

POLNI NABORI RESNIČNOSTNIH FUNKCIJ IN POSTOVA MREŽA

LARA VUKŠIĆ

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 06E30

Resničnostne funkcije so preslikave iz množice $\{0, 1\}^n$ v $\{0, 1\}$ za neko naravno število n . Množico vseh resničnostnih funkcij označimo s P_2 . Skupaj s petimi operacijami na resničnostnih funkcijah, ki jih imenujemo operacije Malceva, P_2 tvori strukturo, imenovano funkcijska algebra. Podmnožice P_2 , zaprte za operacije Malceva, so podrazredi. Množica resničnostnih funkcij je poln nabor natanko tedaj, ko ni vsebovana v nobenem izmed petih maksimalnih podrazredov P_2 .

FUNCTIONALLY COMPLETE SETS OF BOOLEAN FUNCTIONS AND POST'S LATTICE

Boolean functions are maps from $\{0, 1\}^n$ to $\{0, 1\}$ for some natural number n . P_2 is the set of all such functions. Together with the five Maltsev operations on Boolean functions, P_2 forms a structure called function algebra. The subsets of P_2 that are closed under Maltsev operations are called the subclasses of P_2 . A set of Boolean functions is functionally complete if and only if it is not contained in any of the five P_2 's maximal subclasses.

Uvod

Vprašanje, s katerimi resničnostnimi funkcijami je mogoče izraziti vse preostale, je precej staro. V prvem zvezku monumentalnega dela *Principia Mathematica* [6], izdanem leta 1910, Bertrand Russell in W. N. Whitehead pokažeta, da za to zadošča že en par resničnostnih funkcij, denimo disjunkcija z negacijo, Sheffer pa je leta 1912 pokazal, da je vse resničnostne funkcije mogoče izraziti z enim samim veznikom, ki je po njem dobil tudi svoje ime. Emil Leon Post je leta 1921 [4] (in podrobneje leta 1941 [5]) odkril, kaj je potreben in zadosten pogoj za to, da lahko z neko množico resničnostnih funkcij izrazimo vse preostale. Taka množica pomeni poln nabor resničnostnih funkcij.

V članku poleg nekaj najpogostejše uporabljanih resničnostnih funkcij predstavimo tudi nekaj operacij na takih funkcijah ter strukturo, ki jo z njihovo pomočjo tvori množica vseh resničnostnih funkcij. Lastnosti te strukture, ki se imenuje funkcijska algebra, nam bodo pomagale pri dokazu Postovega izreka, ki poda karakterizacijo polnih naborov resničnostnih funkcij. Izrek o polnih naborih resničnostnih funkcij, ki ga sicer pogosto srečamo kot

posledico izreka o strukturi Postove mreže, v članku obravnavamo kot samostojen rezultat in zato podamo krajši in enostavnejši dokaz.

Resničnostne funkcije

Pri logiki se operatorje, ki jih predstavimo v članku, namesto kot funkcije obravnava kot izjavne veznike, s pomočjo katerih iz enostavnih izrazov tvorimo kompleksnejše. Ker bo za naš namen lažje uporabiti drugačen pristop, definiramo pojem resničnostne funkcije.

Definicija 1. Naj bo $n \in \mathbb{N}$. *Resničnostna funkcija n spremenljivk* je preslikava iz $\{0, 1\}^n$ v $\{0, 1\}$. Če želimo poudariti, da je funkcija f funkcija n spremenljivk, namesto f pišemo f^n . Množico vseh resničnostnih funkcij n spremenljivk označimo s P_2 , množico vseh resničnostnih funkcij n spremenljivk pa s P_2^n . Če je A podmnožica P_2 , z A^n označimo $A \cap P_2^n$.

Vsako resničnostno funkcijo je mogoče predstaviti s tabelo resničnostnih vrednosti, iz katere lahko za vsako n -terico $\mathbf{x} = (x_1, \dots, x_n) \in \{0, 1\}^n$ razberemo vrednost $f(\mathbf{x})$. Tako so v tabelah 1 in 2 predstavljene nekatere funkcije ene oz. dveh spremenljivk, ki so najpogostejše v uporabi. V prvi tabeli tako definiramo *negacijo*, v drugi pa (po vrsti) *konjunkcijo*, *disjunkcijo*, *implikacijo*, *negacijo implikacije*, *ekvivalenco*, *strogo disjunkcijo* ter *Shefferjev in Łukasiewiczov veznik*.

x	$\neg x$
0	1
1	0

Tabela 1. Negacija.

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$x \not\rightarrow y$	$x \leftrightarrow y$	$x + y$	$x \uparrow y$	$x \downarrow y$
0	0	0	0	1	0	1	0	1	1
0	1	0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	1	1	0
1	1	1	1	1	0	1	0	0	0

Tabela 2. Nekaj resničnostnih funkcij dveh spremenljivk.

