PROSTA BOOLOVA ALGEBRA
SEMINAR

LUKA PONIKVAR

Povzetek. Teorija Boolovih algeber seže nazaj vse do leta 1847, ko jo je začel razvijati George Bool. Verjel je, da se jo lahko uporabi kot aritmetično orodje za študij in matematično analizo logike. Moderno noto so prispevali: William Stanley Jevons, Augustus De Morgan, Charles Sanders Pierce in Ernst Schröder.

Šele v tretjem desetletju prejšnjega stoletja se je veja osvobodila okov logike in postala samosvoja moderna matematična disciplina z daljnosežnimi izreki in pomembnimi povezavami z drugimi vejami matematike, kot so algebra, logika in teorija mere, če jih naštejemo le par. Za to sta nedvomno najbolj zaslužna Marshall Stone in Alfred Tarski.

V tem besedilu bomo vpeljali najosnovnejše pojme in brez dokazov navedli globlje izreke.

1. Boolove algebre

Definicija 1.1 (Boolova algebra)**. Boolova algebra** je neprazna množica A skupaj z binarnima operacijama $\vee$ [1] in $\wedge$[2], unarno operacijo $\neg$ [3] in dvema elementoma 0 in 1, ki skupaj zadoščajo sledečim aksiomom[4]:

$$
\begin{aligned}
&(1) && \neg 0 = 1, && \neg 1 = 0,\\
&(2) && p \wedge 0 = 0, && p \vee 1 = 1,\\
&(3) && p \wedge 1 = p, && p \vee 0 = p,\\
&(4) && p \wedge \neg p = 0, && p \vee \neg p = 1,\\
&(5) && \neg(\neg p) = p, && \\
&(6) && p \wedge p = p, && p \vee p = p,\\
&(7) && \neg(p \wedge q) = \neg p \vee \neg q, && \neg(p \vee q) = \neg p \wedge \neg q,\\
&(8) && p \wedge q = q \wedge p, && p \vee q = q \vee p,\\
&(9) && p \wedge (q \wedge r) = (p \wedge q) \wedge r, && p \wedge (q \vee r) = (p \vee q) \vee r,\\
&(10) && p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r), && p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r).
\end{aligned}
$$

Primer 1.2 (Izrojena Boolova algebra)**.** Najenostavnejši je primer izrojene Boolove algebre, ki je potenčna množica prazne množice:

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

[1] Imenujemo jo "join" oz. "ali".
[2] Imenujemo jo "meet" oz. "in".
[3] Imenujemo jo komplementacija, označujemo pa tudi kot $'$.
[4] Komplementacija ima najvišjo prioriteto, medtem ko ima "in" višjo prioriteto kot "ali".

Operacije na tej množici definiramo kot konstantne preslikave, ki vse slikajo v

$$0 = 1 = \emptyset.$$

Primer 1.3 (Boolova algebra z dvema elementoma)**.** Najmanjši primer neizrojene Boolove algebre je potenčna množica enojca[5]:

$$\mathbb{2} = \mathcal{P}(\{\infty\}) = \{\emptyset, \{\infty\}\}.$$

Taka Boolova algebra ima le dva elementa:

$$\emptyset = 0, \qquad \{\infty\} = 1.$$

Operaciji ali ter in sta predstavljeni z naslednjima tabelama:

$\vee$	0	1
0	0	1
1	1	1

in

$\wedge$	0	1
0	0	0
1	0	1

,

komplementacija pa 0 preslika v 1 in obratno.

Primer 1.4 (Končno-končna Boolova algebra)**.** Najpreprostejši primer Boolove algebre je potenčna množica neprazne množice X, ki jo seveda opremimo z operacijami unije, preseka in komplementa.

Malce splošnejši primer je, da si ogledamo določeno podmnožico $\mathcal{P}(X)$. Če definiramo $A := \{B \subset X \mid B \text{ končna ali } B' \text{ končna}\}$, tudi dobimo Boolovo algebro, imenovano končno-končna Boolova Algebra.

Lahko se tudi ne omejimo le na končne, ampak na števne množice in dobimo števno-števno Boolovo algebro. Premislek deluje za poljubno kardinalnost, je pa to težje dokazati.

2. Princip dualnosti

Definicija 2.1 (Boolov polinom)**. Boolov polinom** je izraz, sestavljen iz konstant 0 in 1, neznank $p_0, \ldots, p_n$, s pomočjo standardnih operacij meet, join in komplementa.

Primer 2.2 (Boolov polinom)**.** Primer polinoma je

$$p \wedge (q \vee r).$$

Ta polinom, pa je na pogled zelo podoben polinomu

$$p \vee (q \wedge r),$$

kar motivira naslednjo definicijo.

