DRUHÁ ČÁST

BOOLEOVY ALGEBRY

8 BOOLEOVY ALGEBRY

V této kapitole zavedeme pojem Booleovy algebry a ukážeme několik důležitých příkladů těchto algeber. Potom uvedeme některé jejich základní vlastnosti a ukážeme, že existují jak úplné, tak i neúplné Booleovy algebry. V závěru kapitoly budeme pomocí základních booleovských operací $\sqcap$, $\sqcup$ a $'$ definovat několik dalších operací.

8.1 Definice Booleových algeber

Definice 8.1. *Svaz S se nazývá* **Booleova algebra,** *právě když má nulu a jednotku, je komplementární a distributivní.*

Protože Booleova algebra je komplementární a distributivní svaz, můžeme důsledek věty 7.3 vyslovit takto:

Věta 8.1. *Nechť B je Booleova algebra, pak ke každému prvku $x \in B$ existuje právě jeden jeho komplement $x' \in B$.*

Na základě věty 8.1 lze říci, že v Booleových algebrách představuje tvoření komplementu unární operaci. Proto se na tyto algebry můžeme dívat jako na algebraické struktury mající dvě binární operace $\sqcap$ a $\sqcup$ a jednu unární operaci zvanou komplement a značenou $'$. Protože však Booleovy algebry obsahují také nulu a jednotku, můžeme tyto prvky považovat za vymezení dvou nulárních operací, které značíme 0 a 1. Booleovy algebry je proto možné značit $(B, \sqcap, \sqcup, ')$ či dokonce $(B, \sqcap, \sqcup, ', 0, 1)$. Operace $\sqcap$, $\sqcup$ a $'$ se nazývají **základní booleovské operace.** Protože nemůže dojít k nedorozumění, budeme často místo Booleova algebra říkat pouze algebra.

Podle definice 8.1 je tedy Booleova algebra $(B, \sqcap, \sqcup, ', 0, 1)$ algebraická struktura se dvěma binárními operacemi $\sqcap$ a $\sqcup$, jednou unární operací $'$ a dvěma nulárními operacemi 0, 1 splňujícími následující požadavky.

Nechť x, y, z jsou libovolné prvky z B, pak:

$x \sqcap y = y \sqcap x$ komutativnost (8.1)

$x \sqcup y = y \sqcup x$ (8.1')

$(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$ asociativnost (8.2)

$(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ (8.2′)

$x \sqcap x = x$ idempotence (8.3)

$x \sqcup x = x$ (8.3′)

$x \sqcap (x \sqcup y) = x$ absorpce (8.4)

$x \sqcup (x \sqcap y) = x$ (8.4′)

$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ distributivnost (8.5)

$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$ (8.5′)

$x \sqcap 0 = 0 \wedge x \sqcup 0 = x$ nula (8.6)

$x \sqcap 1 = x \wedge x \sqcup 1 = 1$ jednotka (8.6′)

$x \sqcap x' = 0 \wedge x \sqcup x' = 1$ komplementy (8.7)

Předchozí systém požadavků jsme uvedli tak, aby byl „snadný na zapamatování", a také, aby se s ním v další části dobře pracovalo. Z předchozí teorie svazů víme, že by bylo možné tento systém podstatně zestručnit. Např. se ukázalo, že oba požadavky idempotence jsou nadbytečné (viz cv. 4.1). Také lze vypustit jednu z formulí (8.5) a (8.5′) (viz věta 6.2) a vždy po jednom členu v konjunkci (8.6) a (8.6′) (viz lemma 3.2 a 3.2′).

Poznámka. Vyslovením formulí (8.1) až (8.7) jsme získali velmi důležitý **úplný systém axiómů.** Úplností systému axiómů rozumíme to, že pokud bychom přidali další axióm tvaru identity, který není logickým důsledkem uvedených axiómů, dostaneme sporný nebo jinak řečeno nerealizovatelný systém. To znamená, že už neexistuje žádný netriviální svaz, který by splňoval všechny tyto axiómy.

Obecně platí: Jestliže přidáme další logicky nezávislé požadavky na objekty nějaké základní množiny, pak se množina objektů splňujících tyto požadavky stále zužuje. Proto bychom měli vždy po přidání nového požadavku ověřit, zda ještě existuje nějaký objekt, který nově vytvořený systém požadavků splňuje. Následující příklady ukáží (a víme to již z teorie svazů), že v případě Booleových algeber je odpověď kladná.

Příklad 8.1. Uvažujme svaz $(P(M), \cap, \cup)$, kde $P(M)$ je potence libovolné množiny M. Z příkladu 2.7 víme, že se skutečně jedná o svaz. Tento svaz je distributivní (viz př. 6.1) a také komplementární (viz př. 7.2). Nulou a jednotkou tohoto svazu jsou po řadě množiny $\emptyset$ a M. Komplementem libovolné množiny $A \in P(M)$ je množina $A' = M - A$. Proto je tento svaz Booleova algebra. Pro $M = \{a, b, c\}$ je Hasseův diagram Booleovy algebry $P(M)$ znázorněn na obr. 5c. V kapitole 10 ukážeme, že tento druh algeber je mimořádně důležitý, protože se pomocí něho dá reprezentovat libovolná konečná Booleova algebra. Uvedený příklad lze zobecnit.

Lemma 8.1. *Každé těleso množin je Booleova algebra.*

Příklad 8.2. Nejjednodušší Booleova algebra je algebra mající pouze jeden prvek — označme ho 0. Tento prvek je samozřejmě nula i jednotka. Takovéto algebře říkáme **triviální Booleova algebra** a mohli bychom ji značit $(\{0\}, \sqcap, \sqcup, ', 0, 0)$. Pro její operace zřejmě platí:

$$0 \sqcap 0 = 0 \sqcup 0 = 0' = 0$$

Příklad 8.3. Nejjednodušší netriviální Booleova algebra má dva prvky, z nichž jeden musí být nula a druhý jednotka. Můžeme ji proto značit $(\{0, 1\}, \sqcap, \sqcup, ', 0, 1)$ nebo stručně **2**. Tabulky pro její operace jsou:

$\sqcap$	0	1
0	0	0
1	0	1

$\sqcup$	0	1
0	0	1
1	1	1

	$'$
0	1
1	0

(8.8)

Často se místo těchto **Cayleyho tabulek** používají k zadávání tzv. **Schröderovy tabulky** známé z matematické logiky:

x	y	$x \sqcap y$	$x \sqcup y$	x'
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0

(8.9)

Dvouprvkové Booleovy algebry jsou velmi jednoduché a přitom zajímavé a důležité z hlediska svých aplikací. Právě vzhledem k těmto aplikacím pojednáme podrobně v kap. 11 o Booleových funkcích definovaných na těchto algebrách.

Příklad 8.4. Uvažujme množinu B všech dělitelů číslo 30 v množině **N**. Jestliže v množině $B = \{1, 2, 3, 5, 6, 10, 15, 30\}$ zavedeme operace takto (viz př. 2.5b):

$$x \sqcap y =_{\text{df}} D(x, y)$$

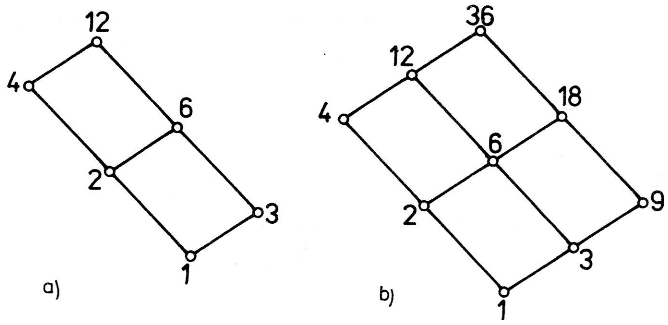
$$x \sqcup y =_{\text{df}} n\,(x, y)$$

$$x' =_{\text{df}} \frac{30}{x},$$

pak B tvoří Booleovu algebru, v níž nulou je číslo 1 a jednotkou je číslo 30. Hasseův diagram této algebry je na obr. 18b.

Právě uvedený příklad lze zobecnit. Pro výchozí číslo 30 platilo: $30 = 2 \,.\, 3 \,.\, 5$. Booleovu algebru totiž obdržíme, právě když úplný rozklad (tj. rozklad v součin prvočísel) výchozího čísla n obsahuje každé prvočíslo nejvýše jednou. Booleovy algebry tak dostaneme např. u těchto výchozích čísel: 2, 3, 7 (dvouprvkové algebry), $10 = 2 \,.\, 5$, $21 = 3 \,.\, 7$ (čtyřprvkové algebry), $30 = 2 \,.\, 3 \,.\, 5$, $42 = 2 \,.\, 3 \,.\, 7$ (osmiprvkové algebry), $210 = 2 \,.\, 3 \,.\, 5 \,.\, 7$ (šestnáctiprvková algebra). Operace komplement je v těchto algebrách pro výchozí číslo n definovaná formulí $x' = \dfrac{n}{x}$.

Svazy, které nejsou Booleovými algebrami, obdržíme např. pro čísla $12 = 2^2 . 3$ (viz obr. 53a) nebo $36 = 2^2 . 3^2$ (viz obr. 53b). Tyto svazy jsou sice distributivní, mají nulu a jednotku (jako každý konečný svaz), nejsou však komplementární.



Obr. 53

Příklad 8.5. Nechť dvojice $(M, \leq)$ je řetězec, kde $M \neq \emptyset$, pak uvažujme v množině M všechny následující druhy intervalů: polouzavřené intervaly $[a, b)$, koncové intervaly příslušné k prvku a $[a, \rightarrow)$, otevřené počáteční intervaly příslušné k prvku a $(\leftarrow, a)$ a ještě celou množinu M. Nechť B je množina všech konečných sjednocení výše uvedených množin, pak $(B, \cap, \cup, ')$ je Booleova algebra. Algebra B se nazývá **intervalová algebra řetězce** M. Pokud např. vyjdeme z řetězce racionálních čísel $(\mathbf{Q}, \leqq)$, pak obdržíme nekonečnou (ale spočetnou) intervalovou Booleovu algebru.

Příklad 8.6. V příkladu 2.13 jsme definovali pojem obojetná množina topologického prostoru M. Tam jsme také uvedli, že množina S^* všech obojetných množin topologického prostoru M tvoří svaz. Nyní můžeme dodat, že čtveřice $(S^*, \cap, \cup, ')$ je dokonce Booleova algebra, v níž je množina $\emptyset$ nula a množina M jednotka. Tato Booleova algebra se nazývá **algebra obojetných množin** topologického prostoru M. Tři konečné případy těchto algeber jsou znázorněny na obr. 20c.

Topologický prostor M se nazývá **souvislý,** právě když má právě dvě obojetné množiny, tj. množinu $\emptyset$ a množinu M. Algebra obojetných množin je v tomto případě dvouprvková (viz př. 8.3). Příkladem souvislého topologického prostoru je euklidovský prostor E_n dimenze n (se standardní topologií).

Z nesouvislých topologických prostorů uveďme ty, jejichž libovolné dva různé body lze oddělit obojetnou množinou. Topologické prostory s touto vlastností se nazývají **totálně nesouvislé.** Jednoduchým příkladem totálně nesouvislého prostoru M je **diskrétní topologický prostor,** tj. prostor, jehož množina S otevřených množin je rovna $P(M)$. Jiným příkladem totálně nesouvislého topologického prostoru je tzv. **Cantorovo diskontinuum,** které popíšeme následovně.

Vyjdeme z intervalu $\langle 0, 1 \rangle$ v řetězci $(\mathbf{R}, \leqq)$, z něhož vynecháme nekonečný spočetný systém otevřených intervalů pomocí této konstrukce: V prvním kroku vynecháme interval $\left(\frac{1}{3}, \frac{2}{3}\right)$. V druhém kroku vynecháme z každého ze zbylých intervalů $\left\langle 0, \frac{1}{3}\right\rangle$ a $\left\langle \frac{2}{3}, 1\right\rangle$ jeho „střední třetinu", tj. vynecháme intervaly $\left(\frac{1}{3^2}, \frac{2}{3^2}\right)$, $\left(\frac{7}{3^2}, \frac{8}{3^2}\right)$. Ve třetím kroku vynecháme zase z každého ze zbývajících čtyř intervalů jeho „střední třetinu" atd.

8.2 Základní vlastnosti Booleových algeber

Prohlédneme-li si seznam základních axiómů kladených na Booleovy algebry, pak zjistíme, že od každé z operací průsek a spojení požadujeme analogické vlastnosti. Proto platí následující metavěta představující **princip duality** i v Booleových algebrách:

Každý pravdivý výrok o Booleových algebrách, v jehož formulaci se vyskytují pouze specifické symboly $\sqcap$, $\sqcup$, $'$, 0 a 1, zůstane pravdivý, pokud symboly $\sqcap$, $\sqcup$, 0, 1 nahradíme po řadě symboly $\sqcup$, $\sqcap$, 1, 0.

Poznamenejme, že v dalším textu někdy spojíme navzájem duální formule pomocí spojky $\wedge$ do jedné formule. Obdržíme tak formuli, která je autoduální a kterou budeme značit bez čárky.

Nyní se budeme zabývat některými důležitými vlastnostmi, které mají Booleovy algebry a které nejsou vysloveny v definici 8.1. Jednu takovou vlastnost už udávala věta 8.1. V první řadě však zopakujme, že jak asociativní zákony, tak i distributivní zákony lze zobecnit pro libovolný konečný počet prvků uvažované Booleovy algebry B. Na základě zobecněného asociativního zákona pro $\sqcap$ i pro $\sqcup$ můžeme bez dvojznačnosti zapisovat symboly

$$\bigsqcap_{i=1}^{n} x_i \quad \text{a} \quad \bigsqcup_{i=1}^{n} x_i\,,$$

nebo

$$\bigsqcap A \quad \text{a} \quad \bigsqcup A,$$

kde A je konečná podmnožina uvažované Booleovy algebry. Zobecněné distributivní zákony můžeme vyjádřit následujícími formulemi (bez uvedení obecných kvantifikátorů):

$$x \sqcap \bigsqcup_{i=1}^{n} x_i = \bigsqcup_{i=1}^{n} (x \sqcap x_i) \tag{8.10}$$

$$x \sqcup \bigsqcap_{i=1}^{n} x_i = \bigsqcap_{i=1}^{n} (x \sqcup x_i) \tag{8.10'}$$

$$\bigsqcup_{i=1}^{n} x_i \sqcap \bigsqcup_{j=1}^{m} y_j = \bigsqcup_{[i,j] \in n \times m} (x_i \sqcap y_j) \tag{8.11}$$

$$\bigsqcap_{i=1}^{n} x_i \sqcup \bigsqcap_{j=1}^{m} y_j = \bigsqcap_{[i,j] \in n \times m} (x_i \sqcup y_j) \tag{8.11'}$$

Formuli (8.11), popř. (8.11′) lze ještě zobecnit pro libovolný počet spojení, popř. průseků.

Věta 8.2. *Nechť B je Booleova algebra, pak platí:*

$$(\forall x \in B)\,(x')' = x \tag{8.12}$$

Důkaz. Nechť x je libovolný prvek Booleovy algebry B a x' je jeho komplement. Pro tyto prvky proto platí formule (8.7). Protože operace $\sqcap$ a $\sqcup$ jsou komutativní, je také prvek x komplementem prvku x', což právě udává formule (8.12).

Věta 8.3 a 8.3′. *Nechť B je Booleova algebra, pak platí de Morganova pravidla:*

$$(\forall x, y \in B)\,(x \sqcap y)' = x' \sqcup y' \tag{8.13}$$

$$(\forall x, y \in B)\,(x \sqcup y)' = x' \sqcap y' \tag{8.13′}$$

Důkaz. Věty 8.3 a 8.3′ jsou důsledkem vět 7.5 a 7.5′. Protože Booleova algebra je distributivní svaz a ke každému prvku existuje komplement, platí formule (7.4) pro libovolnou dvojici prvků x, y, což právě udávají de Morganova pravidla.

Poznámka. Platnost formulí (8.13) a (8.13′) můžeme dokázat také tak, že „spočítáme“ levé strany následujících rovností a obdržíme tak jejich pravé strany. Tím však pouze zopakujeme důkaz věty 7.4: Nechť x, y jsou libovolné prvky z B, pak:

$$(x \sqcap y) \sqcap (x' \sqcup y') = 0 \qquad (x \sqcup y) \sqcap (x' \sqcap y') = 0$$

$$(x \sqcap y) \sqcup (x' \sqcup y') = 1 \qquad (x \sqcup y) \sqcup (x' \sqcap y') = 1$$

De Morganova pravidla lze zobecnit pro libovolný konečný počet prvků Booleovy algebry B, což lze zapsat takto (bez uvedení obecných kvantifikátorů):

$$\left(\textstyle\bigsqcap_{i=1}^{n} x_i\right)' = \textstyle\bigsqcup_{i=1}^{n} x_i' \qquad \left(\textstyle\bigsqcup_{i=1}^{n} x_i\right)' = \textstyle\bigsqcap_{i=1}^{n} x_i' \tag{8.14}$$

Dále lze na základě formulí (8.12), (8.13) a (8.13′) dokázat:

$$(\forall x, y \in B)\; x \sqcap y = (x' \sqcup y')' \tag{8.15}$$

$$(\forall x, y \in B)\; x \sqcup y = (x' \sqcap y')' \tag{8.15′}$$

Tyto formule ukazují, že každou z operací $\sqcap$ a $\sqcup$ lze zavést pomocí komplementu a druhé z nich.

Důsledkem vět 8.2, 8.3 a 8.3′ je následující pravidlo pro určení komplementu k libovolnému termu.

Pravidlo. Nechť τ je libovolný term (jazyka Booleovy algebry B). Tento term nejprve pomocí de Morganových pravidel upravíme tak, aby neobsahoval „očárkované závorky“. Potom stačí vzájemně zaměnit symboly $\sqcap$ a $\sqcup$ a k neočárkovaným proměnným připojit čárky a od očárkovaných proměnných je odebrat. Tím obdržíme term τ'.

Příklad. Určeme komplement k termu $x \sqcup (x' \sqcup y \sqcup z)' \sqcup z$. Nejprve pomocí de Morganova pravidla (8.14) dostaneme $x \sqcup (x \sqcap y' \sqcap z') \sqcup z$.

Předepsanou záměnou symbolů obdržíme term $x' \sqcap (x' \sqcup y \sqcup z) \sqcap z'$, který je komplementem původně zadaného termu.

Důkaz pravidla. Indukcí podle počtu n písmen obsažených v daném termu τ.

a) $n = 1$. V tomto případě $\tau = x$ nebo $\tau = x'$. Pak ale $\tau' = x'$ nebo $\tau' = (x')' = x$.

b) Nechť $n > 1$. Protože je odstraněno „očárkování závorek“, můžeme term τ zapsat takto: $\tau = \tau_1 \sqcap \tau_2$ nebo $\tau = \tau_1 \sqcup \tau_2$. Pro komplement τ' pak platí $\tau' = \tau_1' \sqcup \tau_2'$ nebo $\tau' = \tau_1' \sqcap \tau_2'$. Termy τ_1 a τ_2 však už mají nejvýše n písmen, a proto pro ně platí indukční předpoklad. Tím je pravidlo dokázáno.

Věta 8.4 a 8.4′. *Nechť B je Booleova algebra, pak platí:*

$$(\forall x, y \in B)\, x \sqcap y = x \sqcap (x' \sqcup y) \tag{8.16}$$

$$(\forall x, y \in B)\, x \sqcup y = x \sqcup (x' \sqcap y) \tag{8.16′}$$

Důkaz. Dokážeme pouze formuli (8.16). Nechť x, y jsou libovolné prvky z B, pak:

$x \sqcap (x' \sqcup y) = (x \sqcap x') \sqcup (x \sqcap y) =$	Podle (8.5).
$= 0 \sqcup (x \sqcap y) = x \sqcap y$	Podle (8.7), (8.1′) a (8.6).

Věta 8.5 a 8.5′. *Nechť B je Booleova algebra, pak platí*

$$(\forall x, y \in B)\, x = y \Leftrightarrow (x \sqcup y') \sqcap (x' \sqcup y) = 1 \tag{8.17}$$

$$(\forall x, y \in B)\, x = y \Leftrightarrow (x \sqcap y') \sqcup (x' \sqcap y) = 0 \tag{8.17′}$$

Důkaz. Dokážeme pouze formuli (8.17). Nechť x, y jsou libovolné prvky z B, pro něž platí:

I. 1. $x = y$	Předpoklad
2. $y' = x'$	$'$ je operace na ř. 1.
3. $x \sqcup y' = x' \sqcup y = 1$	$\sqcup$ je operace na ř. 1, 2; podle (8.1′) a (8.7).
$(x \sqcup y') \sqcap (x' \sqcup y) = 1$	Podle (8.3) na ř. 3.
II. 1. $(x \sqcup y') \sqcap (x' \sqcup y) = 1$	Předpoklad
2. $x \sqcup y' = 1$	Podle cv. 3.3.
3. $(x \sqcup y') \sqcap y = 1 \sqcap y = y$	$\sqcap$ je operace na ř. 2, podle (8.1) a (8.6′).
4. $(x \sqcup y') \sqcap y = x \sqcap y$	Podle (8.16), (8.1) a (8.1′).
5. $x \sqcap y = y$	Z ř. 3 a 4.
6. $x \sqcap y = x$	Obdobně jako ř. 5.
$x = y$	Z ř. 5 a 6.

Nyní se budeme zabývat uspořádáním v Booleových algebrách. Zjistili jsme, že ve svazech je možné zavést uspořádání $\trianglelefteq$ pomocí některé z následujících formulí (x, y jsou libovolné prvky z B):

$$x \trianglelefteq y \Leftrightarrow x \sqcap y = x \qquad \text{nebo} \qquad x \trianglelefteq y \Leftrightarrow x \sqcup y = y \tag{8.18}$$

Tuto možnost máme samozřejmě i v Booleových algebrách. V Booleových algebrách jako speciálních svazech však máme ještě další možnosti, jak ukáže následující věta.

Věta 8.6. *Nechť B je Booleova algebra, pak následující formule jsou ekvivalentní (pro libovolné $x, y \in B$):*

$$x \sqcap y = x \tag{8.19}$$

$$x \sqcup y = y \tag{8.20}$$

$$x \sqcap y' = 0 \tag{8.21}$$

$$x' \sqcup y = 1 \tag{8.22}$$

Důkaz. Ekvivalenci formulí (8.19) a (8.20) jsme dokázali ve větách 2.6 a 2.6′. Nyní dokážeme, že a) z formule (8.20) vyplývá formule (8.22), b) z formule (8.22) vyplývá formule (8.21), c) z formule (8.21) vyplývá formule (8.19). Tím se implikační cyklus uzavře.

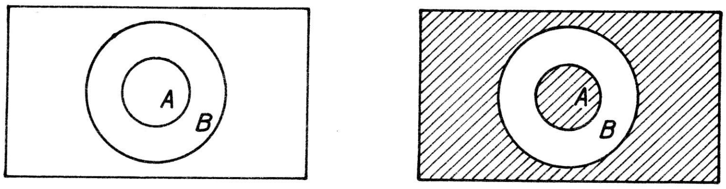
a) $x' \sqcup y = x' \sqcup (x \sqcup y) =$	Podle (8.20).
$= (x' \sqcup x) \sqcup y = 1 \sqcup y =$	Podle (8.2′) a (8.7).
$= 1$	Podle (8.1′) a (8.6′).
b) $x \sqcap y' = (x \sqcap y')'' =$	Podle (8.12).
$= (x' \sqcup y)' = 1' =$	Podle (8.13), (8.12) a (8.22).
$= 0$	Podle věty 7.1.
c) $x \sqcap y = (x \sqcap y) \sqcup 0 =$	Podle (8.6).
$= (x \sqcap y) \sqcup (x \sqcap y') =$	Podle (8.21).
$= x \sqcap (y \sqcup y') = x \sqcap 1 =$	Podle (8.5) a (8.7).
$= x$	Podle (8.6′).

Důsledek věty 8.6. *Nechť B je Booleova algebra, pak platí:*

$$(\forall x, y \in B)\, x \trianglelefteq y \Leftrightarrow x' \sqcup y = 1 \tag{8.23}$$

$$(\forall x, y \in B)\, x \trianglelefteq y \Leftrightarrow x \sqcap y' = 0 \tag{8.24}$$

Uvažujme těleso množin $P(M)$ (viz př. 8.1) a znázorněme např. formuli (8.24) pomocí Vennových diagramů. Situace pak bude velmi názorná. Nechť A, B jsou libovolné podmnožiny množiny M. Na obr. 54 a je vyznačena levá strana ekvivalence (8.24), na obr. 54b její pravá strana. Šrafováním označujeme množiny, jejichž průnik máme sestrojit. Je zřejmé, že jejich průnikem je množina prázdná, tj. nula v $P(M)$.



a) b)

Obr. 54

Věta 8.7. *Nechť B je Booleova algebra, pak platí:*

$$(\forall x, y \in B)\, x \trianglelefteq y \Leftrightarrow y' \trianglelefteq x' \tag{8.25}$$

Důkaz. Nechť x, y jsou libovolné prvky Booleovy algebry B, pro něž platí:

1. $x \trianglelefteq y$	Předpoklad
2. $y = x \sqcup y$	Podle (8.18).
3. $y' = (x \sqcup y)' = x' \sqcap y'$	Podle V 8.1 a (8.13′).
$y' \trianglelefteq x'$	Podle (8.18).

Důkaz obrácené implikace je analogický a přenecháme ho proto čtenáři.

Je vidět, že zobrazení F: $x \in B \mapsto x' \in B$ je prosté zobrazení algebry B na sebe, které obrací uspořádání (je antitonní). Dále na základě de Morganových pravidel (8.13) a (8.13′) víme, že vzájemně zaměňuje operace $\sqcap$ a $\sqcup$.

Z definice komplementu 7.1 vyplývá, že v libovolné Booleově algebře B jsou každé dva komplementární prvky navzájem disjunktní. Navíc platí, že k libovolnému prvku $a \in B$ je jeho komplement a' největší z prvků, které jsou disjunktní s a (viz poznámka na str. 140). Všechny ostatní prvky disjunktní s prvkem a proto předcházejí před prvkem a' a dokonce vyplní celý interval $[0, a']$. To je také obsahem následující věty.

Věta 8.8. *Nechť B je Booleova algebra, pak*

$$(\forall a \in B)(\forall x \in B)\, a \sqcap x = 0 \Leftrightarrow x \trianglelefteq a'.$$

Větou 8.8 jsme prozatím zakončili výčet důležitých vlastností Booleových algeber. V následujícím příkladě si procvičíme některé z těchto vlastností pomocí řešení booleovské rovnice.

Příklad 8.7. V Booleově algebře B řešte následující rovnici, v níž je x neznámá:

$$a \sqcap x = b$$

Zdůvodňování jednotlivých kroků řešení přenecháme čtenáři. Pouze poznamenejme, že vedle vět vyslovených v této kapitole použijeme např. i formuli ze cv. 3.3.

$$[(a \sqcap x) \sqcap b'] \sqcup [(a \sqcap x)' \sqcap b] = 0$$
$$[(a \sqcap b') \sqcap x] \sqcup [(a' \sqcup x') \sqcap b = 0$$
$$[(a \sqcap b') \sqcap x] \sqcup (a' \sqcap b) \sqcup (b \sqcap x') = 0$$
$$(a \sqcap b') \sqcap x = 0 \wedge a' \sqcap b = 0 \wedge b \sqcap x' = 0$$
$$x \trianglelefteq (a \sqcap b')' \wedge b \trianglelefteq a \wedge b \trianglelefteq x$$
$$x \trianglelefteq a' \sqcup b \wedge b \trianglelefteq a \wedge b \trianglelefteq x$$

Protože formule $b \trianglelefteq a' \sqcup b$ platí pro libovolné $a, b \in B$, představuje jedinou podmínku řešitelnosti zadané rovnice formule $b \trianglelefteq a$. V tom případě je množinou všech řešení interval $[b, a' \sqcup b]$. Pokud $\neg(b \trianglelefteq a)$ (tzn. $a \lhd b \vee a \between b$), pak množinou řešení je množina $\emptyset$.

V kapitole 3 jsme zavedli pojem úplný svaz. Tím máme zaveden i pojem úplné Booleovy algebry. Přesto vyslovme definici.

Definice 8.2. Booleova algebra *B se nazývá* **úplná,** *právě když pro libovolnou množinu $A \subseteq B$ existuje $\bigsqcap A$ i $\bigsqcup A$.*

Algebra B je tedy úplná, právě když je možné vedle operací $\sqcap$ a $\sqcup$ definovat i jejich zobecnění, tj. operace $\bigsqcap$ a $\bigsqcup$. Definičním oborem zobecněného průseku a zobecněného spojení je množina $P(B)$. V následujícím příkladě ukážeme, že existují úplné i neúplné Booleovy algebry.

Příklad 8.8. Každá konečná Booleova algebra je úplná. Také libovolná algebra $P(M)$ (viz př. 8.1) je úplná. Její úplností jsme se zabývali v příkladu 3.1.

Uvažujme následující těleso množin: Množina B obsahuje všechny konečné podmnožiny množiny $\mathbf{N}$ a dále všechny jejich (nekonečné) komplementy v $\mathbf{N}$. Množina B tvoří Booleovu algebru (viz lemma 8.1), která však není úplná, protože např. neexistuje spojení prvků množiny A, kde $A = \{\{3\}, \{3, 6\}, \{3, 6, 9\}, \ldots\}$.

Příklad 8.9. Nechť M je topologický prostor a nechť množina $X \subseteq M$, pak **uzávěrem množiny** X, který značíme $\mathrm{cl}\,(X)$, je nejmenší uzavřená nadmnožina množiny X a **vnitřkem množiny** X, který značíme $\mathrm{int}\,(X)$, je největší otevřená podmnožina množiny X. Pro libovolnou množinu $X \subseteq M$ položme $\mathrm{r}\,(X) = \mathrm{int\,cl}\,(X)$. Množina $r\,(X)$ se nazývá **regularizace** množiny X. Říkáme, že X je **regulární otevřená množina,** právě když $\mathrm{r}\,(X) = X$.

Uvažujme neprázdný topologický prostor M. Nechť R značí množinu všech regulárních otevřených množin, pak R je Booleova algebra vzhledem k operacím (X, Y jsou libovolné množiny z R):

$$X \sqcap Y = X \cap Y \qquad X \sqcup Y = \mathrm{r}\,(X \cup Y) \qquad A' = \mathrm{int}\,(M - A)$$

Nula a jednotka této algebry jsou množiny $\emptyset$ a M. Algebra R je navíc úplná a pro její zobecněné operace platí (S je libovolná podmnožina R):

$$\bigsqcap S = \mathrm{r}\left(\bigcap S\right) \qquad \bigsqcup S = \mathrm{r}\left(\bigcup S\right)$$

Uvedený druh algeber je důležitý především proto, že pomocí něho lze reprezentovat libovolnou úplnou algebru.

Poznámka. Ukažme, že každý poset jednoznačně určuje nějakou úplnou Booleovu algebru. Idea uvedené konstrukce je následující: Nechť $(P, \preceq)$ je neprázdný poset. Sestrojíme množinu $D(P)$ všech dolních množin tohoto posetu. Platí, že sjednocení i průnik libovolného systému dolních podmnožin z $D(P)$ je opět dolní podmnožina z $D(P)$. Proto můžeme říci, že systém všech dolních podmnožin je topologie otevřených množin na množině P. Nazývá se topologie dolních podmnožin.

Sestrojíme-li množinu B všech regulárních otevřených množin prostoru P s topologií dolních množin, pak množina B tvoří úplnou Booleovu algebru. O této algebře říkáme, že je určena posetem $(P, \preceq)$.

Z předchozího vyplývá, že také k libovolné Booleově algebře lze sestrojit úplnou Booleovu algebru.

