PROSTE BOOLOVE ALGEBRE

LUKA PONIKVAR

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Namen članka je predstaviti proste Boolove algebre. Logično je razdeljen na dva dela. Prvi del, ki obsega prvih deset poglavij, predstavlja splošno teorijo Boolovih algeber. Teorijo, ki je tu razvita, se sprida uporabi v drugem delu članka, ki obsega zadnje poglavje, naslovljeno Proste Boolove algebre. Najprej se pokaže enoličnost prostih Boolovih algeber, nato pa se v preostanku ugotavlja njihov obstoj. Članek se zaključi s konstrukcijo primera neskončne proste Boolove algebre.

FREE BOOLEAN ALGEBRAS

The purpose of the article is to present free Boolean algebras. It is logically split into two parts. The first part, consisting of the first ten chapters, presents the general theory of Boolean algebras. The theory developed there, will serve well in tackling the second part, namely the final chapter titled Free Boolean Algebras. First uniqueness of such algebras will be shown and then we will continue by studying their existence. The article will conclude with a construction of an infinite free Boolean algebra.

1. Uvod

Teorija Boolovih algeber seže nazaj vse do leta 1847, ko jo je začel razvijati George Boole. 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 samostojna moderna matematična disciplina z daljnosežnimi izreki in pomembnimi povezavami z drugimi vejami matematike, kot so algebra, logika in teorija mere, če jih naštejemo le nekaj. Za to sta nedvomno najbolj zaslužna Marshall Stone in Alfred Tarski.

2. Boolove algebre

Motivacija za osnovno definicijo izhaja iz potenčne množice dane množice in operacij na njej.

Definicija 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]:

[1] Imenujemo jo „ join“ oz. „ali“.
[2] Imenujemo jo „meet“ oz. „in“.
[3] Imenujemo jo komplement, označujemo pa tudi kot $'$.
[4] Komplement ima najvišjo prioriteto, medtem ko ima „in“ višjo prioriteto kot „ali“.

$$
\begin{aligned}
\neg 0 &= 1, & \neg 1 &= 0, \\
p \wedge 0 &= 0, & p \vee 1 &= 1, \\
p \wedge 1 &= p, & p \vee 0 &= p, \\
p \wedge \neg p &= 0, & p \vee \neg p &= 1, \\
\neg\left(\neg p\right) &= p, & & \\
p \wedge p &= p, & p \vee p &= p, \\
\neg\left(p \wedge q\right) &= \neg p \vee \neg q, & \neg\left(p \vee q\right) &= \neg p \wedge \neg q, \\
p \wedge q &= q \wedge p, & p \vee q &= q \vee p, \\
p \wedge \left(q \wedge r\right) &= \left(p \wedge q\right) \wedge r, & p \vee \left(q \vee r\right) &= \left(p \vee q\right) \vee r, \\
p \wedge \left(q \vee r\right) &= \left(p \wedge q\right) \vee \left(p \wedge r\right), & p \vee \left(q \wedge r\right) &= \left(p \vee q\right) \wedge \left(p \vee r\right).
\end{aligned}
$$

Primer 2 (Izrojena Boolova algebra). Najenostavnejši primer Boolove algebre je potenčna množica prazne množice:

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

Imenujemo jo *izrojena* Boolova algebra. Operacije na tej množici definiramo kot konstantne preslikave, ki vse slikajo v

$$0 = 1 = \emptyset.$$

Primer 3 (Boolova algebra z dvema elementoma). Najmanjši primer neizrojene Boolove algebre je potenčna množica enojca[5]:

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

Taka Boolova algebra ima le dva elementa:

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

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

,

komplement pa 0 preslika v 1 in obratno.

Primer 4 (Potenčna množica kot Boolova algebra). Osnovni primer Boolove algebre je potenčna množica neprazne množice X. Omenili smo že, da je to osnovna motivacija za definicijo. Tu sta $\emptyset$ element 0 in X element 1. Operacija presek predstavlja *in*, unija *ali*, komplement pa je naraven komplement iz teorije množic.

Zdaj, ko smo razložili začetne primere in vemo, s čim se bomo ukvarjali, se urno napotimo k zanimivejšim.

[5] Edini element množice smo označili kar z ∞.

Primer 5 (Končno-kokončna Boolova algebra). Oglejmo si določeno podmnožico potenčne množice $\mathcal{P}(X)$. Če definiramo $A := \{B \subset X \mid B \text{ končna ali } B' \text{ končna}\}$, dobimo Boolovo algebro, imenovano končno-kokončna Boolova algebra. Tu operacije in njuni enoti definiramo enako kot v primeru 4. Bralec se lahko prepriča, da A res postane Boolova algebra, pozoren bralec pa bo opazil tudi, da v primeru, ko je X končna, Boolova algebra $\mathcal{P}(X)$ in končno-kokončna Boolova algebra na X sovpadata.

