UNIVERZITET U NOVOM SADU
PRIRODNO–MATEMATIČKI FAKULTET
INSTITUT ZA MATEMATIKU

IGOR DOLINKA

O identitetima algebri regularnih jezika

– DOKTORSKA DISERTACIJA –

Novi Sad, 2000.

U početku bješe riječ...

Jovan I, 1

I like words *much better than numbers;*
and I always did.

P. R. Halmos

Poznajem, poznajem lukavstvo tvoje;
Nikada ne kažeš reč *koju bi trebalo.*

R. Tagore: Gradinar, 35

"Kada se bliži kraj", zapisao je Kartafil,
"iz sećanja nestaju slike; ostaju samo reči."

J. L. Borges: Besmrtnik

Ako jezike *čovečije i anđelske govorim,*
a ljubavi nemam,
onda sam kao zvono koje zvoni,
ili praporac koji zveči.

Kor. XIII, 1

Predgovor

Predmet istraživanja u ovoj disertaciji jesu univerzalno-algebarska pitanja vezana za neke osnovne pojmove iz teorijskog računarstva, naročito iz teorije formalnih jezika i logike računarskih programa. Takva pitanja motivisana su potrebom, koju nameće ubrzani razvitak računarske tehnologije, da se nađu odgovarajući teorijski, matematički okviri unutar kojih bi se na apstraktnom nivou modelirao računarski softver – programi i proces njihovog izvršenja na računaru. Formalizacijom osnovnih gradivnih elemenata programskih jezika i struktura podataka, došlo se do *reči* i njihovih kolekcija, *jezika*, kao matematičkih objekata. Jasno, sam karakter ovih objekata izbacuje u prvi plan interakciju algebre i diskretne matematike kao glavni izvor matematičkih oruđa za rad sa *formalnim jezicima*.

Prirodno, ako je data familija jezika nad nekom azbukom (kao skupom osnovnih, nedeljivih simbola), na njoj se mogu uočiti razne operacije sa jezicima kao načini da se iz datih jezika konstruišu novi. Takvo razmatranje je svakako isuviše grubo za ispitivanje strukture govornih jezika, ali je sasvim zadovoljavajuće ako želimo da opišemo programske jezike. Polazeći od činjenice da se svaki struktuirani programski jezik, u osnovi, gradi uz pomoć tri konstrukcije: selekcije, sekvence i iteracije, nije teško videti da je od naročitog značaja da posmatramo upravo operacije unije, konkatenacije i iteracije jezika nad datom azbukom. Na taj način, dolazimo do *algebri jezika*.

Ali, pri tome se odmah postavlja praktičan, i, sa stanovišta primenjene matematike i računarstva, ključan problem: kako zadati jezik nekim *konačnim* zapisom koji ga u potpunosti određuje. Naravno, na taj način je moguće tretirati samo prebrojivo mnogo jezika (naspram neprebrojivo mnogo, koliko ih ima već nad konačim azbukama). Međutim, takav pristup omogućava ispitivanje najinteresantnijih klasa jezika. Ukoliko za opisani konačan zapis koristimo formalan izraz kojeg formiramo od slova azbuke i simbola koji označavaju operacije sa jezicima (tj. term u signaturi algebri jezika), dolazimo do regu-

larnih izraza, koji predstavljaju *regularne jezike*, tj. jezike konačnih automata. Ali, takva reprezentacija regularnog jezika uopšte ne mora biti jedinstvena: on može biti predstavljen sa više različitih regularnih izraza. Tako, pitanje kada dva regularna izraza određuju isti jezik vodi pojmu regularnog identiteta, odnosno *identiteta u algebri regularnih jezika.*

Drugo značajno oruđe u algebarskoj teoriji računskih mašina jesu algebre binarnih relacija. Jedinstvo sintakse i semantike u logici računarskih programa realizuje se upravo kroz pojam binarne relacije. Razlog za to je što se, apstraktno gledano, programi mogu posmatrati kao binarne relacije na skupu svih mogućih stanja računara, pri čemu svaka elementarna naredba omogućava mašini prelazak iz jednog stanja u drugo. Najzad, to je upravo način na koji rade Tjuringove mašine, koje intuitivno možemo smatrati za računare bez stvarnih fizičkih ograničenja u smislu hardvera.

Ključna veza između jezika i binarnih relacija je sada sledeća: svaka algebra jezika izomorfna je algebri binarnih relacija, tako da se i sami jezici i operacije među njima mogu "kodirati" binarnim relacijama. Štaviše, algebre jezika i njima odgovarajuće algebre binarnih relacija zadovoljavaju potpuno iste identitete, što znači da generišu jedan isti varijetet – varijetet *Kleenejevih algebri.* Ispostavlja se da su algebre regularnih jezika upravo slobodne Kleenejeve algebre. Sve ove veze omogućavaju da se problematika regularnih identiteta osvetli iz više uglova i obezbeđuju bogatu metodologiju u radu sa Kleenejevim algebrama.

Međutim, lako se uočava da Kleenejeve algebre predstavljaju tek prvu stepenicu koja aproksimira problem algebarskog tretmana procesa izvršenja računarskog programa. Naime, glavni nedostatak je u neodređenosti: operacije unije, odnosno refleksivno-tranzitivnog zatvorenja relacija na apstraktnom nivou odgovaraju tek *nedeterminističkoj* (tj. slučajnoj) selekciji, odnosno iteraciji. S druge strane, očekujemo da naše programske aplikacije rade deterministički, tj. tačno onako kako mi želimo, a ne po principu probabiliteta (iako su, sasvim izvesno, mnogi korisnici računara i odgovarajućih progamskih paketa ne jednom iskusili suprotan slučaj!). Nedostajući element je, u stvari, ispitivanje tačnosti iskaza tokom izvršenja programa (a što se svodi na poređenje sadržaja dva registra procesora), što onda određuje njegov dalji tok. Prema tome, kako bi se ukinula neodređenost, neophodno je, osim Kleenejevih algebri programa u razmatranje uvesti i Booleove algebre, čija je uloga da čuvaju informaciju o stanjima mašine na kojoj se program izvršava i, povremeno, omoguće testiranje tih stanja. Na taj način, prirodno se nameće pojam *dinamičke algebre.* Razna pitanja koja se tiču verifikacije, korektnosti, ekvivalentnosti programa i optimizacije programskog koda se mogu formulisati kao pitanja u vezi sa identitetima dinamičkih algebri. Fiksiranjem Kleene-

jeve algebre (što intuitivno odgovara fiksiranju programskog paketa) dolazi se do Jónssonovih dinamičkih algebri. Ovde je stavljen naročit akcenat na uspostavljanje veze između njih i "klasičnih" dinamičkih algebri, kada su u pitanju osobine odgovarajućih jednakosnih teorija.

Materijal koji je izložen u ovoj disertaciji pretpostavlja izvestan fond pojmova i tvrđenja, koji leže u osnovama raznih algebarskih disciplina. Spisak referentne literature sadrži stoga i stavke udžbeničkog i monografskog karaktera. U najkraćem, one su obuhvaćene sledećom listom:

- univerzalna algebra: [36], [68], [108],
- polugrupe i grupe: [29], [38], [45], [76], [98],
- formalni jezici: [54], [63], [74], [75], [98], [99], [104], [141], [142], [152],
- teorija binarnih relacija: [78], [103], [144],
- logika: [16], [20], [35], [70], [71], [91].

Na kraju, želim da pomenem nekolicinu dragih ljudi kojima dugujem veliku zahvalnost na njihovoj ulozi u realizaciji ove doktorske disertacije. Na prvom mestu, reč je o mojim roditeljima, *Jeleni* i *Vojinu*, koji su uspeli da obezbede tako neophodanu ljubav, porodični sklad i mir, atmosferu u kojoj sam preko dve i po decenije, iz dana u dan, dobijao maksimum uslova za kvalitetan rad, neumornu pomoć i nezamenljivu podršku u svakom pogledu, bilo da je u pitanju profesionalno napredovanje, bilo da su u pitanju problemi sa kojima se svi svakodnevno sudaramo.

Kada je u pitanju struka, tu je moj mentor, *dr Siniša Crvenković*, redovni profesor PMF-a u Novom Sadu, koji je bio uz mene od mojih prvih koraka u matematičkoj nauci i sa istrajnošću i strpljenjem me uvodio u istraživački rad. Kada ova disertacija bude branjena, verovatno će se napuniti čitavih jedanaest godina našeg poznanstva: sada mogu reći da one nisu bile ispunjene pukom saradnjom u naučnom radu – bile su, pre svega, ispunjene prijateljstvom. To prijateljstvo je predstavljalo, a i danas predstavlja, veliku inspiraciju za mene.

Osim toga, moram pomenuti *dr Ésik Zoltána*, profesora Informatičkog Instituta "Kálmár László" Univerziteta u Segedinu. Saradnja sa jednim od vodećih stručnjaka u oblasti algebarskih osnova teorijskog računarstva predstavljala je za mene pravo zadovoljstvo. Rezultati te saradnje čine jedan deo originalnih doprinosa izloženih u ovoj disertaciji. Najzad, zahvaljujem se *dr Rozáliji Sz. Madarász* i *dr Đuri Pauniću*, redovnim profesorima PMF-a u Novom Sadu, na pruženoj podršci.

Novi Sad, 27. januar 2000.

1.1. Reči i jezici. Algebre jezika

Neka je Σ proizvoljan neprazan skup. *Reč* nad Σ je bilo koji konačan niz elemenata iz Σ. Naravno, pri tome uzimamo u obzir i prazan niz, kojeg zovemo *prazna reč* i označavamo sa λ. Skup Σ od čijih elemenata gradimo reči zovemo *azbukom*, a njegove elemente *slovima*.

Primera radi, ako je $\Sigma = \{a, b\}$, tada je jedna reč nad ovom azbukom $\langle a, b, b, a, a, a, b, a, a\rangle$. Međutim, uobičajeno je da se (kadgod je to moguće) za zapisivanje reči koristi jednostavnija notacija u kojoj izostavljamo zagrade i zareze, pa će u tom slučaju predthodna reč naprosto glasiti *abbaaabaa*, što mnogo više odgovara našem intuitivnom pojmu reči.

Ako je w neka reč nad azbukom Σ, tada sa $|w|$ označavamo dužinu reči w. Za $a \in \Sigma$, sa $|w|_a$ označavamo broj pojavljivanja slova a u w. Na primer, $|abbaaabaa| = 9$ i $|abbaaabaa|_a = 6$.

Skup svih reči nad azbukom Σ označavamo sa Σ^*. Ako na Σ^* uočimo operaciju *konkatenacije* (dopisivanja) reči, preciznije, operaciju definisanu za $u = a_1 \dots a_n$ i $v = b_1 \dots b_m$ sa

$$uv = a_1 \dots a_n b_1 \dots b_m,$$

tada nije teško videti da se na taj način dobija slobodni monoid nad Σ. Slično, ako sa Σ^+ označimo skup svih *nepraznih* reči nad Σ, $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$, tada dolazimo do slobodne polugrupe nad Σ.

Reč v je *podreč* reči w ako postoje reči u, z tako da je $w = uvz$. Ukoliko je pri tome $u = \lambda$, za v kažemo i da je *prefiks* reči w, dok u slučaju $z = \lambda$ govorimo o *sufiksu* reči w.

Jezik je proizvoljan skup reči, tj. za datu azbuku Σ, proizvoljan podskup slobodnog monoida Σ^*. Na taj način, skup svih jezika nad azbukom Σ jeste partitivni skup $\mathcal{P}(\Sigma^*)$.

Razmotrimo, kao ilustraciju prethodno uvedenih pojmova, sledeći jednostavan program (recimo, u PASCAL-u):

```
program zbir;
const
     Faktor=3;
var
     x,y,z:Integer;
begin
     ReadLn(x);
     ReadLn(y);
     z:=Faktor*(x+y);
     WriteLn(z)
end.
```

Kao i u slučaju prirodnih jezika, i programske jezike i u njima realizovane programe možemo tretirati dvojako (pri čemu uloga rečenice u govornom jeziku odgovara konkretnom programu). Možemo poći od alfabeta nekog jezika (odnosno, simbola koji se nalaze na tastaturi) i od njih formirati reči. Neke od tih reči su smislene u određenom jeziku, a neke ne, i na taj način se, recimo, srpski jezik sastoji od više stotina hiljada reči sastavljenih iz trideset slova. Takođe, PASCAL se onda sastoji od ključnih reči (npr. `program`, `const`, `var`, `Integer`, `begin`, `ReadLn`, itd.), reči koje označavaju imena promenljivih (`zbir`, `Faktor`, `x`,...), operatora (`:=`,`=`, `+`, `*`), specijalnih razdvajajućih simbola (`;`, `.`), itd. Drugi pristup je da zapravo same reči govornog jezika (odnosno, ključne reči i ostale gradivne elemente programskog jezika) smatramo osnovnim, nedeljivim simbolima – znači, elementima alfabeta – dok su rečenice (programi) reči, a jezik skup svih gramatički korektnih rečenica, tj. sintaktički korektnih programa.

Sa jezicima možemo izvoditi različite operacije. Pre svega, tu su osnovne skupovno-teoretske operacije (unija, presek, komplement), od kojih unija ima najveći značaj. Iz tradicionalnih razloga, unija jezika se zapisuje u aditivnoj notaciji, dakle ($L_1, L_2 \subseteq \Sigma^*$):

$$L_1 + L_2 = \{w : \ w \in L_1 \ \vee \ w \in L_2\}.$$

Naravno, operacija konkatenacije se iz Σ^* prenosi na jezike kao proizvod kompleksa:

$$L_1 L_2 = \{w_1 w_2 : \ w_1 \in L_1 \ \wedge \ w_2 \in L_2\}.$$

Najzad, definišemo i jednu unarnu operaciju koju zovemo *Kleenejeva zvezda* (ili *Kleenejeva iteracija*):

$$L^* = \{w : \ (\exists n \in \omega)(\exists w_1, \ldots, w_n \in L) \ w = w_1 \ldots w_n\}.$$

Ako po dogovoru uvedemo da je $L^0 = \{\lambda\}$, tada je zapravo

$$L^* = \bigcup_{n \geq 0} L^n.$$

Na ovaj način (ukoliko još uzmemo u razmatranje dva istaknuta jezika $\emptyset$ i $\{\lambda\}$), mi smo definisali jednu algebru sa nosačem $\mathcal{P}(\Sigma^*)$:

$$\mathbf{Lang}(\Sigma) = \langle \mathcal{P}(\Sigma^*), +, \cdot, ^*, \emptyset, \{\lambda\} \rangle,$$

koju zovemo *algebra jezika nad* Σ. Varijetet generisan svim algebrama jezika (nad svim azbukama) označavamo sa $\mathcal{L}$.

Sada ćemo razmotriti neke osnovne osobine algebri jezika, odnosno identitete koji važe na $\mathcal{L}$. Sledeće tvrđenje se sasvim jednostavno dokazuje.

PROPOZICIJA 1.1.1. *Za proizvoljnu azbuku* Σ, *algebra* $\langle \mathcal{P}(\Sigma^*), +, \cdot, \emptyset, \{\lambda\} \rangle$ *je poluprsten sa jedinicom. Drugim rečima,* $\mathbf{Lang}(\Sigma)$ *zadovoljava identitete (konstantni simboli* $0, 1$ *se interpretiraju redom kao* $\emptyset, \{\lambda\}$*):*

(1) $(x + y) + z = x + (y + z)$,

(2) $x + y = y + x$,

(3) $x + 0 = 0 + x = x$,

(4) $(xy)z = x(yz)$,

(5) $x \cdot 0 = 0 \cdot x = 0$,

(6) $x \cdot 1 = 1 \cdot x = x$,

(7) $x(y + z) = xy + xz$,

(8) $(x + y)z = xz + yz$.

Interesantno je da osim distributivnih zakona *(7)* i *(8)* iz prethodne propozicije, na algebrama jezika važi i osobina koju, grubo govoreći, možemo nazvati "beskonačna distributivnost". Nju ćemo kasnije koristiti u više navrata.

LEMA 1.1.2. *Neka su* A *i* B_i, $i \in I$, *jezici nad azbukom* Σ. *Tada je*

(1) $A \bigcup_{i \in I} B_i = \bigcup_{i \in I} AB_i$,

(2) $\left(\bigcup_{i\in I} B_i\right) A = \bigcup_{i\in I} B_i A.$

Kada uzmemo u obzir operaciju *, imamo, između ostalog, identitete opisane narednom lemom.

LEMA 1.1.3. *Na svakoj algebri jezika važe identiteti:*

(1) $x^*x^* = x^*$,

(2) $xx^* = x^*x$,

(3) $(x^*)^* = x^*$.

Dokaz. Neka je L proizvoljan jezik nad nekom azbukom Σ. Tada je

$$L^*L^* = \left(\bigcup_{n\geq 0} L^n\right)\left(\bigcup_{m\geq 0} L^m\right) = \bigcup_{m,n\geq 0} L^{m+n} = \bigcup_{i\geq 0} L^i = L^*,$$

čime je dokazano *(1)*. Dalje, imamo:

$$LL^* = L\left(\bigcup_{n\geq 0} L^n\right) = \bigcup_{n\geq 1} L^n = \left(\bigcup_{n\geq 0} L^n\right) L = L^*L.$$

Najzad, iz *(1)* imamo da je $(L^*)^2 = L^*$, odakle se induktivnim putem lako dobija $(L^*)^n = L^*$ za sve $n \geq 0$. Zbog toga je

$$(L^*)^* = \bigcup_{n\geq 0} (L^*)^n = \{\lambda\} + L^* = L^*,$$

što se i tražilo. ∎

Takođe, lako se pokazuje da su sve opisane operacije sa jezicima monotone u odnosu na skupovnu inkluziju.

LEMA 1.1.4. *Za proizvoljne jezike* $A, B, C, D \subseteq \Sigma^*$ *takve da je* $A \subseteq B$ *i* $C \subseteq D$ *važi:*

(1) $A + C \subseteq B + D$,

(2) $AC \subseteq BD$,

(3) $A^* \subseteq B^*$.

U daljem radu će nam biti potrebna i naredna tri identiteta.

LEMA 1.1.5. *Na svakoj algebri jezika važe sledeći identiteti:*

(1) $x^* = 1 + xx^* = 1 + x^*x$,

(2) $(xy)^*x = x(yx)^*$.

Dokaz. Identiteti *(1)* slede iz same definicije Kleenejeve zvezde, identiteta *(2)* iz Leme 1.1.3 i činjenice da je za sve jezike L,

$$LL^* = \bigcup_{n \geq 1} L^n.$$

Zato, posmatrajmo prozivoljne jezike $A, B \subseteq \Sigma^*$, gde je Σ neka azbuka, i pretpostavimo da $w \in (AB)^*A$. Tada postoje reči $u_1, \ldots, u_n, u_{n+1} \in A$ i $v_1, \ldots, v_n \in B$ tako da je

$$w = u_1 v_1 \ldots u_n v_n u_{n+1}.$$

Međutim, tada je $v_1 u_2 \ldots v_n u_{n+1} \in (BA)^*$, pa je $w \in A(BA)^*$, tj. $(AB)^*A \subseteq A(BA)^*$. Potpuno analogno se dokazuje i obratna inkluzija, pa dobijamo da važi *(2)*. ∎

Sledeća dva identiteta algebri jezika imaju naročit značaj. Njih zovemo još i *Conwayevi identiteti* (prvi i drugi). Osim toga, identitet *(3)* iz Leme 1.1.3 se ponekad zove i treći Conwayev identitet.

PROPOZICIJA 1.1.6. *Svaka algebra jezika zadovoljava identitete:*

(1) $(x + y)^* = (x^*y)^*x^*$,

(2) $(xy)^* = 1 + x(yx)^*y$.

Dokaz. Na osnovu *(1)* i *(2)* iz prethodne leme odmah imamo

$$(xy)^* = 1 + (xy)^*xy = 1 + x(yx)^*y.$$

Stoga prelazimo na dokaz identiteta *(1)*. Jasno je da je $(A^*B)^*A^* \subseteq (A + B)^*$ (ovo sledi iz činjenice da je $A, B \subseteq (A + B)^*$, Lema 1.1.3 i 1.1.4). Zato, pretpostavimo da je $w \in (A + B)^*$, $w \neq \lambda$. Tada se reč w može predstaviti kao $w = u_1 \ldots u_n$, pri čemu je za sve $1 \leq i \leq n$, $u_i \in A$ ili $u_i \in B$. Odaberimo

sve indekse $i_1 < \ldots < i_k$ za koje je $u_{i_j} \in B$, $1 \leq j \leq k$ (dakle, uočili smo sve one reči iz niza $u_1, \ldots, u_n$ koje pripadaju jeziku B). Tada imamo:

$$\begin{aligned} u_1 \ldots u_{i_1-1} u_{i_1} &\in A^{i_1-1}B \subseteq A^*B, \\ &\vdots \\ u_{i_{k-1}+1} \ldots u_{i_k-1} u_{i_k} &\in A^{i_k-i_{k-1}-1}B \subseteq A^*B, \\ u_{i_k+1} \ldots u_n &\in A^{n-i_k} \subseteq A^*. \end{aligned}$$

Množeći gornje relacije, zaključujemo da važi $w \in (A^*B)^k A^* \subseteq (A^*B)^* A^*$, što je i trebalo dokazati. ∎

Poluprstene sa jedinicom i dodatnom unarnom operacijom * u kojima važe gornja dva identiteta zovemo *Conwayevi *-poluprsteni.*

Primetimo da Conwayevi identiteti, slobodno govoreći, opisuju "dejstvo" zvezde redom na zbir, konkatenaciju i samu zvezdu. Što se tiče dejstva zvezde na konstante, u algebrama jezika očito imamo:

$$0^* = 1, \tag{1}$$

$$1^* = 1. \tag{2}$$

Drugi od gornja dva identiteta zovemo *ω-idempotentni zakon.* Prema tome, svaka algebra jezika je ω-idempotentni Conwayev *-poluprsten.

Do sada smo razmatrali (formalne) jezike nad datom azbukom naprosto kao podskupove slobodnog monoida Σ^*. Međutim, nameće se pitanje kako predstaviti jezike nekom *konačnom* šemom, tj. konačnim zapisom. Naravno, to pitanje je potpuno neinteresantno za konačne jezike; međutim, kada se radi o beskonačnim jezicima, opisani problem ima ključni značaj u slučaju da želimo da zadamo neki jezik tako da ta reprezentacija bude "upotrebljiva" sa stanovišta računarskih nauka. Od te reprezentacije, dakle, očekujemo sledeće:

(1) da je sama reprezentacija konačan niz simbola, znači, reč (nad nekom azbukom),

(2) da različiti jezici imaju različite reprezentacije.

Odmah se može uočiti da gornja dva zahteva u startu ograničavaju mogućnosti teorije formalnih jezika. Naime, svaki slobodni monoid Σ^* jeste (prebrojivo) beskonačan, što povlači da nad Σ imamo $|\mathcal{P}(\Sigma^*)| = 2^{\aleph_0}$ (neprebrojivo mnogo) jezika. To znači da je svaki pokušaj da svakom jeziku dodelimo neku konačnu reprezentaciju *a priori* nemoguć, budući da konačnih zapisa možemo imati najviše prebrojivo mnogo. Prema tome, najveći deo jezika nad datom

azbukom (pa čak i jednoelementnom!) izmiče takvom tretmanu. U tom smislu, najviše što teorija formalnih jezika može postići jeste da izdvoji neke prebrojive klase jezika, koje su zbog svoje strukture naročito interesantne za izučavanje. Takvi su, na primer, regularni jezici: jezici koje dobijamo od konačnih jezika primenjujući (konačno mnogo puta) operacije algebre jezika.

Naravno, u okviru teorije formalnih jezika su razvijeni i "alati" kojima se (napuštajući zahtev za konačnom reprezentacijom) mogu ispitivati mnogo šire klase jezika. Takva je teorija formalnih redova nad poluprstenima [66, 96, 143]. Na taj način, svaki jezik se može posmatrati kao formalni red nad dvoelementnim Booleovim poluprstenom $\mathbf{B}_2$. Ovakav pristup vodi raznim interesantnim generalizacijama, od kojih je u ovom trenutku najaktuelnija teorija formalnih redova nad *tropskim poluprstenima* [124, 151] (za neke rezultate u vezi ove problematike, vidi [30, 95]), tako da je teorija formalnih redova nad poluprstenima prerasla u samostalnu oblast teorijskog računarstva i algebre.

Vraćajući se problemu konačne reprezentacije jezika, možemo uočiti dva osnovna pristupa u rešavanju tog problema:

(1) konačan niz simbola opisuje *mašinu* koja *prepoznaje* reči (koje dobija kao ulazne podatke) u odnosu na to da li pripadaju datom jeziku ili ne,

(2) konačan niz simbola *generiše*, ili opisuje mašinu koja generiše (na osnovu nekog programa) reči traženog jezika.

Kada je u pitanju prvi pristup (za regularne jezike), o njemu će detaljnije biti reči u Poglavlju 1.4. Ovde ćemo se skoncentrisati na *regularne izraze*, konačne sintaktičke objekte koji u sebi čuvaju informaciju o celom regularnom jeziku, i na taj način predstavljaju reprezentaciju tipa (2).

Regularan izraz nad Σ je, u univerzalno-algebarskoj terminologiji [36], term tipa algebri jezika, dakle, tipa $\langle 2,2,1,0,0\rangle$, i to nad Σ kao skupom promenljivih. Detaljnije, imamo sledeću induktivnu definiciju:

- 0,1 i slova $a \in \Sigma$ su regularni izrazi,
- ako su r, s regularni izrazi, onda su to i $(r + s)$, (rs) i (r^*),
- regularni izrazi su samo oni nizovi simbola koji se mogu dobiti konačnom primenom gornja dva pravila.

Osim toga, primenjuju se uobičajene konvencije o izostavljanju spoljašnjih zagrada.

Naravno, sada moramo opisati semantičku interpretaciju regularnih izraza, tj. specifikovati način na koji oni predstavljaju jezike. Stoga uvodimo preslikavanje $\llcorner : Reg_\Sigma \to \mathcal{P}(\Sigma^*)$ (gde smo sa Reg_Σ označili skup svih regularnih izraza nad Σ) koje zovemo *vrednost regularnog izraza* i definišemo ga sa:

- $\mathsf{L}(0) = \emptyset$,
- $\mathsf{L}(1) = \{\lambda\}$,
- $\mathsf{L}(a) = \{a\}$, za sve $a \in \Sigma$,
- $\mathsf{L}(r + s) = \mathsf{L}(r) + \mathsf{L}(s)$,
- $\mathsf{L}(rs) = \mathsf{L}(r)\mathsf{L}(s)$,
- $\mathsf{L}(r^*) = (\mathsf{L}(r))^*$.

Izuzetno je važno primetiti da se sa obe strane gornjih definicionih jednakosti pojavljuju simboli $+, \cdot, ^*$, ali da oni imaju različito značenje: dok su oni sa leve strane formalni, sintaktički simboli koji služe za izgradnju regularnih izraza, dotle je sa desne strane reč o ranije definisanim operacijama sa jezicima.

Nije teško videti da se vrednost regularnog izraza r nad Σ u stvari poklapa sa vrednošću terma r u algebri jezika $\mathbf{Lang}(\Sigma)$ u odnosu na interpretaciju promnljivih $a \mapsto \{a\}$, $a \in \Sigma$, dakle, sa

$$r^{\mathbf{Lang}(\Sigma)}[\{a\}]_{a\in\Sigma}.$$

Opisanu interpretaciju promenljivih u regularnom izrazu zovemo *standardnom interpretacijom.*

Jezik $L \subseteq \Sigma^*$ je *regularan* ako postoji regularan izraz r tako da je $\mathsf{L}(r) = L$. U tom slučaju kažemo da r *predstavlja* jezik L.

Pri tome, reprezentacija regularnog jezika uopšte ne mora biti jedinstvena: više regularnih izraza može predstavljati isti jezik; drugim rečima, za dva regularna izraza r, s se može desiti da je $\mathsf{L}(r) = \mathsf{L}(s)$. U tom slučaju ćemo pisati

$$r = s.$$

Formalnu jednakost gornjeg tipa (razlikujmo je od fizičke jednakosti regularnih izraza, koju ćemo zapisivati kao $r \equiv s$) zvaćemo *regularni identitet.* U Poglavlju 1.3 ćemo videti da se skup svih regularnih identiteta poklapa sa skupom identiteta algebri jezika, tj. sa jednakosnom teorijom varijeteta $\mathcal{L}$.

Sada se lako uočava da se do skupa regularnih jezika nad nekom azbukom može doći i na način opisan u narednoj lemi.

LEMA 1.1.7. *Neka je Σ azbuka. Skup regularnih jezika je najmanja familija jezika nad Σ koja sadrži $\emptyset$, $\{\lambda\}$, jednoelementne jezike oblika $\{a\}$ za $a \in \Sigma$ (ili, sve konačne jezike), i zatvorena je na operacije $+, \cdot, ^*$. Drugim rečima, regularni jezici nad Σ su tačno elementi podalgebre od $\mathbf{Lang}(\Sigma)$ generisane jezicima $\{a\}$, $a \in \Sigma$ (konačnim jezicima).*

Dokaz. Regularni izrazi formiraju apsolutno slobodnu term-algebru tipa $\langle 2,2,1,0,0\rangle$. Po definiciji, regularni jezici su njihove slike u odgovarajućoj algebri jezika u odnosu na preslikavanje L, za koje je iz definicije očito da je reč o homomorfizmu uočene term-algebre u algebru $\mathbf{Lang}(\Sigma)$. Znači, regularni jezici su tačno slike regularnih izraza u odnosu na homomorfizam L, pa oni obrazuju podalgebru od $\mathbf{Lang}(\Sigma)$ i ona je generisana slikama promenljivih – generatora term-algebre regularnih izraza – tj. sa $\{a\}$, gde je $a \in \Sigma$. ∎

Prema tome, regularni jezici obrazuju algebru u odnosu na osnovne operacije sa jezicima,

$$\mathbf{Reg}(\Sigma) = \langle Reg(\Sigma), +, \cdot, ^*, \emptyset, \{\lambda\}\rangle,$$

algebru regularnih jezika nad Σ. Identiteti ovih algebri predstavljaće naš glavni predmet izučavanja.

Primetimo da se pojam *regularnog podskupa* (u literaturi se može naći i termin *racionalan podskup*) može odgovarajućom modifikacijom gornjih definicija uvesti u proizvoljnom monoidu, ne samo u slobodnom monoidu Σ^*. Pretpostavimo da je monoid M generisan skupom $X \subseteq M$. Formirajmo sledeću algebru kompleksa monoida M:

$$\langle \mathcal{P}(M), \cup, \cdot, ^*, \emptyset, \{1\}\rangle,$$

gde je $\cdot$ operacija množenja kompleksa, * je operacija generisanja podmonoida, a 1 je jedinica u M. Sada je regularni podskup od M bilo koji skup oblika $\varphi(L)$, gde je $L \subseteq X^*$ regularan jezik nad X, a $\varphi : X^* \to M$ homomorfizam koji proširuje identičko preslikavanje na X. Drugim rečima, regularni podskupovi nekog monoida su članovi najmanje familije njegovih podskupova zatvorene na uniju, množenje kompleksa i generisanje podmonoida, koja sadrži $\emptyset, \{1\}$ i jednoelementne podskupove $\{x\}$ za $x \in X$.

Ako izbacimo konstantu 1 iz razmatranja, na sličan način možemo definisati pojam regularnog podskupa bilo koje polugrupe.

U radu [55] Eilenberg i Schützenberger ispituju neke osobine regularnih podskupova komutativnih monoida. Između ostalog, oni dokazuju i sledeće tvrđenje.

TEOREMA 1.1.8. (Eilenberg, Schützenberger, [55]) *Ako su* X, Y *regularni podskupovi komutativnog monoida* M*, onda su to i* $X \cap Y$ *i* $X \setminus Y$.

Na osnovu dobro poznate veze konačnih automata i regularnih jezika (koja će biti razmotrena u Poglavlju 1.4), gornja teorema važi i kada se umesto komutativnog monoida M posmatra slobodni monoid Σ^*.

Na kraju, pomenimo da se, kao uopštenje pojmova uvedenih u ovom poglavlju, u novije vreme intenzivno razvija teorija jezika koji se sastoje od *beskonačnih* reči. Osnove ove teorije dao je Büchi [34] još početkom 60-tih godina, ali je njen značaj uočen tek u novije vreme. U okviru ove discipline se sintetišu metode kombinatorike na rečima i matematičke logike. Wilke je u [156] konstruisao algebarsku teoriju beskonačnih reči kao generalizaciju klasične algebarske teorije formalnih jezika (koja počiva na vezi jezika sa automatima i polugrupama).

U prethodnom, uveli smo osnovne pojmove u vezi sa jezicima: to su pojmovi reči, azbuke, jezika i algebre jezika. Sada je trenutak da otkrijemo drugu "glavnu ulogu" u ovoj disertaciji. Ona pripada – binarnim relacijama.

1.2. Relacione algebre

Otkud binarne relacije u teorijskom računarstvu? Odgovor je veoma jednostavan: binarne relacije predstavljaju glavni algebarski aparat kojim se modeliraju procesi automatskog izračunavanja, tj. rad računara. Naime, apstraktno gledajući, računarske programe možemo posmatrati kao relacije na skupu stanja računara, pri čemu svaka elementarna "komanda" omogućava računaru da pređe iz jednog stanja u drugo (što se u konkretnom slučaju odražava na promenu sadržaja memorije, procesorskih registara, aktiviranja ulazno-izlaznih kanala, itd.). Zapravo, ono što smo opisali je upravo način na koji rade Tjuringove mašine, koje možemo zamisliti kao računare bez ikakvih stvarnih ograničenja u odnosu na hardverske mogućnosti. Programirati Tjuringovu mašinu ne znači ništa drugo nego zadati njenu relaciju prelaza.

Početke računa binarnih relacija nalazimo još u prošlom veku, i to najpre kod De Morgana [52] u čuvenom radu *On the syllogism: IV; and on the logic of relations* iz 1860. godine. Polazeći od kritike klasične Aristotelove logike, De Morgan sasvim izvesno prvi zasniva teoriju relacija na egzaktnim, matematičkim osnovama, uvodeći (rudimentarno) osnovne operacije sa relacijama. De Morgan je već tada nazreo da je reč o fundamentalnoj problematici, na kojoj, u stvari, počiva veliki deo matematike.

Međutim, ovo je ostao jedini De Morganov rad iz teorije binarnih relacija.

Oko 1870, ovom tematikom je počeo da se bave C. S. Peirce [119], i izučavao ju je u narednih dvadesetak godina. Peirce je ispitivao *identitete* koji važe za binarne relacije, tako da veliki broj danas poznatih identiteta relacionih algebri potiče od njega. Takođe, od izuzetnog značaja je činjenica što je Peirce prvi uočio strogu razliku između dve vrste operacija sa relacijama: *logičkih* (ili *statičkih*) operacija, koje su zapravno skupovno teoretske operacije (unija $\cup$, presek $\cap$, komplement $^-$, itd.), i čije dejstvo ne zavisi od "unutrašnje" strukture

binarnih relacija kao skupova *uređenih parova*; i *relativnih* (ili *dinamičkih*) operacija, čija definicija suštinski zavisi od te strukture (kao npr. kompozicija relacija $\circ$ ili inverz relacija $^\vee$). Na sličan način se mogu podeliti i konstante relacionih algebri.

Krajem XIX veka, binarnim relacijama i njihovim zakonima se bavio i Schröder [146], koji je uveo operacije tranzitivnog i refleksivno-tranzitivnog zatvorenja (o njemu će biti reči i u narednom poglavlju). Najzad, značaj binarnih relacija u matematici su podvukli Russel [137] i Russel i Whitehead [138]. U [137], Russel kaže:

> "...Peanova logka se teško može smatrati kompletnom bez izričitog uvođenja pojma relacije...definicija *funkcije* je, strogo gledajući, nemoguća bez poznavanja nove, primitivnije ideje, ideje *relacije*." [*Prev. aut.*]

Nakon toga, početkom XX veka, problematika binarnih relacija doslovno pada u zaborav. Razlog za to je što je ova tema bila daleko ispred svog vremena, kako u pogledu zasnivanja matematičkih teorija na onaj način kako ih danas poznajemo (imajući u vidu raspoloživa matematička oruđa i tehnike), tako i pogledu primene i (danas sasvim jasne) veze sa računarskim naukama [144]. Istraživanja u teoriji binarnih relacija će oživeti tek početkom 40-tih godina, pre svega sa antologijskim radom A. Tarskog [153]. Kasnije, najviše zaslugom Tarskog i njegovih učenika, teorija binarnih relacija i relacionih algebri izrasla je u nezavisnu matematičku disciplinu u okvirima *algebarske logike* [16]. Međutim, binarne relacije se sada tretiraju u sasvim novom svetlu, u svetlu moderne matematike: Tarski je opremljen metodologijom savremene, aksiomatske logike, i pre svega, razvijenom *teorijom modela*. Sve ovo bilo je nedostupno matematičarima XIX veka.

Ako je A proizvoljan skup, tada algebru

$$\mathbf{R}(A) = \langle \mathcal{P}(A \times A), \cup, \cap, ^-, \emptyset, \nabla_A, \circ, \Delta_A, ^\vee \rangle$$

zovemo *puna relaciona algebra*. Svaka podalgebra pune relacione algebre je *prava relaciona algebra*.

Gornja konstrukcija se može i uopštiti ako umesto Dekartovog kvadrata $A \times A$ posmatramo proizvoljnu relaciju ekvivalencije ρ na skupu A i sve njene podskupove. Tako, ako $\bar{\sigma}$ označava relativni komplement $\rho \setminus \sigma$, imamo sledeću algebru binarnih relacija:

$$\mathbf{E}(\rho) = \langle \mathcal{P}(\rho), \cup, \cap, ^-, \emptyset, \rho, \circ, \Delta_A, ^\vee \rangle.$$

Sve podalgebre algebri gornjeg oblika zovemo *konkretne relacione algebre*.

U potrazi za apstraktnim, aksiomatskim zasnivanjem teorije relacionih algebri, Chin i Tarski [37] 1951. definišu *relacione algebre* kao klasu svih algebri $\mathbf{A} = \langle A, +, \cdot, {}^{-}, 0, 1, \circ, 1', {}^{\vee} \rangle$ tipa $\langle 2, 2, 1, 0, 0, 2, 0, 1 \rangle$ koje zadovoljavaju sledeće aksiome:

(R1) $\langle A, +, \cdot, {}^{-}, 0, 1 \rangle$ je Booleova algebra,

(R2) $\langle A, \circ, 1' \rangle$ je monoid,

(R3) $(x + y)^{\vee} = x^{\vee} + y^{\vee}$,

(R4) $(x \circ y)^{\vee} = y^{\vee} \circ x^{\vee}$,

(R5) $(x^{\vee})^{\vee} = x$,

(R6) $x \circ (y + z) = (x \circ y) + (x \circ z)$,

(R7) $(x^{\vee} \circ \overline{x \circ y})y = 0$.

Očito, svi gonji uslovi su identiteti, pa je ovim definisan *varijetet relacionih algebri* $\mathcal{RA}$.

Nije teško videti da se svaka Booleova algebra može dodefinisati do relacione algebre. Takođe, postoji način da se od proizvoljne polugrupe konstruiše relaciona algebra koja je (strukturno gledajući) u tesnoj vezi sa tom polugrupom. Na taj način se dobijaju tzv. *polugrupne relacione algebre* [47]. Međutim, klasa polugrupnih relacionih algebri nije elementarna, tj. nije aksiomatizabilna formulama prvog reda, vidi [49].

Relacione algebre koje su izomorfne nekoj konkretnoj relacionoj algebri zovemo *reprezentabilne relacione algebre* (naime, svaka algebra binarnih relacija koja zadovoljava gornje aksiome jeste podalgebra algebre oblika $\mathbf{E}(\rho)$, vidi Teoremu 2.11 u [103]). Klasu reprezentabilnih relacionih algebri označavamo sa $\mathcal{RRA}$. U Teoremi 3.7 u [103] je dokazano sledeće tvrđenje koje pokazuje da sve reprezentabilne relacione algebre na izvesan način "nastaju" od punih relacionih algebri.

PROPOZICIJA 1.2.1. *Neka je $\mathcal{K}$ klasa svih punih relacionih algebri. Tada je $\mathcal{RRA} = \mathsf{ISP}(\mathcal{K})$.*

Svoju aksiomatsku teoriju relacionih algebri Chin i Tarski su (verovatno) uveli sa nadom da bi se na taj način mogla okarakterisati klasa konkretnih algebri relacija, odnosno da važi "kompletnost" ove teorije u smislu da je svaka algebra koja zadovoljava uslove (R1)–(R7) u stvari neka reprezentabilna relaciona algebra (tj. da je $\mathcal{RA} = \mathcal{RRA}$). Da to nije tako, pokazao je Lyndon

[100], još dok je rad [37] China i Tarskog bio u štampi (ironija je u tome da se Lyndonov rad pojavio pre [37]). Naime, koristeći projektivne ravni i neke tehnike iz projektivne geometrije, Lyndon je konstruisao nereprezentabilnu relacionu algebru, dakle, algebru koja zadovoljava sve uslove (R1)–(R7), ali nije izomorfna nijednoj konkretnoj relacionoj algebri. Kasnije, McKenzie je u svojoj doktorskoj disertaciji [107] našao primer nereprezentabilne relacione algebre sa samo 16 elemenata i pokazao da je to baš najmanja nereprezentablina relaciona algebra.

Naravno, to još ne znači da aksiomama relacionih algebri nije opisana jednakosna teorija konkretnih relacionih algebri tj. da nije $Eq(\mathcal{RA}) = Eq(\mathcal{RRA})$. Međutim, Tarski je 1953. dokazao da važi

PROPOZICIJA 1.2.2. (Tarski, [154]) *$\mathcal{RRA}$ je varietet.*

Pošto je $\mathcal{RRA} \neq \mathcal{RA}$, sledi da postoji identitet koji važi na svim reprezentabilnim relacionim algebrama, a da on nije posledica aksioma (R1)–(R7). Teorema 4.33 iz [103] daje primer jednog takvog identiteta. No, postavlja se pitanje da li se sistem aksioma China i Tarskog može "popraviti", tj. dopuniti sa još nekoliko aksioma, pa da se dobije kompletna aksiomatizacija konkretnih algebri relacija (drugim rečima, da je problem samo u tome što su Chin i Tarski "zaboravili" nekoliko identiteta)? Ne! Naime važi

TEOREMA 1.2.3. (J. D. Monk, 1964) *Klasa $\mathcal{RRA}$ nije konačno aksiomatizabilna. Drugim rečima, varijetet $\mathcal{RRA}$ nema konačnu bazu identiteta.*

Na taj način, identiteti konkretnih algebri relacija su neuhvatiljivi bilo kakvom konačnom šemom zakona. Rezultati ovakvog tipa, problemi (bes)konačne aksiomatizacije klasa algebri povezanih sa pojmovima u teorijskom računarstvu i specijalno, u algebarskoj teoriji formalnih jezika, biće prisutni u najvećem delu ove disertacije. Intuitivno, to znači da je problematika formalnih jezika (i sa njima, binarnih relacija) u odnosu na njihove zakone mnogo složenija (i sa računarskog stanovišta "loša") nego što se to čini na prvi pogled. Zato ćemo se (ali ne samo iz tog razloga) na kraju okrenuti dinamičkim algebrama, koje u mnogome rešavaju ove nedostatke [131].

Od rezultata opisanog tipa pomenućemo sledeće tvrđenje za $\{\cup, \circ\}$-redukte konkretnih relacionih algebri. Neka u narednoj propoziciji $\mathcal{K}$ označava klasu svih algebri izomorfnih algebrama binarnih relacija sa operacijama unije i kompozicije relacija.

PROPOZICIJA 1.2.4. (Andréka, [9, 10]) *Klasa $\mathcal{K}$ je kvazivarijetet, ali nije varijetet. Pri tome, $\mathcal{K}$ nije konačno aksiomatizabilna klasa.*

S druge strane, varijetet generisan kvazivarijetetom $\mathcal{K}$ se poklapa sa varijetetom aditivno polumrežnih poluprstena, pa je očito konačno baziran. Za detaljan pregled problematike reprezentacije (redukata) relacionih algebri, upućujemo na rad Scheina [145]. Takođe, izuzetno lep prikaz istorijata teorije binarnih relacija dat je u članku [133]. Uopšte, kada je u pitanju teorija relacionih algebri, bez sumnje centralna literatura (na našem jeziku) jeste monografija Madarász, Crvenković: *Relacione algebre* [103].

Međutim, relacione algebre Tarskog neće biti predmet našeg izučavanja. Naime, kada dođemo do intuitivne interpretacije operacija sa binarnim relacijama u odnosu na osnovne programske konstrukcije (vidi početak narednog poglavlja), vidimo da operacije ovih relacionih algebri omogućavaju isključivo rad sa linearnim programima. Naravno, ono što zaista daje moć struktuiranom programiranju jeste *iteracija*. Za početak, razmatraćemo nedeterminističku iteraciju (kako bismo uveli kontrolu, tj. determinizam kroz ispitivanje Booleovskih uslova u petljama, moramo ponovo pribeći dinamičkim algebrama). Na taj način (grubo govoreći), dolazimo do *regularnog programiranja*. Kako bismo našli relacioni "komplement" takvih programskih struktura, neophodna nam je nova operacija - *(refleksivno-)tranzitivno zatvorenje*. Tako dolazimo do Kleenejevih relacionih algebri.

1.3. Kleenejeve relacione algebre i regularni jezici

Operaciju *refleksivno-tranzitivnog zatvorenja relacija* razmatrao je Schröder [146] još 1895. godine. Motivacija je poticala iz formalne aritmetike (koju je zasnovao Peano 1889.), budući da je relacija poretka na prirodnim brojevima bila definisana kao tranzitivno zatvorenje interpretacije predikata "biti sledbenik". Naime, ako je ρ relacija na skupu A i ako za $n \geq 1$ označimo

$$\rho^n = \underbrace{\rho \circ \ldots \circ \rho}_{n},$$

kao i $\rho^0 = \Delta_A$, tada definišemo

$$\rho^{\mathrm{rtc}} = \bigcup_{n \geq 0} \rho^n.$$

Ako iz gornje unije izostavimo dijagonalu (tj. ρ^0), dobijamo *tranzitivno zatvorenje* ρ^{tc} relacije ρ.

Kao što je već rečeno, (nedeterminističke) računarske programe možemo interpretirati kao neku binarnu relaciju na skupu stanja računara. Tako, ako su A i B dva takva stanja, činjenica da je $A\rho B$ znači da primenom programa

ρ, računar može da pređe iz stanja A u stanje B. Po Wirth-ovoj šemi dobro struktuiranog programa, on se sastoji od elementarnih komandi koje su povezane jednom od sledeće tri konstrukcije:

- *selekcija* (izbor u odnosu na to koji će se od dva ili više potprograma izvršiti),
- *sekvenca* (nadovezivanje potprograma),
- *iteracija* (uzastopno ponavljanje jednog potprograma).

Očito, ovim konstrukcijama odgovaraju redom operacije unije, kompozicije i refleksivno-tranzitivnog zatvorenja.

Značaj ovih operacija (a naročito refleksivno-tranzitivnog zatvorenja) uočio je S. C. Kleene 1956. godine [82]. On je uveo regularne izraze i regularne jezike kako bi modelirao rad neuronskih mreža, dok je konačne automate razmatrao kao prvu aproksimaciju stvarnih računarskih sistema. U istom radu, Kleene je dokazao da su regularni jezici tačno jezici konačnih automata, tvrđenje danas poznato kao *Kleenejeva teorema.* O njoj će više biti reči u narednom poglavlju.

Ako je A proizvoljan skup, tada algebru

$$\mathbf{Rel}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle$$

zovemo *puna Kleenejeva relaciona algebra.* Svaka algebra izomorfna nekoj podalgebri pune Kleenejeve relacione algebre je *standardna* (ili *reprezentabilna*) *Kleenejeva algebra.* Varijetet generisan svim algebrama oblika $\mathbf{Rel}(A)$ označavamo sa $\mathcal{KA}$. Algebre iz tog varijeteta su *Kleenejeve algebre.* Ako algebri $\mathbf{Rel}(A)$ dodamo operaciju $^\vee$ *inverza relacija*, dobijamo algebru $\mathbf{Rel}^\vee(A)$. Sve ovakve algebre generišu varijetet $\mathcal{KA}^\vee$ *Kleenejevih algebri sa inverzijom.*

Veoma je interesantno primetiti da se od svake polugrupe na veoma jednostavan način može napraviti standardna Kleenejeva algebra. U osnovi ove konstrukcije je zapravo algebra kompleksa monoida S^1.

LEMA 1.3.1. *Neka je S proizvoljna polugrupa. Tada algebra*

$$\mathbf{M}(S) = \langle \mathcal{P}(S^1), \cup, \cdot, ^*, \emptyset, \{1\} \rangle,$$

pri čemu je $\cdot$ množenje kompleksa, a * operacija generisanja podmonoida, jeste standardna Kleenejeva algebra.

Dokaz. Posmatrajmo preslikavanje $\xi : \mathcal{P}(S^1) \mapsto \mathcal{P}(S^1 \times S^1)$ definisano za sve $A \subseteq S^1$ sa

$$\xi(A) = \{\langle s, sa \rangle : \ s \in S^1, a \in A\} = \bigcup_{a \in A} \rho_a,$$

gde ρ_a označava desnu translaciju monoida S^1 u odnosu na $a \in S^1$. Sada se direktno pokazuje da je ξ u stvari potapanje algebre $\mathbf{M}(S)$ u $\mathbf{Rel}(S^1)$. ∎

Gornje tvrđenje ima jednu izuzetno značajnu posledicu. Naime, primetimo da ako uzmemo $S = \Sigma^*$, tada je $\mathbf{M}(\Sigma^*) = \mathbf{Lang}(\Sigma)$, algebra jezika nad azbukom Σ. Tako, gornje tvrđenje znači da se *svaki jezik može posmatrati kao binarna relacija*, tačnije kao unija desnih translacija na slobodnom monoidu koje odgovaraju rečima tog jezika. Time je odmah dokazana

PROPOZICIJA 1.3.2. *Svaka algebra jezika jeste standardna Kleenejeva algebra.*

POSLEDICA 1.3.3. $\mathcal{L} \leq \mathcal{KA}$.

Međutim, veza algebri jezika i Kleenejevih algebri ovim nije iscrpljena. Naprotiv, varijetet generisan algebrama jezika, razmatran u prvom poglavlju, poklapa se sa varijetetom Kleenejevih algebri. Ovaj zaključak sledi iz narednog fundamentalnog tvrđenja, poznatog kao *Kozen-Németijeva teorema*. Naime, ovu teoremu je prvi dokazao Kozen 1979. godine u [83], u kontekstu dinamičkih algebri. Međutim, ovaj rad je bio u formi IBM-ovog tehničkog izveštaja i nikad nije bio objavljen. Dokaz je prvi publikovao Németi tri godine kasnije u radu [114].

TEOREMA 1.3.4. (Kozen, [83], Németi, [114]) *Algebra regularnih jezika* $\mathbf{Reg}(\Sigma)$ *je slobodna Kleenejeva algebra nad* Σ, *slobodno generisana preslikavanjem* $a \mapsto \{a\}$, $a \in \Sigma$.

Dokaz. Kako bismo pojednostavili dokaz, koristimo činjenicu da ako je neka algebra slobodna nad nekim skupom za klasu algebri $\mathcal{K}$, tada je ona slobodna nad istim tim skupom za varijetet generisan klasom $\mathcal{K}$. Naravno, ulogu klase $\mathcal{K}$ ovde igra klasa punih Kleenejevih relacionih algebri.

Ako sa ι označimo preslikavanje koje svakom slovu $a \in \Sigma$ dodeljuje jezik $\{a\}$, ono što treba dokazati jeste da za svako preslikavanje $\varphi : \Sigma \to \mathcal{P}(A \times A)$ (gde je A neki skup) postoji homomorfizam $\psi : \mathbf{Reg}(\Sigma) \to \mathbf{Rel}(A)$ takav da je $\iota \circ \psi = \varphi$. Najpre, primetimo da se slobodni monoid Σ^* potapa u monoidni redukt algebre $\mathbf{Reg}(\Sigma)$ (naime, potapanje je $\xi : w \mapsto \{w\}$ za $w \in \Sigma^*$). S druge strane, postoji homomorfizam monoida $\psi_0 : \Sigma^* \to \langle \mathcal{P}(A \times A), \circ, \Delta_A \rangle$ takav da je $\iota \circ \psi_0 = \varphi$. Definišimo sada preslikavanje $\psi : Reg(\Sigma) \to \mathcal{P}(A \times A)$ sa

$$\psi(L) = \bigcup_{w \in L} \psi_0(w).$$

Lako se proverava da je ψ homomorfizam Kleenejevih algebri, kao i da je $\iota \circ \psi = \xi \circ \psi_0$. Ali, takođe je očito da je $\iota \circ \xi = \iota$, pa sledi

$$\iota \circ \psi = \iota \circ \iota \circ \psi = \iota \circ \xi \circ \psi_0 = \iota \circ \psi_0 = \varphi,$$

što se i tražilo. ∎

Gornja teorema ima nekoliko neposrednih, ali veoma značajnih posledica.

POSLEDICA 1.3.5. $\mathcal{L} = \mathcal{KA}$.

Dokaz. Iz Posledice 1.3.3 već imamo da je $\mathcal{L} \leq \mathcal{KA}$. S druge strane, algebre regularnih jezika su podalgebre algebri jezika, pa je varijetet generisan njima sadržan u $\mathcal{L}$. Međutim, algebre regularnih jezika su slobodne Kleenejeve algebre, pa one generišu $\mathcal{KA}$. Zato je $\mathcal{KA} \leq \mathcal{L}$. ∎

POSLEDICA 1.3.6. *Identitet $p = q$ važi za sve jezike ako i samo ako važi za sve regularne jezike.*

Dokaz. Implikacija ($\Rightarrow$) je trivijalna. S druge strane, ako identitet $p = q$ važi za sve regularne jezike, onda on važi na svim algebrama regularnih jezika, i tako, u svim Kleenejevim algebrama, pa specijalno i u algebrama jezika. ∎

Ipak, najvažnija posledica Kozen-Németijeve teoreme je sledeća (podsetimo, regularni izrazi su upravo termi tipa Kleenejevih algebri).