V poslední části této kapitoly ukážeme, že v Booleových algebrách můžeme pomocí základních booleovských operací $\sqcap$, $\sqcup$ a $'$ definovat další binární operace. Pomocí následujících formulí zavedeme tři dvojice navzájem duálních operací:

$$x - y =_{\mathrm{df}} x \sqcap y' \tag{8.26}$$

$$x * y =_{\mathrm{df}} x' \sqcup y \tag{8.26'}$$

$$x \oplus y =_{\mathrm{df}} (x \sqcap y') \sqcup (x' \sqcap y) = (x - y) \sqcup (y - x) \tag{8.27}$$

$$x \Leftrightarrow y =_{\mathrm{df}} (x' \sqcup y) \sqcap (x \sqcup y') = (x * y) \sqcap (y * x) \tag{8.27'}$$

$$x \uparrow y =_{\mathrm{df}} (x \sqcap y)' = x' \sqcup y' \tag{8.28}$$

$$x \downarrow y =_{\mathrm{df}} (x \sqcup y)' = x' \sqcap y' \tag{8.28'}$$

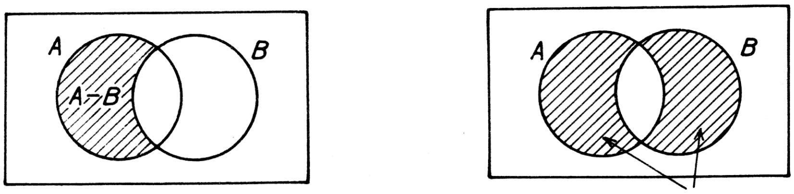
Operace $-$ a $*$ jsou navzájem duální. Operaci $-$ nazýváme **diference** a term $x - y$ čteme „x minus y". Operaci $*$, o níž jsme hovořili v článku 7.2, jsme nazývali **„relativní pseudokomplement"**.

Poznámka. Pokud bychom vyšetřovali Booleovy algebry z hlediska teorie množin (jako zobecnění pojmu těleso množin), pak je booleovské odčítání zobecněním odčítání množin (viz obr. 55a). V teorii množin se však nevyšetřuje operace, která by byla analogií booleovské operace $*$. Naproti tomu, jestliže chceme aplikovat Booleovu algebru na matematickou logiku, pak je operace $*$ velmi důležitá, protože je booleovskou analogií logické operace zvané implikace. Booleovská operace zvaná diference v tomto případě nemá použití.

Operaci $\oplus$ nazýváme **symetrická diference** nebo též **disjunktní sčítání.** Term $x \oplus y$ čteme „x minus symetricky y". Tato operace je opět booleovskou analogií symetrické diference z teorie množin (viz obr. 55b). Pro operaci $\oplus$ např. platí tato formule:

$$(\forall x, y \in B)\; x \oplus y = (x \sqcup y) \sqcap (x \sqcap y)' \tag{8.29}$$

Duální operace k operaci ⊕ je operace ⇔, která se nazývá **ekvivalence** a je skutečně booleovskou analogií logické operace zvané ekvivalence. Term „$x \Leftrightarrow y$" se čte „x je ekvivalentní s y".



a) **Obr. 55** b) $A \oplus B$

K poslední dvojici navzájem duálních operací uvedeme prozatím toto: Jedná se o univerzální operace mající tu vlastnost, že pomocí každé z nich lze definovat všech 16 možných binárních operací a všechny 4 možné unární operace v algebře **2** (viz př. 8.3). **Operace** ↑ se nazývá **Shefferova** a **operace** ↓ se nazývá **Pierceova.** Z výše uvedeného důvodu mají tyto operace mimořádnou důležitost při matematickém zpracovávání konstrukce logických obvodů (viz kapitola 12).

CVIČENÍ 8

1 Sestrojte Hasseovy diagramy Booleových algeber $P(M)$ (viz př. 8.1) pro $M = \emptyset, \{a\}, \{a, b\}, \{a, b, c\}, \{a, b, c, d\}$.

2 Sestrojte Hasseovy diagramy Booleových algeber všech dělitelů čísla n (viz př. 8.4) pro $n = 1,\ 7,\ 2 . 5,\ 2 . 3 . 5,\ 2 . 3 . 5 . 7$. Porovnejte tyto diagramy s diagramy ve cvičení 1.

3 Znázorněte věty 8.4, 8.5, 8.6 a 8.7 pomocí Vennových diagramů (v algebře $P(M)$).

4 Nechť M je topologický prostor, pak množina všech obojetných množin tohoto prostoru (tj. množina všech otevřených a současně uzavřených množin — viz př. 2.13) tvoří Booleovu algebru. Nulou této algebry je množina $\emptyset$ a jednotkou je celý prostor M. Dokažte.

5 Nechť $\mathbf{Z}$ je množina všech celých čísel a nechť $m \in \mathbf{Z}$. Množina $X \subseteq \mathbf{Z}$ se nazývá periodická s periodou m, právě když je rovna množině, kterou obdržíme tak, že ke každému jejímu prvku přičteme m. Množina všech periodických podmnožin množiny $\mathbf{Z}$ majících danou periodu m je Booleova algebra. Dokažte.

6 V Booleově algebře B řešte následující rovnice, kde x je neznámá:

a) $(a \sqcap x) \sqcup (b \sqcap x) \sqcup c = 0$

b) $a' \sqcap x = b$

c) $(a \sqcup b) \sqcap x = b' \sqcup c$

7 Dokažte, že v libovolné Booleově algebře platí formule (8.29).

8 Dokažte, že v libovolné Booleově algebře B platí (x, y jsou libovolné prvky z B):

a) $x * y = y' * x'$
b) $(x * y)' = x \sqcap y'$
c) $(x * y) * x = x$
d) $x' = (x * 0)$

9 Dokažte, že operace $\oplus$ v libovolné Booleově algebře B je asociativní.

10 Dokažte, že Shefferova ani Pierceova operace (viz formule (8.28) a (8.28′)) nejsou asociativní.

9 DALŠÍ VLASTNOSTI BOOLEOVÝCH ALGEBER

V této kapitole zavedeme nejprve binární relaci „být Booleovou podalgebrou“ v třídě všech Booleových algeber a budeme studovat nejdůležitější vlastnosti této relace. Ukážeme např., že unární relace „být Booleovou podalgebrou dané algebry B“ je uzávěrová vlastnost v množině B. V dalším článku se budeme zabývat binární operací „direktní součin“, která přiřazuje Booleovým algebrám „složitější“ Booleovy algebry. V poslední části kapitoly ukážeme, že teorie Booleových algeber je ekvivalentní s teorií určitých speciálních okruhů, kterým se říká Booleovy okruhy.

9.1 Booleovy podalgebry

Jak víme z předchozí kapitoly, je Booleova algebra B struktura se dvěma binárními operacemi $\sqcap$ a $\sqcup$, jednou unární operací $'$ a dvěma nulárními operacemi 0, 1 a můžeme ji značit $B = (B, \sqcap, \sqcup, ', 0, 1)$ nebo stručněji $B = (B, \sqcap, \sqcup, ')$. Dále víme, že podsvazem Booleovy algebry B je každý svaz $A = (A, \bar{\sqcap}, \bar{\sqcup})$, kde $A \subseteq B$ a současně operace $\bar{\sqcap}$ a $\bar{\sqcup}$ jsou zúžením operací $\sqcap$ a $\sqcup$ na množinu A. Definujme nyní relaci „být Booleovou podalgebrou“.

Definice 9.1. *Svaz s unární operací $(A, \bar{\sqcap}, \bar{\sqcup}, ^-)$ se nazývá* **Booleova podalgebra** *Booleovy algebry $(B, \sqcap, \sqcup, ')$, právě když $A \subseteq B$ a operace $\bar{\sqcap}, \bar{\sqcup}, ^-$ jsou zúžením operací $\sqcap, \sqcup, '$ na množinu A.*

Definice 9.1 se někdy vyslovuje také takto: Množina A tvoří Booleovu podalgebru Booleovy algebry $(B, \sqcap, \sqcup, ')$, právě když $A \subseteq B$ a množina A je uzavřená vzhledem k operacím $\sqcap$, $\sqcup$ a $'$.

V dalším textu budeme operace v Booleově algebře i v její podalgebře značit stejně. Navíc jsme právě užili další úmluvu: místo „Booleova podalgebra“ budeme často říkat pouze „podalgebra“.

O extrémních případech podalgeber Booleovy algebry B lze říci následující.

Lemma 9.1. *Podalgebrou každé alespoň dvouprvkové Booleovy algebry B je jednak sama algebra B a dále dvouprvková algebra $\mathbf{2} = \{0, 1\}$, kde $0, 1 \in B$.*

Definice 9.2. *Podalgebry B a **2** z lemmatu 9.1 se nazývají po řadě* **nevlastní a triviální podalgebra algebry** B.

Jestliže je A podalgebrou Booleovy algebry B, pak z uzavřenosti množiny A vzhledem k operacím $\sqcap$, $\sqcup$ a $'$ vyplývá, že si tyto operace v A ponechávají všechny vlastnosti, které jsme požadovali v definici Booleovy algebry (viz def. 8.1). Proto můžeme vyslovit:

Lemma 9.2. *Booleova podalgebra A Booleovy algebry B je Booleovou algebrou.*

Booleova algebra B obsahuje nulární operace 0, 1, a proto se zdá, že jsme i pro prvky $0, 1 \in B$ měli požadovat, aby patřili do podalgebry A. Tento požadavek je však nadbytečný, neboť lze již snadno dokázat:

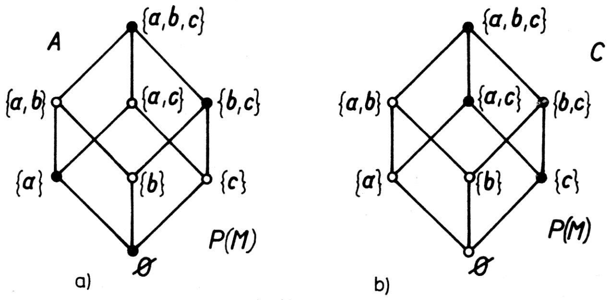
Nechť x je libovolný prvek z A, pak v A existuje i prvek x' a také prvky $x \sqcap x'$ a $x \sqcup x'$, což jsou právě prvky 0, 1. Proto můžeme vyslovit:

Lemma 9.3. *Booleova podalgebra A Booleovy algebry B obsahuje stejnou nulu a jednotku, jako má Booleova algebra B.*

Ukazuje se, že jsme v definici Booleovy podalgebry mohli vyslovit slabší požadavky, neboť na základě formulí (8.15) a (8.15′) můžeme říci.

Lemma 9.4. *Jestliže neprázdná podmnožina A Booleovy algebry $(B, \sqcup, \sqcap, ')$ je uzavřená vzhledem k unární operaci $'$ a dále vzhledem k jedné z binárních operací $\sqcap$ a $\sqcup$, pak je uzavřená i vzhledem k druhé binární operaci.*

Příklad 9.1. Nechť $M = \{a, b, c\}$, pak těleso množin $P(M)$ je Booleova algebra (viz př. 8.1). Množina $A = \{\emptyset, \{a\}, \{b, c\}, \{a, b, c\}\}$ tvoří Booleovu podalgebru algebry $P(M)$ (viz obr. 56a). Naproti tomu množina $C = \{\{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ (viz obr. 56b) sice tvoří podsvaz algebry B, netvoří však podalgebru algebry B, neboť není uzavřená vzhledem k operaci $'$. Množina C např. obsahuje množinu $\{b, c\}$, neobsahuje však její komplement v $P(M)$, tj. množinu $\{a\}$.



Obr. 56

Obecně zřejmě platí, že žádný vlastní interval $[x, y]$ Booleovy algebry B není její podalgebrou, protože není uzavřený vzhledem k operaci komplement. Interval $[x, y]$ nemůže obsahovat ani prvek x', ani prvek y'. Kdyby např. obsahoval prvek x', pak by musel obsahovat i prvky 0 a 1, a to by znamenalo, že splývá s intervalem $[0, 1]$, který však není vlastní. Interval $[0, 1] = B$ je také jediným intervalem, který je podalgebrou Booleovy algebry B.

Zdůrazněme znovu, že pokud množina A tvoří podalgebru algebry B, pak je A sama Booleovou algebrou (viz lemma 9.2). Pokud je však A Booleova algebra a platí, že A je podsvazem algebry B, pak A nemusí být podalgebrou algebry B (viz obr. 56b).

Příklad 9.2. Uvažujme Booleovu algebru $P(\mathbf{N})$, kde $\mathbf{N}$ je množina všech přirozených čísel. Do množiny A zařadíme všechny konečné podmnožiny množiny $\mathbf{N}$ a dále všechny jejich nekonečné komplementy. Množina A je vlastní podmnožinou množiny $P(\mathbf{N})$ a tvoří podalgebru Booleovy algebry $P(\mathbf{N})$. Nulou je množina $\emptyset$ a jednotkou je množina $\mathbf{N}$.

Obecně zřejmě platí, že podalgebru Booleovy algebry $P(M)$, kde M je libovolná množina, tvoří libovolná neprázdná množina $A \subseteq P(M)$, která je uzavřená vzhledem k operaci $'$ a také vzhledem k operacím $\cap$ a $\cup$ (podle lemmatu 9.4 stačí uzavřenost vzhledem k jedné z binárních operací $\cap$, $\cup$). Takovéto množiny A však nazýváme tělesa množin. Je proto dobře vidět, že pojem podalgebry Booleovy algebry B je booleovskou analogií pojmu podtěleso množinového tělesa.

Nyní se budeme zabývat problematikou generování podalgeber dané Booleovy algebry B. Jestliže podalgebra A Booleovy algebry B obsahuje nějaký prvek x, pak musí obsahovat i prvek x' a také prvky 0 a 1. Množina $\{x, x', 0, 1\}$ však již tvoří podalgebru v B, obsahující prvek x. Tato podalgebra je nejmenší podalgebrou algebry B obsahující prvek x a nazývá se **podalgebra generovaná prvkem** x.

Je zřejmé, že průnikem dvou podalgeber A_1, A_2 Booleovy algebry B je opět podalgebra Booleovy algebry B. Jestliže totiž $x, y \in A_1 \cap A_2$, pak i $x \sqcap y$, $x \sqcup y$ a x' leží v $A_1 \cap A_2$, protože tyto prvky patří do obou podalgeber A_1, A_2 algebry B. Vyslovené tvrzení lze rozšířit na libovolný neprázdný systém podalgeber algebry B.

Lemma 9.5. *Nechť B je Booleova algebra a $\{A_i\}_{i \in I}$ je libovolný neprázdný systém jejích podalgeber, pak průnik $\bigcap_{i \in I} A_i$ je také podalgebra algebry B.*

Když si dále uvědomíme, že každá algebra B je podalgebrou sebe sama, dojdeme k závěru, že vlastnost „být Booleovou podalgebrou algebry B" je uzávěrová vlastnost v množině B (viz def. 3.4). Proto platí:

Lemma 9.6. *Množina všech podalgeber dané Booleovy algebry B tvoří úplný svaz.*

Nechť B je Booleova algebra a množina $M \subseteq B$, pak také průnik systému všech podalgeber algebry B obsahujících množinu M (tento systém je neprázdný, neboť určitě obsahuje algebru B) je podalgebrou algebry B obsahující množinu M. Na základě tohoto důsledku lemmatu 9.5 můžeme vyslovit následující definici.

Definice 9.3. *Nechť M je podmnožina Booleovy algebry B, pak algebra, která je průnikem všech podalgeber algebry B obsahujících množinu M se nazývá* **podalgebra generovaná množinou** *M a značí se $[M]$. Množina M se nazývá* **množina generátorů algebry** *$[M]$.*

K definici 9.3 dodejme, že pokud je množina M prázdná, pak podalgebrou algebry B (B má alespoň dva prvky) generovanou touto množinou je algebra **2**.

Na základě definice 9.3 a lemmatu 9.6 lze říci, že podalgebra Booleovy algebry B generovaná množinou $M \subseteq B$ je nejmenší podalgebra algebry B obsahující množinu M. Tato skutečnost se znovu projeví ve znění a především v důkazu následující věty.

Věta 9.1. *Podalgebra A Booleovy algebry B generovaná neprázdnou množinou $M \subseteq B$ je množina právě všech prvků x, které lze zapsat ve tvaru*

$$x = \bigsqcup_{i=1}^{m} \bigsqcap_{j=1}^{n_i} a_{ij}, \tag{9.1}$$

kde pro každé i, j buď $a_{ij} \in M$, nebo $a'_{ij} \in M$. Duálně: do podalgebry A patří právě všechny prvky x, které lze zapsat ve tvaru

$$x = \bigsqcap_{i=1}^{m} \bigsqcup_{j=1}^{n_i} a_{ij}, \tag{9.1'}$$

kde pro každé i, j buď $a_{ij} \in M$, nebo $a'_{ij} \in M$.

Důkaz. Nechť A_1 je množina všech prvků $x \in B$, které lze zapsat ve tvaru (9.1). Je zřejmé, že každý takovýto prvek musí patřit do A, protože množina A je uzavřená vzhledem ke všem třem základním booleovským operacím. Proto stačí dokázat, že množina A_1 již tvoří podalgebru Booleovy algebry B. Spojení dvou prvků z A_1, tj. prvků tvaru (9.1), je opět prvek tvaru (9.1), a tedy prvek z A_1. Dále, jestliže $x \in A_1$, pak dokážeme, že i $x' \in A_1$. Jestliže $x \in A_1$, pak lze x zapsat ve tvaru (9.1). Na základě pravidla pro určení komplementu k danému termu (viz čl. 8.2) platí:

$$x' = \bigsqcap_{i=1}^{m} \bigsqcup_{j=1}^{n_i} a'_{ij} \tag{9.2}$$

Použitím zobecněného distributivního zákona upravíme pravou stranu (9.2) na tvar (9.1), a proto $x' \in A_1$. Na základě lemmatu 9.4 můžeme říci, že množina A_1 je uzavřená i vzhledem k operaci $\sqcup$. Množina A_1 proto tvoří podalgebru Booleovy algebry B. Duálně lze dokázat druhou část věty.

Další věta se bude zabývat počtem prvků Booleovy algebry B v případě, že množina jejích generátorů je konečná.

Věta 9.2. *Podalgebra A Booleovy algebry B generovaná množinou M mající k prvků obsahuje nejvýše* $2^{(2^k)}$ *prvků.*

Věta 9.2 mimo jiné říká, že pokud je množina generátorů M konečná, pak je konečná i Booleova algebra $[M]$. Připomeňme, že v teorii svazů takovéto tvrzení dokázat nelze, protože už tříprvková množina může generovat nekonečný svaz.

Důkaz věty 9.2. Nechť $a_1, a_2, \dots, a_k$ jsou prvky množiny M. Z věty 9.1 vyplývá, že každý prvek x podalgebry A generované množinou M lze např. podle formule (9.1) získat jako spojení konečně mnoha prvků tvaru

$$\bigsqcap_{j=1}^{k} y_j, \tag{9.3}$$

kde y_j je buď a_j, nebo a_j'. Všech posloupností tvaru $y_1, y_2, \dots, y_k$ je celkem 2^k (pro y_1 jsou dvě možnosti a_1 nebo a_1', pro y_2 jsou opět dvě možnosti atd.). Každé takové posloupnosti odpovídá nějaký prvek (9.3), tzn. že různých prvků tvaru (9.3) může být nejvýše 2^k. Uvažujme nyní množinu všech prvků tvaru (9.3). Tato množina má nejvýše 2^k prvků, a proto má nejvýše $2^{(2^k)}$ podmnožin. Každé takovéto podmnožině odpovídá určité spojení prvků tvaru (9.3), tzn. prvek tvaru (9.1). Proto můžeme říci, že všech různých prvků tvaru (9.1) je nejvýše $2^{(2^k)}$, což jsme měli dokázat.

Ukázali jsme, že vlastní interval $[a, b]$ Booleovy algebry B nikdy není Booleovou podalgebrou algebry B. Tento interval je však sám o sobě Booleova algebra. Komplement libovolného prvku $x \in [a, b]$ vzhledem k nové nule a jednotce, kterými jsou prvky a, b, označme y. Tento relativní komplement y můžeme v rámci Booleovy algebry B určovat pomocí formule

$$y = (a \sqcup x') \sqcap b.$$

Tuto skutečnost jsme však už vyslovili ve větě 7.8 a zdůvodnili v jejím důkazu.

V závěru článku ještě připomeňme, že každý distributivní svaz S s nulou a jednotkou v sobě obsahuje určitou největší Booleovu algebru B. Do algebry B zařadíme právě všechny ty prvky svazu S, k nimž existuje komplement (minimálně jsou to prvky 0 a 1). Tuto skutečnost jsme však už vyslovili ve větě 7.4 a zdůvodnili v jejím důkaze.

9.2 Direktní součin Booleových algeber

V článku 4.4 jsme zavedli binární operaci na třídě svazů, kterou jsme nazvali direktní součin svazů. Direktním součinem svazů je svaz (viz věta 4.4). Protože Booleovy algebry jsou speciální svazy, můžeme vytvářet i jejich direktní součiny. Přitom platí následující věta:

Věta 9.3. *Nechť* $A = (A, \sqcap', \sqcup', {}^{\times})$ *a* $B = (B, \overline{\sqcap}, \overline{\sqcup}, {}^{-})$ *jsou Booleovy algebry, pak direktním součinem* $A \times B$ *těchto algeber, v němž operace* $\sqcap$ *a* $\sqcup$ *zavedeme formulemi* (4.12) *a* (4.12′) *a operaci komplement zavedeme takto:*

$$[x_1, x_2]' =_{\mathrm{df}} [x_1^{\times}, \bar{x}_2], \tag{9.4}$$

je Booleova algebra.

Důkaz věty spočívá v tom, že při provádění operací s dvojicemi $[x, y] \in A \times B$ se s prvními složkami dělají booleovské operace z A a nezávisle na tom se s druhými složkami dělají booleovské operace z B. Operace zvaná direktní součin tedy dvojicím Booleových algeber přiřazuje Booleovu algebru.

Definice 9.4. *Nechť* $A = (A, \sqcap', \sqcup', {}^{\times})$ *a* $B = (B, \overline{\sqcap}, \overline{\sqcup}, {}^{-})$ *jsou Booleovy algebry, pak Booleova algebra* $A \times B$, *jejíž operace* $\sqcap$, $\sqcup$ *a* $'$ *jsou definovány po řadě formulemi* (4.12), (4.12′) *a* (9.4), *se nazývá* **direktní součin algeber** A, B.

Jestliže je potřeba zavést v direktním součinu $A \times B$ svazové uspořádání, pak to lze udělat např. pomocí formule

$$[x_1, x_2] \preceq [y_1, y_2] \Leftrightarrow_{\mathrm{df}} (x_1 \preceq_A y_1 \wedge x_2 \preceq_B y_2).$$

Protože operace direktní součin Booleových algeber je asociativní*), lze ji rozšířit na libovolný konečný, popř. i nekonečný soubor Booleových algeber.

Zobrazení

$$F\colon [x, y] \in A \times B \mapsto x \in A \tag{9.5}$$

a zobrazení

$$G\colon [x, y] \in A \times B \mapsto y \in B \tag{9.6}$$

jsou svazovými homomorfismy Booleovy algebry $A \times B$ na Booleovu algebru A, popř. B.

Příklad 9.3. V příkladu 8.1 jsme uvažovali Booleovu algebru $P(M)$, kde $M = \{a, b, c\}$. Tuto algebru lze získat jako direktní součin dvouprvkových Booleových algeber $\{\emptyset, \{a\}\}$, $\{\emptyset, \{b\}\}$ a $\{\emptyset, \{c\}\}$ (viz poznámka na str. 101).

Obecně platí, že libovolnou Booleovu algebru $P(M)$, kde $M = \{a_1, a_2, \ldots, a_n\}$, lze získat jako direktní součin algeber $\{\emptyset, \{a_1\}\}$, $\{\emptyset, \{a_2\}\}$ až $\{\emptyset, \{a_n\}\}$.

Příklad 9.4. V příkladu 8.4 jsme uvažovali Booleovu algebru B všech dělitelů čísla $30 = 2 \,.\, 3 \,.\, 5$ v množině $\mathbf{N}$. Tuto algebru lze získat jako direktní součin dvouprvkových Booleových algeber $\{1, 2\}$, $\{1, 3\}$, $\{1, 5\}$.

Obecně platí, že libovolnou Booleovu algebru B všech dělitelů čísla $n = p_1 \,.\, p_2 \,.\, \ldots \,.\, p_n$, kde p_i jsou navzájem různá prvočísla, lze získat jako direktní součin dvouprvkových Booleových algeber $\{1, p_1\}$, $\{1, p_2\}$ až $\{1, p_n\}$.

---

*) Viz poznámka pod čárou str. 97.

9.3 Booleovy okruhy

Booleovy algebry byly ve skutečnosti prvními svazy, které matematici studovali. Boole pomocí nich formalizoval výrokovou logiku. Poměrně dlouho panoval názor, že Booleovy algebry mají podstatně jiný charakter než ostatní známé algebraické struktury. Později se ukázalo, že tomu tak není. A právě tímto problémem se budeme nyní zabývat. Ukážeme, že teorie Booleových algeber je ekvivalentní s teorií určitých speciálních okruhů.

Je-li dána Booleova algebra $(B, \sqcup, \sqcap, ')$, pak ukážeme, že tuto algebru můžeme považovat za okruh vzhledem k operaci symetrická diference (v tomto kontextu by bylo příhodnější říkat disjunktní sčítání) a dále vzhledem k operaci průsek. Symetrická diference bude hrát roli okruhového sčítání a průsek roli okruhového násobení, které budeme při této příležitosti značit $\cdot$. Pro uvažované operace platí:

$$(\forall x, y \in B)\, x \oplus y = (x \sqcap y') \sqcup (x' \sqcap y) \tag{9.7}$$

$$(\forall x, y \in B)\, x \,.\, y = x \sqcap y \tag{9.8}$$

Věta 9.4. *Nechť $(B, \sqcup, \sqcap, ')$ je Booleova algebra, pak zavedeme-li v ní operace $\oplus$ a $\cdot$ formulemi (9.7) a (9.8), obdržíme okruh $(B, \oplus, \cdot)$. Okruh B má navíc tyto vlastnosti: je komutativní, má jednotkový prvek, každý prvek z B je idempotentní vzhledem k operaci $\cdot$, každý prvek z B má vzhledem k operaci $\oplus$ řád $\leqq 2$, tzn.*

$$(\forall x \in B)\, x \oplus x = 0.$$

Důkaz, že operace $\oplus$ a $\cdot$ mají okruhové i další uvedené vlastnosti, přenecháme čtenáři. Dodejme pouze, že z teorie okruhů je známo, že jestliže je každý prvek okruhu $(M, +, \cdot)$ vzhledem k operaci $\cdot$ idempotentní, pak je okruh M komutativní a každý jeho prvek má řád $\leqq 2$.

Pro okruhy, o nichž se hovoří ve větě 9.4, zavedeme následující název:

Definice 9.5. Okruh $(M, +, \cdot)$ *se nazývá* **Booleův,** *právě když každý jeho prvek je vzhledem k operaci $\cdot$ idempotentní.*

Ve větě 9.4 jsme ukázali, že ke každé Booleově algebře B lze sestrojit určitý Booleův okruh s jednotkovým prvkem. Platí však také obráceně: K libovolnému Booleovu okruhu B s jednotkovým prvkem lze sestrojit Booleovu algebru. Konstrukci uvedeme formou následující věty, jejíž důkaz necháme do cvičení.

Věta 9.5. *Nechť $(B, +, \cdot)$ je Booleův okruh s jednotkovým prvkem, pak definujeme-li v tomto okruhu operace $\sqcup$, $\sqcap$ a $'$ následujícími formulemi:*

$$(\forall x, y \in B)\, x \sqcup y = x + y - x \,.\, y$$

$$(\forall x, y \in B)\, x \sqcap y = x \,.\, y$$

$$(\forall x \in B)\, x' = 1 - x,$$

obdržíme Booleovu algebru $(B, \sqcup, \sqcap, ')$, v níž je nulový a jednotkový prvek okruhu B po řadě nulou a jednotkou.

Konstrukce, která vede od Booleovy algebry k odpovídajícímu Booleovu okruhu s jednotkovým prvkem, a konstrukce, která vede od Booleova okruhu s jednotkovým prvkem k Booleově algebře, jsou k sobě navzájem inverzní. Tím chceme říci toto: Vyjdeme-li např. od určité Booleovy algebry B, můžeme k ní sestrojit odpovídající Booleův okruh s jednotkou. Jestliže potom k tomuto okruhu sestrojíme Booleovu algebru, pak obdržíme Booleovu algebru B, z níž jsme vyšli. Nyní máme vše připraveno k vyslovení tzv. Stoneovy věty.

Věta 9.6. *Teorie Booleových algeber a teorie Booleových okruhů s jednotkovým prvkem jsou ekvivalentní.*

Článek ukončíme příkladem, v němž k zadané Booleově algebře sestrojíme odpovídající Booleův okruh.

Příklad 9.5. Uvažujme Booleovu algebru B všech dělitelů čísla 30 v $\mathbf{N}$ (viz př. 8.4). Tabulky 1, 2, 3 jsou tabulky základních Booleových operací v B.

Tab. 1

$\sqcap$	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

Tab. 2

$\sqcup$	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

Tab. 3

$'$	1	2	3	5	6	10	15	30
	30	15	10	6	5	3	2	1

Sestrojme k uvedené Booleově algebře B odpovídající Booleův okruh, tzn. zaveďme v množině B operace $\oplus$ a $\cdot$ (viz formule (9.7) a (9.8)). Tabulka pro operaci $\cdot$ bude shodná s tabulkou pro operaci $\sqcap$. Vzhledem ke konstrukci tabulky operace $\oplus$ ukážeme nejprve dva výpočty symetrických diferencí a pak vypíšeme celou tabulku 4.

$$5 \oplus 3 = (5 \sqcap 3') \sqcup (5' \sqcap 3) = (5 \sqcap 10) \sqcup (6 \sqcap 3) = 5 \sqcup 3 = 15$$

$$5 \oplus 15 = (5 \sqcap 15') \sqcup (5' \sqcap 15) = (5 \sqcap 2) \sqcup (6 \sqcap 15) = 1 \sqcup 3 = 3$$

Tab. 4

$\oplus$	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	1	6	10	3	5	30	15
3	3	6	1	15	2	30	5	10
5	5	10	15	1	30	2	3	6
6	6	3	2	30	1	15	10	5
10	10	5	30	2	15	1	6	3
15	15	30	5	3	10	6	1	2
30	30	15	10	6	5	3	2	1

Poznamenejme, že tabulka operace $\oplus$ je grupová, v níž je nulovým prvkem číslo1. Prvky 1 v celé hlavní diagonále ukazují, že každé číslo je opačné samo k sobě. Symetričnost tabulky podle hlavní diagonály představuje komutativnost operace $\oplus$. V tabulce operace $\cdot$ vidíme, že jednotkovým prvkem je číslo 30. Idempotenci libovolného prvku vzhledem k této operaci poznáme podle složení hlavní diagonály (hlavní diagonála se shoduje se záhlavím tabulky). Symetričnost tabulky podle této diagonály ukazuje, že operace $\cdot$ je komutativní. Ostatní vlastnosti Booleova okruhu $(B, +, \cdot)$ nechť si čtenář ověří na několika konkrétních případech.

CVIČENÍ 9

1 Určete všechny Booleovy podalgebry Booleovy algebry $P(M)$, kde $M = \{a\}, \{a, b\}, \{a, b, c\}, \{a, b, c, d\}$. Sestrojte Hasseův diagram svazu všech těchto podalgeber.

2 Dokažte, že Booleova podalgebra A algebry B je uzavřená vzhledem k Shefferově i vzhledem k Pierceově operaci. Totéž dokažte pro operace $-$, $*$, $\oplus$, a $\Leftrightarrow$ (viz formule (8.26) až (8.28′)).

3 Nechť A je podalgebra Booleovy algebry B a nechť prvek $a \in B$, pak podalgebra algebry B generovaná množinou $A \cup \{a\}$ je tvořena všemi prvky $x \in B$ tvaru $x = (x_1 \sqcap a) \sqcup (x_2 \sqcap a')$, kde $x_1, x_2 \in A$. Dokažte.

4 K svazu znázorněnému na obr. 47a sestrojte jeho největší Booleovu podalgebru (viz věta 7.4). Totéž udělejte pro svazy znázorněné na obr. 51.

5 Sestrojte Hasseovy diagramy Booleových algeber $P(\{a\})$ a $P(\{a, b\})$ a pomocí nich sestrojte Hasseův diagram algebry $P(\{a\}) \times P(\{a, b\})$. Pomocí Hasseova diagramu algebry $P(\{a, b\})$ sestrojte Hasseův diagram algebry $P(\{a, b\}) \times P(\{a, b\})$.

6 Dokažte věty 9.4 a 9.5.

7 K Booleovým algebrám $P(\{a\})$ a $P(\{a, b\})$ sestrojte odpovídající Booleovy okruhy.

10 BOOLEOVY HOMOMORFISMY

V této kapitole nejprve ukážeme další důležité vlastnosti ideálů a filtrů v rámci Booleových algeber. Dále budeme studovat Booleův homomorfismus, tj. homomorfismus, který zachovává všechny tři základní booleovské operace. Dodatečně se ukáže, že pojmy svazový homomorfismus a Booleův homomorfismus nad třídou Booleových algeber splývají. Důležitou vlastností Booleových algeber je existence vzájemně jednoznačného zobrazení mezi jejich kongruencemi a jejich ideály, popř. filtry. V důsledku toho lze např. homomorfní obrazy Booleových algeber studovat nejen pomocí kongruencí jako u svazů, ale také pomocí ideálů, popř. filtrů. V závěru ukážeme, že libovolnou konečnou Booleovu algebru lze reprezentovat pomocí potence nějaké množiny.