Poleg tega za vsako konstanto $a \in \{0, 1\}$ in vsako naravno število n definiramo *konstantno funkcijo* c_a^n in, če velja $1 \leq i \leq n$, tudi e_i^n – *projekcijo* poljubne n -terice $\mathbf{x}$ na njeno i -to komponento e_i^n :

$$c_a^n(x_1, \dots, x_n) = a,$$

$$e_i^n(x_1, \dots, x_n) = x_i.$$

Funkcijska algebra nad P_2

Nekatere resničnostne funkcije lahko izrazimo s pomočjo drugih. Tako velja npr.

$$\begin{aligned}x \rightarrow y &= \neg x \vee y, \\x \not\rightarrow y &= \neg(x \rightarrow y), \\x \uparrow y &= \neg(x \wedge y), \\x \downarrow y &= \neg(x \vee y).\end{aligned}$$

Znani sta tudi De Morganovi formuli, ki opišeta medsebojno odvisnost disjunkcije, konjunkcije in negacije:

$$\begin{aligned}\neg x \wedge \neg y &= \neg(x \vee y), \\ \neg x \vee \neg y &= \neg(x \wedge y).\end{aligned}$$

Poleg tega lahko v vsaki resničnostni funkciji izenačimo spremenljivke, ki v njej nastopajo, ali pa zamenjamo njihov vrstni red. Te postopke lahko opišemo s pomočjo spodnje peterice operacij na resničnostnih funkcijah. Z njimi bo množica P_2 dobila algebraično strukturo.

Definicija 2. *Operacije Malceva* so naslednje operacije, definirane na funkcijah $f \in P_2^n$ in $g \in P_2^m$:

1. $(\zeta f)(x_1, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1)$ za $n \geq 2$, $\zeta f = f$ za $n = 1$,
2. $(\tau f)(x_1, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n)$ za $n \geq 2$, $\tau f = f$ za $n = 1$,
3. $(\triangle f)(x_1, \dots, x_{n-1}) = f(x_1, x_1, x_2, \dots, x_{n-1})$ za $n \geq 2$, $\triangle f = f$ za $n = 1$,
4. $(\nabla f)(x_1, \dots, x_{n+1}) = f(x_2, x_3, \dots, x_{n+1})$ za $n \geq 1$,
5. $(f \star g)(x_1, \dots, x_{m+n-1}) = f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1})$ za $n \geq 1$, $m \geq 1$.

Pokazali bomo, da s komponiranjem operacij Malceva dobimo še veliko drugih operacij na resničnostnih funkcijah. Z njimi lahko med drugim formaliziramo izražanje veznikov s pomočjo drugih, kar nam bo omogočilo, da kasneje definiramo polni nabor.

Trditev 3. *Za vsako permutacijo $\pi \in S_n$ velja, da lahko s komponiranjem operacij ζ in τ dobimo takšno operacijo nad funkcijo $f^n \in P_2$, ki bo permutirala spremenljivke funkcije tako, kot določa π .*

Dokaz. Trditev, ki jo želimo dokazati, je ekvivalentna trditvi, da cikel in transpozicija generirata celotno grupo permutacij S_n oz. da velja $[(12), (12 \dots n)] = S_n$. Ker je vsaka permutacija produkt transpozicij, bo dovolj, če pokažemo, da lahko tako dobimo poljubno transpozicijo. Če najprej za poljuben i od 1 do n vzamemo produkt $(12 \dots n)^{n-i+1}(12)(12 \dots n)^{i-1}$, vidimo, da je enak transpoziciji $(i, i+1)$. Z dobljenimi transpozicijami zaporednih elementov lahko nadalje izrazimo transpozicije oblike $(1i)$ za vsak i v obliki $(12)(23) \dots (i-1, i)(i-2, i-1) \dots (12)$. Ker lahko poljubno transpozicijo (ij) zapišemo kot produkt $(1i)(1j)(1i)$, je trditev dokazana. ■

Operacija Δ izenači prvo in drugo spremenljivko resničnostne funkcije. S pomočjo zgornje trditve pa hitro vidimo, da lahko ta operacija v kompoziciji s prvima dvema izenači poljubno število spremenljivk na poljubnih mestih. Za opis četrte operacije si bomo pomagali s spodnjo definicijo.

Definicija 4. Naj bo $f^n \in P_2$ in $i \in \{1, \dots, n\}$. Če velja

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) = f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$$

za vse vrednosti $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$, pravimo, da je i -ta spremenljivka x_i v f *nebistvena* ali *fiktivna*. Sicer je x_i *bistvena* spremenljivka funkcije f .

Vidimo, da operacija ∇ funkciji f doda nebistveno spremenljivko na prvo mesto. Podobno kot zgoraj se lahko prepričamo, da je s komponiranjem operacije ∇ s permutacijami spremenljivk mogoče dobiti operacijo, ki resničnostni funkciji doda poljubno mnogo nebistvenih spremenljivk na poljubna mesta. Zadnja izmed petih operacij, $\star$, je kompozicija dveh funkcij, ki na mesto prve (ali, če to operacijo zopet komponiramo s permutacijami spremenljivk, katerekoli druge) spremenljivke prve funkcije vstavi drugo funkcijo.

Sedaj ko smo opisali operacije Malceva in videli, da lahko s komponiranjem teh operacij ustvarimo še več drugih operacij na resničnostnih funkcijah, lahko definiramo algebraično strukturo nad P_2 ter nekaj z njo povezanih uporabnih pojmov.

Definicija 5. *Funkcijska algebra nad P_2* je množica P_2 skupaj z operacijami Malceva. Pravimo, da je množica $A \subseteq P_2$ *zaprt*a ali da je *podrazred* P_2 , če za poljubni funkciji $f, g \in A$ velja $\zeta f, \tau f, \Delta f, \nabla f, f \star g \in A$. Podrazred P_2 je *pravi podrazred*, če ni enak P_2 . *Zaprte* neke množice $A \subseteq P_2$ znotraj funkcijske algebre je najmanjši podrazred P_2 , ki vsebuje A . Označimo ga z $[A]$.

