4. kapitola

BOOLEOVA ALGEBRA A JEJÍ MODELY

Shrňme přehledně všechny závěry o vlastnostech operací definovaných na množinách $\hat{M}$ a H, k nimž jsme dospěli ve 3. kapitole.

Je dána množina $\hat{M}$ všech podmnožin neprázdné množiny M.

Na $\hat{M}$ jsou definovány binární operace sjednocení a průnik.

Každá z těchto operací je komutativní a asociativní.

Operace průnik je distributivní vzhledem k operaci sjednocení a také operace sjednocení je distributivní vzhledem k operaci průnik.

Vzhledem k operaci sjednocení existuje právě jeden neutrální prvek — $\emptyset$.

Vzhledem k operaci průnik existuje právě jeden neutrální prvek — M.

Je dána množina $H = \{0,1\}$ pravdivostních hodnot výroků.

Na H jsou definovány binární operace — „sčítání" a „násobení".

Každá z těchto operací je komutativní a asociativní.

Operace násobení je distributivní vzhledem k operaci sčítání a také operace sčítání je distributivní vzhledem k operaci násobení.

Vzhledem k operaci sčítání existuje právě jeden neutrální prvek — 0.

Vzhledem k operaci násobení existuje právě jeden neutrální prvek — 1.

Platí: $M \neq \varnothing$	Platí: $1 \neq 0$
Na $\widehat{M}$ je definována unární operace „doplněk".	Na H je definována unární operace „doplněk".

Z našeho přehledu je vidět, že uvažované množiny s příslušnými operacemi mají mnoho podstatného společné. Na obou jsou definovány dvě binární operace a jedna operace unární, které mají „stejné" vlastnosti, ke každé binární operaci existuje právě jeden neutrální prvek.

Množinu $\widehat{M}$ spolu s příslušnými binárními operacemi a unární operací označujme v dalším $(\widehat{M}, \cup, \cap, ')$ a nazývejme *množinová algebra.*

Množinu H spolu s operacemi sčítání, násobení a doplněk budeme označovat $(H, +, ., ')$ a nazývat *algebra pravdivostních hodnot výroků,* stručněji jenom *algebra pravdivostních hodnot.*

Vytvořme nyní jistou abstraktní nadstavbu nad oběma algebrami, definujme tzv. *Booleovu algebru.*

Mějme dánu neprázdnou, jinak zcela libovolnou, množinu B, v níž je definována rovnost jejích prvků a na které jsou zavedeny dvě binární operace, „sčítání" a „násobení", a jedna unární operace „doplněk". Množinu B spolu s příslušnými operacemi budeme nazývat Booleova algebra právě tehdy, když platí:
Každá z binárních operací je komutativní a asociativní. Dále je operace „násobení" distributivní vzhledem k operaci „sčítání" a také operace „sčítání" je distributivní vzhledem k operaci „násobení". Ke každé z binárních operací existuje právě jeden neutrální prvek; přitom jsou tyto neutrální prvky vzájemně různé. Unární operace splňuje všechny požadavky definice operace „doplněk" z 3. kapitoly.

Prvky Booleovy algebry budeme označovat malými písmeny $a, b, c, \ldots, x, y, z$. Pro rovnost prvků budeme užívat obyčejného rovnítka. Symboly pro jednotlivé binární operace si „vypůjčíme“ z číselné algebry. Operaci ***sčítání*** budeme symbolicky označovat „$u = x+y$ na B“ (stručněji „$u = x+y$“), operaci *násobení* „$u = x.y$ na B“ nebo „$u = xy$ na B“ (stručněji „$u = x.y$“ nebo „$u = xy$“). Jsou-li x, y prvky množiny B, budeme „$x+y$“ nazývat ***součet*** prvků x, y, „xy“ ***součin*** prvků x, y. *Operaci doplněk* budeme označovat „$u = x'$ na B“ (stručněji „$u = x'$“), *doplněk k prvku* x symbolem x'. Neutrální prvek operace sčítání označíme 0 (čtěte nula), neutrální prvek operace násobení symbolem 1 (čtěte „jedna“). Takto zvolená symbolika se ukáže při „booleovských výpočtech“ nejvhodnější.

