

# PROSTA BOOLOVA ALGEBRA SEMINAR

LUKA PONIKVAR

POVZETEK. Pričetek teorije Boolovih algeber je nepresenetljivo pripisan Georgu Boolu, ki

## 1. BOOLOVE ALGEBRE

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

- |  |   |
|--|---|
| (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) $p \wedge (q \wedge r) = (p \wedge q) \wedge r,$         | $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r),$ |
| (10) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r),$ | $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r).$   |

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

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

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<sup>5</sup>:

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

---

<sup>1</sup>Imenujemo jo “join” oz. “ali”.

<sup>2</sup>Imenujemo jo “meet” oz. “in”.

<sup>3</sup>Imenujemo jo negacija, označujemo pa tudi kot  $'$ .

<sup>4</sup>Negacija ima najvišjo prioriteto, medtem ko ima “in” višjo prioriteto kot “ali”.

<sup>5</sup>Element množice smo označili kar z  $\infty$ .

Taka Boolova algebra ima le dva elementa:

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

Operaciji join in meet 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  $p_0, \dots, p_n$ , 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  $f(p_1, \dots, p_n)$  Boolov polinom v  $n$  spremenljivkah. Takemu polinomu lahko priredimo tri nove polinome:

- (1) **komplement polinoma**  $f(p_1, \dots, p_n)$ :

$$f'(p_1, \dots, p_n),$$

- (2) **dual polinoma**  $f(p_1, \dots, p_n)$ :

$$f'(p'_1, \dots, p'_n),$$

- (3) **kontradual polinoma**  $f(p_1, \dots, p_n)$ :

$$f(p'_1, \dots, p'_n).$$

**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:

$$id : \mathcal{BP} \rightarrow \mathcal{BP}$$

$$id : f(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n).$$

(2) Komplementna funkcija:

$$c : \mathcal{BP} \rightarrow \mathcal{BP}$$

$$c : f(p_1, \dots, p_n) \mapsto f'(p_1, \dots, p_n).$$

(3) Dualna funkcija:

$$d : \mathcal{BP} \rightarrow \mathcal{BP}$$

$$d : f(p_1, \dots, p_n) \mapsto f'(p'_1, \dots, p'_n).$$

(4) Kontradualna funkcija:

$$k : \mathcal{BP} \rightarrow \mathcal{BP}$$

$$k : f(p_1, \dots, p_n) \mapsto f(p'_1, \dots, p'_n).$$

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

*Dokaz.*

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

Druga formula sledi iz dualnosti. □

**Lema 3.2.**  $p \wedge q = p$  natanko tedaj ko  $p \vee q = q$ .

*Dokaz.* Če je  $p \wedge q = p$ , je

$$\begin{aligned}
 p \vee q &= (p \wedge q) \vee q \\
 &\stackrel{(10)}{=} (p \vee q) \wedge (q \vee q) \\
 &\stackrel{(6)}{=} (p \vee q) \wedge q \\
 &\stackrel{3.1}{=} q
 \end{aligned}$$

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

**Definicija 3.3.** Na vsaki Boolovi algebri lahko vpeljemo urejenost kot:

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

**Lema 3.4.** *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  $p = p \wedge q = q \wedge p = q$ . Transitivnost sledi iz (9): če je  $p \leq q$  in  $q \leq r$  je  $p \wedge r = (p \wedge q) \wedge r = p \wedge (q \wedge r) = p \wedge q = p$   $\square$

**Lema 3.5.** (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 3.2. Tretja točka sledi s komplementiranjem.  $\square$

**Definicija 3.6** (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**<sup>6</sup>. Podobno definiramo **infimum** oz. **največjo spodnjo mejo**<sup>7</sup> množice  $E$ .

**Primer 3.7** (Prazna množica). Če je  $E = \emptyset$ , je vsak element na prazno zgornja meja te množice. Tedaj ima  $E$  supremum, in sicer kar element 0 (3.5 točka 2). Podoben razmislek nas privede do zaključka, da je infimum množice  $E$  element 1.

**Primer 3.8** (Enojec). Če je  $E = \{p\}$ , je  $p$  hkrati zgornja in spodnja meja za  $E$ . Sledi da je  $p$  tudi infimum in supremum.

**Lema 3.9.** 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 3.5, 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.  $\square$

**Opomba 3.10** (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).

Primeri 3.7 in 3.8 bi lahko sedaj zapisali kot:

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

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

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

<sup>6</sup>Pišemo tudi natančna zgornja meja.

<sup>7</sup>Pišemo tudi natančna spodnja meja.

## 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:

$$\left(\bigvee_i p_i\right)' = \bigwedge_i p_i' \quad \text{in} \quad \left(\bigwedge_i p_i\right)' = \bigvee_i p_i'.$$

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 3.5, 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.  $\square$

**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

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

*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.  $\square$

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

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

*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

$$q_i \stackrel{(3)}{=} 1 \wedge q_i \stackrel{(4)}{=} (p \vee p') \wedge q_i \stackrel{(10)}{=} (p \wedge q_i) \vee (p' \wedge q_i) \leq r \vee (p' \wedge q_i) \stackrel{3.5}{\leq} r \vee p'.$$

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

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

□

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

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

**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

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

**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. ATOMI

**Definicija 5.1** (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 5.2** (Atom). **Atom** Boolove algebre je neničeln element, ki nima netrivialnih podelementov oz. ko sta njegova edina podelementa natanko 0 in on sam.

**Lema 5.3.** 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. TBD

□

**Lema 5.4.** Če je element  $p$  supremum množice atomov  $E$ , potem je  $E$  množica vseh atomov pod  $p$ .

Dokaz. TBD

□

**Definicija 5.5.** Boolova algebra je atomska, če vsak neničeln element dominira vsaj en atom. Boolova algebra je brezatomska, če nima atomov.

**Lema 5.6.** 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. TBD

□

## 6. PODALGEBRE

**Definicija 6.1.** Boolova podalgebra Boolove algebre  $A$  je neprazna podmnožica  $B$  množice  $A$ , ki je z zožitvijo operacij Boolova algebra.

## 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

## LITERATURA

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

LUKA PONIKVAR, FAKULTETA ZA MATEMATIKO IN FIZIKO, ODDELEK ZA MATEMATIKO, JADRANSKA 21, 1000 LJUBLJANA, SLOVENIJA

*Email address:* `lp29353@student.uni-lj.si`