Zgleda podrazredov P_2 sta, kot ni težko preveriti, denimo množica vseh projekcij in množica vseh konstantnih funkcij. V razširjeni verziji Postovega

izreka je opisanih vseh števno neskončno mnogo podrazredov P_2 , ki glede na relacijo vsebovanosti tvorijo t. i. Postovo mrežo, nas pa bodo zanimali predvsem podrazredi z neko posebno lastnostjo.

Definicija 6. Neprazen pravi podrazred $F \subsetneq P_2$ je *maksimalen*, če za vsako funkcijo $f \in P_2 \setminus F$ velja $\{f\} \cup F = P_2$.

Maksimalni podrazredi nam bodo v veliko pomoč pri karakterizaciji polnih naborov resničnostnih funkcij.

Polni nabori resničnostnih funkcij

Če problem, ki smo ga definirali v uvodu, prevedemo v jezik funkcijske algebre, nas zanimajo takšne množice resničnostnih funkcij, za katere velja, da je njihovo zaprtje enako P_2 . V tem razdelku poiščemo potreben in zadosten pogoj za to, da ima neka množica takšno lastnost.

Definicija 7. *Poln nabor resničnostnih funkcij* je množica funkcij $A \subseteq P_2$, za katero velja $[A] = P_2$. Če je A poln nabor resničnostnih funkcij, za vsako funkcijo $f \in P_2$ torej obstajajo $k \in \mathbb{N}$ in funkcije $f_1, \dots, f_k \in A$, s katerimi lahko s pomočjo operacij Malceva izrazimo f . Poln nabor je *minimalen*, če nobena njegova prava podmnožica ni poln nabor.

Čeprav bomo polne nabore v celoti karakterizirali šele proti koncu članka, lahko za nekatere množice resničnostnih funkcij že sedaj ugotovimo, da pomenijo poln nabor resničnostnih funkcij.

Naj bo f^n resničnostna funkcija, ki ni konstantno enaka nič, predstavljena z resničnostno tabelo. Vsaki vrstici te tabele, pri kateri je vrednost f enaka ena, priredimo konjunkcijo n izrazov oblike bodisi x_i , če je vrednost i -te spremenljivke v tabeli v tej vrstici enaka 1, bodisi $\neg x_i$ v nasprotnem primeru. Potem je *disjunktivna normalna oblika* funkcije f definirana kot disjunkcija vseh takih izrazov. Če pa je f funkcija, ki ni konstantno enaka 1, ji lahko priredimo *konjunktivno normalno obliko*. Ta je enaka konjunkciji negacij tistih izrazov, ki so enako kot zgoraj prirejeni tistim vrsticam resničnostne tabele, pri katerih f zavzame vrednost 0.

Primer 8. S pomočjo tabele 3 definiramo funkcijo f na treh spremenljivkah.

Disjunktivna normalna oblika funkcije f je $(\neg x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z)$, konjunktivna normalna oblika pa $\neg(\neg x \wedge y \wedge \neg z) \wedge \neg(x \wedge \neg y \wedge \neg z) \wedge \neg(x \wedge y \wedge \neg z) \wedge \neg(x \wedge y \wedge z)$ oziroma $(x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee z) \wedge (\neg x \vee \neg y \vee \neg z)$.

x	y	z	$f(x, y, z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Tabela 3

Očitno je, da obe obliki na vseh n -tericah zavzameta isto vrednost kot f . Torej smo tako pri disjunktivni kot pri konjunktivni normalni obliki funkcije to izrazili zgolj s pomočjo disjunkcije, konjunkcije in negacije. Ker lahko vsaki funkciji priredimo vsaj eno izmed teh dveh oblik, sledi spodnji rezultat.

Trditev 9. $\{\vee, \wedge, \neg\}$ je poln nabor resničnostnih funkcij.

Če za neko množico $M \subseteq P_2$ velja, da lahko s pomočjo njenih elementov izrazimo vse funkcije nekega polnega nabora, potem očitno sledi, da je tudi M poln nabor, saj lahko s pomočjo njenih elementov izrazimo vse resničnostne funkcije. To dejstvo uporabimo v dokazu naslednje posledice.

Posledica 10. Množice $\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\neg, \nrightarrow\}$, $\{\uparrow\}$ in $\{\downarrow\}$ so polni nabori resničnostnih funkcij.

Dokaz. Ker iz De Morganovih formul sledi $x \wedge y = \neg(\neg x \vee \neg y)$ in $x \vee y = \neg(\neg x \wedge \neg y)$, sta prvi dve množici v posledici polna nabora, saj smo pokazali, da je množica $\{\vee, \wedge, \neg\}$ vsebovana tako v $[\{\neg, \vee\}]$ kot tudi v $[\{\neg, \wedge\}]$. Velja tudi $x \vee y = \neg x \rightarrow y = \neg(\neg x \nrightarrow y)$, iz česar sledi, da sta polna nabora tudi množici $\{\neg, \rightarrow\}$ in $\{\neg, \nrightarrow\}$. Njuni zaprtji namreč obe vsebujeta polni nabor $\{\vee, \neg\}$.