POSLEDICA 1.3.7. *Kleenejeve algebre zadovoljavaju identitet $p = q$ ako i samo ako regularni izrazi p, q predstavljaju iste regularne jezike, tj.* $\mathsf{L}(p) = \mathsf{L}(q)$.

Dokaz. Implikacija ($\Rightarrow$) je trivijalna. Obratno, pretpostavimo da regularni izrazi $p = p(x_1, \ldots, x_n)$ i $q = q(x_1, \ldots, x_n)$ predstavljaju iste regularne jezike (nad fiksiranim skupom promenljivih X) i neka je $\mathbf{K}$ proizvoljna Kleenejeva algebra. Na proizvoljan način odaberimo $k_1, \ldots, k_n \in K$ i definišimo preslikavanje $\varphi : X \to K$ sa $\varphi(x_i) = k_i$ za sve $1 \leq i \leq n$. Postoji homomorfizam $\psi : \mathbf{Reg}(X) \to \mathbf{K}$ za koji važi $\iota \circ \psi = \varphi$, gde je $\iota(x_i) = \{x_i\}$ za sve $1 \leq i \leq n$. Sada je

$$\begin{aligned}
p^{\mathbf{K}}(k_1, \ldots, k_n) &= p^{\mathbf{K}}(\varphi(x_1), \ldots, \varphi(x_n)) = \\
&= p^{\mathbf{K}}(\psi(\{x_1\}), \ldots, \psi(\{x_n\})) = \\
&= \psi(\mathsf{L}(p)) = \psi(\mathsf{L}(q)) = \\
&= q^{\mathbf{K}}(\psi(\{x_1\}), \ldots, \psi(\{x_n\})) = \\
&= q^{\mathbf{K}}(\varphi(x_1), \ldots, \varphi(x_n)) = \\
&= q^{\mathbf{K}}(k_1, \ldots, k_n).
\end{aligned}$$

Sledi da $\mathbf{K}$ zadovoljava identitet $p = q$. ∎

Dakle, identitet Kleenejevih algebri je dovoljno proveriti u Kleenejevoj algebri regularnih jezika u odnosu na standardnu interpretaciju.

1.4. Automati, regularni jezici i polugrupe

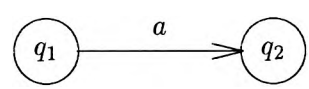
Kao što smo još ranije napomenuli, alternativni način da se (neki) jezici kodiraju konačnim objektima jeste konstrukcija apstraktne matematičke mašine koja *prepoznaje* taj jezik (tj. njegove reči). Takvi objekti su, u izvesnom smislu, "pasivni": potreban im je ulazni signal (reč u nekoj ulaznoj azbuci) kako bi dali odgovor (DA ili NE) da li uneta reč pripada uočenom jeziku ili ne. Doslovno, ovde je reč o programiranim računarima. Krajnji dometi takvog pristupa jesu Tjuringove mašine, kojima odgovaraju rekurzivno nabrojivi jezici (u hijerarhiji Čomskog, jezici tipa 0). Kada su u pitanju regularni jezici, odgovarajuće mašine jesu *konačni automati*. Preko njih, uspostavlja se veza jezika i *konačnih (uređenih) polugrupa*, koje u sebi nose potpunu informaciju o strukturi tog jezika. Štaviše, videćemo da su konačne polugrupe u stvari ti konačni objekti koji prepoznaju regularne jezike, dok je koncept automata samo pomoćno tehničko sredstvo, koje je pogodno kako zbog mogućnosti njihove vizuelizacije (putem grafa automata), tako i zbog činjenice da su oni intuitvno bliže jezicima, pa je rad s njima mnogo lakši.

Osim toga, veza jezika i polugrupa se nastavlja kada počnemo da formiramo klase jezika. Čuvena *Eilenbergova teorema o varijetetima* kaže kako izvesnim "dobrim" klasama formalnih jezika (tzv. *varijetetima jezika*) tačno odgovaraju (kroz vezu koja se ostvaruje preko automata) pseudovarijeteti konačnih polugrupa.

Poluautomat je uređena trojka

$$\mathbf{A} = \langle S, \Sigma, \delta \rangle,$$

gde je S neprazan *skup stanja*, Σ *azbuka*, a $\delta : S \times \Sigma \to S$ *funkcija prelaza*. Grafički, poluautomat predstavljamo usmerenim grafom čiji su čvorovi stanja iz S, dok su lukovi označeni slovima azbuke, $a \in \Sigma$, na taj način što se činjenica da je $\delta(q_1, a) = q_2$ predstavlja strelicom koja vodi iz q_1 u q_2, pri čemu je ona označena slovom a:



Primetimo da smo poluautomat ekvivalentno mogli da definišemo i kao unarnu algebru $\langle S, M_a \rangle_{a \in \Sigma}$ (što se u literaturi često i sreće), gde je

$$M_a(x) = \delta(x, a)$$

prelaz pridružen slovu a. Jasno, funkcija prelaza poluatomata može da se proširi na proizvoljne reči nad Σ, tako da je $\delta(q, \lambda) = q$ i

$$\delta(q, a_1 \ldots, a_n) = \delta(\ldots(\delta(q, a_1), \ldots), a_n) = (M_{a_1} \circ \ldots \circ M_{a_n})(q).$$

Rabin-Scottov konačan automat je uređena petorka

$$\mathbf{A} = \langle S, \Sigma, \delta, q_0, F \rangle,$$

pri čemu je $\langle S, \Sigma, \delta \rangle$ poluautomat, $q_0 \in S$ je *početno stanje*, dok je $F \subseteq S$ skup *završnih stanja.* Kažemo da automat $\mathbf{A}$ *prihvata* reč $w \in \Sigma^*$ ukoliko je $\delta(q_0, w) \in F$, dakle, ukoliko reč w prevodi početno stanje automata u neko od završnih stanja. *Jezik automata* $\mathbf{A}$ (u oznaci $L(\mathbf{A})$) je skup svih reči prihvaćenih od strane $\mathbf{A}$.

Naravno, u duhu prethodnih napomena kako svaki program (što je u ovom slučaju prelaz pridružen nekom slovu) može da se posmatra kao binarna relacija na skupu stanja, koncept automata možemo uopštiti na sledeći način. Naime, gornja definicija automata je "deterministička", pošto za svako slovo $a \in \Sigma$ iz svakog stanja izlazi tačno jedna strelica označena sa a. Na taj način, stanje automata i učitano slovo jednoznačno određuju naredno stanje. *Nedeterministički konačan automat* je uređena petorka

$$\mathbf{A} = \langle S, \Sigma, \{\tau_a\}_{a \in \Sigma}, I, F \rangle,$$

gde je $\tau_a \subseteq S \times S$ za sve $a \in \Sigma$ *relacija prelaza* koja odgovara slovu a, a $I \subseteq S$ *skup početnih stanja* (dok su ostale komponente iste kao i u determinističkoj varijanti). Automat $\mathbf{A}$ *prihvata* reč $w = a_1 \ldots a_n$ ukoliko postoji niz $q_0, q_1 \ldots, q_n \in S$ tako da je $q_0 \in I$, $q_n \in F$ i za sve $1 \leq i \leq n$ važi

$$\langle q_{i-1}, q_i \rangle \in \tau_{a_i}.$$

Pri tome je jezik automata ponovo skup svih prihvaćenih reči. Na ovaj način, do izražaja dolazi relaciona priroda programa: možemo reći da je automat $\mathbf{A}$ opremljen familijom relacija prelaza (elementarnih programa) τ_a. Program je tada sintaktički ispravan niz elementarnih programa, što znači da njegova primena vodi do uspešnog izvršenja (završnog stanja) na automatu.

Može se na prvi pogled učiniti da su nedeterministički automati opštiji i sa stanovišta jezika koje prihvataju. Međutim, to nije slučaj. Naime, važi sledeće tvrđenje.

TEOREMA 1.4.1. *Za svaki nedeterministički automat* $\mathbf{A}$ *postoji deterministički automat* $\mathbf{A}'$ *takav da je* $L(\mathbf{A}) = L(\mathbf{A}')$.

Za dva automata kažemo da su *ekvivalentni* ako prihvataju isti jezik. Tako, svaki nedeterministički automat ima deterministički ekvivalent. Međutim, kako izgledaju jezici automata? Odgovor na to pitanje daje čuvena *Kleenejeva teorema*, dokazana 1956. godine. Slobodno možemo reći da sa njom počinje savremena algebarska teorija automata i formalnih jezika.

TEOREMA 1.4.2. (Kleene, [82]) *Jezik* $L \subseteq \Sigma^*$ *je jezik nekog konačnog automata ako i samo ako je regularan.*

Ako je $\mathbf{A} = \langle S, \Sigma, \delta, q_0, F \rangle$ (deterministički) automat, tada definišemo *monoid automata* $\mathbf{A}$ kao podmonoid polugrupe transformacija $\mathcal{T}r(S)$ generisan funkcijama prelaza M_a, $a \in \Sigma$. Jasno, reč je o konačnom monoidu, kojeg ćemo označavati sa $\mathcal{M}(\mathbf{A})$. Nije teško videti da $\mathcal{M}(\mathbf{A})$ ima reprezentaciju preko Booleovih matrica. Naime, ako za $a \in \Sigma$ definišemo kvadratnu matricu B^a formata $|S|$ (indeksiranu sa $S \times S$) sa

$$B^a_{p,q} = \begin{cases} 1, & \delta(p,a) = q, \\ 0, & \text{inače}, \end{cases}$$

lako se pokazuje da se preslikavanje $M_a \mapsto B^a$, $a \in \Sigma$, može proširiti do potapanja monoida $\mathcal{M}(\mathbf{A})$ u monoid svih Booleovih matrica uočenog formata.

Sada kažemo da homomorfizam monoida $\varphi : \Sigma^* \to M$ *prepoznaje* jezik $L \subseteq \Sigma^*$ ako je $L = \varphi^{-1}(\varphi(L))$, tj. ako postoji podskup $P \subseteq M$ takav da važi $L = \varphi^{-1}(P)$. Dalje, kažemo da monoid M *prepoznaje* jezik $L \subseteq \Sigma^*$ ako postoji homomorfizam $\varphi : \Sigma^* \to M$ koji prepoznaje L. Može se pokazati da ako automat $\mathbf{A}$ prihvata jezik L, tada monoid $\mathcal{M}(\mathbf{A})$ prepoznaje L. S druge strane, od svakog konačnog monoida se lako može napraviti poluautomat čiji je monoid izomorfan polaznom (primetimo da monoid automata u suštini zavisi samo od njegovog poluautomatskog dela), te da se početno stanje i završna stanja odaberu tako da ako uočeni monoid prepoznaje jezik L, da tada dobijeni automat prihvata L (ako je $L = \varphi^{-1}(P)$, dovoljno je staviti za q_0 jedinicu monoida i $F = P$). Tako, Kleenejeva teorema može da se preformuliše na sledeći način.

TEOREMA 1.4.3. *Za proizvoljan jezik* $L \subseteq \Sigma^*$, *sledeći uslovi su ekvivalentni:*

(1) L *je jezik nekog konačnog automata,*

(2) L *je prepoznat nekim konačnim monoidom,*

(3) L *je regularan.*

Iz gornjih ekvivalencija se odmah dobija

POSLEDICA 1.4.4. *Klasa regularnih jezika (nad proizvoljnim alfabetom) je zatvorena na skupovno-teoretske operacije (uniju, presek, komplement, razliku), homomorfizme i inverzne slike homomorfizama (slobodnih) monoida.*

Kako dokaz Kleenejeve teoreme sadrži efektivnu konstrukciju koja za dati regularni izraz daje konačan automat koji prihvata jezik predstavljen tim izrazom i kako se, poznavajući automate koji prihvataju jezike L_1 i L_2 lako konstruišu automati za $L_1 \cap L_2$ i $\Sigma^* \setminus L_1$, to znači da važi

POSLEDICA 1.4.5. *Jednakosna teorija Kleenejevih algebri je odlučiva.*

Dokaz. Po Posledici 1.3.7, identitet $p = q$ važi na svim Kleenejevim algebrama ako i samo ako je $\mathsf{L}(p) = \mathsf{L}(q)$. Konstruišimo automate koji prihvataju jezike $\mathsf{L}(p)$ i $\mathsf{L}(q)$ i od njih napravimo automat koji prihvata jezik $(\mathsf{L}(p) \cap (\Sigma^* \setminus \mathsf{L}(q))) \cup ((\Sigma^* \setminus \mathsf{L}(p)) \cap \mathsf{L}(q))$. Kako postoji algoritam koji daje odgovor na pitanje da li je jezik datog automata prazan (vidi Teoremu I.5.1 iz [104]), time smo dali i odgovor na pitanje da li je $\mathsf{L}(p) = \mathsf{L}(q)$, čime je tvrđenje dokazano. ∎

Neka je $L \subseteq \Sigma^*$ regularan jezik. Jasno, skup svih konačnih monoida koji prepoznaju L je parcijalno uređen u odnosu na relaciju *deljenja* (pri čemu monoid M_1 deli monoid M_2 ako je M_1 izomorfan količniku nekog podmonoida od M_2, tj. $M_1 \in \mathsf{HS}(M_2)$). Može se pokazati da u tom parcijalnom uređenju postoji najmanji monoid. Do na izomorfizam, taj monoid sa opisanim minimalnim svojstvom se može zadati i direktno, kao količnik slobodnog monoida Σ^*. Naime, posmatrajmo relaciju $\sim_L$ na Σ^* definisanu za $u, v \in \Sigma^*$ sa

$$u \sim_L v \text{ ako i samo ako } (\forall x, y \in \Sigma^*)\ xuy \in L \Leftrightarrow xvy \in L.$$

Direktno se pokazuje da je $\sim_L$ kongruencija na Σ^*, koju zovemo *sintaktička kongruencija jezika* L, dok je faktor-monoid $\Sigma^*/\sim_L$ (koji je minimalan konačan monoid koji prepoznaje L) *sintaktički monoid* jezika L.

PROPOZICIJA 1.4.6. *Sintaktički monoid jezika $L \subseteq \Sigma^*$ izomorfan je monoidu minimalnog automata za L.*

Kako bismo profinili ispitivanje regularnih jezika i njihove strukture, često se na sintaktičkom monoidu jezika uvodi poredak, čime se on obogaćuje do uređenog monoida. Najpre uočimo na Σ^* sledeću relaciju $\preceq_L$ ($u, v \in \Sigma^*$):

$$u \preceq_L v \text{ ako i samo ako } (\forall x, y \in \Sigma^*)\ xvy \in L \Rightarrow xuy \in L.$$

Lako se vidi da je $\preceq_L$ kompatiblino kvazi-uređenje na Σ^*, ali u opštem slučaju nije uređenje, jer imamo

$$u \sim_L v \text{ ako i samo ako } u \preceq_L v \text{ i } v \preceq_L u.$$

Međutim, nakon faktorizacije slobodnog monoida sa $\sim_L$, relacija $\leq_L$ definisana sa

$$(u/\sim_L) \leq_L (v/\sim_L) \text{ ako i samo ako } u \preceq_L v$$

(gornja definicija je logički ispravna zbog kompatibilnosti $\preceq_L$), jeste kompatibilni poredak na sintaktičkom monoidu jezika L, koji zovemo *sintaktički poredak* za L. Na taj način, dobijamo *uređeni sintaktički monoid jezika* L. Pokazuje se da ako je L prepoznat homomorfizmom $\varphi : \Sigma^* \to M$, gde je M (uređeni) sintaktički monoid jezika L, tada $P = \varphi(L) \subseteq M$ jeste ideal (sintaktičkog) poretka za L na M (što znači da iz $s \leq t$ i $t \in P$ sledi $s \in P$). Dakle, treća formulacija Kleenejeve teoreme bi mogla biti sledeća.

TEOREMA 1.4.7. *Jezik $L \subseteq \Sigma^*$ je regularan ako i samo ako je prepoznat idealom poretka nekog konačnog uređenog monoida.*

Svi gornji pojmovi mogu se analogno formulisati i za jezike koji ne sadrže praznu reč, pri čemu ulogu slobodnog monoida Σ^* preuzima slobodna polugrupa Σ^+. Tako dobijamo *(uređenu) sintaktičku polugrupu* jezika $L \subseteq \Sigma^+$.

Najraniji pokušaji (od sredine šezdesetih godina) klasifikacije regularnih jezika bili su upravo usmereni na karakterizaciju raznih potklasa regularnih jezika preko njihovih sintaktičkih monoida. Jedna od značajnijih klasa regularnih jezika su tzv. **-slobodni jezici*: reč je o najmanjoj klasi jezika koja sadrži konačne jezike i zatvorena je na Booleove operacije (tu spadaju svi jezici predstavljivi *proširenim regularnim izrazom* – dopuštena je upotreba simbola komplementiranja ^{c} – bez pojavljivanja *). 1965. godine, M. P. Schützenberger (jedan od najistaknutijih predstavnika "francuske škole" u teoriji polugrupa) je dokazao sledeću teoremu.

TEOREMA 1.4.8. (Schützenberger, [147]) *Jezik L je *-slobodan ako i samo ako je njegov sintaktički monoid $\mathcal{H}$-trivijalan, tj. ima samo trivijalne podgrupe.*

Od rezultata ovog tipa pomenućemo još dva. Jezik $L \subseteq \Sigma^+$ je *lokalno testabilan* ako se može dobiti primenom konačno mnogo Booleovih operacija na jezike oblika $u\Sigma^*$, $\Sigma^* v$ i $\Sigma^* w \Sigma^*$ za neke $u, v, w \in \Sigma^+$ (ovim jezicima odgovaraju mašine koje porede sadržaj konačne memorije i "prozora" date dimenzije koji čita deo unete reči, koje se zovu *skeneri*). Početkom sedamdesetih godina, Brzozowski i Simon, i, nezavisno, McNaughton, dobili su sledeći rezultat.

TEOREMA 1.4.9. (Brzozowski, Simon, [33], McNaughton, [109]) *Jezik L je lokalno testabilan ako i samo ako je njegova sintaktička polugrupa S lokalno idempotentna i komutativna (tj. ako je svaki njen lokalni monoid eSe polumreža, gde je $e \in S$ neki idempotent).*

Jezik $L \subseteq \Sigma^*$ je *testabilan po delovima* ako se može dobiti od jezika oblika $\Sigma^* a_1 \Sigma^* \dots \Sigma^* a_k \Sigma^*$ (gde je $a_1, \dots, a_k \in \Sigma$ i $k \geq 0$) primenom konačno mnogo Booleovih operacija. Mašine koje prihvataju ovakve jezike su tzv. *hidra-automati*, koji imaju h linearno uređenih glava, od kojih svaka čita po jedno slovo, tako da mašina može da pročita sve podnizove unete reči dužine $\leq h$ (koji se ne sastoje nužno od uzastopnih slova), a zatim ih poredi sa sadržajem konačne memorije. 1975. godine I. Simon dobija sledeću karakterizaciju.

TEOREMA 1.4.10. (Simon, [150]) *Jezik L je testabilan po delovima ako i samo ako je njegov sintaktički monoid $\mathcal{J}$-trivijalan.*

Međutim, sva navedena tvrđenja su samo instance jednog opštijeg tvrđenja. Kako bismo ga formulisali, potrebni su nam neki novi pojmovi.

Pseudovarijetet (algebri datog tipa) je klasa algebri zatvorena na homomorfne slike, podalgebre i *konačne* direktne proizvode. Na primer, sve konačne polugrupe (konačni monoidi) formiraju pseudovarijetet. Takođe, klase konačnih monoida (polugrupa) koje smo sreli u prethodnim teoremama:

- $\mathcal{H}$-trivijalni (još se zovu i *aperiodični*, ili *kombinatorni*) konačni monoidi,
- lokalno idempotentne i komutativne konačne polugrupe,
- $\mathcal{J}$-trivijalni konačni monoidi,

formiraju pseudovarijetete konačnih monoida (polugrupa). Uskoro ćemo videti da to nije slučajno. (Za detaljan pregled teorije pseudovarijeteta, upućujemo na [8].)

S druge strane, ako je $\mathcal{C}$ neka klasa jezika (u opštem slučaju, nad raznim azbukama), sa $\mathcal{C}(\Sigma^*)$ označavamo skup jezika nad Σ koji pripadaju klasi $\mathcal{C}$. Ako je $L \subseteq \Sigma^*$ i $w \in \Sigma^*$, definišemo *levi (desni) količnik* jezika L po w sa

$$w\backslash L = \{v \in \Sigma^* : wv \in L\} \quad (L/w = \{v \in \Sigma^* : vw \in L\}).$$

Najzad, klasa $\mathcal{V}$ regularnih jezika je $*$-*varijetet jezika* (ovaj termin ne treba mešati sa varijetetom algebri), ako su ispunjeni sledeći uslovi:

(1) za svaku azbuku Σ, $\mathcal{V}(\Sigma^*)$ je zatvoren na Booleove operacije,

(2) za svaki homomorfizam $\varphi : \Sigma_1^* \to \Sigma_2^*$, $L \in \mathcal{V}(\Sigma_2^*)$ povlači

$$\varphi^{-1}(L) \in \mathcal{V}(\Sigma_1^*),$$

(3) za sve $L \in \mathcal{V}(\Sigma^*)$ i $w \in \Sigma^*$ važi

$$w\backslash L, L/w \in \mathcal{V}(\Sigma^*).$$

Slično, ako u prethodnim definicijama slobodni monoid Σ^* zamenimo slobodnom polugrupom Σ^+, dobijamo pojam *+-varijeteta jezika.*

Koristeći Posledicu 1.4.4, možemo videti da svi regularni jezici formiraju $*$-varijetet jezika. Sada ćemo formulisati jedan od kamena temeljaca algebarske teorije formalnih jezika, *Eilenbergovu teoremu o varijetetima*, koju je S. Eilenberg objavio 1976. u drugom tomu svoje knjige [54], dajući tako zajednički okvir svim prethodnim rezultatima iz ovog poglavlja. Ova teorema je u znatnoj meri odredila pravce kasnijih istraživanja u teoriji formalnih jezika.

TEOREMA 1.4.11. (Eilenberg, [54]) *Pridruživanje* $\mathbf{V} \to \mathcal{V}$ *koje pseudovarijetetu konačnih monoida (polugrupa) dodeljuje klasu svih regularnih jezika čiji sintaktički monoidi (sintaktičke polugrupe) pripadaju* $\mathbf{V}$*, je bijekcija pseudovarijeteta konačnih monoida (polugrupa) i* $*$*-varijeteta (+-varijeteta) regularnih jezika.*

Na primer, Kleenejeva teorema tvrdi da pseudovarijetetu svih konačnih monoida odgovara $*$-varijetet svih regularnih jezika. Teoreme Schützenbergera, Brzozowski-Simon-McNaughtona i Simona su takođe tvrđenja gornjeg tipa. Međutim, bitno je napomenuti da ova tvrđenja *nisu posledice* Eilenbergove teoreme (npr. Eilenbergova teorema za aperiodične monoide tvrdi da pseudovarijetetu $\mathcal{H}$-trivijalnih konačnih monoida jednoznačno odgovara *neki* $*$-varijetet regularnih jezika, ali ne precizira koji), već njene instance u okviru kojih se tačno karakteriše odgovarajući varijetet jezika.

Na kraju, napomenimo da Eilenbergova teorema ima i svoj analogon za uređene monoide (polugrupe), koju je dokazao J.-E. Pin 1995. godine, pri čemu se pojam varijeteta jezika zamenjuje pojmom *pozitivnog varijeteta jezika* (vidi [123]).

1.5. Jednakosna logika

U ovom poglavlju ćemo se osvrnuti na neke osnovne činjenice vezane za logiku i univerzalnu algebru. Implicitno, one su već bile korišćene u dosadašnjem izlaganju. Međutim, pošto se najveći deo ove disertacije odnosi na identitete,

bitno je da preciziramo logičko okruženje koje omogućava rad sa njima. Reč je o formalnom sistemu koji zovemo *jednakosna logika*. Kompletnost jednakosne logike u odnosu na njene modele – (univerzalne) algebre (dakle, poklapanje relacije sintaktičke dedukcije sa model-teoretskom relacijom logičke posledice), predstavlja osnovu teorije varijeteta.

Najpre, neka je Θ neki skup identiteta datog tipa τ i $p = q$ identitet istog tipa. Kažemo da je $p = q$ *logička posledica* od Θ (što pišemo $\Theta \models p = q$), ako za svaku algebru $\mathbf{A}$ tipa τ za koju je $\mathbf{A} \models \Theta$ važi $\mathbf{A} \models p = q$. Ono što želimo je da nađemo formalnu teoriju čije će formule biti identiteti takvi da se iz Θ može formalno izvesti $p = q$ ako i samo ako je $\Theta \models p = q$. Razmotrimo sledeća pravila izvođenja (p, q, r, p_i, q_i su termi tipa τ nad unapred fiksiranim prebrojivo beskonačnim skupom promenljivih):

$$(Sim): \quad \frac{p = q}{q = p},$$

$$(Tranz): \quad \frac{p = q,\ q = r}{p = r},$$

$$(Zam): \quad \frac{q(x_1, \ldots, x_n) = r(x_1, \ldots, x_n)}{q(p_1, \ldots, p_n) = r(p_1, \ldots, p_n)},$$

$$(Sagl): \quad \frac{p_1 = q_1, \ldots, p_n = q_n}{f(p_1, \ldots, p_n) = f(q_1, \ldots, q_n)},$$

gde je f proizvoljan n-aran operacijski simbol. Pri tome je aksioma trivijalan identitet $x = x$. Primetimo da smo poslednja dva pravila mogli zameniti jednim pravilom "kompozicije":

$$(Komp): \quad \frac{p_1 = q_1, \ldots, p_n = q_n, r(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)}{r(p_1, \ldots, p_n) = s(q_1, \ldots, q_n)}.$$

Kako je ovim definisana formalna teorija, zapis $\Theta \vdash p = q$ ima svoje uobičajeno značenje: identitet $p = q$ ima svoj formalni dokazni niz iz hipoteza Θ. Sada važi

TEOREMA 1.5.1. (Birkhoff, 1935) *Neka je Θ proizvoljan skup identiteta datog tipa. Tada je $\Theta \models p = q$ ako i samo ako $\Theta \vdash p = q$.*

Dokaz gornje *teoreme kompletnosti za jednakosnu logiku* može se naći npr. u [36], Teorema 14.19.

Ranije smo već pominjali pojam jednakosne teorije. Podsetimo, skup identiteta Θ je *jednakosna teorija* ako postoji klasa algebri $\mathcal{K}$ odgovarajućeg tipa tako da je Θ tačno skup svih identiteta koji važe na svim članovima $\mathcal{K}$. U

tom slučaju pišemo $\Theta = Eq(\mathcal{K})$. S druge strane, skup identiteta je *deduktivno zatvoren* ako je zatvoren na gore navedena pravila izvođenja. Posledica teoreme kompletnosti je i sledeće tvrđenje.

POSLEDICA 1.5.2. *Skup identiteta je jednakosna teorija ako i samo ako je deduktivno zatvoren.*

Ako je Δ proizvoljan skup identiteta, tada *deduktivnim zatvorenjem* od Δ zovemo najmanji deduktivno zatvoren skup identiteta (odgovarajućeg tipa) koji sadrži Δ. Nije teško videti da je reč o svim identitetima koji se mogu formalno izvesti iz Δ, u oznaci

$$D(\Delta) = \{p = q : \ \Delta \vdash p = q\}.$$

Ukoliko Θ deduktivno zatvoren skup identiteta, za $\Delta \subseteq \Theta$ kažemo da je *baza identiteta* za Θ ako je $D(\Delta) = \Theta$. Slično, ako je $\mathcal{K}$ klasa istotipnih algebri, a Θ njena jednakosna teorija, kažemo da je Δ *baza identiteta* za $\mathcal{K}$ ako $\mathcal{K} \models \Delta$ i $\Delta \models \Theta$ (tj. Δ je baza za Θ). Naravno, svaka klasa $\mathcal{K}$ ima trivijalnu bazu $Eq(\mathcal{K})$. Klasa $\mathcal{K}$ je *aksiomatizovana* sa Δ ako su klasom $\mathcal{K}$ iscrpljeni svi modeli skupa identiteta Δ. Jasno, klasa $\mathcal{K}$ ima (jednakosnu) aksiomatizaciju ako i samo ako je $\mathcal{K}$ varijetet.

Naravno, gore opisani pojmovi se mogu definisati i za druge tipove formula (kvazi-identitete, univerzalne formule, itd.), pa tako dolazimo do definicije baze, aksiomatizacije, itd. kada radimo sa takvim formulama, odgovarajućim logičkim sistemima i teorijama (kao što su kvazi-teorija, ili univerzalna teorija klase $\mathcal{K}$, u oznaci $Q(\mathcal{K})$ i $Th_\forall(\mathcal{K})$, respektivno).

Za klasu $\mathcal{K}$ (deduktivno zatvoren skup identiteta) kažemo da je *konačno baziran(a)* ako ima konačnu bazu identiteta. Pitanje konačnih baza za varijetete je možda centralno pitanje jednakosne logike i sigurno je jedno od najinteresantnijih pitanja univerzalne algebre uopšte. Veliki deo ove disertacije posvećen je ovom problemu, specijalizovanom za varijetete Kleenejevih i srodnih algebri, kao i varijetete generisane raznim algebrama jezika. Pri tome će često biti korišćeno sledeće poznato tvrđenje.

TEOREMA 1.5.3. (Teorema kompaktnosti za identitete) *Neka je Θ proizvoljan skup identiteta i $p = q$ identitet odgovarajućeg tipa, tako da je $\Theta \models p = q$. Tada postoji konačan podskup $\Theta_0 \subseteq \Theta$ takav da $\Theta_0 \models p = q$.*

Dokaz. Tvrđenje dokazujemo primenom Teoreme kompletnosti. Naime, $\Theta \models p = q$ ekvivalentno je sa $\Theta \vdash p = q$. Međutim, u formalnom dokazu identiteta $p = q$ po hipotezama iz Θ učestvuje samo konačno mnogo identiteta iz Θ. Neka ti identiteti formiraju skup $\Theta_0 \subseteq \Theta$. Tada je $\Theta_0 \vdash p = q$, što je ekvivalentno sa $\Theta_0 \models p = q$. ∎

Teorema kompaktnosti nam je potrebna u sledećoj formi, u kojoj će ona kasnije imati višestruku primenu.

POSLEDICA 1.5.4. *Neka deduktivno zatvoren skup formula* Θ *(ili klasa* $\mathcal{K}$*) ima konačnu bazu identiteta i neka je* Δ *proizvoljna baza za* Θ *(za* $\mathcal{K}$*). Tada postoji konačna baza* Δ_0 *za* Θ *(za* $\mathcal{K}$*) sadržana u* Δ.

Dokaz. Neka je Γ konačna baza za Θ. Tada za svaki identitet $\varepsilon \in \Gamma$ važi $\Delta \models \varepsilon$, pa se po prethodnoj teoremi može izabrati *konačan* podskup $\Delta_\varepsilon \subseteq \Delta$ tako da važi $\Delta_\varepsilon \models \varepsilon$. Definišimo

$$\Delta_0 = \bigcup_{\varepsilon \in \Gamma} \Delta_\varepsilon.$$

Jasno, reč je o konačnom skupu, i pri tome je $\Delta_0 \models \Gamma$. To znači da je $\Theta = D(\Gamma) \subseteq D(\Delta_0) \subseteq D(\Delta) = \Theta$, tj. $D(\Delta_0) = \Theta$, što znači da je $\Delta_0 \subseteq \Delta$ baza za Θ. ∎

1.6. Problem reči za Kleenejeve algebre

Problem reči je možda najinteresantniji od algoritamskih problema u algebri. U izvesnom smislu, u "menadžeriji" algoritamskih problema, on zauzima centralno mesto: u svakom od njih, članovi varijeteta sa nerešivim problemom reči pružaju veoma značajnu informaciju. Istorijski, ovaj problem potiče iz klasičnih algebarskih struktura, pre svega grupa i polugrupa. Grubo govoreći, polazeći od grupno-teoretskog pojma predstavljanja grupe sistemom generatora i relacija među njima, pitamo se kada dve reči sačinjene od generatora predstavljaju isti element grupe, tj. kada se jednakost te dve reči može izvesti na osnovu datih definišućih jednakosti među generatorima. Problem reči je *rešiv* ako postoji algoritam koji daje odgovor na ovo pitanje.

Probleme reči prvi je razmatrao Axel Thue početkom XX veka. On je posmatrao tzv. *asocijativne račune* (koje danas zovemo "Thueovi sistemi"), drugim rečima, problem reči za polugrupe. Od tada, a naročito u novije vreme, istraživanja na polju problema reči doživljavaju buran razvitak, pri čemu se pojavljuju lepi, interesantni i najčešće veoma teški problemi. Za izuzetno iscrpan pregled problematike algoritamskih problema (a naročito problema reči) za varijetete klasičnih algebri, upućujemo na rad Kharlampovich, Sapir [81].

Primera radi, može se pokazati (vidi Posledicu 15.1 u [45]) da je *diedarska grupa stepena n* (grupa simetrija pravilnog n-tougla) prezentirana na sledeći način:

$$D_n = \langle a, b |\ a^n = 1,\ b^2 = 1,\ ab = ba^{-1} \rangle.$$

Jasno, pri tome a predstavlja rotaciju za $\frac{2\pi}{n}$, a b jednu od osnih simetrija pravilnog n-tougla. Međutim, gornji zapis znači da se sve jednakosti koje važe za ove generatore mogu *formalno* izvesti iz date tri relacije, uz korišćenje aksioma grupa. Pri tome upotrebljavamo pravila jednakosne logike. No, obratimo pažnju na jednu ključnu razliku u odnosu na identitete: dok u identitetima figurišu *promenljive* na koje se mogu primeniti zamene preko pravila (Zam), dotle je ovde reč o *jednakostima* u kojima figurišu generatori a, b koji imaju tretman konstantnih simbola i oni ne mogu, kao promenljive, biti zamenjeni drugim rečima. Dakle, dozvoljene su samo manipulacije rečima u smislu primene operacija na već dobijene reči.

U konkretnom slučaju naše diedarske grupe, dobijamo da se sve grupne reči nad a, b (a u odnosu na date relacije) mogu svesti na oblik $a^i b^j$, gde je $0 \leq i \leq n-1$ i $0 \leq j \leq 1$. Da, međutim, nikoje dve od ovih reči nisu jednake u D_n dokazuje upravo mogućnost *reprezentacije* generatora preko geometrijskih transformacija, što na kraju i daje efektivan algoritam koji rešava problem reči za D_n. Tako problemi reči veoma često podrazumevaju "izlete" iz algebre u geometriju, topologiju, kombinatoriku i teoriju grafova, teoriju diferencijalnih jednačina, itd. To čini probleme reči veoma zanimljivom oblašću za istraživanje. Naravno, i problemi reči za razne klase algebri mogu imati međusobne povezanosti (kao što će to biti i u slučaju Kleenejevih algebri).

Sada ćemo dati opšte-algebarsku, preciznu definiciju problema reči u varijetetu algebri $\mathcal{V}$ tipa τ. Najpre, ako je G neki skup simbola, tada ćemo sa τ_G označiti tip (algebarski jezik) koji je dobijen od τ tako što su mu dodati elementi skupa G kao novi konstantni simboli. Par oblika $\langle G, R\rangle$ je *prezentacija tipa* τ ako je R skup identiteta *bez promenljivih* (znači, u kojima učestvuju samo konstantni simboli) tipa τ_G. Prezentacija je *konačna* ako su i G i R konačni skupovi. Dalje, ako je $\mathbf{A}$ algebra tipa τ i $G \subseteq A$, sa $\mathbf{A}_G$ ćemo označiti algebru tipa τ_G proširenu elementima iz G kao konstantama (čije se interpretacije poklapaju sa odgovarajućim konstantnim simbolima).

Ako je Δ baza identiteta za varijetet $\mathcal{V}$, kažemo da je algebra $\mathbf{A}$ tipa τ *prezentirana sa* $\langle G, R\rangle$, u oznaci $\mathbf{A} = \langle G|R\rangle_{\mathcal{V}}$ (naravno, ovu oznaku treba shvatiti do na izomorfizam), ako važi:

(1) algebra $\mathbf{A}$ je generisana sa G,

(2) $\mathbf{A}_G \models \Delta \cup R$,

(3) za svaki identitet $w_1 = w_2$ tipa τ_G bez promenljivih važi:

$$\text{ako } \mathbf{A}_G \models w_1 = w_2, \text{ onda } \Delta \cup R \vdash w_1 = w_2.$$

Navešćemo još jednu definiciju prezentacije algebre (za koju se može pokazati da je ekvivalentna prethodnoj), koja više korespondira sa klasičnom definicijom prezentacije grupa, i u kojoj više figurišu algebarski nego jednakosnologički pojmovi. Naime, kažemo da je $\mathbf{A} = \langle G|R\rangle_{\mathcal{V}}$ ako je

$$\mathbf{A} \cong \frac{\mathbf{F}_{\mathcal{V}}(G)}{\theta_R},$$

gde je $\mathbf{F}_{\mathcal{V}}(G)$ $\mathcal{V}$-slobodna algebra nad G, a θ_R kongruencija na toj algebri generisana parovima $\langle \bar{w}_1, \bar{w}_2\rangle$ za sve jednakosti $w_1 = w_2$ iz R (pri čemu $\bar{w}$ označava vrednost terma w u $\mathbf{F}_{\mathcal{V}}(G)$ u odnosu na standardnu interpretaciju).

Naravno, sa računarskog (a time i algoritamskog) stanovišta, interesantne su samo algebre date konačnom količinom podataka, dakle *konačno prezentirane algebre*. *Problem reči* za varijetet $\mathcal{V}$ pita da li za svaku konačno prezentiranu algebru $\langle G|R\rangle_{\mathcal{V}}$ iz $\mathcal{V}$ postoji algoritam koji odlučuje da li su dva terma (dve "reči") w_1, w_2 tipa τ_G bez promenljivih jednaki. Drugim rečima (prihvatajući Churchovu tezu), pitamo se da li je skup identiteta tipa τ_G bez promenljivih koji važe na $\mathbf{A}_G$ rekurzivan za svaku konačno prezentiranu algebru iz $\mathcal{V}$ (ekvivalentno, da li je relacija θ_R rekurzivan skup).

Varijetet $\mathcal{V}$ ima *uniformno rešiv* problem reči, ukoliko postoji univerzalni algoritam koji istovremeno rešava problem reči za sve konačno prezentirane algebre iz $\mathcal{V}$. Naravno, uniformna rešivost problema reči povlači njegovu (lokalnu) rešivost u svakom varijetetu, ali obratno ne mora da važi (konstruisani su kontraprimeri). Takođe, Maljcev je 1958. napomenuo da je za proizvoljan varijetet $\mathcal{V}$ uniforman problem reči ekvivalentan odlučivosti njegove kvazi-teorije $Q(\mathcal{V})$.

Kasnije, nađeni su mnogi primeri konačno prezentiranih algebri sa nerešivim problemom reči, čime je negativno rešen problem reči za razne "klasične" varijetete. Tako su, na primer, E. Post i A. Markov nezavisno 1947. našli konačno prezentirane polugrupe sa nerešivim problemom reči. 1953. Tarski nalazi konačno prezentiranu relacionu algebru čiji je problem reči nerešiv. Takođe, 1954/55. P. S. Novikov i W. Boone su (opet, nezavisno) pokazali da varijetet grupa nema rešiv problem reči. Kasnije, Cejtin je našao sasvim jednostavan primer polugrupe sa nerešivim problemom reči. Primer je sledeći:

$$\begin{aligned} G &= \{a, b, c, d, e\}, \\ R &= \{ac = ca,\ ad = da,\ bc = cb,\ bd = db, \\ &\qquad abac = abace,\ eac = ac,\ edb = be\}. \end{aligned}$$

S druge strane, Abelove grupe, kvazigrupe, komutativne polugrupe i komutativni prsteni, kao i neasocijativni prsteni imaju uniformno rešiv problem reči.

Uočimo da je bitno *u odnosu na koji varijetet* se prezentira algebra. Naime, G. Hutchinson i L. Lipschitz su 1973/74. dokazali da varijetet modularnih mreža nema rešiv problem reči, dok varijetet svih mreža ima uniformno rešiv problem reči (T. Evans). Ova prividna protivrečnost znači da postoji mreža koja je konačno prezentirana u varijetetu modularnih mreža i koja ima nerešiv problem reči, ali da baš ta mreža nema konačnu prezentaciju u varijetetu *svih* mreža. Drugim rečima, modularni zakon se nikako ne može "simulirati" konačnim skupom jednakosti na generatorima (ovde do izražaja dolazi razlika između identiteta i jednakosti u smislu primene pravila zamene).

Nerešivost problema reči za polugrupe, tj. egzistencija konačno prezentirane polugrupe sa nerešivim problemom reči omogućava nam da, indirektnim metodama, pokažemo nerešivost problema reči za neke druge klase algebri. Veza se ostvaruje preko sledećeg tvrđenja.

TEOREMA 1.6.1. (Crvenković, Madarász, [50]) *Neka je $\mathcal{V}$ varijetet koji u svom tipu sadrži binarnu asocijativnu operaciju. Ako se svaka polugrupa može potopiti u redukt koji odgovara ovoj operaciji neke algebre iz $\mathcal{V}$, tada $\mathcal{V}$ ima nerešiv problem reči.*

Dokaz. Neka je $S = \langle G|R\rangle_{\mathcal{S}}$ polugrupa sa nerešivim problemom reči (gde $\mathcal{S}$ označava varijetet svih polugrupa). Tada relacije iz R jesu, u stvari, jednakosti između nekih (polugrupnih) reči, pa kako tip varijeteta $\mathcal{V}$ sadrži asocijativnu binarnu operaciju, možemo ih tumačiti kao jednakosti tipa tog varijeteta. Zato možemo posmatrati par $\langle G, R\rangle$ kao prezentaciju u $\mathcal{V}$, pa definišimo $\mathbf{A} = \langle G|R\rangle_{\mathcal{V}}$.

Sada ćemo pokazati da algebra $\mathbf{A} \in \mathcal{V}$ nema rešiv problem reči. Lako se vidi da će taj cilj biti postignut ako pokažemo da za svaki identitet $u = v$ bez promenljivih, a nad skupom konstantnih simbola iz G, koji sadrži samo razmatranu binarnu asocijativnu operaciju (dakle, za svaku polugrupnu G-jednakost) važi:

$$S_G \models u = v \text{ ako i samo ako } \mathbf{A}_G \models u = v.$$

Najpre, ako $S_G \models u = v$, to znači da je relacija $u = v$ logička posledica asocijativnog zakona i relacija iz R. Neka Θ označava neku bazu varijeteta $\mathcal{V}$. Kako je asocijativni zakon za posmatranu binarnu operaciju posledica od Θ, sledi da $\Theta \cup R \vdash u = v$. No, po definiciji prezentacije algebre, imamo da $\mathbf{A}_G \models \Theta \cup R$, pa dobijamo $\mathbf{A}_G \models u = v$.

Obratno, pretpostavimo da $\mathbf{A}_G \models u = v$. Ponovo po definiciji prezentacije algebre $\mathbf{A}$, mora biti $\Theta \cup R \vdash u = v$, gde je Θ neka baza identiteta varijeteta $\mathcal{V}$. Pretpostavimo da $S_G \not\models u = v$. Međutim, po uslovima teoreme, polugrupa

S se može potopiti u odgovarajući redukt neke algebre $\mathbf{B} \in \mathcal{V}$. Ako generatore $G \subseteq S$ označimo istim simbolima i u $\mathbf{B}$, tada imamo $\mathbf{B}_G \models R$, šta više, $\mathbf{B}_G \models \Theta \cup R$, ali $\mathbf{B}_G \not\models u = v$. Ovo je kontradikcija sa zaključkom da $\Theta \cup R \vdash u = v$, pa je tražena ekvivalencija dokazana, a zajedno sa njom i tvrđenje teoreme. ∎

POSLEDICA 1.6.2. (Crvenković, Madarász, [50]) *Varijetet Kleenejevih algebri $\mathcal{KA}$ ima nerešiv problem reči.*

Dokaz. Neka je S proizvoljna polugrupa. Preslikavanjem $\iota : S \to \mathcal{P}(S^1)$ definisanim za sve $s \in S$ sa

$$\iota(s) = \{s\},$$

ona se potapa u multiplikativni redukt Kleenejeve algebre $\mathrm{M}(S)$ definisane u Lemi 1.3.1. Prema tome, ispunjeni su uslovi prethodne teoreme, pa tvrđenje sledi. ∎

Na sličan način se može pokazati nerešivost problema reči za relacione algebre, prstene, involutivne polugrupe, Baerove *-polugrupe, itd.

Osim toga, gornji rezultat ćemo iskoristiti u poslednjoj glavi, kako bismo konstruisali varijetet dinamičkih algebri sa neodlučivom jednakosnom teorijom. Tu neodlučivost ćemo dobiti upravo prenosom nerešivog problema reči za Kleenejeve algebre u indekse unarnih operacija u dinamičkim algebrama.

U ovoj glavi, naš osnovni cilj je da prikažemo jedan od klasičnih rezultata algebarske teorije formalnih jezika (koji je ujedno i polazna tačka za rezultate ove disertacije), a to je da regularni identiteti, tj. identiteti algebri jezika (koji se po Posledici 1.3.5 poklapaju sa identitetima Kleenejevih algebri) nemaju konačnu bazu. Prvi dokaz ovog tvrđenja dao je Redko [134] 1964. godine. Prvu eksplicitnu jednakosnu aksiomatizaciju za varijetet $\mathcal{L} = \mathcal{KA}$ dao je Krob [93] tek 1991. potvrđujući tako dvadeset godina staru hipotezu Conwaya [40].

Međutim, pre toga, razmotrićemo neke mogućnosti da se identiteti Kleenejevih algebri ipak na neki način dobiju iz konačnog skupa formula prvog reda. Tačnije, posmatraćemo razne konačne skupove kvazi-identiteta iz kojih se kao skup jednakosnih posledica dobija baš $Eq(\mathcal{KA})$.

2.1. Meta-pravila i aksiomatizacija kvazi-identitetima

Nakon što je Redko [134] dokazao da identiteti regularnih jezika nemaju konačnu bazu (kasnije su nađeni i drugi dokazi za ovu činjenicu), krenulo se u potragu za nekim načinom da se ovi identiteti ipak opišu konačnim skupom aksioma. Na taj način se otkrilo da postoje konačno bazirane teorije kvazi-identiteta čije su jednakosne posledice tačno posmatrani identiteti. Nije teško videti da, drugim rečima, ovo znači da postoje konačno aksiomatizovani kvazi-varijeteti $\mathcal{Q}$ koji generišu $\mathcal{KA}$, tj. $\mathcal{KA} = \mathsf{HSP}(\mathcal{Q})$.

S druge strane, neki autori, vezujući se više za logičke nego univerzalno-algebarske metode, posmatraju problem na drugi način ostajući tako, na izvestan način, u okvirima jednakosne logike. Naime, za svaki kvazi-identitet φ oblika

$$p_1 = q_1 \ \wedge \ \ldots \ \wedge \ p_k = q_k \ \Rightarrow \ p = q,$$

koji se pojavljuje u opisanim aksiomatizacijama (gde termi p_i, q_i, p, q zavise od promenljivih $x_1, \ldots, x_n$), jednakosna logika za identitete na jeziku $\{+, \cdot, {}^*, 0, 1\}$

se *proširuje* novim pravilom izvođenja

$$(\varphi): \qquad \frac{p_1(r_1,\ldots,r_n)=q_1(r_1,\ldots,r_n),\ldots,p_k(r_1,\ldots,r_n)=q_k(r_1,\ldots,r_n)}{p(r_1,\ldots,r_n)=q(r_1,\ldots,r_n)},$$

gde su $r_1,\ldots,r_n$ proizvoljni regularni izrazi. U ovako modifikovanoj jednakosnoj logici se sada iz konačnog skupa identiteta (najčešće, iz aksioma Conwayevih ω-idempotentnih *-poluprstena) može dobiti tačno jednakosna teorija za $\mathcal{KA}$. Ovakva novouvedena pravila izvođenja (odnosno, odgovarajući kvazi-identiteti) se zovu *meta-pravila.* Dati skup meta-pravila je *kompletan* za $\mathcal{KA}$ u odnosu na skup identiteta Θ ako se iz Θ u odgovarajućoj proširenoj jednakosnoj logici kao skup posledica dobija baš $Eq(\mathcal{KA})$.

Prvi pokušaji ovakvih aksiomatizacija sadržani su, na primer, u [1], [139] i [18]. Verovatno najpoznatija od njih je "aksiomatizacija" koju je 1966. dao Salomaa [139]; međutim, kvazi-identiteti koje je on dao bili su tačni u algebrama regularnih jezika *samo* u odnosu na standardnu interpretaciju (a ne i u odnosu na ostale), a njegovo "meta-pravilo" sadržavalo je nealgebarski uslov za neke od regularnih izraza koji u njemu učestvuju (u smislu da se taj uslov ne može izraziti identitetom).

Možda je najjednostavniji rezultat u ovom pravcu dobio Krob [93], potvrđujući hipotezu koju je postavio Boffa u [28]. Naime, posmatrajmo kvazi-identitet

$$x^2 = x \;\Rightarrow\; x^* = 1 + x. \tag{3}$$

Teorema 2.1.1. (Krob, [93, Posledica 15.13]) *Meta-pravilo (3) je kompletno za $\mathcal{KA}$ u odnosu na identitete koji definišu Conwayeve *-poluprstene, zajedno sa identitetom $1 + 1 = 1$.*

Kvazivarijetet definisan identitetima Conwayevih *-poluprstena, identitetom $1 + 1 = 1$ i (3) označićemo sa $\mathcal{Q}_1$.

Drugi kvazivarijetet (označićemo ga sa $\mathcal{Q}_2$) sa traženim osobinama konstruisao je Kozen u radu [86]. Naime, kako u proizvoljnom idempotentnom poluprstenu imamo prirodno definisanu relaciju poretka, to identitet $p+q = q$ možemo pisati još i kao $p \leq q$. Sada posmatrajmo sledeće kvazi-identitete:

$$xy \leq y \;\Rightarrow\; x^*y \leq y, \tag{4}$$

$$yx \leq y \;\Rightarrow\; yx^* \leq y. \tag{5}$$

Teorema 2.1.2. (Kozen, [86, Teorema 19]) *U odnosu na identitete Conwayevih *-poluprstena i $1+1 = 1$, meta-pravila (4) i (5) čine kompletan sistem pravila za $\mathcal{KA}$.*

Može se pokazati da se implikacije (4) i (5) mogu zameniti sledećom:

$$1 + x + y^2 \leq y \;\Rightarrow\; x^* \leq y.$$

Najzad, treći rezultat ovog tipa dali su Arhangelskij i Gorškov [17]. Njihova aksiomatizacija je sledeća.

Teorema 2.1.3. (Arhangleskij, Gorškov, [17]) *Kvazivarijetet $\mathcal{Q}_3$ definisan identitetima Conwayevih ω-idempotentnih *-poluprstena i kvazi-identitetima*

$$(x_1 + x_2)^* z = (y_1 + y_2)^* u \;\Rightarrow\; (x_1 + x_2)^* z = (x_1 + x_2 y_2^* y_1)^* (z + x_2 y_2^* u),$$
$$z(x_1 + x_2)^* = u(y_1 + y_2)^* \;\Rightarrow\; z(x_1 + x_2)^* = (z + u y_2^* x_2)(x_1 + y_1 y_2^* x_2)^*,$$

generiše varijetet $\mathcal{KA}$.

Podsetimo se, varijetet $\mathcal{KA}$ je po definiciji generisan standardnim Kleenejevim algebrama binarnih relacija. Ova klasa nije kvazivarijetet (jer se može pokazati da nije zatvorena na ultraproizvode), ali važi

Propozicija 2.1.4. *Klasa standardnih Kleenejevih algebri je zatvorena na direktne proizvode.*

Dokaz. Neka je $\{\mathbf{K}_i\}_{i\in I}$ proizvoljna familija standardnih Kleenejevih algebri. Pri tome bez ograničenja opštosti možemo pretpostaviti da je $\mathbf{K}_i \leq \mathbf{Rel}(A_i)$, gde su A_i, $i \in I$, disjunktni skupovi. Posmatrajmo preslikavanje

$$\iota : \prod_{i\in I} K_i \to \mathcal{P}(A \times A),$$

gde je

$$A = \bigcup_{i\in I} A_i,$$

definisano sa

$$\iota(\langle \rho_i \rangle_{i\in I}) = \bigcup_{i\in I} \rho_i.$$

Zbog disjunktnosti osnovnih skupova A_i, jasno je da je ι injektivno preslikavanje. Takođe, lako se pokazuje da je reč o homomorfizmu. ∎

Kvazivarijetet generisan svim standardnim Kleenejevim algebrama označićemo sa $\mathcal{Q}_0$. Može se pokazati da važi $\mathcal{Q}_0 \subseteq \mathcal{Q}_1 \subseteq \mathcal{Q}_2$, pri čemu su sve inkluzije striktne. Prva od ovih inkluzija sledi iz činjenice, koja se može izvesti iz Propozicije 1.2.4, da $\mathcal{Q}_0$ nije konačno aksiomatizabilna klasa. S druge strane, kvazivarijetet $\mathcal{Q}_3$ je neuporediv sa ova preostala tri.

Na kraju, zanimljivo je razmotriti jednu Kleenejevu algebru iz $\mathcal{Q}_3 \setminus \mathcal{Q}_2$. Reč je o $\mathbf{Reg}(\{a\})/\theta$, gde je θ kongruencija algebre $\mathbf{Reg}(\{a\})$ koja ima četiri klase: u jednu klasu spada $\emptyset$, u drugu $\{\lambda\}$, treću klasu čine svi konačni jezici sem prethodna dva, dok su u četvrtoj klasi svi beskonačni jezici. Ova algebra se u literaturi zove *Conwayev skok* (označavaćemo je sa $\mathbf{C}_4$) i reč je o najmanjoj (u smislu broja elemenata) nereprezentabilnoj Kleenejevoj algebri. Kako bismo obrazložili njenu nereprezentabilnost, uočimo sledeći pojam.