Musíme mít ovšem stále na paměti, že v našem případě nejde o běžné sčítání a násobení reálných čísel; neutrální prvky 0 a 1 jsou prvky množiny B a obvykle nejsou rovny číslům 0 a 1.

Na základě předchozích úmluv můžeme definici Booleovy algebry vyslovit také takto:

Mějme dánu neprázdnou množinu B, v níž je definována rovnost, existují v ní vzájemně různé prvky 0,1 a jsou na ní definovány binární operace „$u = x+y$“, „$u = xy$“ a unární operace „$u = x'$“. Množinu B spolu s příslušnými operacemi budeme nazývat Booleova algebra, právě když pro všechny prvky x, y, z množiny B platí:

(1) $x+y = y+x$	$x.y = y.x$ (2)
(3) $(x+y)+z = x+(y+z)$	$(x.y).z = x.(y.z)$ (4)
(5) $x.(y+z) = (x.y)+$ $+ (x.z)$	$x+(y.z) = (x+y).$ $.(x+z)$ (6)

$$(7)\ x+0=x \qquad x.1=x\ (8)$$
$$(9)\ x+x'=1 \qquad x.x'=0\ (10)$$

Takto zavedenou Booleovu algebru budeme označovat $(B, +, ., ')$.

O rovnosti definované v B budeme předpokládat, že je „*rovností vůči booleovským operacím*"; to znamená, že *pro všechny prvky* x, y, z *množiny* B *platí: je-li* $x = y$, *pak platí* $x+z = y+z$, $x.z = y.z$, $x' = y'$.
Poznámka: Pozorný čtenář si jistě všiml, že druhá z definic Booleovy algebry je „slabší" než první. V systému axiómů*), který jsme uvedli, se sice zaručuje existence neutrálních prvků jednotlivých binárních operací, nikoliv však jejich jednoznačnost (axiómy (7), (8)). Tu lze ale velmi snadno z axiómů (1)—(10) dokázat. Naznačme důkaz pro neutrální prvek operace sčítání.
Předpokládejme, že existuje $0_1 \in B$ takový, pro nějž platí: pro každé $x \in B$ je $x+0_1 = x$. Pak je tedy speciálně
$0+0_1 = 0$ a zároveň
$0+0_1 = 0_1+0 = 0_1$ (podle (1) a (7))
Odsud plyne $0_1 = 0$.
Obdobně lze provést důkaz jednoznačnosti neutrálního prvku operace násobení.

O „povaze" prvků množiny B se v definici Booleovy

*) Volně řečeno, axiómy určitého oboru (systému) jsou věty, které se v tomto oboru nedokazují z jiných vět, považují se za pravdivé. Podrobně se můžete s problematikou týkající se pojmu axióm seznámit například v knížce „M. Katětov: Jaká je logická výstavba matematiky?" (edice Cesta k vědění, JČMF, II. vydání 1950).

algebry $(B, +, ., ')$ nic bližšího neříká, právě tak abstraktně pojaté jsou všechny operace i oba neutrální prvky. Známe ale už dva konkrétní příklady Booleovy algebry.

Zvolme za B konkrétně množinu $\widehat{M}$ všech podmnožin neprázdné množiny M. Operace „sčítání", „násobení" a „doplněk" konkretizujme postupně jako operace sjednocení, průnik a doplněk na $\widehat{M}$. Pak pro všechny prvky množiny $\widehat{M}$ axiómy (1)—(10) zřejmě platí. Říkáme, že *množinová algebra* $(\widehat{M}, \cup, \cap, ')$ *je modelem Booleovy algebry.* Roli neutrálních prvků 0,1 hrají množiny $\emptyset$ a M.

Představme si dále namísto množiny B konkrétně množinu H pravdivostních hodnot výroků, operace sčítání, násobení a doplněk na B konkretizujme jako operace sčítání, násobení a doplněk definované na H. Pak opět pro všechny prvky množiny H jsou axiómy (1)—(10) splněny. Říkáme, že *algebra pravdivostních hodnot* $(H, +, ., ')$ *je modelem Booleovy algebry.*

Ve cvičeních budete mít příležitost seznámit se s řadou dalších modelů Booleovy algebry $(B, +, ., ')$. Při ověřování, zda nějaká neprázdná množina s dvěma binárními a jednou unární operací je modelem Booleovy algebry, musíte postupně prozkoumat platnost axiómů (1)—(10) pro všechny její prvky.

