isomorfismem uspořádaných množin $(X_1, \preceq_1)$ a $(X_3, \preceq_3)$.

Důsledek 4.18 *Dvě konečné Booleovy algebry se stejným počtem prvků jsou isomorfní.*

Důkaz. Nechť $\mathcal{A}, \mathcal{B}$ jsou Booleovy algebry (s uspořádáním, které nebudeme výslovně zmiňovat) a $|\mathcal{A}| = |\mathcal{B}| = n$. Víme, že $\mathcal{A} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a $\mathcal{B} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{B})}$, kde uvažované algebry podmnožin jsou uspořádány inkluzí. Ovšem množiny $\mathrm{At}(\mathcal{A})$ a $\mathrm{At}(\mathcal{B})$ jsou stejně velké (jejich velikost je $\log_2 n$), takže můžeme zvolit nějakou bijekci $g : \mathrm{At}(\mathcal{A}) \to \mathrm{At}(\mathcal{B})$. Tato bijekce podle cvičení 4.16 indukuje isomorfismus $\mathbf{2}^g$ mezi Booleovými algebrami $\mathbf{2}^{\mathrm{At}(\mathcal{A})}$ a $\mathbf{2}^{\mathrm{At}(\mathcal{B})}$. Celkem vzato dostáváme

$$\mathcal{A} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{A})} \simeq \mathbf{2}^{\mathrm{At}(\mathcal{B})} \simeq \mathcal{B}$$

a složením těchto tří isomorfismů je isomorfismus mezi $\mathcal{A}$ a $\mathcal{B}$. $\square$

Důsledkem Stoneovy věty je, že Booleovy algebry podmnožin jsou vlastně (až na isomorfismus) jedinými představiteli konečných Booleových algeber. Uvidíme, že s pomocí následujícího pojmu lze tento fakt vyjádřit v ještě minimalističtější podobě.

Definice 4.19 *Direktní součin* Booleových algeber $(\mathcal{A}_1, \preceq_1)$ a $(\mathcal{A}_2, \preceq_2)$ je kartézský součin $\mathcal{A}_1 \times \mathcal{A}_2$ s uspořádáním $\leq$ definovaným 'po složkách':

$$(b_1, b_2) \leq (c_1, c_2), \text{ pokud } b_1 \preceq_1 c_1 \text{ a } b_2 \preceq_2 c_2,$$

kde (b_1, b_2) a (c_1, c_2) jsou prvky součinu $\mathcal{A}_1 \times \mathcal{A}_2$. Je-li $\mathcal{A}_1 = \mathcal{A}_2$, mluvíme také o *direktní mocnině* Booleovy algebry $\mathcal{A}_1$.

Cvičení 4.20 Ukažte, že direktní součin Booleových algeber je Booleova algebra. Jak v ní vypadají suprema, infima a komplementy? Jaké jsou její atomy?

Příklad 4.21 Uvažme dvouprvkovou Booleovu algebru $\mathcal{B}_2 = \{0, 1\}$ z obr. 1. Direktní mocnina $\mathcal{B}_2^2$ sestává ze všech dvojic prvků 0 a 1. Má tedy 4 prvky, které lze psát jako 00, 01, 10 a 11. Obecně n-tou direktní mocninu $\mathcal{B}_2^n$ Booleovy algebry $\mathcal{B}_2$ lze ztotožnit s množinou všech slov, tvořených n-ticí symbolů 0 a 1. Tato slova jsou uspořádána 'po složkách', tj. $(a_1 a_2 \ldots a_n) \leq (b_1 b_2 \ldots b_n)$, pokud $a_i \preceq b_i$ pro každé i.