Za Kleenejevu algebru $\mathbf{K}$ kažemo da je **-neprekidna* (ili samo neprekidna) ako, grubo govoreći, za sve $a \in K$, a^* predstavlja (baš kao za jezike, odnosno relacije) sumu "geometrijskog reda" $\sum_{n\geq 0} a^n$. Preciznije, tražimo da za sve $a, b, c, d \in K$ za koje je $ab^n c \leq d$ za sve $n \geq 0$ (pri čemu je $b^0 = 1$), važi

$$ab^* c \leq d.$$

Drugim rečima, ab^*c je supremum skupa $\{ab^n c : n \geq 0\}$ u odnosu na prirodni poredak u idempotentnom poluprstenu $\mathbf{K}$.

Ako sada izaberemo u $\mathbf{C}_4$ (čije elemente označavamo sa $\emptyset, \lambda, F, \infty$, pri čemu je iz oznaka jasno o kojim se klasama relacije θ radi) da je $a = c = \lambda$ i $b = F$, imamo da je za sve $n \geq 0$, $F^n = F$ (pošto je konkatenacija konačno mnogo konačnih jezika konačan jezik). Stoga je F, a ne $F^* = \infty$, infimum skupa $\{F^n : n \geq 0\}$. S druge strane, jasno je da je svaka standardna Kleenejeva algebra neprekidna.

Pojam neprekidnosti biće detaljnije razmotren u Poglavlju 6.4. Međutim, već sada se postavlja pitanje aksiomatizacije neprekidnih Kleenejevih algebri, kao prirodne potklase od $\mathcal{KA}$ u kojoj * zaista odgovara intuitivnom pojmu iteracije [85]. U tom smislu imamo sledeću hipotezu.

PROBLEM 1. (Kozen, [86]) *Da li je tačno da je kvazivarijetet generisan neprekidnim Kleenejevim algebrama jednak $\mathcal{Q}_2$?*

2.2. Grupe i matrični identiteti Kleenejevih algebri

Kao što smo to već ranije rekli, šezdesetih godina je pokazano da identiteti (regularnih) jezika nemaju konačnu bazu. Međutim, kako izgledaju te (nužno beskonačne) baze identiteta? Ovo pitanje je dugo bilo otvoreno. Odgovarajuću pretpostavku je formulisao Conway [40] još 1971. godine, ali je

njegova hipoteza bila dokazana čitave dve decenije kasnije (Krob [93], 1991. godine). Conwayeva ingeniozna ideja je bila da traženi identiteti moraju, na neki način, da "izraze" prepoznavanje regularnih jezika od strane konačnih monoida (vidi Poglavlje 1.4). Konkretno, Conway svakom konačnom monoidu M pridružuje identitet $P(M)$ nad skupom promenljivih $X_M = \{x_m : m \in M\}$ koji je ekvivalentan sa

$$\left(\sum_{m\in M} x_m\right)^* = \sum_{m\in M} \varphi_M^{-1}(m),$$

gde je $\varphi_M : X_M^* \to M$ homomorfizam monoida koji proširuje preslikavanje $x_m \mapsto m$, $m \in M$. Gornji identitet implicitno izražava poznatu *teoremu Myhill–Nerodea* koja kaže da je jezik regularan ako i samo ako je unija celih klasa ekvivalencije neke kongruencije konačnog indeksa na slobodnom monoidu (što je zapravo još jedna varijanta Kleenejeve teoreme). U potrazi za konkretnijim i formalnijim načinom da se gornji identitet zapiše, Conway dolazi do *monoidnih matričnih identiteta.* Za naša razmatranja će, međutim, biti dovoljno da posmatramo slučaj kada je monoid u pitanju *grupa*, pa ćemo tako raditi sa *grupnim matričnim identitetima.* Ali, najpre moramo definisati operaciju zvezdiranja na kvadratnim matricama regularnih izraza.

Neka je A matrica formata $n \times n$ čiji su elementi regularni izrazi (tj. termi na jeziku Kleenejevih algebri). Definišemo matricu A^* (istog formata) indukcijom po n.

- Za $n = 1$, $A = [r]$, definišemo $A^* = [r^*]$.
- Neka je $n = k + 1$, $k \geq 1$. Podelimo matricu na blokove:

$$A = \begin{bmatrix} P & Q \\ R & S \end{bmatrix},$$

gde je P matrica formata $k \times k$, S je formata 1×1, dok su Q i R redom odgovarajuće vektor-kolone i vektor-vrste. Sada je

$$A^* = \begin{bmatrix} (P + QS^*R)^* & (P + QS^*R)^*QS^* \\ (S + RP^*Q)^*RP^* & (S + RP^*Q)^* \end{bmatrix}.$$

Neka je $G = \{g_1, \ldots, g_n\}$ proizvoljna konačna grupa. Definisaćemo matricu $A_G = [\alpha_{ij}]_{n\times n}$ pridruženu ovoj grupi čiji su elementi promenljive iz skupa $X = \{x_k : k \geq 1\}$ na sledeći način:

$$\alpha_{ij} = x_k \Leftrightarrow g_ig_k = g_j \ (\Leftrightarrow g_i^{-1}g_j = g_k).$$

Dalje, neka $\mathbf{v}_n^{(1)}$ označava vrstu dužine n čiji je prvi element 1, a ostali 0, dok $\mathbf{s}_n$ označava kolonu visine n čiji su svi elementi jednaki 1. Identitet

$$\mathbf{v}_n^{(1)} A_G^* \mathbf{s}_n = (x_1 + \ldots + x_n)^* \tag{6}$$

(gde matricu 1×1 sa leve strane identifikujemo sa njenim jedinim elementom) zovemo *grupni matrični identitet pridružen grupi* G i označavamo ga sa $P(G)$. Primetimo da je leva strana gornjeg identiteta u stvari zbir prve vrste matrice regularnih izraza A_G^*.

Sada možemo formulisati glavni rezultat Krobove fundamentalne studije [93] (reč je o radu od 137 strana, koji je zauzimao čitav drugi broj volumena 89 časopisa *Theoretical Computer Science*). Radi kompletnosti, podsetićemo se *Conwayevih identiteta*:

$$(x + y)^* = (x^* y)^* x^*,$$
$$(xy)^* = 1 + x(yx)^* y.$$

Svaki poluprsten sa unarnom operacijom * koji zadovoljava gornje identitete je *Conwayev* **-poluprsten*. On je ω-idempotentan ako zadovoljava $1^* = 1$.

TEOREMA 2.2.1. (Krob, [93, Teorema 13.5]) *Identiteti* ω*-idempotentnih Conwayevih* **-poluprstena, zajedno sa matričnim identitetima* $P(G)$ *pridruženim svakoj konačnoj grupi* G*, čine bazu regularnih identiteta (tj. bazu identiteta za* $\mathcal{KA}$*).*

Međutim, kasnije se ispostavilo da se gornje tvrđenje može pojačati u smislu potrebnih i dovoljnih uslova da aksiome ω-idempotentnih Conwayevih *-poluprstena i identiteti $P(G)$, gde G pripada nekoj *klasi* konačnih grupa, čine bazu za $\mathcal{KA}$. Podsetimo, grupa H *deli* grupu G ako je H izomorfna faktor-grupi neke podgrupe od G; u univerzalno-algebarskoj terminologiji, $H \in \mathsf{HS}(G)$.

TEOREMA 2.2.2. (Bloom, Ésik, [26]) *Neka je* $\mathcal{G}$ *neka klasa konačnih grupa. Aksiome* ω*-idempotentnih Conwayevih* **-poluprstena i matrični identiteti* $P(G)$ *za* $G \in \mathcal{G}$ *čine bazu identiteta za* $\mathcal{KA}$ *ako i samo ako svaka konačna prosta grupa deli neku grupu iz* $\mathcal{G}$*.*

Gornja teorema vodi nekim redukcijama baze za $\mathcal{KA}$ iz Teoreme 2.2.1. Na primer, dovoljno je uzeti identitete $P(G)$ za sve konačne *proste grupe*, dakle $P(Z_p)$ za sve proste brojeve p i $P(G)$ za sve nekomutativne proste grupe. (Uzgred, pomenimo da je u odnosu na ω-idempotentne Conwayeve *-poluprstene, identitet

$$(1 + x + \ldots + x^{p-1})(x^p)^* = x^*$$

ekvivalentan sa $P(Z_p)$.) Dalje, za klasu $\mathcal{G}$ možemo uzeti samo konačne simetrične grupe permutacija (čak, možemo odabrati proizvoljno $n_0 \geq 1$ i posmatrati samo grupe S_n za $n \geq n_0$). Isto važi i za alternativne grupe permutacija A_n (ove poslednje dve redukcije baze su bile poznate još i Krobu). Na taj način prirodno se postavlja sledeće pitanje.

PROBLEM 2. *Da li Kleenejeve algebre imaju nezavisnu (minimalnu) bazu identiteta?*

Napomenimo da je jedna aksiomatizacija Kleenejevih algebri, suštinski različita od Krobove, data u radu Bloom, Ésik [22]. Ona je dobijena u širem kontekstu *iteracijskih teorija* [23], koje predstavljaju primenu teorije kategorija u teorijskom računarstvu.

Interesantno je da se uz grupne (monoidne) matrične identitete vezuje jedno meta-pravilo, tzv. *Conwayevo meta-pravilo.* Neka je M konačan monoid i $\{r_m\}_{m\in M}$ familija regularnih izraza. Conwayevo meta-pravilo pridruženo monoidu M je sledeće: ako imamo

$$r_m r_n \leq r_{mn}$$

za sve $m, n \in M$, i

$$\left(\sum_{mu=m} r_u\right)^* = \sum_{mu=m} r_u$$

za sve $m \in M$, tada možemo izvesti

$$\left(\sum_{m\in M} r_m\right)^* = \sum_{m\in M} r_m.$$

Međutim, ovo meta-pravilo upotrebljavaćemo u slučaju da je M grupa. Tako, konačnoj grupi G se pridružuje kvazi-identitet

$$[(\forall g, h \in G)\ x_g x_h \leq x_{gh} \ \wedge\ x_1^* = x_1] \ \Rightarrow\ \left(\sum_{g\in G} x_g\right)^* = \sum_{g\in G} x_g.$$

Conwayev kvazi-identitet pridružen monoidu M (grupi G) je u ω-idempotentnim Conwayevim *-poluprstenima ekvivalentan monoidnom (grupnom) matričnom identitetu $P(M)$ ($P(G)$). Ovo tvrđenje se može naći bez dokaza još u Conwayevoj knjizi [40] (prvi njegov dokaz dao je Platieau [125]). U slučaju grupa, dajemo ga u nešto operativnijoj formi. Na taj način, dobijamo praktičan kriterijum kojim možemo proveriti kada ω-idempotentni Conwayev *-poluprsten zadovoljava $P(G)$ za datu konačnu grupu G.

PROPOZICIJA 2.2.3. (Platieau, [125], Krob [93]) *Neka je* $\mathbf{K}$ *ω-idempotentan Conwayev *-poluprsten, a G konačna grupa. Tada* $\mathbf{K}$ *zadovoljava $P(G)$ ako i samo ako za proizvoljnu familiju elementa $\{a_g \in K : g \in G\}$ koja zadovoljava uslove:*

(1) $a_g a_h \leq a_{gh}$ *za sve* $g, h \in G$,

(2) $a_1^* = a_1$,

važi $(\sum_{g\in G} a_g)^* = \sum_{g\in G} a_g$.

2.3. Kleenejeve algebre nemaju konačnu bazu identiteta

U ovom poglavlju dajemo dva dokaza da varijetet $\mathcal{KA}$ nema konačnu bazu identiteta. Prvi od njih je Conwayev dokaz iz [40], dok se drugi izvodi na osnovu eksplicitnog poznavanja baze za $\mathcal{KA}$ i još nekih Krobovih rezultata iz [93], a u vezi sa tzv. *Conwayevim modelima* koji će biti od velikog značaja za naša kasnija razmatranja.

Najpre, primetimo da se na osnovu aksioma poluprstena sa jedinicom (Propozicija 1.1.1) i prvog Conwayevog identiteta (Lema 1.1.6, *(1)*) svaki regularan izraz $\not\equiv 0$ može ekvivalentno zapisati kao zbir regularnih izraza od kojih je svaki ili $\equiv 1$, ili se u njemu od operacijskih simbola pojavljuju samo $\cdot, ^*$. Takve izraze ćemo zvati *kanonički regularni izrazi.* Dužina kanoničkog regularnog izraza se definiše kao broj sabiraka u njemu, a dužina regularnog identiteta u kome učestvuju kanonički izrazi je maksimum njihovih dužina.

Sada ćemo za sve proste brojeve p definisati algebru $\mathbf{A}_p$ tipa $\langle 2,2,1,0,0\rangle$ čiji su elementi svi podskupovi ciklične grupe $Z_p = \{1, a, \ldots, a^{p-1}\}$ zajedno sa simbolom ∞, a operacije redom $+, \cdot, ^*$ i konstante $\emptyset$ i $\{1\}$. Operacija $+$ funkcioniše na $\mathcal{P}(Z_p)$ kao unija, dok je za sve $B \subseteq Z_p$, $B < \infty$ (dakle, $B + \infty = \infty + B = \infty$). Operacija $\cdot$ je množenje kompleksa nad Z_p, pri čemu je $\emptyset \cdot \infty = \infty \cdot \emptyset = \emptyset$ i $B \cdot \infty = \infty \cdot B = \infty$ za sve $B \neq \emptyset$. Najzad, $\emptyset^* = \{1\}^* = \{1\}$, dok * primenjeno na sve druge elemente algebre $\mathbf{A}_p$ daje ∞.

LEMA 2.3.1. *Za sve proste brojeve p,* $\mathbf{A}_p$ *nije Kleenejeva algebra.*

Dokaz. Algebra $\mathbf{A}_p$ ne zadovoljava $P(Z_p)$, tj.

$$(1 + x + \ldots + x^{p-1})(x^p)^* = x^*,$$

ako se x interpretira npr. kao $\{a\}$, skup čiji je jedini element generator ciklične grupe Z_p. Naime, tada je vrednost leve strane $Z_p = \{1, a, \ldots, a^{p-1}\}$, dok vrednost desne strane iznosi ∞. Međutim, lako se pokazuje da gornji identitet važi na svakoj algebri jezika, pa tako i na $\mathcal{KA}$. ∎

LEMA 2.3.2. (Conway, [40]) *Svaki regularni identitet u kome učestvuju samo kanonički izrazi dužine manje od p važi na* $\mathbf{A}_p$.

Dokaz. Posmatrajmo minimalan kanonički regularan identitet

$$r(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$$

koji ne važi u $\mathbf{A}_p$ (npr. minimalan u smislu broja operacijskih simbola koji se u njemu pojavljuju). Tada je za neke $B_1, \ldots, B_n \in \mathcal{P}(Z_p) \cup \{\infty\}$,

$$r^{\mathbf{A}_p}(B_1, \ldots, B_n) \neq s^{\mathbf{A}_p}(B_1, \ldots, B_n).$$

Ako je za neko $1 \leq k \leq n$, $B_k \in \{\emptyset, \{1\}\}$, tada odgovarajuću promenljivu x_k možemo zameniti sa 0, odnosno 1 i tako dobiti prostiji kanonički identitet koji ne važi u $\mathbf{A}_p$, što je po pretpostavci nemoguće.

Posmatrajmo sada relaciju ekvivalencije θ na $\mathcal{P}(Z_p) \cup \{\infty\}$ čija jedna klasa sadrži Z_p i ∞, dok su preostale klase jednoelementne. Lako se proverava da je θ kongruencija algebre $\mathbf{A}_p$, i pri tome je $\mathbf{A}_p/\theta$ očito Kleenejeva algebra (po Lemi 1.3.1, budući da je $\mathbf{A}_p/\theta \cong \mathbf{M}(Z_p)$). Nije teško videti da stoga bez ograničenja opštosti možemo pretpostaviti da je

$$\begin{aligned} r^{\mathbf{A}_p}(B_1, \ldots, B_n) &= Z_p, \\ s^{\mathbf{A}_p}(B_1, \ldots, B_n) &= \infty. \end{aligned}$$

Takođe, jasno je da *iste* promenljive moraju biti pod dejstvom * u r i s (jer u slučaju da je npr. promenljiva x pod dejstvom zvezde u r, ali ne i u s, tada postoji n_s tako da za sve $w \in \mathsf{L}(s)$ imamo $|w|_x \leq n_s$, dok takvog ograničenja nema za reči iz $\mathsf{L}(r)$, pa bismo dobili $\mathsf{L}(r) \neq \mathsf{L}(s)$, kontradikcija sa pretpostavkom da je $r = s$ regularan identitet). Dalje, za svaku promenljivu x_i koja je pod dejstvom * u r i s mora biti $B_i = \{a^{\ell_i}\}$ za neko $1 \leq \ell_i \leq p - 1$, jer se u suprotnom lako pokazuje (induktivnim argumentom) da svaka "zvezda" koja sadrži B_i tako da je $|B_i| > 1$ mora biti jednaka ∞, pa tako i $r^{\mathbf{A}_p}(B_1, \ldots, B_n)$.

Zamenimo sve promenljive koje nisu pod dejstvom * u r, odnosno s, sa 1. Ukoliko ostale promenljive (one pod dejstvom *) interpretiramo, kao i ranije, odgovarajućim skupovima $B_i = \{a^{\ell_i}\}$, tada je jasno da dobijeni identitet takođe ne važi na $\mathbf{A}_p$, jer na levoj strani svi "zvezdirani" izrazi imaju vrednost $\{1\}$ (pa tako leva strana ne može imati vrednost ∞), dok zbog sličnih razloga vrednost desne strane ostaje ∞. Ponavljajući argument s početka dokaza, vrednost leve strane ovako modifikovanog identiteta mora biti Z_p. Ali, sada je vrednost svakog sabirka te leve strane (koja je i dalje kanonički izraz) jednoelementni skup, pa sabiraka mora biti bar p. Kontradikcija sa pretpostavkom da je polazni identitet $r = s$ dužine $< p$. ∎

TEOREMA 2.3.3. (Redko, [134], Conway, [40]) *Varijetet $\mathcal{KA}$ (odnosno, varijetet $\mathcal{L}$) nema konačnu bazu identiteta.*

Dokaz. Pretpostavimo da je Θ konačna baza identiteta za $\mathcal{KA}$. Tada se svaki od identiteta iz Θ može ekvivalentno predstaviti kao identitet u kome učestvuju samo kanonički izrazi. Neka je $m(\Theta)$ maksimum dužina tih (kanoničkih) identiteta. Tada uzmimo prost broj $p > m(\Theta)$. Po prethodnoj lemi, $\mathbf{A}_p$ zadovoljava sve identitete iz Θ, što znači da $\mathbf{A}_p \in \mathcal{KA}$. Kontradikcija sa Lemom 2.3.1. ∎

Kao što smo to ranije najavili, prikazaćemo još jedan dokaz gornje teoreme. On se zasniva na činjenici da aksiome ω-idempotentnih Conwayevih *-poluprstena i grupni matrični identiteti (sa eventualnim redukcijama) čine bazu identiteta za Kleenejeve algebre. Zapravo, pokazaćemo da za ove identitete važi izvesna nezavisnost. Kako bismo to učinili, uvodimo još jednu klasu algebri tipa $\langle 2,2,1,0,0\rangle$.

Neka je G grupa i $\mathcal{F}$ familija nekih njenih podgrupa (u koje uračunavamo i $\emptyset$) koja sadrži $\emptyset$ i trivijalnu podgrupu $\{1\}$. Neka G^0 označava 0-grupu, dobijenu pridruživanjem nule grupi G. Sada definišemo *Conwayev model* pridružen grupi G i familiji $\mathcal{F}$ kao

$$\mathbf{C}_{\mathcal{F}}(G) = \langle \mathcal{P}(G^0), \cup, \cdot, ^*, \emptyset, \{1\}\rangle,$$

gde $\cdot$ označava množenje kompleksa nad G^0, dok je * definisano za sve $A \subseteq G \cup \{0\}$ sa ($\langle A\rangle$ označava podmonoid od G^0 generisan sa A):

$$A^* = \begin{cases} \langle A\rangle, & \langle A\rangle \in \mathcal{F}, \\ \langle A\rangle \cup \{0\}, & \text{inače.} \end{cases}$$

Pri tome je, po dogovoru, $\langle\emptyset\rangle = \{1\}$. Dakle, A^* je uvek podgrupa od G ili unija podgrupe od G sa 0. Lako se vidi da je $\mathbf{C}_{\mathcal{F}}(G)$ uvek ω-idempotentan *-poluprsten. Postavlja se pitanje kada on zadovoljava Conwayeve identitete, kao i grupne matrične identitete.

PROPOZICIJA 2.3.4. (Krob, [93, Propozicija 16.3]) *Neka je G konačna grupa. Na $\mathbf{C}_{\mathcal{F}}(G)$ važi identitet $(x+y)^* = (x^*y)^*x^*$ ako i samo ako za sve $H \in \mathcal{F}$ iz $A \leq H$ sledi $A \in \mathcal{F}$, tj. ako je familija $\mathcal{F}$ zatvorena na podgrupe.*

Dokaz. Najpre, pretpostavimo da je familija $\mathcal{F}$ zatvorena na formiranje podgrupa. Ako je neki od elemenata A, B Conwayevog modela $\mathbf{C}_{\mathcal{F}}(G)$ prazan ili sadrži 0, tada se lako proverava da je

$$(A \cup B)^* = (A^*B)^*A^*.$$

Zato pretpostavimo da A, B nisu prazni i ne sadrže 0. Jasno, tada je $\langle\langle A\rangle B\rangle \subseteq \langle A \cup B\rangle$. S druge strane, također je očito da važi $B \subseteq \langle\langle A\rangle B\rangle$. Međutim, kako je G konačna grupa, za sve $b \in B$ imamo da $b^{-1} \in \langle B\rangle$, pa je zato za proizvoljno $a \in A$,

$$a = abb^{-1} \in \langle\langle A\rangle B\rangle,$$

što znači da $A \subseteq \langle\langle A\rangle B\rangle$. Dobili smo da je $\langle A \cup B\rangle \subseteq \langle\langle A\rangle B\rangle$, odakle je $\langle A \cup B\rangle = \langle\langle A\rangle B\rangle$.

Sada pretpostavimo da $\langle A \cup B\rangle \in \mathcal{F}$, odakle je $\langle\langle A\rangle B\rangle \in \mathcal{F}$ i, po zatvorenosti $\mathcal{F}$ na podgrupe, $\langle A\rangle \in \mathcal{F}$. Stoga je $A^* = \langle A\rangle$ i $(A^*B)^* = \langle\langle A\rangle B\rangle$, pa sledi

$$(A \cup B)^* = \langle A \cup B\rangle = \langle\langle A\rangle B\rangle\langle A\rangle = (A^*B)^*A^*.$$

Međutim, u slučaju da $\langle A \cup B\rangle \notin \mathcal{F}$, imamo $\langle\langle A\rangle B\rangle \notin \mathcal{F}$, zbog čega je

$$(A \cup B)^* = \langle A \cup B\rangle \cup \{0\} = (\langle\langle A\rangle B\rangle \cup \{0\})\langle A\rangle = (A^*B)^*A^*.$$

Obratno, neka na $\mathbf{C}_{\mathcal{F}}(G)$ važi $(x + y)^* = (x^*y)^*x^*$, ali da pri tome familija $\mathcal{F}$ nije zatvorena na podgrupe. Tada postoji $H \in \mathcal{F}$ tako da za neku podgrupu $A \leq H$, $A \notin \mathcal{F}$. Ali, tada je

$$\begin{aligned}(A \cup H)^* = H^* = \langle H\rangle \neq \langle H\rangle \cup \{0\} &= [\langle(\langle A\rangle \cup \{0\})H\rangle \cup \{0\}](\langle A\rangle \cup \{0\}) \\ &= (A^*H)^*A^*.\end{aligned}$$

Kontradikcija. ∎

PROPOZICIJA 2.3.5. (Krob, [93, Propozicija 16.4]) *Neka je G konačna grupa. Na $\mathbf{C}_{\mathcal{F}}(G)$ važi identitet $(xy)^* = 1 + x(yx)^*y$ ako i samo ako je za sve $H \in \mathcal{F}$ i $g \in G$, $g^{-1}Hg \in \mathcal{F}$, tj. ako je familija $\mathcal{F}$ zatvorena na konjugaciju.*

Dokaz. Pođimo prvo od pretpostavke da je familija $\mathcal{F}$ zatvorena na konjugaciju. Ponovo, ako je neki od elementat A, B Conwayevog modela $\mathbf{C}_{\mathcal{F}}(G)$ prazan ili sadrži 0, tada se lako proverava jednakost

$$(AB)^* = \{1\} \cup A(BA)^*B.$$

U suprotnom, za proizvoljne $a, c \in A$, $b \in B$ imamo

$$c^{-1}(ab)c = (bc)^{-1}(ba)(bc) \in \langle BA\rangle,$$

zbog pretpostavke da je G konačna grupa. Sledi da je za sve $c \in A$, $c^{-1}ABc \subseteq \langle BA\rangle$, odakle je

$$c^{-1}\langle AB\rangle c = \langle c^{-1}ABc\rangle \subseteq \langle BA\rangle.$$

Analogno se može pokazati da za proizvoljno $c \in A$ važi $c\langle BA\rangle c^{-1} \subseteq \langle AB\rangle$, pa dobijamo da je $\langle BA\rangle = c^{-1}\langle AB\rangle c$ za sve $c \in A$.

Zbog toga, ako je $\langle AB\rangle \in \mathcal{F}$, tada je po gornjoj relaciji i pretpostavkama propozicije $\langle BA\rangle \in \mathcal{F}$. Sledi

$$(AB)^* = \langle AB\rangle = \{1\} \cup A\langle BA\rangle B = \{1\} \cup A(BA)^*B.$$

S druge strane, ukoliko $\langle AB\rangle \notin \mathcal{F}$, tada $\langle BA\rangle \notin \mathcal{F}$, pa se u tom slučaju dobija

$$(AB)^* = \langle AB\rangle \cup \{0\} = \{1\} \cup A(\langle BA\rangle \cup \{0\})B = \{1\} \cup A(BA)^*B.$$

Obratno, pretpostavimo da $\mathbf{C}_{\mathcal{F}}(G)$ zadovoljava identitet $(xy)^* = 1 + x(yx)^*y$, ali da familija $\mathcal{F}$ nije zatvorena na konjugaciju. Tako, postoji $H \in \mathcal{F}$ tako da za neko $g \in G$, $g^{-1}Hg \notin \mathcal{F}$. Tada uzmimo $A = \{g^{-1}\}$, $B = Hg$. Dobijamo:

$$\begin{aligned} (AB)^* &= (g^{-1}Hg)^* = g^{-1}Hg \cup \{0\}, \\ \{1\} \cup A(BA)^*B &= \{1\} \cup g^{-1}H^*Hg = g^{-1}Hg, \end{aligned}$$

kontradikcija. ∎

Ukoliko je $\mathcal{F}$ familija svih pravih podgrupa date grupe G (dakle, podgrupa $\neq G$), tada Conwayev model kraće pišemo $\mathbf{C}(G)$. Za ovakve specijalne modele (koji će nam biti potrebni u dokazu da $\mathcal{KA}$ nema konačnu bazu) važi sledeći kriterijum koji određuje kada takvi modeli zadovoljavaju neki grupni matrični identitet. Propoziciju ostavljamo bez dokaza, ali on se, uz nešto više tehničkih detalja, pretežno oslanja na Propoziciju 2.2.3.

Propozicija 2.3.6. (Krob, [93, Propozicija 16.6]) *Neka je G konačna prosta grupa. Conwayev model $\mathbf{C}(G)$ zadovoljava matrični identitet $P(H)$ ako i samo ako grupa G ne deli grupu H.*

Sada ponavljamo tvrđenje Teoreme 2.3.3, ali dajemo dokaz koji se zasniva na Krobovim idejama.

Teorema 2.3.7. *Varijetet $\mathcal{KA}$ nema konačnu bazu identiteta.*

Dokaz. Pretpostavimo da je Θ konačna baza identiteta za $\mathcal{KA}$. Tada je svaki od identiteta iz Θ logička posledica konačnog skupa identiteta iz neke unapred zadate baze za $\mathcal{KA}$. Mi ćemo posmatrati bazu koja se sastoji od aksioma ω-idempotentnih Conwayevih *-poluprstena i matričnih identiteta $P(A_n)$, $n \geq 5$, gde A_n označava alternativnu grupu permutacija stepena n. Po

gornjem zaključku sledi da ova baza ima konačnu podbazu, i bez ograničenja opštosti možemo uzeti da su to identiteti ω-idempotentnih Conwayevih *-poluprstena zajedno sa $P(A_n)$, $5 \leq n \leq n_0$ za neko $n_0 \geq 5$.

Posmatrajmo sada Conwayev model $\mathbf{C}(A_{n_0+1})$. Po Propozicijama 2.3.4 i 2.3.5, on zadovoljava oba Conwayeva identiteta. Dalje, on po Propoziciji 2.3.6 zadovoljava i sve identitete $P(A_n)$, $5 \leq n \leq n_0$, pošto je A_k prosta grupa za sve $k \geq 5$, a A_{n_0+1} ne deli A_n zbog $|A_n| < |A_{n_0+1}|$. Zaključujemo da je $\mathbf{C}(A_{n_0+1})$ Kleenejeva algebra, što je netačno jer, takođe po Propoziciji 2.3.6, $\mathbf{C}(A_{n_0+1})$ očito ne zadovoljava identitet $P(A_{n_0+1})$, koji, međutim, važi na svim Kleenejevim algebrama. ∎

Na kraju ove glave pomenimo da je Pratt [132] našao konačno baziranu jednakosnu teoriju $\mathcal{ACT}$ na jeziku koji proširuje tip Kleenejevih algebri, takvu da je njen "regularan deo", tj. skup identiteta koji sadrže samo operacijske simbole $+, \cdot, ^*, 0, 1$, *tačno* $Eq(\mathcal{KA})$ (kažemo da jednakosna teorija $\mathcal{ACT}$ *konzervativno proširuje* jednakosnu teoriju Kleenejevih algebri). Reč je o tzv. *akcionoj jednakosnoj logici* čiji su modeli *akcione algebre*. Jasno, njihovi odgovarajući redukti su Kleenejeve algebre, i pri tome se uvek dobijaju *-*neprekidne* Kleenejeve algebre, tako da * uvek predstavlja refleksivno-tranzitivno zatvorenje. Osim toga, svaka konačna algebra iz Kozenovog kvazivarijeteta $\mathcal{Q}_2$ se može proširiti do akcione algebre.

Dodati binarni simboli su $\rightarrow$ i $\leftarrow$ i oni u akcionim algebrama relacija predstavljaju operacije desne i leve reziduacije. Tačnije, imamo sledeći uslov:

$$a \leq (c \leftarrow b) \;\Leftrightarrow\; ab \leq c \;\Leftrightarrow\; b \leq (a \rightarrow c).$$

U akcionim algebrama uopšte, ove operacije se redom nazivaju *preimplikacija* i *postimplikacija*.

Aksiome za $\mathcal{ACT}$ su identiteti idempotentnih poluprstena sa jedinicom i ($x \leq y$ je zamena za $x + y = y$):

$$\begin{aligned}
xy &\leq (x+z)(y+u),\\
(x \rightarrow y) &\leq (x \rightarrow (y+z)),\\
(y \leftarrow x) &\leq ((y+z) \leftarrow x),\\
x(x \rightarrow y) \leq\ & y \leq (x \rightarrow xy),\\
(y \rightarrow x)x \leq\ & y \leq (yx \rightarrow x),\\
1 + x^*x^* + x &\leq x^*,\\
x^* &\leq (x+y)^*,\\
(x \rightarrow x)^* &= x \rightarrow x.
\end{aligned}$$

Pratt ističe naročit značaj poslednjeg identiteta, kojeg zove *aksioma čiste indukcije*. Ona je ključna u tome da obezbedi da Kleenejevi redukti akcionih algebri budu *-neprekidni i da tako a^* uvek predstavlja infimum skupa $\{a^n : n \geq 0\}$ (u definiciji tog infimuma je zaista "skrivena" indukcija). Možemo reći da je pojam matematičke indukcije u neku ruku dotaknut operacijama $\rightarrow$ i $\leftarrow$ i njihovim osobinama. Specijalno, to znači da se npr. Conwayev skok $\mathbf{C}_4$ ne može proširiti do akcione algebre. Na taj način, po cenu izlaska u širi algebarski jezik je ipak moguća konačna jednakosna aksiomatizacija regularnih identiteta.

Glava 3 MULTIPLIKATIVNE KLEENEJEVE ALGEBRE

U prethodnoj glavi smo videli da Kleenejeve algebre nemaju konačnu bazu identiteta. Ako uđemo u detaljniju analizu tog tvrđenja, postavlja se pitanje koje su od operacija $\cup, \circ, {}^{\mathrm{rtc}}$ sa relacijama (odnosno $+, \cdot, {}^*$ sa jezicima) "odogvorne" za takav negativan rezultat, tj. da li se mogu izdvojiti neke dve od njih čija interakcija forsira beskonačnost baze, ili je ona posledica međudejstva sve tri operacija zajedno.

Nije teško dokazati da se svi regularni identiteti koji sadrže samo $+, \cdot$ (eventualno sa konstantnim simbolima $0, 1$) mogu aksiomatizovati identitetima idempotentnih poluprstena (pa su stoga konačno bazirani). Takođe, može se pokazati da se identiteti koji sadrže $+, {}^*, 0, 1$ mogu dobiti iz identiteta za $+, 0$ koji opisuju polumreže sa nulom, zatim $0^* = 1$, i

$$\begin{aligned} x + x^* &= x^*, \\ x^* + (x + y)^* &= (x + y)^*, \\ (x + y^*)^* &= (x + y)^*. \end{aligned}$$

Prema tome, preostaje da se istraži šta se dešava kada kombinujemo $\cdot$ i * (sa ili bez prisustva $0, 1$). Upravo je to sadržaj problema kojeg je 1993. postavio D. A. Bredikhin. Preciznije, on pita da li varijetet generisan algebrama binarnih relacija

$$\langle \mathcal{P}(A \times A), \circ, {}^{\mathrm{rtc}} \rangle$$

(koje su, eventualno, proširene konstantama $\emptyset, \Delta_A$) ima konačnu jednakosnu bazu. Primetimo da je reč o "multiplikativnim reduktima" punih Kleenejevih relacionih algebri.

U radu [43], S. Crvenković, Z. Ésik i autor disertacije su dali *negativan* odgovor na ovo pitanje. Na taj način, uzroci beskonačne jednakosne aksiomatizacije Kleenejevih algebri leže u superpoziciji kompozicije relacija i refleksivno-tranzitivnog zatvorenja (odnosno, konkatenacije i Kleenejeve iteracije jezika).

U ovoj glavi prikazujemo kompletan dokaz tog rezultata. Ali, najpre ćemo uvesti osnovni pojmovni aparat i razmotriti neka pitanja u vezi sa regularnim jezicima koji su predstavljivi regularnim izrazima u kojima ne učestvuje $+$.

3.1. Osnovne definicije i pojmovi

Za proizvoljan skup A definišemo algebru

$$\mathbf{UFRel}(A) = \langle \mathcal{P}(A \times A), \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A \rangle,$$

koju zovemo *puna multiplikativna Kleenejeva relaciona algebra.* Varijetet generisan ovim algebrama označavamo sa $\mathcal{UF}$, a njegovi članovi su *multiplikativne Kleenejeve algebre.*

Lako se vidi da je $\cup$-slobodni redukt Kleenejeve algebre $\mathbf{M}(S)$ kompleksa monoida S^1 (vidi Lemu 1.3.1) multiplikativna Kleenejeva algebra. Specijalno, ako je $S = \Sigma^*$ slobodan monoid, dobijamo redukt algebre jezika bez $+$,

$$\mathbf{UFLang}(\Sigma) = \langle \mathcal{P}(\Sigma^*), \cdot, ^*, \emptyset, \{\lambda\} \rangle.$$

Podalgebru od $\mathbf{UFLang}(\Sigma)$ generisanu jezicima $\{a\}$, $a \in \Sigma$, označavamo sa $\mathbf{UFReg}(\Sigma)$. Elementi ove podalgebre su *multiplikativni regularni jezici.* Očito, regularni jezik je multiplikativan ako i samo ako se može predstaviti regularnim izrazom u kojem ne figuriše $+$. Ova primedba obrazlaže naredno tvrđenje.

PROPOZICIJA 3.1.1. *$Eq(\mathcal{UF})$ se poklapa sa skupom identiteta iz $Eq(\mathcal{KA})$ koji ne sadrže $+$.*

Takođe, adaptacijom dokaza Kozen-Németijeve teoreme dobija se

PROPOZICIJA 3.1.2. $\mathbf{UFReg}(\Sigma)$ *je $\mathcal{UF}$-slobodna algebra nad Σ, slobodno generisana preslikavanjem $a \mapsto \{a\}$, $a \in \Sigma$.*

Naravno, prirodno se postavlja sledeće pitanje.

PROBLEM 3. *Da li postoji algoritam koji odlučuje da li je dati regularni jezik (određen nekim regularnim izrazom koji ga predstavlja) multiplikativan, tj. da li je skup svih multiplikativnih regularnih jezika (nad nekom datom azbukom Σ) rekurzivan?*

Drugim rečima, traži se (ako postoji) efektivna karakterizacija multiplikativnih regularnih jezika. Zaista se lako pokazuje da klasa svih multiplikativnih regularnih jezika nije $*$-varijetet jezika. Tako, nije moguće rešenje gornjeg problema u duhu Eilenbergove teoreme o varijetetima, tj. sintaktički monoidi koji odgovaraju multiplikativnim regularnim jezicima ne formiraju pseudovarijetet.

U preostalom delu ovog poglavlja ćemo napraviti jednu malu digresiju: naime, daćemo karakterizaciju multiplikativnih regularnih jezika u slučaju jednoelementne azbuke, $\Sigma = \{a\}$. Najpre nam treba jedna lema vezana za teoriju brojeva. Sa ω označavamo skup prirodnih brojeva (koji uključuje 0). Primetimo da je algebra

$$\Omega = \langle \omega, +, 0 \rangle$$

monoid.

LEMA 3.1.3. *Svaki podmonoid monoida Ω je konačno generisan.*

Dokaz. Neka je M podmonoid od Ω i neka je d najveći zajednički deljitelj svih elemenata od M. Jasno, tada postoje $m_1, \ldots, m_\ell \in M$ tako da je

$$(m_1, \ldots, m_\ell) = d.$$

Poznato je iz teorije brojeva da postoji prirodan broj k_0 tako da za sve $k \geq k_0$ jednačina

$$m_1 y_1 + \ldots + m_\ell y_\ell = dk$$

ima *pozitivno* celobrojno rešenje. Sledi da je M kofinitan podskup skupa

$$d\omega = \{dn : \ n \in \omega\}.$$

Sada konstruišemo brojeve $n_1, n_2, \ldots$ na sledeći način. Najpre, n_1 je najmanji nenula element iz M. Zatim, n_2 je najmanji nenula element iz M koji ne pripada podmonoidu $\langle n_1 \rangle$. U k-tom koraku odabiramo najmanji nenula element n_k iz M koji ne pripada podmonoidu $\langle d_{k-1} \rangle$, pri čemu je

$$d_i = (n_1, \ldots, n_i).$$

Po konstrukciji, ako je $d_{k-1} > d$, tada imamo da

$$d_{k-1} = (n_1, \ldots, n_{k-1}) \not| \ n_k,$$

pa mora biti $d_k < d_{k-1}$. Stoga je $d_{\ell_0} = d$ za neko ℓ_0.

Međutim, sada je skup

$$M' = \{n_1 x_1 + \ldots + n_{\ell_0} x_{\ell_0} : \ x_1, \ldots, x_{\ell_0} \in \omega\} \subseteq M$$

kofinitni podskup od $d\omega$, pa je $M \setminus M'$ konačan skup. Kako važi

$$M = M' \cup (M \setminus M'),$$

sledi da je podmonoid M generisan sa $\{n_1, \ldots, n_{\ell_0}\} \cup (M \setminus M')$. Dakle, M ima konačan skup generatora, što je i trebalo dokazati. ∎

Teorema 3.1.4. *Svaki multiplikativni regularni jezik $L \neq \emptyset$ nad azbukom $\Sigma = \{a\}$ se može predstaviti regularnim izrazom oblika*

$$a^m (a^{n_1})^* \ldots (a^{n_k})^*.$$

Drugim rečima, multiplikativni regularni podskupovi monoida Ω su prazan skup i translacije njegovih (konačno generisanih) podmonoida.

Dokaz. Tvrđenje je jasno za jednoelementne jezike. Sada teoremu dokazujemo indukcijom po složenosti multiplikativnog regularnog izraza r koji predstavlja L. Ako je $r = st$, pri čemu su s i t redom ekvivalentni izrazima $a^k(a^{\ell_1})^* \ldots (a^{\ell_b})^*$ i $a^p(a^{q_1})^* \ldots (a^{q_c})^*$, tada je (zbog komutativnosti jezika nad jednoelementnom azbukom u odnosu na konkatenaciju) r ekvivalentno sa

$$a^{k+p}(a^{\ell_1})^* \ldots (a^{\ell_b})^* (a^{q_1})^* \ldots (a^{q_c})^*.$$

U slučaju da je $r = s^*$, neka je

$$M = \{n : \ a^n \in L\}.$$

Tada je $0 \in M$ i važi $M^2 = M$, što znači da je M podmonoid od Ω. Po Lemi 3.1.3, važi

$$M = \langle n_1, \ldots, n_h \rangle$$

za neke $n_1, \ldots, n_h \geq 1$, odakle sledi da je L predstavljen regularnim izrazom $(a^{n_1})^* \ldots (a^{n_h})^*$. ∎

Precizirajući poslednji slučaj u induktivnom koraku u prethodnom dokazu, imamo da je za sve $m, n_1, \ldots, n_k \geq 0$,

$$(a^m (a^{n_1})^* \ldots (a^{n_k})^*)^* = \prod_{0 \leq \alpha_1, \ldots, \alpha_k < m} (a^{m + n_1\alpha_1 + \ldots + n_k\alpha_k})^*.$$

3.2. Uopšteni Conwayevi modeli

Conwayeve modele smo definisali u prethodnoj glavi. Njihova glavna ideja bila je da se, prilikom izračunavanja operacije * za neke komplekse posmatrane (konačne) grupe, podgrupa generisana tim kompleksom proširi dodatim nultim elementom. Time postižemo to da strukturne osobine konačnih grupa utiču na identitete koje takvi modeli zadovoljavaju. Međutim, ispostavlja se da Conwayevi modeli nisu dovoljno "jaki" da bi se njima dokazalo da $\mathcal{UF}$ (odnosno, skup multiplikativnih regularnih identiteta) nema konačnu bazu. Stoga ćemo u ovom poglavlju razmotriti jednu generalizaciju Conwayevih modela, sa nadom da će nam oni omogućiti finiju analizu regularnih identiteta.

Podsećajući se definicije Conwayevih modela, primetimo da smo, umesto familije podgrupa $\mathcal{F}$ date grupe G koja sadrži sve podgrupe od G kojima se prilikom izračunavanja "zvezde" *ne* pridružuje nulti element 0, mogli da definišemo preslikavanje T koje *svakoj* podgrupi H od G (uračunavajući tu i $\emptyset$) dodeljuje T_H koje je ili $\emptyset$, ili $\{0\}$, pri čemu smo se dogovorili da mora biti $T_\emptyset = T_{\{1\}} = \emptyset$ (kako bi bila ispunjena ω-idempotentnost). Sada se "zvezda" jednostavno definiše kao

$$A^* = \langle\!\langle A \rangle\!\rangle \cup T_{\langle\!\langle A \rangle\!\rangle},$$

u slučaju $A \subseteq G$, gde $\langle\!\langle A \rangle\!\rangle$ označava podgrupu od G generisanu sa A, dok je inače $A^* = \langle A \rangle$ (jer je tada $0 \in A$), gde će u ostatku ove glave $\langle \cdot \rangle$ označavati generisanje potpolugrupe. Ovakav pristup Conwayevim modelima omogućava njihovo uopštavanje.

Neka je G grupa, a S polugrupa (pri čemu pretpostavljamo da je $G \cap S = \emptyset$). Neka je G^S polugrupa definsana na skupu $G \cup S$ tako da za sve $g \in G$ i $s \in S$ važi $gs = sg = s$, dok su operacije na G, odnosno S, indukovane iz izvornih struktura. Primetimo da je reč o veoma specijalnom tipu idealskog proširenja polugrupe S 0-grupom G^0, pošto je S očito ideal u G, dok je faktor G^S/S izomorfan sa G^0. Neka je svakoj podgrupi H grupe G pridružena ili potpolugrupa T_H polugrupe S, ili $\emptyset$ (drugim rečima, imamo preslikavanje T iz familije svih podgrupa od G u familiju svih potpolugrupa od S koje uključuju i $\emptyset$). Tada definišemo *uopšteni Conwayev model*

$$\mathrm{M}_T(G,S) = \langle \mathcal{P}(G^S), \cup, \cdot, ^*, \emptyset, \{1\} \rangle,$$

gde je $A \cdot B$ proizvod kompleksa $A, B \subseteq G^S$, 1 jedinica grupe G, dok ćemo * definisati u dva koraka. Najpre, ako je $A \subseteq G$, tada je

$$A^* = \langle\!\langle A \rangle\!\rangle \cup T_{\langle\!\langle A \rangle\!\rangle}.$$

Primetimo da je $\langle A\rangle = \langle\langle A\rangle\rangle$, ukoliko je $A \neq \emptyset$. Međutim, $\langle\emptyset\rangle = \emptyset$, dok je $\langle\langle\emptyset\rangle\rangle = \{1\}$. Najzad, za proizvoljno $A \subseteq G^S$ definišemo

$$A^* = \langle (A \cap S) \cup (A \cap G)^* \rangle.$$

Radi lakšeg zapisa, uvodimo notaciju

$$\begin{aligned} \Gamma(A) &= A \cap G, \\ \Sigma(A) &= A \cap S. \end{aligned}$$

Skupove $\Gamma(A)$ i $\Sigma(A)$ zovemo redom *grupni*, odnosno *polugrupni deo od* A.

Sledeće tvrđenje se odmah dobija direktnom primenom gornjih definicija.

LEMA 3.2.1. *Neka je* $\mathbf{M}_T(G,S)$ *uopšteni Conwayev model i* A, B *njegova proizvoljna dva elementa. Tada važe jednakosti:*

$$\Gamma(A \cup B) = \Gamma(A) \cup \Gamma(B), \tag{7}$$

$$\Gamma(AB) = \Gamma(A)\Gamma(B), \tag{8}$$

$$\Gamma(A^*) = \langle\langle\Gamma(A)\rangle\rangle, \tag{9}$$

$$\Sigma(A \cup B) = \Sigma(A) \cup \Sigma(B), \tag{10}$$

$$\Sigma(AB) = \Sigma(A)B \cup A\Sigma(B), \tag{11}$$

$$\Sigma(A^*) = \langle \Sigma(A) \cup \Sigma(\Gamma(A)^*)\rangle. \tag{12}$$

Primetimo da se jednakost (11) može zapisati u različitim oblicima, u zavisnosti od toga da li su grupni delovi skupova A, odnosno B, prazni ili ne. Na primer, ako su $\Gamma(A)$ i $\Gamma(B)$ neprazni, tada je

$$\Sigma(AB) = \Sigma(A)\Sigma(B) \cup \Sigma(A) \cup \Sigma(B).$$

S druge strane, ako je $\Gamma(A) = \Gamma(B) = \emptyset$, tada imamo $\Sigma(AB) = \Sigma(A)\Sigma(B)$.

Sa uopštenih Conwayevih modela se lako može preći na obične Conwayeve modele putem količnika u odnosu na određene kongruencije. Tačnije, neka je θ_S kongruencija na $\mathbf{M}_T(G,S)$ generisana parovima

$$\{\langle\{s_1\},\{s_2\}\rangle : \ s_1, s_2 \in S\},$$

tj. najmanja kongruencija u kojoj su svi jednoelementni skupovi $\{s\}$, $s \in S$, sadržani u jednoj klasi. Primetimo da par elemenata $A, B \subseteq G^S$ pripada θ_S ako i samo ako $\Gamma(A) = \Gamma(B)$ i pri tome je ili $\Sigma(A) = \Sigma(B) = \emptyset$, ili $\Sigma(A)\Sigma(B) \neq \emptyset$.

LEMA 3.2.2. *Neka je* $\mathbf{M}_T(G,S)$ *uopšteni Conwayev model i*

$$\mathcal{F} = \{H \leq G : \ T_H = \emptyset\}.$$

Tada je $\mathbf{M}_T(G,S)/\theta_S \cong \mathbf{C}_{\mathcal{F}}(G)$.

Gornje očigledno tvrđenje zapravo "deli" postupak provere identiteta na uopštenom Conwayevom modelu na dve faze, kao što je to pokazano u narednoj propoziciji. Međutim, postupak provere je time znatno uprošćen.

PROPOZICIJA 3.2.3. *Neka su* $p = p(x_1,\ldots,x_n)$ *i* $q = q(x_1,\ldots,x_n)$ *dva regularna izraza. Tada model* $\mathbf{M}_T(G,S)$ *zadovoljava identitet* $p = q$ *ako i samo ako* $\mathbf{C}_{\mathcal{F}}(G)$ *zadovoljava identitet* $p = q$*, gde je* $\mathcal{F}$ *definisano u prethodnoj lemi, i za sve* $A_1,\ldots,A_n \subseteq G^S$ *imamo*

$$\Sigma(p(A_1,\ldots,A_n)) = \Sigma(q(A_1,\ldots,A_n)).$$

Dokaz. Ako $p = q$ važi na $\mathbf{M}_T(G,S)$, tada je taj identitet tačan i na količniku $\mathbf{C}_{\mathcal{F}}(G)$, dok je drugi uslov takođe očigledan. Obratno, pretpostavimo da identitet $p = q$ ne važi na $\mathbf{M}_T(G,S)$. Tada je

$$p(A_1,\ldots,A_n) \neq q(A_1,\ldots,A_n)$$

za neke $A_1,\ldots,A_n \subseteq G^S$. Ali, ako $\mathbf{C}_{\mathcal{F}}(G)$ zadovoljava $p = q$, sledi da je

$$\Gamma(p(A_1,\ldots,A_n)) = \Gamma(q(A_1,\ldots,A_n)),$$

jer $\langle A,B\rangle \in \theta_S$ jasno povlači $\Gamma(A) = \Gamma(B)$. U tom slučaju, mora biti

$$\Sigma(p(A_1,\ldots,A_n)) \neq \Sigma(q(A_1,\ldots,A_n)).$$

Kontradikcija, pa je tvrđenje dokazano. ∎

Odmah se vidi da je uopšteni Conwayev model ω-idempotentan ako i samo ako je $T_{\{1\}} = \emptyset$. Sada je naš cilj da nađemo uslove pod kojima on zadovoljava dva Conwayeva identiteta. Jasno, po gornjoj propoziciji, to će se dogoditi samo ako leve i desne strane imaju iste polugrupne delove.

Za uopšteni Conwayev model $\mathbf{M}_T(G,S)$ kažemo da je **-monoton* ako za sve podgrupe $H, K \leq G$, $H \leq K$ povlači $T_H \leq T_K$.

PROPOZICIJA 3.2.4. *Neka su* A, B *elementi* ω*-idempotentnog* **-monotonog uopštenog Conwayevog modela* $\mathbf{M}_T(G,S)$*, gde je* G *konačna grupa, a* S *konačna polugrupa. Tada je*

$$\Sigma((A \cup B)^*) = \Sigma((A^*B)^*A^*).$$

Dokaz. Najpre, po Lemi 3.2.1 imamo

$$\Sigma((A \cup B)^*) = \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle,$$

kao i

$$\Sigma((A^*B)^*A^*) = \Sigma((A^*B)^*)\Sigma(A^*) \cup \Sigma((A^*B)^*) \cup \Sigma(A^*),$$

budući da su grupni delovi "zvezdiranih" skupova neprazni. Nastavljajući gornja izračunavanja, dobijamo

$$\Sigma((A^*B)^*) = \langle \Sigma(A^*B) \cup \Sigma((\Gamma(A^*B))^*) \rangle,$$

gde je

$$\Sigma(A^*B) = \Sigma(A^*)B \cup A^*\Sigma(B) =$$
$$= \Sigma(A^*)B \cup \Sigma(B) \cup \Sigma(A^*)\Sigma(B) = \Sigma(A^*)B \cup \Sigma(B),$$

i $\Sigma(A^*)$ je dato sa (12).

Sada posmatramo dva slučaja.

Prvo, neka je $\Gamma(B) = \emptyset$ i označimo $P = \Sigma(A) \cup \Sigma(\Gamma(A)^*)$ i $Q = \Sigma(B)$, tako da je $\Sigma(A^*) = \langle P \rangle$. Po gornjim relacijama, sledi

$$\Sigma((A \cup B)^*) = \langle P \cup Q \rangle,$$

što je ništa drugo nego vrednost regularnog izraza $(p + q)^+$ u algebri $\mathbf{M}(S)$ (vidi Lemu 1.3.1) u odnosu na interpretaciju $p \mapsto P$, $q \mapsto Q$. S druge strane, imamo (pošto je $B = \Sigma(B)$, $\Gamma(A^*B) = \emptyset$ i $T_{\{1\}} = \emptyset$):

$$\begin{aligned} \Sigma(A^*B) &= \langle P \rangle Q \cup Q \\ \Sigma((A^*B)^*) &= \langle \langle P \rangle Q \cup Q \rangle \end{aligned}$$

i

$$\Sigma((A^*B)^*A^*) = \langle \langle P \rangle Q \cup Q \rangle \langle P \rangle \cup \langle \langle P \rangle Q \cup Q \rangle \cup \langle P \rangle.$$

Desna strana gornje jednakosti je vrednost terma $(p^+q+q)^+p^+ + (p^+q+q)^+ + p^+$ u $\mathbf{M}(S)$ za istu interpretaciju promenljivih kao i malopre. Ali, jasno je da ova dva izraza predstavljaju isti regularni jezik (prvi član drugog izraza predstavlja sve reči koje se završavaju sa p i sadrže bar jedno q, drugi član predstavlja sve reči koje se završavaju sa q, dok treći član predstavlja reči bez q). Zato $\mathbf{M}(S)$ zadovoljava identitet kojeg čine gornja dva regularna izraza, pa je propozicija dokazana u ovom slučaju.

