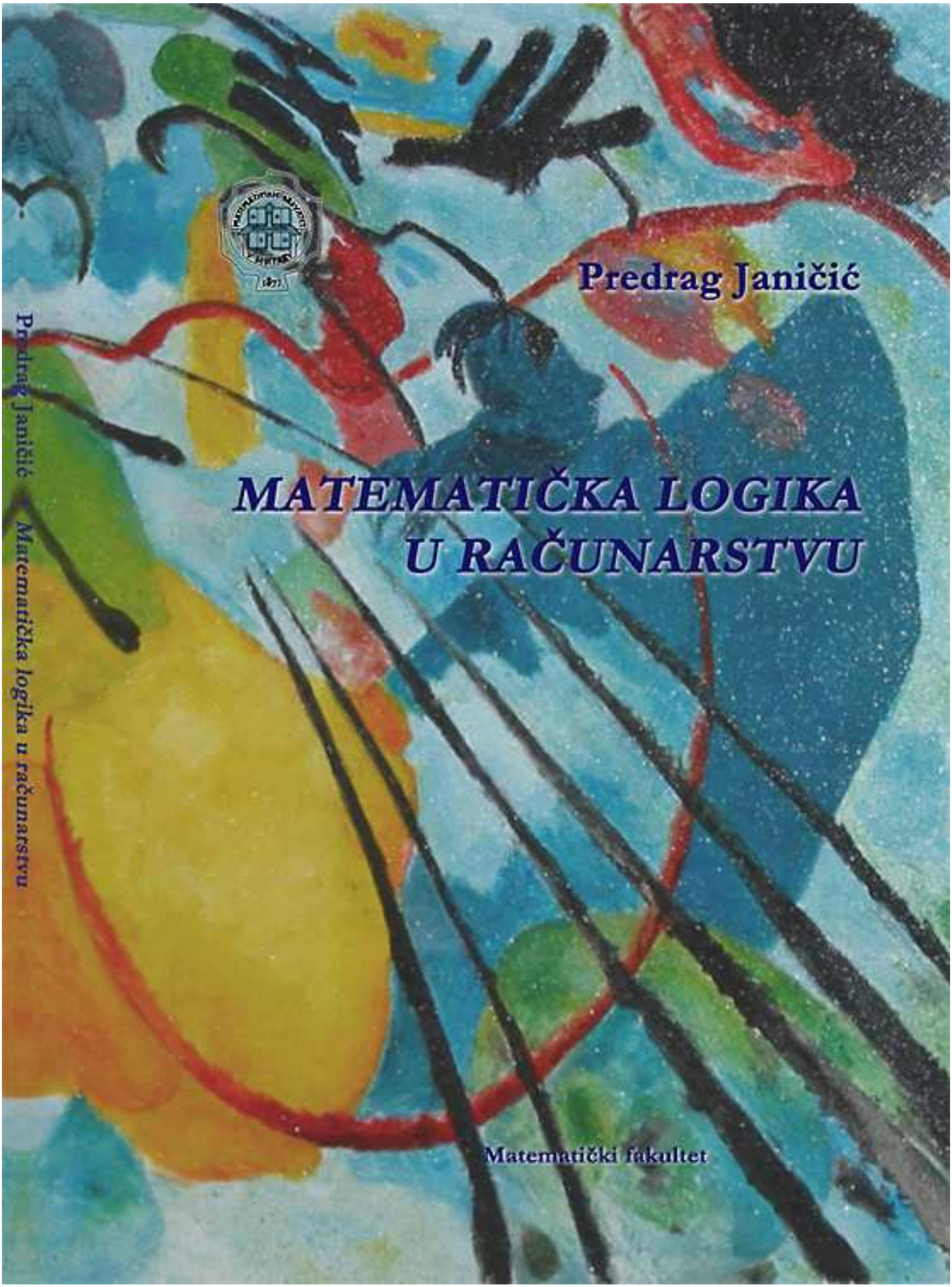
MATEMATIČKA LOGIKA U RAČUNARSTVU

ELEKTRONSKO IZDANJE
05.10.2008.


Predrag Janičić
MATEMATIČKA LOGIKA
U RAČUNARSTVU
Matematički fakultet
Predrag Janičić
Matematička logika u računarstvu

Predrag Janičić

MATEMATIČKA LOGIKA U RAČUNARSTVU

Četvrto, elektronsko izdanje

Beograd
2008.

Autor:
dr Predrag Janičić, docent na Matematičkom fakultetu u Beogradu

MATEMATIČKA LOGIKA U RAČUNARSTVU

Izdavač:
Matematički fakultet, Studentski trg 16, Beograd

Za izdavača:
dr Aleksandar Lipkovski

Recenzenti:
dr Mirjana Borisavljević, vanredni profesor na Saobraćajnom fakultetu u Beogradu
dr Goran Nenadić, docent na School of Informatics, University of Manchester
i asistent na Matematičkom fakultetu u Beogradu
dr Milan Božić, vanredni profesor na Matematičkom fakultetu u Beogradu

Priprema za štampu, crteži i korice:
dr Predrag Janičić

Prvo izdanje 2004. Drugo izdanje 2005. Treće izdanje 2007.
Četvrto izdanje 2008.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

510.6(075.8)
004.42(075.8)

ЈАНИЧИЋ, Предраг
Matematička logika u računarstvu / Predrag Janičić.
– 1. izd. – Beograd : Matematički fakultet, 2004
(Beograd : Skripta Internacional). – VI, 246 str. :
graf. prikazi ; 24 cm

Tiraž 100. – Biografske beleške: str. 213–223. –
Napomene uz tekst. – Bibliografija: str. 236–240. – Registar.

ISBN 86-7589-040-0

a) Математичка логика b) Програмирање
COBISS.SR-ID 117058316

ISBN 86-7589-040-0

Predgovor

Knjiga koja je pred vama nastala je od mojih beleški za predavanja i vežbe iz predmeta *Matematička logika u računarstvu* (sa četvrte godine smera Računarstvo i informatika na Matematičkom fakultetu Univerziteta u Beogradu), koje sam držao tokom akademskih godina 2001/02, 2002/03 i 2003/04. Nadam se da će ova knjiga biti korisna ne samo studentima koji slušaju pomenuti predmet, nego i svima koje interesuju veze matematičke logike i računarstva.

Za pripremu časova kao i ovog materijala koristio sam mnogo izvora, a najčešće [18, 7] (sintaksa i semantika), [66] (metod tabloa), [8, 7] (metod rezolucije), [14] (teorema o kompaktnosti), [48] (Hilbertov sistem), [73, 21] (prirodna dedukcija i račun sekvenata), kao i [64, 62, 43, 42, 35, 60, 58, 63]. Korisni su mi bili i materijali koje je dr Goran Nenadić obrađivao u okviru vežbi za kurs *Matematička logika u računarstvu* tokom akademskih godina od 1995/96 do 1999/00. Prezentovan materijal predstavlja svojevrsnu sintezu navedenih izvora, napravljenu u duhu navedenog kursa, ali i u skladu sa mojim gledanjem na ovu oblast. Na žalost, sve sadržaje koje sam želeo da uključim u ovaj kurs i ovu knjigu ne pokriva nijedan od navedenih izvora, pa čak ni njihova unija. Zbog toga se nadam da je opravdano postojanje ovako koncipiranog materijala i to posebno na našem jeziku.

Trudio sam se da sav materijal prezentujem na jednoobrazan način. Na primer, pokušao sam da jednoobrazno prezentujem iskaznu i predikatsku logiku, kao i pojedinačne metodologije u okviru njih. Usaglašavanje različitih pojmova, ideja, termina i notacijskih rešenja bilo je znatno teže nego što možda može da izgleda. Nadam se da su stil izlaganja, terminologija i notacija koje sam odabrao jednostavni i lako čitljivi.

Na kraju poglavlja dati su zadaci za vežbu. Znakom $\surd$ označeni su zadaci čije je rešenje dato u dodatku.

Dodatak sadrži tekstove o složenosti izračunavanja, o filozofiji i zasnivanju matematike i računarstva, kao i biografske beleške značajnih logičara. Ti materijali bi trebalo da prodube razumevanje osnovnog materijala i da ga smeste u širi matematički kontekst. Kao osnovni izvor informacija za biografske beleške korišćena je Internet enciklopedija matematike univerziteta Sent Endrjus [56].

Značajan deo matematičke logike u računarstvu čine neklasične logike i sistemi za prezapisivanje termova ali, zbog obima, oni se ne obrađuju u okviru pomenutog kursa i ove knjige.

Na izuzetno pažljivom čitanju i brojnim, izuzetno koristnim komentarima i sugestijama, zahvaljujem recenzentima dr Mirjani Borisavljević i dr Goranu Nenadiću. Na dragocenim savetima zahvalan sam i prof. Alanu Bandiju sa Univerziteta u Edinburgu. Tokom pisanja ovog teksta dragocenu pomoć dobijao sam od studenata smera za Računarstvo i informatiku Matematičkog fakulteta koji su kod mene slušali kurs *Matematička logika u računarstvu* akademske 2001/02, 2002/03 i 2003/04 godine. Povratne informacije koje sam dobijao od njih, njihova pitanja i ideje bili su za mene najbolji i najkorisniji putokazi. Zato bi kao moto ove knjige mogle da posluže reči Ivana Saterlenda *Knowledge is a rare thing — you gain by giving it away* („Znanje je čudno — dobijaš dajući ga“). Svojim komentarima i predlozima značajno su mi pomogli Dejan Brezo, Dušan Glavinić, Marija Milanović, Ana Mitrović, Miroslav Obradović, Ivan Petrović, Đorđe Stakić, Ivana Stefanović, Saša Stevanović, Ana Stojanović, Sana Stojanović, Tatjana Stupar, Andrija Tomović, Savo Turčinović i, posebno, veoma pažljivim čitanjem više verzija teksta Milena Vujošević. Svima im najtoplije zahvaljujem na pomoći. Za sve postojeće greške u knjizi odgovornost, naravno, snosim sâm.

Beograd, septembar 2004.

Autor

Predgovor drugom izdanju

U drugom izdanju ispravljeno je nekoliko grešaka uočenih u prvom izdanju. Napravljeno je nekoliko manjih dodataka i pojednostavljeni su dokazi nekoliko teorema. Zahvaljujem studentima koji su slušali kurs *Matematička logika u računarstvu* akademske godine 2004/05 i koji su svojim komentarima uticali na novo izdanje ove knjige.

Beograd, novembar 2005.

Autor

Predgovor trećem izdanju

Ovo, treće izdanje knjige je elektronsko i besplatno dostupno sa Internet adrese www.matf.bg.ac.yu/~janicic. Nadam se da će tako biti pristupačno još širem krugu potencijalnih čitalaca.

Ovu knjigu, na izvestan način, upotpunjuju sledeći (elektronski) materijali, dostupni sa iste Internet adrese:

- *Matematička logika u računarstvu, knjiga II — Domaći zadaci, testovi, ispitni rokovi, ispitna pitanja*, koja sadrži domaće zadatke i njihova rešenja (koja su pisali studenti), testove (kontrolne vežbe), zadatke sa ispitnih rokova i ispitna pitanja.
- *Matematička logika u računarstvu, knjiga III — Odabrana poglavlja matematičke logike u računarstvu*, koja sadrži studentske radove na izabrane teme koje proširuju osnovni sadržaj kursa *Matematička logika u računarstvu*.

U ovom izdanju knjige ispravljeno je nekoliko grešaka uočenih u drugom izdanju i dodato nekoliko objašnjenja. Zahvaljujem studentima koji su slušali kurs *Matematička logika u računarstvu* akademske godine 2005/06 i koji su svojim komentarima i pitanjima uticali na novo izdanje ove knjige. Na izuzetno brižljivom čitanju teksta i brojnim ispravkama i komentarima posebno zahvaljujem Aleksandru Daniloviću. Zahvalnost na kvalitetnim zapažanjima dugujem i Nebojši Taušanu, Milanu Ružiću i Ivanu Čukiću.

Svi komentari na ovu verziju knjige biće veoma dobrodošli, a mogu biti poslati elektronskom poštom na adresu janicic@matf.bg.ac.yu.

Beograd, januar 2007.

Autor

Predgovor četvrtom izdanju

I ovo, četvrto izdanje knjige je elektronsko i besplatno dostupno sa Internet adrese www.matf.bg.ac.yu/~janicic.

U ovom izdanju knjige ispravljene su greške (uglavnom slovne i stilske, ali i nekoliko materijalnih) uočene u trećem izdanju. Skoro sve njih je, izvanredno pažljivim čitanjem, otkrio Ivan Elčić i ja mu na tome najtoplije zahvaljujem.

Svi komentari i na ovu verziju knjige biće veoma dobrodošli, a mogu biti poslati elektronskom poštom na adresu janicic@matf.bg.ac.yu.

Beograd, oktobar 2008.

Autor

Sadržaj

1 Kratka istorija matematičke logike **1**

2 Iskazna logika **7**
2.1 Sintaksa iskazne logike 7
2.2 Semantika iskazne logike 10
2.2.1 Valuacija, interpretacija, model; zadovoljive, valjane,porecive i kontradiktorne formule 10
2.2.2 Istinitosne tablice 13
2.2.3 Logičke posledice, logički ekvivalentne formule,supstitucija 14
2.2.4 Potpuni skupovi veznika 21
2.2.5 Normalne forme 23
2.2.6 Dejvis–Patnam–Logman–Lovelandova procedura 28
2.2.7 Metod rezolucije 31
2.2.8 Metod tabloa 39
2.2.9 Teorema o kompaktnosti za iskaznu logiku 47
2.3 Sistemi za dedukciju u iskaznoj logici 49
2.3.1 Hilbertov sistem 52
2.3.2 Prirodna dedukcija 64
2.3.3 Račun sekvenata 70
2.4 Sažetak 80

3 Logika prvog reda **83**
3.1 Sintaksa logike prvog reda 84
3.2 Semantika logike prvog reda 88
3.2.1 Valuacija, interpretacija, model; zadovoljive, valjane,porecive i kontradiktorne formule 88
3.2.2 Logičke posledice, logički ekvivalentne formule,supstitucija 93
3.2.3 Normalne forme 100
3.2.4 Erbranova teorema 107
3.2.5 Unifikacija 115
3.2.6 Metod rezolucije 119
3.2.7 Metod tabloa 135
3.3 Sistemi za dedukciju u logici prvog reda 145
3.3.1 Hilbertov sistem 146
3.3.2 Prirodna dedukcija 153
3.3.3 Račun sekvenata 155

3.4 Teorije prvog reda . . . 156
3.4.1 Čista teorija jednakosti . . . 158
3.4.2 Teorija grupa . . . 159
3.4.3 Teorija gustih uređenih Abelovih grupa bez krajnjihtačaka 160
3.5 Saželak . . . 162

4 Odlučivost i procedure odlučivanja 165
4.1 Rekurzivne funkcije . . . 165
4.2 Odlučive i neodlučive teorije . . . 168
4.3 Metode za dokazivanje odlučivosti i procedure odlučivanja . . . 170
4.3.1 Furije–Mockinova procedura . . . 172
4.3.2 Kongruentno zatvorenje i Nelson–Openova procedura . 177
4.4 Saželak . . . 183

A Složenost izračunavanja 185
A.1 Klase složenosti . . . 185
A.2 NP-kompletnost . . . 186
A.3 Problem SAT i fazna promena . . . 190
A.4 Značajne klase problema . . . 195
A.5 Složenost teorija . . . 196
A.6 Saželak . . . 196

B Matematička logika i zasnivanje matematike i računarstva 197
B.1 Hilbertov program i Gedelove teoreme . . . 197
B.1.1 Peanova aritmetika . . . 200
B.1.2 Gedelovo kodiranje . . . 201
B.1.3 Prva Gedelova teorema o nepotpunosti . . . 202
B.1.4 Druga Gedelova teorema o nepotpunosti . . . 204
B.1.5 Problem odlučivanja . . . 206
B.2 Matematičko-filozofski pravci . . . 207
B.2.1 Matematički realizam ili platonizam . . . 207
B.2.2 Formalizam . . . 208
B.2.3 Intuicionizam i konstruktivizam . . . 209
B.3 Zasnivanje računarstva . . . 210
B.4 Saželak . . . 211

C Biografske beleške 213

D Rešenja zadataka 225

Glava 1

Kratka istorija matematičke logike

Matematička logika je disciplina koja se bavi analizom metoda za rezonovanje. Osnovna pitanja koja se postavljaju u logici su šta znači to da određeni zaključak sledi iz nekih pretpostavki i šta je to matematički dokaz? Pitanja istinitosti i rezonovanja zaokupljaju filozofe i matematičare hiljadama godina. Značaj matematičke logike, međutim, verovatno nikada nije bio veći nego danas — zbog njene uloge u drugim matematičkim disciplinama, a pre svega zbog njene uloge u računarstvu.

Postojanje određenih logičkih veza između različitih tvrđenja bilo je poznato i mnogo pre Aristotela. Ipak, najraniji poznati dokument koji se detaljno bavi raznim aspektima ovih veza je knjiga *Organon*, kolekcija Aristotelovih spisa sakupljenih nakon njegove smrti 322. p.n.e. Uticaj te knjige oseća se i danas. Ona je postavila temelje za pojmove neophodne za razvoj formalnog logičkog jezika, uvela pojam premisa, demonstrativnih i dijalektičkih argumenata, pojam posebnih argumenata (ili pravila izvođenja) u terminima tzv. *silogizama*, uvela teoriju značenja i istine, a bavila se čak i modalnim tvrđenjima. Aristotel kaže: „silogizam je struktura reči u kojoj, kada se načine izvesne pretpostavke, nešto drugačije od onog što je pretpostavljeno nužno sledi“. U *Organonu* postoje tri osnovne silogističke sheme iz kojih se može izvesti svaki poseban silogizam. Prva dva (u originalnom Aristotelovom označavanju) od četrnaest osnovnih silogizama mogu se predstaviti na sledeći način[1]:

Ako svaki M ima svojstvo L i ako svaki S ima svojstvo M,
onda svaki S ima svojstvo L.

Ako nijedan M nema svojstvo L i ako svaki S ima svojstvo M,
onda nijedan S nema svojstvo L.

[1] Ova dva silogizma kasnije su nazvana *Barbara* i *Celarent*: mnemoničko značenje samoglasnika u ovim rečima (latinskog jezika) je sledeće: *a* označava univerzalno potvrdno (afirmativno) („svaki ima svojstvo ...“), a *e* univerzalno odrično („nijedan nema svojstvo ...“).

Gotovo dve hiljade godina Aristotelove postavke logike nisu bitno promenjene ili bitno unapređene. Izdvojićemo ovde samo nekoliko imena iz tog perioda. Krispius je, u trećem veku pre nove ere, dao veoma precizan pregled dela logike (koji danas zovemo iskazna logika). U četrnaestom veku, Rejmond Lul je radio na mehaničkom sistemu *Ars Magna* („Veliko umeće“) predviđenom da iscrpno ispituje sve mogućnosti u (kombinatornim) matematičkim problemima određene klase i tako omogući neke forme preciznog rezonovanja. Tomas Hobs je u svojoj knjizi *Computatio sive Logica* („Računanje ili logika”) iz 1655. godine tvrdio da je razmišljanje svodljivo na neku vrstu izračunavanja, ali nije dao nikakav praktičan sistem koji bi to mogao da potvrdi.

Lajbnic, „koji zaslužuje da se svrsta među najveće logičare u istoriji“, razvio je bazične Hobsove ideje prilično precizno. Štaviše, Lajbnic je spekulisao da će formalni sistem za logičko rasuđivanje u svom konačnom obliku omogućavati ljudima da razreše nesporazume ili neslaganja po bilo kom pitanju, da će u njihovo razrešavanje ljudi kretati uzevši olovke u ruke i rekavši *Calculemus!* („izračunajmo!“). Gledajući daleko ispred svog vremena, on za svoj planirani sistem govori „... da će biti oslobođen nužnosti razmišljanja o stvarima samim, ali ipak će sve biti ispravno“. Lajbnicov plan bio je da stvori idealni formalni jezik, *lingua philosophica* („jezik filozofije“) ili *characteristica universalis* („opšti opis“, „opšti jezik“), ali u tom planu nije stigao ni do kakvih detalja. Taj, takav jezik trebalo je, po Lajbnicovim idejama, da omogući stvaranje okvira za *calculus rationator* („račun zaključivanja“). Dodatno, i u istom ovom kontekstu, Lajbnic je izneo ideju o enciklopediji, tj. o sistematskoj kolekciji znanja svih vrsta. Lajbnic je pokušavao da izgradi logiku kao sistem za izračunavanje koji bi mogao da se izvodi mehanički, poput aritmetičkih izračunavanja (čime je prvi anticipirao koncepte automatskog rezonovanja). Mada je želeo da izgradi opšti sistem (dovoljno izražajan da uključi i logiku matematičkih oktrića), uspeo je da donekle razvije detalje samo za dve specifične strukture. Jedna je račun za identitet i inkluziju, čime je anticipirao iskazni račun. Druga struktura koju je Lajbnic razvio je geometrijski račun sa sličnošću i podudarnošću. Prvi od ovih računa (iskazni račun, tj. Bulova algebra) razvijen je potpuno precizno (i predstavljen kao račun u lajbnicovskom smislu) 1847. godine u Bulovoj knjizi *Mathematical Analysis of Logic* („Matematička analiza logike“). Dvadesetak godina kasnije napravljen je i prvi mehanički sistem koji je koristio ovaj račun — mašina za proveravanje bulovskih identiteta koju je konstruisao Stenli Dževons. Geometrijski račun (bez korišćenja koordinata) u duhu Lajbnicovih ideja razvijen je prvi put 1844. godine u Grasmanovoj knjizi *Ausdehnunglehre* („Teorija proširenja“).

Ključni korak u definisanju predikatskog računa, verovatno je knjiga *Begriffsschrift — Eine der arithmetischen nachgebildete Formelsprache des reinen Denkens* („Zapisivanje pojmova — jezik formula čiste misli, po uzoru na aritmetiku“) Gotliba Fregea iz 1879. godine. U svom radu Frege se eksplicitno referisao na Lajbnicov pojam univerzalnog jezika. Fregeov jezik *Begriffsschrift* („zapisivanje pojmova“) je, suštinski, ono što mi danas zovemo jezikom prvog reda. Frege je, između ostalog, precizno uveo formalni jezik i svojstva kvan-

tifikatora, određen broj aksiomatskih shema i pravila izvođenja (uključujući *modus ponens*), kao i precizne pojmove *izvođenja* i *dokaza*. Ova Fregeova knjiga može se smatrati i direktnim začetnikom moderne logike i formalnih jezika (uključujući i programske jezike). Fregeova namera bila je da, u okviru svog sistema, opiše i aritmetiku, ali je, što je pokazao Bertrand Rasel, u tom delu Fregeovog sistema postojala nekonzistentnost. Godina 1879. smatra se zbog Fregeovih prodora „najznačajnijom godinom u istoriji logike". Njegovo otkriće kvantifikatora koji vezuju promenljive smatra se jednim od najvećih otkrića devetnaestog veka. Kasnijih godina, računi slični Fregeovom bili su razvijani i popularisani od strane Hilberta, koji je u svojim radovima posvećivao izuzetnu pažnju aksiomatizaciji matematike. Često se termin *Frege-Hilbertov račun* (ili ponekad samo *Hilbertov račun*) koristi za sve sisteme u duhu originalnog Fregeovog. Jedna od najznačajnijih Fregeovih ideja je i tzv. *logistička teza* ili *Fregeova teza* koja tvrdi da je matematika izvodiva iz logike, tj. da ona predstavlja njeno proširenje. Ova ideja izložena je detaljno u znamenitoj knjizi Vajtheda i Rasela *Principia Mathematica* („Principi matematike", 1910/13).

Prve decenije dvadesetog veka bile su ispunjene značajnim rezultatima i oštrim raspravama i suprotstavljanjima po pitanjima poimanja formalnih jezika, dokaza, beskonačnosti i, posebno, koncepta intuicionističke matematike (u to vreme oličenog pre svih u Braueru). U odbranu klasične matematike od kritika intuicionista (koji prihvataju samo konstruktivne metode u izvođenju dokaza) formulisani su jasni „metamatematički programi" u jednom radu Emila Posta iz 1920. godine (koji se odnosio na iskazni račun) i 1928. godine u znamenitoj knjizi *Grundzuge der Theoretischen Logik* („Osnove teorijske logike") Hilberta i Akermana. U ovoj knjizi formulisana je aksiomatika za predikatski račun i dokazano mnoštvo njegovih svojstava. Otvorena su pitanja potpunosti i konzistentnosti formalne aritmetike, kao i tzv. *Entscheidungsproblem* („problem odlučivanja") — problem pronalaženja opšteg algoritma koji za datu rečenicu proverava da li je teorema. Negativni odgovori na ove probleme stigli su nekoliko godina kasnije u rezultatima Gedela, Čerča i Tjuringa u kojima je dokazano postojanje (esencijalno) nepotpunih i neodlučivih teorija.

Početkom dvadesetog veka razmatrani su logički sistemi prihvatljivi po određenim matematičko-filozofskim konceptima. U okviru toga, tragalo se za sistemima koji odgovaraju matematičkom rezonovanju. Uprkos mnogim dobrim karakteristikama, Frege-Hilbertov račun ne oslikava prirodno način na koji matematičari dokazuju teoreme. Matematičari prave pretpostavke, dokazuju nove formule na osnovu tih pretpostavki i, konačno, eliminišu pretpostavke. Na primer, da bi dokazao implikaciju $A \Rightarrow B$, matematičar najpre uvodi pretpostavku da važi A, zatim dokazuje B, i, konačno, eliminisanjem pretpostavke A, zaključuje da važi $A \Rightarrow B$. Težeći računu koji bi odgovarao uobičajenom matematičkom rezonovanju, Gerhard Gencen je tridesetih godina dvadesetog veka razvio *prirodnu dedukciju*. Gencenove motive ilustruju sledeće njegove reči: „... formalizacija logičke dedukcije, pogotovu kako su je razvili Frege, Rasel i Hilbert, prilično je daleko od formi dedukcije koje se u

praksi koriste u matematičkim dokazima. Zauzvrat su dobijene značajne formalne prednosti. Nasuprot tome, moja namera je da izgradim formalni sistem koji je, koliko je to moguće, blizak stvarnom rasuđivanju. Rezultat je 'račun prirodne dedukcije' ...". Na tragu Gencenovih radova, njegove prirodne dedukcije i, posebno, *računa sekvenata*, razvijeno je više varijanti srodnih sistema i sistema za automatsko dokazivanje teorema.

Nakon napora da se izgrade zadovoljavajući formalni sistemi za dedukciju, sredinom tridesetih godina dvadesetog veka Tarski je razvio precizan pojam semantike — pojam značenja formula iskazne i predikatske logike. Za razliku od sintaksno-deduktivnog pristupa, u kojem je proces dokazivanja teorema sveden na kombinatornu igru simbolima, semantika formula se vezuje za istinitost u matematičkim strukturama za koje se veruje da objektivno postoje, nezavisno od ljudskog uma. Uprkos razlikama između semantike i dedukcije, između njih postoje brojne veze (npr. svojstva potpunosti i saglasnosti), a i obe dele isti koncept jezika i skupa formula.

Od prve četvrtine dvadesetog veka razvoj matematičke logike ispretpleten je sa razvojem računarstva, pre svega sa razvojem teorijskog računarstva. Negativan odgovor na Hilbertovo pitanje o potpunosti formalne aritmetike, postavio je granice formalističkog metoda i moći zaključivanja bilo kog budućeg računara. Rezultatima Tjuringa, Čerča i drugih matematičara precizno su uvedeni pojmovi izračunavanja i izračunljivosti i pre pojave prvih računara. Rešenje *halting problema* pokazalo je da ne postoji opšti metod za utvrđivanje da li se zadati program zaustavlja, i to pre prvih programa koji bi mogli da se izvršavaju na računarima. Prvi računari nastali su tokom Drugog svetskog rata i bili su korišćeni u ratne svrhe. Matematička logika bitno je uticala na razvoj prvih programskih jezika i, kasnije, tokom pedesetih i šezdesetih godina, na izgradnju teorije formalnih jezika. Krajem šezdesetih i početkom sedamdesetih, precizno je zasnovana teorija složenosti izračunavanja i razvijen pojam NP-kompletnosti. Semantika programskih jezika proučava se od sedamdesetih godina, a od osamdesetih paralelno izračunavanje, distribuirano izračunavanje i kvantno izračunavanje. Danas se matematička logika koristi u gotovo svim granama računarstva i često je njena uloga vitalna (slično kao što matematička analiza ima fundamentalnu ulogu u fizici i tehničkim naukama). Logika danas ima veliki značaj u širokom spektru disciplina — od teorije izračunljivosti, veštačke inteligencije (automatsko dokazivanje teorema i verifikacija softvera i hardvera), softver inžinjeringa (specifikacija i verifikacija), programskih jezika (semantika programskih jezika, logičko programiranje, funkcionalno programiranje), algoritmike (složenost izračunavanja), obrade teksta i jezika, baza podataka (relaciona algebra i SQL), do arhitekture računara (dizajn i minimizacija logičkih kola). U zavisnosti od konkretnog računarskog konteksta, kao pogodna teorijska osnova koriste se klasična, intuicionistička, modalna, temporalna, relevantna, fazi logika, teorija tipova itd. Ne samo da računarstvo koristi dostignuća matematičke logike, već najvećim delom motiviše i usmerava njen razvoj. Zbog toga je danas nemoguće povući liniju koja razgraničava logiku i računarstvo. Štaviše, znamenita konstruktivistička teorija tipova Martina Lefa

izjednačava pojam specifikacije programa i pojam teoreme, kao i pojam programa i dokaza teoreme, brišući time razliku između računarstva i ostatka matematike.

Istorija razvoja matematičke logike i teorije dokaza gotovo poklapa se i sa istorijom razvoja automatskog rezonovanja. Kako kaže Vos, „lepota matematičke teoreme, preciznost logičkog pravila izvođenja, izazovnost zagonetke i izazov igre — sve je to prisutno u polju automatskog rezonovanja“ [75]. Radovi Skolema i Erbrana iz dvadesetih i tridesetih godina bili su od presudnog uticaja na mnoštvo sistema za automatsko rezonovanje (zasnovanih na pogodnim pravilima izvođenja). To se pogotovo odnosi na šezdesete i sedamdesete godine kada oblast automatske dedukcije uzima maha i kada su razvijeni mnogi značajni sistemi izvođenja prilagođeni automatskoj primeni — pomenimo samo metod tabloa i, jedno vreme dominantan, metod rezolucije (koji je u osnovi programskog jezika PROLOG). Uprkos konciznosti metoda rezolucije koja se ogledala u primeni samo jednog pravila izvođenja i uprkos ogromnoj energiji uloženoj u unapređenja, velika početna očekivanja počela su da splašnjavaju i sve se manje verovalo da metod rezolucije, bez obzira na modifikacije, može da dovede do efikasnih rešenja u automatskom dokazivanju teorema. Već sedamdesetih godina istraživači su se okrenuli kvalitativno drugačijim pristupima, tragajući sve češće za mogućnostima za formalizaciju i oponašanje uobičajenog, intuitivnog rasuđivanja.

Glava 2

Iskazna logika

U iskaznoj logici promenljive reprezentuju iskaze. Iskazi mogu biti kombinovani u složenije iskaze logičkim veznicima. Iskazna logika dovoljno je izražajna za opisivanje i reprezentovanje mnogih problema, uključujući mnoge praktične probleme, kao što je, na primer, dizajn integrisanih kola.

Iskazna logika ima tri aspekta: svoju sintaksu (ili jezik), svoju semantiku (ili značenje iskaza) i svoje deduktivne sisteme. I semantika i deduktivni sistemi grade se nad isto definisanom sintaksom, tj. nad istim skupom formula.

Centralni problemi u iskaznoj logici su ispitivanje da li je data iskazna formula valjana (tautologija) i da li je data iskazna formula zadovoljiva. Ovaj drugi problem poznat je kao problem SAT i on je tipičan predstavnik skupa NP-kompletnih problema.

Postoji više metoda i pristupa za ispitivanje valjanosti i zadovoljivosti. Neki od njih su semantičke, a neki deduktivne (tj. sintaksno-deduktivne) prirode. Ključna veza između ova dva koncepta je tvrđenje da je iskazna formula valjana (što je semantička kategorija) ako i samo ako je ona teorema (što je deduktivna kategorija). Zahvaljujući ovoj vezi, sintaksa iskazne logike (jezik iskazne logike), njena semantika (konvencije o *značenju* formula) i njena deduktivna svojstva čine kompaktnu celinu.

2.1 Sintaksa iskazne logike

Sintaksni aspekt iskazne logike govori o njenom *jeziku*, a o formulama isključivo kao o nizovima simbola i ne uzima u obzir bilo kakvo njihovo (moguće) značenje.

Alfabet (azbuka) je neki neprazan skup simbola. *Reč nad alfabetom* je svaki konačan niz simbola tog alfabeta.

Definicija 2.1 *Neka je alfabet* Σ *unija sledeća četiri skupa:*

1. *prebrojivog skupa* iskaznih slova P;

2. *skupa* logičkih veznika $\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$ *pri čemu je* $\neg$ *unarni veznik, a* $\wedge, \vee, \Rightarrow$ *i* $\Leftrightarrow$ *su binarni veznici;*

3. *skupa* logičkih konstanti $\{\top, \bot\}$*;*

4. *skupa* pomoćnih simbola $\{(,)\}$.

Skup iskaznih formula *(ili* jezik iskazne logike*) nad skupom* P *je najmanji podskup skupa svih reči nad* Σ *takav da važi:*

- *iskazna slova (iz skupa* P*) i logičke konstante su iskazne formule;*
- *ako su* A *i* B *iskazne formule, onda su i* $(\neg A)$*,* $(A \wedge B)$*,* $(A \vee B)$*,* $(A \Rightarrow B)$ *i* $(A \Leftrightarrow B)$ *iskazne formule.*

Umesto termina *iskazna formula* često ćemo pisati kraće *formula* ili *iskaz*.

Elemente skupa P obično označavamo malim latiničnim slovima (eventualno sa indeksima). Iskazne formule obično označavamo velikim latiničnim slovima (eventualno sa indeksima). Skupove iskaznih formula obično označavamo velikim slovima grčkog alfabeta (eventualno sa indeksima).

U daljem tekstu smatraćemo (ako nije drugačije naglašeno) da je skup P fiksiran (za jedan alfabet Σ).

Logičke veznike zovemo i *bulovskim veznicima* ili, kraće, *veznicima*. Veznik $\neg$ zovemo *negacija*, veznik $\wedge$ *konjunkcija*, $\vee$ *disjunkcija*, $\Rightarrow$ *implikacija* i $\Leftrightarrow$ *ekvivalencija*. Zapis $(\neg A)$ čitamo *negacija* A ili *ne* A. Zapis $(A \wedge B)$ čitamo A *konjunkcija* B ili A *i* B. Zapis $(A \vee B)$ čitamo A *disjunkcija* B ili A *ili* B. Zapis $(A \Rightarrow B)$ čitamo A *implikacija* B ili *iz* A *sledi* B. Zapis $(A \Leftrightarrow B)$ čitamo A *ekvivalencija* B ili A *ekvivalentno* B.

Iskazna slova zovemo i *iskazne promenljive* ili *iskazne varijable*. Elemente skupova P i $\{\top, \bot\}$ zovemo *atomičkim iskaznim formulama*. Simbol $\top$ čitamo *te*, a simbol $\bot$ čitamo *nete*. *Literal* je iskazna formula koja je ili atomička iskazna formula ili negacija atomičke iskazne formule. *Klauza* je disjunkcija literala.

Ako su dve iskazne formule A i B sintaksno identične (tj. ako su jednake kao nizovi simbola), onda to označavamo $A = B$. Ako dve iskazne formule A i B nisu sintaksno identične, onda to označavamo $A \neq B$.

Zagrade se koriste kako bi se izbegla višesmislenost. Naime, bez zagrada, iskazna formula $a \Leftrightarrow b \wedge c$ ima dva moguća tumačenja: $((a \Leftrightarrow b) \wedge c)$ i $(a \Leftrightarrow (b \wedge c))$. Višesmislenost se može izbeći i korišćenjem prefiksne poljske notacije. U toj notaciji, iskazna formula $((a \Leftrightarrow b) \wedge c)$ se zapisuje $\wedge \Leftrightarrow a\ b\ c$, a iskazna formula $(a \Leftrightarrow (b \wedge c))$ se zapisuje $\Leftrightarrow a \wedge b\ c$. Ipak, zbog čitljivosti, koristićemo infiksni zapis, zapis iskaznih formula koji odgovara prethodnoj definiciji. Da bismo izbegli korišćenje velikog broja zagrada obično izostavljamo spoljne zagrade i usvajamo konvenciju uz koju u nekim iskaznim formulama neke zagrade mogu biti izostavljene bez straha od višesmislenosti. Ta konvencija zasnovana je na prioritetu veznika i to na sledeći način (veznici su poređani po prioritetima — od većeg ka manjem): $\neg \quad \wedge \quad \vee \quad \Rightarrow \quad \Leftrightarrow$.

Definicija 2.2 *Skup* potformula *formule A je najmanji skup formula koje zadovoljavaju sledeće uslove:*

- *svaka iskazna formula A je potformula sama sebi;*
- *Ako je A jednako $\neg B$, onda je svaka potformula formule B istovremeno i potformula formule A. Ako je A jednako $B \wedge C$, $B \vee C$, $B \Rightarrow C$ ili $B \Leftrightarrow C$, onda je svaka potformula formule B i svaka potformula formule C istovremeno i potformula formule A.*

Primer 2.1 *Skup potformula formule $(p \Rightarrow q) \vee r$ je $\{p, q, r, p \Rightarrow q, (p \Rightarrow q) \vee r\}$.*

Teorema 2.1 (Indukcija nad skupom iskaznih formula) *Neka je ϕ svojstvo reči jezika nad alfabetom Σ. Pretpostavimo da za svojstvo ϕ važi:*

- *svojstvo ϕ važi za svaku atomičku iskaznu formulu;*
- *ako svojstvo ϕ važi za iskazne formule A i B, onda ono važi i za iskazne formule $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$ i $A \Leftrightarrow B$.*

Tada svojstvo ϕ važi za svaku iskaznu formulu.

Dokaz: Neka je L skup svih reči nad alfabetom Σ (za skup P) za koje je zadovoljen uslov ϕ. Skup L zadovoljava oba uslova definicije skupa iskaznih formula. Kako je skup iskaznih formula najmanji takav skup, sledi da je on podskup skupa L, tj. svojstvo ϕ važi za svaku iskaznu formulu nad P. □

Definicija 2.3 *Funkcija c iz skupa iskaznih formula u skup* **N** *(skup prirodnih brojeva) svakoj iskaznoj formuli pridružuje* složenost *na sledeći način:*

1. *ako je A atomička iskazna formula, onda je $c(A) = 0$;*
2. $c(\neg A) = c(A) + 1$;
3. $c(A \wedge B) = c(A) + c(B) + 1$;
4. $c(A \vee B) = c(A) + c(B) + 1$;
5. $c(A \Rightarrow B) = c(A) + c(B) + 1$;
6. $c(A \Leftrightarrow B) = c(A) + c(B) + 1$.

Funkcijom c svakoj iskaznoj formuli pridružuje se (jedinstvena) složenost. Zaista, svakoj atomičkoj formuli A pridružena je vrednost 0 ($c(A) = 0$ na osnovu prvog pravila u definiciji funkcije c). Ako su formulama A i B pridružene vrednosti $c(A)$ i $c(B)$, onda je složenost određena i za formule $c(\neg A)$, $c(A \wedge B)$, $c(A \vee B)$, $c(A \Rightarrow B)$, $c(A \Leftrightarrow B)$ (pravilima od drugog do šestog u definiciji funkcije c). Na osnovu teoreme o indukciji nad skupom iskaznih formula (teorema 2.1), sledi da je funkcijom c složenost pridružena svakoj iskaznoj formuli.

2.2 Semantika iskazne logike

Semantički aspekt iskazne logike govori o *značenju* formula. U nastavku će biti uvedena semantika iskazne logike u stilu Tarskog (koji je prvi precizno uveo pojam semantike 1933. godine) [72]. Tako uvedenu semantiku zovemo i *semantika Tarskog*.

2.2.1 Valuacija, interpretacija, model; zadovoljive, valjane, porecive i kontradiktorne formule

Funkcije v iz P u $\{0,1\}$ zovemo *valuacijama*. Skup $\{0,1\}$ zovemo *domenom* ili *univerzumom* valuacije. Svaka valuacija v određuje funkciju I_v koju zovemo *interpretacijom* za valuaciju v i koja preslikava skup iskaznih formula u skup $\{0,1\}$. Interpretaciju I_v definišemo na sledeći način:

- $I_v(p) = v(p)$, za svaki element p skupa P;
- $I_v(\top) = 1$ i $I_v(\bot) = 0$;
- $I_v(\neg A) = 1$ ako je $I_v(A) = 0$ i $I_v(\neg A) = 0$ ako je $I_v(A) = 1$;
- $I_v(A \wedge B) = 1$ ako je $I_v(A) = 1$ i $I_v(B) = 1$; $I_v(A \wedge B) = 0$ inače;
- $I_v(A \vee B) = 0$ ako je $I_v(A) = 0$ i $I_v(B) = 0$; $I_v(A \vee B) = 1$ inače;
- $I_v(A \Rightarrow B) = 0$ ako je $I_v(A) = 1$ i $I_v(B) = 0$; $I_v(A \Rightarrow B) = 1$ inače;
- $I_v(A \Leftrightarrow B) = 1$ ako je $I_v(A) = I_v(B)$; $I_v(A \Leftrightarrow B) = 0$ inače.

Vrednost $I_v(A)$ zovemo *vrednošću iskazne formule A u interpretaciji I_v*. Ako za valuaciju v važi $I_v(A) = 1$, onda kažemo da je iskazna formula A *tačna u interpretaciji* I_v i da je iskazna formula A *tačna u valuaciji* v. Ako za valuaciju v važi $I_v(A) = 0$, onda kažemo da je iskazna formula A *netačna u interpretaciji* I_v. Nije teško dokazati (indukcijom nad skupom iskaznih formula) da se, za određenu valuaciju v, funkcijom I_v definisanom na navedeni način, svakoj formuli pridružuje (jedinstvena) vrednost (u toj interpretaciji).

Definicija 2.4 *Valuacija v je zadovoljavajuća za formulu A ako je $I_v(A) = 1$. Kažemo i da je zadovoljavajuća valuacija v* model *za A i pišemo $v \models A$.*

Definicija 2.5 *Iskazna formula A je* zadovoljiva *ako postoji valuacija koja je za nju zadovoljavajuća. Formula A je* valjana *ili* tautologija[1] *ako je svaka valuacija za nju zadovoljavajuća, tj. ako za svaku valuaciju v važi $v \models A$ i to zapisujemo*

[1] Reč *tautologija* grčkog je porekla i sačinjena je od reči *tauto* (grčki *isto*) i *logos* (grčki *reč, reći*). U bukvalnom prevodu, „tautologija" znači „reći isto". U lingivstičkom smislu, kao i u svakodnevnom jeziku, označava ponavljanje istog, reći istu stvar drugim rečima, redudantnost (slično, ali ne isto što i *pleonazam* — pleonazam označava korišćenje suvišnih reči prilikom ukazivanja na neki pojam). Opisani pojam tautologije razlikuje se od pojma tautologije u logici. U savremenim evropskim jezicima reč tautologija prvi put se javlja u šesnaestom veku.

$\models A$. *Iskazna formula je* nezadovoljiva *ili* kontradikcija *ako ne postoji valuacija koja je za nju zadovoljavajuća. Formula je* poreciva *ako postoji valuacija koja za nju nije zadovoljavajuća.*

Drugim rečima, iskazna formula je zadovoljiva ako postoji valuacija u kojoj je ta formula tačna. Iskazna formula je valjana ako je tačna u svakoj valuaciji. Iskazna formula je nezadovoljiva ako je netačna u svakoj valuaciji. Iskazna formula je poreciva ako postoji valuacija u kojoj je ta formula netačna.

Primer 2.2 *Iskazne formule $p \Rightarrow p$ i $p \vee \neg p$ su tautologije; iskazna formula $p \Rightarrow q$ je zadovoljiva i poreciva, a iskazna formula $p \wedge \neg p$ je kontradikcija.*

Problem ispitivanja da li je data iskazna formula zadovoljiva označava se sa SAT (od engleskog sat*isfiability problem* — problem zadovoljivosti). SAT problem je NP-kompletan [10] (videti poglavlje A.2). S obzirom na to da se još uvek ne zna da li su klase P i NP problema jednake, to znači da se još uvek ne zna da li postoji algoritam za ispitivanje zadovoljivosti koji je polinomijalne složenosti. Kako je opšte uverenje da su klase P i NP problema različite, veruje se i da ne postoji polinomijalni algoritam za rešavanje SAT problema. I najefikasniji danas poznati algoritmi za rešavanje ovog problema su eksponencijalne složenosti (videti poglavlje A.3). Distribucija zadovoljivih formula nad fiksnim skupom iskaznih slova ima svojstvo tzv. fazne promene (videti poglavlje A.3).

Definicija 2.6 *Skup iskaznih formula Γ je* zadovoljiv *ako postoji valuacija u kojoj je svaka formula iz Γ tačna. Za valuaciju v koja je zadovoljavajuća za sve formule iz Γ kažemo da je model za Γ. Skup iskaznih formula Γ je* nezadovoljiv *ili* kontradiktoran *ako ne postoji valuacija u kojoj je svaka formula iz Γ tačna.*

Primer 2.3 *Skup iskaznih formula $\{p \Rightarrow q, p, \neg q\}$ je kontradiktoran (ali nijedan njegov pravi podskup nije kontradiktoran).*

Teorema 2.2 *Ako su iskazne formule A i $A \Rightarrow B$ tautologije, onda je i B tautologija.*

Dokaz: Pretpostavimo da su A i $A \Rightarrow B$ tautologije. Pretpostavimo da postoji valuacija v u kojoj formula B nije tačna. Formula A je tautologija, pa je tačna i u valuaciji v. U toj valuaciji, dakle, formula $A \Rightarrow B$ nije tačna, što protivreči pretpostavci da je $A \Rightarrow B$ tautologija. Dakle, formula B je tačna u svakoj valuaciji, pa je ona tautologija, što je i trebalo dokazati. □

Zadaci

Zadatak 1 *√ Neka su A, B, C, D iskazne formule takve da su formule $A \Rightarrow (B \Rightarrow C)$ i $(A \wedge C) \Rightarrow \neg D$ tautologije. Dokazati da je i formula $(D \wedge A) \Rightarrow \neg B$ tautologija.*

Zadatak 2 *Dokazati sledeća tvrđenja:*

(a) Ako su formule $A \vee B$ i $\neg A \vee C$ tautologije, onda je i $B \vee C$ tautologija.

(b) Ako su formule $A \vee B$, $A \Rightarrow C$, $B \Rightarrow D$ tautologije, onda je i $C \vee D$ tautologija.

(c) Ako su formule $\neg A \vee B$ i $\neg C \vee \neg B$ tautologije, onda je i $A \Rightarrow \neg C$ tautologija.

Zadatak 3 *Dokazati sledeća tvrđenja:*

(a) Ako je iskazna formula valjana, onda je ona zadovoljiva.

(b) Ako je iskazna formula kontradikcija, onda je ona poreciva.

(c) Ako iskazna formula nije zadovoljiva, onda je ona kontradikcija i obratno.

(d) Ako iskazna formula nije tautologija, onda je ona poreciva i obratno.

Zadatak 4 *Dokazati sledeća tvrđenja:*

(a) Iskazna formula A je valjana ako i samo ako je $\neg A$ kontradikcija.

(b) Iskazna formula A je zadovoljiva ako i samo ako je $\neg A$ poreciva.

Zadatak 5 *Navesti primer iskazne formule koja je:*

(a) zadovoljiva
(b) valjana
(c) poreciva
(d) kontradikcija
(e) zadovoljiva i valjana
(f) zadovoljiva i nije valjana
(g) zadovoljiva i poreciva
(h) zadovoljiva i nije poreciva
(i) zadovoljiva i nije kontradikcija
(j) valjana i nije poreciva
(k) valjana i nije kontradikcija
(l) poreciva i nije zadovoljiva
(m) poreciva i nije valjana
(n) poreciva i kontradikcija
(o) poreciva i nije kontradikcija
(p) kontradikcija i nije zadovoljiva
(q) kontradikcija i nije valjana.

Zadatak 6 *Dokazati sledeća tvrđenja (Γ i Δ su skupovi iskaznih formula, A je iskazna formula):*

(a) Ako je Γ zadovoljiv i $\Delta \subset \Gamma$, onda je Δ zadovoljiv.

(b) Ako je Γ zadovoljiv i A valjana, onda je $\Gamma \cup \{A\}$ zadovoljiv.

(c) Ako je Γ kontradiktoran i $\Gamma \subset \Delta$, onda je Δ kontradiktoran.

(d) Ako je Γ kontradiktoran i A valjana, onda je $\Gamma \setminus \{A\}$ kontradiktoran.

Zadatak 7 *Odrediti (ako postoji) formulu A takvu da je formula $((p \Rightarrow (\neg q \wedge r)) \Rightarrow A) \Rightarrow (A \wedge ((r \Rightarrow q) \wedge p))$ tautologija.*

2.2.2 Istinitosne tablice

Pravila za određivanje vrednosti iskazne formule u zadatoj valuaciji (navedena u prethodnom poglavlju) mogu biti reprezentovana osnovnim *istinitosnim tablicama*:

A	$\neg A$
0	1
1	0

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Na osnovu navedenih tablica (tj. na osnovu pravila za određivanje vrednosti formule), može se kontruisati istinitosna tablica za proizvoljnu iskaznu formulu. U istinitosnoj tablici za neku formulu svakoj vrsti odgovara jedna valuacija iskaznih slova koje se pojavljuju u toj formuli. Svakoj koloni odgovara jedna potformula te formule. Istinitosne tablice su pogodne i za ispitivanje valjanosti, zadovoljivosti, nezadovoljivosti i porecivosti. Ukoliko iskazna formula A sadrži iskazne varijable p_1, p_2, ..., p_n, istinitosna tablica treba da sadrži sve moguće valuacije za ovaj skup varijabli (valuacije za druge varijable nisu relevantne). U zavisnosti od vrednosti iskaznih varijabli, izračunavaju se vrednosti složenijih iskaznih formula, sve do sâme iskazne formule koja se ispituje. Ako su u koloni koja odgovara sâmoj iskaznoj formuli sve vrednosti jednake 1, formula je tautologija; ako je bar jedna vrednost jednaka 1, formula je zadovoljiva; ako je bar jedna vrednost jednaka 0, formula je poreciva; ako su sve vrednosti jednake 0, formula je kontradikcija. Ovo pokazuje da su problemi ispitivanja valjanosti, zadovoljivosti, nezadovoljivosti i porecivosti odlučivi problemi, tj. postoje algoritmi koji ih mogu rešiti (više o odlučivosti videti u delu 4).

Primer 2.4 *Iskaznoj formuli* $(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$ *odgovara sledeća istinitosna tablica:*

p	q	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$	$p \Rightarrow q$	$(\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$
0	*0*	*1*	*1*	*1*	*1*	*1*
0	*1*	*0*	*1*	*1*	*1*	*1*
1	*0*	*1*	*0*	*0*	*0*	*1*
1	*1*	*0*	*0*	*1*	*1*	*1*

Dakle, data formula je zadovoljiva i valjana. Ona nije poreciva i nije kontradikcija.

Primer 2.5 *Istinitosna tablica može biti zapisana u skraćenom obliku — zapisivanjem samo zadate iskazne formule i odgovarajućih vrednosti ispod pojedinačnih iskaznih slova i veznika. Iskaznoj formuli iz prethodnog primera odgovara sledeća skraćena istinitosna tablica (popunjena u nekoliko koraka):*

$(\neg$	q	$\Rightarrow$	$\neg$	$p)$	$\Rightarrow$	$(p$	$\Rightarrow$	$q)$
	0			*0*		*0*		*0*
	1			*0*		*0*		*1*
	0			*1*		*1*		*0*
	1			*1*		*1*		*1*

$(\neg$	q	$\Rightarrow$	$\neg$	$p)$	$\Rightarrow$	$(p$	$\Rightarrow$	$q)$
1	*0*		*1*	*0*		*0*	*1*	*0*
0	*1*		*1*	*0*		*0*	*1*	*1*
1	*0*		*0*	*1*		*1*	*0*	*0*
0	*1*		*0*	*1*		*1*	*1*	*1*

$(\neg$	q	$\Rightarrow$	$\neg$	$p)$	$\Rightarrow$	$(p$	$\Rightarrow$	$q)$
1	*0*	*1*	*1*	*0*		*0*	*1*	*0*
0	*1*	*1*	*1*	*0*		*0*	*1*	*1*
1	*0*	*0*	*0*	*1*		*1*	*0*	*0*
0	*1*	*1*	*0*	*1*		*1*	*1*	*1*

$(\neg$	q	$\Rightarrow$	$\neg$	$p)$	$\Rightarrow$	$(p$	$\Rightarrow$	$q)$
1	*0*	*1*	*1*	*0*	**1**	*0*	*1*	*0*
0	*1*	*1*	*1*	*0*	**1**	*0*	*1*	*1*
1	*0*	*0*	*0*	*1*	**1**	*1*	*0*	*0*
0	*1*	*1*	*0*	*1*	**1**	*1*	*1*	*1*

Zadaci

Zadatak 8 *Ispitati metodom istinitosnih tablica da li je iskazna formula* $\neg((q \Rightarrow p) \Rightarrow p) \Rightarrow \neg p$ *zadovoljiva.*

Zadatak 9 *Ispitati metodom tablica da li je iskazna formula* $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ *tautologija.*

Zadatak 10 $\surd$ *Neka su* A*,* B*,* C*,* D *iskazne formule takve da su formule* $A \Rightarrow (B \Rightarrow C)$ *i* $(A \wedge C) \Rightarrow \neg D$ *tautologije. Dokazati, korišćenjem istinitosnih tablica, da je i formula* $(D \wedge A) \Rightarrow \neg B$ *tautologija.*

Zadatak 11 $\surd$ *Odrediti formulu* A *takvu da je formula* $((A \wedge q) \Rightarrow \neg p) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow A)$ *tautologija.*

Zadatak 12 *Odrediti, korišćenjem istinitosnih tablica, (ako postoji) formulu* A *takvu da je formula* $((p \Rightarrow (\neg q \wedge r)) \Rightarrow A) \Rightarrow (A \wedge ((r \Rightarrow q) \wedge p))$ *tautologija.*

2.2.3 Logičke posledice, logički ekvivalentne formule, supstitucija

Definicija 2.7 *Kažemo da je iskazna formula* A logička posledica *skupa iskaznih formula* Γ *i pišemo* $\Gamma \models A$ *ako je svaki model za skup* Γ *istovremeno i model za formulu* A*.*

Kada je skup Γ konačan, tada $\{A_1, ..., A_n\} \models B$ (tj. $\Gamma \models B$) pišemo kraće $A_1, ..., A_n \models B$. Ako je formula A logička posledica praznog skupa formula, onda to zapisujemo $\models A$. Ako ne važi $\Gamma \models A$, onda to zapisujemo $\Gamma \not\models A$.

Teorema 2.3

(a) Formula je valjana ako i samo ako je logička posledica praznog skupa formula.

(b) Ako je skup Γ kontradiktoran, onda je svaka formula njegova logička posledica. Specijalno, svaka formula je logička posledica skupa $\{\bot\}$.

(c) Ako je $\Gamma \subset \Delta$ i $\Gamma \models A$, onda je $\Delta \models A$.

(d) Ako je formula A valjana i $\Gamma \models B$, onda je $\Gamma \setminus \{A\} \models B$.

Dokaz:

(a) Ako je formula valjana, onda je ona tačna u svakoj valuaciji pa i u svakom modelu praznog skupa formula, te je ona logička posledica praznog skupa formula. Svaka valuacija je model za prazan skup formula, pa ako je formula logička posledica praznog skupa formula, onda je ona tačna u svakoj valuaciji, te je valjana.

(b) Ako je skup Γ kontradiktoran, onda on nema nijedan model. Važi da je svaki model iz tog (praznog!) skupa modela model za proizvoljnu formulu, pa je proizvoljna formula logička posledica skupa Γ.

(c) Pretpostavimo da važi $\Gamma \subset \Delta$ i $\Gamma \models A$. Iz $\Gamma \models A$ sledi da je proizvoljan model za Γ model i za A. Kako je $\Gamma \subset \Delta$, proizvoljan model za Δ je model za Γ, pa i za A. Dakle, važi $\Delta \models A$.

(d) Kako je formula A valjana, ona je tačna u svakoj valuaciji. Zbog toga je proizvoljan model za $\Gamma \setminus \{A\}$ model i za Γ, pa i za B. Dakle, važi $\Gamma \setminus \{A\} \models B$.

□

Primetimo da se simbol $\models$ koristi i za zapisivanje da je valuacija v model formule A i za označavanje relacije logičke posledice. Primetimo i da u oba okvira zapis $\models A$ ima isto značenje — da je formula A valjana.

Teorema 2.4 *$A_1, A_2, \ldots, A_n \models B$ ako i samo ako $\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$*

Dokaz: Pretpostavimo da važi $A_1, A_2, \ldots, A_n \models B$. Pretpostavimo da formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$ nije tautologija. Tada postoji valuacija u kojoj je formula B netačna, a formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n)$ tačna. Ako je u toj valuaciji formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n)$ tačna, onda je tačna i svaka od formula $A_1, A_2, \ldots, A_n$. S druge strane, kako važi $A_1, A_2, \ldots, A_n \models B$, sledi da je

u toj valuaciji tačna i formula B, što protivreči prethodnom zaključku da formula B nije tačna u toj valuaciji. Dakle, pogrešna je pretpostavka da $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$ nije tautologija, tj. važi $\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$.

Pretpostavimo da važi $\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$. Pretpostavimo da ne važi $A_1, A_2, \ldots, A_n \models B$. To znači da postoji valuacija u kojoj je svaka od formula A_1, A_2, ..., A_n tačna, a formula B nije. U toj valuaciji je tačna i formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n)$, a netačna je formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$. Odatle sledi da formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$ nije tautologija, što je suprotno pretpostavci. Dakle, mora da važi $A_1, A_2, \ldots, A_n \models B$, što je i trebalo dokazati. □

Teorema 2.5 *$\Gamma, A \models B$ ako i samo ako $\Gamma \models A \Rightarrow B$.*

Dokaz: Pretpostavimo da važi $\Gamma, A \models B$ i dokažimo $\Gamma \models A \Rightarrow B$. Pretpostavimo da su sve formule iz skupa Γ tačne u nekoj valuaciji v i dokažimo da je u toj valuaciji tačna i formula $A \Rightarrow B$. Pretpostavimo suprotno, da važi $I_v(A \Rightarrow B) = 0$. Odatle sledi $I_v(A) = 1$ i $I_v(B) = 0$. Dakle, valuacija v je model za skup formula $\Gamma \cup \{A\}$, pa iz $\Gamma, A \models B$ sledi da je valuacija v model i za formulu B, što je u suprotnosti sa $I_v(B) = 0$. Dakle, pretpostavka je bila pogrešna, pa sledi $I_v(A \Rightarrow B) = 1$, tj. $\Gamma \models A \Rightarrow B$, što je i trebalo dokazati.

Pretpostavimo da važi $\Gamma \models A \Rightarrow B$ i dokažimo $\Gamma, A \models B$. Pretpostavimo da su sve formule iz skupa $\Gamma \cup \{A\}$ tačne u nekoj valuaciji v i dokažimo da je u toj valuaciji tačna i formula B. U valuaciji v su tačne sve formule iz skupa Γ, pa iz $\Gamma \models A \Rightarrow B$ sledi $I_v(A \Rightarrow B) = 1$. Iz $I_v(A) = 1$ i $I_v(A \Rightarrow B) = 1$ sledi $I_v(B) = 1$ (ako bi važilo $I_v(B) = 0$, iz $I_v(A) = 1$ i $I_v(B) = 0$ bi sledilo $I_v(A \Rightarrow B) = 0$). Dakle, valuacija v je model za formulu B, tj. $\Gamma, A \models B$, što je i trebalo dokazati. □

Definicija 2.8 *Kažemo da su dve iskazne formule A i B* logički ekvivalentne *i pišemo $A \equiv B$ ako je svaki model formule A model i za B i obratno (tj. ako važi $A \models B$ i $B \models A$).*

Ako je svaki model za A istovremeno i model za B i obratno, onda u bilo kojoj valuaciji formule A i B imaju jednake vrednosti. Tvrđenja oblika $A \equiv B$ zovemo *logičkim ekvivalencijama* (ili kraće *ekvivalencijama*). Relacija $\equiv$ je, očigledno, relacija ekvivalencije nad skupom iskaznih formula.

Teorema 2.6 *Ako je $A_1 \equiv A_2$ i $B_1 \equiv B_2$, onda je:*

(a) $\neg A_1 \equiv \neg A_2$

(b) $A_1 \wedge B_1 \equiv A_2 \wedge B_2$

(c) $A_1 \vee B_1 \equiv A_2 \vee B_2$

(d) $A_1 \Rightarrow B_1 \equiv A_2 \Rightarrow B_2$

(e) $A_1 \Leftrightarrow B_1 \equiv A_2 \Leftrightarrow B_2$.

Dokaz:

Neka je v proizvoljna valuacija. Tada je $I_v(A_1) = I_v(A_2)$ i $I_v(B_1) = I_v(B_2)$.

(a)

$$\begin{aligned} I_v(\neg A_1) &= \begin{cases} 1, & I_v(A_1) = 0 \\ 0, & \text{inače} \end{cases} \\ &= \begin{cases} 1, & I_v(A_2) = 0 \\ 0, & \text{inače} \end{cases} \\ &= I_v(\neg A_2)\ . \end{aligned}$$

(b)

$$\begin{aligned} I_v(A_1 \wedge B_1) &= \begin{cases} 1, & I_v(A_1) = 1 \text{ i } I_v(B_1) = 1 \\ 0, & \text{inače} \end{cases} \\ &= \begin{cases} 1, & I_v(A_2) = 1 \text{ i } I_v(B_2) = 1 \\ 0, & \text{inače} \end{cases} \\ &= I_v(A_2 \wedge B_2)\ . \end{aligned}$$

(c)

$$\begin{aligned} I_v(A_1 \vee B_1) &= \begin{cases} 1, & I_v(A_1) = 1 \text{ ili } I_v(B_1) = 1 \\ 0, & \text{inače} \end{cases} \\ &= \begin{cases} 1, & I_v(A_2) = 1 \text{ ili } I_v(B_2) = 1 \\ 0, & \text{inače} \end{cases} \\ &= I_v(A_2 \vee B_2)\ . \end{aligned}$$

(d)

$$\begin{aligned} I_v(A_1 \Rightarrow B_1) &= \begin{cases} 0, & I_v(A_1) = 1 \text{ i } I_v(B_1) = 0 \\ 1, & \text{inače} \end{cases} \\ &= \begin{cases} 0, & I_v(A_2) = 1 \text{ i } I_v(B_2) = 0 \\ 1, & \text{inače} \end{cases} \\ &= I_v(A_2 \Rightarrow B_2)\ . \end{aligned}$$

(e)

$$\begin{aligned} I_v(A_1 \Leftrightarrow B_1) &= \begin{cases} 1, & I_v(A_1) = I_v(B_1) \\ 0, & \text{inače} \end{cases} \\ &= \begin{cases} 1, & I_v(A_2) = I_v(B_2) \\ 0, & \text{inače} \end{cases} \\ &= I_v(A_2 \Leftrightarrow B_2)\ . \end{aligned}$$

□

Teorema 2.7 *Važi $A \equiv B$ ako i samo ako je iskazna formula $A \Leftrightarrow B$ tautologija.*

Dokaz: Pretpostavimo da važi $A \equiv B$. U proizvoljnoj valuaciji v formule A i B imaju istu vrednost, pa je formula $A \Leftrightarrow B$ tačna u v. Odatle sledi da je $A \Leftrightarrow B$ tautologija. Pretpostavimo da je $A \Leftrightarrow B$ tautologija. Ako je u proizvoljnoj valuaciji v formula A tačna, onda mora da je i B tačna u v (jer je formula $A \Leftrightarrow B$ tačna u v). Dakle, svaki model za A je model i za B. Analogno važi obratno — svaki model za B je model i za A, te sledi $A \equiv B$, što je i trebalo dokazati. □

Primer 2.6 *Neke od logičkih ekvivalencija (ili, preciznije, neke od shema logičkih ekvivalencija) su:*

$\neg\neg A$	$\equiv$	A	*zakon dvojne negacije*
$A \vee \neg A$	$\equiv$	$\top$	*zakon isključenja trećeg*
$A \wedge A$	$\equiv$	A	*zakon idempotencije za* $\wedge$
$A \vee A$	$\equiv$	A	*zakon idempotencije za* $\vee$
$A \wedge B$	$\equiv$	$B \wedge A$	*zakon komutativnosti za* $\wedge$
$A \vee B$	$\equiv$	$B \vee A$	*zakon komutativnosti za* $\vee$
$A \Leftrightarrow B$	$\equiv$	$B \Leftrightarrow A$	*zakon komutativnosti za* $\Leftrightarrow$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	*zakon asocijativnosti za* $\wedge$
$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$	*zakon asocijativnosti za* $\vee$
$A \Leftrightarrow (B \Leftrightarrow C)$	$\equiv$	$(A \Leftrightarrow B) \Leftrightarrow C$	*zakon asocijativnosti za* $\Leftrightarrow$
$A \wedge (A \vee B)$	$\equiv$	A	*zakon apsorpcije*
$A \vee (A \wedge B)$	$\equiv$	A	*zakon apsorpcije*
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	*zakon distributivnosti* $\wedge$ *u odnosu na* $\vee$
$(B \vee C) \wedge A$	$\equiv$	$(B \wedge A) \vee (C \wedge A)$	*zakon distributivnosti* $\wedge$ *u odnosu na* $\vee$
$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$	*zakon distributivnosti* $\vee$ *u odnosu na* $\wedge$
$(B \wedge C) \vee A$	$\equiv$	$(B \vee A) \wedge (C \vee A)$	*zakon distributivnosti* $\vee$ *u odnosu na* $\wedge$
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	*De Morganov zakon*
$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$	*De Morganov zakon*
$A \wedge \top$	$\equiv$	A	*zakon konjunkcije sa tautologijom*
$A \vee \top$	$\equiv$	$\top$	*zakon disjunkcije sa tautologijom*
$A \wedge \bot$	$\equiv$	$\bot$	*zakon konjunkcije sa kontradikcijom*
$A \vee \bot$	$\equiv$	A	*zakon disjunkcije sa kontradikcijom*

Logičke ekvivalencije navedene u primeru 2.6, između ostalog, pokazuju da su konjunkcija i disjunkcija komutativni i asocijativni veznici. Zato možemo (uslovno) smatrati da konjunkcija (i disjunkcija) mogu da povezuju više od dve formule, pri čemu ne moramo da vodimo računa o njihovom poretku. Svaki član uopštene konjunkcije zovemo *konjunkt*, a svaki član uopštene disjunkcije zovemo *disjunkt*. Disjunkciju više literala (pri čemu njihov poredak nije bitan) zovemo *klauza*. Klauza je *jedinična* ako sadrži samo jedan literal.

Definicija 2.9 *Rezultat zamene (supstitucije) svih pojavljivanja iskazne formule C u iskaznoj formuli A iskaznom formulom D označavamo sa $A[C \mapsto D]$. Ta zamena (supstitucija) definiše se na sledeći način:*

- *ako za iskazne formule A i C važi $A = C$, onda je $A[C \mapsto D]$ jednako D;*
- *ako za iskazne formule A i C važi $A \neq C$ i A je atomička iskazna formula, onda je $A[C \mapsto D]$ jednako A;*
- *ako za iskazne formule A, B i C važi $A \neq C$ i $A = (\neg B)$, onda je $A[C \mapsto D] = \neg(B[C \mapsto D])$;*
- *ako za iskazne formule A, B_1, B_2 i C važi $A \neq C$ i $A = (B_1 \wedge B_2)$ ($A = (B_1 \vee B_2)$, $A = (B_1 \Rightarrow B_2)$, $A = (B_1 \Leftrightarrow B_2)$), onda je $A[C \mapsto D] = (B_1[C \mapsto D]) \wedge (B_2[C \mapsto D])$ ($(B_1[C \mapsto D]) \vee (B_2[C \mapsto D])$, $(B_1[C \mapsto D]) \Rightarrow (B_2[C \mapsto D])$, $(B_1[C \mapsto D]) \Leftrightarrow (B_2[C \mapsto D])$).*

Definicija 2.10 Uopštena zamena *(supstitucija) je skup zamena $[C_1 \mapsto D_1]$, $[C_2 \mapsto D_2]$, ..., $[C_n \mapsto D_n]$ gde su C_i i D_i proizvoljne iskazne formule. Takvu zamenu zapisujemo $[C_1 \mapsto D_1, C_2 \mapsto D_2, \ldots, C_n \mapsto D_n]$.*

Uopštena zamena primenjuje se simultano na sva pojavljivanja formula C_1, C_2, ..., C_n u polaznoj formuli i samo na njih (tj. ne primenjuje se na potformule dobijene zamenama).

U daljem tekstu ćemo umesto termina *uopštena zamena* (*uopštena supstitucija*) koristiti termin *zamena* (*supstitucija*).

Formulu koja je rezultat primene zamene $[C_1 \mapsto D_1, C_2 \mapsto D_2, \ldots, C_n \mapsto D_n]$ nad formulom A, označavamo sa $A[C_1 \mapsto D_1, C_2 \mapsto D_2, \ldots, C_n \mapsto D_n]$.

Primer 2.7

$((p \Rightarrow q) \Rightarrow r)[p \Rightarrow q \mapsto \neg p \vee q] = (\neg p \vee q) \Rightarrow r$
$((p \Rightarrow q) \Rightarrow (p \Rightarrow r))[p \Rightarrow q \mapsto \neg p \vee q, p \Rightarrow r \mapsto \neg p \vee r] = (\neg p \vee q) \Rightarrow (\neg p \vee r)$
$((p \Rightarrow q) \Rightarrow r)[p \Rightarrow q \mapsto \neg p \vee q, \neg p \vee q \mapsto q \vee \neg p] = (\neg p \vee q) \Rightarrow r$

Teorema 2.8 *Ako je iskazna formula A tautologija koja sadrži iskazna slova p_1, p_2, ..., p_n i ako su A_1, A_2, ..., A_n proizvoljne iskazne formule, onda je iskazna formula $B = A[p_1 \mapsto A_1, p_2 \mapsto A_2, \ldots, p_n \mapsto A_n]$ takođe tautologija.*

Dokaz: Pretpostavimo da je A tautologija. Neka je v proizvoljna valuacija. Neka je w valuacija u kojoj su iskaznim slovima p_1, p_2, ..., p_n dodeljene redom vrednosti $I_v(A_1)$, $I_v(A_2)$, ..., $I_v(A_n)$ i u kojoj je svakom iskaznom slovu p koje se pojavljuje u A, a različito je od $p_1, p_2, \ldots, p_n$ dodeljuje vrednost $I_v(p)$. Indukcijom nad skupom iskaznih formula može se dokazati da važi $I_v(B) = I_w(A)$. Iskazna formula A je tautologija, pa je ona tačna u svakoj valuaciji. Dakle, $I_w(A) = 1$, odakle je $I_v(B) = 1$. Kako je v proizvoljna valuacija, sledi da je formula B tačna u svakoj valuaciji, tj. sledi da je formula B tautologija, što je i trebalo dokazati. □

Teorema 2.9 (Teorema o zameni) *Ako je $C \equiv D$, onda je $A[C \mapsto D] \equiv A$.*

Dokaz: Razmotrimo prvo specijalan slučaj kada je $A = C$. Iz definicije zamene sledi da je $A[C \mapsto D] = D$, pa, kako je $C \equiv D$, očigledno je da važi $A[C \mapsto D] \equiv A$.

Pretpostavimo da je $A \neq C$. Ako je A atomička iskazna formula, iz definicije zamene sledi da je $A[C \mapsto D] = A$, pa je očigledno i $A[C \mapsto D] \equiv A$.

Pretpostavimo da tvrđenje teoreme važi za iskazne formule A i B, proizvoljne složenosti. Dokazaćemo da iz toga sledi da ona važi i za iskazne formule $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$.

(a) Na osnovu definicije zamene, važi $(\neg A)[C \mapsto D] = \neg A[C \mapsto D]$. Na osnovu pretpostavke je $A[C \mapsto D] \equiv A$, pa, na osnovu teoreme 2.6, sledi $\neg A[C \mapsto D] \equiv \neg A$, odakle je $(\neg A)[C \mapsto D] \equiv \neg A$.

(b) Na osnovu definicije zamene, važi $(A \wedge B)[C \mapsto D] = A[C \mapsto D] \wedge B[C \mapsto D]$. Na osnovu pretpostavke je $A[C \mapsto D] \equiv A$ i $B[C \mapsto D] \equiv B$, pa, na osnovu teoreme 2.6, sledi $A[C \mapsto D] \wedge B[C \mapsto D] \equiv A \wedge B$, odakle je $(A \wedge B)[C \mapsto D] \equiv A \wedge B$.

(c) Analogno prethodnom delu, važi $(A \vee B)[C \mapsto D] = A[C \mapsto D] \vee B[C \mapsto D] \equiv A \vee B$.

(d) Analogno prethodnom delu, važi $(A \Rightarrow B)[C \mapsto D] = A[C \mapsto D] \Rightarrow B[C \mapsto D] \equiv A \Rightarrow B$.

(e) Analogno prethodnom delu, važi $(A \Leftrightarrow B)[C \mapsto D] = A[C \mapsto D] \Leftrightarrow B[C \mapsto D] \equiv A \Leftrightarrow B$.

Pošto svojstvo koje opisuje ova teorema važi za atomičke formule, a iz pretpostavke da važi za proizvoljne formule A i B sledi da ono važi i za formule $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$, na osnovu teoreme o indukciji (2.1) sledi da tvrđenje teoreme važi za sve iskazne formule. □

Zadaci

Zadatak 13 *Ako C nije potformula iskazne formule A, onda je $A[C \mapsto D] = A$.*

Zadatak 14 *Dokazati da iz $A \equiv A[C \mapsto D]$ ne sledi $C \equiv D$.*

Zadatak 15 *Iskazna formula A sadrži (samo) iskazna slova p_1, p_2, ..., p_n i (jedino) logički veznik $\Leftrightarrow$. Dokazati sledeće: formula A je tautologija ako i samo ako se svako njeno iskazno slovo pojavljuje paran broj puta. (Uputstvo: iskoristiti činjenicu da $\Leftrightarrow$ ima svojstvo komutativnosti i asocijativnosti.)*

Zadatak 16 *Iskazna formula A sadrži samo veznike $\Leftrightarrow$ i $\neg$. Dokazati da je A tautologija ako i samo ako se svaka promenljiva i znak negacije pojavljuju paran broj puta.*

2.2.4 Potpuni skupovi veznika

Istinitosna funkcija nad n argumenata je funkcija koja preslikava skup $\{0,1\}^n$ u skup $\{0,1\}$. Nad n argumenata ima 2^{2^n} različitih istinitosnih funkcija (jer skup $\{0,1\}^n$ ima 2^n elemenata i svaki od njih se može preslikati u 0 ili u 1). Svaka iskazna formula koja ima n iskaznih slova generiše neku istinitosnu funkciju nad n argumenata. Logički ekvivalentne iskazne formule (sa istim brojem iskaznih slova) generišu identične istinitosne funkcije.

Teorema 2.10 *Svaka istinitosna funkcija je generisana nekom iskaznom formulom koja sadrži samo veznike $\wedge$, $\vee$ i $\neg$.*

Dokaz: Neka je $f(x_1, x_2, \ldots, x_n)$ istinitosna funkcija. Funkcija f može biti reprezentovana istinitosnom tablicom koja ima 2^n vrsta, od kojih svaka sadrži jednu dodelu vrednosti 0 ili 1 varijablama $x_1, x_2, \ldots, x_n$ i odgovarajuću vrednost $f(x_1, x_2, \ldots, x_n)$. Ako je $1 \leq i \leq 2^n$, neka je C_i konjunkcija $l_1^i \wedge l_2^i \wedge \ldots \wedge l_n^i$, gde je l_j^i jednako p_j ako u i-toj vrsti istinitosne tablice x_j ima vrednost 1 i $\neg p_j$, ako x_j ima vrednost 0. Neka je A disjunkcija svih konjunkcija C_i takvih da f ima vrednost 1 u i-toj vrsti istinitosne tablice (ako nema nijedne takve vrste, onda f uvek ima vrednost 0 i može se uzeti da je formula A jednaka $p \wedge \neg p$, što zadovoljava tvrđenje u tom slučaju). Dokažimo da formuli A kao istinitosna funkcija odgovara funkcija f. Neka je data neka valuacija za iskazna slova p_1, p_2, ..., p_n i neka je odgovarajuća dodela varijablama x_1, x_2, ..., x_n k-ta vrsta tablice za f. Formula C_k ima vrednost 1 u toj valuaciji, dok svaka druga C_i ima vrednost 0. Ako f ima vrednost 1 za vrstu k, onda je C_k disjunkt formule A, pa i formula A ima vrednost 1 u toj valuaciji. Ako f ima vrednost 0 za k-tu vrstu, onda C_k nije disjunkt formule A i svi disjunkti formule A imaju vrednost 0 u toj valuaciji, pa i formula A ima vrednost 0 u ovoj valuaciji. Dakle, formula A generiše istinitosnu funkciju f. □

Primer 2.8

x_1	x_2	$f(x_1, x_2)$
1	1	0
0	1	1
1	0	1
0	0	1

Iskazna formula A koja generiše istinitosnu funkciju f je $(\neg p_1 \wedge p_2) \vee (p_1 \wedge \neg p_2) \vee (\neg p_1 \wedge \neg p_2)$.

U bilo kojoj iskaznoj formuli, mogu se, korišćenjem ekvivalencija

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$$
$$A \Rightarrow B \equiv \neg A \vee B$$
$$A \vee B \equiv \neg(\neg A \wedge \neg B)$$

eliminisati sva pojavljivanja veznika $\Leftrightarrow$, $\Rightarrow$ i $\vee$. Dobijena formula sadržaće, dakle, samo veznike $\neg$ i $\wedge$. Kažemo da je skup veznika $\{\neg, \wedge\}$ *potpun*, jer je svaka iskazna formula logički ekvivalentna nekoj iskaznoj formuli samo nad ova dva veznika i bez logičkih konstanti $\top$ i $\bot$. Na osnovu teoreme 2.10, kako je skup $\{\neg, \wedge\}$ potpun, sledi da je svaka istinitosna funkcija generisana nekom iskaznom formulom koja sadrži samo veznike $\wedge$ i $\neg$. Skup $\{\neg, \vee\}$ je, takođe, potpun.

Veznici $\downarrow$ i $\uparrow$ definišu se na sledeći način: $A \downarrow B$ je jednako $\neg(A \vee B)$, a $A \uparrow B$ je jednako $\neg(A \wedge B)$. Naglasimo da su ove definicije čisto sintaksne prirode i da zapis $A \downarrow B$ možemo smatrati samo kraćim zapisom formule $\neg(A \vee B)$. Veznik $\downarrow$ zovemo *nili* ili *Lukašijevičeva funkcija*, a veznik $\uparrow$ zovemo *ni* ili *Šeferova funkcija*. Na osnovu datih definicija mogu se izvesti istinitosne tablice za $\downarrow$ i $\uparrow$.

A	B	$A \downarrow B$	$A \uparrow B$
0	0	1	1
0	1	0	1
1	0	0	1
1	1	0	0

Lako se pokazuje da je $\neg A \equiv (A \downarrow A)$ i $A \wedge B \equiv ((A \downarrow A) \downarrow (B \downarrow B))$. Kako je skup veznika $\{\neg, \wedge\}$ potpun, sledi da je potpun i skup $\{\downarrow\}$. Isto važi i za skup $\{\uparrow\}$.

Teorema 2.11 *Veznici $\downarrow$ i $\uparrow$ su jedina dva binarna veznika koja sama (pojedinačno) čine potpun sistem.*

Dokaz: Pretpostavimo da je moguće definisati binarni veznik $*$ takav da je skup $\{*\}$ potpun. Ako bi važilo $I_v(A * B) = 1$ za $I_v(A) = I_v(B) = 1$, onda bi vrednost svake formule bila jednaka 1 u valuaciji u kojoj je svakom iskaznom slovu pridružena vrednost 1. Tada funkciju $\neg p$ ne bi bilo moguće definisati preko veznika $*$. Dakle, za $I_v(A) = I_v(B) = 1$

mora da važi $I_v(A*B) = 0$. Analogno se dokazuje da za $I_v(A) = I_v(B) = 0$ mora da važi $I_v(A * B) = 1$.

Ako za $I_v(A) = 1$ i $I_v(B) = 0$ važi $I_v(A * B) = 1$ i ako za $I_v(A) = 0$ i $I_v(B) = 1$ važi $I_v(A * B) = 1$, onda je veznik $*$ jednak vezniku $\uparrow$. Ako za $I_v(A) = 1$ i $I_v(B) = 0$ važi $I_v(A * B) = 0$ i ako za $I_v(A) = 0$ i $I_v(B) = 1$ važi $I_v(A * B) = 0$, onda je veznik $*$ jednak vezniku $\downarrow$.

Ako bi za $I_v(A) = 1$ i $I_v(B) = 0$ važilo $I_v(A * B) = 1$ a za $I_v(A) = 0$ i $I_v(B) = 1$ važilo $I_v(A * B) = 0$, onda bi važilo $A * B \equiv \neg B$. Ako bi za $I_v(A) = 1$ i $I_v(B) = 0$ važilo $I_v(A * B) = 0$ a za $I_v(A) = 0$ i $I_v(B) = 1$ važilo $I_v(A*B) = 1$, onda bi važilo $A*B \equiv \neg A$. U oba slučaja, veznik $*$ bi bilo moguće definisati preko veznika $\neg$. Međutim, skup veznika $\{\neg\}$ nije potpun, jer ne postoji tautologija koja sadrži samo veznik $\neg$ (a tautologije postoje, npr. formula $p \vee \neg p$ je tautologija). □

Teorema 2.11 je specijalni slučaj tvrđenja za veznike proizvoljne arnosti [44].

Zadaci

Zadatak 17 *Dokazati da* $\{\Rightarrow, \vee\}$ *i* $\{\neg, \Leftrightarrow\}$ *nisu potpuni skupovi veznika.*

Zadatak 18 $\surd$ *Svaki stanovnik jedne države ili uvek laže ili uvek govori istinu i na svako pitanje odgovara uvek samo sa* da *ili* ne. *Neki turista dolazi na raskrsnicu u toj državi i zna da samo jedan od dva puta vodi do glavnog grada. Ne postoji znak koji pokazuje koji je to put, ali postoji meštanin R koji stoji na raskrsnici. Koje* da-ili-ne *pitanje treba turista da postavi da bi odredio kojim putem da krene?*

Zadatak 19 *Navesti primer iskazne formule koja uključuje tri iskazna slova i koja ima tačno pet zadovoljavajućih valuacija (razmatraju se samo valuacije nad iskaznim slovima koja se pojavljuju u formuli).*

Zadatak 20 *U računarstvu se često koristi logički veznik* $\underline{\vee}$ (isključivo ili, isključiva disjunkcija, ekskluzivno ili, ekskluzivna disjunkcija*) koji može biti definisan na sledeći način:* $A \underline{\vee} B$ *je jednako (tj. to je kraći zapis za)* $\neg(A \Leftrightarrow B)$ *ili* $(A \wedge \neg B) \vee (\neg A \wedge B)$. *Ispitati da li je skup* $\{\wedge, \underline{\vee}\}$ *potpun skup veznika.*

2.2.5 Normalne forme

Definicija 2.11 *Iskazna formula je u* konjunktivnoj normalnoj formi *(*KNF*) ako je oblika*

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n$$

pri čemu je svaka od formula A_i ($1 \leq i \leq n$) klauza (tj. disjunkcija literala).

Definicija 2.12 *Iskazna formula je u* disjunktivnoj normalnoj formi *(DNF) ako je oblika*

$$A_1 \vee A_2 \vee \ldots \vee A_n$$

pri čemu je svaka od formula A_i *(*$1 \leq i \leq n$*) konjunkcija literala.*

Ako je iskazna formula A logički ekvivalentna iskaznoj formuli B i iskazna formula B je u konjunktivnoj (disjunktivnoj) normalnoj formi, onda kažemo da je formula B konjunktivna (disjunktivna) normalna forma formule A.

Iz teoreme 2.10 sledi da za svaku iskaznu formulu postoji njena disjunktivna normalna forma. Dodatno, korišćenjem pogodnih ekvivalencija, svaka iskazna formula može biti transformisana u svoju konjunktivnu (disjunktivnu) normalnu formu. Naglasimo da jedna iskazna formula može da ima više konjunktivnih (disjunktivnih) normalnih formi (na primer, i formula $(p \vee r) \wedge (q \vee r) \wedge (p \vee s) \wedge (q \vee s)$ i formula $(s \vee q) \wedge (p \vee r) \wedge (q \vee r) \wedge (p \vee s) \wedge (p \vee \neg p)$ su konjunktivne normalne forme formule $(p \wedge q) \vee (r \wedge s)$). Slično, jedna formula koja je u konjunktivnoj normalnoj formi može biti konjunktivna normalna forma za više iskaznih formula.

Transformisanje iskazne formule u konjunktivnu normalnu formu može biti opisano algoritmom prikazanim na slici 2.1. Kada govorimo o „primeni neke logičke ekvivalencije“ mislimo na korišćenje logičke ekvivalencije na osnovu teoreme o zameni (teorema 2.9).

Algoritam: KNF

Ulaz: Iskazna formula F
Izlaz: Konjunktivna normalna forma formule F

1. Eliminisati veznik $\Leftrightarrow$ koristeći logičku ekvivalenciju
   $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$.
2. Eliminisati veznik $\Rightarrow$ koristeći logičku ekvivalenciju
   $A \Rightarrow B \equiv \neg A \vee B$.
3. Dok god je to moguće, primenjivati logičke ekvivalencije
   $\neg(A \wedge B) \equiv \neg A \vee \neg B$ i $\neg(A \vee B) \equiv \neg A \wedge \neg B$.
4. Eliminisati višestruke veznike $\neg$ koristeći logičku ekvivalenciju
   $\neg\neg A \equiv A$.
5. Dok god je to moguće, primenjivati logičke ekvivalencije
   $(A \vee (B \wedge C)) \equiv ((A \vee B) \wedge (A \vee C))$ i
   $((B \wedge C) \vee A) \equiv ((B \vee A) \wedge (C \vee A))$.

Slika 2.1: Algoritam KNF

Teorema 2.12 (Korektnost algoritma KNF) *Algoritam KNF se zaustavlja i zadovoljava sledeće svojstvo: ako je F ulazna formula, onda je izlazna formula F' u konjunktivnoj normalnoj formi i logički je ekvivalentna sa F.*

Dokaz: Algoritam se zaustavlja jer se zaustavlja svaki od njegovih koraka. Dokažimo da u svakom koraku navedene logičke ekvivalencije mogu biti primenjene samo konačan broj puta.

1. Nakon svake primene date logičke ekvivalencije za jedan se smanjuje broj pojavljivanja veznika $\Leftrightarrow$ u tekućoj formuli. Kako je broj pojavljivanja ovog simbola u početnoj formuli (formuli F) konačan, sledi da je broj primena date logičke ekvivalencije konačan i da nakon ovog koraka tekuća formula nema više pojavljivanja simbola $\Leftrightarrow$.
2. Analogno kao za prethodni korak.
3. Nakon svake primene neke od datih logičkih ekvivalencija za jedan se smanjuje broj pojavljivanja veznika $\wedge$ i $\vee$ u potformulama čiji je dominantni veznik $\neg$. Kako je broj takvih pojavljivanja[2] ovih simbola u početnoj formuli (izlaznoj formuli za prethodni korak) konačan (a uvek nenegativan), sledi da je broj primena datih logičkih ekvivalencija konačan i da nakon ovog koraka tekuća formula nema više pojavljivanja veznika $\wedge$ i $\vee$ u potformulama čiji je dominantni veznik $\neg$. Dakle, nakon ovog koraka, tekuća formula nema više pojavljivanja simbola $\Leftrightarrow$, $\Rightarrow$, niti simbola $\wedge$ i $\vee$ kojima dominira simbol $\neg$.
4. Nakon svake primene date logičke ekvivalencije za dva se smanjuje broj pojavljivanja veznika $\neg$ u tekućoj formuli. Kako je broj pojavljivanja ovog simbola u početnoj formuli (izlaznoj formuli za prethodni korak) konačan (a uvek nenegativan), sledi da je broj primena date logičke ekvivalencije konačan i da nakon ovog koraka tekuća formula nema višestrukih pojavljivanja simbola $\neg$. Dakle, nakon ovog koraka veznik $\neg$ pojavljuje se u tekućoj formuli samo u potformulama oblika $\neg A$, gde je A atomička formula.
5. Nakon svake primene neke od datih logičkih ekvivalencija za jedan se smanjuje broj pojavljivanja veznika $\wedge$ u potformulama čiji je dominantni veznik $\vee$. Kako je broj takvih pojavljivanja ovih simbola u početnoj formuli (izlaznoj formuli za prethodni korak) konačan (a uvek nenegativan), sledi da je broj primena datih logičkih ekvivalencija konačan i da nakon ovog koraka tekuća formula nema više pojavljivanja veznika $\wedge$ u potformulama čiji je dominantni veznik $\vee$. Dakle, nakon ovog koraka, tekuća formula nema više pojavljivanja simbola $\Leftrightarrow$, $\Rightarrow$, nema simbola $\wedge$ i $\vee$ kojima dominira simbol $\neg$, niti

[2] Broj takvih pojavljivanja simbola $\wedge$ i $\vee$ u formuli može se precizno definisati, slično kao složenost formule.

simbola $\wedge$ kojima dominira simbol $\vee$, a simbol $\neg$ pojavljuje se u potformulama oblika $\neg A$, gde je A atomička formula, što znači da je izlazna formula algoritma u konjunkivnoj normalnoj formi.

Prethodnim je dokazano da se algoritam KNF zaustavlja i da je njegova izlazna formula F' u konjunktivnoj normalnoj formi. Formula F' je poslednja u nizu formula F_1, F_2, ..., F_n, dobijenih nizom primena logičkih ekvivalencija. Na osnovu teoreme o zameni (teorema 2.9), važi $F \equiv F_1$, $F_1 \equiv F_2$, ..., $F_n \equiv F'$, pa na osnovu tranzitivnosti relacije logičke ekvivalencije sledi da važi $F \equiv F'$, čime je dokazana korektnost algoritma KNF. □

Opisani postupak (kao i dokaz korektnosti) može se pogodno iskazati u terminima tzv. *sistema za prezapisivanje* [3]. U tom kontekstu, svaka logička ekvivalencija koja se koristi u algoritmu KNF određuje jedno pravilo prezapisivanja. U cilju dokazivanja zaustavljanja postupka transformisanja formule u konjunktivnu normalnu formu definiše se preslikavanje τ iz skupa iskaznih formula u skup prirodnih brojeva [15]:

$$\begin{aligned} \tau(A) &= 2 \text{ (gde je } A \text{ atomička formula)} \\ \tau(\neg A) &= 2^{\tau(A)} \\ \tau(A \wedge B) &= \tau(A) \cdot \tau(B) \\ \tau(A \vee B) &= \tau(A) + \tau(B) + 1 \end{aligned}$$

Može se jednostavno dokazati da je vrednost $\tau(A')$ uvek manja od $\tau(A)$ ako je formula A' dobijena primenom nekog pravila prezapisivanja na formulu A (jer, na primer, važi da je $\tau(\neg A \wedge \neg B) = 2^{\tau(A)+\tau(B)}$ manje od $\tau(\neg(A \vee B)) = 2^{\tau(A)+\tau(B)+1}$). Odatle sledi da je skup pravila prezapisivanja zaustavljajući i da se postupak transformisanja proizvoljne formule u konjuktivnu normalnu formu zaustavlja za proizvoljnu ulaznu formulu A (jer ne postoji beskonačan strogo opadajući niz prirodnih brojeva čiji je prvi element $\tau(A)$).

Naglasimo da transformisanje formule u njenu konjunktivnu normalnu formu može da dâ formulu čija je dužina eksponencijalna u funkciji dužine polazne formule. Na primer, transformisanjem formule

$$(A_1 \wedge B_1) \vee (A_2 \wedge B_2) \vee \ldots \vee (A_n \wedge B_n)$$

(koja ima n disjunkata) u njenu konjunktivnu normalnu formu, dobija se formula koja ima 2^n konjunkta.

Transformisanje formule u disjunktivnu normalnu formu opisuje se algoritmom analognim algoritmu KNF.

Definicija 2.13 Kanonska disjunktivna normalna forma *formule A koja nije kontradikcija i koja sadrži iskazna slova p_1, p_2, ..., p_n je formula oblika*

$$\bigvee_{I_v(A)=1} (p_1^v \wedge p_2^v \wedge \ldots \wedge p_n^v)$$

pri čemu je $p_i^v = \begin{cases} p_i, & \text{ako je } v(p_i) = 1 \\ \neg p_i, & \text{inače.} \end{cases}$

Formula koja je kontradikcija nema kanonsku disjunktivnu normalnu formu. Može se dokazati da je svaka formula logički ekvivalentna svojoj kanonskoj disjunktivnoj normalnoj formi.

Definicija 2.14 Kanonska konjunktivna normalna forma *formule A koja nije tautologija i koja sadrži iskazna slova $p_1, p_2, \ldots, p_n$ je formula oblika*

$$\bigwedge_{I_v(A)=0} (p_1^{\hat{v}} \vee p_2^{\hat{v}} \vee \ldots \vee p_n^{\hat{v}})$$

pri čemu je $p_i^{\hat{v}} = \begin{cases} \neg p_i, & \text{ako je } v(p_i) = 1 \\ p_i, & \text{inače.} \end{cases}$

Formula koja je tautologija nema kanonsku konjunktivnu normalnu formu. Može se dokazati da je svaka formula logički ekvivalentna svojoj kanonskoj konjunktivnoj normalnoj formi.

Primer 2.9 *Iskazna formula A nad iskaznim slovima p, q, r ima istinitosne vrednosti prikazane u narednoj tabeli:*

p	q	r	A
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Kanonska disjunktivna normalna forma formule A je: $(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$.

Kanonska konjunktivna normalna forma formule A je: $(p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$.

Zadaci

Zadatak 21 *Odrediti konjunktivnu normalnu formu i disjunktivnu normalnu formu za formule:*

(a) $(A \Rightarrow B) \vee (\neg A \wedge C)$
(b) $A \Leftrightarrow (B \wedge \neg A)$
(c) $((A \Rightarrow B) \Rightarrow (C \Rightarrow \neg A)) \Rightarrow (\neg B \Rightarrow \neg C)$
(d) $((((A \Rightarrow B) \Rightarrow \neg A) \Rightarrow \neg B) \Rightarrow \neg C) \Rightarrow C$
(e) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow \neg C) \Rightarrow (A \Rightarrow \neg B))$

Zadatak 22 *Odrediti kanonsku disjunktivnu normalnu formu formule* $(\neg A \Rightarrow \neg B) \Rightarrow ((B \wedge C) \Rightarrow (A \wedge C))$.

Zadatak 23 *Odrediti kanonsku konjunktivnu normalnu formu formule* $(C \Rightarrow A) \Rightarrow (\neg(B \vee C) \Rightarrow A)$.

Zadatak 24 *Konstruisati formulu nad tri iskazne promenljive takvu da je ona tačna u nekoj valuaciji, ako i samo ako su u toj valuaciji tačne tačno dve promenljive.*

Zadatak 25 $\surd$ *(Teorema o interpolaciji) Neka su* A *i* B *iskazne formule takve da* A *nije kontradikcija i* B *nije tautologija i neka je* $A \Rightarrow B$ *tautologija.*

(a) Dokazati da A *i* B *imaju bar jedno zajedničko iskazno slovo.*

(b) Dokazati da postoji iskazna formula C *takva da* C *ima samo iskazna slova koja su zajednička za* A *i* B *i za koju važi da su* $A \Rightarrow C$ *i* $C \Rightarrow B$ *tautologije.*

2.2.6 Dejvis–Patnam–Logman–Lovelandova procedura

Dejvis–Patnam–Logman–Lovelandova procedura[3] (DPLL procedura) vrši ispitivanje zadovoljivosti iskaznih formula [13]. Ona se primenjuje na iskazne formule u konjunktivnoj normalnoj formi (a za svaku iskaznu formulu postoji njena konjunktivna normalna forma). Ulazna formula je konjunkcija klauza. Pri tome (kako su konjunkcija i disjunkcija komutativne i asocijativne) nije bitan poredak tih klauza niti je u bilo kojoj od tih klauza bitan poredak literala; zato se ulazna formula može smatrati skupom (ili, preciznije, multiskupom[4]) klauza, od kojih se svaka može smatrati skupom (ili, preciznije, multiskupom) literala. Ipak, radi određenosti rada algoritma, smatraćemo da je skup (odnosno multiskup) klauza uređen.

U proceduri se podrazumevaju sledeće konvencije:

- prazan skup klauza (zvaćemo ga *praznom formulom*) je zadovoljiv;
- klauza koja ne sadrži nijedan literal (zvaćemo je *prazna klauza*) je nezadovoljiva; formula koja sadrži praznu klauzu je nezadovoljiva.

Dejvis–Patnam–Logman–Lovelandova procedura data je na slici 2.2.

Teorema 2.13 (Korektnost DPLL procedure) *Za svaku iskaznu formulu DPLL procedura se zaustavlja i vraća odgovor* DA *ako i samo ako je polazna formula zadovoljiva.*

[3] Na ovu proceduru se, zbog dve njene verzije, ponekad ukazuje kao na Dejvis–Patnamovu (DP) proceduru ili kao na Dejvis–Logman–Lovelandovu (DLL) proceduru.

[4] Multiskup je, neformalno, skup u kojem se elementi mogu pojavljivati više puta. Formalno, multiskup S je funkcija iz nekog domena D u skup nenegativnih celih brojeva. Kažemo da važi $x \in S$ ako važi $S(x) > 0$. Kažemo da je multiskup S konačan ako je skup $\{x \mid S(x) > 0\}$ konačan. Vrednost $S(x)$ nazivamo višestrukošću elementa x u multiskupu S i ona predstavlja broj pojavljivanja elementa x u multiskupu S. Ako su S i T multiskupovi onda se, na primer, multiskup $S \cup T$ definiše na sledeći način: $(S \cup T)(x) = S(x) + T(x)$ za svako x.

Algoritam: DPLL

Ulaz: Multiskup klauza D ($D = \{C_1, C_2, \ldots, C_n\}$)
Izlaz: *DA*, ako je multiskup D zadovoljiv;
NE, ako multiskup D nije zadovoljiv

1. Ako je D prazan, vrati *DA*.
2. Zameni sve literale $\neg\bot$ sa $\top$ i zameni sve literale $\neg\top$ sa $\bot$.
3. Obriši sve literale jednake $\bot$.
4. Ako D sadrži praznu klauzu, vrati *NE*.
5. Ako neka klauza C_i sadrži literal $\top$ ili sadrži i neki literal i njegovu negaciju, vrati vrednost koju vraća DPLL($D \setminus C_i$) (*tautology*).
6. Ako je neka klauza jedinična i jednaka nekom iskaznom slovu p, onda vrati vrednost koju vraća DPLL($D[p \mapsto \top]$); ako je neka klauza jedinična i jednaka $\neg p$, gde je p neko iskazno slovo, onda vrati vrednost koju vraća DPLL($D[p \mapsto \bot]$) (*unit propagation*).
7. Ako D sadrži literal p (gde je p neko iskazno slovo), a ne i literal $\neg p$, onda vrati vrednost koju vraća DPLL($D[p \mapsto \top]$); ako D sadrži literal $\neg p$ (gde je p neko iskazno slovo), a ne i literal p, onda vrati vrednost koju vraća DPLL($D[\neg p \mapsto \top]$) (*pure literal*).
8. Ako DPLL($D[p \mapsto \top]$) vraća *DA*, onda vrati *DA*; inače vrati vrednost koju vraća DPLL($D[p \mapsto \bot]$) (gde je p jedno od iskaznih slova koje se javljaju u D) (*split*).

Slika 2.2: DPLL procedura

Dokaz: Neka je N broj iskaznih slova, a L broj klauza u D. Može se dokazati da se procedura DPLL zaustavlja indukcijom po $N+L$. Ako je $N+L=0$, onda se procedura zaustavlja u koraku 1. Pretpostavimo da se procedura zaustavlja za vrednosti $N + L$ manje od k i dokažimo da se zaustavlja i za $N + L = k$. Pretpostavimo da za ulazne vrednosti važi $N + L = k$. Tada se procedura ili zaustavlja u koraku 1 ili se zaustavlja u koraku 4 (i za te slučaje je tvrđenje dokazano) ili stiže do koraka 5 (u koracima 2 i 3 zbir $N + L$ se ne menja). Ukoliko je izvršavanje procedure stiglo do koraka 5, ono se nastavlja izvršavanjem (tačno) jednog od koraka 5, 6, 7 ili 8. Ako su ispunjeni preduslovi koraka 5, onda se (rekurzivno) poziva procedura DPLL sa ulaznim parametrima za vrednost $N + (L - 1)$, a kako je $N + (L-1) < k$, na osnovu induktivne pretpostavke taj poziv se izvršava

u konačnom broju koraka, te se zaustavlja korak 5 i time, izvršavanje procedure. Ako su ispunjeni preduslovi koraka 6 ili 7, onda se (rekurzivno) poziva procedura DPLL sa ulaznim parametrima za vrednost $(N-1)+L$, a kako je $(N-1)+L < k$, na osnovu induktivne pretpostavke taj poziv se izvršava u konačnom broju koraka, te se zaustavlja tekući korak i, time, izvršavanje procedure. Konačno, u koraku 8 se (rekurzivno), najviše dva puta, poziva procedura DPLL sa ulaznim parametrima za vrednost $(N-1)+L$, a kako je $(N-1)+L < k$, na osnovu induktivne pretpostavke ti pozivi se izvršavaju u konačnom broju koraka, te se zaustavlja korak 8 i, time, izvršavanje procedure. Time je dokazano da se procedura DPLL uvek zaustavlja.

