U N I V E R Z I T E T  U  B E O G R A D U
PRIRODNO-MATEMATIČKI FAKULTET
INSTITUT ZA MATEMATIKU

Hotomski Z. Petar

# METODE I PRAVILA ZA MEHANIČKO DOKAZIVANJE TEOREMA U TEORIJAMA PRVOG REDA SA MATEMATIČKOM INDUKCIJOM

DOKTORSKA DISERTACIJA

ОСНОВНА ОРГАНИЗАЦИЈА УДРУЖЕНОГ РАДА
ЗА МАТЕМАТИКУ, МЕХАНИКУ И АСТРОНОМИЈУ
Б И Б Л И О Т Е К А
Број: Dokt. 134|1
Датум: 17.6.1983

BEOGRAD 1982.godine

ЗА КАТЕДРУ ...

Број: _____

Датум: _____

# S A D R Ž A J


PREDGOVOR 1

UVODNE NAPOMENE 5

1. O RAZVOJU VEŠTAČKE INTELIGENCIJE I MEHANIČKOG REŠAVANJA ZADATAKA 5

2. O RAZRADI PROGRAMA ZA DOKAZIVANJE TEOREMA 9

3. PRECIZIRANJE ZADATKA MEHANIČKOG DOKAZIVANJA TEOREMA 12

3.1. Metoda potpunog pregleda. Graf dokaza teorema 13

3.2. Napomene o terminologiji 16

G L A V A I

MEHANIČKO DOKAZIVANJE TEOREMA ISKAZNOG RAČUNA 18

1. ARITMETIČKA METODA PREPOZNAVANJA IZVODLJIVOSTI 18

1.1. Neka obeležja argumentnog dela tablice bulove f-je 18

1.2. Proširenje bulovih operacija skupa $L_2$ na $L_{2k}$ 22

1.3. Karakterizacija teorema iskaznog računa - aritmetička metoda prepoznavanja izvodljivosti 24

1.4. Mogućnost programske algoritmizacije 26

G L A V A II

TEORIJSKE OSNOVE MEHANIČKOG DOKAZIVANJA TEOREMA U PREDIKATSKOM RAČUNU PRVOG REDA 28

1. NEODLUČIVOST I OGRANIČENJA NA MEHANIČKE PROCEDURE 28

2. ERBRANOVA TEOREMA ZA KONAČAN NEZADOVOLJIV SKUP SASTAVAKA 31

2.1. Skolemizacija i skup sastavaka 31

2.2. Erbranov univerzum i Erbranova teorema 32

3. PRAVILO REZOLUCIJE. ALGORITAM UNIFIKACIJE 35

3.1. Fundamentalna rezolucija 35

3.2. Zamene, unifikacija i algoritam unifikacije 37

3.3. Pravilo rezolucija 40

4. PROCEDURE MEHANIČKOG DOKAZIVANJA TEOREMA ZASNOVANE NA REZOLUCIJI 42

4.1. Specifične forme rezolucije (informativan pregled) 43

4.1.1. Semantička rezolucija 43

4.1.2. Uredjena rezolucija 45
4.1.3. Hiperrezolucija 46
4.1.4. Rezolucija potpornog skupa 46
4.1.5. Linearna i OL-rezolucija 47
4.2. Strategije pretraživanja (skice osnovnih ideja) 51
4.2.1. Strategije uprošćavanja 51
4.2.2. Strategije zasnovane na funkcijama ocene 52
4.3. Blok sheme algoritama pobijanja zasnovanih na raznim formama rezolucije 54
4.3.1. Opšta blok shema za binarnu rezoluciju 54
4.3.2. Blok shema algoritma pobijanja za hiperrezoluciju 55
4.3.3. Blok shema za uredjenu linearnu OL-rezoluciju 56

G L A V A III
MATEMATIČKA INDUKCIJA U DOKAZIMA "REDUCTIO AD ABSURDUM" 58
1. PRAVILA INDUKCIJE U TEORIJI PRVOG REDA 58
1.1. Pravila P1 i P2. Osnovno pravilo indukcije 60
1.2. Generalizacija osnovnog pravila indukcije 62
1.3. Pravilo indukcije za članove disjunkcije 68
1.4. Primeri dokaza reductio ad absurdum primenom pravila 69
2. POTPUNOST PRAVILA INDUKCIJE 71
3. PRINCIP OBRATNE INDUKCIJE U NEFORMALIZOVANIM DOKAZIMA REDUCTIO AD ABSURDUM 73