Definicija 2.3 (Dualnost)**.** Naj bo $f(p_1, \ldots, p_n)$ Boolov polinom v n spremenljivkah. Takemu polinomu lahko priredimo tri nove polinome:

(1) **komplement polinoma** $f(p_1, \ldots, p_n)$:
$$f'(p_1, \ldots, p_n),$$
(2) **dual polinoma** $f(p_1, \ldots, p_n)$:
$$f'(p_1', \ldots, p_n'),$$
(3) **kontradual polinoma** $f(p_1, \ldots, p_n)$:
$$f(p_1', \ldots, p_n').$$

[5]Element množice smo označili kar z ∞.

Opomba 2.4. V resnici obstaja grupa G, ki deluje na množici $\mathcal{BP}$ vseh Boolovih polinomov. Obstajajo štiri funkcije, ki bijektivno preslikajo množico $\mathcal{BP}$ nazaj nase:

(1) Identična funkcija:
$$id : \mathcal{BP} \to \mathcal{BP}$$
$$id : f(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n).$$

(2) Komplementna funkcija:
$$c : \mathcal{BP} \to \mathcal{BP}$$
$$c : f(p_1, \dots, p_n) \mapsto f'(p_1, \dots, p_n).$$

(3) Dualna funkcija:
$$d : \mathcal{BP} \to \mathcal{BP}$$
$$d : f(p_1, \dots, p_n) \mapsto f'(p_1', \dots, p_n').$$

(4) Kontradualna funkcija:
$$k : \mathcal{BP} \to \mathcal{BP}$$
$$k : f(p_1, \dots, p_n) \mapsto f(p_1', \dots, p_n').$$

Grupa G je zaprta za operacijo $\circ$:

$\circ$	id	c	d	k
id	id	c	d	k
c	c	id	k	d
d	d	k	id	c
k	k	d	c	id

.

Opazimo, da je $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, torej je Kleinova četverka.

Opomba 2.5. Praktična posledica principa dualnosti je moč dokazati le polovico izrekov in trditev, saj druga polovica sledi iz tega principa.

3. Urejenost

V tem razdelku delujemo v poljubni Boolovi algebri A.

Lema 3.1. *Če je $p \vee q = p$ za vse p, potem je $q = 0$; če je $p \wedge q = p$ za vse p, potem je $q = 1$.*

Dokaz. Postavimo $p = 0$ in $p = 1$. □

Lema 3.2. *Če sta p in q taka, da je $p \wedge q = 0$ in $p \vee q = 1$, potem je $q = p'$.*

Dokaz.
$$\begin{aligned} q &= 1 \wedge q \\ &= (p \vee p') \wedge q \\ &= (p \wedge q) \vee (p' \wedge q) \\ &= 0 \vee (p' \wedge q) \\ &= (p' \wedge p) \vee (p' \wedge q) \\ &= p' \wedge (p \vee q) \\ &= p' \wedge 1 \\ &= p' \end{aligned}$$

□

Lema 3.3. *$(p \vee q) \wedge p = p$ in $(p \wedge q) \vee p = p$.*

Dokaz.

$$\begin{aligned}(p \vee q) \wedge p &\overset{(3)}{=} (p \vee q) \wedge (p \vee 0)\\ &\overset{(10)}{=} p \vee (q \wedge 0)\\ &\overset{(2)}{=} p \vee 0\\ &\overset{(3)}{=} p\end{aligned}$$

Druga furmula sledi iz dualnosti.

□

Lema 3.4. *$p \wedge q = p$ natanko tedaj ko $p \vee q = q$.*

Dokaz. Če je $p \wedge q = p$, je

$$\begin{aligned}p \vee q &= (p \wedge q) \vee q\\ &\overset{(10)}{=} (p \vee q) \wedge (q \vee q)\\ &\overset{(6)}{=} (p \vee q) \wedge q\\ &\overset{3.3}{=} q\end{aligned}$$

Drugo implikacijo dobimo z zamenjavo p in q, ter formiranjem dualov. □

Definicija 3.5. Na vsaki Boolovi algebri lahko vpeljemo urejenost kot:

$$p \leq q \text{ natanko tedaj ko } p \wedge q = p.$$

Lema 3.6. *Relacija $\leq$ je delna urejenost.*

Dokaz. Refleksivnost sledi iz (6), antisimetričnost pa sledi iz (8): če je $p \leq q$ in $q \leq p$, potem je $p = p \wedge q = q \wedge p = q$. Tranzitivnost sledi iz (9): če je $p \leq q$ in $q \leq r$ je $p \wedge r = (p \wedge q) \wedge r = p \wedge (q \wedge r) = p \wedge q = p$ □

Lema 3.7.
1. *$0 \leq p$ in $p \leq 1$.*
2. *Če $p \leq q$ in $r \leq s$, potem $p \wedge r \leq q \wedge s$ in $p \vee r \leq q \vee s$.*
3. *Če $p \leq q$, potem $q' \leq p'$.*

Dokaz. Prva točka je očitna. Druga sledi iz definicije in 3.4. Tretja točka sledi s komplemetiranjem.