Potrebno je još dokazati da procedura vraća *DA* ako i samo ako ulazu odgovara zadovoljiva formula. Za to je potrebno i dovoljno dokazati korektnost svakog od koraka, što odgovara sledećim jednostavnim tvrđenjima:

1. Ako je D prazan onda je on zadovoljiv.
2. D je zadovoljiv ako i samo ako je zadovoljiv $D[\neg\bot \mapsto \top, \neg\top \mapsto \bot]$.
3. D je zadovoljiv ako i samo ako je zadovoljiv $D[A \vee \bot \vee B \mapsto A \vee B]$.
4. Ako D sadrži praznu klauzu onda je on nezadovoljiv.
5. Ako neka klauza C_i sadrži literal $\top$ ili sadrži i neki literal i njegovu negaciju, onda je D zadovoljiv ako i samo ako je zadovoljiv $D \setminus C_i$.
6. Ako je neka klauza jedinična i jednaka nekom iskaznom slovu p, onda je D zadovoljiv ako i samo ako je zadovoljiv $D[p \mapsto \top]$.
   Ako je neka klauza jedinična i jednaka $\neg p$, gde je p neko iskazno slovo, onda je D zadovoljiv ako i samo ako je zadovoljiv $D[p \mapsto \bot]$.
7. Ako D sadrži literal p (gde je p neko iskazno slovo), a ne i literal $\neg p$, onda je D zadovoljiv ako i samo ako je zadovoljiv $D[p \mapsto \top]$.
   Ako D sadrži literal $\neg p$ (gde je p neko iskazno slovo), a ne i literal p, onda je D zadovoljiv ako i samo ako je zadovoljiv $D[\neg p \mapsto \top]$.
8. D je zadovoljiv ako i samo ako je zadovoljiv jedan od (multi)skupova $D[p \mapsto \top]$, $D[p \mapsto \bot]$.

□

Dejvis–Patnam–Logman–Lovelandova procedura je u najgorem slučaju eksponencijalne složenosti $O(2^N)$, gde je N broj iskaznih slova u formuli, usled rekurzivne primene *split* pravila (više o složenosti izračunavanja videti u dodatku A). Iste (eksponencijalne) složenosti su i svi drugi do sada poznati algoritmi za ispitivanje zadovoljivosti. Ipak, svi ti algoritmi su znatno efikasniji od metode istinitosnih tablica.

Izbor iskaznog slova u pravilu *split* je veoma važan. Neke varijante ovog pravila su da se bira iskazno slovo sa najviše pojavljivanja u tekućoj formuli, da se bira neko od iskaznih slova iz najkraće klauze itd.

Formula je tautologija ako i samo ako njena negacija nije zadovoljiva, formula je kontradikcija ako i samo ako ona nije zadovoljiva i formula je poreciva ako i samo ako je njena negacija zadovoljiva. Primetimo da odatle sledi da DPLL proceduru možemo iskoristiti i za ispitavanje da li je data formula tautologija, poreciva ili kontradikcija.

Zadaci

Zadatak 26 *Primenom DPLL algoritma ispitati da li su sledeće formule zadovoljive:*

(a) $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r))$

(b) $\neg((p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r)))$

Zadatak 27 *Primenom DPLL algoritma ispitati da li je formula* $(p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r)$ *zadovoljiva, tautologija, poreciva, kontradikcija.*

2.2.7 Metod rezolucije

Metod rezolucije formulisao je Alan Robinson 1965. godine [61]. Tome su prethodili mnogobrojni rezultati koji su doveli do otkrića metoda. U ovom delu teksta opisaćemo metod rezolucije za iskaznu logiku.

Metod rezolucije primenjuje se na iskazne formule koje su u konjunktivnoj normalnoj formi. Zbog asocijativnosti i komutativnosti konjunkcije i disjunkcije, formulu koja je u konjunktivnoj normalnoj formi možemo smatrati multiskupom klauza, pri čemu svaku klauzu možemo smatrati multiskupom literala. Na osnovu logičkih ekvivalencija $A \wedge A \equiv A$ i $A \vee A \equiv A$, mogu se eliminisati višestruka pojavljivanja jedne klauze u formuli i višestruka pojavljivanja jednog literala u klauzi. Time formula kao multiskup klauza od kojih je svaka multiskup literala može da se zameni (logički ekvivalentnom) formulom koja je skup klauza od kojih je svaka skup literala. Metod rezolucije ispituje da li je zadat skup klauza zadovoljiv.

Klauza je zadovoljiva ako postoji valuacija u kojoj je bar jedan literal iz te klauze tačan. Klauza je pobijena valuacijom u kojoj su svi literali netačni. Prazna klauza, u oznaci $\square$, ne sadrži nijedan literal i nije zadovoljiva. Formula koja je skup klauza je zadovoljiva ako postoji valuacija u kojoj su sve klauze te formule tačne, a inače je nezadovoljiva.

Jednostavnosti radi, sve klauze koje sadrže logičke konstante $\top$ ili $\bot$ mogu biti eliminisane ili zamenjene tako da se ne promeni zadovoljivost polaznog skupa klauza. Klauza koja sadrži literal $\top$ je u svakoj valuaciji tačna, pa može biti eliminisana (jer ne utiče na zadovoljivost polaznog skupa klauza). Ako klauza C sadrži literal $\bot$, onda taj literal može biti obrisan, dajući novu klauzu C' (jer je u svakoj valuaciji klauza C tačna ako i samo ako je tačna klauza C'). Dakle, može se smatrati da je u svim klauzama svaki literal ili iskazno slovo ili negacija iskaznog slova. Ako je literal l jednak iskaznom slovu p, onda sa $\overline{l}$ označavamo literal $\neg p$; ako je literal l jednak negaciji iskaznog slova p

(tj. literalu $\neg p$), onda sa $\overline{l}$ označavamo literal p. Za literale l i $\overline{l}$ kažemo da su međusobno *komplementni*.

Ako su C' i C'' klauze, onda se *pravilom rezolucije* iz klauza $C' \vee l$ i $C'' \vee \overline{l}$ izvodi klauza $C' \vee C''$. Pravilo rezolucije može se prikazati u sledećem obliku:

$$\frac{C' \vee l \quad C'' \vee \overline{l}}{C' \vee C''}$$

Klauzu $C' \vee C''$ zovemo *rezolventom* klauza $C' \vee l$ i $C'' \vee \overline{l}$, a klauze $C' \vee l$ i $C'' \vee \overline{l}$ *roditeljima rezolvente*. Kažemo da klauze $C' \vee l$ i $C'' \vee \overline{l}$ *rezolviramo* pravilom rezolucije.

Pravilo rezolucije intuitivno može biti shvaćeno na sledeći način: klauza $C' \vee p$ logički je ekvivalentna formuli $\neg C' \Rightarrow p$, klauza $C'' \vee \neg p$ logički je ekvivalentna formuli $p \Rightarrow C''$, a formule $\neg C' \Rightarrow p$ i $p \Rightarrow C''$ imaju logičku posledicu $\neg C' \Rightarrow C''$ koja je logički ekvivalentna klauzi $C' \vee C''$.

Ako je dat skup klauza S, pravilom rezolucije se roditelji rezolvente *ne zamenjuju* rezolventom, već se rezolventa *dodaje* u skup S.

Metod rezolucije je postupak za ispitivanje zadovoljivosti skupa klauza koji se sastoji od uzastopnog primenjivanja pravila rezolucije. Neka je S početni skup, neka je $S_0 = S$ i neka je S_{i+1} rezultat primene pravila rezolucije na skup S_i. Postupak se zaustavlja na jedan od sledeća dva načina:

- ako u nekom koraku skup S_i sadrži praznu klauzu ($\Box$), onda zaustavi primenu procedure i vrati odgovor da je skup klauza S nezadovoljiv;
- ako ne postoji mogućnost da se primeni pravilo rezolucije tako da se skupovi S_i i S_{i+1} razlikuju, onda zaustavi primenu procedure i vrati odgovor da je skup klauza S zadovoljiv.

Niz klauza (polaznih i izvedenih) označavaćemo obično sa C_i ($i = 1, 2, \ldots$). Iza izvedene klauze zapisivaćemo oznake klauza iz kojih je ona izvedena, kao i redne brojeve literala nad kojim je primenjeno pravilo rezolucije. Literale u klauzama razdvajaćemo obično simbolom ',' (umesto simbolom '$\vee$').

Primer 2.10 *Metodom rezolucije se iz skupa* $\{\{\neg p, \neg q, r\}, \{\neg p, q\}, \{p\}, \{\neg r\}\}$ *može izvesti prazna klauza:*

C_1 :	$\neg p, \neg q, r$	
C_2 :	$\neg p, q$	
C_3 :	p	
C_4 :	$\neg r$	
C_5 :	$\neg p, r$	$(C_1, 2; C_2, 2)$
C_6 :	$\neg p$	$(C_4, 1; C_5, 2)$
C_7 :	$\Box$	$(C_3, 1; C_6, 1)$

Skup klauza $\{\{\neg p, \neg q, r\}, \{\neg p, q\}, \{p\}, \{\neg r\}\}$ *je, dakle, nezadovoljiv.*

Primer 2.11 *Metodom rezolucije se iz skupa* $\{\{\neg p, \neg q, r\}, \{\neg p, q\}, \{p\}\}$ *ne može izvesti prazna klauza. Ovaj skup klauza je, dakle, zadovoljiv.*

Teorema 2.14 (Zaustavljanje metoda rezolucije) *Metod rezolucije se zaustavlja.*

Dokaz: U svakom koraku metoda rezolucije tekućem skupu se dodaje nova klauza.

Klauze su skupovi literala, pa nije bitan poredak literala u njima, a višestruka pojavljivanja literala u klauzi nisu moguća. Nad skupom od n iskaznih slova ima $2n$ različitih literala (za svako iskazno slovo p postoje literali p i $\neg p$) i svaki od njih može da se pojavljuje ili ne pojavljuje u klauzi[5], te različitih klauza ima $2^{2n} = 4^n$.

Dakle, metod rezolucije se *zaustavlja* u konačno mnogo koraka, jer se iz literala iz skupa S može izvesti samo konačan broj (novih) klauza. (Taj broj međutim može biti eksponencijalno veliki (u funkciji broja literala u S) i primena procedure rezolucije može da se sastoji od veoma velikog broja koraka.) □

Teorema 2.15 (Saglasnost pravila rezolucije) *Neka je skup klauza S' dobijen od skupa klauza S primenom pravila rezolucije. Ako neka valuacija zadovoljava skup S, onda ona zadovoljava i skup S'.*

Dokaz: Pretpostavimo da valuacija v zadovoljava sve klauze iz skupa S. Dokažimo da ona zadovoljava i sve klauze iz skupa S'. Pretpostavimo da je pravilo rezolucije primenjeno na klauze C_a i C_b i da je njihova rezolventa klauza C_r. Jedina klauza koja pripada skupu S', a moguće ne pripada skupu S je klauza C_r. Dokažimo da valuacija v zadovoljava klauzu C_r. Pretpostavimo da klauza C_a sadrži literal l, a klauza C_b literal $\overline{l}$. Ako je literal l tačan u valuaciji v, onda je literal $\overline{l}$ netačan, pa u klauzi C_b mora da postoji neki literal (različit od $\overline{l}$) koji je tačan u valuaciji v. Taj literal je i element klauze C_r, pa je i ona zadovoljiva u valuaciji v. Ako je literal l netačan u valuaciji v, onda u klauzi C_a mora da postoji neki literal (različit od l) koji je tačan u valuaciji v. Taj literal je i element klauze C_r, pa je i ona zadovoljiva u valuaciji v. Dakle, svaka klauza iz skupa S' je tačna u valuaciji v, odakle sledi tvrđenje teoreme. □

Teorema 2.16 (Saglasnost metoda rezolucije) *Ako se iz skupa klauza S može izvesti prazna klauza, onda je S nezadovoljiv skup klauza.*

[5] Ukoliko bi bilo uvedeno ograničenje da klauza ne može da sadrži i neko iskazno slovo i njegovu negaciju (takva klauza je u svakoj valuaciji tačna), onda bi nad n iskaznih slova bilo 3^n različitih klauza (jer svako iskazno slovo p može da se ne pojavljuje u klauzi, da se pojavljuje u vidu literala p ili da se pojavljuje u okviru literala $\neg p$).

Dokaz: Na osnovu teoreme 2.15 (i na osnovu jednostavnog induktivnog argumenta), ako je skup klauza S zadovoljiv, zadovoljiv je i svaki skup klauza S', dobijen u nekoj iteraciji metoda. Obratno, skup klauza S je nezadovoljiv ako je nezadovoljiv skup S', dobijen u nekoj iteraciji metoda. Dakle, ako metod rezolucije u nekom koraku doda praznu klauzu u tekući skup klauza, sledi da je skup S nezadovoljiv, što je i trebalo dokazati. □

Teorema o saglasnosti rezolucije tvrdi da iz zadovoljivog skupa ne može biti izvedena prazna klauza. Pokazaćemo u nastavku da iz svakog nezadovoljivog skupa klauza može biti izvedena prazna klauza. Razmatraćemo stablo sa mogućim valuacijama fiksnog skupa iskaznih slova $\{p_1, p_2, \ldots, p_m\}$. Zato najpre navodimo definiciju stabla.

Definicija 2.15 Neuređeno stablo $\mathcal{T}$ *je par* $(S, \prec)$ *sa sledećim svojstvima:*

- S *je skup čije elemente zovemo* čvorovima neuređenog stabla*;*
- $\prec$ *je binarna relacija nad* S*,* $x \prec y$ *čitamo* čvor x je prethodnik (roditelj, direktni predak) čvora y *ili* čvor y je sledbenik (dete, direktni potomak) čvora x*; ova relacija zadovoljava sledeće uslove:*
  - *postoji jedinstven čvor koji nema prethodnika, taj čvor zovemo* koren *stabla;*
  - *svaki čvor različit od korena ima tačno jednog prethodnika;*
  - *ne postoji niz čvorova* $x_1, x_2, \ldots, x_n$ *takav da važi* $x_1 \prec x_2 \prec \ldots \prec x_n \prec x_1$.

Ako za niz čvorova $x_1, x_2, \ldots, x_n$ *važi* $x_1 \prec x_2 \prec \ldots \prec x_{n-1} \prec x_n$*, onda kažemo da je čvor* x_1 predak *čvora* x_n *i da je čvor* x_n potomak *čvora* x_1.

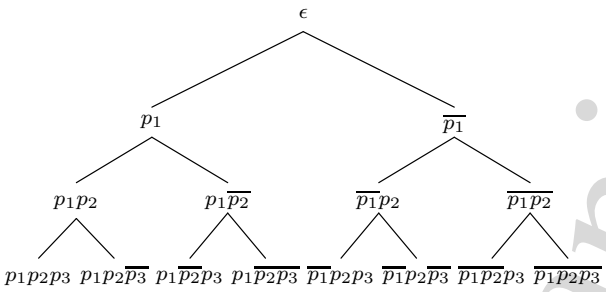
List stabla *je čvor koji nema sledbenika.* Staza stabla (grana stabla) *je niz čvorova* $x_1, x_2, \ldots, x_n$*, pri čemu je* x_1 *koren stabla i čvor* x_1 *je prethodnik čvora* x_2*, čvor* x_2 *je prethodnik čvora* x_3*, . . .,* x_{n-1} *je prethodnik čvora* x_n*.* Maksimalna staza (maksimalna grana) *je niz čvorova* $x_1, x_2, \ldots, x_n$*, pri čemu je* x_1 *koren stabla,* x_n *je list stabla i čvor* x_1 *je prethodnik čvora* x_2*, čvor* x_2 *je prethodnik čvora* x_3*, . . .,* x_{n-1} *je prethodnik čvora* x_n*.*

Ako je x_1 *koren stabla i ako postoji niz čvorova* $x_1, x_2, \ldots, x_k$ *takav da važi* $x_1 \prec x_2 \prec \ldots \prec x_{k-1} \prec x_k$*, onda kažemo da je* visina *čvora* x_k *jednaka* k*.*

Ako čvor stabla ima (samo) direktne potomke $x_1, x_2, \ldots, x_k$ *(*$k \geq 0$*), onda kažemo da je* stepen *tog čvora jednak* k*.*

Definicija 2.16 *Za stablo kažemo da je* binarno *ako svaki čvor ima najviše dva sledbenika. Za stablo kažemo da je* potpuno binarno *ako postoji vrednost* k *takva da svaki čvor visine manje ili jednake* k *ima po tačno dva sledbenika i nijedan čvor visine* $k + 1$ *nema nijednog sledbenika.*

Definicija 2.17 Uređeno stablo *je neuređeno stablo za čiji je svaki čvor skup njegovih sledbenika uređen.*



Slika 2.3: Stablo valuacija za tri iskazna slova

Stablo valuacija je uređeno potpuno binarno stablo visine m, čijem je svakom čvoru pridruženo dodeljivanje vrednosti 0 ili 1 iskaznim slovima iz zadatog skupa i dodeljivanje za svaki čvor (sem listova) je u njegovim direktnim potomcima prošireno dodeljivanjem vrednosti 0 i 1 još jednom iskaznom slovu. U korenu stabla je prazna dodela (označena sa ϵ) koja ne pridružuje vrednost nijednom iskaznom slovu. Čvor u stablu valuacija odgovara parcijalnoj dodeli vrednosti 0 i 1 iskaznim slovima iz nekog skupa. Parcijalne dodele mogu biti dovoljne za utvrđivanje istinitosne vrednosti neke formule. Može se govoriti o parcijalnim dodelama koje *proširuju* druge dodele. Parcijalna dodela koja odgovara nekom čvoru stabla valuacije je proširenje svake dodele koje odgovara prethodnicima tog čvora. Stablo valuacija ima 2^m listova, po jedan za svaku od mogućih valuacija. Parcijalne valuacije zapisujemo kratko kao niske znakova iz skupa znakova od p_1 do p_m i od $\overline{p_1}$ do $\overline{p_m}$. Sa p označavamo da valuacija iskaznom slovu p dodeljuje vrednost 1, a sa $\overline{p}$ da valuacija iskaznom slovu p dodeljuje vrednost 0. Slika 2.3 ilustruje stablo valuacija za tri iskazna slova.

Neka je S skup klauza i neka je S_k poslednji skup klauza dobijen metodom rezolucije. Klauza C *pokriva* čvor n u stablu valuacija ako ona zadovoljava sledeće uslove:

- klauza C je element skupa S_k;
- iskazna slova koja se pojavljuju u C su među slovima kojima su dodeljene vrednosti u čvoru n;
- klauza C je netačna u valuaciji koja odgovara čvoru n.

Na osnovu drugog i trećeg uslova sledi da je klauza C koja pokriva čvor n netačna i u svakoj valuaciji koja proširuje valuaciju koja odgovara čvoru n (tj. netačna i u svakoj valuaciji koja odgovara nekom potomku čvora n). Neki čvorovi mogu biti pokriveni od strane više klauza, dok neki ne moraju biti pokriveni. Prazna klauza je jedina klauza koja može pokriti koren stabla valuacije. Dodatno, prazna klauza može pokriti bilo koji čvor stabla valuacije.

Na primer, klauza $p_1 \vee p_2$ pokriva čvor $\overline{p_1 p_2} p_3$, ali i čvor $\overline{p_1 p_2}$.

Lema 2.1 *Ako su, za skup klauza dobijen metodom rezolucije iz skupa klauza S, oba deteta čvora stabla valuacija pokrivena, onda je i taj čvor pokriven.*

Dokaz: Pretpostavimo da je n čvor čija su oba deteta pokrivena i neka je v valuacija koja mu je pridružena. Neka su čvorovi n_1 i n_2 dva deteta čvora n, neka su im pridružene valuacije vp i $v\overline{p}$ i neka su C_1 i C_2 klauze koje, redom, pokrivaju ta dva čvora. Ako se iskazno slovo p ne pojavljuje u C_1, onda C_1 pokriva čvor n. Slično, ako se iskazno slovo p ne pojavljuje u C_2, onda C_2 pokriva čvor n. Ako se iskazno slovo p pojavljuje i u C_1 i u C_2, onda C_1 sadrži literal $\neg p$, a klauza C_2 literal p. Zaista, čvoru n_1 odgovara valuacija koja dodeljuje iskaznom slovu p vrednost 1, pa literal p ne može da se pojavljuje u C_1 (jer bi klauza C_1 tada bila tačna u valuaciji koja odgovara čvoru n_1). Analogno, klauza C_2 sadrži literal p. Na klauze C_1 i C_2 se, dakle, može primeniti pravilo rezolucije (po iskaznom slovu p). Neka je C_r rezolventa ove dve klauze (po iskaznom slovu p).

Ukoliko je iz skupa S izvedena prazna klauza, onda je ona klauza koja pokriva čvor n. Dokažimo da, ako prazna klauza nije izvedena, onda klauza C_r pokriva čvor n. Potrebno je dokazati tri svojstva klauze C_r.

- Ako, kao što je pretpostavljeno, prazna klauza nije izvedena iz S, onda skup S_k sadrži sve moguće rezolvente izvedene iz skupa S, pa je i klauza C_r element skupa S_k.
- Iskazna slova koja se pojavljuju u klauzi C_r su slova koja se pojavljuju u klauzi C_1 ili klauzi C_2. Za svako slovo koje se pojavljuje u ovim dvema klauzama važi ili da mu je dodeljena vrednost u čvoru n ili da je ono upravo iskazno slovo p. Dovoljno je, dakle, pokazati da iskazno slovo p ne pripada klauzi C_r. Literal p može da pripada klauzi C_r samo ako pripada i klauzi C_1. Međutim, ako bi literal p pripadao klauzi C_1, ta klauza bi sadržala literale p i $\neg p$, pa bi bila tačna u svakoj valuaciji, što je u suprotnosti sa činjenicom da je klauza C_1 netačna u valuaciji vp. Dakle, literal p ne pripada klauzi C_1 i, analogno, literal $\neg p$ ne pripada klauzi C_2. Odatle sledi da se iskazno slovo p ne pojavljuje u klauzi C_r, pa su sva slova koja se pojavljuju u C_r među slovima kojima su dodeljene vrednosti u čvoru n.
- Klauza C_1 pokriva čvor n_1, pa svi njeni literali imaju vrednost 0 u valuaciji vp. Klauza C_1, kao što je pokazano, ne sadrži literal p, pa je svaki literal iz skupa $C_1 \setminus \{\neg p\}$ netačan u valuaciji v. Analogno, svaki literal iz skupa $C_2 \setminus \{p\}$ je netačan u valuaciji v. Dakle, svaki literal klauze C_r (koja je unija skupova $C_1 \setminus \{\neg p\}$ i $C_2 \setminus \{p\}$) je netačan u valuaciji v.

□

Teorema 2.17 (Potpunost metoda rezolucije) *Ako je S nezadovoljiv skup klauza, onda se iz njega može izvesti prazna klauza.*

Dokaz: Neka je S_k poslednji skup dobijen metodom rezolucije od nezadovoljivog skupa S. Neka je $\mathcal{T}$ stablo valuacija za iskazna slova iz skupa S. Kako je skup S nezadovoljiv, on je netačan u svakoj valuaciji, tj. u svakoj valuaciji v bar jedna klauza iz S je netačna, te ona pokriva list stabla $\mathcal{T}$ koji odgovara valuaciji v. Dakle, svaki list stabla $\mathcal{T}$ je pokriven nekom klauzom iz skupa S. Primenom leme 2.1 i na osnovu jednostavnog induktivnog argumenta sledi da su svi čvorovi stabla $\mathcal{T}$ pokriveni elementima skupa S_k. Specijalno, i koren stabla $\mathcal{T}$ mora biti pokriven, a prazna klauza je jedina klauza koja može da pokrije koren. Dakle, prazna klauza je izvedena rezolucijom iz skupa S, što je i trebalo dokazati. □

Metod rezolucije se uvek zaustavlja (teorema 2.14), pa na osnovu dokaza prethodne teoreme sledi da se iz svakog nezadovoljivog skupa klauza nužno mora izvesti prazna klauza bez obzira na izbor klauza za rezolviranje u pojedinim koracima. Zbog toga bi u prethodnoj teoremi umesto reči *može* mogla da stoji i reč *mora*. Dodatno, iz toga sledi i da ukoliko za neki skup klauza metod staje bez izvođenja prazne klauze, onda je taj skup zadovoljiv.

Na osnovu prethodnih teorema sledi naredno tvrđenje.

Teorema 2.18 (Teorema o metodu rezolucije) *Metod rezolucije se zaustavlja za svaku iskaznu formulu i u završnom skupu klauza postoji prazna klauza ako i samo ako je polazna formula nezadovoljiva.*

Metod rezolucije može biti modifikovan tako da bude efikasniji. Modifikacije metoda mogu biti zasnovane na sledećim činjenicama:

- ako je klauza C tautologija, onda je skup S zadovoljiv ako i samo ako je skup $S \setminus \{C\}$ zadovoljiv;
- ako skup S sadrži jediničnu klauzu $\{l\}$, onda je skup S zadovoljiv ako i samo ako je zadovoljiv skup dobijen od S brisanjem svih klauza koje sadrže literal l i, zatim, brisanjem svih pojavljivanja literala $\overline{l}$;
- ako se u skupu klauza S pojavljuje literal l, a ne i literal $\overline{l}$, onda je skup S zadovoljiv ako i samo ako je skup T zadovoljiv, gde je skup T skup svih klauza iz S koje ne sadrže l;
- ako skup S sadrži klauze C_0 i C_1 i ako je klauza C_0 podskup klauze C_1, onda je skup S zadovoljiv ako i samo ako je zadovoljiv skup $S \setminus \{C_1\}$ (pravilo *subsumption*).

Primetimo da su navedene optimizacije slične koracima DPLL procedure. Za efikasnu primenu metoda rezolucije veoma je, u svakom koraku, bitan i izbor para klauza nad kojima se primenjuje pravilo rezolucije.

U svom osnovnom obliku, metod rezolucije proverava da li je dati skup klauza (ne)zadovoljiv. Međutim, metod rezolucije može se koristiti i za ispitivanje valjanosti. Naime, ako je potrebno ispitati da li je formula A valjana, dovoljno je metodom rezolucije utvrditi da li je formula $\neg A$ nezadovoljiva (pri čemu je potrebno najpre formulu $\neg A$ transformisati u konjuktivnu normalnu formu). Ovaj vid dokazivanja da je formula A valjana zovemo *dokazivanje pobijanjem*. Za metod rezolucije primenjen na ovaj način, saglasnost govori da nije moguće rezolucijom pogrešno utvrditi (pobijanjem) da je neka formula valjana, a potpunost govori da je za svaku valjanu formulu metodom rezolucije moguće dokazati (pobijanjem) da je valjana.

Metodom rezolucije može se ispitati i da li važi $A_1, A_2, \ldots, A_n \models B$. Ovo tvrđenje je tačno ako i samo ako je formula $A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B$ valjana (teorema 2.4). Formula $A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B$ je valjana ako i samo ako je formula $\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B)$ nezadovoljiva, tj. ako i samo ako je formula $A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge \neg B$ nezadovoljiva. Ukoliko su formule A_i u konjunktivnoj normalnoj formi, da bi na navedenu formulu bio primenjen metod rezolucije, dovoljno je transformisati formulu $\neg B$ u konjunktivnu normalnu formu.

Primer 2.12 *Važi*

$$(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q) \wedge p \models r$$

ako i samo ako je skup klauza $\{\{\neg p, \neg q, r\}, \{\neg p, q\}, \{p\}, \{\neg r\}\}$ *nezadovoljiv. U primeru 2.10 je pokazano da je taj skup klauza nezadovoljiv.*

Zadaci

Zadatak 28 *Dati su skup P od n ($n \geq 1$) iskaznih slova, skup $\mathcal{C}$ svih klauza nad P i dva podskupa, S_1 i S_2, skupa $\mathcal{C}$.*

(a) Koliko elemenata ima skup $\mathcal{C}$?

(b) Da li je skup $\mathcal{C}$ zadovoljiv?

(c) Ako su skupovi S_1 i S_2 zadovoljivi, da li je i skup $S_1 \cup S_2$ zadovoljiv?

(d) Ako su skupovi S_1 i S_2 zadovoljivi, da li je i skup $S_1 \cap S_2$ zadovoljiv?

(e) Ako je skup S_1 zadovoljiv, da li skup $\mathcal{C} \setminus S_1$ može da bude zadovoljiv?

(f) Ako je skup S_1 zadovoljiv, da li skup $\mathcal{C} \setminus S_1$ mora da bude zadovoljiv?

Zadatak 29 *Dati su skup P od n ($n \geq 1$) iskaznih slova, skup $\mathcal{C}$ svih klauza nad P i dva podskupa, S_1 i S_2, skupa $\mathcal{C}$.*

(a) Da li je skup $\mathcal{C}$ kontradiktoran?

(b) Ako su skupovi S_1 i S_2 kontradiktorni, da li skup $S_1 \cup S_2$ može da bude kontradiktoran?

(c) Ako su skupovi S_1 i S_2 kontradiktorni, da li skup $S_1 \cup S_2$ mora da bude kontradiktoran?

(d) Ako su skupovi S_1 i S_2 kontradiktorni, da li skup $S_1 \cap S_2$ može da bude kontradiktoran?

(e) Ako su skupovi S_1 i S_2 kontradiktorni, da li skup $S_1 \cap S_2$ mora da bude kontradiktoran?

Zadatak 30 *Dokazati metodom rezolucije da su naredne formule tautologije:*
(a) $q \Rightarrow (p \Rightarrow q)$
(b) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
(c) $((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow (q \wedge r))$
(d) $(((p \Rightarrow r) \wedge (q \Rightarrow r)) \wedge (p \vee q)) \Rightarrow r$
(e) $\neg(p \wedge q) \Rightarrow (\neg p \vee \neg q)$
(f) $\neg(p \vee q) \Rightarrow (\neg p \wedge \neg q)$
(g) $(\neg p \vee \neg q) \Rightarrow \neg(p \wedge q)$
(h) $(p \vee (q \wedge r)) \Rightarrow ((p \vee q) \wedge (p \vee r))$

2.2.8 Metod tabloa

Metod semantičkih tabloa prvi je opisao Evert Bet 1955. godine, a dalje ga je razvio Rejmond Smaljan 1971. godine. Metod se često naziva i *metodom analitičkih tabloa*. (Metodi koji kreću od formule koju treba dokazati, transformišu je i pojednostavljuju u nekom smislu dok ne bude ispunjen neki kriterijum za zaustavljanje, obično se nazivaju *analitičkim* metodama; s druge strane, *sintetički* metodi iz aksioma izvode formulu koju treba dokazati.)

Metod tabloa koristi se za pobijanje iskazne formule, tj. za utvrđivanje njene nezadovoljivosti. Naravno, metod se može koristiti i za utvrđivanje valjanosti formule F (tako što bi bilo pokazano da je $\neg F$ nezadovoljiva formula).

Metod tabloa zasniva se na sledećem jednostavnom tvrđenju — u bilo kojoj (fiksnoj) valuaciji važi:

(1) (a) ako je formula $\neg A$ tačna, onda je A netačna;
(b) ako je formula $\neg A$ netačna, onda je A tačna;

(2) (a) ako je formula $A \wedge B$ tačna, onda su A i B tačne;
(b) ako je formula $A \wedge B$ netačna, onda je netačna A ili je netačna B;

(3) (a) ako je formula $A \vee B$ tačna, onda je tačna formula A ili je tačna formula B;
(b) ako je formula $A \vee B$ netačna, onda su A i B netačne;

(4) (a) ako je formula $A \Rightarrow B$ tačna, onda je ili A netačna ili B tačna;
(b) ako je formula $A \Rightarrow B$ netačna, onda je A tačna i B netačna.

Slična pravila mogu biti formulisana i za druge logičke veznike ($\Leftrightarrow$, $\downarrow$, $\uparrow$, $\veebar$).

Za bilo koju fiksnu valuaciju, uvodimo pojam *označene formule*. Ako je A iskazna formula, onda su TA i FA označene formule; svaka označena formula je oblika TA ili FA, gde je A iskazna formula. U datoj valuaciji, označena formula TA je tačna ako je formula A tačna, a netačna inače. U datoj valuaciji, označena formula FA je tačna ako je formula A netačna, a netačna inače.

Dakle, vrednost označene formule TA jednaka je vrednosti formule A, a vrednost označene formule FA jednaka je vrednosti formule $\neg A$. Neformalno, TA čitamo „A je tačna“, a FA čitamo „A je netačna“.

Primetimo da postoje dve grupe formula, odnosno dve grupe odgovarajućih pravila: (A) ona koja daju direktne posledice (takva su pravila (1a), (1b), (2a), (3b), (4b)); (B) ona koja vode do grananja (takva su pravila (2b), (3a), (4a)):

Pravila tipa (A):

$$\frac{T\neg A}{FA} \qquad \frac{F\neg A}{TA}$$

$$\frac{T(A \wedge B)}{\begin{array}{l} TA \\ TB \end{array}} \qquad \frac{F(A \vee B)}{\begin{array}{l} FA \\ FB \end{array}}$$

$$\frac{F(A \Rightarrow B)}{\begin{array}{l} TA \\ FB \end{array}}$$

Pravila tipa (B):

$$\frac{F(A \wedge B)}{FA \mid FB} \qquad \frac{T(A \vee B)}{TA \mid TB}$$

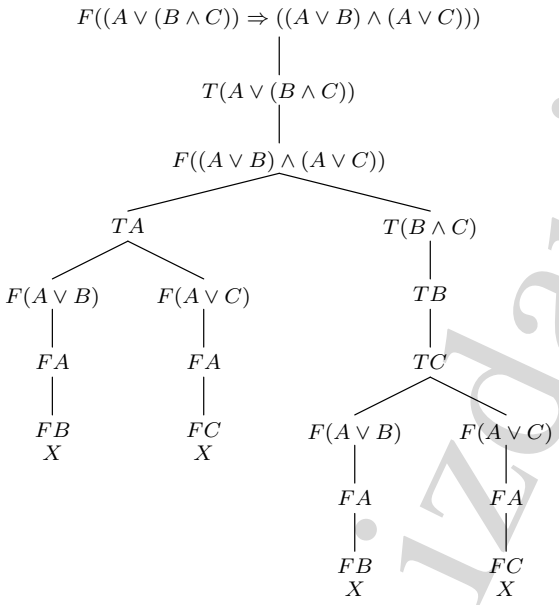
$$\frac{T(A \Rightarrow B)}{FA \mid TB}$$

Ako je na neku formulu moguće primeniti neko pravilo tipa (A), onda kažemo da je ta formula tipa α. Takve formule ćemo ponekad i označavati sa α. Ako je na neku formulu moguće primeniti neko pravilo tipa (B), onda kažemo da je ta formula tipa β. Takve formule ćemo ponekad i označavati sa β. Sva pravila za konstrukciju tabloa imaju jednu od sledećih (opštih) formi:

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\begin{array}{l} \alpha_1 \\ \alpha_2 \end{array}} \qquad \frac{\beta}{\beta_1 \mid \beta_2}$$

Analitički tablo za formulu A je uređeno stablo (videti definiciju 2.17) čijem je svakom čvoru pridružena označena formula, pri čemu je korenu stabla pridružena označena formula FA. Tablo se konstruiše (i proširuje) u iteracijama:

- ukoliko neka grana od korena do nekog lista stabla sadrži formulu tipa α koja nije iskorišćena u toj grani, onda lîstu te grane dodajemo, u zavisnosti od podtipa formule, jedan čvor (i pridružujemo mu formulu α_1) ili sukcesivno dva čvora i pridružujemo im odgovarajuće formule (α_1 i α_2);

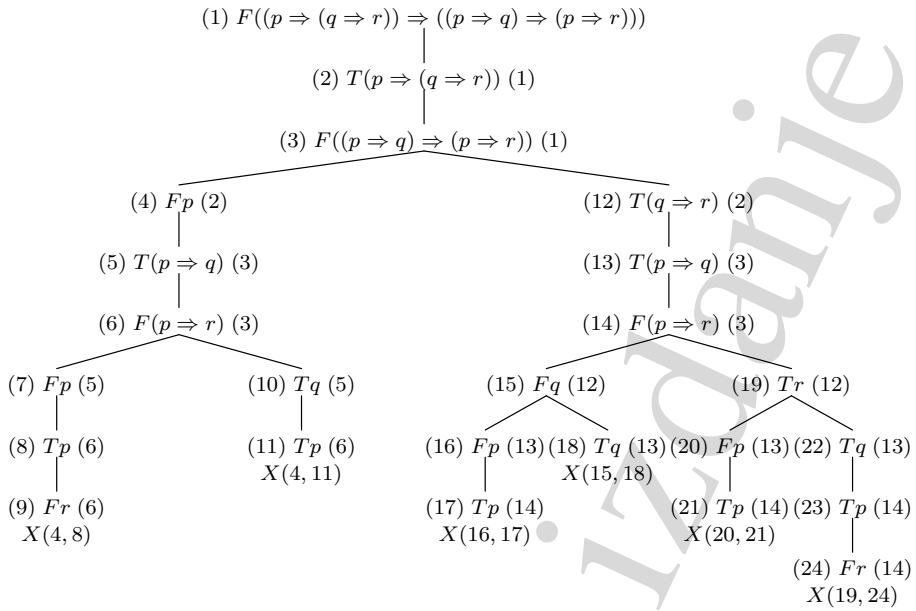


Slika 2.4: Tablo za formulu iz primera 2.13

- ukoliko neka grana od korena do nekog lista stabla sadrži formulu tipa β koja nije iskorišćena u toj grani, onda lîstu te grane dodeljujemo dva čvora sledbenika i pridružujemo im, redom, odgovarajuće formule β_1 i β_2.

Grana analitičkog tabloa je *zatvorena* (i označavamo je sa X) ako sadrži formule (ili, preciznije, ako sadrži čvorove kojima su pridružene formule) TB i FB. Ako grana nije zatvorena, onda kažemo da je ona *otvorena*. Analitički tablo je *zatvoren* ako je svaka njegova grana zatvorena.

Da bi se dokazalo da je formula A valjana (tautologija) dovoljno je dokazati da ni u jednoj valuaciji $\neg A$ nije tačno, tj. dovoljno je dokazati da do kontradikcije dovodi pretpostavka da je označena formula FA tačna u nekoj valuaciji. Iz pretpostavke da je označena formula FA tačna u nekoj valuaciji sledi da su neke označene potformule formule A nužno tačne ili nužno netačne u toj valuaciji. Postupak izvođenja takvih zaključaka (od kojih neki mogu da se granaju u po dve mogućnosti) direktno odgovara postupku konstrukcije tabloa. Protivrečnost polazne pretpostavke (da je označena formula FA tačna u nekoj valuaciji) pokazuje se time što su sve mogućnosti pobijene, tj. tako što je svaka grana tabloa zatvorena. Dakle, da bi se dokazalo da je formula A tautologija, dovoljno je pokazati da postoji zatvoreni analitički tablo za FA. U nastavku će biti dokazano (teoreme 2.20 i 2.21) da je formula A tautologija ako i samo ako postoji zatvoreni analitički tablo za FA.

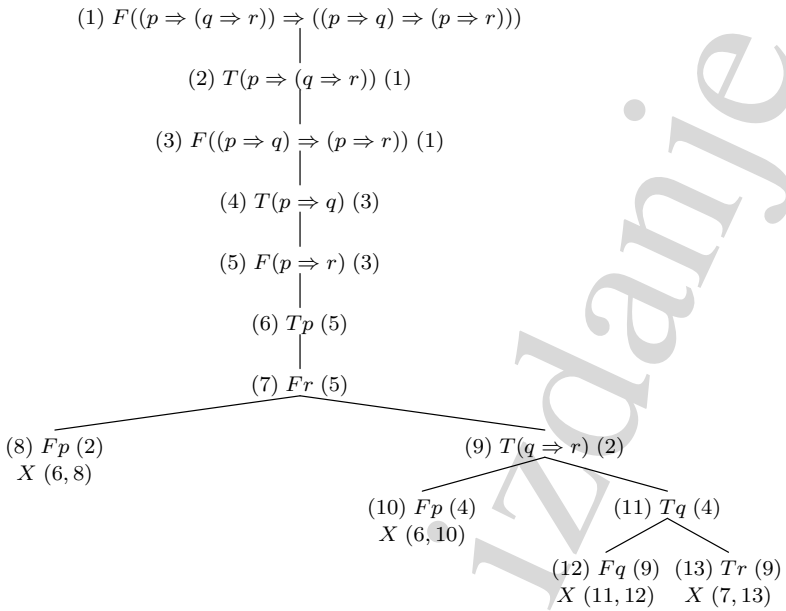


Slika 2.5: Primer sistematskog generisanja tabloa

Primer 2.13 *Formula* $(A \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge (A \vee C))$ *je tautologija. Tablo koji to dokazuje prikazan je na slici 2.4.*

Primetimo da je dobro (kada postoji mogućnost izbora) primenjivati pravila koja se odnose na formule tipa α pre pravila koja se odnose na formule tipa β. Time različite grane tabloa ne sadrže iste delove i sam proces dokazivanja je efikasniji. Ilustrujmo to na primeru formule $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$. Dokažimo navedenu formulu najpre na sledeći način: primenjujmo pravila za konstrukciju tabloa sistematski, tj. nikad ne koristimo neku formulu, ako nisu već iskorišćene sve formule (koje su u istoj grani) iznad nje. Tako konstruisan tablo prikazan je na slici 2.5. Na drugi način moguće je navedenu formulu dokazati dajući prioritet pravilima tipa (A): ne koristiti (u nekoj grani) neko pravilo tipa (B) ako nisu već primenjena sva moguća pravila tipa (A). Tako konstruisan tablo prikazan je na slici 2.6.

Navedenim primerima uvodimo i notaciju kojom se obeležavaju formule u tablou. Sa leve strane formule pisaćemo redni broj formule, a sa desne, broj formule od koje je ona dobijena. Formule mogu biti obeležene onim redom kojim se konstruiše tablo (npr. najpre u dubinu). Dodatno, uz oznaku za zatvorenu granu (X) pisaćemo brojeve formula na osnovu kojih je izvedena kontradikcija. Primetimo da smo u tablou prikazanom na slici 2.5 mogli da izostavimo čvor (9). Taj čvor je uveden primenom pravila tipa (A), ali do kontradikcije vodi formula pridružena čvoru (8), te čvor (9) može da bude izostavljen. U ostalim analognim situacijama takve formule su izostavljene.



Slika 2.6: Primer generisanja tabloa sa davanjem prioriteta formulama α tipa

Teorema 2.19 (Zaustavljanje metoda tabloa) *Metod tabloa se zaustavlja.*

Dokaz: U stablu tabloa svaki čvor je konačnog stepena (0, 1 ili 2). Dodatno, svaka grana je konačne dubine (jer svaka formula ima konačno mnogo potformula, što se jednostavno može dokazati primenom teoreme 2.1). Dakle, stablo tabloa ima konačno čvorova, pa se metod tabloa uvek zaustavlja u konačnom broju koraka. □

Teorema 2.20 (Saglasnost metoda tabloa) *Ako se neka iskazna formula može dokazati metodom tabloa (pobijanjem), onda je ona tautologija.*

Dokaz: Za granu tabloa kažemo da je zadovoljiva ako je zadovoljiv skup formula koje su pridružene čvorovima te grane.

Pretpostavimo da tablo $\mathcal{T}$ ima zadovoljivu granu θ. Neka je tablo $\mathcal{T}'$ neposredno (jednim korakom) dobijen od tabloa $\mathcal{T}$. Dokažimo da i tablo $\mathcal{T}'$ ima zadovoljivu granu. Tablo $\mathcal{T}'$ je dobijen od tabloa $\mathcal{T}$ dodavanjem sledbenika na neku granu θ' tabloa $\mathcal{T}$. Ako je θ različito od θ', onda tablo $\mathcal{T}'$ sadrži granu θ koja je zadovoljiva. Ako su grane θ i θ' jednake, tj. ako je tablo $\mathcal{T}'$ dobijen od tabloa $\mathcal{T}$ dodavanjem sledbenika na granu θ, onda razlikujemo dva slučaja:

- ako je primenjeno pravilo tipa (A) na formulu α, onda su grani sukcesivno dodata dva čvora sa formulama α_1 i α_2 ili čvor sa jednom formulom α_1; trivijalno se pokazuje da su i formule α_1 i α_2 ili, u drugom slučaju, α_1 tačne u svakoj valuaciji u kojoj je formula α tačna, odakle dalje sledi da je grana koja je dobijena od θ zadovoljiva, pa tablo $\mathcal{T}'$ ima zadovoljivu granu;
- ako je primenjeno pravilo tipa (B) na formulu β, onda su grani dodata dva čvora sa, redom, formulama β_1 i β_2; trivijalno se pokazuje da je, u svakoj valuaciji u kojoj je formula β tačna, bar jedna od formula β_1 i β_2 tačna, odakle dalje sledi da je bar jedna grana dobijena od θ zadovoljiva, pa tablo $\mathcal{T}'$ ima zadovoljivu granu;

Dakle, tablo $\mathcal{T}'$ ima zadovoljivu granu. Na osnovu jednostavnog induktivnog argumenta, zaključujemo sledeće: ako je tablo $\mathcal{T}'$ dobijen posredno (u više koraka) od tabloa $\mathcal{T}$ i ako tablo $\mathcal{T}$ ima zadovoljivu granu, onda zadovoljivu granu ima i tablo $\mathcal{T}'$. Početni tablo za datu formulu A sadrži samo koren kojem je pridružena formula FA. Ako je ona zadovoljiva, onda svaki tablo dobijen od tog početnog tabloa ima zadovoljivu granu. Zatvoren tablo nema nijednu zadoljivu granu. Ako je on dobijen od početnog tabloa sa korenom FA, sledi da formula FA nije zadovoljiva, tj. formula $\neg A$ je nezadovoljiva, tj. formula A je tautologija, što je i trebalo dokazati. □

Teorema o saglasnosti govori da je metodom tabloa moguće dokazati samo iskazne formule koje su tautologije. Postavlja se pitanje da li je metodom tabloa moguće dokazati *svaku* tautologiju. Drugim rečima, postavlja se pitanje da li za svaku tautologiju A postoji *bar jedan* zatvoren tablo čijem je korenu pridružena označena formula FA. Postavlja se i pitanje da li se za svaku tautologiju A može zatvoriti svaki tablo čijem je korenu pridružena označena formula FA.

Granu analitičkog tabloa zvaćemo *upotpunjenom* ako joj za svaku formulu tipa α koja joj pripada, pripadaju i odgovarajuće formule α_1 i α_2 ili odgovarajuća formula α_1 i ako joj za svaku formulu tipa β koja joj pripada, pripada i bar jedna od odgovarajućih formula β_1 i β_2. Tablo $\mathcal{T}$ zvaćemo *upotpunjenim* ako je svaka njegova grana upotpunjena ili zatvorena.

Definicija 2.18 *Kažemo da je (konačan ili beskonačan) skup iskaznih formula* S Hintikin *ili* nadole zasićen *ako zadovoljava naredne uslove:*

H_0: *Ne postoji iskazna promenljiva* p *takva da su i* Tp *i* Fp *u skupu* S.

H_1: *Ako skupu* S *pripada neka formula tipa* α*, onda skupu* S *pripadaju i odgovarajuće formule* α_1 *i* α_2 *ili odgovarajuća formula* α_1.

H_2: *Ako skupu* S *pripada neka formula tipa* β*, onda skupu* S *pripada bar jedna od odgovarajućih formula* β_1 *i* β_2.

Neka je θ upotpunjena otvorena grana tabloa $\mathcal{T}$ i neka je S skup svih formula pridruženih čvorovima grane θ. Tada je, očigledno, skup S Hintikin.

Lema 2.2 (Hintikina lema) *Svaki nadole zasićeni skup S (konačan ili beskonačan) je zadovoljiv.*

Dokaz: Neka je S Hintikin skup. Odredimo valuaciju v u kojoj je svaki element skupa S tačan. Svakoj iskaznoj promenljivoj koja se pojavljuje u bar jednom elementu skupa S dodeljujemo istinitosnu vrednost na sledeći način:

- ako je $Tp \in S$, neka je $v(p) = 1$;
- ako je $Fp \in S$, neka je $v(p) = 0$;
- ako ni Tp ni Fp nisu elementi skupa S, onda p može da ima proizvoljnu vrednost, ali radi određenosti uzimamo da je $v(p) = 1$.

Primetimo da prva dva pravila nisu u koliziji, jer ni za jednu iskaznu promenljivu p ne može da važi $Tp \in S$ i $Fp \in S$.

Dokažimo indukcijom po složenosti označene formule (videti definiciju 2.3) da je u valuaciji v tačna svaka formula iz skupa S. Neka je složenost označene formule jednaka složenosti odgovarajuće neoznačene formule (tj. složenost označenih formula TA i FA jednaka je složenosti formule A).

Očigledno, svaka označena iskazna promenljiva (dakle, označena formula složenosti 0) koja je element skupa S tačna je u valuaciji v (valuacija v je konstruisana tako da to važi).

Pretpostavimo da je svaki element skupa S koji je složenosti manje od n ($n > 0$) tačan u valuaciji v i dokažimo da je u toj valuaciji tačna i označena formula A složenosti n. Složenost označene formule A je veća od 0, pa je ona ili tipa α ili tipa β.

- Pretpostavimo da je označena formula A tipa α; onda, na osnovu uslova H_1, mora da, za odgovarajuće formule α_1 i α_2, važi $\alpha_1, \alpha_2 \in S$ (ili, u zavisnosti od oblika formule A, za odgovarajuću formulu α_1, važi $\alpha_1 \in S$). Složenost formula α_1 i α_2 je manja od n, pa za njih važi induktivna pretpostavka, tj. i α_1 i α_2 su tačne u valuaciji v. Odatle neposredno sledi da je i formula α tačna u valuaciji v.
- Pretpostavimo da je označena formula A tipa β; onda, na osnovu uslova H_2, mora da, za odgovarajuće formule β_1 i β_2, važi $\beta_1 \in S$ ili $\beta_2 \in S$. Složenost formula β_1 i β_2 je manja od n, pa ma koja od njih da pripada skupu S, ona, na osnovu induktivne pretpostavke, mora da bude tačna. Odatle neposredno sledi da je i formula β tačna u valuaciji v.

Dakle, u valuaciji v tačna je svaka formula iz skupa S, pa je skup S zadovoljiv. □

Teorema 2.21 (Potpunost metoda tabloa) *Ako je neka iskazna formula valjana, onda se ona može dokazati metodom tabloa.*

Dokaz: Za svaku upotpunjenu otvorenu granu tabloa, skup formula koje su joj pridružene je Hintikin, pa je, na osnovu Hintikine leme, i zadovoljiv. Dakle, ako upotpunjeni tablo $\mathcal{T}$ ima neku otvorenu granu, onda je ta grana zadovoljiva. Odatle sledi: ako je $\mathcal{T}$ upotpunjeni tablo takav da ima neku otvorenu granu, onda je u njegovom korenu zadovoljiva iskazna formula. Obratno, ako je u korenu upotpunjenog tabloa $\mathcal{T}$ formula FA koja nije zadovoljiva (tj. formula A je valjana), onda tablo $\mathcal{T}$ ne može da ima nijednu otvorenu granu. Drugim rečima, ako je formula A valjana, onda je (bilo koji) upotpunjeni tablo sa korenom FA zatvoren, tj. A se može dokazati metodom tabloa. □

Na osnovu prethodnih teorema sledi naredno tvrđenje.

Teorema 2.22 (Teorema o metodu tabloa) *Metod tabloa se zaustavlja za svaku iskaznu formulu. Dobijeni tablo je zatvoren ako i samo ako je polazna formula valjana.*

Da bi se dokazalo da je neka iskazna formula A valjana, dovoljno je konstruisati zatvoreni tablo čijem korenu je pridružena označena formula FA. Da bi se dokazalo da je neka iskazna formula A logička posledica skupa formula B_1, B_2, ..., B_n dovoljno je konstruisati zatvoreni tablo čijem korenu je pridružena označena formula $F(B_1 \wedge B_2 \wedge \ldots \wedge B_n \Rightarrow A)$ ili konstruisati zatvoreni tablo čijim početnim čvorovima (u nizu) su pridružene označene formule TB_1, TB_2, ..., TB_n, FA.

Zadaci

Zadatak 31 *Dokazati metodom tabloa da su naredne formule tautologije:*

(a) $q \Rightarrow (p \Rightarrow q)$
(b) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
(c) $((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow (q \wedge r))$
(d) $(((p \Rightarrow r) \wedge (q \Rightarrow r)) \wedge (p \vee q)) \Rightarrow r$
(e) $\neg(p \wedge q) \Rightarrow (\neg p \vee \neg q)$
(f) $\neg(p \vee q) \Rightarrow (\neg p \wedge \neg q)$
(g) $(\neg p \vee \neg q) \Rightarrow \neg(p \wedge q)$
(h) $(p \vee (q \wedge r)) \Rightarrow ((p \vee q) \wedge (p \vee r))$

Zadatak 32 *Ispitati metodom tabloa da li je formula*
$((A \vee (B \underline{\vee} (P \Rightarrow Q))) \Leftrightarrow (B \Rightarrow A)) \Leftrightarrow (\neg Q \Rightarrow (P \Rightarrow A))$
tautologija.

2.2.9 Teorema o kompaktnosti za iskaznu logiku

Teorema o kompaktnosti govori o odnosu zadovoljivosti i nezadovoljivosti konačnih i beskonačnih skupova formula. Ona tvrdi da je zadovoljiv svaki skup formula čiji je svaki konačan podskup zadovoljiv.

Definicija 2.19 *Skup formula (konačan ili beskonačan) je* konačno zadovoljiv *ako je zadovoljiv svaki njegov konačan podskup.*

Lema 2.3 *Neka je Γ konačno zadovoljiv skup formula i neka je A formula nad istim skupom promenljivih. Tada je skup $\Gamma \cup \{A\}$ konačno zadovoljiv ili skup $\Gamma \cup \{\neg A\}$ konačno zadovoljiv.*

Dokaz: Pretpostavimo suprotno — da ni skup $\Gamma \cup \{A\}$ ni skup $\Gamma \cup \{\neg A\}$ nisu konačno zadovoljivi. Tada postoje konačni podskupovi Δ_1 i Δ_2 skupa Γ takvi da skupovi $\Delta_1 \cup \{A\}$ i $\Delta_2 \cup \{\neg A\}$ nisu zadovoljivi. No, skup $\Delta_1 \cup \Delta_2$ je konačan podskup skupa Γ, pa je on zadovoljiv te postoji valucija v takva da za svaku formulu B iz $\Delta_1 \cup \Delta_2$ važi $I_v(B) = 1$. Za tu (kao i za bilo koju drugu) valuaciju važi $I_v(A) = 1$ ili $I_v(A) = 0$. U prvom slučaju, sve formule iz skupa $\Delta_1 \cup \{A\}$ su tačne u valuaciji v, pa je on zadovoljiv, a u drugom slučaju, analogno, zadovoljiv je skup $\Delta_2 \cup \{\neg A\}$. Dakle, zadovoljiv je ili skup $\Delta_1 \cup \{A\}$ ili skup $\Delta_2 \cup \{\neg A\}$, što dovodi do protivrečnosti. Polazna pretpostavka je bila pogrešna, pa sledi da je skup $\Gamma \cup \{A\}$ konačno zadovoljiv ili skup $\Gamma \cup \{\neg A\}$ konačno zadovoljiv. □

Teorema 2.23 (Teorema o kompaktnosti) *Ako je svaki konačan podskup skupa formula zadovoljiv, onda je i taj skup zadovoljiv (tj. svaki konačno zadovoljiv skup je zadovoljiv).*

Dokaz: Neka je Γ konačno zadovoljiv skup formula nad skupom promenljivih P. Dokažimo da je skup Γ zadovoljiv.

Za skup promenljivih P koji je prebrojiv, prebrojiv je i skup iskaznih formula nad tim skupom. Dakle, sve formule nad tim skupom mogu biti enumerisane u niz $A_0, A_1, A_2, \ldots$. Niz $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ definišimo na sledeći način:

$$\begin{aligned} \Gamma_0 &= \Gamma \\ \Gamma_{n+1} &= \begin{cases} \Gamma_n \cup \{A_n\}, & \text{ako je ovaj skup konačno zadovoljiv} \\ \Gamma_n \cup \{\neg A_n\}, & \text{inače.} \end{cases} \end{aligned}$$

Na osnovu leme 2.3, svaki od skupova Γ_n ($n \geq 0$) je konačno zadovoljiv.

Skup $\tilde{\Gamma}$, definisan na sledeći način

$$\tilde{\Gamma} = \bigcup_{n=0}^{\infty} \Gamma_n$$

je konačno zadovoljiv. Zaista, neka je Δ konačan skup takav da je $\Delta \subseteq \tilde{\Gamma}$. Za svaku formulu A, $A \in \Delta$, važi $A \in \Gamma_n$ za neku vrednost n. Ako je m maksimum tih vrednosti, onda važi $\Delta \subseteq \Gamma_m$. Kako je skup Γ_m konačno zadovoljiv, sledi da je i skup Δ zadovoljiv.

Za svaku formulu A (nad datim skupom promenljivih P) važi ili $A \in \tilde{\Gamma}$ ili $\neg A \in \tilde{\Gamma}$, ali ne i jedno i drugo. Dokažimo to. Formula A nalazi se u nizu formula A_1, A_2, A_3, ..., pa je $A = A_n$ za neku vrednost n. Tada je $A \in \Gamma_{n+1}$ ili $\neg A \in \Gamma_{n+1}$, odakle sledi da formula A ili formula $\neg A$ pripadaju skupu $\tilde{\Gamma}$. Ako bi važilo i $A \in \tilde{\Gamma}$ i $\neg A \in \tilde{\Gamma}$, moralo bi da važi da je konačan (pod)skup $\{A, \neg A\}$ (skupa $\tilde{\Gamma}$) zadovoljiv (jer je skup $\tilde{\Gamma}$ konačno zadovoljiv), što nije moguće. Dakle, važi ili $A \in \tilde{\Gamma}$ ili $\neg A \in \tilde{\Gamma}$, ali ne važi i jedno i drugo.

Neka je valuacija v valuacija za koju važi $v(p) = 1$ ako je $p \in \tilde{\Gamma}$ i $v(p) = 0$ ako je $p \notin \tilde{\Gamma}$, za svaku promenljivu p iz P. Za tu valuaciju (i odgovarajuću interpretaciju I_v) i proizvoljnu formulu A dokažimo da važi:

$$I_v(A) = 1 \text{ ako i samo ako } A \in \tilde{\Gamma}.$$

Kako je $\{\neg, \wedge\}$ potpun skup veznika, jednostavnosti radi, može se pretpostaviti da formula A sadrži samo veznike $\neg$ i $\wedge$. Tvrđenje $I_v(A) = 1$ *ako i samo ako* $A \in \tilde{\Gamma}$ dokažimo indukcijom po složenosti formule (videti definiciju 2.3). Ako je složenost formule A jednaka 0, onda je formula A iskazna promenljiva, $\bot$ ili $\top$. Ako je formula A iskazna promenljiva, tvrđenje sledi na osnovu definicije valuacije v. Skup $\tilde{\Gamma}$ je konačno zadovoljiv, pa ne može da mu pripada formula $\bot$, odakle sledi tvrđenje za $A = \bot$. Skup $\tilde{\Gamma}$ je konačno zadovoljiv, pa ne može da mu pripada formula $\neg\top$; kako važi $\top \in \tilde{\Gamma}$ ili $\neg\top \in \tilde{\Gamma}$, sledi $\top \in \tilde{\Gamma}$, pa važi tvrđenje za $A = \top$. Pretpostavimo da je složenost formule A jednaka n ($n > 0$) i da tvrđenje važi za sve vrednosti manje od n. Kako je formula A složenosti $n > 0$, ona je oblika $\neg B$ ili oblika $B \wedge C$, pri čemu, na osnovu induktivne hipoteze, tvrđenje važi za B i C.

Slučaj $A = \neg B$**:** Ako je $I_v(A) = 1$, onda sledi $I_v(B) \neq 1$, pa, na osnovu induktivne hipoteze, važi $B \notin \tilde{\Gamma}$. Iz $B \notin \tilde{\Gamma}$ sledi $\neg B \in \tilde{\Gamma}$, tj. $A \in \tilde{\Gamma}$.

Ako važi $A \in \tilde{\Gamma}$, onda je $\neg B \in \tilde{\Gamma}$, pa važi $B \notin \tilde{\Gamma}$. Odatle, na osnovu induktivne hipoteze važi $I_v(B) \neq 1$ i, dalje, $I_v(A) = 1$.

Slučaj $A = B \wedge C$**:** Ako važi $I_v(A) = 1$, onda je $I_v(B) = I_v(C) = 1$, pa, na osnovu induktivne hipoteze, važi $B \in \tilde{\Gamma}$ i $C \in \tilde{\Gamma}$. Ne može da važi $\neg A \in \tilde{\Gamma}$, jer je konačan skup $\{B, C, \neg A\}$ nezadovoljiv. Dakle, mora da važi $A \in \tilde{\Gamma}$.

Obratno, ako važi $A \in \tilde{\Gamma}$, onda ni $\neg B$ ni $\neg C$ ne pripadaju skupu $\tilde{\Gamma}$, jer konačni skupovi $\{A, \neg B\}$ i $\{A, \neg C\}$ nisu zadovoljivi. Dakle, važi $B \in \tilde{\Gamma}$ i $C \in \tilde{\Gamma}$. Na osnovu induktivne hipoteze, važi $I_v(B) = I_v(C) = 1$, odakle sledi $I_v(A) = 1$.

Kako važi $\Gamma \subseteq \tilde{\Gamma}$, sledi da važi $I_v(A) = 1$ za svaku formulu A iz skupa Γ. Dakle, skup Γ je zadovoljiv, što je i trebalo dokazati. □

Teorema o kompaktnosti može biti formulisana i na sledeći način: ako je skup Γ iskaznih formula protivrečan, onda postoji konačan podskup od Γ koji je protivrečan.

Teorema 2.24 *Ako je iskazna formula A tačna u svakoj valuaciji koja zadovoljava skup iskaznih formula Γ, onda postoji konačno mnogo formula A_1, A_2, ..., A_n iz Γ takvih da je formula A logička posledica skupa formula $\{A_1, A_2, \ldots, A_n\}$.*

Dokaz: U svakoj valuaciji koja zadovoljava Γ, formula $\neg A$ je netačna, pa je skup $\Gamma \cup \{\neg A\}$ protivrečan. Tada, na osnovu teoreme o kompaktnosti (teorema 2.23), postoji konačan protivrečan podskup Γ_0 skupa $\Gamma \cup \{\neg A\}$. Kako je skup Γ_0 protivrečan, protivrečan je i skup $\Gamma_0 \cup \{\neg A\}$. Ako su A_1, A_2, ..., A_n elementi skupa $\Gamma_0 \cup \{\neg A\}$ različiti od $\neg A$, onda je skup $\{A_1, A_2, \ldots, A_n, \neg A\}$ protivrečan. Odatle sledi da je formula $A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge \neg A$ protivrečna, tj. da je formula $\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge \neg A)$ tautologija. Dakle, formula $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow A$ je tautologija, pa sledi da je formula A logička posledica skupa formula $\{A_1, A_2, \ldots, A_n\}$, što je i trebalo dokazati. □

Zadaci

Zadatak 33 *Da li je skup klauza*

$$\{(p_i \vee \neg p_{i+1}) \mid i = 1, 2, 3, \ldots\}$$

zadovoljiv?

Zadatak 34 *Da li je skup klauza*

$$\{(p_i \vee \neg p_{i+1}), (\neg p_i \vee p_{i+1}) \mid i = 1, 2, 3, \ldots\}$$

zadovoljiv?

2.3 Sistemi za dedukciju u iskaznoj logici

Istinitosne tablice omogućavaju nam da za proizvoljnu iskaznu formulu jednostavno dobijemo odgovor da li je ona tautologija, zadovoljiva, poreciva ili kontradikcija. Međutim, slični metodi neće uvek postojati za složenije teorije i zato ćemo morati da tragamo za drugačijim metodologijama za ispitivanja statusa formula. Osim toga, moći ćemo da razmatramo dodatne statuse, ne

samo one koji proističu iz semantičkih karakteristika formula. Ti statusi biće sintaksne (preciznije, sintaksno-deduktivne) prirode i proizilaziće iz karakteristika konkretnog deduktivnog sistema koji gradimo. Kao što je teorija modela vezana za semantiku, tako su deduktivni sistemi i teorija dokaza vezani za sintaksu.

Zbog jednostavnosti, sisteme za dedukciju ilustrovaćemo najpre na primeru iskazne logike. Sistemi za dedukciju za iskaznu logiku su čisto sintaksne prirode — primenjuju se kroz kombinovanje simbola, ne ulazeći u semantiku formula. Sisteme za dedukciju za iskaznu logiku zovemo i *iskazni račun*.

Na samom početku, daćemo grubi opis pojma formalne teorije.

Formalnu teoriju $\mathcal{T}$ čini:

1. prebrojiv skup Σ simbola koji čine alfabet teorije;
2. podskup skupa svih reči nad alfabetom Σ; elemente tog skupa zovemo *dobro zasnovanim formulama* (ili, kraće, samo *formulama*) teorije $\mathcal{T}$;
3. podskup skupa svih formula teorije $\mathcal{T}$ koji zovemo *skupom aksioma* teorije $\mathcal{T}$; ako je skup aksioma rekurzivan (tj. ako se za svaku formulu može efektivno proveriti da li pripada tom skupu), onda teoriju $\mathcal{T}$ zovemo *aksiomatskom teorijom* (ili *aksiomatibilnom teorijom*);
4. konačan skup R_1, R_2, ..., R_n relacija (ili shema relacija) između formula koje zovemo *pravila izvođenja*; za svako pravilo izvođenja R_i arnosti $j+1$ i za svaki skup od $j+1$ formula (Φ_1, Φ_2, ..., Φ_j, Ψ) može se efektivno utvrditi da li je prvih j formula u relaciji R_i sa $(j+1)$-om formulom; ako jeste, onda kažemo da je ta formula direktna posledica datog skupa j formula na osnovu pravila R_i i pišemo:

$$\frac{\Phi_1 \quad \Phi_2 \quad \dots \quad \Phi_j}{\Psi} \; R_i .$$

Pojam *dokaza* može da se razlikuje od jednog do drugog deduktivnog sistema. Obično je dokaz niz formula (ili skup formula pridruženih stablu) Φ_1, Φ_2, ..., Φ_n, takav da za svako i ili važi da je formula Φ_i aksioma teorije $\mathcal{T}$ ili važi da je Φ_i direktna posledica nekih od prethodnih formula u nizu na osnovu nekog pravila izvođenja. Dobro zasnovana formula Φ teorije $\mathcal{T}$ je *teorema* teorije $\mathcal{T}$ ako postoji dokaz čiji je poslednji član formula Φ. Taj dokaz tada zovemo *dokazom formule* Φ. Tada kažemo i da je formula Φ *dokaziva* u teoriji $\mathcal{T}$. Ponekad pod pojmom „teorija $\mathcal{T}$“ podrazumevamo skup svih teorema teorije $\mathcal{T}$. Ako postoji efektivna procedura za utvrđivanje da li je data formula teorema teorije $\mathcal{T}$, onda kažemo da je teorija $\mathcal{T}$ *odlučiva*, a inače kažemo da je *neodlučiva*. Mnoge interesantne teorije su neodlučive (više o odlučivosti i neodlučivosti videti u glavi 4).

Formula Φ teorije $\mathcal{T}$ je *deduktivna posledica* (ili, kraće, *posledica*) skupa formula Γ ako postoji dokaz formule Φ koji kao aksiome može da uključuje i formule iz skupa Γ. Elemente skupa Γ tada zovemo hipotezama ili premisama

dokaza. Tvrđenje da je Φ posledica skupa Γ u teoriji $\mathcal{T}$ zapisujemo $\Gamma \vdash_{\mathcal{T}} \Phi$ (simbol $\vdash$ čitamo „rampa“). Kada je jasno o kojoj teoriji je reč (tj. kada nema opasnosti od višesmislenosti), pišemo kraće $\Gamma \vdash \Phi$. Ako je skup Γ konačan, onda umesto $\{\Psi_1, \Psi_2, \ldots, \Psi_n\} \vdash \Phi$ pišemo kraće $\Psi_1, \Psi_2, \ldots, \Psi_n \vdash \Phi$. Ako je skup Γ prazan, onda umesto $\emptyset \vdash \Phi$ pišemo obično $\vdash \Phi$. Važi $\vdash \Phi$ ako i samo ako je Φ teorema teorije $\mathcal{T}$.

Sistemi za dedukciju mogu da odgovaraju specifičnom matematičko-filozofskom pravcu. Na primer, intuicionistički pristup matematici orijentisan je ka *eksplicitnoj, efektivnoj dokazivosti*. Svaki intuicionistički dokaz istovremeno je i dokaz u klasičnoj logici, ali ne važi obratno: intuicionistički kriterijum dokaza je strožiji od klasičnog i intuicionisti ne prihvataju sve dokaze koje prihvata klasična matematička logika. Razmotrimo sledeći primer: potrebno je dokazati da postoje iracionalni brojevi p i q takvi da je broj p^q racionalan. Ako je $\sqrt{2}^{\sqrt{2}}$ racionalan broj, onda brojevi $\sqrt{2}$ i $\sqrt{2}$ zadovoljavaju zadati uslov; ako $\sqrt{2}^{\sqrt{2}}$ nije racionalan broj, onda zadati uslov zadovoljavaju brojevi $\sqrt{2}^{\sqrt{2}}$ i $\sqrt{2}$ (jer je broj $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^{2} = 2$ racionalan). Iako su ovim razmatranjem pokrivena oba moguća slučaja, ne zna se koji od njih je istinit, te je zato ovaj dokaz neprihvatljiv intuicionistima. Suštinski, intuicionistička matematika ne prihvata isključenje trećeg ($A \vee \neg A$, *tertium non datur*). U nekim deduktivnim sistemima razlika između klasične i intuicionističke varijante svodi se upravo na uključivanje ili neuključivanje ovog principa kao aksiome (više o intucionizmu videti u poglavlju B.2.3).

I koncept deduktivne posledice može na drugačije načine biti uveden u različitim deduktivnim sistemima. Na primer, svojstvo

„ako je $\Gamma \subseteq \Delta$ i $\Gamma \vdash \Phi$, onda je $\Delta \vdash \Phi$“

važi samo za takozvane *monotone* sisteme za dedukciju, samo za *monotono rezonovanje*. U sistemima za nemonotono rezonovanje zaključci se donose na osnovu raspoloživih podataka i oni mogu biti povučeni kada budu raspoložive nove informacije. U daljem tekstu biće razmatrani samo sistemi za monotono rezonovanje.

Na ovom mestu naglasimo i razliku između dve vrste teorema koje pominjemo u tekstu — između strogo definisanih teorema formalne teorije i teorema u kojima su na prirodnom jeziku iskazana neka tvrđenja. Ove prve formulisane su na jeziku sâme formalne teorije, dok su ove druge formulisane na prirodnom jeziku. Slično je i sa dokazima. Teoreme iz prve grupe jesu *tvrđenja neke formalne teorije*. Teoreme iz druge grupe su obično *tvrđenja o nekoj formalnoj teoriji*. Zato ih, teoreme iz druge grupe, često zovemo *metateoremama*. Slično, jezik sâme formalne teorije kojom se bavimo obično zovemo *objektnim jezikom*, dok jezik teorema koje govore o formalnim teorijama često zovemo *metajezikom* (za neformalnu ilustraciju, možemo reći da časovi engleskog jezika mogu da se drže na srpskom jeziku; pri tome je engleski jezik objektni, a srpski je metajezik i na njemu se diskutuje o objektnom — engleskom jeziku).

U daljem tekstu iz konteksta će se uvek jasno videti da li je, kada kažemo teorema, u pitanju teorema neke formalne teorije ili metateorema.

2.3.1 Hilbertov sistem

U okviru Hilbertovog sistema[6], koji ćemo zvati i teorija L ili teorija H, jezik iskazne logike definisaćemo nešto drugačije nego u poglavlju 2.1. Osnovnim (ili primitivnim) logičkim veznicima zvaćemo samo veznike $\neg$ i $\Rightarrow$, a ostale logičke veznike ćemo definisati i smatrati samo skraćenicama.

Alfabet Σ teorije L čine:

1. *iskazna slova* — elementi skupa P;
2. *skup logičkih veznika* $\{\neg, \Rightarrow\}$ pri čemu je $\neg$ unarni veznik, a $\Rightarrow$ je binarni veznik;
3. *skup pomoćnih simbola* $\{(,)\}$.

Definicija 2.20 Skup iskaznih formula *(ili* skup dobro zasnovanih formula teorije L*) nad skupom* P *je najmanji podskup skupa svih reči nad* Σ *takav da važi:*

1. *iskazna slova su iskazne formule;*
2. *ako su* A *i* B *iskazne formule, onda su i* $(\neg A)$ *i* $(A \Rightarrow B)$ *iskazne formule.*

Koristimo uobičajene konvencije za izostavljanje zagrada u zapisu iskaznih formula.

Aksiome teorije L su sledeće sheme formula (gde su A, B i C proizvoljne iskazne formule):

(A1) $A \Rightarrow (B \Rightarrow A)$

(A2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(A3) $(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$

Naglasimo da je aksiomskim shemama dât beskonačan skup aksioma. Ipak, za svaku iskaznu formulu može se efektivno proveriti da li je ona aksioma teorije L. Skup aksioma teorije L je, dakle, rekurzivan, pa je ona aksiomatska teorija.

Jedino *pravilo izvođenja* teorije L je *modus ponens*, koje kraće označavamo MP. Na osnovu ovog pravila, formula B je direktna posledica formula A i $A \Rightarrow B$, tj:

$$\frac{A \quad A \Rightarrow B}{B}\ \text{MP}.$$

Sledećim definicijama uvodimo logičke veznike $\wedge$, $\vee$, $\Leftrightarrow$:

[6] Postoji više varijanti formalnih teorija koje opisuju iskaznu logiku i definisane su u tzv. Hilbertovom stilu. U ovom tekstu mi ćemo se baviti samo jednom od njih.

(D1) $A \wedge B$ je kraći zapis za $\neg(A \Rightarrow \neg B)$

(D2) $A \vee B$ je kraći zapis za $(\neg A) \Rightarrow B$

(D3) $A \Leftrightarrow B$ je kraći zapis za $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Sledećim definicijama uvodimo logičke konstante $\top$, $\bot$:

(D4) $\top$ je kraći zapis za $A \Rightarrow A$, gde je A proizvoljna formula

(D5) $\bot$ je kraći zapis za $\neg(A \Rightarrow A)$, gde je A proizvoljna formula.

Dokaz (*dedukcija*, *izvod*) u okviru teorije L je niz formula A_1, A_2, ..., A_n, takav da za svako i ili važi da je formula A_i aksioma teorije L ili važi da je A_i direktna posledica nekih od prethodećih formula na osnovu nekog pravila izvođenja. Formula A je *teorema* teorije L ako postoji dokaz čiji je poslednji član formula A. Taj niz tada zovemo *dokazom formule* A i kažemo da je formula A *dokaziva* u teoriji L.

U okviru teorije L, za formulu A kažemo da je *deduktivna posledica* (ili, kraće, *posledica*) skupa formula Γ ako i samo ako postoji niz formula A_1, A_2, ..., A_n, takav da je formula A jednaka formuli A_n i za svaku formulu A_i ($1 \leq i \leq n$) važi da je ili aksioma teorije L, ili da pripada skupu Γ ili da je direktna posledica nekih od prethodećih formula u nizu na osnovu nekog pravila izvođenja. Takav niz zovemo *dokaz* formule A iz Γ. Elemente skupa Γ tada zovemo *hipotezama* ili *premisama*. Tvrđenje da je A posledica skupa Γ u teoriji L zapisujemo $\Gamma \vdash_L A$ ili, kada je jasno da je reč o teoriji L, kraće $\Gamma \vdash A$. Ako je skup Γ konačan, onda umesto $\{B_1, B_2, \ldots, B_n\} \vdash A$ pišemo kraće $B_1, B_2, \ldots, B_n \vdash A$. Ako je skup Γ prazan, onda umesto $\emptyset \vdash A$ pišemo obično $\vdash A$. Važi $\vdash A$ ako i samo ako je A teorema teorije L.

Teorema 2.25 *U teoriji L važi:*

(a) Ako je $\Gamma \vdash A$ i $\Gamma \subseteq \Delta$, onda je $\Delta \vdash A$.

(b) Važi $\Gamma \vdash A$ ako i samo ako postoji konačan podskup Δ skupa Γ takav da je $\Delta \vdash A$.

(c) Ako važi $\Gamma \vdash A$ i ako za svaku formulu B iz Γ važi $\Delta \vdash B$, onda važi $\Delta \vdash A$.

Dokaz: Ako važi $\Gamma \vdash A$, to znači da postoji niz formula A_1, A_2, ..., A_n, takav da je formula A jednaka formuli A_n i za svaku formulu A_i ($1 \leq i \leq n$) važi da je ili aksioma teorije L, ili da pripada skupu Γ ili da je direktna posledica nekih od prethodećih formula u nizu na osnovu nekog pravila izvođenja.

(a) Kako važi $\Gamma \subseteq \Delta$, trivijalno sledi da je u nizu formula A_1, A_2, ..., A_n svaka formula A_i aksioma teorije L, ili da pripada skupu Δ ili da je direktna posledica nekih od prethodećih formula u nizu na osnovu nekog pravila izvođenja, te sledi $\Delta \vdash A$.

(b) Pretpostavimo da važi $\Gamma \vdash A$ i neka je Δ skup svih formula A_i ($1 \leq i \leq n$) koje pripadaju skupu Γ. Tada za niz formula A_1, A_2, ..., A_n važi da je svaka formula A_i aksioma teorije L, ili da pripada skupu Δ ili da je direktna posledica nekih od prethodećih formula u nizu na osnovu nekog pravila izvođenja, te sledi $\Delta \vdash A$.

Pretpostavimo da postoji konačan podskup Δ skupa Γ takav da je $\Delta \vdash A$. Na osnovu dela (a), odatle sledi da važi i $\Gamma \vdash A$.

(c) Neka je u nizu A_1, A_2, ..., A_n svaka od formula B koja pripada skupu Γ zamenjena dokazom (nizom formula) za $\Delta \vdash B$. U tako dobijenom nizu, čiji je poslednji član formula A, svaka formula je aksioma teorije L, ili pripada skupu Δ ili je direktna posledica nekih od prethodećih formula u nizu na osnovu nekog pravila izvođenja, te sledi $\Delta \vdash A$.

□

U dokazima u okviru teorije L, kao objašnjenje nekog koraka dokaza, umesto, na primer „(instanca aksiomske sheme A2)“ pisaćemo kraće „(A2)“. Umesto, na primer „(direktna posledica koraka 3 i 4, na osnovu pravila MP)“ pisaćemo kraće „(3, 4, MP)“. U dokazima ćemo sa (Hyp) označavati da je tvrđenje formula koja pripada skupu hipoteza.

Teorema 2.26 *Za svaku iskaznu formulu A važi $\vdash_L A \Rightarrow A$, tj. formula $A \Rightarrow A$ je teorema teorije L.*

Dokaz: Dokaz teoreme $A \Rightarrow A$:

1. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$	(A2)
2. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$	(A1)
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$	(1, 2, MP)
4. $A \Rightarrow (A \Rightarrow A)$	(A1)
5. $A \Rightarrow A$	(3, 4, MP)

□

U daljem tekstu umesto $\vdash_L$ pisaćemo $\vdash$, podrazumevajući da se izvođenje odnosi na teoriju L.

Teorema 2.27 (Teorema o dedukciji) *Ako je Γ skup iskaznih formula, A i B su iskazne formule i ako važi $\Gamma, A \vdash B$, onda važi i $\Gamma \vdash A \Rightarrow B$. Specijalno, ako važi $A \vdash B$, onda važi i $\vdash A \Rightarrow B$.*

Dokaz: Neka je B_1, B_2, ..., B_n dokaz formule B iz $\Gamma \cup \{A\}$ (pri čemu je $B_n = B$). Dokažimo, indukcijom po i, da važi $\Gamma \vdash A \Rightarrow B_i$ za svako i takvo da je $1 \leq i \leq n$.

Formula B_1 mora biti ili iz Γ ili aksioma ili jednaka formuli A. U prva dva slučaja, iz $\Gamma \vdash B_1$ i $\Gamma \vdash B_1 \Rightarrow (A \Rightarrow B_1)$ (formula $B_1 \Rightarrow (A \Rightarrow B_1)$ je aksioma sheme (A1)), na osnovu pravila MP sledi $\Gamma \vdash A \Rightarrow B_1$. U trećem slučaju, kada je formula B_1 jednaka formuli A, na osnovu teoreme 2.26 važi $\vdash A \Rightarrow B_1$ i, dalje, $\Gamma \vdash A \Rightarrow B_1$ (na osnovu teoreme 2.25). Ovim je tvrđenje $\Gamma \vdash A \Rightarrow B_i$ dokazano za $i = 1$.

Pretpostavimo da $\Gamma \vdash A \Rightarrow B_k$ važi za sve k takve da je $k < i$. Formula B_i je ili aksioma ili je B_i iz Γ ili je B_i jednako A ili je B_i direktna posledica nekih formula B_j i B_m (gde je $j < i$ i $m < i$ i B_m je oblika $B_j \Rightarrow B_i$) na osnovu pravila MP. U prva tri slučaja, važi $\Gamma \vdash A \Rightarrow B_i$, analogno slučaju $i = 1$. U poslednjem slučaju, na osnovu induktivne hipoteze, važi $\Gamma \vdash A \Rightarrow B_j$ i $\Gamma \vdash A \Rightarrow (B_j \Rightarrow B_i)$. Na osnovu aksiomske sheme (A2) važi $\vdash (A \Rightarrow (B_j \Rightarrow B_i)) \Rightarrow ((A \Rightarrow B_j) \Rightarrow (A \Rightarrow B_i))$. Dakle, na osnovu pravila MP, važi $\Gamma \vdash ((A \Rightarrow B_j) \Rightarrow (A \Rightarrow B_i))$ i dalje, ponovo na osnovu pravila MP, $\Gamma \vdash A \Rightarrow B_i$. Time je induktivni dokaz završen. □

Teorema 2.28 (Obrat teoreme o dedukciji) *Ako je Γ skup iskaznih formula, A i B su iskazne formule i ako važi $\Gamma \vdash A \Rightarrow B$, onda važi i $\Gamma, A \vdash B$.*

Dokaz: Iz $\Gamma \vdash A \Rightarrow B$, na osnovu teoreme 2.25(a), sledi $\Gamma, A \vdash A \Rightarrow B$. Iz $\Gamma, A \vdash A \Rightarrow B$ i $\Gamma, A \vdash A$, primenom pravila MP sledi $\Gamma, A \vdash B$. □

Primetimo da tvrđenje teoreme o dedukciji važi za svaku teoriju koja uključuje aksiomske sheme (A1) i (A2) i ima samo jedno pravilo izvođenja — pravilo MP.

Teoreme 2.27 i 2.28 predstavljaju deduktivni pandan teoreme 2.5.

Teorema 2.29

(a) $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$

(b) $A \Rightarrow (B \Rightarrow C), B \vdash A \Rightarrow C$.

Dokaz:

(a) Dokažimo najpre da važi $A \Rightarrow B, B \Rightarrow C, A \vdash C$.

1. $A \Rightarrow B$ (Hyp)
2. $B \Rightarrow C$ (Hyp)
3. A (Hyp)
4. B (1, 3, MP)
5. C (2, 4, MP)

Dakle, važi $A \Rightarrow B, B \Rightarrow C, A \vdash C$. Na osnovu teoreme o dedukciji, važi $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$.

(b) Dokažimo najpre da važi $A \Rightarrow (B \Rightarrow C), B, A \vdash C$.

1. $A \Rightarrow (B \Rightarrow C)$	(Hyp)
2. B	(Hyp)
3. A	(Hyp)
4. $B \Rightarrow C$	(1, 3, MP)
5. C	(2, 4, MP)

Dakle, važi $A \Rightarrow (B \Rightarrow C), B, A \vdash C$. Na osnovu teoreme o dedukciji, važi $A \Rightarrow (B \Rightarrow C), B \vdash A \Rightarrow C$.

□

Teoreme teorije L možemo da koristimo u okviru dokaza drugih formula. Strogo govoreći, pozivanje na određenu teoremu će označavati zamenu za prepisan dokaz te teoreme (za odgovarajuću njenu instancu). Slično, dokazana tvrđenja oblika $\Phi \vdash \Psi$ možemo koristiti kao dodatna pravila izvođenja.

Teorema 2.30 *Za bilo koje formule A i B, sledeće formule su teoreme teorije L:*

(a) $\neg\neg B \Rightarrow B$

(b) $B \Rightarrow \neg\neg B$

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

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

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

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

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

Dokaz:

(a)

1. $(\neg B \Rightarrow \neg\neg B) \Rightarrow ((\neg B \Rightarrow \neg B) \Rightarrow B)$	(A3)
2. $\neg B \Rightarrow \neg B$	(teorema 2.26)
3. $(\neg B \Rightarrow \neg\neg B) \Rightarrow B$	(1, 2, teorema 2.29(b))
4. $\neg\neg B \Rightarrow (\neg B \Rightarrow \neg\neg B)$	(A1)
5. $\neg\neg B \Rightarrow B$	(4, 3, teorema 2.29(a))

(b)

1. $(\neg\neg\neg B \Rightarrow \neg B) \Rightarrow ((\neg\neg\neg B \Rightarrow B) \Rightarrow \neg\neg B)$	(A3)
2. $\neg\neg\neg B \Rightarrow \neg B$	(deo (a))
3. $(\neg\neg\neg B \Rightarrow B) \Rightarrow \neg\neg B$	(2,1,MP)
4. $B \Rightarrow (\neg\neg\neg B \Rightarrow B)$	(A1)
5. $B \Rightarrow \neg\neg B$	(4, 3, teorema 2.29(a))

(c) Dokažimo najpre $\neg A, A \vdash B$.

1. $\neg A$	(Hyp)
2. A	(Hyp)
3. $A \Rightarrow (\neg B \Rightarrow A)$	(A1)
4. $\neg A \Rightarrow (\neg B \Rightarrow \neg A)$	(A1)
5. $\neg B \Rightarrow A$	(2, 3, MP)
6. $\neg B \Rightarrow \neg A$	(1, 4, MP)
7. $(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$	(A3)
8. $(\neg B \Rightarrow A) \Rightarrow B$	(6, 7, MP)
9. B	(5, 8, MP)

Dakle, važi $\neg A, A \vdash B$. Na osnovu teoreme o dedukciji onda važi i $\neg A \vdash (A \Rightarrow B)$ i dalje, takođe na osnovu teoreme o dedukciji $\vdash \neg A \Rightarrow (A \Rightarrow B)$, što je i trebalo dokazati.

(d) Dokažimo najpre $\neg B \Rightarrow \neg A, A \vdash B$.

1. $\neg B \Rightarrow \neg A$	(Hyp)
2. A	(Hyp)
3. $(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)$	(A3)
4. $A \Rightarrow (\neg B \Rightarrow A)$	(A1)
5. $(\neg B \Rightarrow A) \Rightarrow B$	(1, 3, MP)
6. $A \Rightarrow B$	(4, 5, 2.29(a))
7. B	(2, 6, MP)

Dakle, važi $\neg B \Rightarrow \neg A, A \vdash B$. Odatle, dvostrukom primenom teoreme o dedukciji dobijamo $\vdash (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$, što je i trebalo dokazati.

(e) Dokažimo najpre da važi $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$.

1. $A \Rightarrow B$	(Hyp)
2. $\neg\neg A \Rightarrow A$	(deo (a))
3. $\neg\neg A \Rightarrow B$	(2, 1, 2.29(a))
4. $B \Rightarrow \neg\neg B$	(deo (b))
5. $\neg\neg A \Rightarrow \neg\neg B$	(3, 4, 2.29(a))
6. $(\neg\neg A \Rightarrow \neg\neg B) \Rightarrow (\neg B \Rightarrow \neg A)$	(deo (d))
7. $\neg B \Rightarrow \neg A$	(5, 6, MP)

Dakle, važi $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$. Na osnovu teoreme o dedukciji, odatle sledi $\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$.

(f) Na osnovu pravila MP, važi $A, A \Rightarrow B \vdash B$. Odatle, na osnovu teoreme o dedukciji važi $\vdash A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$. Na osnovu dela (e), važi $\vdash ((A \Rightarrow B) \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$. Dakle, na osnovu teoreme 2.29(a), važi $\vdash A \Rightarrow (\neg B \Rightarrow \neg(A \Rightarrow B))$.

(g) Dokažimo najpre da važi $A \Rightarrow B, \neg A \Rightarrow B \vdash B$.

1. $A \Rightarrow B$	(Hyp)
2. $\neg A \Rightarrow B$	(Hyp)
3. $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$	(deo (e))
4. $\neg B \Rightarrow \neg A$	(1, 3, MP)
5. $(\neg A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg\neg A)$	(deo (e))
6. $\neg B \Rightarrow \neg\neg A$	(2, 5, MP)
7. $(\neg B \Rightarrow \neg\neg A) \Rightarrow ((\neg B \Rightarrow \neg A) \Rightarrow B)$	(A3)
8. $(\neg B \Rightarrow \neg A) \Rightarrow B$	(6, 7, MP)
9. B	(4, 8, MP)

Dakle, važi $A \Rightarrow B, \neg A \Rightarrow B \vdash B$. Na osnovu dvostruke primene teoreme o dedukciji, odatle sledi $\vdash (A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow B)$.

□

Teorema 2.31 *U teoriji L važi:*

(a) $\Gamma \vdash A$ *ako i samo ako* $\Gamma, \neg A \vdash \bot$

(b) $\Gamma \vdash \neg A$ *ako i samo ako* $\Gamma, A \vdash \bot$.

Dokaz:

(a) Pretpostavimo da važi $\Gamma \vdash A$. U teoriji L važi $\vdash A \Rightarrow (\neg A \Rightarrow \neg(A \Rightarrow A))$ (teorema 2.30(f)), pa i $\Gamma \vdash A \Rightarrow (\neg A \Rightarrow \neg(A \Rightarrow A))$ (na osnovu teoreme 2.25(a)). Odatle, iz $\Gamma \vdash A$ i na osnovu pravila MP sledi $\Gamma \vdash \neg A \Rightarrow \neg(A \Rightarrow A)$ i, dalje, $\Gamma, \neg A \vdash \neg(A \Rightarrow A)$ (teorema 2.28). Simbol $\bot$ je skraćeni zapis za formulu $\neg(A \Rightarrow A)$, te važi $\Gamma, \neg A \vdash \bot$, što je i trebalo dokazati.

Pretpostavimo da važi $\Gamma, \neg A \vdash \bot$. Na osnovu teoreme o dedukciji (teorema 2.27), važi $\Gamma \vdash \neg A \Rightarrow \bot$, tj. $\Gamma \vdash \neg A \Rightarrow \neg(A \Rightarrow A)$. Važi $\vdash (\neg A \Rightarrow \neg(A \Rightarrow A)) \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (teorema 2.30(d)), pa i $\Gamma \vdash (\neg A \Rightarrow \neg(A \Rightarrow A)) \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (na osnovu teoreme 2.25(a)). Odatle, i iz $\Gamma \vdash \neg A \Rightarrow \neg(A \Rightarrow A)$, na osnovu pravila MP, sledi $\Gamma \vdash (A \Rightarrow A) \Rightarrow A$. Važi $\vdash A \Rightarrow A$ (teorema 2.26) i $\Gamma \vdash A \Rightarrow A$ (na osnovu teoreme 2.25(a)), pa odatle i iz $\Gamma \vdash (A \Rightarrow A) \Rightarrow A$, na osnovu pravila MP, sledi $\Gamma \vdash A$, što je i trebalo dokazati.

(b) Dokažimo najpre da važi $\Gamma, A \vdash \bot$ ako samo ako $\Gamma, \neg\neg A \vdash \bot$. Pretpostavimo da važi $\Gamma, A \vdash \bot$. Važi $\vdash \neg\neg A \Rightarrow A$ (teorema 2.30(a)) i $\neg\neg A \vdash A$ (teorema 2.28), odakle se, na osnovu teoreme 2.25(a), dobija $\Gamma, \neg\neg A \vdash A$. Iz $\Gamma, \neg\neg A \vdash A$ i $\Gamma, A \vdash \bot$, na osnovu teoreme 2.25(c), sledi $\Gamma, \neg\neg A \vdash \bot$. Analogno se dokazuje da iz $\Gamma, \neg\neg A \vdash \bot$ sledi $\Gamma, A \vdash \bot$ (koristi se tvrđenje 2.30(b)).

Na osnovu dela (a), važi $\Gamma \vdash \neg A$ ako i samo ako $\Gamma, \neg\neg A \vdash \bot$. Dodatno, kao što je dokazano, važi $\Gamma, \neg\neg A \vdash \bot$ ako samo ako $\Gamma, A \vdash \bot$. Dakle, važi $\Gamma \vdash \neg A$ ako i samo ako važi $\Gamma, A \vdash \bot$.

□

Teorija L definisana je sa motivacijom da se izgradi formalna teorija u kojoj je svaka teorema tautologija i obratno. Naredne dve teoreme (o saglasnosti i o potpunosti[7]) govore da je to ispunjeno za teoriju L.

Teorema 2.32 (Saglasnost teorije L) *Ako je formula A teorema teorije L, onda je ona tautologija.*

Dokaz: Nije teško pokazati da su aksiome teorije L tautologije. Na osnovu teoreme 2.2, iz tautologija se, na osnovu pravila MP dobijaju ponovo tautologije. Dakle, svaka teorema teorije L je tautologija. □

Lema 2.4 (Kalmarova lema) *Neka je A iskazna formula i neka su p_1, p_2, ..., p_k iskazna slova koja se pojavljuju u formuli A. Neka je v neka valuacija za ta iskazna slova. Definišimo iskazne formule B_1, B_2, ..., B_k na sledeći način: neka je iskazna formula B_i jednaka p_i ako je $v(p_i) = 1$, a neka je jednaka $\neg p_i$ ako je $v(p_i) = 0$ ($1 \leq i \leq k$). Neka je iskazna formula A' jednaka A ako je $I_v(A) = 1$ i neka je jednaka $\neg A$ ako je $I_v(A) = 0$. Tada važi $B_1, B_2, \ldots, B_k \vdash A'$.*

Na primer, neka je A jednako $\neg(\neg p_1 \Rightarrow p_2)$. Tada svakoj vrsti istinitosne tablice

p_1	p_2	$\neg(\neg p_1 \Rightarrow p_2)$
0	0	1
0	1	0
1	0	0
1	1	0

odgovara po jedna relacija izvođenja. Na primer, trećoj vrsti odgovara tvrđenje $p_1, \neg p_2 \vdash \neg\neg(\neg p_1 \Rightarrow p_2)$.

Dokaz: Dokaz ćemo izvesti po složenosti n formule A (tj. po broju logičkih veznika koje formula A sadrži). Pretpostavljamo da formula A sadrži samo veznike $\Rightarrow$ i $\neg$ (tj. da ne koristi skraćenice koje smo definisali).

Ako je $n = 0$, onda je formula A jednaka nekom iskaznom slovu p, pa se tvrđenje leme svodi na $p \vdash p$ i $\neg p \vdash \neg p$, što trivijalno važi.

Pretpostavimo da tvrđenje leme važi za svaku vrednost j takvu da je $j < n$. Dokažimo onda da tvrđenje važi i za vrednost n.

[7] Smisao koncepata saglasnosti i potpunosti se unekoliko razlikuje za efektivne semantičke procedure i za deduktivne sisteme. Naime, na primer, potpunost za metod tabloa znači da se za svaku polaznu formulu koja je valjana, metod nužno zaustavlja i daje zatvoren tablo. S druge strane, potpunost za teoriju L znači da je ona okvir u kojem je *moguće* dokazati svaku valjanu formulu, ali nije specifikovan efektivan postupak koji to obezbeđuje.

Formula A je jednaka $\neg B$: Formula B je manje složenosti od formule A, pa za B važi induktivna pretpostavka (tj. važi $B_1, B_2, \ldots, B_k \vdash B'$).

U datoj valuaciji B ima vrednost 1: Formula A tada ima vrednost 0, pa je formula B' jednaka B, a formula A' jednaka $\neg A$. Na osnovu induktivne hipoteze, važi $B_1, B_2, \ldots, B_k \vdash B$, odakle, na osnovu teoreme 2.30(b) i pravila MP, sledi da važi $B_1, B_2, \ldots, B_k \vdash \neg\neg B$. Međutim, $\neg\neg B$ je jednako A', pa važi $B_1, B_2, \ldots, B_k \vdash A'$.

U datoj valuaciji B ima vrednost 0: Formula A tada ima vrednost 1, pa je formula B' jednaka $\neg B$, a formula A' jednaka A. Na osnovu induktivne hipoteze, važi $B_1, B_2, \ldots, B_k \vdash \neg B$. Međutim, $\neg B$ je jednako A', pa važi $B_1, B_2, \ldots, B_k \vdash A'$.

Formula A je jednaka $B \Rightarrow C$: Formule B i C su manje složenosti od formule A, pa za B i C važi induktivna pretpostavka (tj. važi $B_1, B_2, \ldots, B_k \vdash B'$ i $B_1, B_2, \ldots, B_k \vdash C'$).

U datoj valuaciji B ima vrednost 0: Formula A tada ima vrednost 1, pa je formula B' jednaka $\neg B$, a formula A' jednaka A. Na osnovu induktivne hipoteze, važi $B_1, B_2, \ldots, B_k \vdash \neg B$, odakle, na osnovu teoreme 2.30(c) i pravila MP, sledi da važi $B_1, B_2, \ldots, B_k \vdash B \Rightarrow C$. Međutim, $B \Rightarrow C$ je jednako A', pa važi $B_1, B_2, \ldots, B_k \vdash A'$.

U datoj valuaciji C ima vrednost 1: Formula A tada ima vrednost 1, pa je formula C' jednaka C i formula A' jednaka A. Na osnovu induktivne hipoteze, važi $B_1, B_2, \ldots, B_k \vdash C$. Na osnovu aksiome (A1), važi $\vdash C \Rightarrow (B \Rightarrow C)$, pa na osnovu pravila MP sledi $B_1, B_2, \ldots, B_k \vdash B \Rightarrow C$. Međutim, $B \Rightarrow C$ je jednako A', pa važi $B_1, B_2, \ldots, B_k \vdash A'$.

U datoj valuaciji B ima vrednost 1, a C vrednost 0: Formula A tada ima vrednost 0, pa je formula B' jednaka B, formula C' je jednaka $\neg C$ i formula A' je jednaka $\neg A$. Na osnovu induktivne hipoteze, važi $B_1, B_2, \ldots, B_k \vdash B$ i $B_1, B_2, \ldots, B_k \vdash \neg C$. Na osnovu teoreme 2.30(f) važi $\vdash B \Rightarrow (\neg C \Rightarrow \neg(B \Rightarrow C))$. Jednom primenom pravila MP, dobijamo $B_1, B_2, \ldots, B_k \vdash \neg C \Rightarrow \neg(B \Rightarrow C)$, a zatim, drugom primenom dobijamo $B_1, B_2, \ldots, B_k \vdash \neg(B \Rightarrow C)$. Međutim, $\neg(B \Rightarrow C)$ je jednako A', pa važi $B_1, B_2, \ldots, B_k \vdash A'$.