10.1 Ideály a filtry

Ideály a filtry ve svazech jsme studovali v článku 4.3. Připomeňme, že ideálem I ve svazu S rozumíme každou neprázdnou množinu $I \subseteq S$, pro niž platí:

$$(\forall x, y \in S)\, x \in I \wedge y \in I \Rightarrow x \sqcup y \in I \tag{10.1}$$

$$(\forall x, y \in S)\, x \in I \wedge y \trianglelefteq x \Rightarrow y \in I \tag{10.2}$$

Vlastní ideál I svazu S se nazývá maximální, právě když ve svazu S neexistuje žádný vlastní ideál obsahující I jako vlastní podmnožinu. Vlastní ideál I svazu S se nazývá prvoideál, právě když pro něj platí:

$$(\forall x, y \in S)\, x \sqcap y \in I \Rightarrow x \in I \vee y \in I \tag{10.3}$$

Duálními pojmy k třem výše uvedeným pojmům jsou: filtr, maximální filtr a ultrafiltr.

Ideály a filtry tvoří důležitý druh podsvazů daných svazů. Také v Booleových algebrách tvoří ideály a filtry podsvazy těchto algeber. Z předchozí kapitoly však víme, že žádný vlastní ideál nebo filtr Booleovy algebry B netvoří její podalgebru, neboť neobsahuje buď jednotku, nebo nulu algebry B.

O vztahu mezi ideály a filtry v Booleových algebrách hovoří následující lemmata, jejichž důkazy se opírají o de Morganova pravidla a o formuli (8.25).

Lemma 10.1. *Nechť I je ideál Booleovy algebry B, pak množina F všech prvků x', kde $x \in I$, tvoří filtr algebry B.*

Lemma 10.1′. *Nechť F je filtr Booleovy algebry B, pak množina I všech prvků x', kde $x \in F$, tvoří ideál algebry B.*

Každé z uvedených lemmat určuje vzájemně jednoznačné zobrazení mezi množinou všech ideálů a množinou všech filtrů dané Booleovy algebry B. Jestliže I je ideál v B, pak filtr F zkonstruovaný podle lemmatu 10.1 se nazývá **duální filtr** k I, a obdobně, jestliže F je filtr v B, pak se ideál I zkonstruovaný podle lemmatu 10.1′ nazývá **duální ideál** k F.

Příklad 10.1. Uvažujme těleso množin $P(M)$, kde $M = \{a, b, c, d\}$, pak množina $I = \{\{a, b\}, \{a\}, \{b\}, \emptyset\}$ tvoří ideál v $P(M)$. Duálním filtrem k I je množina $F = \{\{c, d\}, \{b, c, d\}, \{a, c, d\}, \{a, b, c, d\}\}$.

Uvažujme množinu I všech konečných podmnožin nekonečné množiny M. Množina I je vlastní ideál v tělese množin $P(M)$. Duálním filtrem k I je množina F všech nekonečných podmnožin množiny M, které mají konečné komplementy v M.

Přeformulujeme-li lemmata 4.6 a 4.6′ pro Booleovy algebry, obdržíme:

Lemma 10.2 (10.2′). *Každý ideál (filtr) Booleovy algebry B obsahuje nulu (jednotku) algebry B.*

V kapitole 6 jsme dokázali, že v libovolném distributivním svazu S je každý maximální ideál I prvoideálem (viz věta 6.7). Protože Booleovy algebry jsou speciální případ distributivních svazů, platí uvedená věta i v Booleových algebrách. V Booleových algebrách (na rozdíl od libovolných distributivních svazů) platí i obrácení této věty. Proveďme následující úvahu:

Nechť B je Booleova algebra a nechť I je prvoideál v algebře B, pak podle lemmatu 10.2 je $0 \in I$. Pro libovolné $x \in B$ proto musí platit $x \sqcap x' = 0 \in I$. Protože I je prvoideál (viz formule (10.3)), vyplývá z toho, že $x \in I$, nebo $x' \in I$. Oba prvky x a x' však nemohou do ideálu I patřit současně, neboť pak by ideál I podle formule (10.1) obsahoval i jejich spojení $x \sqcup x' = 1$ a ideál by nebyl vlastní. Výsledek naší prozatím nedokončené úvahy můžeme vyslovit takto:

Lemma 10.3 (10.3′). *Nechť B je Booleova algebra a I je prvoideál (F je ultrafiltr) v B, pak platí:*

$$(\forall x \in B)\, x \in I \mathbin{\overline{\vee}} x' \in I, \qquad \text{kde } \overline{\vee} \text{ značí vylučovací nebo} \tag{10.4}$$

$$((\forall x \in B)\, x \in F \mathbin{\overline{\vee}} x' \in F) \tag{10.4′}$$

Pokračujme v úvaze započaté před vyslovením lemmatu 10.3. Vyšli jsme z předpokladu, že I je prvoideál v B a chceme dojít k závěru, že I je maximální ideál v B. K tomuto tvrzení dojdeme sporem. Nechť prvoideál I není maximální v B. To znamená, že existuje vlastní ideál J v B takový, že $I \subset J$, a tedy existuje prvek $x \in B$ takový, že $x \notin I$ a $x \in J$. Protože x nepatří do I, musí do I podle (10.4) patřit jeho komplement x'. Z předpokladu $I \subset J$ vyplývá, že $x' \in J$. Protože J obsahuje jak x, tak i x', musí podle (10.1) obsahovat i $x \sqcup x' = 1$, což je spor, neboť pak by ideál J nebyl vlastní. Ideál I proto musí být maximální. Nyní můžeme vyslovit větu:

Věta 10.1. *V Booleově algebře B jsou následující dvě podmínky ekvivalentní:*
1. *Ideál I je prvoideál.*
2. *Ideál I je maximální.*

Věta 10.1′. *V Booleově algebře B jsou následující dvě podmínky ekvivalentní:*
1. *Filtr F je ultrafiltr.*
2. *Filtr F je maximální.*

Podle lemmatu 10.3 víme, že pokud je I prvoideál v algebře B, pak pro něj platí formule (10.4). Lze též dokázat (viz cv. 10.1), že z platnosti formule (10.4) pro ideál I vyplývá, že I je prvoideál. Podmínka (10.4) je proto ekvivalentní s podmínkou 1. věty 10.1 a v důsledku věty 10.1 i s podmínkou 2. této věty. Můžeme proto vyslovit:

Věta 10.2. *V Booleově algebře B je podmínka* (10.4) *ekvivalentní s každou z podmínek* 1., 2. *z věty* 10.1.

Věta 10.2′. *V Booleově algebře B je podmínka* (10.4′) *ekvivalentní s každou z podmínek* 1., 2. *z věty* 10.1′.

Z lemmatu 4.9 víme, že množina všech ideálů daného svazu S doplněná o množinu $\emptyset$ tvoří úplný svaz. To samozřejmě platí i pro Booleovy algebry. Protože však Booleovy algebry mají nulový prvek, tvoří množina všech ideálů algebry B úplný svaz i bez tohoto doplnění o množinu $\emptyset$.

Lemma 10.4. *Množina všech ideálů dané Booleovy algebry B tvoří úplný svaz, v němž je nulou množina $\{0\}$ a jednotkou množina B.*

Lemma 10.4′. *Množina všech filtrů dané Booleovy algebry B tvoří úplný svaz, v němž je nulou množina $\{1\}$ a jednotkou množina B.*

V závěru článku zdůvodníme, proč užíváme pojem ideál jak v teorii okruhů, tak i v teorii Booleových algeber. Tyto pojmy spolu totiž velmi úzce souvisí. Platí následující věta:

Věta 10.3. *Nechť I je podmnožinou Booleovy algebry B, pak I tvoří ideál v algebře B, právě když I tvoří ideál v odpovídajícím Booleově okruhu B.*

Důkaz. Nejprve dokážeme: pokud je I ideál v algebře B, pak je I ideál v odpovídajícím Booleově okruhu B (viz věta 9.4). Pro ideál I algebry B platí formule (10.1) a (10.2) a ideál I okruhu B je charakterizován formulemi (viz čl. 1.1):

$$(\forall x, y \in B)\, x \in I \wedge y \in I \Rightarrow x \oplus y \in I \tag{10.5}$$

$$(\forall x, y \in B)\, x \in I \Rightarrow x \,.\, y \in I \tag{10.6}$$

Nechť x, y jsou libovolné prvky z algebry B, pak

1. $x \in I \wedge y \in I$	Předpoklad
2. $x \sqcap y' \trianglelefteq x \wedge x' \sqcap y \trianglelefteq y$	Podle (2.13)
3. $(x \sqcap y') \sqcup (x' \sqcap y) \trianglelefteq x \sqcup y$	Podle cv. 2.15 na ř. 2.
4. $x \oplus y \trianglelefteq x \sqcup y \in I$	Podle (9.7) a (10.1)
$\quad x \oplus y \in I$	Podle (10.2) na ř. 4.

1. $x \in I \wedge y \in B$	Předpoklad
2. $x \sqcap y \trianglelefteq x$	Podle (2.13)
$\quad x \,.\, y \in I$	Podle (10.2) a (9.8) na ř. 2.

Nyní obráceně: Dokážeme, že pokud I je ideál okruhu B, pak I je ideál v odpovídající algebře B. Nechť x, y jsou libovolné prvky okruhu B, pak:

1. $x \in I \wedge y \in I$	Předpoklad
2. $(x \oplus y) \oplus (x \sqcap y) = x \sqcup y$	Podle cv. 10.2.
$\quad x \sqcup y \in I$	Podle (10.5), (9.8) a (10.6)

1. $x \in I \wedge y \trianglelefteq x$	Předpoklad
2. $x \sqcap y = y$	Podle (8.18) na ř. 1.
$\quad y \in I$	Podle (10.6) a (9.8) na ř. 2.

10.2 Booleovy homomorfismy

V kapitole 4 jsme studovali relace „být izomorfní“ a „být homomorfní“ mezi svazy. Víme již, že svaz A je homomorfním obrazem Booleovy algebry $B = (B, \sqcap, \sqcup, ')$, právě když existuje zobrazení $F\colon B \overset{\text{na}}{\to} A$, které zachovává operace $\sqcap$ a $\sqcup$. V následující definici budeme požadovat i zachování operace komplement. Dříve však než tuto definici vyslovíme, je vhodné zdůraznit, že pokud existuje zobrazení F Booleovy algebry B na svaz A a pokud zobrazení F zachovává všechny tři základní booleovské operace, pak je svaz A samozřejmě také Booleovou algebrou.

Definice 10.1. *Říkáme, že Booleova algebra* $(A, \bar{\sqcap}, \bar{\sqcup}, {}^{-})$ *je* **Booleovým homomorfním obrazem** *Booleovy algebry* $(B, \sqcap, \sqcup, ')$, *právě když existuje zobrazení*

F množiny B na množinu A, které zachovává všechny tři základní booleovské operace, tzn. když platí:

$$(\forall x, y \in B)\ F(x \sqcap y) = F(x) \sqcap F(y) \tag{10.7}$$

$$(\forall x, y \in B)\ F(x \sqcup y) = F(x) \sqcup F(y) \tag{10.7'}$$

$$(\forall x \in B)\ F(x') = \overline{F(x)} \tag{10.8}$$

Zobrazení F se nazývá **Booleovo homomorfní zobrazení** *nebo* **Booleův homomorfismus** *algebry B na algebru A. Pokud je zobrazení F prosté, nazývá se* **Booleovo izomorfní zobrazení** *nebo* **Booleův izomorfismus** *algebry B na algebru A. Algebra A se v tomto případě nazývá* **Booleův izomorfní obraz algebry** *B.*

V další části budeme operace v algebře B i v jejím Booleově homomorfním obraze značit stejně.

Následující definice ukazuje jedno vhodné rozšíření Booleova izomorfismu, s jehož analogií jsme se seznámili už při studiu svazů. Toto rozšíření využijeme především v článku 10.4.

Definice 10.2. *Nechť F je Booleův izomorfismus algebry A na algebru A', která je podalgebrou algebry B, pak říkáme, že F je* **Booleovo izomorfní vnoření** *algebry A do algebry B.*

Vraťme se však k definici 10.1. Booleova algebra obsahuje také dvě nulární operace 0, 1. Už svazový homomorfismus zachovával tyto operace, a proto i Booleův homomorfismus F tyto operace zachovává, tzn.

$$F(0) = 0 \wedge F(1) = 1. \tag{10.9}$$

Pokud bychom však chtěli provést zdůvodnění formule (10.9) pouze pro Booleovy algebry, můžeme postupovat např. takto:

Nechť F je Booleův homomorfismus algebry B na algebru A a nechť x je libovolný prvek z B a x' je jeho komplement, pak:

$$F(0) = F(x \sqcap x') = F(x) \sqcap F(x') = F(x) \sqcap F(x)' = 0$$

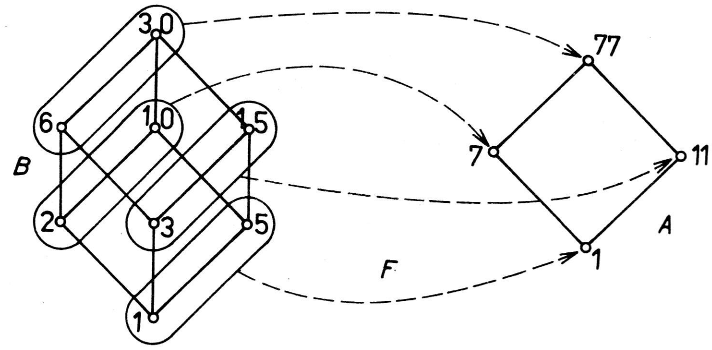
$$F(1) = F(x \sqcup x') = F(x) \sqcup F(x') = F(x) \sqcup F(x)' = 1$$

Příklad 10.2. Uvažujme Booleovu algebru B všech dělitelů čísla 30 a Booleovu algebru A všech dělitelů čísla 77 v množině $\mathbf{N}$. Hasseovy diagramy těchto algeber jsou znázorněny na obr. 57. V množině B jsou vyznačeny čtyři podmnožiny a od každé z nich vede šipka k některému prvku množiny A. Pomocí tohoto obrázku můžeme definovat Booleovo homomorfní zobrazení F algebry B na algebru A. Toto zobrazení přiřazuje každému prvku vyznačené množiny v B ten prvek z A, do něhož směřuje příslušná šipka. Tak např. $F(1) = 1$, $F(10) = 7$ a $F(6) = 77$. Ověřme alespoň na jednom příkladě platnost formulí (10.7), (10.7′) a také formule (10.8).

$$F(6 \sqcap 15) = F(3) = 11 = 77 \sqcap 11 = F(6) \sqcap F(15)$$

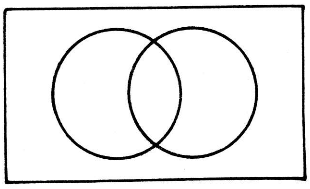
$$F(2 \sqcup 15) = F(30) = 77 = 7 \sqcup 11 = F(2) \sqcup F(15)$$

$$F(3') = F(10) = 7 = F(3)'$$



Obr. 57

Příklad 10.3. Uvažujme Vennův diagram na obr. 58. Dva kruhy vyznačené na tomto obrázku rozdělují celý obdélník (braný jako bodová množina) na čtyři části. Skládáním těchto čtyř částí lze vytvořit celkem 16 obrazců (počítáme i prázdný obrazec). Uvažujeme-li v této množině obrazců operace průnik, sjednocení a komplement, obdržíme Booleovu algebru, jejíž nulou je prázdný obrazec a jednotkou je celý obdélník. Tato algebra je izomorfním a tedy i homomorfním obrazem tělesa množin $P(\{a, b, c, d\})$. Hasseovy diagramy obou těchto algeber lze sestrojit tak, aby byly shodné.



Obr. 58

Poznamenejme, že v příkladu 9.3 jsme uváděli, že algebru $P(M)$ lze získat jako direktní součin určitých dvouprvkových řetězců. Správně bychom však měli říkat, že algebra $P(M)$ je izomorfní s uvažovaným direktním součinem. Obdobně je tomu i v příkladě 9.4.

Na základě de Morganových pravidel či speciálně na základě formulí (8.15) a (8.15′) můžeme snadno dojít k závěru, že lze v definici 10.1 požadovat méně. Platí totiž věta:

Věta 10.4. *Nechť F je zobrazení Booleovy algebry B na Booleovu algebru A, pro které platí formule* (10.8) *a jedna z formulí* (10.7), (10.7′), *pak pro zobrazení F platí i druhá z formulí* (10.7), (10.7′).

Nyní porovnáme definici svazového homomorfismu a Booleova homomorfismu s cílem zjistit, zda vůbec definice 10.1 zavedla nový pojem. Definice 4.13 se týkala libovolné dvojice svazů, a tedy i Booleových algeber, zatímco definice 10.1 se týká pouze Booleových algeber. Je zřejmé, ža každý Booleův homomorfismus algeber B a A je také jejich svazovým homomorfismem. Daleko zajímavější je problém opačný: pokud je zobrazení F svazovým homomorfismem algeber B a A, zda je také Booleovým homomorfismem těchto algeber. K nalezení odpovědi je možné použít následující větu.

Věta 10.5. *Nechť F je zobrazení Booleovy algebry B na Booleovu algebru A, pro které platí formule* (10.7) *a* (10.7′), *pak pro zobrazení F platí také formule* (10.8).

Jinak řečeno: Pokud zobrazení $F: B \overset{\text{na}}{\to} A$ zachovává průsek a spojení, a tedy také nulový a jednotkový prvek, pak zachovává i komplement.

Důkaz. Nechť zobrazení F splňuje předpoklady věty, pak dokážeme platnost formule (10.8). Nechť x je libovolný prvek z B a x' je jeho komplement, pak platí:

$$F(0) = F(x \sqcap x') = F(x) \sqcap F(x') = 0$$

$$F(1) = F(x \sqcup x') = F(x) \sqcup F(x') = 1$$

Prvek $F(x')$ splňuje podmínky komplementu prvku $F(x)$ (viz formule (8.7)), a proto pro libovolný prvek $x \in B$ platí $F(x') = F(x)'$.

Nechť F je svazový homomorfismus algebry B na algebru A, tzn. F zachovává průsek a spojení. Pak ale podle věty 10.5 zachovává homomorfismus F i komplement, a tedy F je Booleův homomorfismus algebry B na algebru A.

Na základě právě provedené úvahy se sice ukázalo, že definice 10.1 je nadbytečná, nicméně, umožnila nám alespoň dobrý vhled do problematiky. Protože je pro Booleovy algebry jedno, zda říkáme, že jsou svazově homomorfní nebo booleovsky homomorfní, budeme v dalším textu říkat pouze, že jsou homomorfní.

Podle definice 10.1 zachovává homomorfismus F mezi Booleovými algebrami všechny tři základní booleovské operace. Homomorfismus F však zachovává i všechny další operace zavedené na konci kap. 8, tzn. operace $-$, $*$, $\oplus$, $\Leftrightarrow$,

$\uparrow$ a $\downarrow$. Tyto operace lze totiž vyjádřit pomocí základních $\sqcap$, $\sqcup$ a $'$, které jsou, jak jsme již řekli, zobrazením F zachovány. Ukažme naše tvrzení na příkladě: Uvažujme homomorfismus $F: B \overset{\text{na}}{\rightarrow} A$, kde B a A jsou Booleovy algebry, pak dokážeme formuli:

$$(\forall x, y \in B)\ F(x * y) = F(x) * F(y) \tag{10.10}$$

$$F(x * y) = F(x' \sqcup y) = F(x') \sqcup F(y) = F(x)' \sqcup F(y) = F(x) * F(y)$$

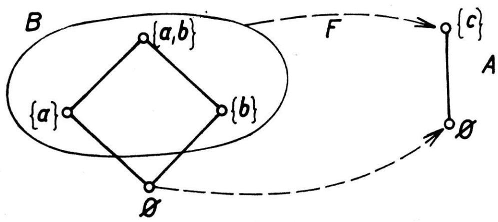
Obdobně jako u svazů, tak i u Booleových algeber zachovává homomorfismus uspořádání $\preceq$ (viz formule (4.18)). Obrácené tvrzení však u svazů neplatilo a neplatí ani u Booleových algeber, jak ukážeme na příkladě. Pokud zobrazení $F: B \overset{\text{na}}{\rightarrow} A$ zachovává uspořádání (je izotonní), pak F nemusí být homomorfismem, tzn. nemusí zachovávat základní booleovské operace.

Příklad 10.4. Uvažujme Booleovy algebry $B = P(\{a, b\})$ a $A = P(\{c\})$. Pak zobrazení $F: B \overset{\text{na}}{\rightarrow} A$, pro něž platí:

$$F(x) = \begin{cases} \emptyset & \text{pro } x = \emptyset \\ \{c\} & \text{pro } x \neq \emptyset \end{cases}$$

zachovává uspořádání (viz obr. 59), ale nezachovává např. operaci $\sqcap$, neboť

$$\begin{array}{lc} \text{v algebře } B \ \ldots\ldots\ldots & \{a\} \sqcap \{b\} = \emptyset \\ \qquad\quad \text{zobrazení } F & \downarrow \qquad \downarrow \\ \text{v algebře } A \ \ldots\ldots\ldots & \{c\} \sqcap \{c\} = \{c\}, \text{ a nikoli } \emptyset. \end{array}$$



Obr. 59

Následující věty umožňují zjistit, zda daný homomorfismus mezi Booleovými algebrami je izomorfismem či nikoli.

Věta 10.6 a 10.6′. *Homomorfismus F Booleovy algebry B na Booleovu algebru A je izomorfismem, právě když*

$$(\forall x \in B)\ F(x) = 0 \Rightarrow x = 0, \tag{10.11}$$

nebo

$$(\forall x \in B)\ F(x) = 1 \Rightarrow x = 1. \tag{10.11'}$$

Formule (10.11) a (10.11′) bychom mohli vyslovit takto: Dolní jádro homomorfismu F obsahuje právě jenom nulu a horní jádro homomorfismu F obsahuje právě jenom jednotku nebo $\square F0 = \{0\}$ a $\square F1 = \{1\}$.

Důkaz. Jestliže F je izomorfismus, pak je platnost fomule (10.11), popř. (10.11′) zřejmá, neboť F je prosté zobrazení a platí (10.9).

Obráceně: Jestliže platí např. formule (10.11′), pak dokážeme, že homomorfismus F je izomorfismem. Nechť x, y jsou libovolné prvky z B, pro něž platí $F(x) = F(y)$. Pak podle (10.10) a lemmatu 7.7 platí: $F(x * y) = F(x) * F(y) = 1$. Proto podle (10.11′) můžeme napsat $x * y = 1$, což je podle lemmatu 7.7 ekvivalentní s formulí $x \trianglelefteq y$. Obdobně lze získat formuli $y \trianglelefteq x$. Protože relace $\trianglelefteq$ je antisymetrická, platí $x = y$. To ale znamená, že F je prosté zobrazení, a tedy F je izomorfismus. Stejné tvrzení obdržíme, budeme-li předpokládat platnost formule (10.11).

10.3 Kongruence, ideály, filtry, homomorfismy

V tomto článku se nejprve budeme zabývat kongruencemi v Booleových algebrách. Ukážeme, že existuje vzájemně jednoznačný vztah mezi kongruencemi a ideály, popř. kongruencemi a filtry. Budeme definovat faktorovou algebru algebry B podle kongruence K, kterou označíme B/K, a ukážeme, že algebra B nemůže mít žádné jiné homomorfní obrazy (až na izomorfismus) než algebry B/K. Dále budeme definovat faktorovou algebru algebry B podle ideálu I, popř. filtru F, kterou označíme B/I, popř. B/F. Na rozdíl od teorie svazů je v tomto případě situace analogická jako v teorii grup.

V článku 4.6 jsme zavedli kongruence ve svazech. Nyní se budeme zabývat kongruencemi v Booleových algebrách. Kongruence, které zavedeme, jsou speciálním případem svazových kongruencí.

Definice 10.3. *Nechť B je Booleova algebra, pak ekvivalence K v B se nazývá* **Booleova kongruence** v B, *právě když*

$$(\forall x, y, z \in B)\, xKy \Rightarrow x \sqcap z\, K\, y \sqcap z, \tag{10.12}$$

$$(\forall x, y, z \in B)\, xKy \Rightarrow x \sqcup z\, K\, y \sqcup z, \tag{10.13}$$

$$(\forall x, y \in B)\, xKy \Rightarrow x'\, K\, y'. \tag{10.14}$$

Booleovu kongruenci budeme značit symbolem $\equiv$ a místo formule xKy píšeme $x \equiv y (\mathrm{mod}\ K)$, nebo pouze $x \equiv y$.

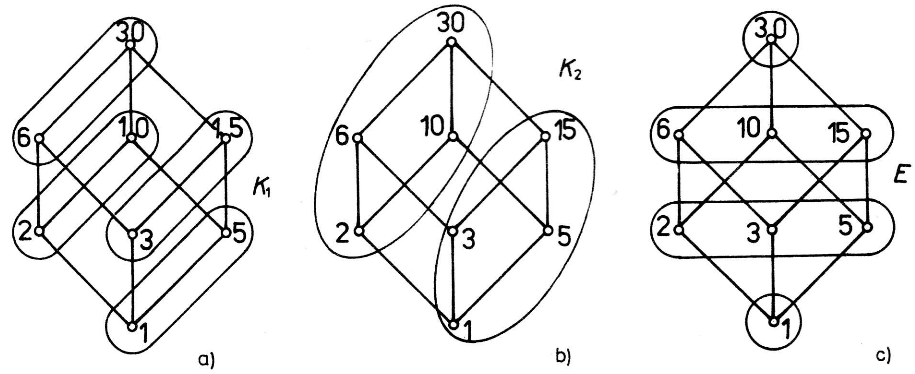
Je zřejmé, že každá Booleova kongruence v algebře B je také svazovou kongruencí. Každá Booleova kongruence v B (stejně jako svazová) je zvláštní případ ekvivalence, a proto indukuje rozklad množiny B. Protože v dalším textu budeme pojednávat výhradně o Booleových kongruencích, budeme přívlastek „Booleova“ vynechávat.

Příklad 10.5. Uvažujme Booleovu algebru B všech dělitelů čísla 30 v $\mathbf{N}$. Na obr. 60 jsou vyznačeny tři různé rozklady množiny B. Rozklady na obr. 60a, b odpovídají kongruencím. Ověřme alespoň na jednom příkladě, že pro ekvivalenci K_1 z obrázku 60a platí formule (10.14).

$$3 \equiv 15 \pmod{K_1} \Rightarrow 3' = 10 \equiv 2 = 15' \pmod{K_1}$$

Rozklad na obr. 60c neodpovídá kongruenci, neboť např.

$$3 \equiv 5 \pmod{E} \quad \text{a přitom} \quad 10 \sqcup 3 = 30 \not\equiv 10 = 10 \sqcup 5 \pmod{E}.$$



Obr. 60

Pomocí formulí (8.15) a (8.15′) lze ukázat, že jsme v definici 10.3 mohli vyslovit méně požadavků. Platí totiž věta:

Věta 10.7. *Jestliže pro ekvivalenci E v Booleově algebře B platí formule* (10.14) *a jedna z formulí* (10.12), (10.13), *pak pro ekvivalenci E platí i druhá z formulí* (10.12), (10.13).

Nyní popíšeme konstrukci nových druhů Booleových algeber.

Věta 10.8. *Nechť $(B, \sqcap, \sqcup, ')$ je Booleova algebra a K je kongruence v B, pak sestrojíme-li faktorovou množinu B/K a definujeme-li na této množině operace $\sqcap$, $\sqcup$ a $'$ takto (T_x a T_y jsou libovolné bloky z B/K obsahující prvky x, y):*

$$T_x \sqcap T_y = T_{x \sqcap y} \tag{10.15}$$

$$T_x \sqcup T_y = T_{x \sqcup y} \tag{10.15'}$$

$$T'_x = T_{x'}, \tag{10.16}$$

pak trojice $(B/K, \sqcup, \sqcap, ')$ je Booleova algebra, v níž je blok T_0 nula a blok T_1 jednotka.

Důkaz. Vzhledem k větě 4.9 stačí dokázat: a) T_0 a T_1 tvoří nulu a jednotku svazu B/K, b) definice komplementu nezávisí na volbě reprezentantů, c) formule (10.16) určuje komplement.

Nechť T_x, T_y jsou libovolné bloky z B/K, pak:

a) $T_x \sqcap T_0 = T_{x \sqcap 0} = T_0$
$T_x \sqcup T_0 = T_{x \sqcup 0} = T_x$
$T_x \sqcap T_1 = T_{x \sqcap 1} = T_x$
$T_x \sqcup T_1 = T_{x \sqcup 1} = T_1$

b) $T_x = T_y \Rightarrow x \equiv y \Rightarrow x' \equiv y' \Rightarrow T_{x'} = T_{y'} \Rightarrow T'_x = T'_y$

c) $T_x \sqcap T_{x'} = T_{x \sqcap x'} = T_0$
$T_x \sqcup T_{x'} = T_{x \sqcup x'} = T_1$

Na základě věty 10.8 můžeme vyslovit následující definici.

Definice 10.4. *Nechť B je Booleova algebra a K je kongruence v B, pak Booleova algebra sestrojená podle věty* 10.8 *se nazývá* **faktorová Booleova algebra algebry** *B podle kongruence K a značí se B/K.*

Spojíme-li větu 10.8 s tím, co víme z článku 4.6 a uvážíme-li i větu 10.5, pak můžeme stručně říci: Každá faktorová algebra B/K je homomorfním obrazem algebry B. Až na izomorfismus neexistují žádné jiné homomorfní obrazy dané Booleovy algebry B než její faktorové algebry B/K, kde K je kongruence v B. A protože dvěma různým kongruencím v B mohou odpovídat izomorfní faktorové algebry, lze říci, že homomorfních obrazů algebry B je až na izomorfismus nejvýše tolik, kolik existuje kongruencí v B.

Nyní se budeme zabývat vztahem mezi ideály (duálně filtry) a kongruencemi v Booleových algebrách. Následující věta ukáže, že ideály a kongruence si vzájemně jednoznačně odpovídají. Tato situace připomíná situaci v teorii grup, kde si také kongruence a normální podgrupy vzájemně jednoznačně odpovídají. Obecně ve svazech však takovýto vztah neplatí (viz př. 4.23).