Sada pretpostavimo da je $\Gamma(B) \neq \emptyset$. Prvo, imamo $\Sigma(A) \subseteq \Sigma(A^*)$, i kako u ovom slučaju važi $\Sigma(A^*B) = \Sigma(A^*)\Sigma(B) \cup \Sigma(A^*) \cup \Sigma(B)$, sledi

$$\Sigma(A) \subseteq \Sigma(A^*B).$$

Dalje, primetimo da je

$$\Gamma((A^*B)^*) = \langle\!\langle \Gamma(A^*B) \rangle\!\rangle = \langle\!\langle \Gamma(A^*)\Gamma(B) \rangle\!\rangle = \langle\!\langle \langle\!\langle \Gamma(A) \rangle\!\rangle \Gamma(B) \rangle\!\rangle,$$

gde se za desnu stranu lako vidi da je jednaka $\langle\!\langle \Gamma(A) \cup \Gamma(B) \rangle\!\rangle$ (vidi Propoziciju 2.3.4). Znači, važi

$$\Sigma(\Gamma(A^*B)^*) = T_{\langle\!\langle \Gamma(A^*B) \rangle\!\rangle} = T_{\langle\!\langle \Gamma(A) \cup \Gamma(B) \rangle\!\rangle} = \Sigma([\Gamma(A) \cup \Gamma(B)]^*).$$

Kako je, po pretpostavci, u posmatranom modelu zvezda monotona, sledi

$$\Sigma(\Gamma(A)^*) \subseteq \Sigma([\Gamma(A) \cup \Gamma(B)]^*),$$

pa je

$$\Sigma(\Gamma(A)^*) \subseteq \Sigma(\Gamma(A^*B)^*).$$

Time smo upravo pokazali da je

$$\Sigma(A^*) = \langle \Sigma(A) \cup \Sigma(\Gamma(A)^*) \rangle \subseteq \langle \Sigma(A^*B) \cup \Sigma(\Gamma(A^*B)^*) \rangle = \Sigma((A^*B)^*),$$

pa se prethodna formula za $\Sigma((A^*B)^*A^*)$ svodi na

$$\Sigma((A^*B)^*A^*) = \Sigma((A^*B)^*) = \langle \Sigma(A^*B) \cup \Sigma((\Gamma(A^*B))^*) \rangle =$$

$$= \langle \Sigma(A^*)\Sigma(B) \cup \Sigma(A^*) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle.$$

Sada se sasvim lako vidi da je gornja potpolugrupa od S jednaka potpolugrupi $\langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle$, koristeći $\Sigma(A^*)\Sigma(B) \subseteq \langle \Sigma(A^*) \cup \Sigma(B) \rangle$, relaciju (12) i monotonost zvezde. Zaista,

$$\Sigma(A^*)\Sigma(B) = \langle \Sigma(A) \cup \Sigma(\Gamma(A)^*) \rangle \Sigma(B) \subseteq$$

$$\subseteq \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle \Sigma(B) \subseteq$$

$$\subseteq \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle,$$

i slično,

$$\Sigma(A^*) = \langle \Sigma(A) \cup \Sigma(\Gamma(A)^*) \rangle \subseteq \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle,$$

što dokazuje da je $\langle \Sigma(A^*)\Sigma(B) \cup \Sigma(A^*) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle$ sadržano u $\langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A) \cup \Gamma(B)]^*) \rangle$. Kako se obratna inkluzija dokazuje neposredno, dokaz drugog slučaja je kompletiran. ∎

Uopšteni Conwayev model $\mathbf{M}_T(G,S)$ je *stabilan na konjugaciju* ako za sve $g \in G$ i sve $H \leq G$ važi $T_H = T_{g^{-1}Hg}$.

PROPOZICIJA 3.2.5. *Neka je G konačna grupa, S konačna polugrupa i neka su A, B elementi uopštenog Conwayevog modela $\mathbf{M}_T(G,S)$ koji je ω-idempotentan i stabilan na konjugaciju. Tada je*

$$\Sigma((AB)^*) = \Sigma(A(BA)^*B).$$

Dokaz. U opštem slučaju, važi

$$\Sigma((AB)^*) = \langle \Sigma(AB) \cup \Sigma([\Gamma(A)\Gamma(B)]^*)\rangle$$

i

$$\Sigma((BA)^*) = \langle \Sigma(BA) \cup \Sigma([\Gamma(B)\Gamma(A)]^*)\rangle.$$

Sada imamo tri slučaja, prema tome da li su neki od skupova $\Gamma(A)$ i $\Gamma(B)$ prazni ili ne.

Najpre, pretpostavimo da je $\Gamma(A) = \Gamma(B) = \emptyset$. U tom specijalnom slučaju je $\Sigma((AB)^*) = \langle \Sigma(A)\Sigma(B)\rangle$ i $\Sigma((BA)^*) = \langle \Sigma(B)\Sigma(A)\rangle$, a takođe i

$$\Sigma(A(BA)^*B) = \Sigma(A)\Sigma(B) \cup \Sigma(A)\langle \Sigma(B)\Sigma(A)\rangle\Sigma(B).$$

Kako identitet $(ab)^+ = ab + a(ba)^+b$ očito važi za regularne jezike, rezultat sledi ako uzmemo interpretaciju $a \mapsto \Sigma(A)$, $b \mapsto \Sigma(B)$.

Drugi slučaj nastupa kada je $\Gamma(A) \neq \emptyset$, ali $\Gamma(B) = \emptyset$ (slučaj kada je $\Gamma(A) = \emptyset$ i $\Gamma(B) \neq \emptyset$ je simetričan i stoga u potpunosti analogan). Sada imamo sledeću situaciju:

$$\Sigma((AB)^*) = \langle \Sigma(B) \cup \Sigma(A)\Sigma(B)\rangle,$$

$$\Sigma((BA)^*) = \langle \Sigma(B) \cup \Sigma(B)\Sigma(A)\rangle.$$

Višestrukom primenom formule (11) za izračunavanje polugrupnog dela proizvoda, sledi

$$\Sigma(A(BA)^*B) = \Sigma(A)\langle \Sigma(B) \cup \Sigma(B)\Sigma(A)\rangle\Sigma(B) \cup$$

$$\cup\langle \Sigma(B) \cup \Sigma(B)\Sigma(A)\rangle\Sigma(B) \cup \Sigma(A)\Sigma(B) \cup \Sigma(B).$$

Tvrđenje propozicije je u ovom slučaju posledica sledećeg regularnog identiteta:

$$(b + ab)^+ = a(b + ba)^+b + (b + ba)^+b + ab + b.$$

Najzad, razmotrimo slučaj kada su skupovi $\Gamma(A)$ i $\Gamma(B)$ neprazni. Tada je

$$\Sigma((AB)^*) = \langle \Sigma(AB) \cup \Sigma([\Gamma(A)\Gamma(B)]^*)\rangle =$$
$$= \langle \Sigma(A)\Sigma(B) \cup \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A)\Gamma(B)]^*)\rangle =$$
$$= \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(A)\Gamma(B)]^*)\rangle$$

i analogno,

$$\Sigma((BA)^*) = \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(B)\Gamma(A)]^*)\rangle.$$

Razvoj za $\Sigma(A(BA)^*B)$ je dat niže:

$$\Sigma(A(BA)^*B) = \Sigma(A)\Sigma((BA)^*)\Sigma(B) \cup \Sigma(A)\Sigma((BA)^*) \cup$$
$$\cup \Sigma((BA)^*)\Sigma(B) \cup \Sigma(A)\Sigma(B) \cup \Sigma(A) \cup \Sigma((BA)^*) \cup \Sigma(B).$$

Međutim, jasno je da je $\Sigma(A), \Sigma(B) \subseteq \Sigma((BA)^*)$, pa se gornja jednakost svodi na

$$\Sigma(A(BA)^*B) = \Sigma((BA)^*) = \langle \Sigma(A) \cup \Sigma(B) \cup \Sigma([\Gamma(B)\Gamma(A)]^*)\rangle.$$

Imitacijom argumenta iz Propozicije 2.3.5, može se pokazati da $\Gamma(A)\Gamma(B)$ i $\Gamma(B)\Gamma(A)$ generišu konjugovane podgrupe od G. Zato je $T_{\langle\langle \Gamma(A)\Gamma(B)\rangle\rangle} = T_{\langle\langle \Gamma(B)\Gamma(A)\rangle\rangle}$ i

$$\Sigma([\Gamma(A)\Gamma(B)]^*) = \Sigma([\Gamma(B)\Gamma(A)]^*),$$

što okončava dokaz propozicije. ∎

Naravno, za ω-idempotentne uopštene Conwayeve modele važe i tvrđenja obratna Propozicijama 3.2.4 i 3.2.5. Kontraprimeri su u suštini isti kao i u Propozicijama 2.3.4 i 2.3.5, dok se obrazloženje prilagođava ambijentu uopštenih modela. Na primer, ako je $H \leq K$ i $s \in T_H \backslash T_K$, tada je $s \in \Sigma((K^*H)^*K^*)$, ali $s \notin \Sigma((K \cup H)^*) = \Sigma(K^*) = T_K$. Ova obratna tvrđenja nismo posebno istakli, jer ih nećemo koristiti van ovog poglavlja. Međutim, time je objašnjen obrat u narednoj teoremi.

Teorema 3.2.6. *Uopšteni Conwayev model* $\mathbf{M}_T(G, S)$ *(za konačne* G, S*) je* ω*-idempotentan Conwayev* **-poluprsten ako i samo ako je* **-monoton, stabilan na konjugaciju i zadovoljava uslov* $T_{\{1\}} = \emptyset$.

Dokaz. Obratna implikacija je razmotrena malopre, pa pođimo od pretpostavke da je uopšteni Conwayev model $\mathbf{M}_T(G, S)$ ω-idempotentan ($T_{\{1\}} = \emptyset$),

*-monoton i stabilan na konjugaciju. Posmatrajmo familiju podgrupa od G definisanu sa

$$\mathcal{F} = \{H \leq G : T_H = \emptyset\}.$$

Dati uslovi povlače da je komplement ove familije filter u mreži podgrupa grupe G koji je zatvoren na konjugovanje. Ali, tada je $\mathcal{F}$ ideal u toj mreži koji je takođe zatvoren na konjugovanje. Po Propozicijama 2.3.4 i 2.3.5, Conwayev model $\mathbf{C}_{\mathcal{F}}(G)$ je ω-idempotentan Conwayev *-poluprsten. Teorema sada neposredno sledi iz Propozicija 3.2.3, 3.2.4 i 3.2.5. ∎

3.3. Multiplikativne Kleenejeve algebre nemaju konačnu bazu identiteta

Kako bismo dokazali rezultat sadržan u naslovu ovog poglavlja, usresredićemo se na jednu specijalnu klasu uopštenih Conwayevih modela.

Neka su $p < q$ prosti brojevi. Sa $\mathbf{M}(p, q)$ označavamo uopšteni Conwayev model $\mathbf{M}_T(Z_{pq}, LN_3)$, gde je Z_{pq} ciklična grupa reda pq, a LN_3 (idempotentna) troelementna polugrupa data tablicom:

	a	b	c
a	a	a	a
b	c	b	c
c	c	c	c

(Lako se vidi da je ova polugrupa prezentirana sa $\langle a, b \mid a^2 = a,\ b^2 = b,\ ab = a\rangle$. Šta više, reč je o poddirektnom proizvodu dvoelementne polumreže i dvoelementne levo nulte trake, pa LN_3 generiše varijetet levo normalnih traka.) Naravno, Z_{pq} ima četiri podgrupe: dve trivijalne i podgrupe izomorfne redom sa Z_p i Z_q. Da bismo sada zadali zvezdu u našem modelu, dovoljno je definisati potpolugrupe od LN_3 pridružene ovim podgrupama. Definišemo da su to $T_{\{1\}} = \emptyset$, $T_{Z_p} = \{a\}$, $T_{Z_q} = \{b\}$ i $T_{Z_{pq}} = LN_3$.

Kao direktnu posledicu tvrđenja dokazanih u prethodnom poglavlju, dobijamo da važi

LEMA 3.3.1. *Za proizvoljne proste brojeve $p < q$, $\mathbf{M}(p, q)$ je ω-idempotentan Conwayev *-poluprsten.*

Sada želimo da pokažemo da za dovoljno velike p i q, $\mathbf{M}(p, q)$ zadovoljava neke od grupnih matričnih identiteta koji odgovaraju simetričnim grupama permutacija.

PROPOZICIJA 3.3.2. *Neka je n prirodan broj, a p, q prosti brojevi takvi da je $n! < p < q$. Neka je S proizvoljna (konačna) polugrupa. Ako je uopšteni Conwayev model $\mathrm{M}_T(Z_{pq}, S)$ ω-idempotentan i *-monoton, tada $\mathrm{M}_T(Z_{pq}, S)$ zadovoljava identitet $P(S_n)$ pridružen simetričnoj grupi permutacija S_n stepena n.*

Dokaz. Po Propoziciji 2.2.3, dovoljno je dokazati da za svaku familiju $\{A_\sigma : \sigma \in S_n\}$ elemenata modela $\mathrm{M}_T(Z_{pq}, S)$ (tj. podskupova od $Z_{pq} \cup S$) takvu da je $A_\sigma A_\tau \subseteq A_{\sigma\circ\tau}$ za sve $\sigma, \tau \in S_n$ i $A_{id}^* = A_{id}$ (id je identička permutacija n-elementnog skupa) važi $A^* = A$, gde je $A = \bigcup_{\sigma\in S_n} A_\sigma$.

Najpre, primetimo da je

$$A^2 = AA = \left(\bigcup_{\sigma\in S_n} A_\sigma\right)\left(\bigcup_{\tau\in S_n} A_\tau\right) = \bigcup_{\sigma,\tau\in S_n} A_\sigma A_\tau \subseteq \bigcup_{\sigma,\tau\in S_n} A_{\sigma\circ\tau} = A.$$

Takođe, pošto je $A_{id}^* = A_{id}$, sledi da je $1 \in A_{id}$, a time i $1 \in A$. Ovi zaključci pokazuju da A mora biti potpolugrupa od Z_{pq}^S koja sadrži jedinicu grupe Z_{pq}, dakle, unija podgrupe od Z_{pq} i potpolugrupe od S. Sledi da je $\Gamma(A^*) = \Gamma(A)$ i stoga preostaje da se dokaže da je $\Sigma(A^*) = \Sigma(A)$. Podsetimo se da je $\Sigma(A^*) = \langle\Sigma(A) \cup \Sigma(\Gamma(A)^*)\rangle$. Međutim, $\Gamma(A)$ je podgrupa od Z_{pq}, pa je $\Sigma(\Gamma(A)^*) = T_{\Gamma(A)}$. Tako, naš cilj je da pokažemo da je $T_{\Gamma(A)} \subseteq \Sigma(A)$ (jer je tada $\Sigma(A^*) = \langle\Sigma(A)\rangle = \Sigma(A)$).

U tom smislu, imamo četiri slučaja. Prvo, ako je $\Gamma(A) = \{1\}$, tada je $T_{\Gamma(A)} = \emptyset$, kada nema šta da se dokazuje. Dalje, neka je $\Gamma(A) = Z_p$. Ako elemente ciklične grupe Z_{pq} označimo sa $1, g, g^2, \ldots, g^{pq-1}$, tada je $g^q \in Z_p = \Gamma(A) \subseteq A$, pa postoji $\sigma \in S_n$ tako da $g^q \in A_\sigma$. Neka je k red permutacije σ u S_n. Sledi

$$g^{kq} = (g^q)^k \in \underbrace{A_\sigma A_\sigma \ldots A_\sigma}_{k \text{ puta}} \subseteq A_{\sigma^k} = A_{id}.$$

Ali, $k \leq n! < p$, pa element g^{kq} takođe generiše Z_p. Sledi $Z_p \leq \langle\!\langle\Gamma(A_{id})\rangle\!\rangle$, odakle je

$$T_{Z_p} \subseteq T_{\langle\!\langle\Gamma(A_{id})\rangle\!\rangle} \subseteq (\Gamma(A_{id}))^* \subseteq A_{id}^* = A_{id} \subseteq A,$$

jer je model $\mathrm{M}_T(Z_{pq}, S)$ *-monoton. Slučaj $\Gamma(A) = Z_q$ se rešava u potpunosti analogno, koristeći činjenicu $n! < q$. Najzad, neka je $\Gamma(A) = Z_{pq}$. Slično kao i malopre, imamo $g \in A_\sigma$ za neko $\sigma \in S_n$. Ako je k red σ u S_n, zaključujemo da $g^k \in A_{id}$. Međutim, $k \leq n! < p < q$, pa je $\langle\!\langle g^k\rangle\!\rangle = Z_{pq}$ i $\Gamma(A_{id}) = Z_{pq}$. Poslednja jednakost očito povlači

$$T_{Z_{pq}} \subseteq \Sigma(A_{id}^*) = \Sigma(A_{id}) \subseteq \Sigma(A),$$

što je i trebalo dokazati. ∎

TEOREMA 3.3.3. *Ne postoji konačan skup regularnih identiteta (identiteta koji važe na $\mathcal{KA}$) iz kojeg se mogu izvesti svi identiteti od jedne promenljive koji važe na $\mathcal{UF}$. Stoga varijetet $\mathcal{UF}$ nema konačnu bazu identiteta.*

Dokaz. Pretpostavimo, suprotno tvrđenju teoreme, da postoji konačan skup identiteta Kleenejevih algebri takav da se svaki identitet od jedne promenljive koji važi na $\mathcal{UF}$ može izvesti iz tog skupa korišćenjem pravila izvođenja jednakosne logike. Po primedbama nakon Teoreme 2.2.2, aksiome ω-idempotentnih Conwayevih *-poluprstena, zajedno sa grupnim matričnim identitetima $P(S_n)$, $n \geq 1$, čine bazu identiteta za $\mathcal{KA}$. Po primedbi iz [93] nakon Posledice 13.6, u klasi ω-idempotentnih Conwayevih *-poluprstena, iz matričnog identiteta $P(S_n)$ se mogu izvesti svi identiteti $P(S_m)$, $m \leq n$. Zbog toga, možemo pretpostaviti da se konačan skup identiteta od kojeg smo pošli sastoji od aksioma poluprstena sa jedinicom, Conwayevih identiteta, ω-idempotentnog zakona i matričnog identiteta $P(S_{n_0})$ za neko $n_0 \geq 1$.

Neka su sada p, q prosti brojevi za koje važi $n_0! < p < q$. Po Lemi 3.3.1, uopšteni Conwayev model $\mathrm{M}(p, q)$ je ω-idempotentan Conwayev *-poluprsten. Prema Propoziciji 3.3.2, $\mathrm{M}(p, q)$ zadovoljava $P(S_{n_0})$. Sledi da redukt modela $\mathrm{M}(p, q)$ iz koga je uklonjena operacija $\cup$ zadovoljava sve identitete varijeteta $\mathcal{UF}$, tj. pripada tom varijetetu. S druge strane, posmatrajmo identitet

$$(x^p)^*(x^q)^* = (x^q)^*(x^p)^*.$$

On je očito zadovoljen na $\mathcal{UF}$. Međutim, on ne važi u $\mathrm{M}(p, q)$, jer ako za x stavimo $\{g\}$ (gde je g generator ciklične grupe Z_{pq}), tada leva strana ima vrednost $Z_{pq} \cup \{a, b, c\}$, dok desna strana postaje $Z_{pq} \cup \{a, b\}$. Kontradikcija. ■

Obratimo pažnju na opštost gornjeg tvrđenja, iz kojeg se rezultat o beskonačnoj bazi za $\mathcal{UF}$ dobija kao posledica. Međutim, ono pruža mogućnosti za druge primene. Jedna od njih je i sledeća.

TEOREMA 3.3.4. *Varijetet $\mathcal{UF}^{\leq}$ uređenih multiplikativnih Kleenejevih algebri, generisan uređenim algebrama $\langle \mathcal{P}(A \times A), \circ, ^{\mathrm{rtc}}, \emptyset, \Delta_A, \subseteq \rangle$, nema konačnu aksiomatizaciju.*

Takođe, primetimo da je u Teoremi 3.3.3 potpuno svejedno da li se u tipu varijeteta $\mathcal{UF}$ pojavljuju konstantni simboli $0, 1$ (koji nastaju redom iz prazne relacije i dijagonale). Zato ta teorema zapravo ima četiri "verzije", ali svaka od njih ima isti zaključak o nepostojanju konačne baze identiteta.

Interesantno bi bilo videti kako eksplicitno izgleda neka netrivijalna (naravno, beskonačna) baza identiteta za $\mathcal{UF}$.

PROBLEM 4. *Naći netrivijalnu bazu za $\mathcal{UF}$.*

Lakša verzija ovog problema bi bila da se nađe baza za identitete od jedne promenljive koji važe na $\mathcal{UF}$. Po Teoremi 3.3.3, ta baza takođe mora biti beskonačna.

Osim toga, imajući u vidu da je $Eq(\mathcal{UF}) \subseteq Eq(\mathcal{KA})$, možemo se zapitati kakav je odnos između ove dve jednakosne teorije.

PROBLEM 5. *Naći relativnu bazu za $\mathcal{KA}$ u odnosu na $\mathcal{UF}$. Da li je varijetet $\mathcal{KA}$ konačno aksiomatizabilan nad $\mathcal{UF}$?*

Ovu glavu ćemo završiti jednim zanimljivim problemom u vezi multiplikativnih regularnih jezika koji je autorima ovde prikazanog rada [43] postavio J. L. Rhodes na IX međunarodnoj konferenciji o automatima i formalnim jezicima AFL '99. (Vasszécsény, Mađarska, 9.-13. avgust 1999.)

PROBLEM 6. (Rhodes, 1999) *Naći geometrijsku karakterizaciju minimalnih automata koji prihvataju multiplikativne regularne jezike nad datom konačnom azbukom Σ.*

Podsetimo se, *Kleenejeve algebre sa inverzijom* su članovi varijeteta $\mathcal{KA}^{\vee}$ generisanog algebrama binarnih relacija

$$\mathbf{Rel}^{\vee}(A) = \langle \mathcal{P}(A \times A), \cup, \circ, ^{\mathrm{rtc}}, ^{\vee}, \emptyset, \Delta_A \rangle.$$

Osim toga, ako je $w = a_1 \dots a_n$ reč nad azbukom Σ, tada definišemo *inverznu reč* $w^{-1} = a_n \dots a_1$. Ova operacija sa rečima indukuje operaciju $^{-1}$ sa jezicima definisanu za $L \subseteq \Sigma^*$ na sledeći način:

$$L^{-1} = \{w^{-1} : \ w \in L\}.$$

Posmatrajmo sada *algebre jezika sa inverzijom*:

$$\mathbf{Lang}^{\vee}(A) = \langle \mathcal{P}(\Sigma^*), +, \cdot, ^*, ^{-1}, \emptyset, \{\lambda\} \rangle.$$

Varijetet generisan svim ovakvim algebrama označićemo sa $\mathcal{L}^{\vee}$. Za razliku od slučaja Kleenejevih algebri bez inverzije, imamo da je $\mathcal{KA}^{\vee} \neq \mathcal{L}^{\vee}$; naime, važi stroga inkluzija $\mathcal{KA}^{\vee} \subset \mathcal{L}^{\vee}$. Ovu činjenicu ćemo obrazložiti u narednom poglavlju.

Naš zadatak u ovoj glavi biće da ispitujemo identitete ova dva varijeteta tj. da ustanovimo na koji način uvođenje nove, involutivne operacije utiče na regularne identitete. Okosnicu glave čini rad Crvenkovića, Ésika i autora disertacije [42] u kojem je na dva načina pokazano da $\mathcal{KA}^{\vee}$ i $\mathcal{L}^{\vee}$ nemaju konačnu bazu identiteta, čime je, između ostalog, rešen Problem 4.2.3 Jónssona [78]. Oba metoda će ovde biti detaljno razmotrena: jedan je više "sintaktički" po karakteru i zasniva se na analizi identiteta involutivnih algebri i njihovih izvođenja u jednakosnoj logici; drugi pristup se sastoji u uvođenju involutivne operacije u (klasične) Conwayeve modele. Ali, pre toga moramo dati pregled ranijih rezultata u vezi razmatrana dva varijeteta, neophodnih za dalji rad.

4.1. $\mathcal{KA}^\vee$ i $\mathcal{L}^\vee$: slobodne algebre i relativna aksiomatizacija

Najpre ćemo definisati još jednu algebru koja predstavlja proširenje algebri jezika. Naime, za azbuku Σ neka je Σ' neka druga azbuka, disjunktna sa Σ, koja je u bijektivnom odnosu sa Σ, tj. svakom slovu $a \in \Sigma$ se obostrano jednoznačno pridružuje slovo $a' \in \Sigma'$. Za jezik $L \subseteq (\Sigma \cup \Sigma')^*$ definišemo $L^\vee = \{w^\vee : w \in L\}$, gde je za $w = a_1 \dots a_n$,

$$w^\vee = a_n^\vee \dots a_1^\vee,$$

pri čemu je za $x \in \Sigma \cup \Sigma'$,

$$x^\vee = \begin{cases} x' & x \in \Sigma, \\ y & x = y' \in \Sigma'. \end{cases}$$

Na taj način smo dobili algebru

$$\mathbf{L}^\vee(\Sigma, \Sigma') = \langle \mathcal{P}((\Sigma \cup \Sigma')^*), +, \cdot, ^*, ^\vee, \emptyset, \{\lambda\} \rangle.$$

Pokazuje se da se algebra $\mathbf{L}^\vee(\Sigma, \Sigma')$ može potopiti u algebru jezika sa inverzijom.

PROPOZICIJA 4.1.1. *Za sve azbuke* Σ *je* $\mathbf{L}^\vee(\Sigma, \Sigma') \in \mathcal{L}^\vee$.

Dokaz. Neka je $\Upsilon = \Sigma \cup \{\sharp\}$, gde je $\sharp$ novi simbol. Definišimo najpre preslikavanje $\phi : \Sigma \cup \Sigma' \to \Upsilon^*$ za $x \in \Sigma$, $x' \in \Sigma'$ sa

$$\begin{aligned} \phi(x) &= x\sharp, \\ \phi(x') &= \sharp x. \end{aligned}$$

Za reč $w = a_1 \dots a_n \in (\Sigma \cup \Sigma')^*$, ova definicija se proširuje sa

$$\phi(w) = \phi(a_1) \dots \phi(a_n).$$

Sada se za preslikavanje $\Phi : \mathcal{P}((\Sigma \cup \Sigma')^*) \to \mathcal{P}(\Upsilon^*)$ dato sa

$$\Phi(L) = \{\phi(w) : w \in L\}$$

rutinski pokazuje da je reč o potapanju $\mathbf{L}^\vee(\Sigma, \Sigma') \to \mathbf{Lang}^\vee(\Upsilon)$. ∎

Neka je sada $\mathbf{R}^\vee(\Sigma, \Sigma')$ podalgebra od $\mathbf{L}^\vee(\Sigma, \Sigma')$ generisana jezicima $\{x\}$, $x \in \Sigma \cup \Sigma'$. Zapravo, reč je o algebri regularnih jezika nad azbukom $\Sigma \cup \Sigma'$ na kojoj je dodefinisana inverzija $^\vee$, koja funkcioniše isto kao i u $\mathbf{L}^\vee(\Sigma, \Sigma')$. Značaj ovih algebri u odnosu na varijetet $\mathcal{L}^\vee$ je iskazan sledećim rezultatom.

TEOREMA 4.1.2. (Bloom, Ésik, Stefanescu, [27]) $\mathbf{R}^{\vee}(\Sigma, \Sigma')$ *je* $\mathcal{L}^{\vee}$*-slobodna algebra nad* Σ. *Stoga baza identiteta za* $\mathcal{KA}$*, zajedno sa identitetima*

$$(x+y)^{\vee} = x^{\vee} + y^{\vee}, \tag{13}$$
$$(xy)^{\vee} = y^{\vee}x^{\vee}, \tag{14}$$
$$(x^*)^{\vee} = (x^{\vee})^*, \tag{15}$$
$$(x^{\vee})^{\vee} = x, \tag{16}$$

čini bazu identiteta za $\mathcal{L}^{\vee}$.

Primetimo da su identiteti

$$0^{\vee} = 0, \tag{17}$$
$$1^{\vee} = 1, \tag{18}$$

posledice identiteta (13)–(16).

Na osnovu gornje teoreme, odgovarajućom adaptacijom dokaza Posledice 1.4.5, odmah se dobija

POSLEDICA 4.1.3. *Jednakosna teorija varijeteta* $\mathcal{L}^{\vee}$ *je odlučiva.*

Posmatrajmo sada identitet

$$x + xx^{\vee}x = xx^{\vee}x. \tag{19}$$

(Ekvivalentno, mogli smo pisati $x \leq xx^{\vee}x$.) Njegov značaj je u tome da on važi na svim algebrama relacija $\mathbf{Rel}^{\vee}(A)$ (a time i na celom varijetetu $\mathcal{KA}^{\vee}$), što se lako proverava. Ali, on očito nije tačan na algebrama jezika $\mathbf{Lang}^{\vee}(\Sigma)$ i $\mathbf{L}^{\vee}(\Sigma, \Sigma')$. Prema tome, $\mathcal{KA}^{\vee} \neq \mathcal{L}^{\vee}$.

U vezi sa identitetom (19), uvodimo sledeći pojam. Kažemo da je jezik $L \subseteq (\Sigma \cup \Sigma')^*$ *zatvoren* ako za svaku reč $w \in L$ oblika $w = u_1 v v^{\vee} v u_2$ važi $u_1 v u_2 \in L$. Najmanji zatvoren jezik koji sadrži L (koji postoji pošto je $(\Sigma \cup \Sigma')^*$ zatvoren jezik i pošto se zatvorenost čuva presecima) je *zatvorenje* od L, koje označavamo sa $cl(L)$. Dakle, jezik je zatvoren ako i samo ako je $L = cl(L)$. Neposredno se pokazuje da je relacija ρ definisana na algebri regularnih jezika $\mathbf{Reg}(\Sigma)$ sa (pri čemu uzimamo v^{-1} umesto $v^{\vee}$):

$$\langle L_1, L_2 \rangle \in \rho \text{ ako i samo ako } cl(L_1) = cl(L_2),$$

kongruencija. Slično se može reći i za $\mathbf{R}^{\vee}(\Sigma, \Sigma')$, pa imamo faktor-algebru

$$\mathbf{CR}^{\vee}(\Sigma, \Sigma') = \mathbf{R}^{\vee}(\Sigma, \Sigma')/\rho.$$

Ispostavilo se da je reč o slobodnim algebrama varijeteta $\mathcal{KA}^{\vee}$.

TEOREMA 4.1.4. (Bloom, Ésik, Stefanescu, [27]) $\mathbf{CR}^{\vee}(\Sigma, \Sigma')$ *je* $\mathcal{KA}^{\vee}$*-slobodna algebra nad* Σ.

Štaviše, u [27] je pokazano da je zatvorenje regularnog jezika regularan jezik, i to efektivno: naime, postoji algoritam koji za dati konačni automat koji prihvata jezik L konstruiše automat koji prihvata jezik $cl(L)$. Specijalno, to znači da važi

POSLEDICA 4.1.5. *Jednakosna teorija varijeteta* $\mathcal{KA}^{\vee}$ *je odlučiva.*

Osim toga, lako se vidi da je algebra $\mathbf{CR}^{\vee}(\Sigma, \Sigma')$ izomorfna algebri čiji su elementi zatvoreni regularni jezici nad Σ, pri čemu je rezultat proizvoda dva jezika zatvorenje konkatenacije ta dva jezika, a zvezda – zatvorenje Kleenejeve iteracije.

Navedeni rezultati bili su dovoljni Ésiku i Bernátskom da nađu relativnu jednakosnu aksiomatizaciju varijeteta Kleenejevih algebri sa inverzijom $\mathcal{KA}^{\vee}$ u odnosu na $\mathcal{KA}$. Time su oni potvrdili hipotezu postavljenu u [27].

TEOREMA 4.1.6. (Ésik, Bernátsky, [58]) *Regularni identiteti, identiteti* (13)–(16) *i* (19) *čine jednakosnu bazu za* $\mathcal{KA}^{\vee}$.

Specijalno, to znači da je $\mathcal{KA}^{\vee} \subset \mathcal{L}^{\vee}$. U daljem, mi ćemo poći upravo od gornjeg ključnog tvrđenja, kako bismo pokazali da $\mathcal{KA}^{\vee}$ nema konačnu bazu, tj. da prisustvo operacije inverza relacija $^{\vee}$ uglavnom ne "remeti" strukturu jednakosne teorije $Eq(\mathcal{KA}^{\vee})$ u odnosu na jednakosnu teoriju $Eq(\mathcal{KA})$.

4.2. Sintaktička teorema o jednakosnim teorijama involutivnih algebri

Neka je τ tip algebri. Sa $\tau^{\vee}$ označavamo tip koji se dobija proširivanjem τ unarnim simbolom $^{\vee}$. Algebra $\mathbf{A}$ tipa $\tau^{\vee}$ je *involutivna* τ*-algebra* ukoliko za sve $f \in \tau$ (f je arnosti $n \geq 0$), $\mathbf{A}$ zadovoljava identitete

$$(f(x_1, \ldots, x_n))^{\vee} = f(x_n^{\vee}, \ldots, x_1^{\vee}), \tag{20}$$

$$(x^{\vee})^{\vee} = x. \tag{21}$$

Primetimo da za $n = 0$ (slučaj konstantnog simbola), identitet (20) glasi $f^{\vee} = f$. Primera radi, ako se tip τ sastoji samo iz jednog binarnog simbola, identitet (20) postaje

$$(xy)^{\vee} = y^{\vee}x^{\vee},$$

i pri tome govorimo o *involutivnim grupoidima.* Asocijativni involutivni grupoidi su *involutivne polugrupe.* Takođe, Teorema 4.1.2 upravo govori da je $\mathcal{L}^\vee$ varijetet svih Kleenejevih algebri sa involucijom.

Neka je $\mathcal{V}$ netrivijalan varijetet τ-algebri. Sa $\widehat{\mathcal{V}}$ obeležavamo varijetet involutivnih τ-algebri koje zadovoljavaju sve identitete koji važe u $\mathcal{V}$. To znači da je τ-redukt svake algebre iz $\widehat{\mathcal{V}}$ algebra koja pripada $\mathcal{V}$ (specijalno, tada je $\widehat{\mathcal{KA}} = \mathcal{L}^\vee$). U ovom poglavlju ćemo dokazati tvrđenje koje daje potreban uslov da podvarijetet $\mathcal{W} \leq \widehat{\mathcal{V}}$ ima konačnu bazu identiteta.

Za term t tipa $\tau^\vee$ definišemo njegovu *pozitivnu normalnu formu* t^+ i *negativnu normalnu formu* t^- na sledeći način.

- Ako je $t \equiv x$ za neko $x \in X$, onda je $t^+ \equiv x$ i $t^- \equiv x^*$.
- Ako je $t \equiv f(t_1, \ldots, t_n)$, gde su $t_1, \ldots, t_n$ termi, tada je

$$\begin{aligned} t^+ &\equiv f(t_1^+, \ldots, t_n^+), \\ t^- &\equiv f(t_n^-, \ldots, t_1^-). \end{aligned}$$

- Ako je $t \equiv s^\vee$, tada je $t^+ \equiv s^-$ i $t^- \equiv s^+$.

Nije teško videti da je zapravo $t^- \equiv (t^\vee)^+$.

Za svaki term t tipa τ definišemo njemu *inverzni term* t^R sa:

- $t^R \equiv x$, ako je $t \equiv x \in X$,
- $t^R \equiv f(t_n^R, \ldots, t_1^R)$, ako je $t \equiv f(t_1, \ldots, t_n)$.

Neka je $\bar{X} = \{\bar{x} : x \in X\}$ disjunktna (bijektivna) kopija skupa X. Tada slobodnu algebru $\mathbf{F}_\mathcal{V}(X)$ možemo posmatrati kao podalgebru od $\mathbf{F}_\mathcal{V}(X \cup \bar{X})$. Za bilo koji term $t \equiv t'(x_1, \ldots, x_n, x_1^\vee, \ldots, x_n^\vee)$ tipa $\tau^\vee$ (gde je t' term tipa τ) koji je u pozitivnoj normalnoj formi, sa $|t|$ označavamo element algebre $\mathbf{F}_\mathcal{V}(X \cup \bar{X})$,

$$(t')^{\mathbf{F}_\mathcal{V}(X \cup \bar{X})}(x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n).$$

Reč je o vrednosti termovskog preslikavanja t' u slobodnoj algebri $\mathbf{F}_\mathcal{V}(X \cup \bar{X})$ kada su vrednosti promenljivih odgovarajući slobodni generatori. Na primer, ako je $\mathcal{V}$ varijetet svih τ-algebri i $t \equiv (x^\vee)^\vee$, $s \equiv x^\vee$, tada je $|t^+| \equiv x$, $|s^+| \equiv \bar{x}$, tako da $|t^+|$ pripada $\mathbf{F}_\mathcal{V}(X)$, ali ne i $|s^+|$

Pretpostavimo da je Ax skup identiteta tipa $\tau^\vee$. Ako su t_1, t_2 termi tog tipa, tada pišemo $t \to_{Ax} t'$ ukoliko su oni oblika

$$\begin{aligned} t_1 &\equiv r(x_1, \ldots, x_m, p_1(q_1, \ldots, q_n)), \\ t_2 &\equiv r(x_1, \ldots, x_m, p_2(q_1, \ldots, q_n)), \end{aligned}$$

gde term $r(x_1, \ldots, x_m, x_{m+1})$ sadrži samo jedno pojavljivanje x_{m+1}, identitet $p_1(x_1, \ldots, x_n) = p_2(x_1, \ldots, x_n)$ pripada Ax, dok su $q_1, \ldots, q_n$ neki termi. Sada se lako pokazuje da važi $Ax \vdash p = q$ ako i samo ako postoji niz terma $t_0, \ldots, t_k$ tako da je $t_0 \equiv p$, $t_k \equiv q$ i da važi $t_{i-1} \to_{Ax} t_i$ za sve $1 \leq i \leq k$.

Skup identiteta E tipa τ je *zatvoren u odnosu na inverziju* ako za svaki identitet $p = q$ koji pripada E, identitet $p^R = q^R$ takođe pripada E. Označimo sa Inv involucijske identitete (20) i (21).

LEMA 4.2.1. *Za bilo koje terme t_1 i t_2 tipa $\tau^\vee$ je $t_1^+ \equiv t_2^+$ ako i samo ako $Inv \vdash t_1 = t_2$.*

Dokaz. Dokaz sledi iz činjenice da za svaki term t važi $Inv \vdash t = t^+$, kao i da $p \to_{Inv} q$ implicira $p^+ \equiv q^+$. ∎

Primetimo da operator $^+$ vrši na termu primenu involucije, sve dok se ona ne "spusti" do nivoa promenljivih.

LEMA 4.2.2. *Neka je E skup identiteta tipa τ. Ako je E zatvoren u odnosu na inverziju i ako je $t_1 \to_E t_2$ za neke terme t_1, t_2, tada je $t_1^+ \to_E t_2^+$ i $t_1^- \to_E t_2^-$.*

Dokaz. Ako je $t_1 \to_E t_2$, onda postoji identitet $p_1 = p_2$ iz E (koji sadrži, recimo, n promenljivih), term $r(x_1, \ldots, x_m, x_{m+1})$ koji sadrži samo jedno pojavljivanje promenljive x_{m+1} i termi $q_1, \ldots, q_n$, tako da je

$$\begin{aligned} t_1 &\equiv r(x_1, \ldots, x_m, p_1(q_1, \ldots, q_n)), \\ t_2 &\equiv r(x_1, \ldots, x_m, p_2(q_1, \ldots, q_n)). \end{aligned}$$

Tvrđenje pokazujemo indukcijom po složenosti terma r.

Najpre, neka je $r \equiv x_{m+1}$. Tada je

$$\begin{aligned} t_1^+ &\equiv p_1(q_1^+, \ldots, q_n^+), \\ t_2^+ &\equiv p_2(q_1^+, \ldots, q_n^+), \\ t_1^- &\equiv p_1^R(q_1^-, \ldots, q_n^-), \\ t_2^- &\equiv p_2^R(q_1^-, \ldots, q_n^-). \end{aligned}$$

Sada $t_1^+ \to_E t_2^+$ sledi trivijalno, dok $t_1^- \to_E t_2^-$ važi pošto identitet $p_1^R = p_2^R$ pripada E.

Neka je sada $r \equiv f(r_1, \ldots, r_\ell)$. Bez ograničenja opštosti, pretpostavimo da je r_ℓ podterm koji sadrži x_{m+1}. Tada imamo

$$\begin{aligned} t_1 &\equiv f(r_1(x_1, \ldots, x_m), \ldots, r_\ell(x_1, \ldots, x_m, p_1(q_1, \ldots, q_n)), \\ t_2 &\equiv f(r_1(x_1, \ldots, x_m), \ldots, r_\ell(x_1, \ldots, x_m, p_2(q_1, \ldots, q_n)). \end{aligned}$$

Primetimo da za bilo koje terme $s_1, s_2, u_1, \ldots, u_{\ell-1}$ takve da $s_1 \to_E s_2$ važi

$$f(u_1, \ldots, u_{\ell-1}, s_1) \to_E f(u_1, \ldots, u_{\ell-1}, s_2),$$

kao i

$$f(s_1, u_{\ell-1}, \ldots, u_1) \to_E f(s_2, u_{\ell-1}, \ldots, u_1).$$

Označimo

$$\begin{aligned} t &\equiv r_\ell(x_1, \ldots, x_m, p_1(q_1, \ldots, q_n)), \\ t' &\equiv r_\ell(x_1, \ldots, x_m, p_2(q_1, \ldots, q_n)). \end{aligned}$$

Tada važi $t \to_E t'$, pa je, po induktivnoj pretpostavci, $t^+ \to_E (t')^+$ i $t^- \to_E (t')^-$. Ali, po prethodnoj primedbi imamo i

$$\begin{aligned} f(r_1^+, \ldots, r_{\ell-1}^+, t^+) &\to_E f(r_1^+, \ldots, r_{\ell-1}^+, (t')^+), \\ f(t^-, r_{\ell-1}^-, \ldots, r_1^-) &\to_E f((t')^-, r_{\ell-1}^-, \ldots, r_1^-). \end{aligned}$$

što u stvari znači $t_1^+ \to_E t_2^+$ i $t_1^- \to_E t_2^-$.

Najzad, razmotrimo slučaj $r \equiv r_1^\vee$. Imamo:

$$\begin{aligned} t_1 &\equiv (r_1(x_1, \ldots, x_m, p_1(q_1, \ldots, q_n)))^\vee, \\ t_2 &\equiv (r_1(x_1, \ldots, x_m, p_2(q_1, \ldots, q_n)))^\vee. \end{aligned}$$

Označimo kraće $t_1 \equiv (s_1)^\vee$ i $t_2 \equiv (s_2)^\vee$. Kako identitet $p_1 = p_2$ pripada E, to je $s_1 \to_E s_2$. Po induktivnoj pretpostavci, važi $s_1^+ \to_E s_2^+$ i $s_1^- \to_E s_2^-$. Tvrđenje sada sledi neposredno, pošto je $t_i^+ \equiv s_i^-$ i $t_i^- \equiv s_i^+$ za $i = 1, 2$. ∎

Ako je $\mathcal{W} \leq \mathcal{V}$, kažemo da skup identiteta Ax čini *relativnu bazu identiteta* za $\mathcal{W}$ u odnosu na $\mathcal{V}$ ako Ax zajedno sa nekom bazom identiteta za $\mathcal{V}$ čini bazu identiteta za $\mathcal{W}$. Tako, Teoreme 4.1.2 i 4.1.6 opisuju (konačne) relativne baze identiteta za $\mathcal{L}^\vee$, tj. $\mathcal{KA}^\vee$ u odnosu na $\mathcal{KA}$.

TEOREMA 4.2.3. *Neka je E neki skup identiteta koji važe u varijetetu τ-algebri $\mathcal{V}$ i neka je Ax relativna baza identiteta za varijetet $\mathcal{W} \leq \widehat{\mathcal{V}}$ u odnosu na $\widehat{\mathcal{V}}$. Pretpostavimo da su ispunjeni sledeći uslovi:*

(1) E je zatvoren na inverziju,

(2) ako su t_1, t_2 termi tipa $\tau^\vee$ takvi da je $t_1 \to_{Ax} t_2$ i $|t_1^+|$ pripada $\mathbf{F}_\mathcal{V}(X)$, tada $E \cup Inv \vdash t_1 = t_2$.

Tada je $E' = E \cup Inv \cup Ax$ baza identiteta za $\mathcal{W}$ ako i samo ako je E baza identiteta za $\mathcal{V}$.

Dokaz. Najpre, jasno je da je za proizvoljnu bazu identiteta E varijeteta $\mathcal{V}$, E' baza identiteta za varijetet $\mathcal{W}$. Obratno, pretpostavimo da identiteti $E' = E \cup Inv \cup Ax$ aksiomatizuju varijetet $\mathcal{W}$. Cilj je da pokažemo da je tada E baza identiteta za $\mathcal{V}$.

Neka su t i t' termi tipa τ i neka identitet $t = t'$ važi u $\mathcal{V}$. Tada postoji niz terma $t_0, t_1, \ldots, t_k$ tako da je $t \equiv t_0$, $t' \equiv t_k$ i $t_{i-1} \to_E t_i$ za sve $1 \leq i \leq k$. Tvrdimo da

$$E \vdash t_{i-1}^+ = t_i^+$$

za sve $1 \leq i \leq k$. Kako su t, t' τ-termi, to je $t \equiv t^+$ i $t' \equiv (t')^+$, pa bi tada sledilo $E \vdash t = t'$, čime bi naš cilj bio postignut.

Dokažimo da je $E \vdash t_{i-1}^+ = t_i^+$ indukcijom po i. Razlikujemo tri slučaja. Ako je $t_{i-1} \to_{Inv} t_i$, tada je $t_{i-1}^+ \equiv t_i^+$ po Lemi 4.2.1. Ako je $t_{i-1} \to_E t_i$, onda je $t_{i-1}^+ \to_E t_i^+$ po Lemi 4.2.2, pa je $E \vdash t_{i-1}^+ = t_i^+$. Najzad, neka je $t_{i-1} \to_{Ax} t_i$. Tada po induktivnoj hipotezi sledi $E \vdash t_{j-1}^+ = t_j^+$ za sve $j \leq i - 1$, odakle $|t_{i-1}^+| \equiv |t^+|$ pripada slobodnoj algebri $\mathbf{F}_{\mathcal{V}}(X)$. Po uslovu *(2)*, imamo da

$$E \cup Inv \vdash t_{i-1} = t_i,$$

što na osnovu prethodne dve leme znači da $E \vdash t_{i-1}^+ = t_i^+$. ∎

Posledica 4.2.4. *Neka konačan skup identiteta Ax tipa τ čini relativnu bazu varijeteta $\mathcal{W} \leq \widehat{\mathcal{V}}$ u odnosu na $\widehat{\mathcal{V}}$. Ako varijetet $\mathcal{V}$ ima konačnu bazu identiteta, onda je ima $\mathcal{W}$. Pretpostavimo da su ispunjeni i sledeći uslovi:*

(1) jednakosna teorija varijeteta $\mathcal{V}$ je zatvorena na inverziju,

(2) postoji konačan skup identiteta F koji važe na $\mathcal{V}$ tako da ako su t_1, t_2 termi tipa $\tau^\vee$ takvi da važi $t_1 \to_{Ax} t_2$ i $|t_1^+|$ pripada $\mathbf{F}_{\mathcal{V}}(X)$, tada

$$F \cup Inv \vdash t_1 = t_2.$$

Tada $\mathcal{W}$ i $\mathcal{V}$ zadovoljavaju iste identitete tipa τ i ako je varijetet $\mathcal{W}$ konačno baziran, onda je to i $\mathcal{V}$.

Dokaz. Kako je $\mathcal{W} \leq \widehat{\mathcal{V}}$, to bilo koji identitet tipa τ koji važi u $\mathcal{V}$ važi i u $\mathcal{W}$. Štaviše, pošto su Inv i Ax konačni skupovi, ako $\mathcal{V}$ ima konačnu bazu identiteta, onda to važi i za $\mathcal{W}$.

Pretpostavimo sada da važe data dva uslova. Neka je E konačan skup identiteta tipa τ koji je zatvoren u odnosu na inverziju koji sadrži skup F i zajedno sa Inv i Ax čini bazu identiteta za $\mathcal{W}$. S obzirom da sada E zadovoljava uslove prethodne teoreme, sledi da je E jednakosna baza za varijetet $\mathcal{V}$. Prema tome, ako $\mathcal{W}$ ima konačnu bazu, onda je ima i $\mathcal{V}$, i ova dva varijeteta, osim toga, zadovoljavaju iste identitete tipa τ. ∎

POSLEDICA 4.2.5. *Varijeteti $\mathcal{V}$ i $\widehat{\mathcal{V}}$ zadovoljavaju iste identitete tipa τ ako i samo ako su identiteti varijeteta $\mathcal{V}$ zatvoreni na inverziju. U tom slučaju $\mathcal{V}$ ima konačnu bazu identiteta ako i samo ako $\widehat{\mathcal{V}}$ ima konačnu bazu identiteta.*

Odavde se neposredno dobija

TEOREMA 4.2.6. *Varijetet $\mathcal{L}^\vee$ nema konačnu bazu identiteta.*

Na osnovu pokazanih opštih jednakosno-logičkih tvrđenja, sada možemo dokazati i glavni rezultat ove glave.

TEOREMA 4.2.7. *Varijetet $\mathcal{KA}^\vee$ nema konačnu bazu identiteta.*

Dokaz. Najpre, jasno je da je $Eq(\mathcal{KA})$ zatvoreno na inverziju, tj. ako je $p = q$ regularni identitet, onda je to i $p^R = q^R$. Stoga je prema Posledici 4.2.4 dovoljno pokazati da postoji konačan skup F regularnih identiteta takav da za sve $^\vee$-regularne izraze t_1, t_2 nad Σ važi: ako je $|t_1^+| \in Reg(\Sigma)$ i $t_1 \to_{E_0} t_2$ (gde se E_0 sastoji iz jedinog identiteta (19)), tada je $F \cup Inv \vdash t_1 = t_2$.

Po pretpostavci, t_2 se dobija iz t_1 zamenom podterma oblika $p + pp^\vee p$ sa $pp^\vee p$, ili obratno. Međutim, regularni jezik $|t_1^+|$ ne sadrži nijednu reč u kojoj se pojavljuje slovo iz $\bar{\Sigma}$, pa se $p + pp^\vee p$, odnosno $pp^\vee p$, mora pojaviti u t_1 u okviru podterma q koji predstavlja prazan jezik, ili pak p predstavlja $\{\lambda\}$. U svakom od ovih slučajeva se lako vidi da $F \cup Inv \vdash t_1 = t_2$, gde je F skup jednakosnih aksioma za ω-idempotentne Conwayeve *-poluprstene. ∎

Ovu teoremu ćemo još jednom dokazati u narednom poglavlju, primenom Conwayevih modela sa involucijom.

Na kraju ovog poglavlja, pomenimo još jednu primenu Teoreme 4.2.3 i njene Posledice 4.2.4, i to u teoriji (involutivnih) polugrupa. Crvenković, Vinčić i autor disertacije [46] su upravo uz pomoć pomenutih tvrđenja opisali klasu involutivnih polugrupa sa beskonačnom bazom identiteta. Najmanji primer te vrste je 13-elementna involutivna polugrupa koja se dobija od šestoelementne *Perkinsove polugrupe*, tj. Brandtovog monoida B_2^1 (gde je $B_2 = \langle a, b |\ a^2 = b^2 = 0,\ aba = a,\ bab = b\rangle$), konstrukcijom koja je u teoriji polugrupa poznata kao *0-direktna unija* (odnosno *ortogonalna suma*) polugrupe sa svojom anti-izomorfnom kopijom.

4.3. Involutivni Conwayevi modeli

Neka je $\mathbf{C}_{\mathcal{F}}(G) = \langle \mathcal{P}(G^0), \cup, \cdot, ^*, \emptyset, \{1\}\rangle$ Conwayev model. Neka za $g \in G$, g^{-1} označava inverz elementa g u grupi G, dok je $0^{-1} = 0$. Jasno, ovim je definisana jedna involucija na 0-grupi G^0. Neka je sada za $A \subseteq G^0$,

$$A^\vee = \{a^{-1} :\ a \in A\}.$$

Tada je

$$\mathbf{C}^{\vee}_{\mathcal{F}}(G) = \langle \mathcal{P}(G^0), \cup, \cdot, ^*, ^{\vee}, \emptyset, \{1\} \rangle$$

involutivni Conwayev model (koji odgovara grupi G i familiji njenih podgrupa $\mathcal{F}$). Kao i u slučaju običnih Conwayevih modela, ako je $\mathcal{F}$ familija svih pravih podgrupa od G, tada izostavljamo donji indeks koji se odnosi na tu familiju.

LEMA 4.3.1. *Neka je G grupa. Tada je $\mathbf{C}^{\vee}_{\mathcal{F}}(G)$ involutivni ω-idempotentni *-poluprsten (dakle, zadovoljava identitete* (13)–(16)*) koji zadovoljava i identitet* (19).

