Mali deduktivni sistemi

Vladan Radivojević

seminarski rad za predmet AUTOMATSKO REZONOVANJE
profesor: Dr Predrag Janičić

Sadržaj

1 Funkcionalno kompletni iskazni veznici

Za skup iskaznih veznika kažemo da je *funkcionalno kompletan* ako se svaka iskazna funkcija može izraziti formulom generisanom samo veznicima iz tog skupa. Ako govorimo o jednočlanom funkcionalno kompletnom skupu $\{f\}$ onda f nazivamo funkcionalno kompletnim veznikom.

1.1 Binarni funkcionalno kompletni iskazni veznici

Razmotrimo dva binarna iskazna veznika: $\uparrow$ (Šeferov veznik) i $\downarrow$ (Lukašijevičev veznik) koji su definisanim sledećom istinitosnom tablicom:

a	b	$a \uparrow b$	$a \downarrow b$
0	0	1	0
0	1	1	1
1	0	1	1
1	1	0	1

Veznici $\uparrow$ i $\downarrow$ su funkcionalno kompletni. Zaista, svaki od binarnih logičkih veznika na kojima je zasnovan klasični iskazni račun se može ekvivalentno zapisati pomoću njih. Navodimo odgovarajuće ekvivalencije za Šeferov veznik, a analogno se može uraditi i za Lukašijevičev veznik:

$\rceil a$ je izraz ekvivalentan sa $a \uparrow a$,
$a \Rightarrow b$ je izraz ekvivalentan sa $a \uparrow (b \uparrow b)$,
$a \wedge b$ je izraz ekvivalentan sa $(a \uparrow b) \uparrow (a \uparrow b)$,
$a \vee b$ je izraz ekvivalentan sa $(a \uparrow a) \uparrow (b \uparrow b)$,
$a \Leftrightarrow b$ je izraz ekvivalentan sa $(a \uparrow b) \uparrow ((a \uparrow a) \uparrow (b \uparrow b))$.

Ovo su jedina dva binarnih iskazna veznika koji su funkcionalno kompletni. Dokaz se može naći npr. u [4], a ova činjenica je i posledica teoreme o kojoj će biti reči u narednom podpoglavlju.

U ovom radu ćemo se baviti samo Šeferovim veznikom, a većina analognih razmatranja važi i za Lukašijevičev veznik.

1.2 Funkcionalno kompletni iskazni veznici proizvoljne arnosti

Neka je φ n-arni iskazni veznik (n-arna logička funkcija) čija je istinitosna tablica:

p_0	p_1	...	p_{n-2}	p_{n-1}	$\varphi(p_0, p_1, ..., p_{n-2}, p_{n-1})$
0	0	...	0	0	t_0
0	0	...	0	1	t_1
0	0	...	1	0	t_2
...	...	...	...	...	...
1	1	...	1	1	t_{2^n-1}

Primetimo da pri ovakvom zapisu važi: $t_\alpha = \varphi(p_0, p_1, p_2, ..., p_{n-1})$ gde je α ceo broj, $0 \leq \alpha \leq 2^n - 1$, a $p_0, p_1, p_2, ..., p_{n-1}$ su cifre binarne reprezentacije tog broja.

U radu [5] formulisan je i dokazan potreban i dovoljan uslov za funkcionalnu kompletnost iskaznog veznika proizvoljne arnosti:

Teorema 1 *Veznik φ je funkcionalno kompletan akko važi:*

1. $t_0 = 1$,
2. $t_{2^n-1} = 0$,
3. postoji x, $0 < x < 2^n - 1$, tako da je $t_x = t_{2^n-1-x}$.

Nešto drugačiji dokaz dovoljnosti pomenutih uslova (u odnosu na dokaz dat u [5]) ćemo navesti u ovom radu.

Dokaz $\Leftarrow$:

Pretpostavimo da su za veznik φ ispunjena tri navedena uslova. Definišimo binarni veznik τ na sledeći način:

$$\tau(p_0, p_1) = \varphi(p_{x_0}, p_{x_1}, p_{x_2}, ...p_{x_{n-1}}),$$

gde su $x_0, x_1, x_2, ...x_{n-1}$ cifre binarne reprezentacije broja x iz trećeg uslova teoreme.

Ako je $p_0 = 0$ i $p_1 = 0$, tada za $0 \leq i \leq n-1$ važi $p_{x_i} = 0$ (jer $x_i \in \{0, 1\}$), pa je

$$\tau(0, 0) = \varphi(0, 0, 0, ...0) = t_0 = 1.$$

Ako je $p_0 = 1$ i $p_1 = 1$, tada za $0 \leq i \leq n-1$ važi $p_{x_i} = 1$, pa je

$$\tau(1, 1) = \varphi(1, 1, 1, ...1) = t_{2^n-1} = 0.$$

Ako je $p_0 = 0$ i $p_1 = 1$, tada za $0 \leq i \leq n-1$ važi $p_{x_i} = x_i$, pa je

$$\tau(0, 1) = \varphi(x_0, x_1, x_2, ...x_{n-1}) = t_x.$$

Ako je $p_0 = 1$ i $p_1 = 0$, tada za $0 \leq i \leq n-1$ važi $p_{x_i} = 1 - x_i$, pa je

$$\tau(1, 0) = \varphi(1 - x_0, 1 - x_1, 1 - x_2, ...1 - x_{n-1}) = t_{2^n-1-x} = t_x.$$

Poslednja jednakost je treći uslov iz teoreme.