Da dokažemo, da sta tudi $\{\uparrow\}$ in $\{\downarrow\}$ polna nabora, se najprej prepričamo, da lahko tako iz Shefferjevega kot tudi iz Łukasiewiczzevega veznika dobimo negacijo: $\neg x = x \uparrow x = x \downarrow x$. Zato iz enakosti $x \wedge y = \neg(x \uparrow y)$ in $x \vee y = \neg(x \downarrow y)$ sledi $\{\neg, \wedge\} \subseteq [\{\uparrow\}]$ in $\{\neg, \vee\} \subseteq [\{\downarrow\}]$, s čimer smo pokazali, da sta tudi zadnji dve množici v posledici polna nabora. ■

Poleg zgornjih dveh oblik si bomo pomagali s še eno normalno obliko, v kateri lahko izrazimo resničnostne funkcije. Spomnimo se, da je ideal I kolobarja K njegov podkolobar, za katerega velja $ak \in I$ in $ka \in I$ za

vse $a \in I$ in $k \in K$. $Z \langle a_1, \dots, a_n \rangle$ označimo najmanjši ideal, ki vsebuje elemente $a_1, \dots, a_n \in K$. Kvocienčni kolobar po idealu K/I pa je množica ekvivalenčnih razredov elementov iz K , za katere velja, da elementa k_1 in k_2 pripadata enakemu ekvivalenčnemu razredu $k_1 + I = k_2 + I$ natanko tedaj, ko je njuna razlika $k_1 - k_2$ vsebovana v I . Tako poistovetimo tiste v K različne elemente, ki pomenijo enak ekvivalenčni razred v K/I .

Izrek 11. *Naj bo $n \in \mathbb{N}$, $f \in P_2^n$ in $J_n = \langle x_1^2 - x_1, x_2^2 - x_2, \dots, x_n^2 - x_n \rangle$ ideal v kolobarju polinomov $K_n = \mathbb{Z}_2[x_1, \dots, x_n]$. Potem obstaja natanko določen polinom $p \in K_n/J_n$, tako da velja:*

$$f(\mathbf{x}) = p(\mathbf{x}) = \sum_{(i_1, \dots, i_n) \in \{0,1\}^n} a_{i_1, \dots, i_n} \cdot x_1^{i_1} \cdot x_2^{i_2} \cdot \dots \cdot x_n^{i_n}$$

za vse $\mathbf{x} \in \{0, 1\}^n$.

Opomba 12. Elementi K_n/J_n za neki $n \in \mathbb{N}$ sicer niso polinomi, temveč ekvivalenčni razredi polinomov iz K_n . Vrednost nekega elementa $p + J_n \in K_n/J_n$ v neki točki $\mathbf{a} \in \{0, 1\}^n$ je kljub temu dobro definirana. Res, razlika dveh polinomov $p, q \in K_n$, ki pripadata istemu ekvivalenčnemu razredu iz K_n/J_n , je namreč vsebovana v $J_n = \langle x_1^2 - x_1, x_2^2 - x_2, \dots, x_n^2 - x_n \rangle$. Ker pa je $0^2 = 0$ in $1^2 = 1$, za vsak polinom $h \in J_n$ in vsako n -terico $\mathbf{a} \in \{0, 1\}^n$ velja $h(\mathbf{a}) = 0$. Iz tega sledi, da imajo vsi elementi nekega ekvivalenčnega razreda $p + J_n$ pri dani n -terici $\mathbf{a}$ enako vrednost. Zato lahko za poljuben element $p + J_n \in K_n/J_n$ definiramo njegovo vrednost pri neki n -terici $\mathbf{a}$ s $q(\mathbf{a})$, kjer je q poljuben predstavnik ekvivalenčnega razreda $p + J_n$. Zavoljo preglednosti zapisa bomo ekvivalenčni razred $p + J_n$ predstavili s polinomom $q \in \mathbb{Z}_2[x_1, \dots, x_n]$, ki je v vsaki od spremenljivk $x_1, \dots, x_n$ stopnje največ 1. Ti polinomi se imenujejo *polinomi Žegalkina* [7].

Dokaz. Izrek dokažemo z indukcijo po n . Če je $n = 1$, f bodisi nima bistvenih spremenljivk oz. je konstantna funkcija, ki jo lahko izrazimo s konstantnim polinomom $p(x) = 0$ oz. $q(x) = 1$ iz K_1/J_1 , bodisi ima f natanko eno bistveno spremenljivko. V tem primeru velja $f(x) = e_1^1(x) = x$ ali $f(x) = \neg x$. Identiteto lahko predstavimo s polinomom $p(x) = x$, negacijo pa s polinomom $q(x) = x + 1$ iz K_1/J_1 . Predpostavimo, da trditev velja za vsako funkcijo manj kot n spremenljivk, in poljubno funkcijo $f \in P_2^n$ zapišimo takole: $f(x_1, \dots, x_n) = (1 - x_n) \cdot f(x_1, \dots, x_{n-1}, 0) + x_n \cdot f(x_1, \dots, x_{n-1}, 1)$. Tako smo funkcijo f izrazili s pomočjo dveh funkcij $n - 1$ spremenljivk, za kateri pa po predpostavki obstajata polinoma iz K_{n-1}/J_{n-1} , s katerima se ujemata pri vseh $(n - 1)$ -tericah $(x_1, \dots, x_{n-1})$. Če v našem zapisu z njima nadomestimo pripadajoči funkciji, dobimo iskani polinom.