□

Definicija 3.8 (Meje)**.** Če je E podmnožica delno urejene Boolove algebre A, lahko govorimo o množici F vseh zgornjih mej za E. Element q pripada množici F, če za vsak $p \in E$ velja $p \leq q$. Če ima F najmanjši element, je ta enolično določen in ga imenujemo **supremum** množice E oz. njena **najmanjša zgornja meja**[6]. Podobno definiramo **infimum** oz. **največjo spodnjo mejo**[7] množice E

[6] Pišemo tudi natančna zgornja meja.
[7] Pišemo tudi natančna spodnja meja.

Primer 3.9 (Prazna množica)**.** Če je $E = \emptyset$, je vsak element na prazno zgornja meja te množice. Tedaj ima E supremum, in sicer kar element 0 (3.7 točka 2). Podoben razmislek nas privede do zaključka, da je infimum množice E element 1.

Primer 3.10 (Enojec)**.** Če je $E = \{p\}$, je p hkrati zgornja in spodnja meja za E. Sledi da je p tudi infimum in supremum.

Lema 3.11. *Za vsaka p in q ima množica $\{p, q\}$ za supremum element $p \vee q$ in za infimum element $\{p \wedge q\}$*

Dokaz. Očitno je $p \vee q$ zgornja meja te množice. Zaradi točke 2 v 3.7, pa je to tudi natančna zgornja meja: če je $p \leq r$ in $q \leq r$ je $p \wedge q \leq r \wedge r = r$. Drug del sledi iz dualnosti.

□

Opomba 3.12 (Posplošitev)**.** Lemo bi lahko posplošili na poljubno končno neprazno množico E. Za infimum pišemo $\bigwedge E$, za supremum pa $\bigvee E$. Enake oznake uporabljamo za supremume in infimume poljubnih množic (če jih te seveda imajo).

Primera 3.9 in 3.10 bi lahko sedaj zapisali kot:

$$\bigvee \emptyset = 0, \qquad \bigwedge \emptyset = 1, \qquad \bigvee \{p\} = p, \qquad \bigwedge \{p\} = p.$$

Če imamo opravka z množico $\{p_i |\ i \in I\}$, kjer je I poljubna indeksna množica, pišemo tudi:

$$\bigvee_{i \in I} p_i \qquad \bigwedge_{i \in I} p_i$$

4. Kompletne Boolove algebre

Končno-končna Boolova algebra nad $\mathbb{N}$ je primer Boolove algebre, kjer nimajo vse podmnožice elementov natančnih spodnjih oz. zgornjih mej. Primer take množice je množica vseh enojcev sodih naravnih števil. To motivira naslednjo definicijo.

Definicija 4.1 (Kompletna Boolova algebra)**.** Boolova algebra z lastnostjo, da ima vsaka njena podmnožica infimum in supremum se imenuje **kompletna Boolova algebra**.

Opomba 4.2. Vsaka končna Boolova algebra je kompletna.

Lema 4.3. *Če je $\{p_i\}$ družina elementov Boolove algebre, potem:*

$$\left(\bigvee_i p_i\right)' = \bigwedge_i p_i' \qquad \textit{in} \qquad \left(\bigwedge_i p_i\right)' = \bigvee_i p_i'.$$

Enačbi povesta, da obstoj ene strani implicira obstoj druge in njuno enakost.

Dokaz. Denimo, da je $p = \bigvee_i p_i$. Ker je $p_i \leq p$ za vsak i, sledi iz 3.7, da je $p' \leq p_i'$ za vsak i. Če je $q \leq p_i'$ za vse i, je $p_i \leq q'$ za vse i in tako po definiciji supremuma $p \leq q'$ in $q \leq p'$. Torej je p' res $\bigwedge_i p_i'$.

Dualni argument zadošča za dokaz v desno druge enačbe. Da dokažemo še obratno smer pa lahko dokazane lastnosti uporabimo na družinah komplementov.

□

Posledica 4.4 (Zadosten pogoj za kompletnost)**.** *Če ima vsaka podmnožica Boolove algebre infimum (supremum), potem je ta Boolova algebra kompletna.*

Zdaj nas zanimajo še lastnosti natančnih zgornjih (spodnjih) mej. Natančneje njihova asociativnost, komutativnost in distributivnost. O komutativnosti ni smisla govoriti, saj je supremum (infimum) pripisan neki množici elementov, torej neodvisno od njihove urejenosti.

Lema 4.5 (Asociativnost)**.** *Če je $\{I_j\}$ družina množic z unijo I, in če je p_i element Boolove algebre za vsak $i \in I$, tedaj je*

$$\bigvee_j \left(\bigvee_{i \in I_j} p_i \right) = \bigvee_{i \in I} p_i \qquad \textit{in} \qquad \bigwedge_j \left(\bigwedge_{i \in I_j} p_i \right) = \bigwedge_{i \in I} p_i .$$

Dokaz. Označimo z $q_j = \bigvee_{i \in I_j} p_i$ in s $q = \bigvee_j q_j$. Za vsak $i \in I$ obstaja j, da je $i \in I_j$. Torej za vsak i obstaja j, da je $p_i \leq q_j$, kar skupaj s $q_j \leq q$ da $p_i \leq q$ za vsak i. Denimo sedaj, da obstaja tak r, da je $p_i \leq r$ za vse i. Tedaj je še toliko bolj $p_i \leq r$ za $i \in I_j$ in po definiciji $q_j \leq r$ za vsak j. Torej je spet po definiciji $q \leq r$, kar dokazuje, da je q res želeni supremum.