Dakle, istinitosna tablica veznika τ je sledećeg oblika:

p_0	p_1	$\tau(p_0, p_1)$
0	0	1
0	1	t_x
1	0	t_x
1	1	0

Ako je $t_x = 1$, tada je veznik τ identičan sa veznikom $\uparrow$, a ako je $t_x = 0$, tada je veznik τ identičan sa veznikom $\downarrow$. Dakle, veznici $\uparrow$ i $\downarrow$ se mogu izraziti pomoću veznika φ koji ispunjava uslove teoreme. Zato iz funkcionalne kompletnosti veznika $\uparrow$ i $\downarrow$ koju smo dokazali u predhodnom poglavlju sledi i funkcionalna kompletnost veznika φ, što je i trebalo dokazati.

Neposredna posledica navedene teoreme je i da su $\uparrow$ i $\downarrow$ jedini funkcionalno kompletni binarni veznici. Naime, nijedan od preostalih binarnih veznika ne ispunjava sva tri uslova teoreme.

2 Neke karakteristike formula sa Šeferovim veznikom

Iz potpunosti Šeferovog veznika (o kojoj je bilo reči u potpoglavlju 1.1) sledi da se svaka iskazna formula može predstaviti pomoću ovog veznika. Zbog toga, proučavanje osobina ovako zapisanih formula može da ima uticaj na zaključivanje o iskaznim formulama uopšte.

U ovom poglavlju ćemo pokazati pojedine empirijske rezultate u vezi sa formulama zapisanim pomoću Šeferovog veznika, kao i neke ideje za njihovo teorijsko tumačenje.

2.1 Broj korektnih formula sa proizvoljnim binarnim veznikom

Razmotrimo sve niske dužine n nad azbukom $\{F, a\}$. Broj ovakvih niski je očigledno 2^n. Neke od ovih niski predstavljaju korektno zapisane formule u prefiksnoj poljskoj notaciji sa binarnim operatorom F i jednom promenljivom a. Takve su npr. niske $FFaaa$ i $FaFaFaa$. Prva se može tumačiti kao zapis formule $F(F(a,a),a)$, a druga kao zapis formule $F(a,F(a,F(a,a)))$.

Uz pomoć jednostavnog programa koji pretražuje svih pomenutih 2^n niski i među njima određuje one koje predstavljaju korektno zapisane formule može se doći do broja korektnih formula sa tačno jednom promenljivom. Taj broj je naveden u prvoj koloni donje tabele.

Prelazak na korektne formule sa više promenljivih je izvršen uz pomoć programa koji iz svake korektne formule sa tačno jednom promenljivom generiše sve korektne formule sa tačno k promenljivih. Dobijeni su sledeći rezultati:

n	k=1	k=2	k=3	k=4	k=5
1	1	0	0	0	0
3	1	1	0	0	0
5	2	6	2	0	0
7	5	35	30	5	0
9	14	210	350	140	14
11	42	1.302	3.780	2.730	630
13	132	8.316	39.732	46.200	18.480
15	429	54.483	414.414	729.729	450.450
17	1.430	364.650	4.325.750	11.111.100	9.939.930
19	4.862	2.484.482	46.362.460	165.818.510	206.756.550
21	16.796	17.182.308	478.702.796	2.448.017.000	4.144.077.080
23	58.786	120.334.942	5.086.517.436	35.947.697.786	81.089.408.400
25	208.012	851.809.140	54.421.193.500	526.796.630.360	1.561.858.310.012

U tabeli su razmatrane samo niske neparne dužine. Lako se dokazuje da niska parne dužine ne može biti zapis korektne formule.

Ovde treba napomenuti da se broje samo formule unutar kojih su promenljive leksikografski poređane po svom prvom pojavljivanju. Tako se npr. iz formule $FaFaa$ sa tačno jednom promenljivom generišu sledeće 3 formule sa tačno 2 promenljive: $FaFab$,$FaFba$,$FaFbb$, dok se npr. niska $FbFba$ ne broji, jer bi takva formula bila jednaka prvoj do na preimenovanje promenljivih.

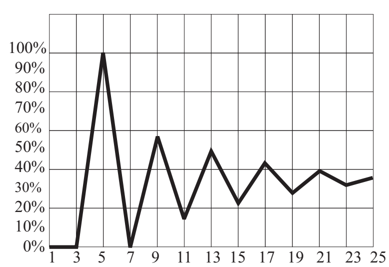
2.2 Broj valjanih formula sa Šeferovim veznikom

Podaci iz prošlog potpoglavlja su se odnosili na proizvoljni binarni veznik. U ovom i narednom delu ćemo podrazumevati da je F Šeferov veznik $\uparrow$.