Pokazati moramo še, da je ta polinom enolično določen. Ni težko videti, da je preslikava, ki vsaki funkciji $f \in P_2^n$ priredi ustrezeni ekvivalenčni razred iz K_n/J_n , predstavljen s polinomom Žegalkina, injektivna. Res: če dvema funkcijama n spremenljivk pripada enak ekvivalenčni razred in posledično enak polinom Žegalkina, potem sta enaki za vse vrednosti $(x_1, \dots, x_n) \in \{0, 1\}^n$. Zato zadošča pokazati, da sta za vsak $n \in \mathbb{N}$ množici P_2^n in K_n/J_n enako veliki, saj bo iz tega sledilo, da je zgoraj definirana preslikava med njima bijekcija. Vsaka funkcija $f^n \in P_2^n$ je enolično določena z 2^n vrednostmi, ki jih zavzame na vseh n -tericah iz $\{0, 1\}^n$. Ker za vsako teh vrednosti obstajata dve možnosti, 0 ali 1, sledi $|P_2^n| = 2^{2^n}$. Polinom Žegalkina funkcije n spremenljivk pa je po drugi strani enolično določen s koeficienti $a_{i_1, \dots, i_n} \in \{0, 1\}$ za vsak $(i_1, \dots, i_n) \in \{0, 1\}^n$, iz česar sledi $|K_n/J_n| = |P_2^n| = 2^{2^n}$. ■

V tabeli 4 so poleg nekaterih resničnostnih funkcij zapisani pripadajoči polinomi Žegalkina.

Funkcija iz P_2	Polinom Žegalkina
$\neg x$	$x + 1$
$x \vee y$	$x + y + xy$
$x \wedge y$	xy
$x \rightarrow y$	$x + xy + 1$
$x + y$	$x + y$
$x \leftrightarrow y$	$x + y + 1$

Tabela 4. Polinom Žegalkina za nekatere funkcije P_2 .

Pet maksimalnih podrazredov

Sedaj lahko naštejemo nekatere podrazrede P_2 . V naslednjem razdelku se bo izkazalo, da so to edini maksimalni razredi P_2 .

Definicija 13. Pravimo, da resničnostna funkcija f *ohranja vrednost 0*, če velja $f(0, \dots, 0) = 0$. Množico vseh tovrstnih funkcij označimo s T_0 .

Pravimo, da resničnostna funkcija f *ohranja vrednost 1*, če velja $f(1, \dots, 1) = 1$. Množico vseh tovrstnih funkcij označimo s T_1 .

Funkcija f je *monotona*, če iz $\mathbf{x} \leq \mathbf{y}$ sledi $f(\mathbf{x}) \leq f(\mathbf{y})$. Pri tem velja $(x_1, \dots, x_n) \leq (y_1, \dots, y_n)$ natanko tedaj, ko je $x_i \leq y_i$ za vsak $1 \leq i \leq n$, pri čemer je $0 \leq 1$. Množico vseh monotonihih funkcij označimo z M .

Funkcija f je *sebidualna*, če za vsak $\mathbf{x}$ velja: $\neg f(\neg \mathbf{x}) = f(\mathbf{x})$, kjer je $\neg(x_1, \dots, x_n) = (\neg x_1, \dots, \neg x_n)$. Množico vseh sebidualnih funkcij označimo s S .

Afine funkcije so natanko tiste, za katere ima pripadajoči polinom Žegalkina skupno stopnjo ≤ 1 . Množico vseh afinih funkcij označimo z L .

S tabelo 5 naprej pokažemo, da so zgoraj navedene množice paroma neprimerljive glede na relacijo vsebovanosti.

	$\notin T_0$	$\notin T_1$	$\notin M$	$\notin S$	$\notin L$
$\in T_0$		+	+	$\wedge, \vee$	$\wedge, \vee$
$\in T_1$	$\rightarrow$		$\leftrightarrow$	$\wedge, \vee$	$\wedge, \vee$
$\in L$	c_1^1	+	$\neg$	+	
$\in M$	c_1^1	c_0^1		$\wedge, \vee$	$\wedge, \vee$
$\in S$	$\neg$	$\neg$	$\neg$		h

Tabela 5. Funkcije, ki dokazujejo neprimerljivost podrazredov P_2 .

Tu je h funkcija treh spremenljivk, katere polinom Žegalkina je enak $xy + xz + yz$. Pokazati moramo tudi, da so zgornje množice zaprte za operacije Malceva.

Trditev 14 ([3]). *Množice T_0, T_1, M, S in L so podrazredi P_2 .*

Dokaz. Ni težko preveriti, da je vseh pet množic zaprtih glede na prve štiri operacije Malceva. Dokažimo še, da so vse zaprte tudi za kompozicijo. Naj bosta f in g funkciji n oz. m spremenljivk, iz česar sledi, da je $h = f \star g$ funkcija $m + n - 1$ spremenljivk.

Naj velja $f, g \in T_0$. Potem je

$$h(0, \dots, 0) = f(g(0, \dots, 0), 0, \dots, 0) = f(0, 0, \dots, 0) = 0.$$

Torej je T_0 zaprta za kompozicijo. Analogno dokažemo, da to velja tudi za T_1 .