Lahko se omejimo tudi na števne množice in dobimo števno-koštevno Boolovo algebro. Premislek v resnici deluje za poljubno kardinalnost.

3. Princip dualnosti

Definicija 6 (Boolov polinom). *Boolov polinom* je izraz, sestavljen iz konstant 0 in 1 ter neznank $p_0, \ldots, p_n$ s pomočjo standardnih operacij *in*, *ali* ter komplementa.

Primer 7. Primer polinoma je

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

Ta polinom je na pogled zelo podoben polinomu

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

kar motivira naslednjo opazko.

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

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

Če smo bolj natančni, ostajajo naslednje funkcije, ki bijektivno preslikajo množico vseh Boolovih polinomov $\mathcal{BP}$ nazaj nase:

1. identična funkcija:
$$\mathrm{id} : \mathcal{BP} \to \mathcal{BP}$$
$$\mathrm{id} : f(p_1, \ldots, p_n) \mapsto f(p_1, \ldots, p_n)\,,$$
2. komplementna funkcija:
$$\mathrm{c} : \mathcal{BP} \to \mathcal{BP}$$
$$\mathrm{c} : f(p_1, \ldots, p_n) \mapsto f'(p_1, \ldots, p_n)\,,$$
3. dualna funkcija:
$$\mathrm{d} : \mathcal{BP} \to \mathcal{BP}$$
$$\mathrm{d} : f(p_1, \ldots, p_n) \mapsto f'\left(p_1', \ldots, p_n'\right),$$
4. kontradualna funkcija:
$$\mathrm{k} : \mathcal{BP} \to \mathcal{BP}$$
$$\mathrm{k} : f(p_1, \ldots, p_n) \mapsto f\left(p_1', \ldots, p_n'\right).$$

Množica $G = \{\mathrm{id}, \mathrm{c}, \mathrm{d}, \mathrm{k}\}$ skupaj z operacijo kompozituma $\circ$ je abelova grupa, kar lahko vidimo iz spodnje tabele:

$\circ$	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 8 (Princip dualnosti). Opazimo lahko, da aksiomi iz definicije 1 za Boolove algebre nastopajo v dualnih parih. Princip dualnosti temelji na tej opazki, in sicer pove, da vse posledice teh aksiomov, splošne trditve o Boolovih algebrah in njihovi dokazi prav tako nastopajo v dualnih parih. Pomembno je to, da z dokazom neke trditve ne dokažemo le te, vendar brezplačno dobimo še dokaz dualne trditve. Lema 11 bo to dejstvo še dodatno osvetlila.

4. Urejenost

V tem razdelku delujemo v poljubni Boolovi algebri.

Lema 9. *Če je $p \vee q = p$ za vse p, potem je $q = 0$. Če pa je $p \wedge q = p$ za vse p, je $q = 1$.*

Dokaz. V prvem primeru postavimo $p = 0$ in dobimo $0 = 0 \vee q = q$, kjer je zadnji enačaj posledica definicije 1. Podobno za $p = 1$ sledi $1 = 1 \wedge q = q$. ∎

Lema 10. *Če sta p in q taka, da je $p \wedge q = 0$ in $p \vee q = 1$, potem je $q = p'$.*

Dokaz. Lema sledi iz naslednje verige enakosti:

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

Lema 11. *Veljata naslednji dve enakosti: $(p \vee q) \wedge p = p$ in $(p \wedge q) \vee p = p$.*

Dokaz. Imamo:

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

Druga formula sledi iz principa dualnosti, a ker ga tu prvič uporabimo, si oglejmo, kako bi izgledal dokaz dualne trditve:

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

Vsak korak v drugem delu dokaza je dualen ustreznemu koraku iz prvega dela. ■

Lema 12. *Enakost $p \wedge q = p$ velja natanko tedaj, ko velja enakost $p \vee q = q$.*

Dokaz. Naj bo $p \wedge q = p$, torej je:

$$\begin{aligned}p \vee q &= (p \wedge q) \vee q\\ &= (p \vee q) \wedge (q \vee q)\\ &= (p \vee q) \wedge q\\ &= q,\end{aligned}$$

kjer zadnja enakost sledi iz leme 11. Drugo implikacijo dobimo z zamenjavo p in q ter formiranjem dualov. ■

Definicija 13 (Urejenost). Na vsaki Boolovi algebri lahko vpeljemo *urejenost*:

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

Prejšnja lema nam pove, da je $p \leq q$ ekvivalentno zahtevi $p \vee q = q$.