Uz pomoć programa koji pretražuje sve korektne formule i generiše one koje su tautologije dužine n sa tačno k promenljivih, dobijamo sledeće rezultate o njihovom broju i udelu među odgovarajućim korektnim formulama:

n	k=1	%	k=2	%	k=3	%	k=4	%	k=5	%
1	0	0,0	0	0,0	0	0,0	0	0,0	0	0,0
3	0	0,0	0	0,0	0	0,0	0	0,0	0	0,0
5	2	100,0	0	0,0	0	0,0	0	0,0	0	0,0
7	0	0,0	0	0,0	0	0,0	0	0,0	0	0,0
9	8	57,1	32	15,2	0	0,0	0	0,0	0	0,0
11	6	14,3	48	3,7	16	0,4	0	0,0	0	0,0
13	64	48,5	1.232	14,8	1.048	2,6	32	0,1	0	0,0
15	96	22,4	3.552	6,6	6.400	1,5	1.640	0,2	80	0,02
17	622	43,5	50.104	13,7	145.024	3,4	62.368	0,6	5.168	0,05
19	1.280	26,3	199.488	8,0	994.160	2,2	866.824	0,5	206.104	0,10
21	6.704	39,9	2.184.832	12,7	16.477.200	3,4	19.872.816	0,8		
23	17.078	29,0	10.870.944	9,0	130.835.872	2,6				
25	78.464	37,7								

Razmotrimo grafik koji predstavlja udeo tautologija sa tačno jednom promenljivom u ukupnom broju korektnih formula sa tačno jednom promenljivom u zavisnosti od dužine formule:



Očigledno je da grafik veoma brzo konvergira ka približno 33%. Odavde sledi hipoteza:

Udeo tautologija u skupu svih formula nad Šeferovim veznikom sa tačno jednom promenljivom teži $\frac{1}{3}$.

Razmatranjem grafika kada su u pitanju formule sa tačno dve promenljive dobija se slična konvergencija, ka 11%.

Do ovog zaključka se može doći i teorijskim razmatranjem. Neka je $\Theta(F)$ zapis činjenice da je formula F tautologija. Tada važi sledeća ekvivalencija:

$$\Theta(F(a,b)) \Leftrightarrow \Theta(F(a,a)) \wedge \Theta(F(a,\neg a))$$

Verovatnoća iskaza sa leve strane je jednaka proizvodu verovatnoća iskaza sa desne strane. Kako su verovatnoće iskaza sa desne strane približno $\frac{1}{3}$, jer se radi o formulama sa tačno jednom promenljivom, verovatnoća iskaza sa leve strane je približno $\frac{1}{9}$. Ovaj rezultat odgovara rezultatu od približno 11% do kojeg smo došli uz pomoć odgovarajućeg grafika.

Analogni zaključak o formulama sa tačno tri promenljive ćemo dobiti kao posledicu sledeće ekvivalencije:

$$\Theta(F(a,b,c)) \Leftrightarrow \Theta(F(a,a,a)) \wedge \Theta(F(a,a,\neg a)) \wedge \Theta(F(a,\neg a,a)) \wedge \Theta(F(\neg a,a,a))$$

Dakle, verovatnoća da je slučajno izabrana formula iz skupa korektnih formula sa tačno 3 promenljive tautologija teži $(\frac{1}{3})^4 = \frac{1}{81}$.

Analognim zaključivanjem za formule sa većim brojem promenljivih se može doći do zaključka:

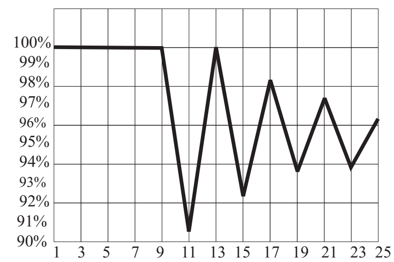
Verovatnoća da je slučajno izabrana formula iz skupa svih korektnih formula sa Šeferovim veznikom koje imaju tačno k promenljivih tautologija teži $(\frac{1}{3})^{2^{k-1}}$.

2.3 Broj zadovoljivih formula sa Šeferovim veznikom

Program sličan onom iz prošlog poglavlja se može koristiti za dobijanje rezultata o broju zadovoljivih formula i njihovom udelu među odgovarajućim korektnim formulama sa Šeferovim veznikom:

n	k=1	%	k=2	%	k=3	%	k=4	%	k=5	%
1	1	100,0	0	0,0	0	0,0	0	0,0	0	0,0
3	1	100,0	1	100,0	0	0,0	0	0,0	0	0,0
5	2	100,0	6	100,0	2	100,0	0	0,0	0	0,0
7	5	100,0	35	100,0	30	100,0	5	100,0	0	0,0
9	14	100,0	210	100,0	350	100,0	140	100,0	14	100,0
11	38	90,5	1.298	99,7	3.780	100,0	2.730	100,0	630	100,0
13	132	100,0	8.316	100,0	39.372	100,0	46.200	100,0	18.480	100,0
15	397	92,5	54.195	99,5	414.286	99,97	729.729	100,0	450.450	100,0
17	1.406	98,3	364.242	99,9	4.325.366	99,99	11.111.036	99,99	9.939.930	100,0
19	4.542	93,4	2.471.234	99,5						
21	16.316	97,1	17.144.964	99,8						
23	55.238	94,0								
25	200.588	96,4								

Razmotrimo i sada grafik koji se odnosi na udeo zadovoljivih formula sa tačno jednom promenljivom u ukupnom broju korektnih formula sa tačno jednom promenljivom u zavisnosti od dužine formule:



Dakle, udeo zadovoljivih formula sa jednom promenljivom među svim dobro formiranim formulama sa jednom promenljivom konvergira ka približno 95%.