Na základě definice Booleovy algebry můžeme nyní vyslovit a dokázat celou řadu vět, které budou při „booleovském počítání" velmi důležité. Předtím však ještě proveďme jednu úvahu, jež se ukáže při důkazech těchto vět užitečná.

Uvažujeme-li libovolný z axiómů (1)—(10) a provedeme-li v něm záměny

$$\begin{aligned} + &\longrightarrow \cdot \\ \cdot &\longrightarrow + \\ 0 &\longrightarrow 1 \\ 1 &\longrightarrow 0, \end{aligned}$$

dospějeme opět k některému z axiómů, a to k tomu, jenž je zapsán ve stejném řádku jako původní. Odsud plyne tento důležitý závěr: Jestliže na základě axiómů (1)—(10) a z nich odvozených vět dokážeme nějakou další větu a přepíšeme-li ji zcela formálně pomocí našeho „seznamu záměn", získáme opět pravdivou větu, tzv. *duální větu* k dané větě. V tomto smyslu mluvíme o tzv. *principu duality* v Booleově algebře.

Obdobně jako v „číselné algebře" a v algebře pravdivostních hodnot umluvíme se i zde psát místo „$(xy)+(xz)$" jenom „$xy+xz$", místo „$x+(yz)$" stručněji pouze „$x+yz$" atd. Jestliže však chceme k dané větě vytvořit větu duální, musí být její zápis uveden v nezkrácené formě, se všemi závorkami (promyslete toto konstatování např. na axiómech (5) a (6)).

Uveďme a dokažme nyní některé důležité věty o prvcích Booleovy algebry $(B, +, ., ')$.

Věta: *Pro každý prvek* $x \in B$ *platí:*

(11) $x+x = x$ $\qquad\qquad$ $x.x = x$ (12)

Důkaz (11): $x+x = (x+x).1 = (x+x).(x+x') =$
$= x+x.x' = x+0 = x$

Při důkazu jsme postupně použili axiómy (8), (9), (6), (10), (7).

Platnost druhé části věty plyne z principu duality Booleovy algebry a z (11). Můžete si však přesto provést podrobný důkaz. Porovnejte pak jednotlivé kroky důkazů (11) a (12).

Poznámky:

1. Z uvedené věty plyne, že v Booleově algebře nemá význam zavádět přirozené násobky prvků ani mocniny s přirozeným exponentem, což v „číselné algebře" jsou naopak pojmy značně důležité.

2. Na tomto místě už můžeme ilustrovat užitečnost uvedené definice Booleovy algebry. Z úvah o modelech Booleovy algebry a shora dokázané věty plynou ihned tyto závěry:

a) Pro každý prvek $A \in \hat{M}$ platí: $A \cup A = A$ a zároveň $A \cap A = A$.

b) Pro každý prvek $h \in H$ platí: $h + h = h$ a zároveň $h . h = h$.

Platí-li nějaká věta v Booleově algebře $(B, +, ., ')$ pak platí i v každém jejím modelu.

V důkazech dalších vět už nebudeme obvykle zdůvodňovat jednotlivé kroky. Prověřujte je podrobně sami!

Věta: *Pro každý prvek $x \in B$ platí:*

$$x . 0 = 0 \qquad (13) \qquad\qquad x + 1 = 1 \qquad (14)$$

Důkaz (13): $x . 0 = x . 0 + 0 = x . 0 + x . x' = x . (0 + x') = = x . x' = 0$

Druhá část věty plyne ihned z principu duality a z (13).

Věta: *Pro každý prvek* $x \in B$ *platí*

(15) $(x')' = x$

Důkaz: Podle definice operace doplněk a podle axiómů (1) a (2) lze psát $x' + x = 1$ a zároveň $x' . x = 0$. Odtud ihned plyne, že x je doplňkem k x', tj. $x = (x')'$.