Kako je dokazan induktivni korak, sledi da tvrđenje leme važi za formulu proizvoljne složenosti, tj. važi za svaku iskaznu formulu A. □

Teorema 2.33 (Potpunost teorije L) *Ako je formula A tautologija, onda je ona teorema teorije L.*

Dokaz: Pretpostavimo da je A tautologija. Neka su $p_1, p_2, \ldots, p_k$ iskazna slova koja sadrži formula A. Za valuaciju v, ako je $v(p_i) = 1$, označimo sa B_i formulu p_i, a ako je $v(p_i) = 0$, označimo sa B_i formulu $\neg p_i$. Na osnovu leme 2.4, za svaku valuaciju v važi $B_1, B_2, \ldots, B_k \vdash A$ (A' je uvek jednako A, jer je A tautologija, pa u svakoj interpretaciji ima vrednost 1). Za svaku valuaciju v' takvu da je $v'(p_k) = 1$ važi $B_1, B_2, \ldots, B_{k-1}, p_k \vdash A$, odakle, na osnovu teoreme o dedukciji, sledi $B_1, B_2, \ldots, B_{k-1} \vdash p_k \Rightarrow A$. Za valuaciju v'' takvu da je $v''(p_i) = v'(p_i)$ za $i < k$ i $v''(p_k) = 0$ važi $B_1, B_2, \ldots, B_{k-1}, \neg p_k \vdash A$, odakle, na osnovu teoreme o dedukciji, sledi $B_1, B_2, \ldots, B_{k-1} \vdash \neg p_k \Rightarrow A$. Iz $B_1, B_2, \ldots, B_{k-1} \vdash p_k \Rightarrow A$ i $B_1, B_2, \ldots, B_{k-1} \vdash \neg p_k \Rightarrow A$, na osnovu teoreme 2.30(g) i dvostrukom primenom pravila MP, sledi $B_1, B_2, \ldots, B_{k-1} \vdash A$. Kako je valuacija v' proizvoljna (do na vrednost za p_k, koja ne utiče na $B_1, B_2, \ldots, B_{k-1}$), sledi da za proizvoljnu valuaciju važi $B_1, B_2, \ldots, B_{k-1} \vdash A$. Analogno, možemo eliminisati B_{k-1} i, redom, preostale formule B_i. Nakon k takvih koraka dobijamo da važi $\vdash A$, što je i trebalo dokazati. □

Teorema 2.34 *Ako formula B sadrži veznike $\neg, \Rightarrow, \wedge, \vee, \Leftrightarrow$ i ako je ona skraćeni zapis iskazne formule A teorije L, onda je B tautologija ako i samo ako je A teorema teorije L.*

Dokaz: Definicijama (D1), (D2) i (D3) formule se zamenjuju formulama koje su sa njima logički ekvivalentne (što je lako utvrditi). Na osnovu teoreme o zameni (2.9) važi da su A i B logički ekvivalentne. Dakle, B je tautologija ako i samo ako je A tautologija. Dodatno, na osnovu prethodne dve teoreme, formula A je tautologija ako i samo ako je A teorema teorije L, pa sledi da je B tautologija ako i samo ako je A teorema teorije L. □

Primetimo da teorema o saglasnosti i teorema o potpunosti teorije L govore o vezi između semantičke prirode i sintaksne (ili, preciznije, sintaksno-deduktivne) prirode neke iskazne formule. Ta veza može kratko biti zapisana i na sledeći način:

$$\models A \text{ ako i samo ako } \vdash_L A$$

Teorema 2.35 *Važi:*

$$\Gamma \models A \text{ ako i samo ako } \Gamma \vdash_L A$$

Dokaz: Pretpostavimo da je skup Γ konačan i neka je $\Gamma = \{B_1, B_2, \ldots, B_n\}$. Dakle, treba dokazati:

$$B_1, B_2, \ldots, B_n \models A \text{ ako i samo ako } B_1, B_2, \ldots, B_n \vdash A\,.$$

$$
\begin{array}{rcl}
B_1, B_2, \ldots, B_n & \models & A \\
 & & \text{ako i samo ako (na osnovu teoreme 2.5)} \\
B_1, B_2, \ldots, B_{n-1} & \models & B_n \Rightarrow A \\
 & & \text{ako i samo ako (na osnovu teoreme 2.5)} \\
B_1, B_2, \ldots, B_{n-2} & \models & B_{n-1} \Rightarrow (B_n \Rightarrow A) \\
 & & \text{ako i samo ako (na osnovu teoreme 2.5)} \\
 & \ldots & \\
 & & \text{ako i samo ako (na osnovu teoreme 2.5)} \\
B_1 & \models & B_2 \Rightarrow (B_3 \Rightarrow (\ldots (B_{n-1} \Rightarrow (B_n \Rightarrow A)) \ldots)) \\
 & & \text{ako i samo ako (na osnovu teoreme 2.5)} \\
 & \models & B_1 \Rightarrow (B_2 \Rightarrow (B_3 \Rightarrow (\ldots (B_{n-1} \Rightarrow (B_n \Rightarrow A)) \ldots))) \\
 & & \text{ako i samo ako (na osnovu teorema 2.32 i 2.33)} \\
 & \vdash & B_1 \Rightarrow (B_2 \Rightarrow (B_3 \Rightarrow (\ldots (B_{n-1} \Rightarrow (B_n \Rightarrow A)) \ldots))) \\
 & & \text{ako i samo ako (na osnovu teorema 2.27 i 2.28)} \\
B_1 & \vdash & B_2 \Rightarrow (B_3 \Rightarrow (\ldots (B_{n-1} \Rightarrow (B_n \Rightarrow A)) \ldots)) \\
 & & \text{ako i samo ako (na osnovu teorema 2.27 i 2.28)} \\
 & \ldots & \\
 & & \text{ako i samo ako (na osnovu teorema 2.27 i 2.28)} \\
B_1, B_2, \ldots, B_{n-2} & \vdash & B_{n-1} \Rightarrow (B_n \Rightarrow A) \\
 & & \text{ako i samo ako (na osnovu teorema 2.27 i 2.28)} \\
B_1, B_2, \ldots, B_{n-1} & \vdash & B_n \Rightarrow A \\
 & & \text{ako i samo ako (na osnovu teorema 2.27 i 2.28)} \\
B_1, B_2, \ldots, B_n & \vdash & A
\end{array}
$$

Pretpostavimo da je skup Γ beskonačan. Ako važi $\Gamma \models A$, na osnovu teoreme 2.24 postoji konačan podskup Δ skupa Γ, takav da je $\Delta \models A$. Na osnovu dokazanog u prethodnom delu važi $\Delta \vdash A$, a odatle (i iz $\Delta \subset \Gamma$) sledi $\Gamma \vdash A$. Ako važi $\Gamma \vdash A$, dokaz formule A iz premisa Γ (kao konačan niz) uključuje samo konačno mnogo elemenata skupa Γ. Neka je Δ skup svih tih formula. Tada važi $\Delta \vdash A$, pa na osnovu dokazanog u prethodnom delu važi $\Delta \models A$. Iz $\Delta \models A$ i $\Delta \subset \Gamma$ sledi $\Gamma \models A$, što je i trebalo dokazati. □

Teorema 2.36 *Teorija L je odlučiva.*

Dokaz: Za svaku iskaznu formulu može se efektivno proveriti da li je tautologija (npr. metodom istinitosnih tablica). Kako je iskazna formula teorema teorije L ako i samo ako je tautologija, sledi da se za svaku iskaznu

formulu može efektivno proveriti da li je teorema teorije L. To znači da je teorija L odlučiva. □

Teorema 2.37 (Konzistentnost teorije L) *Teorija L je konzistentna (neprotivrečna) tj. ne postoji iskazna formula A takva da su i A i $\neg A$ teoreme teorije L.*

Dokaz: Iskazna formula je teorema teorije L ako i samo ako je tautologija. Ne postoji formula A takva da su i A i $\neg A$ tautologije. Odatle sledi da ne postoji formula A takva da su i A i $\neg A$ teoreme teorije L. □

Može se dokazati da je svaka od shema aksioma (A1), (A2), (A3) nezavisna, tj. ne može biti dokazana na osnovu preostale dve sheme aksioma. To dalje znači da ovaj skup shema aksioma ne može da se smanji, a da pri tom zadrži svojstvo potpunosti (videti npr. [48]).

Teorija L je samo jedan od sistema u Hilbertovom stilu (ili preciznije u Frege-Hilbertovom stilu). Navedimo za ilustraciju još jedan sistem (formulisan od strane Hilberta i Akermana): osnovni veznici su $\vee$ i $\neg$, postoji samo jedno pravilo izvođenja (MP) i sledeće četiri aksiomske sheme ($A \Rightarrow B$ je skraćeni zapis za $\neg A \vee B$):

(1) $A \vee A \Rightarrow A$
(2) $A \Rightarrow A \vee B$
(3) $A \vee B \Rightarrow B \vee A$
(4) $(B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow A \vee C)$

Postoje i sistemi Hilbertovog tipa za intuicionističku logiku (videti potpoglavlje B.2.3), kao i varijante za klasičnu i intuicionističku logiku koje se razlikuju samo po tome što prvi sistem (za razliku od drugog) uključuje aksiomu $A \vee \neg A$ (videti npr. [21]).

Zadaci

Zadatak 35 *Dokazati sledeća tvrđenja (ne koristeći teoremu o dedukciji):*
(a) $\vdash_L (\neg A \Rightarrow A) \Rightarrow A$
(b) $A \Rightarrow B, B \Rightarrow C \vdash_L A \Rightarrow C$
(c) $A \Rightarrow (B \Rightarrow C) \vdash_L B \Rightarrow (A \Rightarrow C)$
(d) $\vdash_L (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$

Zadatak 36 *Dokazati da su sledeće formule teoreme teorije L:*
(a) $((A \vee B) \wedge (A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow C$
(b) $A \Rightarrow (B \Rightarrow C) \Leftrightarrow (A \wedge B) \Rightarrow C$

Zadatak 37 *Dokazati da su sledeće formule teoreme teorije L:*
(a) $(\neg A \Rightarrow A) \Rightarrow A$
(b) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
(c) $A \Rightarrow (B \Rightarrow (A \wedge B))$

Zadatak 38 *Dokazati da u teoriji L važi:*
(a) $\neg B \Rightarrow \neg A \vdash A \Rightarrow B$ *(pravilo kontrapozicije)*
(b) $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$ *(inverzno pravilo kontrapozicije)*
(c) $\neg\neg A \vdash A$ *(pravilo dvostruke negacije)*
(d) $A, B \vdash A \wedge B$ *($\wedge$-uvođenje)*
(e) $B \vdash A \vee B$ *($\vee$-uvođenje)*
(f) $A \wedge B \vdash A$ *($\wedge$-eliminacija)*
(g) $A \wedge B \vdash B \wedge A$ *(pravilo komutativnosti za $\wedge$)*
(h) $A \wedge (B \wedge C) \vdash (A \wedge B) \wedge C$ *(pravilo asocijativnosti za $\wedge$)*
(i) $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$ *(pravilo distributivnosti)*
(j) $\neg(A \vee B) \vdash \neg A \wedge \neg B$ *(De Morganov zakon)*
(k) $\vdash A \vee \neg A$ *(zakon isključenja trećeg)*
(l) $\vdash \neg(A \wedge \neg A)$ *(zakon isključenja čuda)*
(m) $\neg A \Rightarrow B, \neg A \Rightarrow \neg B \vdash A$ *(dokaz pobijanjem)*
(n) $A \Rightarrow B, \neg A \Rightarrow B \vdash B$ *(dokaz po slučajevima)*

Zadatak 39 *Dokazati da se aksiomska shema (A3) može zameniti shemom* $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$ *i da se pri tom ne promeni skup teorema teorije* L.

2.3.2 Prirodna dedukcija

Sistem prirodne dedukcije (račun prirodne dedukcije) uveo je, 1935. godine, Gerhard Gencen sa namerom da prirodnije opiše uobičajeno zaključivanje matematičara [21].

U prirodnoj dedukciji koriste se logički veznici[8] $\neg$, $\wedge$, $\vee$, $\Rightarrow$, kao i logička konstanta $\bot$. Formula $A \Leftrightarrow B$ je kraći zapis za $(A \Rightarrow B) \wedge (B \Rightarrow A)$, a formula $\top$ kraći zapis za $A \Rightarrow A$. Skup iskaznih formula definiše se na uobičajeni način.

Postoje sistemi prirodne dedukcije za klasičnu i za intuicionističku logiku.

Pravila izvođenja sistema prirodne dedukcije (za obe logike) data su u tabeli 2.1. Primetimo da za svaki logički veznik postoje pravila koja ga uvode (pravila I-tipa) i pravila koja ga eliminišu (pravila E-tipa). Pravilo efq (*Ex falso quodlibet*) je jedino pravilo koje ne uvodi niti eliminiše neki logički veznik.

U sistemu prirodne dedukcije za klasičnu logiku postoji i jedna aksiomska shema: $A \vee \neg A$ (*tertium non datur*). U sistemu prirodne dedukcije za intuicionističku logiku nema aksioma. Ovakva razlika između ova dva sistema je prirodna i dobro oslikava razliku između klasične i intuicionističke logike. U daljem tekstu će se, ako nije drugačije naglašeno, pod „sistem prirodne dedukcije“ misliti na oba sistema prirodne dedukcije — i na sistem za klasičnu i na sistem za intuicionističku logiku.

Tokom izvođenja dokaza u sistemu prirodne dedukcije mogu se koristiti (nedokazane) pretpostavke, ali one moraju biti eliminisane („oslobođene“) pre kraja izvođenja. U zapisu pravila, $[F]$ označava da se nekoliko (možda i nula)

[8] Iz sistema prirodne dedukcije moguće je eliminisati veznik $\neg$ smatrajući formulu $\neg A$ skraćenim zapisom za $A \Rightarrow \bot$.

pojavljivanja pretpostavke F oslobađa, briše (kao nedokazane, neraspoložive pretpostavke) neposredno nakon primene pravila. Pri tome, može ostati i nekoliko neoslobođenih pojavljivanja pretpostavke F. Pretpostavkama su pridružene oznake (obično prirodni brojevi), koje se zapisuju i u okviru zapisa primenjenog pravila (kako bi se znalo koja pretpostavka je oslodođena u kom koraku).

$$\frac{\begin{array}{c}[A]^u\\ \vdots\\ \bot\end{array}}{\neg A}\ \neg I, u \qquad \frac{A \quad \neg A}{\bot}\ \neg E$$

$$\frac{A \quad B}{A \wedge B}\ \wedge I \qquad \frac{A \wedge B}{A}\ \wedge E \qquad \frac{A \wedge B}{B}\ \wedge E$$

$$\frac{A}{A \vee B}\ \vee I \qquad \frac{B}{A \vee B}\ \vee I \qquad \frac{A \vee B \quad \begin{array}{c}[A]^u\\ \vdots\\ C\end{array} \quad \begin{array}{c}[B]^v\\ \vdots\\ C\end{array}}{C}\ \vee E, u, v$$

$$\frac{\begin{array}{c}[A]^u\\ \vdots\\ B\end{array}}{A \Rightarrow B}\ \Rightarrow I, u \qquad \frac{A \quad A \Rightarrow B}{B}\ \Rightarrow E$$

$$\frac{\bot}{D}\ efq$$

Tabela 2.1: Pravila izvođenja sistema prirodne dedukcije

U sistemu prirodne dedukcije *dokaz* (*dedukcija*, *izvod*) je stablo čijem je svakom čvoru pridružena formula i koje zadovoljava sledeće uslove:

- stablo sa jednim čvorom kojem je pridružena aksioma je dokaz; u tom dokazu nema neoslobođenih pretpostavki;
- stablo sa jednim čvorom kojem je pridružena formula A (koja nije instanca aksiomske sheme) je dokaz; u tom dokazu neoslobođena pretpostavka je formula A;
- ako su $\mathcal{D}_1, \ldots, \mathcal{D}_n$ dokazi sa korenima kojima su pridružene redom formule $A_1, \ldots, A_n$ i ako je formula A direktna posledica formula $A_1, \ldots, A_n$ na osnovu nekog od pravila izvođenja $\neg E$, $\wedge I$, $\Rightarrow E$ (tada je $n = 2$) ili $\wedge E$, $\vee I$, efq (tada je $n = 1$), onda je dokaz i stablo u čijem je korenu A, a čiji su direktni potomci koreni stabala $\mathcal{D}_1, \ldots, \mathcal{D}_n$; u tom dokazu neoslobođene pretpostavke su sve pretpostavke neoslobođene u dokazima $\mathcal{D}_1, \ldots, \mathcal{D}_n$;

- ako je $\mathcal{D}$ dokaz sa korenom kojem je pridružena formula $\bot$ i koji sadrži nula ili više neoslobođenih pretpostavki A, onda je dokaz i stablo (dobijeno primenom pravila $\neg I$) sa korenom $\neg A$ čiji je direktni potomak koren stabla $\mathcal{D}$; u tom dokazu neoslobođene pretpostavke su sve neoslobođene pretpostavke u dokazu $\mathcal{D}$, osim nekoliko (ne nužno svih) neoslobođenih pretpostavki A (koje ovim korakom postaju oslobođene);

- ako je $\mathcal{D}$ dokaz sa korenom kojem je pridružena formula B i koji sadrži nula ili više neoslobođenih pretpostavki A, onda je dokaz i stablo (dobijeno primenom pravila $\Rightarrow I$) sa korenom $A \Rightarrow B$ čiji je direktni potomak koren stabla $\mathcal{D}$; u tom dokazu neoslobođene pretpostavke su sve neoslobođene pretpostavke u dokazu $\mathcal{D}$, osim nekoliko (ne nužno svih) neoslobođenih pretpostavki A (koje ovim korakom postaju oslobođene);

- ako je $\mathcal{D}_1$ dokaz sa korenom kojem je pridružena formula $A \vee B$, ako je $\mathcal{D}_2$ dokaz sa korenom kojem je pridružena formula C i koji sadrži nula ili više neoslobođenih pretpostavki A i ako je $\mathcal{D}_3$ dokaz sa korenom kojem je pridružena formula C i koji sadrži nula ili više neoslobođenih pretpostavki B, onda je dokaz i stablo (dobijeno primenom pravila $\vee E$) sa korenom C čiji su direktni potomci koreni stabala $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{D}_3$; u tom dokazu neoslobođene pretpostavke su sve neoslobođene pretpostavke u dokazu $\mathcal{D}_1$, zatim sve neoslobođene pretpostavke u dokazu $\mathcal{D}_2$, osim nekoliko (ne nužno svih) neoslobođenih pretpostavki A (koje ovim korakom postaju oslobođene), kao i sve neoslobođene pretpostavke u dokazu $\mathcal{D}_3$, osim nekoliko (ne nužno svih) neoslobođenih pretpostavki B (koje ovim korakom postaju oslobođene).

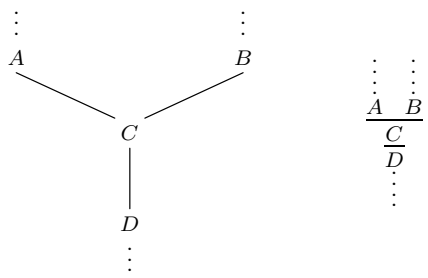
Formula A je *teorema* prirodne dedukcije ako postoji dokaz u čijem je korenu A i koji nema neoslobođenih pretpostavki i tada pišemo $\vdash A$ i kažemo da je formula A *dokaziva* u sistemu prirodne dedukcije. Ako postoji dokaz, u čijem je korenu formula A i koji ima neoslobođene pretpostavke koje pripadaju nekom nizu Γ, onda kažemo da je formula A *deduktivna posledica* niza Γ i tada pišemo $\Gamma \vdash A$. Elemente niza Γ tada zovemo i *premisama* ili *hipotezama* dokaza. Ako je niz Γ jednak $B_1, B_2, \ldots, B_n$, onda pišemo $B_1, B_2, \ldots, B_n \vdash A$.

Za relaciju $\vdash$ u sistemu prirodne dedukcije važe ista svojstva kao za relaciju $\vdash$ u teoriji L (videti teoremu 2.25).

Dokaz u sistemu prirodne dedukcije se obično prikazuje u vidu stabla čiji su listovi na vrhu, a koren na dnu. To stablo se prikazuje pojednostavljeno, stilizovano (videti sliku 2.7).

Primer 2.14 *Formula* $(A \vee B) \Rightarrow (B \vee A)$ *je teorema sistema prirodne dedukcije (i za intuicionističku i za klasičnu logiku), tj. važi* $\vdash (A \vee B) \Rightarrow (B \vee A)$ *:*

$$\dfrac{\dfrac{[A \vee B]^1 \quad \dfrac{[A]^2}{B \vee A} \vee I \quad \dfrac{[B]^3}{B \vee A} \vee I}{B \vee A} \vee E, 2, 3}{(A \vee B) \Rightarrow (B \vee A)} \Rightarrow I, 1$$



Slika 2.7: Deo dokaza i njegov pojednostavljeni prikaz

Primer 2.15 *U sistemu prirodne dedukcije (i za intuicionističku i za klasičnu logiku) važi* $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$*:*

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \Rightarrow B}{B} \Rightarrow E \qquad B \Rightarrow C}{C} \Rightarrow E}{A \Rightarrow C} \Rightarrow I, 1$$

Primer 2.16 *U sistemu prirodne dedukcije (i za intuicionističku i za klasičnu logiku) važi* $\vdash A \Rightarrow (A \vee B) \wedge (A \vee C)$*:*

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]^1}{A \vee B} \vee I \quad \dfrac{[A]^1}{A \vee C} \vee I}{(A \vee B) \wedge (A \vee C)} \wedge I}{A \Rightarrow (A \vee B) \wedge (A \vee C)} \Rightarrow I, 1$$

U prethodnom dokazu, primenom pravila $\Rightarrow I$ *nisu morala da budu oslobođena sva pojavljivanja pretpostavke* A*. Na primer:*

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]^1}{A \vee B} \vee I \quad \dfrac{A}{A \vee C} \vee I}{(A \vee B) \wedge (A \vee C)} \wedge I}{A \Rightarrow (A \vee B) \wedge (A \vee C)} \Rightarrow I, 1$$

Ovaj dokaz je dokaz tvrđenja $A \vdash A \Rightarrow (A \vee B) \wedge (A \vee C)$ *(što je slabije tvrđenje od tvrđenja* $\vdash A \Rightarrow (A \vee B) \wedge (A \vee C)$*).*

Teorema 2.38 *Ako je iskazna formula teorema teorije* L*, onda je ona teorema i sistema prirodne dedukcije za klasičnu logiku.*

Dokaz: Neka je formula A teorema teorije L. U teoriji L postoji dokaz formule A — niz formula $B_1, B_2, \ldots, B_n = A$. Svaka od formula B_i je ili aksioma teorije L ili je dobijena od prethodnih formula u nizu primenom pravila

MP. Dokažimo matematičkom indukcijom da je svaka od formula B_i ($i = 1, 2, \ldots, n$) teorema sistema prirodne dedukcije za klasičnu logiku.

Formula B_1 je aksioma teorije L. Za svaku od aksioma teorije L može se dokazati da je teorema sistema prirodne dedukcije za klasičnu logiku:

$$\dfrac{\dfrac{[A]^1}{B \Rightarrow A} \Rightarrow I}{A \Rightarrow (B \Rightarrow A)} \Rightarrow I, 1$$

(U prethodnom dokazu, formula $B \Rightarrow A$ je izvedena pravilom $\Rightarrow I$ iz formule A i na osnovu *nula* pretpostavki B; zbog toga u oznaci primenjenog pravila ne piše oznaka pretpostavke.)

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]^1 \quad [A \Rightarrow B]^2}{B} \Rightarrow E \quad \dfrac{[A]^1 \quad [A \Rightarrow (B \Rightarrow C)]^3}{B \Rightarrow C} \Rightarrow E}{C} \Rightarrow E}{A \Rightarrow C} \Rightarrow I, 1}{(A \Rightarrow B) \Rightarrow (A \Rightarrow C)} \Rightarrow I, 2}{(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))} \Rightarrow I, 3$$

$$\dfrac{\dfrac{\dfrac{B \vee \neg B \quad [B]^1 \quad \dfrac{\dfrac{[\neg B]^2 \quad [\neg B \Rightarrow A]^3}{A} \Rightarrow E \quad \dfrac{[\neg B]^2 \quad [\neg B \Rightarrow \neg A]^4}{\neg A} \Rightarrow E}{\bot}\neg E}{B}\, efq}{B} \vee E, 1, 2}{(\neg B \Rightarrow A) \Rightarrow B} \Rightarrow I, 3}{(\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B)} \Rightarrow I, 4$$

Kako je svaka od aksioma teorije L teorema sistema prirodne dedukcije za klasičnu logiku, sledi da navedeno tvrđenje važi za B_1.

Pretpostavimo da tvrđenje važi za sve formule B_k za $k < i$ i dokažimo da važi i za B_i. Ako je formula B_i aksioma teorije L, onda je ona, kao što je to pokazano, teorema sistema prirodne dedukcije za klasičnu logiku. Ako je B_i direktna posledica (u okviru teorije L) nekih formula B_j i B_m (gde je $j < i$ i $m < i$) na osnovu pravila MP, onda je B_m oblika $B_j \Rightarrow B_i$. Na osnovu induktivne pretpostavke, formule B_j i $B_j \Rightarrow B_i$ su teoreme sistema prirodne dedukcije za klasičnu logiku, pa postoji dokaz $\mathcal{D}_1$ sa korenom kojem je pridružena formula B_j, kao i dokaz $\mathcal{D}_2$ sa korenom kojem je pridružena formula $B_j \Rightarrow B_i$. Tada je dokaz i stablo (dobijeno primenom pravila $\Rightarrow E$) sa korenom B_i čiji su direktni potomci koreni stabala $\mathcal{D}_1$ i $\mathcal{D}_2$. Dakle, i formula B_i je teorema sistema prirodne dedukcije za klasičnu logiku, čime je dokazan induktivni korak.

Tvrđenje važi i za $i = n$, pa je formula A teorema sistema prirodne dedukcije za klasičnu logiku, što je i trebalo dokazati. □

Primer 2.17 *Dokaz formule $A \Rightarrow A$ u teoriji L:*

1. $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ *(A2)*
2. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ *(A1)*
3. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ *(1, 2, MP)*
4. $A \Rightarrow (A \Rightarrow A)$ *(A1)*
5. $A \Rightarrow A$ *(3, 4, MP)*

može, na osnovu postupka opisanog u dokazu teoreme 2.38, biti transformisan u dokaz ove formule u sistemu prirodne dedukcije:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]^1 \quad \dfrac{[A \Rightarrow (A \Rightarrow A)]^2}{(A \Rightarrow A)} \Rightarrow E}{\dfrac{A}{A \Rightarrow A} \Rightarrow I, 1} \Rightarrow I, 2}{(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)} \Rightarrow I, 3 \quad \dfrac{\dfrac{[A]^1 \quad \dfrac{[A \Rightarrow ((A \Rightarrow A) \Rightarrow A)]^3}{(A \Rightarrow A) \Rightarrow A} \Rightarrow E}{A} \Rightarrow E}{(A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)} \Rightarrow E \quad \dfrac{\dfrac{[A]^4}{(A \Rightarrow A) \Rightarrow A} \Rightarrow I}{A \Rightarrow ((A \Rightarrow A) \Rightarrow A)} \Rightarrow I, 4}{A \Rightarrow A} \Rightarrow E \quad \dfrac{\dfrac{[A]^5}{A \Rightarrow A} \Rightarrow I}{A \Rightarrow (A \Rightarrow A)} \Rightarrow I, 5}{A \Rightarrow A} \Rightarrow E$$

Naravno, dokaz formule u sistemu prirodne dedukcije dobijen transformisanjem dokaza te formule u teoriji L često nije elegantan i optimalan. Na primer, formula $A \Rightarrow A$ se u sistemu prirodne dedukcije, sem na navedeni način, može dokazati i znatno kraće:

$$\dfrac{[A]^1}{A \Rightarrow A} \Rightarrow I, 1$$

U narednom poglavlju biće uveden račun sekvenata i biće dokazana tvrđenja: ako je iskazna formula teorema sistema prirodne dedukcije za klasičnu logiku, onda je ona teorema i računa sekvenata za klasičnu logiku; ako je iskazna formula teorema računa sekvenata za klasičnu logiku, onda je ona i teorema teorije L. Odatle, i iz teoreme 2.38, sledi da su ova tri sistema ekvivalentna. Slično se dokazuje i da važi $\Gamma \vdash A$ u teoriji L ako i samo ako $\Gamma \vdash A$ važi u sistemu prirodne dedukcije. Iz potpunosti i saglasnosti teorije L (u odnosu na semantiku) sledi potpunost i saglasnost prirodne dedukcije za klasičnu logiku, tj. u sistemu prirodne dedukcije za klasičnu logiku važi $\Gamma \vdash A$ ako i samo ako važi $\Gamma \models A$ (gde je Γ konačan niz formula).

Zadaci

Zadatak 40 $\surd$ *Dokazati da u prirodnoj dedukciji važi $A \vee B, \neg A \vdash B$.*

Zadatak 41 $\surd$ *Dokazati da je formula $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ teorema sistema prirodne dedukcije za klasičnu logiku.*

Zadatak 42 $\surd$ *Dokazati da je formula $(A \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge (A \vee C))$ teorema sistema prirodne dedukcije za klasičnu logiku.*

Zadatak 43 $\surd$ *Dokazati da je formula $\neg(A \wedge B) \Rightarrow (\neg A \vee \neg B)$ teorema sistema prirodne dedukcije za klasičnu logiku.*

2.3.3 Račun sekvenata

Račun sekvenata uveo je Gerhard Gencen 1935. godine [21]. Ovaj deduktivni sistem je važan jer je imao i ima veoma veliki uticaj na čitavu teoriju dokaza i, posebno, na sisteme za dedukciju koji su pogodni za korišćenje u automatskom dokazivanju teorema.

Osnovni logički veznici su $\neg$, $\wedge$, $\vee$ i $\Rightarrow$. Skup iskaznih formula definiše se na uobičajeni način. Formula $A \Leftrightarrow B$ je kraći zapis za $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Formula $\bot$ je kraći zapis za $A \wedge \neg A$, a formula $\top$ za $A \Rightarrow A$.

U računu sekvenata, osnovni objekti u izvođenju su *sekventi*. Svaki sekvent je oblika

$$A_1, A_2, \ldots, A_m \vdash B_1, B_2, \ldots, B_n$$

pri čemu je $m \geq 0$, $n \geq 0$. Simbol $\vdash$ nije logički veznik, već pomoćni simbol, kao što je i zarez. Neformalno, sekvent $A_1, A_2, \ldots, A_m \vdash B_1, B_2, \ldots, B_n$ ima značenje kao formula $A_1 \wedge A_2 \wedge \ldots \wedge A_m \Rightarrow B_1 \vee B_2 \vee \ldots \vee B_n$. Ako je $m = 0$, onda, neformalno, sekvent $\vdash B_1, B_2, \ldots, B_n$ ima značenje kao formula $B_1 \vee B_2 \vee \ldots \vee B_n$. Ako je $n = 0$, onda, neformalno, sekvent $A_1, A_2, \ldots, A_m \vdash$ ima značenje kao formula $\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_m)$. Ako je $m = 0$ i $n = 0$, onda, neformalno, sekvent $\vdash$ ima značenje kao $\bot$. Obratno, za svaku formulu A postoji sekvent koji joj odgovara — sekvent $\vdash A$.

Postoji račun sekvenata za klasičnu logiku i račun sekvenata za intuicionističku logiku. Račun sekvenata za intuicionističku logiku karakterisan je time što je dozvoljeno korišćenje samo sekvenata oblika $A_1, A_2, \ldots, A_m \vdash B$ ili oblika $A_1, A_2, \ldots, A_m \vdash$. Ovakva karakterizacija računa sekvenata za klasičnu i za intuicionističku logiku, karakterizacija zasnovana na formi sekvenata, veoma je pogodna za poređenje snaga ova dva sistema. U daljem tekstu će se, ako nije drugačije naglašeno, pod računom sekvenata misliti na oba računa sekvenata — i na račun za klasičnu i na račun za intuicionističku logiku.

Pravila izvođenja računa sekvenata data su u tabelama 2.2 (strukturalna pravila) i 2.3 (operaciona pravila). Primetimo da za svaki logički veznik postoje (operaciona) pravila koja ga uvode sa leve i sa desne strane simbola $\vdash$. Primetimo i da se neka od navedenih pravila ne mogu koristiti u računu sekvenata za intuicionističku logiku (jer uključuju sekvente oblika $A_1 \wedge A_2 \wedge \ldots \wedge A_m \Rightarrow B_1 \vee B_2 \vee \ldots \vee B_n$, gde je nužno $n > 1$), dok se neka pravila mogu koristiti samo u specijalnom obliku. Na primer, u računu sekvenata za intuicionističku logiku ne može se koristiti pravilo

$$\frac{\Gamma \vdash \Theta, D, D}{\Gamma \vdash \Theta, D}$$

dok se pravilo $\Rightarrow R$ može koristiti samo u specijalnom obliku:

$$\frac{A, \Gamma \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow R$$

U računu sekvenata (i za intuicionističku i za klasičnu logiku) postoji samo jedna aksiomska shema — $A \vdash A$ (id) (koju zovemo i *inicijalni sekvent*).

Slabljenje, sužavanje (weakining, thinning)	$\dfrac{\Gamma \vdash \Theta}{D, \Gamma \vdash \Theta}$	$\dfrac{\Gamma \vdash \Theta}{\Gamma \vdash \Theta, D}$
Kontrakcija (contraction)	$\dfrac{D, D, \Gamma \vdash \Theta}{D, \Gamma \vdash \Theta}$	$\dfrac{\Gamma \vdash \Theta, D, D}{\Gamma \vdash \Theta, D}$
Zamena, permutacija (interchange, permutation)	$\dfrac{\Delta, E, D, \Gamma \vdash \Theta}{\Delta, D, E, \Gamma \vdash \Theta}$	$\dfrac{\Gamma \vdash \Theta, E, D, \Lambda}{\Gamma \vdash \Theta, D, E, \Lambda}$
Sečenje (cut)	$\dfrac{\Gamma \vdash \Theta, D \quad D, \Delta \vdash \Lambda}{\Gamma, \Delta \vdash \Theta, \Lambda}$	

Tabela 2.2: Strukturalna pravila izvođenja računa sekvenata

$$\frac{\Gamma \vdash \Theta, A}{\neg A, \Gamma \vdash \Theta}\ \neg L \qquad \frac{A, \Gamma \vdash \Theta}{\Gamma \vdash \Theta, \neg A}\ \neg R$$

$$\frac{A, \Gamma \vdash \Theta}{A \wedge B, \Gamma \vdash \Theta}\ \wedge L \quad \frac{B, \Gamma \vdash \Theta}{A \wedge B, \Gamma \vdash \Theta}\ \wedge L \qquad \frac{\Gamma \vdash \Theta, A \quad \Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \wedge B}\ \wedge R$$

$$\frac{A, \Gamma \vdash \Theta \quad B, \Gamma \vdash \Theta}{A \vee B, \Gamma \vdash \Theta}\ \vee L \qquad \frac{\Gamma \vdash \Theta, A}{\Gamma \vdash \Theta, A \vee B}\ \vee R \quad \frac{\Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \vee B}\ \vee R$$

$$\frac{\Gamma \vdash \Theta, A \quad B, \Delta \vdash \Lambda}{A \Rightarrow B, \Gamma, \Delta \vdash \Theta, \Lambda}\ \Rightarrow L \qquad \frac{A, \Gamma \vdash \Theta, B}{\Gamma \vdash \Theta, A \Rightarrow B}\ \Rightarrow R$$

Tabela 2.3: Operaciona pravila izvođenja računa sekvenata

Dokaz (*dedukcija*, *izvod*) u računu sekvenata je stablo čijim su čvorovima pridruženi sekventi i koje zadovoljava sledeće uslove:

- stablo sa jednim čvorom kojem je pridružena aksioma je dokaz;
- ako su $\mathcal{D}_1$, ..., $\mathcal{D}_n$ dokazi sa korenima kojima su pridruženi redom sekventi $s_1, \ldots, s_n$ i ako je sekvent s direktna posledica sekvenata $s_1, \ldots, s_n$ na osnovu nekog od pravila izvođenja (n je jednako 1 ili 2), onda je dokaz i stablo u čijem je korenu s, a čiji su direktni potomci koreni stabala $\mathcal{D}_1$, ..., $\mathcal{D}_n$.

Sekvent s je *dokaziv* ako postoji dokaz u čijem je korenu s. Ako je dokaziv sekvent $\vdash A$, onda kažemo da je formula A *teorema* računa sekvenata i da je *dokaziva* u računu sekvenata. Ako je dokaziv sekvent $\Gamma \vdash A$, onda kažemo da je formula A deduktivna posledica niza Γ, čije elemente zovemo *premisama* ili *hipotezama* dokaza. Ako je niz Γ jednak $B_1, B_2, \ldots, B_n$, onda pišemo $B_1, B_2, \ldots, B_n \vdash A$.

Za relaciju $\vdash$ u računu sekvenata važe ista svojstva kao za relaciju $\vdash$ u teoriji L (videti teoremu 2.25).

Kao u sistemu prirodne dedukcije, dokaz u računu sekvenata se obično prikazuje u vidu pojednostavljenog, stilizovanog stabla čiji su listovi na vrhu, a koren na dnu.

Gencenova teorema *Hauptsatz* (teorema o elimisanju sečenja) tvrdi da svaka teorema računa sekvenata može biti dokazana i u ovom sistemu bez pravila sečenja. U računu sekvenata bez sečenja važi *svojstvo potformule*. To znači da svaka formula koja se pojavljuje u premisama nekog pravila mora da se pojavljuje i u njegovom zaključku (što ne važi za *formulu sečenja* — za formulu D u pravilu sečenja). Jedna od važnih posledica tvrđenja o eliminaciji sečenja je *pojačano svojstvo potformule*: svaka formula koja se pojavljuje u dokazu nekog sekventa mora da se pojavljuje u samom tom sekventu. Svojstvo potformule garantuje da u dokazivanju zadate formule postoji konačno mnogo mogućnosti (tj. grana u prostoru pretrage) kada se pravila računa sekvenata bez sečenja primenjuju unazad. Invertovanjem pravila izvođenja računa sekvenata dobija se sistem izvođenja *analitičkog* tipa jer funkcioniše na principu raščlanjivanja date formule na njene potformule. Taj sistem izvođenja veoma je pogodan za automatsku primenu, za primenu u automatskom dokazivanju teorema, jer je u svakom koraku postupka dokazivanja dovoljno razmotriti konačno mnogo opcija za izbor pogodne instance pravila izvođenja.

Primer 2.18 *Formula* $((A \vee B) \wedge \neg A) \Rightarrow B$ *je teorema računa sekvenata za klasičnu logiku:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A, B}\, slabljenje}{A \vdash B, A}\, zamena \qquad \dfrac{B \vdash B}{B \vdash B, A}\, slabljenje}{A \vee B \vdash B, A}\, \vee L}{(A \vee B) \wedge \neg A \vdash B, A}\, \wedge L}{\neg A, (A \vee B) \wedge \neg A \vdash B}\, \neg L}{(A \vee B) \wedge \neg A, (A \vee B) \wedge \neg A \vdash B}\, \wedge L}{(A \vee B) \wedge \neg A \vdash B}\, kontrakcija}{\vdash ((A \vee B) \wedge \neg A) \Rightarrow B}\, \Rightarrow R$$

Jednostavnosti radi, često se, u dokazima ne navode primene strukturalnih pravila izvođenja. Ponekad se, kao u narednom primeru, (eventualno višestruke) primene strukturalnih pravila izvođenja označavaju dvostrukom (umesto jednostrukom) linijom.

Primer 2.19 *Formula* $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$ *je teorema i računa*

sekvenata za klasičnu i računa sekvenata za intuicionističku logiku:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B \quad C \vdash C}{B \Rightarrow C, B \vdash C}\Rightarrow L}{A \vdash A \quad B, B \Rightarrow C \vdash C}\Rightarrow L}{A, A \Rightarrow B, B \Rightarrow C \vdash C}\Rightarrow R}{A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C}\Rightarrow R}{B \Rightarrow C, A \Rightarrow B \vdash A \Rightarrow C}\Rightarrow R}{A \Rightarrow B \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\Rightarrow R}{\vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\Rightarrow R$$

Teorema 2.39 *Ako je iskazna formula teorema sistema prirodne dedukcije za klasičnu logiku, onda je ona teorema i računa sekvenata za klasičnu logiku.*

Dokaz: Pretpostavimo da je formula F teorema sistema prirodne dedukcije za klasičnu logiku, tj. da za nju postoji dokaz u sistemu prirodne dedukcije za klasičnu logiku. Taj dokaz je stablo $\mathcal{T}$ čijem je svakom čvoru pridružena po jedna formula. Tvrđenje teoreme dokazaćemo tako što ćemo taj dokaz transformisati u dokaz sekventa $\vdash F$ u računu sekvenata za klasičnu logiku. Prvi korak te transformacije je konstrukcija stabla $\mathcal{T}'$ na sledeći način: za svaki čvor stabla $\mathcal{T}$ formula A koja mu je pridružena, u stablu $\mathcal{T}'$ zamenjuje se sekventom $\Gamma \vdash A$, gde je Γ skup svih neoslobođenih pretpostavki u dokazu formule A. U korenu novodobijenog stabla je sekvent $\vdash F$, a u svakom od listova je ili sekvent oblika $A \vdash A$ (za listove iz polaznog dokaza kojima su pridružene pretpostavke) ili sekvent oblika $\vdash A \vee \neg A$ (za listove iz polaznog dokaza kojima su pridružene aksiome).

Sekventi oblika $\vdash A \vee \neg A$ zamenjuju se izvođenjima:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{\vdash A, \neg A}\neg R}{\vdash A, A \vee \neg A}\vee R}{\vdash A \vee \neg A, A}\,zamena}{\vdash A \vee \neg A, A \vee \neg A}\vee R}{\vdash A \vee \neg A}\,kontrakcija$$

Potrebno je još primene pravila prirodne dedukcije transformisati u dokaze u računu sekvenata.

$\neg I$: Pokažimo najpre da u računu sekvenata važi $\bot \vdash$, gde je $\bot$, kao što je već rečeno, skraćeni zapis za formulu $A \wedge \neg A$, gde je A proizvoljna

formula:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{\neg A, A \vdash}\,\neg L}{A \wedge \neg A, A \vdash}\,\wedge L}{A, A \wedge \neg A \vdash}\,zamena}{A \wedge \neg A, A \wedge \neg A \vdash}\,\wedge L}{A \wedge \neg A \vdash}\,kontrakcija$$

Dakle, važi $A \wedge \neg A \vdash$, tj. $\bot \vdash$. Primene pravila $\neg I$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_k \vdash \bot}{\Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash \neg A}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\dfrac{\dfrac{\Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_k \vdash \bot}{A, \Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash \bot}\qquad \bot \vdash}{A, \Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash}\,sečenje}{\Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash \neg A}\,\neg R$$

$\neg E$: Primene pravila $\neg E$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Gamma \vdash A \quad \Delta \vdash \neg A}{\Gamma, \Delta \vdash \bot}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\dfrac{\dfrac{\Delta \vdash \neg A \quad \dfrac{\Gamma \vdash A}{\neg A, \Gamma \vdash}\,\neg L}{\Delta, \Gamma \vdash}\,sečenje}{\Gamma, \Delta \vdash}}{\Gamma, \Delta \vdash \bot}\,slabljenje$$

$\wedge I$: Primene pravila $\wedge I$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\dfrac{\Gamma \vdash A}{\Gamma, \Delta \vdash A} \quad \dfrac{\Delta \vdash B}{\Gamma, \Delta \vdash B}}{\Gamma, \Delta \vdash A \wedge B}\,\wedge R$$

$\wedge E$: Primene pravila $\wedge E$ u stablu $\mathcal{T}'$ imaju formu:

$$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

i one se zamenjuju sledećim izvođenjima u računu sekvenata:

$$\dfrac{\Gamma \vdash A \wedge B \quad \dfrac{A \vdash A}{A \wedge B \vdash A}\,\wedge L}{\Gamma \vdash A}\,sečenje \qquad \dfrac{\Gamma \vdash A \wedge B \quad \dfrac{B \vdash B}{A \wedge B \vdash B}\,\wedge L}{\Gamma \vdash B}\,sečenje$$

$\vee I$**:** Primene pravila $\vee I$ u stablu $\mathcal{T}'$ imaju forme:

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

i one se zamenjuju sledećim izvođenjima u računu sekvenata:

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\vee R \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,\vee R$$

$\vee E$**:** Primene pravila $\vee E$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Theta \vdash A \vee B \quad \Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_j \vdash C \quad \Delta_1, B, \Delta_2, B, \ldots, B, \Delta_k \vdash C}{\Theta, \Gamma_1, \Gamma_2, \ldots, \Gamma_j, \Delta_1, \Delta_2, \ldots, \Delta_k \vdash C}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\Theta \vdash A \vee B \qquad \dfrac{\dfrac{\dfrac{\Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_j \vdash C}{A, \Gamma \vdash C}}{A, \Gamma, \Delta \vdash C} \quad \dfrac{\dfrac{\dfrac{\Delta_1, B, \Delta_2, B, \ldots, B, \Delta_k \vdash C}{B, \Delta \vdash C}}{B, \Gamma, \Delta \vdash C}}{A \vee B, \Gamma, \Delta \vdash C}\,\vee L}{\Theta, \Gamma, \Delta \vdash C}\,sečenje$$

gde je sa Γ je označen niz formula $\Gamma_1, \Gamma_2, \ldots, \Gamma_j$, a sa Δ niz formula $\Delta_1, \Delta_2, \ldots, \Delta_k$.

$\Rightarrow I$**:** Primene pravila $\Rightarrow I$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_k \vdash B}{\Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash A \Rightarrow B}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\dfrac{\dfrac{\Gamma_1, A, \Gamma_2, A, \ldots, A, \Gamma_k \vdash B}{A, \Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash B}}{\Gamma_1, \Gamma_2, \ldots, \Gamma_k \vdash A \Rightarrow B}\,\Rightarrow R$$

$\Rightarrow E$**:** Primene pravila $\Rightarrow E$ u stablu $\mathcal{T}'$ imaju formu

$$\dfrac{\Gamma \vdash A \quad \Delta \vdash A \Rightarrow B}{\Gamma, \Delta \vdash B}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\Delta \vdash A \Rightarrow B \quad \dfrac{\Gamma \vdash A \quad B \vdash B}{A \Rightarrow B, \Gamma \vdash B}\,\Rightarrow L}{\dfrac{\Delta, \Gamma \vdash B}{\Gamma, \Delta \vdash B}}\,sečenje$$

efq**:** Primene pravila efq u stablu $\mathcal{T}'$ imaju formu

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash D}$$

i one se zamenjuju sledećim izvođenjem u računu sekvenata:

$$\dfrac{\dfrac{\Gamma \vdash \bot \quad \bot \vdash}{\Gamma \vdash}\ sečenje}{\Gamma \vdash D}\ slabljenje$$

Opisanom transformacijom se od dokaza formule F u sistemu prirodne dedukcije dobija dokaz sekventa $\vdash F$ u računu sekvenata, te je F teorema računa sekvenata, što je i trebalo dokazati. □

Primer 2.20 *Dokaz formule* $(A \vee B) \Rightarrow (B \vee A)$ *u sistemu prirodne dedukcije (i za intuicionističku i za klasičnu logiku)*

$$\dfrac{\dfrac{[A \vee B]^1 \quad \dfrac{[A]^2}{B \vee A} \vee I \quad \dfrac{[B]^3}{B \vee A} \vee I}{B \vee A} \vee E, 2, 3}{(A \vee B) \Rightarrow (B \vee A)} \Rightarrow I, 1$$

može, na osnovu postupka opisanog u dokazu teoreme 2.39, biti transformisan u dokaz ove formule u računu sekvenata (i za intuicionističku i za klasičnu logiku):

$$\dfrac{\dfrac{A \vee B \vdash A \vee B \qquad \dfrac{\dfrac{A \vdash A}{A \vdash B \vee A} \vee R \quad \dfrac{B \vdash B}{B \vdash B \vee A} \vee R}{A \vee B \vdash B \vee A} \vee L}{A \vee B \vdash B \vee A}\ sečenje}{\vdash (A \vee B) \Rightarrow (B \vee A)} \Rightarrow R$$

Naravno, dokaz formule u računu sekvenata dobijen transformisanjem dokaza te formule u sistemu prirodne dedukcije često nije elegantan i optimalan. Na primer, formula $(A \vee B) \Rightarrow (B \vee A)$ *se u računu sekvenata, sem na navedeni način, može dokazati i znatno kraće (i bez korišćenja pravila* sečenje*):*

$$\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash B \vee A} \vee R \quad \dfrac{B \vdash B}{B \vdash B \vee A} \vee R}{A \vee B \vdash B \vee A} \vee L}{\vdash (A \vee B) \Rightarrow (B \vee A)} \Rightarrow R$$

Teorema 2.40 *Ako je iskazna formula teorema računa sekvenata za klasičnu logiku, onda je ona teorema i teorije* L.

Dokaz: Pretpostavimo da je formula F teorema računa sekvenata za klasičnu logiku, tj. da za nju postoji dokaz u računu sekvenata za klasičnu logiku. Taj dokaz je stablo $\mathcal{T}$ čijem je svakom čvoru pridružen po jedan sekvent. Tvrđenje teoreme dokazaćemo tako što ćemo taj dokaz transformisati u dokaz tvrđenja $\vdash_L F$ (u teoriji L). Prvi korak te transformacije je konstrukcija stabla $\mathcal{T}'$ na sledeći način: za svaki čvor stabla $\mathcal{T}$ sekvent $A_1, A_2, \ldots, A_j \vdash B_1, B_2, \ldots, B_k$ koji mu je pridružen, u stablu $\mathcal{T}'$ zamenjuje se tvrđenjem (za teoriju L) $A_1, A_2, \ldots, A_j, \neg B_1, \neg B_2, \ldots, \neg B_k \vdash_L \bot$. U korenu novodobijenog stabla je tvrđenje $\neg F \vdash_L \bot$, a u svakom od listova je tvrđenje oblika $A, \neg A \vdash_L \bot$ (videti primer 2.21).

Indukcijom po visini stabla dokazaćemo da je svakom čvoru stabla $\mathcal{T}'$ pridruženo tvrđenje koje je tačno u teoriji L.

- Svakom listu pridruženo je tvrđenje oblika $A, \neg A \vdash_L \bot$. Na osnovu teoreme 2.30(c), važi $\vdash_L \neg A \Rightarrow (A \Rightarrow B)$, pa i $\vdash_L \neg A \Rightarrow (A \Rightarrow \bot)$, odakle se, dvostrukom primenom obratne teoreme o dedukciji (teorema 2.28), dobija $A, \neg A \vdash_L \bot$.
- Pretpostavimo da je tvrđenje tačno za svako podstablo stabla $\mathcal{T}'$ visine manje od n i dokažimo da važi i za podstablo visine n. Označimo sa v koren postabla visine n.

  U teoriji L u tvrđenju $\Gamma \vdash_L A$, Γ je skup (a ne niz kao u računu sekvenata), te nije bitan poredak elemenata skupa Γ, niti su relevantna eventualna višestruka pojavljivanja njegovih elemenata.

  Posebno ćemo razmatrati sva pravila koja su mogla biti primenjena.

  slabljenje: Čvoru v pridruženo je tvrđenje oblika $D, \Delta \vdash_L \bot$ ili $\Delta, D \vdash_L \bot$, a njegovom direktnom potomku u stablu $\mathcal{T}'$ tvrđenje oblika $\Delta \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Delta \vdash_L \bot$, pa, na osnovu teoreme 2.25(a), sledi $D, \Delta \vdash_L \bot$ i $\Delta, D \vdash_L \bot$.

  kontrakcija: Čvoru v pridruženo je tvrđenje oblika $D, \Delta \vdash_L \bot$, a njegovom direktnom potomku $D, D, \Delta \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $D, D, \Delta \vdash_L \bot$, pa važi i $D, \Delta \vdash_L \bot$. Druga mogućnost je da je čvoru v pridruženo tvrđenje oblika $\Delta, D \vdash_L \bot$, a njegovom direktnom potomku $\Delta, D, D \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Delta, D, D \vdash_L \bot$, pa važi i $\Delta, D \vdash_L \bot$.

  zamena: Čvoru v pridruženo je tvrđenje oblika $\Theta, D, E, \Lambda \vdash_L \bot$, a njegovom direktnom potomku $\Theta, E, D, \Lambda \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Theta, E, D, \Lambda \vdash_L \bot$, pa važi i $\Theta, D, E, \Lambda \vdash_L \bot$.

  Druga mogućnost je da je čvoru v pridruženo tvrđenje oblika $\Theta, \neg D, \neg E, \Lambda \vdash_L \bot$, a njegovom direktnom potomku $\Theta, \neg E, \neg D, \Lambda \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Theta, \neg E, \neg D, \Lambda \vdash_L \bot$, pa važi i $\Theta, \neg D, \neg E, \Lambda \vdash_L \bot$.

sečenje: Čvoru v pridruženo je tvrđenje oblika $\Gamma, \Delta, \Theta', \Lambda' \vdash_L \bot$, a njegovim direktnim potomcima $\Gamma, \Theta', \neg D \vdash_L \bot$ i $D, \Delta, \Lambda' \vdash_L \bot$ Na osnovu induktivne pretpostavke važi $\Gamma, \Theta', \neg D \vdash_L \bot$ i $D, \Delta, \Lambda' \vdash_L \bot$. Na osnovu teoreme 2.31 važi $\Gamma, \Theta' \vdash_L D$ i $\Delta, \Lambda' \vdash_L \neg D$. Na osnovu teoreme 2.25(a) sledi $\Gamma, \Theta', \Delta, \Lambda' \vdash_L D$ i $\Gamma, \Theta', \Delta, \Lambda' \vdash_L \neg D$. Odatle, na osnovu $D, \neg D \vdash_L \bot$ (videti dokaz u induktivnoj osnovi) i na osnovu teoreme 2.25(c) važi, $\Gamma, \Theta', \Delta, \Lambda' \vdash_L \bot$, pa i $\Gamma, \Delta, \Theta', \Lambda' \vdash_L \bot$.

$\neg L$: Čvoru v pridruženo je tvrđenje oblika $\neg A, \Delta \vdash_L \bot$, a njegovom direktnom potomku $\Delta, \neg A, \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Delta, \neg A, \vdash_L \bot$, pa važi i $\neg A, \Delta \vdash_L \bot$.

$\neg R$: Čvoru v pridruženo je tvrđenje oblika $\Delta, \neg\neg A \vdash_L \bot$, a njegovom direktnom potomku $A, \Delta \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $A, \Delta \vdash_L \bot$, pa, kako važi $\neg\neg A \vdash_L A$, na osnovu teoreme 2.25(c), važi i $\Delta, \neg\neg A \vdash_L \bot$.

$\wedge L$: Čvoru v pridruženo je tvrđenje oblika $A \wedge B, \Delta \vdash_L \bot$, a njegovom direktnom potomku $A, \Delta \vdash_L \bot$ ili $B, \Delta \vdash_L \bot$. Ako je direktnom potomku čvora v pridruženo tvrđenje $A, \Delta \vdash_L \bot$, onda je ono tačno na osnovu induktivne pretpostavke, pa, kako važi $A \wedge B \vdash_L A$, na osnovu teoreme 2.25(c), sledi $A \wedge B, \Delta \vdash_L \bot$. Tvrđenje se analogno dokazuje u drugom slučaju.

$\wedge R$: Čvoru v pridruženo je tvrđenje oblika $\Delta, \neg(A \wedge B) \vdash_L \bot$, a njegovim direktnim potomcima $\Delta, \neg A \vdash_L \bot$ i $\Delta, \neg B \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $\Delta, \neg A \vdash_L \bot$ i $\Delta, \neg B \vdash_L \bot$ a, na osnovu teoreme 2.31, $\Delta \vdash_L A$ i $\Delta \vdash_L B$. Odatle, na osnovu $A, B \vdash_L A \wedge B$ i na osnovu teoreme 2.25(c) sledi $\Delta \vdash_L A \wedge B$ te, na osnovu teoreme 2.31, važi $\Delta, \neg(A \wedge B) \vdash_L \bot$.

$\vee L$: Čvoru v pridruženo je tvrđenje oblika $A \vee B, \Delta \vdash_L \bot$, a njegovim direktnim potomcima $A, \Delta \vdash_L \bot$ i $B, \Delta \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $A, \Delta \vdash_L \bot$ i $B, \Delta \vdash_L \bot$ a, na osnovu teoreme 2.31, $\Delta \vdash_L \neg A$ i $\Delta \vdash_L \neg B$. Odatle, na osnovu $\neg A, \neg B \vdash_L \neg A \wedge \neg B$ i na osnovu teoreme 2.25(c) sledi $\Delta \vdash_L \neg A \wedge \neg B$ te, na osnovu teoreme 2.31, važi $\Delta, \neg(\neg A \wedge \neg B) \vdash_L \bot$. Važi $A \vee B \vdash_L \neg(\neg A \wedge \neg B)$ te, na osnovu teoreme 2.25(c), važi $\Delta, A \vee B \vdash_L \bot$, pa i $A \vee B, \Delta \vdash_L \bot$.

$\vee R$: Čvoru v pridruženo je tvrđenje oblika $\Delta, \neg(A \vee B) \vdash_L \bot$, a njegovom direktnom potomku $\Delta, \neg A \vdash_L \bot$ ili $\Delta, \neg B \vdash_L \bot$. Ako je direktnom potomku čvora v pridruženo tvrđenje $\Delta, \neg A \vdash_L \bot$, onda je ono tačno na osnovu induktivne pretpostavke, pa, kako važi $\neg(A \vee B) \vdash_L \neg A$, na osnovu teoreme 2.25(c), važi $\Delta, \neg(A \vee B) \vdash_L \bot$. Tvrđenje se analogno dokazuje u drugom slučaju.

$\Rightarrow L$: Čvoru v pridruženo je tvrđenje oblika $A \Rightarrow B, \Gamma, \Delta, \Theta', \Lambda' \vdash_L \bot$, a njegovim direktnim potomcima $\Gamma, \Theta', \neg A \vdash_L \bot$ i $B, \Delta, \Lambda' \vdash_L$

$\bot$. Na osnovu induktivne pretpostavke važi $\Gamma, \Theta', \neg A \vdash_L \bot$ i $B, \Delta, \Lambda' \vdash_L \bot$ a, na osnovu teoreme 2.31, $\Gamma, \Theta' \vdash_L A$ i $\Delta, \Lambda' \vdash_L \neg B$. Na osnovu teoreme 2.25(a) važi $\Gamma, \Theta', \Delta, \Lambda' \vdash_L A$ i $\Gamma, \Theta', \Delta, \Lambda' \vdash_L \neg B$. Odatle, na osnovu $A, \neg B \vdash_L A \wedge \neg B$ i na osnovu teoreme 2.25(c) sledi $\Gamma, \Theta', \Delta, \Lambda' \vdash_L A \wedge \neg B$ i, na osnovu teoreme 2.31, $\Gamma, \Theta', \Delta, \Lambda', \neg(A \wedge \neg B) \vdash_L \bot$. Važi $A \Rightarrow B \vdash_L \neg(A \wedge \neg B)$, pa na osnovu teoreme 2.25(c), sledi $\Gamma, \Theta', \Delta, \Lambda', A \Rightarrow B \vdash_L \bot$ i $A \Rightarrow B, \Gamma, \Delta, \Theta', \Lambda' \vdash_L \bot$.

$\Rightarrow R$**:** Čvoru v pridruženo je tvrđenje oblika $\Delta, \neg(A \Rightarrow B) \vdash_L \bot$, a njegovom direktnom potomku $A, \Delta, \neg B \vdash_L \bot$. Na osnovu induktivne pretpostavke važi $A, \Delta, \neg B \vdash_L \bot$, pa, kako važi $\neg(A \Rightarrow B) \vdash_L A$ i $\neg(A \Rightarrow B) \vdash_L \neg B$, na osnovu teoreme 2.25(c), važi i $\Delta, \neg(A \Rightarrow B) \vdash_L \bot$.

Dakle, svakom čvoru stabla $\mathcal{T}'$ pridruženo je tvrđenje koje je tačno u teoriji L. Korenu tog stabla pridruženo je tvrđenje $\neg F \vdash_L \bot$ i ono je tačno, pa na osnovu teoreme 2.31 važi $\vdash_L F$, što je i trebalo dokazati. □

Primer 2.21 *Dokaz formule* $(A \vee B) \Rightarrow (B \vee A)$ *u računu sekvenata*

$$\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash B \vee A} \vee R \quad \dfrac{B \vdash B}{B \vdash B \vee A} \vee R}{A \vee B \vdash B \vee A} \vee L}{\vdash (A \vee B) \Rightarrow (B \vee A)} \Rightarrow R$$

transformiše se, na osnovu postupka opisanog u dokazu teoreme 2.40 najpre u sledeće stablo (čijem je svakom čvoru pridruženo tvrđenje teorije L):

$$\dfrac{\dfrac{\dfrac{A, \neg A \vdash_L \bot}{A, \neg(B \vee A) \vdash_L \bot} \quad \dfrac{B, \neg B \vdash_L \bot}{B, \neg(B \vee A) \vdash_L \bot}}{A \vee B, \neg(B \vee A) \vdash_L \bot}}{\neg((A \vee B) \Rightarrow (B \vee A)) \vdash_L \bot}$$

Sva tvrđenja pridružena čvorovima ovog stabla tačna su u teoriji L, pa u teoriji L važi i $\neg((A \vee B) \Rightarrow (B \vee A)) \vdash_L \bot$ i $\vdash_L (A \vee B) \Rightarrow (B \vee A)$. Dokaz ove formule u teoriji L zasnovan na konstruisanom stablu zahtevao bi uključivanje dokaza teorema (tj. odgovarajućih instanci) korišćenih u dokazu teoreme 2.40. Naravno, dokaz formule u teoriji L dobijen na taj način često nije elegantan i optimalan.

Iz teorema 2.38, 2.39 i 2.40 neposredno sledi da su teorija L, sistem prirodne dedukcije za klasičnu iskaznu logiku i račun sekvenata za klasičnu iskaznu logiku ekvivalentni, tj. važi naredno tvrđenje.

Teorema 2.41 *Iskazna formula je teorema teorije L ako i samo je ona teorema sistema prirodne dedukcije za klasičnu iskaznu logiku ako i samo ako je teorema računa sekvenata za klasičnu iskaznu logiku.*

Iz navedene teoreme sledi da važi $\Gamma \vdash A$ u teoriji L ako i samo ako $\Gamma \vdash A$ važi u sistemu prirodne dedukcije za klasičnu logiku ako i samo ako $\Gamma \vdash A$ važi u računu sekvenata za klasičnu logiku.

Iz potpunosti i saglasnosti teorije L (u odnosu na semantiku) sledi potpunost i saglasnost računa sekvenata za klasičnu logiku, tj. u računu sekvenata za klasičnu logiku važi $\Gamma \vdash A$ ako i samo ako važi $\Gamma \models A$ (gde je Γ konačan niz formula).

Analogno dokazu teoreme 2.41 dokazuje se da su Hilbertov sistem za intuicionističku logiku, prirodna dedukcija za intuicionističku logiku i račun sekvenata za intuicionističku logiku ekvivalentni sistemi.

Zadaci

Zadatak 44 $\surd$ *Dokazati da je formula* $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ *teorema računa sekvenata za klasičnu logiku.*

Zadatak 45 *Dokazati da je formula* $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$ *teorema računa sekvenata za klasičnu logiku.*

2.4 Sažetak

Iskazna logika ima tri aspekta: svoju sintaksu (ili jezik), svoju semantiku (ili značenje iskaza) i svoje deduktivne sisteme. Poglavlje 2.1 bavi se jezikom iskazne logike, poglavlje 2.2 semantikom, a poglavlje 2.3 dedukcijom u iskaznoj logici.

U potpoglavlju 2.2.1 definisani su pojmovi valjane i zadovoljive iskazne formule. Problemi ispitivanja valjanosti i zadovoljivosti su centralni problemi iskazne logike. Ovi problemi su odlučivi i postoje efektivni metodi za njihovo rešavanje. Neki od tih metoda su: metod istinitosnih tablica (potpoglavlje 2.2.2), Dejvis–Patnam–Longman–Lovelandova procedura (potpoglavlje 2.2.6), metod rezolucije (potpoglavlje 2.2.7) i metod tabloa (potpoglavlje 2.2.8).

Neki od ovih metoda zahtevaju transformisanje zadate formule u neku normalnu formu (potpoglavlje 2.2.5), što obezbeđuju koncepti supstitucije i teorema o zameni (potpoglavlje 2.2.3).

Svi nabrojani metodi imaju svojstvo potpunosti i saglasnosti — ako je formula valjana, onda će to sigurno biti pokazano primenom metoda, i ako metod tvrdi da je neka formula valjana, onda je ona sigurno valjana.

Svaki od nabrojanih metoda ima eksponencijalnu složenost za ispitivanje zadovoljivosti. Problem zadovoljivosti (problem SAT) je tipičan predstavnik klase NP kompletnih problema i ne zna se da li za njega postoji metod čija je složenost polinomijalna.

Koncept „valjane formule“ je semantičke prirode, a njegov sintaksni, deduktivni pandan je koncept „teoreme“. Teorema je formula za koju postoji dokaz u okviru nekog deduktivnog sistema. Dokaz se zasniva na pravilima izvođenja i aksiomama, a ne na definiciji semantike. No, deduktivni sistemi su

običnо izgrađeni tako da imaju svojstvo potpunosti i saglasnosti: ako je neka iskazna formula valjana, onda ona može biti dokazana u okviru deduktivnog sistema, a ako za neku formulu postoji dokaz u okviru deduktivnog sistema, onda je ona sigurno valjana. Neki od deduktivnih sistema za iskaznu logiku su Hilbertov sistem ili teorija L (potpoglavlje 2.3.1), Gencenova prirodna dedukcija (potpoglavlje 2.3.2) i Gencenov račun sekvenata (potpoglavlje 2.3.3).

Glava 3

Logika prvog reda

Logika prvog reda, predikatska logika, znatno je izražajnija od iskazne logike. Osnovna novina u odnosu na iskaznu logiku je uvođenje kvantifikovanja, univerzalnog i egzistencijalnog. Zahvaljujući kvantifikatorima, u logici prvog reda mogu se formulisati tvrđenja koja nije moguće formulisati na jeziku iskazne logike kao, na primer, tvrđenje „za svaku valuaciju postoji klauza iz S koja nije tačna ako i samo ako ne postoji valuacija takva da je svaka klauza iz S tačna“. U logici prvog reda dozvoljeno je samo kvantifikovanje promenljivih.[1] U okviru logike prvog reda mogu se opisati mnoge matematičke teorije.

Kao i iskazna logika, logika prvog reda ima tri aspekta: svoju sintaksu (ili jezik), svoju semantiku (ili značenje iskaza) i svoje deduktivne sisteme. I semantika i deduktivni sistemi grade se nad isto definisanom sintaksom, tj. nad istim skupom formula.

Kao i u iskaznoj logici, centralni problemi u predikatskoj logici su ispitivanje da li je data formula valjana i da li je data formula zadovoljiva. Za razliku od iskazne logike, ovi problemi nisu odlučivi, te ne postoje efektivni algoritmi za njihovo rešavanje. No, problem ispitivanja valjanosti za predikatsku logiku je poluodlučiv, pa postoje metode koje za svaku valjanu formulu mogu da dokažu da je ona valjana (a ne mogu za bilo koju formulu koja nije valjana da utvrde da nije valjana).

Postoji više metoda i pristupa za ispitivanje i dokazivanje valjanosti i zadovoljivosti. Neki od njih su semantičke, a neki deduktivne (tj. sintaksno-deduktivne) prirode. Kao i u iskaznoj logici, ključna veza između ova dva koncepta je tvrđenje da je formula valjana (što je semantička kategorija) ako i samo ako je ona teorema (što je deduktivna kategorija). Zahvaljujući ovoj vezi, sintaksa predikatske logike (jezik predikatske logike), njena semantika (konvencije o *značenju* formula) i njena deduktivna svojstva čine kompaktnu celinu.

[1] U logici višeg reda predikati i funkcije kao argumente mogu imati druge predikate i funkcije i dozvoljeno je njihovo kvantifikovanje. Na primer, u logici drugog reda predikati i funkcije mogu za argumente imati predikate i funkcije prvog reda i mogu biti kvantifikovani. Predikati i funkcije reda n mogu za argumente imati predikate i funkcije $n-1$ reda i mogu biti kvantifikovani.

3.1 Sintaksa logike prvog reda

Sintaksni aspekt logike prvog reda govori o njenom *jeziku*, a o formulama isključivo kao o nizovima simbola i ne uzima u obzir njihovo moguće značenje.

Definicija 3.1 Logički deo *jezika prvog reda čine skupovi:*

1. *prebrojiv skup* promenljivih V*;*
2. *skup* logičkih veznika $\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$*, pri čemu je* $\neg$ *unarni veznik, a* $\wedge, \vee, \Rightarrow$ *i* $\Leftrightarrow$ *su binarni veznici;*
3. *skup* kvantifikatora $\{\forall, \exists\}$*, pri čemu je* $\forall$ univerzalni kvantifikator*, a* $\exists$ egzistencijalni kvantifikator*;*
4. *skup* logičkih konstanti $\{\top, \bot\}$*;*
5. *skup* pomoćnih simbola $\{(,), ,\}$.

Elemente nabrojanih skupova zovemo logički simboli.

Rečnik *ili* signatura $\mathcal{L}$ *sastoji se od najviše prebrojivih skupova* Σ *i* Π*, koje redom nazivamo* skupom funkcijskih simbola *i* skupom predikatskih (relacijskih) simbola*, kao i od funkcije* ar *koja preslikava skup* $\Sigma \cup \Pi$ *u skup nenegativnih celih brojeva. Za* $k \in \Sigma \cup \Pi$*, vrednost* $ar(k)$ *zovemo* stepen *ili* arnost *simbola* k*. Presek svaka dva od skupova* Σ, Π*, skupa promenljivih, skupa logičkih veznika, skupa kvantifikatora, skupa logičkih konstanti i skupa pomoćnih simbola je prazan. Funkcijske simbole arnosti* 0 *zovemo* simbolima konstanti*. Skupovi* Σ *i* Π *čine* nelogički deo *jezika prvog reda, a sve njihove elemente zovemo* nelogičkim simbolima.

Za datu signaturu

$$\mathcal{L} = (\Sigma, \Pi, ar)$$

reč nad $\mathcal{L}$ *je bilo koji niz simbola iz skupova* Σ, Π *ili logičkog dela jezika.*

Uz indeks ili bez indeksa, obično označavamo sa:

- $a, b, c, \ldots$ simbole konstanti;
- $f, g, h, \ldots$ funkcijske simbole arnosti veće od 0;
- $p, q, r, \ldots$ predikatske simbole;
- $x, y, z, \ldots$ promenljive.

Definicija 3.2 *Skup* termova *nad signaturom* $\mathcal{L} = (\Sigma, \Pi, ar)$ *i skupom promenljivih* V *je najmanji skup za koji važi:*

- *svaki simbol konstante (tj. svaki funkcijski simbol arnosti* 0*) je term;*
- *svaki simbol promenljive je term;*

- *ako je f funkcijski simbol za koji je $ar(f) = n$ i t_1, t_2, ..., t_n su termovi, onda je i $f(t_1, t_2, \ldots, t_n)$ term.*

Definicija 3.3 *Skup* atomičkih formula *nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom promenljivih V je najmanji skup za koji važi:*

- *logičke konstante $\top$ i $\bot$ su atomičke formule;*
- *ako je p predikatski simbol za koji je $ar(p) = n$ i t_1, t_2, ..., t_n su termovi, onda je $p(t_1, t_2, \ldots, t_n)$ atomička formula.*

Definicija 3.4 *Skup* dobro zasnovanih formula *nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom promenljivih V (ili* jezik prvog reda nad *$\mathcal{L}$* i *V) je najmanji skup za koji važi:*

- *svaka atomička formula je dobro zasnovana formula;*
- *ako je $\mathcal{A}$ dobro zasnovana formula, onda je i $(\neg\mathcal{A})$ dobro zasnovana formula;*
- *ako su $\mathcal{A}$ i $\mathcal{B}$ dobro zasnovane formule, onda su i $(\mathcal{A}\wedge\mathcal{B})$, $(\mathcal{A}\vee\mathcal{B})$, $(\mathcal{A}\Rightarrow\mathcal{B})$ i $(\mathcal{A}\Leftrightarrow\mathcal{B})$ dobro zasnovane formule;*
- *ako je $\mathcal{A}$ dobro zasnovana formula i x je promenljiva, onda su $((\forall x)\mathcal{A})$ i $((\exists x)\mathcal{A})$ dobro zasnovane formule.*

Umesto termina *dobro zasnovana formula*, često ćemo pisati kraće *formula*.

Dobro zasnovane formule obično označavamo velikim pisanim latiničnim slovima (eventualno sa indeksima). Skupove dobro zasnovanih formula obično označavamo velikim slovima grčkog alfabeta (eventualno sa indeksima).

Logičke veznike zovemo i *bulovskim veznicima* ili, kraće, *veznicima*. Veznik $\neg$ zovemo *negacija*, veznik $\wedge$ *konjunkcija*, $\vee$ *disjunkcija*, veznik $\Rightarrow$ *implikacija* i $\Leftrightarrow$ *ekvivalencija*. Zapis $(\neg\mathcal{A})$ čitamo *negacija $\mathcal{A}$* ili *ne $\mathcal{A}$*. Zapis $(\mathcal{A}\wedge\mathcal{B})$ čitamo *$\mathcal{A}$ konjunkcija $\mathcal{B}$* ili *$\mathcal{A}$ i $\mathcal{B}$*. Zapis $(\mathcal{A}\vee\mathcal{B})$ čitamo *$\mathcal{A}$ disjunkcija $\mathcal{B}$* ili *$\mathcal{A}$ ili $\mathcal{B}$*. Zapis $(\mathcal{A}\Rightarrow\mathcal{B})$ čitamo *$\mathcal{A}$ implikacija $\mathcal{B}$* ili *iz $\mathcal{A}$ sledi $\mathcal{B}$*. Zapis $(\mathcal{A}\Leftrightarrow\mathcal{B})$ čitamo *$\mathcal{A}$ ekvivalencija $\mathcal{B}$* ili *$\mathcal{A}$ ekvivalentno $\mathcal{B}$*. Zapis $((\forall x)\mathcal{A})$ čitamo *za svako x $\mathcal{A}$*. Zapis $((\exists x)\mathcal{A})$ čitamo *postoji x takvo da je $\mathcal{A}$*.

Ako su dve dobro zasnovane formule $\mathcal{A}$ i $\mathcal{B}$ sintaksno identične (tj. ako su jednake kao nizovi simbola), onda to označavamo $\mathcal{A} = \mathcal{B}$. Ako dve dobro zasnovane formule $\mathcal{A}$ i $\mathcal{B}$ nisu sintaksno identične, onda to označavamo $\mathcal{A} \neq \mathcal{B}$.

Termove, atomičke formule i dobro zasnovane formule nad signaturom $\mathcal{L}$ ponekad ćemo kraće zvati i $\mathcal{L}$-termovi, $\mathcal{L}$-atomičke formule i $\mathcal{L}$-formule.

Bazni term je term koji ne sadrži nijednu promenljivu. *Bazna formula* je formula koja ne sadrži nijednu promenljivu.

Literal je atomička formula ili negacija atomičke formule. *Klauza* je disjunkcija literala.

Da bismo izbegli korišćenje velikog broja zagrada obično izostavljamo spoljne zagrade i usvajamo konvenciju uz koju u nekim dobro zasnovanim formulama neke zagrade mogu biti izostavljene i to na isti način kao i za iskazne formule, pri čemu kvantifikatori imaju veći prioritet od svih logičkih veznika.

Kažemo da formula $\mathcal{A}$ *određuje* ili *indukuje* signaturu $\mathcal{L}$, ako je $\mathcal{L}$ signatura koja sadrži sve funkcijske i predikatske simbole iz $\mathcal{A}$ i nijedan više.

Teorema 3.1 (Indukcija nad skupom dobro zasnovanih formula) *Neka je ϕ svojstvo reči jezika nad signaturom $\mathcal{L}$ i skupom promenljivih V. Pretpostavimo da svojstvo ϕ važi za svaku atomičku formulu i pretpostavimo da ako svojstvo ϕ važi za dobro zasnovane formule $\mathcal{A}$ i $\mathcal{B}$, onda ono važi i za dobro zasnovane formule $\neg\mathcal{A}$, $\mathcal{A} \wedge \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \Rightarrow \mathcal{B}$, $\mathcal{A} \Leftrightarrow \mathcal{B}$, $(\forall x)\mathcal{A}$ i $(\exists x)\mathcal{A}$. Tada svojstvo ϕ važi za svaku dobro zasnovanu formulu.*

Dokaz: Neka je L skup svih reči nad signaturom $\mathcal{L}$ (za skup promenljvih V) za koje je zadovoljen uslov ϕ. Skup L zadovoljava uslove definicije skupa dobro zasnovanih formula. Kako je skup dobro zasnovanih formula najmanji takav skup, sledi da je on podskup skupa L, tj. svojstvo ϕ važi za svaku dobro zasnovanu formulu nad signaturom $\mathcal{L}$ i skupom promenljivih V. □

Definicija 3.5 *Funkcija c iz skupa dobro zasnovanih formula u* **N** *svakoj dobro zasnovanoj formuli pridružuje* složenost *na sledeći način:*

1. *ako je $\mathcal{A}$ atomička dobro zasnovana formula, onda je $c(\mathcal{A}) = 0$;*
2. $c(\neg\mathcal{A}) = c(\mathcal{A}) + 1$;
3. $c(\mathcal{A} \wedge \mathcal{B}) = c(\mathcal{A}) + c(\mathcal{B}) + 1$;
4. $c(\mathcal{A} \vee \mathcal{B}) = c(\mathcal{A}) + c(\mathcal{B}) + 1$;
5. $c(\mathcal{A} \Rightarrow \mathcal{B}) = c(\mathcal{A}) + c(\mathcal{B}) + 1$;
6. $c(\mathcal{A} \Leftrightarrow \mathcal{B}) = c(\mathcal{A}) + c(\mathcal{B}) + 1$;
7. $c(\forall x\mathcal{A}) = c(\mathcal{A}) + 1$;
8. $c(\exists x\mathcal{A}) = c(\mathcal{A}) + 1$.

Indukcijom nad skupom dobro zasnovanih formula može se dokazati da se funkcijom c svakoj dobro zasnovanoj formuli pridružuje (jedinstvena) složenost. Na analogan način može se definisati i *složenost terma*.

Definicija 3.6 Slobodno pojavljivanje *i* vezano pojavljivanje promenljive u formuli *definiše se na sledeći način:*

- *svako pojavljivanje promenljive u atomičkoj formuli je slobodno u toj formuli;*
- *svako pojavljivanje promenljive koje je slobodno u $\mathcal{A}$ je slobodno i u $\neg\mathcal{A}$; svako pojavljivanje promenljive koje je vezano u $\mathcal{A}$ je vezano i u $\neg\mathcal{A}$;*

- *svako pojavljivanje promenljive koje je slobodno u $\mathcal{A}$ ili u $\mathcal{B}$ je slobodno i u $\mathcal{A} \wedge \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \Rightarrow \mathcal{B}$, $\mathcal{A} \Leftrightarrow \mathcal{B}$; svako pojavljivanje promenljive koje je vezano u $\mathcal{A}$ ili u $\mathcal{B}$ je vezano i u $\mathcal{A} \wedge \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \Rightarrow \mathcal{B}$, $\mathcal{A} \Leftrightarrow \mathcal{B}$;*
- *svako slobodno pojavljivanje promenljive različite od x u formuli $\mathcal{A}$ je takođe slobodno u formuli $(\forall x)\mathcal{A}$; svako slobodno pojavljivanje promenljive x u $\mathcal{A}$ je vezano (vodećim kvantifikatorom) u $(\forall x)\mathcal{A}$ (tada kažemo da je x u* dosegu *vodećeg kvantifikatora); pojavljivanje promenljive x u $(\forall x)$ u formuli $(\forall x)\mathcal{A}$ je vezano; analogno za egzistencijalni kvantifikator.*

Definicija 3.7 *Promenljiva je* vezana *(*slobodna*) u formuli ako i samo ako ima vezano (slobodno) pojavljivanje u toj formuli.*

Primetimo da promenljiva može biti i slobodna i vezana u jednoj formuli.

Primer 3.1 *U formuli $p(x, y)$, pojavljivanje promenljive x je slobodno i ona je slobodna u ovoj formuli.*

U formuli $p(x, y) \Rightarrow (\forall x)q(x)$ prvo pojavljivanje promenljive x je slobodno, a drugo i treće pojavljivanje je vezano. U ovoj formuli, promenljiva x je i slobodna i vezana.

U formuli $(\forall x)p(x, y) \Rightarrow (\forall x)q(x)$, sva pojavljivanja promenljive x su vezana i promenljiva je vezana u ovoj formuli.

U sva tri primera, pojavljivanja promenljive y su slobodna.

Primer 3.2 *U formuli $(\exists x)(p(x) \wedge (\forall x)q(x))$ četvrto pojavljivanje promenljive x je vezano i ono je u dosegu kvantifikatora $\forall x$, a ne i kvantifikatora $\exists x$.*

Često ćemo pokazivati da formula $\mathcal{A}$ ima slobodne promenljive x_1, x_2, …, x_n zapisom $\mathcal{A}(x_1, x_2, \ldots, x_n)$. Ovaj zapis, međutim, ne znači da formula $\mathcal{A}$ ne sadrži još neke slobodne promenljive, niti znači da promenljive x_1, x_2, …, x_n nemaju i neka vezana pojavljivanja u formuli $\mathcal{A}$. Zapis $\mathcal{A}(x_1, x_2, \ldots, x_n)$ je pogodan, jer možemo da usvojimo konvenciju da kao $\mathcal{A}(t_1, t_2, \ldots, t_n)$ zapisujemo formulu dobijenu zamenjivanjem svih slobodnih pojavljivanja promenljivih $x_1, x_2, \ldots, x_n$ redom termovima $t_1, t_2, \ldots, t_n$.

$\mathcal{L}$-formulu bez slobodnih promenljivih zovemo *zatvorena $\mathcal{L}$-formula* ili *$\mathcal{L}$-rečenica*. Za formulu $\mathcal{A}$ kažemo da je *univerzalno zatvorena* ako je oblika $(\forall x_1)(\forall x_2)\ldots(\forall x_k)\mathcal{A}'$, gde je $x_i \in V$ $(i = 1, 2, \ldots, k)$ i $\mathcal{A}'$ ne sadrži kvantifikatore kao ni slobodne promenljive osim (eventualno) promenljivih $x_1, x_2, \ldots, x_k$. Formula $\mathcal{A}$ je *egzistencijalno zatvorena* ako je oblika $(\exists x_1)(\exists x_2)\ldots(\exists x_k)\mathcal{A}'$ gde je $x_i \in V$ $(i = 1, 2, \ldots, k)$ i $\mathcal{A}'$ ne sadrži kvantifikatore kao ni slobodne promenljive osim (eventualno) promenljivih $x_1, x_2, \ldots, x_k$. Ako formula $\mathcal{A}$ ima kao slobodne samo promenljive $x_1, x_2, \ldots, x_k$ onda formulu $(\forall x_1)(\forall x_2)\ldots(\forall x_k)\mathcal{A}$ nazivamo *univerzalnim zatvorenjem* formule $\mathcal{A}$ i kraće je označavamo sa $\forall * \mathcal{A}$. Ako formula $\mathcal{A}$ ima kao slobodne samo promenljive $x_1, x_2, \ldots, x_k$, onda formulu $(\exists x_1)(\exists x_2)\ldots(\exists x_k)\mathcal{A}$ nazivamo *egzistencijalnim zatvorenjem* formule $\mathcal{A}$ i kraće je označavamo sa $\exists * \mathcal{A}$.

Zadaci

Zadatak 46 *Zapisati narednu rečenicu u vidu dobro zasnovane formule logike prvog reda:*

(a) Svako voli nekoga i niko ne voli svakoga ili neko voli svakoga i neko ne voli nikoga.

(b) Možete lagati neke ljude sve vreme i možete lagati sve ljude neko vreme, ali ne možete lagati sve ljude sve vreme.

3.2 Semantika logike prvog reda

Semantički aspekt logike prvog reda govori o *značenju* formula. U nastavku će biti uvedena semantika logike prvog reda u stilu Tarskog (koji je prvi precizno uveo pojam semantike 1933. godine) [72]. Tako uvedenu semantiku zovemo i *semantika Tarskog*.

3.2.1 Valuacija, interpretacija, model; zadovoljive, valjane, porecive i kontradiktorne formule

U nastavku ćemo smatrati da se podrazumeva (i kada to nije eksplicitno rečeno) da se, kada se govori o formulama, govori o $\mathcal{L}$-formulama za neku fiksnu signaturu $\mathcal{L}$ i fiksan skup promenljivih V.

Definicija 3.8 *Za datu signaturu $\mathcal{L}$, $\mathcal{L}$-struktura $\mathfrak{D}$ je par $(D, I^{\mathcal{L}})$, gde je D skup, a $I^{\mathcal{L}}$ funkcija pri čemu važi sledeće:*

- *D je neprazan skup i zovemo ga* domen, nosač *ili* univerzum*;*
- *svakom simbolu konstante c iz $\mathcal{L}$ (tj. svakom funkcijskom simbolu arnosti 0), funkcija $I^{\mathcal{L}}$ pridružuje jedan element c_I iz D;*
- *svakom funkcijskom simbolu f iz $\mathcal{L}$ za koji je $ar(f) = n$ i $n > 0$, funkcija $I^{\mathcal{L}}$ pridružuje jednu totalnu funkciju f_I iz D^n u D;*
- *svakom predikatskom simbolu p iz $\mathcal{L}$ za koji je $ar(p) = n$ (i $n > 0$) funkcija $I^{\mathcal{L}}$ pridružuje jednu totalnu funkciju p_I iz D^n u $\{0, 1\}$.*

Valuacija v za skup promenljivih V u odnosu na domen D je preslikavanje koje svakom elementu iz V dodeljuje jedan element iz D. Ako je $v(x_i) = d_j$, onda kažemo da je d_j *vrednost* promenljive x_i u valuaciji v. Ako su v i w valuacije za isti skup promenljivih i u odnosu na isti domen, onda sa $v \sim_x w$ označavamo da je $v(y) = w(y)$ za svaku promenljivu y različitu od x.

Ako je $\mathfrak{D} = (D, I^{\mathcal{L}})$ $\mathcal{L}$-struktura za neku signaturu $\mathcal{L}$ i v valuacija za skup promenljivih V i za domen D, onda par $(\mathfrak{D}, v)$ određuje *interpretaciju*, tj. funkciju I_v koja preslikava skup $\mathcal{L}$-termova nad skupom promenljivih V u skup D, a skup $\mathcal{L}$-formula nad skupom promenljivih V u skup $\{0, 1\}$. Funkcija I_v uvodi se narednim dvema definicijama.

Definicija 3.9 Vrednost *(ili* značenje*) terma* t *u interpretaciji* I_v*, određenoj* $\mathcal{L}$*-strukturom* $\mathfrak{D}$ *i valuacijom* v*, označavamo sa* $I_v(t)$ *i definišemo na sledeći način:*

- *ako je* t *simbol promenljive* x*, onda je* $I_v(t) = v(x)$*;*
- *ako je* t *simbol konstante* c*, onda je* $I_v(t) = c_I$*;*
- *ako je* t *jednako* $f(t_1, t_2, \ldots, t_n)$ *(pri čemu je* $ar(f) = n$*) i ako je* $I_v(t_i) = d_i$ *za* $i = 1, 2, \ldots, n$ *(pri čemu je* $d_i \in D$*), onda je* $I_v(t) = f_I(d_1, d_2, \ldots, d_n)$*.*

Definicija 3.10 Vrednost *(ili* značenje*) formule* $\mathcal{A}$ *u interpretaciji* I_v*, određenoj* $\mathcal{L}$*-strukturom* $\mathfrak{D}$ *i valuacijom* v*, označavamo sa* $I_v(\mathcal{A})$ *i definišemo na sledeći način:*

- *ako je* $\mathcal{A}$ *atomička formula* $\top$ *onda je* $I_v(\mathcal{A}) = 1$*;*
- *ako je* $\mathcal{A}$ *atomička formula* $\bot$ *onda je* $I_v(\mathcal{A}) = 0$*;*
- *ako je* $\mathcal{A}$ *atomička formula* $p(t_1, t_2, \ldots, t_n)$ *(pri čemu je* $ar(p) = n$*) i ako je* $I_v(t_i) = d_i$ *za* $i = 1, 2, \ldots, n$ *(pri čemu je* $d_i \in D$*), onda je* $I_v(\mathcal{A}) = p_I(d_1, d_2, \ldots, d_n)$*;*
- *ako je* $\mathcal{A} = \neg\mathcal{B}$*, onda je*

$$I_v(\mathcal{A}) = \begin{cases} 0, & \text{ako je } I_v(\mathcal{B}) = 1 \\ 1, & \text{ako je } I_v(\mathcal{B}) = 0 \end{cases}$$

- *ako je* $\mathcal{A} = \mathcal{B}_1 \wedge \mathcal{B}_2$*, onda je*

$$I_v(\mathcal{A}) = \begin{cases} 1, & \text{ako je } I_v(\mathcal{B}_1) = 1 \text{ i } I_v(\mathcal{B}_2) = 1 \\ 0, & \text{inače} \end{cases}$$

- *ako je* $\mathcal{A} = \mathcal{B}_1 \vee \mathcal{B}_2$*, onda je*

$$I_v(\mathcal{A}) = \begin{cases} 1, & \text{ako je } I_v(\mathcal{B}_1) = 1 \text{ ili } I_v(\mathcal{B}_2) = 1 \\ 0, & \text{inače} \end{cases}$$

- *ako je* $\mathcal{A} = \mathcal{B}_1 \Rightarrow \mathcal{B}_2$*, onda je*

$$I_v(\mathcal{A}) = \begin{cases} 0, & \text{ako je } I_v(\mathcal{B}_1) = 1 \text{ i } I_v(\mathcal{B}_2) = 0 \\ 1, & \text{inače} \end{cases}$$

- *ako je* $\mathcal{A} = \mathcal{B}_1 \Leftrightarrow \mathcal{B}_2$*, onda je*

$$I_v(\mathcal{A}) = \begin{cases} 1, & \text{ako je } I_v(\mathcal{B}_1) = I_v(\mathcal{B}_2) \\ 0, & \text{inače} \end{cases}$$

- *ako je* $\mathcal{A} = (\exists x)\mathcal{B}$*, onda je* $I_v(\mathcal{A}) = 1$ *ako postoji valuacija* w *sa domenom* D *takva da je* $w \sim_x v$ *i* $I_w(\mathcal{B}) = 1$*; inače je* $I_v(\mathcal{A}) = 0$*;*

- *ako je* $\mathcal{A} = (\forall x)\mathcal{B}$*, onda je* $I_v(\mathcal{A}) = 0$ *ako postoji valuacija* w *sa domenom* D *takva da je* $w \sim_x v$ *i* $I_w(\mathcal{B}) = 0$*; inače je* $I_v(\mathcal{A}) = 1$.

Indukcijom se može dokazati da je na opisani način svakoj formuli $\mathcal{A}$ nad signaturom $\mathcal{L}$ i skupom V pridružena (jedinstvena) vrednost $I_v(\mathcal{A})$. Primetimo da $I_v(\mathcal{A})$ zavisi od $v(x)$ samo ako promenljiva x ima slobodna pojavljivanja u formuli $\mathcal{A}$. Vrednost $I_v(\mathcal{A})$, dakle, zavisi samo od slobodnih promenljivih u formuli $\mathcal{A}$. Specijalno, ako je $\mathcal{A}$ rečenica, vrednost $I_v(\mathcal{A})$ uopšte ne zavisi od v, pa tada umesto $I_v(\mathcal{A})$ pišemo kraće $I(\mathcal{A})$.

Definicija 3.11 *Ako je interpretacija* I_v *određena* $\mathcal{L}$*-strukturom* $\mathfrak{D}$ *i valuacijom* v *i ako za* $\mathcal{L}$*-formulu* $\mathcal{A}$ *važi* $I_v(\mathcal{A}) = 1$*, onda kažemo da interpretacija* I_v zadovoljava *formulu* $\mathcal{A}$*, da je formula* $\mathcal{A}$ tačna u interpretaciji I_v *i da je* $\mathcal{L}$*-struktura* $\mathfrak{D}$ *sa valuacijom* v model *formule* $\mathcal{A}$ *i pišemo* $(\mathfrak{D}, v) \models \mathcal{A}$*. Formula* $\mathcal{A}$ *je* zadovoljiva *u* $\mathcal{L}$*-strukturi* $\mathfrak{D}$ *ako postoji valuacija* v *takva da je* $(\mathfrak{D}, v) \models \mathcal{A}$*.* $\mathcal{L}$*-formula* $\mathcal{A}$ *je* zadovoljiva *ako postoje* $\mathcal{L}$*-struktura* $\mathfrak{D}$ *i valuacija* v *takve da je* $(\mathfrak{D}, v) \models \mathcal{A}$*.*

Ako formula nije zadovoljiva, onda kažemo da je ona kontradiktorna*.*

Definicija 3.12 *Ako je za neku* $\mathcal{L}$*-strukturu* $\mathfrak{D}$ *formula* $\mathcal{A}$ *tačna za svaku valuaciju* v*, tj. u svakoj interpretaciji* I_v*, onda kažemo da je* $\mathcal{L}$*-struktura* $\mathfrak{D}$ model *formule* $\mathcal{A}$*, kažemo da je formula* $\mathcal{A}$ valjana *u* $\mathcal{L}$*-strukturi* $\mathfrak{D}$ *i pišemo* $\mathfrak{D} \models \mathcal{A}$*. Ako je formula nad signaturom* $\mathcal{L}$ *valjana u svakoj* $\mathcal{L}$*-strukturi, onda za tu formulu kažemo da je* valjana *i to zapisujemo* $\models \mathcal{A}$*.*

Ako formula nije valjana, onda kažemo da je ona poreciva*.*

Ako nije $\mathfrak{D} \models \mathcal{A}$*, onda pišemo* $\mathfrak{D} \not\models \mathcal{A}$ *i kažemo da je* $\mathfrak{D}$ kontramodel *za* $\mathcal{A}$*.*

Analogne definicije uvodimo za skupove formula.

Definicija 3.13 *Skup rečenica* Γ *je* konzinstentan *ili* zadovoljiv *ako ima bar jedan model. Inače, kažemo da je* nekonzistentan, nezadovoljiv, protivrečan *ili* kontradiktoran*.*

Teorema 3.2 *Ako su formule* $\mathcal{A}$ *i* $\mathcal{A} \Rightarrow \mathcal{B}$ *(nad nekom signaturom* $\mathcal{L}$*) valjane, onda je i formula* $\mathcal{B}$ *valjana.*

Dokaz: Pretpostavimo da postoje $\mathcal{L}$-struktura $\mathfrak{D}$ i odgovarajuća interpretacija I_v u kojoj formula $\mathcal{B}$ nije tačna. Formula $\mathcal{A}$ je valjana, pa je tačna i u interpretaciji I_v. U toj interpretaciji, onda, formula $\mathcal{A} \Rightarrow \mathcal{B}$ nije tačna (jer je $I_v(\mathcal{A}) = 1$ i $I_v(\mathcal{B}) = 0$), što protivreči pretpostavci da je formula $\mathcal{A} \Rightarrow \mathcal{B}$ valjana. Dakle, polazna pretpostavka je pogrešna, pa je formula $\mathcal{B}$ tačna u svakoj interpretaciji, tj. ona je valjana, što je i trebalo dokazati. □

Teorema 3.3 *Formula* $\mathcal{A}$ *nad signaturom* $\mathcal{L}$ *je valjana u* $\mathcal{L}$*-strukturi* $\mathfrak{D}$ *ako i samo ako je formula* $(\forall x)\mathcal{A}$ *valjana u* $\mathfrak{D}$*.*

Dokaz: Pretpostavimo da je formula $\mathcal{A}$ valjana u $\mathfrak{D}$. Pretpostavimo da formula $(\forall x)\mathcal{A}$ nije valjana u $\mathfrak{D}$, tj. pretpostavimo da postoji valuacija v takva da je $I_v((\forall x)\mathcal{A}) = 0$. Odatle sledi da postoji valuacija w za koju je $w \sim_x v$ i važi $I_w(\mathcal{A}) = 0$, pa formula $\mathcal{A}$ nije valjana u $\mathfrak{D}$, što je u suprotnosti sa pretpostavkom. Dakle, formula $(\forall x)\mathcal{A}$ je valjana u $\mathfrak{D}$.

Pretpostavimo da je formula $(\forall x)\mathcal{A}$ valjana u $\mathfrak{D}$. To znači da za svaku valuaciju v važi $I_v((\forall x)\mathcal{A}) = 1$. Pretpostavimo da formula $\mathcal{A}$ nije valjana u $\mathfrak{D}$. Tada postoji valuacija w takva da je $I_w(\mathcal{A}) = 0$, pa je $I_w((\forall x)\mathcal{A}) = 0$, što je u suprotnosti sa pretpostavkom. Dakle, formula $\mathcal{A}$ je valjana u $\mathfrak{D}$. □

Teorema 3.4 *Formula $\mathcal{A}$ je valjana ako i samo ako je formula $(\forall x)\mathcal{A}$ valjana.*

Dokaz: Neka je $\mathcal{A}$ formula nad signaturom $\mathcal{L}$. Ako je formula $\mathcal{A}$ valjana, onda je ona valjana u svakoj $\mathcal{L}$-strukturi $\mathfrak{D}$, pa je onda, na osnovu teoreme 3.3, u svakoj $\mathcal{L}$-strukturi $\mathfrak{D}$ valjana i formula $(\forall x)\mathcal{A}$. Analogno važi i obratno, pa je formula $\mathcal{A}$ valjana ako i samo ako je formula $(\forall x)\mathcal{A}$ valjana. □

Na osnovu teorema 3.3 i 3.4 i jednostavnog induktivnog argumenta slede naredne dve teoreme.

Teorema 3.5 *Formula $\mathcal{A}$ nad signaturom $\mathcal{L}$ je valjana u $\mathcal{L}$-strukturi $\mathfrak{D}$ ako i samo ako je formula $\forall * \mathcal{A}$ valjana u $\mathfrak{D}$.*

Teorema 3.6 *Formula $\mathcal{A}$ je valjana ako i samo ako je formula $\forall * \mathcal{A}$ valjana.*

Ako je formula rečenica, ona nema slobodnih promenljivih, pa na njenu vrednost u interpretaciji ne utiče valuacija. Dakle, ako je rečenica nad signaturom $\mathcal{L}$ zadovoljiva u $\mathcal{L}$-strukturi $\mathfrak{D}$, onda je ona i valjana u $\mathfrak{D}$, a trivijalno važi i obratno — ako je rečenica nad signaturom $\mathcal{L}$ valjana u $\mathcal{L}$-strukturi $\mathfrak{D}$, onda je ona i zadovoljiva u $\mathfrak{D}$. Specijalno, rečenica $\forall * \mathcal{A}$ nad signaturom $\mathcal{L}$ je zadovoljiva u $\mathfrak{D}$ akko je valjana u $\mathfrak{D}$. Odatle i iz teoreme 3.5 neposredno sledi naredno tvrđenje.

Teorema 3.7 *Za formulu $\mathcal{A}$ nad signaturom $\mathcal{L}$ i $\mathcal{L}$-strukturu $\mathfrak{D}$ važi:*
$\forall * \mathcal{A}$ je zadovoljiva u $\mathfrak{D}$ akko $\forall * \mathcal{A}$ je valjana u $\mathfrak{D}$ akko $\mathcal{A}$ je valjana u $\mathfrak{D}$.

Naredne tri teoreme analogne su (preciznije dualne) prethodnim teoremama (i ne navodimo njihove dokaze).

Teorema 3.8 *Formula $\mathcal{A}$ nad signaturom $\mathcal{L}$ je zadovoljiva u $\mathcal{L}$-strukturi $\mathfrak{D}$ ako i samo ako je formula $\exists * \mathcal{A}$ zadovoljiva u $\mathfrak{D}$.*

Teorema 3.9 *Formula $\mathcal{A}$ je zadovoljiva ako i samo ako je formula $\exists * \mathcal{A}$ zadovoljiva.*

Teorema 3.10 *Za formulu $\mathcal{A}$ nad signaturom $\mathcal{L}$ i $\mathcal{L}$-strukturu $\mathfrak{D}$ važi:*
$\exists * \mathcal{A}$ je valjana u $\mathfrak{D}$ akko $\exists * \mathcal{A}$ je zadovoljiva u $\mathfrak{D}$ akko $\mathcal{A}$ je zadovoljiva u $\mathfrak{D}$.

Zadaci

Zadatak 47 $\surd$ *Odrediti bar jedan model formule* $(\forall x)(p(x) \Rightarrow p(f(x)))$.

Zadatak 48 $\surd$ *Ispitati da li je* $\mathcal{L}$*-struktura data sa* $D = \{a, b, c\}$ *i*

	f_I
a	b
b	a
c	a

p_I	a	b	c
a	1	1	0
b	1	0	1
c	0	0	1

model formule $(\forall x)(p(x, f(x)) \Rightarrow p(f(x), x))$.

Zadatak 49 $\surd$ *Odrediti sve dvočlane modele formule* $(\forall x)(\exists y)(p(x, y) \Rightarrow \neg p(y, x))$.

Zadatak 50 $\surd$ *Odrediti jedan model i jedan kontramodel za formulu* $(\forall x)(\exists y)(p(f(x, y), a))$.

Zadatak 51 $\surd$ *Data je formula*
$\mathcal{A} = (\forall x)(p(x, f(x)) \wedge \neg p(x, x)) \wedge (\forall x)(\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))$.
(a) Odrediti bar jedan model za formulu $\mathcal{A}$.
(b) Odrediti bar jedan kontramodel za formulu $\mathcal{A}$.
(c) Dokazati da svaki model formule $\mathcal{A}$ *ima beskonačan domen.*

Zadatak 52 $\surd$ *Dokazati da je formula* $(\forall x)(\forall y)(\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))$ *valjana.*

Zadatak 53 *Dokazati da su naredne formule valjane:*
(a) $(\exists x)(\forall y)\mathcal{A} \Rightarrow (\forall y)(\exists x)\mathcal{A}$
(b) $((\exists x)(\mathcal{A} \Rightarrow \mathcal{B})) \Leftrightarrow (\mathcal{A} \Rightarrow (\exists x)\mathcal{B})$*, pri čemu promenljiva* x *nije slobodna u* $\mathcal{A}$.