Kada su u pitanju formule koje imaju više od jedne promenljive ovaj procenat je veći od 99, odnosno sa povećanjem broja promenljivih skoro sve formule postaju zadovoljive.

2.4 Veza KNF formula i formula sa Šeferovim veznikom

U prethodna dva potpoglavlja su iznete neke procene procenta valjanih i zadovoljivih formula zapisanih nad Šeferovim veznikom. Ovo je motiv i za traženje veze između ovakvih formula i formula u konjuktivnoj normalnoj formi.

Uz pomoć veza koje su date u 1.1 dobijamo da važi:

Ekvivalentan zapis formule $a \wedge b$ pomoću Šeferovog veznika je $FFabFab$, tj. formula sa 7 simbola.

Ekvivalentan zapis formule $a \wedge b \wedge c$ pomoću Šeferovog veznika je $FFFFabFabcFFFabFabc$, tj. formula sa 19 simbola.

Matematičkom indukcijom se može pokazati da se na ovaj način formula $a_1 \wedge a_2 \wedge ... \wedge a_n$ prevodi u formulu sa $6 \cdot 2^{n-1} - 5$ simbola.

Daljim izvođenjem, uzimajući u obzir da su a_i klauze sa po npr. 3 litarala, dobija se da se KNF formula koja sadrži n klauza sa po 3 nenegativna literala prevodi u formulu dužine $60 \cdot 2^{n-1} - 41$ nad Šeferovim veznikom. Ovakav rezultat govori da temeljna eksperimentalna analiza otpada kao mogućnost.

Za teorijsku analizu bi bilo značajno ako bi imali poznatu formu formula koje se ovako dobijaju i teorijsku procenu procenta zadovoljivosti takvih formula. U tom slučaju bi smo imali i procenu procenta zadovoljivih običnih KNF formula.

3 Minimalni sistemi izvođenja za iskazni račun

Postoji više varijanti formalnih teorija koje opisuju klasičnu iskaznu logiku. Cilj koji se nameće pri razvoju istih je da one budu što je moguće manje, tj. da imaju minimalan broj aksioma, kao i što manje pravila izvođenja. Na ovaj način se dobijaju sistemi manje intuitivni od sistema prirodne dedukcije, ali su istovremeno jednostavniji za programsku implentaciju.

3.1 Minimalni sistemi izvođenja nad skupom $\{\neg, \Rightarrow\}$

Jedan od sistema izvođenja nad skupom veznika $\{\neg, \Rightarrow\}$ je *Hilbertov sistem* ili *teorija* L koji je pojednostavljenje sistema koji je Frege dao krajem 19. veka.

Hilbertov sistem sadrži sledeće aksiome:

H1 $A \Rightarrow (B \Rightarrow A)$

H2 $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

H3 $(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$

i jedno pravilo izvođenja, *modus ponens*:

MP $\frac{A, A \Rightarrow B}{B}$

Napomenimo da su ovde A, B i C oznake za proizvoljne iskazne formule, pa kada govorimo o aksiomama, govorimo zapravo o aksiomatskim šemama.

Teorija L je *saglasna* i *potpuna*[1], tj. svaka formula koja je teorema ove teorije je tautologija i obratno. Dodatno, ova teorija je neprotivrečna, tj. ne postoji formula A takva da su i A i $\neg A$ teoreme teorije L. Dokazi ovih činjenica se mogu naći na primer u [4].

Teorija L je i *neredundantna* tj. skup njenih aksioma je nezavisan. Dokaz ove činjenice tj. dokaz činjenice da nijednu od aksioma nije moguće izvesti pomoću preostale dve aksiome i pravila izvođenja se može naći na primer u [3].

Navodimo jedan primer sistema ekvivalentnog teoriji L. To je Lukašijevičev sistem. Pravilo izvođenja i skup veznika su isti, a aksiome su sledeće:

L1 $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$

L2 $(\neg A \Rightarrow A) \Rightarrow A$

L3 $A \Rightarrow (\neg A \Rightarrow B)$

Dokaz ekvivalencije ova dva sistema se može naći u [2].

Nad istim skupom veznika $\{\neg, \Rightarrow\}$ i sa istim pravilom izvođenja je moguće konstruisati i sisteme sa manjim brojem aksioma.

Jedan takav sistem je konstruisao Meredit 1953. godine. On sadrži samo sledeću aksiomu:

$$((((A \Rightarrow B) \Rightarrow (\neg C \Rightarrow \neg D)) \Rightarrow C) \Rightarrow E) \Rightarrow ((E \Rightarrow A) \Rightarrow (D \Rightarrow A))$$

Dokaz ekvivalencije ovog sistema sa gore pomenutim sistemima je dat u [2].

[1] Ovde se misli na potpunost u smislu snage deduktivnog sistema, jer se u okviru računa L može dokazati svaka tautologija. Međutim, u smislu stroge definicije potpunosti formalne teorije, L nije potpuna, jer postoje formule takve da ni one ni njihove negacije nisu teoreme teorije L.

Drugi primer sistema sa jednom aksiomom (dužom od Mereditove) je dao Lukašijevič:

$$((A \Rightarrow B) \Rightarrow (((\neg C \Rightarrow \neg D) \Rightarrow E) \Rightarrow C)) \Rightarrow (F \Rightarrow ((C \Rightarrow A) \Rightarrow (D \Rightarrow A)))$$

U radu [9] autor je dao izvođenje aksioma $L1$, $L2$ i $L3$ iz Mereditove, kao i iz Lukašijevičeve aksiome koje je generisao programom *Otter*.