□

Lema 4.6. *Če je p element in $\{q_j\}$ družina elementov v neki Boolovi algebri, potem*

$$p \wedge \bigvee_i q_i = \bigvee_i (p \wedge q_i).$$

Dokaz. Pišimo $q = \bigvee_i q_i$. Ker velja $p \wedge q_i \leq p \wedge q$ za vse i, je torej element $p \wedge q$ zgornja meja za $\bigvee_i (p \wedge q_i)$. Denimo, da je tudi r zgornja meja. Tedaj velja

$$q_i \overset{(3)}{=} 1 \wedge q_i \overset{(4)}{=} (p \vee p') \wedge q_i \overset{(10)}{=} (p \wedge q_i) \vee (p' \wedge q_i) \leq r \vee (p' \wedge q_i) \overset{3.7}{\leq} r \vee p'.$$

Po definiciji supremuma je $q \leq r \vee p'$. Sledi

$$p \wedge q \leq p \wedge (r \vee p') \overset{(10)}{=} (p \wedge r) \vee (p \wedge p') \overset{(4)}{=} (p \wedge r) \vee 0 \overset{(3)}{=} (p \wedge r) \leq r.$$

□

Posledica 4.7. *Če sta $\{p_i\}$ in $\{q_j\}$ družini elementov v Boolovi algebri, potem je*

$$\left(\bigvee_i p_i \right) \wedge \left(\bigvee_j q_j \right) = \bigvee_{i,j} \left(p_i \wedge q_j \right).$$

Definicija 4.8 (Kompletno distributivnostno pravilo)**.** Naj bo A Boolova algebra, I in J pa taki indeksni množici, da za vsaka $i \in I$ in $j \in J$ element $p(i,j)$ leži v A. Pravimo, da družina $\{p(i,j)\}$ zadošča **kompletnemu distributivnostnemu pravilu**, če je

$$\bigwedge_{i \in I} \bigvee_{j \in J} p(i,j) = \bigvee_{a \in J^I} \bigwedge_{i \in I} p(i, a(i)). \tag{11}$$

Definicija 4.9 (Kompletno distributivna algebra)**.** Boolova algebra A je **kompletno distributivna**, ko ima naslednjo lastnost: ko vsi supremumi $\bigvee_{j \in J} p(i,j)$ in infimumi $\bigwedge_{i \in I} p(i, a(i))$ obstajajo za vsako družino $\{p(i,j)\}$, potem obstoj leve strani (11) implicira obstoj desne strani in njuno enakost.

5. Podalgebre

Definicija 5.1. Boolova podalgebra Boolove algebre A je neprazna podmnožica B množice A, ki je z zožitvijo operacij Boolova algebra. Vsaka neizrojena Boolova Algebra A ima trivialno podalgebro $\mathbb{2}$, ostale imamo za netrivialne. Vsaka Boolova algebra A premore tudi nepravo podalgebro A, vse ostale podalgebre so prave.

Opomba 5.2. Presek poljubne družine Boolovih podalgeber je ponovno podalgebra. Presek prazne družine porodi nepravo podalgebro.

Če vzamemo neko podmnožico E v Boolovi algebri A, lahko tvorimo presek vseh podalgeber, ki vsebujejo E (vsaj ena taka obstaja, namreč A). Ta presek, recimo B je najmanjša podalgebra, ki vsebuje E. Rečemo, da je B generirana z E oz. da je E množica generatorjev za B.

Primer 5.3. Vzemimo $E = \emptyset$. Podalgebra, ki jo ta množica generira je najmanjša podalgebra, ki jo A premore, namreč $\mathbb{2}$. Če je E sam po sebi podalgebra pa generira samega sebe.

Definicija 5.4. Podalgebra Boolove algebre A je končno generirana, če je generirana s kakšno končno podmnožico A.

Izrek 5.5. *Naj bo B podalgebra generirana s končno množico E. Atomi v B so neničelni elementi oblike*
$$p_a = \bigwedge_{i\in E} p(i, a(i)),$$
in elementi B so oblike
$$\bigvee_{a\in A\subseteq E} p_a.$$
Za vsak element B je ta zapis enoličen.