Dokaz. Najpre, još smo ranije videli da je $\mathbf{C}_{\mathcal{F}}(G)$ ω-idempotentni *-poluprsten. Identitet (13) je očito zadovoljen u $\mathbf{C}^{\vee}_{\mathcal{F}}(G)$, kao i (16), pošto je $(a^{-1})^{-1} = a$ za sve $a \in G \cup \{0\}$. Identitet (14) takođe lako sledi, jer je unarna operacija $^{-1}$ involucija ne samo na grupi G, već i na 0-grupi G^0. Dalje, primetimo da za podskup $A \subseteq G \cup \{0\}$ koji sadrži element $a \neq 0$ imamo

$$A = A\{a^{-1}\}\{a\} \subseteq AA^{\vee}A,$$

dok se inkluzija $A \subseteq AA^{\vee}A$ dobija neposredno ako je $A = \emptyset$ ili $A = \{0\}$. Tako, $\mathbf{C}^{\vee}_{\mathcal{F}}(G)$ zadovoljava identitet (19).

Preostaje da ispitamo identitet (15). Prvo, primetimo da je A^* ili podgrupa od G, ili unija podgrupe od G i $\{0\}$. Zato je $(A^*)^{\vee} = A^*$. S druge strane, svaki podskup $A \subseteq G$ generiše istu podgrupu od G kao i $A^{\vee}$. Takođe, $0 \in A$ ako i samo ako $0 \in A^{\vee}$. Otuda je $(A^{\vee})^* = A^*$, tj. imamo $(A^*)^{\vee} = (A^{\vee})^*$ za sve $A \subseteq G \cup \{0\}$. ∎

Sada možemo pokazati analogon Teoreme 2.2.2 Blooma i Ésika za varijetet $\mathcal{KA}^{\vee}$.

TEOREMA 4.3.2. *Neka je $\mathcal{G}$ neka klasa konačnih grupa. Aksiome involutivnih ω-idempotentnih Conwayevih *-poluprstena, matrični identiteti $P(G)$ za $G \in \mathcal{G}$ i identitet (19) čine bazu identiteta za $\mathcal{KA}^{\vee}$ ako i samo ako svaka konačna prosta grupa deli neku grupu iz $\mathcal{G}$.*

Dokaz. Ako svaka konačna prosta grupa deli neku grupu iz $\mathcal{G}$, tada nabrojani identiteti čine bazu identiteta za $\mathcal{KA}^{\vee}$ po Teoremama 2.2.2 i 4.1.6. Obratno, neka je $\mathcal{G}$ neka klasa konačnih grupa koja na u teoremi opisan način indukuje bazu identiteta za $\mathcal{KA}^{\vee}$ i neka je G konačna prosta grupa. Posmatrajmo involutivni Conwayev model $\mathbf{C}^{\vee}(G)$. Ako G ne deli nijednu grupu iz $\mathcal{G}$, tada po Propoziciji 2.3.6 model $\mathbf{C}^{\vee}(G)$ zadovoljava sve grupne matrične identitete pridružene članovima klase $\mathcal{G}$. Prema ovom zaključku i prethodnoj lemi, sledilo bi $\mathbf{C}^{\vee}(G) \in \mathcal{KA}^{\vee}$. Međutim (ponovo po Propoziciji 2.3.6), $\mathbf{C}^{\vee}(G)$ očito ne zadovoljava identitet $P(G)$, što je kontradikcija. ∎

Najzad, ponavljamo Teoremu 4.2.7 sa dokazom koji koristi involutivne Conwayeve modele (njihova upotreba je sadržana u pozivu na gornju teoremu).

TEOREMA 4.3.3. *Varijetet $\mathcal{KA}^{\vee}$ nema konačnu bazu identiteta.*

Dokaz. Analogno kao i u dokazu Teoreme 2.3.7, dolazimo do zaključka da ako $\mathcal{KA}^{\vee}$ ima konačnu bazu identiteta, tada se jedna takva konačna baza sastoji od aksioma involutivnih ω-idempotentnih Conwayevih *-poluprstena, identiteta (19) i grupnih identiteta $P(A_n)$, $5 \leq n \leq n_0$, za neko $n_0 \geq 5$. Ali, tada prosta grupa A_{n_0+1} ne deli nijednu od grupa $A_5, \ldots, A_{n_0}$, što je kontradikcija sa prethodnom teoremom. ∎

4.4. Multiplikativne Kleenejeve algebre sa inverzijom

Neka je za bilo koji skup A, $\mathbf{UFRel}^{\vee}(A)$ algebra koja se dobija od $\mathbf{UFRel}(A)$ proširivanjem operacijom inverzije relacija, tj.

$$\mathbf{UFRel}^{\vee}(A) = \langle \mathcal{P}(A \times A), \circ, {}^{\mathrm{rtc}}, {}^{\vee}, \emptyset, \Delta_A \rangle.$$

Varijetet generisan ovim algebrama označavamo sa $\mathcal{UF}^{\vee}$. Njegovi članovi su *multiplikativne Kleenejeve algebre sa inverzijom.*

Imajući u vidu Teoremu 4.1.6, prirodno je odmah postaviti

PROBLEM 7. *Da li je $\mathcal{UF}^{\vee}$ relativno konačno baziran nad $\mathcal{UF}$? Ako jeste, odrediti jednu konačnu relativnu bazu identiteta za navedene varijetete.*

S druge strane, može se pokazati da varijetet generisan *multiplikativnim algebrama jezika sa inverzijom* $\mathbf{UFLang}_{\Sigma}^{\vee}$ (koje se dobijaju od $\mathbf{UFLang}_{\Sigma}$ dodavanjem operacije inverza jezika) ima konačnu bazu identiteta nad $\mathcal{UF}$. Dovoljno je uzeti u obzir involucijske aksiome $(xy)^{\vee} = y^{\vee}x^{\vee}$, $(x^*)^{\vee} = (x^{\vee})^*$, $0^{\vee} = 0$ (pri čemu iz poslednja dva identiteta i $0^* = 1$ sledi $1^{\vee} = 1$).

Ukoliko bismo našli konačnu aksiomatizaciju $\mathcal{UF}^{\vee}$ nad $\mathcal{UF}$ koja se traži u gornjem problemu, mogli bismo lako, adaptacijom metoda prikazanih u ovoj i prethodnoj glavi, dokazati da varijetet $\mathcal{UF}^{\vee}$ takođe nema konačnu jednakosnu bazu. Međutim, u ovom poglavlju ćemo pokazati upravo to tvrđenje čak i bez poznavanja rešenja Problema 7. Kako bismo mogli da ga "zaobiđemo", biće nam ponovo potrebna specijalna klasa uopštenih Conwayevih modela (različita od one upotrebljene u prethodnoj glavi), koju ćemo dobiti komponovanjem dve konačne grupe.

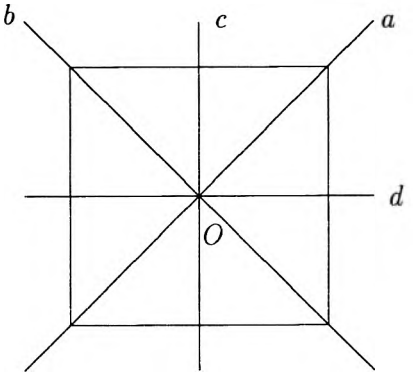
Označimo sa $\mathbf{D}(p, q)$ uopšteni Conwayev model $\mathbf{M}_T(Z_{pq}, D_4)$, koji je uz to proširen involutivnom operacijom ${}^{\vee}$, kao što sledi. Ovde je Z_{pq} (kao i ranije)

ciklična grupa reda pq, gde su $p < q$ prosti brojevi, dok je D_4 grupa simetrija kvadrata, *diedarska grupa stepena 4*. Podsetimo se da su elementi grupe D_4 osne simetrije u odnosu na prave a, b, c, d (vidi sliku), rotacije $\rho_O^{\frac{\pi}{2}}$ i $\rho_O^{-\frac{\pi}{2}}$ oko O za ugao $\pm\frac{\pi}{2}$, centralna simetrija u odnosu na O i identičko preslikavanje u ravni (dakle, ukupno osam elemenata). Osne simetrije $\sigma_a, \sigma_b, \sigma_c$ i σ_d generišu ciklične podgrupe od D_4 reda 2. Primetimo da podgrupe $H_a = \langle\langle \sigma_a \rangle\rangle$ i $H_c = \langle\langle \sigma_c \rangle\rangle$ ne komutiraju, pošto je

$$\sigma_a \circ \sigma_c = \rho_O^{\frac{\pi}{2}}$$

i

$$\sigma_c \circ \sigma_a = \rho_O^{-\frac{\pi}{2}}.$$



Neka je $T_{\{1\}} = \emptyset$, $T_{Z_p} = H_a$, $T_{Z_q} = H_c$ i $T_{Z_{pq}} = D_4$. Najzad, operacija $^\vee$ je definisana isto kao i u prethodnom poglavlju:

$$A^\vee = \{a^{-1} : a \in A\},$$

gde a^{-1} označava grupni inverz elementa $a \in Z_{pq} \cup D_4$ (već prema tome da li $a \in Z_{pq}$, ili $a \in D_4$).

Kako je pridruživanje T definisano u $\mathbf{D}(p, q)$ tako da je odgovarajući uopšteni Conwayev model *-monoton, stabilan na konjugaciju i ω-idempotentan, odmah se dobija

LEMA 4.4.1. $\mathbf{D}(p, q)$ *zadovoljava identitete* ω*-idempotentnih Conwayevih* **-poluprstena.*

Primetimo da smo malopre opisano proširenje uopštenog Conwayevog modela involutivnom operacijom $^\vee$ mogli da jednako izvedemo i na svakom drugom uopštenom Conwayevom modelu u kojem je "polugrupni deo" takođe

grupa (ili, još opštije, polugrupa na kojoj se može definisati neki antiautomorfizam). Na taj način se dobija model $\mathbf{M}_T^{\vee}(G,H)$.

PROPOZICIJA 4.4.2. *Neka su G, H proizvoljne konačne grupe. Tada svaki involutivni uopšteni Conwayev model oblika $\mathbf{M}_T^{\vee}(G,H)$ zadovoljava identitete* (13)–(16) *i* (19).

Dokaz. Kako je operacija $^{\vee}$ definisana kao tačkasta primena grupnog inverza, identiteti (14) i (16) slede kao posledice dobro poznatih identiteta grupa, dok je identitet (13) očigledan. Stoga preostaje da se provere identiteti (15) i (19).

Pretpostavimo prvo da je $A \subseteq G$. Tada sledi

$$(A^*)^{\vee} = (\langle\!\langle A \rangle\!\rangle \cup T_{\langle\!\langle A \rangle\!\rangle})^{\vee} = \langle\!\langle A \rangle\!\rangle^{\vee} \cup T^{\vee}_{\langle\!\langle A \rangle\!\rangle} = \langle\!\langle A \rangle\!\rangle \cup T_{\langle\!\langle A \rangle\!\rangle} = A^*,$$

pošto za svaku grupu K (pa tako i za svaku podgrupu od H) važi $K^{\vee} = K$. Kako A i $A^{\vee}$ generišu istu podgrupu od G, imamo

$$(A^{\vee})^* = A^*.$$

Posmatrajmo sada opšti slučaj. Tada je

$$\begin{aligned}(A^*)^{\vee} &= \langle (A \cap H) \cup (A \cap G)^* \rangle^{\vee} = \langle (A \cap H)^{\vee} \cup ((A \cap G)^*)^{\vee} \rangle = \\ &= \langle (A^{\vee} \cap H) \cup (A^{\vee} \cap G)^* \rangle = (A^{\vee})^*,\end{aligned}$$

pošto se lako proverava da u polugrupi G^H važi $\langle B \rangle^{\vee} = \langle B^{\vee} \rangle$ za sve $B \subseteq G \cup H$.

Konačno, za sve $A \subseteq G \cup H$ imamo

$$\begin{aligned}A &= \{a : a \in A\} = \{aa^{-1}a : a \in A\} \subseteq \\ &\subseteq \{a : a \in A\}\{a^{-1} : a \in A\}\{a : a \in A\} = AA^{\vee}A,\end{aligned}$$

što pokazuje tvrđenje za identitet (19). ∎

TEOREMA 4.4.3. *Ne postoji konačan skup identiteta koji važe na $\mathcal{KA}^{\vee}$ iz kojeg se mogu izvesti svi identiteti od jedne promenljive koji važe na $\mathcal{UF}^{\vee}$. Stoga varijetet $\mathcal{UF}^{\vee}$ nema konačnu bazu identiteta.*

Dokaz. Analogno kao i u dokazu Teoreme 3.3.3, pretpostavka da $\mathcal{UF}^{\vee}$ ima konačnu bazu vodi zaključku da se iz aksioma ω-idempotentnih Conwayevih *-poluprstena, (13)–(16), (19) i grupnog matričnog identiteta $P(S_n)$, za dovoljno veliko n, može izvesti cela jednakosna teorija $Eq(\mathcal{KA}^{\vee})$. Ali tada, po Lemi

4.4.1, Propoziciji 4.4.2 i Propoziciji 3.3.2, $\mathbf{D}(p, q)$ je model za sve pobrojane identitete. Međutim, u ovom modelu ne važi

$$(x^p)^*(x^q)^* = (x^q)^*(x^p)^*$$

(što očito važi na $\mathcal{UF}^\vee$), jer se za interpretaciju $x \mapsto a$, (gde je a generator ciklične grupe Z_{pq}) dobija $Z_{pq} \cup H_c H_a$ na levoj strani (jer je $H_a \cup H_c \cup H_c H_a = H_c H_a$), dok desna strana ima vrednost $Z_{pq} \cup H_a H_c$. Ali, kao što smo primetili, imamo $H_a H_c \neq H_c H_a$, pa dobijena kontradikcija okončava dokaz. ∎

Prethodni dokaz se može prepraviti tako da se dobije

TEOREMA 4.4.4. *Varijetet generisan multiplikativnim algebrama jezika sa inverzijom* $\mathbf{UFLang}_\Sigma^\vee$ *nema konačnu bazu identiteta.*

Primetimo da je u gornjem dokazu suštinska bila jedino činjenica da D_4 ima dve nekomutirajuće podgrupe. Na taj način, gornji dokaz smo mogli izvesti uz pomoć bilo koje konačne grupe sa ovom osobinom; međutim, opredelili smo se za D_4, jer je reč o grupi sa *najmanjim* brojem elemenata koja ima dve nekomutirajuće podgrupe (vidi [45], strane 203–204).

Već smo u prvoj glavi napomenuli da se celokupna teorija algebri jezika i, specijalno, regularnih jezika, može uopštiti na komplekse proizvoljnog monoida i njegove regularne podskupove. Takođe, možemo posmatrati algebre $\mathbf{M}(S)$ (gde je S monoid) kao analogone algebri jezika (koje se pokalapaju sa $\mathbf{M}(\Sigma^*)$). Varijetet generisan klasom ovakvih algebri svakako je podvarijetet od $\mathcal{KA}$. U ovoj glavi ćemo posmatrati slučaj kada radimo sa kompleksima i regularnim podskupovima slobodnih *komutativnih* monoida nad nekom azbukom Σ. Te monoide ćemo označavati sa $\Sigma^{\oplus}$.

Komutativna reč nad azbukom Σ je proizvoljni element monoida $\Sigma^{\oplus}$. Jasno, ako je $\Sigma = \{a_1, a_2, a_3, \ldots\}$, i ako se u komutativnoj reči $w \in \Sigma^{\oplus}$ pojavljuju slova $a_1, \ldots, a_n$, tada imamo veoma prirodno kanoničko predstavljanje za w:

$$w = a_1^{k_1} \ldots a_n^{k_n},$$

gde su $k_1, \ldots, k_n \geq 1$ prirodni brojevi. *Komutativni jezik* L nad Σ je sada proizvoljan skup komutativnih reči, odnosno, proizvoljan podskup $L \subseteq \Sigma^{\oplus}$.

Ovde moramo skrenuti pažnju na izvesnu terminološku nepravilnost u gornjim definicijama. Naime, komutativne reči (jezici), strogo uzev, *nisu* reči (jezici) u smislu definicija sa početka disertacije. Redko [135] i Conway [40] koriste izraz "komutativni događaj" umesto termina "komutativni jezik". Međutim, ovakvu terminologiju je koristio Salomaa u svojoj knjizi [141], i čini se da se (pod njegovim uticajem) ona ustalila u literaturi. Ovde ćemo preuzeti njegove nazive, imajući stalno u vidu da se pri tome "reč" i "jezik" ne upotrebljavaju u smislu višeg rodnog pojma.

5.1. Identiteti komutativnih jezika

Algebra komutativnih jezika nad azbukom Σ je algebra

$$\mathbf{CLang}(\Sigma) = \langle \mathcal{P}(\Sigma^{\oplus}), +, \cdot, ^*, \emptyset, \{\lambda\} \rangle,$$

gde je + skupovna unija, · prozivod kompleksa određen komutativnim množenjem u monoidu $\Sigma^{\oplus}$, a * iteracija komutativnih jezika definisana sa

$$L^* = \bigcup_{n \geq 0} L^n,$$

pri čemu je ponovo $L^0 = \{\lambda\}$. Varijetet generisan svim algebrama komutativnih jezika (lako se vidi da je dovoljno uzeti samo one konstruisane nad najviše prebrojivom azbukom) označavamo sa $\mathcal{CL}$. Može se pokazati da se $\mathcal{CL}$ poklapa sa varijetetom koji je generisan svim komutativnim standardnim Kleenejevim algebrama binarnih relacija. Međutim, veze varijeteta $\mathcal{CL}$ sa Kleenejevim relacionim algebrama nisu toliko transparentne kao u slučaju "velikog" varijeteta $\mathcal{KA}$, pa ćemo se ovde mnogo više oslanjati na komutativne jezike.

Podalgebru od $\mathbf{CLang}(\Sigma)$ generisanu sa $\{a\}$, $a \in \Sigma$ (ili, ekvivalentno, konačnim komutativnim jezicima), označavamo sa $\mathbf{CReg}(\Sigma)$, a njene elemente zovemo *komutativnim regularnim jezicima.* Reč je o slikama običnih regularnih jezika nad Σ u odnosu na homomorfizam $\mathbf{Reg}(\Sigma) \to \mathbf{CLang}(\Sigma)$ koji je određen homomorfizmom monoida $\Sigma^* \to \Sigma^{\oplus}$ koji fiksira slova iz Σ. Primetimo da ako je $|\Sigma_1| = 1$, tada je $\mathbf{CLang}(\Sigma_1) = \mathbf{Lang}(\Sigma_1)$ i, sledstveno tome, $\mathbf{CReg}(\Sigma_1) = \mathbf{Reg}(\Sigma_1)$ (u daljem ćemo, za proizvoljan kardinalni broj κ, koristiti notaciju Σ_κ kako bismo označili azbuku sa κ slova).

Imitacijom dokaza Kozen-Németijeve teoreme, možemo pokazati da važi njen komutativni analogon.

PROPOZICIJA 5.1.1. $\mathbf{CReg}(\Sigma)$ *je* $\mathcal{CL}$*-slobodna algebra nad* Σ*, slobodno generisana preslikavanjem* $a \mapsto \{a\}$, $a \in \Sigma$.

Gornja propozicija i primedba pre nje imaju jednu interesantnu posledicu. Za proizvoljan varijetet $\mathcal{V}$, sa $Eq_n(\mathcal{V})$ ćemo označiti onaj deo jednakosne teorije $Eq(\mathcal{V})$ čiji identiteti sadrže najviše n promenljivih.

POSLEDICA 5.1.2. $Eq_1(\mathcal{CL}) = Eq_1(\mathcal{KA})$.

Dokaz. Dokaz sledi neposredno iz prethodne propozicije, Kozen-Németijeve teoreme, jednakosti $\mathbf{CReg}(\Sigma_1) = \mathbf{Reg}(\Sigma_1)$ i činjenice da za proizvoljan varijetet $\mathcal{V}$, skup X i prirodan broj n takav da je $|X| \geq n$, važi $Eq_n(\mathbf{F}_{\mathcal{V}}(X)) = Eq_n(\mathcal{V})$. ∎

Redko [134], Conway [40] i Krob [93] daju (istu, ali sa različitim dokazima) jednakosnu aksiomatizaciju za $Eq_1(\mathcal{KA})$ u okviru $Eq(\mathcal{KA})$, tj. netrivijalnu kolekciju regularnih identiteta iz kojih se mogu izvesti svi regularni

identiteti sa jednom promenljivom. Podsetimo se, grupni matrični identitet $P(Z_p)$ pridružen cikličnoj grupi Z_p prostog reda p je ekvivalentan identitetu

$$(1 + x + \ldots + x^{p-1})(x^p)^* = x^*.$$

Gornji identitet označavamo sa C_p. Identiteti ω-idempotentnih Conwayevih *-poluprstena, zajedno sa identitetima C_p za sve proste brojeve p, nazivaju se *klasične aksiome.*

Teorema 5.1.3. (Redko, [134], Conway, [40, Teorema IV.5], Krob [93, Teorema 14.8]) *Skup posledica klasičnih aksioma sa samo jednom promenljivom je tačno* $Eq_1(\mathcal{KA})$.

U preostalom delu ovog poglavlja prikazujemo glavni rezultat Redkovog rada [135] koji opisuje jednu bazu identiteta za varijetet $\mathcal{CL}$. Treba pomenuti da je Redkov dokaz imao grešku, koju je primetio i korigovao Pilling [120]. Pillingova ispravka je u formi rukopisa bila dostupna još krajem šezdesetih godina Conwayu, pa se ispravljen dokaz pojavio već u [40]. Ovde je prezentiran upravo taj dokaz, prilagođen našem pojmovnom aparatu i notaciji. U narednom poglavlju ćemo pokazati da $\mathcal{CL}$ nema konačnu bazu identiteta, tako da *svaka* baza za $\mathcal{CL}$ mora biti beskonačna.

Posmatrajmo identitete

$$xy = yx, \tag{22}$$
$$x^*y^* = (xy)^*(x^* + y^*). \tag{23}$$

Skup koji se sastoji od klasičnih aksioma i ova dva identiteta označićemo sa Θ_{CL}. Primetimo da iz Θ_{CL} sledi

$$x^*y^* = (x^*)^*(y^*)^* = (x^*y^*)^*(x^* + y^*) \geq (x^*y^*)^* = (x + y)^* \geq x^*y^*$$

(podsetimo se, $r \leq s$ je skraćeni zapis za $r + s = s$), odakle dobijamo

$$(x + y)^* = x^*y^*. \tag{24}$$

Dalje, odavde imamo

$$(x^*y)^* = 1 + (x^*y)^*x^*y = 1 + (x + y)^*y = 1 + x^*y^*y. \tag{25}$$

Primetimo da se, uz pomoć klasičnih aksioma, iz identiteta C_p mogu izvesti identiteti

$$(1 + x + \ldots + x^{n-1})(x^n)^* = x^*,$$

za sve $n \geq 1$. Gornji identitet označavamo sa C_n. Ako uvedemo skraćenu oznaku $x^{<n} \equiv 1 + x + \ldots + x^{n-1}$, tada C_n pišemo kao $x^{<n}(x^n)^* = x^*$. Induktivnim putem, iz Θ_{CL} se sada za svaki niz prirodnih brojeva $\mathbf{n} = \langle n_1, \ldots, n_k \rangle$, $k \geq 1$, može dobiti identitet $C_{\mathbf{n}}$:

$$x_1^* \ldots x_k^* = (x_1^{n_1} \ldots x_k^{n_k})^* (x_1^{<n_1} x_2^* \ldots x_k^* + \ldots + x_1^* \ldots x_{k-1}^* x_k^{<n_k}).$$

Za (komutativni) regularni izraz r nad Σ kažemo da je u *normalnoj formi* ako je r zbir izraza oblika $uv_1^* \ldots v_n^*$, gde su $u, v_1, \ldots, v_n$ reči nad Σ.

LEMA 5.1.4. *Svaki komutativni regularni izraz je Θ_{CL}-ekvivalentan nekom komutativnom regularnom izrazu u normalnoj formi (tj. iz Θ_{CL} se može izvesti identitet u kome učestvuju uočeni izraz i neki izraz u normalnoj formi).*

Dokaz. Putem (24) eliminišemo sva pojavljivanja simbola + pod dejstvom zvezde, dok korišćenjem (22) i (25) uklanjamo zvezde na koje deluju druge zvezde. Nakon ovih transformacija, svaki "zvezdirani" izraz je reč, pa se normalna forma dobija primenom komutativnog zakona (22). ∎

Za (komutativne) reči $w_1, \ldots, w_n$ kažemo da su *nezavisne* ako iz

$$w_1^{\alpha_1} \ldots w_n^{\alpha_n} \equiv w_1^{\beta_1} \ldots w_n^{\beta_n}$$

sledi $\alpha_i = \beta_i$ za sve $1 \leq i \leq n$. Normalna forma je *nezavisna* ako su za svaki njen sabirak $uv_1^* \ldots v_n^*$, reči $v_1, \ldots, v_n$ nezavisne.

LEMA 5.1.5. *Svaki komutativni regularni izraz je Θ_{CL}-ekvivalentan nekoj nezavisnoj normalnoj formi.*

Dokaz. Pretpostavimo da se u normalnoj formi datog izraza nalazi sabirak $uv_1^* \ldots v_n^*$, pri čemu su reči $v_1, \ldots, v_n$ zavisne. Tada ih možemo prenumerisati tako da ta zavisnost glasi $v_1^\alpha v_2^\beta \ldots = v_r^\gamma v_{r+1}^\delta \ldots$ za neko $r \geq 1$ i eksponente $\alpha, \beta, \gamma, \delta, \ldots$ koji nisu svi nula. Ako označimo $\mathbf{n} = \langle \alpha, \beta, \ldots \rangle$ i $\mathbf{m} = \langle \gamma, \delta, \ldots \rangle$, tada redom iz identiteta $C_{\mathbf{n}}$ i $C_{\mathbf{m}}$ dobijamo

$$v_1^* v_2^* \ldots = (v_1^\alpha v_2^\beta \ldots)(v_1^{<\alpha} v_2^* \ldots + v_1^* v_2^{<\beta} \ldots + \ldots)$$

i

$$v_r^* v_{r+1}^* \ldots = (v_r^\gamma v_{r+1}^\delta \ldots)(v_r^{<\gamma} v_{r+1}^* \ldots + v_r^* v_{r+1}^{<\delta} \ldots + \ldots).$$

Množenjem ova dva identiteta, korišćenjem komutativnog zakona (22) i identiteta $x^* x^* = x^*$, a zatim i množenjem sa u, dobijamo zbir Θ_{CL}-ekvivalentan izrazu $uv_1^* \ldots v_n^*$ u kojem svaki od sabiraka ima manje od n reči pod dejstvom zvezde. Upravo opisani postupak se nastavlja (jasno, on se na datu normalnu formu može primeniti samo konačno mnogo puta) sve dok ne dobijemo nezavisnu normalnu formu. ∎

Do kraja poglavlja ćemo fiksirati komutativni izraz

$$t = t_0 t_1^* \dots t_m^*,$$

takav da su reči $t_1, \dots, t_m$ nezavisne. Zatim, primetimo da se svaka reč nad azbukom $\Sigma_M = \{a_1, \dots, a_M\}$ (koju ćemo takođe smatrati fiksiranom) $w = a_1^{\alpha_1} \dots a_M^{\alpha_M}$ može identifikovati sa uređenom M-torkom nenegativnih celih brojeva $\langle \alpha_1, \dots, \alpha_M \rangle$. Na taj način, komutativne reči jesu elementi skupa ω^M, a komutativni jezici – podskupovi ovog skupa. Naravno, na ovom skupu se može definisati struktura polumodula nad jediničnim poluprstenom $\langle \omega, +, \cdot, 0, 1 \rangle$; međutim, opisane nizove brojeva možemo posmatrati i kao specijalne elemente vektorskog prostora

$$\mathbf{Q}^M = \underbrace{\mathbf{Q} \oplus \dots \oplus \mathbf{Q}}_{M}$$

dimenzije M nad poljem racionalnih brojeva $\mathbf{Q}$. Formalno, elementima ovog vektorskog prostora bismo mogli pridružiti pojam *razlomljene reči*, u kojima su eksponenti α_i proizvoljni racionalni brojevi (pri čemu smo prešli na multiplikativno-eksponencijalnu notaciju). Primetimo da u tom smislu nezavisne reči $t_1, \dots, t_m$ zaista predstavljaju skup linearno nezavisnih vektora, jer ako je u $\mathbf{Q}^M$ neka netrivijalna racionalna linearna kombinacija vektora (u ovom slučaju $t_1, \dots, t_m$) jednaka nuli, od nje se lako dobija celobrojna linearna kombinacija, koja, opet, lako daje neku relaciju zavisnosti sa nenegativnim koeficijentima, što predstavlja upravo zavisnost u smislu zavisnosti reči. Stoga se skup reči $t_1, \dots, t_m$ može dopuniti do baze $t_1, \dots, t_m, t_{m+1}, \dots, t_M$ prostora $\mathbf{Q}^M$, u odnosu na koju svaka "razlomljena" (pa tako i obična komutativna) reč w ima jedinstvenu reprezentaciju

$$w = t_1^{\alpha_1} \dots t_m^{\alpha_m} t_{m+1}^{\alpha_{m+1}} \dots t_M^{\alpha_M},$$

gde je za sve $1 \leq i \leq M$, $\alpha_i \in \mathbf{Q}$. Komutativna reč w je *t_i-pozitivna*, *t_i-nula*, odnosno *t_i-negativna* za $1 \leq i \leq M$, prema tome da li je redom $\alpha_i > 0$, $\alpha_i = 0$, ili $\alpha_i < 0$. Izraz $uv_1^* \dots v_n^*$ je *t_i-mešovit* ako među rečima $v_1, \dots, v_n$ ima i t_i-pozitivnih, i t_i-negativnih. U suprotnom, taj izraz je *t_i-nemešovit*. On je *nemešovit* ako je t_i-nemešovit za sve $1 \leq i \leq M$.

LEMA 5.1.6. *Svaki izraz oblika $uv_1^* \dots v_n^*$ se može Θ_{CL}-ekvivalentno predstaviti kao zbir nemešovitih sabiraka.*

Dokaz. Pretpostavimo, na primer, da je dati izraz t_1-mešovit; bez ograničenja opštosti razmatranja, pretpostavimo da je reč v_1 t_1-pozitivna, dok je v_2

t_1-negativna reč. Tada je za pogodne *prirodne* brojeve a, b reč $v_1^a v_2^b$ t_1-nula. Sada zamenimo sabirak $uv_1^* v_2^* \dots v_n^*$ Θ_{CL}-ekvivalentnim izrazom

$$u(v_1^a v_2^b)^*(v_1^{<a} v_2^* + v_1^* v_2^{<b}) \dots v_n^*.$$

Time je prethodni sabirak zamenjen sa dva koji sadrže isti broj simbola *, ali je pri tome povećan broj t_1-nula reči po sabirku. Jasno, ovaj postupak zamene se mora završiti nakon konačno mnogo koraka, pa ćemo doći do Θ_{CL}-ekvivalentnog predstavljanja početnog izraza kao zbira t_1-nemešovitih sabiraka. Dalje, na dobijeni prikaz primenjujemo isti postupak za dobijanje redom $t_2, \dots, t_M$-nemešovitih zbirova. Kako t_i-nemešoviti sabirci ostaju t_i-nemešoviti prilikom primene postupka za konstrukciju t_j-nemešovitog predstavljanja ($j > i$), na kraju opisanog algoritma se dobija zbir sabiraka koji su t_i-nemešoviti za sve $1 \leq i \leq M$. ∎

Ako su r_1, r_2 dva (komutativna) regularna izraza, pisaćemo $r_1 \cap r_2 = s$ ako izraz s predstavlja (komutativni) jezik jednak preseku (komutativnih) jezika predstavljenih izrazima r_1 i r_2 (vidi Teoremu 1.1.8).

LEMA 5.1.7. *Svaki nemešovit izraz $w = uv_1^* \dots v_n^*$, sa t_i-negativnom zvezdiranom reči ($1 \leq i \leq M$) ili t_j-pozitivnom zvezdiranom reči ($m+1 \leq j \leq M$) se može Θ_{CL}-ekvivalentno prikazati kao zbir nemešovitih izraza w_ℓ od kojih svaki ili ima manje zvezdiranih reči od w, ili zadovoljava $w_\ell \cap t = 0$.*

Dokaz. Pođimo od pretpostavke da je, recimo, reč v_1 t_1-negativna. Predstavimo reči t_0, v_1, u u bazi $t_1, \dots, t_M$ prostora $\mathbf{Q}^M$:

$$\begin{aligned} t_0 &= t_1^{\alpha_1} \dots t_M^{\alpha_M}, \\ v_1 &= t_1^{\beta_1} \dots t_M^{\beta_M}, \\ u &= t_1^{\gamma_1} \dots t_M^{\gamma_M}. \end{aligned}$$

Primetimo da eksponent koji odgovara baznom vektoru t_1 u prikazu reči $uv_1^{\ell_1} \dots v_n^{\ell_n}$ (koja pripada komutativnom jeziku kojeg predstavlja izraz w) nije veći od $\beta_1 \ell_1 + \gamma_1$, dok je odgovarajući eksponent u razvoju bilo koje reči iz komutativnog jezika predstavljenog izrazom t bar α_1. Kako je po pretpostavci $\beta_1 < 0$, za dovoljno veliko ℓ_1 imaćemo da komutativna reč $uv_1^{\ell_1} \dots v_n^{\ell_n}$ ne pripada komutativnom jeziku kojeg predstavlja t. U tom slučaju, izraz $w_{\ell_1} = uv_1^{\ell_1} v_1^* \dots v_n^*$ zadovoljava $w_{\ell_1} \cap t = 0$. Zamenimo sada w zbirom

$$uv_1^{\ell_1} v_1^* \dots v_n^* + uv_1^{<\ell_1} v_2^* \dots v_n^*.$$

Time je lema dokazana u razmatranom slučaju, dok se ostali slučajevi rešavaju analogno. ∎

PROPOZICIJA 5.1.8. *Za svaki komutativni regularni izraz r postoje izrazi r_1, r_2 takvi da $\Theta_{CL} \vdash r = r_1 + r_2$, pri čemu $\Theta_{CL} \vdash r_1 \leq t$ i važi $r_2 \cap t = 0$.*

Dokaz. Koristeći identitete iz Θ_{CL}, razložimo izraz r, po Lemi 5.1.6, na zbir nemešovitih sabiraka, a zatim na taj zbir uzastopno primenjujmo Lemu 5.1.7. Na kraju tog procesa se dobija zbir

$$\sum_{\ell \in I} w_\ell,$$

pri čemu svaki od sabiraka w_ℓ zadovoljava ili $w_\ell \cap t = 0$ (zbir svih ovakvih sabiraka će biti r_2), ili sadrži samo t_i-nenegativne reči za $1 \leq i \leq m$, odnosno samo t_j-nula reči za $m+1 \leq j \leq M$. Ali, ako reč v zadovoljava ova poslednja dva uslova, tada postoji prirodan broj k tako da je

$$v^k = t_1^{k_1} \ldots t_m^{k_m},$$

gde su $k_1, \ldots, k_m$ nenegativni *celi* brojevi. Za svaku zvezdiranu (komutativnu) reč v iz napred dobijenog normalnog predstavljanja izraza r, zamenimo (po identitetu C_k) sva pojavljivanja v^* sa $v^{<k}(v^k)^*$. Na taj način smo dobili da svi sabirci $w = uv_1^* v_2^* \ldots$ koje nismo već smestili u r_2 zadovoljavaju $w \cap t \neq 0$ (neka je, na primer, $uv_1^a v_2^b \ldots$ zajednička reč komutativnih jezika predstavljenih izrazima w i t) i svaka od reči $v_1, v_2, \ldots$ je proizvod reči $t_1, \ldots, t_m$ sa nenegativnim celobrojnim eksponentima. U sabircima opisanog tipa, zamenimo $v_1^*, v_2^*, \ldots$ redom sa $v_1^{<a} + v_1^a v_1^*$, $v_2^{<b} + v_2^b v_2^*$, itd. Time se w zamenjuje zbirom izraza sa manjim brojem zvezda od w i izraza

$$w' = uv_1^a v_2^b \ldots v_1^* v_2^* \ldots.$$

Kako su $v_1, v_2, \ldots$ proizvodi reči $t_1, \ldots, t_m$, a $uv_1^a v_2^b \ldots$ pripada komutativnom jeziku kojeg predstavlja t, iz Θ_{CL} lako izvodimo identitet $w' \leq t$. Sada se izraz r_1 formira od sabiraka tipa w' indukcijom po maksimalnom broju zvezda u sabircima koji ne ulaze u izraz r_2. ∎

PROPOZICIJA 5.1.9. *Ako komutativni regularni izrazi r, s redom predstavljaju komutativne jezike R, S takve da je $R \subseteq S$, tada $\Theta_{CL} \vdash r \leq s$.*

Dokaz. Na osnovu Θ_{CL} i Leme 5.1.5, najpre s izražavamo u nezavisnoj normalnoj formi, $s = s_1 + \ldots + s_k$. Po prethodnoj propoziciji, $\Theta_{CL} \vdash r = r_1 + r'$ za neke komutativne izraze r_1, r' takve da $r_1 \leq s_1$ sledi iz Θ_{CL} i $r' \cap s_1 = 0$.

Zatim, r' izražavamo kao $r_2 + r''$, gde $\Theta_{CL} \vdash r_2 \leq s_2$ i $r'' \cap s_2 = 0$. Ponavljajući ovo razmatranje k puta, dobijamo

$$\Theta_{CL} \vdash r = r_1 + r_2 + \ldots + r_k + r^{(k)},$$

gde je za sve $1 \leq i \leq k$, $\Theta_{CL} \vdash r_i \leq s_i$ i $r^{(k)} \cap s_i = 0$. To znači da je

$$r^{(k)} \cap s = 0.$$

Međutim, komutativni jezik predstavljen sa $r^{(k)}$ je sadržan u R, pa $R \subseteq S$ povlači da taj komutativni jezik mora biti prazan, tj. $r^{(k)} = 0$. Otuda očito sledi $\Theta_{CL} \vdash r \leq s$. ∎

TEOREMA 5.1.10. (Redko, [135], Pilling, [120]) Θ_{CL} *je baza identiteta za varijetet* $\mathcal{CL}$.

Dokaz. Neka na svim algebrama komutativnih jezika važi identitet $r = s$. Tada r i s predstavljaju iste komutativne jezike, pa po prethodnoj propoziciji sledi $\Theta_{CL} \vdash r = s$. Obratno, ako se identitet $r = s$ izvodi iz Θ_{CL}, on tada važi na $\mathcal{CL}$, pošto je očito da $\mathcal{CL} \models \Theta_{CL}$. ∎

5.2. Identiteti algebri jezika nad jednoelementnim alfabetom

U prethodnom poglavlju smo videli da se regularni identiteti nad jednoelementnom azbukom poklapaju sa identitetima sa jednom promenljivom koji važe na $\mathbf{CReg}(\Sigma_1) = \mathbf{Reg}(\Sigma_1)$, i oni svi slede iz klasičnih aksioma. Ali, šta je sa celokupnom jednakosnom teorijom $Eq(\mathbf{CReg}(\Sigma_1))$, i uopšte, šta se može reći o jednakosnim teorijama algebri $\mathbf{CReg}(\Sigma_n)$ za $1 \leq n \leq \omega$? Ako su u pitanju algebre (običnih) regularnih jezika, tada imamo sledeću situaciju.

PROPOZICIJA 5.2.1. *Za sve prirodne brojeve* $n \geq 1$, $\mathbf{Reg}(\Sigma_n)$ *se može potopiti u* $\mathbf{Reg}(\Sigma_2)$.

Dokaz. Tvrđenje je jasno za $n = 1, 2$, pa pretpostavimo da je $n > 2$. Neka je $\Sigma_n = \{a_1, \ldots, a_n\}$ i $f : \Sigma_n^* \to \Sigma_2^*$ homomorfizam monoida koji proširuje preslikavanje

$$a_i \mapsto a_2^{i-1} a_1 a_2^{n-i},$$

$1 \leq i \leq n$. Lako se vidi da f dalje indukuje homomorfizam Kleenejevih algebri $f^\sharp : \mathbf{Reg}(\Sigma_n) \to \mathbf{Reg}(\Sigma_2)$ dat sa

$$f^\sharp(L) = \{f(w) : \ w \in L\}.$$

Propozicija će biti dokazana, ako pokažemo da je $f^\sharp$ injektivno preslikavanje. Za to je (potrebno i) dovoljno da pokažemo injektivnost preslikavanja f. Zaista, neka je

$$w_j = a_{k_{j,1}} \dots a_{k_{j,\ell_j}}$$

za $j = 1, 2$. Tada je

$$f(w_j) = a_2^{k_{j,1}-1} a_1 a_2^{n-k_{j,1}+k_{j,2}-1} a_1 \dots a_1 a_2^{n-k_{j,\ell_j-1}+k_{j,\ell_j}-1} a_1 a_2^{n-k_{j,\ell_j}}.$$

Stoga iz $f(w_1) = f(w_2)$ sledi $\ell_1 = \ell_2 = \ell$, kao i:

$$\begin{aligned} k_{1,1} - 1 &= k_{2,1} - 1, \\ n - k_{1,1} + k_{1,2} - 1 &= n - k_{2,1} + k_{2,2} - 1, \\ &\vdots \\ n - k_{1,\ell-1} + k_{1,\ell} - 1 &= n - k_{2,\ell-1} + k_{2,\ell} - 1, \\ n - k_{1,\ell} &= n - k_{2,\ell}. \end{aligned}$$

Gornji sistem očito daje $k_{1,m} = k_{2,m}$ za sve $1 \leq m \leq \ell$, pa je $w_1 = w_2$, što je i trebalo pokazati. ∎

TEOREMA 5.2.2. (Salomaa, [141, Teorema III.3.1]) *Za sve $n \geq 2$ je*

$$Eq(\mathbf{Reg}(\Sigma_n)) = Eq(\mathcal{KA}).$$

Dokaz. Očito za sve $n \geq 2$ imamo $Eq(\mathbf{Reg}(\Sigma_2)) \supseteq Eq(\mathbf{Reg}(\Sigma_n))$, a zbog prethodne propozicije je zapravo $Eq(\mathbf{Reg}(\Sigma_2)) = Eq(\mathbf{Reg}(\Sigma_n))$. Međutim, odavde je

$$Eq_k(\mathbf{Reg}(\Sigma_2)) = Eq_k(\mathbf{Reg}(\Sigma_n))$$

za sve $k \geq 0$, pa imamo

$$\begin{aligned} Eq(\mathcal{KA}) &= \bigcup_{n<\omega} Eq_n(\mathcal{KA}) = \bigcup_{n<\omega} Eq_n(\mathbf{Reg}(\Sigma_n)) = \\ &= \bigcup_{n<\omega} Eq_n(\mathbf{Reg}(\Sigma_2)) = Eq(\mathbf{Reg}(\Sigma_2)), \end{aligned}$$

što se i tražilo. ∎

POSLEDICA 5.2.3. *Varijetet Kleenejevih algebri $\mathcal{KA}$ je generisan (ponaosob) svakom od algebri $\mathbf{Reg}(\Sigma_\kappa)$, $\mathbf{Lang}(\Sigma_\kappa)$, za sve $\kappa \geq 2$.*

U radu [44] je pokazano da je situacija slična u slučaju komutativnih jezika. Štaviše, ispostavilo se da je lanac jednakosnih teorija

$$Eq(\mathbf{CReg}(\Sigma_1)) \supseteq Eq(\mathbf{CReg}(\Sigma_2)) \supseteq \ldots Eq(\mathbf{CReg}(\Sigma_\omega)) = Eq(\mathcal{CL})$$

trivijalan, tj. da u njemu figurišu sve jednakosti (tako je $Eq(\mathbf{Reg}(\Sigma_1))$ jednakosna teorija algebri komutativnih jezika, dok je $Eq(\mathbf{Reg}(\Sigma_2))$ već cela teorija algebri jezika, tj. skup svih regularnih identiteta). Time je rešen trideset godina star Problem III.5.1 koji je postavio Salomaa u [141].

PROPOZICIJA 5.2.4. *Za sve prirodne brojeve* $n \geq 1$ *je*

$$\mathbf{CReg}(\Sigma_n) \in \mathsf{ISP}(\mathbf{CReg}(\Sigma_1)).$$

Dokaz. Pokažimo najpre da se za sve $n \geq 1$ algebra $\mathbf{CReg}(\Sigma_{n+1})$ može potopiti u direktan stepen algebre $\mathbf{CReg}(\Sigma_n)$ (gde je $\Sigma_n = \{a_1, \ldots, a_n\}$). Neka je za sve $m \geq 0$, $h_m : \mathbf{CReg}(\Sigma_{n+1}) \to \mathbf{CReg}(\Sigma_n)$ homomorfizam Kleenejevih algebri, jedinstveno određen preslikavanjem

$$\begin{aligned} \{a_0\} &\mapsto \{a_0^m\}, \\ \{a_1\} &\mapsto \{a_0^{m+1}\}, \\ \{a_i\} &\mapsto \{a_{i-1}\}, \quad 2 \leq i \leq n. \end{aligned}$$

To znači da je za sve $L \subseteq \Sigma_{n+1}^{\oplus}$, $h_m(L)$ skup svih komutativnih reči koje se dobijaju od komutativnih reči iz L zamenom svakog pojavljivanja slova a_0 sa a_0^m, slova a_1 sa a_0^{m+1}, dok se svako pojavljivanje slova a_i, $2 \leq i \leq n$, zamenjuje sa a_{i-1}. Definišimo homomorfizam $h : \mathbf{CReg}(\Sigma_{n+1}) \to (\mathbf{CReg}(\Sigma_n))^\omega$ sa

$$h(L) = \langle h_m(L) \rangle_{m<\omega}.$$

Ako je $L \neq L'$, tada postoji komutativna reč $u \in \Sigma^{\oplus}$ koja leži npr. u $L \setminus L'$. Neka je ta reč baš $u = a_0^p a_1^q a_2^{\alpha_2} \ldots a_n^{\alpha_n}$. Neka je m prirodan broj za koji je $m > p + q$. Sledi da je

$$a_0^{mp+(m+1)q} a_1^{a_2} \ldots a_{n-1}^{a_n} \in h_m(L).$$

Pretpostavimo da gornja komutativna reč pripada $h_m(L')$. Tada je ona dobijena kao homomorfna slika neke reči $v \in L'$ $(v \neq u)$, $v = a_0^r a_1^s a_2^{\beta_2} \ldots a_n^{\beta_n}$. U tom slučaju, imamo $\alpha_i = \beta_i$ za sve $2 \leq i \leq n$, kao i

$$m(p+q) + q = m(r+s) + s.$$

Stoga, ako je $p+q < r+s$, tada je $q \geq m$, kontradikcija. Međutim, ako je $p+q > r+s$, tada je $s \geq m$, pa sledi

$$m(p+q)+q \geq m^2.$$

Ali, tada zbog $q < m$ imamo $p+q \geq m$, što je suprotno našoj pretpostavci. Zato je $p+q = r+s$, odakle dobijamo $q = s$ i $p = r$. Odatle je $h_m(L) \neq h_m(L')$, tj. $h(L) \neq h(L')$, što znači da je preslikavanje h injektivno.

Sada se dokaz tvrđenja propozicije okončava rutinskim induktivnim argumentom. ∎

Prethodni dokaz se može upotrebiti i da bi se pokazalo da za sve prirodne brojeve $n \geq 1$ važi $\mathbf{CLang}(\Sigma_n) \in \mathsf{ISP}(\mathbf{CLang}(\Sigma_1))$.

TEOREMA 5.2.5. (Crvenković, Dolinka, Ésik, [44]) *Za sve $n \geq 1$ je*

$$Eq(\mathbf{CReg}(\Sigma_n)) = Eq(\mathcal{CL}).$$

Dokaz. Dovoljno je pokazati da se algebra $\mathbf{CReg}(\Sigma_\omega)$ (koja očito generiše $\mathcal{CL}$) može potopiti u direktan stepen algebre $\mathbf{CReg}(\Sigma_1)$. Za sve prirodne brojeve $n \geq 1$, neka je $h_n : \mathbf{CReg}(\Sigma_\omega) \to \mathbf{CReg}(\Sigma_n)$ homomorfizam Kleenejevih algebri određen preslikavanjem $\{a_i\} \mapsto \{a_i\}$ za $i < n$ i $\{a_i\} \mapsto \{\lambda\}$ za sve $i \geq n$. Kako se u svakom komutativnom regularnom jeziku nad Σ_ω pojavljuje samo konačno mnogo slova, lako sledi da direktan proizvod ovih funkcija daje injektivni homomorfizam

$$\mathbf{CReg}(\Sigma_\omega) \to \prod_{n<\omega} \mathbf{CReg}(\Sigma_n).$$

Međutim, svaki od faktora $\mathbf{CReg}(\Sigma_n)$ u gornjem direktnom proizvodu se po Propoziciji 5.2.4 potapa u direktan stepen od $\mathbf{CReg}(\Sigma_1)$, pa teorema sledi. ∎

POSLEDICA 5.2.6. *Varijetet $\mathcal{CL}$ je generisan (ponaosob) svakom od algebri $\mathbf{CReg}(\Sigma_\kappa)$, $\mathbf{CLang}(\Sigma_\kappa)$, za sve $\kappa \geq 1$.*

Prema tome, jednakosna teorija algebri komutativnih jezika se poklapa sa jednakosnom teorijom regularnih jezika nad jednoelementnim alfabetom. U Teoremi 5.1.10 je data jedna beskonačna baza za $\mathcal{CL}$ (a time i za $\mathbf{Reg}(\Sigma_1)$). Međutim, da li jednakosna teorija u pitanju možda ima konačnu bazu identiteta? Negativan odgovor na ovo pitanje su nedavno dali Aceto, Fokkink, Ingólfsdóttir u [5], rešivši tako još jedan stari problem iz [141]. Kako bismo

iskazali njihov rezultat, potrebna su nam dva nova pojma vezana za regularne izraze.

Dužina $\ell(r)$ regularnog izraza r (nad azbukom Σ) definiše se induktivno u odnosu na složenost r na sledeći način: dužina svakog slova iz Σ je jednaka 1, dok je

$$\begin{aligned} \ell(0) &= 0, \\ \ell(1) &= 1, \\ \ell(r_1 + r_2) &= \ell(r_1) + \ell(r_2), \\ \ell(r_1 r_2) &= \ell(r_1)\ell(r_2), \\ \ell(r_1^*) &= 1. \end{aligned}$$

Ako sa $\mathsf{var}(r)$ označimo ukupan broj pojavljivanja (ne obavezno različitih) slova iz Σ u regularnom izrazu r, tada je *težina* izraza r broj $2^{\mathsf{var}(r)}\ell(r)$. Sada možemo formulisati glavni rezultat rada [5].

TEOREMA 5.2.7. (Aceto, Fokkink, Ingólfsdóttir, [5]) *Za svaki prost broj p postoji algebra $\mathbf{M}_p$ tipa $\langle 2, 2, 1, 0, 0\rangle$ sa sledećim osobinama:*

(1) za sve proste brojeve q, $\mathbf{M}_p \models C_q$ ako i samo ako $p \neq q$,

(2) svaki identitet $r = s$ koji važi u $\mathbf{Reg}(\Sigma_1)$, pri čemu regularni izrazi r, s imaju težinu manju od p, važi i u $\mathbf{M}_p$.

Ovde ćemo izostaviti tehničke detalje dokaza gornje teoreme, već samo dajemo njegovu ideju tako što ćemo opisati konstrukciju algebre $\mathbf{M}_p$. Nosač ove algebre čine svi podskupovi skupa $p = \{0, 1, \ldots, p-1\}$ i skup prirodnih brojeva ω. Konstante su redom $\emptyset$ i $\{0\}$, dok se $+$ interpretira kao skupovna unija. Dalje, za dva elementa I, J (podsetimo, I, J su skupovi brojeva) definišemo množenje sa

$$I \cdot J = \begin{cases} \omega, & I = \omega, J \neq \emptyset \text{ ili } I \neq \emptyset, J = \omega, \\ (I + J) \bmod p, & \text{inače.} \end{cases}$$

Ovde za skup A, koji se sastoji od prirodnih brojeva, $A \bmod p$ označava skup svih ostataka elemenata iz A pri deljenju sa p. Najzad, unarna operacija je data sa

$$I^* = \begin{cases} \{0\}, & I = \emptyset \text{ ili } I \neq \{0\}, \\ \omega, & \text{inače.} \end{cases}$$

Sada se lako pokazuje da C_p ne važi na $\mathbf{M}_p$: naime, dovoljno je uzeti valuaciju $x \mapsto \{1\}$, jer tada leva strana identiteta C_p ima vrednost $\{0, 1, \ldots, p-1\}$, dok

je vrednost desne strane ω. Takođe, nije teško dokazati da za $q \neq p$, C_q važi na $\mathbf{M}_p$, imajući u vidu da je $(I^q)^* = \omega$ kadgod I sadrži broj različit od 0.

Najznačajnija posledica gornje teoreme je

POSLEDICA 5.2.8. *Algebra* $\mathbf{Reg}(\Sigma_1)$ *nema konačnu bazu identiteta.*

Dokaz. Pretpostavimo da postoji konačna baza identiteta Θ za algebru $\mathbf{Reg}(\Sigma_1)$. Neka je p prost broj veći od težine svih regularnih izraza koji se pojavljuju u identitetima iz Θ. Tada $\mathbf{M}_p$ zadovoljava sve identitete iz Θ, ali ne zadovoljava identitet C_p, koji očito važi u $\mathbf{Reg}(\Sigma_1)$. Kontradikcija. ∎

Kombinovanjem gornje posledice i Teoreme 5.2.5 se neposredno dobija

POSLEDICA 5.2.9. *Varijetet* $\mathcal{CL}$ *nema konačnu bazu identiteta.*

Izlaganje u ovoj glavi završavamo problemom vezanim za pitanja razmotrena u Glavi 3. Naime, neka $\mathbf{UFCLang}(\Sigma)$ označava redukt algebre komutativnih jezika $\mathbf{CLang}(\Sigma)$ koji se dobija uklanjanjem operacije $+$ (*multiplikativne algebre komutativnih jezika*). Sa $\mathcal{UFCL}$ označavamo varijetet generisan opisanim reduktima.