Naj bosta zdaj f in $g \in M$. Če velja $(x_1, \dots, x_{m+n-1}) \leq (y_1, \dots, y_{m+n-1})$, potem je

$$\begin{aligned}
 h(x_1, \dots, x_{m+n-1}) &= f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}) \\
 &\leq f(g(y_1, \dots, y_m), x_{m+1}, \dots, x_{m+n-1}) \\
 &\leq f(g(y_1, \dots, y_m), y_{m+1}, \dots, y_{m+n-1}) \\
 &= h(y_1, \dots, y_{m+n-1}).
 \end{aligned}$$

Iz tega sledi, da je M zaprta za kompozicijo.

Če sta f in $g \in S$, velja:

$$\begin{aligned} h(x_1, \dots, x_{m+n-1}) &= f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}) \\ &= \neg f(\neg g(x_1, \dots, x_m), \neg x_{m+1}, \dots, \neg x_{m+n-1}) \\ &= \neg f(g(\neg x_1, \dots, \neg x_m), \neg x_{m+1}, \dots, \neg x_{m+n-1}) \\ &= \neg h(\neg x_1, \dots, \neg x_{m+n-1}). \end{aligned}$$

Torej je za kompozicijo zaprta tudi S , zaprtost L pa sledi iz tega, da je kompozicija afinih funkcij spet afina. Pokazali smo, da je pet zgoraj opisanih množic zaprtih za operacije Malceva, s čimer smo dokazali trditev. ■

Postov izrek

V spodnjem izreku podamo potreben in zadosten pogoj, ki mu mora neka množica $A \subseteq P_2$ zadoščati, da pomeni poln nabor resničnostnih funkcij. Iz njega bo sledilo, da so T_0, T_1, M, L in S edini maksimalni podrazredi P_2 .

Izrek 15 ([2, izrek 3.2.4.1]). *Množica $A \subseteq P_2$ je poln nabor resničnostnih funkcij natanko tedaj, ko ni vsebovana v nobenem od podrazredov T_0, T_1, M, L in S .*

Dokaz. Če je A vsebovana v nekem podrazredu $B \in \{T_0, T_1, M, L, S\}$, velja $[A] \subseteq B \subsetneq P_2$. Torej A ni poln nabor resničnostnih funkcij.

Predpostavimo sedaj, da A ni vsebovana v nobenem izmed petih podrazredov v izreku. Pokazali bomo, da v tem primeru velja $\{\vee, \wedge, \neg\} \subseteq [A]$, iz česar po lemi 9 sledi $[A] = P_2$. Ker velja $A \not\subseteq B$ za vsako množico $B \in \{T_0, T_1, M, L, S\}$, obstajajo funkcije $f_0, f_1, f_M, f_S, f_L \in A$, ki med seboj niso nujno različne in za katere velja:

$$f_0 \notin T_0, f_1 \notin T_1, f_M \notin M, f_S \notin S, f_L \notin L.$$

Če sedaj izenačimo vse spremenljivke funkcije f_0 , dobimo funkcijo ene spremenljivke $f'_0 \in [A]$, za katero velja $f'_0(0) = 1$. Ločimo dva primera glede na to, ali velja $f'_0(1) = 1$, s čimer dobimo konstantno funkcijo c_1^1 , ali pa velja $f'_0(1) = 0$, kar nam da $f'_0(x) = \neg x$.

Primer 1: Predpostavimo najprej, da velja $f'_0(1) = 1$. Dobljeno konstantno funkcijo c_1^1 vstavimo v f_1 . Ker ta ne ohranja vrednosti 1, velja $f_1(1, \dots, 1) = 0$, s čimer smo dobili tudi drugo konstantno funkcijo c_0^1 .

Ker f_M , funkcija $n \geq 1$ spremenljivk (konstantni funkciji sta monotoni), ne pripada razredu M , obstajata n -terici $\mathbf{a} \leq \mathbf{b}$, za kateri velja $f_M(\mathbf{a}) > f_M(\mathbf{b})$. Naj bo I množica vseh takšnih $1 \leq i \leq n$, za katere velja $a_i = b_i$,

J pa naj bo množica $[n] \setminus I$, kjer z $[n]$ označimo množico $\{1, 2, \dots, n\}$. Če za vsak $i \in I$ na i -to mesto v f_M vstavimo konstantno funkcijo, enako a_i oz. b_i , spremenljivke na mestih $j \in J$ pa med seboj izenačimo, dobimo negacijo. Res, naj brez škode za splošnost velja $J = \{1, 2, \dots, k\}$ in $I = \{k+1, \dots, n\}$ za $1 \leq k \leq n$, saj lahko spremenljivke med seboj poljubno permutiramo. Tedaj je $f'_M(x) = f_M(x, \dots, x, a_{k+1}, \dots, a_n)$ in velja $1 = f'_M(0) = f_M(0, \dots, 0, a_{k+1}, \dots, a_n) > f_M(1, \dots, 1, a_{k+1}, \dots, a_n) = f'_M(1) = 0$. Dokazali smo, da velja $\{c_0^1, c_1^1, \neg\} \subseteq [A]$.