Dokaz. Za vsak $i \in A$ in $j \in \mathbb{2}$ vpeljimo oznako
$$p(i,j) = \begin{cases} i & \text{če } j = 1, \\ i' & \text{če } j = 0. \end{cases}$$
Pišimo tudi $\mathbb{2}^E$ za vse funkcije iz E v $\mathbb{2}$ in za vsak $a \in \mathbb{2}^E$ vpeljimo
$$p_a := \bigwedge_{i\in E} p(i, a(i)).$$

Opazimo lahko, da za $a \neq b \in \mathbb{2}^E$ velja $p_a \wedge p_b \leq i \wedge i' = 0$, za nek i, kjer se funkciji razlikujeta. Po drugi strani pa velja
$$1 = \bigwedge_{i\in E} (i \vee i') \overset{(11)}{=} \bigvee_{a\in \mathbb{2}^E} \bigwedge_{i\in E} p(i, a(i)) = \bigvee_{a\in \mathbb{2}^E} p_a. \tag{12}$$

Naj bo K množica vseh $a \in \mathbb{2}^E$, da je $p_a \neq 0$ in za vsako podmnožico X pod K pišimo
$$p_X = \bigvee_{a\in X} p_a. \tag{13}$$

Veljajo naslednje ugotovitve

(1) $p_\emptyset = 0$,
(2) $p_X = 1$,

(3) $p_X \wedge p_Y = p_{X\cap Y}$,
(4) $p_X \vee p_Y = p_{X\cup Y}$,
(5) $p'_X = p_{X'}$,

kjer X' pomeni komplement množice X v K. Prva točka sledi iz tega, da je supremum prazne množice enak 0. Druga točka sledi iz (12) in definicije K. Četrta točka je posledica definicije (13).

$$\begin{aligned} p_X \wedge p_Y = \bigvee_{a\in X} p_a \wedge \bigvee_{b\in Y} p_b = \bigvee_{\substack{a\in X\\ b\in Y}} (p_a \wedge p_b) \\ = \bigvee_{a\in X\cap Y} (p_a \wedge p_a) = \bigvee_{a\in X\cap Y} p_a = p_{X\cap Y} \end{aligned}$$

dokazuje točko tri, peta točka pa sledi iz

$$p_X \wedge p_{X'} = p_{x\cap X'} = p_\emptyset = 0 \qquad \text{in} \qquad p_X \vee p_{X'} = p_{x\cup X'} = p_K = 1,$$

in leme 3.2.

Označimo $C := \{p_X \mid X \subseteq K\}$. Ugotovitve dokazujejo, da je C podalgebra v A. Po (1) je C neprazna, po (6)-(8) pa je zaprta za operacije. Za $a \in K$ je p_a atom. Vsak element iz C se da enolično zapisati kot “join” teh elementov. Če je $p_X = p_Y$, je

$$\begin{aligned} 0 = (p_X \wedge p'_Y) \vee (p'_X \wedge p_Y) = (p_X \wedge p_{Y'}) \vee (p_{X'} \wedge p_Y) \\ = p_{(X\cap Y')\cup(X'\cap Y)} =: p_{X\oplus Y} \end{aligned}$$

kar je enako 0 natanko tedaj, ko je $X \oplus Y = \emptyset$, to pa velja izključno, ko je $X = Y$.

Denimo, da je $F \subseteq E$ in $b \in 2^F$. Pišimo

$$p_b = \bigwedge_{i\in F} p(i, b(i)).$$

Pokazali bomo, da je p_b v C, tako da bomo pokazali

$$p_b = \bigwedge\{p_a \mid a \in K \text{ in } a \text{ razširja } b\}.$$

Naj bo L množica funkcij v K, ki razširjajo b. Če je a v L, potem je $a(i) = b(i)$ in zatorej

$$p(i, b(i)) = p(i, a(i)),$$

za vsak $i \in F$, posledično

$$\{p(i, b(i)) \mid i \in F\} \subseteq \{p(i, a(i)) \mid i \in E\}.$$

Sledi, da

$$p_b = \bigwedge_{i\in F} p(i, b(i)) \geq \bigwedge_{i\in E} p(i, a(i)) = p_a.$$

V drugih besedah,

$$p_b \wedge p_a = p_a \qquad \text{ko} \qquad a \in L.$$

Po drugi strani pa se v primeru $a \notin L$ a in b razlikujeta na nekem argumentu $i \in F$. Eden izmed $p(i, b(i))$ in $p(i, a(i))$ je torej i, drug pa i', torej

$$p_b \wedge p_a \leq p(i, b(i)) \wedge p(i, a(i)) = 0.$$

Torej

$$p_b \wedge p_a = 0 \qquad \text{ko} \qquad a \notin L.$$

Sklenimo razmislek sedaj z

$$p_b = p_b \wedge 1 = p_b \wedge p_K = p_b \wedge \bigvee_{a \in K} p_a = \bigvee_{a \in K} (p_b \wedge p_a) = \bigvee_{a \in L} (p_b \wedge p_a) = \bigvee_{a \in L} p_a$$