Věta 10.9. *V Booleově algebře B existuje vzájemně jednoznačné zobrazení množiny všech ideálů v B na množinu všech kongruencí v B.*

Důkaz. Nechť I je ideál algebry B, pak dokážeme, že k němu lze sestrojit kongruenci K pomocí následující formule:

$$x \equiv y(\text{mod } K) \Leftrightarrow_{\text{df}} x \oplus y \in I \qquad (10.17)$$

Připomeňme, že $\oplus$ značí symetrickou diferenci (viz formule (8.27)). Důkaz, že relace K je ekvivalence v B, necháme do cvičení. Zde pouze dokážeme a) platnost formule (10.13)) a b) platnost formule (10.14). Na základě věty 10.7 pak můžeme říci, že platí i formule (10.12). Nechť x, y, z jsou libovolné prvky z B:

a) Předpokládejme, že $x \oplus y \in I$, pak chceme dokázat, že $(x \sqcup z) \oplus (y \sqcup z) \in I$.

$$\begin{aligned}
&(x \sqcup z) \oplus (y \sqcup z) = \\
&= [(x \sqcup z) \sqcap (y \sqcup z)'] \sqcup [(x \sqcup z)' \sqcap (y \sqcup z)] = && \text{Podle (8.27)} \\
&= [(x \sqcup z) \sqcap (y' \sqcap z')] \sqcup [(x' \sqcap z') \sqcap (y \sqcup z)] = && \text{Podle (8.13').} \\
&= (x \sqcap y' \sqcap z') \sqcup (z \sqcap y' \sqcap z') \sqcup (x' \sqcap z' \sqcap y) \sqcup \\
&\quad \sqcup (x' \sqcap z' \sqcap z) = && \text{Podle (8.5), (8.1).} \\
&= (x \sqcap y' \sqcap z') \sqcup (x' \sqcap y \sqcap z') = && \text{Podle (8.7), (8.6).} \\
&= z' \sqcap [(x \sqcap y') \sqcup (x' \sqcap y)] = && \text{Podle (8.5).} \\
&= z' \sqcap (x \oplus y) \trianglelefteq x \oplus y && \text{Podle (8.27), (2.13).}
\end{aligned}$$

Protože $(x \sqcup z) \oplus (y \sqcup z) \trianglelefteq x \oplus y \in I$, platí podle (10.2) i formule $(x \sqcup z) \oplus (y \sqcup z) \in I$.

b) Předpokládejme, že $x \oplus y \in I$, pak chceme dokázat, že $(x' \oplus y') \in I$.

$$\begin{aligned}
&x' \oplus y' = \\
&= (x' \sqcap y'') \sqcup (x'' \sqcap y') = && \text{Podle (8.27).} \\
&= (x' \sqcap y) \sqcup (x \sqcap y') = x \oplus y \in I && \text{Podle (8.12), (8.1'), (8.27) a předpokladu.}
\end{aligned}$$

Důkaz obrácené implikace. Nechť K je kongruence v algebře B, pak dokážeme, že k ní lze sestrojit vhodný ideál I. Za tento ideál prohlásíme blok rozkladu B/K obsahující nulu, tzn.

$$I = \{x \in B;\ x \equiv 0 \ (\mathrm{mod}\ K)\}.$$

Musíme však dokázat, že ideál I souvisí s kongruencí K tak, jak to předepisovala formule (10.17). Postupovat můžeme např. tak, že sestrojíme množinu M všech takových prvků $x \oplus y$, kde oba prvky x, y patří vždy do téhož bloku z B/K, a zjistíme, zda $M = I$. Nechť tedy

$$M = \{z \in B;\ (\exists x, y \in B)\ x \equiv y \ (\mathrm{mod}\ K) \wedge z = x \oplus y\}.$$

Nejprve dokážeme, že $M \subseteq I$. Nechť z je libovolný prvek z M, tzn. existují prvky $x, y \in B$ takové, že $z = x \oplus y$ a $x \equiv y \ (\mathrm{mod}\ K)$, pak:

$$\begin{aligned}
&z = x \oplus y = && \text{Předpoklad} \\
&= (x \sqcup y) \sqcap (x \sqcap y)' \equiv && \text{Podle (8.29).} \\
&\equiv (x \sqcap y) \sqcap (x \sqcap y)' = 0 && \text{Podle cv. 4.21, (8.7).}
\end{aligned}$$

Odtud vyplývá, že $z \equiv 0 \ (\mathrm{mod}\ K)$, a proto $z \in I$. Dokažme, že $I \subseteq M$. Nechť z je libovolný prvek z I, tzn. $z \equiv 0 \ (\mathrm{mod}\ K)$, pak:

$$\begin{aligned}
&z \oplus 0 = (z \sqcap 0') \sqcup (z' \sqcap 0) = && \text{Podle (8.27).} \\
&= (z \sqcap 1) \sqcup (z' \sqcap 0) = && \text{Podle V 7.1.} \\
&= z \sqcup 0 = z && \text{Podle (8.6), (8.6').}
\end{aligned}$$

Vyjdeme-li od ideálu I v B, pak po provedení obou výše uvedených konstrukcí (v patřičném pořadí) obdržíme opět ideál I. Obdobně, pokud bychom vyšli od kongruence K v B, pak po provedení obou konstrukcí obdržíme opět kongruenci K v B. Zobrazení F, které každému ideálu I v B přiřazuje odpovídající kongruenci v B (viz formule 10.17), je proto vzájemně jednoznačným zobrazením množiny všech ideálů na množinu všech kongruencí.

Věta 10.9′. *V Booleově algebře B existuje vzájemně jednoznačné zobrazení množiny všech filtrů v B na množinu všech kongruencí v B.*

Místo důkazu, který je duální k důkazu věty 10.9, pouze zopakujme obě konstrukce, které tvoří jeho základ. Jestliže je v algebře B zadán filtr F, pak odpovídající kongruenci sestrojíme pomocí následující formule:

$$(\forall x, y \in B)\; x \equiv y (\mathrm{mod}\; K) \Leftrightarrow (x \Leftrightarrow y) \in F \tag{10.17′}$$

Druhý symbol $\Leftrightarrow$ značí operaci zavedenou formulí (8.27′). Tato operace je duální k operaci $\oplus$. Jestliže je v algebře B zadána kongruence K, pak odpovídající filtr F sestrojíme takto:

$$F = \{x \in B;\, x \equiv 1 (\mathrm{mod}\; K)\}$$

Příklad 10.6. Nechť B je Booleova algebra všech dělitelů čísla 30 v $\mathbf{N}$. Uvažujme ideál $I = \{1, 5\}$. Tomuto ideálu odpovídá podle formule (10.17) kongruence K, jejíž rozklad je vyznačen na obr. 60a. Uvažujeme-li ideál $I = \{1, 3, 5, 15\}$, pak tomuto ideálu odpovídá kongruence, jejíž rozklad je znázorněn na obr. 60b.

Analogicky jako jsme se u svazů v čl. 4.6 zabývali vztahem mezi kongruencemi a homomorfními obrazy daného svazu, můžeme se nyní zabývat vztahem mezi ideály (filtry) a homomorfními obrazy dané Booleovy algebry. Dříve však připomeňme: Nechť B, A jsou Booleovy algebry, pak dolním jádrem homomorfismu $F: B \overset{\text{na}}{\rightrightarrows} A$ je idál $\square F0$ a horním jádrem je filtr $\square F1$ (pokud $0, 1 \in A$).

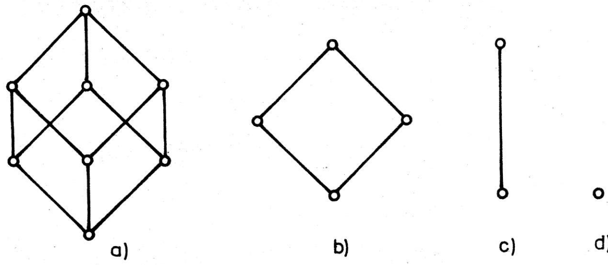
Nechť I je ideál v B, pak definujeme-li faktorovou množinu B/I předpisem $\{x \oplus I\}_{x \in B}$ a na ní operace $\sqcap$, $\sqcup$ a $'$ formulemi (10.15), (10.15′) a (10.16), obdržíme Booleovu algebru. Důkaz tohoto tvrzení přenecháme čtenáři.

Definice 10.5. *Nechť I je ideál v Booleově algebře B, pak $(B/I, \sqcap, \sqcup, ')$, kde operace $\sqcap$, $\sqcup$ a $'$ jsou definovány formulemi* (10.15), (10.15′) *a* (10.16) *se nazývá* **faktorová Booleova algebra algebry B podle ideálu** *I a značí se B/I.*

Duálně lze vyslovit definici faktorové **Booleovy algebry algebry B podle filtru** F, kterou značíme B/F.

Příklad 10.7. Uvažujme Booleovu algebru B všech dělitelů čísla 30 v $\mathbf{N}$ (viz obr. 60a). V ní existuje jeden jednoprvkový ideál $\{1\}$, tři dvouprvkové ideály $\{1, 2\}$,

$\{1, 3\}$, $\{1, 5\}$, tři čtyřprvkové ideály $\{1, 2, 3, 6\}$, $\{1, 2, 5, 10\}$, $\{1, 3, 5, 15\}$ a jeden nevlastní ideál, tj. B. Ke každému z těchto ideálů lze sestrojit faktorovou algebru B/I. Např. prvky faktorové algebry B/I, kde I je ideál $\{1, 5\}$, jsou bloky rozkladu vyznačené na obr. 60a. Je zřejmé, že pomocí výše uvedených ideálů lze sestrojit jednu osmiprvkovou faktorovou algebru, tj. $B/\{1\}$ (viz obr. 61a), dále tři čtyřprvkové faktorové algebry, tři dvouprvkové faktorové algebry a jednu jednoprvkovou faktorovou algebru, tj. B/B (viz obr. 61d). Všechny tři čtyřprvkové faktorové algebry jsou navzájem izomorfní a odpovídá jim Hasseův diagram na obr. 61b. Také všechny dvouprvkové Booleovy algebry jsou navzájem izomorfní a odpovídá jim diagram na obr. 61c.



Obr. 61

Poznámka. Připomeňme situaci u grup. Sestrojujeme-li rozklad grupy $(G, \cdot)$ podle normální podgrupy H, pak bloky tohoto rozkladu zapisujeme $a \,.\, H$, kde a je některý prvek tohoto bloku. Pro každý prvek $x \in G$ platí, že vynásobíme-li postupně prvek x zprava (popř. zleva) všemi prvky normální podgrupy H grupy G, pak obdržíme všechny prvky bloku, v němž tento prvek leží.

Praktický postup konstrukce faktorové množiny G/H pro konečnou grupu G je tento: Jeden blok rozkladu tvoří normální podgrupa H. V prvním kroku zvolíme libovolný prvek $a_1 \in G - H$ a sestrojíme $a_1 \,.\, H$. Obdržíme další blok rozkladu. Dále zvolíme $a_2 \in (G - H) - a_1 \,.\, H$ a sestrojíme $a_2 \,.\, H$. Opět obdržíme blok rozkladu atd. Po konečném počtu kroků, který je menší nebo roven počtu prvků grupy G, získáme všechny bloky rozkladu G/H.

I když u Booleových algeber nezdůrazňujeme svazové uspořádání, projeví se nám jeho existence na nejrůznějších místech. Např. právě nyní. Jestliže chceme bloky rozkladu Booleovy algebry B podle jejího ideálu I zapisovat v analogickém tvaru jako u grup, pak můžeme použít značení $a \sqcup I$, kde a je nejmenší prvek tohoto bloku. Množinu $a \sqcup I$ obdržíme jako spojení prvku a s každým z prvků ideálu I. Pokud bychom za a nevzali nejmenší prvek uvažovaného bloku, pak bychom při popsaném spojování tento nejmenší prvek nemohli dostat.

Praktický postup konstrukce faktorové množiny B/I pro konečnou algebru B je tento: Jeden blok rozkladu tvoří ideál I. V prvním kroku zvolíme libovolný minimální prvek $a_1 \in B - I$ a sestrojíme $a_1 \sqcup I$. Obdržíme blok rozkladu obsahující prvek a_1. Dále zvolíme libovolný minimální prvek $a_2 \in (B - I) - a_1 \sqcup I$ a sestrojíme $a_2 \sqcup I$. Obdržíme blok rozkladu obsahující prvek a_2, atd. Po konečném počtu kroků, který je menší nebo roven počtu prvků Booleovy algebry B, získáme všechny bloky rozkladu B/I.

O vztahu mezi Booleovou algebrou B a její faktorovou algebrou B/I hovoří následující věta, která úzce souvisí s větou 4.10.

Věta 10.10. *Nechť B je Booleova algebra a I je ideál v B, pak faktorová algebra B/I je homomorfním obrazem algebry B.*

Uveďme pouze, že homomorfismem je zobrazení (T_x značí blok rozkladu B/I obsahující prvek x):

$$F\colon x \in B \mapsto T_x \in B/I$$

Věta 10.10′. *Nechť B je Booleova algebra a F je filtr v B, pak faktorová algebra B/F je homomorfním obrazem algebry B.*

Věta 10.10 říká, že každá faktorová algebra B/I algebry B podle ideálu I je homomorfním obrazem algebry B. Následující věta, která souvisí s větou 4.11, ukáže, že až na izomorfismus žádné jiné homomorfní obrazy algebry B neexistují. Této větě se ve spojení s větou 10.10 říká základní věta o homomorfismu Booleových algeber.

Věta 10.11. *Nechť Booleova algebra A je homomorfním obrazem Booleovy algebry B, pak existuje taková faktorová algebra B/I, kde I je ideál v B, že algebra A je izomorfní s algebrou B/I.*

Podle věty 10.11 existuje ideál I v B takový, že faktorová algebra B/I je izomorfní s algebrou A. Místo důkazu se omezíme pouze na konstatování, že hledaný ideál I je dolním jádrem homomorfismu $F\colon B \overset{\text{na}}{\Rightarrow} A$, tzn. množina $\square F0$. Izomorfismem algeber B/I a A je následující zobrazení:

$$G\colon T_x \in B/I \mapsto F(x) \in A$$

Věta 10.11′. *Nechť Booleova algebra A je homomorfním obrazem Booleovy algebry B, pak existuje taková faktorová algebra B/F, kde F je filtr v B, že algebra A je izomorfní s algebrou B/F.*

Shrňme: Každá faktorová algebra B/I je homomorfním obrazem algebry B. Až na izomorfismus neexistují žádné jiné homomorfní obrazy dané Booleovy algebry B než její faktorové algebry B/I, kde I je ideál v B. A protože dvěma různým ideálům v B mohou odpovídat izomorfní faktorové algebry (viz př. 10.7), lze říci, že homomorfních obrazů algebry B je až na izomorfismus nejvýše tolik, kolik existuje ideálů v B. Duální shrnutí lze vyslovit pro filtry.

Příklad 10.7 (pokračování). V Booleově algebře B existuje celkem 8 různých ideálů. Hasseovy diagramy všech faktorových algeber B/I jsou znázorněny na obr. 61. Podle základní věty o homomorfismu Booleových algeber můžeme proto říci, že kromě algeber znázorněných na obr. 61 nemá uvažovaná algebra B žádné jiné homomorfní obrazy.

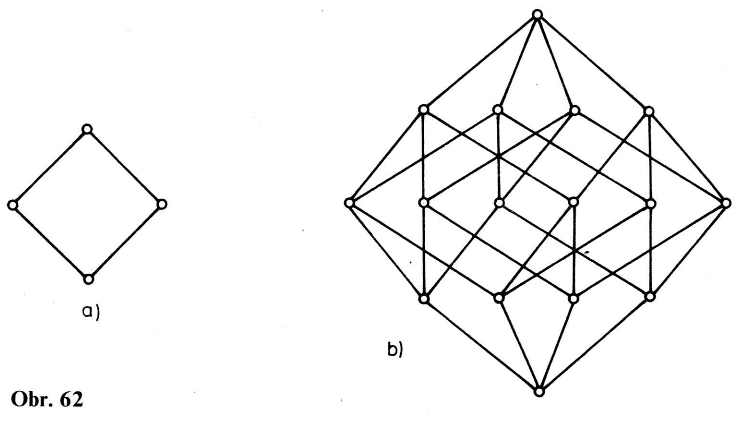
Nyní je zcela zřejmé, že studujeme-li otázku homomorfních obrazů dané Booleovy algebry B pomocí ideálů (filtrů) nebo pomocí kongruencí, pak dostáváme různými postupy stejné výsledky. Tento závěr jsme sice mohli vyslovit ihned po vyslovení definice 10.5, ale raději jsme zvolili delší postup, aby měl čtenář dostatek času vytvořit si správnou představu. Na rozdíl od teorie svazů je tedy tato problematika v Booleových algebrách zcela analogická obdobné problematice v teorii grup nebo okruhů. Víme, že studujeme-li např. v teorii grup otázku homomorfních obrazů dané grupy G, je zcela jedno, zda to děláme pomocí normálních podgrup v G nebo pomocí kongruencí v G.

10.4 Množinová reprezentace

V posledním článku této kapitoly se budeme zabývat problematikou reprezentace konečných Booleových algeber. Protože Booleovy algebry jsou speciální případ distributivních svazů, bude tento článek bezprostředně souviset s článkem 6.2, v němž jsme hovořili o reprezentaci konečných distributivních svazů. Ukážeme, že k libovolné konečné Booleově algebře B existuje potence určité množiny, která je s algebrou B izomorfní. Ještě před toto pojednání však zařadíme několik příkladů různých, ale navzájem izomorfních booleovských algeber. Všechny tyto algebry budou mít $2^{(2^n)}$ prvků, kde n je určité přirozené číslo.

Příklad 10.8. Nechť M je neprázdná množina mající 2^n prvků. Utvořme potenci $P(M)$. Tato potence má celkem $2^{(2^n)}$ prvků. Booleovské operace průsek, spojení a komplement jsou realizovány po řadě množinovými operacemi průnik, sjednocení a komplement. Uspořádání množiny $P(M)$ je dáno relací „být podmnožinou“. Nulou je množina prázdná, jednotkou je množina M. Booleova algebra $P(M)$ je těleso množin, v němž je atomem, tj. horním sousedem nuly, každá jednoprvková množina $\{x\}$, kde $x \in M$. Algebra $P(M)$ má celkem 2^n atomů.

Pro $n = 1$ a $n = 2$ obdržíme algebry mající 4 a 16 prvků. Hasseovy diagramy těchto algeber jsou na obr. 62a, b.



Obr. 62

Příklad 10.9. Nechť $2, 3, 5, 7, \ldots, p$ je prvních 2^n prvočísel. Sestrojíme číslo m, které je jejich součinem, tzn. $m = 2 \,.\, 3 \,.\, 5 \,.\, 7 \,.\, \ldots \,.\, p$. Utvořme množinu K všech dělitelů čísla m v $\mathbf{N}$, tzn. $K = \{x \in \mathbf{N};\ x \mid m\}$. Booleovské operace průsek a spojení jsou realizovány po řadě operacemi „největší společný dělitel“ a „nejmenší společný násobek“. Booleovským komplementem čísla $x \in K$ je číslo $\dfrac{m}{x}$. Uspořádání množiny K je dáno relací „dělit“. Nulou algebry je číslo 1, jednotkou je číslo m. Atomem je každé z prvočísel $2, 3, 5, 7, \ldots, p$. Tato algebra má opět 2^n atomů.

Pro $n = 1$ a $n = 2$ obdržíme algebry mající 4 a 16 prvků. Hasseovy diagramy těchto algeber jsou opět na obr. 62.

Příklad 10.10. Nejprve zavedeme Booleovy algebry, o nichž jsme prozatím nehovořili, a pak je dáme do souvislosti s ostatními příklady.

Uvažujme množinu K všech vrcholů n-dimenzionální krychle v euklidovském prostoru E_n dimenze n. Ukažme, jak vytvoříme grafické znázornění množiny K, čímž zároveň obdržíme Hasseův diagram níže uvedené algebry. Nechť je dán systém n orientovaných os prostoru dimenze n. V jednotkových bodech těchto os umístíme určité vrcholy krychle (souřadnice bodu na i-té ose bude tvořit uspořádaná n-tice mající pouze na i-tém místě číslo 1 a na všech ostatních místech číslo 0). Tyto vrcholy či jejich souřadnice budou tvořit atomy algebry K. Z množiny A všech těchto atomů vytvoříme potenci $P(A)$. Každou množinu $X \subseteq P(A)$ nahradíme jednou uspořádanou n-ticí, v níž je na i-tém místě číslo 1, právě když v některé n-tici z X je na témže místě číslo 1. Na ostatních místech budou nuly. Např. pro $n = 4$ a $X = \{(1, 0, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$ obdržíme uspořádanou čtveřici $(1, 0, 1, 1)$, která zastupuje množinu X a která navíc představuje souřadnice jednoho z vrcholů čtyřdimenzionální krychle. Uvedeným postupem získáme souřadnice všech vrcholů krychle o hraně 1 (pro prázdnou množinu $\emptyset \subseteq A$ obdržíme n-tici $(0, 0, \ldots, 0)$). Načrtnutím hran spojujících sousední vrcholy získáme Hasseův diagram algebry K. Nulou algebry K je vrchol o souřadnicích $(0, 0, \ldots, 0)$, jednotkou je vrchol o souřadnicích $(1, 1, \ldots, 1)$.

Je zřejmé, jak se v uvedeném grafickém znázornění sestrojuje průsek a spojení vrcholů krychle. Komplementem vrcholu X je protilehlý vrchol krychle, tj. vrchol, který leží na spojnici vrcholu X se středem krychle. Pro $n = 3$ obdržíme trojrozměrnou krychli (viz obr. 61a), pro $n = 4$ obdržíme čtyřrozměrnou krychli (viz obr. 62b), pro $n = 2$ obdržíme dvojrozměrnou krychli (viz obr. 62a).

Zařaďme právě uvedený druh Booleových algeber do našeho souboru příkladů: Sestrojme množinu K vrcholů 2^n-dimenzionální krychle. Množina K má $2^{(2^n)}$ prvků. Atomem je každý vrchol mající právě jednu souřadnici 1. Algebra K má proto 2^n atomů. Pro $n = 1$ a $n = 2$ obdržíme algebry mající 4 a 16 prvků. Hasseovy diagramy těchto algeber jsou na obr. 62.

Příklad 10.11. Nechť je dáno n jednoduchých navzájem nezávislých výroků $a_1, a_2, \ldots, a_n$. Uvažujme množinu V všech výpovědí, které lze z daných n výroků vytvořit pomocí spojek $\wedge$, $\vee$ a $\neg$. Každá výpověď představuje množinu navzájem logicky ekvivalentních výroků. Množina V má celkem $2^{(2^n)}$ prvků. Booleovský průsek dvou výpovědí je realizován pomocí spojky $\wedge$, spojení pomocí spojky $\vee$ a komplement pomocí spojky $\neg$. Jednotkou algebry V je výpověď vyslovená pomocí výroku majícího stavbu tautologie, nulou je výpověď, kterou lze vyslovit pomocí výroku majícího stavbu negace tautologie. Atomem této algebry je každá výpověď, kterou lze vyslovit ve tvaru

$$x_1 \wedge x_2 \wedge \ldots \wedge x_n,$$

kde každé x_i je buď a_i, nebo $\neg a_i$. Algebra V má proto 2^n atomů.

Pro $n = 1$ a $n = 2$ obdržíme algebry mající 4 a 16 prvků. Hasseovy diagramy těchto algeber jsou na obr. 62.

Uvedené čtyři příklady jsou pro $n = 1$ a $n = 2$ navzájem izomorfní. Graficky se tato skutečnost projeví tím, že mají stejné Hasseovy diagramy. Zřejmě bude platit obecně, že pro stejné n dostáváme čtveřici navzájem izomorfních algeber.

O dalších příkladech Booleových algeber, které jsou izomorfní s uvedenými příklady, budeme hovořit v následujících kapitolách. Je to především algebra A_n všech booleovských funkcí n-proměnných definovaných v algebře $\mathbf{2} = \{0, 1\}$, algebra P_n všech úplných disjunktivních normálních forem n-proměnných definovaných také v algebře $\mathbf{2}$, algebra Q_n všech úplných konjunktivních normálních forem n-proměnných definovaných v algebře $\mathbf{2}$. Dále to budou algebry představující fyzikální realizaci Booleových funkcí v algebře $\mathbf{2}$, tj. algebry logických obvodů.

Přistupme k pojednání o množinové reprezentaci konečných Booleových algeber. Specifičnost řešení tohoto problému v Booleových algebrách se proti řešení v libovolných distributivních svazech projeví v následujícím lemmatu.

Lemma 10.5. *Nechť B je Booleova algebra, pak prvek $p \in B$ je zdola ireducibilní, právě když p je nula nebo p je atom.*

Z lemmatu 10.5 vyplývá, že v Booleově algebře B jsou každé dva různé, nenulové a zdola ireducibilní prvky p, q navzájem disjunktní, tzn. $p \sqcap q = 0$. Nemůže proto nastat případ znázorněný na obr. 49b. V distributivním svazu D existuje zdola ireducibilní prvek p, který není sousedem nuly a není disjunktní se svým předchůdcem, který je také ireducibilní.

Příklad 10.12. V libovolné Booleově algebře $P(M)$ jsou nenulovými zdola ireducibilními prvky, tzn. atomy, právě všechny jednoprvkové množiny $\{x\}$, kde $x \in M$. Čtenář si může vyznačit atomy např. v diagramech na obr. 61 a 62.

Důkaz lemmatu 10.5. Nechť p je libovolný atom z B, pak z rovnosti $p = a \sqcup b$ vyplývá $a = p$ nebo $a = 0$. Pokud $a = 0$, pak $p = 0 \sqcup b = b$. V obou případech tak docházíme k závěru (viz formule (6.5)), že prvek p je zdola ireducibilní.

Obráceně: nechť x je libovolný prvek z B, který není nula ani atom, pak existuje takový prvek $a \in B$, že platí

$$0 \lhd a \lhd x, \tag{10.18}$$

a proto

$$x = x \sqcap 1 = x \sqcap (a \sqcup a') = (x \sqcap a) \sqcup (x \sqcap a') = a \sqcup (x \sqcap a'). \tag{10.19}$$

Poslední term jsme získali z předposledního pomocí formule (10.18) a formule (8.18). Z formule $x = a \sqcup (x \sqcap a')$ vyplývá podle (2.13'), že $x \sqcap a' \unlhd x$. Ukážeme, že dokonce musí platit $x \sqcap a' \lhd x$. Předpokládejme, že $x \sqcap a' = x$. Z tohoto předpokladu vyplývá, že

$$a = x \sqcap a = (x \sqcap a') \sqcap a = x \sqcap 0 = 0,$$

což je spor s formulí (10.18). Proto skutečně platí $x \sqcap a' \lhd x$. Z rovnosti prvního a posledního termu v (10.19) proto vyplývá, že prvek x není zdola ireducibilní.

Vyslovme lemma 6.6 pro Booleovy algebry.

Lemma 10.6. *Nechť B je konečná Booleova algebra, pak každý její prvek x lze zapsat jako spojení určitých atomů.*

Poznamenejme, že nulu algebry B lze zapsat jako spojení prázdné množiny atomů, tzn. $0 = \bigsqcup \emptyset$. Označíme-li $A(x)$ množinu všech atomů p algebry B předcházejících před prvkem $x \in B$, pak lze lemma 10.6 přepsat v silnější podobě (viz lemma 6.7).

Lemma 10.7. *Nechť B je konečná Booleova algebra, pak každý její prvek lze zapsat ve tvaru*

$$x = \bigsqcup A(x).$$

Místo zobrazení F definovaného u distributivních svazů formulí (6.6) zavedeme nyní zobrazení G, které každému prvku $x \in B$ přiřadí množinu $A(x)$, která je podmnožinou množiny A všech atomů z B, tzn.

$$G\colon x \in B \mapsto A(x) \in P(A). \tag{10.20}$$

Protože pro libovolný prvek $x \in B$ platí

$$A(x) = I(x) - \{0\}$$

a protože nula je obsažena ve všech množinách $I(x)$, má zobrazení G tytéž pro nás důležité vlastnosti, jako mělo zobrazení F, tzn. G je prosté, převádí průsek na množinový průnik

$$A(x \sqcap y) = A(x) \cap A(y)$$

a dále převádí spojení na množinové sjednocení

$$A(x \sqcup y) = A(x) \cup A(y).$$

Také platí $A(0) = \emptyset \wedge A(1) = A$.

Ukažme ještě, že každá množina $X \in P(A)$ je obrazem nějakého prvku Booleovy algebry B, tzn. že

$$G\colon B \overset{\text{na}}{\rightrightarrows} P(A). \tag{10.21}$$

Stačí ukázat, že různým množinám atomů X, Y přiřazuje operace $\sqcup$ různé prvky z B. Postupujme takto: Nechť p je atom, pro nějž platí $p \trianglelefteq \bigsqcup X$, kde $X \in P(A)$, pak podle formule (8.10) platí:

$$p = p \sqcap \bigsqcup X = \bigsqcup_{q_i \in X} (p \sqcap q_i)$$

Protože p je ireducibilní prvek, musí existovat atom $q_i \in X$ takový, že $p = p \sqcap q_i$, což znamená $0 \vartriangleleft p \trianglelefteq q_i$. Protože q_i je atom, dostáváme $p = q_i$, a proto $p \in X$.

Důsledkem právě provedené úvahy je následující tvrzení:

Lemma 10.8. *Nechť X, Y jsou různé podmnožiny množiny A atomů konečné Booleovy algebry B, pak platí*

$$\bigsqcup X \neq \bigsqcup Y.$$

Z lemmatu 10.8 již bezprostředně vyplývá formule (10.21). Všimněme si, že podle věty 10.5 zachovává zobrazení G i operaci komplement. Lemma 6.8 můžeme proto pro Booleovy algebry vyslovit takto:

Lemma 10.9. *Nechť B je konečná Booleova algebra a nechť A je množina atomů této algebry, pak zobrazení G definované formulí (10.20) je izomorfismus algebry B na těleso množin $P(A)$.*

Na závěr našeho teoretického pojednání vyslovme lemma 10.9 ve zjednodušené formě. Obdržíme větu, která se nazývá věta o množinové reprezentaci konečných Booleových algeber.

Věta 10.12. *Ke každé konečné Booleově algebře B existuje těleso množin $P(M)$, které je s algebrou B izomorfní.*

Větu 10.12 můžeme vyslovit také takto: V každém bloku navzájem izomorfních konečných Booleových algeber existuje alespoň jedno těleso množin $P(M)$.

Z věty 10.12 vyplývá, že konečné Booleovy algebry můžeme považovat za abstraktní analogie konečných množinových těles $P(M)$. Další důsledky:

1. Každá konečná Booleova algebra má 2^n prvků, kde n je určité přirozené číslo, neboť jestliže množina M má n prvků, pak její potence $P(M)$ má 2^n prvků. Booleovy algebry proto mají 1, 2, 4, 8, 16 atd. prvků. Neexistuje tedy Booleova algebra mající např. 7 nebo 11 prvků.

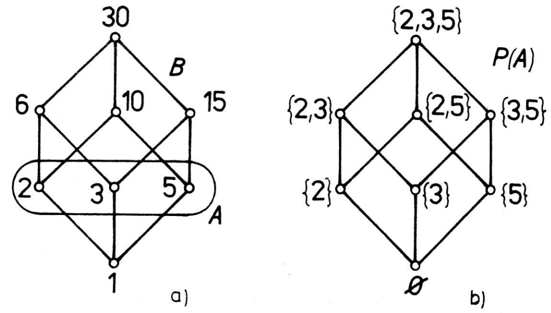
2. Každé dvě Booleovy algebry o stejném počtu prvků jsou navzájem izomorfní.

Na základě výše provedených úvah můžeme nyní popsat konstrukci množinového tělesa, které je izomorfní se zadanou konečnou Booleovou algebrou.

Konstrukce:

0. Nechť B je konečná Booleova algebra.
1. Určíme množinu A všech atomů algebry B.
2. Sestrojíme potenci $P(A)$. Uspořádáme-li množinu $P(A)$ relací $\subseteq$, obdržíme těleso množin izomorfní s algebrou B. Izomorfismem je zobrazení G zadané formulí (10.20).

Příklad 10.13. Uvažujme Booleovu algebru B všech dělitelů čísla 30 v $\mathbf{N}$. Konstrukci odpovídajícího tělesa množin, které je izomorfní s B, popíšeme pomocí obr. 63. Značení je zde stejné jako ve výše popsané konstrukci. Na obr. 63a je zadaná algebra B, v níž je vyznačena množina atomů A. Na obr. 63b je potence $P(A)$.



Obr. 63

Poznámka. Větu o množinové reprezentaci lze formulovat i pro libovolnou úplnou atomární algebru, přičemž **Booleova algebra** B se nazývá **atomární,** právě když pro libovolný nenulový prvek $x \in B$ existuje aspoň jeden atom p, pro který platí $p \preceq x$. Každá konečná Booleova algebra je atomární. Nekonečnou atomární Booleovu algebru B obdržíme např. takto: Uvažujme nekonečnou množinu M. Množina B obsahuje všechny konečné podmnožiny množiny M a jejich (nekonečné) komplementy.

Označme A množinu všech atomů úplné atomární algebry B, pak zobrazení G definované formulí (10.20) představuje izomorfní vnoření algebry B do potence $P(A)$. Těleso množin, které je obrazem algebry B a které je v případě nekonečné atomární algebry B vlastním podtělesem potence $P(A)$, je množinovým reprezentantem algebry B.

Pro Booleovy algebry B, které nejsou atomární, je třeba nalézt objekty, které budou hrát roli atomů, tzn. které budou hrát roli prvků výchozí množiny množinového tělesa. Protože existuje vzájemně jednoznačný vztah mezi atomy a hlavními ultrafiltry, lze množinu U všech ultrafiltrů považovat za rozšíření množiny všech atomů. Množina U je výchozí množinou pro hledané množinové těleso.

Nechť B je libovolná (i neatomární) Booleova algebra a nechť U je množina všech ultrafiltrů v B, pak zobrazení

$$G: x \in B \mapsto \{F \in U; x \in F\} \in P(U)$$

představuje izomorfní vnoření B do tělesa množin $P(U)$. Těleso množin, které je obrazem algebry B a které je v případě neatomární algebry B vlastním podtělesem potenční algebry $P(U)$, je množinovým reprezentantem algebry B.