3.2 Minimalni sistemi izvođenja nad skupom $\{\uparrow\}$

Jednostavan način za dobijanje deduktivnog sistema nad Šeferovim veznikom sa jednom aksiomom je transformisanje Mereditove aksiome u formulu koja sadrži samo Šeferov veznik. Ovo se može uraditi uz pomoć ekvivalencija o kojima je bilo reči u podpoglavlju 1.1. Pri tome se dobija veoma duga aksioma (sa 36 veznika), a broj promenljivih kao kod Mereditove aksiome ostaje pet. Pravilo izvođenja (modus ponens) se transformiše u: $\frac{A, A\uparrow(B\uparrow B)}{B}$.

Drugačiji sistem koji sadrži takođe jednu, ali znatno kraću aksiomu sa pet promenljvih, dao je Nikod 1917. godine:

N1 $(A \uparrow (B \uparrow C)) \uparrow ((D \uparrow (D \uparrow D)) \uparrow ((E \uparrow B) \uparrow ((A \uparrow E) \uparrow (A \uparrow E))))$

Ovaj sistem sadrži sledeće pravilo izvođenja:

MP' $\frac{A, A\uparrow(B\uparrow C)}{C}$

Ovo pravilo izvođenja je "jače"od pravila modus ponens, jer u premisama imamo više mogućnosti, tj. ograničenje da su promenljive u zagradi jednake ovde ne postoji.

U ovom i narednim poglavljima ćemo osim klasičnog infiksnog zapisa, formule sa binarnim veznikom zapisivati i pomoću prefiksne poljske notacije pri čemu ćemo za binarni veznik koristiti simbol F, a promenljive ćemo označavati malim slovima abecede.

Na taj način zapisan Nikodov sistem sadrži aksiomu sa 23 simbola i 5 promenljivih:

$$FFaFbcFFdFddFFebFFaeFae,$$

a pravilo izvođenja je:

$$\frac{a, FaFbc}{c}.$$

Lukašijevič je konstruisao sistem sa istim pravilom izvođenja i aksiomom iste dužine, ali sa 4 promenljive:

$$FFaFbcFFaFcaFFdbFFadFad.$$

Ova aksioma ima i osobinu da ne sadrži nijednu podformulu koja je tautologija. Za razliku od nje, Nikodova aksioma sadrži podformulu FdFdd koja jeste tautologija.

Ne može se konstruisati sistem sa jednom aksiomom manje dužine od 23. [7]

3.3 Najvažnija svojstva proizvoljne formalne teorije

U potpoglavlju 3.1 naveli smo da je moguće dokazati potpunost, saglasnost, neprotivrečnost i nezavisnost Hilbertovog sistema. Ovo su osobine koje su ključne za bilo koju formalnu teoriju, jer donose vezu između sintaksnog i semantičkog pristupa toj teoriji.

Za *proizvoljan sistem* se postavljaju sledeća najvažnija pitanja [6] :

- Da li postoji algoritam koji utvrđuje da li je taj sistem potpun i saglasan?
- Da li postoji algoritam koji za proizvoljan skup aksioma utvrđuje da li je on nezavisan?
- Da li postoji algoritam koji utvrđuje da li je neka iskazna formula teorema sistema?

Lineal i Post su 1949. godine pokazali da su sva tri odgovora negativna, tj. da su ovi problemu neodlučivi.

Traženi algoritmi iz prva dva pitanja ne postoje, a što se tiče trećeg pitanja - može se konstruisati sistem za koji traženi algoritam ne postoji.

4 Implementacija deduktivnih sistema

Kao primeri implementacije deduktivnih sistema su realizovani:

- *Program1* implementira deduktivni sistem nad skupom veznika $\{\neg, \Rightarrow\}$. Pravilo izvođenja je MP (opisano u potpoglavlju 3.1), a skup aksioma je promenljiv. U programu se primenjuje prefiksna poljska notacija uz korišćenje unarnog operatora N za veznik $\neg$ i binarnog operatora I za operator $\Rightarrow$.
- *Program2* implementira deduktivni sistem nad skupom veznika $\{\uparrow\}$. Pravilo izvođenja je MP' (opisano u potpoglavlju 3.2), a skup aksioma je promenljiv. U programu se primenjuje prefiksna poljska notacija uz korišćenje binarnog operatora F za veznik $\uparrow$.

Programi se pokreću iz komandne linije. Kao prvi, obavezan parametar komandne linije se zadaje ime datoteke koja sadrži niz aksioma, po jednu u svakom redu. Drugi, opcioni parametar predstavlja maksimalan broj iteracija (opisanih u algoritmu) koje će program izvršiti. Ako ovaj parametar nije naveden njegova vrednost je 10. Po pokretanju programa sa standardnog ulaza se unosi formula koja se dokazuje(teorema), a dokaz se ispisuje u datoteci čije ime je oblika: *dokaz_ime datoteke sa aksiomama_teorema*.