Lema 14. *Relacija $\leq$ je delna urejenost.*

Dokaz. Refleksivnost sledi iz definicije. Dokaza antisimetričnosti in tranzitivnosti sta skoraj očitna. Dokaz prve se opre na enakosti $p = p \wedge q = q \wedge p = q$, slednja pa sledi iz dejstva, da $p \leq q$ in $q \leq r$ implicirata $p \wedge r = (p \wedge q) \wedge r = p \wedge (q \wedge r) = p \wedge q = p$. ■

Lema 15. *Veljajo naslednje trditve.*

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

Dokaz. Prva točka je očitna posledica definicije. Če privzamemo $p \wedge q = p$ in $r \wedge s = r$, imamo $(p \wedge r) \wedge (q \wedge s) = (p \wedge r) \wedge (q \wedge s)\,(p \wedge q) \wedge (r \wedge s) = p \wedge r$, kar dokazuje prvi del točke (2). Drugi del sledi s pomočjo leme 12. Če je $p \wedge q = p$ po komplementu obeh strani sledi, da je $p' \vee q' = p'$, kar pa je bilo potrebno dokazati pri točki (3). ■

Definicija 16 (Meje). Če je E podmnožica 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 17 (Prazna množica). Če je $E = \emptyset$, je za vsak element pogoj za zgornjo mejo te množice na prazno izpolnjen. Tedaj ima E supremum, in sicer kar element 0. Podoben razmislek nas privede do zaključka, da je infimum množice E element 1.

Primer 18 (Enojec). Če je $E = \{p\}$, je p tako zgornja kot tudi spodnja meja za E. Sledi, da je p infimum in supremum množice E.

Lema 19. *Za vsaka p in q ima množica $\{p, q\}$ supremum enak $p \vee q$ in infimum enak $p \wedge q$.*

Dokaz. Očitno je $p \vee q$ zgornja meja te množice. Zaradi točke 2 v lemi 15 pa je to tudi natančna zgornja meja: če je $p \leq r$ in $q \leq r$, je $p \wedge q \leq r \wedge r = r$. Drugi del sledi z uporabo principa dualnosti. ∎

Opomba 20 (Supremum in infimum končne in neskončne množice). Lema 19 zagotavlja obstoj supremuma in infimuma dvoelementne množice. Lahko bi jo posplošili in ugotovili, da ima poljubna končna neprazna množica E infimum, ki ga bomo označevali z $\bigwedge E$ in supremum, ki ga bomo označevali z $\bigvee E$.

Za neskončno množico E podobna trditev ne drži. Infimum in supremum tedaj ne obstajata vedno. Če obstaja prvi, ga označimo z $\bigwedge E$, če pa obstaja slednji, ga označimo z $\bigvee E$.

Primera 17 in 18 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:

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

5. Kompletne Boolove algebre

Končno-kokončna 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:

$$\{\{n\} \ \mid n \text{ sodo naravno število}\}.$$

To motivira naslednjo definicijo:

Definicija 21 (Kompletna Boolova algebra). Boolova algebra, v kateri ima vsaka podmnožica infimum in supremum, se imenuje *kompletna Boolova algebra.*

Opomba 22. Vsaka končna Boolova algebra je kompletna.

Lema 23. *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, iz leme 15 sledi, da je $p' \leq p_i'$ za vsak i. Če je $q \leq p_i'$ za vse i, je tudi $p_i \leq q'$ za vse i in tako po definiciji supremuma $p \leq q'$, kar implicira $q \leq p'$. Torej je p' res $\bigwedge_i p_i'$.

Dualni argument utemelji, da iz $p = \bigwedge_i p_i$ sledi $p' = \bigvee_i p_i'$. Da dokažemo še obratni smeri, pa lahko ravnokar dokazana dejstva uporabimo na družini komplementov $\{p_i'\}$. ∎

Posledica 24 (Zadosten pogoj za kompletnost). *Če ima vsaka podmnožica Boolove algebre supremum (infimum), potem je ta Boolova algebra kompletna.*

Oglejmo si nekaj lastnosti natančnih zgornjih (spodnjih) mej, natančneje njihovo asociativnost in distributivnost. O komutativnosti ni smisla govoriti, saj je supremum (infimum) pripisan neki množici elementov, torej neodvisno od njihove urejenosti.

Lema 25 (Asociativnost). *Naj bo J neka indeksna množica. Če je $\{I_j\}_{j\in J}$ družina množic z unijo I in je p_i element Boolove algebre za vsak $i \in I$, tedaj je*

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

Enačbi povesta, da obstoj supremumov (infimumov) na levi implicira obstoj supremuma (infimuma) na desni in želeno enakost.

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

Dualni argument utemelji še drugo enakost. ∎

Lema 26. *Če je p element in $\{q_i\}$ družina elementov v neki Boolovi algebri, potem*

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

Enačba pove, da obstoj leve strani implicira obstoj desne in njuno enakost.