CVIČENÍ 10

1 Pokud pro ideál I Booleovy algebry B platí formule (10.4), pak I je prvoideál. Dokažte.

2 Dokažte, že pokud B je Booleův okruh a I je jeho ideál, pak platí:
$(\forall x, y \in I)\,(x \oplus y) \oplus (x \sqcap y) = x \sqcup y$

3 Dokažte, že Booleův homomorfismus F Booleovy algebry B na Booléovu algebru A zachovává operace $-$, $\oplus$, $\uparrow$ a $\downarrow$.

4 Dokažte, že zobrazení F Booleovy algebry B na algebru A je izomorfismus, právě když
$(\forall x, y \in B)\; x \trianglelefteq y \Leftrightarrow F(x) \trianglelefteq F(y)$.

5 Dokažte, že relace K zavedená formulí (10.17) v důkazu věty 10.9 je ekvivalence.

6 Uvažujte Booleovu algebru $P(\{a, b, c, d\})$. Vypište všechny její ideály a sestrojte Hasseovy diagramy všech homomorfních obrazů této algebry.

7 Definujte izomorfismus mezi Booleovými algebrami uvedenými v příkladech 10.8, 10.9, 10.10 a 10.11 pro $n = 1$, $n = 2$ a pro libovolné n.

8 Nechť K je kongruence v Booleově algebře B, pak množina všech prvků, které jsou kongruentní s nulou, tvoří ideál v B. Dokažte.

9 Nechť F je homomorfní zobrazení Booleovy algebry B na Booleovu algebru A, pak množina $I = \{x \in B: F(x) = 0\}$ je ideál v B. Dokažte.

10 Nechť B je Booleova algebra a I je ideál v B, pak zobrazení
$F: x \in B \mapsto T_x \in B/I$
je homomorfní zobrazení algebry B na faktorovou algebru B/I. Dokažte.

11 Dokažte, že formule (10.15), (10.15′) a (10.16) definují skutečně operace ve faktorové algebře B/K, tzn. že výsledek nezávisí na volbě reprezentantů.

12 Popište konstrukci faktorové algebry B/F Booleovy algebry B podle jejího filtru F.

13 Sestrojte množinového reprezentanta následujících Booleových algeber: a) algebra všech dělitelů čísla 7 v $\mathbf{N}$, b) algebra všech dělitelů čísla 6 v $\mathbf{N}$ a c) algebra všech dělitelů čísla 210 v $\mathbf{N}$.

11 BOOLEOVY FUNKCE

Studium Booleových funkcí je matematicky zajímavé a přitom důležité vzhledem k aplikacím. Z tohoto hlediska mají mimořádné postavení funkce v dvouprvkové Booleově algebře $\mathbf{2} = \{0, 1\}$. Jim také budeme věnovat hlavní pozornost. Nejprve ukážeme, jak Booleovy funkce zadávat. Půjde jednak o zadávání pomocí tabulek, jednak také pomocí termů, kterým budeme v této souvislosti říkat polynomy. Z tohoto hlediska jsou důležité polynomy, kterým říkáme úplná disjunktivní normální forma a úplná konjunktivní normální forma. V druhé části se budeme zabývat problémem co nejjednoduššího vyjádření funkce pomocí polynomu. Především pro aplikace má tato problematika minimalizace mimořádnou důležitost. Podrobně popíšeme metodu Quineovu—Mc Cluskeiovu.

11.1 Booleovy funkce, Booleovy polynomy

Zaveďme nejprve pojem Booleovy funkce v libovolné algebře B.

Definice 11.1. Booleovou funkcí n **proměnných** *v Booleově algebře B se nazývá libovolné zobrazení F množiny B^n do množiny B, tzn.*

$$F: B^n \to B. \tag{11.1}$$

Speciálně: *Booleovou funkcí n proměnných v Booleově algebře* $\mathbf{2}$ *je libovolné zobrazení*

$$F: \mathbf{2}^n \to \mathbf{2}. \tag{11.2}$$

Příklady 11.1. V každé Booleově algebře B jsou podle definice 8.1 zavedeny dvě Booleovy funkce dvou proměnných, tj. průsek $\sqcap$ a spojení $\sqcup$, jedna Booleova funkce jedné proměnné, tj. komplement $'$, a dvě nulární Booleovy funkce, tj. prvek 0 a prvek 1. V libovolné Booleově algebře však můžeme zavést řadu dalších Booleových funkcí. Jednou z funkcí dvou proměnných je např. symetrická diference $\oplus$, pro niž platí:

$$(\forall x, y \in B)\; x \oplus y = (x \sqcap y') \sqcup (x' \sqcap y) \tag{11.3}$$

Další příklady Booleových funkcí dvou proměnných jsme zavedli pomocí formulí (8.26) až (8.28′).

Protože v následujícím textu budeme pojednávat výhradně o Booleových funkcích, přijměme úmluvu, že přívlastek „Booleova" budeme často vynechávat.

Na množině A_n všech Booleových funkcí n proměnných $x_1, x_2, \ldots, x_n$ v Booleově algebře B lze definovat operace $\sqcap$, $\sqcup$ a $'$ následujícím způsobem:

$$(F \sqcap G)(x_1, \ldots, x_n) =_{\mathrm{df}} F(x_1, \ldots, x_n) \sqcap G(x_1, \ldots, x_n) \tag{11.4}$$

$$(F \sqcup G)(x_1, \ldots, x_n) =_{\mathrm{df}} F(x_1, \ldots, x_n) \sqcup G(x_1, \ldots, x_n) \tag{11.4'}$$

$$F'(x_1, \ldots, x_n) =_{\mathrm{df}} [F(x_1, \ldots, x_n)]' \tag{11.5}$$

Vidíme, že průsek funkcí F a G definujeme pomocí průseku funkčních hodnot funkcí F a G, což jsou prvky Booleovy algebry B. Obdobně je tomu pro spojení a komplement. Proto je ihned zřejmé, že operace $\sqcap$, $\sqcup$ a $'$ jsou booleovské operace v množině A_n. Lze vyslovit následující větu.

Věta 11.1. *Nechť A_n je množina všech Booleových funkcí n proměnných v Booleově algebře B, pak struktura $(A_n, \sqcap, \sqcup, ')$, kde operace $\sqcap$, $\sqcup$ a $'$ jsou definovány formulemi* (11.4), (11.4′) *a* (11.5), *je Booleova algebra, v níž nulou je nulová funkce $F(x_1, \ldots, x_n) = 0$ a jednotkou je jednotková funkce $F(x_1, \ldots, x_n) = 1$.*

Uspořádání $\trianglelefteq$ můžeme v množině A_n definovat buď pomocí některé z formulí:

$$F \trianglelefteq G \Leftrightarrow_{\mathrm{df}} F \sqcap G = F \qquad F \trianglelefteq G \Leftrightarrow_{\mathrm{df}} F \sqcup G = G, \tag{11.6}$$

nebo následujícím ekvivalentním způsobem:

$$F \trianglelefteq G \Leftrightarrow (\forall x_1, \ldots, x_n \in B)\, F(x_1, \ldots, x_n) \trianglelefteq G(x_1, \ldots, x_n) \tag{11.7}$$

Především formule (11.7) zřetelně ukazuje, že uspořádání v A_n velmi úzce souvisí s uspořádáním v algebře B.

Příklad 11.2. V množině A_2 všech Booleových funkcí dvou proměnných v algebře $\mathbf{2} = \{0, 1\}$ uvažujme funkce F_5^2 a F_6^2 definované tabulkami 9 a 10 v příkladě 11.4. Pro jejich průsek a spojení platí:

$$F_5^2 \sqcap F_6^2 = F_4^2 \qquad \text{a} \qquad F_5^2 \sqcup F_6^2 = F_7^2$$

Pro funkce F_2^2 a F_7^2 z téhož příkladu platí $F_2^2 \trianglelefteq F_7^2$. Budeme-li uvažovat funkce F_3^2 a F_{14}^2, pak zjistíme, že jsou neporovnatelné. Nulou v algebře A_2 je funkce F_0^2 a jednotkou je funkce F_{15}^2.

Poznámka. Uvažujme množinu A_n všech Booleových funkcí n proměnných v algebře $\mathbf{2}$. Z formule (11.7) vyplývá, že Hasseův diagram uspořádání $\trianglelefteq$ v množině A_n bude vypadat takto: nejníže je umístěna nulová funkce. V prvním patře diagramu jsou všechny funkce, které nabývají právě pro jeden vektor $(x_1, x_2, \ldots, x_n) \in 2^n$ hodnoty 1. V druhém patře jsou všechny funkce, které nabývají právě dvakrát hodnoty 1 atd. Nejvýše bude jednotková funkce. Atomy algebry A_n by podle této představy měly být všechny ty funkce, které nabývají právě jednou hodnoty 1. Koatomy by měly být všechny ty funkce, které nabývají právě jednou hodnoty 0.

Poznamenejme ještě, že místo o množině všech Booleových funkcí n proměnných můžeme stejně tak dobře hovořit o množině všech Booleových funkcí s nejvýše n proměnnými. Jestliže má totiž funkce $F(x_1, x_2, \dots, x_r)$ r proměnných, kde $r < n$, pak ji můžeme považovat za funkci n proměnných, pokud uděláme tuto úmluvu: při daných hodnotách $x_1, \dots, x_r$ jsou hodnoty funkce $F(x_1, \dots, x_n)$ pro libovolné hodnoty proměnných $x_{r+1}, \dots, x_n$ stále stejné a rovny hodnotě funkce $F(x_1, \dots, x_r)$. Po této úmluvě můžeme např. funkci jedné proměnné F_2^1 (viz př. 11.3) považovat za funkci dvou proměnných F_{12}^2 (viz př. 11.4).

Položme si otázku, jaký největší počet prvků má algebra A_n všech Booleových funkcí v konečné algebře B. Počet nezávisle proměnných v uvažovaných funkcích F je tak omezen shora číslem n. Nechť pro algebru B platí, že B je izomorfní s algebrou $P(M)$ (viz věta 10.12), kde množina M má r prvků. Z právě vyslovených předpokladů vyplývá, že algebra $P(M)$, a tedy i algebra B mají celkem 2^r prvků. Každá funkce $F \in A_n$ má definiční obor složen z uspořádaných n-tic $(v_1, \dots, v_n)$, tj. z vektorů $\boldsymbol{v} \in B^n$. Těchto vektorů $\boldsymbol{v}$ lze sestrojit celkem

$$\underbrace{2^r \,.\, 2^r \,.\, \dots \,.\, 2^r}_{n} = (2^r)^n.$$

Každá funkce F přiřazuje každému takovémuto vektoru nějaký prvek z B, neboť $F\colon B^n \to B$ (viz formule (11.1)). Všech možných funkcí F majících n proměnných je proto

$$\underbrace{2^r \,.\, 2^r \,.\, \dots \,.\, 2^r}_{2^{rn}} = 2^{r \,.\, 2^{rn}}.$$

Speciálně, počet funkcí n proměnných v algebře **2** je $2^{(2^n)}$. Na základě právě provedených úvah můžeme vyslovit následující lemma.

Lemma 11.1. *Množina A_n všech Booleových funkcí n proměnných v konečné Booleově algebře B tvoří konečnou Booleovu algebru.*

Jestliže chceme s Booleovými funkcemi pracovat, pak je musíme určitým způsobem zadat. My se budeme zabývat zadáváním pomocí tabulek a pomocí formulí. V technické praxi se však v algebře **2** často používá i zadávání pomocí map (např. Karnaughova a Svobodova mapa), jejichž podstatu tvoří Vennovy diagramy, a dále zadávání pomocí n-rozměrných krychlí (viz [5] nebo [14]).

Nyní se budeme zabývat zadáváním funkcí pomocí tabulek, a to pouze v algebře **2**.

Příklad 11.3. Uvažujme v dvouprvkové algebře **2** funkce jedné proměnné, které budeme značit F_i^1. Těmto funkcím odpovídá tabulka 5.

Tab. 5

x	F_0^1	F_1^1	F_2^1	F_3^1
0	0	0	1	1
1	0	1	0	1

Algebra A_1 v algebře **2** má tedy $2^{(2^1)} = 4$ prvky. Tabulky 6, 7, 8 ukazují, jak se mezi těmito funkcemi provádí booleovské operace $\sqcap$, $\sqcup$ a $'$. Označíme-li např. funkci F_1^1 znakem F, pak uvedené čtyři funkce jsou označeny po řadě symboly 0, F, F' a 1.

Tab. 6

	$'$
0	1
F	F'
F'	F
1	0

Tab. 7

$\sqcap$	0	F	F'	1
0	0	0	0	0
F	0	F	0	F
F'	0	0	F'	F'
1	0	F	F'	1

Tab. 8

$\sqcup$	0	F	F'	1
0	0	F	F'	1
F	F	F	1	1
F'	F'	1	F'	1
1	1	1	1	1

Protože pomocí funkce F můžeme vyjádřit všechny tři zbylé funkce z A_1 ($F \sqcap F' = 0$ a $F \sqcup F' = 1$), platí:

Lemma 11.2. *Existuje jednoprvková množina generátorů algebry A_1 v algebře* **2**.

Příklad 11.4. Uvažujme v dvouprvkové algebře **2** funkce dvou proměnných, které budeme značit F_i^2. Sestrojme jejich tabulky 9, 10. Dříve však poznamenejme, že kombinace hodnot nezávisle proměnných uspořádáme lexikograficky (shora dolů) a že index i bude vlastně desítkovým vyjádřením čísla zapsaného ve dvojkové soustavě v tabulce pod symbolem F_i^2 (číslo čteme shora dolů). Obdobně tomu bylo i v tabulkách z příkladu 11.3 a obdobně tomu bude i u libovolné funkce F_i^n n proměnných v algebře **2**.

Tab. 9

	x	y	F_0^2	F_1^2	F_2^2	F_3^2	F_4^2	F_5^2	F_6^2	F_7^2
0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	1	1	1	1
2	1	0	0	0	1	1	0	0	1	1
3	1	1	0	1	0	1	0	1	0	1

Tab. 10

	x	y	F_8^2	F_9^2	F_{10}^2	F_{11}^2	F_{12}^2	F_{13}^2	F_{14}^2	F_{15}^2
0	0	0	1	1	1	1	1	1	1	1
1	0	1	0	0	0	0	1	1	1	1
2	1	0	0	0	1	1	0	0	1	1
3	1	1	0	1	0	1	0	1	0	1

Upozorněme ještě na jednu zajímavou skutečnost. Označíme-li řádky v tabulce po řadě čísly 0, 1, 2, 3, pak vektor $(x, y) \in 2^2$ na j-tém řádku představuje dvojkové vyjádření čísla tohoto řádku. Obdobně tomu bude i u tabulek funkcí n proměnných. Např. vektor (0101) funkce F čtyř proměnných leží v řádku s číslem 5.

Algebra A_2 v algebře **2** má $2^{(2^2)} = 16$ prvků. Ukažme, že libovolnou z těchto šestnácti funkcí lze vyjádřit pomocí dvou z nich. Označíme-li funkci F_3^2 písmenem G a funkci F_5^2 písmenem H, pak platí:

$$\begin{array}{llll}
F_0^2 = 0 = G \sqcap G' & F_4^2 = G' \sqcap H & F_8^2 = G' \sqcap H' & F_{12}^2 = G' \\
F_1^2 = G \sqcap H & F_5^2 = H & F_9^2 = G' \oplus H & F_{13}^2 = G' \sqcup H \\
F_2^2 = G \sqcap H' & F_6^2 = G \oplus H & F_{10}^2 = H' & F_{14}^2 = G' \sqcup H' \\
F_3^2 = G & F_7^2 = G \sqcup H & F_{11}^2 = G \sqcup H' & F_{15}^2 = 1 = G \sqcup G'
\end{array}$$

Proto lze vyslovit následující lemma.

Lemma 11.3. *Existuje dvouprvková množina generátorů algebry A_2 v algebře* **2**.

V následující kapitole dokonce ukážeme, že existují dvě jednoprvkové množiny generátorů algebry A_2 v algebře **2**. Jednu z těchto množin tvoří Shefferova funkce F_{14}^2 a druhou Peirceova funkce F_8^2.

Než budeme pokračovat ve studiu funkcí, zavedeme pojem Booleův polynom. Na základě toho, co jsme řekli o termech při budování jazyka teorie svazů, můžeme nyní vyslovit definici **termu** v Booleově algebře $(B, \sqcap, \sqcup, ', 0, 1)$.

Definice termu Booleovy algebry B.

1. *Každá proměnná $x, y, \ldots$ (pro prvky z B) i konstanty* 0, 1 *jsou termy.*
2. *Jestliže jsou slova τ_1, τ_2 termy, pak jsou i slova $(\tau_1) \sqcap (\tau_2)$, $(\tau_1) \sqcup (\tau_2)$ a $(\tau_1)'$ termy.*
3. *Jinak utvořená slova nejsou termy.*

K úmluvám o vypouštění závorek v termech řekněme pouze toto: Proměnné a konstanty nepíšeme do závorek a dále, v posloupnosti znaků $'$, $\sqcap$, $\sqcup$ má znak více nalevo přednost před znakem více napravo. Tzn. např. term $x \sqcap y \sqcup z$ chápeme takto: $(x \sqcap y) \sqcup z$ nebo term $x \sqcap y' \sqcup z$ chápeme takto: $[x \sqcap (y')] \sqcup z$. Závorky můžeme vypouštět také na základě asociativnosti operací $\sqcap$ a $\sqcup$.

V teorii Booleových algeber bývá zvykem používat především v souvislosti se studiem Booleových funkcí místo názvu term jazyka algebry B název **Booleův polynom algebry** B. Booleův polynom, či pouze polynom algebry B je proto každé slovo, které je vytvořeno na základě definice termu. Speciálně, podle počtu různých proměnných, které jsme při vytváření termu použili, mluvíme o polynomech jedné proměnné, dvou proměnných a obecně o polynomech n proměnných. Polynomy n proměnných x_1, x_2 až x_n budeme značit $f(x_1, x_2, \ldots, x_n)$.

Příklad. V Booleově algebře B jsou polynomy např. slova: x, $(x \sqcup 1)' \sqcap x$ (polynomy jedné proměnné), $x \sqcap y$, $(x \sqcap y')'$, $(x \sqcap z) \sqcup (x \sqcap z')$ (polynomy dvou proměnných), $(x \sqcap y \sqcap z') \sqcup 0$ (polynom tří proměnných).

V následující části se budeme zabývat vztahem mezi Booleovými funkcemi z A_n v algebře B a Booleovými polynomy v B. Je zřejmé, že každý Booleův polynom n proměnných $f(x_1, \ldots, x_n)$ definuje v algebře B funkci n proměnných, tzn. polynomu $f(x_1, \ldots, x_n)$ odpovídá funkce $F\colon B^n \to B$. Funkční hodnotu funkce F pro určitý konkrétní vektor $(v_1, \ldots, v_n) \in B^n$ obdržíme tak, že jeho složky prostě dosadíme do polynomu F a vzniklý term „spočítáme".

Příklad 11.5. Uvažujme polynom dvou proměnných $(x \sqcap y) \sqcup (x' \sqcap y)$ v algebře **2**. Tento polynom definuje funkci F, pro niž platí $F\colon (0, 1) \mapsto 1$, neboť

$$(0 \sqcap 1) \sqcup (0' \sqcap 1) = 0 \sqcup (1 \sqcap 1) = 0 \sqcup 1 = 1.$$

Jestliže spočítáme hodnoty funkce F pro všechny vektory $(x, y) \in 2^2$, pak obdržíme tabulku funkce F_5^2 z příkladu 11.4.

Poznamenejme, že rovnost dvou polynomů lze zavést různě. Pro naše účely se dobře hodí tzv. funkční definice rovnosti polynomů.

Definice 11.2. *Říkáme, že* **polynomy** $f(x_1, \ldots, x_n)$ *a* $g(x_1, \ldots, x_n)$ *Booleovy algebry B* **jsou si rovny,** *právě když oba určují stejnou Booleovu funkci n proměnných, a zapisujeme:*

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$$

Nyní přistoupíme k popisování funkcí pomocí polynomů. Nejprve zopakujme, že libovolný polynom $f(x_1, \ldots, x_n)$ definuje pro libovolnou Booleovu algebru B funkci $F\colon B^n \to B$. Toto tvrzení lze částečně obrátit. Částečným obrácením myslíme to, že se nový výrok nebude týkat libovolné Booleovy algebry, ale pouze algebry **2**. V další části kapitoly proto budeme pojednávat už jenom o dvouprvkových algebrách $\{0, 1\}$.

Věta 11.2. *Každou Booleovu funkci* $F\colon \mathbf{2}^n \to \mathbf{2}$ *lze vyjádřit nějakým Booleovým polynomem.*

Abychom lépe rozuměli následujícímu konstruktivnímu důkazu, zavedeme v algebře **2** polynomy speciálního druhu.

Definice 11.3. *Polynomy tvaru* $\bigsqcap_{i=1}^{n} y_i = y_1 \sqcap y_2 \sqcap \dots \sqcap y_n$, *kde* y_i *je buď* x_i, *nebo* x_i', *se nazývají* **minimální průsekové polynomy** *proměnných* x_1 *až* x_n. *O polynomu, který je spojením minimálních průsekových polynomů proměnných* x_1 *až* x_n, *říkáme, že je zapsán v* **úplné disjunktivní (spojové) normální formě.**

Definice 11.3′. *Polynomy tvaru* $\bigsqcup_{i=1}^{n} y_i = y_1 \sqcup y_2 \sqcup \dots \sqcup y_n$, *kde* y_i *je buď* x_i, *nebo* x_i', *se nazývají* **maximální spojové polynomy** *proměnných* x_1 *až* x_n. *O polynomu, který je průsekem maximálních spojových polynomů proměnných* x_1 *až* x_n, *říkáme, že je zapsán v* **úplné konjunktivní (průsekové) normální formě.**

V minimálním průsekovém polynomu $m(x_1, \dots, x_n)$ se každá proměnná vyskytuje právě jednou, a to buď ve formě x_i, nebo x_i'. Úplná disjunktivní normální forma je spojením několika minimálních polynomů. Protože minimálních polynomů $m(x_1, \dots, x_n)$ lze zkonstruovat 2^n, je úplná disjunktivní normální forma $f(x_1, \dots, x_n)$ spojením nejvýše 2^n různých minimálních polynomů. Z praktických důvodů je vhodné dodržovat v jednotlivých minimálních polynomech stejné pořadí proměnných. Analogické poznámky lze vyslovit i o úplné konjunktivní normální formě.

Příklad 11.6. Následující polynomy $f(x, y)$ a $g(x_1, x_2, x_3)$ jsou zapsány v úplné disjunktivní normální formě, polynom $h(x_1, x_2, x_3)$ je zapsán v úplné konjunktivní normální formě:

$$f(x, y) = (x \sqcap y) \sqcup (x' \sqcap y) \sqcup (x' \sqcap y')$$
$$g(x_1, x_2, x_3) = (x_1' \sqcap x_2 \sqcap x_3) \sqcup (x_1' \sqcap x_2 \sqcap x_3')$$
$$h(x_1, x_2, x_3) = (x_1 \sqcup x_2' \sqcup x_3) \sqcap (x_1' \sqcup x_2 \sqcup x_3) \sqcap (x_1' \sqcup x_2' \sqcup x_3')$$

Důkaz věty 11.2. Podstata důkazu spočívá v tom, že popíšeme, jak k Booleově funkci F sestrojíme její úplnou disjunktivní normální formu. Nechť F je libovolná Booleova funkce $\mathbf{2}^n \to \mathbf{2}$. Pak ke každému vektoru $\mathbf{v} = (v_1, \dots, v_n) \in \mathbf{2}^n$ můžeme sestrojit následujícím způsobem minimální polynom $m_\mathbf{v}$:

$$m_\mathbf{v}(x_1, \dots, x_n) = y_1 \sqcap y_2 \sqcap \dots \sqcap y_n, \qquad \text{kde } y_i = \begin{cases} x_i, \text{ jestliže } v_i = 1 \\ x_i', \text{ jestliže } v_i = 0 \end{cases}$$

Z konstrukce minimálního polynomu $m_\mathbf{v}$ vyplývá, že $m_\mathbf{v}$ nabývá hodnoty 1 přesně jenom pro vektor $\mathbf{v}$. Pro jakýkoli jiný vektor $\mathbf{u} \in 2^n$ obdržíme 0. Označme množinu všech vektorů, pro něž nabývá funkce F hodnoty 1, symbolem $T(F)$ a sestrojme ke každému vektoru $\mathbf{v} \in T(F)$ odpovídající minimální polynom $m_\mathbf{v}$. Sestrojíme-li dále spojení všech těchto minimálních polynomů $m_\mathbf{v}$, pro $\mathbf{v} \in T(F)$, obdržíme úplnou disjunktivní normální formu:

$$f(x_1, \dots, x_n) = \bigsqcup_{\mathbf{v} \in T(F)} m_\mathbf{v}(x_1, \dots, x_n)$$

Na základě toho, co jsme řekli o vlastnostech minimálních polynomů, a protože jsou tyto polynomy spojeny znaky $\sqcup$, můžeme o polynomu $f(x_1, \dots, x_n)$ říci toto:

$$(\forall \boldsymbol{v} \in \mathbf{2}^n)\ F(\boldsymbol{v}) = \left\{ \begin{matrix} 1 \\ 0 \end{matrix} \right\} \quad \Leftrightarrow \quad \left\{ \begin{matrix} f(\boldsymbol{v}) = 1 \\ f(\boldsymbol{v}) = 0 \end{matrix} \right.$$

Zkonstruovaný polynom $f(x_1, \dots, x_n)$ proto definuje zadanou Booleovu funkci F.

Důkaz věty 11.2 je cenný především proto, že dává návod, jak k dané funkci F sestrojit odpovídající polynom. Tento polynom má úplnou disjunktivní normální formu. Uvedenou konstrukci budeme demonstrovat v příkladě 11.7. Zopakujme ještě, že každý vektor $\boldsymbol{v} \in \mathbf{2}^n$ představuje dvojkové vyjádření nějakého desítkového čísla j. Odpovídající minimální polynom se značí m_j. Důkaz věty 11.2 bychom mohli podat také tak, aby vedl k zadání funkce F pomocí úplné konjunktivní normální formy. Maximální polynom odpovídající výše uvedenému vektoru $\boldsymbol{v}$ pak značíme M_j.

Příklad 11.7. Uvažujme funkci $F(x, y, z)$ v algebře **2**, která je zadaná tabulkou 11.

Tab. 11

	x	y	z	$F(x, y, z)$
0	0	0	0	0
1	0	0	1	1
2	0	1	0	0
3	0	1	1	0
4	1	0	0	0
5	1	0	1	1
6	1	1	0	0
7	1	1	1	1

Sestrojme úplnou disjunktivní normální formu odpovídající funkci F. Minimální polynomy odpovídající třem řádkům s jednotkami (v posledním sloupci) jsou:

$$m_1 = x' \sqcap y' \sqcap z, \qquad m_5 = x \sqcap y' \sqcap z, \qquad m_7 = x \sqcap y \sqcap z$$

Hledaná úplná disjunktivní normální forma definující funkci F proto vypadá takto:

$$f(x, y, z) = (x' \sqcap y' \sqcap z) \sqcup (x \sqcap y' \sqcap z) \sqcup (x \sqcap y \sqcap z) = m_1 \sqcup m_5 \sqcup m_7$$

Úplnou konjunktivní normální formu funkce F sestrojíme takto: Maximální polynomy odpovídající řádkům s nulami jsou

$$M_0 = x \sqcup y \sqcup z, \qquad M_2 = x \sqcup y' \sqcup z, \qquad M_3 = x \sqcup y' \sqcup z',$$
$$M_4 = x' \sqcup y \sqcup z, \qquad M_6 = x' \sqcup y' \sqcup z.$$

Úplná konjunktivní normální forma funkce F:

$$g(x, y, z) = M_0 \sqcap M_2 \sqcap M_3 \sqcap M_4 \sqcap M_6$$

Ukažme ještě přechod od úplné disjunktivní normální formy f funkce F k její úplné konjunktivní normální formě:

a) Sestrojíme úplnou disjunktivní normální formu funkce F' (tzn. sestrojíme spojení minimálních polynomů pro řádky s nulami v posledním sloupci tabulky F)

$$f'(x, y, z) = m_0 \sqcup m_2 \sqcup m_3 \sqcup m_4 \sqcup m_6 .$$

b) Pomocí de Morganových pravidel sestrojíme k polynomu f' jeho komplement f''

$$g(x, y, z) = M_0 \sqcap M_2 \sqcap M_3 \sqcap M_4 \sqcap M_6 .$$

Z předchozích úvah vyplývá, že pokud zadáme dvě úplné disjunktivní normální formy, které budou vytvořeny z různých minimálních průseků, pak budou tyto formy definovat různé Booleovy funkce. Zdůvodnění můžeme podat ještě takto: Nechť existují dvě různé úplné disjunktivní normální formy f_1, f_2, které určují stejnou Booleovu funkci F, tzn.

$$f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) \tag{11.8}$$

Protože f_1, f_2 jsou různé disjunktivní normální polynomy, musí existovat alespoň jeden minimální polynom $m(x_1, \ldots, x_n)$, který se vyskytuje např. v f_1 a nevyskytuje se v f_2. Pokud sestrojíme průsek rovnosti (11.8) s tímto minimálním polynomem $m(x_1, \ldots, x_n)$, obdržíme rovnost:

$$m(x_1, \ldots, x_n) = 0$$

(použili jsme zobecněný distributivní zákon, formuli (8.3), a dále to, že libovolné dva různé minimální polynomy jsou disjunktní — viz cv. 11.7). Minimální polynom však nemůže určovat nulovou funkci, protože nabývá právě pro jeden vektor $\boldsymbol{v} \in \mathbf{2}^n$ hodnoty 1. Tím jsme obdrželi spor.

Úvahy o zobrazení, které každé Booleově funkci přiřazuje její úplnou disjunktivní normální formu, nás vedou k vyslovení následujícího lemmatu.

Lemma 11.4. *Množina A_n všech Booleových funkcí n proměnných a množina P_n všech Booleových polynomů n proměnných majících úplnou disjunktivní normální formu v Booleově algebře* **2** *jsou navzájem ekvivalentní.*

Množina P_n všech polynomů n proměnných majících úplnou disjunktivní normální formu je uzavřená vzhledem k operacím $\sqcap$, $\sqcup$, $'$ (viz cv. 11.8), a tvoří proto Booleovu algebru. Poznamenejme, že toto tvrzení také bezprostředně vyplývá z níže uvedené věty 11.4. Nulou této algebry je nulový polynom, který vznikne jako spojení prázdné množiny minimálních polynomů, jednotkou je polynom, který vznikne spojením všech 2^n minimálních polynomů, a atomem je právě každý minimální polynom. Zobrazení, které jsme zavedli v důkazu věty 11.2 určuje izomorfismus algeber A_n a P_n.

Hasseův diagram Booleovy algebry P_n má nejníže nulu, v prvním patře všechny minimální polynomy, v druhém patře všechna spojení právě dvou minimálních polynomů atd. Nejvýše je jednotka, která vznikne spojením všech minimálních polynomů. Hasseův diagram algebry P_n lze proto načrtnout tak, aby vypadal stejně jako diagram algebry A_n (viz poznámka na str. 194). Naše úvahy shrneme do následující věty.

Věta 11.3. *Nechť P_n je množina všech polynomů n proměnných majících úplnou disjunktivní normální formu v Booleově algebře* **2**. *Pak P_n tvoří Booleovu algebru, jejímiž atomy jsou právě všechny minimální polynomy $m(x_1, \ldots, x_n)$. Algebra P_n je izomorfní s algebrou A_n všech Booleových funkcí F: $\mathbf{2}^n \to \mathbf{2}$.*

Věta 11.3′. *Nechť Q_n je množina všech polynomů n proměnných majících úplnou konjunktivní normální formu v Booleově algebře* **2**. *Pak Q_n tvoří Booleovu algebru, jejímiž atomy jsou právě všechny maximální polynomy $M(x_1, \ldots, x_n)$. Algebra Q_n je izomorfní s algebrou A_n všech Booleových funkcí F: $\mathbf{2}^n \to \mathbf{2}$.*

Poznámka. V kapitole 10 jsme ukázali čtyři příklady navzájem izomorfních Booleových algeber majících $2^{(2^n)}$ prvků, kde n je určité přirozené číslo. Tyto algebry jsou uvedeny v příkladech 10.8, 10.9, 10.10 a 10.11. Nyní k nim můžeme přidat další tři druhy. Jsou to:

— algebra A_n všech Booleových funkcí n proměnných definovaných v algebře **2**. Atomy této algebry jsou všechny funkce, které nabývají právě jednou hodnoty 1;

— algebra P_n všech úplných disjunktivních normálních forem n proměnných v algebře **2**. Atomy této algebry jsou právě všechny minimální polynomy $m(x_1, \ldots, x_n)$;

— algebra Q_n všech úplných konjunktivních normálních forem n proměnných v algebře **2**. Atomy této algebry jsou právě všechny maximální polynomy $M(x_1, \ldots, x_n)$.