Naj bo B podalgebra v A generirana z E. Vzemimo $i \in E$. Če je b funkcija iz $\{i\}$ v $\mathbb{2}$, definirana z $b(i) = 1$, potem je $p_b = p(i, b(i)) = i$ in $i \in C$. Posledično je E vsebovan v C in s tem cel B. Za dokaz druge smeri se moramo spomniti, da je vsak atom p_a končen "meet" elementov iz E in njihovih komplementov. Posledično pripada p_a k B. Element p_X je končen "join" takih elementov in tudi sam pripada B. $\square$

Posledica 5.6. *Vsaka končno generirana Boolova algebra je končna in število njenih elementov je 2^m, kjer je m število atomov v A. Če ima množica generatorjev n elementov, ima kvečjemu 2^n atomov in kvečjemu 2^{2^n} elementov.*

Dokaz. Če ima E n elementov, potem je 2^n funkcij iz E v $\mathbb{2}$. Tako obstaja kvečjemu 2^n atomov. Denima da je m atomov. Vsak element se da zapisati kot "join" atomov in vsak "join" atomov predstavlja nek element. Tedaj je natanko 2^m elementov. $\square$

Posledica 5.7. *Element poljubne Boolove algebre je v podalgebri generirani z E natanko tedaj, ko se da zapisati kot končen "join" končnih "meetov" elementov iz E in njihovih elementov.*

Dokaz. Denimo, da je E podmnožica v Boolovi algebri A. Za vsako končno podmnožico F pod E naj bo B_F podalgebra v A generirana z F in naj bo K_F množica funkcij $b \in$ $\square$

Naj bo A Boolova algebra in B podalgebra. Izkaže se, da se poljubni supremumi in infimumi obnašajo nepohlevno. Supremumi in infimumi lahko spreminjajo vrednosti, lahko jih celo zgubimo ali pa dobimo, ko prehajamo med A in B.

Definicija 5.8. Naj bo A kompletna Boolova algebra in B njena podalgebra. Če za vsako podmnožico B njen supremum (v A) leži v B pravimo, da je B kompletna Boolova podalgebra. Seveda to avtomatično implicira identično trditev za infimume.

Ta definicija je močnejša, kot če bi zahtevali, da je B sama kompletna boolova algebra.

6. Homomorfizmi

Definicija 6.1 (Boolov homomorfizem)**.** Boolov homomorfizem je taka preslikava f iz Boolova algebre B v Boolovo algebro A, da je

$$f(p \wedge q) = f(p) \wedge f(q),$$
$$f(p \vee q) = f(p) \vee f(q),$$
$$f(p') = (f(p))',$$

[8] za vsaka $p, q \in B$.

Z lahkoto se prepričamo, da velja $f(0) = 0$ in $f(1) = 1$. Posledica tega dejstva je, da ne obstaja trivialni homomorfizem med dvema neizrojenima Boolovima algebrama. Prepričamo se lahko tudi, da je $f_*(B)$ podalgebra v A.

[8] Pišemo tudi $f(p)'$.

Definicija 6.2. Izomorfizem Boolovih algeber je bijekcija, ki je hkrati homomorfizem.

Izomorfizem ohranja vse morebitne supremume in infimume, homomorfizem pa v splošnem ne. Homomorfizem imenujemo kompleten, če ohranja vse supremume (in posledično infimume), ki obstajajo.

Lema 6.3. *Boolov monomorfizem f iz B v A je kompleten natanko tedaj, ko je slika $f_*(B)$ regularna podalgebra v A.*

Dokaz. □

7. Razširitve homomorfizmov

Definicija 7.1. Boolov homomorfizem f je razširitev Boolovega homomorfizma g, če je domena g podalgebra domene f in se homomorfizma ujemata na elementih iz domene g.

Trditev 7.2. *Če se dva homomorfizma ujemata na množici generatorjev domene, tedaj se ujemata povsod na domeni.*

Dokaz. Naj bosta $f, g : B \to A$ homomorfizma, ki se ujemata na množici generatorjev E. $C := \{p \in B \mid f(p) = g(p)\}$. Množica E je očitno vsebovana v C, hkrati pa iz $p, q \in C$ in

$$f(p \vee q) = f(p) \vee f(q) = g(p) \vee g(q) = g(p \vee q)$$

sledi, da so $p \vee q$, $p \wedge q$ in p' tudi elementi C. Sklepamo, da je C podalgebra v B, ki vsebuje E, iz česar pa takoj sledi, enakost $C = B$. □

8. Atomi

Definicija 8.1 (Podelement)**.** Naj bo p_0 element Boolove algebre. Podelement elementa p_0 je vsak element p, za katerega velja $p \leq p_0$ oz. ekvivalentno je podelement elementa p_0 vsak element oblike $p_0 \wedge p$ za nek element p.

Definicija 8.2 (Atom)**. Atom** Boolove algebre je neničeln element, ki nima netrivialnih podelementov oz. ko sta njegova edina podelementa natanko 0 in on sam.