Věta: *Pro všechny prvky* x, y *množiny* B *platí:*

(16) $(x+y)' = x' . y'$ $\qquad$ $(x . y)' = x' + y'$ (17)

Důkaz (16): Naším úkolem je dokázat, že $x' . y'$ je doplňkem k prvku $x+y$, tj. musíme ověřit, že platí

1) $(x' . y') . (x+y) = 0$ a zároveň
2) $x' . y' + (x+y) = 1$

Nejprve dokažme 1):

$(x' . y') . (x+y) = (x' . y') . x + (x' . y') . y = (x' . x) . y' + x' .$
$. (y' . y) = 0 . y' + x' . 0 = 0 + 0 = 0$

Dokažme dále 2):

$x' . y' + (x+y) = (x' + (x+y)) . (y' + (x+y)) = ((x'+x) +$
$+ y) . ((y'+y)+x) = (1+y) . (1+x) = 1 . 1 = 1$

Tím je důkaz (16) proveden.
Poznámka: Mnozí z vás jistě znáte (16) a (17) v modelu množinové algebry pod názvem „de Morganovy zákony“.

Věta: *Pro všechny prvky* x, y *množiny* B *platí*:

(18) $x + xy = x$ $\qquad$ $x . (x+y) = x$ (19)

Důkaz (18): $x + xy = x . 1 + xy = x . (1+y) = x . 1 = x$

Věta: *Pro všechny prvky x, y množiny B platí:*

(20) $x + x'.y = x + y$ $\qquad$ $x.(x' + y) = xy$ (21)

Důkaz (20): $x + x'.y = (x + x').(x + y) = 1.(x + y) =$
$= x + y$

Věta: *Nechť x, y jsou libovolné prvky množiny B. Pak platí:*

(22) $x + y = 0$, *právě když je* $x = 0$ *a zároveň* $y = 0$

(23) $x.y = 1$, *právě když je* $x = 1$ *a zároveň* $y = 1$

Důkaz (22): a) Nechť je $x = 0$ a zároveň $y = 0$. Pak je podle (7) $x + y = 0$.
b) Nechť je $x + y = 0$. Pak je $x + (x + y) = (x + x) + y =$ $= x + y = 0$ a zároveň $x + (x + y) = x + 0 = x$. Odtud plyne $x = 0$. Zcela obdobně zjistíme, že je také $y = 0$. Tím je důkaz (22) proveden.

Věta: *Nechť jsou x, y libovolné prvky množiny B. Pak platí:*

(24) $x = y$, *právě když je* $xy' + x'y = 0$

(25) $x = y$, *právě když je* $(x + y').(x' + y) = 1$

Důkaz (24): a) Nechť je $x = y$. Pak $xy' = yy'$, čili $xy' = 0$, a zároveň také $x'.y = 0$. Podle (22) je tedy $xy' + x'y = 0$.
b) Nechť je nyní $x \neq y$. Chceme dokázat, že potom platí $xy' + x'y \neq 0$. Předpokládejme, že existují prvky x, y množiny B, $x \neq y$, pro něž je $xy' + x'y = 0$. Podle (22)

je pak $\qquad xy' = 0 \quad$ (a)
a zároveň $\quad x'y = 0 \quad$ (b)

Z (a) plyne dále $xy'+y=y$ a podle (20) je $x+y=y$. Z (b) obdobným postupem dostaneme $x+y=x$. Odtud plyne $x=y$, což je spor s předpokladem $x \neq y$.
Tím je důkaz (24) proveden.

Užijme nyní dokázaných vět k řešení několika příkladů, naučme se „booleovsky počítat". Ve všech příkladech značí a, b, c, d, e prvky Booleovy algebry $(B, +, ., ')$. Vždy si podrobně zdůvodňujte jednotlivé kroky řešení podle axiómů a vět (1)—(25).

Příklad 15: Dokažte, že pro všechny prvky a, b, c, d platí

$$(a+b).(c+d) = ac+bc+ad+bd$$

Řešení: $(a+b).(c+d) = (a+b).c + (a+b).d =$
$= ac+bc+ad+bd$

Příklad 16: Zjednodušte zápis prvku

$$abc+[b'.(a'+c)]'$$

tak, aby obsahoval co nejméně symbolů.
Řešení: $abc+[b'.(a'+c)]' = abc+(b')'+(a'+c)' =$
$= abc+b+(a')'.c' = b+ac'$

Příklad 17: Zjednodušte zápis prvku

$$(ab+de)'.(d+e).ca.(c'+b')$$

tak, aby obsahoval co nejméně symbolů.