4.1 Algoritam

Oba programa koriste isti algoritam:

Niz formula koje čine dokaz se smešta u listu. Kao prvi elementi liste se upisuju aksiome sistema, a zatim se sprovodi niz iteracija. Jedna iteracija podrazumeva sledeća dva koraka:

1. na svaku formulu u trenutnoj listi se, ako je to moguće, primenjuje pravilo izvođenja sa svakom formulom koja joj prethodi. Na ovaj način se eventualno dobijaju nove formule, koje se dodaju na kraj liste.

2. u svakoj formuli koja je u listi se vrši instanciranje promenljivih podtermovima formule koja se dokazuje. Pri ovome se vrši instanciranje svih promenljivih svim kombinacijama odgovarajućih podtermova, a novodobijene formule se dodaju na kraj liste.

Iteracije se ponavljaju ili do pojave tražene formule, kada program prekida sa radom, a na standardnom izlazu se ispisuje poruka *Teorema je dokazana* ili do trenutka kada broj iteracija postane veći od parametra koji predstavlja njihov maksimalan broj. U tom slučaju se na standardnom izlazu ispisuje poruka *Teorema nije dokazana*.

4.2 Primeri

Primer 1 *Skup aksioma je jednak Hilbertovom skupu aksioma:*

H1 IaIba

H2 IIaIbcIIabIac

H3 IINaNbIINaba

Program1 daje sledeći dokaz teoreme IINaaa [2]*:*

1. IaIIINaaaa (u H1: b/IINaaa)
2. IaIINaaa (u H1: b/INaa)
3. IIaIIINaaaaIIaIINaaaIaa (u H2: b/IINaaa, c/a)
4. IINaNaIINaaa (u H3: b/a)
5. IIaIINaaaIaa (MP 1 i 3)
6. Iaa (MP 2 i 5)
7. INaNa (u 6: a/Na)
8. IINaaa (MP 4 i 7)

[2] $(\neg a \Rightarrow a) \Rightarrow a$

Primer 2 *Skup aksioma je jednak Hilbertovom skupu aksioma, zapisanom preko Šeferovog veznika:*

H1' FaFFbFaaFbFaa

H2' FFaFFbFccFbFccFFFaFbbFFaFccFaFccFFaFbbFFaFccFaFcc

H3' FFFbbFFaaFaaFFFFbbFaaFbbFFFbbFaaFbb

Program2 daje sledeći dokaz teoreme FaFaa [3]*:*

1. FaFFFaFaaFaaFFaFaaFaa (u H1': b/FaFaa)
2. FaFFaFaaFaFaa (u H1': b/a)
3. FFaFFFaFaaFaaFFaFaaFaaFFFaFFaFaaFaFaaFFaFaaFaFaaFFaFFaFaaFaFaaFFaFaaFaFaa (u H2': b/FaFaa, c/a)
4. FFaFFaFaaFaFaaFFaFaaFaFaa (MP' 1 i 3)
5. FaFaa (MP' 2 i 4)

5 S. Wolfram: "New kind of science"- kratak sažetak

Ovo poglavlje sadrži kratak pregled knjige [10], tačnije nekih delova koji se odnose na matematičku logiku i aksiomatske sisteme. Ono što bi trebalo naglasiti kao bitnu karakteristiku knjige je da ona obiluje rezultatima empirijskih istraživanja vezanim za automatsko dokazivanje, kao i aksiomatizaciju matematike uopšte.

5.1 Osnovne ideje

Jedan od pojmova koje autor uvodi i čijom se analizom bavi u toku cele knjige su tzv. *celularni automati*. Takav automat je, ustvari specifična formalna teorija nad binarnom azbukom $\{0,1\}$ sa 8 pravila izvođenja, koja ga jednoznačno određuju.

U donjoj tabeli su navedena pravila izvođenja za neke od automata:

automat A_i	pravila izvođenja
A_0	$\{\frac{000}{0},\frac{001}{0},\frac{010}{0},\frac{011}{0},\frac{100}{0},\frac{101}{0},\frac{110}{0},\frac{111}{0}\}$
A_1	$\{\frac{000}{0},\frac{001}{0},\frac{010}{0},\frac{011}{0},\frac{100}{0},\frac{101}{0},\frac{110}{0},\frac{111}{1}\}$
A_2	$\{\frac{000}{0},\frac{001}{0},\frac{010}{0},\frac{011}{0},\frac{100}{0},\frac{101}{0},\frac{110}{1},\frac{111}{0}\}$
...	
A_{129}	$\{\frac{000}{1},\frac{001}{0},\frac{010}{0},\frac{011}{0},\frac{100}{0},\frac{101}{0},\frac{110}{0},\frac{111}{1}\}$
...	
A_{255}	$\{\frac{000}{1},\frac{001}{1},\frac{010}{1},\frac{011}{1},\frac{100}{1},\frac{101}{1},\frac{110}{1},\frac{111}{1}\}$

[3] $a \uparrow (a \uparrow a)$, tj. $a \Rightarrow a$

Pravila izvođenja se ne primenjuju kao kod klasičnih formalnih teorija na celokupan string, već na svaku trojku uzastopnih bitova, proizvodeći jedan rezultujući bit u novom stringu. Npr. značenje pravila $\frac{001}{1}$ je: Ako se na pozicijama $k-1, k$ i $k+1$ u polaznom stringu nalaze redom bitovi $0, 0$ i 1, tada se na poziciji k u novom stringu nalazi bit 1.

Za početni string, tj. aksiomu autor u većini primera uzima string oblika: 000...00100...000.