Ker velja $f_L \notin L$, jo lahko brez škode za splošnost zapišemo s polinomom Žegalkina skupne stopnje najmanj 2:

$$f_L(\mathbf{x}) = a_0 + \sum_{i=1}^n a_i \cdot x_i + x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_r} + g(\mathbf{x}),$$

kjer je $r \geq 2$, $1 \leq i_1 \leq i_2 \leq \dots \leq i_r \leq n$ in je g polinom, katerega vsak člen je skupne stopnje r ali več, koeficient pri $x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_r}$ v g pa je enak nič. Naj bo $f'_L(x, y)$ funkcija, ki jo dobimo iz $f_L(\mathbf{x})$, če spremenljivko x_{i_1} nadomestimo z x , spremenljivke $x_{i_2}, x_{i_3}, \dots, x_{i_r}$ z y , vse preostale spremenljivke pa s konstantno funkcijo c_0^1 . Potem lahko funkcijo $f'_L(x, y)$ predstavimo s polinomom Žegalkina oblike $a + bx + cy + xy \in \mathbb{Z}_2[x, y]$. Vseh osem možnosti za funkcijo f'_L prikazuje tabela 6.

a	b	c	$a + bx + cy + xy$	$f'_L(x, y)$
0	0	0	xy	$x \wedge y$
0	0	1	$y + xy$	$y \nrightarrow x$
0	1	0	$x + xy$	$x \nrightarrow y$
0	1	1	$x + y + xy$	$x \vee y$
1	0	0	$1 + xy$	$x \uparrow y$
1	0	1	$1 + y + xy$	$y \rightarrow x$
1	1	0	$1 + x + xy$	$x \rightarrow y$
1	1	1	$1 + x + y + xy$	$x \downarrow y$

Tabela 6. Funkcija f'_L glede na parametre a, b in c .

V vseh primerih je $\{\neg, f'_L\}$ poln nabor resničnostnih funkcij. To sledi iz posledice 10. Ker velja $\{\neg, f'_L\} \subseteq [A]$, sledi, da je tudi A poln nabor.

Primer 2: Predpostavimo sedaj, da velja $f'_0(1) = 0$ in zato $f'_0(x) = \neg x$. Ker velja $f_S \notin S$, obstaja takšna n -terica $(a_1, \dots, a_n)$, da je $f_S(a_1, \dots, a_n) = f_S(\neg a_1, \dots, \neg a_n)$. Naj bo za to n -terico I množica tistih indeksov $1 \leq i \leq n$, za katere je $a_i = 0$, in $J = [n] \setminus I$. Brez škode za splošnost naj velja $I = \{1, \dots, k\}$ ter $J = \{k+1, \dots, n\}$ za $0 \leq k \leq n$. Potem je $f_S(0, \dots, 0, 1, \dots, 1) = f_S(1, \dots, 1, 0, \dots, 0)$. V $f_S(x_1, \dots, x_n)$ prvih k

spremenljivk nadomestimo z $\neg x$, preostale pa z x . Tako dobimo funkcijo $f'_S(x) = f_S(\neg x, \dots, \neg x, x, \dots, x)$. Ker velja $f'_S(1) = f_S(0, \dots, 0, 1, \dots, 1) = f_S(1, \dots, 1, 0, \dots, 0) = f'_S(0)$, je funkcija f'_S konstantna. Dobili smo bodisi c_0^1 bodisi c_1^1 in ker imamo na voljo tudi negacijo, smo primer 2 prevedli na primer 1. ■

Posledica 16. *Maksimalni podrazredi P_2 so natanko T_0, T_1, L, M in S .*

Dokaz. Najprej pokažimo, da so T_0, T_1, L, M, S maksimalni podrazredi P_2 . Pa recimo, da obstaja neki podrazred $B \in \{T_0, T_1, L, M, S\}$, ki ni maksimalen. Potem obstaja taka funkcija $f \in P_2 \setminus B$, da velja $[B \cup \{f\}] \subsetneq P_2$. Po izreku 15 zato velja, da je množica $B \cup \{f\}$ vsebovana v nekem podrazredu $C \in \{T_0, T_1, L, M, S\} \setminus \{B\}$, saj ni poln nabor. To pa je v nasprotju z dejstvom, da so podrazredi T_0, T_1, M, L in S medsebojno različni in paroma neprimerljivi glede na relacijo vsebovanosti.

Pokazati moramo še, da so T_0, T_1, M, L in S edini maksimalni podrazredi P_2 . Naj bo B maksimalen podrazred P_2 , različen od T_0, T_1, L, M in S . Zaradi maksimalnosti sledi, da ni vsebovan v nobenem od njih, zato je po izreku 15 poln nabor in velja: $B = [B] = P_2$. To pa je v nasprotju z definicijo 6, po kateri so maksimalni razredi prave podmnožice P_2 . Torej takega podrazreda ni. ■

Sedaj ko smo spoznali potreben in zadosten pogoj za to, da je neka množica resničnostnih funkcij poln nabor, lahko za poljubno podmnožico P_2 povemo, ali je poln nabor. Določimo vse minimalne polne nabore, ki so vsebovani v P_2^2 in imajo moč kvečjemu dve. Najprej si oglejmo, katerim maksimalnim podrazredom pripadajo funkcije iz P_2^2 . Ker sta projekciji e_0^2 in e_1^2 vsebovani v vseh maksimalnih podrazredih, ne nastopata v nobenem minimalnem polnem naboru. V tabeli 7 prikažemo, katerim maksimalnim podrazredom pripada večina preostalih funkcij iz P_2^2 .

	c_0^2	c_1^2	$\neg x_1$	$\rightarrow$	$\nrightarrow$	$\wedge$	$\vee$	$\leftrightarrow$	$+$	$\uparrow$	$\downarrow$
T_0	$\in$	$\notin$	$\notin$	$\notin$	$\in$	$\in$	$\in$	$\notin$	$\in$	$\notin$	$\notin$
T_1	$\notin$	$\in$	$\notin$	$\in$	$\notin$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$
L	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\in$	$\in$	$\notin$	$\notin$
M	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$
S	$\notin$	$\notin$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$

Tabela 7. Pripadnost nekaterih funkcij iz P_2^2 podrazredom T_0, T_1, L, M, S .