Řešení: $(ab+de)'.(d+e).ca.(c'+b') = (ab)'.(de)'.$
$.(d+e).ca.(c'+b') = a.(a'+b').(d'+e').(d+e).c.$
$.(c'+b') = (aa'+ab').(d'd+e'd+d'e+e'e).(cc'+cb') =$
$= ab'.(e'd+d'e).cb' = ab'c.(de'+d'e)$

Poznámka: V 1. kapitole (příklad 3) jsme ukázali, že pro všechny prvky A, B množiny $\hat{M}$ platí $(A' \cap B')' = A \cup B$. Ve cvičení 4a) ke kapitole 2 jste měli možnost dokázat, že pro všechny prvky X, Y z dané množiny výroků platí $(X' \wedge Y')' \Leftrightarrow (X \vee Y)$; z toho také vyplývá, že pro všechny prvky r, s množiny H pravdivostních hodnot výroků je $(r'.s')' = r + s$.

Odsud plyne, že Booleovu algebru je možno zavést i jiným způsobem, než jsme uvedli zde. Můžeme vyjít z neprázdné množiny B, na níž jsou definovány operace násobení a doplněk, uvedeme vhodný systém axiómů pro tuto „algebru" a teprve poté definujeme operaci součet na základě zavedených operací násobení a doplněk.

Má-li čtenář chuť, může se tímto problémem zabývat hlouběji.

Cvičení

1. Je dána množina K, jejímiž prvky jsou uzavřené intervaly $\langle \frac{5}{2}, 3\rangle$ a $\langle 2, 3\rangle$. Definujme na K binární operace sjednocení a průnik a unární operaci „$u = x'$" tabulkou:

x	$\langle \frac{5}{2}, 3\rangle$	$\langle 2,3\rangle$
x'	$\langle 2, 3\rangle$	$\langle \frac{5}{2}, 3\rangle$

Rozhodněte, zda $(K, \cup, \cap, ')$ je modelem Booleovy algebry.

2. Je dána úsečka AB, A $\neq$ B. Uvažujme množinu G, jejímiž prvky jsou prázdná část úsečky O_u, body A, B a úsečka AB. Definujme na G operace tabulkami takto:

$x * y$:

$x \backslash y$	O_u	A	B	AB
O_u	O_u	A	B	AB
A	A	A	AB	AB
B	B	AB	B	AB
AB	AB	AB	AB	AB

$x \circ y$:

$x \backslash y$	O_u	A	B	AB
O_u	O_u	O_u	O_u	O_u
A	O_u	A	O_u	A
B	O_u	O_u	B	B
AB	O_u	A	B	AB

x	O_u	A	B	AB
$\bar{x}$	AB	B	A	O_u

Dokažte, že $(G, *, \circ, ^-)$ je modelem Booleovy algebry.

3. Pokuste se sami konstruovat další modely Booleovy algebry obdobně jako v předchozím příkladě. Vyjděte například z těchto geometrických útvarů: trojúhelník; čtverec; čtyřstěn; krychle. Volte příslušné množiny analogicky jako množinu G v příkladu 2.

4. Zvolme množinu $C = \{1, 2, 3, 6\}$. Definujme na C binární operace „tvoření nejmenšího společného násobku", „tvoření největšího společného dělitele" a unární operaci „$u = \frac{6}{x}$". Dokažte, že C s takto definovanými operacemi je modelem Booleovy algebry.

5. Uvažujme množinu $T = \{2, 3\}$ a definujme na ní binární operace „$u = \max(x, y)$", „$u = \min(x, y)$" (viz cvičení 3, 3. kapitola) a unární operaci „$u = \bar{x}$" takto:

x	2	3
$\bar{x}$	3	2

Dokažte, že množina T spolu s uvedenými operacemi je modelem Booleovy algebry.

6. Zvolme množinu U všech uspořádaných dvojic $[x,y]$, kde x a y patří množině $\{2, 3\}$. Definujme na U rovnost a binární operace „$u = x \ast y$", „$u = x \circ y$" takto:
Pro všechny prvky $[x_1, y_1]$, $[x_2,y_2]$ množiny U je
$[x_1, y_1] = [x_2, y_2]$ právě tehdy, když $x_1 = x_2$ a zároveň $y_1 = y_2$;
$[x_1, y_1] \ast [x_2, y_2] = [\max(x_1, x_2), \max(y_1, y_2)]$;
$[x_1, y_1] \circ [x_2, y_2] = [\min(x_1, x_2), \min(y_1, y_2)]$.