Lema 8.3. *Naslednje trditve o elementu q so ekvivalentne:*

1. *q je atom;*
2. *za vsak element p velja natanko ena izmed $q \leq p$ ali $q \wedge p = 0$;*
3. *za vsak element p velja natanko ena izmed $q \leq p$ ali $q \leq p'$;*
4. *$q \neq 0$ in če je q pod $p \vee r$, potem je $q \leq p$ ali $q \leq r$;*
5. *$q \neq 0$ in če je q pod supremumom neke družine $\{p_i\}$, potem je q pod p_i za nek i.*

Dokaz. $1 \Rightarrow 2$) $q \wedge p \leq q$, kar implicira ali $q \wedge p = 0$ ali $q \wedge p = q$ $(q \leq p)$. Če bi veljalo oboje, bi bil $q = 0$, kar pa je protislovje.

$2 \Rightarrow 3$) Če je $q \wedge p = 0$ je

$$q = q \wedge 1 = q \wedge (p \vee p') = (q \wedge p) \vee (q \wedge p') = 0 \vee (q \wedge p') = (q \wedge p'),$$

torej $q \leq p'$. Če bi veljalo oboje, bi veljalo $q \leq 0$, kar pa je možno le če je $q = 0$ in spet dobimo protislovje, saj veljata obe izmed $q \leq p$ ali $q \wedge p = 0$.

$3 \Rightarrow 4$) Če je $q = 0$ dobimo protislovje kot prej. Če ne, je $q \leq p', r'$, potem je $q = q \wedge (p' \wedge r') = q \wedge (p \vee r)'$ in $q \leq (p \vee r)'$.

$4 \Rightarrow 5)$

□

Lema 8.4. *Če je element p supremum množice atomov E, potem je E množica vseh atomov pod p.*

Dokaz. Očitno je vsak element iz E pod p. Če je r nek atom pod p velja, da je r pod nekim atomom $q \in E$, Od tod pa sledi $r = q$. □

Definicija 8.5. Boolova algebra je atomska, če vsak neničeln element dominira vsaj en atom. Boolova algebra je brezatomska, če nima atomov.

Lema 8.6. *Naslednje trditve o Boolovi algebri A so ekvivalentne.*

(1) *A je atomska.*
(2) *Vsak element je supremum atomov, ki jih dominira.*
(3) *Enota je supremum množice vseh atomov.*

Dokaz. $1 \Rightarrow 2)$ Naj bo p element A in E množica atomov, ki jih dominira. Očitno je p zgornja meja te množice. Denimo, da je tudi r zgornja meja te množice. Denimo, da $p \not\leq q$ oz. $p \wedge r' \neq 0$. Ker je A atomska obstaja atom $q \leq (p \wedge r')$. Ker pa je presek na desni pod p je tedaj $q \in E$, $q \leq r$ in

$$q \leq (p \wedge r') \wedge r = p \wedge (r' \wedge r) = p \wedge 0 = 0.$$

Sklepamo lahko, da je $q = 0$, kar je protislovje.

$2 \Rightarrow 3)$ Očitno.

$3 \Rightarrow 1)$ Naj bo E množica vseh atomov in p neničeln element. Tedaj je

$$p = p \wedge 1 = p \wedge \bigvee E = \bigvee \{p \wedge q \mid q \in E\},$$

po lemi 4.6. Ker je p neničeln je gotovo $p \wedge q$ neničeln za nek $q \in E$, to pa je atom pod p. □

Definicija 8.7. Reprezentacija Boolove algebre A (nad množico X) je vložitev A v $\mathcal{P}(X)$. Če reprezentacija ohranja supremume kot unije (torej tudi infimume kot preseke) ji pravimo kompletna. Z drugimi besedami, reprezentacija f je kompletna, ko za vsako družino $\{p_i\}$ s supremumom p velja

$$f(p) = \bigcup_i f(p_i).$$

Izrek 8.8. *Naj bo A atomska Boolova algebra in X množica njenih atomov. Korespondenca*

$$p \to \{q \in X \mid q \leq p\}$$

je kompletna reprezentacija A nad X.

Dokaz. TBD □

Posledica 8.9. *Dve kompletni, atomski Boolovi algebri z enakim številom atomov sta izomorfni. Še več, vsaka bijekcija med množicama atomov se lahko razširi do izomorfizma med algebrama.*

Dokaz. TBD □

9. Končne Boolove algebre

Trditev 9.1. *Končna Boolova algebra je atomska.*

Dokaz. Naj bo p element končne Boolove algebre. p je atom, ali pa obstaja neničeln element p_1, ki je strogo manjši. p_1 je atom (in smo končali), ali pa obstaja neničeln element p_2, ki je strogo manjši in tako naprej. Ker je elementov le končno nonogo se mora ta proces ustaviti in tako dobimo atom, ki je manjši od p. □

Posledica 9.2. *Vsaka končna Boolova algebra A je izomorfna $\mathcal{P}(n)$, kjer je n število atomov v A.*

Dokaz. Končna Boolova algebra je atomska in kompletna. Naj bo n število atomov v njej. $\mathcal{P}(n)$ je tudi atomska kompletna algebra, ki ima n atomov, ki so ravno vse enoelementne množice. Taki pa sta po posledici **??** izomorfni. □

Posledica nam pove, da ni končnih Boolovih algeber moči, ki ni potenca števila 2.