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 zaradi leme 15 velja:

$$q_i = 1 \wedge q_i = (p \vee p') \wedge q_i = (p \wedge q_i) \vee \big(p' \wedge q_i\big) \leq r \vee \big(p' \wedge q_i\big) \leq r \vee p'.$$

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

$$p \wedge q \leq p \wedge \big(r \vee p'\big) = (p \wedge r) \vee \big(p \wedge p'\big) = (p \wedge r) \vee 0 = (p \wedge r) \leq r,$$

kar dokazuje želeno enakost. ∎

Posledica 27. *Če sta $\{p_i\}$ in $\{q_j\}$ družini elementov v Boolovi algebri, potem je*

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

Enačba pove, da obstoj supremumov na levi implicira obstoj supremuma na desni in želeno enakost.

6. Podalgebre

Definicija 28 (Boolova podalgebra). *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, ki ima le dva elementa, in sicer 0 in 1, ostale podalgebre pa imamo za netrivialne. Vsaka Boolova algebra A premore tudi nepravo podalgebro A, vse ostale podalgebre so prave.

Ker imamo v tem besedilu opravka izključno z Boolovimi algebrami in njihovimi Boolovimi podalgebrami, bomo te včasih krajše označevali le kot podalgebre.

Opomba 29. 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 B vseh podalgeber, ki vsebujejo E (vsaj ena taka obstaja, namreč A). Presek B je najmanjša podalgebra, ki vsebuje E. Rečemo, da je B *generirana* z E oz. da je E *množica generatorjev* za B.

Primer 30. Vzemimo $E = \emptyset$. Podalgebra, ki jo ta množica generira, je najmanjša podalgebra, ki jo A premore, torej $\mathbb{2}$.

Če za množico generatorjev vzamemo kar neko podalgebro, bo ta generirala samo sebe.

Definicija 31 (Končno generirana Boolova podalgebra). Podalgebra Boolove algebre A je *končno generirana*, če je generirana s kakšno končno podmnožico A.

7. Homomorfizmi

Definicija 32 (Boolov homomorfizem). *Boolov homomorfizem* je taka preslikava f iz Boolove 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 $f(1) = 1$. Posledično trivialni homomorfizem med dvema neizrojenima Boolovima algebrama ne obstaja. Prepričamo se lahko tudi, da je $f(B)$ podalgebra v A.

Definicija 33 (Izomorfizem). *Izomorfizem Boolovih algeber* je bijekcija, ki je hkrati homomorfizem.

Definicija 34 (Razširitev homomorfizma). 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 35. *Če se dva homomorfizma ujemata na množici generatorjev domene, potem se ujemata povsod na domeni.*

[8] Pišemo tudi $f(p)'$.

Dokaz. Naj bosta $f, g : B \to A$ homomorfizma, ki se ujemata na množici generatorjev E, in naj bo $C := \{p \in B \mid f(p) = g(p)\}$. 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 $C = B$. ∎

Za dokaz obstoja prostih Boolovih algeber bomo potrebovali naslednji izrek o razširitvah homomorfizmov.

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 $\mathbb{2}^E$ za vse funkcije iz E v $\mathbb{2}$ in za vsak $a \in \mathbb{2}^E$ vpeljimo

$$p_a := \bigwedge_{i \in E} p(i, a(i)).$$

Izrek 36. *Preslikavo g iz množice generatorjev E Boolove algebre B v Boolovo algebro A se da razširiti do homomorfizma iz B v A natanko tedaj, ko za vsako funkcijo $a : F \to \mathbb{2}$, definirano na končni podmnožici $F \subseteq E$ velja, da*

$$\bigwedge_{i \in F} p(i, a(i)) = 0 \quad \textit{implicira} \quad \bigwedge_{i \in F} p(g(i), a(i)) = 0.$$

Dokaz izreka lahko bralec najde v [1].

8. Atomi

Definicija 37 (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: *podelement* elementa p_0 je vsak element oblike $p_0 \wedge p$ za nek element p. Če je p podelement p_0, rečemo, da p_0 *dominira* p.

Definicija 38 (Atom). *Atom* Boolove algebre je neničeln element, ki nima neničelnih podelementov oz. sta njegova edina podelementa natanko 0 in on sam.

Bralec se lahko prepriča, da velja naslednja preprosta lema.

Lema 39. *Naslednje trditve so ekvivalentne:*

1. *element 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. *velja $q \neq 0$ in če je q podelement $p \vee r$, potem je $q \leq p$ ali $q \leq r$,*
5. *velja $q \neq 0$ in če je q podelement supremuma neke družine $\{p_i\}$, potem je q podelement p_i za nek i.*

Lema 40. *Če je element p supremum množice atomov E, potem je E množica vseh atomov, ki jih p dominira.*

Dokaz. Očitno je vsak element iz E dominiran s p. Če je r nek atom, dominiran s p, je po lemi 39 r podelement nekega atoma $q \in E$. Od tod sledi $r = q$. ∎

Definicija 41 (Atomske in brezatomske Boolove Algebre). Boolova algebra je *atomska*, če ima vsak neničeln element za podelement vsaj en atom. Boolova algebra je *brezatomska*, če nima atomov.