Tvrzení 4.22 *Je-li X n-prvková množina, pak $\mathbf{2}^X \simeq \mathcal{B}_2^n$.*

Důkaz. Bez újmy na obecnosti (díky cvičení 4.16) můžeme předpokládat, že $X = \{1, \dots, n\}$. Pro $i \in X$ uvažme 'slovo' $w_i = (0 \dots 010 \dots 0)$ s jedničkou právě na i-tém místě. Isomorfismus $f : \mathbf{2}^X \to \mathcal{B}_2^n$ je pak dán předpisem

$$f(Y) = \sum_{i \in Y} w_i,$$

kde $Y \in \mathbf{2}^X$ a symbol $\sum$ označuje sčítání v Booleově algebře $\mathcal{B}_2^n$. Je snadné nahlédnout, že f je opravdu isomorfismus. □

Důsledek 4.23 *Každá konečná Booleova algebra je isomorfní s Booleovou algebrou $\mathcal{B}_2^n$ pro nějaké n.*

Důkaz. Plyne přímo ze Stoneovy věty a tvrzení 4.22. □

4.4 Booleovské funkce

Definice 4.24 *Booleovská funkce n proměnných* je libovolná funkce $f : \mathcal{B}_2^n \to \mathcal{B}_2$.

Příkladem booleovské funkce 2 proměnných je funkce $+$, kterou už známe. Její hodnoty ukazuje tab. 1.

$+$	0	1
0	0	1
1	1	1

Tabulka 1: Hodnoty booleovské funkce $+$.

Obvyklejší tvar tabulky má jeden řádek pro každou kombinaci hodnot proměnných, jako v tab. 4.4, která ukazuje kromě funkce $+$ i funkce $\cdot$ a komplement. Jedná se o tzv. *pravdivostní tabulky*.

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

x	$\bar{x}$
0	1
1	0

Tabulka 2: Hodnoty booleovských funkcí $+$, $\cdot$ a komplement.

Cvičení 4.25 Ukažte, že definujeme-li na množině všech booleovských funkcí n proměnných uspořádání $\leq$ předpisem $f \leq g$, pokud $f(x) \preceq g(x)$ pro každé $x \in \mathcal{B}_2^n$, potom opět obdržíme Booleovu algebru. Popište suprema, infima a komplementy v této Booleově algebře.

Cvičení 4.26 Sestrojte pravdivostní tabulky následujících booleovských funkcí dvou proměnných:

(a) *symetrický rozdíl* $x \oplus y = \bar{x}y + x\bar{y}$,

(b) *implikace* $x \rightarrow y = \bar{x} + y$.

Jak je vidět z tohoto cvičení, základní booleovské funkce je možné kombinovat do funkcí složitějších. To je idea booleovských polynomů, definovaných následujícím rekurentním způsobem.

Definice 4.27 (1) Výrazy $0, 1$ a x_i (pro libovolné $i = 1, \ldots, n$) jsou booleovské polynomy v proměnných $x_1, \ldots, x_n$.

(2) Jsou-li f a g booleovské polynomy v proměnných $x_1, \ldots, x_n$, pak výrazy $(f + g), (f \cdot g)$ a $\bar{g}$ rovněž.

(3) Dva booleovské polynomy v proměnných $x_1, \ldots, x_n$ jsou si rovny, pokud určují stejnou booleovskou funkci.

Cvičení 4.28 Je výraz $x_2 + x_2 + x_2$ booleovským polynomem v proměnných $x_1, \ldots, x_5$? Je roven booleovskému polynomu x_2?

Příklad 4.29 Výraz $x \oplus y := \bar{x}y + x\bar{y}$ je booleovský polynom v proměnných x, y. Platí ovšem také $x \oplus y = (x + y)(\bar{x} + \bar{y})$. Můžeme se o tom přesvědčit pravdivostní tabulkou (tab. 4.29):

x	y	$x \oplus y$	$(x + y)(\bar{x} + \bar{y})$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

Tabulka 3: Booleovské polynomy se stejnou pravdivostní tabulkou.