Tako, npr. prvih 5 izvođenja za automat A_{129} je:

0	0	0	0	0	1	0	0	0	0	0
1	1	1	1	0	0	0	1	1	1	1
0	1	1	0	0	1	0	0	1	1	0
0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	1	1	1	1	1	0
				.	.	.				

Pojmove teorema i dokaz uvodimo analogno kao i kod drugih formalnih teorija: svaki string koji se može izvesti je teorema, a niz izvođenja do njega, dokaz teoreme.

Pre uvođenja pojmova potpunosti i neprotivrečnosti definišemo pojam negacije stringa: Za dati binarni niz s njegova negacija je niz $\bar{s}$ koji na svakoj svojoj poziciji ima inverzan bit u odnosu na string s. Na primer, string 0010 je negacija stringa 1101.

Za automat A kažemo da je *potpun* ako se za svaki string može izvesti ili on ili njegova negacija, a da je *neprotivrečan* ako ne postoji string takav da se mogu izvesti i on i njegova negacija.

Autor navodi da je pitanje da li je neki string teorema ovakvog sistema *neodlučivo*, tj. ne postoji generalni postupak koji bi to utvrđivao ili opovrgavao. Takođe navodi i potreban uslov za istovremenu potpunost i neprotivrečnost:

Ako je automat A potpun i neprotivrečan, tada on generiše tačno 2^{n-1} različitih teorema dužine n.

Zaista, ako je automat i potpun i neprotivrečan tada se iz njega može izvesti tačno polovina svih stringova neke dužine. Naime, ako bi taj broj bio veći od polovine tada bi postojao string s, takav da su i s i $\bar{s}$ teoreme, tj. automat bi bio protivrečan. U suprotnom, ako bi broj stringova koji se mogu izvesti bio manji od polovine, automat bi bio nepotpun, jer bi postojao string s, takav da ni s ni $\bar{s}$ nisu teoreme.

Iz ovakve karakterizacije sledi da je za istovremeno ispunjenje obe osobine potrebno da važi veoma strog uslov, tj. da su osobine kompletnosti i neprotivrečnosti u izvesnom smislu u koliziji. Ovo je i razlog zbog kojeg je vrlo mali broj automata A_i i potpun i neprotivrečan.

Analognim razlozima autor objašnjava i relativnu malobrojnost drugih formalnih teorija koje su istovremeno i potpune i neprotivrečne. Ovde daje poseban osvrt na Peanovu aritmetiku za koju je dugo važilo uverenje da ima obe osobine, ali je Gedelov stav o njenoj nepotpunosti to porekao.

5.2 Zavisnost dužine dokaza od broja i dužina aksioma

Jedno od pitanja koje se razmatra je i sledeće: Da li su dokazi bazirani na aksiomatskom sistemu sa manjim brojem aksioma neminovno duži kao što intuitivno izgleda od dokaza baziranih na sistemima sa većim brojem aksioma?

Da bi dao empirijski odgovor na ovo pitanje autor navodi 8 ekvivalentnih aksiomatskih sistema za klasičnu iskaznu logiku, baziranih na Šeferovom vezniku. Oni respektivno sadrže 6, 4, 3, 3, 2, 2, 1 i 1 aksiomu. Zatim navodi i oko 500 numerisanih ekvivalencija koje važe u iskaznoj logici (što se može proveriti npr. pomoću istinitosnih tablica) i upoređuje dužine dokaza svih ovih ekvivalencija u svakom aksiomatskom sistemu.

Npr. ekvivalencija $a \uparrow b \Leftrightarrow b \uparrow a$ u pomenutih 8 sistema ima dokaze sledećih dužina, respektivno: 6, 1, 8, 49, 8, 1, 119, 118.

Posle analize dužina svih dokaza dolazi do (empirijskog) zaključka da aksiomatski sistemi sa više aksioma generalno ne moraju da budu mnogo efikasniji od onih sa manjim brojem aksioma.

5.3 Oblasti matematike kao grafovi

Autor se bavi i aksiomatizacijom raznih polja matematike, razmatrajući svaku teoriju kao graf čiji su koreni aksiome iz kojih se zatim vrše sva moguća izvođenja i na taj način dobijaju čvorovi grafa tj. teoreme. Grane ovakvog grafa odgovaraju dokazima.

Razmatrajući skup svih teorema neke teorije među mnoštvom se ističu pojedine koje imaju svoja eksplicitna imena i koje su u nekom smislu poznatije od ostalih. Npr. takve, "opšte poznate" teoreme u klasičnoj logici su $a \wedge b \Leftrightarrow b \wedge a$ (komutativnost veznika $\wedge$) ili $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$ (De Morganov zakon), za razliku od drugih teorema bez eksplicitnog imena kao što su npr. $a \wedge a \Leftrightarrow a \vee a$ ili $a \wedge b \Leftrightarrow (a \wedge b) \wedge a$.

Pitanje na koje autor pokušava da odgovori je da li osim "slučajnog istorijskog konteksta" postoji neka bitna karakteristika koju poseduju ove opšte prihvaćene teoreme, a nemaju je one manje poznate. Odgovor do kojeg dolazi razmatrajući njihovu poziciju u grafovima koji predstavljaju pojedina polja matematike je da su to najčešće teoreme koje se dobijaju izvođenjem direktno iz aksioma, a ne iz drugih teorema, a i kada je to slučaj to su vrlo dugi dokazi.