Tu je na mestu opozorilo, da si pojma atomska in brezatomska nista nasprotna.

Lema 42. *Naslednje trditve o Boolovi algebri A so ekvivalentne:*

1. *A je atomska,*
2. *vsak element je supremum atomov, ki jih dominira,*
3. *element 1 je supremum množice vseh atomov.*

Dokaz. (1) ⇒ (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 $p \nleq r$ oz. $p \wedge r' \neq 0$. Ker je A atomska, obstaja atom $q \leq (p \wedge r')$. Ker pa je presek na desni podelement p, je tedaj $q \in E$, $q \leq r$ in

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

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

(2) ⇒ (3) Očitno.

(3) ⇒ (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 26. Ker je p neničeln, je gotovo $p \wedge q$ neničeln za nek $q \in E$, to pa je atom dominiran s p. ∎

Definicija 43 (Reprezentacija). *Reprezentacija* Boolove algebre A (nad množico X) je vložitev A v $\mathcal{P}(X)$.

Naslednji izrek, ki ga bomo navedli brez dokaza, nam pove, da ima vsaka Boolova algebra reprezentacijo. Radoveden bralec dokaz najde v [1].

Izrek 44. *Naj bo X množica vseh homomorfizmov $f : A \to \mathbb{2}$ na Boolovi algebri A. Potem se A da vložiti v $\mathcal{P}(X)$ s preslikavo s predpisom:*

$$f(p) = \{x \in X \mid x(p) = 1\}$$

za vsak p v A.

Izrek 45. *Naj bo B podalgebra, generirana s končno množico E. Atomi v B so neničelni elementi oblike*

$$p_a = \bigwedge_{i \in E} p(i, a(i)),$$

kjer je $a \in \mathbb{2}^E$, elementi B pa so oblike

$$\bigvee_{a \in A \subseteq E} p_a.$$

Za vsak element B je ta zapis enoličen.

Dokaz tega izreka se prav tako nahaja v [1], navedli pa smo ga zaradi zelo pomembne posledice.

Posledica 46. *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 po izreku 45 obstaja kvečjemu 2^n atomov. Denimo, da je atomov m. Vsak element se da zapisati kot *„in“* atomov in vsak *„in“* atomov predstavlja nek element. Zaradi enoličnosti zapisa to nanese natanko 2^m elementov. ∎

9. Končne Boolove algebre

Trditev 47. *Končna Boolova algebra je atomska.*

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

Naslednjega izreka ni težko dokazati, a bi nas zaneslo predaleč s poti. Dokaz se nahaja v [1].

Izrek 48. *Naj* $\mathcal{P}(n)$ *označuje množico* $\{1, 2, \ldots, n\}$*. Vsaka končna Boolova algebra* A *je izomorfna* $\mathcal{P}(n)$*, kjer je* n *število atomov v* A*.*

Posledica 49. *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 n atomov. Po prejšnji lemi je $A \cong \mathcal{P}(n)$ in $B \cong \mathcal{P}(n)$. Ker sta obe izomorfni isti Boolovi algebri, sta tudi med sabo izomorfni. ∎

10. Proste Boolove algebre

Preden se lotimo definicije, razvijmo intuicijo. Prostost generatorjev povezujemo z „odsotnostjo relacij med njimi“. Bralec pozna pojem linearno neodvisnih vektorjev. Kaj nam to pove? Ravno to, da med linearno neodvisnimi vektorji ni nobenih netrivialnih relacij. Vsaka relacija, na primer $v_1 + 2v_3 = v_7$, nam netrivialno reši enačbo

$$\sum_{i=1}^{n} \alpha_i v_i = 0,$$

kar pa je v protislovju z linearno neodvisnostjo vektorjev. Ker v drugih algebrajskih strukturah nimamo množenja s skalarji, moramo ta pogoj prevesti v jezik tiste algebrajske strukture. V našem primeru nam to da naslednjo definicijo:

Definicija 50 (Prosta Boolova algebra). Množica generatorjev E 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. Preslikava h je identična preslikava iz E v B, preslikava g je definirana na E, preslikava f pa je porojen homomorfizem iz definicije.

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

Iz trditve 35 sledi, da je dobljeni homomorfizem enolično določen z g.