Edine funkcije ene ali dveh spremenljivk, ki jih še nismo navedli, so $\neg x_2$, $\leftarrow$ in $\nleftarrow$. Ker pa lahko te funkcije s pomočjo operacije τ dobimo iz $\neg x_1$, $\rightarrow$ oz. $\nrightarrow$ in obratno, sledi, da so funkcije $\neg x_2$, $\leftarrow$ oz. $\nleftarrow$ vsebovane v natanko istih maksimalnih podrazredih kot $\neg x_1$, $\rightarrow$ oz. $\nrightarrow$.

S pomočjo tabele 7 vidimo, da sta $\uparrow$ in $\downarrow$ edini funkciji iz P_2^2 , ki nista vsebovani v nobenem maksimalnem podrazredu, iz česar sledi, da sta $\{\uparrow\}$ in $\{\downarrow\}$ edina polna nabora, ki vsebujeta natanko en element P_2^2 .

Poiščimo še minimalne polne nabore, ki vsebujejo dve funkciji iz P_2^2 . Jasno je, da nobeden od njih ne vsebuje ne $\uparrow$ ne $\downarrow$.

1. Nabori, ki vsebujejo $\rightarrow$: Dodati moramo funkcijo, ki ni vsebovana v T_1 . Minimalni polni nabori, ki vsebujejo $\rightarrow$, so torej $\{\rightarrow, c_0^2\}$, $\{\rightarrow, \neg\}$, $\{\rightarrow, \nrightarrow\}$ in $\{\rightarrow, +\}$.
2. Nabori, ki vsebujejo $\nrightarrow$, ne pa $\rightarrow$: Dodati moramo funkcijo, ki ni vsebovana v T_0 . Tako dobimo $\{\nrightarrow, c_1^2\}$, $\{\nrightarrow, \neg\}$ in $\{\nrightarrow, \leftrightarrow\}$.
3. Nabori, ki vsebujejo $\neg$, a ne vsebujejo ne $\rightarrow$ ne $\nrightarrow$: Dodati moramo funkcijo, ki ni niti v L niti v S . Tako dobimo $\{\neg, \vee\}$ in $\{\neg, \wedge\}$.

Minimalni polni nabori, ki ne vsebujejo nobene izmed funkcij $\rightarrow$, $\nrightarrow$ in $\neg$, pa vsi vsebujejo vsaj tri elemente. Res: vsebovati morajo funkcijo, ki ni v T_0 , funkcijo, ki ni v T_1 , in funkcijo, ki ni v L . Zato morajo vsebovati vsaj po eno funkcijo iz množic $\{c_1^2, \leftrightarrow\}$, $\{c_0^2, +\}$ in $\{\wedge, \vee\}$. Sledi, da so edini minimalni polni nabori, ki vsebujejo dve funkciji iz P_2^2 , v točkah (1), (2) in (3).

Za konec

V članku smo predstavili maksimalne podrazrede funkcijske algebre P_2 v povezavi s polnimi nabori resničnostnih funkcij. Omenili pa smo tudi, da razširjena verzija Postovega izreka poleg maksimalnih razredov predstavi vse druge podrazrede P_2 ter odnose med njimi glede na vsebovanost. Strukturo funkcijske algebre pa lahko definiramo tudi na množicah funkcij, ki slikajo iz $\{0, 1, \dots, k-1\}^n$ za neki n v $\{0, 1, \dots, k-1\}$, kjer je k poljubno naravno število. Tudi v teh strukturah lahko določimo maksimalne razrede, a je to zaradi tega, ker se njihovo število zelo hitro povečuje, zahtevno.

LITERATURA

- [1] G. P. Gavrilo in A. A. Sapozhenko, *Problems and Exercises in Discrete Mathematics*, Kluwer, Dordrecht, Boston, London, 1996.
- [2] D. Lau, *Function Algebras on Finite Sets*, Springer, Berlin, 2006.
- [3] F. J. Pelletier in N. M. Martin, *Post's functional completeness theorem*, Notre Dame J. Formal Logic **31** (1990) 462–475, dostopno na www.sfu.ca/~jeffpell/papers/PostPellMartin.pdf, ogled 2. 1. 2017.
- [4] E. L. Post, *Introduction to a general theory of elementary propositions*, Amer. J. Math. **43** (1921) 163–185.
- [5] E. L. Post, *The Two-Valued Iterative Systems of Mathematical Logic*, Princeton University Press, Princeton, New Jersey, 1941.
- [6] A. N. Whitehead in B. Russell, *Principia mathematica*, vol. 1, Cambridge University Press, Cambridge, 1910.
- [7] *Zhegalkin polynomial*, v: Wikipedia: The Free Encyclopedia, dostopno na en.wikipedia.org/wiki/Zhegalkin_polynomial, ogled 16. 9. 2016.