Zadatak 54 *Dokazati da naredne formule nisu valjane:*
(a) $(\exists x)\mathcal{A}_1 \wedge (\exists x)\mathcal{A}_2 \Leftrightarrow (\exists x)(\mathcal{A}_1 \wedge \mathcal{A}_2)$
(b) $(\forall x)\mathcal{A}_1 \vee (\forall x)\mathcal{A}_2 \Leftrightarrow (\forall x)(\mathcal{A}_1 \vee \mathcal{A}_2)$

Zadatak 55 *Dokazati da formula* $(\forall x)(\exists y)p(x, y) \Leftrightarrow (\exists y)(\forall x)p(x, y)$ *nije valjana.*

Zadatak 56 *Dokazati da je sledeća formula valjana:*

$$((\forall x)\mathcal{A}) \wedge \mathcal{B} \Leftrightarrow (\forall x)(\mathcal{A} \wedge \mathcal{B})$$

pri čemu formula $\mathcal{B}$ *nema slobodnih pojavljivanja promenljive* x*. Dokazati da data formula nije valjana ako se izostavi navedeni dodatni uslov.*

3.2.2 Logičke posledice, logički ekvivalentne formule, supstitucija

Definicija 3.14 *Neka je Γ skup formula i neka je $\mathcal{A}$ formula nad signaturom $\mathcal{L}$. Kažemo da je formula $\mathcal{A}$* logička posledica *skupa formula Γ i pišemo $\Gamma \models \mathcal{A}$ ukoliko za svaku $\mathcal{L}$-strukturu $\mathfrak{D}$ i svaku valuaciju v važi: ako za svaku formulu $\mathcal{B}$ iz Γ važi $(\mathfrak{D}, v) \models \mathcal{B}$, onda važi $(\mathfrak{D}, v) \models \mathcal{A}$.*

Drugim rečima, kažemo da je formula $\mathcal{A}$ logička posledica skupa formula Γ ako je svaki model za Γ istovremeno i model za $\mathcal{A}$.

Ako je skup Γ konačan, tj. ako je $\Gamma = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k\}$, onda pišemo $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k \models \mathcal{A}$. Ako je Γ prazan skup, onda pišemo $\models \mathcal{A}$. Ako je $\models \mathcal{A}$, onda formulu $\mathcal{A}$ zadovoljava svaka interpretacija i tada je formula $\mathcal{A}$ valjana.

Ako ne važi $\Gamma \models \mathcal{A}$, onda to zapisujemo $\Gamma \not\models \mathcal{A}$.

Na osnovu definicije logičke posledice, jednostavno se dokazuje naredno tvrđenje (analogno teoremi 2.3).

Teorema 3.11

(a) Svaka valjana formula je logička posledica praznog skupa formula.

(b) Ako je skup Γ kontradiktoran, onda je svaka formula njegova logička posledica. Specijalno, svaka formula je logička posledica skupa $\{\bot\}$.

(c) Ako je $\Gamma \subset \Delta$ i $\Gamma \models \mathcal{A}$, onda je $\Delta \models \mathcal{A}$.

(d) Ako je formula $\mathcal{A}$ valjana i $\Gamma \models \mathcal{B}$, onda je $\Gamma \setminus \{\mathcal{A}\} \models \mathcal{B}$.

Definicija 3.15 *Kažemo da su formule $\mathcal{A}$ i $\mathcal{B}$* logički ekvivalentne *i pišemo $\mathcal{A} \equiv \mathcal{B}$ ako je $\mathcal{A}$ logička posledica formule $\mathcal{B}$ i $\mathcal{B}$ je logička posledica formule $\mathcal{A}$.*

Ako je svaki model za $\mathcal{A}$ istovremeno i model za $\mathcal{B}$ i obratno, onda u bilo kojoj valuaciji formule $\mathcal{A}$ i $\mathcal{B}$ imaju jednake vrednosti. Tvrđenja oblika $\mathcal{A} \equiv \mathcal{B}$ zovemo *logičkim ekvivalencijama* (ili kraće *ekvivalencijama*). Relacija $\equiv$ je, očigledno, relacija ekvivalencije nad skupom formula.

Teorema 3.12 *Ako za $\mathcal{L}$-formule $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{B}_1$ i $\mathcal{B}_2$ važi $\mathcal{A}_1 \equiv \mathcal{A}_2$ i $\mathcal{B}_1 \equiv \mathcal{B}_2$, onda je:*

(a) $\neg\mathcal{A}_1 \equiv \neg\mathcal{A}_2$

(b) $\mathcal{A}_1 \wedge \mathcal{B}_1 \equiv \mathcal{A}_2 \wedge \mathcal{B}_2$

(c) $\mathcal{A}_1 \vee \mathcal{B}_1 \equiv \mathcal{A}_2 \vee \mathcal{B}_2$

(d) $\mathcal{A}_1 \Rightarrow \mathcal{B}_1 \equiv \mathcal{A}_2 \Rightarrow \mathcal{B}_2$

(e) $\mathcal{A}_1 \Leftrightarrow \mathcal{B}_1 \equiv \mathcal{A}_2 \Leftrightarrow \mathcal{B}_2$

(f) $(\forall x)\mathcal{A}_1 \equiv (\forall x)\mathcal{A}_2$

(g) $(\exists x)\mathcal{A}_1 \equiv (\exists x)\mathcal{A}_2$

Dokaz: Delovi *(a)–(e)* dokazuju se jednostavno, analogno kao u dokazu teoreme 2.6.

Dokažimo deo *(f)*. Neka je $\mathfrak{D}$ proizvoljna $\mathcal{L}$-struktura. Pretpostavimo da važi $I_v((\forall x)\mathcal{A}_1) = 1$ i dokažimo da onda važi i $I_v((\forall x)\mathcal{A}_2) = 1$. Iz $I_v((\forall x)\mathcal{A}_1) = 1$ sledi da za svaku valuaciju v', takvu da je $v' \sim_x v$, važi $I_{v'}(\mathcal{A}_1) = 1$. Kako važi $\mathcal{A}_1 \equiv \mathcal{A}_2$ (tj. važi $I_v(\mathcal{A}_1) = 1$ ako i samo ako važi $I_v(\mathcal{A}_2) = 1$), sledi da za svaku valuaciju v', takvu da je $v' \sim_x v$, važi i $I_{v'}(\mathcal{A}_2) = 1$, odakle dalje sledi da važi $I_v((\forall x)\mathcal{A}_2) = 1$. Dakle, važi $(\forall x)\mathcal{A}_1 \models (\forall x)\mathcal{A}_2$, pa, potpuno analogno, važi i $(\forall x)\mathcal{A}_2 \models (\forall x)\mathcal{A}_1$, odakle sledi $(\forall x)\mathcal{A}_1 \equiv (\forall x)\mathcal{A}_2$. Deo *(g)* dokazuje se analogno. □

Teorema 3.13 *Za datu signaturu $\mathcal{L}$, dve $\mathcal{L}$-formule $\mathcal{A}$ i $\mathcal{B}$ su logički ekvivalentne ako i samo ako je formula $\mathcal{A} \Leftrightarrow \mathcal{B}$ valjana.*

Dokaz: Pretpostavimo da su formule $\mathcal{A}$ i $\mathcal{B}$ logički ekvivalentne. Dakle, za svaku $\mathcal{L}$-strukturu $\mathfrak{D}$ i valuaciju v, iz $(\mathfrak{D}, v) \models \mathcal{A}$ sledi $(\mathfrak{D}, v) \models \mathcal{B}$ i iz $(\mathfrak{D}, v) \models \mathcal{B}$ sledi $(\mathfrak{D}, v) \models \mathcal{A}$. Dakle, ako je $I_v(\mathcal{A}) = 1$, onda mora da je i $I_v(\mathcal{B}) = 1$ i obratno, tj. nije moguće da jedna od formula $\mathcal{A}$ i $\mathcal{B}$ ima vrednost 1, a druga vrednost 0 u $\mathfrak{D}$ sa valuacijom v. Dakle, uvek važi $I_v(\mathcal{A}) = I_v(\mathcal{B})$, pa je (na osnovu definicije 3.10) uvek $I_v(\mathcal{A} \Leftrightarrow \mathcal{B}) = 1$. Dakle, formula $\mathcal{A} \Leftrightarrow \mathcal{B}$ je valjana u $\mathcal{L}$-strukturi $\mathfrak{D}$, a kako to važi za svaku $\mathcal{L}$-strukturu, sledi da je formula $\mathcal{A} \Leftrightarrow \mathcal{B}$ valjana.

Pretpostavimo da je formula $\mathcal{A} \Leftrightarrow \mathcal{B}$ valjana. Onda je ona valjana u svakoj $\mathcal{L}$-strukturi $\mathfrak{D}$, tj. za svaku $\mathcal{L}$-strukturu $\mathfrak{D}$ (i odgovarajuću interpretaciju I) važiće $I(\mathcal{A} \Leftrightarrow \mathcal{B}) = 1$, pa će za svaku valuaciju v važiti $I_v(\mathcal{A} \Leftrightarrow \mathcal{B}) = 1$. Odatle sledi da je $I_v(\mathcal{A}) = I_v(\mathcal{B})$. Ako je $I_v(\mathcal{A}) = 1$, onda je $I_v(\mathcal{B}) = 1$, pa je $\mathcal{A} \models \mathcal{B}$. Analogno, važi i obratno — $\mathcal{B} \models \mathcal{A}$, pa su formule $\mathcal{A}$ i $\mathcal{B}$ logički ekvivalentne. □

Primer 3.3 *Može se dokazati da za proizvoljnu $\mathcal{L}$-formulu $\mathcal{A}$ važi $\neg(\exists x)\mathcal{A} \equiv (\forall x)\neg\mathcal{A}$. Neka je $\mathfrak{D}$ proizvoljna $\mathcal{L}$-struktura. Pretpostavimo da važi $I_v(\neg(\exists x)\mathcal{A}) = 1$ i dokažimo da onda važi i $I_v((\forall x)\neg\mathcal{A}) = 1$. Iz $I_v(\neg(\exists x)\mathcal{A}) = 1$ sledi $I_v((\exists x)\mathcal{A}) = 0$, pa u svakoj valuaciji v', takvoj da je $v' \sim_x v$, važi $I_{v'}(\mathcal{A}) = 0$. To znači da u svakoj valuaciji v', takvoj da je $v' \sim_x v$, važi $I_{v'}(\neg\mathcal{A}) = 1$, a odatle sledi da u svakoj valuaciji v'', takvoj da je $v'' \sim_x v'$, važi $I_{v''}((\forall x)\neg\mathcal{A}) = 1$, pa i u valuaciji v, tj. $I_v((\forall x)\neg\mathcal{A}) = 1$, što je i trebalo dokazati. Drugi smer tvrđenja (da iz $I_v((\forall x)\neg\mathcal{A}) = 1$ sledi $I_v(\neg(\exists x)\mathcal{A}) = 1$) dokazuje se analogno.*

Primer 3.4 *Neke od logičkih ekvivalencija logike prvog reda (ili, preciznije, neke od shema logičkih ekvivalencija logike prvog reda) su:*

$\neg(\exists x)\mathcal{A}$	$\equiv$	$(\forall x)\neg\mathcal{A}$	*De Morganov zakon*
$\neg(\forall x)\mathcal{A}$	$\equiv$	$(\exists x)\neg\mathcal{A}$	*De Morganov zakon*
$(\exists x)(\mathcal{A}\vee\mathcal{B})$	$\equiv$	$(\exists x)\mathcal{A}\vee(\exists x)\mathcal{B}$	*zakon distributivnosti* $\exists$ *prema* $\vee$
$(\forall x)(\mathcal{A}\wedge\mathcal{B})$	$\equiv$	$(\forall x)\mathcal{A}\wedge(\forall x)\mathcal{B}$	*zakon distributivnosti* $\forall$ *prema* $\wedge$
$(\exists x)(\mathcal{A}\wedge\mathcal{B})$	$\equiv$	$(\exists x)\mathcal{A}\wedge\mathcal{B}$	*zakon distributivnosti* $\exists$ *prema* $\wedge$ *(pri čemu* $\mathcal{B}$ *ne sadrži slobodna pojavljivanja promenljive* x*)*
$(\forall x)(\mathcal{A}\vee\mathcal{B})$	$\equiv$	$(\forall x)\mathcal{A}\vee\mathcal{B}$	*zakon distributivnosti* $\forall$ *prema* $\vee$ *(pri čemu* $\mathcal{B}$ *ne sadrži slobodna pojavljivanja promenljive* x*)*

Definicija 3.16 *Term dobijen zamenom (supstitucijom) promenljive x termom t_x u termu t označavamo sa $t[x\mapsto t_x]$ i definišemo na sledeći način:*

- *ako je t simbol konstante, onda je $t[x\mapsto t_x]=t$;*
- *ako je $t=x$, onda je $t[x\mapsto t_x]=t_x$;*
- *ako je $t=y$, gde je $y\neq x$, onda je $t[x\mapsto t_x]=t$;*
- *ako je $t=f(t_1,t_2,\ldots,t_n)$, onda je $t[x\mapsto t_x]=f(t_1[x\mapsto t_x],t_2[x\mapsto t_x],\ldots,t_n[x\mapsto t_x])$.*

Definicija 3.17 *Formulu dobijenu zamenom (supstitucijom) promenljive x termom t_x u formuli $\mathcal{A}$ označavamo sa $\mathcal{A}[x\mapsto t_x]$ i definišemo na sledeći način:*

- $\top[x\mapsto t_x]=\top$;
- $\bot[x\mapsto t_x]=\bot$;
- *ako je $\mathcal{A}=p(t_1,t_2,\ldots,t_n)$, onda je $\mathcal{A}[x\mapsto t_x]=p(t_1[x\mapsto t_x],t_2[x\mapsto t_x],\ldots,t_n[x\mapsto t_x])$;*
- $(\neg\mathcal{A})[x\mapsto t_x]=\neg(\mathcal{A}[x\mapsto t_x])$;
- $(\mathcal{A}\wedge\mathcal{B})[x\mapsto t_x]=(\mathcal{A}[x\mapsto t_x]\wedge\mathcal{B}[x\mapsto t_x])$;
- $(\mathcal{A}\vee\mathcal{B})[x\mapsto t_x]=(\mathcal{A}[x\mapsto t_x]\vee\mathcal{B}[x\mapsto t_x])$;
- $(\mathcal{A}\Rightarrow\mathcal{B})[x\mapsto t_x]=(\mathcal{A}[x\mapsto t_x]\Rightarrow\mathcal{B}[x\mapsto t_x])$;
- $(\mathcal{A}\Leftrightarrow\mathcal{B})[x\mapsto t_x]=(\mathcal{A}[x\mapsto t_x]\Leftrightarrow\mathcal{B}[x\mapsto t_x])$;
- $(\forall x\mathcal{A})[x\mapsto t_x]=(\forall x\mathcal{A})$;
- $(\exists x\mathcal{A})[x\mapsto t_x]=(\exists x\mathcal{A})$;
- *ako je $x\neq y$, neka je z promenljiva koja se ne pojavljuje ni u $(\forall y)\mathcal{A}$ ni u t_x; tada je $(\forall y\mathcal{A})[x\mapsto t_x]=(\forall z)\mathcal{A}[y\mapsto z][x\mapsto t_x]$;*
- *ako je $x\neq y$, neka je z promenljiva koja se ne pojavljuje ni u $(\exists y)\mathcal{A}$ ni u t_x; tada je $(\exists y\mathcal{A})[x\mapsto t_x]=(\exists z)\mathcal{A}[y\mapsto z][x\mapsto t_x]$.*

Primetimo da poslednja dva pravila u prethodnoj definiciji obezbeđuju, na primer, da $((\forall y)p(x,y))[x \mapsto y]$ ne bude $(\forall y)p(y,y)$ već $(\forall z)p(y,z)$.

Primer 3.5 *Važi:*

$(\forall x)\mathcal{A} \equiv (\forall y)(\mathcal{A}[x \mapsto y])$ *zakon o preimenovanju vezane promenljive (pri čemu $\mathcal{A}$ ne sadrži slobodna pojavljivanja promenljive y)*

$(\exists x)\mathcal{A} \equiv (\exists y)(\mathcal{A}[x \mapsto y])$ *zakon o preimenovanju vezane promenljive (pri čemu $\mathcal{A}$ ne sadrži slobodna pojavljivanja promenljive y)*

U daljem tekstu ćemo pod terminom *izraz* podrazumevati i termove i formule.

Definicija 3.18 Uopštena zamena *(supstitucija) σ je skup zamena $[x_1 \mapsto t_1]$, $[x_2 \mapsto t_2]$, ..., $[x_n \mapsto t_n]$ gde su x_i promenljive i t_i su proizvoljni termovi i gde je $x_i \neq x_j$ za $i \neq j$. Takvu zamenu zapisujemo kraće $[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]$.*

Uopštena zamena primenjuje se simultano na sva pojavljivanja promenljivih x_1, x_2, ..., x_n u polaznom izrazu i samo na njih (tj. ne primenjuje se na podtermove dobijene zamenama).

U daljem tekstu ćemo umesto termina *uopštena zamena* (*uopštena supstitucija*) koristiti termin *zamena* (*supstitucija*).

Izraz koji je rezultat primene zamene σ nad izrazom E, označavamo sa $E\sigma$.

Očigledno, iz zamene $[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]$ se mogu (ali ne moraju) izostaviti sve pojedinačne zamene oblika $x_i \mapsto x_i$.

Primer 3.6 *Za $\sigma = [x \mapsto f(y)]$ i $s = g(a,x)$ važi $s\sigma = g(a, f(y))$.*

Za $\sigma = [x \mapsto f(x)]$ i $s = g(a,x)$ važi $s\sigma = g(a, f(x))$.

Za $\sigma = [x \mapsto f(y), y \mapsto a]$, $s = g(a,x)$ i $t = g(y, g(x,y))$ važi $s\sigma = g(a, f(y))$ i $t\sigma = g(a, g(f(y), a))$.

Ukoliko u zameni $\sigma = [x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]$ nijedan od termova t_i ne sadrži nijednu od promenljivih x_j (sem, eventualno, ako je $t_i = x_i$ za neko i), onda je efekat te zamene jednak efektu sukcesivno primenjenih pojedinačnih zamena. Supstitucija σ je idempotentna (tj. za bilo koji izraz E važi $E\sigma = (E\sigma)\sigma$) ako i samo ako važi taj uslov — da nijedan od termova t_i ne sadrži nijednu od promenljivih x_j (sem, eventualno, ako je $t_i = x_i$ za neko i).

Definicija 3.19 *Za supstitucije $\phi = [x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]$ i $\lambda = [y_1 \mapsto s_1, y_2 \mapsto s_2, \ldots, y_m \mapsto s_m]$,* kompozicija supstitucija *$\phi\lambda$ je supstitucija $[x_1 \mapsto t_1\lambda, x_2 \mapsto t_2\lambda, \ldots, x_n \mapsto t_n\lambda, y_1 \mapsto s_1, y_2 \mapsto s_2, \ldots, y_m \mapsto s_m]$ iz koje su izbrisane zamene oblika $x_i \mapsto x_i$, kao i zamene oblika $y_i \mapsto s_i$, gde je $y_i = x_j$ za neko j.*

Primer 3.7 *Za* $\phi = [x \mapsto f(y)]$ *i* $\lambda = [y \mapsto g(z)]$*, važi* $\phi\lambda = [x \mapsto f(g(z)), y \mapsto g(z)]$.
Za $\phi = [x \mapsto f(y)]$ *i* $\lambda = [y \mapsto g(x)]$*, važi* $\phi\lambda = [x \mapsto f(g(x)), y \mapsto g(x)]$.
Za $\phi = [x \mapsto y]$ *i* $\lambda = [y \mapsto x]$*, važi* $\phi\lambda = [y \mapsto x]$.
Za $\phi = [x \mapsto f(y)]$ *i* $\lambda = [x \mapsto g(z)]$*, važi* $\phi\lambda = [x \mapsto f(y)]$.
Za $\phi = [x \mapsto f(x)]$ *i* $\lambda = [x \mapsto a]$*, važi* $\phi\lambda = [x \mapsto f(a)]$.

Može se dokazati da je kompozicija supstitucija asocijativna, kao i da važi $E(\phi\lambda) = (E\phi)\lambda$.

Definicija 3.20 *Ako je* E *izraz (term ili formula) i ako je* ϕ *supstitucija, onda kažemo da je* $E\phi$ instanca *(ili* primerak*) izraza* E*. Ako je izraz* $E\phi$ *bazni, onda kažemo da je on* bazna instanca *izraza* E*.*

Definicija 3.21 *Neka su formule* $\mathcal{B}_1$ *i* $\mathcal{B}_2$ *takve da formula* $\mathcal{B}_2$ *nema nijednu slobodnu promenljivu koju nema formula* $\mathcal{B}_1$*. Formulu dobijenu zamenom (supstitucijom) formule* $\mathcal{B}_1$ *formulom* $\mathcal{B}_2$ *u formuli* $\mathcal{A}$*, označavamo sa* $\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ *i definišemo na sledeći način:*

- *ako je formula* $\mathcal{A}$ *instanca formule* $\mathcal{B}_1$*, tj. ako je* $\mathcal{A} = \mathcal{B}_1\sigma$ *za neku supstituciju* σ*, onda je* $\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] = \mathcal{B}_2\sigma$*;*
- *ako je formula* $\mathcal{A}$ *atomička formula i nije instanca formule* $\mathcal{B}_1$*, onda je* $\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] = \mathcal{A}$*;*
- $(\neg\mathcal{A})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = \neg(\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\mathcal{A} \wedge \mathcal{B})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] \wedge \mathcal{B}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\mathcal{A} \vee \mathcal{B})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] \vee \mathcal{B}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\mathcal{A} \Rightarrow \mathcal{B})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] \Rightarrow \mathcal{B}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\mathcal{A} \Leftrightarrow \mathcal{B})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] \Leftrightarrow \mathcal{B}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\forall x\mathcal{A})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\forall x)(\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$*;*
- $(\exists x\mathcal{A})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\exists x)(\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$.

Naglasimo da smo u prethodnoj definiciji datom restrikcijom pojednostavili problem slobodnih pojavljivanjima promenljivih u formulama $\mathcal{B}_1$ i $\mathcal{B}_2$. Osnovna svrha koncepta zamene formule formulom je u zameni formule logički ekvivalentnom formulom i za tu svrhu je data definicija dovoljna.

Teorema 3.14 (Teorema o zameni) *Ako važi* $\mathcal{B}_1 \equiv \mathcal{B}_2$*, onda je* $\mathcal{A} \equiv \mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2]$.

Dokaz: Ako je formula $\mathcal{A}$ instanca formule $\mathcal{B}_1$, tj. ako je $\mathcal{A} = \mathcal{B}_1\sigma$ za neku supstituciju σ, onda je $\mathcal{A} = \mathcal{B}_1\sigma \equiv \mathcal{B}_2\sigma = \mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2]$.

Ako je $\mathcal{A}$ atomička formula i nije instanca formule $\mathcal{B}_1$, onda je $\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2] = \mathcal{A}$, pa trivijalno važi $\mathcal{A} \equiv \mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2]$.

Pretpostavimo da tvrđenje važi za formule $\mathcal{A}_1$ i $\mathcal{A}_2$ i dokažimo da važi i za formule $\neg\mathcal{A}_1$, $\mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A}_1 \vee \mathcal{A}_2$, $\mathcal{A}_1 \Rightarrow \mathcal{A}_2$, $\mathcal{A}_1 \Leftrightarrow \mathcal{A}_2$, $(\forall x)\mathcal{A}_1$ i $(\exists x)\mathcal{A}_1$.

Na osnovu definicije 3.21 važi $(\neg\mathcal{A}_1)[\mathcal{B}_1 \mapsto \mathcal{B}_2] = \neg(\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2])$. Na osnovu teoreme 3.12, iz $\mathcal{A}_1 \equiv \mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ sledi $\neg\mathcal{A}_1 \equiv \neg(\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2])$, pa važi $\neg\mathcal{A}_1 \equiv \neg(\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]) = (\neg\mathcal{A}_1)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$, što je i trebalo dokazati.

Na osnovu definicije 3.21 važi $(\mathcal{A}_1 \wedge \mathcal{A}_2)[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]) \wedge (\mathcal{A}_2[\mathcal{B}_1 \mapsto \mathcal{B}_2])$. Na osnovu teoreme 3.12, iz $\mathcal{A}_1 \equiv \mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ i $\mathcal{A}_2 \equiv \mathcal{A}_2[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ sledi $(\mathcal{A}_1 \wedge \mathcal{A}_2) \equiv (\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]) \wedge (\mathcal{A}_2[\mathcal{B}_1 \mapsto \mathcal{B}_2])$, pa važi $\mathcal{A}_1 \wedge \mathcal{A}_2 \equiv (\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]) \wedge (\mathcal{A}_2[\mathcal{B}_1 \mapsto \mathcal{B}_2]) = (\mathcal{A}_1 \wedge \mathcal{A}_2)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$, što je i trebalo dokazati. Analogno se dokazuje i $\mathcal{A}_1 \vee \mathcal{A}_2 \equiv (\mathcal{A}_1 \vee \mathcal{A}_2)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$, $\mathcal{A}_1 \Rightarrow \mathcal{A}_2 \equiv (\mathcal{A}_1 \Rightarrow \mathcal{A}_2)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$, $\mathcal{A}_1 \Leftrightarrow \mathcal{A}_2 \equiv (\mathcal{A}_1 \Leftrightarrow \mathcal{A}_2)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$.

Dokažimo da iz $\mathcal{A}_1 \equiv \mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ sledi $(\forall x)\mathcal{A}_1 \equiv ((\forall x)\mathcal{A}_1)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$. Na osnovu teoreme 3.12, iz $\mathcal{A}_1 \equiv \mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2]$ sledi $(\forall x)\mathcal{A}_1 \equiv (\forall x)(\mathcal{A}_1[\mathcal{B}_1 \mapsto \mathcal{B}_2])$. Na osnovu definicije zamene, važi $((\forall x)\mathcal{A})[\mathcal{B}_1 \mapsto \mathcal{B}_2] = (\forall x)(\mathcal{A}[\mathcal{B}_1 \mapsto \mathcal{B}_2])$, pa važi $(\forall x)\mathcal{A}_1 \equiv ((\forall x)\mathcal{A}_1)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$, što je i trebalo dokazati. Analogno se dokazuje i $(\exists x)\mathcal{A}_1 \equiv ((\exists x)\mathcal{A}_1)[\mathcal{B}_1 \mapsto \mathcal{B}_2]$.

S obzirom na to da tvrđenje važi za sve atomičke formule i na to da iz pretpostavke da važi za formule $\mathcal{A}_1$ i $\mathcal{A}_2$ sledi da važi i za formule $\neg\mathcal{A}_1$, $\mathcal{A}_1 \wedge \mathcal{A}_2$, $\mathcal{A}_1 \vee \mathcal{A}_2$, $\mathcal{A}_1 \Rightarrow \mathcal{A}_2$, $\mathcal{A}_1 \Leftrightarrow \mathcal{A}_2$, $(\forall x)\mathcal{A}_1$ i $(\exists x)\mathcal{A}_1$, na osnovu teoreme o indukciji (3.1) proizilazi da tvrđenje važi za svaku formulu. □

Definicijom 2.9 uvedena je zamena jedne iskazne formule u nekoj iskaznoj formuli drugom iskaznom formulom. Na analogan način se uvodi zamena iskaznog slova proizvoljnim izrazom nad određenim jezikom (npr. dobro zasnovanom formulom) u iskaznoj formuli. Naglasimo da je tako uvedena zamena čisto sintaksne prirode i da ona može da prevede iskaznu formulu u dobro zasnovanu formulu.

Teorema 3.15 *Ako je A iskazna formula koja je tautologija i sadrži (samo) iskazna slova $p_1, p_2, \ldots, p_n$ i ako su $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ proizvoljne dobro zasnovane formule nad signaturom $\mathcal{L}$, onda je $A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ dobro zasnovana formula (nad signaturom $\mathcal{L}$) i pri tom valjana. Formulu $A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ tada zovemo* izvodom tautologije *(ili* tautologijom prvog reda*).*

Dokaz: Indukcijom (nad skupom formula) jednostavno se dokazuje da je formula $A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ dobro zasnovana.

Neka je $\mathfrak{D}$ proizvoljna $\mathcal{L}$-struktura i v proizvoljna valuacija (prvog reda) promenljivih koje se pojavljuju u $\mathcal{A}_1$, $\mathcal{A}_2$, ..., $\mathcal{A}_n$. Neka je w iskazna valuacija za skup $\{p_1, p_2, \ldots, p_n\}$ takva da je $w(p_i) = I_v(\mathcal{A}_i)$ (gde je I_v interpretacija (prvog reda)). Indukcijom (nad skupom formula), jednostavno se dokazuje da onda važi $I_w(A) = I_v(A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n])$ (gde je I_w iskazna interpretacija, a I_v interpretacija prvog reda). Formula A je tautologija, pa za iskaznu interpretaciju I_w važi $I_w(A) = 1$, odakle sledi $I_v(A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]) = 1$. Kako to važi za proizvoljnu $\mathcal{L}$-strukturu i valuaciju v, sledi da je formula $A[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ valjana, što je i trebalo dokazati. □

Ako je formula izvod tautologije, onda je ona i valjana, ali ne važi obratno.

Primer 3.8 *Iskazna formula $A = (p \wedge q) \Leftrightarrow (q \wedge p)$ je tautologija, pa je formula $A[p \mapsto \mathcal{A}, q \mapsto \mathcal{B}] = (\mathcal{A} \wedge \mathcal{B}) \Leftrightarrow (\mathcal{B} \wedge \mathcal{A})$ tautologija prvog reda i, zato, valjana.*

Primer 3.9 *Formula $\neg(\exists x)\mathcal{A} \Leftrightarrow (\forall x)\neg\mathcal{A}$ je valjana, ali nije tautologija prvog reda.*

Teorema 3.16 *Neka za dve iskazne formule A_1 i A_2 važi $A_1 \equiv A_2$ i neka one zajedno sadrže (samo) iskazna slova p_1, p_2, ..., p_n. Ako su $\mathcal{A}_1$, $\mathcal{A}_2$, ..., $\mathcal{A}_n$ proizvoljne dobro zasnovane formule, onda su $A_1[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] = \mathcal{B}_1$ i $A_2[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] = \mathcal{B}_2$ dobro zasnovane formule i važi $\mathcal{B}_1 \equiv \mathcal{B}_2$.*

Dokaz: Iz $A_1 \equiv A_2$, na osnovu teoreme 2.7 sledi da je iskazna formula $A_1 \Leftrightarrow A_2$ tautologija. Na osnovu teoreme 3.15 sledi da je formula $(A_1 \Leftrightarrow A_2)[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ dobro zasnovana i valjana. Na osnovu svojstava zamene sledi da je formula $(A_1 \Leftrightarrow A_2)[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ (sintaksno) jednaka dobro zasnovanoj formuli $A_1[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] \Leftrightarrow A_2[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$. Kako je formula $(A_1 \Leftrightarrow A_2)[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ valjana, sledi da je valjana i formula $A_1[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] \Leftrightarrow A_2[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$. Kako je dobro zasnovana formula $A_1[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] \Leftrightarrow A_2[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$ valjana, na osnovu teoreme 3.13 sledi $A_1[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n] \equiv A_2[p_1 \mapsto \mathcal{A}_1, p_2 \mapsto \mathcal{A}_2, \ldots, p_n \mapsto \mathcal{A}_n]$, što je i trebalo dokazati. □

Na osnovu teoreme o zameni (3.14) sledi da svaku dobro zasnovanu formulu možemo transformisati, korišćenjem pogodnih logičkih ekvivalencija, u dobro zasnovane formule koje su sa njom logički ekvivalentne. Logičke ekvivalencije iskazne logike prirodno se prenose i u logiku prvog reda na osnovu teoreme 3.16.

Primer 3.10 *Neke od logičkih ekvivalencija logike prvog reda (koje proizilaze iz iskazne logike) su (videti i primer 2.6):*

$$\begin{array}{rcll} \neg\neg\mathcal{A} & \equiv & \mathcal{A} & \textit{zakon dvojne negacije} \\ \mathcal{A}\vee\neg\mathcal{A} & \equiv & \top & \textit{zakon isključenja trećeg} \\ (\mathcal{A}\wedge\mathcal{B}) & \equiv & (\mathcal{B}\wedge\mathcal{A}) & \textit{zakon komutativnosti za } \wedge \end{array}$$

Primer 3.11 *Važi* $\neg(\exists x)(\mathcal{A}\wedge\neg\mathcal{B}) \equiv (\forall x)\neg(\mathcal{A}\wedge\neg\mathcal{B}) \equiv (\forall x)(\neg\mathcal{A}\vee\neg\neg\mathcal{B}) \equiv (\forall x)(\neg\mathcal{A}\vee\mathcal{B}) \equiv (\forall x)(\mathcal{A}\Rightarrow\mathcal{B})$. *Iz* $\neg(\exists x)(\mathcal{A}\wedge\neg\mathcal{B}) \equiv (\forall x)(\mathcal{A}\Rightarrow\mathcal{B})$, *na osnovu teoreme 3.13 sledi da je formula* $\neg(\exists x)(\mathcal{A}\wedge\neg\mathcal{B}) \Leftrightarrow (\forall x)(\mathcal{A}\Rightarrow\mathcal{B})$ *valjana.*

Zadaci

Zadatak 57 $\surd$ *Navesti primer formule koja je valjana a nije izvod tautologije.*

Zadatak 58 $\surd$ *Dokazati da je formula* $(\exists x)(\mathcal{A}\Rightarrow\mathcal{B}) \Leftrightarrow ((\forall x)\mathcal{A}\Rightarrow(\exists x)\mathcal{B})$ *valjana.*

Zadatak 59 *Dokazati da za svaku supstituciju* σ *iz* $\mathcal{A}\equiv\mathcal{B}$ *sledi* $\mathcal{A}\sigma\equiv\mathcal{B}\sigma$.

Zadatak 60 *Dokazati da je formula* $(\forall x)(\exists y)\mathcal{A}\Rightarrow(\exists y)(\mathcal{A}[x\mapsto y])$ *valjana.*

Zadatak 61 *Dokazati sledeću logičku ekvivalenciju:*

$$\exists x\mathcal{A}\equiv\exists y(\mathcal{A}[x\mapsto y])$$

pri čemu formula $\mathcal{A}$ *nema slobodnih pojavljivanja promenljive* y. *Dokazati da data logička ekvivalencija ne važi ako se izostavi navedeni dodatni uslov.*

Zadatak 62 *Dokazati da je supstitucija* $\sigma = [x_1\mapsto t_1, x_2\mapsto t_2, \ldots, x_n\mapsto t_n]$ *idempotentna (tj. da za bilo koji izraz* E *važi* $E\sigma = (E\sigma)\sigma$*) ako i samo ako nijedan od termova* t_i *ne sadrži nijednu od promenljivih* x_j *(sem, eventualno, ako je* $t_i = x_i$ *za neko* i*).*

3.2.3 Normalne forme

Definicija 3.22 *Kažemo da je formula u* preneks formi *ili* preneks normalnoj formi *ako je ona oblika*

$$Q_1x_1Q_2x_2\ldots Q_nx_n\mathcal{A}$$

pri čemu je Q_i *ili* $\forall$ *ili* $\exists$ *i* $\mathcal{A}$ *ne sadrži kvantifikatore, kao ni slobodne promenljive osim (eventualno) promenljivih* $x_1, x_2, \ldots, x_n$.

Ako je rečenica (zatvorena formula) $\mathcal{A}$ logički ekvivalentna formuli $\mathcal{B}$ i formula $\mathcal{B}$ je u preneks normalnoj formi, onda kažemo da je formula $\mathcal{B}$ preneks normalna forma formule $\mathcal{A}$. Korišćenjem pogodnih logičkih ekvivalencija, svaka zatvorena formula može biti transformisana u svoju preneks normalnu formu. Radi jednostavnosti procedure i rezultujuće formule, obično se u okviru transformisanja formule u preneks formu najpre eliminišu veznici $\Leftrightarrow$ i $\Rightarrow$. Naglasimo da jedna formula može da ima više preneks normalnih formi (na primer, i formula $(\forall x)(\forall y)(\mathcal{A}(x)\wedge\mathcal{B}(y))$ i formula $(\forall y)(\forall x)(\mathcal{B}(y)\wedge\mathcal{A}(x))$ su preneks

normalne forme formule $(\forall x)\mathcal{A}(x) \wedge (\forall y)\mathcal{B}(y))$. Slično, jedna formula koja je u preneks normalnoj formi može biti preneks normalna forma za više formula.

Transformisanje formule u preneks normalnu formu može biti opisano procedurom prikazanom na slici 3.1 (kada govorimo o „primeni neke logičke ekvivalencije" mislimo na korišćenje ekvivalencije na osnovu teoreme o zameni (3.14)).

Korektnost navedenog algoritma može se dokazati slično kao korektnost procedure za transformisanje formule u konjunktivnu normalnu formu (teorema 2.12). Za slučaj kada (prilikom primene koraka 4 algoritma) promenljiva x ima slobodna pojavljivanja u formuli $\mathcal{B}$, izborom nove promenljive od, na primer, formule $(\forall x\mathcal{A}) \wedge \mathcal{B}$ dobija se formula $\forall u(\mathcal{A}[x \mapsto u] \wedge \mathcal{B})$, pa je potrebno dokazati i:

$$(\forall x\mathcal{A}) \wedge \mathcal{B} \equiv \forall u(\mathcal{A}[x \mapsto u] \wedge \mathcal{B})$$

(kao i preostale analogne logičke ekvivalencije). Bez detalja dokaza, navodimo teoremu o korektnosti algoritma PRENEX.

Teorema 3.17 (Korektnost algoritma PRENEX) *Algoritam PRENEX se zaustavlja i zadovoljava sledeće svojstvo: ako je $\mathcal{A}$ ulazna formula, onda je izlazna formula $\mathcal{A}'$ u preneks normalnoj formi i logički je ekvivalentna sa $\mathcal{A}$.*

Za transformisanje formule u njenu preneks normalnu formu mogu se koristiti i logičke ekvivalencije kao što su

$\mathcal{B} \Rightarrow (\forall x\mathcal{A}) \equiv (\forall x)(\mathcal{B} \Rightarrow \mathcal{A})$,

$(\forall x)\mathcal{A} \Rightarrow \mathcal{B} \equiv (\exists x)(\mathcal{A} \Rightarrow \mathcal{B})$,

pri čemu x nema slobodna pojavljivanja u formuli $\mathcal{B}$, ali to nije potrebno ako su na početku eliminisani veznici $\Rightarrow$ i $\Leftrightarrow$.

U nekim situacijama moguće je primeniti neki korak navedenog algoritma na više od jednog načina. Na primer, formulu $(\forall x)p(x) \wedge (\exists y)q(y)$ moguće je transformisati i u $(\forall x)(p(x) \wedge (\exists y)q(y))$ i u $(\exists y)((\forall x)p(x) \wedge q(y))$. Obe ove formule su, naravno, logički ekvivalentne sa polaznom formulom. Ipak, u situacijama kada je moguće „pomeriti" i univerzalni i egzistencijalni kvantifikator, uvek ćemo radije „pomeriti" najpre egzistencijalni, a onda univerzalni. Takav prioritet uvodimo zarad jednostavnijeg koraka skolemizacije (o kojem će biti reči u nastavku). Naglasimo da univerzalni i egzistencijalni kvantifikator ne mogu, u opštem slučaju, da menjaju mesta, tj. formule $(\forall x)(\exists y)\mathcal{A}$ i $(\exists y)(\forall x)\mathcal{A}$ nisu u opštem slučaju logički ekvivalentne. S druge strane, dva univerzalna kvantifikatora mogu da zamene mesta, tj. formule $(\forall x)(\forall y)\mathcal{A}$ i $(\forall y)(\forall x)\mathcal{A}$ su logički ekvivalentne. Slično, dva egzistencijalna kvantifikatora mogu da zamene mesta, tj. formule $(\exists x)(\exists y)\mathcal{A}$ i $(\exists y)(\exists x)\mathcal{A}$ su logički ekvivalentne. To suštinski znači da u bloku kvantifikatora istog tipa, njihov poredak nije bitan.

Primer 3.12 *Razmotrimo formulu*

$$\forall x\ p(x) \wedge \forall x\exists y\forall z(q(y,z) \Rightarrow r(g(x),y))\ .$$

Nakon koraka

$$\forall x(p(x) \wedge \forall x\exists y\forall z(q(y,z) \Rightarrow r(g(x),y)))\ ,$$

Algoritam: PRENEX

Ulaz: Zatvorena dobro zasnovana formula $\mathcal{A}$
Izlaz: Preneks normalna forma formule $\mathcal{A}$

1. Dok god je to moguće, primenjivati logičke ekvivalencije
   $\mathcal{A} \Leftrightarrow \mathcal{B} \equiv (\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})$ i
   $\mathcal{A} \Rightarrow \mathcal{B} \equiv \neg\mathcal{A} \vee \mathcal{B}$.
2. Dok god je to moguće, primenjivati sledeće logičke ekvivalencije:
   $\neg(\mathcal{A} \wedge \mathcal{B}) \equiv \neg\mathcal{A} \vee \neg\mathcal{B}$,
   $\neg(\mathcal{A} \vee \mathcal{B}) \equiv \neg\mathcal{A} \wedge \neg\mathcal{B}$,
   $\neg(\forall x)\mathcal{A} \equiv (\exists x)\neg\mathcal{A}$,
   $\neg(\exists x)\mathcal{A} \equiv (\forall x)\neg\mathcal{A}$.
3. Eliminisati višestruke veznike $\neg$ koristeći zakon dvojne negacije:
   $\neg\neg\mathcal{A} \equiv \mathcal{A}$.
4. Dok god je to moguće, primenjivati sledeće logičke ekvivalencije:
   $(\forall x\mathcal{A}) \wedge \mathcal{B} \equiv (\forall x)(\mathcal{A} \wedge \mathcal{B})$,
   $(\forall x\mathcal{A}) \vee \mathcal{B} \equiv (\forall x)(\mathcal{A} \vee \mathcal{B})$,
   $\mathcal{B} \wedge (\forall x)\mathcal{A} \equiv (\forall x)(\mathcal{B} \wedge \mathcal{A})$,
   $\mathcal{B} \vee (\forall x)\mathcal{A} \equiv (\forall x)(\mathcal{B} \vee \mathcal{A})$,
   $(\exists x\mathcal{A}) \wedge \mathcal{B} \equiv (\exists x)(\mathcal{A} \wedge \mathcal{B})$,
   $(\exists x\mathcal{A}) \vee \mathcal{B} \equiv (\exists x)(\mathcal{A} \vee \mathcal{B})$,
   $\mathcal{B} \wedge (\exists x)\mathcal{A} \equiv (\exists x)(\mathcal{B} \wedge \mathcal{A})$,
   $\mathcal{B} \vee (\exists x)\mathcal{A} \equiv (\exists x)(\mathcal{B} \vee \mathcal{A})$,
   pri čemu x nema slobodna pojavljivanja u formuli $\mathcal{B}$. Ako x ima slobodna pojavljivanja u $\mathcal{B}$, onda treba najpre preimenovati promenljivu x u formuli $(\forall x)\mathcal{A}$ (odnosno u formuli $(\exists x)\mathcal{A}$).

Slika 3.1: Algoritam PRENEX

kako je promenljiva x slobodna u $p(x)$, najpre ćemo preimenovati vezanu promenljivu x u u (u okviru formule $\forall x \exists y \forall z(q(y,z) \Rightarrow r(g(x),y))$):

$$\forall x(p(x) \wedge \forall u \exists y \forall z(q(y,z) \Rightarrow r(g(u),y))) \ .$$

Nakon toga kvantifikatori $\forall u$, $\exists y$, $\forall z$ mogu, jedan po jedan, biti pomereni na početak formule:

$$\forall x \forall u \exists y \forall z(p(x) \wedge (q(y,z) \Rightarrow r(g(u),y))) \ .$$

Definicija 3.23 *Formula bez kvantifikatora je u konjunktivnoj normalnoj formi ako je oblika*

$$\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_n$$

pri čemu je svaka od formula $\mathcal{A}_i$ ($1 \leq i \leq n$) disjunkcija literala.

Konjunktivna normalna forma formule predikatske logike može se dobiti na isti način kao i u slučaju iskazne logike (videti poglavlje 2.2.5).

Primer 3.13 *Konjunktivna normalna forma formule*

$$p(x) \wedge (q(y,z) \Rightarrow r(g(u),y))$$

je formula

$$p(x) \wedge (\neg q(y,z) \vee r(g(u),y)) \ .$$

Definicija 3.24 *Formula je u* klauzalnoj *formi ako je oblika*

$$\forall x_1 \forall x_2 \ldots \forall x_n \mathcal{A}$$

gde je $\mathcal{A}$ formula bez kvantifikatora koja je u konjunktivnoj normalnoj formi i $\mathcal{A}$ nema slobodnih promenljivih osim, eventualno, promenljivih $x_1, x_2, \ldots, x_n$.

Ako je formula $\forall x_1 \forall x_2 \ldots \forall x_n \mathcal{A}$ u klauzalnoj formi, onda se često u zapisu izostavljaju kvantifikatori i piše samo $\mathcal{A}$, podrazumevajući da se misli na univerzalno zatvorenje formule $\mathcal{A}$.

Ne postoji za svaku rečenicu formula koja je u klauzalnoj formi i koja joj je logički ekvivalentna. Na primer, za rečenicu $(\exists x)p(x)$ ne postoji formula koja je u klauzalnoj formi i koja joj je logički ekvivalentna. Međutim, može se dokazati da za svaku rečenicu $\mathcal{A}$ postoji formula $\mathcal{B}$ u klauzalnoj formi takva da je $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva (videti teoremu 3.20). To je dovoljno i pogodno za ispitivanje zadovoljivosti formula — ako se ispituje zadovoljivost rečenice $\mathcal{A}$, dovoljno je ispitati zadovoljivost formule $\mathcal{B}$ koja je u klauzalnoj formi (pogodnoj za neke metode) i zadovoljiva je ako i samo ako je zadovoljiva formula $\mathcal{A}$. Uslov da je formula $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva zove se *slaba ekvivalencija*.

Transformisanje rečenice $\mathcal{A}$ u formulu $\mathcal{B}$ koja je u klauzalnoj formi i koja je zadovoljiva ako i samo ako je $\mathcal{A}$ zadovoljiva uključuje eliminisanje egzistencijalnih kvantifikatora. Ono se zasniva na izmeni polazne signature dodavanjem novih funkcijskih simbola. Te dodatne funkcijske simbole zovemo *Skolemovim konstantama* (za funkcijske simbole arnosti 0) i *Skolemovim funkcijama*, a proces eliminisanja egzistencijalnih kvantifikatora zovemo *skolemizacijom* (po matematičaru Skolemu koji ih je prvi koristio). Prvi korak je transformisanje formule u preneks normalnu formu. Drugi korak je transformisanje dela formule bez kvantifikatora u konjunktivnu normalnu formu. Nakon toga, postupkom skolemizacije eliminišu se egzistencijalni kvantifikatori, jedan po jedan, sleva nadesno.

Pretpostavimo da rečenica počinje egzistencijalnim kvantifikatorom: $\exists y\mathcal{A}$. Treba izabrati novi simbol konstante d koji se ne pojavljuje u signaturi, obrisati kvantifikator i zameniti promenljivu y simbolom d. Na taj način formula $\exists y\mathcal{A}$ transformiše se u formulu $\mathcal{A}[y \mapsto d]$. Može se dokazati da je formula $\exists y\mathcal{A}$ zadovoljiva ako i samo ako je formula $\mathcal{A}[y \mapsto d]$ zadovoljiva.

Ako rečenica počinje nizom univerzalnih kvantifikatora: $\forall x_1 \forall x_2 \ldots \forall x_n \exists y\mathcal{A}$, onda uvodimo novi funkcijski simbol f arnosti n koji do tada nije postojao u signaturi. Polazna formula biće onda transformisana u formulu $\forall x_1 \forall x_2 \ldots \forall x_n$ $\mathcal{A}[y \mapsto f(x_1, x_2, \ldots, x_n)]$. Može se dokazati da je formula $\forall x_1 \forall x_2 \ldots \forall x_n \exists y\mathcal{A}$ zadovoljiva ako i samo ako je formula $\forall x_1 \forall x_2 \ldots \forall x_n \mathcal{A}[y \mapsto f(x_1, x_2, \ldots, x_n)]$ zadovoljiva. (Primetimo da je uvođenje nove konstante samo specijalni slučaj uvođenja novog funkcijskog simbola.)

Teorema 3.18 (Teorema o skolemizaciji) *Ako je formula $\mathcal{B}$ nad signaturom $\mathcal{L}'$ dobijena skolemizacijom od rečenice $\mathcal{A}$ nad signaturom $\mathcal{L}$ koja je u preneks normalnoj formi, onda je $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva.*

Dokaz: Pretpostavimo da je formula $\mathcal{B}$ dobijena eliminisanjem jednog egzistencijalnog kvantifikatora iz rečenice $\mathcal{A}$. Moguća su dva slučaja.

- Formula $\mathcal{A}$ je oblika $(\exists y)\mathcal{A}'$. Skolemizacijom se tada dobija formula $\mathcal{B}$ koja je jednaka $\mathcal{A}'[y \mapsto d]$ gde je d nova, Skolemova konstanta koja ne postoji u signaturi $\mathcal{L}$. Neka je $\mathcal{L}'$ signatura dobijena od signature $\mathcal{L}$ dodavanjem funkcijskog simbola d arnosti 0.

  Pretpostavimo da je formula $\mathcal{A}$ zadovoljiva, tj. da postoje $\mathcal{L}$-struktura $\mathfrak{D} = (D, I^{\mathcal{L}})$ i valuacija v takve da važi $(\mathfrak{D}, v) \models (\exists y)\mathcal{A}'$. U odgovarajućoj interpretaciji I_v je, dakle, $I_v((\exists y)\mathcal{A}') = 1$, pa postoji valuacija w takva da je $w \sim_y v$ i $I_w(\mathcal{A}') = 1$. Neka je $w(y) = d_y$. Dokažimo da je formula $\mathcal{B}$ zadovoljiva. Neka je $\mathfrak{D}'$ $\mathcal{L}'$-struktura $(D, I^{\mathcal{L}'})$, pri čemu je $I^{\mathcal{L}'}(f) = I^{\mathcal{L}}(f)$ za svaki funkcijski simbol f iz $\mathcal{L}$ i $I^{\mathcal{L}'}(p) = I^{\mathcal{L}}(p)$ za svaki predikatski simbol p iz $\mathcal{L}$ i, dodatno, neka je $I^{\mathcal{L}'}(d) = d_y$. U interpretaciji I'_w (određenoj $\mathcal{L}'$-strukturom $\mathfrak{D}'$ i valuacijom w) važi $I'_w(\mathcal{B}) = I'_w(\mathcal{A}'[y \mapsto d])$. Kako je $w(y) = I'_w(y) = I'_w(d)$, može se dokazati (npr. indukcijom po složenosti formule $\mathcal{A}'$)

da važi $I'_w(\mathcal{A}'[y \mapsto d]) = I'_w(\mathcal{A}') = I_w(\mathcal{A}') = 1$, odakle sledi da je $I'_w(\mathcal{B}) = 1$, tj. $\mathcal{L}'$-struktura $\mathfrak{D}'$ i valuacija w čine model formule $\mathcal{B}$, pa je ona zadovoljiva.

Pretpostavimo da je formula $\mathcal{B}$ zadovoljiva, tj. da postoji $\mathcal{L}'$-struktura $\mathfrak{D}' = (D, I^{\mathcal{L}'})$ i valuacija v takve da važi $(\mathfrak{D}', v) \models \mathcal{B}$. U odgovarajućoj interpretaciji I'_v je, dakle, $I'_v(\mathcal{B}) = I'_v(\mathcal{A}'[y \mapsto d]) = 1$. Označimo sa d_y vrednost $I^{\mathcal{L}'}(d)$. Neka je $\mathfrak{D}$ $\mathcal{L}$-struktura $(D, I^{\mathcal{L}})$, pri čemu je $I^{\mathcal{L}}(f) = I^{\mathcal{L}'}(f)$ za svaki funkcijski simbol f iz $\mathcal{L}$ i $I^{\mathcal{L}}(p) = I^{\mathcal{L}'}(p)$ za svaki predikatski simbol p iz $\mathcal{L}$ i neka je I_w interpretacija određena $\mathcal{L}$-strukturom $\mathfrak{D}$ i valuacijom w. Ako je w valuacija takva da važi $w \sim_y v$ i $w(y) = d_y$, onda je $1 = I'_v(\mathcal{B}) = I'_v(\mathcal{A}'[y \mapsto d]) = I'_w(\mathcal{A}')$. Kako je $I'_w(\mathcal{A}') = I_w(\mathcal{A}')$, sledi da je $I_w(\mathcal{A}') = 1$, pa je formula $(\exists y)\mathcal{A}'$ (tj. formula $\mathcal{A}$) zadovoljiva.

- Formula $\mathcal{A}$ je oblika $(\forall x_1)(\forall x_2)\dots(\forall x_n)(\exists y)\mathcal{A}'$. Skolemizacijom se tada dobija formula $\mathcal{B}$ koja je jednaka $(\forall x_1)(\forall x_2)\dots(\forall x_n)\mathcal{A}'[y \mapsto g(x_1, x_2, \dots, x_n)]$, gde je g simbol nove, Skolemove funkcije koji ne postoji u signaturi $\mathcal{L}$. Neka je $\mathcal{L}'$ signatura dobijena od signature $\mathcal{L}$ dodavanjem funkcijskog simbola g arnosti n.

  Pretpostavimo da je formula $\mathcal{A}$ zadovoljiva, tj. da postoji $\mathcal{L}$-struktura $\mathfrak{D} = (D, I^{\mathcal{L}})$ i valuacija v takve da u odgovarajućoj interpretaciji I_v važi $I_v((\forall x_1)(\forall x_2)\dots(\forall x_n)(\exists y)\mathcal{A}') = 1$. Na osnovu teoreme 3.7 sledi da je formula $(\exists y)\mathcal{A}'$ valjana u $\mathfrak{D}$, tj. da za svaku valuaciju w važi $I_w((\exists y)\mathcal{A}') = 1$. Odatle sledi da za svaku valuaciju w postoji valuacija w' takva da je $w' \sim_y w$ i $I_{w'}(\mathcal{A}') = 1$. Dokažimo da je formula $\mathcal{B}$ zadovoljiva. Neka je $\mathfrak{D}'$ $\mathcal{L}'$-struktura $(D, I^{\mathcal{L}'})$, pri čemu je $I^{\mathcal{L}'}(f) = I^{\mathcal{L}}(f)$ za svaki funkcijski simbol f iz $\mathcal{L}$ i $I^{\mathcal{L}'}(p) = I^{\mathcal{L}}(p)$ za svaki predikatski simbol p iz $\mathcal{L}$ i, dodatno, neka je $I^{\mathcal{L}'}(g) = g_I$, gde je g_I preslikavanje iz D^n u D. Vrednost $g_I(d_1, d_2, \dots, d_n)$ (gde je $d_1, d_2, \dots, d_n \in D$) definišemo posebno za svaku torku $(d_1, d_2, \dots, d_n)$ i to na sledeći način: neka je w valuacija u kojoj je $w(x_i) = d_i$ $(i = 1, 2, \dots, n)$; za valuaciju w postoji valuacija w' takva da je $w' \sim_y w$ i $I_{w'}(\mathcal{A}') = 1$; vrednost $g_I(d_1, d_2, \dots, d_n)$ neka je jednaka $w'(y)$. Tada za svaku valuaciju w važi $I_w(\mathcal{A}'[y \mapsto g(x_1, x_2, \dots, x_n)]) = I_{w'}(\mathcal{A}'[y \mapsto g(x_1, x_2, \dots, x_n)]) = I_{w'}(\mathcal{A}') = 1$. Kako je formula $\mathcal{A}'[y \mapsto g(x_1, x_2, \dots, x_n)]$ valjana, sledi, na osnovu teoreme 3.7, da je formula $\mathcal{B}$ zadovoljiva.

  Pretpostavimo da je formula $\mathcal{B}$ zadovoljiva, tj. da postoji $\mathcal{L}'$-struktura $\mathfrak{D}' = (D, I^{\mathcal{L}'})$ i valuacija v takve da važi $(\mathfrak{D}', v) \models \mathcal{B}$. Neka je I'_v interpretacija određena $\mathcal{L}'$-strukturom $\mathfrak{D}'$ i valuacijom v. Neka je $\mathfrak{D}$ $\mathcal{L}$-struktura $(D, I^{\mathcal{L}})$, pri čemu je $I^{\mathcal{L}}(f) = I^{\mathcal{L}'}(f)$ za svaki funkcijski simbol f iz $\mathcal{L}$ i $I^{\mathcal{L}}(p) = I^{\mathcal{L}'}(p)$ za svaki predikatski simbol p iz $\mathcal{L}$ i neka je I_w interpretacija određena $\mathcal{L}$-strukturom $\mathfrak{D}$ i valuacijom w. Za interpretaciju I'_v važi $I'_v((\forall x_1)(\forall x_2)\dots(\forall x_n)\mathcal{A}'[y \mapsto g(x_1, x_2, \dots, x_n)]) = 1$. Odatle, na osnovu teoreme 3.7, sledi da je

formula $\mathcal{A}'[y \mapsto g(x_1, x_2, \ldots, x_n)]$ valjana u $\mathfrak{D}'$, tj. da za svaku valuaciju w važi $I'_w(\mathcal{A}'[y \mapsto g(x_1, x_2, \ldots, x_n)]) = 1$. Neka je w' valuacija takva da je $w' \sim_y w$ i $w'(y) = I'_w(g(x_1, x_2, \ldots, x_n))$. Tada je $I'_{w'}(\mathcal{A}') = I'_w(\mathcal{A}'[y \mapsto g(x_1, x_2, \ldots, x_n)]) = 1$. Iz $I'_{w'}(\mathcal{A}') = 1$ sledi $I_{w'}(\mathcal{A}') = 1$. Iz $I_{w'}(\mathcal{A}') = 1$ sledi da $I_{w''}((\exists y)\mathcal{A}') = 1$ važi za svaku valuaciju w'', pa je formula $(\exists y)\mathcal{A}'$ valjana u $\mathfrak{D}$. Odatle, na osnovu teoreme 3.7, sledi da je formula $(\forall x_1)(\forall x_2)\ldots(\forall x_n)(\exists y)\mathcal{A}'$ zadovoljiva u $\mathfrak{D}$, tj. ova formula je zadovoljiva.

Opšte tvrđenje teoreme (slučaj da je formula $\mathcal{B}$ dobijena eliminisanjem više egzistencijalnih kvantifikatora iz formule $\mathcal{A}$) sledi na osnovu dokazanog specijalnog slučaja (eliminisanje jednog egzistencijalnog kvantifikatora) i na osnovu jednostavnog induktivnog argumenta. □

Primer 3.14 *Skolemizacijom se formula*

$$\forall x \forall u \exists y \forall z (p(x) \wedge (\neg q(y, z) \vee r(g(u), y)))$$

transformiše u formulu

$$p(x) \wedge (\neg q(h(x, u), z) \vee r(g(u), h(x, u))) \ .$$

Teorema 3.19 *Neka je formula $\mathcal{B}$ (u klauzalnoj formi) dobijena od rečenice $\mathcal{A}$ uzastopnom primenom sledećih postupaka:*

- *transformisanje formule u preneks normalnu formu;*
- *transformisanje dela formule bez kvantifikatora u konjunktivnu normalnu formu;*
- *skolemizacija.*

Tada je formula $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva.

Dokaz: Transformacija formule u preneks normalnu formu i transformacija dela formule bez kvantifikatora u konjunktivnu normalnu formu zasnovane su na logičkim ekvivalencijama, pa ako je formula $\mathcal{B}$ dobijena od formule $\mathcal{A}$ uzastopnom primenom navedene dve transformacije, važi $\mathcal{A} \equiv \mathcal{B}$, što je jači uslov nego uslov da je $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva. Na osnovu teoreme 3.18 sledi da skolemizacija čuva zadovoljivost i nezadovoljivost, pa je formula $\mathcal{B}$ zadovoljiva ako i samo ako je $\mathcal{A}$ zadovoljiva. □

Na osnovu prethodne teoreme neposredno sledi naredno tvrđenje.

Teorema 3.20 *Za svaku rečenicu $\mathcal{A}$ postoji formula $\mathcal{B}$ u klauzalnoj formi takva da je $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva.*

Klauzalna forma je pogodna za dokazivanje pobijanjem. Da bi se dokazalo da je formula $\mathcal{A}$ valjana, dovoljno je dokazati da je formula $\neg\mathcal{A}$ nezadovoljiva, pa je dovoljno i dokazati da je klauzalna forma formule $\neg\mathcal{A}$ nezadovoljiva.

Primer 3.15 *Formula $\mathcal{A} = (\forall x)p(x,x) \Rightarrow (\forall y)p(y,y)$ nad signaturom $\mathcal{L}$ je valjana. To se može dokazati na sledeći način.*

Formula $\neg\mathcal{A}$ je jednaka $\neg((\forall x)p(x,x) \Rightarrow (\forall y)p(y,y))$ i njena preneks normalna forma je $(\exists y)(\forall x)(p(x,x) \wedge \neg p(y,y))$. Skolemizacijom dobijamo formulu $p(x,x) \wedge \neg p(c,c)$, gde je c novi simbol konstante. Neka je $\mathcal{L}'$ signatura dobijena proširivanjem signature $\mathcal{L}$ simbolom c. Pokažimo da je formula $p(x,x) \wedge \neg p(c,c)$ nezadovoljiva. Pretpostavimo suprotno — pretpostavimo da navedena formula ima model. Neka je to $\mathcal{L}'$-struktura $\mathfrak{D} = (D, I^{\mathcal{L}'})$ sa valuacijom v. Neka je $I^{\mathcal{L}'}(p) = p_I$ i $I^{\mathcal{L}'}(c) = c_I$. Važi $I_v(p(x,x) \wedge \neg p(c,c)) = 1$ tj. $I_v((\forall x)(p(x,x) \wedge \neg p(c,c))) = 1$, pa za svaku valuaciju w takvu da je $w \sim_x v$ važi $I_w(p(x,x) \wedge \neg p(c,c)) = 1$. To, dakle, važi i za valuaciju w u kojoj je $w(x) = c_I$. Iz $I_w(p(x,x) \wedge \neg p(c,c)) = 1$ sledi $I_w(p(x,x)) = 1$ i $I_w(p(c,c)) = 0$. Iz $I_w(p(x,x)) = 1$ sledi $p_I(c_I, c_I) = 1$, a iz $I_w(p(c,c)) = 0$ sledi $p_I(c_I, c_I) = 0$, što je kontradikcija. Dakle, formula $p(x,x) \wedge \neg p(c,c)$ je nezadovoljiva, pa je polazna formula $\mathcal{A}$ valjana.

Zadaci

Zadatak 63 *Odrediti klauzalne forme za formule:*

(a) $(\exists x)\mathcal{A}_1 \wedge (\exists x)\mathcal{A}_2 \Rightarrow (\exists x)(\mathcal{A}_1 \wedge \mathcal{A}_2)$

(b) $(\forall x)\mathcal{A}_1 \vee (\forall x)\mathcal{A}_2 \Rightarrow (\forall x)(\mathcal{A}_1 \vee \mathcal{A}_2)$

(c) $(\forall x)(\exists y)\mathcal{A} \Rightarrow (\exists y)\mathcal{A}(f(y), y)$

3.2.4 Erbranova teorema

Erbranova teorema iz tridesete godine dvadesetog veka jedan je od temelja više sistema za automatsko dokazivanje teorema. Njen značaj proističe iz same prirode predikatske logike. U predikatskoj logici (za razliku od iskazne), naime, u opštem slučaju nije odlučivo da li je neka formula valjana. Međutim, primenom Erbranove teoreme pitanje ispitavanja valjanosti svodi se na problem konačne dimenzije (tj. na problem koji se može rešiti u konačno mnogo koraka). Naime, da bi se, u kontekstu dokazivanja pobijanjem, pokazalo da je neka formula $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{B}$ kontradiktorna, na osnovu Erbranove teoreme dovoljno je pokazati da postoji konačan kontradiktoran skup baznih instanci formule $\mathcal{B}$.

Prilikom testiranja da li je neka formula $\mathcal{B}$ nezadovoljiva, generisanje instanci se može kontrolisati tako da se osigura da nijedna od mogućih instanci ne bude izostavljena prilikom testiranja. Tako se može obezbediti sledeće: ako je formula $\mathcal{B}$ nezadovoljiva, onda će njena nezadovoljivost biti pokazana u konačnom broju koraka. S druge strane, moguće je da se traganje kroz sve moguće instance ne zaustavlja. Preciznije, mogući su sledeći slučajevi:

- formula $\mathcal{B}$ je nezadovoljiva; u ovom slučaju proces se uspešno zaustavlja, tj. biće pronađena konačna kontradikcija sačinjena od instanci formule $\mathcal{B}$;
- formula $\mathcal{B}$ nije nezadovoljiva; u ovom slučaju moguća su dva ishoda:
  - u jednom trenutku nema više instanci koje je moguće generisati i do tada nije otkrivena kontradikcija; u ovom slučaju zna se da $\mathcal{B}$ nije nezadovoljiva (tj. zna se da je zadovoljiva);
  - proces generisanja instanci se ne zaustavlja, tj. ni u jednom koraku se ne može detektovati kontradikcija; u ovom slučaju se ne zna da li je formula $\mathcal{B}$ nezadovoljiva ili nije.

Na osnovu navedenih svojstava sledi i da je svaku valjanu formulu moguće dokazati pobijanjem (ali nije za svaku formulu koja nije valjana moguće dokazati da nije valjana). Dakle, problem ispitivanja valjanosti (i, analogno, problem ispitivanja nezadovoljivosti) u logici prvog reda je poluodlučiv (ali nije odlučiv). Erbranova teorema implicitno daje proceduru poluodlučivanja za logiku prvog reda, ali je ta procedura izuzetno neefikasna i praktično neupotrebljiva za netrivijalne formule.

Erbranova teorema omogućava da se problem zadovoljivosti formule sa razmatranja proizvoljnog modela svede na razmatranje samo posebnog skupa modela. U tome ključnu ulogu ima posebna klasa interpretacija, tzv. *Erbranove interpretacije* koje, u ovom smislu, mogu da zamene sve ostale interpretacije. Sve Erbranove interpretacije za jednu formulu dele isti domen — *Erbranov univerzum*. Erbranov univerzum formule $\mathcal{A}$ označavamo sa $H(\mathcal{A})$ i definišemo ga kao skup svih termova nad $\mathcal{L}$ koji nemaju promenljive, tj. kao skup svih baznih termova nad $\mathcal{L}$.

Primer 3.16 *Razmotrimo formulu* $\forall x \forall y\ (p(x,y) \vee p(x, f(y,c)))$ *nad signaturom* $\mathcal{L}$ *određenom skupovima* $\Sigma = \{c, f\}$ *i* $\Pi = \{p\}$ *i* $ar(c) = 0, ar(f) = 2, ar(p) = 2$. *Erbranov univerzum za signaturu* $\mathcal{L}$ *jednak je skupu* $\{c, f(c,c),\ f(f(c,c),c),\ f(c,f(c,c)),\ f(f(c,c),f(c,c)), \ldots\}$.

Ako signatura sadrži i funkcijske simbole arnosti 0 i funkcijske simbole arnosti veće od 0, onda je Erbranov univerzum beskonačan i prebrojiv. Ako signatura sadrži funkcijske simbole arnosti 0, ali ne sadrži funkcijske simbole arnosti veće od 0, onda je Erbranov univerzum konačan. Ako signatura ne sadrži funkcijske simbole arnosti 0, onda se Erbranovom univerzumu (da ne bi bio prazan) dodaje jedan element (npr. a) čime se kasnije dolazi do jednog od prethodna dva slučaja.

Neka je data formula $\mathcal{A}$ koja određuje signaturu $\mathcal{L}$. Erbranovu interpretaciju određuje $\mathcal{L}$-struktura $\mathcal{H} = (H(\mathcal{A}), I^{\mathcal{L}})$. Primetimo da je ova $\mathcal{L}$-struktura čisto sintaksne prirode. Erbranovom interpretacijom I svaki bazni term se preslikava u isti taj (ili, preciznije, isti takav) term (koji je element skupa $H(\mathcal{A})$). Ovaj, specijalan primer interpretacije zovemo *samooznačavanje*. Erbranova interpretacija I_v potpuno je određena valuacijom v i preslikavanjem $I^{\mathcal{L}}$ koje svakom predikatskom simbolu p (arnosti n) iz $\mathcal{L}$ pridružuje funkciju p_I iz $H(\mathcal{A})^n$ u

skup $\{0, 1\}$, koja svaku torku $(t_1, t_2, \ldots, t_n)$ elemenata iz $H(\mathcal{A})$ preslikava u 0 ili 1. Erbranove interpretacije za fiksiranu signaturu i fiksiranu valuaciju razlikuju se, dakle, jedino po interpretaciji predikatskih simbola. Ona može biti definisana pojedinačnim definisanjem istinitosnih vrednosti svih baznih atomičkih formula nad datom signaturom. Skup svih baznih atomičkih formula nad datom signaturom može biti dobijen formiranjem skupa svih atomičkih formula nad datom signaturom i zatim zamenjivanjem promenljivih termovima iz Erbranovog univerzuma na sve moguće načine.

Primer 3.17 *Razmotrimo formulu* $\forall x \forall y \ (p(x, y) \vee p(x, f(y, c)))$ *koja određuje signaturu* $\mathcal{L}$ *sa skupovima* $\Sigma = \{c, f\}$ *i* $\Pi = \{p\}$ *i* $ar(c) = 0$, $ar(f) = 2$, $ar(p) = 2$. *Njene atomičke formule su* $\{p(x, y), p(x, f(y, c))\}$. *Erbranov univerzum je* $\{c, f(c, c), f(f(c, c), c), f(c, f(c, c)), f(f(c, c), f(c, c)), \ldots\}$. *Zamenjivanjem promenljivih* x *i* y *u atomičkim formulama* $p(x, y)$ *i* $p(x, f(y, c))$, *dobija se skup baznih atomičkih formula od kojih svakoj treba dodeliti istinitosnu vrednost:* $\{p(c, c), p(c, f(c, c)), p(f(c, c), c), p(f(c, c), f(c, c)), \ldots\}$.

Primetimo da za ispitivanje istinitosne vrednosti polazne formule $\mathcal{A}$ nisu relevantne sve atomičke formule nad indukovanom signaturom. Umesto svih tih atomičkih formula dovoljno je dodeliti istinitosne vrednosti instancama atomičkih formula koje se pojavljuju u $\mathcal{A}$ (pri čemu pod instancama podrazumevamo formule dobijene zamenjivanjem promenljivih elementima Erbranovog univerzuma). Takav skup instanci atomičkih formula zovemo *Erbranovom bazom* formule. Erbranovoj bazi, dakle, ne pripada nužno svaka atomička formula nad predikatima iz signature i elementima Erbranovog univerzuma.

Primer 3.18 *Razmotrimo formulu* $\forall x \forall y \ p(x, f(y, c))$ *koja određuje signaturu* $\mathcal{L}$ *sa skupovima* $\Sigma = \{c, f\}$ *i* $\Pi = \{p\}$ *i* $ar(c) = 0$, $ar(f) = 2$, $ar(p) = 2$. *Skup njenih atomičkih formula je* $\{p(x, f(y, c))\}$. *Erbranov univerzum je* $\{c, f(c, c), f(f(c, c), c), f(c, f(c, c)), f(f(c, c), f(c, c)), \ldots\}$. *Zamenjivanjem promenljivih* x *i* y *u atomičkoj formuli* $p(x, f(y, c))$, *dobija se Erbranova baza:* $\{\ p(c, f(c, c)), p(f(c, c), f(c, c)),\ p(c, f(f(c, c), c)), p(f(c, c), f(f(c, c), c)), \ldots\}$. *Primetimo da atomička formula* $p(c, c)$ *nije u Erbranovoj bazi jer ona nije instanca formule* $p(x, f(y, c))$. *Istinitosna vrednost formule* $p(c, c)$ *u interpretaciji ne utiče na istinitosnu vrednost formule* $\forall x \forall y \ p(x, f(y, c))$ *u toj interpretaciji.*

Primetimo da je Erbranova baza uvek konačna ili prebrojiva. Ako signatura nema funkcijskih simbola arnosti veće od 0, onda je Erbranov univerzum konačan, pa je i odgovarajuća Erbranova baza konačna. Dakle, s obzirom na to da atomičke formule nad signaturom $\mathcal{L}$ koje ne postoje u Erbranovoj bazi određene formule ne utiču na njenu istinitosnu vrednost, svaka Erbranova interpretacija formule je jednoznačno određena preslikavanjem iz Erbranove

baze u skup $\{0, 1\}$. Na primer, preslikavanje

$$\begin{array}{lcl} p(c,c) & \mapsto & 1 \\ p(c,f(c,c)) & \mapsto & 0 \\ p(f(c,c),c) & \mapsto & 0 \\ p(f(c,c),f(c,c)) & \mapsto & 1 \\ p(c,f(f(c,c),c)) & \mapsto & 1 \\ \ldots & & \end{array}$$

određuje jednu Erbranovu interpretaciju za formulu $\forall x \exists y (p(x,y) \vee p(x, f(y,c)))$.

Istinitosna vrednost formule $\mathcal{A}$ u Erbranovoj interpretaciji I_v određuje se na uobičajeni način. Na primer, $I_v(\forall x \mathcal{A}) = 1$ ako za svaku valuaciju w takvu da je $w \sim_x v$ važi $I_w(\mathcal{A}) = 1$, tj. ako za svaku vrednost d iz Erbranovog univerzuma važi $I_v(\mathcal{A}[x \mapsto d]) = 1$. Ako je u ovako opisanoj $\mathcal{L}$-strukturi sa valuacijom v vrednost $I_v(\mathcal{A})$ jednaka 1, onda kažemo da je ta struktura Erbranov model formule $\mathcal{A}$.

Teorema 3.21 *Neka je rečenica $\mathcal{A}$ oblika $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{B}$, pri čemu formula $\mathcal{B}$ nema kvantifikatora. Formula $\mathcal{A}$ ima model ako i samo ako skup $\Gamma = \{\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n] \mid t_1, t_2, \ldots, t_n \in H(\mathcal{A})\}$ ima model.*

Dokaz: Neka je $\mathcal{L}$ signatura koju određuje formula $\mathcal{A}$.

Ako $\mathcal{A}$ ima model, onda Γ ima model: Pretpostavimo da rečenica $\mathcal{A}$ ima model. Neka je to $\mathcal{L}$-struktura $\mathfrak{D}$. Formula $\mathcal{A}$ je rečenica, pa za svaku valuaciju v važi $I_v(\mathcal{A}) = 1$. Formula $\mathcal{A}$ je univerzalno kvantifikovana, pa na osnovu teoreme 3.7 za svaku valuaciju v važi i $I_v(\mathcal{B}) = 1$.

Konstruišimo model za skup formula Γ. Taj model može da bude konstruisan nad $\mathcal{L}$-strukturom $\mathfrak{D}$ a valuacija nije relevantna (jer formule iz skupa Γ nemaju slobodne promenljive). Definišimo da u traženoj interpretaciji J važi $J(X) = I(X)$ za svaku baznu atomičku formulu X nad signaturom $\mathcal{L}$ (naglasimo da za svaku baznu formulu X vrednost $I_v(X)$ ne zavisi od valuacije v i da tu vrednost označavamo sa $I(X)$). Tada, za proizvoljne bazne termove $t_1, t_2, \ldots, t_n$ nad signaturom $\mathcal{L}$, važi:

$$J(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) =$$

$$= I(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) = I_v(\mathcal{B})$$

gde je v valuacija u kojoj je $v(x_i) = I_v(t_i)$ za $i = 1, 2, \ldots, n$.

Kako za svaku valuaciju v važi $I_v(\mathcal{B}) = 1$, sledi da za proizvoljne bazne termove $t_1, t_2, \ldots, t_n$ nad signaturom $\mathcal{L}$ važi $J(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) = 1$. Time je pokazano da interpretacija J zadovoljava skup Γ, tj. da taj skup ima model.

Ako Γ *ima model, onda* $\mathcal{A}$ *ima model:* Pretpostavimo da je $\mathcal{L}$-struktura $\mathfrak{D} = (D, I^{\mathcal{L}})$ model za skup formula Γ. Sve formule iz skupa Γ su bazne, pa valuacije nisu relevantne. Za svaku formulu X iz skupa Γ važi $I(X) = 1$, pa za svaku torku t_1, t_2, ..., t_n skupa $H(\mathcal{A})$ važi $I(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) = 1$.

Konstruišimo model za formulu $\mathcal{A}$. Taj model neka je izgrađen nad skupom $H(\mathcal{A})$ kao domenom. Označimo sa J odgovarajuću interpretaciju i definišimo je na sledeći način:

- za svaki simbol konstante c iz signature $\mathcal{L}$, neka je $c_J = c$;
- za svaki funkcijski simbol f arnosti n iz signature $\mathcal{L}$, i svaku torku t_1, t_2, ..., t_n skupa $H(\mathcal{A})$ neka je $f_J(t_1, t_2, \ldots, t_n) = f(t_1, t_2, \ldots, t_n)$;
- za svaki predikatski simbol p arnosti n iz signature $\mathcal{L}$, i svaku torku $t_1, t_2, \ldots, t_n$ skupa $H(\mathcal{A})$ neka je $p_J(t_1, t_2, \ldots, t_n) = I(p(t_1, t_2, \ldots, t_n))$.

Korišćenjem matematičke indukcije jednostavno se može dokazati da važi sledeće:

- ako je $t \in H(\mathcal{A})$, onda je $J(t) = t$;
- ako je X bazna formula nad $\mathcal{L}$ koja ne sadrži kvantifikatore, onda je $J(X) = I(X)$.

Neka je v proizvoljna valuacija i neka je $v(x_i) = t_i$, za $i = 1, 2, \ldots, n$. Tada važi

$$J_v(\mathcal{B}) = J(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) =$$

$$= I(\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]) = 1 \ ,$$

pa je formula $\mathcal{B}$ valjana u konstruisanoj strukturi, odakle, na osnovu teoreme 3.7, sledi da je formula $\mathcal{A}$ zadovoljiva, što je i trebalo dokazati.

□

Prethodna teorema može biti formulisana i na sledeći način: ako je rečenica $\mathcal{A}$ oblika $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{B}$, pri čemu formula $\mathcal{B}$ nema kvantifikatora, onda formula $\mathcal{A}$ ima model ako i samo ako formula $\mathcal{A}$ ima Erbranov model.

Skup $\Gamma = \{\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n] \mid t_1, t_2, \ldots, t_n \in H(\mathcal{A})\}$ zovemo *zasićenjem* ili *saturacijom* formule $\mathcal{B}$.

Teorema 3.22 (Erbranova teorema) *Neka je rečenica* $\mathcal{A}$ *oblika* $(\forall x_1)(\forall x_2)\ldots(\forall x_n)$ $\mathcal{B}$*, pri čemu formula* $\mathcal{B}$ *nema kvantifikatora. Formula* $\mathcal{A}$ *je nezadovoljiva ako i samo ako postoji konačan nezadovoljiv podskup skupa* $\Gamma = \{\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n] \mid t_1, t_2, \ldots, t_n \in H(\mathcal{A})\}$.

Dokaz: Na osnovu prethodne teoreme, formula $\mathcal{A}$ je nezadovoljiva ako i samo ako je nezadovoljiv skup Γ. Skup Γ sastoji se samo od baznih formula. Svakoj od atomičkih formula koje se pojavljuju u skupu Γ možemo da pridružimo jedno iskazno slovo. Neka je Γ' tako dobijen skup iskaznih formula. Skup baznih formula prvog reda Γ nezadovoljiv je ako i samo ako je skup iskaznih formula Γ' nezadovoljiv. Na osnovu teoreme o kompaktnosti za iskaznu logiku (2.23), skup Γ' je nezadovoljiv ako i samo ako on ima konačan nezadovoljiv podskup. Nezadovoljivom podskupu skupa Γ' odgovara nezadovoljiv podskup skupa Γ i obratno. Odatle sledi da je skup Γ nezadovoljiv ako i samo ako on ima konačan nezadovoljiv podskup. To dokazuje tvrđenje teoreme. □

Na Erbranovoj teoremi zasniva se i Gilmorov program za ispitivanje valjanosti formula prvog reda (razvijen sredinom dvadesetog veka), program koji se može smatrati jednim od prvih dokazivača teorema. U Gilmorovom dokazivaču Erbranova teorema je prilagođena automatskoj primeni. Uprkos izvesnim idejama usmerenim na popravljanje efikasnosti, Gilmorov dokazivač mogao je da dokaže samo trivijalne teoreme.

Jedna od Gilmorovih ideja pojednostavljuje skup Γ u kojem se traži kontradiktoran podskup. Pretpostavimo da je potrebno dokazati da je nezadovoljiva rečenica $\mathcal{A}$ koja je oblika $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{B}$ (pri čemu formula $\mathcal{B}$ nema kvantifikatora). Neka je $\mathcal{B}'$ konjunktivna normalna forma formule $\mathcal{B}$ i neka je ona oblika $\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_m$. Na osnovu Erbranove teoreme, formula $\mathcal{A}$ ima model ako i samo ako svaki konačan podskup skupa $\Gamma = \{\mathcal{B}[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n] \mid t_1, t_2, \ldots, t_n \in H(\mathcal{A})\}$ ima model. Međutim, svaki model formule $(\mathcal{B}_1 \wedge \mathcal{B}_2 \ldots \wedge \mathcal{B}_m)[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]$ je istovremeno i model skupa $\{\mathcal{B}_1[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n], \mathcal{B}_2[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n], \ldots, \mathcal{B}_m[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n]\}$. Zbog toga skup Γ umesto instanci formule $\mathcal{B}$ može da sadrži samo instance klauza konjunktivne forme formule $\mathcal{B}$, tj. važi sledeće tvrđenje.

Teorema 3.23 (Erbran-Gilmorova teorema) *Neka je* $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\ (\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_m)$ *klauzalna forma rečenice* $\mathcal{A}$. *Formula* $\mathcal{A}$ *je nezadovoljiva ako i samo ako postoji konačan nezadovoljiv podskup skupa* $\Gamma = \{\mathcal{B}_i[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_n \mapsto t_n] \mid t_1, t_2, \ldots, t_n \in H(\mathcal{A}), 1 \leq i \leq m\}$.

Da bi se Erbranova ili Erbran-Gilmorova teorema upotrebile u konstruisanju procedure odlučivanja potrebno je obezbediti sistematično nabrajanje elemenata skupa Γ (skupa koji je zasićenje date formule). Kako je Erbranov univerzum uvek konačan ili prebrojiv, sledi da je i zasićenje date formule (za koju treba pokazati da je nezadovoljiva) uvek konačan ili prebrojiv skup. Dakle, elementi skupa Γ (i u Erbranovoj i u Erbran-Gilmorovoj varijanti) mogu se (efektivno) poređati u niz, a odatle sledi da se i skup Γ može graditi sukcesivno, dodavanjem jednog po jednog elementa, dajući skupove $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$. Na ovaj način obezbeđuje se sledeće: ako skup Γ ima kontradiktoran konačan podskup, onda postoji vrednost n takva da skup Γ_n sadrži taj kontradiktoran podskup.

To znači da za datu formulu, treba redom proveravati da li je nezadovoljiv skup Γ_0, skup Γ_1, skup Γ_2, ... Ako se detektuje kontradiktoran skup, onda to znači da je kontradiktoran i skup Γ, tj. data formula je nezadovoljiva. Ako data formula nije nezadovoljiva, onda neće biti detektovan kontradiktoran skup Γ_n ni za jednu vrednost n.

U narednim primerima nećemo kontruisati efektivno nabrajanje elemenata Erbranovog univerzuma i odgovarajućih podskupova skupa zasićenja. Zahvaljujući jednostavnosti primera, kontradiktorne podskupove skupova zasićenja moći ćemo da odredimo i bez takvog, sistematičnog pristupa koji daje proceduru odlučivanja.

Primer 3.19 *Dokažimo da je formula* $(\forall y)p(y,y)$ *logička posledica skupa formula* $\{(\forall x)p(x,x)\}$. *Dovoljno je dokazati da je formula* $(\forall x)p(x,x) \Rightarrow (\forall y)p(y,y)$ *valjana, odnosno da je formula* $\neg((\forall x)p(x,x) \Rightarrow (\forall y)p(y,y))$ *nezadovoljiva. Preneks normalna forma ove formule je* $(\exists y)(\forall x)(p(x,x) \wedge \neg p(y,y))$. *Nakon skolemizacije, dobijamo* $p(x,x) \wedge \neg p(c,c)$, *gde je* c *nova Skolemova konstanta. Konjunktivna normalna forma formule* $p(x,x) \wedge \neg p(c,c)$ *je* $p(x,x) \wedge \neg p(c,c)$. *Erbranov univerzum je konačan (jer u signaturi nema funkcijskih simbola) i jednak skupu* $\{c\}$. *Skup svih mogućih instanci klauza formule* $p(x,x) \wedge \neg p(c,c)$ *jednak je* $\Gamma = \{p(c,c), \neg p(c,c)\}$. *Taj skup je kontradiktoran, te je, na osnovu teoreme 3.23, formula* $(\forall x)p(x,x) \Rightarrow (\forall y)p(y,y)$ *valjana.*

Primer 3.20 *Dokažimo da je formula*

$$(\forall x)(\exists y)q(x,y)$$

logička posledica skupa formula

$$\{(\forall x)(\exists y)p(x,y), (\forall x)(\forall y)(p(x,y) \Rightarrow q(x,y))\} .$$

Dovoljno je dokazati da je formula

$$\mathcal{A} = ((\forall x)(\exists y)p(x,y) \wedge (\forall x)(\forall y)(p(x,y) \Rightarrow q(x,y))) \Rightarrow (\forall x)(\exists y)q(x,y)$$

valjana, odnosno dokazati da je formula

$$\neg(((\forall x)(\exists y)p(x,y) \wedge (\forall x)(\forall y)(p(x,y) \Rightarrow q(x,y))) \Rightarrow (\forall x)(\exists y)q(x,y))$$

nezadovoljiva. Dovoljno je, dakle, dokazati da je formula

$$((\forall x)(\exists y)p(x,y) \wedge (\forall u)(\forall v)(\neg p(u,v) \vee q(u,v)) \wedge (\exists w)(\forall z)\neg q(w,z))$$

nezadovoljiva. Preneks normalna forma ove formule je

$$(\exists w)(\forall x)(\exists y)(\forall u)(\forall v)(\forall z)(p(x,y) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(w,z)) .$$

Nakon skolemizacije, formula dobija oblik:

$$(\forall x)(\forall u)(\forall v)(\forall z)(p(x,g(x)) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(c,z)) ,$$

pri čemu je c nova Skolemova konstanta, a g nova Skolemova funkcija. Konjunktivna normalna forma formule

$$p(x, g(x)) \wedge (\neg p(u, v) \vee q(u, v)) \wedge \neg q(c, z)$$

je

$$p(x, g(x)) \wedge (\neg p(u, v) \vee q(u, v)) \wedge \neg q(c, z) \ .$$

Erbranov univerzum formule $\mathcal{A}$ je sledeći skup

$$H(\mathcal{A}) = \{c, g(c), g(g(c)), \ldots\}$$

Skup klauza čije instance treba razmatrati je skup

$$\{p(x, g(x)), \neg p(u, v) \vee q(u, v), \neg q(c, z)\} \ .$$

Skup

$$\{p(c, g(c)), \neg p(c, g(c)) \vee q(c, g(c)), \neg q(c, g(c))\}$$

je nezadovoljiv, pa na osnovu teoreme 3.23, sledi da je i formula $\neg(((\forall x)(\exists y)$ $p(x, y) \wedge (\forall x)(\forall y)(p(x, y) \Rightarrow q(x, y))) \Rightarrow (\forall x)(\exists y)q(x, y))$ nezadovoljiva, tj. da je formula $\mathcal{A}$ valjana.

Na osnovu svojstava Erbranovih interpretacija može se dokazati da svaki zadovoljiv skup rečenica prvog reda ima model sa konačnim ili prebrojivim domenom. O tome govori naredna teorema.

Teorema 3.24 *Formula logike prvog reda $\mathcal{A}$ je zadovoljiva ako i samo ako za nju postoji model sa konačnim ili prebrojivim domenom.*

Dokaz: Na osnovu teoreme 3.20 za svaku rečenicu $\mathcal{A}$ postoji formula $\mathcal{B}$ u klauzalnoj formi takva da je $\mathcal{A}$ zadovoljiva ako i samo ako je $\mathcal{B}$ zadovoljiva. Na osnovu teoreme 3.21 sledi da je rečenica $\mathcal{B}$ zadovoljiva ako i samo ako ima Erbranov model. Erbranov model uvek ima konačan ili prebrojiv domen. Dakle, rečenica $\mathcal{A}$ je zadovoljiva ako i samo ako ima model sa konačnim ili prebrojivim domenom. □

Iz navedene teoreme direktno sledi naredno tvrđenje.

Teorema 3.25 (Skolem-Lovenhajmova teorema za logiku prvog reda) *Svaki zadovoljiv skup rečenica prvog reda ima model sa konačnim ili prebrojivim domenom.*

Mnogi beskonačni skupovi važni u matematici nisu prebrojivi. Na primer, metodom dijagonalizacije može se dokazati da skup realnih brojeva nije prebrojiv. Skolem-Lovenhajmova teorema tvrdi da skup formula ne može da karakteriše beskonačan neprebrojiv skup na način koji bi isključivao prebrojive modele.

Zadaci

Zadatak 64 *Dokazati da je formula* $(\exists x)(\forall y)p(x,y) \Rightarrow (\forall y)(\exists x)p(x,y)$ *valjana.*

Zadatak 65 *Formulisati rečenicu „*Ako su svi ljudi smrtni i ako je Sokrat čovek, onda je Sokrat smrtan*“ kao formulu logike prvog reda i dokazati da je valjana koristeći Erbran-Gilmorovu teoremu.*

Zadatak 66 *Primenom Erbran-Gilmorove teoreme dokazati da važi*

$$\forall x(p(x) \Rightarrow q(x)), \forall x(q(x) \Rightarrow s(x)), \forall x(r(x) \Rightarrow s(x)), \forall x(p(x) \vee r(x)) \models \forall x\ s(x)\ .$$

3.2.5 Unifikacija

Problem unifikacije je problem ispitivanja da li postoji supstitucija koja čini dva izraza (dva terma ili dve formule) jednakim. Unifikacija se prvi put pominje u radovima Posta, a zatim i u radovima Erbrana.

Definicija 3.25 *Ako su* e_1 *i* e_2 *izrazi i ako postoji supstitucija* σ *takva da važi* $e_1\sigma = e_2\sigma$*, onda kažemo da su izrazi* e_1 *i* e_2 unifikabilni *i da je supstitucija* σ unifikator *za ta dva izraza.*

Dva unifikabilna izraza mogu da imaju više unifikatora. Za dva unifikatora σ_1 i σ_2 kažemo da su jednaka do na preimenovanje promenljivih ako postoji supstitucija λ koja je oblika $[v_1' \mapsto v_1'', v_2' \mapsto v_2'', \ldots, v_n' \mapsto v_n'']$, pri čemu su v_i' i v_i'' simboli promenljivih i važi $\sigma_1\lambda = \sigma_2$.

Primer 3.21 *Neka je term* t_1 *jednak* $g(x,z)$*, neka je term* t_2 *jednak* $g(y,f(y))$ *i neka je* σ *supstitucija* $[y \mapsto x, z \mapsto f(x)]$*. Tada je i* $t_1\sigma$ *i* $t_2\sigma$ *jednako* $g(x,f(x))$*, pa su termovi* t_1 *i* t_2 *unifikabilni, a* σ *je (jedan) njihov unifikator. Unifikator termova* t_1 *i* t_2 *je npr. i* $[x \mapsto a, y \mapsto a, z \mapsto f(a)]$*. Termovi* $g(x,x)$ *i* $g(y,f(y))$ *nisu unifikabilni.*

Definicija 3.26 *Supstitucija* σ *je* najopštiji unifikator *za izraze* e_1 *i* e_2 *ako svaki unifikator* τ *izraza* e_1 *i* e_2 *može biti predstavljen u obliku* $\tau = \sigma\mu$ *za neku supstituciju* μ*.*

Na osnovu definicije, svaki unifikator izraza e_1 i e_2 može biti dobijen od najopštijeg unifikatora primenom neke supstitucije. Svaka dva unifikabilna izraza imaju najopštiji unifikator. Može se dokazati da za dva izraza postoji najviše jedan najopštiji unifikator (do na preimenovanje promenljivih).

Unifikacija ima mnoge primene. Jedna od najznačajnijih je u metodu rezolucije.

Na slici 3.2 dat je opis opšteg algoritma za određivanje najopštijeg unifikatora. Pretpostavimo da je dat niz parova izraza

$$(s_1,t_1),(s_2,t_2),\ldots,(s_n,t_n)$$

Algoritam: Najopštiji unifikator

Ulaz: Niz jednakosti $s_1 = t_1, s_2 = t_2, \ldots, s_n = t_n$
Izlaz: Najopštiji unifikator (ako on postoji)

Primenjuj, dok je to moguće, sledeće korake:

1. Ako postoje jednakosti koje imaju više od jednog pojavljivanja, obriši za svaku od njih sva pojavljivanja osim jednog (factoring).
2. Obriši sve jednakosti oblika $t = t$ (tautology).
3. Ako je x promenljiva i t term koji nije promenljiva i ako se $t = x$ pojavljuje u nizu jednakosti, zameni jednakost $t = x$ sa $x = t$. Ovo uraditi za sve jednakosti tog oblika (orientation).
4. Pretpostavimo da je jednakost $s = t$ element niza jednakosti i da ni s ni t nisu promenljive. Razmotri sledeće slučajeve:
   (a) Ako je s jednako $\varphi(u_1, u_2, \ldots, u_k)$ i t je jednako $\varphi(v_1, v_2, \ldots, v_k)$ (gde je φ funkcijski ili predikatski simbol), onda dodaj jednakosti $u_1 = v_1$, $u_2 = v_2$, ..., $u_k = v_k$ i zatim obriši jednakost $s = t$ (decomposition).
   (b) Ako su s i t bilo koje druge forme, zaustavi rad i kao rezultat vrati *neuspeh* (ovo se odnosi na slučajeve kada je jedan od termova simbol konstante, a drugi nije; kada se u s i t razlikuju vodeći funkcijski (odnosno predikatski) simboli i kada su vodeći funkcijski (odnosno predikatski) simboli s i t različite arnosti) (collision).
5. Ako je x promenljiva, t term koji sadrži x i $x = t$ se pojavljuje u nizu jednakosti, zaustavi rad i kao rezultat vrati *neuspeh* (cycle).
6. Ako je x promenljiva, t term koji ne sadrži x, x se pojavljuje i u nekim drugim jednakostima i $x = t$ se pojavljuje u nizu jednakosti, onda primeni supstituciju $[x \mapsto t]$ na sve druge jednakosti (application).

Ako nije moguće primeniti nijedan od navedenih koraka vrati tekući skup jednakosti kao najopštiji unifikator.

Slika 3.2: Algoritam Najopštiji unifikator

i da se traži supstitucija σ takva da važi

$$s_1\sigma = t_1\sigma, s_2\sigma = t_2\sigma, \ldots, s_n\sigma = t_n\sigma \ .$$

Algoritam unifikacije ili vraća traženu supstituciju ili se zaustavlja neuspešno, ukazujući na to da tražena supstitucija ne postoji. Ukoliko postoji bar jedna supstitucija koja zadovoljava traženi uslov, algoritam unifikacije vraća najopštiji unifikator (za date parove izraza). Ulaz za algoritam unifikacije za parove $(s_1, t_1), (s_2, t_2), \ldots, (s_n, t_n)$ se obično zadaje u vidu niza jednakosti $s_1 = t_1, s_2 = t_2, \ldots, s_n = t_n$.

Primetimo da je korak 6 algoritma moguće u opštem slučaju primeniti na više načina. Bilo koji od tih načina vodi istom rezultatu — neuspehu (ako ne postoji traženi unifikator) ili jednom od unifikatora koji se mogu razlikovati samo do na preimenovanje promenljivih.

U koracima 5 i 6 se primenjuje tzv. provera pojavljivanja čime se obezbeđuje zaustavljanje procedure (tj. sprečava pojavljivanje beskonačnih petlji).

Primer 3.22 *Ilustrujmo rad algoritma za određivanje na primeru sledeće dve jednakosti:*

$$g(y) = x$$
$$f(x, h(x), y) = f(g(z), w, z)$$

Polazni niz jednakosti je
$g(y) = x, f(x, h(x), y) = f(g(z), w, z)$.
Primenom koraka 3 *dobijamo*
$x = g(y), f(x, h(x), y) = f(g(z), w, z)$.
Primenom koraka $4(a)$ *dobijamo*
$x = g(y), x = g(z), h(x) = w, y = z$.
Korak 6 *je moguće primeniti na više načina. Primenom koraka* 6 *za* $y = z$ *dobijamo*
$x = g(z), x = g(z), h(x) = w, y = z$.
Primenom koraka 1 *dobijamo*
$x = g(z), h(x) = w, y = z$.
Primenom koraka 3 *dobijamo*
$x = g(z), w = h(x), y = z$.
Primenom koraka 6 *dobijamo*
$x = g(z), w = h(g(z)), y = z$.
Ovaj niz jednakosti određuje traženi najopštiji unifikator σ. *Za*

$$\sigma = [x \mapsto g(z), w \mapsto h(g(z)), y \mapsto z]$$

važi

$$g(y)\sigma = x\sigma$$
$$f(x, h(x), y)\sigma = f(g(z), w, z)\sigma$$

tj. važi

$$g(z) = g(z)$$
$$f(g(z), h(g(z)), z) = f(g(z), h(g(z)), z) \ .$$

Primer 3.23 *Razmotrimo sledeću jednakost:*

$$g(x, x) = g(y, f(y)) \ .$$

Primenom koraka $4(a)$ *dobijamo*
$x = y, x = f(y)$.
Korak 6 *može se primeniti samo na dva načina:*

- *primenom koraka za jednakost* $x = y$*; tada se dobija* $x = y, y = f(y)$*, odakle se, primenom koraka* 5 *dolazi do neuspeha.*
- *primenom koraka za jednakost* $x = f(y)$*; tada se dobija* $f(y) = y, x = f(y)$*, odakle se, primenom koraka 3 i koraka* 5 *dolazi do neuspeha.*

Bez dokaza navodimo teoremu o korektnosti navedenog algoritma za određivanje najopštijeg unifikatora (videti, na primer, [3, 18]).

Teorema 3.26 (Korektnost algoritma Najopštiji unifikator) *Algoritam Najopštiji unifikator zadovoljava sledeće uslove:*

- *zaustavlja se;*
- *ako vrati supstituciju, onda je ona najopštiji unifikator za dati niz parova izraza;*
- *ako se algoritam zaustavi sa neuspehom, onda ne postoji unifikator za dati niz parova izraza.*

Navedeni algoritam nije efikasan. Postoje znatno efikasniji algoritmi za unifikaciju. Mnogi od njih zasnovani su na korišćenju pogodnih struktura podataka i implicitnom primenjivanju supstitucije (iz koraka 6). Neki od tih algoritama imaju linearnu složenost (po broju polaznih jednakosti), ali, u opštem slučaju, najopštiji unifikator može imati i eksponencijalnu dužinu (po broju polaznih jednakosti), te ga nije moguće eksplicitno predstaviti u linearnom vremenu. To ilustruje sledeći primer.

Primer 3.24 *Za skup jednakosti*

$$x_1 = f(x_0, x_0)$$
$$x_2 = f(x_1, x_1)$$
$$\dots$$
$$x_n = f(x_{n-1}, x_{n-1})$$

Najopštiji unifikator sadrži zamenu $x_n \mapsto t$*, gde je* t *term koji sadrži samo simbole* x_0 *i* f*, pri čemu ima* $2^n - 1$ *pojavljivanja simbola* f.

Primetimo da je problem ispitivanja da li je neka formula instanca neke aksiomske sheme blizak problemu unifikacije. Navedeni algoritam za određivanje najopštijeg unifikatora može se koristiti i za unifikovanje dobro zasnovanih formula. Prilikom ispitivanja da li neka formula čini instancu neke aksiomske sheme, međutim, vrši se samo *jednosmerno uparivanje* i varijable u formulama se smatraju konstantama koje nije moguće instancirati. Postoje i drugi algoritmi za jednosmerno uparivanje.

Primer 3.25 *Za testiranje da li je* $p(f(s(a), f(u, v)), s(f(a, f(u, v))))$ *instanca formule* $p(f(s(x), y), s(f(x, y)))$ *može se primeniti algoritam za određivanje najopštijeg unifikatora na jednakost*

$$p(f(s(a), f(u, v)), s(f(a, f(u, v)))) = p(f(s(x), y), s(f(x, y)))$$

uz restrikciju da se koristi samo jednostrano uparivanje tj. da se sve promenljive iz prve formule smatraju konstantama koje nije moguće supstituisati. Time se dobija najopštiji unifikator

$$\sigma = [x \mapsto a, y \mapsto f(u, v)] \ .$$

Zbog restrikcije nad varijablama u jednosmernom uparivanju, u testiranju da li je $p(f(s(a), f(u, y)), s(f(a, f(u, y))))$ *instanca formule* $p(f(s(x), y), s(f(x, y)))$*, simboli* y *u prvoj i drugoj formuli ne smatraju se jednakim, te je najopštiji unifikator za ove dve formule*

$$\sigma = [x \mapsto a, y \mapsto f(u, y)] \ .$$

Zadaci

Zadatak 67 *Odrediti najopštiji unifikator za sledeći skup parova termova:*

$$\{(g(x, h(y, z)), g(u, x)),\ (f(x), f(h(c, v))),\ (g(z, u), g(y, u))\} \ .$$

Zadatak 68 *Ispitati da li je relacija unifikabilnosti tranzitivna.*

Zadatak 69 $\surd$ *Dokazati da za dva izraza postoji najviše jedan najopštiji unifikator (do na preimenovanje promenljivih).*

3.2.6 Metod rezolucije

Metod rezolucije je postupak za ispitivanje (ne)zadovoljivosti skupa klauza logike prvog reda [61]. Ovaj metod je, u određenom smislu, unapređenje Gilmorove procedure i svojstava koje obezbeđuje Erbran-Gilmorova teorema (teorema 3.23). U Gilmorovoj proceduri mnoge od generisanih instanci klauza su jednake. Dodatno, kada se pokaže da jedan skup instanci klauza nije nezadovoljiv, to ne daje sugestiju koju instancu generisati sledeću. Metod rezolucije ispravlja ove neefikasnosti time što ne radi direktno sa instancama klauza. Naime, potraga za kontradikcijom izvodi se nad originalnim klauzama (a ne

samo nad njihovim instancama). Testiranje nezadovoljivosti zasniva se na korišćenju pravila rezolucije za izvođenje novih klauza, u pokušajima da se izvede kontradikcija.