Če imamo dve Boolovi algebri B_1 in B_2, ki sta prosti in 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}, kot kaže spodnji diagram na levi. Preslikava $f_2 \circ f_1$ je endomorfizem B_1, ki razširi $g^{-1} \circ g$, torej identiteto na E_1, kar vidimo na desnem diagramu spodaj. Sama identiteta na B_1 pa je že razširitev te preslikave, torej je po lemi 35 zaradi enoličnosti razširitve $f_2 \circ f_1 = \mathrm{id}_{B_1}$. Podobno vidimo, da je $f_1 \circ f_2 = \mathrm{id}_{B_2}$. Torej je f_1 izomorfizem, f_2 pa njegov inverz.

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

V teoriji prostih Boolovih algeber, ki smo jo predstavili do sedaj, nastopa velika luknja. Čeprav vemo vse o njihovi enoličnosti, v tem trenutku ne vemo čisto nič o njihovem obstoju. Naš naslednji cilj je vzpostaviti dejstvo, da za vsako kardinalno število obstaja Boolova algebra, ki je prosta na množici generatorjev s to kardinalnostjo.

Definicija 51 (Projekcija). Naj bo I poljubna množica in $S = \mathbb{2}^I$. Elementi S so funkcije iz I v $\mathbb{2}$, torej funkcije x z argumenti i iz I in vrednostmi $x(i) = x_i$, ki so ali 1 ali 0. V $\mathbb{2}^S$ funkcije oblike

$$p_i : S \to \mathbb{2}$$

$$p_i(x) = x_i$$

imenujemo *projekcije*.

Lema 52. *Množica generatorjev E Boolove algebre B je prosta, če in samo če za vsako funkcijo $a \in \mathbb{2}^F$, kjer je F končna podmnožica E, velja*

$$\bigwedge_{i \in F} p(i, a(i)) \neq 0. \tag{1}$$

Dokaz. Lema na prazno drži, če je B izrojena Boolova algebra, kajti nobena množica generatorjev ni prosta in nobena množica generatorjev ne izpolnjuje pogojev leme.

Denimo, da E prosto generira B. Vzemimo funkcijo $a : F \to \mathbb{2}$, kjer je F končna podmnožica E. Naj bo $g : E \to \mathbb{2}$ poljubna funkcija, ki se z a ujema na F, recimo

$$g(i) = \begin{cases} a(i) & \text{če je } i \in F, \\ 0 & \text{sicer.} \end{cases}$$

Pokažimo, da za $i \in F$ velja $p(g(i), a(i)) = 1$. Če je $a(i) = 1$, je $p(g(i), a(i)) = g(i) = a(i) = 1$ in če je $a(i) = 0$, je $p(g(i), a(i)) = g(i)' = a(i)' = 0' = 1$.

Posledično je $\bigwedge_{i \in F} p(g(i), a(i)) = 1$.

Po predpostavki obstaja razširitev funkcije g na cel B. Če bi veljalo $\bigwedge_{i\in F} p(i, a(i)) = 0$, bi po izreku 36 veljalo tudi $\bigwedge_{i\in F} p(g(i), a(i)) = 0$, kar vodi do protislovja.

Denimo sedaj, da velja (1). Izrek 36 pove, da se tedaj vsako preslikavo $g : E \to A$ iz E da razširiti do homomorfizma iz B v A. ∎

Izrek 53. *Za vsako množico I je Boolova podalgebra $\mathbb{2}^{\mathbb{2}^I}$, generirana z množico projekcij $E = \{p_i \mid i \in I\}$, prosto generirana z E.*

Dokaz. Naj bo B Boolova podalgebra $\mathbb{2}^{\mathbb{2}^I}$, generirana z množico E. Dovolj je pokazati, da drži pogoj iz leme 52. Pri preverjanju pogoja si lahko poenostavimo notacijo in gledamo funkcije z vrednostmi v $\mathbb{2}$ iz končnih podmnožic I in ne iz končnih podmnožic E.

Naj bo $a \in \mathbb{2}^F$, kjer je F končna podmnožica I. Naj bo x poljuben element iz $\mathbb{2}^I$, ki razširja a (na primer vzemimo, da je $x_i = 0$ za vsak $i \in I - F$). Enostaven račun pokaže, da je

$$p(p_i, a(i))(x) = 1$$

za vsak $i \in F$. Res, če je $a(i) = 1$, je

$$p(p_i, a(i))(x) = p(p_i, 1)(x) = p_i(x) = x(i) = a(i) = 1,$$

in če je $a(i) = 0$, je

$$p(p_i, a(i))(x) = p(p_i, 0)(x) = p_i'(x) = p_i(x)' = x(i)' = a(i)' = 0' = 1.$$

Če pišemo

$$p_a = \bigwedge_{i\in F} p(p_i, a(i)),$$

prejšnji argument pokaže, da je

$$p_a(x) = \bigwedge_{i\in F} p(p_i, a(i))(x) = 1.$$

Posledično lahko zaključimo, da p_a ni ničeln element B (funkcija z domeno $\mathbb{2}^I$, ki je identično enaka 0). Ker drži pogoj iz leme 52, je podalgebra, generirana z E, prosta. ∎

Privzemimo sedaj v skladu z von Neumannovo definicijo naravnega števila, da je naravno število m množica svojih predhodnikov: $m = \{0, 1, \ldots, m-1\}$.