Dále definujme na U unární operaci „$u = \bar{x}$" takto:
Pro každou dvojici $[x_1, x_2] \in U$ je $[\overline{x_1, x_2}] = [\bar{x}_1, \bar{x}_2]$, kde pro $i = 1, 2$ je $\bar{x}_i = 2$ právě tehdy, když $x_i = 3$ (a tedy $\bar{x}_i = 3$ právě tehdy, když je $x_i = 2$).
Dokažte, že $(U, \ast, \circ, ^-)$ je modelem Booleovy algebry.

7. Nechť n je libovolné přirozené číslo. Uvažujme množinu V všech uspořádaných n-tic $[x_1, x_2, \ldots, x_n]$, kde $x_1, x_2, \ldots, x_n$ patří do množiny $\{2, 3\}$.
Definujte na V rovnost, binární operace „$u = x \ast y$", „$u = x \circ y$" a unární operaci „$u = \bar{x}$" obdobně jako v příkladě 6.
Rozhodněte pak, zda $(V, \ast, \circ, ^-)$ je modelem Booleovy algebry.

8. Uvažujme množinu F všech reálných funkcí jedné reálné proměnné, jejichž definiční obor je množina všech reálných čísel R a pro něž platí: pro každé $f \in F$ a každé $z \in R$ je $f(z) = 2$ nebo $f(z) = 3$.
Definujme v F rovnost funkcí takto: pro všechny prvky f, g množiny F je f rovno g (symbolicky „$f = g$") právě tehdy, když pro každé $z \in R$ je $f(z) = g(z)$.
Zaveďme dále na F binární operace „$u = x \ast y$" a „$u = x \circ y$":
Pro všechny prvky f, g z množiny F je

$f \ast g$ rovno funkci h, pro niž platí: pro každé $z \in R$ je $h(z) = \max(f(z), g(z))$;

$f \circ g$ rovno funkci k, pro niž platí: pro každé $z \in R$ je $k(z) = \min(f(z), g(z))$.

Definujme na F unární operaci „$u = \bar{x}$“ takto: Pro všechna $f \in F$ je $\bar{f}$ funkce, pro niž platí: pro každé $z \in R$ je $\bar{f}(z) = 2$ právě tehdy, když $f(z) = 3$ (a tedy $\bar{f}(z) = 3$, právě když $f(z) = 2$). Dokažte, že $(F, \ast, \circ, {}^{-})$ je modelem Booleovy algebry.

9. Dokažte, že pro všechny prvky a, b, c, d Booleovy algebry $(B, +, ., ')$ platí:

a) $a.(b+c+d) = ab+ac+ad$ b) $a+bcd = (a+b).(a+c).(a+d)$

c) $(a+b+c)' = a'b'c'$ d) $(abc)' = a'+b'+c'$

10. Zjednodušte zápisy prvků Booleovy algebry tak, aby obsahovaly co nejméně symbolů:

a) $a+a'b+ab'+a'b'$ b) $(a+b'+c').(a+b'c)$

c) $abc'+a'b'c'+a'bc'+abc$ d) $a+c'+b.(a+c')'+(a+c').(a+b+c')$

e) $((ab+c)'+ab+d)'$ f) $(abc+ab'+bc')'$

g) $b.(a+c+d).(a+e).b.(e+d).(bd)'.(e+c+d)$

h) $(a+c).(dg)'.(ab)'.(d+a').(f+g).c'.(ad)'.(dc)'$

11. Říkáme, že systém axiómů je nezávislý, když žádný z axiómů tohoto systému nelze dokázat z ostatních.

Pokuste se ukázat, že systém axiómů Booleovy algebry, uvedený v této kapitole, je závislý. Můžete například dokázat, že axiómy (3) a (4) lze odvodit pomocí axiómů (1), (2), (5)—(10) a vět, jež byly v této kapitole dokázány bez použití axiómů (3) a (4).