Další možností je přímý výpočet podle booleovských zásad. Z distributivity totiž máme

$$\begin{aligned}(x + y)(\bar{x} + \bar{y}) &= x\bar{x} + x\bar{y} + y\bar{x} + y\bar{y} \\ &= 0 + x\bar{y} + y\bar{x} + 0 \\ &= \bar{x}y + x\bar{y}. \quad \square\end{aligned}$$

4.5 Součtový a součinový tvar

Definice 4.30 *Literál* v proměnných $x_1, \ldots, x_n$ je libovolný booleovský polynom ve tvaru x_i nebo $\bar{x}_i$, kde $i = 1, \ldots, n$. Booleovský polynom p je v *součtovém tvaru*, je-li zapsán jako součet polynomů, z nichž každý je součinem literálů. Podobně p je v *součinovém tvaru*, pokud je zapsán jako součin součtů literálů.

Příklad 4.31 Polynom $x_1x_2 + x_1\bar{x}_3$ je zapsán v součtovém, nikoli však součinovém tvaru. Polynom $x_1(x_2 + \bar{x}_3)$, který je mu roven, je zapsán v součinovém tvaru. Polynom $x_1(x_2 + \bar{x}_3) + x_1x_2$ není ani v jednom z těchto tvarů.

Naskýtá se otázka, zda každou booleovskou funkci je možné vyjádřit booleovským polynomem v součtovém tvaru. Uvidíme, že platí mnohem víc.

Definice 4.32 Booleovský polynom p v proměnných $x_1, \ldots, x_n$ je v *úplném součtovém tvaru*, jestliže je v součtovém tvaru a každý ze sčítanců obsahuje pro každé $i = 1, \ldots, n$ buďto literál x_i nebo literál $\bar{x}_i$ (ne však oba). Symetricky: p je v *úplném součinovém tvaru*, jestliže je v součinovém tvaru a každý z činitelů obsahuje pro každé $i = 1, \ldots, n$ literál x_i nebo $\bar{x}_i$.

Příklad 4.33 Polynom $\bar{x}y + x\bar{y}$ v proměnných x, y je zapsán v úplném součtovém tvaru. Jeho alternativní vyjádření, $(x + \bar{x})(y + \bar{y})$, je v úplném součinovém tvaru.

Věta 4.34 *Každou nekonstantní booleovskou funkci n proměnných lze zapsat booleovským polynomem n proměnných v úplném součtovém (úplném součinovém) tvaru.*

Důkaz. Dokážeme nejprve část o úplném součtovém tvaru. Uvažme libovolné $a = (a_1, \ldots, a_n) \in \mathcal{B}_2^n$. Nechť p_a je součin literálů x_i přes všechna i taková, že $a_i = 1$, a literálů $\bar{x}_i$ přes všechna i taková, že $a_i = 0$. Každé p_a je tedy booleovský polynom v úplném součtovém tvaru, který je navíc nenulový jen pro jediné $z \in \mathcal{B}_2^n$ (totiž $z = a$).

Mějme nyní booleovskou funkci f, kterou chceme reprezentovat booleovským polynomem v úplném součtovém tvaru, a nechť $A \subset \mathcal{B}_2^n$ je množina všech $z \in \mathcal{B}_2^n$, pro něž je $f(z) = 1$. Položíme-li

$$p_f = \sum_{a \in A} p_a,$$

pak p_f je booleovský polynom v úplném součtovém tvaru a očividně nabývá stejných hodnot jako funkce f. Vzhledem k tomu, že f není konstantní nulová funkce, není součet v definici polynomu p_f prázdný.

Pokud jde o vyjádření v úplném součinovém tvaru, stačí vyjádřit (nekonstantní) funkci $\bar{f}$ polynomem $p_{\bar{f}}$ v úplném součtovém tvaru a upravit komplement $\overline{p_{\bar{f}}}$ podle de Morganova pravidla do součinového tvaru. □

Cvičení 4.35 Jaká je situace u *konstantních* booleovských funkcí? Ukažte, že funkci s konstantní hodnotou 1 (v n proměnných) lze zapsat v úplném součtovém tvaru, ale nikoli v úplném součinovém tvaru. Odvoďte podobný výsledek pro funkci s konstantní hodnotou 0.