PROBLEM 8. *Da li varijetet* $\mathcal{UFCL}$ *ima konačnu bazu identiteta? Naći neku netrivijalnu bazu za* $\mathcal{UFCL}$.

6.1. Dinamičke logike i algebre u teorijskom računarstvu

Još u prvoj glavi smo napomenuli da operacije Kleenejevih algebri (binarnih relacija) $+, \cdot, ^*$ intuitivno odgovaraju osnovnim konstrukcijama struktuiranog programiranja, kojima se od atomarnih programa dobijaju složeniji. Na taj način, regularni izrazi modeliraju "regularne programe". Međutim, odmah moramo naglasiti da takav pristup predstavlja samo prvu, najgrublju aproksimaciju problema algebarskog modeliranja *stvarnih* struktuiranih programskih jezika, budući da on ima sledeću očiglednu manjkavost: operacije $+, ^*$ odgovaraju *nedeterminističkoj* selekciji (grananju), odnosno *nedeterminističkoj* iteraciji, što znači da ako a, b reprezentuju neke programe, $a + b$ predstavlja slučajan izbor da li će se izvršiti program a ili b, dok a^* odgovara iteraciji programa a proizvoljan (slučajan) broj puta.

Ako za naš "softver" uzmemo najjednostavniji model stukturiranog programskog jezika – `while` *programe* [82, 91, 90], koji se, polazeći od atomarnih programa $a, b, c, \ldots$, grade pomoću sekvence $a; b$, uslovnog grananja

`if` p `then` a `else` b

(gde je p neki iskaz) i petlje

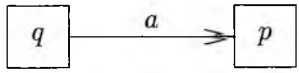
`while` p `do` a

(i, naravno, zagrada `begin`...`end`), tada je jasno da je modeliranje poslednje dve konstrukcije apsolutno nemoguće putem regularnih izraza.

Ono što očito nedostaje jeste *kontrola*, odnosno mogućnost ispitivanja tačnosti Booleovih iskaza (u ovom slučaju p). Prema tome, moramo očekivati da strukture čiji će termi modelirati konstrukciju `while` programa (koji uz ulazno-izlazne procedure i neke druge, manje dodatke već jesu PASCAL) na neki način sadrže kako Kleenejeve algebre, tako i *Booleove algebre*. Booleovu algebru će činiti *iskazi* (npr. o sadržaju registara procesora i memorijskih

lokacija), dok elemente Kleenejeve algebre (ili još opštije, *regularne algebre*, algebre tipa $\langle 2,2,1,0,0\rangle$) treba zamisliti kao *akcije* procesora koje se dešavaju u toku izvršenja programa.

Ovakva razmišljanja vode pojmu *dinamičke algebre*. Naime, akcije (procesora) proizvode nova stanja (registara). Primetimo da smo prethodnom rečenicom dobili novi iskaz; tako, ako a označava neku akciju, a p iskaz (o stanju registara), tada imamo iskaz $\langle a\rangle p$, "akcija a proizvodi p". Pisaćemo $\langle a\rangle p = q$ ako tačnost iskaza q, nakon izvršenja akcije a, povlači tačnost iskaza p, odnosno, ako računar iz stanja q akcijom a prelazi u stanje p:



Prema tome, dinamička algebra će biti dvosortna algebra $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$, gde je $\mathbf{K}$ regularna algebra, $\mathbf{B}$ Booleova algebra, a $\langle\cdot\rangle\cdot : K \times B \to B$ operator "...proizvodi...", pri čemu će biti zadovoljeni neki identiteti. Primetimo da se od algebre $\mathbf{K}$ uopšte ne zahteva da bude Kleenejeva: glavna ideja dinamičkih algebri upravo i jeste u tome da se uz pomoć Booleove algebre $\mathbf{B}$ (preko konačnog skupa identiteta) definišu željene osobine regularnih operacija $+, \cdot, ^*$.

Dinamičke algebre su nezavisno definisali Kozen [83] i Pratt [127] 1979. godine kao algebarske modele *dinamičke iskazne logike*. Ova logika je izučavana i ranije (Fischer, Ladner [61, 62], prvi nagoveštaji Hoare [73], Dijkstra [53], Pratt [126]) i njeno uvođenje bilo je motivisano potragom za odgovarajućim formalno-logičkim sistemom koji bi omogućio matematički tretman strukture imperativnih programskih jezika. Aksiomatiku za ovu logiku dao je Segerberg 1977. godine [148], a jednakosnom transkripcijom tih aksioma došlo se do definišućih identiteta za dinamičke algebre.

Možda najjasniji primer kroz koji se ilustruje kako akcije proizvode iskaze, kao i intuitivnu motivaciju aksioma dinamičkih algebri je dao sam autor teorije, Pratt, u [127], pa ovde preuzimamo njegovo objašnjenje.

Neka, na primer, `x:=5` označava program koji postavlja vrednost promenljive x na 5. Tada iskaz $\langle \mathtt{x} := 5\rangle x = 5$ tvrdi da nakon dodele vrednosti 5 promenljivoj x važi $x = 5$, što je nužno istinit iskaz, pa ćemo pisati

$$\langle \mathtt{x} := 5\rangle x = 5 \;=\; \top.$$

S druge strane, iskaz $\langle \mathtt{x} := \mathtt{x} + 1\rangle x = 5$ je očito ekvivalentan iskazu $x = 4$, jer $x = 5$ može postati tačan iskaz nakon izvršenja komande `x:=x+1` ako i samo ako je prethodno važilo $x = 4$. Najzad,

$$\langle (\mathtt{x} := \mathtt{x} - 1)^*\rangle x = 0 \;=\; x \geq 0,$$

budući da nije moguće da negativan broj uzastopnim umanjivanjem za 1 postane 0.

Naravno, gornja razmatranja zavise od tipa promenljivih u konkretnom programu, aritmetike podataka (u ovom slučaju, celih brojeva) sa kojima radimo, itd. Međutim, možemo uočiti neke opštije zakonitosti ne znajući ništa o karakteru podataka koji se obrađuju u datom programu i detaljima implementacije. Najpre, nijedna akcija (program) ne može proizvesti nijedan drugi iskaz polazeći od kontradiktornog iskaza, tj. očekujemo da važi

$$\langle a\rangle\bot = \bot. \tag{26}$$

Osim toga, program a proizvodi iskaz $p \vee q$ ako i samo ako proizvodi p ili proizvodi q, tj.

$$\langle a\rangle(p \vee q) = \langle a\rangle p \vee \langle a\rangle q. \tag{27}$$

Dalje, ako imamo selekciju akcija $a + b$, ona može proizvesti p ako i samo ako ili a, ili b prozivodi p, što zapisujemo kao

$$\langle a + b\rangle p = \langle a\rangle p \vee \langle b\rangle p. \tag{28}$$

Niz akcija ab proizvodi p ako i samo ako a proizvodi iskaz iz kojeg b može proizvesti p:

$$\langle ab\rangle p = \langle a\rangle\langle b\rangle p. \tag{29}$$

Najzad, po dogovoru, prazna akcija proizvodi svaki iskaz iz kontradikcije:

$$\langle 0\rangle p = \bot, \tag{30}$$

a identička akcija fiksira svaki iskaz:

$$\langle 1\rangle p = p. \tag{31}$$

Pretpostavimo sada da ili važi p, ili pak program a proizvodi situaciju iz koje iteracija akcije a može nakon nekog broja koraka proizvesti p. Tada, jasno, a iteracijom može proizvesti p, odnosno, imamo $p \vee \langle aa^*\rangle p \leq \langle a^*\rangle p$ (pri čemu $p \leq q$ znači da p implicira q, tj. $p \vee q = q$). S druge strane, ako a iteracijom proizvodi p, tada ili već važi p, ili a iteracijom proizvodi stanje u kojem ne važi p, ali *još jedna* primena programa a daje p. Drugim rečima, $\langle a^*\rangle p \leq p \vee \langle a^*\rangle(\neg p \wedge \langle a\rangle p)$. Tako smo dobili dve nejednakosti:

$$p \vee \langle aa^*\rangle p \;\leq\; \langle a^*\rangle p \;\leq\; p \vee \langle a^*\rangle(\neg p \wedge \langle a\rangle p). \tag{32}$$

Gornja aksioma se naziva *aksioma indukcije*. Zaista, ako posmatramo drugu od ovih nejednakosti (tj. njenu kontrapoziciju, dobijenu primenom negacije),

i ako pišemo $[a]p$ umesto $\neg(\langle a\rangle\neg p)$, $p \Rightarrow q$ umesto $\neg p \vee q$ i r umesto $\neg p$, tada ona glasi:

$$r \vee [a^*](r \Rightarrow [a]r) \leq [a^*]r,$$

gde je sada veza sa principom matematičke indukcije jasna. Ovde je operacija $[\cdot]\cdot$ *dual* operacije $\langle\cdot\rangle\cdot$, i $[a]p$ intuitivno znači: "štagod radio program a, p će važiti kada i ako se on izvrši".

Sada možemo dati preciznu definiciju *dinamičke algebre*: reč je o dvosortnoj algebri $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$, gde je $\mathbf{K}$ regularna algebra, $\mathbf{B} = \langle B, \vee, \wedge, \neg, \bot, \top\rangle$ Booleova algebra, pri čemu su zadovoljeni identiteti (26)–(32). Varijetet dinamičkih algebri označavamo sa $\mathcal{DA}$.

Ovde ćemo napraviti jednu malu digresiju u vezi osnovnih algebarskih konstrukcija i pojmova u vezi sa dvosortnim (specijalno, dinamičkim) algebrama. Najpre, primetimo da terme koje formiramo od simbola u tipu dinamičkih algebri možemo podeliti u dve klase, pošto se njihovom interpretacijom mogu dobiti term funkcije kako na regularnoj, tako i na Booleovoj algebri date dinamičke algebre. Stoga ćemo ove terme redom zvati *regularni*, odnosno *Booleovi termi*. Ista podela se odnosi i na identitete, pa govorimo o regularnim i Booleovim identitetima. Na taj način se jednakosna teorija svakog varijeteta $\mathcal{V} \leq \mathcal{DA}$ deli na *regularni deo* $Eq_R(\mathcal{V})$ i *Booleov deo* $Eq_B(\mathcal{V})$.

Direktan proizvod dinamičkih algebri se definiše na očigledan način, primenom operacija po komponentama. *Podalgebra* dinamičke algebre $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ je dinamička algebra $\mathbf{D}' = \langle \mathbf{K}', \mathbf{B}', \langle\cdot\rangle\cdot\rangle$ takva da su $\mathbf{K}', \mathbf{B}'$ redom podalgebre od $\mathbf{K}, \mathbf{B}$ i $\mathbf{D}'$ je zatvorena na mešovitu operaciju $\langle\cdot\rangle\cdot$, tj. za sve $a \in K'$, $p \in B'$ važi $\langle a\rangle p \in B'$. Najzad, *homomorfizam* $f : \mathbf{D}_1 \to \mathbf{D}_2$ dinamičkih algebri je par preslikavanja $f = \langle g, h\rangle$ takav da je g homomorifzam regularnih algebri $\mathbf{K}_1 \to \mathbf{K}_2$, h homomorfizam Booleovih algebri $\mathbf{B}_1 \to \mathbf{B}_2$, i za sve $a \in K_1$, $p \in B_1$ važi

$$h(\langle a\rangle p) = \langle g(a)\rangle h(p).$$

Shodno tome, *kongruencija* dinamičke algebre $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ je par kongruencija $\theta = \langle \theta_K, \theta_B\rangle$ redom na $\mathbf{K}$ i $\mathbf{B}$ takav da za sve $a, b \in K$ i $p, q \in B$, iz $\langle a, b\rangle \in \theta_K$ i $\langle p, q\rangle \in \theta_B$ sledi $\langle\langle a\rangle p, \langle b\rangle q\rangle \in \theta_B$.

Sa stanovišta primena u računarstvu, naročito je interesantna još jedna operacija, koju možemo dodati dinamičkim algebrama: to je operacija *testa* $? : B \to K$, tako da je za $p \in B$, $p?$ akcija ispitivanja tačnosti uslova p. Test $p?$, jasno, ne može proizvesti novo stanje; štaviše, on ne može proizvesti ni stanje p ukoliko ono već nije nastupilo. Zato je

$$\langle p?\rangle q = p \wedge q. \tag{33}$$

Dvosortne algebre $\mathbf{T} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot, ? \rangle$ u kojima je $\langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot \rangle$ dinamička algebra, a koje zadovoljavaju (33), su *test algebre*. Sada se grananje "`if` p `then` a `else` b" prikazuje u test algebrama kao regularni test-izraz

$$p?a + (\neg p)?b,$$

dok petlja "`while` p `do` a" očito odgovara izrazu

$$(p?a)^*(\neg p)?.$$

Modifikujući pojam test algebre, Kozen je nedavno uveo *Kleenejeve algebre sa testovima*. On je u [90] neposredno primenio identitete koji važe na tim algebrama kako bi dokazao ekvivalenciju određenih programskih struktura u `while` programima. Reč je o čisto formalnim, jednakosnim dokazima koji se izvode iz aksioma (Kleenejevih) test algebri. Između ostalog, on daje do sada najkraći i najelegantniji dokaz sledećeg klasičnog teorijsko-računarskog rezultata (koji je verovatno bio poznat još Kleeneju, iako se pripisuje Böhmu i Jacopiniju).

TEOREMA 6.1.1. *Svaki* `while` *program se može simulirati* `while` *programom sa najviše jednom "*`while...do`*" petljom, pod uslovom da se dopusti uvođenje novih Booleovih promenljivih.*

Ranije poznati dokazi koje su dali K. Hirose i M. Oya, odnosno G. Mirkowska (oba 1972.) su znatno složeniji, i nisu čisto sintaktički (kao Kozenov). Prema tome, dinamičke algebre, test algebre i njihova uopštenja pružaju veoma pogodno matematičko okruženje za rad sa programskim celinama, tj. razmatranje pitanja korektnosti programa, njihove ekvivalentnosti, optimizovanosti koda, i drugih.

U ovoj disertaciji, međutim, neće biti formulisan nijedan rezultat za test algebre. Razlog za to je što se gotovo svako tvrđenje o dinamičkim algebrama uz izvesne dodatne tehničke detalje može preformulisati i analogno dokazati za test algebre, što treba imati u vidu u celokupnom daljem tekstu. Tvrđenja su formulisana samo za dinamičke algebre kako bi ideje sadržane u tim tvrđenjima bile jasnije i transparentnije.

S druge strane, Jónsson [78] je ponudio jedan interesantan alternativni pristup dinamičkim algebrama. Naime, on polazi od toga da je unapred fiksirana neka *Kleenejeva algebra* $\mathbf{K} = \langle K, +, \cdot, ^*, 0, 1 \rangle$, i definiše dinamičke algebre kao Booleove algebre sa normalnim unarnim operatorima koji su indeksirani algebrom $\mathbf{K}$. Naj taj način se dobijaju $\mathbf{K}$-*dinamičke algebre*, koje obrazuju varijetet $\mathcal{DA}(\mathbf{K})$. Tačnije, reč je o algebrama

$$\mathbf{D} = \langle B, \vee, \wedge, \neg, \bot, \top, f_a \rangle_{a \in K},$$

takim da je $\langle B, \vee, \wedge, \neg, \bot, \top \rangle$ Booleova algebra, pri čemu imamo sledeće definišuće identitete:

$$\begin{aligned} f_a(0) &= 0, && (34)\\ f_a(x \vee y) &= f_a(x) \vee f_a(y), && (35)\\ f_{a+b}(x) &= f_a(x) \vee f_b(x), && (36)\\ f_{ab}(x) &= f_a(f_b(x)), && (37)\\ f_0(x) &= \bot, && (38)\\ f_1(x) &= x, && (39)\\ f_{a^*}(x) &= x \vee f_{a^*}(\neg x \wedge f_a(x)), && (40) \end{aligned}$$

za sve $a, b \in K$. Gornji spisak aksioma (koji je beskonačan čim je $\mathbf{K}$ beskonačna algebra) označićemo sa $\Theta(\mathbf{K})$, a tip $\mathbf{K}$-dinamičkih algebri sa $\tau(\mathbf{K})$.

Primetimo malu razliku u aksiomama indukcije (32) i (40). Naime, u Kleenejevim algebrama važi identitet $1 + xx^* = x^*$, pa se otuda iz (36), (37) i (39) kao posledica izvodi

$$f_{a^*}(x) = x \vee f_a(f_{a^*}(x))$$

za sve $a \in K$, tako da se leva nejednakost iz (32) u "Jónssonovoj varijanti" izvodi iz ostalih aksioma. Takođe, na osnovu istih identiteta kao i malopre, odnosno iz regularnog identiteta $1 + x^*x = x^*$, za sve $a \in K$ dobijamo:

$$\begin{aligned} x \vee f_{a^*}(\neg x \wedge f_a(x)) &\leq x \vee f_{a^*}(f_a(x)) = \\ &= f_1(x) \vee f_{a^*a}(x) = f_{1+a^*a}(x) = f_{a^*}(x), \end{aligned}$$

pošto iz (35) sledi da u $\mathbf{K}$-dinamičkim algebrama važi

$$x \leq y \;\Rightarrow\; f_a(x) \leq f_a(y)$$

za sve $a \in K$. Tako, (40) je zapravo analogon desne strane u (32), pojačan obratnom nejednakošću koja sledi iz ostalih aksioma $\mathbf{K}$-dinamičkih algebri.

Razlike koje nastupaju u ova dva pristupa su očite. Najpre, Jónssonove $\mathbf{K}$-dinamičke algebre su jednosortne univerzalne algebre. Dok u slučaju dvosortnih dinamičkih algebri imamo *jedan jedini* varijetet, dotle u drugom slučaju dobijamo *po jedan* varijetet za svaku Kleenejevu algebru indeksa $\mathbf{K}$, pa tako imamo klasu varijeteta $\mathbf{K}$-dimaičkih algebri indeksiranu varijetetom Kleenejevih algebri. Jasno je da će ova razlika imati veliki uticaj na razna pitanja u vezi identiteta i jednakosnih teorija. Razlog za to je taj što dok u prvom slučaju imamo dve vrste identiteta, pa tako i dve vrste promenljivih – regularne i

Booleove, na koje se jednako primenjuju manipulacije određene jednakosnom logikom, dotle u drugom slučaju imamo samo obične, jednosortne identitete u kojima su unarne operacije indeksirane *elementima konkretne algebre*, na koje se, naravno, ne mogu primeniti pomenute manipulacije u smislu jednakosne logike.

Stoga je naš cilj u ovoj glavi dvojak. Jedan se sastoji u tome da prikažemo neke osnovne, klasične rezultate vezane za dinamičke algebre, a naročito za jednu klasu dinamičkih algebri koja odgovara intuitivnoj vezi sa programskim strukturama, tzv. *separabilne* dinamičke algebre. Pokazaće se da su one na neposredan način povezane sa algebrama jezika, te da pružaju mogućnost da se (uz pomoć Booleovih algebri) jednakosna teorija Kleenejevih algebri ipak, u izvesnom smislu, dobije iz konačnog skupa identiteta. Drugi cilj jeste da istražimo veze (kako različitosti, tako i sličnosti) dinamičkih i **K**-dinamičkih algebri i da, koliko je god to moguće, izvršimo "transfer" dvosortnih rezultata na Jónssonove dinamičke algebre. Neke mogućnosti takvog prenosa rezultata su razmotrene u radu Crvenkovića i autora disertacije [41], i ovde će detaljno biti prikazani odgovarajući rezultati tog istraživanja.

6.2. Osnovne osobine dinamičkih algebri

Na početku ovog poglavlja ćemo razmotriti jednu mogućnost da se alternativno formuliše aksioma indukcije (32). Ta formulacija neće biti u obliku identiteta, ali može biti mnogo operativnija za rad.

Neka je $\langle a! \rangle p = \{q : p \vee \langle a \rangle q \leq q\}$. Za parcijalno uređen skup P, neka $min(P)$ označava *najmanji* element u P, ako on postoji; u suprotnom, $min(P)$ nije definisano.

LEMA 6.2.1. *Aksioma indukcije* (32) *se u dinamičkim algebrama može zameniti sa*

$$\langle a^* \rangle p = min(\langle a! \rangle p).$$

Dokaz. ($\Rightarrow$) Pođimo od dvostruke nejednakosti (32). Leva nejednakost je očito ekvivalentna sa $\langle a^* \rangle p \in \langle a! \rangle p$. Neka je sada $q \in \langle a! \rangle p$; dokazaćemo da je tada $\langle a^* \rangle p \leq q$. Zaista, iz $p \vee \langle a \rangle q \leq q$ sledi $p \leq q$, pa iz (27), desne nejednakosti (32) i (26) dobijamo

$$\langle a^* \rangle p \leq \langle a^* \rangle q \leq q \vee \langle a^* \rangle(\neg q \wedge \langle a \rangle q) \leq q \vee \langle a^* \rangle \bot = q,$$

jer iz $p \vee \langle a \rangle q \leq q$ sledi $\neg q \wedge \langle a \rangle q = \bot$.

($\Leftarrow$) Pretpostavimo da važi $\langle a^* \rangle p = min(\langle a! \rangle p)$. Tada je $\langle a^* \rangle p \in \langle a! \rangle p$, pa sledi leva nejednakost u (32). Po učinjenim pretpostavkama, sada je dovoljno

da pokažemo $p \vee \langle a^* \rangle(\neg p \wedge \langle a \rangle p) \in \langle a! \rangle p$. Sledeći niz identiteta i nejednakosti dobijamo iz aksioma Booleovih algebri, (27) i činjenice da smo već dobili levu nejednakost u (32):

$$\begin{aligned} p \vee \langle a \rangle(p \vee \langle a^* \rangle(\neg p \wedge \langle a \rangle p)) &= p \vee (\neg p \wedge \langle a \rangle(p \vee \langle a^* \rangle(\neg p \wedge \langle a \rangle p))) = \\ &= p \vee (\neg p \wedge (\langle a \rangle p \vee \langle aa^* \rangle(\neg p \wedge \langle a \rangle p))) \leq \\ &\leq p \vee ((\neg p \wedge \langle a \rangle p) \vee \langle aa^* \rangle(\neg p \wedge \langle a \rangle p))) \leq \\ &\leq p \vee \langle a^* \rangle(\neg p \wedge \langle a \rangle p), \end{aligned}$$

što je i trebalo dokazati. ∎

Ako je $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle \cdot \rangle \cdot \rangle$ dinamička algebra, tada element $a \in K$ zovemo *refleksivnim* ako za sve $p \in B$ važi $p \leq \langle a \rangle p$. On je *tranzitivan* ako je za sve $p \in B$ ispunjeno $\langle a^2 \rangle p \leq \langle a \rangle p$. Prema tome, a je refleksivan i tranzitivan ako je

$$p \vee \langle a^2 \rangle p \leq \langle a \rangle p,$$

tj. $\langle a \rangle p \in \langle a! \rangle p$. S druge strane, a je *zvezda* ako je za sve $p \in B$, $\langle a^* \rangle p = \langle a \rangle p$.

LEMA 6.2.2. *U svakoj dinamičkoj algebri, regularni element a je zvezda ako i samo ako je refleksivan i tranzitivan.*

Dokaz. ($\Rightarrow$) Kako je $\langle a \rangle p = \langle a^* \rangle p \in \langle a! \rangle p$, sledi da je a refleksivan i tranzitivan element.

($\Leftarrow$) Po prethodnoj lemi, $\langle a^* \rangle p = min(\langle a! \rangle p) \leq \langle a \rangle p$. S druge strane, po (32) je $p \leq \langle a^* \rangle p$, odakle je $\langle a \rangle p \leq \langle aa^* \rangle p \leq \langle a^* \rangle p$, pa je a zvezda. ∎

Prethodne leme smo analogno mogli formulisati i za Jónssonove $\mathbf{K}$-dinamičke algebre, a to će biti slučaj još nekoliko puta u daljem tekstu. Razlog za to je što važe sledeća dva tvrđenja opšteg karaktera, koja uspostavljaju "most" između opisana dva pristupa dinamičkim algebrama.

PROPOZICIJA 6.2.3. *Neka je* $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle \cdot \rangle \cdot \rangle$ *dinamička algebra takva da je* $\mathbf{K} \in \mathcal{KA}$. *Definišimo algebru* $\mathsf{Os}(\mathbf{D}) = \langle \mathbf{B}, f_a \rangle_{a \in K}$, *gde su unarni operatori dati sa* $f_a(x) = \langle a \rangle x$. *Tada je* $\mathsf{Os}(\mathbf{D})$ $\mathbf{K}$*-dinamička algebra.*

PROPOZICIJA 6.2.4. *Za* $\mathbf{K}$*-dinamičku algebru* $\mathbf{D} = \langle \mathbf{B}, f_a \rangle_{a \in K}$ *definišimo dvosortnu algebru* $\mathsf{Ts}(\mathbf{D}) = \langle \mathbf{K}, \mathbf{B}, \langle \cdot \rangle \cdot \rangle$ *sa* $\langle a \rangle x = f_a(x)$. *Tada je* $\mathsf{Ts}(\mathbf{D})$ *dinamička algebra. Štaviše, konstrukcije* Os *(iz prethodne propozicije) i* Ts *su uzajamno inverzne, što znači da za sve* $\mathbf{K}$*-dinamičke algebre* $\mathbf{D}$ *imamo* $\mathsf{Os}(\mathsf{Ts}(\mathbf{D})) = \mathbf{D}$, *odnosno da za sve dinamičke algebre* $\mathbf{D}'$ *sa Kleenejevom regularnom komponentom važi* $\mathsf{Ts}(\mathsf{Os}(\mathbf{D}')) = \mathbf{D}'$.

Na početku disertacije smo videli da su tipični primeri Kleenejevih algebri bili Kleenejeve algebre binarnih relacija (štaviše, one su generisale varijetet $\mathcal{KA}$). U slučaju dinamičkih algebri, takođe možemo konstruisati algebre sačinjene od binarnih relacija. Međutim, one sada moraju da deluju na neku Booleovu algebru: u pitanju će biti polje skupova nad istim skupom nad kojim su definisane odgovarajuće binarne relacije.

Neka je A neki skup i neka $\mathbf{2}^A$ označava punu Booleovu algebru skupova nad A. *Puna dinamička algebra relacija* nad A je algebra $\langle \mathbf{Rel}(A), \mathbf{2}^A, \langle\cdot\rangle\cdot\rangle$, gde je za $\rho \subseteq A \times A$ i $X \subseteq A$:

$$\langle\rho\rangle X = \{b \in A : (\exists a \in X)\ \langle a, b\rangle \in \rho\}.$$

(Važna napomena: kako bismo bili u saglasnosti sa (29) i (37), u ovoj glavi ćemo koristiti kompoziciju relacija definisanu obratno u odnosu na prethodne glave.) Svaka podalgebra pune dinamičke algebre relacija (znači, dinamička algebra koja se sastoji od standardne Kleenejeve algebre i polja skupova nad datim skupom) je *Kripkeova dinamička algebra (KDA)* [92]. Dinamička algebra je *reprezentabilna* ako je izomorfna nekoj KDA. Klasu reprezentabilnih dinamičkih algebri označavamo sa $\mathcal{RDA}$.

Putem operatora Os, možemo definisati jednosortne Kripkeove $\mathbf{K}$-dinamičke algebre, kao i pojam reprezentabilnosti. Naravno, taj pojam se može "preneti" na jednosortni slučaj samo ukoliko je $\mathbf{K}$ standardna Kleenejeva algebra relacija. U suprotnom, varijetet $\mathcal{DA}(\mathbf{K})$ nema reprezentabilne algebre.

Slično Propoziciji 2.1.4, važi i naredna (u stvari, Propoziciju 2.1.4 smo dobili razmatranjem "Kleenejevog dela" ovog tvrđenja).

PROPOZICIJA 6.2.5. (Németi, [114]) *Klasa $\mathcal{RDA}$ je zatvorena na direktne proizvode.*

Dokaz. Neka je za $i \in I$, $\mathbf{D}_i = \langle \mathbf{K}_i, \mathbf{B}_i, \langle\cdot\rangle_i\cdot\rangle$ KDA nad skupom A_i (pretpostavimo, bez ograničenja opštosti, da su svi skupovi A_i, $i \in I$, disjunktni). Neka je $\mathbf{D}$ puna KDA nad

$$A = \bigcup_{i\in I} A_i.$$

Definišimo preslikavanje

$$\iota : \prod_{i\in I} \mathbf{D}_i \to \mathbf{D}$$

sa

$$\begin{aligned} \iota_K(\langle\rho_i\rangle_{i\in I}) &= \bigcup_{i\in I} \rho_i, \\ \iota_B(\langle X_i\rangle_{i\in I}) &= \bigcup_{i\in I} X_i. \end{aligned}$$

Disjunktnost skupova A_i implicira da je ι injektivno preslikavanje. Takođe, lako se pokazuje da je ι homomorfizam dinamičkih algebri, čime smo izvršili potapanje direktnog proizvoda algebri $\mathbf{D}_i$ u $\mathbf{D}$, odnosno, pokazali njegovu reprezentabilnost. ∎

Kripkeove dinamičke algebre igraju ključnu ulogu u razmatranju separabilnih dinamičkih algebri i njihovom povezivanju sa jednakosnom teorijom Kleenejevih algebri.

6.3. Separabilnost dinamičkih algebri

Budući da je prvobitna motivacija za izučavanje dinamičkih algebri modeliranje računarskih programa i njihovog dejstva na stanja računara, očekujemo da dinamičke algebre na određeni način odgovaraju "programerskoj" intuiciji. Tako, ako dva programa proizvode isto dejstvo na sva moguća stanja računara, njih smatramo ekvivalentnim, odnosno, jednakim. Primetimo da, kada su u pitanju dinamičke algebre, ovu osobinu imaju pune KDA. Naime, ako su $\rho_1 \neq \rho_2$ dve relacije na skupu A, tada postoje $x, y \in A$ tako da, na primer, $\langle x, y\rangle \in \rho_1 \setminus \rho_2$. Ali, tada $y \in \langle\rho_1\rangle\{x\}$ i $y \notin \langle\rho_2\rangle\{x\}$, tj.

$$\langle\rho_1\rangle\{x\} \neq \langle\rho_2\rangle\{x\}.$$

Dinamičke algebre $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ takve da za sve $a, b \in K$ postoji $p \in B$ tako da je

$$\langle a\rangle p \neq \langle b\rangle p$$

se zovu *separabilne* dinamičke algebre. Klasu svih separabilnih dinamičkih algebri označavamo sa $\mathcal{SDA}$.

Kako su separabilne dinamičke algebre definisane u odnosu na $\mathcal{DA}$ Hornovom formulom

$$(\forall a)(\forall b)(\exists p)(a \neq b \Rightarrow \langle a\rangle p \neq \langle b\rangle p),$$

odmah je jasno da je klasa $\mathcal{SDA}$ zatvorena na direktne proizvode. S druge strane, $\mathcal{SDA}$ nije zatvoreno na homomorfizme i podalgebre. Naime, posmatrajmo dinamičku algebru čija regularna algebra ima elemente $K = \{0, 1, a, b\}$, dok je odgovarajuća Booleova algebra $B = \{\bot, p, \neg p, \top\}$. Neka je $\langle b\rangle p = \top$, dok je u svim ostalim slučajevima $\langle a\rangle x = \langle b\rangle x = x$. Rezultati ostalih operacija se definišu tako da se dobije dinamička algebra (specijalno, dati uslovi forsiraju jednoznačnu definisanost regularnih operacija $+, \cdot, ^*$). Neka je sada h endomorfizam opisane dinamičke algebre koji fiksira regularne elemente, dok je $h_B(\bot) = h_B(\neg p) = \bot$ i $h_B(\top) = h_B(p) = \top$. Odgovarajuća homomorfna slika (koja je ujedno i podalgebra polazne algebre) očito nije separabilna. Stoga $\mathcal{SDA}$ nije varijetet. Varijetet generisan sa $\mathcal{SDA}$ označavaćemo sa $\mathcal{S}$.

PROPOZICIJA 6.3.1. *Neka je* $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ *podalgebra separabilne dinamičke algebre takva da je Booleova algebra* $\mathbf{B}$ *kompletna i atomična. Tada je* $\mathbf{D}$ *reprezentabilna. Specijalno, svaka konačna podalgebra separabilne dinamičke algebre je reprezentabilna.*

Dokaz. Neka je A skup atoma algebre $\mathbf{B}$. Po datim uslovima, $\mathbf{B} \cong \mathbf{2}^A$. Dalje, za $a \in K$ definišimo $\rho_a \subseteq A \times A$ sa

$$\langle p, q\rangle \in \rho_a \;\Leftrightarrow\; q \leq \langle a\rangle p.$$

Lako se vidi da je preslikavanje $a \mapsto \rho_a$ izomorfizam regularnih algebri i, štaviše, da on zajedno sa malopređašnjim izomorfizmom Booleovih algebri daje izomorfizam dinamičkih algebri. ∎

Odmah se postavlja pitanje kakav je odnos između jednakosnih teorija varijeteta $\mathcal{DA}$ i njegovog podvarijeteta $\mathcal{S}$ (odnosno, klase $\mathcal{SDA}$). Iz samih definicionih identiteta za dinamičke algebre nije teško videti da je regularni deo jednakosne teorije za $\mathcal{DA}$, $Eq_R(\mathcal{DA})$, trivijalan (budući da su pomenuti definicioni identiteti svi Booleovog tipa). Ispostavilo se da je $Eq_R(\mathcal{SDA}) = Eq(\mathcal{KA})$ (što sledi iz prvobitnog oblika Kozen-Németijeve teoreme, koja je izvorno bila formulisana u kontekstu dinamičkih algebri), dok je $Eq_B(\mathcal{SDA}) = Eq_B(\mathcal{DA})$. Najpre ćemo pokazati kako iz glavnog rezultata Prattovog antologijskog rada [127], datog niže, sledi jednakost Booleovih jednakosnih teorija za $\mathcal{SDA}$ i ceo varijetet $\mathcal{DA}$.

TEOREMA 6.3.2. (Pratt, [127]) *Neka dinamička algebra* $\mathbf{D}$ *ima osobinu univerzalnog preslikavanja za klasu* $\mathcal{SDA}$. *Tada za svaki konačan skup* B_0 *Booleovih elemenata algebre* $\mathbf{D}$ *postoji konačna separabilna dinamička algebra* $\mathbf{D}'$ *i sirjektivni homomorfizam* $f_{B_0} : \mathbf{D} \to \mathbf{D}'$ *koji je injektivan na* B_0.

Pri tome se homomorfizam f_{B_0} (algebra $\mathbf{D}'$) zove *filtracija* (*filtrat*) za B_0.

TEOREMA 6.3.3. (Pratt, [127]) *Svaka* $\mathcal{DA}$*-slobodna algebra* $\mathbf{F}_{\mathcal{DA}}(X, Y)$ *je poddirektan proizvod konačnih dinamičkih algebri i jedne dinamičke algebre sa trivijalnim Booleovim nosačem.*

Dokaz. Za Booleove elemente p, q slobodne dinamičke algebre $\mathbf{F}_{\mathcal{DA}}(X, Y)$ takve da je $p \neq q$ postoji, po prethodnoj teoremi, filtracija $f_{\{p,q\}}$, pa definišimo $\theta_{p,q} = ker(f_{\{p,q\}})$. Osim toga, neka je θ_0 relacija koja je dijagonala na regularnom delu posmatrane dinamičke algebre, a univerzalna relacija na njenom Booleovom delu. Jasno, presek opisane familije kongruencija je trivijalna kongruencija. Faktori oblika $\mathbf{F}_{\mathcal{DA}}(X, Y)/\theta_{p,q}$ su, prema Teoremi 6.3.2, konačne dinamičke algebre, dok je $\mathbf{F}_{\mathcal{DA}}(X, Y)/\theta_0$ algebra sa trivijalnim Booleovim nosačem. ∎

Neka je sada $\mathcal{RDA}^+$ klasa svih reprezentabilnih dinamičkih algebri koja je proširena svim dinamičkim algebrama sa trivijalnim Booleovim nosačem. Ispostavlja se da ova klasa generiše varijetet $\mathcal{DA}$.

TEOREMA 6.3.4. $\mathcal{DA} = \mathsf{HSP}(\mathcal{RDA}^+)$.

Dokaz. Jasno, $\mathcal{RDA}^+ \subseteq \mathcal{DA}$. Obratno, po Propoziciji 6.3.1 i Teoremi 6.3.3, svaka slobodna dinamička algebra je poddirektan prozivod algebri iz $\mathcal{RDA}^+$, odakle sledi $\mathcal{DA} \subseteq \mathsf{HSP}(\mathcal{RDA}^+)$. ∎

Klasa separabilnih dinamičkih algebri $\mathcal{SDA}$ nije zatvorena na podalgebre, što znači da, *a priori*, nismo sigurni da ta klasa sadrži slobodne algebre. Da je to ipak slučaj, pokazuje naredna lema (zajedno sa Teoremom 6.3.14).

LEMA 6.3.5. *Ako je* $|Y| \geq 1$, *tada* $\mathbf{F}_{\mathcal{S}}(X,Y) \in \mathcal{SDA}$.

Dokaz. Neka je $\mathbf{D}$ $\mathcal{S}$-slobodna algebra sa bar jednim Booleovim slobodnim generatorom p_1. Po definiciji slobodne algebre, za sve regularne elemente $a \neq b$ algebre $\mathbf{D}$ postoji $\mathbf{D}' \in \mathcal{SDA}$ i homomorfizam $f : \mathbf{D} \to \mathbf{D}'$ takav da je $f_R(a) \neq f_R(b)$. Ali, tada postoji Booleov element p_0 algebre $\mathbf{D}'$ tako da je $\langle f_R(a)\rangle p_0 \neq \langle f_R(b)\rangle p_0$. Neka je sada $g : \mathbf{D} \to \mathbf{D}'$ homomorfizam koji se poklapa sa f na regularnom delu i za koji važi $g(p_1) = p_0$. Imamo:

$$\begin{aligned} g(\langle a\rangle p_0) &= \langle g_R(a)\rangle g_B(p_0) = \langle f_R(a)\rangle p_1 \neq \langle f_R(b)\rangle p_1 = \\ &= \langle g_R(b)\rangle g_B(p_0) = g(\langle b\rangle p_0), \end{aligned}$$

odakle je $\langle a\rangle p_0 \neq \langle b\rangle p_0$, tj. $\mathbf{D}$ je separabilna dinamička algebra. ∎

TEOREMA 6.3.6. *Svaka slobodna separabilna dinamička algebra je poddirektan proizvod konačnih dinamičkih algebri.*

Dokaz. Analogno kao u dokazu Teoreme 6.3.3, uzmimo jezgra $\theta_{p,q}$ filtracija dvoelementnih Booleovih podskupova algebre $\mathbf{F}_{\mathcal{S}}(X,Y)$. Presek tih kongruencija je očito trvijalan na Booleovom nosaču ove algebre. Međutim, on mora biti trivijalan i na regularnom nosaču, jer zbog separabilnosti $\mathcal{S}$-slobodnih algebri (vidi Lemu 6.3.5 i Teoremu 6.3.14) postoji Booleov element p tako da je $\langle a\rangle p \neq \langle b\rangle p$, što znači da neka od kongruencija $\theta_{p,q}$ razdvaja $\langle a\rangle p, \langle b\rangle p$, a time i a, b. Količnici $\mathbf{F}_{\mathcal{S}}(X,Y)/\theta_{p,q}$ su konačni po Teoremi 6.3.2. ∎

Najzad, sada možemo da pokažemo *Segerberg-Parikhovu teoremu kompletnosti* [148, 118], koja tvrdi da je aksiomatika separabilnih algebri kompletna za identitete reprezentabilnih dinamičkih algebri (odnosno, KDA). Tačnije, važi

TEOREMA 6.3.7. $\mathcal{S} = \mathsf{HSP}(\mathcal{RDA})$.

Dokaz. Svaka puna KDA je separabilna, pa sledi $\mathcal{RDA} \subseteq \mathcal{S}$, pošto je svaka reprezentabilna dinamička algebra izomorfna podalgebri pune KDA. Po Propoziciji 6.3.1 i Teoremi 6.3.6, svaka $\mathcal{S}$-slobodna algebra je poddirektan proizvod reprezentabilnih dinamičkih algebri, odakle sledi obratna inkluzija, tj. $\mathcal{S} \subseteq \mathsf{HSP}(\mathcal{RDA})$. ∎

Direktno iz Teorema 6.3.4 i 6.3.7 (imajući u vidu definiciju klase $\mathcal{RDA}^+$ i činjenicu da na trivijalnim algebrama važi svaki identitet odgovarajućeg tipa), dobija se

POSLEDICA 6.3.8. $Eq_B(\mathcal{SDA}) = Eq_B(\mathcal{DA})$.

Gornji rezultat znači da nametanje uslova separabilnosti *ništa* ne doprinosi Booleovoj jednakosnoj teoriji dinamičkih algebri, tj. ostavlja je neizmenjenu. S druge strane, isti taj jednostavni uslov *drastično* menja regularni deo jednakosne teorije. Pokazuje se da je on dovoljan da od trivijalnih identiteta tipa $\langle 2, 2, 1, 0, 0\rangle$ "izgradi" čitavu jednakosnu teoriju Kleenejevih algebri.

TEOREMA 6.3.9. $Eq_R(\mathcal{SDA}) = Eq(\mathcal{KA})$.

Dokaz. Iz Teoreme 6.3.7 imamo da je $Eq(\mathcal{SDA}) = Eq(\mathcal{RDA})$, pa se ta jednakost odnosi i na regularne delove jednakosnih teorija. Međutim, klasa regularnih algebri sadržanih u reprezentabilnim dinamičkim algebrama se poklapa sa klasom standardnih Kleenejevih algebri (koje generišu $\mathcal{KA}$), odakle rezultat sledi. ∎

POSLEDICA 6.3.10. (Kozen, [83], Németi, [114]) *Regularni deo $\mathcal{S}$-slobodne algebre $\mathbf{F}_{\mathcal{S}}(X, Y)$ izomorfan je algebri regularnih jezika* $\mathbf{Reg}(X)$.

Kao što smo već pomenuli, ovo je originalna forma u kojoj se prvi put pojavila Kozen-Németijeva teorema. Teorema 1.3.4 jeste dobijena "odsecanjem" Booleovog dela u gornjem tvrđenju, imajući u vidu činjenicu da svaka standardna Kleenejeva algebra učestvuje u nekoj KDA, kao i Teoremu 6.3.7.

POSLEDICA 6.3.11. $Eq(\mathcal{S}) = Eq(\mathcal{DA}) \cup Eq(\mathcal{KA})$. *Tako, aksiome* (26)–(32) *zajedno sa identitetima Kleenejevih algebri aksiomatizuju varijetet $\mathcal{S}$. Prema tome, $\mathcal{S}$ se sastoji tačno od onih dinamičkih algebri čija je regularna komponenta Kleenejeva algebra.*

To znači da se konstrukcija **Ts** odnosi tačno na elemente varijeteta $\mathcal{S}$, odnosno da je rezultat konstrukcije **Os** upravo dinamička algebra iz tog varijeteta.

Specijalno, gornja posledica znači i da svaka dinamička algebra sa regularnom komponentom koja nije Kleenejeva algebra nije separabilna. Ali, s druge strane postoje i Kleenejeve algebre koje *forsiraju* neseparabilnost, iako odgovarajuće dinamičke algebre leže u $\mathcal{S}$. Takva je ranije već razmotrena četvoroelementna algebra "Conwayev skok" $\mathbf{C}_4$ (interesantno je da je ona kontraprimer u gotovo svakoj "problematičnoj" situaciji). Podsetimo se, reč je količniku algebre (regularnih) jezika, koju čine prazan jezik $\emptyset$, jezik $\{\lambda\}$ pisan kao λ, dok su preostali konačni jezici reprezentovani sa F, a beskonačni jezici sa ∞.

PROPOZICIJA 6.3.12. *U svakoj dinamičkoj algebri* $\mathbf{D} = \langle \mathbf{C}_4, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ *važi* $\langle F\rangle p = \langle\infty\rangle p$ *za sve* $p \in B$. *Drugim rečima, svaka* $\mathbf{C}_4$*-dinamička algebra je neseparabilna, tj. identitet* $f_F(x) = f_\infty(x)$ *sledi iz aksioma* $\Theta(\mathbf{C}_4)$.

Dokaz. Kako je $\lambda \leq F$, sledi da je $p = \langle\lambda\rangle p \leq \langle F\rangle p$ za sve $p \in B$. Takođe, $F^2 = F$, pa je $\langle F^2\rangle p = \langle F\rangle p$. Dakle, element F je refleksivan i tranzitivan, pa je zvezda, po Lemi 6.2.2, tj. $\langle F\rangle p = \langle\infty\rangle p$ za sve $p \in B$ (pošto je $F^* = \infty$). Međutim, $F \neq \infty$. ∎

Do sada izloženi materijal je dovoljan da pokažemo kako jednakosna teorija Kleenejevih algebri nije samo deo jednakosne teorije (takođe beskonačno baziranog) varijeteta $\mathcal{S}$, nego da je ona ipak "skrivena" već u konačno baziranom varijetetu $\mathcal{DA}$, iako je njegova regularna teorija trivijalna. Međutim, ako se "angažuje" Booleov deo dinamičkih algebri i ima u vidu dejstvo regularnih elemenata na Booleove promenljive – tada odmah imamo regularne identitete, kao što je to opisano u narednoj teoremi.

TEOREMA 6.3.13. $\mathcal{KA} \models r = s$ *ako i samo ako* $\mathcal{DA} \models \langle r\rangle x = \langle s\rangle x$.

Dokaz. Ako je $r = s$ identitet Kleenejevih algebri, tada po Teoremi 6.3.8, $\mathcal{S} \models r = s$, odakle $\mathcal{S} \models \langle r\rangle x = \langle s\rangle x$. Ali, kako je $\langle r\rangle x = \langle s\rangle x$ Booleov identitet, po Posledici 6.3.8 dobijamo $\mathcal{DA} \models \langle r\rangle x = \langle s\rangle x$.

Obratno, iz $\mathcal{DA} \models \langle r\rangle x = \langle s\rangle x$ sledi $\mathcal{S} \models \langle r\rangle x = \langle s\rangle x$. Specijalno, ako je Σ prebrojiva azbuka, imamo $\mathbf{F}_{\mathcal{S}}(\Sigma, \{x\}) \models \langle r\rangle x = \langle s\rangle x$. Po Teoremi 6.3.10 dobijamo $\mathbf{Reg}(\Sigma) \models r = s$, što znači da $\mathcal{KA} \models r = s$. ∎

Time smo rešili još jedan problem u vezi sa praktičnom, računarskom primenom Kleenejevih algebri, a koji nismo pomenuli na početku glave. Naime, činjenica da $\mathcal{KA}$ nema konačnu bazu identiteta u startu onemogućava bilo

kakvu automatsku (mašinsku) produkciju regularnih identiteta, na čemu bi se zasnivali razni postupci optimizacije programskih celina. Ali, ispostavilo se da ipak postoji "zaobilazni" način da se uz pomoć konačne šeme identiteta dobiju svi regularni identiteti – u pomoć su nam pritekle Booleove algebre i dinamičke algebre kao njihov spoj sa Kleenejevim algebrama. Tako (po gornjoj teoremi), dovoljno je iz aksioma (26)–(32) izvesti sve posledice oblika $\langle r\rangle x = \langle s\rangle x$ i iz njih "filtrirati" regularne izraze r, s.

U narednom ćemo dovršiti posao započet Lemom 6.3.5. Slučaj slobodnih separabilnih algebri sa $Y = \emptyset$ (praznim skupom Booleovih generatora) razrešio je Németi 1982. godine.

TEOREMA 6.3.14. (Németi, [114]) *Sve dinamičke algebre oblika* $\mathbf{F}_{\mathcal{S}}(X, \emptyset)$ *su separabilne. Stoga sve* $\mathcal{S}$*-slobodne algebre pripadaju klasi* $\mathcal{SDA}$.

Dokaz. Dokazaćemo da je $\neg\langle x\rangle\top$ univerzalni separator za svaka dva različita regularna elementa algebre $\mathbf{F}_{\mathcal{S}}(X, \emptyset)$ (podsetimo se da su to regularni jezici, po Teoremi 6.3.10). Neka su uočeni neekvivalentni regularni izrazi r, s koji redom predstavljaju jezike L_1, L_2 i neka je, na primer, $w \in L_1 \setminus L_2$. Neka je $\mathbf{D}$ puna KDA nad skupom X^*. Za $y \in X$, definišimo ρ_y kao desnu translaciju koja odgovara slovu y na slobodnom monoidu X^*. Dalje, definišimo binarne relacije na X^*, $\sigma_x = \rho_x^\vee \setminus \{\langle wx, w\rangle\}$ i $\sigma_y = \rho_y^\vee$ za sve $y \in X \setminus \{x\}$. Tada u $\mathbf{D}$ imamo

$$\overline{\langle\sigma_x\rangle X^*} = \{w\}.$$

Međutim, lako se vidi da za interpretaciju $\sigma : y \mapsto \sigma_y$, $y \in X$, imamo $\langle w, \lambda\rangle \in r^{\mathbf{D}}(\sigma) \setminus s^{\mathbf{D}}(\sigma)$ (zbog $w \in L_1 \setminus L_2$), odakle je

$$\lambda \in \langle r^{\mathbf{D}}(\sigma)\rangle\{w\} \setminus \langle s^{\mathbf{D}}(\sigma)\rangle\{w\}.$$

To znači da

$$\mathbf{D} \not\models \langle r\rangle\neg\langle x\rangle\top = \langle s\rangle\neg\langle x\rangle\top,$$

pa tako ni klasa $\mathcal{RDA}$ ne zadovoljava gornji identitet. Ali, po Teoremi 6.3.7, odavde sledi da ga ne zadovoljava ni $\mathcal{S}$, tj. da imamo

$$\langle L_1\rangle\neg\langle x\rangle\top \neq \langle L_2\rangle\neg\langle x\rangle\top$$

u $\mathbf{F}_{\mathcal{S}}(X, \emptyset)$. ∎

Na osnovu ove teoreme i Propozicije 6.3.1, dobija se

POSLEDICA 6.3.15. *Svaka* $\mathcal{S}$*-slobodna dinamička algebra je reprezentabilna.*

Propozicija 6.3.12 pokazuje da je situacija sa separabilnošću slobodnih algebri drugačija u slučaju Jónssonovih $\mathbf{K}$-dinamičkih algebri u odnosu na do sada razmatrane dvosortne dinamičke algebre. Razlog za to leži u činjenici da je separabilnost slobodnih algebri u varijetetu $\mathcal{DA}(\mathbf{K})$ ekvivalentna postojanju separabilne $\mathbf{K}$-dinamičke algebre, odnosno, u terminima dinamičkih algebri, postojanju separabilne dinamičke algebre sa regularnom komponentom $\mathbf{K}$. Drugim rečima, pitanje karakterizacije varijeteta Jónssonovih dinamičkih algebri sa separabilnim slobodnim algebrama svodi se na karakterizaciju onih Kleenejevih algebri koje se pojavljuju kao regularne komponente algebri iz $\mathcal{SDA}$. Svakako, među njima su sve standardne Kleenejeve algebre binarnih relacija. U daljem, naš cilj će biti da opišemo jednu klasu Kleenejevih algebri $\mathbf{K}$ koja daje separabilne $\mathcal{DA}(\mathbf{K})$-slobodne algebre, što je jedan od glavnih rezultata u [41]. Između ostalog, pokazaćemo da je klasa regularnih komponenti separabilnih dinamičkih algebri kvazivarijetet kojem pripadaju sve slobodne algebre svih podvarijeteta od $\mathcal{KA}$. Ali, prvo nam treba nekoliko tehničkih pojmova i pomoćnih tvrđenja u vezi sa njima.

Neka je $\alpha : \mathbf{K} \to \alpha(\mathbf{K})$ sirjektivni homomorfizam Kleenejevih algebri. Za term t tipa $\tau(\mathbf{K})$ definišemo term t^α tipa $\tau(\alpha(\mathbf{K}))$ koji se dobija od t zamenom svakog unarnog simbola f_a sa $f_{\alpha(a)}$. Za skup identiteta E ćemo koristiti analognu notaciju; prema tome, E^α označava skup identiteta koji se dobija kada se na obe strane svih identiteta iz E primeni operator $^\alpha$.

LEMA 6.3.16. *Neka je* $\mathbf{K}$ *Kleenejeva algebra i* $\alpha : \mathbf{K} \to \alpha(\mathbf{K})$ *sirjektivni homomorfizam. Tada iz* $\mathcal{DA}(\mathbf{K}) \models p = q$ *sledi* $\mathcal{DA}(\mathbf{K}) \models p^\alpha = q^\alpha$.

Dokaz. Lemu dokazujemo indukcijom po dužini formalnog dokaza identiteta $p = q$ iz aksioma $\Theta(\mathbf{K})$. Pre svega, primetimo da je $(\Theta(\mathbf{K}))^\alpha = \Theta(\alpha(\mathbf{K}))$, pa je tvrđenje tačno ako je $p = q$ neka od aksioma. Takođe, induktivni korak je jasan, ukoliko je $p = q$ dobijeno iz nekih identiteta primenom pravila (Sim) ili $(Tranz)$.

Ako je $p \equiv f(p_1, \ldots, p_n)$ i $q \equiv f(q_1, \ldots, q_n)$, pri čemu su identiteti $p_i = q_i$, $1 \leq i \leq n$, ranije dokazani (što znači da je $p = q$ dobijeno primenom pravila $(Sagl)$), tada po induktivnoj pretpostavci imamo identitete $p_i^\alpha = q_i^\alpha$ za sve $1 \leq i \leq n$, odakle izvodimo

$$f^\alpha(p_1^\alpha, \ldots, p_n^\alpha) = f^\alpha(q_1^\alpha, \ldots, q_n^\alpha),$$

što je tačno identitet $p^\alpha = q^\alpha$.