Posledica 9.3. *Končni Boolovi algebri z enakim številom elementov sta izomorfni.*

Dokaz. Denimo da imata končni Boolovi algebri A in B enako število elementov. Obe sta atomski in imata m in n atomov. Po prejšnji lemi je $A \cong \mathcal{P}(n)$ in $B \cong \mathcal{P}(m)$. Ker imata enako število elementov velja $n = m$. Ker sta izomorfni isti Boolovi algebri sta tudi med samo izomorfni. □

Izrek 9.4. *Boolova identiteta velja v $\mathbb{2}$ natanko tedaj, ko jo lahko izpeljemo iz aksiomov iz definicije.*

Trditev 9.5. *Enak nabor identitet velja v vsaki neizrojeni Boolovi algebri.*

Dokaz. Naj bo A poljubna neizrojena Boolova algebra. Identiteta je univerzalna trditev o elementih in operacijah Boolove algebre: če valja v A, velja tudi v vsaki podalgebri, saj so elementi podalgebre med elementi iz A in so operacije le zožitve operacij v A. Ker je A neizrojena vsebuje kopijo $\mathbb{2}$ kot podalgebro, torej lastnosti v A veljajo tudi v $\mathbb{2}$. Če lastnost velja v $\mathbb{2}$, se jo da po prejšnjem izreku izpeljati iz aksiomov, torej velja tudi v A. □

10. Proste Boolove algebre

Definicija 10.1. Množica E generatorjev Boolove algebre B je prosta, če lahko vsako funkcijo iz E v poljubno Boolovo algebro A razširimo do homomorfizma iz B v A. Tedaj pravimo, da E prosto generira B oz. B je prosta na E. Boolova algebra je prosta, če premore prosto množico generatorjev.

Definicijo lahko razložimo s pomočjo naslednjega diagrama. h je identična preslikava iz E v B, g je preslikava, definirana na E, f pa je porojen homomorfizem iz definicije.

$$\begin{tikzcd} E \arrow[r, "h"] \arrow[dr, "g"'] & B \arrow[d, dashed, "f"] \\ & A \end{tikzcd}$$

Posledica trditve 7 je, da je dobljeni homomorfizem enolično določen z g.

Če imamo dve Boolovi algebri B_1 in B_2, ki sta prosti generirani z ekvipolentnima množicama generatorjev E_1 in E_2, sta ti izomorfni. Izomorfizem je porojen z vsako bijekcijo g med E_1 in E_2. Predpostavka o prostosti zagotovi homomorfizma $f_1 : B_1 \to B_2$ in $f_2 : B_2 \to B_1$, ki razširita g in g^{-1}. $f_2 \circ f_1$ je endomorfizem B_1, ki razširi $g^{-1} \circ g$, torej identiteto na E_1. Identiteta na B_1 sama pa je že razširitev te preslikave, torej je zaradi enoličnosti $f_2 \circ f_1 = id_{B_1}$. Podobno vidimo, da je $f_1 \circ f_2 = id_{B_2}$. Torej je f_1 izomorfizem, f_2 pa njegov inverz.

$$\begin{tikzcd} E_1 \arrow[r, "h_1"] \arrow[d, "g"'] & B_1 \arrow[d, dashed, shift left, "f_1"] \\ E_2 \arrow[r, "h_2"'] & B_2 \arrow[u, dashed, shift left, "f_2"] \end{tikzcd} \qquad \begin{tikzcd} E_1 \arrow[r, "h_1"] \arrow[dr, "g^{-1} \circ g"'] & B_1 \arrow[d, dashed, "f_1"] \\ & B_1 \end{tikzcd}$$

Trditev 10.2. *Neskončna prosta Boolova algebra je brezatomska.*

Angleško-slovenski slovar strokovnih izrazov

Boolean algebra Boolova algebra
Degenerate Izrojena
The principle of duality Princip dualnosti
Lower (upper) bound Spodnja(zgornja) meja
Least upper bound Najmanjša zgornja meja
Greatest lower bound Največja spodnja meja
Complete Boolean algebra Kompletna Boolova algebra
Finite-cofinite Boolean algebra Končno-končna Boolova algebra
Countable-cocountable Boolean algebra Števno-števna Boolova algebra
Atom Atom

Literatura

[1] Givant, Steven; Halmos, Paul. "Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)," Springer (2009).
[2] Jonsson, W. (1970) 'Boolean Algebras. by Roman Sikorski. Ergebnisse der Math. 25 Springer Verlag, New York, 1969 (third edition)

Luka Ponikvar, Fakulteta za matematiko in fiziko, Oddelek za matematiko, Jadranska 21, 1000 Ljubljana, Slovenija
Email address: lp29353@student.uni-lj.si