Analogno metodu rezolucije za iskaznu logiku (videti poglavlje 2.2.7), metod rezolucije za logiku prvog reda primenjuje se na formule koje su u klauzalnoj formi. Formula se reprezentuje kao skup klauza od kojih je svaka skup literala. Kao i u iskaznom slučaju, sve klauze koje sadrže literale jednake logičkim konstantama $\top$ ili $\bot$ se eliminišu ili zamenjuju tako da se ne promeni zadovoljivost polaznog skupa klauza (videti poglavlje 2.2.7). Ako je literal l jednak $p(t_1, t_2, \ldots, t_n)$, onda sa $\overline{l}$ označavamo literal $\neg p(t_1, t_2, \ldots, t_n)$; ako je literal l jednak $\neg p(t_1, t_2, \ldots, t_n)$, onda sa $\overline{l}$ označavamo literal $p(t_1, t_2, \ldots, t_n)$. Za literale l i $\overline{l}$ kažemo da su (međusobno) *komplementni*.

U metodu rezolucije za iskaznu logiku primenjuje se pravilo rezolucije sledećeg oblika:

$$\frac{C' \vee l \quad C'' \vee \overline{l}}{C' \vee C''}$$

U logici prvog reda, pravilo rezolucije je opštije, i umesto da zahteva da u dve klauze postoje komplementni literali, zahteva da u dve klauze postoje literali $\mathcal{A}'$ i $\neg\mathcal{A}''$ takvi da su atomičke formule $\mathcal{A}'$ i $\mathcal{A}''$ unifikabilne. *Pravilo rezolucije* za logiku prvog reda (u njegovom osnovnom obliku, tzv. binarna rezolucija) može se prikazati na sledeći način:

$$\frac{\Gamma' \vee \mathcal{A}' \quad \Gamma'' \vee \neg\mathcal{A}''}{(\Gamma' \vee \Gamma'')\sigma}$$

gde su Γ' i Γ'' klauze, a σ je najopštiji unifikator za $\mathcal{A}'$ i $\mathcal{A}''$.

Obe klauze na koje se primenjuje pravilo rezolucije su (implicitno) univerzalno kvantifikovane. Zbog toga se svaka od njihovih varijabli može preimenovati (jer su formule $\forall x \mathcal{A}(x)$ i $\forall x' \mathcal{A}(x')$ logički ekvivalentne). Štaviše, to je neophodno uraditi za sve deljene varijable, jer bi, inače, neke primene pravila rezolucije bile (pogrešno) onemogućene (jer odgovarajući literali ne bi bili unifikabilni). Preimenovanje varijabli može se primeniti pre primene pojedinačnog pravila rezolucije ili unapred, pre primene sâmog metoda rezolucije. Ako se preimenovanje varijabli primenjuje unapred, pre primene metoda rezolucije, onda ono treba da obezbedi da nikoje dve klauze nemaju zajedničku promenljivu. Dodatno, u svakoj novoizvedenoj klauzi treba preimenovati promenljive tako da se novi simboli promenljivih ne pojavljuju ni u jednoj drugoj klauzi.

Klauzu koja nema nijedan literal zovemo *prazna klauza* i obeležavamo sa $\square$. Ona je, na osnovu dogovora, uvek nezadovoljiva.

Primer 3.26 *Nad klauzama*

$\neg p(x, y) \vee \neg p(z, y) \vee p(x, z)$

i

$\neg p(b, a)$

se može primeniti pravilo rezolucije, jer su literali $p(x,z)$ *i* $p(b,a)$ *unifikabilni (uz najopštiji unifikator* $\sigma = [x \mapsto b, z \mapsto a]$*). Rezolventa ove dve klauze je klauza*

$\neg p(b,y) \vee \neg p(a,y)$.

Ako se pravilo rezolucije primenjuje dalje, onda u dobijenoj klauzi sve promenljive treba da budu preimenovane (treba da dobiju imena koja do tada nisu korišćena):

$\neg p(b,y') \vee \neg p(a,y')$.

Puno pravilo rezolucije omogućava rezolviranje više literala odjednom. Ono može biti reprezentovano na sledeći način:

$$\frac{\Gamma' \vee \mathcal{A}'_1 \vee \mathcal{A}'_2 \vee \ldots \vee \mathcal{A}'_m \quad \Gamma'' \vee \neg\mathcal{A}''_1 \vee \neg\mathcal{A}''_2 \vee \ldots \vee \neg\mathcal{A}''_n}{(\Gamma' \vee \Gamma'')\sigma}$$

gde je σ najopštiji unifikator za formule $\mathcal{A}'_1, \mathcal{A}'_2, \ldots, \mathcal{A}'_m, \mathcal{A}''_1, \mathcal{A}''_2, \ldots, \mathcal{A}''_n$.

Primer 3.27 *Razmotrimo klauze* $\neg p(x,y) \vee \neg p(z,y) \vee p(x,z)$ *i* $\neg p(b,u) \vee \neg p(v,a)$. *Prva sadrži literal* $p(x,z)$ *a druga literale* $\neg p(b,u)$ *i* $\neg p(v,a)$. *Literali* $p(x,z)$, $p(b,u)$ *i* $p(v,a)$ *mogu biti unifikovani (najopštijim) unifikatorom* $[x \mapsto b, v \mapsto b, z \mapsto a, u \mapsto a]$ *i rezolventa date dve klauze je* $\neg p(b,y) \vee \neg p(a,y)$.

Definicija 3.27 Forma Kovalskog *klauze*

$$\neg\mathcal{A}_1 \vee \neg\mathcal{A}_2 \vee \ldots \vee \neg\mathcal{A}_m \vee \mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n$$

je formula

$$\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_m \Rightarrow \mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n \ .$$

Specijalno, forma Kovalskog klauze

$$\mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n$$

je formula

$$\Rightarrow \mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n \ ,$$

a klauze

$$\neg\mathcal{A}_1 \vee \neg\mathcal{A}_2 \vee \ldots \vee \neg\mathcal{A}_m$$

formula

$$\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_m \Rightarrow \ .$$

Ako je u $\neg\mathcal{A}_1 \vee \neg\mathcal{A}_2 \vee \ldots \vee \neg\mathcal{A}_m \vee \mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n$ *i* $m = 0$ *i* $n = 0$, *onda je to prazna klauza, koju označavamo* $\Rightarrow$ *ili* $\square$.

Precizno govoreći, forme Kovalskog $\Rightarrow \mathcal{B}_1 \vee \mathcal{B}_2 \vee \ldots \vee \mathcal{B}_n$, $\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_m \Rightarrow$ i $\Rightarrow$ nisu dobro zasnovane formule, ali čine zapis klauza koji je intuitivan i blizak zapisu u PROLOG-u.

Pravilo rezolucije može da se reprezentuje i koristeći formu Kovalskog:

$$\frac{\Gamma' \Rightarrow \mathcal{B}' \vee \mathcal{A}'_1 \vee \mathcal{A}'_2 \vee \ldots \vee \mathcal{A}'_m \quad \Gamma'' \wedge \mathcal{A}''_1 \wedge \mathcal{A}''_2 \wedge \ldots \wedge \mathcal{A}''_n \Rightarrow \mathcal{B}''}{(\Gamma' \wedge \Gamma'' \Rightarrow \mathcal{B}' \vee \mathcal{B}'')\sigma}$$

gde je σ najopštiji unifikator za formule $\mathcal{A}'_1$, $\mathcal{A}'_2$, ..., $\mathcal{A}'_m$, $\mathcal{A}''_1$, $\mathcal{A}''_2$, ..., $\mathcal{A}''_n$.

Zaista, primenom supstitucije σ na prvu formulu ($\Gamma' \Rightarrow \mathcal{B}' \vee \mathcal{A}'_1 \vee \mathcal{A}'_2 \vee \ldots \vee \mathcal{A}'_m$) dobija se

$$\Gamma'\sigma \wedge \neg\mathcal{B}'\sigma \Rightarrow \mathcal{A} \ ,$$

gde je $\mathcal{A} = \mathcal{A}'_i\sigma = \mathcal{A}''_j\sigma$. Primenom supstitucije σ na drugu formulu ($\Gamma'' \wedge \mathcal{A}''_1 \wedge \mathcal{A}''_2 \wedge \ldots \wedge \mathcal{A}''_n \Rightarrow \mathcal{B}''$) dobija se

$$\mathcal{A} \Rightarrow \neg\Gamma''\sigma \vee \mathcal{B}''\sigma \ .$$

Iz $\Gamma'\sigma \wedge \neg\mathcal{B}'\sigma \Rightarrow \mathcal{A}$ i $\mathcal{A} \Rightarrow \neg\Gamma''\sigma \vee \mathcal{B}''\sigma$ dobija se

$$\Gamma'\sigma \wedge \neg\mathcal{B}'\sigma \Rightarrow \neg\Gamma''\sigma \vee \mathcal{B}''\sigma \ ,$$

što je logički ekvivalentnto sa

$$(\Gamma' \wedge \Gamma'' \Rightarrow \mathcal{B}' \vee \mathcal{B}'')\sigma \ .$$

Primer 3.28 *Razmotrimo sledeće dve klauze Kovalskog:* $p(x, y) \wedge p(z, y) \Rightarrow p(x, z)$ *i* $p(b, u) \wedge p(v, a) \Rightarrow$. *Literali* $p(x, z)$, $p(b, u)$ *i* $p(v, a)$ *mogu biti unifikovani supstitucijom* $[x \mapsto b, z \mapsto a, u \mapsto a, v \mapsto b]$. *Tada je forma Kovalskog rezolvente date dve klauze:* $p(b, y) \wedge p(a, y) \Rightarrow$.

Metod rezolucije sastoji se od uzastopnog primenjivanja pravila rezolucije. Neka je S početni skup, neka je $S_0 = S$ i neka je S_{i+1} rezultat primene pravila rezolucije na skup S_i.[2] Postupak se zaustavlja na jedan od sledeća dva načina:

- ako u nekom koraku skup S_i sadrži praznu klauzu ($\square$), onda zaustavi primenu procedure i vrati odgovor da je skup klauza S nezadovoljiv;
- ako ne postoji mogućnost da se primeni pravilo rezolucije tako da se skupovi S_i i S_{i+1} razlikuju, onda zaustavi primenu procedure i vrati odgovor da je skup klauza S zadovoljiv.

Da bi se dokazalo da je neka formula $\mathcal{A}$ valjana, njena negacija se transformiše u klauzalnu formu i onda se na dobijeni skup klauza primenjuje metod rezolucije. Ako se izvede prazna klauza, onda to znači da je formula $\neg\mathcal{A}$ nezadovoljiva, pa je $\mathcal{A}$ valjana; ako u nekom koraku ne može da se izvede nijedna nova klauza, onda to znači je formula $\neg\mathcal{A}$ zadovoljiva, pa $\mathcal{A}$ nije valjana. Moguć je i ishod da nove klauze mogu da se izvode beskonačno, a da se pri tome ne izvede prazna klauza.

Da bi se dokazalo da je neka formula $\mathcal{A}$ logička posledica formula $\mathcal{B}_1$, $\mathcal{B}_2$, ..., $\mathcal{B}_n$ potrebno je dokazati da je formula $\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_n \Rightarrow \mathcal{A}$ valjana, tj. dokazati da formula $\neg(\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_n \Rightarrow \mathcal{A})$ nije zadovoljiva. Potrebno je, dakle, dokazati da formula $\mathcal{B}_1 \wedge \mathcal{B}_2 \wedge \ldots \wedge \mathcal{B}_n \wedge \neg\mathcal{A}$ nije zadovoljiva.

[2] Primetimo da u opštem metodu nije specifikovano kako se, od svih mogućih, bira par klauza nad kojim se primenjuje pravilo rezolucije.

Primer 3.29 *Dokazati da je formula* $p(a) \Rightarrow (\exists x)p(x)$ *valjana. Negacija date formule je logički ekvivavalentna formuli* $p(a) \wedge (\forall x)\neg p(x)$. *Metod rezolucije primenjujemo na skup klauza* $\{p(a), \neg p(x)\}$. *Pravilo rezolucije moguće je primeniti samo na jedan način — literali* $p(a)$ *i* $\neg p(x)$ *se unifikuju supstitucijom* $[x \mapsto a]$ *i njime se dobija prazna klauza. Odatle sledi da je formula* $p(a) \Rightarrow (\exists x)p(x)$ *valjana.*

Primer 3.30 *Formula* $(\forall x)(\exists y)p(x,y) \Rightarrow (\exists y)(\forall x)p(x,y)$ *nije valjana. Negacija date formule je logički ekvivalentna sa formulom* $(\forall x)(\exists y)(p(x,y) \wedge (\forall y)(\exists x)\neg p(x,y))$ *i sa formulom* $(\forall x)(\exists y)(\forall u)(\exists v)(p(x,y) \wedge \neg p(v,u))$. *Skolemizacijom se dobija skup od dve klauze:* $\{p(x, f(x)), \neg p(g(x,u), u)\}$. *Pravilo rezolucije nije moguće primeniti na ove dve klauze, odakle sledi da je formula* $(\forall x)(\exists y)(p(x,y) \wedge (\forall y)(\exists x)\neg p(x,y))$ *zadovoljiva, tj. polazna formula nije valjana.*

Niz klauza (polaznih i izvedenih) označavaćemo obično sa C_i ($i = 1, 2, \ldots$). Izvedene klauze označavaćemo ponekad i sa R_i ($i = 1, 2, \ldots$). Iza izvedene klauze zapisivaćemo oznake klauza iz kojih je ona izvedena, redne brojeve literala u tim klauzama, iskorišćeni najopštiji unifikator, kao i supstituciju kojom se preimenuju promenljive. Literale u klauzama razdvajaćemo obično simbolom ',' (umesto simbolom '$\vee$').

Primer 3.31 *Dokažimo da je formula*

$$(\forall x)(\exists y)q(x,y)$$

logička posledica skupa formula

$$\{(\forall x)(\exists y)p(x,y), (\forall x)(\forall y)(p(x,y) \Rightarrow q(x,y))\} .$$

Dovoljno je dokazati da je formula

$$\mathcal{A} = ((\forall x)(\exists y)p(x,y) \wedge (\forall x)(\forall y)(p(x,y) \Rightarrow q(x,y))) \Rightarrow (\forall x)(\exists y)q(x,y)$$

valjana. Preneks normalna forma negacije ove formule je

$$(\exists w)(\forall x)(\exists y)(\forall u)(\forall v)(\forall z)(p(x,y) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(w,z)) .$$

Nakon skolemizacije, ova formula dobija oblik:

$$(\forall x)(\forall u)(\forall v)(\forall z)(p(x, g(x)) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(c,z)) ,$$

pri čemu je c *nova Skolemova konstanta, a* g *nova Skolemova funkcija. Konjunktivna normalna forma formule*

$$p(x, g(x)) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(c,z)$$

je

$$p(x, g(x)) \wedge (\neg p(u,v) \vee q(u,v)) \wedge \neg q(c,z) .$$

Elementi početnog skupa klauza su:

H_1 : $p(x, g(x))$ *(prvi deo hipoteze)*
H_2 : $\neg p(u, v), q(u, v)$ *(drugi deo hipoteze)*
C_1 : $\neg q(c, z)$ *(zaključak)*

Prazna klauza se izvodi na sledeći način.

R_1 : $q(x', g(x'))$ $(H_1, 1; H_2, 1)$, $[v \mapsto g(x), u \mapsto x]$; *preimenovanje:* $[x \mapsto x']$
R_2 : $\square$ $(C_1, 1; R_1, 1)$, $[x' \mapsto c, z \mapsto g(c)]$

Primer 3.32 *Dokazati da je formula* $\mathcal{A} = \forall x \forall y \forall z (x \subseteq y \wedge y \subseteq z \Rightarrow x \subseteq z)$ *logička posledica formule* $\mathcal{B} = \forall x \forall y (x \subseteq y \Leftrightarrow \forall w (w \in x \Rightarrow w \in y))$ *(simboli* $\in$ *i* $\subseteq$ *su predikatski simboli arnosti* 2 *zapisani infiksno).*

Transformisanjem formule $\neg(\mathcal{B} \Rightarrow \mathcal{A}) \equiv \mathcal{B} \wedge \neg\mathcal{A}$ *dobija se sledeći skup klauza:*

H_1 : $\neg(x_1 \subseteq y_1), \neg(w_1 \in x_1), w_1 \in y_1$ *(deo* $\Rightarrow$ *formule* $\mathcal{B}$*)*
H_2 : $x_2 \subseteq y_2, f(x_2, y_2) \in x_2$ *(dva dela* $\Leftarrow$ *formule* $\mathcal{B}$*,*
H_3 : $x_3 \subseteq y_3, \neg(f(x_3, y_3) \in y_3)$ *f je Skolemova funkcija za* w*)*
C_1 : $a \subseteq b$ *(tri dela negacije formule* $\mathcal{A}$*,*
C_2 : $b \subseteq c$ a, b, c *su Skolemove konstante za*
C_3 : $\neg(a \subseteq c)$ *promenljive* x, y, z *u formuli* $\mathcal{A}$*)*

Izvedene klauze označavaćemo sa R_i $(i = 1, 2, \ldots)$.

R_1 : $\neg(w_2 \in a), w_2 \in b$ $(H_1, 1; C_1, 1)$, $[x_1 \mapsto a, y_1 \mapsto b]$; *preimenovanje:* $[w_1 \mapsto w_2]$
R_2 : $\neg(w_3 \in b), w_3 \in c$ $(H_1, 1; C_2, 1)$, $[x_1 \mapsto b, y_1 \mapsto c]$; *preimenovanje:* $[w_1 \mapsto w_3]$
R_3 : $a \subseteq y_4, f(a, y_4) \in b$ $(H_2, 2; R_1, 1)$, $[x_2 \mapsto a, w_2 \mapsto f(a, y_2)]$; *preimenovanje:* $[y_2 \mapsto y_4]$
R_4 : $x_4 \subseteq c, \neg(f(x_4, c) \in b)$ $(H_3, 2; R_2, 2)$, $[y_3 \mapsto c, w_3 \mapsto f(x_3, c)]$; *preimenovanje:* $[x_3 \mapsto x_4]$
R_5 : $a \subseteq c, a \subseteq c$ $(R_3, 2; R_4, 2)$, $[x_4 \mapsto a, y_4 \mapsto c]$;
R_6 : $\square$ $(R_5, 1, 2; C_3, 1)$

Hornove klauze su klauze u kojima postoji najviše jedan literal koji nije pod negacijom. U PROLOG-u se koriste upravo Hornove klauze. Četiri tipa Hornovih klauza prikazana su u sledećoj tabeli.

Tip	standardna forma	forma Kovalskog	PROLOG
implikaciona klauza	$\neg\mathcal{A}_1 \vee \ldots \vee \neg\mathcal{A}_n \vee \mathcal{A}$	$\mathcal{A}_1 \wedge \ldots \wedge \mathcal{A}_n \Rightarrow \mathcal{A}$	$\mathcal{A} :- \mathcal{A}_1, \ldots, \mathcal{A}_n.$
ciljna klauza	$\neg\mathcal{A}_1 \vee \ldots \vee \neg\mathcal{A}_n$	$\mathcal{A}_1 \wedge \ldots \wedge \mathcal{A}_n \Rightarrow$	$?- \mathcal{A}_1, \ldots, \mathcal{A}_n.$
činjenica	$\mathcal{A}$	$\Rightarrow \mathcal{A}$	$\mathcal{A}.$
prazna klauza	$\square$	$\Rightarrow$	`false`

Može se dokazati da svaki nezadovoljiv skup Hornovih klauza sadrži bar jednu činjenicu i bar jednu ciljnu klauzu. Programski jezik PROLOG zasnovan je na metodu rezolucije i na korišćenju Hornovih klauza. Postoji polinomijalni algoritam za ispitivanje zadovoljivosti skupa iskaznih Hornovih klauza i on se koristi u PROLOG-u.

Primer 3.33 *Pretpostavimo da je u* PROLOG*-u zadata činjenica* (assertion)*:*

```
man(sokrat).
```

i pravilo (rule)*:*

```
mortal(X) :- man(X).
```

*(*PROLOG *konvencija je da se konstante zapisuju malim početnim slovom, a promenljive velikim početnim slovom.) Ako se zada upit:*

```
? - mortal(sokrat).
```

onda se metodom rezolucije pokušava izvođenje prazne klauze iz skupa klauza:

$$\{man(sokrat), \neg man(X) \vee mortal(X), \neg mortal(sokrat)\} .$$

U ovom slučaju, prazna klauza se izvodi jednostavno (koristeći unifikaciju $\{X \mapsto sokrat\}$*) i* PROLOG *vraća rezultat:*

```
Yes
```

Primetimo da, na primer, upit

```
? - mortal(platon).
```

ne može da uspe (sem ako nije zadata i činjenica `man(platon)`*).*

Da bi se pokazalo da je neka formula nezadovoljiva, dovoljno je, primenom metoda rezolucije, iz njenog skupa klauza izvesti praznu klauzu. Dodatno, metod rezolucije ima svojstvo da iz zadovoljivog skupa klauza ne može da izvede nezadovoljiv skup klauza. Ova dva svojstva dokazaćemo kao teoremu o potpunosti i teoremu o saglasnosti za rezoluciju (teoreme 3.28 i 3.30). Metod rezolucije, dakle, ima sledeće karakteristike:

- metod rezolucije je saglasan: ako je primenom metoda dobijena prazna klauza, onda je i polazni skup klauza nezadovoljiv (ili, drugim rečima, iz zadovoljivog skupa klauza može se dobiti samo zadovoljiv skup klauza);
- metod rezolucije nije potpun, ali je potpun za pobijanje: iz svakog nezadovoljivog skupa klauza moguće je izvesti praznu klauzu;
- logika prvog reda nije odlučiva, pa najviše što može metod rezolucije da bude je procedura poluodlučivanja (za problem ispitivanja valjanosti).

Teorema 3.27 (Saglasnost pravila rezolucije) *Ako je skup klauza* S *zadovoljiv i ako je klauza* $\mathcal{B}$ *izvedena iz dve klauze iz skupa* S *pravilom rezolucije, onda je i skup* $S \cup \{\mathcal{B}\}$ *zadovoljiv.*

Dokaz: Neka su klauze iz skupa S klauze nad nekom signaturom $\mathcal{L}$. Naglasimo da su sve klauze u skupu S, kao i klauza $\mathcal{B}$, implicitno univerzalno kvantifikovane.

Pretpostavimo da je skup S zadovoljiv: neka je $\mathfrak{D}$ $\mathcal{L}$-struktura i v valuacija takve da za odgovarajuću interpretaciju I_v i za svaku klauzu C iz S važi $I_v(\forall * C) = 1$. Na osnovu teoreme 3.7, onda važi da je svaka formula C iz S valjana u $\mathfrak{D}$.

Dokažimo da je i skup $S \cup \{\mathcal{B}\}$ zadovoljiv, tj. dokažimo da je i formula $\forall * \mathcal{B}$ tačna u interpretaciji I_v. Na osnovu teoreme 3.7, dovoljno je dokazati da za svaku valuaciju w važi $I_w(\mathcal{B}) = 1$.

Pretpostavimo da je klauza $\mathcal{B}$ izvedena iz klauza $C' = \Gamma' \vee \mathcal{A}'_1 \vee \mathcal{A}'_2 \vee \ldots \vee \mathcal{A}'_m$ i $C'' = \Gamma'' \vee \neg\mathcal{A}''_1 \vee \neg\mathcal{A}''_2 \vee \ldots \vee \neg\mathcal{A}''_n$, pri čemu je $\mathcal{B} = (\Gamma' \vee \Gamma'')\sigma$, gde je σ najopštiji unifikator za formule $\mathcal{A}'_1, \mathcal{A}'_2, \ldots, \mathcal{A}'_m, \mathcal{A}''_1, \mathcal{A}''_2, \ldots, \mathcal{A}''_n$. Neka je $\mathcal{A} = \mathcal{A}'_1\sigma = \mathcal{A}'_2\sigma = \ldots = \mathcal{A}'_m\sigma = \mathcal{A}''_1\sigma = \mathcal{A}''_2\sigma = \ldots = \mathcal{A}''_n\sigma$. Neka je σ supstitucija $[x_1 \mapsto t_1, x_2 \mapsto t_2, \ldots, x_k \mapsto t_k]$.

Neka je w proizvoljna valuacija. Neka je w' valuacija takva da je $w'(x_i) = I_w(t_i)$ za $i = 1, 2, \ldots, k$ i $w'(x) = w(x)$ za sve druge promenljive x (sve promenljive različite od $x_1, x_2, \ldots, x_k$) koje se pojavljuju u C' i C''. Formule C' i C'' su valjane u $\mathfrak{D}$, pa važi $I_{w'}(C') = 1$ i $I_{w'}(C'') = 1$. Važi i $I_w(C'\sigma) = I_{w'}(C') = 1$ i $I_w(C''\sigma) = I_{w'}(C'') = 1$. Iz $I_w(C'\sigma) = 1$ sledi $I_w(\Gamma'\sigma \vee \mathcal{A}) = 1$, pa je $I_w(\Gamma'\sigma) = 1$ ili $I_w(\mathcal{A}) = 1$. Ako je $I_w(\Gamma'\sigma) = 1$, onda važi $I_w(\Gamma'\sigma \vee \Gamma''\sigma) = 1$, tj. $I_w(\mathcal{B}) = 1$. Ako je $I_w(\mathcal{A}) = 1$, onda je $I_w(\neg\mathcal{A}) = 0$, pa iz $1 = I_w(C''\sigma) = I_w(\Gamma''\sigma \vee \neg\mathcal{A})$, sledi $I_w(\Gamma''\sigma) = 1$ i, dalje, $I_w(\Gamma'\sigma \vee \Gamma''\sigma) = 1$, tj. $I_w(\mathcal{B}) = 1$. U oba slučaja, za svaku valuaciju w važi $I_w(\mathcal{B}) = 1$, što je i trebalo dokazati. Dakle, skup $S \cup \{\mathcal{B}\}$ je zadovoljiv. □

Naredna teorema sledi neposredno iz teoreme o saglasnosti pravila rezolucije (3.27) i na osnovu jednostavnog induktivnog argumenta.

Teorema 3.28 (Saglasnost metoda rezolucije) *Iz zadovoljivog skupa klauza ne može se izvesti prazna klauza.*

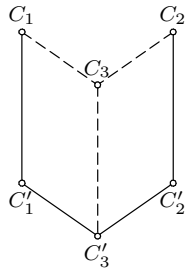
Potpunost metoda rezolucije za logiku prvog reda zasniva se na potpunosti metoda rezolucije za iskaznu logiku i na lifting lemi.

Teorema 3.29 (Lifting lema (lema o podizanju)) *Neka su C_1 i C_2 dve klauze sa baznim instancama C'_1 i C'_2 redom. Ako je C'_3 rezolventa klauza C'_1 i C'_2, onda postoji rezolventa C_3 klauza C_1 i C_2, takva da je C'_3 bazna instanca klauze C_3.*

Dokaz: Dokazaćemo tvrđenje teoreme samo za binarnu rezoluciju. Dokaz za puno pravilo rezolucije je jednostavno uopštenje. Tvrđenje teoreme ilustruje slika 3.3.

Ne narušavajući opštost, pretpostavimo da važi:

- C_1 i C_2 nemaju zajedničke promenljive;
- rezolvirani literal je poslednji u C'_1 i C'_2; on je u pozitivnoj formi u C'_1 i u negativnoj formi u C'_2; tada možemo da pišemo $C_1 = D_1 \vee \mathcal{A}_1$ i $C_2 = D_2 \vee \neg\mathcal{A}_2$ za pogodne klauze D_1, D_2 i literale $\mathcal{A}_1$ i $\mathcal{A}_2$;



Slika 3.3: Ilustracija za lifting lemu (teorema 3.29)

- supstitucija ϕ_1 koja instancira C_1 u C_1' utiče samo na promenljive koje se pojavljuju u C_1; supstitucija ϕ_2 koja instancira C_2 u C_2' utiče samo na promenljive koje se pojavljuju u C_2.

Kako klauze C_1 i C_2 nemaju zajedničkih promenljivih važi $\phi_1\phi_2 = \phi_2\phi_1$. Neka je $\phi = \phi_1\phi_2 = \phi_2\phi_1$. Tada je $\mathcal{A}_1\phi = \mathcal{A}_2\phi = \mathcal{A}$ rezolvirani literal u rezoluciji C_1' i C_2'. Dakle, literali $\mathcal{A}_1$ i $\mathcal{A}_2$ su unifikabilni. Neka je C_3 rezolventa dobijena rezolviranjem ovih literala u klauzama C_1 i C_2. Neka je σ najopštiji unifikator literala $\mathcal{A}_1$ i $\mathcal{A}_2$ i neka je $\phi = \sigma\lambda$ (σ je najopštiji unifikator literala $\mathcal{A}_1$ i $\mathcal{A}_2$, pa svaki drugi unifikator može da se reprezentuje korišćenjem σ). Tada važi $C_3\lambda = C_3'$ (jer je $C_3' = (D_1 \vee D_2)\phi$ i $C_3 = (D_1 \vee D_2)\sigma$), što dokazuje tvrđenje teoreme. □

Teorema 3.30 (Potpunost (za pobijanje) metoda rezolucije) *Ako je Γ nezadovoljiv skup klauza, onda se iz njega metodom rezolucije može izvesti prazna klauza.*

Dokaz: Kako je skup Γ nezadovoljiv, on nema Erbranov model. Na osnovu Erbran-Gilmorove teoreme (3.23), onda postoji konačan skup baznih instanci klauza iz Γ koji je nezadovoljiv. Na osnovu teoreme o potpunosti iskazne rezolucije (2.17) iz tog konačnog skupa baznih klauza može se izvesti prazna klauza. Na osnovu lifting leme (3.29) to izvođenje prazne klauze može se „podići“ do izvođenja (u logici prvog reda) prazne klauze iz skupa Γ. □

Primer 3.34 *Formula $\forall x \forall y\ (p(x,y) \Rightarrow p(y,x))$ je logička posledica formula $\forall x\ p(x,x)$ i $\forall u \forall v \forall w\ (p(u,v) \wedge p(w,v) \Rightarrow p(u,w))$, pa je formula*

$$\mathcal{A} = (\forall x\ p(x,x)) \wedge (\forall u \forall v \forall w\ (p(u,v) \wedge p(w,v) \Rightarrow p(u,w))) \Rightarrow$$
$$(\forall x \forall y\ (p(x,y) \Rightarrow p(y,x)))$$

valjana. Formula $\neg\mathcal{A}$*, transformisanjem u klauzalnu formu, dobija oblik:*

$$p(x,x) \wedge (\neg p(u,v) \vee \neg p(w,v) \vee p(u,w)) \wedge p(a,b) \wedge \neg p(b,a)\ ,$$

gde su a *i* b *nove, Skolemove konstante. Erbranov univerzum formule* $\mathcal{A}$ *je jednak* $\{a,b\}$*. Instanciranjem klauza formule* $\neg\mathcal{A}$ *elementima Erbranovog univerzuma može se dobiti skup* $\{p(b,b), \neg p(b,b) \vee \neg p(a,b) \vee p(b,a), p(a,b), \neg p(b,a)\}$ *(koji je podskup skupa svih instanci klauza formule* $\neg\mathcal{A}$*). Baznom rezolucijom (suštinski — iskaznom rezolucijom), može se pokazati da je navedeni skup nezadovoljiv:*

$C_1:$	$p(b,b)$	
$C_2:$	$\neg p(b,b), \neg p(a,b), p(b,a)$	
$C_3:$	$p(a,b)$	
$C_4:$	$\neg p(b,a)$	
$C_5:$	$\neg p(b,b), p(b,a)$	$(C_2,2;C_3,1)$
$C_6:$	$\neg p(b,b)$	$(C_4,1;C_5,2)$
$C_7:$	$\square$	$(C_1,1;C_6,1)$

Navedeno bazno izvođenje prazne klauze može biti „podignuto" do izvođenja prvog reda:

$C_1:$	$p(x,x)$	
$C_2:$	$\neg p(u,v), \neg p(w,v), p(u,w)$	
$C_3:$	$p(a,b)$	
$C_4:$	$\neg p(b,a)$	
$C_5:$	$\neg p(u',b), p(u',a)$	$(C_2,2;C_3,1)\ [w \mapsto a, v \mapsto b]$; *preimenovanje:* $[u \mapsto u']$
$C_6:$	$\neg p(b,b)$	$(C_4,1;C_5,2)\ [u' \mapsto b]$
$C_7:$	$\square$	$(C_1,1;C_6,1)\ [x \mapsto b]$

Metod rezolucije se može koristiti i za dokazivanje da je neka formula posledica aksioma neke teorije (više o teorijama prvog reda videti u poglavlju 3.4). Teorija jednakosti je deo mnogih interesantnih matematičkih teorija (više o čistoj teoriji jednakosti videti u potpoglavlju 3.4.1), te se često javlja potreba za korišćenjem njenih aksioma. Postoji nekoliko varijanti skupa aksioma jednakosti. Jedna od njih je:

E1 $(\forall x)(x = x)$

E2 $(\forall x)(\forall y)(x = y \Rightarrow y = x)$

E3 $(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow x = z)$

E4 $(\forall x_1)(\forall x_2)\ldots(\forall x_n)(\forall y_1)(\forall y_2)\ldots(\forall y_n)(x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n))$, za svaki funkcijski simbol f arnosti n.

E5 $(\forall x_1)(\forall x_2)\ldots(\forall x_n)(\forall y_1)(\forall y_2)\ldots(\forall y_n)(x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow (p(x_1, x_2, \ldots, x_n) \Rightarrow p(y_1, y_2, \ldots, y_n)))$, za svaki predikatski simbol p arnosti n.

Da bi se koristile u metodu rezolucije, navedene aksiome moraju biti prevedene u klauzalnu formu:

EC1 $(x = x)$

EC2 $\neg(x = y), y = x$

EC3 $\neg(x = y), \neg(y = z), x = z$

EC4 $\neg(x_1 = y_1), \ldots, \neg(x_n = y_n), f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$, za svaki funkcijski simbol f arnosti n.

EC5 $\neg(x_1 = y_1), \ldots, \neg(x_n = y_n), \neg p(x_1, \ldots, x_n), p(y_1, \ldots, y_n)$, za svaki predikatski simbol p arnosti n.

U postupku primene metoda rezolucije često je potreban veliki broj korišćenja aksioma jednakosti (tj. klauza dobijenih od njih), čak i za veoma jednostavna tvrđenja. To ilustruje sledeći primer.

Primer 3.35 *Pretpostavimo da je potrebno korišćenjem aksioma jednakosti dokazati sledeće tvrđenje: formula* $\neg(h(c) = b)$ *je logička posledica skupa formula* $\{\neg(h(a) = b),\ c = a\}$.

Jedina instanca aksiomske sheme EC4 koja je potrebna (jer je h *jedini funkcijski simbol u indukovanoj signaturi) je*

$$\neg(x_1 = y_1), h(x_1) = h(y_1).$$

Jedina instanca aksiomske sheme EC5 koja je potrebna je instanca za predikatski simbol $=$*, ali ona može biti izostavljena zahvaljujući preostalim aksiomama.*

Dodavanjem klauza izvedenih iz zadatog tvrđenja skupu klauza izvedenih iz aksioma jednakosti dobija se početni skup klauza na koji se zatim primenjuje metod rezolucije.

$EC1:$	$(x' = x')$	
$EC2:$	$\neg(x'' = y''), y'' = x''$	
$EC3:$	$\neg(x''' = y'''), \neg(y''' = z'''),$ $x''' = z'''$	
$EC4:$	$\neg(x_1 = y_1), h(x_1) = h(y_1)$	
$C_1:$	$\neg(h(a) = b)$	
$C_2:$	$c = a$	
$C_3:$	$h(c) = b$	
$R_1:$	$\neg(h(a) = y''''), \neg(y'''' = b)$	$(EC3, 3; C_1, 1)\ [x''' \mapsto h(a), z''' \mapsto b]$; *preimenovanje:* $[y''' \mapsto y'''']$
$R_2:$	$\neg(a = y_1'), \neg(h(y_1') = b)$	$(EC4, 2; R_1, 1)\ [x_1 \mapsto a, y'''' \mapsto h(y_1)]$; *preimenovanje:* $[y_1 \mapsto y_1']$
$R_3:$	$\neg(y_1'' = a), \neg(h(y_1'') = b)$	$(EC2, 2; R_2, 1)\ [x'' \mapsto y_1', y'' \mapsto a]$; *preimenovanje:* $[y_1' \mapsto y_1'']$
$R_4:$	$\neg(h(c) = b)$	$(C_2, 1; R_3, 1)\ [y_1'' \mapsto c]$
$R_5:$	$\square$	$(C_3, 1; R_4, 1)$

Primetimo da u opisu metoda rezolucije nije specifikovan način na koji se biraju klauze nad kojim se primenjuje pravilo rezolucije. Takođe, teorema o potpunosti (teorema 3.30) tvrdi da se iz svakog nezadovoljivog skupa klauza *može* izvesti prazna klauza, a ne tvrdi da se iz svakog nezadovoljivog skupa klauza *mora* izvesti prazna klauza bez obzira na izbor klauza za rezolviranje. Naime, u zavisnosti od izbora klauza na koje se primenjuje pravilo rezolucije moguće je da se i za nezadovoljiv skup klauza metod rezolucije ne zaustavlja. Način na koji se biraju klauze na koje se primenjuje pravilo rezolucije čini *strategiju* ili *strategiju za upravljanje* konkretne verzije metoda rezolucije. Strategija je od suštinske važnosti za obezbeđivanje nužnog izvođenja prazne klauze iz nezadovoljivog skupa, ali i za efikasnost metoda.

Jedna od mogućnosti za obezbeđivanje potpunosti metoda rezolucije u strožijem smislu (da postoji strategija za upravljanje metoda rezolucije takva da se iz svakog nezadovoljivog skupa klauza nužno izvodi prazna klauza u konačno mnogo koraka) je sistematsko izvođenje svih rezolventi iz skupa klauza koji se širi tokom primene metoda. *Sistematski metod rezolucije* može se definisati na sledeći način: metod se primenjuje u stupnjevima; prvi stupanj čini kreiranje početnog skupa klauza; neka pre i-tog stupnja tekući skup klauza čine klauze $C_1, C_2, \ldots, C_n$, i-ti stupanj sastoji se od izvođenja (i dodavanja tekućem skupu klauza) svih mogućih rezolventi iz po svake dve klauze iz skupa $C_1, C_2, \ldots, C_n$ (broj tih klauza je konačan); metod se zaustavlja ako se u nekom koraku izvede prazna klauza ili ako se u nekom stupnju ne može izvesti nijedna nova klauza.

Teorema 3.31 (Potpunost sistematskog metoda rezolucije) *Ako je Γ nezadovoljiv skup klauza, onda se iz njega sistematskim metodom rezolucije mora izvesti prazna klauza.*

Dokaz: Ako je skup klauza Γ nezadovoljiv, onda se, na osnovu teoreme o potpunosti metoda rezolucije (teorema 3.30) iz njega metodom rezolucije može izvesti prazna klauza, tj. postoji niz rezolventi $R_1, R_2, \ldots, R_n$ (koje se izvode iz početnih i izvedenih klauza) od kojih je poslednja u nizu prazna klauza. Ako se na skup klauza Γ primeni sistematski metod rezolucije, u nekom stupnju biće (ako već pre toga nije izvedena prazna klauza) izvedene sve klauze iz skupa $R_1, R_2, \ldots, R_n$, pa i prazna klauza. □

Očigledno je da je sistematski metod rezolucije izuzetno neefikasan. Postoji više strategija koje obezbeđuju nužno izvođenje prazne klauze iz nezadovoljivog skupa klauza (tj. sprečavaju beskonačne petlje), ali na efikasniji način. Te strategije su od suštinske važnosti i za broj klauza koje se izvode i, shodno tome, za efikasnost metoda. Smanjivanje izvođenja nepotrebnih klauza jedan je od najvažnijih problema metoda rezolucije. U daljem tekstu biće ukratko opisane neke od strategija koje se koriste u različitim varijantama metoda rezolucije.

Razmotrimo ponovo sledeći primer (videti primer 3.34): potrebno je dokazati da je formula $\forall x \forall y(p(x, y) \Rightarrow p(y, x))$ logička posledica formula $\forall x p(x, x)$ i

$\forall u \forall v \forall w (p(u,v) \wedge p(w,v) \Rightarrow p(u,w))$. Dovoljno je dokazati da formula $\forall x\ p(x,x) \wedge (\forall u \forall v \forall w\ (p(u,v) \wedge p(w,v) \Rightarrow p(u,w))) \wedge \neg(\forall x \forall y\ (p(x,y) \Rightarrow p(y,x)))$ nije zadovoljiva. Negacija navedene formule, transformisanjem u klauzalnu formu, dobija oblik: $p(x,x) \wedge (\neg p(u,v) \vee \neg p(w,v) \vee p(u,w)) \wedge p(a,b) \wedge \neg p(b,a)$ (gde su a i b nove, Skolemove konstante). Primenimo metod rezolucije na ovako dobijen skup klauza:

$C_1:$	$p(x_1,x_1)$	(prva hipoteza)
$C_2:$	$\neg p(u_1,v_1), \neg p(w_1,v_1), p(u_1,w_1)$	(druga hipoteza)
$C_3:$	$p(a,b)$	(prvi deo zaključka)
$C_4:$	$\neg p(b,a)$	(drugi deo zaključka)
$C_5:$	$\neg p(b,v_2), \neg p(a,v_2)$	$(C_4,1;C_2,3)\ [u_1 \mapsto b, w_1 \mapsto a]$; preimenovanje: $[v_1 \mapsto v_2]$
$C_6:$	$\neg p(b,b)$	$(C_5,2;C_3,1)\ [v_2 \mapsto b]$
$C_7:$	$\square$	$(C_6,1;C_1,1)\ [x_1 \mapsto b]$

Primetimo da se u navedenom primeru u svakoj primeni pravila rezolucije koristi poslednja klauza u nizu (osim u prvom koraku, to je uvek rezolventa iz prethodno primenjenog pravila rezolucije) i rezolvira sa nekom od originalnih klauza. Ovaj vid pobijanja je veoma prirodan. On, u izvesnom smislu, oponaša rezonovanje matematičara koji kreće od tvrđenja koje treba dokazati i u dokazu koristi aksiome i date hipoteze. Ova strategija za upravljanje metodom rezolucije zove se *linearna ulazna rezolucija — linearna*, jer se u svakoj primeni pravila rezolucije koristi poslednja klauza u nizu; *ulazna*, jer se u svakoj primeni pravila rezolucije koristi jedna od početnih klauza.

Naglasimo da je navedeno tvrđenje moguće dokazati na više načina. Jedan od načina je i sledeći:

$C_1:$	$p(x_1,x_1)$	(prva hipoteza)
$C_2:$	$\neg p(u_1,v_1), \neg p(w_1,v_1), p(u_1,w_1)$	(druga hipoteza)
$C_3:$	$p(a,b)$	(prvi deo zaključka)
$C_4:$	$\neg p(b,a)$	(drugi deo zaključka)
$C_5:$	$\neg p(b,v_2), \neg p(a,v_2)$	$(C_4,1;C_2,3)\ [u_1 \mapsto b, w_1 \mapsto a]$; preimenovanje: $[v_1 \mapsto v_2]$
$C_6:$	$\neg p(a,b)$	$(C_5,1;C_1,1)\ [x_1 \mapsto b, v_2 \mapsto b]$
$C_7:$	$\square$	$(C_6,1;C_3,1)$

Linearna ulazna rezolucija je jedna od varijanti opšteg metoda rezolucije. S obzirom na to da ona isključuje mnoge puteve izvođenja novih klauza, ona je obično znatno efikasnija nego opšti metod rezolucije. Međutim, iz istog razloga, linearna ulazna rezolucija nema svojstvo potpunosti (kao što ga ima opšti metod rezolucije). Nepotpunost linearne ulazne rezolucije ilustruje sledeći primer:

$C_1:$	$p(x_1), q(x_1)$	
$C_2:$	$\neg p(x_2), q(x_2)$	
$C_3:$	$\neg q(x_3), p(x_3)$	
$C_4:$	$\neg p(x_4), \neg q(x_4)$	
$C_5:$	$\neg p(x_5), \neg p(x_5)$	$(C_4, 2; C_2, 2)\ [x_4 \mapsto x_2]$; preimenovanje: $[x_2 \mapsto x_5]$
$C_6:$	$q(x_6)$	$(C_5, 1, 2; C_1, 1)\ [x_5 \mapsto x_1]$; preimenovanje: $[x_1 \mapsto x_6]$
$C_7:$	$p(x_7)$	$(C_6, 1; C_3, 1)$, $[x_6 \mapsto x_3]$; preimenovanje: $[x_3 \mapsto x_7]$

Klauza C_7 može se rezolvirati samo sa klauzom C_2 ili sa klauzom C_4. Rezolucija sa C_2 daje $q(x)$, što vodi u beskonačnu petlju. Rezolucija sa C_4 daje $\neg q(x)$, što, dalje, daje simetričnu situaciju. Slično važi i za sve ostale mogućnosti, te praznu klauzu nije moguće izvesti ukoliko se koristi linearna ulazna strategija.

Linearna ulazna rezolucija ima svojstvo potpunosti za pobijanje za neke klase formula. Na primer, linearna ulazna rezolucija ima svojstvo potpunosti za pobijanje skupova Hornovih klauza, tj. linearna ulazna rezolucija može dovesti do prazne klauze za svaki kontradiktoran skup Hornovih klauza (u navedenom primeru, prva klauza nije Hornova). Linearna ulazna rezolucija nad Hornovim klauzama se koristi u PROLOG-u.

Uslov linearne strategije može biti korišćen i bez uslova ulazne strategije. Takva strategije daje *linearnu rezoluciju*. Linearna rezolucija ima svojstvo potpunosti (i za ne-Hornove klauze). Iako je linearnom rezolucijom (kao i opštim metodom rezolucije) moguće pobiti svaki kontradiktoran skup klauza, nema garancija (kao i u opštem slučaju) da svaki postupak primene pravila rezolucije nužno vodi izvođenju prazne klauze. Na primer, u pobijanju datog skupa klauza primenom linearne rezolucije moguće je doći i do beskonačne petlje:

$C_1:$	$p(x_1, x_1)$	(prva hipoteza)
$C_2:$	$\neg p(u_1, v_1), \neg p(w_1, v_1), p(u_1, w_1)$	(druga hipoteza)
$C_3:$	$p(a, b)$	(prvi deo zaljučka)
$C_4:$	$\neg p(b, a)$	(drugi deo zaključka)
$C_5:$	$\neg p(b, v_2), \neg p(a, v_2)$	$(C_4, 1; C_2, 3)\ [u_1 \mapsto b, w_1 \mapsto a]$; preimenovanje: $[v_1 \mapsto v_2]$
$C_6:$	$\neg p(b, a)$	$(C_5, 2; C_1, 1)\ [x_1 \mapsto a, v_2 \mapsto a]$
$C_7:$	$\neg p(b, v_3), \neg p(a, v_3)$	$(C_6, 1; C_2, 3)\ [u_1 \mapsto b, w_1 \mapsto a]$; preimenovanje: $[v_1 \mapsto v_3]$
$C_8:$	$\neg p(b, a)$	$(C_7, 2; C_1, 1)\ [x_1 \mapsto a, v_3 \mapsto a]$
	$\ldots$	

Pored opisane ulazne strategije i linearne strategije, neke od najznačajnijih strategija za upravljanje metodom rezolucije su:

- prednost jediničnim klauzama (u ovoj strategiji prednost imaju primene pravila rezolucije u kojima je bar jedna roditeljska klauza jedinična (tj. ima samo jedan literal));
- skup potpore (u ovoj strategiji pre primene samog metoda rezolucije odre-

đuje se tzv. skup potpore — skup klauza koji je nezadovoljiv, ali je svaki njegov pravi podskup zadovoljiv; svako pravilo rezolucije primenjuje se onda nad bar jednom klauzom iz tog skupa. Ideja ove strategije je da se izbegne primenjivanje pravila rezolucije nad parovima klauza iz skupa koji je zadovoljiv (npr. nad klauzama koje su izvedene iz aksioma neprotivrečne teorije) i time popravi efikasnost sistema).

U cilju efikasnijeg izvođenja prazne klauze u metodu rezolucije se ponekad koriste i dodatna pravila (pored pravila rezolucije).

Paramodulacija Sa ciljem da zameni veliki broj (često komplikovanih i neprirodnih) koraka u korišćenju aksioma jednakosti, uvodi se pravilo *paramodulacije*. Ono povećava efikasnost metoda rezolucije, ali nije nužno njegov deo (jer pravilo paramodulacije može biti izvedeno pravilom rezolucije). Pravilo paramodulacije može biti reprezentovano na sledeći način:

$$\frac{\mathcal{A} \quad t = s \vee \mathcal{B} \;\; (\text{ ili } s = t \vee \mathcal{B})}{(\mathcal{A}[t' \mapsto s] \vee \mathcal{B})\sigma}$$

gde je σ najopštiji unifikator za termove t i t' i gde je $\mathcal{A}$ formula koja sadrži term t'. Na primer, iz klauza $\neg h(a) = b$ i $c = a$ može da se izvede klauza $\neg h(c) = b$ primenom pravila paramodulacije (u jednom koraku) na sledeći način (videti primer 3.35):

$$\frac{\neg h(a) = b \quad c = a}{((\neg h(a) = b)[a \mapsto c])\,[\,]}$$

Grupisanje U nekim sistemima, umesto punog pravila rezolucije koriste se dva pravila — binarna rezolucija i grupisanje. Grupisanje se može opisati na sledeći način:

$$\frac{\Gamma \vee \mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_m}{(\Gamma \vee \mathcal{A}_1)\sigma}$$

gde je σ najopštiji unifikator za formule $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$.

Sadržanost Pravilo sadržanosti omogućava brisanje klauze $\mathcal{A}$ iz skupa klauza Γ ako u tom skupu postoje klauza $\mathcal{B}$ i supstitucija σ takve da $\mathcal{A}$ sadrži klauzu $\mathcal{B}\sigma$. Dodatno, iz skupa klauza Γ mogu se obrisati i sve klauze koje sadrže komplementne literale.

Može se dokazati da saglasnost i potpunost metoda rezolucije važe i kada se pored pravila rezolucije koriste i pravila paramodulacije, grupisanja i sadržanosti.

Za detaljniji opis ovih i srodnih tehnika videti na primer, [8, 62].

Zadaci

Zadatak 70 *Koristeći metod rezolucije dokazati da važi:*

$$(\forall x)(p(x) \Rightarrow q(x)), p(c) \models q(c) \ .$$

Zadatak 71 *Metodom rezolucije dokazati da je naredna formula valjana:*

$$(\exists x)(\forall y)p(x,y) \Rightarrow (\forall y)(\exists x)p(x,y) \ .$$

Zadatak 72 *Metodom rezolucije dokazati da je naredna formula valjana:*

(a) $(\forall y)((\forall x)p(x) \Rightarrow p(y))$
(b) $(\forall x)p(x) \Rightarrow (\exists x)p(x)$
(c) $\neg(\exists y)p(y) \Rightarrow (\forall y)((\exists x)p(x) \Rightarrow p(y))$
(d) $(\exists x)p(x) \Rightarrow (\exists y)p(y)$
(e) $(\forall x)(p(x) \wedge q(x)) \Leftrightarrow (\forall x)p(x) \wedge (\forall x)q(x)$
(f) $(\forall x)p(x) \vee (\forall x)q(x) \Rightarrow (\forall x)(p(x) \vee q(x))$
(g) $(\exists x)(p(x) \vee q(x)) \Leftrightarrow (\exists x)p(x) \vee (\exists x)q(x)$
(h) $(\exists x)(p(x) \wedge q(x)) \Rightarrow (\exists x)p(x) \wedge (\exists x)q(x)$

Zadatak 73 *Metodom rezolucije dokazati da je formula* $(H \wedge K) \Rightarrow L$ *valjana, gde je*

$H = (\forall x)(\forall y)(p(x,y) \Rightarrow p(y,x))$
$K = (\forall x)(\forall y)(\forall z)((p(x,y) \wedge p(y,z)) \Rightarrow p(x,z))$
$L = (\forall x)(\forall y)(p(x,y) \Rightarrow p(x,x))$.

Zadatak 74 *Metodom rezolucije dokazati da je formula* $(\forall x)s(x)$ *logička posledica skupa formula* $\{\forall x(p(x) \Rightarrow q(x)), \forall x(q(x) \Rightarrow s(x)), \forall x(r(x) \Rightarrow s(x)), \forall x(p(x) \vee r(x))\}$.

Zadatak 75 *Metodom rezolucije dokazati da je formula* $\forall x \forall y \ (x = y \Rightarrow y = x)$ *logička posledica formula* $\forall x \ (x = x)$ *i* $\forall u \forall v \forall w \ (u = v \wedge w = v \Rightarrow u = w)$.

Zadatak 76 $\surd$ *Važi sledeće:*
Janko ima psa.
Svaki vlasnik psa voli životinje.
Nijedna osoba koja voli životinje ne može da udari životinju.
Janko ili Marko su udarili mačku čije je ime Tuna.
Svaka mačka je životinja.
Metodom rezolucije dokazati da je Marko udario Tunu.

Zadatak 77 *Za narednu formulu metodom rezolucije dokazati da je valjana:*

$$(\forall x)(\mathcal{A}(x) \Rightarrow C) \Leftrightarrow ((\exists x)\mathcal{A}(x) \Rightarrow C)$$

pri čemu je C *rečenica. (Ovaj zadatak ilustruje kako metod rezolucije može biti oslabljen tako da se primenjuje i na formule koje nisu u klauzalnoj formi.)*

Zadatak 78 *Prevesti na jezik logike prvog reda i dokazati metodom rezolucije sledeće tvrđenje: Ako su svi političari lukavi i ako su samo pokvareni ljudi političari, onda, ako postoji bar jedan političar, onda je neki pokvaren čovek lukav.*

3.2.7 Metod tabloa

U opisu metoda tabloa oslanjaćemo se na opis metoda tabloa za iskaznu logiku (videti poglavlje 2.2.8) i pojmove koji su tamo uvedeni. Jednostavnosti radi, smatraćemo da u signaturi $\mathcal{L}$ formula koje ispitujemo nema funkcijskih simbola arnosti veće od 0. To ograničenje nije suštinsko i ne umanjuje opštost metoda. Zaista, svaki skup formula može biti zamenjen skupom formula nad signaturom koja nema funkcijske simbole arnosti veće od 0. Neka je, na primer, $\mathcal{L}$ signatura koja sadrži predikatski simbol q arnosti 2 i funkcijski simbol f arnosti 1. Ovoj signaturi možemo da pridružimo signaturu $\mathcal{L}'$ sa predikatskim simbolom q arnosti 2, predikatskim simbolom p_f arnosti 2 i predikatskim simbolom = arnosti 2 (za jednakost). Na primer, skup formula $\Gamma = \{(\forall x)(\exists y)(q(x,y) \Rightarrow q(x,f(y)))\}$ nad signaturom $\mathcal{L}$ je valjan ako i samo ako je valjan skup formula Γ' nad signaturom $\mathcal{L}'$ koji sadrži aksiome jednakosti (videti poglavlje 3.4.1) i formule $(\forall x)(\forall y)(\forall z)(p_f(x,y) \wedge p_f(x,z) \Rightarrow y = z)$ i $(\forall x)(\exists y)(\forall z)(q(x,y) \wedge p_f(y,z) \Rightarrow q(x,z))$.

U metodu tabloa za predikatsku logiku koriste se dve sheme pravila analogne shemama za iskaznu logiku (videti poglavlje 2.2.8):

Pravila tipa (A):

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\begin{array}{l}\alpha_1\\ \alpha_2\end{array}}$$

Pravila tipa (B):

$$\frac{\beta}{\beta_1 \mid \beta_2}$$

Ova dva tipa pravila specifikovana su na sledeći način.

Pravila tipa (A):

$$\frac{T\neg\mathcal{A}}{F\mathcal{A}} \qquad \frac{F\neg\mathcal{A}}{T\mathcal{A}} \qquad \frac{T(\mathcal{A}\wedge\mathcal{B})}{\begin{array}{l}T\mathcal{A}\\ T\mathcal{B}\end{array}} \qquad \frac{F(\mathcal{A}\vee\mathcal{B})}{\begin{array}{l}F\mathcal{A}\\ F\mathcal{B}\end{array}} \qquad \frac{F(\mathcal{A}\Rightarrow\mathcal{B})}{\begin{array}{l}T\mathcal{A}\\ F\mathcal{B}\end{array}}$$

Pravila tipa (B):

$$\frac{F(\mathcal{A}\wedge\mathcal{B})}{F\mathcal{A} \mid F\mathcal{B}}$$

$$\frac{T(\mathcal{A} \vee \mathcal{B})}{T\mathcal{A} \mid T\mathcal{B}}$$

$$\frac{T(\mathcal{A} \Rightarrow \mathcal{B})}{F\mathcal{A} \mid T\mathcal{B}}$$

Pored ove dve sheme pravila (za odgovarajuće tipove formula), u metodu tabloa za predikatsku logiku koriste se dodatne dve grupe pravila (za odgovarajuće tipove formula).

Pravila tipa (C):

$\frac{T(\forall x)\mathcal{A}}{T\mathcal{A}[x \mapsto a]}$ gde je a bilo koji simbol konstante iz signature

$\frac{F(\exists x)\mathcal{A}}{F\mathcal{A}[x \mapsto a]}$ gde je a bilo koji simbol konstante iz signature

Pravila tipa (D):

$\frac{T(\exists x)\mathcal{A}}{T\mathcal{A}[x \mapsto a]}$ gde je a novi simbol konstante

$\frac{F(\forall x)\mathcal{A}}{F\mathcal{A}[x \mapsto a]}$ gde je a novi simbol konstante

Pravila tipa (C) i (D) eliminišu kvantifikatore i zovemo ih i *direktna pravila*.

Za označenu formulu kažemo da je tipa γ ako je ona oblika $T(\forall x)\mathcal{A}$ ili $F(\exists x)\mathcal{A}$ i tada se na nju može primeniti pravilo tipa (C). Takvu formulu ćemo ponekad i označavati sa γ, a sa $\gamma(a)$ formulu $T\mathcal{A}[x \mapsto a]$ i $F\mathcal{A}[x \mapsto a]$, gde je a simbol konstante upotrebljen u pravilu.

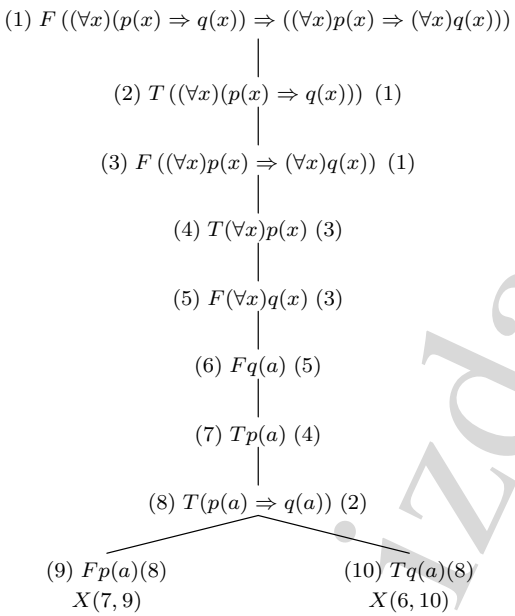
Za označenu formulu kažemo da je tipa δ ako je ona oblika $T(\exists x)\mathcal{A}$ ili $F(\forall x)\mathcal{A}$ i tada se na nju može primeniti pravilo tipa (D). Takvu formulu ćemo ponekad i označavati sa δ, a sa $\delta(a)$ formulu $T\mathcal{A}[x \mapsto a]$ i $F\mathcal{A}[x \mapsto a]$, gde je a simbol konstante upotrebljen u pravilu.

Dakle, pravila tipa (C) i (D) imaju sledeću (opštu) formu:

$\frac{\gamma}{\gamma(a)}$ gde je a bilo koji simbol konstante iz signature

$\frac{\delta}{\delta(a)}$ gde je a novi simbol konstante

Tablo se u metodu za logiku prvog reda konstruiše analogno kao u metodu za iskaznu logiku. U korenu tabloa je označena formula $F\mathcal{A}$, gde je $\mathcal{A}$ zatvorena (dobro zasnovana) formula čija se valjanost ispituje. Sve formule koje se pridružuju čvorovima tabloa su takođe zatvorene (dobro zasnovane) formule.



Slika 3.4: Tablo za formulu iz primera 3.36

Primer 3.36 *Formula* $(\forall x)(p(x) \Rightarrow q(x)) \Rightarrow ((\forall x)p(x) \Rightarrow (\forall x)q(x))$ *je valjana. Tablo koji to dokazuje prikazan je na slici 3.4.*

Pravila tipa (D) mogu se smatrati formalizacijom sledećeg intuitivnog argumenta koji se koristi u matematičkim dokazima. Pretpostavimo da smo u okviru nekog dokaza pokazali da postoji element x sa određenim svojstvom p, tj. pretpostavimo da smo dokazali da je formula $(\exists x)p(x)$ valjana. Tada obično kažemo „neka je a takav element x“ i možemo da tvrdimo $p(a)$. Naravno, mi time ne tvrdimo da p važi za svako a, nego za bar jedno. Ako u nastavku pokažemo da za neko svojstvo q postoji element x takav da važi $q(x)$, mi ne možemo ponovo da kažemo „neka je a takav element x“, jer je a simbol nove konstante takav da je $p(a)$ a ne znamo da li postoji element x takav da važi $p(x)$ i $q(x)$. Zato tada kažemo „neka je b takav element x“ i možemo da tvrdimo $q(b)$. Uvođenje novih simbola konstanti primenom pravila tipa (D) (u iteracijama) proširuje signaturu i analogno je skolemizaciji. Na osnovu svojstava skolemizacije (3.18), ako je formula $\mathcal{A}$ dobijena skolemizacijom od zadovoljive formule $\mathcal{B}$, onda je i formula $\mathcal{A}$ zadovoljiva. Odatle sledi i četvrti deo narednog tvrđenja (prva tri su jednostavna). U tvrđenju se pod signaturom $\mathcal{L}$ misli na signaturu dobijenu od polazne signature proširivanjem novim simbolima konstanti.

Teorema 3.32 (Saglasnost pravila metoda tabloa) *Ako je S dati skup označenih formula nad signaturom $\mathcal{L}$, onda važi:*

- *ako je skup S zadovoljiv i $\alpha \in S$, onda je i skup $\{S, \alpha_1, \alpha_2\}$ zadovoljiv;*
- *ako je skup S zadovoljiv i $\beta \in S$, onda je bar jedan od skupova $\{S, \beta_1\}$, $\{S, \beta_2\}$ zadovoljiv;*
- *ako je skup S zadovoljiv i $\gamma \in S$, onda za bilo koji simbol konstante a (iz signature $\mathcal{L}$) važi da je skup $\{S, \gamma(a)\}$ zadovoljiv;*
- *ako je skup S zadovoljiv i $\delta \in S$, i ako je a simbol konstante (iz signature $\mathcal{L}$) koji se ne pojavljuje ni u jednoj formuli iz S, onda je skup formula $\{S, \delta(a)\}$ zadovoljiv.*

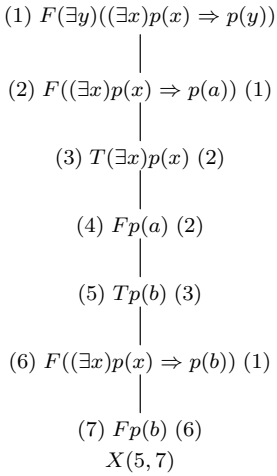
Teorema 3.33 (Saglasnost metoda tabloa) *Ako se neka formula može dokazati metodom tabloa (pobijanjem), onda je ona valjana.*

Dokaz: Pretpostavimo da je θ grana tabloa i pretpostavimo da je grana θ zadovoljiva. Ako proširimo granu θ primenom pravila tipa (A), (C) ili (D), onda je dobijeno proširenje grane θ takođe zadovoljivo (na osnovu teoreme 3.32). Ako granu θ proširimo primenom pravila tipa (B) na dve grane θ_1 i θ_2, simultano, onda je (na osnovu teoreme 3.32) bar jedna od grana θ_1 i θ_2 zadovoljiva. Indukcijom se onda jednostavno može pokazati sledeće: ako je koren tabloa zadovoljiv, onda je bar jedna grana tabloa zadovoljiva i, stoga, otvorena. Dakle, ako je tablo zatvoren (tj. ako je svaka njegova grana zatvorena), onda njegov koren mora da bude nezadovoljiv. Drugim rečima, ako se neka formula može dokazati metodom tabloa, onda je ona valjana. □

Može se smatrati da su simboli konstanti koje se uvode pravilima tipa (D) (i koji proširuju polaznu signaturu) elementi prebrojivog skupa i da su enumerisani (npr. a_1, a_2, a_3, ...). Ta pretpostavka, za sada, omogućava uvođenje novih simbola nekim redom, a kasnije će biti iskorišćena i u izvođenju bitnih svojstava metoda tabloa i logike prvog reda.

Pravila tipa (D) mogu biti oslabljena tako da se umesto uslova „a je novi simbol konstante“, koristi uslov „a je novi simbol konstante ili a je prethodno uveden pravilom tipa (C) i ne pojavljuje se u formuli δ“. Korišćenjem ove slabije varijante pravila tipa (D) dokazi izvedeni metodom tabloa mogu biti bitno kraći. Ovo slabljenje pravila tipa (D) može se opravdati na sledeći način: pretpostavimo da smo dokazali formulu $(\forall x)p(x)$ (koja je tipa γ). Tada možemo da zaključimo $p(a)$ (za novi simbol konstante a). Time nismo označili sa a neki poseban element, već $p(a)$ važi za *bilo koju* vrednost a. Dakle, ako naknadno dokažemo formulu $(\exists x)q(x)$ onda možemo da kažemo „neka je a takva vrednost x“ i za tu vrednost važiće i $p(a)$. Može se dokazati saglasnost i ove varijante metoda tabloa.

Primer 3.37 *Formula $(\exists y)((\exists x)p(x) \Rightarrow p(y))$ je valjana. To može biti dokazano koristeći osnovnu verziju pravila tipa (D), kao i kraće, koristeći modifikovana pravila tipa (D). Odgovarajuća dva tabloa prikazana su na slikama 3.5 i 3.6.*



Slika 3.5: Tablo za formulu $(\exists y)((\exists x)p(x) \Rightarrow p(y))$ dobijen primenom osnovnih pravila tipa (D)

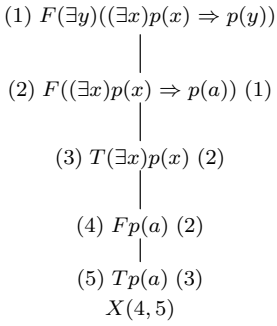
Metod tabloa za predikatsku logiku je potpun (za pobijanje). Naime, svaka valjana formula može biti dokazana (pobijanjem) metodom tabloa. To će biti dokazano u nastavku.

Definicija 3.28 *Kažemo da je skup označenih zatvorenih formula S nad signaturom $\mathcal{L}$* Hintikin *ako naredni uslovi važe za sve α, β, γ, δ formule iz S:*

- *ne postoji formula $\mathcal{A}$ takva da i $T\mathcal{A}$ i $F\mathcal{A}$ pripadaju skupu S;*
- *ako $\alpha \in S$, onda važi $\alpha_1 \in S$ i $\alpha_2 \in S$;*
- *ako $\beta \in S$, onda važi $\beta_1 \in S$ ili $\beta_2 \in S$;*
- *ako $\gamma \in S$, onda za svaki simbol konstante a iz $\mathcal{L}$ važi $\gamma(a) \in S$;*
- *ako $\delta \in S$, onda postoji simbol konstante a iz $\mathcal{L}$ takav da važi $\delta(a) \in S$.*

Teorema 3.34 (Hintikina lema za logiku prvog reda) *Svaki Hintikin skup formula S nad signaturom $\mathcal{L}$ je zadovoljiv.*

Dokaz: Pretpostavimo da je S Hintikin skup za $\mathcal{L}$. Konstruišimo model skupa S u $\mathcal{L}$-strukturi $\mathfrak{D} = (D, I^{\mathcal{L}})$ čiji domen D je skup svih simbola konstanti iz signature $\mathcal{L}$. Neka za svaki simbol konstante a iz $\mathcal{L}$ važi $I^{\mathcal{L}}(a) = a$. Potrebno je konstruisati interpretaciju za domen D u kojoj su svi elementi skupa S tačni. Interpretaciju $I^{\mathcal{L}}$ konstruišemo tako što za svaki predikatski simbol p arnosti n definišemo preslikavanje p_I iz D^n u $\{0, 1\}$



Slika 3.6: Tablo za formulu $(\exists y)((\exists x)p(x) \Rightarrow p(y))$ dobijen primenom oslabljenih pravila tipa (D)

i to na sledeći način: baznoj atomičkoj formuli $p(a_1, a_2, \ldots, a_n)$ nad $\mathcal{L}$ pridružujemo vrednost 1 ako $Tp(a_1, a_2, \ldots, a_n)$ pripada skupu S, a vrednost 0 ako $Fp(a_1, a_2, \ldots, a_n)$ pripada skupu S; inače, formuli $p(a_1, a_2, \ldots, a_n)$ pridružujemo bilo vrednost 1 bilo vrednost 0. Dokažimo da je svaka formula $\mathcal{A}$ iz skupa S tačna u ovako određenoj interpretaciji. Dokažimo to indukcijom po složenosti formule $\mathcal{A}$.

Ako je složenost formule $\mathcal{A}$ jednaka 0, onda je $\mathcal{A}$ atomička formula, pa je ona tačna u konstruisanoj interpretaciji (na osnovu konstrukcije interpretacije). Pretpostavimo da je tvrđenje tačno za sve formule složenosti manje od n $(n > 0)$ i dokažimo da je tačno i za sve formule složenosti jednake n. Ako je složenost formule $\mathcal{A}$ jednaka n, onda je formula $\mathcal{A}$ ili tipa α, ili tipa β ili tipa γ ili tipa δ. Ako je $\mathcal{A}$ tipa α, onda i α_1 i α_2 pripadaju skupu S, a ove formule su složenosti manje od n, pa je, na osnovu induktivne hipoteze, bar jedna tačna u konstruisanoj interpretaciji; odatle sledi da je i formula $\mathcal{A}$ tačna u konstruisanoj interpretaciji. Ako je $\mathcal{A}$ tipa β, onda β_1 ili β_2 pripada skupu S, a ove formule su složenosti manje od n, pa su, na osnovu induktivne hipoteze, one tačne u konstruisanoj interpretaciji; odatle sledi da je i formula $\mathcal{A}$ tačna u konstruisanoj interpretaciji. Ako je $\mathcal{A}$ tipa γ, onda za svaki simbol konstante a iz $\mathcal{L}$ važi $\gamma(a) \in S$, a $\gamma(a)$ je složenosti manje od složenosti formule γ, pa su, na osnovu induktivne hipoteze, one tačne u konstruisanoj interpretaciji; odatle sledi da je i formula $\mathcal{A}$ tačna u konstruisanoj interpretaciji. Ako je $\mathcal{A}$ tipa δ, onda postoji simbol konstante a iz $\mathcal{L}$ takav da važi $\delta(a) \in S$, a $\delta(a)$ je složenosti manje od složenosti formule δ, pa je, na osnovu induktivne hipoteze, $\delta(a)$ tačna u konstruisanoj interpretaciji; odatle sledi da je i formula $\mathcal{A}$ tačna u konstruisanoj interpretaciji. □

Teorema 3.35 (Kenigova lema) *Neka u stablu $\mathcal{T}$ svaki čvor ima konačno mnogo neposrednih potomaka. Ako stablo $\mathcal{T}$ ima beskonačno mnogo čvorova, onda ono ima bar jednu beskonačnu granu.*

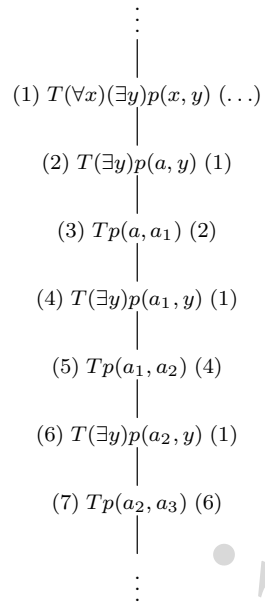
Dokaz: Čvor stabla ćemo zvati *dobrim* ako on ima beskonačno mnogo (neposrednih i posrednih) potomaka, a *lošim* ako on ima konačno mnogo (neposrednih i posrednih) potomaka. Na osnovu pretpostavke, stablo $\mathcal{T}$ ima beskonačno mnogo čvorova. Svi ti čvorovi (sem korena) su potomci korena, pa je koren dobar čvor. Ako su svi neposredni potomci jednog čvora loši, onda i taj čvor mora biti loš (jer ima konačno mnogo neposrednih potomaka i svaki od njih je loš). Dakle, dobar čvor mora imati bar jednog neposrednog potomka koji je dobar čvor. Zato koren n_0 mora imati dobrog neposrednog potomka n_1, n_1 mora imati dobrog neposrednog potomka n_2, n_2 mora imati dobrog neposrednog potomka n_3, itd. Dakle, postoji beskonačna grana $(n_0, n_1, n_2, n_3, \ldots)$ stabla $\mathcal{T}$, što je i trebalo dokazati. □

U iskaznoj logici, za svaku polaznu formulu metod tabloa se zaustavlja. Međutim, u logici prvog reda metod tabloa se ne zaustavlja uvek. Ako se desi da se metod ne zaustavlja, onda se generiše beskonačno stablo $\mathcal{T}$ i, na osnovu Kenigove leme, to stablo $\mathcal{T}$ sadrži bar jednu beskonačnu granu θ. Grana θ je otvorena, ali ona nije nužno Hintikin skup i to će biti pokazano u nastavku. U tom kontekstu biće razmatrana signatura $\mathcal{L}$ koja odgovara beskonačnoj grani θ. Signatura $\mathcal{L}$ dobijena je proširivanjem originalne signature novim simbolima konstanti primenama pravila tipa (D) na formulama na grani θ. I ako polazna signatura sadrži konačno mnogo simbola konstanti, proširena signatura $\mathcal{L}$ sadrži beskonačno mnogo simbola konstanti (jer je grana θ beskonačna). Primer 3.38 ilustruje kako se signatura može proširiti beskonačnim (prebrojivim) skupom (novih) simbola konstanti.

Primer 3.38 *Primenom metoda tabloa (i to primenom pravila tipa (D)) može se dobiti beskonačan (ali prebrojiv) niz novih simbola konstanti. Na slici 3.7 dat je primer situacije u kojoj se početna signatura koja sadrži samo simbol konstante a proširuje simbolima konstanti a_1, a_2, a_3, ...*

Za svaku formulu $\mathcal{A}$ (nad signaturom $\mathcal{L}$) složenosti veće od 0 koja pripada grani θ reći ćemo da je *ispunjena* na θ ako važi jedan od uslova:

- $\mathcal{A}$ je tipa α i obe odgovarajuće formule α_1 i α_2 pripadaju grani θ;
- $\mathcal{A}$ je tipa β i bar jedna od odgovarajućih formula β_1 i β_2 pripada grani θ;
- $\mathcal{A}$ je tipa γ i za svaki simbol konstante a iz $\mathcal{L}$ odgovarajuća formula $\gamma(a)$ pripada grani θ;
- $\mathcal{A}$ je tipa δ i bar za jedan simbol konstante a iz $\mathcal{L}$ odgovarajuća formula $\delta(a)$ pripada grani θ.



Slika 3.7: Primer uvođenja novih simbola konstanti a_1, a_2, a_3, ...

Pretpostavimo da neka grana tabloa $\mathcal{T}$ sadrži dve formule γ tipa — označimo ih sa γ' i γ''. Korišćenjem formule γ' grani možemo dodati formule $\gamma'(a_1)$, $\gamma'(a_2)$, $\gamma'(a_3)$, ... za postojeće i novouvedene simbole konstanti a_1, a_2, a_3, ... (tim dodavanjem može da se omogućava novo primenjivanje δ pravila i uvođenje novih konstanti, te tako može da se uvede prebrojivo mnogo novih simbola konstanti, slično kao u primeru 3.38). Time je generisana beskonačna grana koja *ispunjava* formulu γ', ali ne i formulu γ''. Slično, moguće je *ispuniti* jednu γ formulu, ali ostaviti *neispunjenim* formule α, β i δ tipa. Dakle, postoji mnogo načina za generisanje beskonačnog tabloa takvog da nisu sve njegove otvorene grane Hintikini skupovi (ili, čak, takvog da nijedna njegova otvorena grana nije Hintikin skup). Suštinski problem je utvrđivanje *sistematske* procedure koja garantuje da, ako se ne zaustavlja, onda je u generisanom tablou svaka otvorena grana Hintikin skup. Postoji mnoštvo takvih sistematskih procedura i u daljem tekstu opisaćemo jednu od najjednostavnijih.

U *sistematskom metodu tabloa*, u svakom koraku određeni čvorovi stabla se označavaju kao *upotrebljeni* (na primer, takvi čvorovi, odnosno odgovarajuće formule, mogu se označiti sa desne strane simbolom $\surd$). Postupak se započinje time što se polazna formula (formula za koju se ispituje da li je valjana) označava sa F i pridružuje korenu stabla. Ovim se završava prvi stupanj. Pretpostavimo da je završen n-ti stupanj postupka. Nastavak postupka odvija se na sledeći način. Ako je konstruisani tablo zatvoren, onda se prekida izvršavanje procedure. Takođe, izvršavanje procedure prekida se ako je svaka neatomička formula na svakoj otvorenoj grani konstruisanog tabloa *upotrebljena*. Inače, bira se čvor najmanje dubine (tj. najbliže korenu) i odgovarajuća

formula $\mathcal{A}$ koja nije do tada upotrebljena i koja pripada bar jednoj otvorenoj grani (ako ima više takvih čvorova, može se prihvatiti dogovor na osnovu kojeg se onda bira *najlevlji* takav čvor); tada se konstruisani tablo proširuje na sledeći način:

- za svaku otvorenu granu θ koja sadrži izabrani čvor, ako je $\mathcal{A}$ formula tipa α, onda se grani θ dodaju čvorovi α_1 i α_2 (tj. grana θ se produžava do grane $(\theta, \alpha_1, \alpha_2)$);
- za svaku otvorenu granu θ koja sadrži izabrani čvor, ako je $\mathcal{A}$ formula tipa β, onda se grana θ produžava simultano na dve grane (θ, β_1) i (θ, β_2);
- za svaku otvorenu granu θ koja sadrži izabrani čvor, ako je $\mathcal{A}$ tipa γ, onda se, za prvi simbol konstante a takav da se $\gamma(a)$ ne pojavljuje na θ, grana θ proširuje do grane $(\theta, \gamma(a), \gamma)$;
- za svaku otvorenu granu θ koja sadrži izabrani čvor, ako je $\mathcal{A}$ tipa δ, onda se, za prvi simbol konstante a koji se ne pojavljuje u $\mathcal{T}$, grana θ proširuje čvorom $\delta(a)$ (tj. grana θ se proširuje do grane $(\theta, \delta(a))$).

Nakon tog koraka, izabrani čvor označavamo kao *upotrebljen* i time se završava $(n+1)$-i stupanj procedure.

Naglasimo da stablo generisano ovom procedurom, strogo govoreći, nije tablo, jer ne postoji tablo pravilo koje dozvoljava ponavljanje formula tipa γ (ili bilo kojeg drugog tipa). Međutim, jednostavno se može dokazati da ako naknadno obrišemo sva ponavljanja, onda je dobijeno stablo zaista tablo. Drugim rečima, ako je moguće zatvoriti tablo dozvoljavajući proizvoljna ponavljanja, onda je moguće zatvoriti tablo i bez tih ponavljanja (jer, šta god da je dobijeno od ponovljenih formula, moglo bi biti dobijeno i od sâmih originalnih formula).

Tablo koji je konstruisan korišćenjem opisanog postupka zvaćemo *sistematski tablo*. Za sistematski tablo ćemo reći da je *upotpunjen* u sledećim slučajevima: ako je on beskonačan ili ako je konačan i ne može biti proširen korišćenjem sistematske procedure (drugim rečima, za svaku otvorenu granu sve neatomičke formule su već upotrebljene).

Teorema 3.36 *U upotpunjenom sistematskom tablou svaka otvorena grana je zadovoljiva.*

Dokaz: U upotpunjenom sistematskom tablou bilo da je otvorena grana konačna ili beskonačna, na osnovu osobina postupka za sistematski tablo, sve formule na toj grani su ispunjene, pa je ta grana Hintikin skup. Na osnovu teoreme 3.34, sledi da je taj skup zadovoljiv, pa je u upotpunjenom sistematskom tablou svaka otvorena grana zadovoljiva, što je i trebalo dokazati. □

Teorema 3.37 (Potpunost metoda tabloa za logiku prvog reda) *Ako je formula $\mathcal{A}$ valjana, onda se sistematski tablo za $F\mathcal{A}$ zatvara nakon konačnog broja koraka. Dakle, ako je formula $\mathcal{A}$ valjana, onda je ona dokaziva metodom tabloa, tj. postoji zatvoreni tablo za $F\mathcal{A}$.*

Dokaz: Pretpostavimo da je formula $\mathcal{A}$ valjana. Neka je $\mathcal{T}$ upotpunjeni sistematski tablo sa korenom $F\mathcal{A}$. Ako bi tablo $\mathcal{T}$ sadržao otvorenu granu θ, onda bi, na osnovu teoreme 3.36, grana θ bila zadovoljiva, pa bi i označena formula $F\mathcal{A}$ bila zadovoljiva (jer pripada grani θ), što je u suprotnosti sa pretpostavkom da je formula $\mathcal{A}$ valjana. Dakle, svaka grana tabloa $\mathcal{T}$ je zatvorena. Na osnovu Kenigove leme (3.35), zatvoreni beskonačan tablo je nemoguć (ako je tablo $\mathcal{T}$ zatvoren, onda je svaka grana tabloa $\mathcal{T}$ konačna), pa je tablo $\mathcal{T}$ konačan. Dakle, formula $\mathcal{A}$ je dokaziva metodom tabloa i to u konačnom broju koraka. □

Svaka grana generisana sistematskim metodom tabloa ima konačno ili prebrojivo mnogo čvorova. Svakim dodavanjem novog simbola konstante proširuje se tekuća signatura. Za jednu granu tabloa broj uvedenih simbola konstanti je najviše prebrojiv (jer grana ima najviše prebrojivo mnogo čvorova). Kako se tablo za zadovoljivu formulu ne može zatvoriti, on mora da sadrži neku otvorenu granu. Toj grani odgovara signatura sa najviše prebrojivo mnogo simbola konstanti. Skup formula na toj grani je zadovoljiv i on je tačan u modelu indukovanom skupom svih simbola konstanti kao domenom (slično kao kod Erbranovog modela). Taj model je najviše prebrojivog domena, pa odatle proizilazi tvrđenje teoreme 3.24 i njen opštiji oblik — Skolem-Lovenhajmova teorema za logiku prvog reda (teorema 3.25).

Zadaci

Zadatak 79 *Koristeći metod tabloa dokazati da važi $(\forall x)(p(x) \Rightarrow q(x)), p(c) \models q(c)$ valjana.*

Zadatak 80 *Primenom metoda tabloa dokazati da su sledeće formule valjane:*
(a) $(\forall y)((\forall x)p(x) \Rightarrow p(y))$
(b) $(\forall x)p(x) \Rightarrow (\exists x)p(x)$
(c) $(\exists y)(p(y) \Rightarrow (\forall x)p(x))$
(d) $\neg(\exists y)p(y) \Rightarrow (\forall y)((\exists x)p(x) \Rightarrow p(y))$
(e) $(\exists x)p(x) \Rightarrow (\exists y)p(y)$
(f) $(\forall x)(p(x) \wedge q(x)) \Leftrightarrow (\forall x)p(x) \wedge (\forall x)q(x)$
(g) $(\forall x)p(x) \vee (\forall x)q(x) \Rightarrow (\forall x)(p(x) \vee q(x))$
(h) $(\exists x)(p(x) \vee q(x)) \Leftrightarrow (\exists x)p(x) \vee (\exists x)q(x)$
(i) $(\exists x)(p(x) \wedge q(x)) \Rightarrow (\exists x)p(x) \wedge (\exists x)q(x)$

Zadatak 81 *Primenom metoda tabloa dokazati da su sledeće formule valjane (u svakoj od datih formula, $\mathcal{A}$ je zatvorena formula):*

(a) $(\forall x)(p(x) \vee \mathcal{A}) \Leftrightarrow ((\forall x)p(x) \vee \mathcal{A})$
(b) $(\exists x)(p(x) \wedge \mathcal{A}) \Leftrightarrow ((\exists x)p(x) \wedge \mathcal{A})$
(c) $(\exists x)\mathcal{A} \Leftrightarrow \mathcal{A}$
(d) $(\forall x)\mathcal{A} \Leftrightarrow \mathcal{A}$
(e) $(\exists x)(\mathcal{A} \Rightarrow p(x)) \Leftrightarrow (\mathcal{A} \Rightarrow (\exists x)p(x))$
(f) $(\exists x)(p(x) \Rightarrow \mathcal{A}) \Leftrightarrow ((\forall x)p(x) \Rightarrow \mathcal{A})$
(g) $(\forall x)(\mathcal{A} \Rightarrow p(x)) \Leftrightarrow (\mathcal{A} \Rightarrow (\forall x)p(x))$
(h) $(\forall x)(p(x) \Rightarrow \mathcal{A}) \Leftrightarrow ((\exists x)p(x) \Rightarrow \mathcal{A})$

Zadatak 82 *Metodom tabloa dokazati da je formula* $(H \wedge K) \Rightarrow L$ *valjana, gde je*

$H = (\forall x)(\forall y)(p(x, y) \Rightarrow p(y, x))$
$K = (\forall x)(\forall y)(\forall z)((p(x, y) \wedge p(y, z)) \Rightarrow p(x, z))$
$L = (\forall x)(\forall y)(p(x, y) \Rightarrow p(x, x))$.

Zadatak 83 *Metodom tabloa dokazati da je formula* $(A \wedge B) \Rightarrow C$ *valjana, gde je*

$A = (\forall x)((p(x) \wedge q(x)) \Rightarrow r(x)) \Rightarrow (\exists x)(p(x) \wedge \neg q(x))$
$B = (\forall x)(p(x) \Rightarrow q(x)) \vee (\forall x)(p(x) \Rightarrow r(x))$
$C = (\forall x)(p(x) \wedge r(x) \Rightarrow q(x)) \Rightarrow (\exists x)(p(x) \wedge q(x) \wedge \neg r(x))$.

Zadatak 84 *Za narednu formulu metodom tabloa dokazati da je valjana:*

$$(\forall x)(\mathcal{A}(x) \Rightarrow C) \Leftrightarrow ((\exists x)\mathcal{A}(x) \Rightarrow C) \ ,$$

gde je C *rečenica.*

Zadatak 85 *Metodom tabloa dokazati da je formula* $\forall x \forall y \ (x = y \Rightarrow y = x)$ *logička posledica formula* $\forall x \ (x = x)$ *i* $\forall u \forall v \forall w \ (u = v \wedge w = v \Rightarrow u = w)$.

Zadatak 86 *Prevesti na jezik logike prvog reda i dokazati metodom tabloa sledeće tvrđenje: Ako su svi političari lukavi i ako su samo pokvareni ljudi političari, onda, ako postoji ijedan političar, onda je neki pokvaren čovek lukav.*

3.3 Sistemi za dedukciju u logici prvog reda

Pojam valjanosti je semantičke prirode, a koncept dokazivanja i sistema za dedukciju vodi do pojma teoreme koji je sintaksno-deduktivne prirode. Kao što je teorija modela vezana za semantiku, tako su deduktivni sistemi i teorija dokaza vezani za sintaksu. Pojam *teoreme* je deduktivni pandan pojma *valjane formule*, koji je semantičke prirode. Između ova dva pojma postoji veza i deduktivni sistemi koji će biti opisani u nastavku imaju svojstvo potpunosti i saglasnosti: ako je neka formula valjana, onda ona može biti dokazana u okviru deduktivnog sistema, a ako za neku formulu postoji dokaz u okviru deduktivnog sistema, onda je ona sigurno valjana.

Sistemi za dedukciju za predikatsku logiku su čisto sintaksne prirode — primenjuju se kroz kombinovanje simbola, ne ulazeći u semantiku formula. Sisteme za dedukciju za predikatsku logiku zovemo i *predikatski račun*.

3.3.1 Hilbertov sistem

U okviru Hilbertovog sistema[3], koji zovemo i teorija K (videti analogni sistem za iskaznu logiku, poglavlje 2.3.1), jezik logike prvog reda definiše se nešto drugačije nego u poglavlju 3.1. Naime, osnovnim (ili primitivnim) logičkim veznicima zvaćemo samo veznike $\neg$ i $\Rightarrow$, osnovnim kvantifikatorom zvaćemo samo kvantifikator $\forall$, a ostale logičke veznike i kvantifikator $\exists$ definisaćemo i smatrati samo skraćenicama.

U definisanju jezika teorije K koriste se sledeći skupovi:

1. prebrojiv skup *promenljivih* V;
2. skup *logičkih veznika* $\{\neg, \Rightarrow\}$, pri čemu je $\neg$ unarni, a $\Rightarrow$ binarni veznik;
3. skup *kvantifikatora* $\{\forall\}$, pri čemu je $\forall$ univerzalni kvantifikator;
4. skup *pomoćnih simbola* $\{(,), ,\}$.

Termove, atomičke formule i dobro zasnovane formule definišemo za navedene skupove, analogno kao u poglavlju 3.1. U zapisu formula koristimo uobičajene konvencije za izostavljanje zagrada.

Kažemo da je term t *slobodan za* x u $\mathcal{A}$ ako nijedno slobodno pojavljivanje promenljive x nije u dosegu kvantifikatora takvog da t sadrži odgovarajuću kvantifikovanu promenljivu. Drugim rečima, kažemo da je term t slobodan za x u $\mathcal{A}$ ako nijedna promenljiva iz t ne postaje vezana u $\mathcal{A}[x \mapsto t]$.

Aksiome teorije K su sledeće sheme formula (gde su $\mathcal{A}$, $\mathcal{B}$ i $\mathcal{C}$ proizvoljne formule):

(A1) $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$

(A2) $(\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$

(A3) $(\neg\mathcal{B} \Rightarrow \neg\mathcal{A}) \Rightarrow ((\neg\mathcal{B} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{B})$

(A4) $(\forall x)\mathcal{A} \Rightarrow \mathcal{A}[x \mapsto t]$, pri čemu je term t slobodan za x u $\mathcal{A}$

(A5) $(\forall x)(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow (\forall x)\mathcal{B})$, pri čemu $\mathcal{A}$ ne sadrži slobodna pojavljivanja promenljive x.

Primetimo da u aksiomskoj shemi (A4) term t može da bude jednak x, što daje aksiomsku shemu $(\forall x)\mathcal{A} \Rightarrow \mathcal{A}$.

Prokomentarišimo smisao ograničenja u aksiomskim shemama (A4) i (A5). Ona mogu biti motivisana i objašnjena sa stanovišta semantike. Razmotrimo sledeći primer u vezi sa aksiomskom shemom (A4): neka je formula $\mathcal{A}$ jednaka $\neg(\forall y)p(x, y)$ i neka je term t jednak y. Primetimo da term t nije slobodan za x u $\mathcal{A}$. Formula

$$(\forall x)(\neg(\forall y)p(x, y)) \Rightarrow \neg(\forall y)p(y, y)$$

[3]Postoji više varijanti formalnih teorija koje opisuju logiku prvog reda i definisane su u tzv. Hilbertovom stilu. Mi ćemo se u ovom tekstu baviti samo jednom od njih.

je instanca aksiomske sheme (A4), ali nije valjana (ona nije tačna, na primer, u modelu čiji domen ima bar dva člana i u kojem predikatskom simbolu p odgovara relacija identičnosti). To nije željena primena sheme (A4) i zato je neophodno dodati date uslove.

Razmotrimo sledeći primer u vezi sa aksiomskom shemom (A5): neka su i formula $\mathcal{A}$ i formula $\mathcal{B}$ jednake $p(x)$. Dakle, promenljiva x je slobodna u $\mathcal{A}$. Formula

$$(\forall x)(p(x) \Rightarrow p(x)) \Rightarrow (p(x) \Rightarrow (\forall x)p(x))$$

je instanca aksiomske sheme (A5), ali nije valjana (ona nije tačna, na primer, u modelu u kojem je relacija p_I tačna za neke, ali ne za sve elemente domena). To nije željena primena sheme (A5) i zato je neophodno dodati date uslove.

Naglasimo da je aksiomskim shemama dât beskonačan skup aksioma. Ipak, za svaku formulu može se jednostavno proveriti (npr. primenom algoritma za jednosmernu unifikaciju) da li je ona aksioma teorije K. Skup aksioma teorije K je, dakle, rekurzivan, pa je ona aksiomatska teorija.

Pravila izvođenja teorije K su:

- *modus ponens* (koje kraće označavamo MP):

$$\frac{\mathcal{A} \quad \mathcal{A} \Rightarrow \mathcal{B}}{\mathcal{B}}\ MP$$

- *generalizacija* (koje kraće označavamo Gen):

$$\frac{\mathcal{A}}{(\forall x)\mathcal{A}}\ Gen$$

Pojmovi dokaza i teoreme, definišu se analogno kao u teoriji L (videti poglavlje 2.3.1).

Primer 3.39 *Važi* $\mathcal{A}, (\forall x)\mathcal{A} \Rightarrow \mathcal{C} \vdash (\forall x)\mathcal{C}$*:*

1.	$\mathcal{A}$	*(Hyp)*
2.	$(\forall x)\mathcal{A}$	*(1, Gen)*
3.	$(\forall x)\mathcal{A} \Rightarrow \mathcal{C}$	*(Hyp)*
4.	$\mathcal{C}$	*(2,3,MP)*
5.	$(\forall x)\mathcal{C}$	*(4,Gen)*

Sledećim definicijama uvodimo logičke veznike $\wedge$, $\vee$, $\Leftrightarrow$, kvantifikator $\exists$ i logičke konstante $\top$ i $\bot$:

(D1) $\mathcal{A} \wedge \mathcal{B}$ je kraći zapis za $\neg(\mathcal{A} \Rightarrow \neg\mathcal{B})$

(D2) $\mathcal{A} \vee \mathcal{B}$ je kraći zapis za $(\neg\mathcal{A}) \Rightarrow \mathcal{B}$

(D3) $\mathcal{A} \Leftrightarrow \mathcal{B}$ je kraći zapis za $(\mathcal{A} \Rightarrow \mathcal{B}) \wedge (\mathcal{B} \Rightarrow \mathcal{A})$

(D4) $(\exists x)\mathcal{A}$ je kraći zapis za $\neg(\forall x)(\neg\mathcal{A})$

(D5) $\top$ je kraći zapis za $\mathcal{A} \Rightarrow \mathcal{A}$, gde je $\mathcal{A}$ proizvoljna formula

(D6) $\bot$ je kraći zapis za $\neg(\mathcal{A} \Rightarrow \mathcal{A})$, gde je $\mathcal{A}$ proizvoljna formula.

Teorema 3.38 *Svaka tautologija prvog reda je teorema teorije K.*

Dokaz: Aksiome teorije K obuhvataju sve aksiome teorije L (tj. njima odgovarajuće sheme na jeziku logike prvog reda) i teorija K obuhvata sva pravila izvođenja (tj. jedino pravilo izvođenja — pravilo MP) teorije L. Na osnovu teoreme, 2.33 svaka tautologija je teorema teorije L. Njen dokaz u okviru teorije L može se jednostavno transformisati u dokaz odgovarajuće tautologije prvog reda u okviru teorije K. Dakle, svaka tautologija prvog reda je teorema teorije K. □

Zahvaljujući prethodnoj teoremi možemo, u cilju konstruisanja kraćih dokaza, koristiti sve tautologije prvog reda kao aksiome.

U daljem tekstu umesto $\vdash_K$ pisaćemo samo $\vdash$, podrazumevajući da se izvođenje odnosi na teoriju K.

Teorema 3.39 (Teorema o dedukciji) *Ako važi $\Gamma, \mathcal{A} \vdash \mathcal{B}$ i $\mathcal{A}$ je zatvorena formula, onda važi i $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$.*

Dokaz: Neka je $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n = \mathcal{B}$ dokaz formule $\mathcal{B}$ iz $\Gamma, \mathcal{A}$. Dokažimo indukcijom da važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ za svako i, $1 \leq i \leq n$.

Dokažimo da važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_1$. Formula $\mathcal{B}_1$ je ili aksioma ili pripada skupu Γ ili je jednaka formuli $\mathcal{A}$. Ako je $\mathcal{B}_1$ aksioma ili pripada skupu Γ, onda važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_1$ (što, primenom pravila MP, sledi iz $\Gamma \vdash \mathcal{B}_1$ i aksiome $\mathcal{B}_1 \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_1)$). Ako je formula $\mathcal{B}_1$ jednaka formuli $\mathcal{A}$, onda važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_1$ (jer je $\mathcal{A} \Rightarrow \mathcal{A}$ tautologija prvog reda pa, na osnovu teoreme 3.38, važi $\vdash \mathcal{A} \Rightarrow \mathcal{A}$, tj. $\vdash \mathcal{A} \Rightarrow \mathcal{B}_1$ i $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_1$).

Pretpostavimo da $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_l$ važi za svako l, $l < i$ i dokažimo da važi i za $l = i$:

- ako je $\mathcal{B}_i$ aksioma ili pripada skupu Γ, onda važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ (što, primenom pravila MP, sledi iz $\Gamma \vdash \mathcal{B}_i$ i aksiome $\mathcal{B}_i \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_i)$);
- ako je formula $\mathcal{B}_i$ jednaka formuli $\mathcal{A}$, onda važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ (jer je $\mathcal{A} \Rightarrow \mathcal{A}$ tautologija prvog reda pa, na osnovu teoreme 3.38, važi $\vdash \mathcal{A} \Rightarrow \mathcal{A}$, tj. $\vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ i $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$);
- ako je formula $\mathcal{B}_i$ dobijena primenom pravila MP iz neke formule $\mathcal{B}_j$ i formule $\mathcal{B}_k$ koja je oblika $\mathcal{B}_j \Rightarrow \mathcal{B}_i$, za neke vrednosti j i k takve da je $j < i$ i $k < i$, tada, na osnovu induktivne hipoteze, važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_j$ i $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_k$ (tj. važi $\Gamma \vdash \mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_i)$); formula $(\mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_i)) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_i))$ je instanca aksiomske sheme (A2), pa, na osnovu pravila MP, iz $\Gamma \vdash (\mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_i)) \Rightarrow ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow$

$(\mathcal{A} \Rightarrow \mathcal{B}_i))$ i $\Gamma \vdash \mathcal{A} \Rightarrow (\mathcal{B}_j \Rightarrow \mathcal{B}_i)$ sledi $\Gamma \vdash ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_i))$. Iz $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_j$ i $\Gamma \vdash ((\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B}_i))$, na osnovu pravila MP, sledi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$.

- ako je formula $\mathcal{B}_i$ oblika $(\forall x)\mathcal{B}_j$ i dobijena primenom pravila Gen iz neke formule $\mathcal{B}_j$ za neku vrednost j, $j < i$, tada na osnovu instance aksiomske sheme (A5) važi $\Gamma \vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow (\forall x)\mathcal{B}_j)$ (jer je formula $\mathcal{A}$ zatvorena, pa promenljiva x nema slobodna pojavljivanja u $\mathcal{A}$); na osnovu induktivne hipoteze važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_j$, a odatle, na osnovu pravila Gen, sledi $\Gamma \vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}_j)$. Iz $\Gamma \vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}_j) \Rightarrow (\mathcal{A} \Rightarrow (\forall x)\mathcal{B}_j)$ i $\Gamma \vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}_j)$ na osnovu pravila MP sledi $\Gamma \vdash \mathcal{A} \Rightarrow (\forall x)\mathcal{B}_j$, tj. $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$.

Dakle, važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_i$ za svako i, $1 \leq i \leq n$. Za $i = n$ važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}_n$, tj. $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$, što je i trebalo dokazati. □

Važi i obrat teoreme o dedukciji i to bez ograničenja za formulu $\mathcal{A}$.

Teorema 3.40 (Obrat teoreme o dedukciji) *Ako važi* $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$*, onda važi i* $\Gamma, \mathcal{A} \vdash \mathcal{B}$.