Uvedené druhy algeber mají 2^n atomů a $2^{(2^n)}$ prvků. Pro $n = 1$ a $n = 2$ jsou jejich Hasseovy diagramy znázorněny na obr. 62a, b.

V následující části se budeme zabývat úpravou libovolného polynomu $f(x_1, \ldots, x_n)$ z algebry **2** na úplnou disjunktivní normální formu. Popis konstrukce:

Konstrukce úplné disjunktivní normální formy polynomu f:

0. Nechť $f(x_1, \ldots, x_n)$ je polynom n proměnných v algebře **2**.

1. Pokud $f(x_1, \ldots, x_n)$ obsahuje čárkované závorky, pak lze pomocí de Morganových pravidel (viz formule (8.13) a (8.13′)) přemístit tyto čárky k jednotlivým proměnným, popř. použít ještě formuli $x'' = x$ (viz formule (8.12)).

2. Pokud se v polynomu $f(x_1, \ldots, x_n)$ vyskytuje symbol $\sqcap$ mimo závorku, v níž je nějaký symbol $\sqcup$, pak můžeme tento symbol přemístit dovnitř pomocí zobecněného distributivního zákona (viz formule (8.10)).

3. Polynom $f(x_1, \ldots, x_n)$ lze dále upravit např. na základě následujících formulí:

$$x \sqcap x = x \qquad x \sqcup x = x$$
$$x \sqcap x' = 0 \qquad x \sqcap 0 = 0$$
$$x \sqcup 0 = x$$

4. Pokud je polynom $f(x_1, \ldots, x_n)$ vyjádřen jako spojení průseků a přitom v některém průseku p chybí určitá proměnná x_i, sestrojíme průsek tohoto p s jednotkou ve formě $x_i \sqcup x_i'$. Tím z průseku p obdržíme spojení dvou nových průseků, z nichž jeden bude obsahovat navíc proměnnou x_i a druhý x_i':

$$p = p \sqcap 1 = p \sqcap (x \sqcup x_i') = (p \sqcap x_i) \sqcup (p \sqcap x_i')$$

5. Ve všech minimálních polynomech, jejichž spojením je výsledný polynom $g(x_1, \ldots, x_n)$, vypíšeme proměnné ve stejném pořadí. Získaný polynom g má úplnou disjunktivní normální formu a přitom je roven zadanému polynomu f.

Z předchozího vyplývá, že uvedené kroky jsou postačující k sestrojení úplné normální disjunktivní formy. Ukažme právě popsanou konstrukci na příkladě.

Příklad 11.8. Úprava polynomu na úplnou disjunktivní normální formu.
0. Uvažujme polynom $f(x, y) = [(x' \sqcap y)' \sqcap x'] \sqcup y =$
Úpravy polynomu $f(x, y)$ budeme číslovat stejně, jako tomu bylo v uvedené konstrukci.

1. $= [x'' \sqcup y') \sqcap x'] \sqcup y = [(x \sqcup y') \sqcap x'] \sqcup y =$
2. $= [(x \sqcap x') \sqcup (y' \sqcap x')] \sqcup y =$
3. $= 0 \sqcup (y' \sqcap x') \sqcup y = (y' \sqcap x') \sqcup y =$
4. $= (y' \sqcap x') \sqcup [y \sqcap (x \sqcup x')] = (y' \sqcap x') \sqcup (y \sqcap x) \sqcup (y \sqcap x') =$
5. $= (x' \sqcap y') \sqcup (x' \sqcap y) \sqcup (x \sqcap y) = m_0 \sqcup m_1 \sqcup m_3$

Na základě výše popsané konstrukce nebo na základě lemmatu 11.4 můžeme vyslovit následující větu.

Věta 11.4. *Každý Booleův polynom $f(x_1, \ldots, x_n)$ v Booleově algebře* **2** *lze vyjádřit právě jedním způsobem v úplné disjunktivní normální formě.*

Věta 11.4′. *Každý Booleův polynom $f(x_1, \ldots, x_n)$ v Booleově algebře* **2** *lze vyjádřit právě jedním způsobem v úplné konjunktivní normální formě.*

Poznámka. Uvažujme Booleovu algebru V_n všech polynomů $f(x_1, \ldots, x_n)$ v algebře **2**. Zobrazení H, které každému polynomu f přiřadí funkci F definovanou polynomem f, je homomorfismem algebry V_n na algebru A_n všech funkcí n proměnných v algebře **2**. Jádrem J homomorfismu H je ideál všech polynomů určujících nulovou funkci. Sestrojíme-li faktorovou Booleovu algebru V_n/J, pak je tato algebra izomorfní s algebrou A_n a na základě věty 11.3 a 11.3′ s algebrou P_n a Q_n. To souvisí se skutečností, že každý blok rozkladu V_n/J lze charakterizovat určitou úplnou disjunktivní či konjunktivní normální formou, na niž lze polynomy tohoto bloku upravit.

Na předchozích stránkách jsme se seznámili se dvěma způsoby, jak upravit libovolný Booleův polynom $f(x_1, \dots, x_n)$ na úplnou disjunktivní normální formu. Připomeňme oba tyto postupy. Jeden z nich označíme jako přímý a druhý jako nepřímý.

Přímá metoda:

Při této metodě upravujeme zadaný polynom tak, jak jsme vypsali v konstrukci před příkladem 11.8 a jak jsme konkrétně ukázali v příkladu 11.8. Podstatou je tedy přímá úprava zadaného polynomu na úplnou disjunktivní normální formu.

Nepřímá metoda:

Při této metodě nejprve k zadanému polynomu sestrojíme tabulku odpovídající Booleovy funkce a potom pomocí této tabulky zkonstruujeme úplnou disjunktivní normální formu. Postup při konstrukci této formy je popsán v důkaze věty 11.2 a konkrétní ukázku představuje příklad 11.7.

Obdobně lze vyslovit obě metody i pro úpravu libovolného Booleova polynomu na úplnou konjunktivní normální formu.

Na závěr článku poznamenejme, že jsme získali metodu dovolující rozhodnout o rovnosti dvou Booleových polynomů $f(x_1, \cdots, x_n)$ a $g(x_1, \cdots, x_n)$. Stačí když např. přímou metodou upravíme polynomy f a g na úplnou disjunktivní normální formu. Pokud z obou polynomů získáme tutéž formu, pak jsou si oba uvažované polynomy f a g skutečně rovny.

11.2 Minimalizace Booleových funkcí

Celá tato problematika je podstatně ovlivněna především používáním teorie Booleových algeber při konstrukcích logických obvodů, které se vyskytují v číslicových počítačích. Problematice těchto obvodů se však budeme věnovat až v následující kapitole. Nyní tuto souvislost připomínáme především proto, že od symboliky a terminologie, které jsme používali v předchozím textu, přejdeme k symbolice a terminologii, která se používá právě v aplikacích. Podrobně rozebereme **Quineovu—Mc Cluskeiovu metodu** minimalizace Booleových polynomů, která se stala východiskem pro celou řadu dalších metod, při jejichž realizaci se využívají počítače.

Úmluvy o nové symbolice a terminologii

Operaci průsek začneme nazývat **násobení** a místo symbolu $\sqcap$ budeme používat obvyklý symbol $\cdot$. Místo průsek $x \sqcap y$ budeme tedy psát $x \,.\, y$ nebo pouze xy. Operaci spojení začneme nazývat **sčítání** a místo symbolu $\sqcup$ budeme používat symbol $+$. Operaci komplement budeme nazývat **negace** a značit pruhem $^{-}$. Tabulky 12a, b představují booleovské operace $\cdot$ a $+$ v algebře **2**. Pozor! Nesmíme zaměnit operaci $+$ s operací symetrické odčítání $\oplus$ (viz tabulka 12c)), která je totožná s operací sčítání modulo 2.

Tab. 12a

$\cdot$	0	1
0	0	0
1	0	1

Tab. 12b

$+$	0	1
0	0	1
1	1	1

Tab. 12c

$\oplus$	0	1
0	0	1
1	1	0

Protože se v dalších výrazech budou vyskytovat jak proměnné, tak i jejich negace, budeme pro jejich označení používat slovo literál. Literál proto značí jak proměnnou, tak i její negaci. Příklady čtyř různých literálů jsou $x, \bar{x}, y, \bar{z}$.

Součinovým členem nebo pouze **součinem** nazveme průsek několika literálů. **Součtovým členem** nebo pouze **součtem** nazveme spojení několika literálů. Součinovými členy jsou např. $x \sqcap y \sqcap z'$ nebo $x' \sqcap y$. Součtovými členy jsou např. $x' \sqcup y \sqcup z$ nebo $x' \sqcup y \sqcup z'$. Tyto termy však budeme zapisovat po řadě $xy\bar{z}$, $\bar{x}y$, $\bar{x} + y + z$ a $\bar{x} + y + \bar{z}$.

Součtem součinových členů rozumíme spojení několika součinových členů. Příkladem součtu součinových členů jsou např. termy $(x \sqcap y \sqcap z) \sqcup (x' \sqcap y \sqcap z) \sqcup (x' \sqcap y' \sqcap z')$ nebo $(x' \sqcap y \sqcap z) \sqcup z' \sqcup (x \sqcap y)$, které budeme zapisovat: $xyz + \bar{x}yz + \bar{x}\bar{y}\bar{z}$ nebo $\bar{x}yz + \bar{z} + xy$. **Součinem součtových členů** rozumíme průsek několika součtových členů. Příkladem součinu součtových členů jsou termy $(x \sqcup y \sqcup z') \sqcap (x \sqcup y' \sqcup z') \sqcap (x' \sqcup y)$ nebo $x \sqcap (y \sqcup x \sqcup z')$, které budeme zapisovat $(x + y + \bar{z}) \,.\, (x + \bar{y} + \bar{z}) \,.\, (\bar{x} + y)$ nebo $x(y + x + \bar{z})$.

Místo úplná disjunktivní normální forma budeme říkat **úplná součtová normální forma** a místo úplná konjunktivní normální forma budeme říkat **úplná součinová normální forma.**

Vzhledem k úplné součtové normální formě f, kterou budeme v dalším textu neustále používat, zavedeme následující názvy: Každý součin (minimální polynom) v této formě budeme nazývat **mintermem** nebo **termem řádu 0.** Odstraníme-li z mintermu n literálů, pak obdržíme **term řádu** n. Např. v úplné součtové normální formě

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

jsou mintermy $\bar{x}y\bar{z}$, $xy\bar{z}$ a xyz. Z mintermu $xy\bar{z}$ lze vytvořit tři termy prvního řádu xy, $x\bar{z}$ a $y\bar{z}$ a tři termy druhého řádu $x, y, \bar{z}$. Pojmu minterm v úplné součinové formě odpovídá **maxterm.**

Zde úmluvy a zavádění nových pojmů prozatím končí.

Vyslovme základní problém tohoto článku: Je zadána určitá Booleova funkce F mající n proměnných (např. tabulkou nebo polynomem) a my máme sestrojit polynom f, který by definoval funkci F a přitom byl mezi všemi takovými polynomy co nejjednodušší. Chceme-li se touto problematikou zabývat hlouběji, musíme v první řadě vymezit pojem „být jednodušší" mezi polynomy. Existuje celá řada i neekvivalentních definic tohoto pojmu. Záleží vždy na tom, kterou vlastnost polynomu preferujeme. Uvedeme zde na ukázku dvě takové definice. Vzhledem k tomu, že se v celém článku budeme zabývat pouze polynomy majícími tvar součtu součinových členů, budou se i tato dvě kritéria vztahovat pouze k polynomům uvedeného tvaru.

Kritérium 1. Součet součinových členů f je **minimální vzhledem k počtu literálů,** právě když žádný Booleův polynom g, pro nějž platí $g = f$, neobsahuje menší počet literálů než f, přičemž počítáme i vícenásobné výskyty literálů.

Např. v polynomu $xy\bar{z} + x\bar{y}\bar{z}$ je 6 literálů, a přitom výskyt literálů x, $\bar{z}$ je dvojnásobný.

Kritérium 2. Součet součinových členů f je **minimální vzhledem k počtu součinových členů,** právě když žádný Booleův polynom g, pro nějž platí $g = f$, neobsahuje menší počet členů a pokud jich obsahuje stejně, pak neobsahuje menší počet literálů než f, přičemž počítáme i vícenásobné výskyty literálů.

Příklad: Lze dokázat např. pomocí tabulky, že polynom

$$\bar{x}yz + x\bar{y}z + xy\bar{z} + xyz \tag{11.9}$$

je roven polynomu

$$xy + yz + xz. \tag{11.10}$$

Je zřejmé, že polynom (11.10) je jednodušší než polynom (11.9), a to jak vzhledem k počtu literálů, tak i vzhledem k počtu členů. Poznamenejme, že postup zjednodušení polynomu (11.9) na polynom (11.10) ukážeme v příkladě 11.9.

Zdůrazněme, že pod pojmem minimální polynom rozumíme maximální prvek v příslušném uspořádání polynomů. Duální kritéria pro polynomy mající tvar součinu součtových členů si může čtenář vyslovit sám. Poznamenejme ještě, že jiné kritérium by se např. mohlo týkat počtu výskytu negovaných proměnných.

Přistupme k problematice minimalizace. Existuje více metod, pomocí nichž můžeme daný nepříliš složitý polynom minimalizovat. Vyjmenujme na tomto místě alespoň tři nejznámější:
- minimalizace algebraická neboli přímá,
- minimalizace pomocí Karnaughovy mapy,
- metoda Quineova—Mc Cluskeiova.

Metoda pomocí Karnaughovy mapy je pravděpodobně ze všech nejznámější a užívá se s úspěchem především u polynomů obsahujících maximálně čtyři proměnné. Dá se však použít i pro větší počet proměnných. Touto metodou se zde zabývat nebudeme. Odkazujeme čtenáře např. na knihu [5].

Minimalizace přímá je nejjednodušší prostředek pro úpravu polynomů. Tento způsob využívá pravidla pro počítání v Booleově algebře. Ukažme si příklad:

Příklad 11.9. Zjednodušme co nejvíce následující polynom:

$$xyz + xy\bar{z} + x\bar{y}z + \bar{x}yz$$

Řešení. $xyz + xy\bar{z} + x\bar{y}z + \bar{x}yz =$	zadaný polynom
$= (xyz + xy\bar{z}) + (x\bar{y}z + xyz) + (\bar{x}yz + xyz) =$	Podle (8.3′).
$= xy(z + \bar{z}) + xz(y + \bar{y}) + yz(x + \bar{x}) =$	Podle (8.5).
$= xy \,.\, 1 + xz \,.\, 1 + yz \,.\, 1 = xy + xz + yz$	Podle (8.7) a (8.6′).

Uvedená metoda je vhodná ve velmi jednoduchých případech. Jinak je dosti riskantní a úpravy nejsou vždy jednoduché. Pro více než tři proměnné se však prakticky nedá použít.

Zdůrazněme, že podstatu této metody vyjadřuje následující řetězec rovností, kde t je součin neobsahující proměnnou x ani její negaci:

$$\underline{tx + t\bar{x}} = t(x + \bar{x}) = t \,.\, 1 = \underline{t} \tag{11.11}$$

Součiny tx a $t\bar{x}$ nazýváme **sousední součiny** (termy) a dále říkáme, že součin t vznikl z jejich součtu **vykrácením** proměnné x. Z (11.11) vyplývá, že funkční hodnota součtu $tx + t\bar{x}$ vůbec nezávisí na hodnotě proměnné x. Toto zjištění budeme využívat i v následující metodě.

Hlavní pozornost budeme věnovat **metodě Quineově—Mc Cluskeiově,** která je z hlediska algebry velmi zajímavá. Při jejím popisu budeme používat binární relaci „implikovat“ mezi polynomy.

Definice 11.4. *Říkáme, že* **polynom** f_1 **implikuje polynom** f_2 *právě když neexistuje taková kombinace hodnot proměnných, pro kterou nabývá polynom* f_1 *hodnoty* 1 *a současně polynom* f_2 *hodnoty* 0.

Definici 11.4 lze formulovat také takto: polynom f_1 implikuje polynom f_2, právě když funkce F_1 definovaná polynomem f_1 předchází před funkcí F_2 definovanou polynomem f_2, tzn.

$$f_1 \text{ implikuje } f_2 \quad \Leftrightarrow \quad F_1 \trianglelefteq F_2 .$$

Příklady 11.10. Polynom $xy + \bar{x}y$ implikuje polynom $\bar{x}y + x\bar{y} + xy$. Důvodem je to, že první polynom určuje funkci F_5^2, zatímco druhý polynom určuje funkci F_7^2 (viz tabulka v příkladu 11.4) a přitom $F_5^2 \trianglelefteq F_7^2$. Také minterm $x\bar{y}$ implikuje polynom $\bar{x}y + x\bar{y} + xy$. Obdobně i mintermy $\bar{x}y$ a xy implikují tento polynom.

Zaveďme ještě tři nové pojmy a ukažme jejich důležité vlastnosti. Tyto pojmy budou prakticky ukazovat cestu, jak se od úplné součtové normální formy nějaké funkce F dostaneme k jejímu minimálnímu polynomu.

Definice 11.5. Implikantem Booleovy funkce *F se nazývá každý součin, který implikuje funkci F či přesněji, který implikuje úplnou součtovou normální formu funkce F.*

Poznamenejme, že existuje jednoduchý způsob dovolující zjistit, zda daný součin p je implikantem funkce F. Stačí, když proměnným bez pruhů přiřadíme hodnotu 1 a proměnným s pruhem hodnotu 0. Součin p pro tuto (a jenom tuto) kombinaci hodnot proměnných nabývá hodnoty 1. Pokud pro uvedenou kombinaci hodnot proměnných nabývá i funkce F hodnoty 1, pak p je implikantem funkce F.

V příkladu 11.10 jsme uvedli, že mintermy $\bar{x}y$, $x\bar{y}$ a xy jsou implikanty polynomu $\bar{x}y + x\bar{y} + xy$. Zřejmě platí obecně, že každý minterm obsažený v úplné součtové normální formě f je implikantem f (viz lemma 11.5).

Příklad 11.11. Uvažujme polynom

$$f(x, y, u, v) = \bar{x}yuv + \bar{x}yu\bar{v} + \bar{x}y\bar{u}v + \bar{x}y\bar{u}\bar{v},$$

pak implikantem tohoto polynomu je např. minterm $\bar{x}yuv$, ale také term prvního řádu $\bar{x}yv$ a také dokonce term druhého řádu $\bar{x}y$. Dokažme toto poslední tvrzení. Term $\bar{x}y$ nabývá hodnoty 1, právě když $x = 0$ a $y = 1$. Dosadíme-li tyto hodnoty do polynomu f, pak obdržíme:

$$\begin{aligned} f(0, 1, u, v) &= 1 \,.\, 1 \,.\, uv + 1 \,.\, 1 \,.\, u\bar{v} + 1 \,.\, 1 \,.\, \bar{u}v + 1 \,.\, 1 \,.\, \bar{u}\bar{v} = \\ &= u(v + \bar{v}) + \bar{u}(v + \bar{v}) = u \,.\, 1 + \bar{u} \,.\, 1 = u + \bar{u} = 1 \end{aligned}$$

Mezi všemi implikanty dané funkce F nás budou zajímat především ty nejkratší.

Definice 11.6. Implikant *p funkce F se nazývá* **prostý,** *právě když p přestane být implikantem funkce F, pokud z něho odstraníme libovolný literál neboli pokud zvýšíme jeho řád.*

Příklad 11.11 (pokračování). Uvedli jsme, že součiny $\bar{x}yuv$, $\bar{x}yv$ a $\bar{x}y$ jsou implikanty funkce F zadané polynomem f. Dokažme, že $\bar{x}y$ je prostým implikantem. Z termu druhého řádu $\bar{x}y$ lze vytvořit dva termy třetího řádu $\bar{x}$ a y. Ukážeme, že žádný z nich už není implikantem. Platí $\bar{x} = 1$, právě když $x = 0$. Proto

$$\begin{aligned} f(0, y, u, v) &= 1 \,.\, yuv + 1 \,.\, yu\bar{v} + 1 \,.\, y\bar{u}v + 1 \,.\, y\bar{u}\bar{v} = \\ &= yu(v + \bar{v}) + y\bar{u}(v + \bar{v}) = y(u + \bar{u}) = y. \end{aligned}$$

Protože y může nabývat jak hodnoty 0, tak i hodnoty 1, může i polynom f určující funkci F nabývat jak hodnoty 0, tak i hodnoty 1. Závěr: Pro $\bar{x} = 1$ může f nabývat hodnoty 0. Obdobně je tomu pro term y.

Mezi všemi součty prostých implikantů určujícími funkci F nás budou zajímat ty součty, které mají nejmenší počet členů.

Definice 11.7. Součet součinových členů *f určující funkci F se nazývá* **nezkratitelný**, *právě když platí současně:*

1. *každý součinový člen z f je prostý implikant funkce F;*
2. *vynecháme-li v polynomu f libovolný člen, pak vzniklý polynom nedefinuje funkci F.*

Nyní uvedeme několik pro nás důležitých vlastností právě zavedených pojmů. Nechť je nenulová Booleova funkce F n proměnných vyjádřena pomocí polynomu f ve tvaru součtu součinových členů. Jestliže je p libovolný součin z f, pak pro každý vektor $(v_1, v_2, \dots, v_n)$, pro nějž $p = 1$, platí, že i $f = 1$, a tedy i funkce F má hodnotu 1. Proto lze vyslovit:

Lemma 11.5. *Nechť je Booleova funkce F vyjádřena pomocí polynomu f majícího tvar součtu součinových členů a nechť p je jedním z těchto součinových členů, pak p je implikantem funkce F.*

Důsledkem lemmatu 11.5 je následující tvrzení: Jestliže je Booleova funkce F vyjádřena pomocí minimálního polynomu f majícího tvar součtu součinových členů, pak každý součin z f je implikantem funkce F.

Jestliže funkci F vyjádříme pomocí úplné součtové normální formy f a jestliže z každého mintermu polynomu f vytvoříme zvyšováním řádu prostý implikant, pak obdržíme vyjádření funkce F pomocí součtu prostých implikantů. Proto platí:

Lemma 11.6. *Libovolnou nenulovou Booleovu funkci F lze zadat alespoň jedním polynomem f, který je součtem prostých implikantů.*

Nechť $p(x_1, \dots, x_r)$ je implikantem Booleovy funkce F mající úplnou součtovou normální formu $f(x_1, \dots, x_n)$. Je zřejmé, že platí $r \leq n$. Proměnné x_{r+1} až x_n se proto vyskytují ve formě f a nevyskytují se v implikantu p. Jestliže z implikantu p vytvoříme součin

$$s(x_1, \dots, x_n) = p(x_1, \dots, x_r) \,.\, y_{r+1} \,.\, \dots \,.\, y_n, \tag{11.12}$$

kde literály y_{r+1} až y_n jsou vytvořeny po řadě z proměnných x_{r+1} až x_n, pak součin (11.12) je sčítancem ve formě f.

Zdůvodnění. Nechť doplněný součinový člen s není obsažen ve formě f. Přiřadíme-li proměnným x_1 až x_n takové hodnoty, aby $s = 1$ (to lze právě jedním způsobem), pak i implikant $p = 1$. Protože forma f neobsahuje součin s, nabývá pro tuto kombinaci hodnoty 0. To je však spor s předpokladem, že p je implikant funkce F, která má úplnou součtovou normální formu f. Závěr vyslovíme takto:

Lemma 11.7. *Jestliže je p implikantem Booleovy funkce F mající úplnou součtovou normální formu f, pak forma f obsahuje všechna možná doplnění* (11.12) *implikantu p.*

Příklad 11.12. Nechť $p = \bar{x}u$ je implikantem funkce F, která má úplnou součtovou normální formu $f(x, y, z, u)$. Pak musí forma f obsahovat všechna možná doplnění součinu p, tj.

$$\bar{x}uyz, \qquad \bar{x}uy\bar{z}, \qquad \bar{x}u\bar{y}z, \qquad \bar{x}u\bar{y}\bar{z}. \tag{11.13}$$

Poznamenejme ještě, že právě z těchto čtyř součinů obsažených v f získáme pomocí trojího použití formule (11.11), tj. pomocí trojího krácení, implikant p.

Zaveďme ještě následující relaci mezi součinovými členy.

Definice 11.8. *Říkáme, že* **součin** s_1 **pokrývá součin** s_2, *právě když každý literál, který se vyskytuje v* s_1, *vyskytuje se i v* s_2.

Poznamenejme, že relace „pokrývat" zavedená definicí 11.8 je reflexívní, antisymetrická a tranzitivní*). Je to tedy uspořádání na množině součinů. Budeme-li tuto relaci uvažovat pouze na množině součinů, pomocí nichž může být vyjádřena daná funkce F (ve tvaru součtu součinů), pak minimálními prvky zavedeného posetu jsou mintermy a maximálními prvky jsou prosté implikanty.

Příklad 11.12 (pokračování). Součin $p = \bar{x}u$ pokrývá každý z mintermů (11.13).

Vraťme se k definici 11.6. Je zřejmé, že pokud je polynom minimální (podle kteréhokoli z uvedených kritérií), pak je nezkratitelný. Obrácené tvrzení však neplatí. Můžeme říci pouze toto: Jestliže je zkonstruovaná množina všech nezkratitelných polynomů dané funkce F, pak jsou v této množině obsaženy všechny minimální polynomy. Jestliže chceme sestrojit libovolný nezkratitelný polynom funkce F, pak musíme v první řadě sestrojit množinu všech prostých implikantů a potom z ní vybrat takovou podmnožinu, aby jejím součtem vznikl nezkratitelný polynom.

Nyní máme připraveno vše k tomu, abychom popsali konstrukci minimálních polynomů funkce F.

Konstrukce minimálního polynomu Booleovy funkce F.

0. Nechť F je Booleova funkce (zadaná např. pomocí tabulky nebo pomocí formule).
1. Sestrojíme úplnou součtovou normální formu f odpovídající funkci F.
2. Sestrojíme množinu všech prostých implikantů funkce F.
3. Sestrojíme množinu M všech nezkratitelných polynomů funkce F.
4. Z množiny M vybereme všechny polynomy splňující dané kritérium minimálnosti.

---

*) Uvažovanou relaci nazýváme tak, jak je to v technické literatuře zvykem. Jde však o relaci různou od relace zavedené v definici 1.8.

Nechť je zadána Booleova funkce F, pak podle bodu 1. konstrukce sestrojíme nejprve její úplnou součtovou normální formu f. Použít k tomu můžeme buď přímou, nebo nepřímou metodu uvedenou na konci článku 11.1.

Nyní přistoupíme k bodu 2. konstrukce a popíšeme, jak z formy f získáme všechny prosté implikanty funkce F. Podstatou postupu je neustálé **krácení** sousedních součinů, tj. používání formule

$$t \,.\, x + t \,.\, \bar{x} = t. \tag{11.14}$$

Nejprve vykrátíme všechny možné dvojice sousedních mintermů (liší se v právě jednom literálu). Tím získáme termy 1. řádu. Potom vykrátíme všechny možné dvojice sousedních termů 1. řádu. Tím obdržíme termy 2. řádu atd. Součin p, který při tomto postupu pokryjeme kratším součinem, nemůže být prostým implikantem. Prostým implikantem je proto každý takový součin, který už nelze pokrýt dalším součinem. Abychom získali dobrý přehled, můžeme oba krácené sousední součiny označit hvězdičkou. Prostými implikanty jsou pak neoznačené součiny. Popsaný postup nejlépe osvětlí konkrétní příklad.

Příklad 11.13. Určeme všechny prosté implikanty funkce F, mající následující úplnou součtovou normální formu:

$$\begin{aligned} f &= \bar{x}yz\bar{u} + \bar{x}yzu + x\bar{y}\bar{z}u + x\bar{y}zu + xy\bar{z}u + xyzu = \\ &= m_6 + m_7 + m_9 + m_{11} + m_{13} + m_{15} \end{aligned}$$

Vykrácením m_6 a m_7 obdržíme $\bar{x}yz$, m_7 a m_{15} obdržíme yzu, m_9 a m_{11} obdržíme $x\bar{y}u$ atd. Zapíšeme-li mintermy do prvního sloupce, termy 1. řádu získané krácením do druhého sloupce a termy 2. řádu získané krácením termů druhého sloupce do třetího sloupce, obdržíme:

$\bar{x}yz\bar{u}$ *	$\bar{x}yz$	xu
$\bar{x}yzu$ *	yzu	xu
$x\bar{y}\bar{z}u$ *	$x\bar{y}u$ *	
$x\bar{y}zu$ *	$x\bar{z}u$ *	
$xy\bar{z}u$ *	xzu *	
$xyzu$ *	xyu *	

Neoznačené zůstaly pouze součiny $\bar{x}yz$, yzu a xu, a proto jsou tyto součiny prostými implikanty funkce F.

Postup, který jsme demonstrovali v příkladě 11.13, je možné zdokonalit tak, že nebudeme pracovat přímo se součiny z polynomu f, ale s dvojkovými čísly, která těmto součinům odpovídají. Původní metodu vymyslel Quine a její zdokonalení (vzhledem k použití počítačů) navrhl Mc Cluskei. Postup rozdělíme do několika kroků.

2a) Ve všech mintermech uspořádáme proměnné stejně a potom každému součinu přiřadíme dvojkové číslo (místo x_i píšeme 1 a místo $\bar{x}_i$ píšeme 0). Každému tomuto číslu dále přiřadíme jednak **index termu,** což je počet jedniček v dvojkovém zápisu, a dále **stavový index,** což je desítkový zápis tohoto dvojkového čísla (tzn. index i v zápise m_i). Poznamenejme, že stavový index pro minterm n proměnných může být nejvýše roven číslu $2^n - 1$.

Příklad 11.13 (pokračování). Ukažme pomocí tabulky 13, jak bude vypadat krok 2a) v případě formy f:

Minterm	Dvojkové číslo	Index termu	Stavový index
$\bar{x}yz\bar{u}$	0110	2	6
$\bar{x}yzu$	0111	3	7
$x\bar{y}\bar{z}u$	1001	2	9
$x\bar{y}zu$	1011	3	11
$xy\bar{z}u$	1101	3	13
$xyzu$	1111	4	15

Tab. 13

2b) Zápis pomocí dvojkových čísel upravíme takto: Vytvoříme skupiny dvojkových čísel se stejným indexem termu, tzn. se stejným počtem jedniček. Tyto skupiny mezi sebou uspořádáme (shora dolů) podle vzrůstajícího indexu termu. Jednotlivé skupiny od sebe oddělíme vodorovnou čárou (viz první sloupec tabulky 14).

2c) Nyní přistoupíme ke krácení dvojkových čísel. Abychom toto krácení mohli lépe popsat, připíšeme před každé dvojkové číslo i jeho stavový index. Porovnávat lze pouze čísla ze sousedních skupin. Jestliže se porovnávaná čísla liší právě v jedné dvojkové číslici (na stejném místě), zkrátíme je, označíme a nahradíme číslem novým, které zapíšeme do dalšího sloupce i se stavovými indexy obou krácených čísel. Zkrácenou číslici nahradíme pomlčkou (-), aby i nadále zůstalo zachováno původní přiřazení dvojkových číslic a literálů.

Příklad 11.13 (pokračování). Abychom při porovnávání dvojkových čísel na žádnou dvojici nezapomněli, vypíšeme je pomocí stavových indexů:
6,7; 6,11; 6,13; 9,7; 9,11; 9,13; 7,15; 11,15; 13,15
Krácení zapíšeme pomocí tabulky 14.

Mintermy	Termy 1. řádu	Termy 2. řádu
6 0110 *	6,7 011-	9, 11, 13, 15 1--1
9 1001 *	9,11 10-1 *	9, 13, 11, 15 1--1
7 0111 *	9,13 1-01 *	
11 1011 *	7,15 -111	
13 1101 *	11,15 1-11 *	
15 1111 *	13,15 11-1 *	

Tab. 14

Neoznačená zůstala čísla 011–, –111 a 1– –1. Těm odpovídají prosté implikanty $\bar{x}yz$, yzu a xu.

Zdůrazněme, že krátit můžeme pouze taková čísla, která mají stejný počet pomlček na stejných místech a jejichž dvojkové číslice se liší právě na jednom místě. Tím je konstrukce prostých implikantů ukončena.