Příklad 4.36 Vyjádříme v úplném součtovém a součinovém tvaru booleovskou funkci f v proměnných x, y, z, zadanou pravdivostní tabulkou 4.36.

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

Tabulka 4: Pravdivostní tabulka funkce f.

Řádky tabulky, které v důkazu věty 4.34 odpovídají množině A, jsou znázorněny tučně. První z nich např. odpovídá prvku $(010) \in \mathcal{B}_2^3$, takže příslušný polynom $p_{(010)}$ je $\bar{x}y\bar{z}$. (Ověřte, že $\bar{x}y\bar{z}$ nabývá nenulové hodnoty právě pro tento jediný prvek.) Podobné členy přispějí i zbylé dva tučné řádky, takže vyjádření funkce f v úplném součtovém tvaru je

$$p_f = \bar{x}y\bar{z} + \bar{x}yz + xy\bar{z}.$$

Vyjádříme f ještě v úplném součinovém tvaru. Funkce $\bar{f}$ má hodnotu 1 všude tam, kde f má hodnotu 0. Snadno tedy vidíme, že

$$p_{\bar{f}} = \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + x\bar{y}\bar{z} + x\bar{y}z + xyz.$$

(Každý z pěti členů zde odpovídá jednomu netučnému řádku.) Nás ale zajímá součinový tvar pro funkci f. Vezmeme tedy komplement $\overline{p_{\bar{f}}}$:

$$\begin{aligned}
\overline{p_{\bar{f}}} &= \overline{\bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + x\bar{y}\bar{z} + x\bar{y}z + xyz} \\
&= \overline{\bar{x}\bar{y}\bar{z}} \cdot \overline{\bar{x}\bar{y}z} \cdot \overline{x\bar{y}\bar{z}} \cdot \overline{x\bar{y}z} \cdot \overline{xyz} \\
&= (x+y+z)(x+y+\bar{z})(\bar{x}+y+z)(\bar{x}+y+\bar{z})(\bar{x}+\bar{y}+\bar{z})
\end{aligned}$$

Příklad 4.37 Upravíme do úplného součtového tvaru polynom

$$f(x,y) = (\overline{(\bar{x}y)} \cdot \bar{x}) + y.$$

Mohli bychom sestrojit tabulku a postupovat stejně jako v minulém příkladu, ale ukážeme řešení s využitím booleovského počítání.

Nejprve se zbavíme komplementu v první závorce:

$$\begin{aligned} f(x,y) &= ((\bar{\bar{x}} + \bar{y}) \cdot \bar{x}) + y = (x + \bar{y})\bar{x} + y \\ &= x\bar{x} + \bar{y}\bar{x} + y = \bar{x}\bar{y} + y. \end{aligned}$$

Výsledný polynom je sice v součtovém tvaru, ne však v úplném součtovém tvaru, protože druhý sčítanec neobsahuje žádný literál proměnné x. Použijeme trik: vynásobíme tento sčítanec výrazem $x + \bar{x} = 1$ a upravíme. Hodnoty funkce se tím nezmění.

$$f(x,y) = \bar{x}\bar{y} + y = \bar{x}\bar{y} + y(x + \bar{x}) = \bar{x}\bar{y} + xy + \bar{x}y,$$

a to je také hledané vyjádření polynomu f v úplném součtovém tvaru.

Cvičení 4.38 * Dokažte, že pro každou Booleovskou funkci je zápis v *úplném* součtovém tvaru jednoznačný.

Poznamenejme ještě, že místo označení 'součtový tvar' se obvykle používá o něco odtažitější 'disjunktivní normální forma' (DNF); místo 'součinový tvar' se říká 'konjunktivní normální forma' (KNF). Adjektivum 'úplný' zůstává beze změny, mluvíme tedy například o úplné disjunktivní normální formě.