Dokaz: Ako važi $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$, onda važi i $\Gamma, \mathcal{A} \vdash \mathcal{A} \Rightarrow \mathcal{B}$, a iz $\Gamma, \mathcal{A} \vdash \mathcal{A}$ i $\Gamma, \mathcal{A} \vdash \mathcal{A} \Rightarrow \mathcal{B}$, na osnovu pravila MP, sledi $\Gamma, \mathcal{A} \vdash \mathcal{B}$. □

Primer 3.40 *Pretpostavimo da su* x *i* y *jedine dve slobodne promenljive formule* $\mathcal{A}$*. Formula* $(\forall x)(\forall y)\mathcal{A} \Rightarrow (\forall y)(\forall x)\mathcal{A}$ *je teorema teorije* K*. Dokažimo najpre da važi* $(\forall x)(\forall y)\mathcal{A} \vdash (\forall y)(\forall x)\mathcal{A}$*:*

1.	$(\forall x)(\forall y)\mathcal{A}$	*(Hyp)*
2.	$(\forall x)(\forall y)\mathcal{A} \Rightarrow (\forall y)\mathcal{A}$	*(A4)*
3.	$(\forall y)\mathcal{A}$	*(1,2,MP)*
4.	$(\forall y)\mathcal{A} \Rightarrow \mathcal{A}$	*(A4)*
5.	$\mathcal{A}$	*(3,4,MP)*
6.	$(\forall x)\mathcal{A}$	*(5,Gen)*
7.	$(\forall y)(\forall x)\mathcal{A}$	*(6,Gen)*

Iz $(\forall x)(\forall y)\mathcal{A} \vdash (\forall y)(\forall x)\mathcal{A}$*, na osnovu teoreme o dedukciji (formula* $(\forall x)(\forall y)\mathcal{A}$ *je zatvorena), sledi* $\vdash (\forall x)(\forall y)\mathcal{A} \Rightarrow (\forall y)(\forall x)\mathcal{A}$.

Naglasimo da se u teoremi o dedukciji (3.39) ne može izostaviti uslov da je formula $\mathcal{A}$ zatvorena: na primer, važi $p(x) \vdash (\forall x)p(x)$, ali $p(x) \Rightarrow (\forall x)p(x)$ nije teorema. Ipak, uslov da je formula $\mathcal{A}$ zatvorena može biti oslabljen. Navedimo bez dokaza i jednu jaču varijantu teoreme o dedukciji.

Teorema 3.41 *Ako postoji dokaz za* $\Gamma, \mathcal{A} \vdash \mathcal{B}$ *u kojem se ne koristi pravilo Gen čija promenljiva je slobodna u* $\mathcal{A}$*, onda važi i* $\Gamma \vdash \mathcal{A} \Rightarrow \mathcal{B}$.

Teorema 3.42 (Pravilo A) *Ako je term t slobodan za x u $\mathcal{A}$, onda važi $(\forall x)\mathcal{A} \vdash \mathcal{A}[x \mapsto t]$. Specijalno, ako je term t jednak x, onda važi $(\forall x)\mathcal{A} \vdash \mathcal{A}$.*

Dokaz:

1.	$(\forall x)\mathcal{A}$	(Hyp)
2.	$(\forall x)\mathcal{A} \Rightarrow \mathcal{A}[x \mapsto t]$	(A4)
3.	$\mathcal{A}[x \mapsto t]$	(1,2,MP)

Dakle, važi $(\forall x)\mathcal{A} \vdash \mathcal{A}[x \mapsto t]$. □

Primer 3.41 *Može se dokazati da, ako je x jedina slobodna promenljiva u formulama $\mathcal{A}$ i $\mathcal{B}$, onda važi $\vdash (\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \Rightarrow ((\forall x)\mathcal{A} \Leftrightarrow (\forall x)\mathcal{B})$.*

Dokažimo najpre da važi $(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}), (\forall x)\mathcal{A} \vdash (\forall x)\mathcal{B}$:

1.	$(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B})$	*(Hyp)*
2.	$(\forall x)\mathcal{A}$	*(Hyp)*
3.	$\mathcal{A} \Leftrightarrow \mathcal{B}$	*(1, pravilo A)*
4.	$\mathcal{A}$	*(2, pravilo A)*
5.	$(\mathcal{A} \Leftrightarrow \mathcal{B}) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$	*(tautologija $(A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$)*
6.	$\mathcal{A} \Rightarrow \mathcal{B}$	*(3,5,MP)*
7.	$\mathcal{B}$	*(4,6,MP)*
8.	$(\forall x)\mathcal{B}$	*(7, Gen)*

Dakle, važi $(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}), (\forall x)\mathcal{A} \vdash (\forall x)\mathcal{B}$, pa, na osnovu teoreme o dedukciji važi $(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \vdash (\forall x)\mathcal{A} \Rightarrow (\forall x)\mathcal{B}$.

Analogno se dokazuje $(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \vdash (\forall x)\mathcal{B} \Rightarrow (\forall x)\mathcal{A}$.

Može se dokazati da iz $\mathcal{C} \vdash \mathcal{D}_1$ i $\mathcal{C} \vdash \mathcal{D}_2$ sledi $\mathcal{C} \vdash \mathcal{D}_1 \wedge \mathcal{D}_2$, pa važi
$(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \vdash ((\forall x)\mathcal{A} \Rightarrow (\forall x)\mathcal{B}) \wedge ((\forall x)\mathcal{B} \Rightarrow (\forall x)\mathcal{A})$,
odakle, na osnovu definicije (D3), sledi
$(\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \vdash (\forall x)\mathcal{A} \Leftrightarrow (\forall x)\mathcal{B}$.

Konačno, na osnovu teoreme o dedukciji (teorema 3.39), sledi
$\vdash (\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \Rightarrow ((\forall x)\mathcal{A} \Leftrightarrow (\forall x)\mathcal{B})$.

Može se dokazati da $\vdash (\forall x)(\mathcal{A} \Leftrightarrow \mathcal{B}) \Rightarrow ((\forall x)\mathcal{A} \Leftrightarrow (\forall x)\mathcal{B})$ važi i za proizvoljne formule $\mathcal{A}$ i $\mathcal{B}$. To se može dokazati korišćenjem teoreme 3.41 umesto teoreme o dedukciji (3.39).

Teorema 3.43 (Pravilo E) *Ako je term t slobodan za x u $\mathcal{A}$, onda važi $\vdash \mathcal{A}[x \mapsto t] \Rightarrow (\exists x)\mathcal{A}$ i $\mathcal{A}[x \mapsto t] \vdash (\exists x)\mathcal{A}$.*

Dokaz:

1.	$(\forall x)\neg\mathcal{A} \Rightarrow \neg\mathcal{A}[x \mapsto t]$	(A4)
2.	$((\forall x)\neg\mathcal{A} \Rightarrow \neg\mathcal{A}[x \mapsto t]) \Rightarrow$ $(\mathcal{A}[x \mapsto t] \Rightarrow \neg(\forall x)\neg\mathcal{A})$	(tautologija $(A \Rightarrow \neg B) \Rightarrow (B \Rightarrow \neg A)$)
3.	$\mathcal{A}[x \mapsto t] \Rightarrow \neg(\forall x)\neg\mathcal{A}$	(1,2,MP)
4.	$\mathcal{A}[x \mapsto t] \Rightarrow (\exists x)\mathcal{A}$	(3,D4)

Iz $\vdash \mathcal{A}[x \mapsto t] \Rightarrow (\exists x)\mathcal{A}$, na osnovu obrata teoreme o dedukciji, sledi $\mathcal{A}[x \mapsto t] \vdash (\exists x)\mathcal{A}$. □

Primer 3.42 (Pravilo C) *U matematičkim dokazima uobičajeno je sledeće rasuđivanje: pretpostavimo da smo dokazali formulu oblika* $(\exists x)\mathcal{A}(x)$*, onda kažemo neka je* c *objekat takav da važi* $\mathcal{A}(c)$*; nastavljamo dokaz i, konačno, dolazimo do tražene formule koja ne sadrži element* c*. Na primer, dokažimo da važi* $(\exists x)(\mathcal{B}(x) \Rightarrow \mathcal{C}(x)), (\forall x)\mathcal{B}(x) \vdash (\exists x)\mathcal{C}(x)$*:*

1.	$(\exists x)(\mathcal{B}(x) \Rightarrow \mathcal{C}(x))$	*(Hyp)*
2.	$(\forall x)\mathcal{B}(x)$	*(Hyp)*
3.	$\mathcal{B}[x \mapsto c] \Rightarrow \mathcal{C}[x \mapsto c]$ *za neko* c	*(1)*
4.	$\mathcal{B}[x \mapsto c]$	*(2, pravilo* **A***)*
5.	$\mathcal{C}[x \mapsto c]$	*(3,4, MP)*
6.	$(\exists x)\mathcal{C}(x)$	*(5, pravilo* **E***)*

Dakle, važi $(\exists x)(\mathcal{B}(x) \Rightarrow \mathcal{C}(x)), (\forall x)\mathcal{B}(x) \vdash (\exists x)\mathcal{C}(x)$*.*

Pravilo primenjeno u trećem koraku dokaza zvaćemo pravilo **C** *(***C** *dolazi od engleskog* choice*). Svaki dokaz koji može biti izveden uz korišćenje pravila* **C***, može biti transformisan u dokaz bez njegovog korišćenja (što opravdava njegovu upotrebu). U dokazima u kojima se koristi pravilo* **C***, pravilo Gen ne sme da se koristi nad promenljivom koja je slobodna u nekoj formuli* $(\exists x)\mathcal{C}$ *na koju je primenjeno pravilo* **C***.*

Teorema 3.44 (Saglasnost teorije K**)** *Ako je formula* $\mathcal{A}$ *teorema teorije* K*, onda je formula* $\mathcal{A}$ *valjana.*

Dokaz: Nije teško pokazati (na osnovu definicije semantike logike prvog reda) da je svaka instanca svake od aksioma teorije K valjana formula. Na osnovu teorema 3.2 i 3.4 iz valjanih formula se, primenom pravila MP i Gen dobijaju ponovo valjane formule. Dakle, svaka teorema teorije K je valjana formula. □

Teorema 3.45 (Konzistentnost teorije K**)** *Teorija* K *je konzistentna (neprotivrečna), tj. ne postoji formula* $\mathcal{A}$ *takva da su i* $\mathcal{A}$ *i* $\neg\mathcal{A}$ *teoreme teorije* K*.*

Dokaz: Pretpostavimo suprotno — pretpostavimo da postoji formula $\mathcal{A}$ takva da su i $\mathcal{A}$ i $\neg\mathcal{A}$ teoreme teorije K. Na osnovu teoreme 3.44, i formula $\mathcal{A}$ i formula $\neg\mathcal{A}$ su valjane, što je nemoguće (na osnovu definicije semantike logike prvog reda). Dakle, polazna pretpostavka je bila pogrešna, pa je teorija K konzistentna. □

Teorema 3.46 (Potpunost teorije K**)** *Ako je formula* $\mathcal{A}$ *valjana, onda je ona teorema teorije* K*.*

Dokaz: Dovoljno je razmatrati zatvorene formule jer za svaku formulu Φ važi da je valjana ako i samo ako je valjana formula $\forall * \Phi$ i važi da je teorema teorije K ako i samo ako je formula $\forall * \Phi$ teorema teorije K.

Neka je formula $\mathcal{A}$ zatvorena i valjana. Suprotno tvrđenju teoreme, pretpostavimo da formula $\mathcal{A}$ nije teorema teorije K. Neka je K' teorija dobijena dodavanjem formule $\neg\mathcal{A}$ kao aksiome teoriji K. Dokažimo da je teorija K' konzistentna.

Pretpostavimo da teorija K' nije konzistentna. Tada postoji formula $\mathcal{B}$ takva da važi $\vdash_{K'} \mathcal{B}$ i $\vdash_{K'} \neg\mathcal{B}$. Formula $\mathcal{B} \Rightarrow (\neg\mathcal{B} \Rightarrow \mathcal{A})$ je tautologija prvog reda i ona je teorema teorije K' (na osnovu teoreme 3.38 i jer u teoriji K' mogu da se dokažu sve teoreme teorije K). Iz $\vdash_{K'} \mathcal{B}$, $\vdash_{K'} \neg\mathcal{B}$ i $\vdash_{K'} \mathcal{B} \Rightarrow (\neg\mathcal{B} \Rightarrow \mathcal{A})$ dvostrukom primenom pravila MP dobija se $\vdash_{K'} \mathcal{A}$. Teorija K' izgrađena je tako što je teoriji K dodata kao aksioma formula $\neg\mathcal{A}$, pa iz $\vdash_{K'} \mathcal{A}$ sledi $\neg\mathcal{A} \vdash_K \mathcal{A}$. Na osnovu teoreme 3.39, sledi $\vdash_K \neg\mathcal{A} \Rightarrow \mathcal{A}$. Formula $(\neg\mathcal{A} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A}$ je tautologija prvog reda, te je ona teorema teorije K (na osnovu teoreme 3.38). Iz $\vdash_K \neg\mathcal{A} \Rightarrow \mathcal{A}$ i $\vdash_K (\neg\mathcal{A} \Rightarrow \mathcal{A}) \Rightarrow \mathcal{A}$ primenom pravila MP dobija se $\vdash_K \mathcal{A}$, što protivreči pretpostavci da formula $\mathcal{A}$ nije teorema teorije K. Dakle, teorija K' jeste konzistentna.

Teorija K' je konzistentna, pa ima model $\mathfrak{D}$ (videti teoremu 3.52). Kako je formula $\neg\mathcal{A}$ aksioma teorije K', ona je valjana u $\mathfrak{D}$ (videti definiciju 3.30). S druge strane, kako je formula $\mathcal{A}$ valjana, ona je valjana i u $\mathfrak{D}$. Međutim, nemoguće je da su i $\neg\mathcal{A}$ i $\mathcal{A}$ istovremeno valjane u $\mathfrak{D}$. Dakle, polazna pretpostavka je bila pogrešna, te sledi da je formula $\mathcal{A}$ teorema teorije K. □

Bez dokaza navodimo naredno tvrđenje (dokaz videti, na primer, u [48] ili [14]).

Teorema 3.47 (Neodlučivost teorije K) *Teorija K je neodlučiva.*

Više o teoremama 3.46 i 3.47 videti u poglavlju B.1.5.

Zadaci

Zadatak 87 *Dokazati da, ako je u formulama $\mathcal{A}$ i $\mathcal{B}$ promenljiva x jedina slobodna promenljiva, važi:*
(a) $\vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\forall x)\mathcal{A} \Rightarrow (\forall x)\mathcal{B})$
(b) $\vdash (\forall x)(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\exists x)\mathcal{A} \Rightarrow (\exists x)\mathcal{B})$
(c) $\vdash (\forall x)(\mathcal{A} \wedge \mathcal{B}) \Rightarrow ((\forall x)\mathcal{A} \wedge (\forall x)\mathcal{B})$

Zadatak 88 *Dokazati da važi* $\vdash ((\forall x)\mathcal{A} \Leftrightarrow \neg(\exists x)\neg\mathcal{A})$.

Zadatak 89 *Neka formula $\mathcal{A}$ sadrži kvantifikatore i veznike $\wedge$, $\vee$ i $\neg$, ali ne i veznike $\Rightarrow$, $\Leftrightarrow$. Ako u formuli $\mathcal{A}$ zamenimo univerzalne kvantifikatore egzistencijalnim i obratno, ako zamenimo veznike $\wedge$ veznicima $\vee$ i obratno, i ako*

svakom literalu dodamo veznik negacije, dobijeni rezultat zovemo dualnom formulom *za formulu $\mathcal{A}$ i označavamo sa $\mathcal{A}^*$. Dokazati da važi:*

(a) $\vdash \mathcal{A}$ *ako i samo ako* $\vdash \neg\mathcal{A}^*$

(b) $\vdash \mathcal{A} \Rightarrow \mathcal{B}$ *ako i samo ako* $\vdash \mathcal{B}^* \Rightarrow \mathcal{A}^*$

(c) $\vdash \mathcal{A} \Leftrightarrow \mathcal{B}$ *ako i samo ako* $\vdash \mathcal{A}^* \Leftrightarrow \mathcal{B}^*$

3.3.2 Prirodna dedukcija

Sistem prirodne dedukcije uveo je Gerhard Gencen, 1935. godine [21]. Sistem prirodne dedukcije za logiku prvog reda analogan je sistemu prirodne dedukcije za iskaznu logiku (videti poglavlje 2.3.2).

Postoji sistem prirodne dedukcije za klasičnu logiku (koji zovemo sistem NK) i sistem prirodne dedukcije za intuicionističku logiku (koji zovemo sistem NJ). Kao i u iskaznom slučaju, sistem prirodne dedukcije za klasičnu logiku ima jednu aksiomsku shemu — $\mathcal{A} \vee \neg\mathcal{A}$ (isključenje trećeg, *tertium non datur*), dok sistem za intuicionističku logiku nema aksioma. I za klasičnu i za intuicionističku logiku, sistem prirodne dedukcije za logiku prvog reda ima pravila izvođenja analogna pravilima izvođenja za iskaznu logiku, kao i pravila za uvođenje i eliminisanje kvantifikatora prikazana u tabeli 3.1.

$$\frac{\mathcal{A}[x \mapsto y]}{(\forall x)\mathcal{A}}\ \forall I \qquad \frac{(\forall x)\mathcal{A}}{\mathcal{A}[x \mapsto t]}\ \forall E$$

uz dodatni uslov

$$\frac{\mathcal{A}[x \mapsto t]}{(\exists x)\mathcal{A}}\ \exists I \qquad \frac{(\exists x)\mathcal{A} \qquad \begin{array}{c}[\mathcal{A}[x \mapsto y]]^u \\ \vdots \\ \mathcal{B}\end{array}}{\mathcal{B}}\ \exists E, u$$

uz dodatni uslov

Tabela 3.1: Pravila za uvođenje i eliminisanje kvantifikatora

U pravilima izvođenja prikazanim u tabeli 3.1 simbol t označava proizvoljan term. Simbol y označava tzv. eigenvariable (*pravu promenljivu*) — simbol promenljive za koju važi tzv. *eigenvariable uslov*. Ovaj uslov za pravilo $\forall I$ je da važi da je $x = y$ ili da promenljiva y nije slobodna u $\mathcal{A}$, kao i da važi da y nije slobodna ni u jednoj neoslobođenoj pretpostavci u izvođenju formule $\mathcal{A}[x \mapsto y]$. Eigenvariable uslov za pravilo $\exists E$ je da važi da je $x = y$ ili da promenljiva y nije slobodna u $\mathcal{A}$, kao i da važi da y nije slobodna u $\mathcal{B}$ niti u bilo kojoj neoslobođenoj pretpostavci u izvođenju formule $\mathcal{B}$ osim, eventualno, u formuli $\mathcal{A}[x \mapsto y]$.

Pojmovi dokaza i teoreme, definišu se analogno iskaznom slučaju (videti poglavlje 2.3.2).

Primer 3.43 *Formula* $(\exists x)(\forall y)p(x,y) \Rightarrow (\forall y)(\exists x)p(x,y)$ *je teorema sistema prirodne dedukcije (i za klasičnu i za intuicionističku logiku). Neki matematičar bi ovu formulu (neformalno) dokazao na sledeći način:*

1. *Pretpostavimo da važi* $(\exists x)(\forall y)p(x,y)$.
2. *Pretpostavimo da važi* $(\forall y)p(x',y)$ *za neko* x'.
3. *Neka je* y' *proizvoljni objekat. Tada važi* $p(x',y')$.
4. *Iz* $p(x',y')$ *sledi da važi* $(\exists x)p(x,y')$.
5. *Objekat* y' *je proizvoljan, pa važi* $(\forall y)(\exists x)p(x,y)$.
6. *Iz* $(\exists x)(\forall y)p(x,y)$ *i iz toga što pretpostavka* $(\forall y)p(x',y)$ *ima za posledicu* $(\forall y)(\exists x)\ p(x,y)$*, sledi* $(\forall y)(\exists x)p(x,y)$.
7. *Iz pretpostavke* $(\exists x)(\forall y)p(x,y)$ *sledi* $(\forall y)(\exists x)p(x,y)$*, pa važi* $(\exists x)(\forall y)\ p(x,y) \Rightarrow (\forall y)(\exists x)p(x,y)$.

Ovaj dokaz može se precizno opisati u vidu dokaza u sistemu prirodne dedukcije (i za klasičnu i za intuicionističku logiku):

$$\dfrac{\dfrac{\dfrac{\dfrac{[(\forall y)p(x',y)]^1}{p(x',y')}\,\forall E}{(\exists x)p(x,y')}\,\exists I}{(\forall y)(\exists x)p(x,y)}\,\forall I \qquad [(\exists x)(\forall y)p(x,y)]^2}{(\forall y)(\exists x)p(x,y)}\,\exists E,1}{(\exists x)(\forall y)p(x,y) \Rightarrow (\forall y)(\exists x)p(x,y)}\,\Rightarrow I,2$$

Primer 3.44 *Formula* $\neg(\exists x)p(x) \Rightarrow (\forall y)\neg p(y)$ *je teorema sistema prirodne dedukcije (i za klasičnu i za intuicionističku logiku):*

$$\dfrac{\dfrac{\dfrac{\dfrac{[p(z)]^1}{(\exists x)p(x)}\,\exists I \qquad [\neg(\exists x)p(x)]^2}{\bot}\,\neg E}{\neg p(z)}\,\neg I,1}{(\forall y)\neg p(y)}\,\forall I}{\neg(\exists x)p(x) \Rightarrow (\forall y)\neg p(y)}\,\Rightarrow I,2$$

Primer 3.45 *U sistemu prirodne dedukcije važi* $\forall x\mathcal{A}, \forall x(\mathcal{A} \Rightarrow \mathcal{B}) \vdash \forall x\mathcal{B}$*:*

$$\dfrac{\dfrac{\dfrac{\forall x\mathcal{A}}{\mathcal{A}}\,\forall E \qquad \dfrac{\forall x(\mathcal{A} \Rightarrow \mathcal{B})}{\mathcal{A} \Rightarrow \mathcal{B}}\,\forall E}{\mathcal{B}}\,\Rightarrow E}{\forall x\mathcal{B}}\,\forall I$$

Naredna teorema o ekvivalentnosti teorije K i sistema prirodne dedukcije za klasičnu logiku dokazuje se slično kao u iskaznom slučaju.

Teorema 3.48 *Formula logike prvog reda je teorema sistema prirodne dedukcije za klasičnu logiku ako i samo ako je ona teorema teorije* K.

3.3.3 Račun sekvenata

Račun sekvenata uveo je Gerhard Gencen 1935. godine. Račun sekvenata za logiku prvog reda analogan je računu sekvenata za iskaznu logiku (videti poglavlje 2.3.3).

Postoji račun sekvenata za klasičnu logiku (koji zovemo račun LK) i račun sekvenata za intuicionističku logiku (koji zovemo račun LJ). Račun sekvenata za intuicionističku logiku odlikuje se time što se u njoj koriste samo sekventi oblika $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \vdash \mathcal{B}$ ili oblika $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \vdash$.

Kao i u iskaznom slučaju, i u računu za klasičnu i u računu za intuicionističku logiku, postoji samo jedna aksiomska shema — $\mathcal{A} \vdash \mathcal{A}$ (id). I za klasičnu i za intuicionističku logiku, račun sekvenata za logiku prvog reda ima pravila izvođenja analogna pravilima izvođenja za iskaznu logiku, kao i pravila za uvođenje kvantifikatora sa leve i desne strane, prikazana u tabeli 3.2.

$\forall$-uvođenja	$\dfrac{\mathcal{A}[x \mapsto t], \Gamma \vdash \Theta}{(\forall x)\mathcal{A}, \Gamma \vdash \Theta}\ \forall L$	$\dfrac{\Gamma \vdash \Theta, \mathcal{A}[x \mapsto y]}{\Gamma \vdash \Theta, (\forall x)\mathcal{A}}\ \forall R$ uz dodatni uslov
$\exists$-uvođenja	$\dfrac{\mathcal{A}[x \mapsto y], \Gamma \vdash \Theta}{(\exists x)\mathcal{A}, \Gamma \vdash \Theta}\ \exists L$ uz dodatni uslov	$\dfrac{\Gamma \vdash \Theta, \mathcal{A}[x \mapsto t]}{\Gamma \vdash \Theta, (\exists x)\mathcal{A}}\ \exists R$

Tabela 3.2: Pravila za uvođenje kvantifikatora

U pravilima prikazanim u tabeli 3.2 simbol t označava proizvoljan term. Simbol y označava tzv. eigenvariable (*pravu promenljivu*) — simbol promenljive za koju važi tzv. *eigenvariable uslov*. Taj uslov u pravilu $\forall R$ je da promenljiva y nije slobodna u formulama Γ, Θ, $(\forall x)\mathcal{A}$. Taj uslov u pravilu $\exists L$ je da promenljiva y nije slobodna u formulama Γ, Θ, $(\exists x)\mathcal{A}$.

Pojmovi dokaza i teoreme, definišu se analogno iskaznom slučaju (videti poglavlje 2.3.3).

Kao i u iskaznom slučaju, račun sekvenata je potpun i bez *cut* pravila. U računu sekvenata bez *cut* pravila važi *svojstvo potformule*.

Primer 3.46 *Formula* $\neg(\exists x)p(x) \Rightarrow (\forall y)\neg p(y)$ *je teorema računa sekvenata (i za klasičnu i za intuicionističku logiku):*

$$\dfrac{\dfrac{\dfrac{\dfrac{p(z) \vdash p(z)}{p(z) \vdash (\exists x)p(x)}\ \exists R \quad \dfrac{\dfrac{(\exists x)p(x) \vdash (\exists x)p(x)}{\neg(\exists x)p(x), (\exists x)p(x) \vdash}\ \neg L}{(\exists x)p(x), \neg(\exists x)p(x) \vdash}\ \textit{zamena}}{p(z), \neg(\exists x)p(x) \vdash}\ \textit{sečenje}}{\neg(\exists x)p(x) \vdash \neg p(z)}\ \neg R}{\neg(\exists x)p(x) \vdash (\forall y)\neg p(y)}\ \forall R}{\vdash \neg(\exists x)p(x) \Rightarrow (\forall y)\neg p(y)}\ \Rightarrow R$$

Istu formulu moguće je, naravno, dokazati i bez korišćenja cut *pravila:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(z) \vdash p(z)}{p(z) \vdash (\exists x)p(x)}\ \exists R}{\neg(\exists x)p(x), p(z) \vdash}\ \neg L}{p(z), \neg(\exists x)p(x) \vdash}\ zamena}{\neg(\exists x)p(x) \vdash \neg p(z)}\ \neg R}{\neg(\exists x)p(x) \vdash (\forall y)\neg p(y)}\ \forall R}{\vdash \neg(\exists x)p(x) \Rightarrow (\forall y)\neg p(y)}\ \Rightarrow R$$

Naredna teorema o ekvivalentnosti teorije K i računa sekvenata za klasičnu logiku dokazuje se slično kao u iskaznom slučaju.

Teorema 3.49 *Formula logike prvog reda je teorema računa sekvenata za klasičnu logiku ako i samo ako je ona teorema teorije K.*

3.4 Teorije prvog reda

Logika prvog reda je dovoljno izražajna da u okviru nje mogu da se opišu raznovrsne teorije.

Definicija 3.29 Teorija prvog reda $\mathcal{T}$ *zadata je signaturom $\mathcal{L}$, aksiomama (odnosno aksiomskim shemama) $\mathcal{A}_1, \mathcal{A}_2, \ldots$ nad tom signaturom i sistemom D za dedukciju u logici prvog reda. Formula* Φ *je* teorema teorije $\mathcal{T}$ *ako važi*

$$\mathcal{A}_1, \mathcal{A}_2, \ldots \vdash_D \Phi\ .$$

Tada pišemo i:

$$\mathcal{T} \vdash \Phi$$

ili

$$\vdash_{\mathcal{T}} \Phi$$

ili, ako je iz konteksta jasno o kojoj teoriji je reč:

$$\vdash \Phi\ .$$

*Ukoliko je u teoriji $\mathcal{T}$ iz skupa formula (*hipoteza*) Γ moguće izvesti formulu Φ, onda to zapisujemo*

$$\Gamma \vdash \Phi\ .$$

Teorija može da se razmatra u okviru teorije K ili u okviru nekog drugog sistema za dedukciju. Ako se teorija prvog reda razmatra u okviru teorije K, onda se njene aksiome dodaju skupu aksiomskih shema teorije K i jedina pravila izvođenja koja se koriste su pravila izvođenja teorije K (MP i Gen). Slično se teorija prvog reda opisuje u okviru nekog drugog sistema za dedukciju, na primer, u okviru sistema za prirodnu dedukciju ili u okviru računa sekvenata.

Ponekad se pod *teorijom* podrazumeva skup svih njenih teorema.

Definicija 3.30 *Neka je $\mathcal{T}$ teorija prvog reda nad signaturom $\mathcal{L}$. Za $\mathcal{L}$-strukturu $\mathfrak{D}$ kažemo da je* model *teorije $\mathcal{T}$ ako je svaka aksioma teorije $\mathcal{T}$ valjana u $\mathfrak{D}$.*

Teorema 3.50 *Neka je teorija $\mathcal{T}$ opisana u okviru teorije K. Ako je formula $\mathcal{A}$ teorema teorije $\mathcal{T}$, onda je ona valjana u svakom modelu $\mathfrak{D}$ teorije $\mathcal{T}$ (tj. ona je logička posledica skupa aksioma teorije $\mathcal{T}$).*

Dokaz: Neka je $\mathfrak{D}$ proizvoljan model teorije $\mathcal{T}$. Ako je formula $\mathcal{A}$ teorema teorije $\mathcal{T}$, onda postoji niz formula $\mathcal{B}_1$, $\mathcal{B}_2$, ..., $\mathcal{B}_n = \mathcal{A}$ takav da je svaka od formula $\mathcal{B}_i$ ili aksioma teorije K, ili aksioma teorije $\mathcal{T}$ ili je dobijena od nekih formula u nizu primenom nekog pravila izvođenja teorije K. Aksiome teorije K su valjane formule, a aksiome teorije $\mathcal{T}$ valjane su u svakom modelu teorije $\mathcal{T}$. Primenom pravila izvođenja teorije K (MP i Gen) iz formula koje su valjane u $\mathfrak{D}$ dobijaju se formule koje su takođe valjane u $\mathfrak{D}$. Dakle, indukcijom se jednostavno dokazuje da je formula $\mathcal{B}_i$ ($i = 1, 2, \ldots, n$) valjana u $\mathfrak{D}$, pa je i formula $\mathcal{A}$ valjana u $\mathfrak{D}$. Model $\mathfrak{D}$ je proizvoljan, pa sledi da je formula $\mathcal{A}$ valjana u svakom modelu teorije $\mathcal{T}$, tj. formula $\mathcal{A}$ je logička posledica skupa aksioma teorije $\mathcal{T}$. □

Iz svojstva potpunosti teorije K sledi naredno tvrđenje — obrat navedene teoreme.

Teorema 3.51 *Neka je teorija $\mathcal{T}$ opisana u okviru teorije K. Ako je formula $\mathcal{A}$ valjana u svakom modelu $\mathfrak{D}$ teorije $\mathcal{T}$ (tj. ona je logička posledica skupa aksioma teorije $\mathcal{T}$), onda je ona teorema teorije $\mathcal{T}$.*

Za teoriju $\mathcal{T}$ nad signaturom $\mathcal{L}$ kažemo da je *neprotivrečna* (*konzistentna)* ako ne postoji formula $\mathcal{A}$ nad signaturom $\mathcal{L}$ takva da važi $\mathcal{T} \vdash \mathcal{A}$ i $\mathcal{T} \vdash \neg\mathcal{A}$.

Bez dokaza navodimo narednu teoremu koja predstavlja još jednu vezu između deduktivnih i semantičkih svojstava teorije (dokaz videti, na primer, u [48]).

Teorema 3.52 *Neka je teorija $\mathcal{T}$ opisana u okviru teorije K. Ako je teorija $\mathcal{T}$ konzistentna, onda ona ima model (štaviše, onda ona ima model sa najviše prebrojivim domenom).*

Teorija prvog reda može se zasnovati i semantički. Za datu signaturu $\mathcal{L}$ i datu $\mathcal{L}$-strukturu $\mathcal{D}$, *teorija strukture* $\mathcal{D}$ je skup svih rečenica nad signaturom $\mathcal{L}$ koje su valjane u $\mathcal{D}$. U daljem tekstu neće se koristiti ovaj vid zasnivanja teorija.

Teorija nad signaturom koja sadrži prebrojivo mnogo funkcijskih i predikatskih simbola (za arnosti $0, 1, 2, \ldots$) i koja nema drugih aksioma sem aksioma teorije K je primer teorije prvog reda (tu teoriju zovemo *čist predikatski račun*). Čist predikatski račun je, očito, neodlučiva teorija.

U nastavku će, kao primeri teorija prvog reda, ukratko biti opisane čista teorija jednakosti, teorija grupa, kao i teorija gustih uređenih Abelovih grupa bez krajnjih tačaka.

3.4.1 Čista teorija jednakosti

Signaturu čiste teorije jednakosti čini bilo koja signatura koja uključuje predikatski simbol arnosti 2 koji zapisujemo kao simbol $=$ i to u infiksnoj notaciji[4]. Aksiome čiste teorije jednakosti su:

E1 $(\forall x)(x = x)$

E2 $(\forall x_1)(\forall x_2)\ldots(\forall x_n)(\forall y_1)(\forall y_2)\ldots(\forall y_n)(x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n))$, za svaki funkcijski simbol f arnosti n.

E3 $(\forall x_1)(\forall x_2)\ldots(\forall x_n)(\forall y_1)(\forall y_2)\ldots(\forall y_n)(x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n \Rightarrow (p(x_1, x_2, \ldots, x_n) \Rightarrow p(y_1, y_2, \ldots, y_n)))$, za svaki predikatski simbol p arnosti n.

Primer 3.47 *U čistoj teoriji jednakosti naredna formula je teorema:*

$$(\forall x)(\forall y)(x = y \Rightarrow y = x)\ .$$

Dokažimo, najpre, u okviru teorije K, da važi $x = y \vdash y = x$.

1.	$x = y$	*(Hyp)*
2.	$(\forall x)(x = x)$	*(E1)*
3.	$x = x$	*(2, pravilo A)*
4.	$(\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)(x_1 = y_1 \wedge x_2 = y_2 \Rightarrow (x_1 = x_2 \Rightarrow y_1 = y_2))$	*(E3)*
5.	$x = y \wedge x = x \Rightarrow (x = x \Rightarrow y = x)$	*(4, 4 × A, $[x_1 \mapsto x, y_1 \mapsto y, x_2 \mapsto x, y_2 \mapsto x]$)*
6.	$x = y \wedge x = x$	*(1, 3, $\mathcal{A}, \mathcal{B} \vdash \mathcal{A} \wedge \mathcal{B}$)*
7.	$x = x \Rightarrow y = x$	*(5,6,MP)*
8.	$y = x$	*(3,7,MP)*

(Sa „4 × A“ je označena četvorostruka primena pravila A.)

Dakle, važi $x = y \vdash y = x$. Na osnovu teoreme 3.41 sledi $\vdash x = y \Rightarrow y = x$ i, na osnovu (dvostruke) primene pravila Gen, sledi $\vdash (\forall x)(\forall y)(x = y \Rightarrow y = x)$.

Primer 3.48 *U čistoj teoriji jednakosti naredna formula je teorema:*

$$(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow x = z)\ .$$

Dokažimo, najpre, u okviru teorije K, da važi $x = y, y = z \vdash x = z$.

[4] Treba praviti razliku između predikatskog simbola $=$ teorije jednakosti i simbola $=$ koji na metanivou koristimo za označavanje sintaksne jednakosti formula. Iz konteksta treba da je uvek jasno na koji od ova dva simbola se misli.

1.	$x = y$	*(Hyp)*
2.	$y = z$	*(Hyp)*
3.	$(\forall x)(\forall y)(x = y \Rightarrow y = x)$	*(primer 3.47)*
4.	$x = y \Rightarrow y = x$	*(3, 2 × A)*
5.	$y = x$	*(1,4,MP)*
6.	$(\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)(x_1 = y_1 \wedge x_2 = y_2 \Rightarrow (x_1 = x_2 \Rightarrow y_1 = y_2))$	*(E3)*
7.	$y = x \wedge y = z \Rightarrow (y = y \Rightarrow x = z)$	*(6, 4 × A, $[x_1 \mapsto y, y_1 \mapsto x, x_2 \mapsto y, y_2 \mapsto z]$)*
8.	$y = x \wedge y = z$	*(5, 2, $\mathcal{A}, \mathcal{B} \vdash \mathcal{A} \wedge \mathcal{B}$)*
9.	$y = y \Rightarrow x = z$	*(7,8,MP)*
10.	$(\forall y)(y = y)$	*(E1)*
11.	$y = y$	*(10, A)*
12.	$x = z$	*(11,9,MP)*

Dakle, važi $x = y, y = z \vdash x = z$. Na osnovu teoreme 3.41 sledi $\vdash x = y \Rightarrow (y = z \Rightarrow x = z)$, a na osnovu $A \Rightarrow (B \Rightarrow C) \vdash (A \wedge B) \Rightarrow C$ sledi $\vdash x = y \wedge y = z \Rightarrow x = z$. Na osnovu (trostruke) primene pravila Gen, sledi $\vdash (\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow x = z)$.

Bez dokaza navodimo naredne značajne teoreme (dokaze videti, na primer, u [18]).

Teorema 3.53 *Čista teorija jednakosti je neodlučiva.*

Teorema 3.54 *Čista teorija jednakosti nad signaturom koja nema funkcijskih simbola arnosti veće od 0 i ima jedino predikatski simbol $=$ je odlučiva.*

Teorema 3.55 *Univerzalno kvantifikovan fragment čiste teorije jednakosti nad signaturom koja nema predikatskih simbola sem $=$ je odlučiv.*

Prethodno tvrđenje može se dokazati postojanjem procedure odlučivanja za univerzalno kvantifikovan fragment čiste teorije jednakosti nad signaturom koja nema predikatskih simbola sem $=$ (videti potpoglavlje 4.3.2).

3.4.2 Teorija grupa

Signaturu teorije grupa čine

- funkcijski simbol 0 (arnosti 0);
- funkcijski simbol $+$ (arnosti 2), koji zapisujemo u infiksnom obliku;
- funkcijski simbol $-$ (arnosti 1), koji zapisujemo u prefiksnom obliku;
- predikatski simbol $=$ (arnosti 2), koji zapisujemo u infiksnom obliku.

Aksiome teorije grupa su aksiome teorije jednakosti i:

G1 $(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z)$

G2 $(\forall x)(x + 0 = x \wedge 0 + x = x)$

G3 $(\forall x)((-x) + x = 0 \wedge x + (-x) = 0)$

Primer 3.49 *Može se dokazati da je naredna formula teorema teorije grupa:*

$$(\forall x)(\forall y)(\forall z)(x + z = y + z \Rightarrow x = y) \ .$$

Bez dokaza navodimo narednu teoremu (dokaz videti, na primer, u [14]).

Teorema 3.56 *Teorija grupa je neodlučiva.*

3.4.3 Teorija gustih uređenih Abelovih grupa bez krajnjih tačaka

Signaturu teorije gustih uređenih Abelovih (komutativnih) grupa bez krajnjih tačaka čine:

- funkcijski simbol 0 (arnosti 0);
- funkcijski simbol $+$ (arnosti 2), koji zapisujemo u infiksnom obliku;
- funkcijski simbol $-$ (arnosti 1), koji zapisujemo u prefiksnom obliku;
- predikatski simbol $=$ (arnosti 2), koji zapisujemo u infiksnom obliku;
- predikatski simbol $<$ (arnosti 2), koji zapisujemo u infiksnom obliku.

Aksiome teorije gustih uređenih Abelovih grupa bez krajnjih tačaka su aksiome teorije jednakosti, aksiome teorije grupa i sledeće aksiome:

L1 $(\forall x)(\forall y)(x + y = y + x)$

L2 $(\forall x)\neg(x < x)$

L3 $(\forall x)(\forall y)(\forall z)(x < y \wedge y < z \Rightarrow x < z)$

L4 $(\forall x)(\forall y)(x < y \vee y < x \vee x = y)$

L5 $(\forall x)(\forall y)(\forall z)(x < y \Rightarrow x + z < y + z)$

L6 $(\forall x)(\forall y)(\exists z)(x < y \Rightarrow (x < z \wedge z < y))$

L7 $(\forall x)(\exists y)(x < y)$

L8 $(\forall x)(\exists y)(y < x)$

U teoriji gustih uređenih Abelovih grupa bez krajnjih tačaka funkcijski simbol $+$ je asocijativan, pa u termu kao što je $x + x + \ldots + x$ zagrade nisu bitne. Dodatno, term

$$\underbrace{x + x + \ldots + x}_{n}$$

zapisivaćemo kraće nx i tada ćemo vrednost n zvati *koeficijent uz* x.

Primer 3.50 *Može se dokazati da je*

$$(\forall x)(\forall y)(\forall z)(y < x \wedge z < x \Rightarrow y + z < 2x)$$

teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka.

Dokažimo najpre da važi

$$y < x \wedge z < x \vdash y + z < 2x \ .$$

1.	$y < x \wedge z < x$	*(Hyp)*
2.	$y < x$	*(1, $\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{A}$)*
3.	$z < x$	*(1, $\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{B}$)*
4.	$(\forall x_1)(\forall x_2)(\forall x_3)(x_1 < x_2 \Rightarrow x_1 + x_3 < x_2 + x_3)$	*(L5)*
5.	$y < x \Rightarrow y + z < x + z$	*(4, 3 × A, $[x_1 \mapsto y, x_2 \mapsto x, x_3 \mapsto z]$)*
6.	$y + z < x + z$	*(2, 5, MP)*
7.	$z < x \Rightarrow z + x < 2x$	*(4, 3 × A, $[x_1 \mapsto z, x_2 \mapsto x, x_3 \mapsto x]$)*
8.	$z + x < 2x$	*(3, 7, MP)*
9.	$(\forall x_1)(\forall x_2)(x_1 + x_2 = x_2 + x_1)$	*(L1)*
10.	$x + z = z + x$	*(9, 2 × A, $[x_1 \mapsto x, x_2 \mapsto z]$)*
11.	$(\forall x_1)(x_1 = x_1)$	*(E1)*
12.	$y + z = y + z$	*(11, A, $[x_1 \mapsto y + z]$)*
13.	$(\forall y_1)(\forall y_2)(\forall z_1)(\forall z_2)(y_1 = z_1 \wedge y_2 = z_2 \Rightarrow (y_1 < y_2 \Rightarrow z_1 < z_2))$	*(E3)*
14.	$y + z = y + z \wedge x + z = z + x \Rightarrow (y + z < x + z \Rightarrow y + z < z + x)$	*(13, 4 × A, $[y_1 \mapsto y + z, y_2 \mapsto x + z, z_1 \mapsto y + z, z_2 \mapsto z + x]$)*
15.	$y + z = y + z \wedge x + z = z + x$	*(12, 10, $\mathcal{A},\mathcal{B} \vdash \mathcal{A} \wedge \mathcal{B}$)*
16.	$y + z < x + z \Rightarrow y + z < z + x$	*(15, 14, MP)*
17.	$y + z < z + x$	*(6, 16, MP)*
18.	$(\forall x_1)(\forall x_2)(\forall x_3)(x_1 < x_2 \wedge x_2 < x_3 \Rightarrow x_1 < x_3)$	*(L3)*
19.	$y + z < z + x \wedge z + x < 2x \Rightarrow y + z < 2x$	*(18, 3 × A, $[x_1 \mapsto y + z, x_2 \mapsto z + x, x_3 \mapsto 2x]$)*
20.	$y + z < z + x \wedge z + x < 2x$	*(17, 8, $\mathcal{A},\mathcal{B} \vdash \mathcal{A} \wedge \mathcal{B}$)*
21.	$y + z < 2x$	*(19, 20, MP)*

Kako u dokazu nije korišćeno pravilo Gen, na osnovu oslabljene teoreme o dedukciji (teorema 3.41) važi:

$$\vdash y < x \wedge z < x \Rightarrow y + z < 2x$$

odakle se, trostrukom primenom pravila Gen, dobija:

$$\vdash (\forall x)(\forall y)(\forall z)(y < x \wedge z < x \Rightarrow y + z < 2x) \ .$$

Naredno tvrđenje dokazuje se postojanjem procedure odlučivanja za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka (videti potpoglavlje 4.3.1).

Teorema 3.57 *Teorija gustih uređenih Abelovih grupa bez krajnjih tačaka je odlučiva.*

Zadaci

Zadatak 90 *Dokazati (u okviru teorije K) da je*

$$(\forall x)(\forall y)(\forall z)(x = y \wedge x = z \Rightarrow y = z)$$

teorema čiste teorije jednakosti.

Zadatak 91 *Dokazati (koristeći teoremu 3.50) da formula*

$$(\forall x)(\forall y)(y = f(x) \vee (\forall x)(x = f(y) \vee y = f(f(x))))$$

nije teorema čiste teorije jednakosti.

Zadatak 92 *U čistoj teoriji jednakosti za bilo koja tri terma s, t i u i bilo koju formulu $\mathcal{A}$ (u kojoj s nije kvantifikovana promenljiva) sledeće formule su teoreme:*

(a) $s = t \Rightarrow u = u[s \mapsto t]$

(b) $s = t \Rightarrow (\mathcal{A} \Leftrightarrow \mathcal{A}[s \mapsto t])$

Zadatak 93 *Dokazati (u okviru teorije K) da je naredna formula teorema teorije grupa:*

$$(\forall x)(\forall y)(\forall z)(x + z = y + z \Rightarrow y = x)\ .$$

Zadatak 94 *Dokazati (koristeći teoremu 3.50) da formula*

$$(\forall x)(\forall y)(x < y \Rightarrow (\forall z)(x < z \Rightarrow z < y))$$

nije teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka.

3.5 Sažetak

Kao i iskazna logika, logika prvog reda (predikatska logika) ima tri aspekta: svoju sintaksu (ili jezik), svoju semantiku (ili značenje formula) i svoje deduktivne sisteme. Poglavlje 3.1 bavi se jezikom logike prvog reda, poglavlje 3.2 semantikom, a poglavlje 3.3 dedukcijom u logici prvog reda.

U potpoglavlju 3.2.1 definisani su pojmovi modela, valjane i zadovoljive formule. Koncept modela je u logici prvog reda daleko bogatiji nego u iskaznoj logici (gde je domen uvek isti skup — skup $\{0, 1\}$). Problemi ispitivanja valjanosti i zadovoljivosti su centralni problemi logike prvog reda. Za razliku od iskazne logike, u logici prvog reda ovi problemi su neodlučivi i ne postoje efektivni metodi za njihovo rešavanje. Međutim, problem ispitivanja valjanosti (kao i problem ispitivanja nezadovoljivosti) je poluodlučiv, te postoje metodi koji za svaku valjanu formulu mogu da utvrde da je valjana (ali ne mogu

za svaku formulu koja nije valjana da utvrde da ona nije valjana). Neki od tih metoda su metod koji proizilazi iz Erbranove teoreme (potpoglavlje 3.2.4), metod rezolucije (potpoglavlje 3.2.6) i metod tabloa (potpoglavlje 3.2.7).

Neki od ovih metoda zahtevaju transformisanje zadate formule u neku normalnu formu (potpoglavlje 3.2.3), što obezbeđuju koncepti supstitucije i teorema o zameni (potpoglavlje 3.2.2).

Svi nabrojani metodi imaju svojstvo potpunosti i saglasnosti — ako je formula valjana, onda će to sigurno biti pokazano primenom metoda, i ako metod tvrdi da je neka formula valjana, onda je ona sigurno valjana.

Kao i u iskaznoj logici, koncept „valjane formule“ je semantičke prirode, a njegov sintaksni, deduktivni pandan je koncept „teoreme“. Teorema je formula za koju postoji dokaz u okviru nekog deduktivnog sistema. Dokaz se zasniva na pravilima izvođenja i aksiomama, a ne na definiciji semantike. No, deduktivni sistemi su obično izgrađeni tako da imaju svojstvo potpunosti i saglasnosti: ako je neka formula valjana, onda ona može biti dokazana u okviru deduktivnog sistema, a ako za neku formulu postoji dokaz u okviru deduktivnog sistema, onda je ona sigurno valjana. Neki od deduktivnih sistema za logiku prvog reda su Hilbertov sistem ili teorija K (potpoglavlje 3.3.1), Gencenov sistem prirodne dedukcije (potpoglavlje 3.3.2) i Gencenov račun sekvenata (potpoglavlje 3.3.3).

Na jeziku logike prvog reda moguće je opisati mnoštvo matematičkih teorija (poglavlje 3.4). Neke od njih su čista teorija jednakosti (potpoglavlje 3.4.1), teorija grupa (potpogljavlje 3.4.2) i teorija gustih uređenih Abelovih grupa bez krajnjih tačaka (potpoglavlje 3.4.3).

Glava 4

Odlučivost i procedure odlučivanja

Iskazna logika je odlučiva tj. postoje efektivni postupci za ispitivanje da li je neka iskazna formula valjana ili nije. Logika prvog reda nije odlučiva i ne postoji opšti postupak za određivanje da li je neka predikatska formula valjana ili nije. Ovaj problem je poluodlučiv i postoje procedure koje za proizvoljnu valjanu predikatsku formulu mogu da utvrde da je ona valjana (ali ne mogu da za proizvoljnu formulu koja nije valjana utvrde da ona nije valjana). Iako predikatska logika nije odlučiva, neke teorije prvog reda (teorije koju se mogu opisati u okviru logike prvog reda) jesu odlučive i za njih postoje efektivni postupci za ispitivanje da li je neka njihova formula teorema ili nije. Ovi postupci su obično znatno efikasniji od opštih (poluodlučivih) postupaka za ispitivanje valjanosti.

Pre nego što se razvila teorija odlučivosti, opšte uverenje bilo je da su svi matematički problemi odlučivi, s tim što nije uvek lako konstruisati postupak odlučivanja. Danas se zna da su mnogi matematički problemi neodlučivi i za većinu netrivijalnih matematičkih teorija se zna ili očekuje da su neodlučive. Odlučivi problemi se, sa teorijske strane, često smatraju manje interesantnim, a odlučive teorije kao, na primer, iskazna logika, sada su predmet interesovanja uglavnom teorije složenosti. Teorija odlučivosti bavi se uglavnom neodlučivim problemima, neodlučivim teorijama i predstavlja disciplinu koja se pre svega bavi „negativnim rezultatima“.

4.1 Rekurzivne funkcije

Pojam odlučivih teorija uvodimo neformalno koristeći koncept intuitivne izračunljivosti, a formalno koristeći formalizme koji opisuju izračunljive funkcije. Postoji više formalizama kojima se uvodi pojam izračunljivosti (UR mašine, Tjuringove mašine, Postove mašine, rekurzivne funkcije, Markovljevi algo-

ritmi) i za njih se može dokazati da su ekvivalentni. Čerčova teza tvrdi da je klasa intuitivno, neformalno izračunljivih funkcija identična sa strogo zasnovanim klasama izračunljivih funkcija (tj. da je funkcija intuitivno izračunljiva ako i samo ako je, na primer, URM-izračunljiva).

U nastavku ćemo opisati koncept rekurzivnih funkcija i koncept odlučivosti i odlučivih teorija koji odatle proizilaze (za više detalja videti npr. [68]).

Osnovne (bazične) funkcije date su u tabeli 14.[1]

Naziv funkcije	Opis
nula–funkcija	$z(x) = 0$
funkcija sledbenik	$s(x) = x + 1$
projektivna funkcija	$P_i^n(x_1, x_2, \ldots, x_n) = x_i,\ 1 \leq i \leq n$

Tabela 4.1: Tabela osnovnih funkcija

Za funkciju $f : \mathbf{N}^{n+1} \to \mathbf{N}$ kažemo da je dobijena *primitivnom rekurzijom* od funkcija $g : \mathbf{N}^n \to \mathbf{N}$ i $h : \mathbf{N}^{n+2} \to \mathbf{N}$ ako važi:

$$\begin{aligned} f(x_1, x_2, \ldots, x_n, 0) &= g(x_1, x_2, \ldots, x_n) \\ f(x_1, x_2, \ldots, x_n, y+1) &= h(x_1, x_2, \ldots, x_n, y, f(x_1, x_2, \ldots, x_n, y)) \end{aligned}$$

i pišemo $f = Rec(g; h)$.

Za funkciju $f : \mathbf{N}^n \to \mathbf{N}$ kažemo da je dobijena *supstitucijom* (*slaganjem*) od funkcija $h : \mathbf{N}^k \to \mathbf{N}$ i $g_1, g_2, \ldots, g_k : \mathbf{N}^n \to \mathbf{N}$ ako važi:

$$f(x_1, x_2, \ldots, x_n) = h(g_1(x_1, x_2, \ldots, x_n), g_2(x_1, x_2, \ldots, x_n), \ldots, g_k(x_1, x_2, \ldots, x_n))$$

i pišemo $f = Sub(h; g_1, g_2, \ldots, g_k)$.

Minimizaciju definišemo na sledeći način:

$$\mu y[g(x_1, x_2, \ldots, x_n, y) = 0] \stackrel{def}{=} \begin{cases} y, & \text{gde je } y \text{ najmanja vrednost takva da je } g(x_1, x_2, \ldots, x_n, y) = 0, \text{ ako takva postoji i ako je } g(x_1, x_2, \ldots, x_n, z) \text{ definisano za sve vrednosti } z \text{ takve da je } z \leq y; \\ \textit{nedefinisano}, & \text{inače.} \end{cases}$$

Skup *rekurzivnih funkcija* je skup koji zadovoljava sledeća svojstva:

1. svaka osnovna funkcija je rekurzivna funkcija;
2. ako su funkcije $g : \mathbf{N}^n \to \mathbf{N}$ i $h : \mathbf{N}^{n+2} \to \mathbf{N}$ rekurzivne, onda je i $Rec(g; h)$ rekurzivna funkcija;

[1] Oznake osnovnih funkcija potiču od naziva na engleskom jeziku (*zero function, succesor function, projection function*).

3. ako su funkcije $g_1, g_2, \ldots, g_k : \mathbf{N}^n \to \mathbf{N}$ i $h : \mathbf{N}^k \to \mathbf{N}$ rekurzivne, onda je i $Sub(h; g_1, g_2, \ldots, g_k)$ rekurzivna funkcija;

4. ako je $g : \mathbf{N}^{n+1} \to \mathbf{N}$ rekurzivna funkcija, onda je rekurzivna i funkcija $\mu y[g(x_1, x_2, \ldots, x_n, y) = 0]$;

5. rekurzivne funkcije su samo one koje se mogu dobiti konačnom primenom prethodnih pravila.

Skup *totalnih rekurzivnih funkcija* je skup rekurzivnih funkcija koje su definisane za svaku torku svojih argumenata.

Za podskup A skupa prirodnih brojeva kažemo da je *odlučiv* (ili *rekurzivan*) ako je njegova *karakteristična funkcija* $f : \mathbf{N} \to \mathbf{N}$, definisana na sledeći način:

$$f(x) = \begin{cases} 1, & \text{ako je } x \in A \\ 0, & \text{ako je } x \notin A \end{cases}$$

rekurzivna.

Za podskup A skupa prirodnih brojeva kažemo da je *poluodlučiv* (ili *polurekurzivan, rekurzivno nabrojiv*) ako je funkcija $f : \mathbf{N} \to \mathbf{N}$, definisana na sledeći način:

$$f(x) = \begin{cases} 1, & \text{ako je } x \in A \\ \textit{nedefinisano}, & \text{ako je } x \notin A \end{cases}$$

rekurzivna.

Svaki odlučiv skup je i poluodlučiv, ali obratno ne važi.

Svaki prebrojiv skup moguće je preslikati u skup prirodnih brojeva. *Gedelova funkcija* predstavlja osnovu mehanizma za kodiranje formula prirodnim brojevima i njihovo dekodiranje. Smisao gedelizacije je u tome da se odlučivost teorije razmatra u terminima rekurzivnosti skupa svih teorema.

Neka je $\mathcal{L}$ signatura (prvog reda) i neka je V (prebrojiv) skup varijabli. Funkcija g_s koja logičke simbole, elemente skupa simbola signature $\mathcal{L}$ i elemente skupa V preslikava u skup prirodnih brojeva je *Gedelova funkcija* ako je bijektivna i ako je skup njenih vrednosti rekurzivan. Funkcija g_e, koja proširuje na nizove simbola funkciju g_s, preslikava niz simbola s_1, s_2, . . ., s_n jezika $\mathcal{L}$ nad V u sledeći prirodan broj:

$$\prod_{i=1}^{n} pn(i)^{1+g_s(s_i)}$$

gde je sa $pn(i)$ označen i-ti prost broj. Ovu vrednost zovemo i *Gedelovim kôdom* (ili, kraće, *kôdom*) niza s_1, s_2, . . ., s_n. Može se dokazati da je funkcija g_e injektivna, tj. različitim nizovima simbola odgovaraju različiti kôdovi. Može se dokazati i da je skup kôdova svih rečenica nad $\mathcal{L}$ rekurzivan podskup skupa $\mathbf{N}$.

Jezik prvog reda (za signaturu $\mathcal{L}$) kojem je na opisani način pridružena funkcija g_e nazivamo *efektivizovanim jezikom* i označavamo sa $\hat{\mathcal{L}}$. Kôdove $g_s(s)$ i $g_e(\mathcal{A})$ označavamo najčešće sa $\ulcorner s \urcorner$ i $\ulcorner \mathcal{A} \urcorner$.

4.2 Odlučive i neodlučive teorije

U prethodnim delovima knjige upoznali smo se sa procedurama odlučivanja za iskazni račun (koje se mogu konstruisati korišćenjem DPLL procedure, metoda rezolucije ili metoda tabloa), kao i sa procedurama poluodlučivanja za predikatski račun. U ovom delu, nakon formalnog uvođenja pojma odlučive teorije, upoznaćemo se sa procedurama odlučivanja za dve teorije prvog reda. Naglasimo da procedure odlučivanja najčešće ne generišu dokaze za zadate teoreme (u okviru nekog deduktivnog sistema) već na specifičan način samo proveravaju da li je zadata formula teorema ili ne.

Za teoriju $\mathcal{T}$ nad signaturom $\mathcal{L}$ kažemo da je *potpuna* (*kompletna)* ako za svaku rečenicu $\mathcal{A}$ nad signaturom $\mathcal{L}$ važi $\mathcal{T} \vdash \mathcal{A}$ ili $\mathcal{T} \vdash \neg\mathcal{A}$.[2]

Neka je $\mathcal{T}$ teorija prvog reda efektivizovanog jezika $\hat{\mathcal{L}}$ i g_e njegova Gedelova funkcija. Za teoriju $\mathcal{T}$ kažemo da je *odlučiva*[3] (*rekurzivna*, *razrešiva*) ako je skup $\{\lceil\mathcal{A}\rceil \mid \vdash_{\mathcal{T}} \mathcal{A}\}$ odlučiv, tj. ako je *karakteristična funkcija* teorije $\mathcal{T}$, funkcija $f_{\mathcal{T}} : \mathbf{N} \to \mathbf{N}$, definisana na sledeći način

$$f_{\mathcal{T}}(\lceil\mathcal{A}\rceil) = \begin{cases} 1, & \text{ako važi } \vdash_{\mathcal{T}} \mathcal{A} \\ 0, & \text{ako važi } \nvdash_{\mathcal{T}} \mathcal{A} \end{cases}$$

rekurzivna. Funkciju $f_{\mathcal{T}}$ tada nazivamo i *procedurom odlučivanja*[4] za teoriju $\mathcal{T}$. Za teoriju $\mathcal{T}$ kažemo da je *neodlučiva* ako nije odlučiva.

Za teoriju $\mathcal{T}$ kažemo da je *poluodlučiva* ako je skup $\{\lceil\mathcal{A}\rceil \mid \vdash_{\mathcal{T}} \mathcal{A}\}$ poluodlučiv, tj. ako je funkcija $f_{\mathcal{T}} : \mathbf{N} \to \mathbf{N}$, definisana na sledeći način:

$$f_{\mathcal{T}}(\lceil\mathcal{A}\rceil) = \begin{cases} 1, & \text{ako važi } \vdash_{\mathcal{T}} \mathcal{A} \\ \textit{nedefinisano}, & \text{ako važi } \nvdash_{\mathcal{T}} \mathcal{A} \end{cases}$$

rekurzivna. Funkciju $f_{\mathcal{T}}$ tada nazivamo i *procedurom poluodlučivanja* za teoriju $\mathcal{T}$.

Prethodnim definicijama strogo je uveden pojam odlučive teorije. Taj pojam moguće je uvesti i neformalno, na sledeći način: ukoliko postoji algoritam (postupak, procedura) A takav da za svaku rečenicu $\mathcal{A}$ daje odgovor *da* ako i samo ako je $\mathcal{A}$ teorema teorije $\mathcal{T}$ (i *ne* inače) onda kažemo da je teorija $\mathcal{T}$ odlučiva. Veza između formalno i neformalno uvedenog pojma odlučive teorije bazira se (između ostalog) na Čerčovoj tezi koja tvrdi da su klase rekurzivnih i intuitivno izračunljivih funkcija identične.

[2] Naglasimo da se termin *potpunost* koristi u različitim kontekstima i sa različitim značenjima. Na primer, za teoriju K (tj. za predikatski račun) važi da je, u smislu snage deduktivnog sistema, potpuna, jer u njoj može da se dokaže svaka valjana formula. S druge strane, teorija K (kao formalna teorija, kao „čist predikatski račun“) u smislu izražajnosti formalne teorije, nije potpuna, jer postoje dobro zasnovane formule takve da ni one ni njihove negacije nisu teoreme teorije K.

[3] Termin *odlučiv* ima sasvim drugačiji smisao kada je u pitanju pojedinačna formula: kažemo da je formula $\mathcal{A}$ neprotivrečne teorije $\mathcal{T}$ *odlučiva* ako je ili $\mathcal{A}$ ili $\neg\mathcal{A}$ teorema teorije $\mathcal{T}$. Ako je teorija potpuna, sve rečenice na njenom jeziku su odlučive. Teorija može da bude nepotpuna i odlučiva.

[4] Ponekad se procedurom odlučivanja naziva funkcija koja je definisana samo za Gedelove kodove nizova simbola koji su formule jezika $\hat{\mathcal{L}}$. U skladu sa ovde navedenom definicijom, funkcija $f_{\mathcal{T}}$ najpre „proverava“ da li je za datu vrednost argumenta $\lceil\mathcal{A}\rceil$ niz simbola $\mathcal{A}$ zaista formula teorije $\mathcal{T}$ i ako jeste, onda se proverava da li je ta formula teorema teorije $\mathcal{T}$.

Za jezik nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ i skupom varijabli V kažemo da je rekurzivan ako je rekurzivan skup vrednosti $\lceil \mathcal{A} \rceil$ za formule $\mathcal{A}$ nad signaturom $\mathcal{L}$. Jezik nad signaturom $\mathcal{L} = (\Sigma, \Pi, ar)$ je rekurzivan ako su skupovi Σ, Π i V rekurzivni. Za teoriju $\mathcal{T}$ nad rekurzivnim jezikom kažemo da je *aksiomatibilna* (ili *aksiomatska*) ako je ispunjen sledeći uslov: postoji rekurzivan neprotivrečan skup Γ rečenica nad $\mathcal{L}$ takav da je proizvoljna rečenica $\mathcal{A}$ nad $\mathcal{L}$ teorema teorije $\mathcal{T}$ (tj. $\vdash_{\mathcal{T}} \mathcal{A}$) ako i samo ako važi $\Gamma \vdash \mathcal{A}$ (u izabranom deduktivnom sistemu); tada skup Γ zovemo *skup aksioma* teorije $\mathcal{T}$.

Ako za signature $\mathcal{L}^e = (\Sigma^e, \Pi^e, ar^e)$ i $\mathcal{L} = (\Sigma, \Pi, ar)$ važi $\Sigma \subseteq \Sigma^e$, $\Pi \subseteq \Pi^e$, kao i $ar^e(f) = ar(f)$ za $f \in \Sigma$, $ar^e(p) = ar(p)$ za $p \in \Pi$, kažemo da je signatura $\mathcal{L}^e$ *proširenje* signature $\mathcal{L}$. Ako je $\mathcal{T}$ teorija nad signaturom $\mathcal{L}$, a $\mathcal{T}^e$ teorija nad signaturom $\mathcal{L}^e$ i ako je svaka teorema teorije $\mathcal{T}$ teorema teorije $\mathcal{T}^e$, onda kažemo da je teorija $\mathcal{T}^e$ *proširenje* teorije $\mathcal{T}$ (i da je $\mathcal{T}$ *podteorija* teorije $\mathcal{T}^e$). Za teoriju $\mathcal{T}^e$ kažemo da je *kompletno proširenje teorije* $\mathcal{T}$ ako je $\mathcal{T}^e$ proširenje teorije $\mathcal{T}$ i $\mathcal{T}^e$ je kompletna teorija. Za teoriju $\mathcal{T}^e$ kažemo da je *konzervativno proširenje teorije* $\mathcal{T}$ ako je presek skupa formula jezika $\mathcal{L}$ i skupa teorema teorije $\mathcal{T}^e$ upravo skup teorema teorije $\mathcal{T}$. Za teoriju $\mathcal{T}^e$ kažemo da je *definicijsko proširenje teorije* $\mathcal{T}$ ako se svaki simbol iz $\mathcal{L}^e \setminus \mathcal{L}$ može definisati na jeziku $\mathcal{L}$. Svako definicijsko proširenje teorije je konzervativno. Za teoriju $\mathcal{T}^e$ kažemo da je *konačno proširenje teorije* $\mathcal{T}$ ako postoji konačan skup Γ teorema teorije $\mathcal{T}^e$ takav da je svaka teorema teorije $\mathcal{T}^e$ izvodiva iz skupa koji čine teoreme teorije $\mathcal{T}$ i rečenice iz skupa Γ. Za teoriju $\mathcal{T}$ kažemo da je *esencijalno neodlučiva* ako je neodlučiva teorija $\mathcal{T}$, kao i bilo koje njeno neprotivrečno proširenje.

Naredna teorema daje potrebne i dovoljne uslove da potpuna teorija bude (ne)odlučiva (dokaz teoreme videti u [71]).

Teorema 4.1 *Za potpunu teoriju $\mathcal{T}$ sledeći uslovi su ekvivalentni:*

- *$\mathcal{T}$ je neodlučiva,*
- *$\mathcal{T}$ je esencijalno neodlučiva,*
- *$\mathcal{T}$ nije aksiomatibilna.*

O odnosu odlučivosti i proširenja teorije govore naredna dva tvrđenja (videti [49]).

Teorema 4.2 *Neka su $\mathcal{T}_1$ i $\mathcal{T}_2$ dve teorije sa istim konstantama takve da je $\mathcal{T}_2$ konačno proširenje teorije $\mathcal{T}_1$. Ako je teorija $\mathcal{T}_2$ neodlučiva, onda je neodlučiva i teorija $\mathcal{T}_1$.*

Teorema 4.3 *Ako teorija $\mathcal{T}$ ima najviše prebrojivo mnogo kompletnih proširenja i ako se ona mogu efektivno nabrojati, onda je ona odlučiva.*

Postoji značajna metodološka razlika u proučavanju odlučivosti i neodlučivosti, uprkos činjenici da su ta dva pojma u neposrednoj vezi. Da bi se pokazalo da je neka teorija neodlučiva, obično se poseže za strogim formalizmima za opisivanje izračunljivih funkcija. S druge strane, za dokaz odlučivosti neke teorije dovoljno je postojanje efektivnog postupka koji za svaku

rečenicu utvrđuje da li jeste ili nije teorema date teorije. Zbog toga, prvi rezultati u vezi sa odlučivošću prethodili su uvođenju pojma rekurzivnih funkcija sredinom tridesetih godina dvadesetog veka, a prvi rezultati u vezi sa neodlučivošću pojavili su se tek nakon toga. Više o odlučivim teorijama videti u [59]; više o neodlučivim teorijama videti u [71].

Neke od odlučivih teorija su: iskazni račun, predikatski račun sa jednakošću i bez drugih funkcijskih i predikatskih simbola, teorija unarnih relacija, teorija ekvivalencije, teorija unarne operacije, teorija linearnog uređenja, teorija gusto uređenih skupova, Prezburgerova aritmetika, teorija množenja prirodnih brojeva, teorija Abelovih grupa, teorija gustih uređenih Abelovih grupa bez krajnjih tačaka, teorija algebarski zatvorenih polja. Neke od neodlučivih teorija su: Peanova aritmetika, Zermelo–Fraenkelova teorija skupova, teorija grupa, teorija polja, projektivna geometrija (za više detalja videti [49, 16]).

Zadaci

Zadatak 95 $\surd$ *Dokazati da je potpuna teorija odlučiva ako i samo ako je aksiomatibilna.*

4.3 Metode za dokazivanje odlučivosti i procedure odlučivanja

Tri osnovna metoda za dokazivanje odlučivosti teorije prvog reda su (opširniji pregled videti u [59, 49, 67]):

- model–teoretski metod;
- metod interpretacija;
- metod eliminacije kvantora.

U svojoj osnovnoj formi, *model–teoretski metod* zasniva se na teoremi 4.3 i razmatranju rekurzivnog skupa aksioma Γ teorije $\mathcal{T}$. Razmatranje svojstava mogućih modela koristi se ili u dokazivanju da je $\mathcal{T}$ potpuna teorija (odakle na osnovu teoreme 4.1 sledi da je $\mathcal{T}$ odlučiva) ili za sistematično nabrajanje svih potpunih proširenja skupa Γ (u tom slučaju možemo za svaku rečenicu $\mathcal{A}$ da ispitamo da li je teorija $\mathcal{T} \cup \{\neg\mathcal{A}\}$ neprotivrečna i, odatle, da li važi $\vdash_{\mathcal{T}} \mathcal{A}$).

Neka je $\mathcal{T}$ teorija jezika $\mathcal{L}$ i $\mathcal{T}'$ teorija jezika $\mathcal{L}'$. *Metod interpretacija* zasniva se na efektivnom preslikavanju t koje svakoj rečenici $\mathcal{A}$ jezika $\mathcal{L}$ pridružuje rečenicu $t(\mathcal{A})$ jezika $\mathcal{L}'$ takvu da važi

$$\vdash_{\mathcal{T}} \mathcal{A} \text{ ako i samo ako } \vdash_{\mathcal{T}'} t(\mathcal{A}) .$$

Ako takvo preslikavanje postoji i ako je teorija $\mathcal{T}'$ odlučiva, onda je odlučiva i teorija $\mathcal{T}$. Naime, da bismo utvrdili da li važi $\vdash_{\mathcal{T}} \mathcal{A}$ dovoljno je odrediti $t(\mathcal{A})$ i ispitati da li važi $\vdash_{\mathcal{T}'} t(\mathcal{A})$. Obično interpretacija t uključuje model–teoretska

razmatranja. Pokazuje se da modeli teorije $\mathcal{T}$ mogu biti izomorfno reprodukovani iz modela teorije $\mathcal{T}'$ relacijama koje se mogu definisati u $\mathcal{L}'$. Metod interpretacija se često koristi i za dokazivanje neodlučivosti teorija. Ako je teorija $\mathcal{T}'$ neodlučiva i ako postoji opisano preslikavanje t, onda je neodlučiva i teorija $\mathcal{T}$.

Metod eliminacije kvantora je najstariji i u kontekstu automatskog dokazivanja teorema najznačajniji. Naziv metoda[5] — *eliminacija kvantora* — potiče od Tarskog (1935) koji je dao nekoliko njegovih najznačajnih primena, dokazavši odlučivost nekoliko teorija: algebarski zatvorena polja (1949), realno zatvorena polja (1949), teorija dobrog uređenja (1949), Bulove algebre (1951) (više o ovom metodu videti u [39, 67]). Suštinski isti metod bio je primenjivan i pre toga za predikatski račun sa jednakošću (Lovenhajm, 1915), gusto linearno uređenje bez krajnjih tačaka (1927), Prezburgerovu aritmetiku (1929), a kasnije, između ostalih, i za dokaz odlučivosti teorije Abelovih grupa (1955). Metod eliminacije kvantora zasniva se na transformisanju date rečenice $\mathcal{A}$ u rečenicu $\mathcal{B}$ takvu da je $\vdash_{\mathcal{T}} \mathcal{A}$ ako i samo ako važi $\vdash_{\mathcal{T}} \mathcal{B}$ i formula $\mathcal{B}$ je, u nekom smislu, jednostavnija od formule $\mathcal{A}$ (obično ima manje varijabli od $\mathcal{A}$). U poslednjoj iteraciji takvog transformisanja dobija se formula $\mathcal{C}$ koja pripada klasi rečenica za koje se može trivijalno proveriti da li su teoreme teorije $\mathcal{T}$ (obično je to skup baznih formula).

Metod eliminacije kvantora za dokazivanje odlučivosti neke teorije je značajan i po tome što ima i nekoliko „sporednih efekata“:

- u nekim slučajevima (onda kada je teorija data aksiomatski), metod može da indukuje i dokaz potpunosti teorije;
- metod indukuje proceduru odlučivanja koja je efektivno opisiva i moguće ju je automatizovati.

Neformalno, smisao metoda eliminacije kvantora je u tome da se odredi skup „jednostavnih“ formula jezika takav da je svaka formula tog jezika ekvivalentna nekoj jednostavnoj formuli. Termin „jednostavna formula“ međutim često nije najpogodniji za različite primene ove metode, jer su formule dobijene njegovom primenom zapravo izuzetno složene. U primenama, termin „jednostavna formula“ odnosiće se najčešće na formule bez kvantifikatora.

Neka je $\mathcal{K}$ efektivno izabran skup formula jezika $\mathcal{L}$. Kažemo da teorija $\mathcal{T}$ *dopušta eliminaciju kvantora* do na klasu $\mathcal{K}$ ako i samo ako za svaku formulu $\mathcal{A}$ jezika $\mathcal{L}$ postoji formula $\mathcal{B}$ iz skupa $\mathcal{K}$ takva da važi $\vdash_{\mathcal{T}} \mathcal{A}$ ako i samo ako $\vdash_{\mathcal{T}} \mathcal{B}$. Ukoliko je za sve rečenice iz klase $\mathcal{K}$ moguće efektivno odrediti da li pripadaju teoriji $\mathcal{T}$, onda je teorija koja dopušta eliminaciju kvantora odlučiva. Pored toga, ako za svaku rečenicu $\mathcal{A}$ iz klase $\mathcal{K}$ važi $\vdash_{\mathcal{T}} \mathcal{A}$ ili $\vdash_{\mathcal{T}} \neg\mathcal{A}$, onda je teorija $\mathcal{T}$ potpuna. U većini primena, klasa $\mathcal{K}$ je skup formula bez kvantora.

Uopšteno govoreći, metod (za dokazivanje odlučivosti teorije $\mathcal{T}$ jezika $\mathcal{L}$) se sastoji od sledećih koraka:

- bira se pogodan skup osnovnih formula jezika $\mathcal{L}$ i on se proglašava klasom $\mathcal{K}$;

[5] Hilbert ovaj metod naziva *metodom redukcije* [26].

- pokaže se da za svaku formulu $\mathcal{A}$ jezika $\mathcal{L}$ postoji formula $\mathcal{B}$ iz klase $\mathcal{K}$ takva da je $\vdash_{\mathcal{T}} \mathcal{A}$ ako i samo ako $\vdash_{\mathcal{T}} \mathcal{B}$;
- pokaže se da je za svaku formulu $\mathcal{B}$ iz $\mathcal{K}$ moguće efektivno ispitati da li važi $\vdash_{\mathcal{T}} B$.

O tome kako se procedure odlučivanja mogu koristiti u dokazivanju teorema i kombinovati sa drugim dokazivačkim strategijama videti npr. [33, 32, 31].

U daljem tekstu metod eliminacije kvantora ilustrovaćemo Furije–Mockinovom procedurom odlučivanja za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka.

4.3.1 Furije–Mockinova procedura

Furije–Mockinova procedura je procedura odlučivanja za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka (videti potpoglavlje 3.4.3). Ona je, suštinski, zasnovana na Furijeovom metodu za rešavanje linearnih nejednakosti nad poljem racionalnih brojeva [28, 41]. Furije–Mockinovu proceduru čini sledeći niz koraka:

1. Neka je rečenica za koju treba ispitati da li je teorema u preneks normalnoj formi.

   (a) Za pojednostavljivanje tekuće rečenice koristimo sledeće logičke ekvivalencije:

   $$\begin{aligned} 0 = 0 &\equiv \top \\ \neg(0 = 0) &\equiv \bot \\ 0 < 0 &\equiv \bot \\ \neg(0 < 0) &\equiv \top \\ \mathcal{A} \wedge \top &\equiv \mathcal{A} \\ \top \wedge \mathcal{A} &\equiv \mathcal{A} \\ \mathcal{A} \vee \top &\equiv \top \\ \top \vee \mathcal{A} &\equiv \top \\ \mathcal{A} \wedge \bot &\equiv \bot \\ \bot \wedge \mathcal{A} &\equiv \bot \\ \mathcal{A} \vee \bot &\equiv \mathcal{A} \\ \bot \vee \mathcal{A} &\equiv \mathcal{A}\,. \end{aligned}$$

   Ako je, primenom navedenih veza, formula transformisana u $\top$, onda procedura vraća odgovor da je početna formula teorema. Inače, tj. ako je formula transformisana u $\bot$, onda procedura vraća odgovor da početna formula nije teorema.

   (b) Ako rečenica nije bazna i ako je njen unutrašnji kvantifikator univerzalni, onda ga zamenimo egzistencijalnim koristeći logičku ekvivalenciju $(\forall x)\mathcal{A} \equiv \neg(\exists x)\neg\mathcal{A}$. Pri tome, ako je formula $\mathcal{A}$ oblika $\neg\mathcal{B}$, onda formulu $(\forall x)\mathcal{A}$ zamenjujemo formulom $\neg(\exists x)\mathcal{B}$.

2. Koristimo naredne korake da odredimo rečenicu $(Q_1x_1)(Q_2x_2)\ldots(Q_nx_n)$ $\mathcal{F}'(x_1, x_2, \ldots, x_n)$ takvu da je ona teorema ako i samo ako je (tekuća) rečenica $(Q_1x_1)(Q_2x_2)\ldots(Q_nx_n)(\exists y)\mathcal{F}(x_1, x_2, \ldots, x_n, y)$ teorema ($Q_i \in \{\forall, \exists\}, 1 \leq i \leq n$); nakon toga zamenjujemo tekuću formulu

$$(Q_1x_1)(Q_2x_2)\ldots(Q_nx_n)(\exists y)\mathcal{F}(x_1, x_2, \ldots, x_n, y)$$

formulom

$$(Q_1x_1)(Q_2x_2)\ldots(Q_nx_n)\mathcal{F}'(x_1, x_2, \ldots, x_n)$$

i idemo na početni korak.

   (a) Eliminišemo sva pojavljivanja ekvivalencije i implikacije u tekućoj formuli koristeći logičke ekvivalencije:

$$\begin{aligned} \mathcal{A}_1 \Leftrightarrow \mathcal{A}_2 &\equiv (\mathcal{A}_1 \Rightarrow \mathcal{A}_2) \wedge (\mathcal{A}_2 \Rightarrow \mathcal{A}_1) \\ \mathcal{A}_1 \Rightarrow \mathcal{A}_2 &\equiv \neg\mathcal{A}_1 \vee \mathcal{A}_2\ . \end{aligned}$$

   (b) Koristimo logičke ekvivalencije

$$\begin{aligned} \neg(\mathcal{A}_1 \wedge \mathcal{A}_2) &\equiv (\neg\mathcal{A}_1 \vee \neg\mathcal{A}_2) \\ \neg(\mathcal{A}_1 \vee \mathcal{A}_2) &\equiv (\neg\mathcal{A}_1 \wedge \neg\mathcal{A}_2) \\ \neg\neg\mathcal{A}_1 &\equiv \mathcal{A}_1 \end{aligned}$$

   za eliminisanje svih simbola $\neg$, osim onih koji neposredno dominiraju atomičkim formulama.

   (c) Preostale negacije eliminišemo koristeći sledeće veze:

$$\begin{aligned} \neg(t_1 = t_2) &\equiv (t_1 < t_2) \vee (t_2 < t_1) \\ \neg(t_1 < t_2) &\equiv (t_1 = t_2) \vee (t_2 < t_1) \\ \neg\bot &\equiv \top \\ \neg\top &\equiv \bot\ . \end{aligned}$$

   Novodobijena formula sadrži samo veznike $\wedge$ i $\vee$.

   (d) Svaku od atomičkih formula pojednostavljujemo tako da sadrži najviše jedno pojavljivanje terma oblika ny. To postižemo koristeći veze:

$$\begin{aligned} (t_1 = (t_2 + ny) + t_3) &\equiv (t_1 = (t_2 + t_3) + ny) \\ (t_1 = (t_2 + ny) + my) &\equiv (t_1 = t_2 + (m+n)y) \\ (t_1 + ny = t_2 + my) &\equiv (t_1 = t_2), \text{ pri čemu je } m = n \\ (t_1 + ny = t_2 + my) &\equiv (t_1 = t_2 + (m-n)y), \text{ pri čemu je } m > n \\ (t_1 + ny = t_2 + my) &\equiv (t_1 + (n-m)y = t_2), \text{ pri čemu je } n > m \\ (t_1 < (t_2 + ny) + t_3) &\equiv (t_1 < (t_2 + t_3) + ny) \\ (t_1 < (t_2 + ny) + my) &\equiv (t_1 < t_2 + (m+n)y) \\ (t_1 + ny < t_2 + my) &\equiv (t_1 < t_2), \text{ pri čemu je } m = n \\ (t_1 + ny < t_2 + my) &\equiv (t_1 < t_2 + (m-n)y), \text{ pri čemu je } m > n \\ (t_1 + ny < t_2 + my) &\equiv (t_1 + (n-m)y < t_2), \text{ pri čemu je } n > m. \end{aligned}$$

(e) Koristimo logičke ekvivalencije

$$\begin{array}{rcl} \mathcal{A}_1 \wedge (\mathcal{A}_2 \vee \mathcal{A}_3) & \equiv & (\mathcal{A}_1 \wedge \mathcal{A}_2) \vee (\mathcal{A}_1 \wedge \mathcal{A}_3) \\ (\mathcal{A}_1 \vee \mathcal{A}_2) \wedge \mathcal{A}_3 & \equiv & (\mathcal{A}_1 \wedge \mathcal{A}_3) \vee (\mathcal{A}_2 \wedge \mathcal{A}_3) \end{array}$$

za transformisanje tekuće formule (tj. njenog dela bez kvantifikatora) u disjunktivnu normalnu formu:

$$\mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_n$$

gde je $\mathcal{A}_i$ $(i = 1, 2 \ldots, n)$ konjunkcija atomičkih formula.

(f) Egzistencijalni kvantifikator može da „prolazi" kroz disjunkciju, pa važi:

$$(\exists y)\mathcal{F} \equiv (\exists y)(\mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_n) \equiv (\exists y)\mathcal{A}_1 \vee (\exists y)\mathcal{A}_2 \vee \ldots \vee (\exists y)\mathcal{A}_n \ .$$

Ako u $\mathcal{A}_i$ nema atomičkih formula koje sadrže y onda je

$$(\exists y)\mathcal{A}_i \equiv \mathcal{A}_i \ ,$$

čime je eliminisan kvantifikator $\exists y$ iz $(\exists y)\mathcal{A}_i$. U suprotnom, formula $\mathcal{A}_i$ može biti napisana u obliku $\mathcal{B}_i \wedge \mathcal{C}_i$ gde je $\mathcal{B}_i$ konjunkcija svih atomičkih formula iz $\mathcal{A}_i$ koje ne sadrže y. Kako $\mathcal{B}_i$ ne sadrži y važi

$$(\exists y)(\mathcal{B}_i \wedge \mathcal{C}_i) \equiv \mathcal{B}_i \wedge (\exists y)\mathcal{C}_i \ .$$

(g) Potrebno je eliminisati kvantifikatore $\exists y$ iz svih formula $(\exists y)\mathcal{C}_i$. Svaka od ovih formula je oblika

$$(\exists y)(t_1 = s_1 \wedge \ldots \wedge t_j = s_j \wedge q_1 < r_1 \wedge \ldots \wedge q_k < r_k)$$

pri čemu važi $j + k > 0$, za svako i, $1 \leq i \leq j$, y se pojavljuje u t_i ili u s_i i za svako i, $1 \leq i \leq k$, y se pojavljuje u q_i ili u r_i.
Najpre razmatramo slučaj $j > 0$, tj. slučaj da postoji bar jedna jednakost. Ako je $j = 1$ i $k = 0$, onda $(\exists y)(t_1 = s_1)$ može biti zamenjeno logičkom konstantom $\top$. Inače, obrišimo jednu jednakost, $t_m = s_m$, i iskoristimo je za eliminisanje promenljive y iz preostalih $j + k - 1$ atomičkih formula. Pretpostavimo da se promenljiva y pojavljuje u termu t_m i to sa koeficijentom c_m (postupak je analogan ako se y pojavljuje u termu s_m). Ako je atomička formula oblika $q_p < r_p$ i y se u termu q_p pojavljuje sa koeficijentom c_p, onda je u nejedankosti

$$c_m q_p + c_p s_m < c_m r_p + c_p t_m$$

koeficijent uz y sa obe strane jednak $c_p c_m$, pa promenljiva y može biti eliminisana. Ako je atomička formula oblika $q_p < r_p$ i y se u termu r_p pojavljuje sa koeficijentom c_p, onda je u nejedankosti

$$c_m q_p + c_p t_m < c_m r_p + c_p s_m$$

koeficijent uz y sa obe strane jednak $c_p c_m$, pa promenljiva y može biti eliminisana. Analogno se y može eliminisati iz jednakosti oblika $s_p = t_p$. U dobijenoj konjunkciji više nema pojavljivanja promenljive y, pa kvantifikator $(\exists y)$ iz $(\exists y)\mathcal{C}_i$ može biti eliminisan.

Razmotrimo slučaj $j = 0$. Formula $(\exists y)\mathcal{C}_i$ je oblika

$$(\exists y)(q_1 < r_1 \wedge \ldots \wedge q_k < r_k)$$

Ako se y u svakoj nejednakosti nalazi sa desne strane tada zamenjujemo $(\exists y)\mathcal{C}_i$ logičkom konstantom $\top$. Slično, ako se y u svakoj nejednakosti nalazi sa leve strane zamenjujemo $(\exists y)\mathcal{C}_i$ konstantom $\top$. Inače, za svaki par m, p takav da se y nalazi sa raznih strana u nejednakostima $q_m < r_m$ i $q_p < r_p$, odgovarajući par nejednakosti zamenjujemo novom nejednakošću

$$c_p q_m + c_m q_p < c_p r_m + c_m r_p$$

pri čemu je c_m koeficijent uz y u m-toj, a c_p koeficijent uz y u p-toj nejednakosti (pa je koeficijent uz y sa obe strane nejednakosti jednak $c_p c_m$); tako dobijene nejednakosti vezane su konjunkcijama. Ako u polaznoj formuli $\mathcal{C}_i$ ima j nejednakosti sa promenljivom y na levoj i k nejednakosti sa promenljivom y na desnoj strani, onda novodobijena formula ima ukupno jk nejednakosti (vezanih konjunkcijama) iz kojih se promenljiva y trivijalno može eliminisati. Nakon toga, u dobijenoj konjunkciji više nema pojavljivanja promenljive y, pa je kvantifikator $(\exists y)$ iz $(\exists y)\mathcal{C}_i$ redundantan i može biti eliminisan.

Navedena procedura može se učiniti efikasnijom različitim heuristikama.

Za navedenu proceduru može se dokazati da je korektna, tj. da se uvek zaustavlja, da je potpuna i da je saglasna [41]. Njeno vreme izvršavanja ograničeno je sa $O(2^n)$, gde je n dužina ulazne formule.

Naglasimo da Furije–Mockinova procedura ne generiše formalni dokaz u okviru nekog deduktivnog sistema — ona je procedura za „proveravanje" da li je neka formula teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka.

Primer 4.1 *Formula* $(\forall x)(\forall y)(\forall z)(x < y \wedge y < z \Rightarrow x < z)$ *je teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka. To se može pokazati primenom Furuje–Mockinove procedure na sledeći način (u zagradi su navedene oznake primenjenih koraka procedure; nisu navođeni koraci primene procedure koji ne menjaju tekuću formulu):*

$(\forall x)(\forall y)(\forall z)(x < y \wedge y < z \Rightarrow x < z)$
$\equiv$ *(1(b))*
$(\forall x)(\forall y)\neg((\exists z)\neg(x < y \wedge y < z \Rightarrow x < z))$
$\equiv$ *(2(a))*
$(\forall x)(\forall y)\neg((\exists z)(x < y \wedge y < z \wedge \neg x < z))$
$\equiv$ *(2(c))*

$(\forall x)(\forall y)\neg((\exists z)(x < y \wedge y < z \wedge (x = z \vee z < x)))$
$\equiv$ *(2(e))*
$(\forall x)(\forall y)\neg((\exists z)((x < y \wedge y < z \wedge x = z) \vee (x < y \wedge y < z \wedge z < x)))$
$\equiv$ *(2(f))*
$(\forall x)(\forall y)(\neg(((\exists z)(x < y \wedge y < z \wedge x = z)) \vee ((\exists z)(x < y \wedge y < z \wedge z < x))))$
$\equiv$ *(2(f))*
$(\forall x)(\forall y)(\neg((x < y \wedge (\exists z)(y < z \wedge x = z)) \vee (x < y \wedge (\exists z)(y < z \wedge z < x))))$
$\equiv$ *(2(g))*
$(\forall x)(\forall y)(\neg((x < y \wedge y < x) \vee (x < y \wedge y < x)))$
$\equiv$ *(1(b))*
$(\forall x)\neg(\exists y)((x < y \wedge y < x) \vee (x < y \wedge y < x))$
$\equiv$ *(2(f))*
$(\forall x)\neg(((\exists y)(x < y \wedge y < x)) \vee ((\exists y)(x < y \wedge y < x)))$
$\equiv$ *(2(g))*
$(\forall x)\neg(x < x \vee x < x)$
$\equiv$ *(1(b))*
$\neg(\exists x)(x < x \vee x < x)$
$\equiv$ *(2(d))*
$\neg(\exists x)(0 < 0 \vee 0 < 0)$
$\equiv$ *(2(f))*
$\neg(0 < 0 \vee 0 < 0)$
$\equiv$ *(1(a))*
$\neg(\bot \vee \bot)$
$\equiv$ *(1(a))*
$\top$

Primer 4.2 *Formula* $(\forall x)(\forall y)(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y)$ *je teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka. To se može pokazati primenom Furije–Mockinove procedure na sledeći način:*

$(\forall x)(\forall y)(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y)$
$\equiv$ *(1(b))*
$(\forall x)\neg(\exists y)\neg(2x < 3y \wedge 3x < 2y \Rightarrow 7x < 7y)$
$\equiv$ *(2(a))*
$(\forall x)\neg(\exists y)(2x < 3y \wedge 3x < 2y \wedge \neg 7x < 7y)$
$\equiv$ *(2(c))*
$(\forall x)\neg(\exists y)(2x < 3y \wedge 3x < 2y \wedge (7x = 7y \vee 7y < 7x))$
$\equiv$ *(2(e))*
$(\forall x)\neg(\exists y)((2x < 3y \wedge 3x < 2y \wedge 7x = 7y) \vee (2x < 3y \wedge 3x < 2y \wedge 7y < 7x))$
$\equiv$ *(2(f))*
$(\forall x)\neg((\exists y)(2x < 3y \wedge 3x < 2y \wedge 7x = 7y) \vee (\exists y)(2x < 3y \wedge 3x < 2y \wedge 7y < 7x))$
$\equiv$ *(2(g))*
$(\forall x)\neg((14x < 21x \wedge 21x < 14x) \vee (14x < 21x \wedge 21x < 14x))$
$\equiv$ *(1(b))*
$\neg(\exists x)((14x < 21x \wedge 21x < 14x) \vee (14x < 21x \wedge 21x < 14x))$
$\equiv$ *(2(d))*
$\neg(\exists x)((0 < 7x \wedge 7x < 0) \vee (0 < 7x \wedge 7x < 0))$

$\equiv$ *(2(f))*
$\neg((\exists x)(0 < 7x \wedge 7x < 0)) \vee ((\exists x)(0 < 7x \wedge 7x < 0))$
$\equiv$ *(2(g))*
$\neg(0 < 0 \vee 0 < 0)$
$\equiv$ *(1(a))*
$\neg(\bot \vee \bot)$
$\equiv$ *(1(a))*
$\top$

Zadaci

Zadatak 96 *Data je formula*

$$(\forall x)(\forall y)(\forall z)(\forall u)(x < y \wedge y < z \wedge z < u \Rightarrow x < u) .$$

Dokazati da je ona teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka:
(a) formalno, u okviru teorije K;
(b) primenom Furije–Mockinove procedure.

Zadatak 97 *Data je formula*

$$(\forall x)(\forall y)(\forall z)(y < z \wedge x < y \Rightarrow x < z) .$$

Dokazati da je ona teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka:
(a) formalno, u okviru sistema K;
(b) primenom Furije–Mockinove procedure.

Zadatak 98 *Data je formula*

$$(\forall x)(\forall y)(x < y \Rightarrow (\forall z)(x < z \Rightarrow z < y)) .$$

Dokazati da ona nije teorema teorije gustih uređenih Abelovih grupa bez krajnjih tačaka primenom Furije–Mockinove procedure.

4.3.2 Kongruentno zatvorenje i Nelson–Openova procedura

Problem ispitivanja da li je neka jednakost izvodiva iz datog skupa hipoteza u teoriji jednakosti (videti potpoglavlje 3.4.1) može biti, u različitim kontekstima, rešavan na više načina: na primer, primenom tehnika prezapisivanja i Knut–Bendiksove procedure upotpunjavanja [38] ili primenom metoda *kongruentnog zatvorenja* [55, 65, 4] koji će biti opisan u nastavku.

Neka je λ funkcija koja preslikava skup termova u skup funkcijskih simbola i vraća dominirajući funkcijski simbol terma:

$$\lambda(t) = \begin{cases} f, & \text{ako je } t = f(x_1, \ldots, x_n) \\ \epsilon, & \text{ako je } t \text{ simbol promenljive ili konstante} \end{cases}$$

pri čemu je ϵ novi, specijalni funkcijski simbol.

Neka je δ funkcija koja preslikava skup termova u skup **N** i vraća arnost dominirajućeg funkcijskog simbola:

$$\delta(t) = \begin{cases} n, & \text{ako je } t = f(x_1, \ldots, x_n) \\ 0, & \text{ako je } t \text{ simbol promenljive ili konstante.} \end{cases}$$

Neka $u[i]$ označava i-ti argument terma u:

$$t[i] = x_i, \text{za } 1 \leq i \leq n, \text{ako je } t = f(x_1, \ldots, x_n) \ .$$

Za datu binarnu relaciju R nad skupom termova T, *ekvivalencijsko zatvorenje* relacije R, u oznaci R^*, je najmanje refleksivno, simetrično i tranzitivno zatvorenje relacije R. *Kongruentno zatvorenje* $\hat{R}$ binarne relacije R je najmanje proširenje relacije R^* takvo da za svaka dva terma u, v ako važi $\lambda(u) = \lambda(v)$, $\delta(u) = \delta(v)$ i $u[i]\hat{R}v[i]$ za $1 \leq i \leq \delta(u)$, onda važi i $u\hat{R}v$. Kongruentno zatvorenje određuje klase ekvivalencije elemenata skupa T.

Primer 4.3 *Neka je skup termova T jednak $\{x, y, z, f(x), f(z)\}$ i neka je relacija R zadata sledećom tabelom:*

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

Relacija R^* (ekvivalencijsko zatvorenje relacije R) opisana je tabelom:

R^*	x	y	z	$f(x)$	$f(z)$
x	**1**	1	**1**	0	0
y	**1**	**1**	1	0	0
z	**1**	**1**	**1**	0	0
$f(x)$	0	0	0	**1**	0
$f(z)$	0	0	0	0	**1**

Relacija $\hat{R}$ (kongruentno zatvorenje relacije R) opisana je tabelom:

$\hat{R}$	x	y	z	$f(x)$	$f(z)$
x	1	1	1	0	0
y	1	1	1	0	0
z	1	1	1	0	0
$f(x)$	0	0	0	1	**1**
$f(z)$	0	0	0	**1**	1

Iz svake klase ekvivalencije određene kongruentnim zatvorenjem može se odabrati njen predstavnik. Neka $\nu(u)$ označava predstavnika klase ekvivalencije kojoj pripada element u. Naredna teorema govori o odnosu deduktivnog izvođenja (koje se oslanja na aksiome jednakosti), logičke posledice (sematničke prirode) i odnosa predstavnika klasa ekvivalencije u kongruentnom zatvorenju (dokaz videti u [18]).

Teorema 4.4 *Neka je E skup baznih jednakosti, T skup termova zatvoren za podtermove*[6] *koji sadrži sve termove iz E. Tada za svaka dva terma s i t iz T i za kongruentno zatvorenje relacije $=$ (za relaciju $\hat{=}$) u čistoj teoriji jednakosti važi:*

$$E \vdash s = t \quad \textit{ako i samo ako} \quad E \models s = t \quad \textit{ako i samo ako} \quad \nu(s) \hat{=} \nu(t) \ .$$

Postoji više algoritama za izračunanje kongruentnog zatvorenja i njihovih varijanti [55, 65, 12]. Izračunavanje kongruentnog zatvorenja moguće je u vremenu $O(n \log n)$ (gde je n broj jednakosti i ima najviše n različitih termova), pri čemu se koristi i prostor $O(n \log n)$ [6]. Za dodatne varijante algoritma za kongruentno zatvorenje videti [6, 5, 37].

Nelson–Openov algoritam za određivanje kongruentnog zatvorenja [55, 12] za skup jednakosti E i skup termova T prikazan je na slici 4.1.

Lista $use(s)$, koja se koristi u algoritmu, sadrži skup svih termova iz T čiji je jedan od neposrednih argumenata term s. Dakle, skup elemenata liste $use(s)$ jednak je skupu $\{v \in T \mid \exists i : v[i] = s \}$.

Procedura $MakeUse$ je jednostavna i ovde nije definisana. U okviru nje, za svaki term t iz početnog skupa termova određuje se lista $use(t)$ i pamti uređeni par $(t, use(t))$. Početni skup termova T mora da sadrži sve termove iz E (gde je E dati skup jednakosti) i sve njihove podtermove. Za Nelson–Openov algoritam karakteristično je, dakle, da skup termova koji se obrađuju mora da bude poznat unapred.

Glavna funkcija (Nelson–Open) obrađuje jednu po jednu jednakost iz liste E. Operacija $union$ spaja dve klase ekvivalencije, a $find$ vraća kanonskog predstavnika klase ekvivalencije (tj. za zadati element određuje njegovu klasu ekvivalencije i vraća njenog kanonskog predstavnika). Ključna procedura algoritma je $Merge$, koja spaja dve klase ekvivalencije i propagira spajanje svim termovima koji sadrže upravo spojene termove ili termove koji su sa njima u istoj klasi (tj. ispituje elemente skupova P_u i P_v). Za dva takva terma (iz skupova P_u i P_v) proverava se da li su oni već u istoj klasi ekvivalencije (korišćenjem operacije $find$) i, ako nisu, proverava se (funkcijom $Congruent$) da li treba da budu u istoj klasi. Ako treba, onda se vrši objedinjavanje i njihovih klasa ekvivalencije funkcijom $Merge$.

Operacija $find$ može se implementirati koristeći parove $(t, find(t))$ koji za svaki obrađeni term sadrže kanonskog predstavnika klase ekvivalencije kojoj pripadaju. U tom pristupu, nema eksplicitnog memorisanja klasa ekvivalencija, pronalaženje kanonskog predstavnika je jednostavno i efikasno, ali

[6] Kažemo da je skup termova S *zatvoren za podtermove* ako za svaki term t iz S svi podtermovi terma t takođe pripadaju skupu S.

Algoritam: Nelson–Open

Ulaz: Skup jednakosti E i skup termova T
Izlaz: Kongruentno zatvorenje za E (reprezentovano strukturom $find$)

1. Izvršiti $MakeUse(T)$.
2. Za svaku jednakost $s = t$ iz E uraditi:

   Ako je $find(s) \neq find(t)$, onda izvršiti $Merge(s, t)$.

Funkcija: $Merge$

Ulaz: Par termova (u, v)
Izlaz: Ažurirana struktura $find$ nakon spajanja klasa za u i v

1. Neka je $P_u = \bigcup \{use(u') \mid find(u') = find(u)\}$.
2. Neka je $P_v = \bigcup \{use(v') \mid find(v') = find(v)\}$.
3. Izvršiti $union(u, v)$.
4. Za svaki term t_1 iz P_u:

   Za svaki term t_2 iz P_v:

   Ako je $find(t_1) \neq find(t_2)$ a važi $Congruent(t_1, t_2)$, onda izvršiti $Merge(t_1, t_2)$.

Funkcija: $Congruent$

Ulaz: Par termova (u, v)
Izlaz: $true$ ako su u i v kongruentni termovi, $false$ inače

1. Ako je $\lambda(u) \neq \lambda(v)$ vratiti $false$.
2. Ako je $\delta(u) \neq \delta(v)$ vratiti $false$.
3. Za svako i od 1 do $\delta(u)$:

   Ako je $find(u[i]) \neq find(v[i])$, onda vratiti $false$.
4. Vratiti $true$.

Slika 4.1: Pseudokôd Nelson–Openovog algoritma

je nešto složenije izvršavanje operacije $union$. Klase ekvivalencija moguće je memorisati i kao uređene parove (c, C) gde je C tekuća lista svih termova u toj klasi, a c njen kanonski predstavnik; u tom pristupu ne postoji struktura koja neposredno odgovara operaciji $find$, već se ona izračunava na osnovu činjenice da za svaki element s iz C, važi $find(s) = c$. Na osnovu konvencije, pri određivanju unije dve klase ekvivalencije C_1 i C_2, za kanonskog predstavnika nove klase uzima se kanonski predstavnik klase C_2. U pomenutoj reprezentaciji, operacija $union$ nad elementima s i t redom iz klasa reprezentovanih sa (c_1, C_1) i (c_2, C_2) zamenila bi te dve klase novom klasom reprezentovanom sa $(c_2, C_1 \cup C_2)$. U oba slučaja, ukoliko term t nije u zadatom, polaznom skupu termova, funkcija $find$ vraća sâm taj term. Operacije $find$ i $union$ mogu se implementirati i efikasnije [70].