Najzad, ako je $p = q$ dobijeno primenom pravila (Zam), tada je taj identitet oblika $r(t_1, \ldots, t_n) = s(t_1, \ldots, t_n)$, pri čemu su $t_1, \ldots, t_n$ neki termi, a

identitet $r = s$ je dobijen ranije u dokazu. Ali, tada sledi $r^\alpha = s^\alpha$, što znači da

$$r^\alpha(t_1^\alpha, \ldots, t_n^\alpha) = s^\alpha(t_1^\alpha, \ldots, t_n^\alpha),$$

odnosno $p^\alpha = q^\alpha$, važi u $\mathcal{DA}(\mathbf{K})$. ∎

Takođe, biće nam potrebna jedna lema opšte-algebarskog karaktera, a u duhu teorije kategorija.

LEMA 6.3.17. *Neka algebra* $\mathbf{U}_X$ *ima osobinu univerzalnog preslikavanja (nad* X*) za klasu algebri* $\mathcal{C}$ *odgovarajućeg tipa. Tada za svaku algebru* $\mathbf{A} \in \mathcal{C}$ *i svaka dva homomorfizma* $\xi, \xi' : \mathbf{U}_X \to \mathbf{A}$ *postoji endomorfizam* η *algebre* $\mathbf{U}_X$ *takav da je* $\xi' = \eta \circ \xi$.

Dokaz. Za $x_i \in X$ označimo $\xi(x_i) = a_i$ i $\xi'(x_i) = a_i'$. Kako je ξ sirjektivni homomorfizam, elementi a_i generišu algebru $\mathbf{A}$, pa postoji term t_j tako da je $a_j' = t_j^{\mathbf{A}}(a_1, a_2, \ldots)$ za sve j. Definišimo preslikavanje $\eta_0 : X \to U_X$ sa

$$\eta_0(x_i) = t_i^{\mathbf{U}_X}(x_1, x_2, \ldots).$$

Po datim uslovima, ovo preslikavanje se (na jedinstven način) proširuje do endomorfizma $\eta : \mathbf{U}_X \to \mathbf{U}_X$. Pri tome je

$$\xi(\eta(x_i)) = \xi(\eta_0(x_i)) = \xi(t_i^{\mathbf{U}_X}(x_1, x_2, \ldots)) = t_i^{\mathbf{A}}(a_1, a_2, \ldots) = a_i',$$

što zapravo znači da je

$$(\eta \circ \xi)|_X = \xi'|_X.$$

Po uslovu jedinstvenosti homomorfizma koji proširuje dato preslikavanje na generatornom skupu, sledi $\eta \circ \xi = \xi'$. Na kraju, primetimo da se opisani dokaz lako može prilagoditi i za višesortne algebre. ∎

Neka je sada $\mathbf{T}_X$ term algebra tipa $\langle 2, 2, 1, 0, 0\rangle$ i $h : \mathbf{T}_X \to \mathbf{K}$ sirjektivni homomorfizam takav da je $\mathbf{K}$ Kleenejeva algebra. Ako je t Booleov term na jeziku dinamičkih algebri, tada sa $\hat{t}^h$ označavamo term tipa $\tau(\mathbf{K})$ koji se dobija od t zamenom svakog podterma oblika $\langle r\rangle s$ (gde je r regularan izraz, a s Booleov term) sa $f_{h(r)}(s)$.

Sada dokazujemo jedno tehničko tvrđenje, na osnovu kojeg ćemo biti u mogućnosti da detaljnije ispitujemo problem separabilnosti, odnosno da razmatranja sa dvosortnih dinamičkih algebri prenosimo na Jónssonove jednosortne modele, kao i obratno.

PROPOZICIJA 6.3.18. *(1) Neka je* $\mathbf{K}$ *Kleenejeva algebra i* X, Y *proizvoljni skupovi. Tada za svaku Kleenejevu algebru* $\mathbf{K}$ *(generisanu sa najviše* $|X|$ *elemenata) postoji Booleova algebra* $\mathbf{B}_{\mathbf{K}}(Y)$ *tako da za sve dinamičke algebre* $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ *i za svaki sirjektivni homomorfizam*

$$h : \mathbf{F}_{\mathcal{DA}}(X, Y) \to \mathbf{D}$$

postoje sirjektivni homomorfizmi φ, ψ *tako da dijagram*

$$\begin{array}{ccc} \mathbf{F}_{\mathcal{DA}}(X,Y) = \langle \mathbf{T}_X, \mathbf{B}_0, \langle\cdot\rangle\cdot\rangle & & \\ \Big\downarrow \varphi & \searrow^{h} & \\ \langle \mathbf{K}, \mathbf{B}_{\mathbf{K}}(Y), \langle\cdot\rangle\cdot\rangle & \xrightarrow{\quad\psi\quad} & \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle = \mathbf{D} \end{array}$$

komutira. U tom slučaju je $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y) = \mathsf{Os}(\langle \mathbf{K}, \mathbf{B}_{\mathbf{K}}(Y), \langle\cdot\rangle\cdot\rangle)$.

(2) Neka je $\mathbf{K}$ *Kleenejeva algebra,* $\varphi : \mathbf{F}_{\mathcal{DA}}(X, Y) \to \langle \mathbf{K}, \mathbf{B}_{\mathbf{K}}(Y), \langle\cdot\rangle\cdot\rangle$ *homomorfizam* $(\varphi = \langle \varphi_K, \varphi_B \rangle)$*, a* p, q *Booleovi dvosortni termi. Tada je*

$$\langle \mathbf{K}, \mathbf{B}_{\mathbf{K}}(Y), \langle\cdot\rangle\cdot\rangle \models p = q \text{ ako i samo ako } \mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y) \models \hat{p}^{\varphi_K} = \hat{q}^{\varphi_K}.$$

(3) Neka je $\mathcal{V}$ *podvarijetet od* $\mathcal{KA}$ *i neka* $\mathcal{DA}(\mathcal{V})$ *označava podvarijetet od* $\mathcal{DA}$ *definisan istim identitetima koji određuju* $\mathcal{V}$ *(specijalno,* $\mathcal{DA}(\mathcal{KA}) = \mathcal{S}$*). Ako je* $\mathbf{K} = \mathbf{F}_{\mathcal{V}}(X)$*, tada je*

$$\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y) = \mathsf{Os}(\mathbf{F}_{\mathcal{DA}(\mathcal{V})}(X, Y)).$$

(4) $\mathbf{F}_{\mathcal{S}}(X, Y) = \langle \mathbf{Reg}(X), \mathbf{B}_{\mathbf{Reg}(X)}(Y), \langle\cdot\rangle\cdot\rangle$*, pa je stoga* $\mathbf{F}_{\mathcal{DA}(\mathbf{Reg}(X))}(Y)$ *separabilna* $\mathbf{Reg}(X)$*-dinamička algebra.*

Dokaz. (1) Najpre primetimo da je regularni deo algebre $\mathbf{F}_{\mathcal{DA}}(X, Y)$ jednak $\mathbf{T}_X$, budući da $\mathcal{DA}$ zadovoljava samo trivijalne identitete regularnog tipa. Sada fiksirajmo proizvoljni sirjektivni homomorfizam $\xi : \mathbf{T}_X \to \mathbf{K}$ i definišimo kongruenciju na $\mathbf{F}_{\mathcal{DA}}(X, Y)$ sa:

$$\theta_0(\xi) = \bigcap \{ \langle \theta_K, \theta_B \rangle \in Con\, \mathbf{F}_{\mathcal{DA}}(X, Y) : \ \theta_K = ker\, \xi \},$$

$\theta_0(\xi) = \langle \theta_0(\xi)_K, \theta_0(\xi)_B \rangle$. Pokazaćemo da tada dinamička algebra

$$\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle = \frac{\mathbf{F}_{\mathcal{DA}}(X, Y)}{\theta_0(\xi)}$$

zadovoljava sve tražene uslove.

Neka je $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ i $h_\xi : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{D}$ sirjektivni homomorfizam, $h_\xi = \langle h_{\xi,K}, h_{\xi,B}\rangle$, takav da je $h_{\xi,K} = \xi$ (lako se vidi da postoji bar jedan takav homomorfizam). Očito, važi $\theta_0(\xi) \subseteq ker(h_\xi)$, što povlači

$$(ker(h_\xi)/\theta_0(\xi)) \in Con\,(\mathbf{F}_{\mathcal{DA}}(X,Y)/\theta_0(\xi))$$

i

$$\frac{\left(\frac{\mathbf{F}_{\mathcal{DA}}(X,Y)}{\theta_0(\xi)}\right)}{\left(\frac{ker(h_\xi)}{\theta_0(\xi)}\right)} \cong \frac{\mathbf{F}_{\mathcal{DA}}(X,Y)}{ker(h_\xi)} \cong \mathbf{D}.$$

Ovo nam omogućava da u slučaju homomorfizma h_ξ za φ i ψ uzmemo odgovarajuće prirodne homomorfizme.

Neka je sada $h : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{D}$ proizvoljan sirjektivni homomorfizam. Po Lemi 6.3.17, postoji endomorfizam η na $\mathbf{F}_{\mathcal{DA}}(X,Y)$ takav da je $h = \eta \circ h_\xi$. Sada za h_ξ već imamo traženu dekompoziciju $h_\xi = \varphi_\xi \circ \psi$. Stoga definišimo $\varphi = \eta \circ \varphi_\xi$.

Pokažimo sada da je φ injektivno nad Y. Nije teško videti da za svaku Kleenejevu algebru $\mathbf{K}$ postoji dinamička algebra sa regularnim nosačem $\mathbf{K}$ i netrivijalnim Booleovim nosačem (dinamičke algebre $\mathsf{Ts}(\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(\emptyset))$, odnosno $\langle \mathbf{K}, \{\bot, \top\}, \langle\cdot\rangle\cdot\rangle$ tako da je $\langle 0\rangle p = \bot$ i $\langle a\rangle p = p$ za sve $a \in K \setminus \{0\}$, $p \in \{\bot, \top\}$, su primeri te vrste). Ako uočimo preslikavanje $g : Y \to B$ dato sa $g(y_i) = \bot$ i $g(y_j) = \top$ za sve $j \neq i$, tada se par preslikavanja $\langle \xi, g\rangle$ (jedinstveno) proširuje do homomorfizma $\mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{D}$ čija je prva komponenta ξ, što pokazuje da

$$\langle y_i, y_j\rangle \notin \theta_0(\xi)_B$$

za sve $y_i, y_j \in Y$. Traženi zaključak sledi po konstrukciji homomorfizma φ.

Kako bismo pokazali da $\mathsf{Os}(\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle)$ ima osobinu univerzalnog preslikavanja nad Y u $\mathcal{DA}(\mathbf{K})$ (tj. da je reč o slobodnoj algebri tog varijeteta), označimo

$$\tilde{y}_i = \frac{y_i}{\theta_0(\xi)_B}.$$

Gornji elementi (algebre $\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle$) su različiti, zbog malopre dokazane injektivnosti φ nad Y. Neka je χ_0 preslikavanje definisano sa

$$\chi_0(\tilde{y}_i) = d_i,$$

gde su d_i elementi proizvoljne algebre $\mathbf{D}_0 \in \mathcal{DA}(\mathbf{K})$. Neka je $\mathbf{D}_0' = \mathsf{Ts}(\mathbf{D}_0)$. Sada postoji jedinstven homomorfizam $\chi' : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{D}_0'$ koji proširuje ξ na regularnom, odnosno χ_0 na Booleovom delu. Primenjujući prethodno

obrazloženu dekompoziciju homomorfizma χ', dobijamo $\chi' = \varphi' \circ \psi'$. Preslikavanje $\chi : \mathsf{Os}(\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle) \to \mathbf{D}_0$ definisano sa

$$\chi(p) = \psi'_B(p)$$

je homomorfizam $\mathbf{K}$-dinamičkih algebri; osim toga, imamo

$$\chi(\bar{y}_i) = \chi(\varphi'_B(y_i)) = \psi'_B(\varphi'_B(y_i)) = \chi'_B(y_i) = d_i = \chi_0(\bar{y}_i^*),$$

pa stoga χ proširuje χ_0. Identifikacijom elemenata $\bar{y}_i$ sa odgovarajućim slovima y_i (odnosno, pogodnim preimenovanjem elemenata) dolazimo do traženog rezultata.

Na kraju, primetimo da, pošto je algebra sa osobinom univerzalnog preslikavanja nad datim skupom do na izomorfizam jedinstvena u svakom varijetetu, algebra $\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle$ ne može da zavisi od izbora sirjektivnog homomorfizma ξ. Drugim rečima, važi

$$\langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi}(Y), \langle\cdot\rangle\cdot\rangle \cong \langle \mathbf{K}, \mathbf{B}_{\mathbf{K},\xi'}(Y), \langle\cdot\rangle\cdot\rangle,$$

pa se indeks ξ može ispustiti.

(2) Radi kraće i jednostavnije notacije, uvedimo oznake $\mathbf{D} = \mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y)$ i $\mathbf{C} = \langle \mathbf{K}, \mathbf{B}_{\mathbf{K}}(Y), \langle\cdot\rangle\cdot\rangle$. Po tački *(1)*, važi $\mathbf{C} = \mathsf{Ts}(\mathbf{D})$.

Pretpostavimo prvo da imamo $\mathbf{C} \models p = q$, gde je

$$p = p(x_1, \ldots, x_m; y_1, \ldots, y_n), \quad q = q(x_1, \ldots, x_m; y_1, \ldots, y_n).$$

Tada za sve $a_1, \ldots, a_m \in K$ i $b_1, \ldots, b_n \in B_{\mathbf{K}}(Y)$ sledi

$$p^{\mathbf{C}}(a_1, \ldots, a_m; b_1, \ldots, b_n) = q^{\mathbf{C}}(a_1, \ldots, a_m; b_1, \ldots, b_n).$$

S druge strane, za svaki Booleov dinamički term t važi

$$t^{\mathbf{C}}(\varphi_K(x_1), \ldots, \varphi_K(x_m); b_1, \ldots, b_n) = (\hat{t}^{\varphi_K})^{\mathbf{D}}(b_1, \ldots, b_n),$$

pa dobijamo

$$(\hat{p}^{\varphi_K})^{\mathbf{D}}(b_1, \ldots, b_n) = (\hat{q}^{\varphi_K})^{\mathbf{D}}(b_1, \ldots, b_n)$$

za sve $b_1, \ldots, b_n \in B_{\mathbf{K}}(Y) = F_{\mathcal{DA}(\mathbf{K})}(Y)$, tj.

$$\mathbf{D} \models \hat{p}^{\varphi_K} = \hat{q}^{\varphi_K}.$$

Obratno, pođimo od gornjeg tvrđenja. Tada imamo

$$(\hat{p}^{\varphi_K})^{\mathbf{D}}(\varphi_B(y_1), \ldots, \varphi_B(y_n)) = (\hat{q}^{\varphi_K})^{\mathbf{D}}(\varphi_B(y_1), \ldots, \varphi_B(y_n)),$$

pa je, po već razmotrenim jednakostima,

$$p^{\mathbf{C}}(\varphi_K(x_1),\dots,\varphi_K(x_m);\varphi_B(y_1),\dots,\varphi_B(y_n)) =$$

$$= q^{\mathbf{C}}(\varphi_K(x_1),\dots,\varphi_K(x_m);\varphi_B(y_1),\dots,\varphi_B(y_n)).$$

Kako p i q nisu regularni termi, poslednja jednakost je ekvivalentna sa

$$\varphi_B(p(x_1,\dots,x_m;y_1,\dots,y_n)) = \varphi_B(q(x_1,\dots,x_m;y_1,\dots,y_n)).$$

Ali, ovo po definiciji homomorfizma $\varphi : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{C}$ znači, u stvari, da je $\mathbf{C} \models p = q$.

(3) Neka je $\mathbf{D} = \langle \mathbf{K}', \mathbf{B}', \langle\cdot\rangle\cdot\rangle \in \mathcal{DA}(\mathcal{V})$. Primetimo najpre da je $\mathbf{K}' \in \mathcal{V}$. Koristeći *(1)*, dobijamo dekompoziciju homomorfizma $h : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \mathbf{D}$ u obliku $h = \varphi \circ \psi$, gde je $\varphi : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \langle \mathbf{K}', \mathbf{B}_{\mathbf{K}'}(Y), \langle\cdot\rangle\cdot\rangle$. Nije teško videti da će tačka *(3)* biti pokazana ako φ razložimo u obliku $\varphi = \mu \circ \nu$, gde je $\mu : \mathbf{F}_{\mathcal{DA}}(X,Y) \to \langle \mathbf{F}_{\mathcal{V}}(X), \mathbf{B}_{\mathbf{F}_{\mathcal{V}}(X)}(Y), \langle\cdot\rangle\cdot\rangle$ sirjektivni homomorfizam koji proširuje identička preslikavanja na odgovarajućim generatornim skupovima, tj. ako dokažemo da je $ker(\mu) \subseteq ker(\varphi)$.

Najpre, ako je $\mu_K(r) = \mu_K(s)$ za neke regularne izraze r, s, tada

$$\begin{aligned} &\Rightarrow \quad \mathbf{F}_{\mathcal{V}}(X) \models r = s \\ &\Rightarrow \quad \mathcal{V} \models r = s \\ &\Rightarrow \quad \mathbf{K}' \models r = s \\ &\Rightarrow \quad \varphi_K(r) = \varphi_K(s). \end{aligned}$$

S druge strane, ako su p, q Booleovi termi takvi da je $\mu_B(p) = \mu_B(q)$, sledi

$$\begin{aligned} &\Rightarrow \quad \mathcal{DA}(\mathbf{F}_{\mathcal{V}}(X)) \models \hat{p}^{\mu_K} = \hat{q}^{\mu_K} && \text{(zbog } \textit{(1)} \text{ i } \textit{(2)}\text{)} \\ &\Rightarrow \quad \mathcal{DA}(\mathbf{K}') \models \hat{p}^{\varphi_K} = \hat{q}^{\varphi_K} && \text{(L. 6.3.16, } ker(\mu_K) \subseteq ker(\varphi_K)\text{)} \\ &\Rightarrow \quad \mathsf{Os}(\langle \mathbf{K}', \mathbf{B}_{\mathbf{K}'}(Y), \langle\cdot\rangle\cdot\rangle) \models \hat{p}^{\varphi_K} = \hat{q}^{\varphi_K} && \\ &\Rightarrow \quad \langle \mathbf{K}', \mathbf{B}_{\mathbf{K}'}(Y), \langle\cdot\rangle\cdot\rangle \models p = q && \text{(zbog } \textit{(2)}\text{)} \\ &\Rightarrow \quad \varphi_B(p) = \varphi_B(q), && \end{aligned}$$

čime je naš cilj postignut.

(4) Prema *(1)* i *(3)*, za specijalni slučaj $\mathcal{V} = \mathcal{KA}$ (imajući u vidu da je $\mathcal{DA}(\mathcal{KA}) = \mathcal{S}$) važi

$$\langle \mathbf{Reg}(X), \mathbf{B}_{\mathbf{Reg}(X)}(Y), \langle\cdot\rangle\cdot\rangle = \mathbf{F}_{\mathcal{S}(\mathcal{KA})}(X,Y).$$

Koristeći tačku *(1)* i Teoremu 6.3.14, dobijamo da je algebra $\mathbf{F}_{\mathcal{DA}(\mathbf{Reg}(X))}(Y)$ separabilna za proizvoljan skup Y. ∎

Gornji niz tvrđenja nam sada omogućava da dokažemo separabilnost slobodnih algebri za čitavu klasu varijeteta Jónssonovih dinamičkih algebri. Ali, pre glavnog rezultata koji opisuje tu klasu, potreban nam je još jedan pomoćni rezultat.

LEMA 6.3.19. *Neka je X proizvoljan skup, $\mathcal{V}$ podvarijetet od $\mathcal{KA}$ i neka je $\alpha : \mathbf{T}_X \to \mathbf{F}_{\mathcal{V}}(X)$ homomorfizam koji proširuje identičko preslikavanje na X. Tada $\mathbf{F}_{\mathcal{DA}(\mathcal{V})}(X,Y) \models p = q$ (gde su p, q Booleovi termi) ako i samo ako postoje termi p_1, q_1 takvi da je $\hat{p}_1^\alpha = \hat{p}^\alpha$, $\hat{q}_1^\alpha = \hat{q}^\alpha$ i $\mathcal{S} \models p_1 = q_1$.*

Dokaz. Za (dinamički) term t, označimo sa $\bar{t}$ vrednost terma t u slobodnoj dinamičkoj algebri $\mathbf{F}_{\mathcal{DA}}(X,Y)$ u odnosu na standardnu interpretaciju (u kojoj se promenljivama dodeljuju odgovarajući slobodni generatori). Sada nije teško videti da je za proizvoljan podvarijetet $\mathcal{V} \leq \mathcal{KA}$, relacija $\rho(\mathcal{V})$ definisana na oba nosača algebre $\mathbf{F}_{\mathcal{DA}}(X,Y)$ sa

$$\langle \bar{p}, \bar{q} \rangle \in \rho(\mathcal{V}) \;\Leftrightarrow\; Eq(\mathcal{V}) \vdash p = q \;\Leftrightarrow\; \mathcal{DA}(\mathcal{V}) \models p = q,$$

$\rho(\mathcal{V}) = \langle \rho_K(\mathcal{V}), \rho_B(\mathcal{V}) \rangle$, kongruencija. Pri tome se lako vidi da je za Booleove terme p, q iskaz $\langle \bar{p}, \bar{q} \rangle \in \rho_B(\mathcal{V})$ ekvivalentan sa

$$\hat{p}^\alpha = \hat{q}^\alpha.$$

Osim toga, očito imamo $\rho(\mathcal{KA}) \subseteq \rho(\mathcal{V})$, što povlači

$$\rho(\mathcal{V}) = \rho(\mathcal{KA}) \circ \rho(\mathcal{V}) = \rho(\mathcal{V}) \circ \rho(\mathcal{KA}) \circ \rho(\mathcal{V}).$$

Sada gornja jednakost, zajedno sa prethodnim primedbama i činjenicom da je

$$\mathbf{F}_{\mathcal{DA}(\mathcal{V})}(X,Y) \cong \frac{\mathbf{F}_{\mathcal{DA}}(X,Y)}{\rho(\mathcal{V})},$$

dokazuje tvrđenje leme. ∎

Najzad, dajemo glavni rezultat iz [41] o separabilnosti slobodnih $\mathbf{K}$-dinamičkih algebri.

TEOREMA 6.3.20. (Crvenković, Dolinka, [41]) *Neka je $\mathcal{K}$ klasa svih Kleenejevih algebri $\mathbf{K}$ takvih da su slobodne algebre varijeteta $\mathcal{DA}(\mathbf{K})$ separabilne (ili, ekvivalentno, klasa svih regularnih komponenti separabilnih dinamičkih algebri). Tada je $\mathcal{K}$ kvazivarijetet koji sadrži sve standardne Kleenejeve algebre, kao i klasu $\mathcal{F}$ svih slobodnih algebri svih podvarijeteta od $\mathcal{KA}$. Specijalno, za sve Kleenejeve algebre $\mathbf{K} \in \mathsf{ISPP}_U(\mathcal{SKA} \cup \mathcal{F})$ (gde je $\mathcal{SKA}$ klasa svih standardnih Kleenejevih algebri), varijetet $\mathcal{DA}(\mathbf{K})$ ima separabilne slobodne algebre.*

Dokaz. Na početku, primetimo da za $\mathbf{K} = \mathbf{Reg}(X)$ tvrđenje sledi iz Propozicije 6.3.18, *(4)*.

Neka je sada $\mathcal{V} \leq \mathcal{KA}$ i $\mathbf{K} = \mathbf{F}_{\mathcal{V}}(X)$ za neki skup X. Jasno, algebra $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y)$ je separabilna ako i samo ako je to (dvosortna) dinamička algebra $\mathsf{Ts}(\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y))$. Prema Propoziciji 6.3.18, *(3)*, ova dinamička algebra je izomorfna sa $\mathbf{F}_{\mathcal{DA}(\mathcal{V})}(X, Y)$. Primenimo sada Lemu 6.3.19 na terme $p = \langle r_1 \rangle y$ i $q = \langle r_2 \rangle y$, gde je $y \in Y$, dok su r_1, r_2 regularni izrazi. Ako, dakle, $\mathbf{F}_{\mathcal{DA}(\mathcal{V})}(X, Y) \models p = q$, tada postoje regularni izrazi s_1, s_2 takvi da je $\alpha(r_1) = \alpha(s_1)$ i $\alpha(r_2) = \alpha(s_2)$ za prirodni homomorfizam $\alpha : \mathbf{T}_X \to \mathbf{K}$, i

$$\mathcal{S} \models \langle s_1 \rangle y = \langle s_2 \rangle y.$$

Kako su slobodne algebre varijeteta $\mathcal{S}$ separabilne, sledi da s_1 i s_2 predstavljaju iste regularne jezike, tj. $\mathcal{KA} \models s_1 = s_2$. Ali, tada $\mathcal{V} \models s_1 = s_2$, odakle $\mathcal{V} \models r_1 = r_2$ (jer $\alpha(r_i) = \alpha(s_i)$ za $i = 1, 2$ daje $\mathcal{V} \models r_i = s_i$). Drugim rečima, dobili smo da regularni izrazi r_1, r_2 (u odnosu na standardnu interpretaciju) predstavljaju iste elemente u $\mathbf{K}$, što znači da za sve $a, b \in K$,

$$\mathcal{DA}(\mathbf{K}) \models f_a(y) = f_b(y)$$

povlači $a = b$.

Dalje, pretpostavimo da je $\mathbf{K}$ Kleenejeva algebra za koju varijetet $\mathcal{DA}(\mathbf{K})$ ima separabilne slobodne algebre i $\mathbf{K}' \leq \mathbf{K}$. Tada je algebra $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(\emptyset)$ separabilna, pa to važi i za njen redukt tipa $\tau(\mathbf{K}')$, koji pripada $\mathcal{DA}(\mathbf{K}')$. Međutim, reč je o homomorfnoj slici algebre $\mathbf{F}_{\mathcal{DA}(\mathbf{K}')}(\emptyset)$, pa zbog toga ova slobodna algebra mora takođe biti separabilna, odakle su sve slobodne algebre u $\mathcal{DA}(\mathbf{K}')$ separabilne.

Neka je sada $\langle \mathbf{K}_i \rangle_{i \in I}$ familija Kleenejevih algebri sa osobinom da su slobodne algebre $\mathbf{F}_{\mathcal{DA}(\mathbf{K}_i)}(\emptyset)$ separabilne. Tada uočimo algebru

$$\mathbf{D} = \langle \prod_{i \in I} \mathbf{B}_i, f_{\mathbf{a}} \rangle_{\mathbf{a} \in \prod_{i \in I} \mathbf{K}_i} \in \mathcal{DA}(\prod_{i \in I} \mathbf{K}_i),$$

pri čemu su unarni operatori definisani sa

$$f_{\mathbf{a}}(x) = \langle f_{a_i}(x_i) \rangle_{i \in I}.$$

Sada je $\mathbf{D}$ očito separabilna dinamička algebra, odakle se analogno kao i u prethodnom pasusu izvodi zaključak da su sve slobodne $\prod_{i \in I} \mathbf{K}_i$-dinamičke algebre separabilne.

Najzad, klasa $\mathcal{SDA}$ je očito aksiomatizabilna, pa je zatvorena za ultraproizvode. Tako, ako uzmemo, kao i malopre, familiju $\langle \mathbf{K}_i \rangle_{i \in I}$ Kleenejevih

algebri sa osobinom da su slobodne algebre $\mathbf{F}_{\mathcal{DA}(\mathbf{K}_i)}(\emptyset)$ separabilne, tada su separabilne i dinamičke algebre $\mathsf{Ts}(\mathbf{F}_{\mathcal{DA}(\mathbf{K}_i)}(\emptyset))$, pa to važi i za svaki ultraproizvod ovih algebri. Ali, tada je regularna komponenta ove algebre (označimo je sa $\mathbf{K}$) ultraproizvod Kleenejevih algebri $\mathbf{K}_i$, $i \in I$, odakle sledi da je $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(\emptyset)$ separabilna $\mathbf{K}$-dinamička algebra. Drugim rečima, klasa $\mathcal{K}$ je zatvorena i na ultraproizvode.

Činjenica da $\mathbf{K} \cong \mathbf{K}'$ implicira

$$\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y) \cong \mathbf{F}_{\mathcal{DA}(\mathbf{K}')}(Y)$$

za sve skupove Y, i primedba da za sve $\mathbf{K} \in \mathcal{SKA}$ varijeteti $\mathcal{DA}(\mathbf{K})$ imaju separabilne slobodne algebre, okončavaju dokaz teoreme. ∎

PROBLEM 9. *Opisati kvazivarijetet Kleenejevih algebri $\mathcal{K}$ iz prethodne teoreme. Po mogućnosti, dati aksiomatizaciju za $\mathcal{K}$ preko kvazi-identiteta. Da li je klasa $\mathcal{K}$ uopšte konačno aksiomatizabilna?*

6.4. Neprekidnost dinamičkih algebri

U Glavi 2 smo definisali neprekidnost Kleenejevih algebri. U izvesnom smislu, one odgovaraju intuiciji koja je motivisala uvođenje operacije *. Naime, očekujemo da * uvek bude "refleksivno-tranzitivno zatvorenje", tj. da je za proizvoljan element a date Kleenejeve algebre, a^* supremum (u odnosu na odgovarajući polumrežni poredak) suma $a^0 + a^1 + \ldots + a^n$, $n \geq 0$ (gde je $a^0 = 1$ i $a^1 = a$). Međutim, primer Conwayevog skoka $\mathbf{C}_4$ pokazuje da ovo naše očekivanje nije ispunjeno, tj. da postoji Kleenejeva algebra koja nije neprekidna. U ovoj algebri je za sve $n \geq 1$, $F^n = F$ (F, podsetimo se, označava klasu ekvivalencije koju čine konačni jezici), pa je stoga F supremum odgovarajućih suma, ali je, s druge strane, $F^* = \infty \neq F$.

Dinamičke algebre pružaju mogućnost da se problem neprekidnosti razmatra nešto preciznije, ali u osnovi, situacija nije ništa bolja nego u slučaju Kleenejevih algebri. Naprotiv, pokazalo se da klasa neprekidnih dinamičkih (Kleenejevih) algebri čak nije ni aksiomatizabilna formulama prvog reda, pa stoga ove algebre, ma kako prirodne bile, čine, sa stanovišta matematičke logike, prilično "neuhvatljivu" klasu.

Dinamička algebra $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot \rangle$ je *neprekidna* ako iz $\langle a^n \rangle p \leq q$ za sve $n \geq 0$, sledi $\langle a^* \rangle p \leq q$. Drugim rečima,

$$\langle a^* \rangle p = \bigvee_{n \geq 0} \langle a^n \rangle p.$$

Kozen u [83] *definiše* dinamičke algebre tako da od njih zahteva neprekidnost. Primetimo da, iako $\mathbf{C}_4$ nije neprekidna Kleenejeva algebra, dinamičke algebre sa regularnim delom jednakim $\mathbf{C}_4$ (odnosno, $\mathbf{C}_4$-dinamičke algebre, gde se za Jónssonove dinamičke algebre neprekidnost definiše analogno) *jesu* neprekidne, pošto upravo imamo neseparabilnost elemenata F i ∞: važi $\langle F\rangle p = \langle\infty\rangle p = \langle F^*\rangle p$ (po Propoziciji 6.3.12). Međutim, postoji (čak, separabilna) dinamička algebra koja nije neprekidna.

Neka je $\mathbf{B}$ puna Booleova skupovna algebra ordinala $\omega^+ = \omega \cup \{\omega\}$ i neka je $\mathbf{K} \leq \mathbf{Rel}(\mathcal{P}(\omega^+))$ algebra koja se sastoji od svih normalnih unarnih operatora na $\mathbf{B}$ (konačno aditivnih funkcija f na $\mathbf{B}$ za koje je $f(\emptyset) = \emptyset$), pri čemu funkcije deluju na elemente $\mathbf{B}$ (tj. podskupove od ω^+) na prirodan način (primetimo da *nije* reč o KDA, jer $\mathbf{K}$ nije podalgebra od $\mathbf{Rel}(\omega^+)$). Označimo sa ϕ sledeći normalni operator $B \to B$ (ovde je $A \subseteq \omega^+$):

$$\phi(A) = \begin{cases} \{\alpha + 1 : \alpha \in A\} & A \text{ je konačan,} \\ \{\alpha + 1 : \alpha \in A\} \cup \{\omega\} & A \text{ je beskonačan,} \end{cases}$$

pri čemu je $\omega + 1 = \omega$. Sada se lako dobija da je

$$\bigvee_{n \geq 0} \langle \phi^n \rangle \{0\} = \omega,$$

ali

$$\langle \phi^* \rangle \{0\} = \omega^+,$$

pa dinamička algebra $\langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot\rangle$ nije neprekidna.

S druge strane, sve reprezentabilne dinamičke algebre su očito neprekidne (Kozen je pokazao da je ovde reč o strogoj inkluziji). Odavde se odmah vidi da neprekidne dinamičke algebre ne čine varijetet, jer bi u suprotnom sve algebre iz $\mathsf{HSP}(\mathcal{RDA}) = \mathcal{S}$ bile neprekidne, a što smo u gornjem primeru videli da nije slučaj. Štaviše, neprekidne dinamičke algebre ne čine čak ni aksiomatizabilnu klasu.

TEOREMA 6.4.1. (Kozen, [85]) *Klase neprekidnih Kleenejevih, odnosno neprekidnih dinamičkih algebri nisu zatvorene na ultraproizvode, pa stoga nisu aksiomatizabilne formulama prvog reda. Takođe, isto važi i za klasu $\mathcal{RDA}$.*

Može se pokazati da je malopre prikazani primer dinamičke algebre koja nije neprekidna zapravo jedan ultrastepen pune KDA na skupu ω.

Danas je poznata tačna karakterizacija aksiomatizabilnih klasa koje se sastoje od neprekidnih (reprezentabilnih) dinamičkih algebri, što čini pojačanje gornjeg tvrđenja.

TEOREMA 6.4.2. (Andréka, Guessarian, Németi, [12]) *Klasa $\mathcal{K}$ neprekidnih dinamičkih algebri (odnosno, $\mathcal{K} \subseteq \mathcal{RDA}$) je zatvorena na ultraproizvode ako i samo ako je klasa redukata algebri iz $\mathcal{K}$ bez * zatvorena na ultraproizvode i operacija * se nad $\mathcal{K}$ može izraziti preko ostalih operacija.*

S druge strane, klasa neprekidnih dinamičkih algebri je, baš kao i $\mathcal{RDA}$, zatvorena na podalgebre i direktne proizvode. Ovakve klase se nazivaju *uopšteni kvazivarijeteti* i one imaju veliki značaj u teorijskom računarstvu (algebarska specifikacija struktura podataka i sl.). Takve klase su određene *uopštenim kvazi-identitetima*, gde su *uopštene formule* objekti koji se dobijaju na isti način kao i obične formule, sa jedinom razlikom što je dopuštena primena beskonačno mnogo iskaznih veznika $\wedge, \vee$ (tj. logičkih veznika beskonačne arnosti). Nije teško videti da je ustvari reč o logici drugog reda, gde je dozvoljena ograničena kvantifikacija po nekom ordinalu.

6.5. Odlučivost jednakosnih teorija dinamičkih algebri

Verovatno najveća razlika u pogledu jednakosnih osobina dinamičkih i **K**-dinamičkih algebri nastaje kada su u pitanju problemi odlučivosti. Naime, Fischer i Ladner [61, 62] su 1977. pokazali da je jednakosna teorija klase $\mathcal{RDA}$ odlučiva, pokazavši da za svaki identitet koji je izgrađen od n simbola koji ne važi na $\mathcal{RDA}$, ne važi već na nekoj KDA nad skupom U tako da je $|U|$ ograničeno eksponencijalnom funkcijom po n (što znači da odgovarajući algoritam zahteva eksponencijalno vreme). Po ranije dokazanim tvrđenjima, ovo povlači da varijeteti $\mathcal{S}$, odnosno $\mathcal{DA}$ imaju odlučive jednakosne teorije.

S druge strane, Crvenković i Madarász [51] su 1994. pokazali da postoji Kleenejeva algebra **K** sa osobinom da varijetet $\mathcal{DA}(\mathbf{K})$ ima neodlučivu jednakosnu teoriju. To je, ako se detaljnije proanalizira, i prirodno, jer dok jednakosna teorija dinamičkih algebri na regularnoj koordinati "krije" odlučivu jednakosnu teoriju Kleenejevih algebri, odnosno regularne identitete, dotle je, putem unarnih operatora, u jednakosnu teoriju varijeteta $\mathcal{DA}(\mathbf{K})$ "utisnut" problem reči za konkretnu algebru **K**. Postojanje Kleenejeve algebre sa nerešivim problemom reči (Posledica 1.6.2) onda direktno daje malopre opisani rezultat.

Iz ovih razloga, prirodno se postavlja pitanje karakterizacije onih Kleenejevih algebri **K** za koje $\mathcal{DA}(\mathbf{K})$ ima odlučivu jednakosnu teoriju. U [41] je opisana jedna klasa Kleenejevih algebri sa tom osobinom, i ovde ćemo prikazati odgovarajuća tvrđenja. Ali, najpre ćemo u najgrubljim crtama skicirati kako su Fischer i Ladner u [61] dokazali odlučivost jednakosne teorije dinamičkih algebri.

Za skup Booleovih terma T na jeziku dinamičkih algebri ćemo reći da je *FL-zatvoren* ako on ima sledećih šest osobina (gde su a, b regularni, a p, q Booleovi termi):

1. $p \vee q \in T \Rightarrow p, q \in T$,
2. $\neg p \in T \Rightarrow p \in T$,
3. $\langle x \rangle p \in T \Rightarrow p \in T$, gde je x regularna promenljiva,
4. $\langle a + b \rangle p \in T \Rightarrow \langle a \rangle p, \langle b \rangle p, p \in T$,
5. $\langle ab \rangle p \in T \Rightarrow \langle a \rangle \langle b \rangle p, \langle b \rangle p, p \in T$,
6. $\langle a^* \rangle p \in T \Rightarrow p, \langle a \rangle \langle a^* \rangle p \in T$.

Osim toga, za term p sa $||p||$ označavamo dužinu od p, tj. ukupan broj simbola koji se pojavljuju u p. Pokazuje se da gornja definicija određuje jedan operator zatvorenja na skupu svih Booleovih terma, pa postoji *FL-zatvorenje* datog skupa terma T, najmanja FL-zatvorena familija koja sadrži T. Sada navodimo prvu od dve ključne leme iz [61].

LEMA 6.5.1. (Fischer, Ladner, [61]) *Neka je T skup Booleovih terma na jeziku dinamičkih algebri. Tada postoji FL-zatvoren skup $T' \supseteq T$ takav da je*

$$|T'| \leq \sum_{p \in T} ||p||.$$

Specijalno, FL-zatvorenje konačnog skupa Booleovih terma je konačan skup.

Gornja lema je bila, u stvari, "ključni sastojak" u dokazu Teoreme 6.3.2, koji je omogućio Prattu da dokaže postojanje filtracija, iz čega onda, kao što smo videli, sledi većina klasičnih rezultata o varijetetima dinamičkih algebri.

Neka je sada $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle \cdot \rangle \cdot \rangle$ KDA nad skupom U i v neka valuacija u $\mathbf{D}$ (preslikavanje koje svakoj regularnoj promenljivoj dodeljuje binarnu relaciju na U iz $\mathbf{K}$, a svakoj Booleovoj promenljivoj podskup od U koji pripada $\mathbf{B}$), i neka je T skup Booleovih terma. Uvodimo relaciju ekvivalencije $\equiv_{v,T}$ na osnovnom skupu U na sledeći način ($u_1, u_2 \in U$):

$$u_1 \equiv_{v,T} u_2 \Leftrightarrow (\forall p \in T)(u_1 \in p^{\mathbf{D}}(v) \Leftrightarrow u_2 \in p^{\mathbf{D}}(v)).$$

Ova relacija nam omogućava da, polazeći od $\mathbf{D}$, definišemo KDA $\mathbf{D}_{v,T}$ na skupu $U/\equiv_{v,T}$, čiji se Booleov deo sastoji od skupova oblika

$$\frac{U_1}{\equiv_{v,T}} = \{u/\equiv_{v,T}: \ u \in U_1\},$$

$U_1 \in B$, odnosno, sa regularnim delom koji čine relacije

$$\frac{\rho}{\equiv_{v,T}} = \{\langle u_1/\equiv_{v,T}, u_2/\equiv_{v,T}\rangle : \langle u_1, u_2\rangle \in \rho\},$$

$\rho \in K$. Takođe, definišemo valuaciju $\bar{v}$ tako da je za proizvoljnu promenljivu x (bilo regularnog, bilo Booleovog tipa):

$$\bar{v}(x) = \frac{v(x)}{\equiv_{v,T}}.$$

LEMA 6.5.2. (Fischer, Ladner, [61]) *Neka je* $\mathbf{D}$ *KDA nad* U, v *valuacija u* $\mathbf{D}$, *a* T *skup Booleovih terma. Tada za sve* $u \in U$ *i* $p \in T$ *važi:*

$$u \in p^{\mathbf{D}}(v) \text{ ako i samo ako } u/\equiv_{v,T} \in p^{\mathbf{D}_{v,T}}(\bar{v}).$$

Booleov term p je *zadovoljiv* ako postoji KDA $\mathbf{D}$ i valuacija v u $\mathbf{D}$ tako da $p^{\mathbf{D}}(v) \neq \emptyset$ (tj. ako u $\mathbf{D}$ ne važi identitet $p = \bot$). Jasno, provera Booleovog identiteta na $\mathbf{D}$ se svodi na proveru zadovoljivosti nekog terma na $\mathbf{D}$, budući da se lako vidi da je identitet

$$p = q$$

ekvivalentan sa

$$(\neg p \wedge q) \vee (p \wedge \neg q) = \bot.$$

Tako $p = q$ važi na $\mathcal{RDA}$ ako i samo ako term $(\neg p \wedge q) \vee (p \wedge \neg q)$ *nije* zadovoljiv. Zbog toga, naredna teorema daje algoritam za odlučivanje Booleovih identiteta u $\mathcal{RDA}$.

TEOREMA 6.5.3. (Fischer, Ladner, [61]) *Neka je* p *zadovoljiv term. Tada postoji KDA* $\mathbf{D}$ *nad skupom* U *takvim da* $|U| \leq 2^{||p||}$ *u kojoj ne važi* $p = \bot$.

Dokaz. Neka je $\mathbf{D}$ proizvoljna KDA za koju postoji valuacija v u odnosu na koju je $p^{\mathbf{D}}(v) \neq \emptyset$. Po Lemi 6.5.1, postoji konačan FL-zatvoren skup T koji sadrži term p, takav da je $|T| \leq ||p||$. Međutim, tada po Lemi 6.5.2 važi

$$p^{\mathbf{D}_{v,T}}(\bar{v}) \neq \emptyset,$$

pa KDA $\mathbf{D}_{v,T}$ takođe ne zadovoljava identitet $p = \bot$. Time je dokaz teoreme okončan, pošto za osnovni skup ove KDA važi

$$\left|\frac{U}{\equiv_{v,T}}\right| \leq 2^{|T|}$$

(jer ako za $u \in U$ definišemo

$$T_u = \{p \in T : u \in p^{\mathbf{D}}(v)\},$$

tada očito imamo $u_1 \equiv_{v,T} u_2$ ako i samo ako $T_{u_1} = T_{u_2}$; stoga $\equiv_{v,T}$ može imati na U najviše onoliko klasa koliko T ima podskupova). ∎

Prema tome, da bismo proverili da li identitet $p = q$ važi na klasi $\mathcal{RDA}$ (odnosno, na varijetetu $\mathcal{S} = \mathsf{HSP}(\mathcal{RDA})$), dovoljno je konstruisati (do na izomorfizam) sve KDA sa osnovnim skupovima kardinalnosti ne veće od $2^{\|r\|}$, gde je $r = (\neg p \wedge q) \vee (p \wedge \neg q)$ (kojih ima konačno mnogo), i videti da li je r zadovoljiv na nekoj od njih, kada $\mathcal{RDA} \not\models p = q$. Ako to nije slučaj, tada, po prethodnoj teoremi, $p = q$ važi na svim reprezentabilnim dinamičkim algebrama (a time i na svim separabilnim dinamičkim algebrama). Kako se jednakosne teorije varijeteta $\mathcal{S}$ i $\mathcal{DA}$ razlikuju (po Posledici 6.3.11) samo za odlučivu jednakosnu teoriju $Eq(\mathcal{KA})$ (pri čemu je regularna teorija varijeteta $\mathcal{DA}$ trivijalna), odmah se dobija

POSLEDICA 6.5.4. *Varijeteti $\mathcal{DA}$ i $\mathcal{S}$ imaju odlučive jednakosne teorije.*

Podsetimo se da smo u Lemi 1.3.1 za svaku polugrupu konstruisali Kleenejevu algebru $\mathbf{M}(S^1)$ koja se sastoji od kompleksa monoida S^1. Da je zaista reč o Kleenejevoj algebri, pokazali smo tako što smo je potopili u Kleenejevu relacionu algebru $\mathbf{Rel}(S^1)$. Pri tome je uspostavljen izomorfizam između $\mathbf{M}(S^1)$ i podalgebre od $\mathbf{Rel}(S^1)$ tako što proizvoljnom podskupu od S^1 odgovara unija desnih translacija monoida S^1 pridruženih elementima uočenog podskupa. Sličnu konstrukciju ćemo imati i u ovom slučaju. Podsetimo se, *leva translacija* monoida S^1 je funkcija

$$\lambda_a = \{\langle s, as\rangle : \ s \in S^1\},$$

$a \in S^1$. Ali, sada možemo uočiti jednu manju podalgebru od $\mathbf{Rel}(S^1)$: podalgebru *generisanu* levim translacijama. Tu podalgebru (u skladu sa notacijom iz [51]) označavamo sa $\Psi(S^1)$. Sada definišemo reprezentabilnu $\Psi(S^1)$-dinamičku algebru $\mathbf{D}(S^1)$ tako da je njena "osnovna" Booleova algebra puna skupovna algebra nad S^1. Osnovu za prenos nerešivosti problema reči za Kleenejeve algebre na neodlučivost jednakosnih teorija nekih varijeteta Jónssonovih dinamičkih algebri predstavlja sledeće tvrđenje.

LEMA 6.5.5. (Crvenković, Madarász, [51, Lema 3.7]) *Neka je S monoid prezentiran sa $\langle G, R\rangle$ i neka je $a_1, \ldots, a_n, b_1, \ldots, b_m \in G$. Tada*

$$S_G \models a_1 \ldots a_n = b_1 \ldots b_m$$

ako i samo ako

$$\mathbf{D}(S) \models f_{\lambda_{a_1}}(\ldots(f_{\lambda_{a_n}}(x))) = f_{\lambda_{b_1}}(\ldots(f_{\lambda_{b_m}}(x))).$$

Dokaz. Najpre, primetimo da je (zbog prisustva jediničnog elementa)

$$S_G \models a_1 \dots a_n = b_1 \dots b_m$$

ekvivalentno sa

$$\lambda_{a_1} \circ \dots \circ \lambda_{a_n} = \lambda_{a_1 \dots a_n} = \lambda_{b_1 \dots b_m} = \lambda_{b_1} \circ \dots \circ \lambda_{b_m}.$$

Pri tome je $\Lambda_G = \{\lambda_g : g \in G\}$ očito generatorni skup za monoid levih translacija na S. Odavde, međutim, imamo da je Λ_G generatorni skup ujedno i za Kleenejevu algebru $\Psi(S)$, i osim toga, u $\Psi(S)$ takođe važi gornja jednakost. Zbog toga u $\mathbf{D}(S)$ važe identiteti

$$f_{\lambda_{a_1}}(\dots(f_{\lambda_{a_n}}(x))) = f_{\lambda_{a_1} \circ \dots \circ \lambda_{a_n}}(x) = f_{\lambda_{b_1} \circ \dots \circ \lambda_{b_m}}(x) = f_{\lambda_{b_1}}(\dots(f_{\lambda_{b_m}}(x))).$$

Obratno, ako $S_G \not\models a_1 \dots a_n = b_1 \dots b_m$, tada je

$$\lambda_{a_1 \dots a_n} \neq \lambda_{b_1 \dots b_m},$$

pa imamo

$$\begin{aligned} f_{\lambda_{a_1}}(\dots(f_{\lambda_{a_n}}(\{1\}))) &= f_{\lambda_{a_1} \circ \dots \circ \lambda_{a_n}}(\{1\}) = \{a_1 \dots a_n\}, \\ f_{\lambda_{b_1}}(\dots(f_{\lambda_{b_m}}(\{1\}))) &= f_{\lambda_{b_1} \circ \dots \circ \lambda_{b_m}}(\{1\}) = \{b_1 \dots b_m\}, \end{aligned}$$

čime je lema dokazana. ∎

Ako sada za S uzmemo bilo koji monoid sa nerešivim problemom reči, imaćemo da ni $\Psi(S)$ nema rešiv problem reči, što upravo vodi traženom varijetetu Jónssonovih dinamičkih algebri sa neodlučivom jednakosnom teorijom.

TEOREMA 6.5.6. (Crvenković, Madarász, [51]) *Neka je S monoid sa nerešivim problemom reči. Tada varijetet $\mathcal{DA}(\Psi(S))$ ima neodlučivu jednakosnu teoriju.*

Dokaz. Kako $\mathbf{D}(S) \in \mathcal{DA}(\Psi(S))$, to iz pretpostavke da $\mathcal{DA}(\Psi(S))$ zadovoljava identitet oblika

$$f_{\lambda_{a_1}}(\dots(f_{\lambda_{a_n}}(x))) = f_{\lambda_{b_1}}(\dots(f_{\lambda_{b_m}}(x)))$$

sledi da $\mathbf{D}(S)$ zadovoljava gornji identitet, odakle po Lemi 6.5.5 dobijamo

$$S_G \models a_1 \dots a_n = b_1 \dots b_m.$$

Obratno, ako važi gornji uslov, tada je

$$\lambda_{a_1} \circ \dots \circ \lambda_{a_n} = \lambda_{b_1} \circ \dots \circ \lambda_{b_m},$$

pa identitet

$$f_{\lambda_{a_1}}(\dots(f_{\lambda_{a_n}}(x))) = f_{\lambda_{b_1}}(\dots(f_{\lambda_{b_m}}(x)))$$

sledi uzastopnom primenom aksiome (37), tj. važi na $\mathcal{DA}(\Psi(S))$. ∎

Na taj način dobijamo beskonačno mnogo Kleenejevih algebri kojima odgovaraju varijeteti Jónssonovih dinamičkih algebri sa nerekurzivnim jednakosnim teorijama. S druge strane, mogli smo, kao što se to obično zahteva u razmatranju algoritamskih problema za module i polugrupne algebre (vidi [81]), da isključimo Kleenejeve algebre indeksa kao izvor neodlučivosti za odgovarajuće varijetete dinamičkih algebri, tj. da pretpostavimo da su kako nosači, tako i operacije tih Kleenejevih algebri rekurzivni skupovi (odnosno, da te algebre imaju rešiv problem reči). To otvara sledeći problem.

PROBLEM 10. *Neka je* $\mathbf{K}$ *Kleenejeva algebra sa rešivim problemom reči. Da li je tada jednakosna teorija varijeteta* $\mathcal{DA}(\mathbf{K})$ *odlučiva? Specijalno, kakva je situacija sa konačnim Kleenejevim algebrama* $\mathbf{K}$*?*

Imajući u vidu težinu sličnih problema za polugrupne algebre, module, prstene i Lie algebre [81], verovatno je da je gornji problem takođe veoma težak.

U preostalom delu ovog poglavlja, biće izloženi neki parcijalni rezultati u vezi sa Problemom 10 do kojih se došlo u [41]. Glavni rezultat u tom pravcu je sledeći: ako se Kleenejeva algebra $\mathbf{K}$ može prikazati kao konačan direktan proizvod slobodnih algebri nekih podvarijeteta od $\mathcal{KA}$ generisanih standardnim Kleenejevim algebrama, tada $\mathcal{DA}(\mathbf{K})$ ima odlučivu jednakosnu teoriju. Da ovaj poslednji zaključak važi u slučaju kada je $\mathbf{K}$ slobodna Kleenejeva algebra, tj. neka algebra regularnih jezika, možemo zaključiti odmah, "prenosom" rezultata Fischera i Ladnera, uz korišćenje ključne Propozicije 6.3.18.

TEOREMA 6.5.7. *Varijetet* $\mathcal{DA}(\mathbf{Reg}(X))$ *ima odlučivu jednakosnu teoriju.*

Dokaz. Prema Propoziciji 6.3.18, *(1)*, *(2)* i *(4)*, očito imamo:

$$Eq(\mathcal{DA}(\mathbf{Reg}(X))) = \{\hat{p}^{\mathsf{L}} = \hat{q}^{\mathsf{L}} : \mathcal{S} \models p = q\},$$

gde je $\mathsf{L} : \mathbf{T}(X) \to \mathbf{Reg}(X)$ prirodni homomorfizam, zapravo preslikavanje koje svakom regularnom izrazu dodeljuje jezik koji predstavlja. Stoga se algoritam za odlučivanje da li dati identitet $t_1 = t_2$ važi u $\mathcal{DA}(\mathbf{Reg}(X))$ sastoji od sledećih koraka:

- najpre, pretpostavljamo da su svi regularni jezici koji se pojavljuju u indeksima unarnih operatora u termima t_1, t_2 dati na neki uniforman i konačan način: regularnim izrazom, odgovarajućim automatom koji ga prihvata, ili slično,

- na proizvoljan način rekonstruišimo terme p_1, p_2 za koje važi $\hat{p}_1^{\mathsf{L}} = t_1$ i $\hat{p}_2^{\mathsf{L}} = t_2$ (ovo se svodi na zamenu svakog podterma od t_i $(i = 1, 2)$ oblika $f_L(s)$ sa $\langle r \rangle s$, pri čemu je r regularan izraz takav da je $\mathsf{L}(r) = L$; primetimo da se, po prethodnoj tački, takvi regularni izrazi nalaze algoritamski, npr. analizom automata),
- koristeći algoritam Fischera i Ladnera, odlučujemo da li važi

$$\mathcal{S} \models p_1 = p_2.$$

Ako opisani algoritam daje pozitivan odgovor, jasno je da

$$\mathcal{DA}(\mathbf{Reg}(X)) \models t_1 = t_2.$$

Obratno, pretpostavimo da $t_1 = t_2$ važi na $\mathcal{DA}(\mathbf{Reg}(X))$. Tada postoje Booleovi dinamički termi q_1, q_2 tako da je $\hat{q}_1^{\mathsf{L}} = t_1$, $\hat{q}_2^{\mathsf{L}} = t_2$ i $\mathcal{S} \models q_1 = q_2$. Ali, tada po Lemi 6.3.19 (primenjenoj za $\mathcal{V} = \mathcal{KA}$) imamo

$$\mathcal{S} = \mathcal{DA}(\mathcal{KA}) \models p_1 = p_2,$$

odakle dobijamo da $t_1 = t_2$ važi na $\mathcal{DA}(\mathbf{Reg}(X))$. Prema tome, ovaj varijetet ima odlučivu jednakosnu teoriju. ∎

U daljem, potrebna nam je jedna konstrukcija koja je implicitno korišćena u dokazu Teoreme 6.3.20, ali sa dodatnim informacijama koje se mogu dobiti iz te konstrukcije. Podsetimo, u direktnom stepenu Y^I skupa Y, *dijagonalnim elementima* zovemo konstantna preslikavanja $I \to Y$.