3. Přistupme ke konstrukci nezkratitelných polynomů. Z množiny prostých implikantů zkonstruované v bodě 2 c) je třeba vybrat takové podmnožiny, aby jejich součet definoval původní funkci F a přitom aby byl nezkratitelný. Tuto problematiku budeme řešit pomocí **mřížky prostých implikantů.**

3a) Mřížku prostých implikantů sestrojíme tak, že do vodorovného záhlaví vypíšeme stavové indexy odpovídající všem mintermům a do svislého záhlaví vypíšeme dvojková čísla odpovídající prostým implikantům získaným v bodě 2c). Skutečnost, že prostý implikant p pokrývá určitý minterm, vyznačíme křížkem v příslušném políčku.

Příklad 11.13 (pokračování). Vyznačme pro porovnání mřížku prostých implikantů dvojím způsobem:

a) pomocí součinů v tabulce 15

Tab. 15

	$\bar{x}yz\bar{u}$	$\bar{x}yzu$	$x\bar{y}\bar{z}u$	$x\bar{y}zu$	$xy\bar{z}u$	$xyzu$
$\bar{x}yz$	×	×				
yzu		×				×
xu			×	×	×	×

b) pomocí dvojkových čísel a stavových indexů v tabulce 16

Tab. 16

	6	7	9	11	13	15
011–	×	×				
–111		×				×
1– –1			×	×	×	×

3b) Nyní je třeba nalézt takové co nejmenší množiny prostých implikantů, aby každý minterm z f byl pokrytý některým z těchto implikantů. Z hlediska mřížky to znamená, že musíme nalézt vždy takovou co nejmenší množinu řádků, aby v každém sloupci byl alespoň jeden křížek.

Je zřejmé, že pokud některý sloupec obsahuje jen jeden křížek, pak prostý implikant označující řádek tohoto křížku musí patřit do každého výběru prostých implikantů. Těmto prostým implikantům říkáme **podstatné implikanty** a množina všech podstatných implikantů tvoří tzv. **jádro.**

V případě, že podstatné implikanty z jádra pokrývají všechny mintermy z f, je jejich součtem minimální polynom (podle obou kritérií), čímž je vyřešen i bod 4 konstrukce.

Příklad 11.13 (pokračování). Jádro tvoří dvojková čísla 011– (v prvním sloupci je jediný křížek) a 1––1 (ve třetím, čtvrtém a pátém sloupci je jediný křížek). Těmto číslům odpovídají prosté implikanty $\bar{x}yz$ a xu. Protože tyto dva podstatné implikanty pokrývají všechny mintermy z f, platí, že minimálním polynomem funkce F je polynom

$$\bar{x}yz + xu.$$

Obecně však prvky z jádra nemusí pokrývat všechny mintermy z f. V tom případě je třeba při konstrukci nezkratitelných polynomů přidat k jádru ještě další prosté implikanty a to tak, abychom vždy „co nejúsporněji" pokryli všechny mintermy z f.

Příklad 11.14. Sestrojme všechny nezkratitelné polynomy funkce F, jejíž mřížka prostých implikantů je v tabulce 17.

Tab. 17

	6	7	10	11	14
011–	×	×			
–110	×				×
101–			×	×	
1–10			×		×

Do jádra náleží zřejmě součiny odpovídající dvojkovým číslům 011– a 101–, tzn. $\bar{x}yz$ a $x\bar{y}z$. Abychom však pokryli všechny mintermy formy f, musíme k jádru přidat buď prostý implikant $yz\bar{u}$ (odpovídá číslu –110), nebo prostý implikant $xz\bar{u}$ (odpovídá číslu 1–10). Nezkratitelnými polynomy funkce F jsou v tomto případě

$$\bar{x}yz + x\bar{y}z + yz\bar{u} \quad \text{a} \quad \bar{x}yz + x\bar{y}z + xz\bar{u}. \tag{11.15}$$

4. Jestliže porovnáme nezkratitelné polynomy získané v bodě 3c) konstrukce pomocí příslušného kritéria minimálnosti, pak získáme hledané minimální polynomy splňující dané kritérium.

Příklad 11.14 (pokračování). Booleova funkce F má dva nezkratitelné polynomy (viz (11.15)), přičemž jsou oba minimální podle obou výše uvedených kritérií.

V závěru tohoto článku načrtneme ve formě poznámek některé další problémy minimalizace ve spojení s technickou praxí, i když o logických obvodech budeme pojednávat až v další kapitole.

Poznámka o neurčených stavech funkce. V praxi se setkáváme s tím, že pro některé vektory z definičního oboru Booleovy funkce není určena funkční hodnota. Těmto stavům říkáme **neurčité stavy** a budeme je označovat symbolem „x“. V technické realizaci to znamená, že se buď příslušný vektor z definičního oboru vůbec nevyskytuje, nebo že jeho přítomnost nikterak neovlivní funkční správnost obvodu. Jinými slovy: neurčitý stav x je možné nahradit podle potřeby buď hodnotou 1, nebo hodnotou 0. Tuto skutečnost lze dobře využít právě při minimalizaci, což ukážeme na příkladě. Z matematického hlediska to znamená, že začínáme uvažovat „ne úplně“ zadané Booleovy funkce. Tyto funkce však můžeme vzhledem k naší problematice vhodně dodefinovat na „úplně“ zadané Booleovy funkce.

Při minimalizaci jsme vycházeli z mintermů obsažených v úplné součtové normální formě. Nahradíme-li neurčitý stav „x“ hodnotou 1, pak se zvýší počet výchozích mintermů. Tím se ale rozšiřuje i možnost zvýšení řádu prostých implikantů a současně snížení počtu těchto implikantů potřebných k pokrytí všech mintermů. Zdůrazněme, že dodatečně přibrané mintermy (tj. mintermy získané nahrazením stavu x hodnotou 1) nemusíme pokrývat. Ukažme problematiku na příkladě.

Příklad 11.15. Uvažujme funkci F tří proměnných zadanou tabulkou 18.

Tab. 18

	x	y	z	$F(xyz)$
0	0	0	0	0
1	0	0	1	x
2	0	1	0	1
3	0	1	1	1
4	1	0	0	1
5	1	0	1	1
6	1	1	0	1
7	1	1	1	x

Sestrojíme minimální polynom tak, jak jsme uvedli při popisu Quineovy—Mc Cluskeiovi metody:

1. $f = \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}\bar{z} + x\bar{y}z + xy\bar{z} =$
$= m_2 + m_3 + m_4 + m_5 + m_6$

2. Tab. 19

Mintermy	Termy 1. řádu
2 010 *	2,3 01–
4 100 *	2,6 –10
3 011 *	4,5 10–
5 101 *	4,6 1–0
6 110 *	

3. Tab. 20

	2	3	4	5	6
01–	×	×			
–10	×				×
10–			×	×	
1–0			×		×

4. Minimálními polynomy funkce F jsou:

$$f_1 = \bar{x}y + x\bar{y} + y\bar{z} \qquad \text{nebo} \qquad f_2 = \bar{x}y + x\bar{y} + x\bar{z}$$

Provedeme-li minimalizaci tak, jak jsme uvedli v předchozí poznámce, tzn. nahradíme-li neurčité stavy x v druhém a osmém řádku tabulky hodnotou 1, obdržíme:

1. $f' = \bar{x}\bar{y}z + \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}\bar{z} + x\bar{y}z + xy\bar{z} + xyz =$
$= m_1 + m_2 + m_3 + m_4 + m_5 + m_6 + m_7$

Tab. 21

2.

Mintermy	Termy 1. řádu	Termy 2. řádu
1 001 *	1,3 0-1 *	1, 5, 3, 7 --1
2 010 *	1,5 -01 *	2, 6, 3, 7 -1-
4 100 *	2,3 01- *	1, 3, 5, 7 --1
3 011 *	2,6 -10 *	4, 6, 5, 7 1--
5 101 *	4,5 10- *	2, 3, 6, 7 -1-
6 110 *	4,6 1-0 *	4, 5, 6, 7 1--
7 111 *	3,7 -11 *	
	5,7 1-1 *	
	6,7 11- *	

Tab. 22

3.

	1	2	3	4	5	6	7
--1	×		×		×		×
-1-		×	×			×	×
1--				×	×	×	×

4. Minimálním polynomem funkce F je $f_3 = y + x$ (není třeba pokrýt m_1).

Pokud jsme při minimalizaci využili i stavy x, pak jsme získali minimální polynom, který je jednodušší (podle obou kritérií) než polynomy f_1, f_2 sestrojené obvyklou metodou minimalizace.

Poznámka o minimalizaci souboru Booleových funkcí. Dosud jsme se zabývali minimalizací jedné Booleovy funkce. V praxi však existují logické obvody mající více výstupů, přičemž množina vstupů je stejná. Nechť je vstupů n a výstupů m, pak z matematického hlediska studujeme zobrazení Z: $\mathbf{2}^n \to \mathbf{2}^m$. Toto zobrazení však můžeme považovat za m samostatných Booleových funkcí F: $\mathbf{2}^n \to \mathbf{2}$.

Minimalizaci uvedeného souboru funkcí lze provést tak, že minimalizujeme každou z těchto funkcí zvlášť. Výsledné řešení však může být značně neekonomické, neboť v množinách prostých implikantů jednotlivých funkcí se mohou některé implikanty opakovat. Takovýmto implikantům říkáme **skupinové implikanty**.

Základní princip metody minimalizace souboru logických funkcí spočívá v tom, že zkonstruujeme nejen množiny prostých implikantů jednotlivých funkcí, ale také prosté skupinové implikanty všech dvojic, trojic atd. funkcí. Z těchto všech implikantů se pak vyhledá minimální množina. Je zřejmé, že při pokrývání množiny mintermů výchozích funkcí mají přednost skupinové implikanty.

Poznámka o dalších metodách minimalizace. Quineovou—Mc Cluskeiovou metodou lze při ručním zpracování minimalizovat úplné součtové normální formy mající osm až deset proměnných. Při použití počítačů lze počet proměnných zvýšit až na několik desítek. Přesto se však od poloviny sedmdesátých let a zvláště pak v osmdesátých letech objevují snahy vytvořit nové metody minimalizace. Šlo především o to, aby zjednodušením algoritmu obsaženého v Quineově—Mc Cluskeiově metodě byla snížena náročnost na čas a paměť počítače. A tak se objevily další metody, které dávají prakticky stejně dobré výsledky jako uvedená metoda a které jsou časově i paměťově méně náročné. Jmenujme zde pro zajímavost tyto metody: MINI, PRESTO, PRONTO a CAMP.

CVIČENÍ 11

1 Uvažujme množinu A_1 všech Booleových funkcí F_i^1 jedné proměnné v Booleově algebře **2**. Sestrojte tabulky operací $\sqcap$, $\sqcup$ a $'$ v množině A_1 a dále Hasseův diagram uspořádání $\trianglelefteq$ v této množině.

2 Určete počet všech funkcí jedné proměnné, dvou proměnných, tří proměnných a n proměnných v algebře **2**.

3 Sestrojte úplnou disjunktivní normální formu funkcí F_1^2, F_6^2, F_{13}^2 a F_{15}^2 (viz př. 11.4). Jak vypadá tato forma pro funkci F_0^2? K těmto funkcím sestrojte také úplnou konjunktivní normální formu.

4 Sestrojte tabulky Booleových funkcí tří proměnných x, y, z zadaných následujícími úplnými disjunktivními normálními formami:

$(x \sqcap y \sqcap z) \sqcup (x' \sqcap y \sqcap z)$

$(x \sqcap y \sqcap z') \sqcup (x \sqcap y' \sqcap z) \sqcup (x \sqcap y' \sqcap z') \sqcup (x' \sqcap y \sqcap z') \sqcup (x' \sqcap y' \sqcap z')$

$(x \sqcap y \sqcap z) \sqcup (x' \sqcap y \sqcap z) \sqcup (x' \sqcap y' \sqcap z')$

5 K funkcím ze cv. 4 sestrojte úplné konjunktivní normální formy.

6 Sestrojte úplnou disjunktivní normální formu funkcí tří proměnných zadaných následujícími polynomy:

$x \sqcup (x \sqcap y')' \sqcup x \sqcap y \sqcap z'$

$(x \sqcap y \sqcap z)' \sqcap (x \sqcup y') \sqcap (x \sqcup z)' \sqcup z$

$[(x \sqcup y) \sqcap (x \sqcup z)]' \sqcup [(x \sqcup z)' \sqcap (x \sqcup y')]$

7 Dokažte, že libovolné dva různé minimální polynomy p_1, p_2 proměnných $x_1, \dots, x_n$ jsou disjunktní, tzn. $p_1 \sqcap p_2 = 0$. Návod: různé minimální polynomy se musí lišit alespoň v jedné proměnné x_i (v jednom je x_i a v druhém x_i'). Sestrojte průsek $p_1 \sqcap p_2$ a přitom využijte výše uvedené zjištění.

8 Dokažte, že množina P_n všech polynomů n proměnných majících úplnou disjunktivní normální formu je uzavřená vzhledem k operacím $\sqcap$, $\sqcup$ a $'$.

9 Odůvodněte, proč lze libovolnou Booleovu funkci jedné proměnné F_i^1 v algebře **2** vyjádřit formulí
$y = (F_i^1(0) \sqcap x') \sqcup (F_i^1(1) \sqcap x)$.

10 Odůvodněte, proč lze libovolnou Booleovu funkci dvou proměnných F_i^2 v algebře **2** vyjádřit formulí
$z = (F_i^2(00) \sqcap x' \sqcap y') \sqcup (F_i^2(01) \sqcap x' \sqcap y) \sqcup (F_i^2(10) \sqcap x \sqcap y') \sqcup$
$\sqcup (F_i^2(11) \sqcap x \sqcap y)$.

11 Na základě cvičení 9 a 10 napište formuli pro vyjádření libovolné funkce n proměnných F_i^n v algebře **2**.

12 Sestrojte důkaz věty 11.2 tak, aby vedl k úplné konjunktivní normální formě.

13 Zdůvodněte přímou konstrukci úplné disjunktivní normální formy polynomu $f(x_1, \dots, x_n)$ v algebře **2**.

14 Vyslovte kritéria minimálnosti pro polynomy mající tvar součinu součtových členů.

15 Popište konstrukci minimálních polynomů majících tvar součinu součtových členů.

16 Sestrojte všechny minimální polynomy pro funkce tří proměnných, které jsou uvedeny v tabulce 23.

Tab. 23.

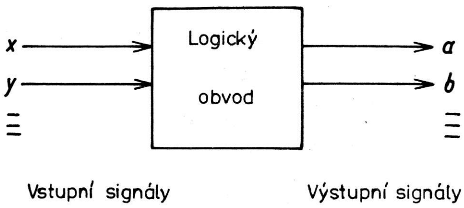
	x	y	z	F_1	F_2	F_3
0	0	0	0	1	1	0
1	0	0	1	0	1	0
2	0	1	0	0	0	1
3	0	1	1	0	0	1
4	1	0	0	1	1	0
5	1	0	1	1	1	0
6	1	1	0	1	0	1
7	1	1	1	1	1	0

17 Sestrojte minimální polynomy pro funkce čtyř proměnných zadané následujícími formulemi:
a) $f_1 = (\overline{xy} + zux)(x + u)$
b) $f_2 = (x + yu + yv)(y + u + \bar{x}y)\bar{y}$
c) $f_3 = \overline{x\bar{y}} + xy\bar{u} + x\bar{y}u + \overline{(xy + \bar{x}\bar{y}\bar{z}\bar{u})}\,\bar{y}$

12 LOGICKÉ OBVODY

V této kapitole se budeme zabývat použitím Booleových algeber při konstrukci určitých logických obvodů.

Hlavní a nejdůležitější součástí nejrůznějších logických automatů je logický obvod. **Logický obvod** přetváří vstupní signály ve výstupní signály podle žádané činnosti zařízení (viz obr. 64). Všechny uvedené signály nabývají pouze dvou hodnot, které budeme označovat 0 a 1. Tyto hodnoty signálu však nijak přímo nesouvisí se skutečnou fyzikální hodnotou signálu. Speciálním případem logických obvodů jsou tzv. **kombinační logické obvody,** jejichž výstupní signály jsou jednoznačně určeny kombinací současně působících vstupních signálů. Těmito obvody se budeme v další části zabývat.

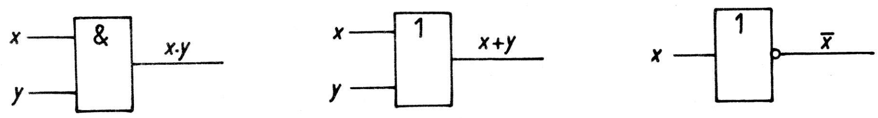


Obr. 64

Obvod mající n vstupů a m výstupů představuje zobrazení Z: $\mathbf{2}^n \to \mathbf{2}^m$. V další části pojednáme pouze o obvodech s n vstupy a jedním výstupem. Každý takový obvod představuje Booleovu funkci F: $\mathbf{2}^n \to \mathbf{2}$. Výše uvedené zobrazení Z lze pak chápat jako m samostatných Booleových funkcí n proměnných. Z předchozího textu víme, že při n vstupech můžeme vytvořit celkem 2^n různých kombinací vstupních signálů, a proto existuje přesně $2^{(2^n)}$ různých Booleových funkcí F: $\mathbf{2}^n \to \mathbf{2}$. Také víme, že všechny tyto funkce lze popsat pomocí Booleových polynomů.

12.1 Systém logický součin, logický součet, negace

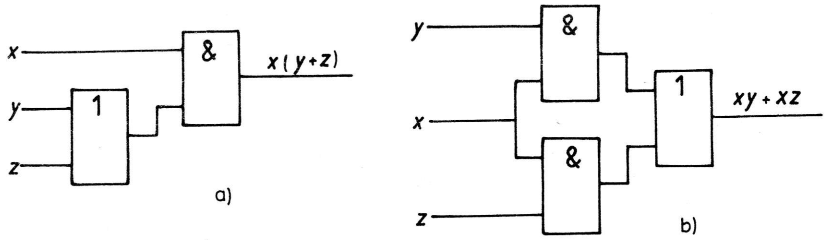
Logické obvody, o nichž budeme pojednávat, jsou vlastně fyzikální realizací Booleových funkcí. Tyto funkce, jak jsme již uvedli, lze definovat pomocí polynomů, v nichž se vyskytují pouze symboly základních Booleových operací součin, součet a negace*). Abychom mohli sestavit libovolný logický obvod, budeme muset zvládnout realizaci těchto základních booleovských operací. Proto musíme mít k dispozici základní stavební prvky (viz obr. 65), které realizují po řadě logický součin, logický součet a negaci. Fyzikální podstatou těchto stavebních částí, kterým se říká **logické členy** nebo také **hradla,** se nebudeme zabývat.



Obr. 65

Schématům, která znázorňují logické obvody, budeme říkat **logické sítě** (viz např. obr. 66). Jsou to vlastně ohodnocené grafy, jejichž hrany reprezentují elektrické vodiče a jejichž uzly jsou logické členy.

Dva logické obvody nazveme **funkčně ekvivalentní,** právě když realizují stejnou Booleovu funkci. Protože Booleovy algebry jsou distributivní, jsou např. obvody znázorněné na obr. 66 funkčně ekvivalentní. Obvod na obr. 66a realizuje funkci zadanou polynomem $x \,.\, (y + z)$, zatímco obvod na obr. 66b realizuje tutéž funkci, ale tentokráte zadanou polynomem $x \,.\, y + x \,.\, z$.



Obr. 66

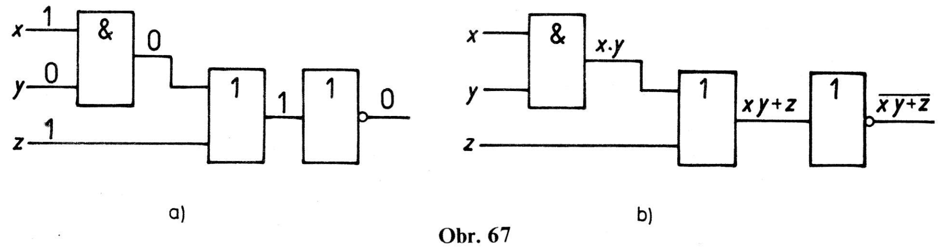
Obraťme pozornost k **analýze** nebo jinak řečeno k logické simulaci logických obvodů. Nechť je z logických členů sestaven určitý logický obvod. Úloha zní: Určete Booleovu funkci F, kterou tento obvod realizuje.

Jeden možný způsob určení funkce F spočívá v tom, že budeme postupně volit všechny možné kombinace hodnot na vstupech a podle vlastností logických členů doplníme hodnoty na jejich výstupech až k výsledné hodnotě výstupu z logického obvodu. Tak můžeme sestrojit tabulku funkce F.

---

*) Protože Booleovy algebry úzce souvisí s logikou, nazývá se někdy navrhování logického obvodu pro počítač navrhováním logiky počítače. Proto se používá i terminologie užívaná v logice. Logické členy znázorněné na obr. 65 se např. často nazývají: člen a, člen nebo a člen ne (anglicky: and, or, not).

Příklad 12.1. Na obr. 67a je znázorněn určitý logický obvod se třemi vstupy. Jestliže na vstupech x, y, z budou po řadě hodnoty 1, 0, 1, pak na výstupu z logického obvodu bude hodnota 0. Booleova funkce, kterou tento logický obvod realizuje, proto přiřazuje vektoru (1, 0, 1) funkční hodnotu 0. Obdobně bychom mohli určit funkční hodnoty i v sedmi zbylých případech, a tak sestrojit tabulku funkce F, kterou obvod realizuje.



Obr. 67

Druhá metoda určení Booleovy funkce F je mnohem efektivnější. Při postupném procházení obvodem od vstupů k výstupu nebudeme pracovat s konkrétními hodnotami proměnných, ale přímo s proměnnými nebo s termy, které jsou z těchto proměnných vytvořeny. U výstupu z obvodu pak obdržíme polynom odpovídající hledané Booleově funkci. Tento polynom můžeme ještě upravit a bude-li to potřeba, sestrojit na jeho základě tabulku funkce F.

Příklad 12.1 (pokračování). Určeme Booleovu funkci F, která je realizována logickým obvodem znázorněným na obr. 67b. Postup určení polynomu pro funkci F jsme vepsali přímo do logické sítě. Je vidět, že uvažovaný logický obvod lze popsat formulí $f(x, y, z) = \overline{xy + z}$.

Nyní se budeme zabývat problematikou **syntézy** logických obvodů. Jde o úlohu opačnou k té, kterou jsme řešili v předchozí části. Nechť je zadána Booleova funkce F. Máme sestrojit logický obvod, který funkci F realizuje.

Postupovat můžeme např. takto: Pokud není funkce F zadána tabulkou, pak tuto tabulku sestavíme. Pomocí tabulky vytvoříme úplnou součtovou normální formu funkce F (viz nepřímá metoda uvedená na konci kap. 10). K této formě pak sestrojíme logickou síť. Problematiku ukážeme na příkladě.

Příklad 12.2. Sestrojme logickou síť odpovídající Booleově funkci F tří proměnných zadané tabulkou 24.

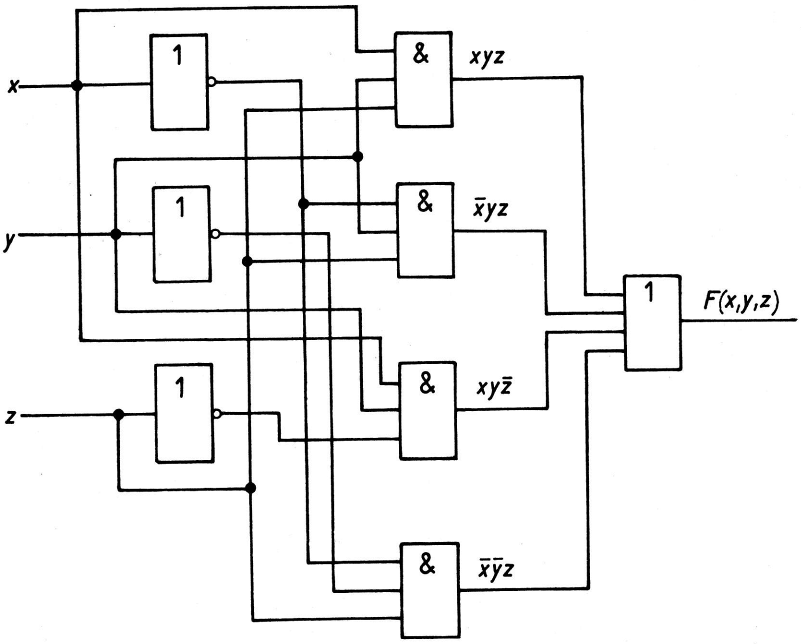
Úplná součtová normální forma funkce F je

$$\begin{aligned} f &= \bar{x}\bar{y}z + \bar{x}yz + xy\bar{z} + xyz = \\ &= m_1 + m_3 + m_6 + m_7 . \end{aligned} \tag{12.1}$$

Logická síť je znázorněná na obr. 68a.

Tab. 24

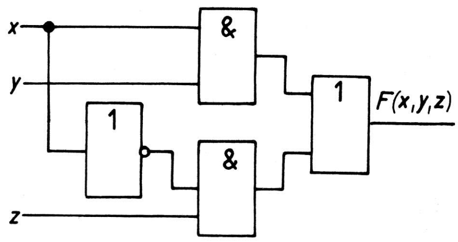
	x	y	z	$F(x, y, z)$
0	0	0	0	0
1	0	0	1	1
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	0
6	1	1	0	1
7	1	1	1	1



Obr. 68a

Logický obvod uvedený v příkladě 12.2 zřejmě není nejekonomičtější pro danou funkci F a tak obvykle dříve, než určitý logický obvod sestrojíme, provedeme minimalizaci příslušné úplné součtové normální formy např. metodou Quineo-vou—Mc Cluskeiovou (viz článek 11.2).

Příklad 12.2 (pokračování). Pokud budeme polynom (12.1) minimalizovat, obdržíme polynom $f_1 = xy + \bar{x}z$. Logický obvod odpovídající tomuto polynomu je znázorněn na obr. 68b. Logické obvody vyznačené na obr. 68a, b tedy realizují stejnou Booleovu funkci a jsou proto funkčně ekvivalentní. Obvod na obr. 68b je však zřejmě ekonomičtější.



Obr. 68b

Poznamenejme, že logickou síť libovolné Booleovy funkce zadané ve tvaru součtu součinových členů „lze načrtnout" tak, aby logické členy byly ve třech sloupcích. V posledním sloupci je člen realizující součet a počet jeho vstupů odpovídá počtu součinů. V prostředním sloupci jsou členy, které realizují součiny, a v prvním sloupci jsou členy realizující negování (viz obr. 68). Takovým logickým obvodům se říká **dvoustupňové logické obvody *AND—OR*** (neuvažujeme tvoření negací vstupních proměnných) *).

12.2 Další logické systémy

První logické systémy odvozené z teorie Booleových algeber byly skutečně založené na třech logických členech realizujících logické násobení, logické sčítání a negaci. Na základě formulí (8.15) a (8.15′), které jsou bezprostředními důsledky de Morganových pravidel, však víme, že počet základních operací lze zredukovat na dvě. Uvedené formule v naší nové symbolice zapíšeme takto:

$$(\forall x, y)\; x \,.\, y = \overline{\bar{x} + \bar{y}} \tag{12.2}$$

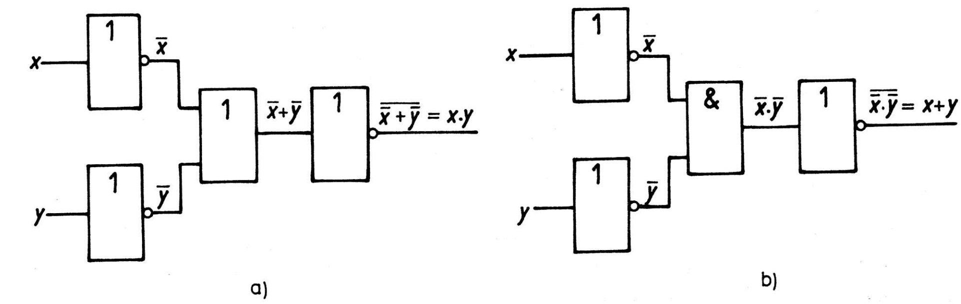
$$(\forall x, y)\; x + y = \overline{\bar{x} \,.\, \bar{y}} \tag{12.2'}$$

Z libovolného Booleova polynomu, v němž se mohou vyskytovat všechny základní booleovské operace, lze pomocí těchto formulí vytvořit polynomy, které jsou jim rovny a které obsahují pouze dvě z těchto operací: + a ¯ nebo · a ¯. Tato skutečnost byla také brzy využita při tvorbě dalších logických systémů.

---

*) Ve dvoustupňovém obvodu projde vstupní signál nejvýše dvěma logickými členy (neuvažujeme člen ne), než dosáhne výstupu. Protože na každém členu dojde k určitému zpoždění signálu, je rychlost obvodu nepřímo úměrná počtu stupňů. Dvoustupňové obvody mají tedy výhodu, že jsou poměrně rychlé.

Máme-li při konstrukci logického obvodu k dispozici pouze logické členy realizující sčítání a negování, lze logický součin vyjádřit způsobem, který ukazuje síť na obr. 69a. Máme-li při konstrukci logického obvodu k dispozici logické členy realizující násobení a negování, lze logický součet vyjádřit způsobem, který ukazuje síť na obr. 69b. Je bezprostředně vidět, že při konstrukci uvedených logických sítí využíváme formule (12.2) a (12.2′).



Obr. 69

Vedle původního logického systému majícího tři základní logické členy realizující logické násobení, sčítání a negování, kterému se říká **úplný systém logických funkcí,** tak existují i logické systémy mající pouze dva základní členy realizující buď násobení a negování, nebo sčítání a negování. Tyto systémy patří mezi tzv. **minimální úplné systémy logických funkcí.** Konstruktéři logických obvodů však poměrně rychle zmenšili počet základních členů až na jeden. Tomu se samozřejmě přizpůsobili i výrobci.

Víme již, že existuje dvojice univerzálních operací taková (viz formule (8.28) a (8.28′)), že pomocí každé z nich lze vyjádřit libovolnou Booleovu funkci. Jsou to **operace Shefferova** a **Pierceova.** V naší současné symbolice lze tyto operace popsat pomocí následujících formulí:

$$(\forall x, y)\ x \uparrow y = \overline{x \cdot y} = \bar{x} + \bar{y} \qquad \text{Shefferova operace} \quad (12.3)$$

$$(\forall x, y)\ x \downarrow y = \overline{x + y} = \bar{x} \cdot \bar{y} \qquad \text{Pierceova operace} \quad (12.3')$$

Těmto operacím odpovídá tabulka 25.

Tab. 25

x	y	$x \uparrow y$	$x \downarrow y$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

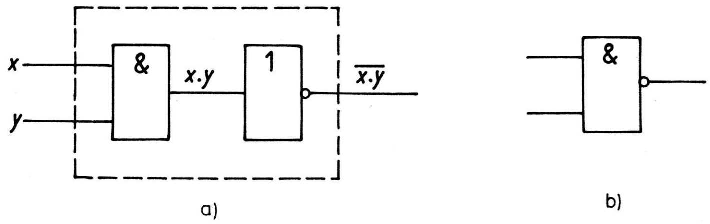
Chceme-li dokázat, že tyto operace jsou skutečně univerzální, stačí ukázat, jak pomocí každé z nich zavést negaci a jednu z operací · nebo +. Zmíněné definice lze formulovat takto (pro libovolné x, y):

$$\bar{x} = x \uparrow x \qquad \text{a} \qquad x + y = \bar{x} \uparrow \bar{y}$$

$$\bar{x} = x \downarrow y \qquad \text{a} \qquad x \,.\, y = \bar{x} \downarrow \bar{y}$$

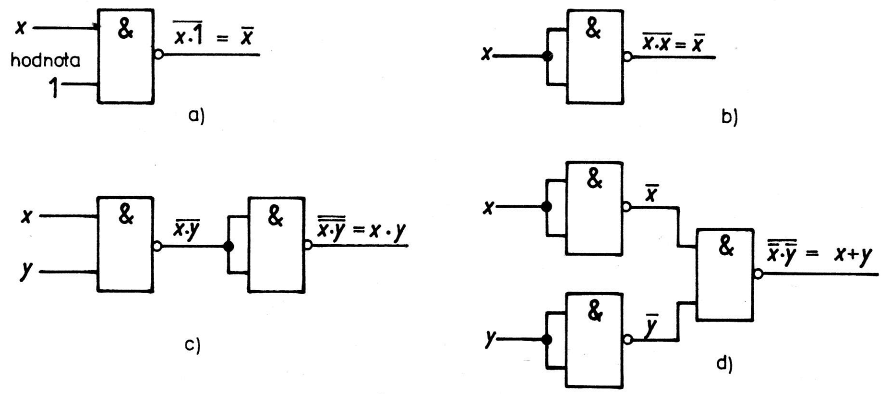
Logický člen, který realizuje Shefferovu operaci, se nazývá NAND (spojení anglických slov Not AND — česky: ne a) a logický člen, který realizuje Pierceovu operaci, se nazývá NOR (spojení anglických slov Not OR — česky: ne nebo). Formule (12.3) a (12.3′) ukazují opodstatněnost přijatých názvů.