Lako se dokazuje da se navedena procedura zaustavlja (jer se broj klasa ekvivalencija smanjuje svakim pozivanjem procedure $Merge$). Naredna teorema tvrdi da algoritam Nelson–Open generiše kongruentno zatvorenu kolekciju klasa ekvivalencija termova (dokaz videti u [55, 12]).

Teorema 4.5 (Korektnost procedure Nelson–Open) *Neka je E skup baznih jednakosti i T skup termova koji je zatvoren za podtermove i sadrži sve termove iz E. Nelson–Openov algoritam se zaustavlja i nakon njegovog zaustavljanja za svaka dva terma s i t iz T i za kongruentno zatvorenje relacije $=$ (relaciju $\hat{=}$) važi*

$$find(s) = find(t) \quad \textit{ako i samo ako} \quad \nu(s) \hat{=} \nu(t) \ .$$

Na osnovu teorema 4.4 i 4.5 sledi da za skup baznih jednakosti u čistoj teoriji jednakosti važi $E \vdash s = t$ ako i samo ako važi $find(s) = find(t)$.

Prosečno vreme izvršavanja Nelson–Openove procedure, zasnovane na efikasnim rešenjima za operacije $find$ i $union$ [70], je $O(n \log n)$, gde je n broj jednakosti u početnom skupu [55].

Nelson–Openova procedura za određivanje kongruentnog zatvorenja može se iskoristiti i kao procedura odlučivanja za univerzalno kvantifikovani fragment teorije jednakosti. Neka je $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{A}$ formula teorije jednakosti za koju treba dokazati da je teorema i neka formula $\mathcal{A}$ nema ni kvantifikatora ni slobodnih promenljivih sem, eventualno, promenljivih $x_1, x_2, \ldots, x_n$. Dovoljno je dokazati da formula $\neg(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{A}$ nije zadovoljiva u teoriji jednakosti, tj. da je nezadovoljiva formula $(\exists x_1)(\exists x_2)\ldots(\exists x_n)\neg\mathcal{A}$. Formula $\neg\mathcal{A}$ može se transformisati u disjunktivnu normalnu formu — neka je $\neg\mathcal{A} \equiv \mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_m$, gde su formule $\mathcal{A}_i$ $(i = 1, \ldots, m)$ konjunkcije literala. Da bi se pokazalo da je formula $(\forall x_1)(\forall x_2)\ldots(\forall x_n)\mathcal{A}$ teorema, dovoljno je dokazati da je formula $(\exists x_1)(\exists x_2)\ldots(\exists x_n)(\mathcal{A}_1 \vee \mathcal{A}_2 \vee \ldots \vee \mathcal{A}_m)$ nezadovoljiva, tj. dovoljno je dokazati da je svaka od formula $(\exists x_1)(\exists x_2)\ldots(\exists x_n)\mathcal{A}_i$ $(i = 1, \ldots, m)$ nezadovoljiva. Da bi se dokazalo da formula teorije jednakosti oblika $(\exists x_1)(\exists x_2)\ldots(\exists x_n)\mathcal{B}$ nije zadovoljiva (formula $\mathcal{B}$ sadrži literale oblika $t_1 = t_2$ i literale oblika $\neg(t_1 = t_2)$), algoritam za kongruentno zatvorenje može se iskoristiti na sledeći način: algoritam se primenjuje za sve jednakosti (to je skup E) i za sve termove i sve podtermove iz formule $\mathcal{B}$, uključujući i one iz nejednakosti (to je skup T); nakon primene algoritma, svaki term se zamenjuje

predstavnikom svoje klase ekvivalencije (generisane algoritmom), tj. vrši se *normalizacija*; ako, nakon normalizacije, u formuli postoji literal oblika $\neg(t = t)$, onda formula $(\exists x_1)(\exists x_2)\ldots(\exists x_n)\mathcal{B}$ nije zadovoljiva. Ovakom primenom Nelson–Openovog algoritma, egzistencijalno kvantifikovane varijable tretiraju se, praktično, kao konstante. Primetimo da, slično kao i Furije–Mockinova procedura, opisana procedura, zasnovana na Nelson–Openovom algoritmu, ne generiše formalni dokaz u okviru nekog deduktivnog sistema, već je ona samo procedura za „proveravanje" da li je neka formula teorema univerzalnog fragmenta čiste teorije jednakosti.

Primer 4.4 *Dokažimo da je u teoriji jednakosti (sa signaturom koja uključuje funkcijski simbol f arnosti 1) naredna formula teorema:*

$$(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow f(x) = f(z)) \ .$$

Dokažimo da formula

$$(\exists x)(\exists y)(\exists z)\neg(x = y \wedge y = z \Rightarrow f(x) = f(z)) \ ,$$

tj. formula

$$(\exists x)(\exists y)(\exists z)(x = y \wedge y = z \wedge \neg(f(x) = f(z))) \ ,$$

nije zadovoljiva. Skup literala koji se ispituje je $\{x = y, y = z, \neg(f(x) = f(z))\}$.

Primenimo Nelson–Openov algoritam za kongruentno zatvorenje na skup jednakosti $\{x = y, y = z\}$ i na skup termova $\{x, y, z, f(x), f(z)\}$. Inicijalno, svaki od termova iz skupa $\{x, y, z, f(x), f(z)\}$ čini posebnu klasu ekvivalencije (i za svaki od njih važi $find(t) = t$). Inicijalno, važi $use(x) = \{f(x)\}$, $use(y) = \{\}$, $use(z) = \{f(z)\}$, $use(f(x)) = \{\}$ i $use(f(z)) = \{\}$. U glavnoj funkciji, Nelson–Open, ulazi se u petlju i najpre obrađuje jednakost $x = y$. Važi $find(x) \neq find(y)$, pa se poziva funkcija $Merge$ za par (x, y). Za argument u jednak x i za argument v jednak y, određuje se skup P_u jednak $\{f(x)\}$ i skup P_v jednak $\{\}$. Pozivom $union(u, v)$ spajaju se klase ekvivalencija za termove x i y i za kanonskog predstavnika novodobijene klase uzima se vrednost y (pa će biti $find(x) = y$ i $find(y) = y$). Skup P_v je prazan, pa se ne ulazi u dvostruku for petlju i funkcija $Merge$ završava rad. Nakon toga, u glavnoj funkciji obrađuje se jednakost $y = z$. Važi $find(y) \neq find(z)$, pa se poziva funkcija $Merge$ za par (y, z). Za argument u jednak y i za argument v jednak z, određuje se skup P_u jednak $\{f(x)\}$ i skup P_v jednak $\{f(z)\}$. Pozivom $union(u, v)$ spajaju se klase ekvivalencija za termove y i z i za kanonskog predstavnika novodobijene klase uzima se vrednost $find(z)$, tj. vrednost z (pa će biti i $find(x) = z$). U dvostrukoj for petlji, za vrednost t_1 jednaku $f(x)$ i vrednost t_2 jednaku $f(z)$, utvrđuje se da važi $find(t_1) \neq find(t_2)$ (jer je $find(f(x)) = f(x)$ i $find(f(z)) = f(z)$) i poziva funkcija $Congruent$ (sa argumentima $f(x)$ i $f(z)$). U funkciji $Congruent$ utvrđuje se da važi $\lambda(u) = \lambda(v)$ (jer je $\lambda(f(x)) = f$ i $\lambda(f(z)) = f$) i da važi $\delta(u) = \delta(v)$ (jer je $\delta(f(x)) = 1$ i $\delta(f(z)) = 1$). Dodatno, važi i $find(u[1]) = find(v[1])$ (jer je $find(x) = find(z) = z$), pa funkcija $Congruent$ vraća $true$. U funkciji $Merge$ se onda rekurzivno poziva

$Merge$ — za vrednost u jednaku $f(x)$ i vrednost v jednaku $f(z)$. Pozivom funkcije $union$ za ove dve vrednosti spajaju se klase ekvivalencija za termove $f(x)$ i $f(z)$ i za kanonskog predstavnika novodobijene klase uzima se vrednost $f(z)$ (pa će biti $find(f(x)) = f(z)$ i $find(f(z)) = f(z)$). Skupovi P_u i P_v su prazni, pa se ne ulazi u dvostruku for petlju i funkcija $Merge$ završava rad, kao i funkcija $Merge$ iz koje je ona bila pozvana. Nakon toga i glavna funkcija (Nelson–Open) završava rad i trenutno stanje ($find(x) = find(y) = find(z) = z$ i $find(f(x)) = find(f(z)) = f(z)$) daje dve klase ekvivalencije sa izabranim predstavnicima. Ti predstavnici se koriste za normalizaciju (svih) nejednakosti u polaznom skupu literala, čime se dobija literal $\neg(f(z) = f(z))$ odakle sledi da formula $(\exists x)(\exists y)(\exists z)(x = y \wedge y = z \wedge \neg(f(x) = f(z)))$ nije zadovoljiva, odnosno da je formula $(\forall x)(\forall y)(\forall z)(x = y \wedge y = z \Rightarrow f(x) = f(z))$ teorema čiste teorije jednakosti.

Zadaci

Zadatak 99 *Pokazati, koristeći Nelson–Openov algoritam, da je naredna formula teorema čiste teorije jednakosti:*

(a) $(\forall x)(\forall y)(x = y \Rightarrow f(f(x)) = f(f(y)))$
(b) $(\forall x)(f(f(f(x))) = x \wedge f(f(f(f(f(x))))) = x \Rightarrow f(x) = x)$
(c) $(\forall x)(x = f(x) \Rightarrow x = f(f(f(f(f(x))))))$

Zadatak 100 *Data je formula*

$$(\forall x)(\forall y)(y = f(x) \vee (\forall x)(x = f(y) \vee y = f(f(x)))) \ .$$

Dokazati da ona nije teorema čiste teorije jednakosti:
(a) koristeći teoremu 3.50;
(b) primenom Nelson–Openovog algoritma.

4.4 Sažetak

Pojam odlučivosti teorije može se definisati neformalno (intuitivno) ili formalno, pri čemu vezu ova dva pristupa čini Čerčova teza (poglavlje 4.2). Intuitivna definicija kaže da je teorija odlučiva ako postoji efektivni postupak koji za svaku formulu može da utvrdi da li ona jeste ili nije teorema date teorije. Formalno, teorija je odlučiva ako je njen skup teorema rekurzivan skup (poglavlje 4.1). Postoji više metoda za dokazivanje odlučivosti neke teorije (poglavlje 4.3). Jedan od tih metoda je metod eliminacije kvantora koji pored dokaza odlučivosti teorije, daje i proceduru odlučivanja za nju. Primer takve procedure je Furije–Mockinova procedura za teoriju gustih uređenih Abelovih grupa bez krajnjih tačaka (poglavlje 4.3.1). Postoje i drugi tipovi procedura odlučivanja, a jedan od njih je Nelson–Openova procedura odlučivanja za univerzalno kvantifikovan fragment čiste teorije jednakosti (poglavlje 4.3.2).

Dodatak A

Složenost izračunavanja

Razvrstavanje problema odlučivanja (problema koji mogu da imaju samo odgovore *da* i *ne*) na odlučive i neodlučive je polazna osnova, ali je za razne primene i previše gruba. Na primer, u kontekstu pitanja odlučivosti teorija može se, za neodlučive teorije, govoriti o stepenu nerazrešivosti. S druge strane, za odlučive teorije važno je, pogotovu iz perspektive automatskog dokazivanja teorema, pitanje složenosti pojedinih procedura odlučivanja za konkretnu teoriju. Pojam složenosti obično se vezuje za Tjuringovu mašinu (ili neki drugi ekvivalentan formalizam) i opisuje resurse potrebne da bi neki problem bio rešen. Mere resursa izračunavanja koje oslikavaju složenost algoritma su *vreme* (odnosno broj koraka koje izvršava algoritam) i *prostor* (memorijski prostor koji algoritam koristi). Razmatranje složenosti od izuzetne je važnosti za automatsko rezonovanje. Na primer, činjenica da je neka teorija odlučiva nije od velike koristi ukoliko je donja granica potrebnog vremena i prostora previsoka, tj. ako je teorija *praktično* neodlučiva. Pitanje složenosti izračunavanja posebno je dobilo na značaju početkom sedamdesetih godina dvadesetog veka rezultatima Kuka [10]. Više o složenosti izračunavanja videti u [69], knjiga [19] sadrži pregled NP-kompletnih problema, tekst [54] govori o složenosti iz perspektive računarstva i automatskog rezonovanja.

A.1 Klase složenosti

Za dati, specifični odlučiv problem, gornja granica potrebnog vremena i prostora određuje se razmatranjem konkretnog algoritma koji rešava dati problem. Dodatno, da bi se dokazala optimalnost algoritma, potrebno je imati i odgovarajuće donje granice složenosti problema.

Često se algoritam ne izvršava isto za sve ulaze istih veličina, pa je potrebno naći način za opisivanje i poređenje efikasnosti različitih algoritama. *Analiza najgoreg slučaja* zasniva procenu složenosti algoritma u najgorem slučaju (u slučaju za koji se algoritam najduže izvršava ili zahteva najviše memorijskog prostora). Ta procena može da bude varljiva, ali ne postoji bolji opšti način za

poređenje efikasnosti algoritama. Čak i kada bi uvek bilo moguće izračunati prosečno vreme izvršavanja algoritma (odnosno prosečne memorijske zahteve) i takva procena bi često mogla da bude varljiva.

U analizi složenosti algoritma, obično nas najviše interesuje asimptotsko ponašanje i u tome se koristi tzv. *o-notacija*.

Definicija A.1 *Ako postoje pozitivna konstanta c i prirodan broj n_0 takvi da za funkcije f i g nad prirodnim brojevima važi*

$$f(n) \leq c \cdot g(n) \quad \textit{za sve vrednosti } n \textit{ veće od } n_0$$

onda pišemo

$$f = O(g)$$

i čitamo „f je veliko 'o' od g“.

Naglasimo da O nije funkcija — O označava klasu funkcija. Aditivne i multiplikativne konstante ne utiču na klasu kojoj funkcija pripada.

Definicija A.2 *Ako je $T(n)$ vreme izvršavanja algoritma A (čiju veličinu ulaza karakteriše prirodan broj n), ako važi $T = O(g)$, onda kažemo da je algoritam A* vremenske složenosti *(ili* reda*) g i da pripada klasi $O(g)$.*

Analogno se definiše *prostorna složenost* algoritma.

Formalno se pojmovi vremenske i prostorne složenosti izračunavanja definišu u odnosu na Tjuringovu mašinu. Ako je prilikom izračunavanja promenjeno t konfiguracija mašine, onda je t *vreme* tog izračunavanja. *Prostor* izračunavanja je broj polja mašine kojima se pristupa tokom izračunavanja. Tjuringova mašina *prihvata problem u vremenu (prostoru)* $F(n)$, ako za svaku ulaznu vrednost (čija veličina može biti opisana prirodnim brojem n) koju prihvata (tj. za koju je odgovor na problem potvrdan) postoji izračunavanje koje je prihvata u vremenu (prostoru) koje ne prelazi $F(n)$.

Primer A.1 *Algoritam za izračunavanje vrednosti faktorijela prirodnog broja n je vremenske složenosti $O(n)$, algoritam bubble-sort za sortiranje n elemenata je vremenske složenosti $O(n^2)$, algoritam merge-sort za sortiranje n elemenata je vremenske složenosti $O(n \log n)$, algoritam za ispitivanje zadovoljivosti iskazne formule nad n slova, zasnovan na istinitosnim tablicama je vremenske složenosti $O(2^n)$.*

A.2 NP-kompletnost

Problem odlučivanja (problem za koji su mogući odgovori samo *da* i *ne*) smatra se efikasno rešivim ako postoji algoritam koji rešava problem za sve njegove instance u broju koraka koji je polinomijalno ograničen veličinom ulazne instance, pri čemu se podrazumeva „tradicionalni“ model izračunavanja tj. sekvencijalni, deterministički model (kao što je deterministička Tjuringova mašina (DTM) ili UR-mašina). Smatramo da problemi koji nisu u ovoj klasi nisu efikasno rešivi.

Definicija A.3 *Za problem odlučivanja sa ulaznom vrednošću n kažemo da je polinomijalne vremenske složenosti ako je njegovo vreme izvršavanja* $O(P(n))$ *gde je* $P(n)$ *polinom po* n*. Klasu polinomijalnih algoritama označavamo sa* P*.*

Primer A.2 *Problem izračunavanja vrednosti faktorijela prirodnog broja pripada klasi* P*.*

Nedeterministički algoritam (opisan, na primer, u formalizmu nedeterminističke Tjuringove mašine (NTM)) može u svojim koracima da nedeterministički bira između dva moguća, različita puta za nastavak rada koristeći tzv. *nd-izbore*. Kažemo da nedeterministički algoritam rešava problem odlučivanja ako važi: za zadatu ulaznu vrednost x, postoji niz nd-izbora takav da vodi prihvatanju te vrednosti u polinomijalnom (po veličini ulaza) vremenu ako x pripada skupu svih ulaznih vrednosti za koje je odgovor na problem potvrdan (za više detalja videti, na primer, [14, 74, 45]).

Definicija A.4 *Klasu svih problema odlučivanja za koje postoje nedeterministički algoritmi čije je vreme izvršavanja polinomijalno (po veličini ulaza) zovemo klasa* NP*.*

Klasu NP možemo neformalno da opišemo i na sledeći način: ako neki problem odlučivanja može da se predstavi u vidu najviše eksponencijalno mnogo instanci (po veličini ulaza) i ako za bilo koju instancu za koju je odgovor potvrdan problem može da bude rešen u polinomijalnom vremenu, onda kažemo da taj problem pripada klasi NP. Vreme rešavanja instanci za koje je odgovor na problem negativan nije relevantan za klasu NP. Nije relevantno čak ni to da li se rešavanje zaustavlja za te instance. Međutim, kako se rešavanje problema zaustavlja za sve instance za koje je odgovor potvrdan i to u vremenu ograničnom vrednošću konkretnog polinoma, to znači da se sistematskim proveravanjem može utvrditi da li neka instanca pripada ili ne pripada skupu instanci za koje je odgovor potvrdan. Odatle sledi da svaki problem koji pripada klasi NP mora da bude rekurzivan.

Očigledno, važi P $\subseteq$ NP, ali se još uvek ne zna da li važi P = NP. Ako bi se pokazalo da neki problem iz klase NP nema polinomijalno rešenje, onda bi to značilo da ne važi P = NP. Ako neki problem iz klase NP ima polinomijalno rešenje, onda to još ne znači da P = NP.

Primer A.3 *Problem ispitivanja zadovoljivosti logičkih iskaza (*SAT*) pripada klasi* NP*, a ne zna se da li pripada klasi* P*.*

Za probleme iz posebne potklase klase NP (to je klasa NP-kompletnih problema) važi da ako neki od njih ima polinomijalno rešenje, onda važi P = NP. NP-kompletni problemi su „najteži“ problemi u klasi NP. Okvir za definisanje ovog pojma je pojam *svodljivosti*. Kažemo da se skup A (odnosno problem za koji je odgovor potvrdan za elemente skupa A i samo za njih) može *više-jedan* svesti na skup B (odnosno odgovarajući problem) i pišemo $A \leq_m B$ ako postoji funkcija f takva da može da bude izračunata u polinomijalnom vremenu i

ima svojstvo $w \in A$ ako i samo ako je $f(w) \in B$. Intuitivno, algoritam za problem B može biti iskorišćen za rešavanje problema A sa određenim dodatnim vremenom i prostorom potrebnim za svođenje problema.

Definicija A.5 *Za problem X kažemo da je* NP-težak problem *ako je svaki* NP *problem u polinomijalnom vremenu svodljiv na X.*

Definicija A.6 *Za problem X kažemo da je* NP*-kompletan problem ako pripada klasi* NP *i ako je* NP*-težak.*

Opštije, ako problem A pripada klasi $\mathcal{C}$ i ako je svaki problem iz klase $\mathcal{C}$ svodljiv u polinomijalnom vremenu na A, onda za problem A kažemo da je $\mathcal{C}$-kompletan.

Teorema A.1 *Ako bilo koji* NP*-težak problem pripada klasi* P*, onda važi* P=NP.

Dokaz: Neka je problem X NP-težak. To znači da se proizvoljan problem Y iz klase NP može svesti na njega u polinomijalnom vremenu. Ako bi problem X pripadao klasi P, to bi značilo da za njega postoji polinomijalno rešenje, a odatle bi sledilo da postoji polinomijalno rešenje i za problem Y, tj. i problem Y bi pripadao klasi P. Problem Y je proizvoljan problem Y iz klase NP, pa bi iz $X \in$ P sledilo P=NP. □

Na osnovu navedene teoreme, da bi se dokazalo da je P=NP, dovoljno je dokazati za jedan NP-kompletan problem da pripada klasi P. Potrebno je, dakle, razmatrati neki pogodan NP-kompletan problem. Veoma je teško direktno sledeći definiciju dokazati za neki problem da je NP-kompletan. Naredna teorema omogućava jednostavnije dokazivanje da je neki problem NP-kompletan.

Teorema A.2 *Problem X je* NP*-kompletan ako:*

- *X pripada klasi* NP*;*
- *Y je polinomijalno svodljiv na X, gde je Y neki* NP*-kompletan problem.*

Dokaz: Kako X pripada klasi NP, dovoljno je dokazati da je on NP-težak.

Ako je Y NP-kompletan problem, to znači da se proizvoljan problem Z iz klase NP može svesti na problem Y u polinomijalnom vremenu. To dalje znači da se proizvoljan problem Z iz klase NP može u polinomijalnom vremenu svesti i na problem X, jer je Y polinomijalno svodljiv na X, a kompozicija dva polinomijalna svođenja je ponovo polinomijalno svođenje. Dakle, problem X je NP-težak, što je i trebalo dokazati. □

Navedena teorema omogućava utvrđivanje da je neki problem NP-kompletan, ako je za neki drugi već poznato da je NP-kompletan. Međutim, postavlja se pitanje da li uopšte postoji ijedan NP-kompletan problem. Stiven Kuk prvi je, 1971. godine, dokazao (neposredno, koristeći formalizam Tjuringove mašine) da postoje NP-kompletni problemi[1] i to njegovo tvrđenje jedan je od najznačajnijih rezultata teorijskog računarstva (za dokaz narednog tvrđenja videti [10]).

Teorema A.3 (Kukova teorema) *Problem* SAT *(problem ispitivanja zadovoljivosti logičkih iskaza) je* NP*-kompletan.*

Neposredna posledica Kukove teoreme je tvrđenje:

$$\text{P=NP ako i samo ako SAT} \in \text{P}\ .$$

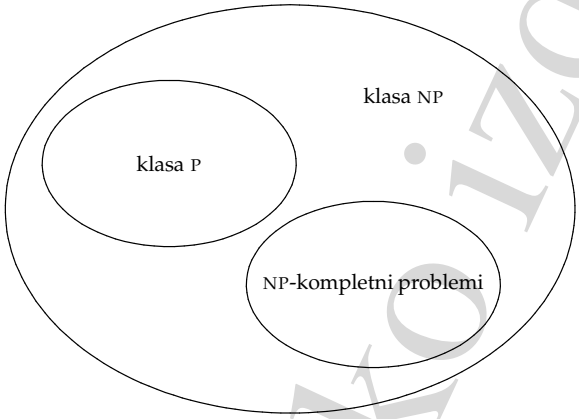
Primer A.4 *Zahvaljujući teoremama A.2 i A.3 može se, na primer, dokazati da su sledeći problemi* NP*-kompletni:*

- *3-*SAT *problem (*SAT *problem u kojem su sve klauze dužine 3);*
- *3-obojivost (ispitivanje da li postoji pridruživanje tri različite boje čvorovima grafa, takvo da je svakom čvoru pridružena neka boja, a da su susednim čvorovima pridružene različite boje);*
- *pokrivač grana (ispitivanje da li postoji podskup D skupa čvorova grafa takav da D ima manje od k elemenata i da svaka grana grafa sadrži bar jedan čvor iz D);*
- *dominirajući skup (ispitivanje da li postoji podskup D skupa čvorova grafa takav da D ima manje od k elemenata i da je svaki čvor grafa ili u D ili je susedan nekom čvoru iz D);*
- *problem klika (ispitivanje da li postoji potpun podgraf G grafa takav da G ima bar k čvorova);*
- *Hamiltonov ciklus (ispitivanje da li graf sadrži prost ciklus koji sadrži svaki čvor grafa tačno jednom);*
- *Hamiltonov put (ispitivanje da li graf sadrži prost put koji sadrži svaki čvor grafa tačno jednom);*
- *problem trgovačkog putnika (ispitivanje da li težinski potpun graf sadrži Hamiltonov ciklus sa zbirom težina grana manjim od zadate vrednosti).*

Koristeći Kukovu teoremu i tehnike svođenja, u godinama koje su sledile za mnoge probleme je dokazano da su NP-kompletni [19]. Postojala je nada da je za neki od njih moguće dokazati da nema polinomijalnog rešenja, što bi bio

[1] Kuk je prvi dokazao i da postoje P-kompletni problemi (jedan od njih je CVP — problem vrednosti kola).

dokaz za tvrđenje P $\neq$ NP. Sa druge strane, ukoliko bi se za neki NP-kompletan problem dokazalo da ima polinomijalno rešenje, to bi značilo da važi P=NP. Ni za jedan NP-kompletan problem, međutim, još uvek nije dokazano niti da ima niti da nema polinomijalno rešenje. Rasprostranjeno je uverenje da važi P $\neq$ NP. Samo malobrojni istraživači veruju da važi P = NP. Postoje i mišljenja da je tvrđenje P = NP neodlučivo u matematičkim teorijama koje se koriste za njegovo ispitivanje. Ukoliko bi se pokazalo da važi P = NP, onda bi region klase P pokrio čitav region klase NP. Ne zna se da li važi P = NP, ali je poznato da postoje problemi koji su izvan klase NP (i, time, naravno i izvan klase P). Postoje i problemi koji su u klasi NP, ali nisu NP-kompletni. Trenutno dominantno uverenje o odnosu klasa P i NP ilustrovano je na slici A.1.



Slika A.1: Klase P i NP

Tokom poslednje decenije, pored pokušaja da se dokaže da ne važi P = NP, radi se i na ispitivanju raspodela najtežih problema u pojedinim klasama NP-kompletnih problema (videti poglavlje A.3). Naime, nisu sve instance NP-kompletnih problema podjednako teške i važno je utvrditi koje su najteže i šta ih to čini najtežim.

A.3 Problem SAT i fazna promena

Kao što je rečeno, problem iskazne zadovoljivosti (SAT) jedan je od tipičnih NP-kompletnih problema. Duboko razumevanje prirode SAT problema od suštinske je važnosti za razumevanje prirode klase NP. Za sada se ne zna da li za NP-kompletne probleme postoje polinomijalna rešenja (tj. ne zna se da li važi P=NP), ali nije teško naslutiti da ne zahteva svaka instanca (primerak) NP-kompletnog problema jednako vreme izračunavanja. Na primer, lako se može konstruisati iskazna formula nad skupom od N iskaznih slova koja je u konjunktivnoj normalnoj formi i čiju je zadovoljivost trivijalno ispitati (npr. takva je formula $p_1 \wedge p_2 \wedge \ldots \wedge p_N$). Opštije, formule u konjuktivnoj normalnoj formi

sa malo klauza (u odnosu na broj promenljivih) su slabo ograničene i relativno jednostavne za svaku proceduru odlučivanja za iskaznu logiku (jer postoji mnogo zadovoljavajućih valuacija); formule sa mnogo klauza (u odnosu na broj promenljivih) su jako ograničene, pa je relativno lako pokazati da su nezadovoljive. Da bi se razumelo šta NP kompletne probleme čini teškim, potrebno je znati koje su instance tog problema najteže. Dodatno, prilikom konstrukcije algoritma za rešavanje nekog NP kompletnog problema potrebno je algoritam ispitivati (i porediti sa drugim algoritmima) upravo na najtežim instancama problema. Dakle, u vezi sa zadovoljivošću iskaznih formula postavljaju se sledeća važna pitanja na koja sâmi metodi za ispitivanje zadovoljivosti ne mogu da odgovore:

- Kakva je distribucija (raspodela) zadovoljivih iskaznih formula i da li za određene klase iskaznih formula možemo da procenimo udeo zadovoljivih formula samo na osnovu njihovih sintaksnih karakteristika?
- Da li je ispitivanje zadovoljivosti jednako teško za sve iskazne formule? Ako nije, za koje je formule najteže ispitati zadovoljivost?
- Da li su za različite metode jednaki ili ne skupovi iskaznih formula za koje je ispitivanje zadovoljivosti najzahtevnije (u smislu potrebnog vremena)?

Sa motivacijom u navedenim pitanjima, tokom poslednje decenije dvadesetog veka takozvana *fazna promena* za mnoge NP-kompletne probleme postala je predmet mnogih i teorijskih i eksperimentalnih istraživanja. Uopšteno govoreći, fazna promena je ponašanje neke karakteristike skupova instanci problema, karakteristike koja prelazi iz oblasti u kojoj dominira jedna vrednost u oblast u kojoj dominira neka druga vrednost. Za skupove instanci SAT problema ta karakteristika je procenat zadovoljivih formula, a te dve vrednosti su 100% i 0%. Među prvim radovima o faznoj promeni bili su znameniti radovi [9] i [52], koji se odnose na faznu promenu upravo u SAT problemu.

U izučavanju fazne promene u SAT problemima, pažnju ćemo usredsrediti na iskazne formule u konjunktivnoj normalnoj formi i u nastavku ćemo pod SAT problemom smatrati problem ovog oblika. Sa $M(N, L)$ označavaćemo skup iskaznih formula koje se sastoje od L klauza nad skupom od N iskaznih slova i koje zadovoljavaju neka dodatna sintaksna svojstva (npr. sve klauze su im iste dužine, ili ne sadrže višestruka pojavljivanja iste klauze; različite takve skupove obeležavamo koristeći i indekse: M_1, M_2, ...). Posebno, sa k-SAT označavamo klasu SAT problema koje čine iskazne formule u konjunktivnoj normalnoj formi i čije su sve klauze dužine k. Sa sat označavamo *funkciju zadovoljivosti* koja odgovara procentu zadovoljivih formula: $sat(M(N, L))$ je procenat zadovoljivih formula u skupu $M(N, L)$. Primetimo da za svaku fiksiranu vrednost N važi da, ako se ne dozvoljavaju višestruka pojavljivanja literala u klauzama niti višestruka pojavljivanja klauza u formulama, onda ima konačno mnogo formula u skupu $M(N, L)$, pa konačno mnogo ima i onih zadovoljivih i onih nezadovoljivih. Za prebrojiv skup promenljivih ima besko-

načno ali prebrojivo mnogo iskaznih formula (ponovo takvih da se ne dozvoljavaju višestruka pojavljivanja literala u klauzama niti višestruka pojavljivanja klauza u formulama) i beskonačno ali prebrojivo mnogo onih iskaznih formula koje su zadovoljive, kao i onih koje su nezadovoljive.

Većina SAT eksperimenata izvodi se na sledeći način: za neko N i za vrednosti L/N koje se povećavaju za neku konstantnu vrednost, slučajno se generiše veliki broj formula, instanci nekog SAT problema, tj. slučajno se bira veliki broj elemenata skupa $M(N, L)$; za velike brojeve takvih instanci, procenat zadovoljivih formula aproksimira funkciju zadovoljivosti $sat(M(N, L))$. Obično se ne proverava da li se neka formula pojavljuje više nego jednom. Eksperimentalni rezultati (nad skupovima instanci SAT problema sa različitim sintaksnim ograničenjima) sugerišu da u SAT problemima postoji fazna promena između zadovoljivosti i nezadovoljivosti kada se odnos L/N povećava. Za različite tipove skupova $M(N, L)$, veruje se da postoji kritična vrednost c_0 za odnos L/N, koju zovemo *prelomna tačka* ili *tačka fazne promene* takva da važi:

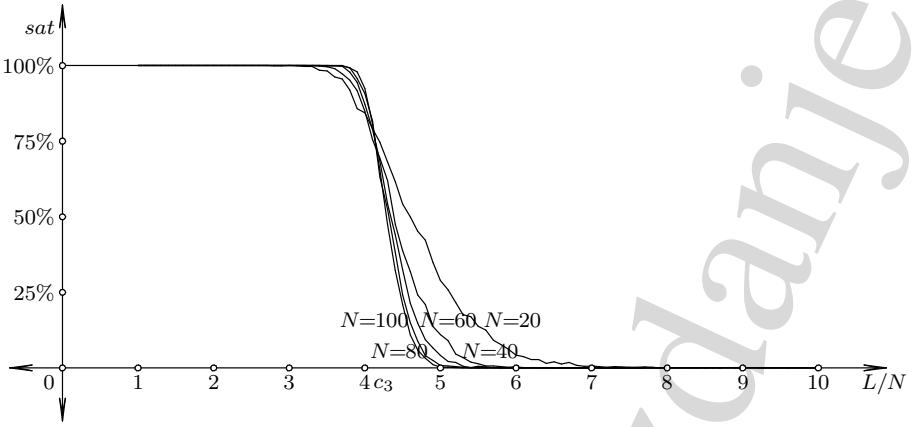
$$\lim_{N\to\infty} sat(M(N, [cN])) = \begin{cases} 100\%, & \text{za } c < c_0 \\ 0\%, & \text{za } c > c_0 \end{cases}$$

Za većinu skupova instanci SAT problema $M(N, L)$ može se pokazati da funkcija $sat(M(N, L))$ strogo opada kada vrednost L raste, kao i da, za fiskirano N, važi $\lim_{L\to\infty} sat(M(N, L)) = 0\%$. Dodatno, ako prelomna tačka postoji, ona je jedinstvena (za jedan tip SAT problema). Do sada ni za jedan tip SAT problema nije teorijski određena prelomna tačka, pa čak ni dokazano da ona postoji (sa jedinim izuzetkom koji čini problem 2-SAT). Dokazano je da postoji region fazne promene za k-SAT probleme koji se sužava kada raste broj iskaznih varijabli, ali to još uvek ne znači da postoji tačka fazne promene [17]. Prelomne tačke mogu biti (i najčešće jesu) različite za različite tipove SAT problema.

Za fiksiran model M, prelomna tačka (ako postoji) jednaka je vrednosti kojoj, kada $N \to \infty$, konvergiraju vrednosti L/N u kojima je p (gde je p bilo koja vrednost između 0% i 100%) zadovoljivih formula iz skupa $M(N, L)$. Ovo svojstvo koristi se za eksperimentalno aproksimiranje prelomnih tačaka.

Eksperimentalni rezultati sugerišu i da je u prelomnoj tački približno jednak procenat zadovoljivih formula za sve velike vrednosti N (pri čemu taj procenat zavisi od konkretnog modela) [40, 20] (videti sliku A.2). Neke sintaksne restrikcije (npr. uslov da se jedna iskazna promenljiva u jednoj klauzi ne pojavljuje i u pozitivnoj i u negativnoj formi) ne utiču na vrednost prelomne tačke [34].

Eksperimenti pokazuju i da u svim SAT problemima postoji tipičan obrazac *jednostavno-teško-jednostavno* kada se vrednost L/N povećava. Zaista, za male vrednosti L/N, problemi su veoma slabo ograničeni i relativno jednostavni za svaku proceduru odlučivanja za iskaznu logiku (jer postoji mnogo zadovoljavajućih valuacija); za velike vrednosti L/N, problemi su veoma jako ograničeni, pa je relativno lako pokazati da su oni nezadovoljivi. Interesantno je da su najteže instance SAT problema za sve procedure odlučivanja upravo instance koje se nalaze u regionu fazne promene (videti sliku A.3). Sve poznate procedure odlučivanja za iskaznu logiku su eksponencijalne složenosti u



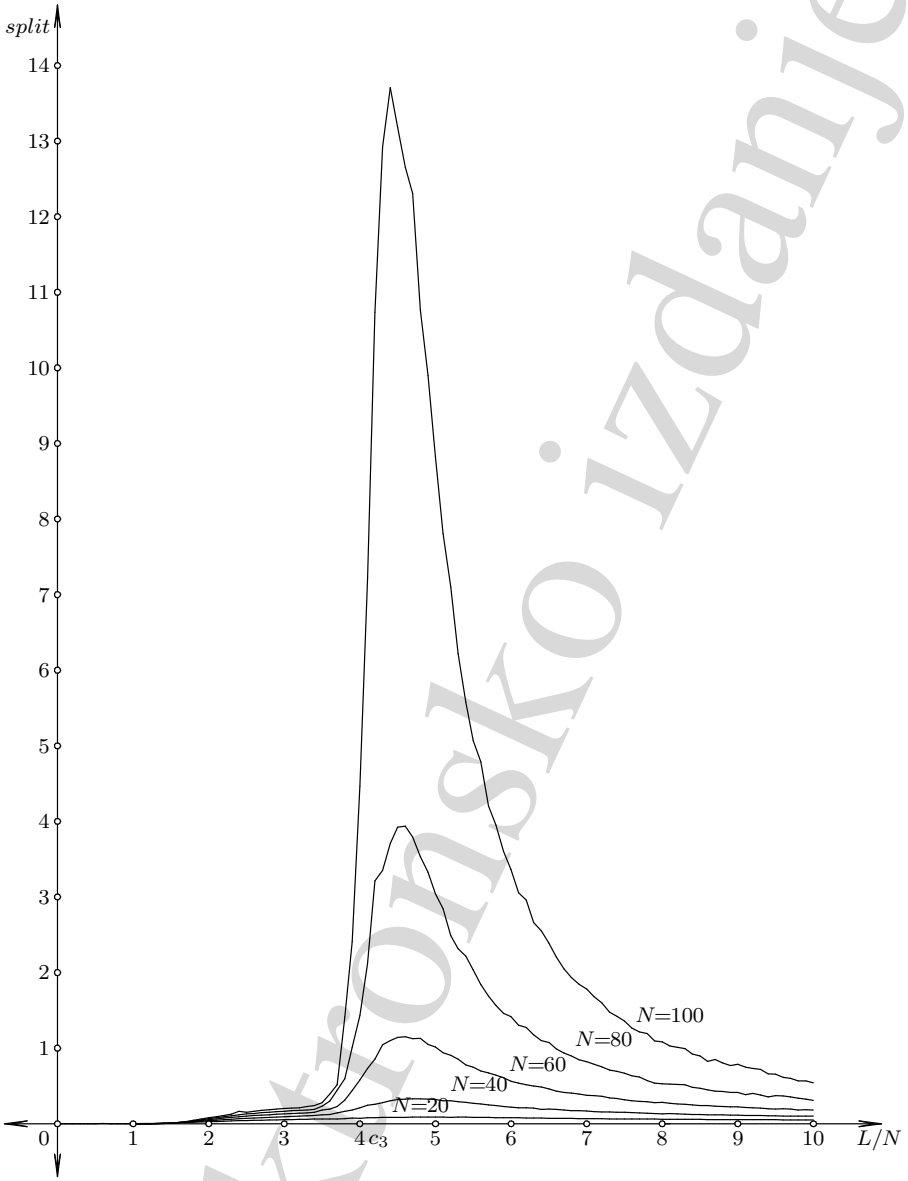
Slika A.2: Eksperimentalna aproksimacija funkcije zadovoljivosti za 3-SAT problem za $N = 20$, $N = 40$, $N = 60$, $N = 80$ i $N = 100$; sa c_3 označena je prelomna tačka

najgorem slučaju (obično složenosti $O(2^{(N/K)})$, gde je N broj promenljivih, a K konstanta koja zavisi od konkretne procedure), ali nisu sve instance SAT problema za njih podjednako teške.

Jedan od najviše izučavanih modela za slučajno generisanje instanci SAT problema je slučajni k-SAT model (model sa fiksnom dužinom klauza). U ovom modelu, za date vrednosti N i L, instanca slučajne k-SAT formule se određuje slučajnim generisanjem L klauza dužine k. Svaka klauza se određuje slučajnim biranjem k različitih elemenata iz skupa od N iskaznih varijabli i, za svaki od njih, dodavanjem negacije sa verovatnoćom 0.5 [52]. Poznato je da je k-SAT NP-kompletan problem za prirodne brojeve k takve da je $k > 2$. Postoji polinomijalna procedura odlučivanja za 2-SAT problem (tj. 2-SAT $\in P$), ali i za ovaj problem postoji fazna promena kao za k-SAT probleme za $k > 2$. Dokazano je (teorijski) da je prelomna tačka za 2-SAT problem jednaka 1 [24]. Za slučajni 3-SAT problem teorijski je dokazano da je prelomna tačka (ako postoji) između vrednosti 3.003 i 4.87 [36], a eksperimentalno je locirana kao vrednost $L/N \approx 4.25$ [11]. Za slučajni 4-SAT problem, prelomna tačka je aproksimirana kao $L/N \approx 9.76$ [20]. Dokazano je da je za slučajni k-SAT problem prelomna tačka (ako postoji) jednaka $2^k \ln 2 - O(k)$ [2].

Neki od modela sa promenljivom dužinom klauza su model sa konstantnom verovatnoćom [29], slučajni mešoviti SAT model [20], $(2 + p)$-SAT model [53, 1] i GS-SAT model [30].

Fazna promena za SAT probleme govori nam o nekim od suštinskih svojstava problema zadovoljivosti. Eksperimentalni rezultati nam sugerišu kakva je distribucija zadovoljivih formula u zavisnosti od pogodno izabranog parametra (parametra L/N). Dodatno, eksperimentalni rezultati pokazuju da za razne klase SAT problema postoje kritične tačke u kojima su problemi najteži i



Slika A.3: Eksperimentalna aproksimacija složenosti izračunavanja za 3-SAT problem za $N = 20$, $N = 40$, $N = 60$, $N = 80$ i $N = 100$ za DPLL proceduru (kao mera složenosti uzet je broj primena *split* pravila)

to za sve do sada poznate metode za ispitivanje zadovoljivosti. Različite algoritme smisleno je ispitivati i porediti upravo na tim formulama.

A.4 Značajne klase problema

Sa NTIME($F(n)$) označava se klasa problema koje nedeterministička Tjuringova mašina prihvata u vremenu $F(n)$. Sa NSPACE($F(n)$) označava se klasa problema koje nedeterministička Tjuringova mašina prihvata u prostoru $F(n)$. Sa DTIME($F(n)$) (DSPACE($F(n)$) označava se klasa problema koje deterministička Tjuringova mašina prihvata u vremenu (prostoru) $F(n)$ (npr. DTIME($2^{O(n)}$) označava uniju skupova DTIME(2^{cn}) za sve konstante c). Klasa $O(G(n)^{O(1)})$ (klasa funkcija koje su ograničene odozgo nekom polinomijalnom funkcijom od G) označava se sa $poly(G(n))$. Od posebne su važnosti sledeće klase problema:

$$\begin{aligned} \text{P} &= \text{DTIME}(poly(n)) \\ \text{NP} &= \text{NTIME}(poly(n)) \\ \text{PSPACE} &= \text{DSPACE}(poly(n)) \\ \text{DLOG} &= \text{DSPACE}(\log(n)) \\ \text{NLOG} &= \text{NSPACE}(\log(n)) \end{aligned}$$

Između ostalog, može se dokazati da važi [54, 57]:

$$\begin{aligned} \text{P} &\subseteq \text{NP} \\ \text{NP} &\subseteq \text{PSPACE} \\ \text{DTIME}(T(n)) &\subseteq \text{NTIME}(T(n)) \\ \text{NTIME}(T(n)) &\subseteq \text{DTIME}(2^{O(T(n))}) \\ \text{DSPACE}(S(n)) &\subseteq \text{NSPACE}(S(n)) \\ \text{NSPACE}(S(n)) &\subseteq \text{DSPACE}(S(n)^2) \\ \text{NTIME}(T(n)) &\subseteq \text{DSPACE}(T(n)) \\ \text{DTIME}(T(n)) &\subseteq \text{DSPACE}(T(n)/\log T(n)) \\ \text{NSPACE}(S(n)) &\subseteq \text{DTIME}(2^{O(S(n))}) \end{aligned}$$

Između ostalih, još uvek su otvorena sledeća pitanja:

$$\begin{aligned} \text{P} &\stackrel{?}{=} \text{NP} \\ \text{P} &\stackrel{?}{=} \text{PSPACE} \\ \text{DLOG} &\stackrel{?}{=} \text{NLOG} \end{aligned}$$

Kao što je rečeno, problem SAT (problem ispitivanja zadovoljivosti iskazne formule) je NP-kompletan. Naglasimo da to ne znači i da je problem ispitivanja *nezadovoljivosti* iskazne formule (problem UNSAT) NP-kompletan. Problem UNSAT pripada klasi co-NP — klasa co-NP je klasa problema čije su negacije problemi iz klase NP. Otvoreno je pitanje da li je problem UNSAT NP-kompletan i da li su klase NP i co-NP jednake. Može se dokazati sledeće: ako postoji problem X takav da je on NP-kompletan i da pripada klasi co-NP, onda važi NP = co-NP [14].

A.5 Složenost teorija

Tabela A.4 prikazuje rezultate o složenosti (kompleksnosti) nekoliko teorija (više detalja videti u [69]). $\mathcal{C}_{lower}$ označava klasu problema koje je moguće svesti na ispitivanje dokazivosti rečenice date teorije (sva svođenja su ili polinomijalno–vremenskog ili logaritamsko–prostornog tipa). $\mathcal{C}_{upper}$ označava klasu za koju je dokazano da joj data teorija pripada.

Teorija	$\mathcal{C}_{lower}$	$\mathcal{C}_{upper}$
jednakost	NSPACE$(\sqrt{n})$	DSPACE$(n \log n)$
N sa sledbenikom	NSPACE(n)	DSPACE(n^2)
N sa sabiranjem	NTIME(2^{2^n})	DSPACE$(2^{2^{O(n)}})$
N sa množenjem	NTIME$(2^{2^{2^n}})$	DSPACE$(2^{2^{2^{O(n)}}})$
R sa sabiranjem	NTIME(2^n)	DSPACE$(2^{O(n)})$
R sa sabiranjem i množenjem	NTIME(2^n)	DSPACE$(2^{O(n^2)})$
konačne Abelove grupe	NTIME(2^{2^n})	DSPACE$(2^{2^{O(n)}})$

Slika A.4: Kompleksnost nekih teorija prvog reda

Iz tabele se vidi da su navedene teorije eksponencijalne ili supereksponencijalne složenosti. Isto važi za veliku većinu netrivijalnih teorija. Važno je, pogotovu sa aspekta automatskog dokazivanja teorema, i razmatranje veze složenosti teorije i odgovarajućih procedura odlučivanja. Kažemo da teorija $\mathcal{T}$ ima *inherentnu složenost* $f(n)$ ako za svaku proceduru odlučivanja P za tu teoriju postoji beskonačno mnogo rečenica ϕ takvih da P zahteva više od $f(|\phi|)$ koraka za ispitivanje da li važi $\phi \in \mathcal{T}$.

A.6 Sažetak

Za odlučive probleme veoma je važno pitanje složenosti njihovih procedura odlučivanja. Poglavlje A.1 sadrži osnovne definicije koje se odnose na složenost izračunavanja. Ako za neki problem odlučivanja postoji algoritam polinomijalne složenosti, onda kažemo da je on efikasno rešiv i pripada klasi P. Ako za neki problem postoji nedeterministički automat koji nakon polinomijalnog broja nd-izbora može da u polinomijalnom vremenu ispita da li je instanca problema rešenje ili ne, onda on pripada klasi NP. NP-kompletni problemi su „najteži“ problemi u klasi NP. SAT problem je prvi problem za koji je dokazano da je NP-kompletan (A.2). Pitanje P$\stackrel{?}{=}$NP je najveće otvoreno pitanje teorijskog računarstva, a verovatno i matematike uopšte. U okviru jednog NP-kompletnog problema, kao što je SAT, nisu sve instance (nad istim brojem iskaznih promenljivih) nužno podjednako teške za rešavanje i o tome govori tzv. fenomen fazne promene (poglavlje A.3). Pored klasa P i NP, postoji još klasa složenosti veoma važnih u računarstvu (poglavlje A.4). Odnosi između nekih od njih nisu poznati. Od posebne važnosti za automatsko rezonovanje je istraživanje složenosti odlučivih teorija i složenosti njihovih procedura odlučivanja (poglavlje A.5).

Dodatak B

Matematička logika i zasnivanje matematike i računarstva

Filozofija matematike bavi se pitanjima koja se mogu okarakterisati kao metafizička: šta je to (matematička) istina, da li matematika opisuje fizičku stvarnost, šta je prihvatljiv koncept dokaza, iz kojeg dela matematike proizilaze svi ostali itd.

Značenje matematičkih formula i pojam matematičke istine nisu za sve matematičare isti. Koncepti matematičke istine oduvek su se menjali i još uvek se menjaju uporedo sa razvojem matematike. Matematika uvek napreduje u dva smera: naviše — tražeći nove informacije (ili nove „istine“) i naniže — tražeći svoje korene.

Većina matematičko-filozofskih pravaca počela je da se razvija u prvoj polovini dvadesetog veka u vreme reforme i novog utemeljivanja matematike. U to vreme, različitosti u matematičko-filozofskim gledanjima bile su često veoma oštre, dok se danas većina matematičkih pravaca smatra jednako legitimnim. U istoriji zasnivanja matematike istaknuta mesta imaju Hilbertov program i Gedelove teoreme.

B.1 Hilbertov program i Gedelove teoreme

Hilbertov rad na polju zasnivanja matematike započeo je, početkom devedesetih godina devetnaestog veka, njegovim istraživanjima geometrije koja su 1899. godine krunisana znamenitom knjigom *Grundlagen der Geometrie* („Osnove geometrije“) [27]. Hilbert je verovao da je jedini ispravan način za izgradnju bilo koje naučne discipline njeno rigorozno aksiomatsko zasnivanje. Teorija treba da bude razvijena bez potrebe za intuicijom i treba da omogući uspostavljanje strogih odnosa između osnovnih pojmova, aksioma i teorema. Za aksi-

omatski pristup, po Hilbertovom mišljenju, od ključne važnosti su pitanje nezavisnosti aksioma i, još više, pitanje konzistentnosti (neprotivrečnosti) aksioma. Za geometriju, na primer, konzistentnost može biti dokazana interpretacijom čiji je domen struktura realnih brojeva i time je konzistentnost geometrije svedena na konzistentnost teorije polja realnih brojeva. Konzistentnost teorije polja realnih brojeva, međutim, takođe zahteva aksiomatizaciju i dokaz konzistentnosti. Hilbert je 1900. godine ponudio jednu takvu aksiomatizaciju, ali je ubrzo postalo jasno da pitanje konzistentnosti i dalje nailazi na mnoge teškoće. Hilbert je došao do zaključka da je za konzistentnost teorije realnih brojeva potreban *direktan* dokaz konzistentnosti aritmetike (ne dokaz koji problem svodi na neku drugu teoriju). Problem konstruisanja takvog dokaza Hilbert je izneo kao drugi od dvadeset tri matematička problema kojim se obratio Međunarodnom kongresu matematičara 1900. godine.

Na tragu dugogodišnjeg rada na problemima zasnivanja matematike, Hilbert je 1921. godine izneo nov predlog za zasnivanje klasične matematike, koji će kasnije postati poznat kao *Hilbertov program.* Osnovni zahtevi programa su:

- izgraditi formalnu teoriju $\mathcal{T}$ koja pokriva čitavu matematiku (tj. formalizovati sve matematičke discipline u aksiomatski oblik);
- koristeći Peanovu aritmetiku, dokazati konzistentnost teorije $\mathcal{T}$.

Dokaz konzistentnosti trebalo je izvesti koristeći samo „finitističke (konačne) metode“, što bi trebalo da pruži potreban oslonac i potvrdu klasične matematike, uzdrmane Raselovim i drugim paradoksima[1]. Jedan od ključnih problema za finitističku logiku je kvantifikovanje, koje može da uvede beskonačnost. Vremenom je ponuđeno nekoliko pristupa za finitarnu analizu kvantifikatora. Hilbert svoje shvatanje dozvoljenih, finitističkih (konačnih) metoda nije precizno opisao, a danas se smatra da tom njegovom shvatanju najbolje odgovaraju metode primitivno rekurzivne aritmetike. Hilbert je govorio da u matematici postoji privilegovan deo, elementarna teorija brojeva, koja počiva samo na intuitivnim osnovama konkretnih simbola. Ovi simboli za Hilberta su numerali (videti potpoglavlje B.1.1), koji nemaju značenja, ne reprezentuju apstraktne objekte, ali se oni mogu dopisivati i porediti. Znanje o njihovim svojstvima je potpuno intuitivno. Evo Hilbertovih reči o tome:

> „Kao preduslov za korišćenje logičkih izvođenja i izvođenja logičkih operacija, nešto mora biti već dato našim sredstvima izražavanja, određeni vanlogički konkretni objekti koji su intuitivno prisutni

[1] Znameniti paradoks Rasel je otkrio 1901. godine radeći na svojoj knjizi *Principles of Mathematics* („Principi matematike“). Neka je M skup svih skupova koji ne sadrže sebe same ili, preciznije, skup A je element skupa M ako i samo ako A nije element skupa A. Paradoks je sledeći: ako skup M pripada samom sebi, to znači da on ne pripada samom sebi, a ako ne pripada samom sebi, to znači da on mora da pripada samom sebi. Raselov paradoks pokazao je da su Fregeova i Kantorova naivne teorije skupova kontradiktorne i uzdrmao čitavu tadašnju matematiku. Većina pristupa razrešavanju Raselovog paradoksa usmerena je ka ograničavanju načina na koji mogu biti definisani skupovi.

> kao neposredno iskustvo koje prethodi promišljanju. Ako logičko izvođenje treba da je pouzdano, onda mora biti moguće imati pregled tih objekata u svim njihovim delovima a činjenice da se oni pojavljuju, da su međusobno različiti, da prethode jedan drugom ili su dopisani, su neposredno intuitivne, kao i ti objekti sâmi, kao nešto što ja smatram neophodnim sredstvom matematike i, opštije, svakog naučnog mišljenja, razumevanja i komuniciranja."

Hilbertov program vršio je godinama snažan uticaj na razvoj teorije dokaza, logike, ali i čitave matematike. On je uticao i na Gedela, čije teoreme nepotpunosti su pokazale da je Hilbertov program nemoguće sprovesti. I pored toga, Hilbertov program je i dalje uticao na razvoj matematike, a takozvani relativizovani Hilbertovi programi postali su centralni problemi u teoriji dokaza. U relativizovanom programu traži se svođenje teorija slabijih od čitave klasične matematike na teorije jače nego što je finitistička matematika.

Prva Gedelova teorema tvrdi da ne postoji konzistentna aksiomatska teorija koja pokriva sve istine intuitivne aritmetike (tj. sva tačna tvrđenja o prirodnim brojevima), a druga da se konzistentnost formalnog sistema koji sadrži aritmetiku ne može dokazati sredstvima samog tog sistema i predikatske logike.

Gedelove teoreme odnose se, u principu, na ,,sisteme koji sadrže Peanovu aritmetiku", ali je zapravo dovoljan uslov da sistem sadrži ,,dovoljno aritmetike" da može da izrazi konstrukciju kodiranja koja se koristi u dokazu, dakle — suštinski — samo osnovna svojstva sabiranja i množenja. Gedelove teoreme mogu se odnositi na teorije sa beskonačnim skupom aksioma (kao što je to slučaj sa Peanovom aritmetikom), ali on mora biti rekurzivan. Na primer, teorija čije su aksiome sve rečenice koje su tačne u svakom standardnom modelu aritmetike je potpuna, ali se Gedelova teorema ne može primeniti na nju jer njen skup aksioma nije rekurzivan.

Svoje teoreme nepotpunosti Gedel je prikazao prvi put na naučnom skupu *Druga konferencija o epistemologiji egzaktnih nauka* u Kenigsbergu, 7. septembra 1930. (a publikovao sledeće godine [23]). Na istom skupu, dan kasnije, Hilbert je održao svoje znamenito predavanje (i istovremeno poslednje svoje javno izlaganje) *Logika i razumevanje prirode*, posvećeno očekivanjima od deduktivističkog pristupa, koje je završio rečima ,,Wir muessen wissen. Wir werden wissen" (,,Mi moramo znati. Mi ćemo znati"). Međutim, dan ranije, za ta ista očekivanja Gedel je već nagovestio da su neosnovana. U ta dva dana, dakle, dve epohe u razvoju matematike zamenile su jedna drugu. Uprkos njihovim posledicama, Hilbert je prihvatao Gedelove teoreme i čak ih unapredio i uopštio u godinama koje su sledile. Nakon što su Gedelovi rezultati pokazali da ne može biti apsolutnog dokaza konzistentnosti čitave matematike, pažnja teorije dokaza usmerena je ka relativnim rezultatima — relativnim i u odnosu na sistem u kojem se daje dokaz konzistentnosti i u odnosu na metode dokazivanja koje se koriste. Tako je, na primer, nekoliko godina nakon Gedelovih rezultata, Gencen dokazao (1936) konzistentnost i potpunost aritmetike koristeći transfinitnu indukciju (ni ovaj pristup, međutim, ne omogućava dokazivanje konzistentnosti čitave matematike).

B.1.1 Peanova aritmetika

Peanova aritmetika (u daljem tekstu označavaćemo je sa PA) je teorija prvog reda sa signaturom $\mathcal{L}$ koja sadrži:

- funkcijski simbol 0 (arnosti 0);
- funkcijski simbol $+$ (arnosti 2), koji zapisujemo u infiksnom obliku;
- funkcijski simbol $\cdot$ (arnosti 2), koji zapisujemo u infiksnom obliku;
- funkcijski simbol s (arnosti 1), koji zapisujemo u prefiksnom obliku;
- predikatski simbol $=$ (arnosti 2), koji zapisujemo u infiksnom obliku.

Aksiome Peanove aritmetike su:

- $(\forall x)(\forall y)(\forall z)(x = y \Rightarrow (x = z \Rightarrow y = z))$
- $(\forall x)(\forall y)(x = y \Rightarrow s(x) = s(y))$
- $(\forall x)(\neg(0 = s(x)))$
- $(\forall x)(\forall y)(s(x) = s(y) \Rightarrow x = y)$
- $(\forall x)(x + 0 = x)$
- $(\forall x)(\forall y)(x + s(y) = s(x + y))$
- $(\forall x)(x \cdot 0 = 0)$
- $(\forall x)(\forall y)(x \cdot s(y) = (x \cdot y) + y))$
- $(\Phi(0) \wedge \forall x(\Phi(x) \Rightarrow \Phi(s(x))) \Rightarrow \forall x \Phi(x)$ (indukcijska shema)

Predikatski simboli $<$ i $\leq$ arnosti dva definišu se na sledeći način:

$$\begin{aligned} u < v &= \exists x(u + s(x) = v) \\ u \leq v &= u < v \vee u = v \end{aligned}$$

Numerali su kraće oznake za termove $s(s(s(\ldots(0)\ldots)))$ i definišu se na sledeći način:

$$\begin{aligned} \overline{1} &= s(0) \\ \overline{2} &= s(s(0)) \\ \overline{3} &= s(s(s(0))) \\ &\ldots \end{aligned}$$

Numerali reprezentuju prirodne brojeve i u standardnom modelu Peanove aritmetike (u kojem je domen skup $\mathbf{N}$), term $\bar{n}$ dobija značenje prirodnog broja n.

U okviru Peanove aritmetike može se dokazati da za numerale važe očekivana svojstva (tj. svojstva koja važe za prirodne brojeve). Na primer, važi

$$\overline{n} + \overline{m} = \overline{m} + \overline{n} \, .$$

U daljem tekstu pod formalnom aritmetikom podrazumevaćemo Peanovu aritmetiku u okviru Hilbertovog deduktivnog sistema za logiku prvog reda.

B.1.2 Gedelovo kodiranje

Kao što je rečeno, Gedelove teoreme odnose se na svaku (aksiomatibilnu) teoriju koja sadrži „dovoljno aritmetike" da može da izrazi koncept kodiranja, a za to su, suštinski, potrebna samo osnovna svojstva sabiranja i množenja. Neka je teorija $\mathcal{T}$ (nad signaturom $\mathcal{L}$) teorija koja ispunjava taj uslov. Neka je $\lceil \ \rceil$ (Gedelovo) kodiranje uvedeno kao u poglavlju 4.1 (ili na neki drugi analogan način), s tim što ono kodira termove i formule ne prirodnim brojevima, nego (odgovarajućim) numeralima. Teorija $\mathcal{T}$ je dovoljno izražajna da za numerale i uvedeno kodiranje važe svojstva koja važe za prirodne brojeve i kodiranje prirodnim brojevima. Mogu se definisati sledeći predikatski simboli (sa datim pridruženim značenjem):

$Term(x)$	ako je x kôd nekog terma nad signaturom $\mathcal{L}$
$For(x)$	ako je x kôd neke formule nad signaturom $\mathcal{L}$
$Ded(x, y)$	ako je x kôd dokaza formule čiji je kôd y
$Pr(x)$	ako je x kôd neke teoreme aritmetike, tj. $Pr(x) = \exists y Ded(y, x))$
$Con(\mathrm{PA})$	ako ne postoji broj koji je kôd dokaza kontradikcije, tj. $Con(\mathrm{PA}) = \neg Pr(\lceil 0 = s(0) \rceil)$

$Pr(\lceil \Phi \rceil)$ se može interpretirati kao „formula Φ je dokaziva u $\mathcal{T}$".
$Con(\mathrm{PA})$ se može interpretirati kao „teorija PA je konzistentna".

Pretpostavlja se da teorija $\mathcal{T}$ zadovoljava sledeće uslove[2] za zatvorene formule $\mathcal{A}$ i $\mathcal{B}$ (u daljem tekstu, umesto $\vdash_{\mathcal{T}}$ kraće pišemo $\vdash$):

H1: ako $\vdash \mathcal{A}$, onda $\vdash Pr(\lceil \mathcal{A} \rceil)$;

H2: $\vdash Pr(\lceil \mathcal{A} \rceil) \Rightarrow Pr(\lceil Pr(\lceil \mathcal{A} \rceil) \rceil)$;

H3: $\vdash Pr(\lceil \mathcal{A} \Rightarrow \mathcal{B} \rceil) \Rightarrow (Pr(\lceil \mathcal{A} \rceil) \Rightarrow Pr(\lceil \mathcal{B} \rceil))$.

Takođe se pretpostavlja da je u teoriji $\mathcal{T}$ raspoloživo pravilo *modus ponens* i da se u njoj za bilo koje zatvorene formule $\mathcal{A}$ i $\mathcal{B}$ može dokazati:

D1: $\vdash \bot \Rightarrow \mathcal{A}$;

D2: $\vdash \mathcal{A} \Rightarrow \mathcal{B}$ ako i samo ako $\vdash \neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ i $\vdash \mathcal{A} \Rightarrow \neg\mathcal{B}$ ako i samo ako $\vdash \mathcal{B} \Rightarrow \neg\mathcal{A}$;

[2] Navedeni uslovi su jedna varijanta Hilbert-Bernajs-Lebovih „uslova izvodivosti".

D3: iz $\vdash \mathcal{A} \Rightarrow \mathcal{B}$ i $\vdash \mathcal{B} \Rightarrow \mathcal{C}$ sledi $\vdash \mathcal{A} \Rightarrow \mathcal{C}$;

D4: $\vdash \neg\mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \bot)$;

D5: iz $\vdash \mathcal{A} \Rightarrow (\mathcal{A} \Rightarrow \mathcal{B})$ sledi $\vdash \mathcal{A} \Rightarrow \mathcal{B}$.

Svaka formula teorije $\mathcal{T}$ gedelizacijom dobija svoj jedinstveni broj, kôd (na osnovu kojeg ta formula može jednoznačno da se odredi). Kako je teorija $\mathcal{T}$ dovoljno izražajna da pokriva svojstva prirodnih brojeva (odnosno svojstva numerala), onda je u njoj moguće rezonovati i o (njenim) formulama.

B.1.3 Prva Gedelova teorema o nepotpunosti

Prva Gedelova teorema tvrdi da ne postoji konzistentna aksiomatska teorija koja pokriva sve istine intuitivne aritmetike (tj. sva tačna tvrđenja o prirodnim brojevima). Naime, za svaki efektivno zadat konzistentan aksiomatski sistem koji sadrži aritmetiku postoji neodlučiva zatvorena formula (tj. zatvorena formula Φ takva da ni Φ ni $\neg\Phi$ nisu dokazive u tom sistemu). Štaviše, postoji neodlučiva zatvorena formula koja je tačna u strukturi prirodnih brojeva. Dakle, svaka aksiomatska teorija koja uključuje aritmetiku je ili nekonzistentna ili nepotpuna. Ova teorema predstavlja odgovor na Hilbertovo pitanje da li je aritmetika potpuna, u smislu da je svako tvrđenje o prirodnim brojevima moguće ili dokazati ili opovrgnuti. Jedna neformalna interpretacija prve Gedelove teoreme je da nije moguće izgraditi aksiomatski sistem sposoban da dokaže sve matematičke (ili samo aritmetičke) istine (i nijednu neistinu). Ovaj rezultat bio je porazan za formaliste, ali je ipak ostavljao jednu nadu: možda je moguće konstruisati algoritam koji za datu formulu određuje da li je ona odlučiva ili ne (tj. da li je moguće dokazati nju ili njenu negaciju). Time bi sve neodlučive formule bile zaobiđene. Međutim, nekoliko godina kasnije pokazano je da ni to nije moguće tj. da ne postoji takav algoritam (videti potpoglavlje B.1.5).

Pojednostavljeno govoreći, osnovna ideja dokaza[3] Gedelove prve teoreme o nepotpunosti je konstruisanje, u okviru formalne aritmetike, rečenice Φ=„Ova rečenica ne može biti dokazana“. Takva rečenica je, zapravo, moderna varijanta *paradoksa lažova*[4]. U Gedelovom dokazu pokazuje se da iz konzistentnosti aksiomatskog sistema sledi da ni formula Φ ni formula $\neg\Phi$ nisu dokazive. Dakle, formula Φ je tačna (jer Φ tvrdi da nije dokaziva i to je tačno), a nije dokaziva. Ni dodavanje rečenice Φ u skup aksioma ne bi rešilo problem: postojala bi druga, analogna Gedelova rečenica za tu, proširenu teoriju. Dakle, svaka teorija koja sadrži aritmetiku je ne samo nepotpuna, nego i esencijalno nepotpuna (nijedno njeno konzistentno proširenje nije potpuna teorija).

[3] Data skica dokaza Gedelovih teorema zasnovana je na [50, 51].

[4] *Paradoks lažova*: Neka je $\mathcal{A}$ rečenica „Ova rečenica je netačna“. Važi $\mathcal{A}$ ako i samo ako „Ova rečenica je netačna“ ako i samo ako „$\mathcal{A}$ je netačna“ ako i samo ako nije $\mathcal{A}$, što je kontradikcija.

Lema B.1 (Lema o dijagonalizaciji) *Neka formula $\Psi(x)$ ima kao slobodnu samo promenljivu x. Tada postoji rečenica Φ takva da u teoriji $\mathcal{T}$ važi* $\vdash (\Phi \Leftrightarrow \Psi(\ulcorner\Phi\urcorner))$.

Dokaz: Uvedimo najpre takozvanu funkciju supstitucije $sub(x, y)$. Vrednost $sub(x, y)$ definišemo na sledeći način: ako je x Gedelov kôd neke formule $\mathcal{A}(u, v, w, \ldots)$, onda zamenjujemo sve slobodne promenljive u toj formuli termom y (i dobijamo formulu $\mathcal{A}(y, y, y, \ldots)$), izračunavamo kôd $\overline{n}$ dobijene formule i $sub(x, y)$ dobija vrednost $\overline{n}$. Ako x nije Gedelov kôd neke formule, onda je $sub(x, y) = 0$. Za funkciju sub, za svaku formulu $\mathcal{A}$ i za svaki numeral $\overline{n}$ važi:

$$sub(\ulcorner\mathcal{A}(x)\urcorner, \overline{n}) = \ulcorner\mathcal{A}(\overline{n})\urcorner \ .$$

Neka je $\Delta(x)$ formula $\Psi(sub(x, x))$, neka je $\overline{n} = \ulcorner\Delta(x)\urcorner$ i neka je formula Φ jednaka formuli $\Delta(\overline{n})$. Onda u teoriji $\mathcal{T}$ važi:

$$\begin{aligned}
\Phi &= \Delta(\overline{n}) \\
&= \Psi(sub(\overline{n}, \overline{n})) \\
&= \Psi(sub(\ulcorner\Delta(x)\urcorner, \overline{n})) \\
&= \Psi(\ulcorner\Delta(\overline{n})\urcorner) \\
&= \Psi(\ulcorner\Phi\urcorner)
\end{aligned}$$

odakle sledi $\vdash (\Phi \Leftrightarrow \Psi(\ulcorner\Phi\urcorner))$ (tj. $\vdash (\Phi \Rightarrow \Psi(\ulcorner\Phi\urcorner))$ i $\vdash (\Psi(\ulcorner\Phi\urcorner) \Rightarrow \Phi)$). □

Navedena lema ponekad se naziva lema o samoukazivanju ili lema o fiksnoj tački.

Teorema B.1 (Prva Gedelova teorema o nepotpunosti) *Neka je $\mathcal{T}$ formalna teorija prvog reda koja sadrži Peanovu aritmetiku i neka je rečenica Φ takva da važi* $\vdash (\Phi \Rightarrow \neg Pr(\ulcorner\Phi\urcorner))$ *i* $\vdash (\neg Pr(\ulcorner\Phi\urcorner) \Rightarrow \Phi)$. *Ako je teorija $\mathcal{T}$ konzistentna, onda važi:*

(i) $\nvdash \Phi$

(ii) $\nvdash \neg\Phi$.

Dokaz: Na osnovu leme B.1 postoji takva rečenica Φ (za $\Psi(x) = \neg Pr(x)$).

(i) Pretpostavimo suprotno — pretpostavimo da važi $\vdash \Phi$. Na osnovu osobine H1, iz $\vdash \Phi$ sledi $\vdash Pr(\ulcorner\Phi\urcorner)$. Na osnovu svojstva formule Φ (svojstvo $\vdash (\Phi \Rightarrow \neg Pr(\ulcorner\Phi\urcorner))$), iz $\vdash \Phi$ sledi $\vdash \neg Pr(\ulcorner\Phi\urcorner)$. Kako je teorija $\mathcal{T}$ konzistentna, nemoguće je da važi i $\vdash Pr(\ulcorner\Phi\urcorner)$ i $\vdash \neg Pr(\ulcorner\Phi\urcorner)$, pa sledi da je polazna pretpostavka pogrešna, tj. važi $\nvdash \Phi$.

(ii) Pretpostavimo suprotno — pretpostavimo da važi $\vdash \neg\Phi$. Na osnovu osobine H1, važi $\vdash Pr(\lceil\neg\Phi\rceil)$, tj. $\vdash Pr(\lceil\Phi \Rightarrow \bot\rceil)$, tj. $\vdash Pr(\lceil\Phi \Rightarrow 0 = s(0)\rceil)$. Na osnovu osobine H3 važi $\vdash Pr(\lceil\Phi \Rightarrow 0 = s(0)\rceil) \Rightarrow (Pr(\lceil\Phi\rceil) \Rightarrow Pr(\lceil 0 = s(0)\rceil))$, pa odatle i iz $\vdash Pr(\lceil\Phi \Rightarrow 0 = s(0)\rceil)$, na osnovu pravila MP, sledi $\vdash Pr(\lceil\Phi\rceil) \Rightarrow Pr(\lceil 0 = s(0)\rceil)$. Na osnovu pretpostavke, teorija $\mathcal{T}$ je konzistentna pa je $\vdash Pr(\lceil 0 = s(0)\rceil) \Leftrightarrow \bot$, tj. $\vdash Pr(\lceil 0 = s(0)\rceil) \Leftrightarrow 0 = s(0)$, odakle sledi $\vdash Pr(\lceil\Phi\rceil) \Rightarrow 0 = s(0)$ (tj. $\vdash Pr(\lceil\Phi\rceil) \Rightarrow \bot$) i, dalje, $\vdash \neg Pr(\lceil\Phi\rceil)$. Na osnovu svojstva formule Φ (svojstvo $\vdash (\neg Pr(\lceil\Phi\rceil) \Rightarrow \Phi)$ i osobine D2 važi $\vdash \neg\Phi \Rightarrow Pr(\lceil\Phi\rceil)$), pa iz $\vdash \neg\Phi$ sledi $\vdash Pr(\lceil\Phi\rceil)$. Međutim, kako je teorija $\mathcal{T}$ konzistentna, nemoguće je da važi i $\vdash \neg Pr(\lceil\Phi\rceil)$ i $\vdash Pr(\lceil\Phi\rceil)$, pa sledi da je polazna pretpostavka pogrešna, tj. važi $\nvdash \neg\Phi$.

□

Na osnovu prve Gedelove teoreme sledi da za svaku aksiomatibilnu teoriju $\mathcal{T}$ koja sadrži Peanovu aritmetiku (ili „dovoljno aritmetike“) postoji rečenica Φ takva da ni ona ni njena negacija nisu dokazive (a pri tome je Φ tačna). U dokazu je ta rečenica Φ formula koja tvrdi svoju nedokazivost (a i zaista je nedokaziva). Tvrđenje formule Φ je, u izvesnom smislu, metatvrđenje. Pokazano je, međutim, da postoje i drugačija neodlučiva aritmetička tvrđenja (tvrđenja bliža uobičajenom objektnom nivou). Na primer, Kirbi, Paris i Harington su dokazali 1977. godine da je jedno tvrđenje iz kombinatorike (verzija Remzijeve teoreme) neodlučivo u Peanovoj aritmetici, ali se može dokazati u širem sistemu teorije skupova. Kruskalova teorema o stablima je takođe neodlučiva u Peanovoj aritmetici, ali se može dokazati u teoriji skupova. Goldštajnova teorema je jedno relativno jednostavno tvrđenje o prirodnim brojevima koje je neodlučivo u Peanovoj aritmetici.

Prva Gedelova teorema sledi i iz činjenice da je skup teorema bilo koje formalne teorije rekurzivno nabrojiv, dok skup aritmetičkih istina (skup svih tačnih tvrđenja o prirodnim brojevima) nije rekurzivno nabrojiv. Dakle, ni u jednoj formalnoj teoriji ne mogu se dokazati sve aritmetičke istine.

Neki matematičari shvataju Gedelove teoreme kao dokaz da postoji razlika između onoga što je mehanički dokazivo i onoga što čovek može da utvrdi da je tačno, kao i da ljudska inteligencija ne može biti mehanizovana. Sâm Gedel, kao platonista, verovao je da čovek ima i intuitivan (ne samo izračunljiv) način dolaženja do istine, pa time njegove teoreme ne postavljaju granicu ljudskog znanja.

B.1.4 Druga Gedelova teorema o nepotpunosti

Pitanje konzistentnosti (neprotivrečnosti) formalne aritmetike bilo je za Hilberta fundamentalno, jer se mnoge matematičke teorije oslanjaju na aritmetiku. Pri tome, Hilbert je očekivao finitistički dokaz konzistentnosti aritmetike. Druga Gedelova teorema tvrdi da se konzistentnost formalnog sistema koji sadrži

Peanovu aritmetiku ne može dokazati sredstvima samog tog sistema. Naime, rečenica takvog sistema koja reprezentuje tvrđenje da je taj sistem konzistentan nije dokaziva u njemu samom.

Teorema B.2 (Druga Gedelova teorema o nepotpunosti) *Neka je $\mathcal{T}$ neka formalna teorija prvog reda koja sadrži Peanovu aritmetiku. Ako je teorija $\mathcal{T}$ konzistentna, onda važi $\nvdash Con(\mathcal{T})$.*

Dokaz: Neka je rečenica Φ odabrana kao u dokazu teoreme B.1. Dokazaćemo da važi

$$\vdash \Phi \text{ ako i samo ako } \vdash Con(\mathcal{T})$$

U teoriji $\mathcal{T}$ može se izvesti sledeći dokaz:

1.	$0 = s(0) \Rightarrow \Phi$	(D1)
2.	$Pr(\lceil 0 = s(0) \Rightarrow \Phi \rceil)$	(1,H1)
3.	$Pr(\lceil 0 = s(0) \Rightarrow \Phi \rceil)$ $\Rightarrow (Pr(\lceil 0 = s(0) \rceil) \Rightarrow Pr(\lceil \Phi \rceil))$	(H3)
4.	$Pr(\lceil 0 = s(0) \rceil) \Rightarrow Pr(\lceil \Phi \rceil)$	(2,3,MP)
5.	$\neg Pr(\lceil \Phi \rceil) \Rightarrow \neg Pr(\lceil 0 = s(0) \rceil)$	(4,D2)
6.	$\Phi \Rightarrow \neg Pr(\lceil \Phi \rceil)$	(svojstvo formule Φ)
7.	$\Phi \Rightarrow \neg Pr(\lceil 0 = s(0) \rceil)$	(6,5,D3)
8.	$\Phi \Rightarrow Con(\mathcal{T})$	(7)

Dakle, iz $\vdash \Phi$ sledi $\vdash Con(\mathcal{T})$.

Važi i:

1.	$Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil Pr(\lceil \Phi \rceil) \rceil)$	(H2)
2.	$\Phi \Rightarrow \neg Pr(\lceil \Phi \rceil))$	(svojstvo formule Φ)
3.	$Pr(\lceil \Phi \rceil) \Rightarrow \neg \Phi$	(2,D2)
4.	$Pr(\lceil Pr(\lceil \Phi \rceil) \Rightarrow \neg \Phi \rceil)$	(3,H1)
5.	$Pr(\lceil Pr(\lceil \Phi \rceil) \Rightarrow \neg \Phi \rceil) \Rightarrow$ $(Pr(\lceil Pr(\lceil \Phi \rceil) \rceil) \Rightarrow Pr(\lceil \neg \Phi \rceil))$	(H3)
6.	$Pr(\lceil Pr(\lceil \Phi \rceil) \rceil) \Rightarrow Pr(\lceil \neg \Phi \rceil)$	(4,5,MP)
7.	$Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil \neg \Phi \rceil)$	(1,6,D3)
8.	$\neg \Phi \Rightarrow (\Phi \Rightarrow (0 = s(0)))$	(D4)
9.	$Pr(\lceil \neg \Phi \Rightarrow (\Phi \Rightarrow (0 = s(0))) \rceil)$	(8,H1)
10.	$Pr(\lceil \neg \Phi \Rightarrow (\Phi \Rightarrow (0 = s(0))) \rceil) \Rightarrow$ $(Pr(\lceil \neg \Phi \rceil) \Rightarrow Pr(\lceil \Phi \Rightarrow (0 = s(0)) \rceil))$	(H3)
11.	$Pr(\lceil \neg \Phi \rceil) \Rightarrow Pr(\lceil \Phi \Rightarrow (0 = s(0)) \rceil)$	(9,10,MP)
12.	$Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil \Phi \Rightarrow (0 = s(0)) \rceil)$	(7,11,D3)
13.	$Pr(\lceil \Phi \Rightarrow (0 = s(0)) \rceil) \Rightarrow$ $(Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil 0 = s(0) \rceil))$	(H3)
14.	$Pr(\lceil \Phi \rceil) \Rightarrow (Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil 0 = s(0) \rceil)$	(12,13,D3)
15.	$Pr(\lceil \Phi \rceil) \Rightarrow Pr(\lceil 0 = s(0) \rceil)$	(14,D5)
16.	$\neg Pr(\lceil 0 = s(0) \rceil) \Rightarrow \neg Pr(\lceil \Phi \rceil)$	(15,D2)
17.	$Con(\mathcal{T}) \Rightarrow \neg Pr(\lceil \Phi \rceil)$	(16)
18.	$\neg Pr(\lceil \Phi \rceil) \Rightarrow \Phi$	(svojstvo formule Φ)
19.	$Con(\mathcal{T}) \Rightarrow \Phi$	(17,18,D3)

Dakle, iz $\vdash Con(\mathcal{T})$ sledi $\vdash \Phi$.

Iz prethodne dve implikacije sledi da je formula $Con(\mathcal{T})$ dokaziva u teoriji $\mathcal{T}$ ako i samo ako je dokaziva rečenica Φ. Međutim, na osnovu dokaza teoreme B.1, rečenica Φ nije dokaziva, pa ne važi $\vdash Con(\mathcal{T})$, što je i trebalo dokazati. □

Jedna neformalna interpretacija druge Gedelove teoreme je: ukoliko je moguće dokazati konzistentnost aksiomatskog sistema u okviru njega samog, onda je on nekonzistentan. Dakle, da bi se dokazala konzistentnost sistema $\mathcal{T}$, potrebno je izgraditi i upotrebiti neki sistem $\mathcal{S}$ za dokazivanje konzistentnosti sistema $\mathcal{T}$. Međutim, i takav dokaz nije poptuno prihvatljiv ako konzistentnost sistema $\mathcal{S}$ nije već dokazana (bez korišćenja konzistentnosti sistema $\mathcal{T}$). Konzistentnost Peanove aritmetike ne može biti dokazana u samom tom sistemu, ali može, na primer, biti dokazana u teoriji skupova.

B.1.5 Problem odlučivanja

Problem odlučivanja (nem. *Entscheidungsproblem*) je problem postojanja ili konstruisanja algoritma (pri čemu se misli na formalno definisan koncept algoritma, kao u poglavlju 4.1) koji za proizvoljnu formulu logike prvog reda utvrđuje da li je ona teorema zadate teorije ili nije. Navedeni problem, u određenom smislu seže u prošlost sve do Lajbnica, koji je razmišljao o mehaničkoj napravi sposobnoj da izračunava istinitosnu vrednost logičkih iskaza. U modernom obliku, ovaj problem formulisan je eksplicitno (kao *Entscheidungsproblem*) u Hilbertovoj i Akermanovoj značajnoj knjizi *Grundzuge der Theoretischen Logik* („Osnove teorijske logike“). Hilbert je bio duboko verovao da takav opšti algoritam postoji, tj. da je predikatska logika odlučiva.

Gedelova *teorema o potpunosti* (dokazana 1929. i objavljena 1930. godine) tvrdi da je neka formula teorema predikatskog računa ako i samo ako je tačna u svakoj interpretaciji [22]. To znači da se problem odlučivanja može formulisati u sintaksno-deduktivnoj (ispitivanje da li je formula teorema) ili semantičkoj formi (ispitivanje da li je formula valjana).

Čerč i Tjuring nezavisno jedan od drugoga dali su 1936. godine negativan odgovor na problem odlučivanja. Čerčov negativan odgovor zasnivao se na činjenici da nije odlučivo da li su dva izraza lambda računa ekvivalentna ili ne. Tjuringov dokaz zasnivao se na svođenju na *halting problem*[5]: pretpostavimo da postoji procedura odlučivanja za logiku prvog reda; pitanje da li se zadata Tjuringova mašina zaustavlja može se formulisati kao formula logike prvog reda i na njega se može odgovoriti raspoloživom procedurom; međutim, halting problem je neodlučiv, što znači da je i predikatska logika neodlučiva.

[5] *Halting problem* („problem zaustavljanja“) je problem određivanja da li se za ulaznu vrednost y zaustavlja program sa rednim brojem x (u nekom formalizmu, npr. za UR mašine ili Tjuringove mašine). Za neke konkretne vrednosti x i y ovaj problem može biti rešen, ali je u opštem slučaju neodlučiv. Neodlučivost halting problema dokazao je Tjuring [68].

Rad oba autora je bio pod snažnim uticajem Gedelovih teorema nepotpunosti i posebno pod uticajem ideje kodiranja („gedelizacije“).

Iako ne postoji opšta procedura odlučivanja za predikatsku logiku i za teorije prvog reda, treba naglasiti da postoje procedure odlučivanja za neke teorije prvog reda (nad specifičnom signaturom i sa specifičnim aksiomama). Neke od odlučivih teorija nabrojane su u poglavlju 4.2. Sa druge strane, mnoge teorije prvog reda, uključujući Peanovu aritmetiku su neodlučive (što takođe sledi iz Tjuringovog dokaza).

B.2 Matematičko-filozofski pravci

Po ključnim pitanjima, pitanjima matematičke istinitosti i matematičke stvarnosti, dominantni matematički pogledi od dvadesetog veka su *platonizam*, *formalizam* i *intuicionizam*. Njima treba dodati i *logicizam*, koji je bio aktuelan početkom dvadesetog veka. Logicizam tvrdi da se čitava matematika može svesti na logiku i da sve matematičke discipline proizilaze iz logike. Sve matematičke teoreme su istovremeno logičke istine. Jedan od prvih zagovornika ovog pravca bio je Frege, koji je kasnije promenio svoje stavove, suočen sa Raselovim paradoksom. Ideju logicizma nastavili su da razvijaju Rasel i Vajthed.

B.2.1 Matematički realizam ili platonizam

Platonistička istinitost vezana je za semantiku i značenje formula. Značenje matematičkih formula zasniva se na matematičkim strukturama za koje se veruje da objektivno postoje, nezavisno od ljudskog uma i od stupnja ljudskog znanja. Platonisti smatraju da čovek ne izmišlja matematiku, već je samo otkriva. Termin „platonizam“ koristi se jer je ovo shvatanje slično Platonovom shvatanju „sveta ideja“. U definisanju relevantnih matematičkih struktura (preko kojih se onda definiše značenje formula) prihvata se *a priori* (bar) postojanje strukture prirodnih brojeva (sa svim njenim relevantnim svojstvima). Svako tvrđenje o bilo kojoj (konačnoj ili beskonačnoj) matematičkoj strukturi je tačno ili netačno, ima nedvosmisleno određenu objektivnu istinitosnu vrednost, iako možda čovek ne može da je utvrdi. Za platonistički pristup matematici od temeljnog značaja je teorija modela.

Skup-teoretski platonizam je danas dominantna varijanta platonizma. U skladu sa ovom filozofijom, beskonačni skupovi postoje u nematerijalnom, čisto matematičkom svetu. Primena teorije beskonačnih skupova na konačan svet rađa mnoga pitanja i njihovo razumevanje trebalo bi da vodi dubljem shvatanju problema do kojih dovode Gedelove teoreme o nepotpunosti. Najznačajniji predstavnik ove varijante platonizma je sâm Gedel. Gedel, platonista, svojim teoremama o nepotpunosti raspršio je hilbertovske formalističke nade dokazavši da čak ni o prirodnim brojevima nije moguće sve istine opisati formalnim sistemom. Platonisti prihvataju Gedelove dokaze kao argument da

je matematičko mišljenje suštinski kreativno i da je osnovni smisao matematičkih formula u njihovom značenju, u njihovoj istinitosti.

Mnogi matematičari ne prihvataju za ovaj pravac ime „platonizam“, jer to ime implicira sasvim specifičnu ontologiju koja nije neophodna u svakodnevnoj matematičkoj praksi.

B.2.2 Formalizam

Formalistički pojam istinitosti vezan je za dokazivost — tačno je ono što je dokazivo u okviru nekog deduktivnog sistema i ništa više. Formalisti mogu da prihvate kao istinito neko svojstvo brojeva jedino ako je ono dokazano u okviru nekog strogog aksiomatskog sistema (kao što je Peanova aritmetika). Za formalistički pristup matematici od temeljnog značaja je teorija dokaza.

Formalizam zagovara odvajanje značenja od matematike. Dok platonisti, makar načelno, pokušavaju da matematičkim tvrđenjima opišu matematičku stvarnost, formalisti nisu zainteresovani za tako nešto. Za njih se ne postavlja pitanje „objektivnosti“ deduktivnog sistema koji grade ili koriste, već samo pitanje njegove konzistentnosti. Njihovi sistemi su čisto sintaksno-kombinatorne prirode i nemaju nikakve veze sa bilo kakvom semantikom („formule ne govore ni o čemu, one su samo nizovi simbola“). Zato se često kaže kako formalisti shvataju matematiku kao igru, igru kombinovanja simbola. U ekstremnijem obliku (ne široko prihvaćenom) jedini matematički objekti i jedini predmet istraživanja za formaliste su simboli sâmi. Formalisti su često optuživani da zamenjuju sadržinu matematike igrom formulama bez značenja i da ne žele da obezbede istinu, već samo konzistentnost svojih analiza.

Formalisti odbacuju platonističko vezivanje za određene matematičke strukture kao „misticizam“ jer ne postoji način da se precizno (formalno) utvrde svojstva takvih struktura. S druge strane, platonisti tvrde da slična primedba može da se stavi i formalističkom pristupu jer svako pitanje konzistentnosti deduktivnog sistema koji se koristi zahteva razmatranje sličnog sistema na višem nivou i time, beskonačnu regresiju.

Osnovni problem postavki formalizma je u tome što je mnoštvo stvarnih matematičkih ideja i problema daleko od puke manipulacije nizovima simbola. Mada dokazi iz uobičejene matematičke prakse mogu (ako su korektni), u principu, biti formulisani u terminima formalnog izvođenja, pravila tog izvođenja nisu suštinska sadržina tih dokaza. Formalizam ne daje okvir za razumevanje ljudskog bavljenja matematikom niti okvir za razmatranje primena matematike.

Deduktivizam je rasprostranjen vid formalizma i on zagovara bavljenje relativnom istinom, pre nego apsolutnom. Naime, deduktivizam dozvoljava pridruživanje značenja određenim nizovima simbola; ako su aksiomama pridružena tačna tvrđenja i ako pravila izvođenja čuvaju tačnost, onda su u toj izabranoj interpretaciji sve teoreme tačne. Dakle, formalizam ne mora nužno da bude potpuno lišen matematičkog značenja. Obično je poželjno da postoji interpretacija u kojoj „pravila igre“ važe i u kojoj su formalne teoreme tačne,

tj. da je aksiomatski sistem sugerisan od strane neke druge nauke, neke druge matematičke grane ili od fizičke stvarnosti.

Formalizam je bio u posebnom zamahu krajem devetnaestog i početkom dvadesetog veka kada su Hilbertov program i aksiomatski trend davali nagoveštaje i nadu u potpunost i odlučivost svih bitnih matematičkih teorija. Novi impuls filozofija formalizma dobila je sa razvojem računarstva i algoritmike, čime je logika u bitnoj meri ,,mehanizovana". Najznačajniji predstavnici formalističke (deduktivističke) škole su Hilbert i Tarski.

B.2.3 Intuicionizam i konstruktivizam

Za konstruktivizam (intuicionizam, kao i za ostale varijante konstruktivizma) jedino prihvatljivo matematičko znanje je ono koje se može dobiti kao rezultat efektivnih, eksplicitnih mentalnih konstrukcija. Ne može se tvrditi postojanje nekog objekta ako ga nije moguće efektivno konstruisati. Jedino takvo znanje i jedino takvi matematički objekti su dozvoljeni u matematičkoj praksi. Matematički objekti postoje samo u okviru uma matematičara, te je matematičko znanje apsolutno pouzdano. Konstruktivisti ne prihvataju aksiomu izbora niti zakon isključenja trećeg kao legitimnu aksiomu (jer vodi zaključcima tipa ,,da ili ne" pri čemu se ne zna koji od ta dva odgovora može biti konstruisan), pa ne prihvataju ni dokaz svođenjem na protivrečnost (što je jedno od najjačih oružja u svakodnevnoj matematičkoj praksi). Brauer, jedan od najznamenitijih intuicionista, verovao je da se matematika izvodi intuitivno, te da je nezavisna od logike i jezika. Verovao je da se logika zasniva na matematici, a ne matematika na logici. Za intuicionistu, dakle, logicizam nije prihvatljiv.

Smatra se da su prirodni brojevi dati i intuitivni, a da sve ostalo treba da se eksplicitno i konačnim sredstvima konstruiše od strane čoveka. Iako postoji rezerva po pitanju da li su prirodni brojevi zaista intuitivni, najozbiljnija zamerka intuicionizmu je ipak da on zahteva strožiju logiku od one koja se koristi u matematičkoj praksi. Intuicionisti su, u cilju odbrane od ovih kritika, demonstrirali da se veliki broj matematičkih tvrđenja može dokazati i intuicionističkim sredstvima. Na primer, mnoštvo tvrđenja realne analize i drugih matematičkih disciplina može se dokazati u intuicionističkom sistemu, na efektivan način, mada je većina tih dokaza izuzetno komplikovana. I sâm Brauer je priznavao da je intuicionistička matematika (kao preteška) beskorisna za praktične primene i svakodnevnu upotrebu.

U intuicionizmu, pojam ,,eksplicitna konstrukcija" nije uvek bio sasvim jasno definisan i to je bio razlog za kritike. Za rešavanje ovog problema korišćeni su pojmovi Tjuringove mašine ili rekurzivne funkcije, vodeći do ideje da su smislena jedino pitanja vezana za konačne algoritme i da jedino ta matematička pitanja treba da budu razmatrana.

Konstruktivistička logika je mešavina intuicionističkog pogleda na matematiku i formalizma, koja proizvodi (samo) efektivne metode za konstrukciju potrebnih objekata. U konstruktivističkoj logici, dokaz za $\exists x P(x)$ mora da pruži način za konstruisanje objekta c i pokazivanje da važi $P(c)$. Takođe, dokaz za $p \vee q$ mora da pruži dokaz za p ili dokaz za q (tj. nije dovoljno dokazati

$\neg(\neg p \wedge \neg q)$). Jedna od najznačajnijih modernih konstruktivističkih logika (posebno za računarstvo) je konstruktivistička teorija tipova Martina Lefa.

B.3 Zasnivanje računarstva

Matematička logika ima ključnu ulogu u zasnivanju računarstva. Jaki temelji računarstva postavljeni su i pre nego što je napravljen prvi računar. Tu se ne misli samo na intuitivan pojam algoritma i mnoge efektivne algoritme koji su definisani vekovima, već pre svega na formalni pojam izračunljivosti. Formalna izračunljivost (koja je, na osnovu Čerčove teze, ekvivalentna intuitivnoj izračunljivosti) ima svoja ograničenja koja su otkrivena, među prvima, od strane Tjuringa. Naime, *halting* problem je neodlučiv (videti potpoglavlje B.1.5) i to znači da ni za jedan računar (izgrađen na principima današnjih računara) ne postoji i ne može da postoji program koji ispituje da li se proizvoljan program zaustavlja. Nemogućnost odgovaranja na tako fundamentalno pitanje govori o granicama efektivne izračunljivosti, pa time i o granicama svih računara. Teorija izračunljivosti ne ukazuje samo na nemogućnosti rešavanja nekih problema, već i na pojedina rešenja, kao i na klasifikacije rešivih problema u zavisnosti od njihove složenosti. Teorija složenosti izračunavanja, koja se oslanja i na teoriju brojeva i na logiku i na računarstvo, uvodi klase problema i vodi do pitanja da li važi P=NP — najznačajnijeg otvorenog matematičkog pitanja današnjice. Eventualni odgovor na ovo pitanje, bilo potvrdan bilo odrečan, bitno bi uticao na savremeno gledanje na mnoge teorijske i praktične probleme. Na primer, sigurnost gotovo svih savremenih kriptografskih sistema zasnovana je, suštinski, na težini problema faktorizacije prirodnih brojeva i ako bi se pokazalo da važi P=NP, to bi značilo da je za razbijanje većine šifara dovoljno polinomijalno vreme (koje bi, zbog veličine ulaza, i dalje bilo veoma dugo).

Koncepti matematičke logike nisu važni samo u pitanjima mogućnosti nekog izračunavanja, već i u razumevanju i opisivanju svakog mogućeg izračunavanja. Horova logika je jedan od formalnih sistema za opisivanje programskih jezika i njihove semantike [25], kao i dokazivanje korektnosti programa. U Horovoj logici, u okvirima logike prvog reda i za zadatu signaturu, definiše se jednostavan programski jezik na sledeći način:

- promenljive programskog jezika su iste kao i promenljive jezika logike; izrazi u programskom jeziku su termovi nad datom signaturom;
- postoji naredba dodele ($:=$);
- postoji prazna naredba (;);
- dozvoljeno je nadovezivanje naredbi i raspoložive su kontrolne strukture $while$ i $if - then - else$.

U ovom sistemu, u terminima *preuslova* i *posleuslova*, moguće je formalno dokazavati korektnost algoritama napisanih na konstruisanom programskom

jeziku. Ovaj, kao i drugi slični pristupi, predstavlja korak ka automatizovanom dokazivanju korektnosti algoritama. Do danas je od strane automatskih dokazivača teorema formalno verifikovano mnogo softverskih i hardverskih sistema. Štaviše, automatski dokazivači teorema već su uspeli da reše i važna otvorena matematička pitanja. Na primer, jedan automatski dokazivač teorema (autora Larija Vosa i njegovih saradnika) dokazao je, 1997. godine, šezdeset godina otvorenu, Robinsovu hipotezu. Tako računarstvo i automatsko rezonovanje danas vraćaju svoj dug matematici i logici.

Što se tiče logičkog pravca, računarstvo je, prirodno, najbliže konstruktivističkoj logici. U računarstvu nije dovoljno dokazati da postoji program koji rešava neki problem, već je potrebno efektivno konstruisati takav program (i dokazati njegovu korektnost). Veoma važna za računarsvo je konstruktivistička teorija tipova Martina Lefa, izgrađena tokom sedamdesetih godina dvadesetog veka [46, 47]. Ta logika unifikuje matematiku i računarstvo sledećim načelima: teorema je isto što i skup, a skup je isto što i specifikacija, dokaz teoreme je isto što i element skupa, a element skupa je isto što i program koji zadovoljava specifikaciju. Teorija Martina Lefa omogućava i pogodno dokazivanje korektnosti algoritama, ali i njihovo direktno konstruisanje na osnovu specifikacije. Ovom teorijom brišu se (ako uopšte i postoje) različitosti između matematike i računarstva, a dokazivanje teorema postaje isto što i konstrukcija programa.

B.4 Sažetak

Početkom dvadesetih godina dvadesetog veka Hilbert je izneo program koji poziva na formalističko, aksiomatsko zasnivanje čitave matematike, kao i na dokazivanje konzistentnosti takvog sistema. Desetak godina kasnije Gedel je pokazao da Hilbertov program nije moguće u potpunosti ostvariti. I Hilbertov program i Gedelovi rezultati fundamentalno su uticali na razvoj matematičke logike i matematike uopšte.

Tokom dvadesetog veka matematikom dominiraju tri matematičko-filozofske doktrine: platonizam (pre svega skup-teoretski platonizam), formalizam (pre svega deduktivizam) i konstruktivizam. Nijedna od njih ne zadovoljava u potpunosti sva relevantna filozofska pitanja i potrebe matematičke prakse. Kao rezultat toga, danas se ti pravci smatraju podjednako legitimnim, a krajem dvadesetog i početkom dvadeset i prvog veka većina matematičara je pseudoformalističke orijentacije koja se obično opisuje kao „platonista preko nedelje, formalista vikendom“. Naime, oni u svojoj svakodnevnoj matematičkoj praksi prihvataju objektivno postojanje matematičkih objekata i beskonačnosti, ali kada je reč o filozofskim razmatranjima, onda zauzimaju formalistički stav. Uostalom, teorema o potpunosti predikatskog računa (formula je teorema predikatskog računa ako i samo ako je tačna u svakoj interpretaciji) i teorema o postojanju modela (teorija prvog reda je konzistentna ako i samo ako ima model sa konačnim ili prebrojivim domenom) smanjuju jaz koji je nekad postojao između formalista i anti-formalista. Matematika se obično i podučava

u pseudo-formalističkom maniru. Nema mnogo izgleda da će se pojaviti objedinjeno matematičko gledanje koje potpuno pokriva i smisao matematičkog znanja i njegovu primenu u realnom svetu.

Dodatak C

Biografske beleške

Abel Niels Henrik Abel (1802–1829), norveški matematičar. Nakon studija u Norveškoj, nekoliko godina proveo je u različitim gradovima Evrope. Tokom kratke matematičke karijere, bavio se uglavnom algebrom.

Aristotel Aristotel (384. p.n.e–322. p.n.e.), starogrčki filozof, utemeljivač logike. Dok je Aristotel bio dete, njegov otac živeo je u gradu Pela, gde je radio kao lekar Amintasa III, kralja Makedonije. Tamo se Aristotel sprijateljio sa Filipom, sinom kralja Amintasa. Godine 367. p.n.e. Aristotel je postao član Platonove Akademije u Atini, gde je onda ostao narednih dvadeset godina, najpre kao učenik, a zatim kao nastavnik retorike i dijalektike. U to vreme Akademija je imala jak uticaj, ne samo u naučnom i filozofskom, nego i političkom životu. Aristotel je napustio Akademiju u vreme Platonove smrti (347. p.n.e) i sa grupom naučnika bavio se problemima biologije i zoologije na ostrvima Asos i Lezbos. Godine 343. p.n.e. otišao je na dvor Filipa II (na makedonskom prestolu od 359. p.n.e). Tamo je proveo narednih sedam godina i veruje se da je u tom periodu podučavao Filipovog sina, budućeg Aleksandra Velikog. Filipova podrška Aristotelu da preuzme vođstvo nad atinskom Akademijom (motivisana željom da se utiče na politiku Atine) nije dala rezultate. Godine 335. p.n.e, kao vladar Makedonije i Atine, Aleksandar je omogućio nastavak rada Akademije, ali je u isto vreme poslao u Atinu Aristotela da tamo osnuje drugu školu — Licej. Za razliku od Akademije, na Liceju se izučavao širok spektar oblasti: logika, fizika, astronomija, meteorologija, zoologija, metafizika, teologija, psihologija, politika, ekonomija, etika, retorika, poetika. Za većinu ovih oblasti (od kojih mnoge nisu pre toga bile konstituisane kao naučne oblasti) pažljivo su sastavljani udžbenici i sistematizovane naučne discipline. Nakon smrti Aleksandra Velikog (323. p.n.e), anti-makedonsko raspoloženje nateralo je Aristotela da napusti Atinu i vrati se na poluostrvo Halkidiki gde je bio rođen. Tamo je umro godinu dana kasnije. U Aristotelova dela spadaju knjige koje su objavljene tokom njegovog života (i kasnije izgubljene) i radovi od preko 2000 strana, sakupljeni u 30 knjiga i objavljivani nakon njegove smrti. Većinu tih ma-

terijala Aristotel nije bio imao nameru da objavi, već su oni služili kao materijali za predavače na Liceju. Ovi materijali sadrže mnoge znamenite Aristotelove radove u raznim oblastima, pre svega u filozofiji i logici. Aristotel je verovao da je logika posebna vrsta nauke, koja treba da se proučava pre upuštanja u bilo koju drugu oblast. Za logiku je Aristotel koristio termin „analitika“ (termin „logika“ prvi je uveo Ksenokrat sa atinske Akademije). Aristotel je verovao da logika može da se primeni na sve nauke i da za svaku nauku postoji jedinstven, pogodan aksiomatski sistem. Pridavao je veliki značaj matematici, kao jednoj od tri teorijske nauke (pored, u današnjim terminima, filozofije i teorijske fizike). Iako nije napravio nijedno matematičko otkriće, Aristotelov doprinos razvoju matematike je veliki, pre svega u sistematizovanju deduktivne logike i konstituisanju naučne metodologije koju je onda preneo i na druge oblasti. Smatra se jednim od najvećih filozofa i jednim od četiri najveća logičara svih vremena (pored Fregea, Gedela i Tarskog). Neprocenjiv je njegov uticaj na razvoj nauke i savremenog društva.