Autor, takođe iznosi i ideju da su epiteti koje intuitivno dodeljujemo teoremama vezani zapravo za strukturu mreže koja predstavlja određenu teoriju i poziciju teoreme o kojoj govorimo u njoj. Tako, npr. "komplikovana" je teorema koja ima dug dokaz, "korisna" je ona koja dovodi do mnogo novih, a "iznenadjujuća" ona koja se pojavljuje u nekom odvojenom delu mreže od svojih lema itd.

6 Zaključak

Glavni problemi u iskaznoj logici su da li je data iskazna formula valjana i da li je data iskazna formula zadovoljiva. Pristup ovim problemima može biti *semantički* i *sintaksni* (deduktivni), a ključna veza između ova dva pojma je činjenica da je iskazna formula valjana (što je semantički pojam) akko je teorema nekog deduktivnog sistema (što je sintaksni pojam).

Kada govorimo o *semantičkom pristupu*, postavlja se pitanje koji zapis iskazne formule je najpogodniji za njenu analizu. Kao najpogodniji način zapisa se uglavnom koristi zapis u KNF formi gde je formula predstavljena kao konjukcija klauza, koje su diskunkcije literala. Ovaj način zapisa dakle, podrazumeva formule zapisane sa 2 binarna veznika: $\wedge$ i $\vee$.

Pitanje koje se nameće je da li se proučavanjem iskaznih formula zapisanih na drugačiji način, pomoću samo jednog veznika mogu dobiti neki novi zaključci i da li takav zapis ima neke svoje prednosti, pored očigledne mane da su takvi zapisi foprmula znatno duži i manje intuitivni od KNF zapisa.

Poglavlje 1 obrađuje temu koji veznici se samostalno mogu koristiti za zapis proizvoljne iskazne formule, tj. u ovom poglavlju smo se bavili potrebnim i dovoljnim uslovima za kompletnost iskaznih veznika.

Jedan od takvih veznika je Šeferov binarni veznik: $\uparrow$. U poglavlju 2 smo se detaljnije bavili formulama zapisanim pomoću njega. Potpoglavlja 2.2 i 2.3 sadrže empirijske rezultate o udelu valjanih i zadovoljivih formula nad veznikom $\uparrow$ među svim formulama nad tim veznikom. Zaključak do kojeg se na ovaj način dolazi je da su funkcije koje predstavljaju ove udele konvergentne, kada se dužina formule povećava.

Potpoglavlje 2.4 obrađuje neke od veza između formula zapisanih pomoću Šeferovog veznika i formula u KNF zapisu. Ovde smo došli do zaključka da se direktnim prevođenjem KNF formula u formule sa Šeferovim veznikom dužina zapisa eksponencijalno uvećava, pa je zbog toga temeljna ekperimentalna analiza otpala kao mogućnost.

Kada je u pitanju *sintaksni pristup* ispitivanju valjanosti i zadovoljivosti iskaznih formula, postavlja se pitanje kakav je deduktivni sistem najpogodniji za to. U poglavlju 3 smo se bavili minimalnim deduktivnim sistemima i u potpoglavljima 3.1 i 3.2. predstavili neke sisteme koji imaju jednočlane skupove aksioma. To su sistemi koji su manje intuitivni od sistema prirodne dedukcije, ali su istovremeno jednostavniji za programsku implementaciju. Sa druge strane dokazi generisani pomoću ovakvih sistema su znatno duži od dokaza u sistemima sa više aksioma.

U poglavlju 4 je dat kratak pregled programa koji predstavljaju implementaciju deduktivnih sistema sa jednim i dva veznika.

Poglavlje 5 sadrži pregled razmatranja S.Wolframa u vezi sa aksiomatskim sistemima koji se ne odnose samo na matematiku, već i na nauku, uopšte. Sva razmatranja sadrže ideju da se u matematici, pa i u celokupnoj nauci, a time i u prirodi od vrlo jednostavnih početnih uslova pomoću krajnje elementarnih pravila može doći do iznenađujuće raznovrsnih i složenih krajnjih ishoda.

Literatura

[1] http://www.iep.utm.edu, *Internet Encyclopedia of Philosophy - Propositional logic*

[2] http://us.metamath.org/mpegif/meredith.html

[3] http://people.umass.edu/klement/513/independ.pdf, *Independence of the axioms*

[4] P.Janičić. *Matematička logika u računarstvu.* Matematički fakultet, elektronsko izdanje, 2007.

[5] P.Janičić, P.Maksimović. *Simple characterization of functionally complete one-element sets of propositional connectives.* Mathematical Logic Quartely, Volume 52, Number 5, 498-504, 2006.

[6] S.Burris. *Comments on propositional proof systems*, 2001.

[7] http://fitelson.org/ar.html *New elegant axiomatizations of some sentential logics.*

[8] T.Sharle. *Axiomatization of propositional calculus with Sheffer functors.* Notre Dame Journal of Formal Logic, Volume 6, Number 2, 209-217,1965.

[9] L.Wos. *Conquering the Meredith single axiom.* Journal of automated reasoning, Volume 27, Number 2, 175-199, 2001.

[10] S.Wolfram. *A new kind of science*,Wolfram Media,Inc.2002.