Trditev 54. *Za vsako naravno število m, je Boolova algebra $\mathbb{2}^{\mathbb{2}^m}$ prosto generirana z m generatorji.*

Dokaz. Pišimo $S = \mathbb{2}^m$ in $A = \mathbb{2}^S$. Po izreku 53 ima množica $E = \{p_i \mid i \in m\}$ moč m in prosto generira podalgebro A. Pokazali bomo, da je omenjena generirana podalgebra kar cel A.

Za vsak $a \in S$ kot v izreku 45 pišimo

$$p_a := \bigwedge_{i\in m} p(p_i, a(i)), \tag{2}$$

ki vedno obstaja, saj je m končna. Element p_a je očitno generiran z E, velja pa tudi:

$$p_a(x) = 1 \iff x = a, \tag{3}$$

za vsak $x \in S$. Res, p_a je infimum elementov $p(p_i, a(i))(x) \in \{0, 1\}$ in je enak 1 le, ko je $p(p_i, a(i))(x) = 1$ za vsak i v m. Definicija p implicira, da je

$$p(p_i, a(i))(x) = p_i(x) = x_i \quad \text{ali} \quad p(p_i, a(i))(x) = p_i'(x) = x_i',$$

glede na to, ali je $a(i)$ enak 0 ali 1. Posledično moramo imeti $x_i = 1$, ko je $a(i) = 1$, in $x_i = 0$, ko je $a(i) = 0$, če želimo, da je $p_a(x) = 1$. To dokazuje (3).

Za vsako podmnožico X v S postavimo

$$p_X = \bigvee_{a \in X} p_a.$$

Ta supremum ponovno obstaja, saj je S in s tem X končna, enako očitno kot prej pa je tudi ta element generiran z E. Iz (3) sledi, da za vsak $x \in S$ velja

$$p_X(x) = 1 \iff x \in X.$$

Poljuben element $q \in A$ je enolično določen s tistimi x iz S, za katere je $q(x) = 1$. Če to množico označimo z X, velja

$$\begin{aligned} q(x) = 1 &\iff x \in X \\ &\iff p_X(x) = 1, \end{aligned}$$

torej je $q = p_X$. Posledično vsi elementi A sovpadajo s p_X za nek $X \subseteq S$ in je torej q generiran z E, kar smo želeli pokazati. ∎

Opomba 55. Iz dokaza je razvidno, da so elementi iz (2) atomi.

Trditev 56. *Neskončna prosta Boolova algebra je brezatomska.*

Končno generirana Boolova algebra je po posledici 46 končna, kar pa po izreku 47 pomeni, da je atomska. Torej se moramo v trditvi res omejiti na neskončne Boolove algebre, te pa so, kot smo videli, gotovo generirane z neskončno množico prostih generatorjev.

Dokaz. Naj bo I neskončna množica z m elementi (tu je m neko kardinalno število). Po izreku 53 je Boolova algebra, generirana z m generatorji, do izomorfizma natančno podalgebra B Boolove algebre $\mathbb{2}^{\mathbb{2}^I}$, ki je generirana z množico projekcij

$$E = \{p_i \mid i \in I\}.$$

Pokazali bomo, da je

$$B = \bigcup_{F \subseteq I} B_F, \tag{4}$$

kjer je B_F podalgebra, generirana s končno podmnožico projekcij

$$E_F = \{p_i \mid i \in F\},$$

F pa teče po vseh končnih podmnožicah I. Vsaka B_F je končno generirana in po enakem razmisleku kot prej atomska. Njeni atomi so po izreku 45 oblike

$$p_a = \bigwedge_{i \in F} p(p_i, a(i)),$$

kjer je $a \in \mathbb{2}^F$. Vsi ti elementi pa so po lemi 52 neničelni.