Zabývejme se nejprve logickým členem NAND. Na obr. 70a je znázorněn logický obvod realizující logický člen NAND pomocí základních logických členů násobení a negace. Tyto dva členy jsou ve většině případů spojeny již ve výrobě v jeden standardní prvek a tím právě vzniká člen NAND. Symbolická značka členu NAND je na obr. 70b.



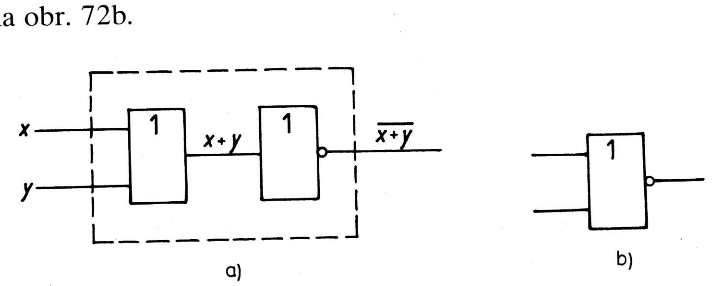
Obr. 70

Ukažme, jak pomocí členů NAND realizovat základní booleovské operace: negaci, násobení a sčítání. Na obr. 71a, b jsou znázorněny dvě možnosti negování, přičemž se obě v praxi využívají, na obr. 71c, d je znázorněno násobení a sčítání.



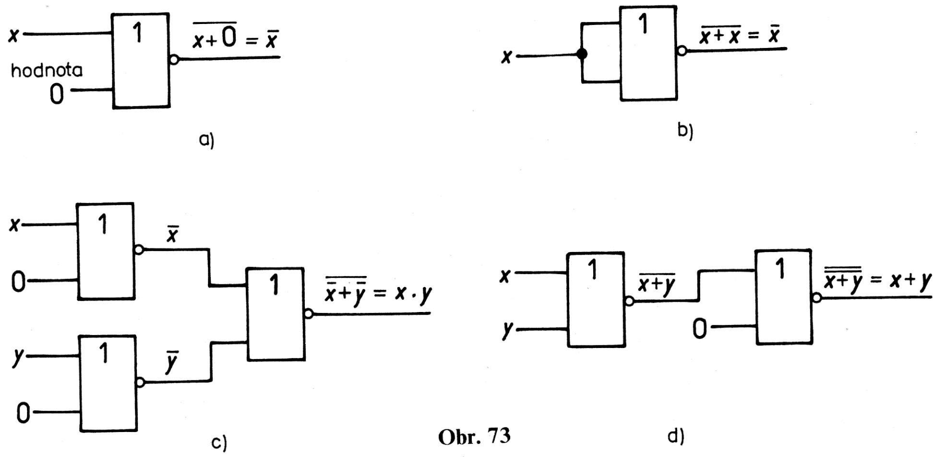
Obr. 71

Nyní obraťme pozornost k logickému členu NOR. Na obr. 72a je znázorněn logický obvod realizující logický člen NOR pomocí základních logických členů sčítání a negace. Tyto dva členy jsou ve většině případů spojeny již ve výrobě v jeden standardní prvek a tím právě vzniká člen NOR. Symbolická značka členu NOR je na obr. 72b.



Obr. 72

Ukažme, jak pomocí členů NOR realizovat základní booleovské operace: negaci, násobení a sčítání. Na obr. 73a, b jsou znázorněny dvě možnosti negování, na obr. 73c a d je znázorněno násobení a sčítání.



Obr. 73

Poznamenejme, že ani Shefferova, ani Pierceova operace nejsou asociativní. Např. platí

$$(x \uparrow y) \uparrow z \neq x \uparrow (y \uparrow z),$$

pokud za proměnné x, y, z dosadíme hodnoty 0, 1, 1. Proto není obecně možné realizovat logické členy tohoto typu s více vstupy tak, že vedle sebe zapojíme více logických členů stejného typu se dvěma vstupy.

Ukažme, jak pomocí logických členů NAND a NOR realizovat libovolnou Booleovu funkci. Uvažujme nejprve logický člen NAND. Nechť F je libovolná

Booleova funkce. K funkci F sestrojme její úplnou součtovou normální formu (popř. úplnou součinovou normální formu). Potom formu minimalizujeme. Minimální polynom upravíme tak, aby obsahoval pouze negace a negace součinů. Získaný polynom pak již snadno realizujeme pomocí logických členů NAND. Ukažme postup na konkrétních příkladech.

Příklad 12.3. Nechť Booleova funkce F tří proměnných je pro jednoduchost zadána přímo minimálním polynomem

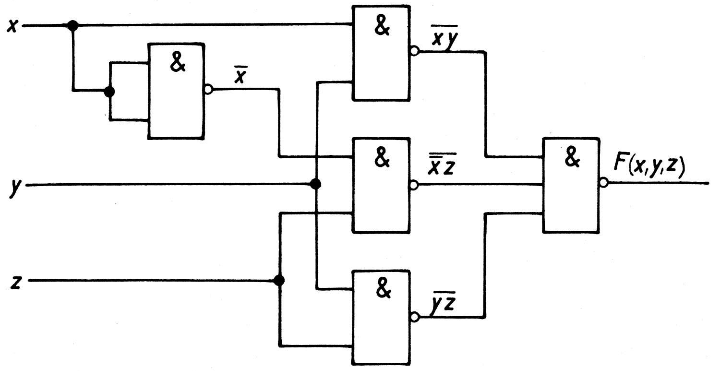
$$f = xy + \bar{x}z + yz.$$

Upravme tento polynom následujícím způsobem:

$$f = \overline{\overline{xy + \bar{x}z + yz}}$$

$$f = \overline{\overline{xy} \,.\, \overline{\bar{x}z} \,.\, \overline{yz}}$$

Takto upravený polynom již můžeme realizovat pomocí logických členů NAND. Logická síť je na obr. 74.



Obr. 74

Příklad 12.4. Nechť Booleova funkce F tří proměnných je pro jednoduchost zadána přímo minimálním polynomem (získaným z úplné součinové normální formy):

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

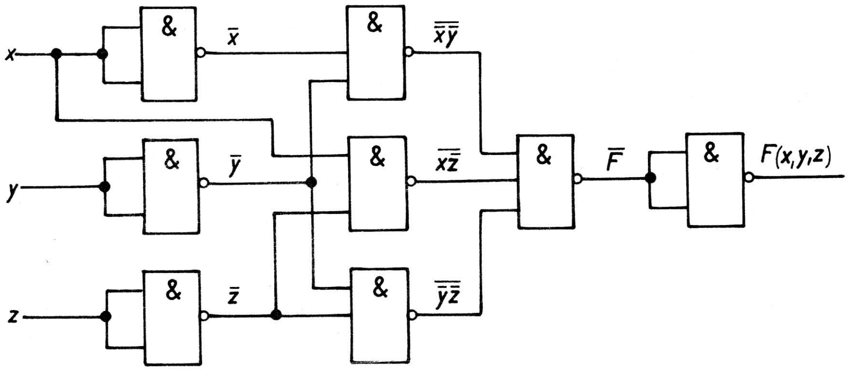
Upravme tento polynom tak, abychom ho mohli realizovat opět pomocí logických členů NAND. Úprava bude vypadat následovně:

$$f \dot{=} \overline{\overline{x + y}} \cdot \overline{\overline{\bar{x} + z}} \cdot \overline{\overline{y + z}}$$

$$f = \overline{\bar{x} \,.\, \bar{y}} \cdot \overline{x \,.\, \bar{z}} \cdot \overline{\bar{y} \,.\, \bar{z}}$$

$$f = \overline{\overline{\overline{\bar{x} \,.\, \bar{y}} \cdot \overline{x \,.\, \bar{z}} \cdot \overline{\bar{y} \,.\, \bar{z}}}}$$

Takto upravený polynom již můžeme realizovat pomocí logických členů NAND. Logická síť je na obr. 75.



Obr. 75

Zcela analogicky lze postupovat, pokud chceme vyjádřit libovolnou Booleovu funkci pomocí logických členů NOR. Nechť F je libovolná Booleova funkce F. K funkci F sestrojíme její úplnou součtovou normální formu (popř. úplnou součinovou normální formu). Potom tuto formu minimalizujeme. Minimální polynom upravíme tak, aby obsahoval pouze negace a negace součtů. Získaný polynom potom již snadno realizujeme pomocí logických členů NOR. Ukažme postup na konkrétních příkladech.

Příklad 12.5. Nechť Booleova funkce F tří proměnných je pro jednoduchost zadána přímo minimálním polynomem

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

Upravme tento polynom následujícím způsobem:

$$f = \overline{\overline{x\,.\,y}} + \overline{\overline{\bar{x}\,.\,z}} + \overline{\overline{y\,.\,z}}$$

$$f = \overline{\bar{x} + \bar{y}} + \overline{x + \bar{z}} + \overline{\bar{y} + \bar{z}}$$

$$f = \overline{\overline{\overline{\bar{x} + \bar{y}} + \overline{x + \bar{z}} + \overline{\bar{y} + \bar{z}}}}$$

Konstrukci logické sítě funkce F pomocí logických členů NOR necháme čtenáři jako cvičení.

Příklad 12.6. Nechť Booleova funkce F tří proměnných je pro jednoduchost zadána přímo minimálním polynomem (získaným z úplné součinové normální formy):

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

Upravme tento polynom následujícím způsobem:

$$f = \overline{\overline{(x + y)(\bar{x} + z)(y + z)}}$$

$$f = \overline{\overline{x + y} + \overline{\bar{x} + y} + \overline{y + z}}$$

Konstrukci logické sítě funkce F pomocí logických členů NOR necháme čtenáři jako cvičení.

Zdůrazněme, že při konstrukci logických obvodů pomocí členů NAND postupujeme většinou tak, že zadanou funkci nejprve vyjádříme ve tvaru úplné součtové normální formy. Pak provedeme minimalizaci a teprve minimální polynom převedeme do tvaru realizovatelného pomocí členů NAND. Při konstrukci logických obvodů pomocí členů NOR vycházíme obvykle z úplné součinové normální formy.

Uveďme ještě konkrétní příklad konstrukce jednoduchého logického obvodu.

Příklad 12.7. Sestrojme logický obvod pro sčítání tří jednociferných dvojkových čísel, máme-li k dispozici členy NAND se dvěma, třemi a čtyřmi vstupy.

Označme jednociferná dvojková čísla písmeny x, y, z. Je zřejmé, že sečteme-li tři jednociferná dvojková čísla, obdržíme maximálně dvojciferné dvojkové číslo, které označíme ab. Proměnná b představuje číslici nultého řádu a proměnná a číslici prvního řádu nebo jinak řečeno proměnná a představuje přechod do vyššího řádu. Uvažujme proto dvě Booleovy funkce, které jsou zadány tabulkou 26.

Tab. 26

x	y	z	a	b
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Úplné součtové normální formy získané z uvedených tabulek jsou následující:

$$a = \bar{x}yz + x\bar{y}z + xy\bar{z} + xyz$$

$$b = \bar{x}\bar{y}z + \bar{x}y\bar{z} + x\bar{y}\bar{z} + xyz$$

Polynom a lze minimalizovat, zatímco polynom b nikoli. Minimální polynom pro funkci a je následující:

$$a = xy + xz + yz$$

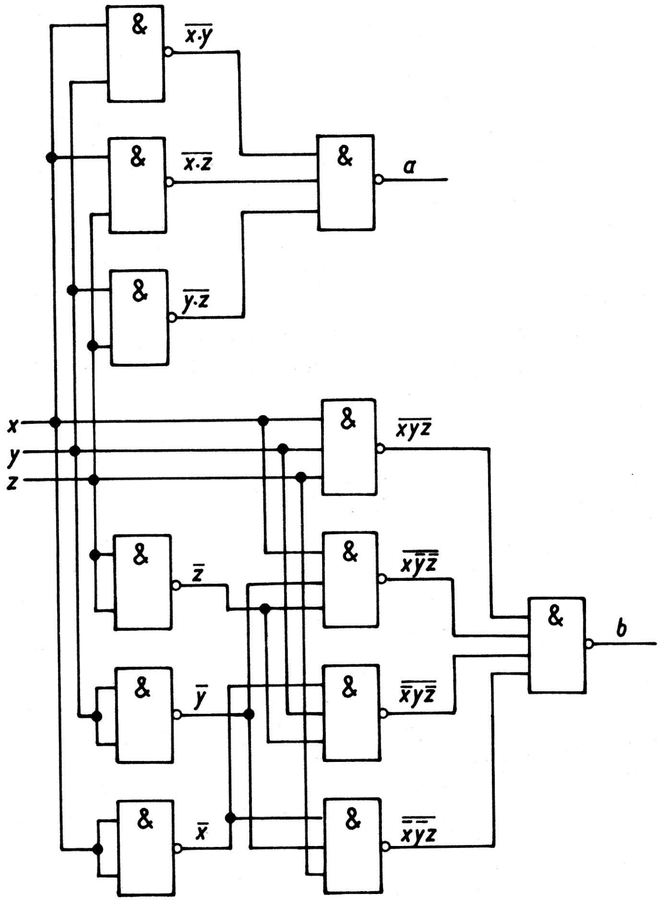
Upravme polynomy a a b tak, aby při návrhu logického obvodu bylo možné použít pouze logické členy NAND:

$$a = \overline{\overline{xy + xz + yz}} \qquad b = \overline{\overline{\bar{x}\bar{y}z + \bar{x}y\bar{z} + x\bar{y}\bar{z} + xyz}}$$

$$a = \overline{\overline{xy} \cdot \overline{xz} \cdot \overline{yz}} \qquad b = \overline{\overline{\bar{x}\bar{y}z} \cdot \overline{\bar{x}y\bar{z}} \cdot \overline{x\bar{y}\bar{z}} \cdot \overline{xyz}}$$

Logická síť je na obr. 76.

Nechť si čtenář provede analýzu uvedeného obvodu, aby ověřil, že skutečně realizuje obě uvažované funkce.



Obr. 76

Poznámka. Zájem používat spíš členy NAND a NOR místo členů logického součtu, součinu a negace je dán snahou o zmenšení počtu typů členů. V souvislosti se vznikem stavebnic integrovaných obvodů se však v praxi používají v jednom obvodu jak členy NAND, tak i NOR a i negace.

Cesta od předepsání funkce a návrhu vysoce integrovaného obvodu k vlastní výrobě je proces velmi složitý, který vyžaduje spolupráci týmu odborníků. Např. nejjednodušší zápis polynomu nemusí vždy vést k nejlepší realizaci. Ve velkých systémech je často výhodnější zapsat některé funkce jako funkce jiných funkcí, protože je výhodnější využívat mezivýpočty než optimalizovat každou z nich. Při vytváření návrhů optimálních integrovaných obvodů se proto využívají i statistické metody a používají se i samotné počítače.

Rychlý vývoj polovodičové techniky dosáhl toho, že lze na jediném polovodičovém krystalu vytvářet veliké množství elektronických součástek spojených ve složité elektronické logické obvody. Právě v souvislosti s tím se mluví o integrovaných obvodech. Technici navrhují s rostoucí integrací stále složitější obvody. V současné době se již vyrábějí obvody velmi velké integrace, jako jsou např. mikroprocesory a paměťové čipy, které obsahují až několik miliónů tranzistorů.

CVIČENÍ 12

1 Načrtněte logické sítě logických obvodů realizujících funkce tří proměnných F_1, F_2, F_3 ze cvičení 11.16 a přitom použijte tyto logické členy: a) součet, součin, negace; b) součet, negace; c) součin, negace; d) NAND; e) NOR. Logickou síť zkonstruujte před provedením minimalizace příslušného polynomu i po provedení minimalizace.

2 Načrtněte logické sítě logických obvodů realizujících funkce čtyř proměnných ze cvičení 11.17. Před konstrukcí proveďte minimalizaci. Použijte logické členy a) součet, součin, negace; b) součet, negace; c) součin, negace; d) NAND; e) NOR.

3 Načrtněte logickou síť logického obvodu pro automat na nápoje. Tento automat má pracovat tak, aby si zákazník po vhození příslušné mince a stisknutí jednoho z tlačítek „čaj" nebo „káva" mohl vybrat nápoj, který si přeje. K dispozici máte a) logické členy pro sčítání, násobení a negování; b) logické členy NAND s potřebným počtem vstupů.

Návod.

1. Formulujte jasně úlohu a označte vstupní i výstupní proměnné.

Vstupní proměnné:	Výstupní proměnné:
x: žádáme čaj	F: přidává se čajový extrakt
y: žádáme kávu	G: přidává se kávový extrakt
z: vhodili jsme minci	H: vytéká horká voda

2. Sestavte tabulky Booleových funkcí.
3. Určete úplné součtové normální formy funkcí a minimalizujte je.
4. Načrtněte logickou síť.

13 DODATEK. BOOLEOVY ALGEBRY V LOGICE

Vzhledem k zjednodušení vyslovíme úmluvu, že v rámci výrokové logiky budeme uvažovat pouze logické spojky $\wedge$, $\vee$ a $\neg$.

Nechť V je třída všech formulí výrokové logiky, pak V spolu s operacemi $\wedge$, $\vee$ a $\neg$ tvoří algebraickou strukturu, kterou nazýváme **algebra formulí výrokové logiky.** V třídě V zavedeme relaci „být ekvivalentní“:

Formule φ a ψ z F se nazývají **ekvivalentní,** právě když formule $(\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$ je tautologie*). Ekvivalenci formulí φ, ψ označíme $\varphi \equiv \psi$.

Relace „být ekvivalentní“ je ekvivalence v třídě V a dokonce kongruence v rámci algebry formulí. Sestrojme faktorovou množinu $V/\equiv$. Bloky rozkladu budeme značit T_φ, kde φ je některá z formulí tohoto bloku. Na faktorové množině můžeme zavést operace $\wedge$, $\vee$ a $\neg$ takto:

$$T_\varphi \wedge T_\psi =_{\mathrm{df}} T_{\varphi \wedge \psi} \tag{13.1}$$

$$T_\varphi \vee T_\psi =_{\mathrm{df}} T_{\varphi \vee \psi} \tag{13.2}$$

$$\neg T_\varphi =_{\mathrm{df}} T_{\neg\varphi} \tag{13.3}$$

Výrazy (13.1) až (13.3) skutečně definují operace, neboť relace $\equiv$ je kongruence. Čtveřice $(V/\equiv, \wedge, \vee, \neg)$ je proto algebraická struktura. Lze snadno dokázat, že je dokonce Booleovou algebrou. Tuto algebru nazýváme **Booleova algebra formulí výrokové logiky.** Jednotkou této algebry je blok všech tautologií, nulou je blok všech vyvratitelných formulí (tj. formulí, jejichž negace je tautologie).

Poznámka. Pokud uvažujeme při konstrukci množiny V pouze n proměnných $a_1, a_2, \dots, a_n$, pak má algebra $V/\equiv$ celkem $2^{(2^n)}$ prvků. Atomy této algebry jsou bloky, které obsahují formule tvaru

$$x_1 \wedge x_2 \wedge \dots \wedge x_n, \qquad \text{kde } x_i \text{ je buď } a_i, \text{ nebo } \neg a_i.$$

Těchto atomů je 2^n (viz př. 10.11).

Obdobně můžeme uvažovat třídu P všech formulí predikátové logiky a **algebru formulí predikátové logiky** $(P, \wedge, \vee, \neg)$. Zavedeme-li v třídě P relaci „být ekvivalentní“, kterou označíme opět $\equiv$, pak struktura $(P/\equiv, \wedge, \vee, \neg)$ je Booleova algebra,

*) Za použití spojky $\Leftrightarrow$ bychom mohli psát $\varphi \Leftrightarrow \psi$.

kterou nazýváme **Booleova algebra predikátové logiky**. Jednotkou a nulou této algebry je po řadě blok tautologií a blok „vyvratitelných" formulí.

Na operace $\forall$ a $\exists$ můžeme v rámci Booleovy algebry $P/\equiv$ pohlížet jako na zobecněné operace $\wedge$ a $\vee$. Algebra $P/\equiv$ má dvě významné podalgebry. Jsou jimi: **algebra otevřených formulí** a **algebra uzavřených formulí.**

LITERATURA

[1] Abbot, J. C.: Sets, Lattice and Boolean Algebra. New York 1969.
[2] Adámek, J.—Koubek, V.—Reiterman, J.: Základy obecné topologie, Praha, SNTL 1977.
[3] Balcar, B.—Štěpánek, P.: Teorie množin. Praha, Academia 1986.
[4] Beran, L.: Grupy a svazy. Praha, SNTL 1974.
[5] Bernard, J. M.: Od logických obvodů k mikroprocesorům I. Praha, SNTL 1982.
[6] Birkhoff, G.—Bartee, T. O.: Aplikovaná algebra. Bratislava, Alfa 1979.
[7] Birkhoff, G.—Mac Lane, S.: Prehľad modernej algebry. Bratislava, Alfa 1979.
[8] Birkhoff, G.: Lattice Theory. Providence 1966.
[9] Blažek, J. a kol.: Algebra a teoretická aritmetika I a II. Praha SPN, 1983, 1985.
[10] Borůvka, O.: Základy teorie grupoidů a grup. Praha 1962.
[11] Bourbaki, N.: Algebra. Moskva 1962.
[12] Cohn, P.: Universaľnaja algebra. Moskva 1986.
[13] Faure, R.—Heurgonová, E.: Uspořádání a Booleovy algebry. Praha, Academia 1984.
[14] Friedman, A. D.—Menon, P. R.: Teorie a návrh logických obvodů. Praha, SNTL 1983.
[15] Geoseg, F.—Peak, I.: Algebraic Theory of Automata. Budapešť 1972.
[16] Grätzer, G.: Lattice Theory. New York, Freeman 1971.
[17] Grätzer, G.: Universal algebra. Princeton, D Van Nostrand Co, Inc 1968.
[18] Halmor, P.: Lectures on Boolean Algebra. New York, Van Nostrand 1966.
[19] Hejný, M.—Kulich, I.—Tvarožek, J.: Čo je topológia? Bratislava, Alfa 1983.
[20] Hohn, F. E.: Applied Boolean Algebra. New York, Mac Millan 1960.
[21] Jacobson, N.: Lectures in Abstract Algebra. New York 1951.
[22] Ježek, J.: Univerzální algebra a teorie modelů. Praha, SNTL 1976.
[23] Kalužin, A. A.: Vvedenije v obščuju algebru. Moskva 1973.
[24] Katriňak, T.—Gavalec, M.—Gedeonová, E.—Smítal, J.: Algebra a teoretická aritmetika I. Bratislava, Alfa 1985 — Praha, SNTL 1985.
[25] Kelley, J. L.: Obščaja topologia. Moskva, Nauka 1968.
[26] Kořínek, V.: Základy algebry. Praha, ČSAV 1956.
[27] Kosmák, L.: Množinová algebra. Bratislava, Alfa 1987.
[28] Kuroš, L. G.: Kapitoly z obecné algebry. Praha, Academia 1966.
[29] Legéň, A.: Grupy, okruhy a zväzy. Bratislava, Alfa 1980.
[30] Mac Lane, S.—Birkhoff, G.: Algebra. Bratislava, Alfa 1973.
[31] Malcev, A. I.: Algebraičeskije sistemy. Moskva, 1970.
[32] Nagy, J.: Vybrané partie z moderní matematiky. Praha, SNTL 1976.
[33] Preparata, F. P.—Yeh, R.: Úvod do teórie diskrétnych matematických štruktúr. Bratislava, Alfa 1982.
[34] Pritz, J. a kol.: Úvod do číslicové techniky. Praha, SNTL 1983.
[35] Rasiowa, H.—Sikorski, R.: The Mathematics of Metamathematics. Warszawa, PWN 1963.

[36] Rieger, L.: O svazech a grupách. Praha, Přírodověd. nakladatelství 1952.
[37] Rutherford, D. E.: Introduction to Lattice Theory. New York, Hafner 1965.
[38] Sikorski, R.: Bulevy algebry. Moskva, Mir 1969.
[39] Słupecki, J.—Borkowski, L.: Elementy logiky matematycnej i teorii mnogošči. Warszawa, PWN 1963.
[40] Szasz, G.: Introduction to Lattice Theory. New York, Mc Graw Hill 1963.
[41] Šalát, T.—Haviar, A.—Hecht, T.—Katriňak, T.: Algebra a teoretická aritmetika II. Bratislava, Alfa 1986 — Praha, SNTL 1986.
[42] Tarski, A.: Úvod do logiky a metodologie deduktivních věd. Praha, SNTL 1969.
[43] Van der Warden, B. L.: Algebra. Moskva, Mir 1976.
[44] Whitesid, J. E.: Boolean Algebra and its Application. New York 1961.

SEZNAM UŽITÝCH SYMBOLŮ

Užití	Význam
φ	formule (daného jazyka)
$\varphi \wedge \psi$	φ a ψ
$\varphi \vee \psi$	φ nebo (nevylučovací) ψ
$\varphi \overline{\vee} \psi$	φ nebo (vylučovací) ψ
$\varphi \Rightarrow \psi$	jestliže φ pak ψ
$\varphi \Leftrightarrow \psi$	φ právě když ψ
$(\forall x)$	pro všechna x
$(\exists x)$	existuje aspoň jedno x
$(\exists !\, x)$	existuje právě jedno x
$\varphi \Leftrightarrow_{\mathrm{df}} \psi$	φ je ekvivalentní s ψ na základě definice
N	množina všech přirozených čísel
Z	množina všech celých čísel
Q	množina všech racionálních čísel
R	množina všech reálných čísel
K	množina všech komplexních čísel
$x \in M$	x je prvkem množiny M
$x \notin M$	x není prvkem množiny M
$A \subseteq M$	množina A je podmnožinou množiny M
$A \subset M$	množina A je vlastní podmnožinou množiny M
$A \cup B$	sjednocení množin A, B
$A \cap B$	průnik množin A, B
A'	komplement množiny A
$P(M)$	potence množiny M
$\{M_i\}_{i \in I}$	soubor množin M_i
$\bigcup_{i \in I} M_i$	sjednocení souboru množin M_i
$\bigcap_{i \in I} M_i$	průnik souboru množin M_i
$A \times B$	kartézský součin množin A, B
A^n	n-tá kartézská mocnina množiny A
xRy	prvek x je v relaci R s prvkem y
$\square R$	první obor relace R
$R \square$	druhý obor relace R
$\square R \cup R \square$	obor relace R

$\square Rb$	první obor relace R příslušný prvku b
$aR\square$	druhý obor relace R příslušný prvku a
R^{-1}	inverzní relace k relaci R
$R \circ Q$	složená relace z relací R a Q
$\square F$	definiční obor zobrazení F
$F\square$	obor hodnot zobrazení F
$F\colon x \mapsto y$	zobrazení F přiřazuje prvku x prvek y
$F\colon A \to B$	F je zobrazení množiny A do množiny B
$F\colon A \overset{\text{na}}{\to} B$	F je zobrazení množiny A na množinu B
$F\colon A \leftrightarrow B$	F je vzájemně jednoznačné zobrazení množiny A na množinu B
F^{-1}	inverzní zobrazení k zobrazení F
x^{-1}	prvek inverzní k prvku x
$x \mid y$	x dělí y
$x \equiv y (\mathrm{mod}\ E)$	x je ekvivalentní (kongruentní) s y modulo E
M/E	rozklad množiny M indukovaný ekvivalencí E
M/S	ekvivalence indukovaná v množině M rozkladem S
$x \trianglelefteq y$	x předchází před y
$x \lhd y$	x ostře předchází před y
$x \blacktriangleleft y$	x bezprostředně předchází před y
$x \trianglerighteq y$	x následuje za y
$x \rhd y$	x ostře následuje za y
$x \blacktriangleright y$	x bezprostředně následuje za y
$x \asymp y$	x je neporovnatelné s y
$\trianglelefteq_P$	uspořádání $\trianglelefteq$ v množině P
(M, R)	relační struktura, kde M je množina a R je uspořádání v této množině
$(P, \trianglelefteq)$	poset s nosičem P a uspořádáním $\trianglelefteq$
0	nula posetu (svazu, Booleovy algebry)
1	jednotka posetu (svazu, Booleovy algebry)
$\overrightarrow{\{\ldots, a_i, a_{i+1}, \ldots\}}$	řetězec, kde a_{i+1} bezprostředně následuje za a_i
$\inf M$	infimum množiny M
$\sup M$	supremum množiny M
$[a, b]$	uspořádaná dvojice nebo uzavřený interval
(a, b)	otevřený interval
$[a, b)$	polouzavřený interval
$(a, b]$	polouzavřený interval
$(\leftarrow, a)$	otevřený počáteční interval příslušný prvku a
$(a, \rightarrow)$	otevřený koncový interval příslušný prvku a
$x \sqcap y, x . y$	x průsek y
$x \sqcup y, x + y$	x spojeno s y
$\bigsqcap X$	průsek množiny X

$\bigsqcup X$	spojení množiny X
$\bigsqcap_{i=1}^{n} x_i$	průsek prvků x_1 až x_n
$\bigsqcup_{i=1}^{n} x_i$	spojení prvků x_1 až x_n
$(S, \trianglelefteq)$	svaz s nosičem S a uspořádáním $\trianglelefteq$
$D(x, y)$	největší společný dělitel prvků x, y
$n(x, y)$	nejmenší společný násobek prvků x, y
$[p_1 \cup p_2]$	lineární obal množiny $p_1 \cup p_2$
$X^{\triangledown}$	dolní kužel příslušný k množině X
$X^{\vartriangle}$	horní kužel příslušný k množině X
$(S, \sqcap, \sqcup)$	svaz s nosičem S a operacemi $\sqcap$, $\sqcup$
$[M]$	podsvaz generovaný množinou M
I_M	ideál generovaný množinou M
F_M	filtr generovaný množinou M
I_a	hlavní ideál generovaný prvkem a
F_a	hlavní filtr generovaný prvkem a
$A \times B$	direktní součin svazů A, B
$D(P)$	množina všech dolních podmnožin posetu P
$I(x)$	množina zdola ireducibilních prvků předcházejících před prvkem x
$\square F0$	dolní jádro homomorfismu F
$\square F1$	horní jádro homomorfismu F
x^*	pseudokomplement prvku x
$(B, \sqcap, \sqcup, ')$	Booleova algebra s nosičem B a operacemi $\sqcap$, $\sqcup$, $'$
$\mathrm{cl}\,(X)$	uzávěr množiny X
$\mathrm{int}\,(X)$	vnitřek množiny X
$r(X)$	regularizace množiny X
$x - y$	diference prvků x, y
$x \oplus y$	symetrická diference prvků x, y
$x \Leftrightarrow y$	ekvivalence prvků x, y
$x * y$	relativní pseudokomplement prvku x vzhledem k prvku y
$x \uparrow y$	Schefferova operace
$x \downarrow y$	Pierceova operace
$m(x_1, \ldots, x_n)$	minimální polynom proměnných x_1 až x_n
$M(x_1, \ldots, x_n)$	maximální polynom proměnných x_1 až x_n
$x', \bar{x}$	komplement prvku x
T_φ	blok ekvivalentních formulí výrokové (predikátové) logiky obsahující formuli φ
2	dvouprvková Booleova algebra $\{0, 1\}$
F_i^n	i-tá Booleova funkce F mající n proměnných

REJSTŘÍK

Prof. RNDr. Jan Kopka, CSc.

SVAZY A BOOLEOVY ALGEBRY

Obrázky narýsoval RNDr. Vlastimil Macháček
Vydala Univerzita J. E. Purkyně v Ústí nad Labem
roku 1991 jako svou publikaci č. 116-91
Edice Učebnice pro vysoké školy
Vytiskl Tisk, s. p., Brno
Počet stran 244
AA 14,81 (AA 13,50 textu, AA 1,31 grafiky) – VA 15,63
Náklad 1300 výtisků
Tematická skupina a podskupina 03/2
1. vydání
Cena brožovaného výtisku Kčs 45,–

ISBN 80-7044-025-2