Bet Evert Willem Beth (1908–1964), holandski filozof, logičar i matematičar.

Bul George Boole (1815–1864), engleski matematičar. Nije stekao akademska zvanja i bio je praktično samouk. Od 1849. predavao je matematiku na Kvins koledžu u Korku (Irska) i imao reputaciju izvanrednog nastavnika. Pristupao je logici na nov način, svodeći je na jednostavne algebre. To je bio početak rada na algebri koju danas zovemo Bulova algebra i koja se smatra jednim od ključnih koraka u razvoju računarstva. Značajne rezultate Bul je imao i u oblasti diferencijalnih jednačina.

Brauer Luitzen Egbertus Jan Brouwer (1881–1966), holandski matematičar. Predavao je teoriju skupova i teoriju funkcija na univerzitetu u Amsterdamu. Smatra se jednim od osnivača topologije. Još od svoje doktorske teze (1907) suprotstavljao se Hilbertovom formalizmu i Raselovom logicizmu. Propagirao je intuicionističku matematiku i smatra se jednim od njenih najznačajnijih predstavnika. Između 1918. i 1923. objavio je teoriju skupova, teoriju mere i teoriju funkcija, razvijene bez korišćenja pravila isključenja trećeg. Uprkos svojim značajnim rezultatima u topologiji, nikada nije držao predavanja iz topologije, smatrajući da njegovi stari rezultati nisu prihvatljivi sa stanovišta intuicionizma. Bio je čudna osoba, na svojim predavanjima nije dozvoljavao pitanja, uvek je gledao ka tabli i nikad ka studentima.

Čerč Alonzo Church (1903–1995), američki logičar. Bio je profesor matematike na univerzitetu Prinston od 1929. do 1967. kada je postao profesor matematike i filozofije na univerzitetu u Kaliforniji. Njegov rad imao je izuzetan uticaj na razvoj matematičke logike, teorije rekurzije i teorijskog računarstva. Početkom devedesetih, smatran je najvećim živim svetskim logičarem. Njegova najznačajnija dela su Čerčova teorema (1936), koja tvrdi da je aritmetika

neodlučiva i Čerčova teza, koja tvrdi da je efektivna izračunljivost ekvivalentna pojmu rekurzivnih funkcija.

De Morgan Augustus De Morgan (1806–1871), britanski matematičar. Studije je završio na Kembridžu i nakon toga je radio kao profesor u Londonu. Godine 1830. objavio je knjigu *Elementi aritmetike* koja je imala mnogo izdanja. Godine 1833. uveo je termin ,,matematička indukcija" i precizno definisao princip indukcije. U jednom radu iz 1849. prvi je dao geometrijsku interpretaciju kompleksnih brojeva. Shvatao je da je priroda algebre simbolička. Uveo je De Morganove zakone i značajno reformisao dotadašnju matematičku logiku. Među prvima je shvatio nedostatke i ograničenja u izražajnosti aristotelovskih silogizama. Bio je prvi predsednik Londonskog matematičkog društva.

Dejvis Martin Davis (1928–), američki matematičar i logičar. Studirao je pod rukovodstvom Posta i sarađivao sa njim. Doktorirao je na univerzitetu Prinston, pod rukovodstvom Alonza Čerča. Doprineo je rešenju desetog Hilbertovog problema. Njegova knjiga ,,Computability and Unsolvability" (1958) smatra se ,,jednim od nekoliko stvarnih klasika računarstva". Smatra se jednim od od najznačajnijih imena u razvoju automatskog rezonovanja. Od 1965. godine radi na univerzitetu u Njujorku, gde je sada počasni profesor na odseku za računarstvo.

Dževons William Stanley Javons (1835-1882), engleski matematičar, profesor na univerzitetu u Mančesteru. Godine 1870. konstruisao je mehaničku napravu, ,,logički klavir" koji je koristio kao pomoć na svojim predavanjima iz logike i koja je baratala bulovskim identitetima.

Erbran Jacques Herbrand (1908-1931), francuski matematičar. Doktorirao je u Parizu godine 1929, a 1931. počeo da radi u Nemačkoj, sa Fon Nojmanom (John von Neumann) i Emi Neter (Emmy Noether). Njegovi najznačajniji radovi su iz matematičke logike, a bavio se i algebrom i teorijom prstenova. Tragično je izgubio život tokom planinarenja u francuskim Alpima.

Frege Gottlob Frege (1848–1925), nemački matematičar, logičar i filozof. Najveći deo svoje naučne karijere proveo je na univerzitetu u Jeni. Bavio se zasnivanjem matematičke logike i 1879. godine konstruisao prvu varijantu predikatskog računa, veoma sličnu sistemima koji se koriste i danas. Da bi utemeljio svoje poglede na veze matematike i logike, Frege je razvio specifičnu filozofiju jezika, koju mnogi filozofi i dalje smatraju inspirativnom. Nije uspeo da ostvari svoj životni cilj, da pokaže da je čitava matematika svodiva na logiku. Smatra se jednim od četiri najveća logičara svih vremena (pored Aristotela, Gedela i Tarskog).

Furije Jean Baptiste Joseph Fourier (1768–1830), francuski matematičar. Tokom francuske revolucije, aktivno je učestovao u političkom životu i revolucionarnim telima, a 1794. umalo je izbegao giljotinu. Godine 1798. učestovao u Napoleonovoj invaziji na Egipat kao naučni savetnik, a u godinama koje su sledile bio sa Napoleonom i u veoma dobrim i u veoma lošim odnosima. Član francuske Akademije nauka postao je 1817. Najznačajniji radovi su mu u oblasti algebre, mehanike, teorije funkcija i trigonometrijskih redova.

Gedel Kurt Gödel (1906–1978), austrijski matematičar. Rođen je u Austro-Ugarskoj monarhiji, na teritoriji današnje Češke republike. Studirao je, doktorirao i dugo radio na univerzitetu u Beču. Najznačajniji rezultat su mu teoreme o nepotpunosti, koje je objavio 1930. godine. Ove teoreme pokazuju da za svaki aksiomatski sistem koji sadrži aritmetiku postoje tačna tvrđenja koja u okviru njega ne mogu biti ni dokazana ni pobijena. Dodatno, konzistentnost takvog sistema aksioma ne može biti dokazana u okviru njega samog. Ovim rezultatom, koji je verovatno najveći matematički rezultat dvadesetog veka, okončan je dug niz pokušaja da se čitava matematika zasnuje na aksiomama. Ove teoreme nisu uništile osnovnu ideju Hilbertovog formalizma, ali su pokazale njegova ograničenja. Dodatno, one su pokazale da računar nikada neće moći da odgovori na proizvoljno matematičko pitanje. Nakon dolaska Hitlera na vlast i ubistva jednog Gedelovog kolege od strane pripadnika nacional-socialističke partije, Gedel je doživeo nervni slom i već 1934. otišao je u Ameriku (na univerzitet Prinston), gde je ostao do kraja života (uz jedan prekid tokom 1938. i 1939. kada je boravio u Beču). Značajni rezultati su mu i u domenu aksiome izbora i uopštene hipoteze kontinuuma. Krajem života bio je ubeđen da pokušavaju da ga otruju, te je, uporno odbijajući hranu, umro od gladi. Dok je čekao na to da postane državljanin Sjedinjenih Američkih Država otkrio je nekoliko nekonzistentnosti u ustavu ove zemlje. Smatra se jednim od četiri najveća logičara svih vremena (pored Aristotela, Fregea i Tarskog).

Gencen Gerhard Gentzen (1909–1945), nemački matematičar. Radio je kao Hilbertov asistent u Getingenu 1934. godine. Najznačajniji rezultati su mu u logici i zasnivanju matematike. U svom znamenitom radu objavljenom u časopisu *Mathematische Zeitschrift* 1935, Gencen je uveo sistem prirodne dedukcije i račun sekvenata, koji su logiku približili matematičkom rezonovanju više nego što je to bio slučaj sa sistemima Fregea i Hilberta. Sredinom tridesetih godina dvadesetog veka dao je prvi dokaz konzistentnosti formalne aritmetike (zasnovan na korišćenju transfinitnu indukciju). Tokom 1939. i 1941. bio je u vojnoj službi, a od 1942. predavao je na nemačkom univerzitetu u Pragu. Krajem rata biva zarobljen od strane lokalnog stanovništva, a zatim od strane sovjetske armije. Umro je od neuhranjenosti tri meseca kasnije. Prijatelj koji je bio u zatočeništvu s njim, svedočio je kako je Gencen prvih nedelja bio sasvim spokojan, konačno imajući dovoljno vremena da razmišlja o dokazu konzistentnosti za analizu, o veštačkom jeziku i drugim temama koje su ga zanimale.

Gilmor Paul Gilmore, američki matematičar i logičar. Godine 1960. napravio je prvi dokazivač teorema zasnovan na Erbranovoj teoremi. Sada živi u Kanadi, gde je počasni profesor na univerzitetu Britiš Kolumbija (na kojem je i diplomirao, 1949. godine).

Grasman Hermann Grassmann (1809-1877), nemački matematičar. Živeo je u Šćećinu (današnja Poljska) i predavao matematiku u tamošnjoj gimnaziji. Razvio je prvi precizan geometrijski (vektorski) račun slêdeći Lajbnicove ideje. Njegovi matematički radovi nisu bili prihvatani sa pažnjom, uključujući i doktorsku tezu koja je odbijena bez pažljivijeg proučavanja. Razočaran prijemom svojih matematičkih ideja, posvetio se lingvistici, pre svega nemačkoj gramatici i rečniku sanskrta, koji se i danas koristi.

Hilbert David Hilbert (1862–1943), nemački matematičar. Jedan je od najvećih matematičara devetnaestog i dvadesetog veka. Njegovi najznačajniji rezultati su u zasnivanju matematike, geometriji, teoriji brojeva i integralnom računu. Neki od dvadeset i tri problema koje je početkom dvadesetog veka predstavio na svetskom kongresu matematičara i danas predstavljaju veliki izazov. Godine 1921. zasnovao je program (koji se oslanjao na rezultate i razmišljanja od kraja devetnaestog veka) za zasnivanje klasične matematike (koji će kasnije biti nazvan Hilbertov program). Taj program zahteva formalizovanje čitave matematike u aksiomatskoj formi, zajedno sa dokazom da je takva aksiomatizacija konzistentna. Nemogućnost ostvarivanja Hilbertovog programa dokazale su Gedelove teoreme. Uprkos tome, Hilbertov program je nastavio da snažno utiče na razvoj matematike i teorije dokaza (između ostalog, u vidu, takozvanog relativizovanog Hilbertovog programa).

Hintika Kaarlo Jaakko Juhani Hintikka (1929–), finski matematičar. Najznačajniji rezultati su mu u polju distributivnih normalnih formi, semantike mogućih svetova, metoda stabala, beskonačno dubokih logika i induktivnih generalizacija. Sada radi na odseku za filozofiju, univerziteta u Bostonu.

Hor Charles Antony Richard Hoare (Tony Hoare), britanski informatičar. Rođen je u Kolombu (Šri Lanka), a diplomirao na univerzitetu u Oksfordu 1956. godine. Radio je u Oksfordu, zatim na Državnom univerzitetu u Moskvi, na univerzitetu u Belfastu, od 1977. ponovo na univerzitetu u Oksfordu, sve do 1999. kada je prešao u Majkrosoftov centar u Kembridžu. Konstruisao je, 1960. godine, algoritam za sortiranje *quicksort*, jedan od najkorišćenijih algoritama uopšte. Razvio je tzv. Horovu logiku i formalni jezik CSP za specifikovanje konkurentnih procesa. Godine 1980. dobio je Tjuringovu nagradu za „svoje fundamentalne doprinose definiciji i dizajnu programskih jezika“. Poznate su sledeće njegove reči: „Postoje dva puta za konstruisanje dizajna softvera: jedan je napraviti ga tako jednostavnim da očigledno nema nedostataka i drugi — napraviti ga tako komplikovanim tako da nema očiglednih nedostataka.“

Hobs Thomas Hobbes (1588–1679), engleski filozof. Najznačajnije delo mu je *Leviathan* (1651), pisano tokom engleskog građanskog rata. Ova knjiga je jedna od najznačajnijih u istoriji političke filozofije. Verovao je da bez jake kontrole ljudi nužno idu ka ratu i destrukciji.

Horn Alfred Horn (1918–2001), američki algebrista i logičar. Doktorirao je 1947. na univerzitetu u Kaliforniji, gde je proveo čitavu karijeru i radio do 1988. Većina njegovih radova odnosi se na univerzalne algebre. Godine 1951. objavio je rad u kojem se uvode Hornove klauze koje će kasnije postati osnova za logičko programiranje.

Kalmar László Kalmár (1905–1976), mađarski matematičar. Studirao je matematiku na univerzitetu u Budimpešti, a najveći deo karijere proveo je na univerzitetu u Segedinu. Najznačajnije rezultate ostvario je u domenu problema odlučivanja za neke klase formula prvog reda, programskih jezika, automatskog ispravljanja grešaka i veza računarstva i matematičke logike. Bio je član mađarske Akademije nauka od 1949. godine.

Kenig Denes König (1884-1944), mađarski matematičar. Dokazao je tzv. Kenigovu lemu 1924. godine.

Kovalski Robert Kowalski (1941–), američki logičar poljskog porekla. Doktorirao je na univerzitetu u Edinburgu, a sada je počasni profesor na odseku za računarstvo na Imperijal koledžu (London).

Krispius Krispius (280. p.n.e–207. p.n.e), starogrčki filozof.

Kuk Stephen Cook, američki matematičar. Doktorirao je na univerzitetu Harvard 1966. godine. Od 1970. radi na univerzitetu u Torontu, sada kao počasni profesor. Bavi se složenošću izračunavanja i vezama između logike i teorije složenosti. Uveo je pojam NP-kompletnosti 1971. godine. Dobitnik je Tjuringove nagrade za 1982. godinu. Član je američke akademije nauka.

Lajbnic Gottfried Wilhelm Leibnitz (1646–1716), nemački diplomata, filozof, pisac i matematičar. Pre svoje dvadesete godine poznavao je dobro tadašnje udžbenike matematike, filozofije, teologije i prava. Radio je kao diplomata i u Hanoverskoj biblioteci. Najznačajniji matematički radovi su mu u oblasti diferencijalnog računa i mehanike, kao i ideje vezane za matematičku logiku.

Lef Martin Löf (1940–), švedski logičar. Sedamdesetih godina dvadesetog veka utemeljio je novu varijantu konstruktivističke logike, sada poznatu pod nazivom konstruktivistička teorija tipova Martina Lefa. U ovoj znamenitoj teoriji, koja pokušava da objedini matematiku i računarstvo i njihove potrebe,

teorema ima isti status kao skup, a njeni dokazi kao elementi skupa. I specifikacija programa ima isti status kao teorema, a program koji zadovoljava tu specifikaciju ima status dokaza teoreme.

Logman George Logemann, američki matematičar. Doktorirao je na univerzitetu u Njujorku 1965. godine. Zajedno sa Dejvisom i Lovelandom implementirao je početkom šezdesetih godina dvadesetog veka jedan od prvih automatskih dokazivača teorema.

Loveland Donald W. Loveland, američki informatičar. Doktorirao je na univerzitetu u Njujorku 1964. godine. Zajedno sa Dejvisom i Logmanom implementirao je početkom šezdesetih godina dvadesetog veka jedan od prvih automatskih dokazivača teorema. Sada je počasni profesor računarstva na univerzitetu Djuk.

Lovenhajm Leopold Lövenheim (1878–1957), nemački matematičar. Tokom Prvog svetskog rata, Lovenhajm je bio na ratnoj službi u Francuskoj, Mađarskoj i Srbiji, ali je i u tom periodu objavio nekoliko značajnih radova iz matematičke logike, pre svega unapređujući rezultate Pirsa, Šredera i Vajtheda. Znamenita je Skolem-Lovenhajmova teorema koji tvrdi postojanje tzv. nestandardnih modela, na primer prebrojivog modela za teoriju realnih brojeva. Pošto jednom četvrtinom nije bio Arijevac, prinuđen je da napusti posao 1934. godine. Tokom bombdardovanja Berlina 1943. godine izgubio je sve svoje matematičke rukopise i oko hiljadu crteža i modela. Nakon rata ponovo je predavao matematiku.

Lukašijevič Jan Lukasiewicz (1878–1956), poljski matematičar. Rođen je u poljskoj porodici u Lavovu (današnja Ukrajina), koji je tada bio pod kontrolom Austrije. Nakon povlačenja ruskih trupa iz Poljske, obnovljen je univerzitet u Varšavi (kao Poljski univerzitet) i Lukašijevič je prešao tamo iz Lavova. Utemeljio je varšavsku školu logike. Godine 1939. pred naletom nemačkih trupa, Lukašijevič je napustio Poljsku i, nakon boravaka u nekoliko zemalja, godine 1946. otišao u Dablin (Irska) i počeo da radi na tamošnjem univerzitetu. Uveo je trovrednosnu logiku i radio na drugim viševrednosnim logikama. Uveo je i tzv. poljsku notaciju koja omogućava jednoznačno zapisivanje izraza bez zagrada.

Lul Raymond Lull (ili Ramon Lullus) (1235–1316), rođen je na Majorki, gde je mladost proveo kao trubadur. U svojoj trideset i sedmoj godini doživeo je religijsko prosvetljenje i nakon toga potpuno se posvetio pisanju knjiga i naučnim istraživanjima. Nije imao formalno obrazovanje, ali je poznavao učenje španskih kabalista. Njegove ideje o apstraktnim, dinamičkim ,,algebrama“ odgovaraju sistematskom menjanju određenog broja promenljivih. Bez formula za permutacije i kombinacije, Lul je konstruisao mehanički uređaj za njihovo generisanje, uređaj zasnovan na rotirajućim krugovima sa simbolima slova

na obodima. Radio je i na opštijem sistemu, zvanom *Ars Magna*. Godine 1316. otišao je u severnu Afriku kako bi svojim veštinama privoleo Arape da pređu u hrišćanstvo, a ubrzo nakon je bio kamenovan do smrti od strane lokalnog stanovništva.

Mockin Theodore Samuel Motzkin (1908–1970), poreklom ruski Jevrejin, rođen je i završio osnovne i doktorske studije matematike u Nemačkoj. Godine 1935. otišao je u Jerusalim i tamo ostao i tokom rata, radeći za britansku vladu na kriptografskim zadacima. Preselio se u Sjedinjene Američke Države 1948. godine. Bavio se linearnim programiranjem, teorijom grafova i geometrijom.

Nelson Greg Nelson, američki informatičar. Doktorirao je na univerzitetu Stanford 1980. godine. Sada radi u kompaniji Compaq.

Fon Nojman John (Johann) Louis von Neumann (1903–1957), mađarski matematičar i informatičar. Rođen je u Budimpešti. Studirao je hemiju i matematiku na univerzitetima u Budimpešti, Berlinu i Cirihu. Doktorirao je matematiku 1926. godine na univerzitetu u Budimpešti. Predavao je na univerzitetu u Berlinu do 1930. godine, a od tada na univerzitetu Prinston. Među prvima je uvideo značaj i posledice Gedelovih teorema nepotpunosti. Tokom Drugog svetskog rata, radio je na nekoliko vojnih projekata zbog svog poznavanja matematike, hemije, hidrodinamike, balistike, meteorologije, teorije igara i statistike. U to vreme susreo se sa prvim računarima. Godine 1945. uveo je pojam pohranjenih programa (temelj „Fon Nojmanove arhitekture“) i time ih izjednačio sa podacima (do tada su računari morali da budu rekonfigurisani za izvršavanje svakog novog zadatka). Pored doprinosa arhitekturi računara i teoriji izračunljivosti, značajni su i njegovi doprinosi primenama računara u fizici i ekonomiji.

Open Derek C. Oppen, američki informatičar. Doktorirao je na univerzitetu u Torontu 1974. godine, pod rukovodstvom Stivena Kuka.

Patnam Hilary Putnam (1926–), američki matematičar i logičar. Sada je počasni profesor na odseku za filozofiju na univerzitetu Harvard.

Post Emil Leon Post (1897–1954), američki logičar jevrejskog porekla. Rođen je u delu (današnje) Poljske koji je tada bio pod ruskom kontrolom, u porodici poljskih Jevreja, koja se 1904. preselila u Njujork. Tamo je kasnije studirao astronomiju i matematiku. U svojoj doktorskoj disertaciji iz matematičke logike (na univerzitetu Kolumbija) dokazao je potpunost i konzistentnost iskaznog računa. Najznačajniji rezultati su mu u teoriji grupa, rekurzivno nabrojivih skupova i stepenima nerešivosti. Godine 1920. Post je došao do rezultata sličnih rezultatima Gedela, Čerča i Tjuringa, ali ih nije objavio, smatrajući da

nisu upotpunjeni. O Gedelovoj teoremi o nepotpunosti napisao je: ,,Zaključak je neizbežan: matematičko mišljenje je, i mora ostati, suštinski kreativno... Ovaj zaključak mora neizbežno rezultovati makar delimičnim povlačenjem čitavog aksiomatičkog trenda sa kraja devetnaestog i početka dvadesetog veka, sa povratkom značenja i istinitosti kao suštine matematike... Nakon Gedelovih znamenitih dostignuća tekući pogledi na prirodu matematike su izmenjeni samo utoliko što se uviđa potreba za više formalnih sistema umesto samo jednog, univerzalnog.“. Godine 1936. definisao je tzv. Postovu mašinu. Smatra se jednim od osnivača teorije rekurzije. Bio je veoma neobičan, ali i izuzetno popularan predavač. Patio je od maničnih depresija, koje su ga drastično ometale u radu.

Rasel Bertrand Arthur William Russell, 3rd Earl Russell (1872-1970), britanski filozof i matematičar. Njegove logičke analize imale su veliki uticaj na tok razvoja filozofije i matematike dvadesetog veka. Jedno od najznačajnijih dela mu je *The Principles of Mathematics* (1902), knjiga u kojoj je pokušao da matematiku pomeri iz apstraktnih filozofskih koncepata i dâ joj precizan naučni okvir. Sa britanskim filozofom i matematičarom Vajthedom radio je osam godina na monumentalnom delu *Principia Mathematica* (3 toma, 1910-1913). Ova knjiga, koja se smatra jednim od remek-dela racionalne misli, pokazala je da matematika može biti razmatrana u terminima opšte logike. U svojoj knjizi *The Problems of Philosophy* (1912), Rasel se, kao realista i logički pozitivista, suprotstavio idealizmu, dominantnoj filozofskoj školi tog vremena. Tokom Prvog svetskog rata, Rasel je osuđivao obe strane u ratu, i zbog toga je kažnjavan, zatvaran i udaljen sa svog predavačkog mesta u Kembridžu. Nakon rata, posetio je Sovjetski Savez i bio razočaran tamošnjim socijalizmom. Tokom 1921. i 1922. predavao je na univerzitetu u Pekingu, a u godinama koje su sledile, u privatnoj školi u Engleskoj koju je osnovao i, kasnije, na različitim mestima u Sjedinjenim Američkim Državama. Nakon rata aktivno se borio protiv nuklearnog naoružavanja. Godine 1950. dobio je Nobelovu nagradu za književnost i pominjan kao ,,šampion humanizma i slobode misli“. U svojoj osamdeset devetoj godini ponovo je bio u zatvoru, zbog učešća u anti-nuklearnim demonstracijama.

Robinson Alan Robinson, američki matematičar, logičar i informatičar. Doktorirao je na univerzitetu Prinston 1956. godine, i nakon toga radio na više univerziteta i istraživačkih institucija. Objavio je veliki broj naučnih radova, uključujući znameniti rad o rezoluciji 1965. Smatra se jednim od istraživača koji su dali najveći doprinos razvoju automatskog dokazivanja teorema. Sada je počasni profesor logike i računarstva na univerzitetu Sirakuza.

Skolem Thoralf Albert Skolem (1887–1963), norveški matematičar. Najveći deo naučne karijere proveo je na univerzitetu u Oslu. Objavio je oko 190 radova, od kojih oko trećinu čine radovi iz matematičke logike, a ostatak radovi iz algebre i teorije grupa, teorije skupova i teorije brojeva. Proširio je Lovenhajmovu

teoremu do tzv. Skolem-Lovenhajmove teoreme koja kaže da ako teorija ima model, onda ima prebrojiv model.

Smaljan Raymond Smullyan (1919–), američki logičar i matematičar. Napisao je nekoliko veoma popularnih knjiga o matematičkoj logici, šahu i zanimljivim matematičkim problemima.

Šefer H. M. Sheffer (1883–1964), američki filozof. Godine 1913. definisao je logički veznik koji danas zovemo Šeferov simbol (eng. Sheffer's stroke) i koji čini potpuni sistem veznika za iskaznu logiku. Često se otkriće da postoji jednočlan potpuni skup veznika pogrešno pripisuje Šeferu; ta činjenica, međutim, kao i jedan takav veznik (dualan Šeferovom) bili su poznati i pre Šeferovog otrkića.

Tarski Alfred Tarski (1902–1983), poljski matematičar. Rođen je u porodici poljskih Jevreja Tajtelbaum (Teitelbaum), u Varšavi, koja je tada bila deo Ruske imperije. U toku Prvog svetskog rata, nakon što su 1915. Centralne sile (Nemačka i Austro-Ugarska) potisnule ruske snage iz Poljske, počelo je obnavljanje poljskih institucija, uključujući Poljski univerzitet u Varšavi. Za kratko vreme ovaj univerzitet okupio je mnoge istaknute poljske matematičare tog doba i postao jedan od vodećih svetskih univerziteta. Na tom univerzitetu, Alfred Tajtelbaum godinu dana je studirao biologiju, a onda prešao na studije matematike. U jeku obnavljanja države i poljskih nacionalnih osećanja, Alfred Tajtelbaum promenio je, 1923. godine, svoje prezime u Tarski i umesto judaizma prihvatio katoličku veru. Doktorirao je 1924. i već te godine došao do izuzetno značajnih rezultata u teoriji skupova. Nekoliko godina radio je i sarađivao sa Lukašijevičem. Godine 1933. objavio je svoj koncept istinitosti u radu koji mnogi smatraju jednim od najznačajnijih radova u razvoju matematičke logike (*Pojam istinitosti u formalizovnim jezicima*, originalno objavljen na poljskom jeziku), a godine 1936. koncept logičke posledice (u radu *O pojmu logičke posledice*). Napad nemačkih snaga zatekao ga je u poseti univerzitetu Harvard. Od 1942. najveći deo karijere proveo je na univerzitetu Kalifornije u Berkliju, pri čemu je nekoliko godina proveo kao gostujući profesor u Londonu, Parizu, Los Anđelesu i Čileu. Smatra se jednim od četiri najveća logičara svih vremena (pored Aristotela, Fregea i Gedela). Njegovo delo čini oko 2500 strana iz mnogih oblasti matematike: teorije skupova, teorije mere, topologije, geometrije, algebre i, naravno, matematičke logike. Najznačajniji njegovi doprinosi matematičkoj logici su koncept semantike i semantički metodi koji su doveli do nastanka i razvoja teorije modela, kao i rezultati u polju odlučivosti i neodlučivosti. Dokazao je da su teorija realnih zatvorenih polja i elementarna geometrija odlučive, a da su teorija grupa i projektivna geometrija neodlučive. U okviru jednog predavanja na Harvardu 1940. godine, rekao je „problem odlučivanja u opštem obliku nema rešenje... mnogi matematičari osetili su istinsko olakšanje kada su saznali za ovaj rezultat. Možda su tokom besanih

noći sa užasom razmišljali o trenutku kada će neki uvrnuti metamatematičar naći rešenje za problem odlučivanja i napraviti mašinu koja može da automatski reši bilo koji matematički problem... Opasnost je sada okončana. . . i matematičari. . . mogu da spavaju spokojno". Bio je ekstrovertna ličnost, snažne volje i energije i oštrog jezika. Bio je harizmatski predavač, poznat po svom briljantnom stilu izlaganja.

Tjuring Alan Mathison Turing (1912–1954), engleski matematičar i logičar. Studirao je i najveći deo karijere proveo na Kembridžu. Najpre se bavio verovatnoćom, a kasnije uglavnom matematičkom logikom. Godine 1936. definisao je apstraktnu mašinu, danas poznatu kao Tjuringova mašina. Nezavisno od Čerča dokazao je 1936. godine neodlučivost aritmetike. Nakon toga, proveo je dve godine u Americi radeći zajedno sa Čerčom. Tokom rata radio je za britansku vladu u Bletchley Park, na razbijanju nemačkih ratnih šifara. Posle rata njegovi planovi za konstrukciju računara bili su odbijeni kao preambiciozni. Pored rada na problemu reči u teoriji grupa, bavio se i pisanjem programa za apstraktne računare, neurologijom i kvantnom teorijom, ali i kriptografskim problema (za britansku tajnu službu). Godine 1950. objavio je znameniti rad *Computing machinery and intelligence in Mind* u kojem je vizionarski otvorio mnoga pitanja koja će postati aktuelna sa razvojem računara. U tom tekstu predložio je test, koji se danas naziva *Tjuringov test* i dalje koristi kao mera inteligentnog ponašanja računara. Bio je hapšen i kažnjavan zbog homoseksualizma i pod jakim pritiscima britanske tajne službe. Preminuo je od trovanja cijanidom, pod nedovoljno razjašnjenim okolnostima.

Vajthed Alfred North Whitehead (1861–1947), britanski matematičar i filozof. Predavao je na Kembridžu, na Imperijal koledžu (London) i na univerzitetu u Harvardu. Rođen je u anglikanskoj porodici, tokom svojih tridesetih godina počeo je da se približava katoličkoj crkvi, da bi sredinom devedestih godina devetnaestog veka, pod uticajem razvoja nauke, postao agnostik. Bavio se algebrom, zasnivanjem projektivne i nacrtne geometrije i filozofijom nauke. Sa Raselom je napisao monumentalno delo *Principia Mathematica*. Najznačajnije samostalno delo mu je knjiga *Process and Reality* (1929), u kojoj je izložio svoje metafizičke teorije.

Vos Larry Wos, američki matematičar i informatičar. Od 1957. godine radi u Argon nacionalnoj laboratoriji (SAD). Uveo je novi naziv za oblast automatskog dokazivanja teorema — *automatsko rezonovanje*, označavajući time da je oblast sazrela dovoljno da pokriva mnogo više od pronalaženja dokaza. Uveo je koncept strategije u automatsko rezonovanje, propagirao eksperimentalni pristup i razvio sisteme za automatsko rezonovanje koji su dali odgovore na nekoliko do tada otvorenih matematičkih pitanja. Godine 1997. sistem razvijen u njegovom timu automatski je dokazao tzv. Robinsovu hipotezu, tvrđenje koje je šezdeset godina do tada bilo nedokazano. Smatra se jednim od najznačajnijih istraživača u istoriji automatskog rezonovanja.

Dodatak D

Rešenja zadataka

1. Pretpostavimo suprotno — pretpostavimo da formula $(D \wedge A) \Rightarrow \neg B$ nije tautologija, tj. pretpostavimo da postoji valuacija v takva da je $I_v((D \wedge A) \Rightarrow \neg B) = 0$. Iz $I_v((D \wedge A) \Rightarrow \neg B) = 0$ sledi $I_v(D \wedge A) = 1$ i $I_v(\neg B) = 0$, a odatle $I_v(D) = 1$, $I_v(A) = 1$ i $I_v(B) = 1$. Formula $(A \wedge C) \Rightarrow \neg D$ je tautologija, pa važi $I_v((A \wedge C) \Rightarrow \neg D) = 1$. Kako je $I_v(\neg D) = 0$, mora da važi $I_v(A \wedge C) = 0$, odakle sledi da je $I_v(C) = 0$ (jer je $I_v(A) = 1$). S druge strane, formula $A \Rightarrow (B \Rightarrow C)$ je tautologija, pa važi $I_v(A \Rightarrow (B \Rightarrow C)) = 1$. Kako je $I_v(A) = 1$, mora da važi $I_v(B \Rightarrow C) = 1$. Važi $I_v(B) = 1$, pa mora da važi i $I_v(C) = 1$, što je u kontradikciji sa $I_v(C) = 0$. Dakle, polazna pretpostavka je bila pogrešna, odakle sledi da je formula $(D \wedge A) \Rightarrow \neg B$ tautologija.

10. Dokažimo najpre, metodom istinitosnih tablica, da je formula

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

tautologija:

$(A$	$\Rightarrow$	$(B$	$\Rightarrow$	$C))$	$\Rightarrow$	$(((A$	$\wedge$	$C)$	$\Rightarrow$	$\neg$	$D)$	$\Rightarrow$	$((D$	$\wedge$	$A)$	$\Rightarrow$	$\neg$	$B))$
0	1	0	1	0	1	0	0	0	1	1	0	1	0	0	0	1	1	0
0	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	1	1	0
0	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0
0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0
0	1	1	0	0	1	0	0	0	1	1	0	1	0	0	0	1	0	1
0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	1	0	1
0	1	1	1	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1
0	1	1	1	1	1	0	0	1	1	0	1	1	1	0	0	1	0	1
1	1	0	1	0	1	1	0	0	1	1	0	1	0	0	1	1	1	0
1	1	0	1	0	1	1	0	0	1	0	1	1	1	1	1	1	1	0
1	1	0	1	1	1	1	1	1	1	1	0	1	0	0	1	1	1	0
1	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0
1	0	1	0	0	1	1	0	0	1	1	0	1	0	0	1	1	0	1
1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1
1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	1	0	1
1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	0	0	1

Formula $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (((A \wedge C) \Rightarrow \neg D) \Rightarrow ((D \wedge A) \Rightarrow \neg B))$ je, dakle, tautologija i, na osnovu pretpostavke, formula $A \Rightarrow (B \Rightarrow C)$ je tautologija, pa, na osnovu teoreme 2.2, sledi da je i formula $((A \wedge C) \Rightarrow \neg D) \Rightarrow ((D \wedge A) \Rightarrow \neg B)$ tautologija. Formula $((A \wedge C) \Rightarrow \neg D) \Rightarrow ((D \wedge A) \Rightarrow \neg B)$ je tautologija i, na

osnovu pretpostavke, formula $(A \wedge C) \Rightarrow \neg D$ je tautologija, pa na osnovu teoreme 2.2, sledi da je i formula $(D \wedge A) \Rightarrow \neg B$ tautologija.

11. Ako je $v(p) = 0$ i $v(q) = 0$, onda je $I_v(A \wedge q) = 0$ i $I_v((A \wedge q) \Rightarrow \neg p) = 1$. Slično, ako je $v(p) = 1$ i $v(q) = 1$, onda je $I_v(A \wedge q) = I_v(A)$ i $I_v(\neg p) = 0$, pa je $I_v((A \wedge q) \Rightarrow \neg p) = 1 - I_v(A)$. Analogno određujemo istinitosnu vrednost date formule za svaku kombinaciju vrednosti $v(p)$ i $v(q)$. Te vrednosti prikazane su u narednoj tablici:

$((A$	$\wedge$	$q)$	$\Rightarrow$	$\neg$	$p)$	$\Rightarrow$	$((p$	$\Rightarrow$	$\neg$	$q)$	$\Rightarrow$	$A)$
	0	0	1	1	0	$I_v(A)$	0	1	1	0	$I_v(A)$	
	$I_v(A)$	1	1	1	0	$I_v(A)$	0	1	0	1	$I_v(A)$	
	0	0	1	0	1	$I_v(A)$	1	1	1	0	$I_v(A)$	
	$I_v(A)$	1	$1 - I_v(A)$	0	1	1	1	0	0	1	1	

Dakle, da bi data formula bila tautologija mora da važi $I_v(A) = 1$ u slučajevima $v(p) = v(q) = 0$, $v(p) = 0, v(q) = 1$, $v(p) = 1, v(q) = 0$, dok u slučaju $v(p) = v(q) = 1$, formula A može da ima proizvoljnu vrednost. Dakle, formula A za koju u svakoj valuaciji važi $I_v(A) = 1$ ispunjava uslov zadatka, pa A može biti formula $\top$.

18. Neka p označava tvrđenje „R uvek govori istinu“ i neka q označava tvrđenje „Levi put vodi u glavni grad“. Meštaninu R treba postaviti pitanje „Da li je tačno P?“ (gde je P iskaz izražen u funkciji p i q). Označimo sa $R(A)$ odgovor meštanina na pitanje „Da li je tačno A?“ — 0 ako je njegov odgovor *ne* i 1 ako je njegov odgovor *da*. Postavljeno pitanje treba da bude takvo da je $R(P)$ u svakom slučaju jednak vrednosti iskaza q. Odredimo tvrđenje P.

Ako je u nekoj valuaciji $I_v(p) = 0$ (tj. R uvek govori laž) i ako je $R(A)$ jednako 0, onda u toj valuaciji mora da važi $I_v(A) = 1$. Ako je u nekoj valuaciji $I_v(p) = 0$ (tj. R uvek govori laž) i ako je $R(A)$ jednako 1, onda u toj valuaciji mora da važi $I_v(A) = 0$. Ako je u nekoj valuaciji $I_v(p) = 1$ (tj. R uvek govori istinu) i ako je $R(A)$ jednako 0, onda u toj valuaciji mora da važi $I_v(A) = 0$. Ako je u nekoj valuaciji $I_v(p) = 1$ (tj. R uvek govori istinu) i ako je $R(A)$ jednako 1, onda u toj valuaciji mora da važi $I_v(A) = 1$. Dobijeni zaključci mogu biti prikazani u vidu sledeće istinitosne tablice:

p	$R(A)$	A
0	0	1
0	1	0
1	0	0
1	1	1

Iskaz P može da ima formu $R(B)$ i onda je potrebno da je u svakoj valuaciji vrednost $R(R(B))$ jednaka q. Odredimo tvrđenje B. Vrednosti za iskaze $R(B)$ i B dobijaju se na osnovu prethodne istinitosne tablice. Te vrednosti prikazane su u sledećoj istinitosnoj tablici:

p	q	$R(R(B))$	$R(B)$	B
0	0	0	1	0
0	1	1	0	1
1	0	0	0	0
1	1	1	1	1

Očigledno, u svakoj valuaciji je $I_v(B) = I_v(q)$, pa zaključujemo da traženo pitanje može da bude „Da li je tačno $R(q)$?“ ili „Da li je tačno da bi mi ti odgovorio potvrdno ako bih te pitao da li levi put vodi u glavni grad?“.

25.

(a) Formula A nije kontradikcija, pa postoji valuacija v_1 takva da je $I_{v_1}(A) = 1$. Formula B nije tautologija, pa postoji valuacija v_2 takva da je $I_{v_2}(B) = 0$. Pretpostavimo da formule A i B nemaju zajedničko nijedno iskazno slovo. Tada možemo da definišemo valuaciju v na sledeći način:

$$v(p) = \begin{cases} v_1(p), & \text{ako se } p \text{ pojavljuje u } A \\ v_2(p), & \text{inače} \end{cases}$$

Tada važi $I_v(A) = I_{v_1}(A) = 1$ i $I_v(B) = I_{v_2}(B) = 0$, pa $A \Rightarrow B$ nije tautologija, što je suprotno zadatim uslovima. Dakle, polazna pretpostavka je pogrešna, pa zaključujemo da formule A i B moraju da imaju bar jedno zajedničko iskazno slovo.

(b) Neka je kanonska disjunktivna normalna forma formule A jednaka $A_1 \vee A_2 \vee \ldots \vee A_m$ i neka je kanonska konjunktivna normalna forma formule B jednaka $B_1 \wedge B_2 \wedge \ldots \wedge B_n$. Formula $A \Rightarrow B$ je tautologija, pa na osnovu logičke ekvivalencije $(P \vee Q) \Rightarrow R \equiv (P \Rightarrow R) \wedge (Q \Rightarrow R)$ i jednostavnog induktivnog argumenta zaključujemo da je svaka od formula $A_i \Rightarrow B$ $(i = 1, 2, \ldots, m)$ tautologija. Analogno, kako je formula $A_i \Rightarrow B$ $(i = 1, 2, \ldots, m)$ tautologija, na osnovu logičke ekvivalencije $P \Rightarrow (Q \wedge R) \equiv (P \Rightarrow Q) \wedge (P \Rightarrow R)$ i jednostavnog induktivnog argumenta zaključujemo da je svaka od formula $A_i \Rightarrow B_j$ $(i = 1, 2, \ldots, m,$ $j = 1, 2, \ldots, n)$ tautologija. To je moguće samo ako za svaki par A_i, B_j postoji literal l_{ij} koji se u A_i pojavljuje kao konjunkt, a u B_j kao disjunkt. Neka je formula C jednaka

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} l_{ij}$$

Kako je skup literala $\bigwedge_{j=1}^{n} l_{ij}$ podskup skupa literala formule A_i sledi da je $A_i \Rightarrow \bigwedge_{j=1}^{n} l_{ij}$ tautologija (jer je formula $P \wedge Q \Rightarrow P$ tautologija). Dodatno, korišćenjem tautologije $((P \Rightarrow Q) \wedge (R \Rightarrow S)) \Rightarrow (P \vee R \Rightarrow Q \vee S)$ može se matematičkom indukcijom dokazati da je formula

$$A_1 \vee A_2 \vee \ldots \vee A_m \Rightarrow \bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} l_{ij}$$

tautologija, tj. da je formula $A \Rightarrow C$ tautologija.

Kako je literal l_{ij} ($i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$) disjunkt formule B_j, sledi da je $l_{ij} \Rightarrow B_j$ tautologija (jer je formula $P \Rightarrow P \vee Q$ tautologija). Dodatno, korišćenjem tautologije $((P \Rightarrow Q) \wedge (R \Rightarrow S)) \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$ može se matematičkom indukcijom dokazati da je formula $\bigwedge_{j=1}^{n} l_{ij} \Rightarrow B_1 \wedge B_2 \wedge \ldots \wedge B_n$ tautologija. Kako to važi za svako i ($i = 1, 2, \ldots, m$), na osnovu logičke ekvivalencije $(P \Rightarrow R) \wedge (Q \Rightarrow R) \equiv (P \vee Q) \Rightarrow R$ sledi da je i

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} l_{ij} \Rightarrow B_1 \wedge B_2 \wedge \ldots \wedge B_n$$

tautologija, tj. da je formula $C \Rightarrow B$ tautologija.

40.

$$\dfrac{A \vee B \qquad \dfrac{\dfrac{\neg A \quad [A]^1}{\dfrac{\bot}{B}\, efq} \neg E \qquad [B]^2}{B} \vee E, 1, 2}{}$$

41.

$$\dfrac{\dfrac{\dfrac{[\neg B]^1 \qquad \dfrac{[A]^2 \quad [A \Rightarrow B]^3}{B} \Rightarrow E}{\bot} \neg E}{\neg A} \neg I, 2}{\neg B \Rightarrow \neg A} \Rightarrow I, 1}{(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)} \Rightarrow I, 3$$

42.

$$\dfrac{\dfrac{[A \vee (B \wedge C)]^1 \quad \dfrac{\dfrac{[A]^2}{A \vee B} \vee I \quad \dfrac{[A]^2}{A \vee C} \vee I}{(A \vee B) \wedge (A \vee C)} \wedge I \qquad \dfrac{\dfrac{\dfrac{[B \wedge C]^3}{B} \wedge E}{A \vee B} \vee I \quad \dfrac{\dfrac{[B \wedge C]^3}{C} \wedge E}{A \vee C} \vee I}{(A \vee B) \wedge (A \vee C)} \wedge I}{(A \vee B) \wedge (A \vee C)} \vee E, 2, 3}{(A \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge (A \vee C))} \Rightarrow I, 1$$

43

$$\dfrac{\dfrac{A \vee \neg A \qquad \dfrac{\dfrac{\dfrac{[\neg(A \wedge B)]^4 \qquad \dfrac{[A]^2 \quad [B]^1}{A \wedge B} \wedge I}{\bot} \neg E}{\neg B} \neg I, 1}{\neg A \vee \neg B} \vee I \qquad \dfrac{[\neg A]^3}{\neg A \vee \neg B} \vee I}{\neg A \vee \neg B} \vee E, 2, 3}{\neg(A \wedge B) \Rightarrow (\neg A \vee \neg B)} \Rightarrow I, 4$$

44.

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{\vdash \neg A, A}\ \neg R \quad \dfrac{B \vdash B}{B, \neg B \vdash}\ \neg L}{A \Rightarrow B, \neg B \vdash \neg A}\ \Rightarrow L}{A \Rightarrow B \vdash (\neg B \Rightarrow \neg A)}\ \Rightarrow R}{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)}\ \Rightarrow R$$

47. Neka je $\mathcal{L} = (\Sigma, \Pi, ar)$, gde je $\Sigma = \{f\}$, $\Pi = \{p\}$ i $ar(f) = 1$ i $ar(p) = 1$. Odredimo $\mathcal{L}$-strukturu $\mathfrak{D} = (D, I^{\mathcal{L}})$ takvu da je ona model date formule, pri čemu je $I^{\mathcal{L}}(f) = f_I$ i $I^{\mathcal{L}}(p) = p_I$.

Neka je $D = \mathbf{N}$, $f_I(n) = n + 2$ (gde je $n \in \mathbf{N}$) i $p_I(n) = 1$ ako i samo ako je n paran broj. Dokažimo da je $\mathfrak{D} = (D, I^{\mathcal{L}})$ model formule $\mathcal{A} = (\forall x)(p(x) \Rightarrow p(f(x))$.

Dokažimo da je $I_v(\mathcal{A}) = 1$ za svaku valuaciju v. Pretpostavimo suprotno – pretpostavimo da postoji valuacija v takva da je $I_v(\mathcal{A}) = 0$. Na osnovu definicije 3.10, iz $I_v(\mathcal{A}) = 0$ sledi da postoji valuacija w takva da je $v \sim_x w$ i $I_w(p(x) \Rightarrow p(f(x))) = 0$. Na osnovu iste definicije, odatle sledi da je $I_w(p(x)) = 1$ i $I_w(p(f(x))) = 0$. Neka je $w(x) = n$, gde je n element skupa $\mathbf{N}$. Tada je $1 = I_w(p(x)) = p_I(n)$ i $0 = I_w(p(f(x))) = p_I(f_I(n)) = p_I(n + 2)$, odakle sledi da je n paran broj, a $n + 2$ neparan, što je netačno za svaki prirodan broj n. Dakle, $I_v(\mathcal{A}) = 1$ za svaku valuaciju v, tj. $\mathcal{L}$-struktura $\mathfrak{D} = (\mathbf{N}, I^{\mathcal{L}})$ je model date formule $\mathcal{A}$.

48. Neka je v proizvoljna valuacija. $\mathcal{L}$-struktura $\mathfrak{D}$ je model date formule ako je $I_v((\forall x)(p(x, f(x)) \Rightarrow p(f(x), x)) = 1$, tj. ako za svaku valuaciju w takvu da je $v \sim_x w$ važi $I_w(p(x, f(x)) \Rightarrow p(f(x), x)) = 1$.

Dovoljno je razmatrati mogućnosti $w(x) = a$, $w(x) = b$ i $w(x) = c$. Vrednosti $I_w(p(x, f(x)) \Rightarrow p(f(x), x)) = 1$ mogu tada biti prikazane i u vidu tablice:

$w(x)$	$f_I(w(x))$	$p_I(w(x), f_I(w(x)))$	$p_I(f_I(w(x)), w(x))$	$I_w(p(x, f(x)) \Rightarrow p(f(x), x))$
a	b	1	1	1
b	a	1	1	1
c	a	0	0	1

Dakle, za proizvoljnu valuaciju v je $I_v(\forall x)(p(x, f(x)) \Rightarrow p(f(x), x)) = 1$, pa je $\mathfrak{D}$ model formule $(\forall x)(p(x, f(x)) \Rightarrow p(f(x), x))$.

49. Neka je $\mathcal{L} = (\Sigma, \Pi, ar)$, $\Sigma = \{\}$, $\Pi = \{p\}$ i $ar(p) = 2$, $D = \{a, b\}$ i neka je $I^{\mathcal{L}}(p) = p_I$. Da bi $\mathfrak{D} = (D, I^{\mathcal{L}})$ bio model formule $\mathcal{A}$ treba da za proizvoljnu valuaciju v važi $I_v((\forall x)(\exists y)(p(x, y) \Rightarrow \neg p(y, x))) = 1$, tj. za svaku valuaciju w takvu da je $v \sim_x w$ važi $I_w((\exists y)(p(x, y) \Rightarrow \neg p(y, x))) = 1$. Postoje dve mogućnosti: $w(x) = a$ i $w(x) = b$ i za obe treba da važi $I_w((\exists y)(p(x, y) \Rightarrow \neg p(y, x))) = 1$. Važi $I_w((\exists y)(p(x, y) \Rightarrow \neg p(y, x))) = 1$ ako postoji valuacija w' takva da je $w \sim_y w'$ i $I_{w'}(p(x, y) \Rightarrow \neg p(y, x)) = 1$. Za svaku valuaciju w postoje dve takve valuacije w' — jedna, za koju važi $w'(y) = a$ i druga, za koju važi $w'(y) = b$ (pri tome važi i $w'(x) = w(x)$). Važi $I_{w'}(p(x, y) \Rightarrow \neg p(y, x)) = 1$ ako je $I_{w'}(p(x, y)) = 0$ ili $I_{w'}(\neg p(y, x)) = 1$, tj. ako je $I_{w'}(p(x, y)) = 0$ ili $I_{w'}(p(y, x)) = 0$. Dakle, važi:

$(w(x) = a$ i $I_w((\exists y)(p(x,y) \Rightarrow \neg p(y,x))) = 1)$ i $(w(x) = b$ i $I_w((\exists y)(p(x,y) \Rightarrow \neg p(y,x))) = 1)$
odakle sledi
$(w(x) = a$ i $((w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)))$ i $(w(x) = b$ i $((w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)))$
odakle sledi
$((w(x) = a$ i $w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w(x) = a$ i $w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1))$ i $((w(x) = b$ i $w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w(x) = b$ i $w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1))$
odakle sledi
$((w'(x) = a$ i $w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w'(x) = a$ i $w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1))$ i $((w'(x) = b$ i $w'(y) = a$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1)$ ili $(w'(x) = b$ i $w'(y) = b$ i $I_{w'}(p(x,y) \Rightarrow \neg p(y,x)) = 1))$
odakle sledi
$((w'(x) = a$ i $w'(y) = a$ i $(I_{w'}(p(x,y)) = 0$ ili $I_{w'}(p(y,x)) = 0))$ ili $(w'(x) = a$ i $w'(y) = b$ i $(I_{w'}(p(x,y)) = 0$ ili $I_{w'}(p(y,x)) = 0)))$ i $((w'(x) = b$ i $w'(y) = a$ i $(I_{w'}(p(x,y)) = 0$ ili $I_{w'}(p(y,x)) = 0))$ ili $(w'(x) = b$ i $w'(y) = b$ i $(I_{w'}(p(x,y)) = 0$ ili $I_{w'}(p(y,x)) = 0)))$
odakle sledi
$((p_I(a,a)) = 0$ ili $p_I(a,a)) = 0)$ ili $(p_I(a,b) = 0$ ili $p_I(b,a) = 0))$ i $((p_I(b,a)) = 0$ ili $p_I(a,b) = 0)$ ili $(p_I(b,b) = 0$ ili $p_I(b,b) = 0))$
odakle sledi
$(p_I(a,a)) = 0$ ili $p_I(a,b) = 0$ ili $p_I(b,a) = 0)$ i $(p_I(b,a)) = 0$ ili $p_I(a,b) = 0$ ili $p_I(b,b) = 0)$

Da bi $\mathcal{L}$-struktura $\mathfrak{D}$ bila model za datu formulu mora da važi $(p_I(a,a)) = 0$ ili $p_I(a,b) = 0$ ili $p_I(b,a) = 0)$ i $(p_I(b,a)) = 0$ ili $p_I(a,b) = 0$ ili $p_I(b,b) = 0)$. Neposredno se može proveriti da ima 13 (od ukupno 16) funkcija $p_I : D^2 \mapsto \{0,1\}$ koje zadovoljavaju taj uslov. Svakoj od tih funkcija odgovara po jedan traženi model (do na izomorfizam).

50. Neka je $\mathcal{L} = (\Sigma, \Pi, ar)$, pri čemu je $\Sigma = \{f, a\}$, $\Pi = \{p\}$, $ar(f) = 2$, $ar(a) = 0$ i $ar(p) = 2$.

Neka je $D = \mathbf{Z}$, $I^{\mathcal{L}}(f) = f_I$, $I^{\mathcal{L}}(a) = a_I$ i $I^{\mathcal{L}}(p) = p_I$, pri čemu je $f_I(z_1, z_2) = z_1 + z_2$ $(z_1, z_2 \in \mathbf{Z})$, $a_I = 0$ i $p_I(z_1, z_2) = 1$ ako i samo ako je $z_1 = z_2$ $(z_1, z_2 \in \mathbf{Z})$. Dokažimo da je $\mathfrak{D} = (D, I^{\mathcal{L}})$ model date formule. Dokažimo da za proizvoljnu valuaciju v važi $I_v((\forall x)(\exists y)p(f(x,y),a)) = 1$. Pretpostavimo suprotno — pretpostavimo da postoji valuacija v za koju važi $I_v((\forall x)(\exists y)p(f(x,y),a)) = 0$. Tada, na osnovu definicije 3.10, sledi da postoji valuacija w takva da je $w \sim_x v$ i $I_w((\exists y)p(f(x,y),a)) = 0$ (neka je u toj valuaciji $w(x) = z$, $z \in \mathbf{Z}$). To dalje znači da za svaku valuaciju w' takvu da je $w' \sim_y w$ (dakle, važi $w'(x) = z$) i važi $I_{w'}(p(f(x,y),a)) = 0$. Međutim, u valuaciji u kojoj je $w'(y) = -z$ važi $I_{w'}(p(f(x,y),a)) = p_I(f_I(z,-z),0) = p_I(z + (-z),0) = p_I(0,0) = 1$, što je u kontradikciji sa $I_{w'}(p(f(x,y),a)) = 0$. Dakle, polazna pretpostavka je bila pogrešna, te sledi da za proizvoljnu valuaciju v važi $I_v((\forall x)(\exists y)p(f(x,y),a)) =$

1, tj. $\mathcal{L}$-struktura $\mathfrak{D}$ je model date formule.

Neka je $D = \mathbf{N}$, $I^{\mathcal{L}}(f) = f_I$, $I^{\mathcal{L}}(a) = a_I$ i $I^{\mathcal{L}}(p) = p_I$, pri čemu je $f_I(n_1, n_2) = n_1 + n_2$ ($n_1, n_2 \in \mathbf{N}$), $a_I = 0$ i $p_I(n_1, n_2) = 1$ ako i samo ako je $n_1 = n_2$ ($n_1, n_2 \in \mathbf{N}$). Dokažimo da je $\mathfrak{D} = (D, I^{\mathcal{L}})$ kontramodel date formule. Dokažimo da postoji valuacija v za koju važi $I_v((\forall x)(\exists y)p(f(x,y),a)) = 0$. Pretpostavimo suprotno — da za proizvoljnu valuaciju v važi $I_v((\forall x)(\exists y)p(f(x,y),a)) = 1$. Tada, na osnovu definicije 3.10, sledi da za svaku valuaciju w takvu da je $w \sim_x v$ važi $I_w((\exists y)p(f(x,y),a)) = 1$. Neka je w proizvoljna valuacija i neka je $w(x) = n$, gde je $n \in \mathbf{N}$ i $n > 0$. Iz $I_w((\exists y)p(f(x,y),a)) = 1$ sledi da postoji valuacija w' takva da je $w' \sim_y w$ (dakle, važi $w'(x) = n$) i važi $I_{w'}(p(f(x,y),a)) = 1$. Pretpostavimo da je $w'(y) = m$, $m \in \mathbf{N}$. Tada važi $I_{w'}(p(f(x,y),a)) = p_I(f_I(n,m),0) = p_I(n+m,0)$. Međutim, $p_I(n+m,0)$ je jednako 1 samo ako je $n+m = 0$, što nije tačno ni za koju vrednost m, $m \in \mathbf{N}$ (jer je $n > 0$). Dakle, polazna pretpostavka je bila pogrešna, te sledi da postoji valuacija v za koju važi $I_v((\forall x)(\exists y)p(f(x,y),a)) = 0$, tj. $\mathcal{L}$-struktura $\mathfrak{D}$ je kontramodel date formule.

51. Neka je $\mathcal{L} = (\Sigma, \Pi, ar)$, pri čemu je $\Sigma = \{f\}$, $\Pi = \{p\}$, $ar(f) = 1$, $ar(p) = 2$.

(a) Neka je $\mathfrak{D} = (\mathbf{N}, I^{\mathcal{L}})$ i $I^{\mathcal{L}}(f) = f_I$, $I^{\mathcal{L}}(p) = p_I$, pri čemu je $f_I(n) = n + 1$ i $p_I(n_1, n_2) = 1$ ako i samo ako je $n_1 < n_2$. Dokažimo da je $\mathcal{L}$-struktura $\mathfrak{D}$ model date formule $\mathcal{A}$, tj. dokažimo da za svaku valuaciju v važi $I_v(\mathcal{A}) = 1$. Pretpostavimo suprotno — pretpostavimo da postoji valuacija v takva da je $I_v(\mathcal{A}) = 0$. Na osnovu definicije 3.10, sledi da $I_v((\forall x)(p(x,f(x)) \wedge \neg p(x,x))) = 0$ ili $I_v((\forall x)(\forall y)(\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$.

- Pretpostavimo da je $I_v(\forall x)(p(x,f(x)) \wedge \neg p(x,x)) = 0$. Odatle sledi da postoji valuacija w takva da je $w \sim_x v$ takva da je $I_w((p(x,f(x)) \wedge \neg p(x,x))) = 0$. Pretpostavimo da je u toj valuaciji $w(x) = n$, gde je $n \in \mathbf{N}$. Iz $I_w((p(x,f(x)) \wedge \neg p(x,x))) = 0$ sledi da je $I_w(p(x,f(x))) = 0$ ili $I_w(\neg p(x,x)) = 0$, tj. da je $p_I(w(x), f_I(w(x))) = 0$ ili $p_I(w(x), w(x)) = 1$, tj. da nije $n < n+1$ ili da je $n < n$, što nije ispunjeno ni za jedan broj n, $n \in \mathbf{N}$.
- Pretpostavimo da je $I_v((\forall x)(\forall y)(\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$. Odatle sledi da postoji valuacija w takva da je $w \sim_x v$ takva da je $I_w((\forall y)(\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$. Neka je $w(x) = n_1$. Iz $I_w((\forall y)(\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$ sledi da postoji valuacija w' takva da je $w' \sim_y w$ (dakle, važi $w'(x) = w(x) = n_1$) takva da je $I_{w'}((\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$. Neka je $w'(y) = n_2$. Iz $I_{w'}((\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$ sledi da postoji valuacija w'' takva da je $w'' \sim_z w'$ (dakle, važi $w''(x) = w'(x) = w(x) = n_1$ i $w''(y) = w'(y) = n_2$) takva da je $I_{w''}((p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$. Neka je $w''(z) = n_3$. Iz $I_{w''}((p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 0$ sledi da je $I_{w''}(p(x,y) \wedge p(y,z)) = 1$ i $I_{w''}(p(x,z)) = 0$ i, dalje, $I_{w''}(p(x,y)) = 1$, $I_{w''}(p(y,z)) = 1$ i $I_{w''}(p(x,z)) = 0$, tj. $p_I(w''(x), w''(y)) = 1$, $p_I(w''(y), w''(z)) = 1$ i $p_I(w''(x), w''(z)) =$

0. Odatle sledi $p_I(n_1, n_2) = 1$, $p_I(n_2, n_3) = 1$ i $p_I(n_1, n_3) = 0$ i, dalje, sledi da je tačno $n_1 < n_2$, $n_2 < n_3$ i da nije tačno $n_1 < n_3$. Međutim, to nije ispunjeno ni za koja tri prirodna broja n_1, n_2, n_3.

Dakle, pretpostavka je bila pogrešna, te sledi da za svaku valuaciju v važi $I_v(\mathcal{A}) = 1$, tj. $\mathcal{L}$-struktura $\mathfrak{D}$ je model formule $\mathcal{A}$.

(b) Neka je $\mathfrak{D} = (\{a\}, I^{\mathcal{L}})$ i $I^{\mathcal{L}}(f) = f_I$, $I^{\mathcal{L}}(p) = p_I$, pri čemu je $f_I(a) = a$ i $p_I(a, a) = 1$. Dokažimo da je $\mathfrak{D}$ kontramodel za formulu $\mathcal{A}$. Pretpostavimo suprotno — pretpostavimo da za proizvoljnu valuaciju v važi da je $I_v(\mathcal{A}) = 1$. Tada je, na osnovu definicije 3.10, $I_v((\forall x)(p(x, f(x)) \wedge \neg p(x, x))) = 1$ i $I_v((\forall x)(\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))) = 1$. Iz $I_v((\forall x)(p(x, f(x)) \wedge \neg p(x, x))) = 1$ sledi da za proizvoljnu valuaciju w takvu da je $w \sim_x v$ važi $I_w((p(x, f(x)) \wedge \neg p(x, x))) = 1$. Mora da je $w(x) = a$ (jer je $D = \{a\}$), pa je $I_w(p(x, f(x))) = 1$ i $I_w(\neg p(x, x)) = 1$. Iz $I_w(\neg p(x, x)) = 1$ sledi $I_w(p(x, x)) = 0$, tj. $p_I(w(x), w(x)) = 0$, tj. $p_I(a, a) = 0$, što je netačno, pa sledi da je pretpostavka bila pogrešna, odakle dalje sledi da postoji valuacija v takva da je $I_v(\mathcal{A}) = 0$, tj. sledi da je $\mathfrak{D}$ kontramodel za datu formulu $\mathcal{A}$.

(c) Pretpostavimo da je $\mathcal{L}$-struktura $\mathfrak{D} = (D, I^{\mathcal{L}})$ model date formule $\mathcal{A}$ i pretpostavimo da je skup D konačan, tj. pretpostavimo da je $D = \{d_1, d_2, \ldots, d_m\}$.

Neka je $I^{\mathcal{L}}(f) = f_I$ i $I^{\mathcal{L}}(p) = p_I$. Neka je d'_i određen na sledeći način:

- neka je d'_0 proizvoljan element skupa D;
- neka je $d'_{i+1} = f_I(d'_i)$ za $i \geq 0$.

Skup D je konačan, pa u nizu d'_i, $i = 0, 1, 2, \ldots$, mora da postoji bar jedan element koji se ponavlja, tj. postoje vrednosti j i k ($j < k$) takve da je $d'_j = d'_k$.

Na osnovu pretpostavke, $\mathfrak{D}$ je model za formulu $\mathcal{A}$, pa za proizvoljnu valuaciju v važi $I_v(\mathcal{A}) = 1$. Odatle, na osnovu definicije 3.10, sledi da važi $I_v((\forall x)(p(x, f(x)) \wedge \neg p(x, x))) = 1$ i $I_v((\forall x)(\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))) = 1$.

Iz $I_v((\forall x)(p(x, f(x)) \wedge \neg p(x, x))) = 1$ sledi da za proizvoljnu valuaciju w takvu da je $w \sim_x v$ važi $I_w(p(x, f(x)) \wedge \neg p(x, x)) = 1$. Odatle dalje sledi $p_I(w(x), f_I(w(x))) = 1$ i $p_I(w(x), w(x)) = 0$. Valuacija w je proizvoljna, pa je možemo odabrati tako da važi $w(x) = d'_i$. Tada važi $p_I(d'_i, f_I(d'_i)) = 1$ i $p_I(d'_i, d'_i) = 0$, tj. za svako i ($i = 0, 1, 2, \ldots$) važi $p_I(d'_i, d'_{i+1}) = 1$ i $p_I(d'_i, d'_i) = 0$.

S druge strane, iz $I_v((\forall x)(\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))) = 1$ sledi da za proizvoljnu valuaciju w takvu da je $w \sim_x v$ važi $I_w((\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))) = 1$. Kako je w proizvoljna valuacija, možemo je odabrati tako da važi $w(x) = d'$. Iz $I_w((\forall y)(\forall z)(p(x, y) \wedge p(y, z) \Rightarrow p(x, z))) = 1$ sledi da za proizvoljnu valuaciju w' takvu da je $w' \sim_y w$ (dakle, važi

$w'(x) = w(x) = d'$) važi $I_{w'}((\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 1$. Kako je w' proizvoljna valuacija za koju važi $w' \sim_y w$, možemo je odabrati tako da važi $w'(y) = d''$. Iz $I_{w'}((\forall z)(p(x,y) \wedge p(y,z) \Rightarrow p(x,z))) = 1$ sledi da za proizvoljnu valuaciju w'' takvu da je $w'' \sim_z w'$ (dakle, važi $w''(x) = w'(x) = w(x) = d'$ i $w''(y) = w'(y) = d''$) važi $I_{w''}(p(x,y) \wedge p(y,z) \Rightarrow p(x,z)) = 1$. Kako je w'' proizvoljna valuacija za koju važi $w'' \sim_z w'$, možemo je odabrati tako da važi $w''(z) = d'''$. Iz $I_{w''}(p(x,y) \wedge p(y,z) \Rightarrow p(x,z)) = 1$ sledi da je $I_{w''}(p(x,y) \wedge p(y,z)) = 0$ ili $I_{w''}(p(x,z)) = 1$, tj. da važi $I_{w''}(p(x,y)) = 0$ ili $I_{w''}(p(y,z)) = 0$ ili $I_{w''}(p(x,z)) = 1$, tj. da važi $p_I(w''(x), w''(y)) = 0$ ili $p_I(w''(y), w''(z)) = 0$ ili $p_I(w''(x), w''(z)) = 1$. Dakle, za svaka tri elementa d', d'', d''' skupa D važi $p_I(d', d'') = 0$ ili $p_I(d'', d''') = 0$ ili $p_I(d', d''') = 1$. Već smo dokazali da za svako i ($i = 0, 1, 2, \ldots$) važi $p_I(d'_i, d'_{i+1}) = 1$, odakle sledi da za $d' = d'_i$, $d'' = d_{i+1}$, $d''' = d_{i+2}$ (za proizvoljno i, $i = 0, 1, 2, \ldots$) mora da važi $p_I(d', d''') = 1$, tj. $p_I(d'_i, d'_{i+2}) = 1$. Analogno, jednostavno se pokazuje matematičkom indukcijom da važi $p_I(d'_i, d'_{i+l}) = 1$ za proizvoljno i, $i = 0, 1, 2, \ldots$ i proizvoljno l, $l = 1, 2, \ldots$. Dakle, važiće i $p_I(d'_j, d'_k) = 1$, tj. $p_I(d'_j, d'_j) = 1$ (jer je $d'_j = d'_k$). Međutim, već smo pokazali da za svako i ($i = 0, 1, 2, \ldots$) važi $p_I(d'_i, d'_i) = 0$, što je u kontradikciji sa $p_I(d'_j, d'_j) = 1$. Dakle, polazna pretpostavka je bila pogrešna, odakle sledi da za datu formulu $\mathcal{A}$ ne postoji model koji ima konačan domen.

52. Neka je $\mathfrak{D}$ proizvoljna $\mathcal{L}$-struktura, pri čemu za signaturu $\mathcal{L} = (\Sigma, \Pi, ar)$ važi $p \in \Pi$ i $ar(p) = 1$ i neka je V proizvoljan skup promenljivih takav da je $x, y, z \in V$. Neka je $I^{\mathcal{L}}(p) = p_I$ (gde je p_I funkcija iz D u skup $\{0, 1\}$) i neka je v proizvoljna valuacija. Dokažimo da važi $I_v((\forall x)(\forall y)(\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))) = 1$. Pretpostavimo suprotno — da važi $I_v((\forall x)(\forall y)(\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))) = 0$. To znači da postoji valuacija v_x takva da je $v_x \sim_x v$ (neka je $v_x(x) = d_x$) i $I_{v_x}((\forall y)(\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))) = 0$. To znači da postoji valuacija v_y takva da je $v_y \sim_y v_x$ (važi $v_y(x) = v_x(x) = d_x$; neka je $v_y(y) = d_y$) i $I_{v_y}((\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))) = 0$. To znači da za svaku valuaciju v_z takvu da je $v_z \sim_z v_y$ važi $I_{v_z}(p(x) \wedge p(y) \Leftrightarrow p(z)) = 0$. Odaberimo valuaciju v_z takvu da je $v_z \sim_z v_y$ (važi $v_z(x) = v_y(x) = d_x$ i $v_z(y) = v_y(y) = d_y$) na sledeći način:

(a) ako je $p_I(d_y) = 1$, neka je $v_z(z) = d_x$;

(b) ako je $p_I(d_y) = 0$, neka je $v_z(z) = d_y$.

U slučaju (a), važi $I_{v_z}(p(y)) = 1$, pa je $I_{v_z}(p(x) \wedge p(y)) = I_{v_z}(p(x)) = I_{v_z}(p(z))$, odakle sledi $I_{v_z}(p(x) \wedge p(y) \Leftrightarrow p(z)) = 1$, što je u suprotnosti sa $I_{v_z}(p(x) \wedge p(y) \Leftrightarrow p(z)) = 0$. U slučaju (b), važi $I_{v_z}(p(y)) = 0$ i $I_{v_z}(p(z)) = 0$, odakle sledi $I_{v_z}(p(x) \wedge p(y)) = 0$ i $I_{v_z}(p(x) \wedge p(y) \Leftrightarrow p(z)) = 1$, što je nemoguće. Dakle, u svakom slučaju dolazimo do kontradikcije, što znači da polazna pretpostavka nije bila ispravna. Dakle, mora da važi $I_v((\forall x)(\forall y)(\exists z)(p(x) \wedge p(y) \Leftrightarrow p(z))) =$

1. Kako je I_v proizvoljna valuacija, sledi da je data formula valjana.

57. Na primer, $\neg(\exists x)\mathcal{A} \Leftrightarrow (\forall x)\neg\mathcal{A}$.

58. Važi $(\exists x)(\mathcal{A} \Rightarrow \mathcal{B}) \equiv (\exists x)(\neg\mathcal{A} \vee \mathcal{B}) \equiv (\exists x)(\neg\mathcal{A}) \vee (\exists x)\mathcal{B} \equiv \neg(\forall x)\mathcal{A} \vee (\exists x)\mathcal{B} \equiv (\forall x)\mathcal{A} \Rightarrow (\exists x)\mathcal{B}$. Iz $(\exists x)(\mathcal{A} \Rightarrow \mathcal{B}) \equiv (\forall x)\mathcal{A} \Rightarrow (\exists x)\mathcal{B}$, na osnovu teoreme 3.13 sledi da je data formula valjana.

69. Tvrđenje je moguće dokazati indukcijom po složenosti izraza ili na sledeći način: pretpostavimo da za date izraze e_1 i e_2 postoje dva najopštija unifikatora σ_1 i σ_2. Tada postoje supstitucije λ_1 i λ_2 takve da važi $\sigma_1 = \sigma_2\lambda_2$ i $\sigma_2 = \sigma_1\lambda_1$ odakle sledi $\sigma_2 = (\sigma_2\lambda_2)\lambda_1$ i $\sigma_2 = \sigma_2(\lambda_2\lambda_1)$. Dakle, $\lambda_2\lambda_1$ je trivijalna supstitucija $[\,]$, pa, na osnovu definicije kompozicije supstitucija sledi da λ_1 i λ_2 mogu da sadrže samo zamene oblika $v' \mapsto v''$ (gde su v' i v'' simboli promenljivih), pa su unifikatori σ_1 i σ_2 jednaki do na preimenovanje promenljivih.

76. Dati uslovi mogu se reprezentovati na sledeći način:
C1: $vlasnikpsa(Janko)$
C2: $\forall x(vlasnikpsa(x) \Rightarrow volizivotinje(x))$
C3: $\forall x(volizivotinje(x) \Rightarrow (\forall y(zivotinja(y) \Rightarrow \neg udario(x, y))))$
C4: $udario(Janko, Tuna) \vee udario(Marko, Tuna)$
C5: $macka(Tuna)$
C6: $\forall x(macka(x) \Rightarrow zivotinja(x))$
Metodom rezolucije može se dokazati da iz navedenih formula sledi formula $udario(Marko, Tuna)$.

95. Pretpostavimo da je teorija $\mathcal{T}$ potpuna.

Pretpostavimo da je teorija $\mathcal{T}$ aksiomatibilna. Kako je skup aksioma teorije $\mathcal{T}$ rekurzivan, rekurzivan je i skup svih dokaza teorije $\mathcal{T}$. Za svaki od njih može se neposredno proveriti da li je dokaz neke formule. Kako je teorija $\mathcal{T}$ potpuna, za proizvoljnu rečenicu $\mathcal{A}$ važi $\mathcal{T} \vdash \mathcal{A}$ ili $\mathcal{T} \vdash \neg\mathcal{A}$. Skup svih dokaza je rekurzivan i idući redom kroz njega, naići će se (u konačno mnogo koraka) ili na dokaz za $\mathcal{A}$ ili na dokaz za $\neg\mathcal{A}$. U prvom slučaju zna se da važi $\mathcal{T} \vdash \mathcal{A}$, a u drugom slučaju zna se da važi $\mathcal{T} \nvdash \mathcal{A}$. Opisani postupak, predstavlja, dakle, proceduru odlučivanja za teoriju $\mathcal{T}$, pa je ona odlučiva.

Pretpostavimo da je teorija $\mathcal{T}$ odlučiva. Tada je skup njenih teorema rekurzivan, pa on može da ima ulogu skupa aksioma. Taj skup aksioma je rekurzivan, pa je teorija $\mathcal{T}$ aksiomatibilna.

Literatura

[1] D. Achlioptas, L. M. Kirousis, E. Kranakis, and D. Krizanc. Rigorous results for random $(2 + p)$-SAT. In Proceedings of RALCOM' 97, 1997.

[2] Dimitris Achlioptas and Yuval Peres. The Threshold for Random k-SAT is $2^k \log 2 - O(k)$. In *STOC'03*, pages 223–231, 2003.

[3] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[4] L. Bachmair and A. Tiwari. Abstract Congruence Closure and Specializations. In David A. MacAllester, editor, *Proceedings of the 17th Conference on Automated Deduction (CADE-17)*, number 1831 in Lecture Notes in Artificial Intelligence. Springer, 2000.

[5] C. Barrett, D. Dill, and J. Levitt. Validity Checking for Combinations of Theories with Equality. In *International Conference on Formal Methods in Computer-Aided Design*, number 1166 in LNCS, pages 187–201. Springer, 1996.

[6] N. S. Bjørner. *Integrating decision procedures for temporal verification*. PhD thesis, Stanford University, 1998.

[7] Everett L. Bull. Logic for Computer Science. Lecture notes, Pomona College/Harvey Mudd College, 2000. on line: http://www.cs.hmc.edu/courses/2001/spring/cs80/.

[8] Alan Bundy. *The Computer Modelling of Mathematical Reasoning*. Academic Press, 1983.

[9] Peter Cheeseman, Bob Kanefsky, and William M. Taylor. Where the really hard problems are. In John Myopoulos and Ray Reiter, editors, *Proceedings of the 12th International Joint Conference on Artificial Intelligence*, pages 331–340. Morgan Kaufmann, 1991.

[10] Stephen A. Cook. The complexity of theorem-proving procedures. In *STOC '71: Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158. ACM Press, 1971.

[11] M. James Crawford and D. Larry Auton. Experimental results on the crossover point in random 3-sat. Artificial Intelligence, 81:31–57, 1996.

[12] D. Cyrluk, P. Lincoln, and N. Shankar. On Shostak's Decision Procedure for Combinations of Theories. In M. A. McRobbie and J. K. Slaney, editors, *Proceedings of the 13th Conference on Automated Deduction*, number 1104 in Lecture Notes in Artificial Intelligence. Springer, 1996.

[13] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.

[14] Martin Davis, Ron Sigal, and Elaine Weyuker. *Computability, Complexity, and Languages (Fundamentals of Theoretical Computer Science)*. Morgan Kaufmann/Academic Press, 1994.

[15] N. Dershowitz and J.-P. Jouannaud. Rewriting systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Methods and Semantics, pages 243–320. Elsevier, Amsterdam, 1990.

[16] Ершов, Ю.Л., Лавров, И.А., Тайманов, А.Д., and Тайцлин, М.А. Елементарные теории. Успехи математических наук, XX(4(124)):37–108, 1965.

[17] E. Friedgut. Sharp threshold for graph properties and the k-sat problem. *Journal of the American Mathematical Society*, 12:1017–1054, 1999.

[18] B. M. Gabbay, C. J. Hogger, and J. A. Robinson, editors. *Handbook of Logic in Artificial Intelligence and Logic Programming*. Oxford University Press, Oxford, 1993.

[19] M. R. Garey and D. S. Johnson. *Computers and Intractability*. W. H. Freeman, New York, 1979.

[20] Ian P. Gent and Toby Walsh. The SAT phase transition. In *Proceedings of ECAI-94*, pages 105–109, 1994.

[21] Gerhard Gentzen. Untersuchungen über das logische Schliessen, I, II. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. English translation in "The Collected Papers of Gerhard Gentzen", North-Holland Publ.Co, 1969.

[22] Kurt Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatshefte für Mathematik und Physik*, 37:349–360, 1930.

[23] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[24] A. Goerdt. A treshold for unsatisfiability. In *Proceedings of the 17th International Symposium on Mathematical Foundations of Computer Science*, 1992.

[25] D. I. Good. Mechanical proofs about computer programs. In C. A. R. Hoare and J. C. Shepherdson, editors, *Mathematical Logic and Programming Languages*, pages 55–75. Prentice-Hall, 1985.

[26] D. Hilbert and P. Bernays. *Grundlagen der Mathematik (Zweite Auflage)*. Springer–Verlag, 1968. Izdanje na ruskom jeziku: Основания Математики, Москва, "Наука", 1979.

[27] David Hilbert. *Grundlagen der Geometrie*. 1899. (translation into Serbian: *Osnovi geometrije*, Naučno delo, 1957, Beograd).

[28] Louis Hodes. Solving Problems by Formula Manipulation in Logic and Linear Inequalities. In *Proceedings of the 2nd International Joint Conference on Artificial Intelligence*, Imperial College, London, England, 1971.

[29] J.N. Hooker and C. Fedjki. Branch-and-cut soultion of inference problems in propositional logic. *Ann. Math. Artif. Intell.*, 1:123–139, 1990.

[30] Predrag Janičić. GD-SAT model and crossover line. Journal of Experimental and Theoretical Artificial Intelligence, 13(3):181–198, 2001.

[31] Predrag Janičić and Alan Bundy. Strict general setting for building decision procedures into theorem provers. In Rajeev Goré, Alexander Leitsch, and Tobias Nipkow, editors, *The 1st International Joint Conference on Automated Reasoning (IJCAR-2001) — Short Papers*, Technical Report DII 11/01, pages 86–95. Universita degli Studi di Siena, Italia, 2001.

[32] Predrag Janičić and Alan Bundy. A General Setting for the Flexible Combining and Augmenting Decision Procedures. *Journal of Automated Reasoning*, 28(3):257–305, 2002.

[33] Predrag Janičić, Alan Bundy, and Ian Green. A framework for the flexible integration of a class of decision procedures into theorem provers. In Harald Ganzinger, editor, *Proceedings of the 16th Conference on Automated Deduction (CADE-16)*, number 1632 in Lecture Notes in Artificial Intelligence Series, pages 127–141. Springer, 1999.

[34] Predrag Janičić, Nenad Dedić, and Goran Terzić. On different models for generating random SAT problems. Computing and Informatics *(former* Computers and Artificial Intelligence*)*, 20(5):451–469, 2001.

[35] M. Jocković, Z. Ognjanović, and S. Stankovski. *Veštačka inteligencija, inteligentne mašine i sistemi*. Krug, Beograd, 1997.

[36] A. Kamath, R. Motwani, K. Palem, and P. Spirakis. Tail bounds for occupancy and the satisfiability treshhold conjecture. In *Proceedings 35th Symposium on Foundation of Computer Science*, pages 592–603, 1994.

[37] Deepak Kapur. Shostak's Congruence Closure as Completion. In *International Conference on Rewriting Techniques and Applications, RTA '97*, Barcelona, Spain, June 1997.

[38] D. E. Knuth and P. B. Bendix. Simple word problems in universal algebra. In J. Leech, editor, *Computational problems in abstract algebra*, pages 263–297. Pergamon Press, 1970.

[39] Peter Krauss. Quantifier elimination. In G. et al. Muller, editor, *Logic Conference, Kiel 1974*. Springer–Verlag, Berlin, 1975.

[40] T. Larrabee and Y. Tsuji. Evidence for a satisfiability threshold for random 3cnf formulas. Technical Report UUCSC-CRL-92-42, University of California, Santa Cruz, 1992.

[41] J.-L. Lassez and M.J. Maher. On Fourier's algorithm for linear arithmetic constraints. *Journal of Automated Reasoning*, 9:373–379, 1992.

[42] Лавров, И. А и Л. Л. Максимова. Задачи по теории множеств, математической логике и теории алгоритмов. Наука, Москва, 1984.

[43] George F. Luger and William A. Stubblefield. *Artificial Intelligence: Structures and strategies for complex problem solving*. Benjamin/Cummings Publishing Company, Inc., Redwood City, California, 1993.

[44] Petar Maksimović and Predrag Janičić. Simple characterization of functionally complete one-element sets of propositional connectives. *Mathematical Logic Quarterly*, 52(5):498–504, 2006.

[45] Udi Manber. *Introduction to Algorithms, A Creative Approach*. Addison-Wesley Publishing Company Inc., 1989.

[46] Per Martin-Löf. Constructive mathematics and computer programming. In *6th International Congress for Logic, Methodology and Philosophy of Science*, pages 153–175. Published by North Holland, Amsterdam. 1982., 1979.

[47] Per Martin-Löf. *Intuitionistic Type Theory*. Bibliopolis, Naples, 1984. Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980.

[48] E. Mendelson. *Introduction to Mathematical Logic*. Van Nostrand Reinhold Co., 1964.

[49] Žarko Mijajlović. Odlučive teorije. *Računarstvo*, 1(1):3–21, 1991.

[50] Žarko Mijajlović. Gödel's theorems. *Scientific Review, Series: Science and Engineering, Serbian Scientific Society*, 16:75–82, 1996.

[51] Žarko Mijajlović, Zoran Marković, and Kosta Došen. *Hilbertovi problemi i logika*. Zavod za udžbenike i nastavna sredstva, Beograd, 1986.

[52] G. David Mitchell, Bart Selman, and J. Hector Levesque. Hard and easy distributions of sat problems. In *Proceedings AAAI-92*, pages 459–465, San Jose, CA, 1992. AAAI Press/The MIT Press.

[53] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky. Phase transition and search cost in the $2+p$-sat problem. In Proceedings of the Fourth Workshop on Physics and Computation, pages 229–232. Boston University, 1996.

[54] Bernhard Nebel. Artificial Intelligence: A Computational Perspective. In Gerhard Brewka, editor, *Principles of Knowledge Representation*, pages 237–266. CSLI Publications, 1996.

[55] G. Nelson and D. C. Oppen. Fast decision procedures based on congruence closure. *Journal of the ACM*, 27(2):356–364, April 1980. Also: Stanford CS Report STAN-CS-77-646, 1977.

[56] University of St. Andrews. History of Mathematics. on-line at: http://www-gap.dcs.st-and.ac.uk/~history/.

[57] Christos Papadimitriou. *Computational Complexity*. Addison Wesley Longman, 1995.

[58] Ian Pratt. *Artificial intelligence*. The Macmillan Press Ltd., London, 1994.

[59] O. Michael Rabin. Decidable theories. In Barwise Jon, editor, *Handbook of Mathematical Logic*, pages 595–629. North–Holland Publishing Company, 1977.

[60] Greg Restall. *An introduction to substructural logic*. Routledge, Taylor and Francis Group, London and New York, 2000.

[61] J. A. Robinson. A machine oriented logic based on the resolution principle. *J Assoc. Comput. Mach.*, 12:23–41, 1965.

[62] Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Prentice-Hall International, London, 1995.

[63] Josef Schicho. Logic II. Lecture notes, RISC Linz, Johannes Kepler University, 1998. on line: http://www.risc.uni-linz.ac.at/people/jschicho.

[64] Joseph R. Shoenfield. *Mathematical logic*. Addison–Wesley, Reading, MA, 1967.

[65] R. E. Shostak. Deciding combinations of theories. *Journal of the ACM*, 31(1):1–12, January 1984. Also: *Proceedings of the 6th International Conference on Automated Deduction*, volume 138 of *Lecture Notes in Computer Science*, pp. 209–222. Springer-Verlag, June 1982.

[66] Raymond M. Smullyan. *First Order Logic*. Springer-Verlag, Berlin, 1968.

[67] Željko Sokolović. Odlučivost matematičkih teorija. magistarski rad, Matematički fakultet, Beograd, 1987.

[68] Irena Spasić and Predrag Janičić. *Teorija algoritama, jezika i automata – zbirka zadataka*. Matematički fakultet, Beograd, 1999.

[69] Larry Stockmeyer. Classifying the computational complexity of problems. *The Journal of Symbolic Logic*, 52(1):1–44, March 1987.

[70] R. E. Tarjan. Efficiency of a good but not linear set union algorithm. *J. ACM*, 22(2):215–225, April 1975.

[71] A. Tarski, A. Mostowski, and Robinson R. M. *Undecidable Theories*. North Holland, 1953.

[72] Alfred Tarski. *Logic, Semantics, Metamathematics*. Hackett, Indianapolis, 1983. 1st edition edited and translated by J. H. Woodger, Oxford 1956.

[73] A.S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, 2000.

[74] Miodrag Živković. *Algoritmi*. Matematički fakultet, Beograd, 2000.

[75] Larry Wos. *Automated Reasoning: 33 Basic Research Problems*. Prentice-Hall, 1987.

Indeks

$\mathcal{L}$-struktura (eng. $\mathcal{L}$-structure), 88

Abel (Abel), 157, 160, 170–172, 213
Akerman (Ackerman), 206
aksiomatska teorija (eng. axiomatic theory), 50
alfabet (eng. alphabet), 7
analitički računi (eng. analytic calculi), 72
analiza najgoreg slučaja (eng. worst case analysis), 185
Aristotel, 1, 213
arnost (stepen) (eng. arity (degree)), 84
atomička formula (eng. atomic formula), 85

bazna formula (eng. ground formula), 85
bazni term (eng. ground term), 85
Bet (Beth), 39, 214
binarna rezolucija (eng. binary resolution), 120
Brauer (Brouwer), 3, 209, 214
Bul (Boole), 2, 214

Čerč (Church), 3, 165, 214
čist predikatski račun (eng. pure predicate calculus), 157
čista teorija jednakosti (eng. pure theory of equality), 158

Dževons (Javons), 2, 215
De Morgan (De Morgan), 18, 24, 95, 215
Dejvis (Davis), 28, 215
direktna posledica (eng. direct consequence), 50
direktna pravila (eng. direct rules), 136
disjunkt (eng. disjunct), 19
disjunktivna normalna forma (eng. disjunctive normal form), 24
dobro zasnovane formule (eng. well-formed formulae), 50, 85
dokaz (dedukcija) (eng. proof (deduction)), 50, 53, 65, 70
dokazivanje pobijanjem (eng. proof by refutation), 38, 107
domen (eng. domain), 10
domen (nosač, univerzum) (eng. domain, carrier, universe), 88
doseg (eng. scope), 87

egzistencijalno zatvorenje (eng. existential closure), 87
ekvivalencijsko zatvorenje (eng. equivalence closure), 178
eliminacija kvantora (eng. quantifier elimination), 170
Erbran (Herbrand), 5, 107, 115, 215
Erbranov model (eng. Herbrand model), 110
Erbranova baza (eng. Herbrand base), 109
Erbranove interpretacije (eng. Herbrand interpretations), 108
Erbranovov univerzum (eng. Herbrand universe), 108

fazna promena (eng. phase tranzition), 190
Fon Nojman (von Neumann), 220
forma Kovalskog (eng. Kowalski form), 121

formalism (eng. formalism), 208
formalna teorija (eng. formal theory), 50
formula (eng. formula)
dokaziva (eng. provable), 50, 53, 66, 71, 147, 153, 155
egzistencijalno zatvorena (eng. existentially closed), 87
sečenja (eng. cut formula), 72
tačna u interpretaciji (eng. true in an interpretation), 10, 90
tačna u valuaciji (eng. true in a valuation), 10
univerzalno zatvorena (eng. universally closed), 87
valjana u $\mathcal{L}$ strukturi (eng. formula valid in $\mathcal{L}$), 90
zadovoljiva (eng. satisfiable), 90
Frege (Frege), 2, 215
funkcija zadovoljivosti (eng. satisfiability function), 192
funkcijski simboli (eng. function symbols), 84
Furije (Fourier), 172, 216

Gedel (Gödel), 3, 167, 207, 216
Gencen (Gentzen), 3, 64, 70, 153, 155, 216
generalizacija (eng. generalisation), 147
Gilmor (Gilmore), 112, 217
Grasman (Grassmann), 2, 217
grupisanje (eng. factoring), 133

halting problem (eng. halting problem), 4, 206
Hilbert (Hilbert), 3, 206, 209, 217
Hintika (Hintikka), 44, 139, 217
Hintikin skup (eng. Hintikka set), 44, 139
hipoteze (premise) (eng. hypothesis (premises)), 50, 53
Hobs (Hobbes), 2, 218
Hor (Hoare), 210, 217
Horn (Horn), 124, 131, 218

instanca (primerak) (eng. instance), 97
bazna (eng. ground), 97
interpretacija (eng. interpretation), 10, 88
intuicionizam (eng. intuitionism), 209
iskaz (eng. proposition), 8
iskazna formula (eng. propositional formula), 8, 52
atomička (eng. atomic), 8
kontradikcija (eng. contradictory), 10
nezadovoljiva (eng. unsatisfiable), 10
poreciva (eng. falsifiable), 10
tautologija (eng. tautology), 10
valjana (eng. valid), 10
zadovoljiva (eng. satisfiable), 10
iskazna logika (eng. propositional logic), 7
iskazna slova (eng. propositional letters), 7
iskazne formule (eng. propositional formulae
logički ekvivalentne (eng. logically equivalent), 16
iskazne promenljive (eng. propositional variables), 8
iskazni račun (eng. propositional calculus), 50
isključenje trećeg, tertium non datur (eng. excluding middle), 51, 64, 153
istinitosna funkcija (eng. truth function), 21
istinitosna tablica (eng. truth table), 13
izraz (eng. expression), 96, 115
izvod (end. derivation), 53, 65, 70
izvod tautologije (eng. tautology derivation), 98

jednosmerno uparivanje (eng. one way-matching), 119
jezik prvog reda (eng. first order language), 85

Kalmar (Kalmár), 59, 218
kanonska disjunktivna normalna forma (eng. canonical disjunctive normal form), 26
kanonska konjunktivna normalna forma (eng. canonical conjunctive normal form), 27
Kenig (König), 140, 218
klauza (eng. clause), 8, 19, 85
  činjenica (eng. assertion), 124
  ciljna (eng. goal), 124
  Hornova (eng. Horn), 124
  implikaciona (eng. implication), 124
  jedinična (eng. unit), 19
  prazna (eng. empty), 124
klauzalna forma (eng. clausal form), 103
Knut-Bendiksova procedura upotpunjavanja (eng. Knuth-Bendix completion procedure, 177
komplementni literali (eng. complementary literals), 32, 120
kongruentno zatvorenje (eng. congruence closure), 177, 178
  Nelson–Openov algoritam (Nelson–Oppen's algorithm), 179
konjunkt (eng. conjunct), 19
konjunktivna normalna forma (eng. conjunctive normal form), 23, 103
konstruktivizam (eng. constructivism), 209
kontramodel (eng. countermodel), 90
konzistentan (zadovoljiv) skup (eng. consistent (satisfiable) set), 90
Kovalski (Kowalski), 121, 218
Krispius, 2, 218
Kuk (Cook), 189, 190, 218
kvantifikatori (kvantori) (eng. quantifiers), 84, 146

Lajbnic (Leibnitz), 2, 218
Lef (Löf), 5, 209, 211, 218
lema o dijagonalizaciji (eng. diagonal lemma), 203
lema o fiksnoj tački (eng. fixed point lemma), 203
lema o samoukazivanju (eng. self-reference lemma), 203
linearna input rezolucija (eng. linear input resolution), 131
linearna strategija (eng. linear strategy), 131
literal (eng. literal), 8, 85
logička ekvivalencija (eng. logical equivalence), 16, 93
logička posledica (eng. logical consequence), 14, 93
logičke konstante (eng. logical constants), 8, 84
logički simboli (eng. logical symbols), 84
logički veznici (eng. logical connectives), 7, 52, 84, 146
logika drugog reda (eng. second order logic), 83
logika prvog reda (predikatska logika) (eng. first order logic (predicate logic)), 83
logika višeg reda (eng. higher order logic), 83
Logman (Logemann), 28, 219
Loveland (Loveland), 28, 219
Lovenhajm (Lövenheim), 114, 219
Lukašijevič (Lukasiewicz), 22, 219
Lul (Lull), 2, 219

metajezik (eng. metalanguage), 51
metod analitičkih tabloa (method of analytic tableaux), 39
metod rezolucije (eng. resolution method), 32, 119
  sistematski (eng. systematic), 130
metod tabloa (eng. tableaux method), 39, 135
  sistematski (eng. systematic), 142
Mockin (Motzkin), 172, 220
model (eng. model), 10, 90

modus ponens (eng. modus ponens), 52, 147
multiskup (eng. multiset), 28

nadole zasićen skup (eng. downwards saturated set), 44
nekonzistentan (nezadovoljiv, protivrečan, kontradiktoran) skup (eng. inconsistent (unsatisfiable, contradictory) set), 90
nelogički simboli (eng. non-logical symbols), 84
Nelson (Nelson), 179, 220
neuređeno stablo (eng. non-ordered tree), 34
NP-kompletni problemi (eng. NP-complete problems), 7, 11, 80, 186, 190
NP-kompletnost (eng. NP-completeness), 186
numeral (eng. numeral), 198, 200

objektni jezik (eng. object language), 51
Open (Oppen), 179, 220
označena formula (eng. signed formula), 39

Patnam (Putnam), 28, 220
Peano (Peano), 200, 208
platonizam (eng. platonism), 207
pobijanje (eng. refutation), 38
podteorija (eng. subtheory), 169
pomoćni simboli (eng. auxiliary simbols), 8, 52, 84, 146
posledica (eng. consequence), 50, 53
Post (Post), 3, 115, 165, 220
potformula (eng. subformula), 9
potpun skup veznika (eng. complete set of connectives), 22
potpunost za pobijanje (eng. refutation complete), 125
pravila izvođenja (rules of inference), 50
pravilo paramodulacije (eng. paramodulation rule), 133
pravilo rezolucije (eng. resolution rule), 32
pravilo **A** (eng. rule **A**), 150
pravilo **C** (eng. rule **C**), 151
pravilo **E** (eng. rule **E**), 150
prazna klauza (eng. empty clause), 28
predikatska logika (logika prvog reda) (eng. predicate logic (first order logic)), 83
predikatski račun (eng. predicate calculus), 145
predikatski simboli (eng. predicate symbols), 84
prednost jediničnim klauzama (eng. unit preference), 132
prelomna tačka (eng. crossover point), 192
preneks normalna forma (eng. prenex normal form), 100
primerak (instanca) (eng. instance), 97
  bazni (eng. ground), 97
prirodna dedukcija (eng. natural deduction), 64, 153
problem odlučivanja (eng. decision problem), 206
problem unifikacije (eng. unification problem), 115
procedura odlučivanja (eng. decision procedure), 168
PROLOG, 124
promenljive (eng. variables), 84, 146
provera pojavljivanja (eng. occur check), 117

račun sekvenata (eng. sequent calculus), 70, 155
rampa (eng. turnstyle), 50, 53
Rasel (Russel), 3, 207, 221
Raselov paradoks (eng. Russell's paradox), 198, 207
reč nad alfabetom (eng. word over alphabet), 7
rečenica (eng. sentence), 87
rečnik (eng. vocabulary), 84

rekurzivan skup (eng. recursive set), 167
rekurzivno nabrojiv skup (eng. recursively enumerable set), 167
rezolventa (eng. resolvant), 32
Robinson (Robinson), 31, 221
roditelji rezolvente (eng. parents of the resolvant), 32

sadržanost (eng. subsumption), 133
samooznačavanje (eng. self denotation), 108
SAT problem (eng. SAT problem), 7, 11, 80, 187, 189, 190, 193, 196
sekvent (eng. sequent), 70, 155
semantički tablo (eng. semantic tableaux), 39
semantika (eng. semantics)
  iskazne logike (eng. of propositional logic), 10
  predikatske logike (eng. of predicate logic), 88
semantika Tarskog (eng. Tarski semantics), 10, 88
Šefer (Sheffer), 22, 222
signatura (eng. signature), 84
silogizam (eng. silogism), 1
sintaksa (eng. syntax)
  iskazne logike (eng. of propositional logic), 7
  predikatske logike (eng. of predicate logic), 84
sistematski metod rezolucije (eng. systematic resolution method), 130
sistematski metod tabloa (eng. systematic tableaux method), 142
sistemi za prezapisivanje (eng. rewriting systems), 26
sistemi za prezapisivanje termova (eng. term rewriting systems), iii
Skolem (Skolem), 5, 103, 114, 221
Skolemizacija (eng. skolemization), 103
Skolemove funkcije (eng. Skolem functions), 103
Skolemove konstante (eng. Skolem constants), 103
skup aksioma (eng. set of axioms), 50
skup iskaznih formula (eng. set of propositional formulae, 8
  kontradiktoran (eng. contradictory), 11
  zadovoljiv (eng. satisfiable), 11
skup iskaznih formula (eng. set of propositional formulae), 52
skup potpore (eng. set of support), 132
skup prirodnih brojeva (eng. set of natural numbers), 9
slaba ekvivalencija (eng. weak equivalence), 103
složenost (eng. complexity), 9, 86, 186
slobodna promenljiva (eng. free variable), 87
slobodno pojavljivanje promenljive (eng. free occurrence of a variable), 86
Smaljan (Smullyan), 39, 222
stablo (eng. tree)
  binarno (eng. binary), 34
  neuređeno (eng. non-ordered), 34
  uređeno (eng. ordered), 34
svojstvo potformula (eng. subformula property), 155
svojstvo potformule (eng. subformula property), 72

tačka fazne promene (eng. phase transition point), 192
Tarski (Tarski), 4, 209, 222
tautologija prvog reda (eng. first order tautology), 98
teorema (eng. theorem), 50, 53, 66, 71, 147, 153, 155

teorija (eng. theory)
aksiomatibilna (eng. axiomatizable), 168
kompletno proširenje (eng. complete extension), 169
konačno proširenje (eng. finite extension), 169
konzervativno proširenje (eng. conservative extension), 169
konzistentna, neprotivrečna (eng. consistent), 63, 157
neodlučiva (eng. undecidable), 50
odlučiva (eng. decidable), 50, 62, 168
potpuna, kompletna (eng. complete), 168
proširenje (eng. extension), 169
prvog reda (eng. first order), 156
term (eng. term), 84
slododan za primenljivu (eng. free for a variable), 146
tertium non datur, isključenje trećeg (eng. excluding middle), 51, 64, 153
Tjuring (Turing), 3, 165, 223

ulazna strategija (eng. input strategy), 131
unifikabilni izrazi (eng. unifiable expressions), 115
unifikator (eng. unifier), 115
najopštiji (eng. most general), 115
univerzalno zatvorenje (eng. universal closure), 87
univerzum (eng. universe), 10
UNSAT problem (eng. UNSAT problem), 195

Vajthed (Whitehead), 3, 207, 223
valjana formula (eng. valid formula), 90
valuacija (eng. valuation)
zadovoljavajuća (eng. satisfying valuation (interpretation)), 10
valuacija (eng. valuation, assignment), 10, 88
vezana promenljiva (eng. bound variable), 87
vezano pojavljivanje promenljive (eng. bound occurrence of a variable), 86
Vos (Wos), 5, 211, 223
vrednost (eng. value), 88

zadovoljavajuća interpretacija (eng. satisfying interpretation), 90
zamena (supstitucija) (eng. substitution), 95, 97
zasićenje (saturacija) (eng. saturation), 111