Da dokažemo trditev, je dovolj pokazati, da vsak atom p_a v B_F dominira dva disjunktna, neničelna elementa iz B. Opozorimo, da takih elementov gotovo ne bomo našli v B_F. Naj bo i_0 nek indeks v I, ki ni v F. Funkcija a ima dve razširitvi, denimo b in c, do funkcij iz $F \cup \{i_0\}$ v $\mathbb{2}$, za kateri zahtevamo:

$$b(i_0) = 1 \quad \text{in} \quad c(i_0) = 0.$$

Elementa

$$p_b = \bigwedge_{i \in F \cup \{i_0\}} p(p_i, b(i)) \quad \text{in} \quad p_c = \bigwedge_{i \in F \cup \{i_0\}} p(p_i, c(i))$$

v B sta neničelna in očitno podelementa p_a. Disjunktna sta, saj je

$$p_b \wedge p_c \leq p(p_{i_0}, b(i_0)) \wedge p(p_{i_0}, c(i_0)) = p(p_{i_0}, 1) \wedge p(p_{i_0}, 0) = p_{i_0} \wedge p'_{i_0} = 0.$$

Dokažimo še (4). Najprej se prepričamo, da je unija na desni res podalgebra. Vzemimo elementa $p, q \in \bigcup_{F \subseteq I} B_F$. Oba pripadata nekima podalgebrama iz unije, recimo $p \in B_{F_1}$ in $q \in B_{F_2}$. Tedaj oba pripadata podalgebri $B_{F_1 \cup F_2}$ in očitno so tudi $p \wedge q, p \vee q, p', q' \in B_{F_1 \cup F_2} \subseteq \bigcup_{F \subseteq I} B_F$. Dokažimo sedaj, da sta podalgebri iz (4) enaki. Hitro vidimo, da je $\bigcup_{F \subseteq I} B_F$ vsebovana v B. Vemo tudi, da je za vsak element $k \in E$ podalgebra, generirana s $\{k\}$, vsebovana v $\bigcup_{F \subseteq I} B_F$, torej je E vsebovana v $\bigcup_{F \subseteq I} B_F$ in je po definiciji tudi $B \subseteq \bigcup_{F \subseteq I} B_F$. ∎

Opomba 57. Iz dokaza je razvidno, da je prosta Boolova algebra, generirana z m generatorji, kardinalnosti m. Torej je nemogoče pričakovati, da bi trditev 54 veljala za splošna kardinalna števila. Ko je m neskončno kardinalno število, je prosta Boolova algebra, generirana z m elementi, kardinalnosti m, $\mathbb{2}^{\mathbb{2}^m}$ pa ima kardinalnost strogo več kot m.

Primer 58 (Neskončna prosta Boolova algebra). *Levi polzaprt interval* ali (ker ne bomo omenjali drugih) *polzaprt interval* je množica ene izmed oblik:

$$\begin{aligned} [a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\}, \\ [a, \infty) &= \{x \in \mathbb{R} \mid a \leq x\}, \\ (-\infty, b) &= \{x \in \mathbb{R} \mid x < b\}, \\ (-\infty, \infty) &= \mathbb{R}, \end{aligned}$$

kjer sta seveda $a, b \in \mathbb{R}$ in $a < b$.

Označimo z A množico vseh končnih unij polzaprtih intervalov. A vsebuje $\mathbb{R}$ in kot prazno unijo tudi $\emptyset$. Zaprtost A za operacijo unije je očitna. Utemeljimo zdaj še zaprtost za komplement. Najprej opazimo, da je presek dveh polzaprtih intervalov polzaprt interval ali pa je prazen. Tu bi morali ločiti veliko primerov, je pa bralcu toplo priporočeno, da to stori za vajo. Nato opazimo, da je komplement polzaprtega intervala unija kvečjemu dveh polzaprtih intervalov. Če je P končna unija polzaprtih intervalov, je P' po De Morganovem zakonu končen presek komplementov polzaprtih intervalov. Zaradi druge opazke je to končen presek družine množic, vsaka pa je sestavljena iz unije kvečjemu dveh polzaprtih intervalov. Zaradi distributivnega pravila je to enako končni uniji končnih presekov polzaprtih intervalov. Po prvi opazki se to da zapisati kot končno unijo polzaprtih intervalov (morebitne prazne množice odstranimo iz unije). Množica A je torej zaprta za operacije unije, preseka in komplementa.

Hitro se lahko prepričamo, da je A brezatomska, saj lahko za vsak polzaprt interval najdemo polzaprt interval, ki je strogo vsebovan v prejšnjem, torej ne moremo imeti atomov.

Označimo z B sedaj podalgebro A, ki je sestavljena le iz vseh končnih unij polzaprtih intervalov, ki imajo za oglišča racionalna števila (lahko pa seveda tudi ∞ ali $-\infty$). Ta je števna in brezatomska. V [2] lahko najdemo dokaz izreka, ki trdi, da sta poljubni števni, brezatomski Boolovi algebri z več kot enim elementom izomorfni. Če ta izrek združimo s trditvijo 56, ugotovimo, da je B prosto generirana s števno množico generatorjev. Jih znate poiskati?

LITERATURA

[1] Givant, Steven; Halmos, Paul. *Introduction to Boolean Algebras (Undergraduate Texts in Mathematics)*, Springer 2009.

[2] Sikorski, R. *Boolean Algebras*, Springer-Verlag, N.Y., 1969.