LEMA 6.5.8. *Neka su* $\mathbf{B}_i$ *Booleovi redukti slobodnih algebri* $\mathbf{F}_{\mathcal{DA}(\mathbf{K}_i)}(Y)$, $i \in I$, *i neka je*

$$\mathbf{D} = \langle \prod_{i \in I} \mathbf{B}_i, f_a \rangle_{a \in \prod_{i \in I} \mathbf{K}_i},$$

pri čemu su unarni operatori definisani po komponentama, kao u dokazu Teoreme 6.3.20. Tada je podalgebra od $\mathbf{D}$ *generisana dijagonalnim elementima direktnog stepena* Y^I *izomorfna slobodnoj algebri* $\mathbf{F}_{\mathcal{DA}(\prod_{i \in I} \mathbf{K}_i)}(Y)$.

Dokaz. Pišimo kraće $\mathbf{K} = \prod_{i \in I} \mathbf{K}_i$ i označimo sa $\widetilde{Y}$ skup dijagonalnih elemenata u Y^I. Jasno, imamo očitu bijekciju $g : Y \to \widetilde{Y}$. Primetimo da se svaki element $z \in F_{\mathcal{DA}(\mathbf{K})}(Y)$ može predstaviti u obliku

$$z = \bar{t}(y_1, \ldots, y_n),$$

gde je t neki term tipa $\tau(\mathbf{K})$, $\bar{t}$ indukovana term-funkcija i $y_1, \ldots, y_n \in Y$.

Definišimo sada preslikavanje $\gamma : \mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y) \to \langle \widetilde{Y} \rangle_{\mathbf{D}}$ (gde $\langle \cdot \rangle_{\mathbf{D}}$ označava operator generisanja podalgebri u $\mathbf{D}$) sa:

$$\gamma(z) = \langle \bar{t}_i(y_1, \ldots, y_n) \rangle_{i \in I},$$

gde je t_i term tipa $\tau(\mathbf{K}_i)$ koji se dobija od t zamenom svakog pojavljivanja unarnog simbola f_a sa f_{a_i}. Kako je zapravo

$$\gamma(z) = t^{\mathbf{D}}(g(y_1), \ldots, g(y_n)),$$

rutinski se proverava da je γ dobro definisana bijekcija i homomorfizam. Stoga je γ izomorfizam. ∎

Sada možemo preći na uopštenje Teoreme 6.5.7. Dokaz narednog tvrđenja dobijamo imitacijom dokaza te teoreme, ali će nam biti neophodan jedan dodatni korak.

TEOREMA 6.5.9. *Neka Kleenejeva algebra* $\mathbf{K}$ *ima konačno direktno razlaganje*

$$\mathbf{K} \cong \mathbf{F}_{\mathcal{V}_1}(X_1) \times \ldots \times \mathbf{F}_{\mathcal{V}_n}(X_n),$$

gde su $\mathcal{V}_i$, $1 \leq i \leq n$, *podvarijeteti od* $\mathcal{KA}$ *takvi da su Booleove jednakosne teorije* $Eq_B(\mathcal{DA}(\mathcal{V}_i))$ *odlučive. Tada* $\mathcal{DA}(\mathbf{K})$ *ima odlučivu jednakosnu teoriju.*

Dokaz. Pretpostavimo prvo da je $\mathbf{K} = \mathbf{F}_{\mathcal{V}}(X)$, pri čemu je $Eq_B(\mathcal{DA}(\mathcal{V}))$ odlučiv skup identiteta Booleovog tipa. Po Propoziciji 6.3.18, *(1)*, *(2)* i *(3)*, zaključujemo

$$Eq(\mathcal{DA}(\mathbf{F}_{\mathcal{V}}(X))) = \{\hat{p}^{\alpha} = \hat{q}^{\alpha} : \mathcal{DA}(\mathcal{V}) \models p = q\},$$

gde je $\alpha : \mathbf{T}(X) \to \mathbf{F}_{\mathcal{V}}(X)$ (prirodni) homomorfizam koji proširuje identičko preslikavanje na X. Uz pretpostavku da su elementi slobodne algebre $\mathbf{F}_{\mathcal{V}}(X)$ dati preko regularnih izraza koji ih standardnom interpretacijom indukuju, imamo sledeći algoritam za dati identitet $t_1 = t_2$:

- rekonstruišimo Booleove terme p_1, p_2 tako da važi $\hat{p}_i^{\alpha} = t_i$, za $i = 1, 2$,
- ispitajmo da li $\mathcal{DA}(\mathcal{V}) \models p_1 = p_2$, što je odlučivo, po pretpostavci teoreme.

Ponovo, ako algoritam daje pozitivan odgovor, jasno je da mora biti

$$\mathcal{DA}(\mathbf{K}) \models t_1 = t_2.$$

Obratno, pretpostavimo da važi poslednji uslov. Tada postoje termi q_1, q_2 za koje je $q_i^\alpha = t_i$, $i = 1, 2$, i $\mathcal{DA}(\mathcal{V}) \models q_1 = q_2$. Ali, tada po Lemi 6.3.19 postoje termi u_i, $i = 1, 2$, tako da imamo $u_i^\alpha = q_i^\alpha = t_i = p_i^\alpha$, kao i

$$\mathcal{S} = \mathcal{DA}(\mathcal{KA}) \models u_1 = u_2.$$

Po istoj lemi, korišćenoj u suprotnom smeru, zaključujemo da

$$\mathcal{DA}(\mathcal{V}) \models p_1 = p_2.$$

Najzad, neka je

$$\mathbf{K} \cong \mathbf{F}_{\mathcal{V}_1}(X_1) \times \ldots \times \mathbf{F}_{\mathcal{V}_n}(X_n),$$

gde varijeteti $\mathcal{DA}(\mathcal{V}_1), \ldots, \mathcal{DA}(\mathcal{V}_n)$ svi imaju odlučive Booleove delove jednakosnih teorija. Za term t tipa $\tau(\mathbf{K})$ označimo sa t_i term koji se dobija zamenom svakog pojavljivanja simbola f_a sa f_{a_i} ($a = \langle a_1, \ldots, a_n \rangle$). Po Lemi 6.5.8, sledi:

$$\mathcal{DA}(\mathbf{K}) \models p = q \;\Leftrightarrow\; (\forall i \leq n)\; \mathcal{DA}(\mathbf{F}_{\mathcal{V}_i}(X_i)) \models p_i = q_i.$$

Međutim, uslov na desnoj strani gornje ekvivalencije je, po prethodnim razmatranjima, odlučiv. ∎

Videli smo da je glavni uslov u prethodnoj teoremi bio odlučivost Booleovih jednakosnih teorija varijeteta dinamičkih algebri $\mathcal{DA}(\mathcal{V}_i)$. Naredna teorema nam daje primere upravo takvih varijeteta.

Teorema 6.5.10. *Ako je varijetet $\mathcal{V} \leq \mathcal{KA}$ generisan standardnim Kleenejevim algebrama, tada je skup identiteta $Eq_B(\mathcal{DA}(\mathcal{V}))$ odlučiv.*

Dokaz. Ako je $\mathcal{V}$ generisan standardnim Kleenejevim algebrama, tada je varijetet $\mathcal{DA}(\mathcal{V})$ generisan reprezentabilnim dinamičkim algebrama, tj. tačno onim KDA $\mathbf{D} = \langle \mathbf{K}, \mathbf{B}, \langle\cdot\rangle\cdot \rangle$ za koje je $\mathbf{K} \in \mathcal{V}$. Označimo ovu potklasu od $\mathcal{RDA}$ sa $\mathcal{RDA}_\mathcal{V}$. Sada se lako vidi da se tvrđenja Fischera i Ladnera mogu prepraviti tako da dobijemo sledeći zaključak: ako neka KDA $\mathbf{D} \in \mathcal{RDA}_\mathcal{V}$ zadovoljava term p, tada postoji KDA u $\mathcal{RDA}_\mathcal{V}$ koja ga zadovoljava nad skupom sa ne više od $2^{\|p\|}$ elemenata. Naravno, takvih KDA može biti samo konačno mnogo, pa se, slično kao i ranije, provera nekog identiteta na $\mathcal{DA}(\mathcal{V})$ svodi na proveru zadovoljivosti nekog terma u konačnoj klasi konačnih KDA. To je algoritamski rešiv problem, pa tvrđenje sledi. ∎

POSLEDICA 6.5.11. *Neka je* $\mathbf{K}$ *Kleenejeva algebra sa konačnim direktnim razlaganjem*

$$\mathbf{K} \cong \mathbf{F}_{\mathcal{V}_1}(X_1) \times \ldots \times \mathbf{F}_{\mathcal{V}_n}(X_n),$$

gde su $\mathcal{V}_i$, $1 \leq i \leq n$, *podvarijeteti od* $\mathcal{KA}$ *generisani standardnim Kleenejevim algebrama. Tada* $\mathcal{DA}(\mathbf{K})$ *ima odlučivu jednakosnu teoriju.*

Ako je varijetet $\mathcal{V}$ generisan klasom $\mathcal{C}$ standardnih Kleenejevih algebri, tada je za sve skupove X, $\mathbf{F}_{\mathcal{V}}(X) \in \mathsf{ISP}(\mathcal{C})$. Međutim, primetimo da se (po Propoziciji 2.1.4) klasa $\mathsf{ISP}(\mathcal{C})$ sastoji iz standardnih Kleenejevih algebri, pa su sve slobodne algebre varijeteta $\mathcal{V}$ standardne. Na taj način, mi smo prethodnom posledicom konstruisali klasu *standardnih* Kleenejevih algebri $\mathbf{K}$ kojima odgovaraju varijeteti $\mathcal{DA}(\mathbf{K})$ sa odlučivom jednakosnom teorijom.

Zanimljivo je da rezultati o separabilnosti i odlučivosti dinamičkih algebri imaju kombinovan efekat, dajući rezultat o odlučivosti za Kleenejeve algebre. Poslednja tvrđenja u ovoj disertaciji zapravo "kompletiraju" odlučivost jednakosnih teorija varijeteta $\mathcal{DA}(\mathcal{V})$ opisanih u Teoremi 6.5.10.

POSLEDICA 6.5.12. *Svaki podvarijetet* $\mathcal{V} \leq \mathcal{KA}$ *generisan standardnim Kleenejevim algebrama ima odlučivu jednakosnu teoriju.*

Dokaz. Neka je $\mathbf{K} = \mathbf{F}_{\mathcal{V}}(X)$. Tada je algebra $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y)$ separabilna (po Teoremi 6.3.20), pa koristeći Propoziciju 6.3.18, *(3)*, zaključujemo:

$$\mathcal{DA}(\mathcal{V}) \models \langle r\rangle x = \langle s\rangle x \;\Leftrightarrow\; \mathcal{V} \models r = s.$$

Traženi rezultat se sada dobija neposredno iz Teoreme 6.5.10. ∎

Dakle, po prethodnim primedbama, važi

POSLEDICA 6.5.13. *Svaki podvarijetet od* $\mathcal{DA}$ *generisan reprezentabilnim dinamičkim algebrama ima odlučivu jednakosnu teoriju.*

Na kraju, primetimo da u odnosu na konstrukcije na Kleenejevim algebrama indeksa Jónssonovih dinamičkih algebri koje čuvaju separabilnost, pri razmatranju odlučivosti njihovih jednakosnih teorija postoji problem sa podalgebrama. Naime, nije jasno da li za $\mathbf{K}' \leq \mathbf{K}$, identiteti iz $\Theta(\mathbf{K}')$ aksiomatizuju sve identitete tipa $\tau(\mathbf{K}')$ koji važe na $\mathcal{DA}(\mathbf{K})$ (tj. slede iz $\Theta(\mathbf{K})$). Postoji opasnost da identiteti iz $\Theta(\mathbf{K}) \setminus \Theta(\mathbf{K}')$ proizvedu nove identitete tipa $\tau(\mathbf{K}')$ koji se ne mogu dobiti iz $\Theta(\mathbf{K}')$. Naravno, ove teškoće bi se razrešile ako bi se pokazalo da za sve identitete $p = q$ tipa $\tau(\mathbf{K}')$ važi

$$\mathcal{DA}(\mathbf{K}) \models p = q \;\Leftrightarrow\; \mathcal{DA}(\mathbf{K}') \models p = q.$$

To bi proširilo klasu (standardnih) Kleenejevih algebri koje daju varijetete Jónssonovih dinamičkih algebri sa odlučivom jednakosnom teorijom. Upravo opisani problem ima svoju alternativnu formulaciju.

PROBLEM 11. *Ako je* $\mathbf{K}' \leq \mathbf{K}$, *da li je tačno da je homomorfizam iz* $\mathbf{F}_{\mathcal{DA}(\mathbf{K}')}(Y)$ *u* $\tau(\mathbf{K}')$*-redukt algebre* $\mathbf{F}_{\mathcal{DA}(\mathbf{K})}(Y)$ *koji proširuje identičko preslikavanje na* Y *injektivan?*

[1] AANDERAA, S., *On the algebra of regular expressions.* U: "Applied Mathematics", pp. 1–18, Harvard University Press, 1965.

[2] ACETO, L., FOKKINK, W. J., *An equational axiomatization for multi-exit iteration.* Inform. Comput. **137** (1997), 121–158.

[3] ACETO, L., FOKKINK, W. J., VAN GLABBEEK, R. J., INGÓLFSDÓTTIR, A., *Axiomatizing prefix iteration with silent steps.* Inform. Comput. **127** (1996), 26–40.

[4] ACETO, L., FOKKINK, W. J., INGÓLFSDÓTTIR, A., *A menagerie of non-finitely based process semantics over BPA*: from ready simulation semantics to completed traces.* Math. Struct. Comput. Sci. **8** (1998), 193–230.

[5] ACETO, L., FOKKINK, W. J., INGÓLFSDÓTTIR, A., *On a question of A. Salomaa: the equational theory of regular expressions over a singleton alphabet is not finitely based.* Theoret. Comput. Sci. **209** (1998), 163–178.

[6] ACETO, L., JEFFREY, A. S. A., *A complete axiomatization of timed bisimulation for a class of timed regular behaviours.* Theoret. Comput. Sci. **152** (1995), 251–268

[7] AHO, A. V., HOPCROFT, J. E., ULLMAN, J. D., "The Design and Analysis of Computer Algorithms". Addison-Wesley, 1975.

[8] ALMEIDA, J., "Finite Semigroups and Universal Algebra". World Scientific, 1994.

[9] ANDRÉKA, H., *On the "union – relation composition" reducts of relation algebras.* Preprint, Math. Inst. Hungar. Acad. Sci., Septembar, 1988.

[10] ANDRÉKA, H., *Representations of distributive semilattice-ordered semigroups with binary relations.* Algebra Universalis **28** (1991), 12–25.

[11] ANDRÉKA, H., GORANKO, V., MIKULÁS SZ., NÉMETI, I., SAIN, I., *Effective temporal logics of programs.* U: eds. L. Bolc, A. Szałas, "Time and Logic – a Computational Approach" pp. 51–129, UCL Press, 1995.

[12] ANDRÉKA, H., GUESSARIAN, I., NÉMETI, I., *A unifying theorem for algebraic semantics and dynamic logics.* Inform. Comput. **72** (1987), 31–45.

[13] ANDRÉKA, H., KURUCZ, Á., NÉMETI, I., SAIN, I., SIMON, A., *Exactly which logics touched by the dynamic trend are decidable?* U: eds. P. Dekker, M. Stokhof, Proc. 9th Amsterdam Colloq., pp. 67–85, University of Amsterdam, 1994.

[14] ANDRÉKA, H., NÉMETI, I., *Representation theory of dynamic algebras.* Preprint, Math. Inst. Hungar. Acad. Sci., Decembar 1979.

[15] ANDRÉKA, H., NÉMETI, I., *Applications of universal algebra, modal theory and categories in computer science.* U: Proc. Int. Conf. FCT '81., Lecture Notes in Comput. Sci., Vol. 117, pp. 16–23, Springer-Verlag, 1981.

[16] ANDRÉKA, H., NÉMETI, I., SAIN, I., *Algebraic logic.* U: ed. D. M. Gabbay, "Handbook of Philosophical Logic", Vol. I (2nd edition), Kluwer Academic Press (u štampi).

[17] ARHANGELSKIJ, K. B., GORŠKOV, P. V., *Implikacijske aksiome za algebru regularnih jezika* (ruski). Dokl. Akad. Nauk USSR (Ser. A) **10** (1987), 67–69.

[18] BACKHOUSE, R. C., "Closure Algorithms and the Star-Height Problem of Regular Languages". Doktorska disertacija, Imperial College, London, 1975.

[19] VAN BENTHEM, J., *The Lambek calculus.* U: eds. R. T. Oerhrle, E. Bach, D. Wheeler, "Categorial Grammars and Natural Language Structures", pp. 35–68, Reidel, 1988.

[20] VAN BENTHEM, J., "Language in Action (Categories, Lambdas and Dynamic Logic)". Studies in Logic, Vol. 130, North-Holland, 1991.

[21] BERNÁTSKY, L., BLOOM, S. L., ÉSIK, Z., STEFANESCU, GH., *Equational theories of relations and regular sets.* U: eds. M. Ito, H. Jürgensen, Proc. Int. Conf. on Words, Languages and Combinatorics II (Kyoto, 1992), pp. 40–48, World Scientific, 1994.

[22] BLOOM, S. L., ÉSIK, Z., *Equational axioms for regular sets.* Math. Struct. Comput. Sci. **3** (1993), 1–24.

[23] BLOOM, S. L. AND ÉSIK, Z., "Iteration Theories: The Equational Logic of Iterative Processes". EATCS Monographs on Theoretical Computer Science, Springer-Verlag, 1993.

[24] BLOOM, S. L., ÉSIK, Z., *Nonfinite axiomatizability of shuffle inequalities.* U: Proc. TAPSOFT '95., Lecture Notes Comput. Sci., Vol. 915, pp. 318–333, Springer-Verlag, 1995.

[25] BLOOM, S. L., ÉSIK, Z., *Free shuffle algebras in language varieties.* Theoret. Comput. Sci. **163** (1996), 55–98. Prošireni rezime u: Proc. LATIN (Valparaiso, 1995), Lecture Notes Comput. Sci., Vol. 911, pp. 99–111, Springer-Verlag, 1995.

[26] BLOOM, S. L., ÉSIK, Z., *The equational logic of fixed points.* Theoret. Comput. Sci. **179** (1997), 1–60.

[27] BLOOM, S. L., ÉSIK Z., STEFANESCU, GH., *Notes on equational theories of relations.* Algebra Universalis **33** (1995), 98–128.

[28] BOFFA, M., *Une remarque sur les systèmes complets d'identités rationelles.* Theoret. Inform. Appl. **24** (1990), 419–423.

[29] BOGDANOVIĆ, S., ĆIRIĆ, M., "Polugrupe". Prosveta, Niš, 1993.

[30] BONNIER-RIGNY, A., KROB, D., *A complete system of identities for one-letter rational expressions with multiplicites in the tropical semiring.* Theoret. Comput. Sci. **134** (1994), 27–50.

[31] BREDIKHIN, D. A., ANDRÉKA, H., *The equational theory of union-free algebras of relations.* Algebra Universalis **33** (1994), 516–532.

[32] BRINK, C., *Boolean modules.* J. Algebra **71** (1981), 291–313.

[33] BRZOZOWSKI, J. A., SIMON, I., *Characterizations of locally testable languages.* Discrete Math. **4** (1973), 243–271.

[34] BÜCHI, J. R., *Weak second-order arithmetic and finite automata.* Z. Math. Logik und Grundl. Math. **6** (1960), 66–92.

[35] BULL, R., SEGERBERG, K., *Basic modal logic.* U: eds. D. M. Gabbay, F. Guenther, "Handbook of Philosophical Logic", Vol. II, pp. 1–88, Reidel, 1984.

[36] BURRIS, S., SANKAPPANAVAR, H. P., "A Course in Universal Algebra". Graduate Texts in Mathematics, Springer-Verlag, 1981.

[37] CHIN, L. H., TARSKI, A., *Distributive and modular laws in the arithmetic of relation algebras.* Univ. Calif. Publ. Math. **1** (1951), 341–384.

[38] CLIFFORD, A. H., PRESTON, G. B., "Algebraic Theory of Semigroups". American Mathematical Society, Vol. I, 1961., Vol. II, 1967.

[39] COHEN, E., *Using Kleene algebra to reason about concurrency control.* Rukopis, `ftp://ftp.bellcore.com/pub/ernie/research/homepage.html`, 1994.

[40] CONWAY, J. H., "Regular Algebra and Finite Machines". Chapman & Hall, 1971.

[41] CRVENKOVIĆ, S., DOLINKA, I., *Separability and decidability results for varieties of Jónsson dynamic algebras.* Algebra Universalis (u štampi).

[42] CRVENKOVIĆ, S., DOLINKA, I., ÉSIK, Z., *The variety of Kleene algebras with conversion is not finitely based.* Theoret. Comput. Sci. **230** (2000), 235–245.

[43] CRVENKOVIĆ, S., DOLINKA, I., ÉSIK, Z., *On equations for union-free regular languages.* Inform. Comput. (u štampi).

[44] CRVENKOVIĆ, S., DOLINKA, I., ÉSIK, Z., *A note on equations for commutative regular languages.* Inform. Process. Lett. **70** (1999), 265–267.

[45] CRVENKOVIĆ, S., DOLINKA, I., MADARÁSZ, R. SZ., "Odabrane teme opšte algebre: grupe, prsteni, polja, mreže". Edicija "Univerzitetski udžbenik", Vol. 47, Univerzitet u Novom Sadu, 1998.

[46] CRVENKOVIĆ, S., DOLINKA, I., VINČIĆ, M., *Equational bases for some 0-direct unions of semigroups.* Studia Sci. Math. Hungar. (u štampi).

[47] CRVENKOVIĆ, S., MADARÁSZ, R. SZ., *On semigroup relation algebras.* U: Proc. 6th Conf. "Algebra & Logic" (Sarajevo, 1987), pp. 17–28, University of Novi Sad, 1989.

[48] CRVENKOVIĆ, S., MADARÁSZ, R. SZ., *On equational base for Kleene relation algebras.* U: ed. M. Ito, Proc. Int. Conf. on Words, Languages and Combinatorics (Kyoto, 1990), pp. 64–71, World Scientific, 1991.

[49] CRVENKOVIĆ, S., MADARÁSZ, R. SZ., *A non-axiomatizability result in algebraic logic.* Algebra Universalis **28** (1991), 487–494.

[50] CRVENKOVIĆ, S., MADARÁSZ, R. SZ., *On Kleene algebras.* Theoret. Comput. Sci. **108** (1993), 17–24.

[51] CRVENKOVIĆ, S., MADARÁSZ, R. SZ., *On dynamic algebras.* Theoret. Comput. Sci. **134** (1994), 79–86.

[52] DE MORGAN, A., *On the syllogism: IV; and on the logic of relations.* Trans. Cambridge Phil. Soc. **10** (1860), 331–358.

[53] DIJKSTRA, E. W., "A Discipline of Programming". Prentice Hall, 1976.

[54] EILENBERG, S., "Automata, Languages, and Machines". Academic Press, Vol. A., 1974., Vol. B, 1976.

[55] EILENBERG, S., SCHÜTZENBERGER, M. P., *Rational sets in commutative monoids.* J. Algebra **13** (1969), 173–191.

[56] ÉSIK, Z., *Independence of the equational axioms for iteration theories.* J. Comput. Syst. Sci. **36** (1988), 66–76.

[57] ÉSIK, Z., *Group axioms for iteration.* Inform. Comput. (u štampi).

[58] ÉSIK, Z., BERNÁTSKY, L., *Equational properties of Kleene algebras of relations with conversion.* Theoret. Comput. Sci. **137** (1995), 237–251.

[59] ÉSIK, Z., BERTOL, M., *Nonfinite axiomatizability of the equational theory of shuffle.* Acta Informatica (u štampi). Prošireni rezime u: Proc. ICALP'95, Lecture Notes Comput. Sci., Vol. 944, pp. 27–38, Springer-Verlag, 1995.

[60] ÉSIK, Z., KATSURA, M., ITO, M., *The equational theory of reversal.* U: Proc. Int. Workshop on Formal Languages and Computer Systems (Kyoto, 1997), World Scientific (u štampi).

[61] FISCHER, M. J., LADNER, R. E., *Propositional modal logic of programs.* U: Proc. 9th Annual ACM Symp. on Theory of Computing, pp. 286–294, Assoc. Comput. Mach., 1977.

[62] FISCHER, M. J., LADNER, R. E., *Propositional dynamic logic of regular programs.* J. Comput. Syst. Sci. **18** (1979), 194–211.

[63] GÉCSEG, F., PEÁK, I., "Algebraic Theory of Automata". Akadémiai Kiadó, 1972.

[64] GIBBONS, A., RYTTER, W., *On the decidability of some problems about rational subsets of free partially commutative monoids.* Theoret. Comput. Sci. **48** (1986), 329–337.

[65] GISCHER, J. L., *The equational theory of pomsets.* Theoret. Comput. Sci. **61** (1988), 199–224.

[66] GOLAN, J. S., "The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science". Longman Scientific and Technical, 1993.

[67] GORŠKOV, P. V., *Rational data structures and their applications.* Cybernetics **25** (1989), 760–765.

[68] GRÄTZER, G., "Universal Algebra". Springer-Verlag, 1979.

[69] GUESSARIAN, I., *Algebraic semantics and logics of programs.* U: eds. J. Demetrovics, G. Katona, A. Salomaa, "Algebra, Combinatorics and Logic in Computer Science", Vol. I (Győr, 1983), Colloq. Math. Soc. János Bolyai, Vol. 42, pp. 423–431, North Holland, 1986.

[70] HAREL, D., "First-Order Dynamic Logic". Lecture Notes Comput. Sci., Vol. 68, Springer-Verlag, 1979.

[71] HAREL, D., *Dynamic logic.* U: eds. D. M. Gabbay, F. Guenther, "Handbook of Philosophical Logic", Vol. II, pp. 497–604, Reidel, 1984.

[72] HENNESSEY, M. C. B., *A proof system for the first-order relational calculus.* J. Comput. Syst. Sci. **20** (1980), 96–110.

[73] HOARE, C. A. R., *An axiomatic basis for computer programming.* Commun. Assoc. Comput. Mach. **12** (1969), 576–580.

[74] HOPCROFT, J. E., ULLMAN, J. D., "Introduction to Automata Theory, Languages, and Computation". Addison-Wesley, 1979.

[75] HOWIE, J. M., "Automata and Languages". Clarendon Press & Oxford University Press, 1991.

[76] HOWIE, J. M., "Fundamentals of Semigroup Theory". Clarendon Press & Oxford University Press, 1995.

[77] JÓNSSON, B., *Varieties of relation algebras.* Algebra Universalis **15** (1982), 273–298.

[78] JÓNSSON, B., *The theory of binary relations.* U: eds. H. Andréka, J. D. Monk, I. Németi, "Algebraic Logic" (Budapest, 1988), Colloq. Math. Soc. János Bolyai Vol. 54, pp. 245–292, North Holland, Amsterdam, 1991.

[79] JÓNSSON, B., TARSKI, A., *Boolean algebras with operators. Part I.* Amer. J. Math. **73** (1951), 891–939.

[80] JÓNSSON, B., TARSKI, A., *Boolean algebras with operators. Part II.* Amer. J. Math. **74** (1952), 127–162.

[81] KHARLAMPOVICH, O. G., SAPIR, M. V., *Algorithmic problems in varieties.* Int. J. Algebra Comput. **5** (1995), 379–602.

[82] KLEENE, S. C., *Representation of events in nerve nets and finite automata.* U: eds. C. E. Shannon, J. McCarthy, "Automata Studies", pp. 3–42, Princeton University Press, 1956.

[83] KOZEN, D., *A representation theorem for models of *-free PDL.* Report RC 7864, IBM Research, Yorktown Heights, 1979.

[84] KOZEN, D., *On the duality of dynamic algebras and Kripke models.* Report RC 7893, IBM Research, Yorktown Heights, 1979.

[85] KOZEN, D., *On induction vs. *-continuity.* U: ed. D. Kozen, Proc. Workshop on Logic of Programs, Lecture Notes Comput. Sci., Vol. 131, pp. 167–176, Springer-Verlag, 1981.

[86] KOZEN, D., *A completeness theorem for Kleene algebras and the algebra of regular events.* Technical report 90-1123, Cornell University, 1990. Inform. Comput. **110** (1994), 366–390.

[87] KOZEN, D., *On Kleene algebras and closed semirings.* U: "Mathematical Foundations of Computer Science", Lecture Notes Comput. Sci., Vol. 452, pp. 26–47, Springer-Verlag, 1990.

[88] KOZEN, D., "The Design and Analysis of Algorithms". Springer-Verlag, 1991.

[89] KOZEN, D., *On the complexity of reasoning in Kleene algebra.* U: Proc. 12th Annual IEEE Symp. on Logic in Comput. Sci., pp. 195–202, IEEE, 1997.

[90] KOZEN, D., *Kleene algebra with tests.* Trans. Program. Languages and Systems (May, 1997), 427–443.

[91] KOZEN, D., TIURYN, J., *Logic of programs.* U: "Handbook of Theoretical Computer Science", Vol. B, pp. 789–840, Elsevier, 1990.

[92] KRIPKE, S. A., *Semantical analysis of modal logic I: normal modal propositional calculi.* Z. Math. Logik und Grundl. Math. **9** (1963), 67–96.

[93] KROB, D., *Complete systems of $\mathcal{B}$-rational identities.* Theoret. Comput. Sci. **89** (1991), 207–343.

[94] KROB, D., *Models of a $\mathcal{K}$-rational identity system.* J. Comput Syst. Sci. **45** (1992), 396–434.

[95] KROB, D., *The equality problem for rational series with multiplicities in the tropical semiring is undecidable.* Int. J. Algebra Comput. 4 (1994), 405–425.

[96] KUICH, W., SALOMAA, A., "Semirings, Automata and Languages". EATCS Monographs on Theoretical Computer Science, Springer-Verlag, 1986.

[97] KURUCZ, Á., "Decision Problems in Algebraic Logic". Kandidatska disertacija, 102 pp., Math. Inst. Hungar. Acad. Sci., 1997.

[98] LALLEMENT, G., "Semigroups and Combinatorial Applications". John Wiley & Sons, 1979.

[99] LEWIS, H. R., PAPADIMITRIOU, C. H., "Elements of the Theory of Computation". Prentice-Hall, 1981.

[100] LYNDON, R. C., *The representation of relation algebras.* Ann. Math. **51** (1950), 707–729.

[101] LYNDON, R. C., *The representation of relation algebras II.* Ann. Math. **63** (1956), 294–307.

[102] MADARÁSZ, R. Sz., "Univerzalno-algebarski prilozi algebarskoj logici". Doktorska disertacija, v+138 pp., Univerzitet u Novom Sadu, 1989.

[103] MADARÁSZ, R. Sz., CRVENKOVIĆ, S., "Relacione algebre". Matematički institut SANU, 1992.

[104] MADARÁSZ, R. Sz., CRVENKOVIĆ, S., "Uvod u teoriju automata i formalnih jezika". Edicija "Univerzitetski udžbenik", Vol. 15, Univerzitet u Novom Sadu & Stylos, 1995.

[105] MARX, M., "Algebraic Relativization and Arrow Logic". Doktorska diserticija, vii+165 pp., University of Amsterdam, 1995.

[106] MARX, M., VENEMA, Y., "Multi-Dimensional Modal Logic". Kluwer Academic Press, 1997.

[107] MCKENZIE, R. N., "The Representation of Relation Algebras". Doktorska disertacija, 127 pp. University of Colorado, 1966.

[108] MCKENZIE, R. N., MCNULTY, G. F., TAYLOR, W. F., "Algebras, Lattices, Varieties", Vol. I. Wadsworth & Brooks/Cole, 1987.

[109] MCNAUGHTON, R., *Algebraic decision procedures for local testability.* Math. Syst. Theory **8** (1974), 60–76.

[110] MCNULTY, G. F., *A field guide to equational logic.* J. Symbolic Comput. **14** (1992), 371–397.

[111] MILNER, R., *A complete inference system for a class of regular behaviours.* J. Comput. Syst. Sci. **28** (1984), 439–466.

[112] NÉMETI, I., *Some constructions of cylindric algebra theory applied to dynamic algebras of programs.* Comput. Linguist. Comput. Lang. **14** (1980), 43–65.

[113] NÉMETI, I., *Dynamic algebras of programs.* U: Proc. Int. Conf. FCT '81., Lecture Notes in Comput. Sci., Vol. 117, pp. 281–290, Springer-Verlag, 1981.

[114] NÉMETI, I., *Every free algebra in the variety generated by the representable dynamic algebras is separable and representable.* Theoret. Comput. Sci. **17** (1982), 343–347.

[115] NÉMETI, I., *Algebraizations of quantifier logics: an introductory overview.* Studia Logica **50** (1991), 485–569.

[116] NG, K. C., "Relation Algebras with Transitive Closure". Doktorska diseratcija, iv+157 pp., University of California at Berkeley, 1984.

[117] PARIKH, R. J., *On context-free languages.* J. Assoc. Comput. Mach. **13** (1966), 570–581.

[118] PARIKH, R. J., *A completeness result for a propositional dynamic logic.* U: Lecture Notes Comput. Sci., Vol. 64, pp. 403–415, Springer-Verlag, 1978.

[119] PEIRCE, C. S., *Description of a notation for the logic of relatives, resulting from an amplification of the conceptions of Boole's calculus of logic.* U: "Collected Papers of C. S. Peirce, Vol. III. Exact Logic", Harvard University Press, 1933.

[120] PILLING, D. L., *Commutative regular equations and Parikh's theorem.* J. London Math. Soc. **6** (1973), 663–666.

[121] PIN, J.-E., "Varieties of Formal Languages". Plenum Press, 1986.

[122] PIN, J.-E., *Finite semigroups and recognizable languages: an introduction.* U: ed. J. Fountain, "Semigroups, Formal Languages and Groups", pp. 1–32, NATO Advanced Study Institute & Kluwer Academic Press, 1995.

[123] PIN, J.-E., *Syntactic semigroups.* U: eds. G. Rozenberg, A. Salomaa, "Handbook of Formal Language Theory", pp. 679–746, Springer-Verlag, 1997.

[124] PIN, J.-E., *Tropical semirings.* U: ed. J. Gunawardena, "Idempotency Analysis", Publ. Newton Institute, No. 11, Cambridge University Press, 1998.

[125] PLATIEAU, J., "Automates finis et algèbres régulières de Kleene". Mémoire de Licence, Université Mons, 1984.

[126] PRATT, V. R., *Semantical considerations of Floyd-Hoare logic.* U: Proc. 17th Annual IEEE Symp. on Found. Comput. Sci., pp. 109–121, IEEE, 1976.

[127] PRATT, V. R., *Dynamic algebras: examples, constructions, applications.* Report MIT/LCS/TM-138, MIT, Cambridge, 1979. Studia Logica **50** (1991), 571–605.

[128] PRATT, V. R., *Models of program logics.* U: Proc. 20th Annual IEEE Symp. on Found. Comput. Sci., pp. 115–122, IEEE, 1979.

[129] PRATT, V. R., *Dynamic algebras and the nature of the induction.* U: Proc. 12th Annual ACM Symp. on Theory of Computing, pp. 22–28, Assoc. Comput. Mach., 1980.

[130] PRATT, V. R., *Application of modal logic to programming.* Studia Logica **39** (1980), 257–274.

[131] PRATT, V. R., *Dynamic algebras as a well-behaved fragment of relation algebras.* U: ed. D. Pigozzi, "Algebraic Logic and Universal Algebra in Computer Science", Lecture Notes in Comput. Sci., Vol. 425, pp. 77–110, Springer-Verlag, 1990.

[132] PRATT, V. R., *Action logic and pure induction.* U: ed. J. van Eijck, "Logics in AI: European Workshop JELIA '90.", Lecture Notes in Comput. Sci., Vol. 478, pp. 97–120, Springer-Verlag, 1991.

[133] PRATT, V. R., *Origins of the calculus of binary relations.* U: Proc. 7th Annual IEEE Symp. on Logic in Comput. Sci., pp. 248–254, IEEE, 1992.

[134] REDKO, V. N., *O definišućim relacijama za algebru regularnih događaja* (ruski). Ukrain. Mat. Ž. **16** (1964), 120–126.

[135] REDKO, V. N., *O algebri komutativnih događaja* (ruski). Ukrain. Mat. Ž. **16** (1964), 185–195.

[136] REDKO, V. N., LISOVIK, L. P., *Regularni događaji u polugrupama* (ruski). Probl. Kibernet. **37** (1980), 155–184.

[137] RUSSEL, B., *The logic of relations.* Rivista di Mat. **7** (1900), 115–148.

[138] RUSSEL, B., WHITEHEAD, A. N., "Principia Mathematica" (3rd edition). Cambridge University Press, 1935.

[139] SALOMAA, A., *Two complete axiom systems for the algebra of regular events.* J. Assoc. Comput. Mach. **13** (1966), 158–169.

[140] SALOMAA, A., *On regular expressions and regular canonical systems.* Math. Syst. Theory **2** (1968), 341–355.

[141] SALOMAA, A., "Theory of Automata". Pergamon Press, 1969.

[142] SALOMAA, A., "Jewels of Formal Language Theory". Computer Sceince Press, 1981.

[143] SALOMAA, A., SOITTOLA, M., "Automata-Theoretic Aspects of Formal Power Series". Springer-Verlag, 1978.

[144] SANDERSON, J. G., "A Relational Theory of Computing". Lecture Notes Comput. Sci., Vol. 82, Springer-Verlag, 1980.

[145] SCHEIN, B. M., *Representation of subreducts of Tarski relation algebras.* U: eds. H. Andréka, J. D. Monk, I. Németi, "Algebraic Logic" (Budapest, 1988), Colloq. Math. Soc. János Bolyai Vol. 54, pp. 621–635, North Holland, Amsterdam, 1991.

[146] SCHRÖDER, E., "Vorlesungen über die Algebra der Logik (Exacte Logik). Dritter Band: Algebra und Logik der Relative". Teubner, 1895.

[147] SCHÜTZENBERGER, M. P., *On finite monoids having only trivial subgroups.* Inform. Control **8** (1965), 190–194.

[148] SEGERBERG, K., *A completeness theorem in the modal logic of programs.* Notices Amer. Math. Soc. **24** (1977), A–552.

[149] SEWELL, P. M., *Bisimulation is not finitely (first-order) equationally axiomatizable.* U: Proc. 9th Annual IEEE Symp. on Logic in Comput. Sci., pp. 62–70, IEEE, 1994.

[150] SIMON, I., *Piecewise testable languages.* U: Proc. 2nd GI Conf., Lecture Notes Comput. Sci., Vol. 33, pp. 214–222, Springer-Verlag, 1975.

[151] SIMON, I., *Recognizable sets with multiplicities in the tropical semiring.* U: eds. M. Chytil, L. Janiga, V. Koubek, "Mathematical Foundations of Computer Science", Lecture Notes Comput. Sci., Vol. 324, pp. 107–120, Springer-Verlag, 1988.

[152] STARKE, P. H., "Abstract Automata". North Holland, 1972.

[153] TARSKI, A., *On the calculus of binary relations.* J. Symbolic Logic **6** (1941), 73–89.

[154] TARSKI, A., *Some metalogical results concerning the calculus of relations.* J. Symbolic Logic **18** (1953), 188–189.

[155] VENEMA, Y., "Many-Dimensional Modal Logics". Doktorska disertacija, vii+178 pp., University of Amsterdam, 1991.

[156] WILKE, T., *An algebraic theory for regular languages of finite and infinite words.* Int. J. Algebra Comput. **3** (1993), 447–489.

Z

Igor Dolinka je rođen 26. juna 1973. u Subotici, gde je završio Osnovnu školu "Jovan Jovanović-Zmaj" i Gimnaziju "Svetozar Marković". U tom periodu, učestvujući na matematičkim takmičenjima, tri puta je bio prvak Jugoslavije, dva puta prvak Balkana i tri godine član jugoslovenske reprezentacije na Međunarodnim matematičkim olimpijadama, gde je dva puta osvajao srebrnu, a jednom bronzanu medalju. Takođe, jednom je bio prvak Jugoslavije iz fizike.

Prirodno-matematički fakultet u Novom Sadu, odsek za matematiku, smer profesor matematike, upisao je 1992. godine. Vojni rok je odslužio u toku školske 1993/94. godine. Dobitnik je univerzitetske nagrade "Mileva Marić-Einstein" za 1996. godinu, za seriju seminarskih radova iz opšte algebre. Fakultet je završio 11. juna 1997. sa prosečnom ocenom 10. Iste godine, proglašen je za studenta godine Prirodno-matematičkog fakulteta i celog Univerziteta.

Od 6. oktobra 1997. radi kao asistent-pripravnik na Institutu za matematiku Prirodno-matematičkog fakulteta u Novom Sadu. U zimskom semestru školske 1997/98. godine, upisao je poslediplomske studije na odseku za matematiku, smer algebra. Ispite na poslediplomskim studijama je položio sa prosečnom ocenom 10, a magistarski rad pod naslovom "Slobodni spektri i p_n-nizovi polugrupa" odbranio je 29. juna 1999. godine.

Autor je ili koautor 24 naučna rada kako u inostranim, tako i u domaćim časopisima (od kojih 4 još za vreme redovnih studija), zatim 2 stručna članka i jednog univerzitetskog udžbenika. Imao je do sada 5 predavanja po pozivu (od kojih 3 u inostranstvu), kao i 5 saopštenja na međunarodnim konferencijama. Njegov istraživački rad obuhvata algebarske osnove teorijskog računarstva, teoriju polugrupa, univerzalnu algebru i algoritamske probleme u algebri.

Od 1996. godine je saradnik, a od 1997. godine stručni saradnik Odeljenja za matematiku Istraživačke stanice Petnica.

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
Ključna dokumentacijska informacija

Redni broj (RBR):

Identifikacioni broj (IBR):

Tip dokumentacije (TD): monografska dokumentacija

Tip zapisa (TZ): tekstualni štampani materijal

Vrsta rada (VR): doktorska disertacija

Autor (AU): mr Igor Dolinka

Mentor (MN): dr Siniša Crvenković, redovni profesor

Naslov rada (NR): "O identitetima algebri regularnih jezika"

Jezik publikacije (JP): srpski

Jezik izvoda (JI): srpski/engleski

Zemlja publikovanja (ZP): SR Jugoslavija

Uže geografsko područje (UGP): Vojvodina

Godina (GO): 2000.

Izdavač (IZ): autorski reprint

Mesto i adresa (MA): Novi Sad, Puškinova 23

Fizički opis rada (FO): 6/ix+143/156/0/4/0/0

Naučna oblast (NO): matematika

Naučna disciplina (ND): algebra

Predmetna odrednica/Ključne reči (PO): algebarske osnove teorijskog računarstva; formalni jezici, algebre jezika, identiteti, varijeteti, regularni jezici, komutativni jezici, logika programskih jezika, dinamičke algebre

UDK:

Čuva se (ČU): Biblioteka Instituta za matematiku, Prirodno-matematički fakultet, Novi Sad, Trg Dositeja Obradovića 4

Važna napomena (VN):

Izvod (IZ): Jezik nad Σ je proizvoljan skup reči nad Σ, tj. proizvoljan podskup slobodnog monoida Σ^*. Jezici nad datom azbukom formiraju algebre jezika, sa operacijama unije, konkatenacije (dopisivanja reči), Kleenejeve iteracije i sa $\emptyset, \{\lambda\}$ kao konstantama. Regularni jezici nad Σ su elementi podalgebre algebre jezika nad Σ generisane konačnim jezicima. Ispostavlja se da algebre jezika generišu isti varijetet (i stoga zadovoljavaju iste identitete) kao i algebre binarnih relacija snabdevene operacijama unije, kompozicije, refleksivno-tranzitivnog zatvorenja i praznom relacijom i dijagonalom kao konstantama. Reč je o varijetetu Kleenejevih algebri, i slobodne algebre tog varijeteta su baš algebre regularnih jezika.

Na početku disertacije, izloženi su neki aspekti algebarske teorije automata i formalnih jezika, teorije binarnih relacija i univerzalne algebre, relevantni za ispitivanje identiteta na algebrama jezika. Zatim je dat klasični rezultat (Redko, 1964.) da varijetet Kleenejevih algebri nema konačnu bazu identiteta. Ovde je prikazan dokaz Conwaya iz 1971., budući da on sadrži neke ideje koje su se pokazale korisne za dalji rad.

Glave 3 i 4 sadrže originalne rezultate usmerene na profinjenje Redkovog rezultata. Pokazano je da uzroci beskonačnosti baze identiteta za Kleenejeve algebre leže u interakciji operacija konkatenacije i iteracije jezika (odnosno, kompozicije i refleksivno-tranzitivnog zatvorenja relacija). Drugim rečima, klasa redukata algebri jezika bez operacije unije nema konačnu bazu identiteta. To daje odgovor na problem D. A. Bredikhina iz 1993. godine. S druge strane, proširenjem tipa Kleenejevih algebri involutivnom operacijom inverza jezika, odnosno relacija, takođe se dolazi do beskonačno baziranih varijeteta, čime se rešava problem B. Jónssona iz 1988. godine.

Analogno, komutativni jezici nad Σ su proizvoljni podskupovi slobodnog komutativnog monoida $\Sigma^{\oplus}$. U Glavi 5 je dokazano da se jednakosna teorija algebri komutativnih jezika poklapa sa jednakosnom teorijom algebre (regularnih) jezika nad jednoelementnim alfabetom, što daje odgovor na problem koji je još 1969. formulisao A. Salomaa u svojoj monografiji *Theory of Automata*. Na taj način, iz poznatih rezultata o jednakosnoj aksiomatizaciji komutativnih jezika se dobija jedna baza za algebre jezika nad jednoelementnim alfabetom, kao i veoma kratak dokaz poznate činjenice (takođe Redko, 1964.) da algebre komutativnih jezika nemaju konačnu bazu identiteta.

Na kraju disertacije, identiteti Kleenejevih algebri se posmatraju u kontekstu dinamičkih algebri. Reč je o algebarskoj verziji dinamičkih logika, koje su konstruisane sedamdesetih godina kao matematički model rada računara, kada se na njima izvršava program pisan u nekom imperativnom programskom jeziku. Na primer, problemi verifikacije i ekvivalentnosti programa se lako izražavaju preko identiteta dinamičkih algebri, tako da razne njihove jednakosne osobine odgovaraju pojmovima iz teorijskog računarstva. Takođe, interesatno je da je jednakosna teorija Kleenejevih algebri "kodirana" u konačno baziranoj jednakosnoj teoriji dinamičih algebri. Polazeći od poznatih rezultata za dvosortne dinamičke algebre (pri čemu je jedna komponenta algebra istog tipa kao i Kleenejeve algebre, dok je druga Booleova algebra), neki od tih rezultata su transformisani i prošireni za Jónssonove dinamičke algebre (jednosortne modele dinamičkih logika). Na primer, ako se Kleenejeva algebra $\mathbf{K}$ može predstaviti kao konačan direktan proizvod slobodnih algebri varijeteta Kleenejevih algebri generisanih Kleenejevim relacionim algebrama, tada varijetet $\mathbf{K}$-dinamičkih algebri ima odlučivu jednakosnu teoriju. Odavde se izvodi da svaki varijetet Kleenejevih algebri generisan Kleenejevim relacionim algebrama takođe ima odlučivu jednakosnu teoriju.

Datum prihvatanja teme od strane NN Veća (DP): 21.10.1999.

Datum odbrane (DO):

Članovi komisije (KO):

Predsednik: dr Đura Paunić, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Mentor: dr Siniša Crvenković, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Rozália Sz. Madarász, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Stojan Bogdanović, redovni profesor, Ekonomski fakultet, Univerzitet u Nišu

Član: dr Miroslav Ćirić, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Nišu

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCE
Key words documentation

Accession number (ANO):

Identification number (INO):

Documentation type (DT): Monographic documentation

Type of record (TR): Textual printed material

Contents code (CC): Ph.D. thesis

Author (AU): Igor Dolinka, M.Sc.

Mentor (MN): Siniša Crvenković, Ph.D., Full Professor

Title (TI): "On Identities of Algebras of Regular Languages"

Language of text (LT): Serbian

Language of abstract (LA): Serbian/English

Country of publication (CP): F.R. of Yugoslavia

Locality of publication (LP): Vojvodina

Publication year (PY): 2000

Publisher (PU): Author's reprint

Publication place (PP): Novi Sad, Puškinova 23

Physical description (PD): 6/ix+143/156/0/4/0/0

Scientific field (SF): Mathematics

Scientific discipline (SD): Algebra

Subject/Key words (SKW): Algebraic Foundations of the Theory of Computation; formal languages, language algebras, identities, varieties, regular languages, commutative languages, logic of programming, dynamic algebras

UC:

Holding data (HD): The Library of the Institute of Mathematics, Faculty of Science, Novi Sad, Trg Dositeja Obradovića 4

Notes (N):

Abstract (AB): A language over Σ is an arbitrary set of words, i.e. any subset of the free monoid Σ^*. All languages over a given alphabet form the algebra of languages, which is equipped with the operations of union, concatenation, Kleene iteration and $\emptyset, \{\lambda\}$ as constants. Regular languages over Σ are the elements of the subalgebra of the algebra of languages over Σ generated by finite languages. It turns out that algebras of languages generate exactly the same variety as algebras of binary relations, endowed with union, relation composition, formation of the refelxive-transitive closure and the empty relation and the diagonal as constants. The variety in question is the variety of Kleene algebras, and the algebras of regular languages are just its free algebras.

The present dissertation starts with several aspects of algebraic theory of automata and formal languages, theory of binary relations and universal algebra, which are related to problems concerning identities of language algebras. This material is followed by the classical result (Redko, 1964) claiming that the variety of Kleene algebras have no finite equational base. We present the proof of Conway from 1971, since it contains some ideas which can be used for generalizations in different directions.

Chapters 3 and 4 contain original results which refine the one of Redko. It is shown that the cause of nonfinite axiomatizability of Kleene algebras lies in the superposition of the concatenation and the iteration of languages, that is, composition of relations and reflexive-transitive closure. In other words, the class of $+$-free reducts of algebras of languages has no finite equational base, which answers in the negative a problem of D. A. Bredikhin from 1993. On the other hand, by extending the type of Kleene algebras by the involutive operation of inverse of languages (converse of relations), we also obtain a nonfinitely based variety, which solves a problem of B. Jónsson from 1988.

Analogously, commutative languages over Σ are defined as subsets of the free commutative monoid $\Sigma^{\oplus}$. It is proved in Chapter 5 that equational theories of algebras of commutative languages and, respectively, of the algebra of (regular) languages over the one-element alphabet, coincide. This result settles a thirty year old problem of A. Salomaa, formulated back in his well-known monograph *Theory of Automata*. Thus, we obtain an equational base for the algebra of one-letter languages, and, on the other hand, a very short proof of another Redko's result from 1964, according to which there is no finite

equational base for algebras of commutative languages.

Finally, identities of Kleene algebras are considered in the context of dynamic algebras, which are just algebraic counterparts of dynamic logics. They were discovered in the seventies as a result of the quest for an appropriate logic for reasoning about computer programs written in an imperative programming language. For example, problems concerning program verification and equivalence can be easily translated into identities of dynamic algebras, so that many of their equational properties correspond to notions from computer science. It is also interesting that the whole equational theory of Kleene algebras is "encoded" in the finitely based equational theory of dynamic algebras. Starting with known results on two-sorted dynamic algebras (where one component is an algebra of the same signature as Kleene algebras, while the other is a Boolean algebra), some of those results are transformed and extended for Jónsson dynamic algebras (that is, one-sorted models of dynamic logics). For example, if a Kleene algebra $\mathbf{K}$ can be represented as a finite direct product of free algebras of varieties of Kleene algebras generated by Kleene relation algebras, then the variety of $\mathbf{K}$-dynamic algebras has a decidable equational theory. The latter yields that all varieties of Kleene algebras generated by Kleene relation algebras have decidable equational theories, too.

Accepted by the Scientific Board of the Faculty on (ASB): 10/21/1999

Defended (DE):

Thesis defend board (DB):

President: dr Đura Paunić, Full Professor, Faculty of Science, University of Novi Sad

Mentor: dr Siniša Crvenković, Full Professor, Faculty of Science, University of Novi Sad

Member: dr Rozália Sz. Madarász, Full Professor, Faculty of Science, University of Novi Sad

Member: dr Stojan Bogdanović, Full Professor, Faculty of Economics, University of Niš

Member: dr Miroslav Ćirić, Associate Professor, Faculty of Science, University of Niš