G L A V A IV
MATEMATIČKA INDUKCIJA U MEHANIČKOM DOKAZIVANJU TEOREMA 75
1. O REALIZACIJI MATEMATIČKE INDUKCIJE U MEHANIČKOM DOKAZIVANJU 75
1.1. Dovoljni uslovi za realizaciju matematičke indukcije rezolucijskom procedurom pobijanja 75
1.2. Realizacija matematičke indukcije po J.L.Darlington-u 80
1.2.1. Nedostaci f-tehnike. Pravilo paramodulacije 83
2. PRAVILO INDUKCIJE U MEHANIČKOM DOKAZIVANJU TEOREMA 84
2.1. Algoritam za odredjivanje zamene 87
2.2. Ugradjivanje pravila binarne indukcije u procedure zasnovane na rezoluciji 91
3. O POTPUNOSTI PRAVILA BINARNE INDUKCIJE U MEHANIČKOM DOKAZIVANJU TEOREMA METODOM POBIJANJA 93

G L A V A  V

INFORMACIJE O PROGRAMSKOJ REALIZACIJI REZOLUCIJSKO-INDUKCIJSKE METODE DOKAZIVANJA TEOREMA 98

1. PROGRAMSKI MODUO ZA REZOLUCIJSKO-INDUKCIJSKO DOKAZIVANJE TEOREMA U TEORIJAMA PRVOG REDA 99

1.1. Opšte informacije 99

1.2. Oblik registrovanja podataka 101

1.3. Ulazni podaci, nizovi i ograničenja 103

2. PREGLED POTPROGRAMA MODULA ZA REZOLUCIJSKO-INDUKCIJSKO DOKAZIVANJE TEOREMA 107

2.1. Kratak opis funkcija pojedinih potprograma 107

2.2. Struktura programskog modula 113

3. INFORMACIJA O PRVIM REZULTATIMA TESTIRANJA 115

B I B L I O G R A F I J A 118

# P R E D G O V O R

Mehaničko dokazivanje teorema je pravac u kiberneti ci koji ima za cilj modeliranje procesa dokazivanja teorema na računarima. Dokazivanje teorema primenom računara u tesnoj je vezi sa "veštačkom inteligencijom" - disciplinom koja istražuje mogućnosti računara u intelektualnoj sferi.

Teorijsku osnovu za mehaničko dokazivanje teorema čine algebra i matematička logika, posebno teorija logičkog izvodjenja i teorija algoritama. Programski sistem za mehaničko dokazivanje teorema obuhvata: formalizme za predstavljanje problema, metode i procedure traženja dokaza, algoritme i sheme programa, programske jezike i metode programiranja. Izgradjivanje sistema ima povratno dejstvo na teorije u okviru kojih se sistem razvija. Na primer, ne prilagodjenost računara za neposrednu realizaciju pravila izvodjenja razradjenih u logici, malaže razradu novih metoda i pravila izvodjenja. Zbog toga novi pristupi i metode često imaju širi značaj.

Prvi pokušaji programiranja dokaza teorema datiraju iz 50-tih godina ovog veka. Zatim je usledio intenzivan razvoj metoda dokazivanja i tehnika programiranja, praćen usavršavanjem računara. Ipak, postignuti praktični rezultati znatno zaostaju za prvobitnim predvidjanjima.

Polje primene mehaničkog dokazivanja teorema je vrlo široko. Osim u raznim oblastima matematike, koristi se kao aparat i u raznim zadacima kibernetike: prepoznavanje oblika, ponašanje robota, sistemi za vodjenje dijaloga na prirodnom jeziku, provera korektnosti programa, sistemi obučavanja, igre i dr.

U ovom radu razmatramo neke poznate, i navodimo nove metode za mehaničko dokazivanje teorema u klasičnom iskaznom računu i teorijama prvog reda sa matematičkom indukcijom.

Sadržaj je podeljen u pet glava. Prvoj glavi prethode Uvodne napomene koje čine samostalnu celinu.

U Uvodnim napomenama navode se prema literaturi, važniji rezultati u vezi sa razvojem veštačke inteligencije i mehanič kog rešavanja zadatąka. Poseban osvrt daje se na rešavanje ne kih matematičkih zadataka, dokazivanje teorema i tendencije ra zvoja. Navodi se okviran pregled programa. Precizira se zada- tak dokazivanja teorema.

U Glavi I izlažemo jednu novu, aritmetičku metodu za pre poznavanje izvodljivosti u iskaznom računu. Metoda je zasnova na na ideji aritmetizacije i numeričkom kriterijumu za prepo- znavanje izvodljivosti. Nešto izmenjena verzija ove metode ob javljena je u [70]. Kao pomoćni rezultati navode se neka obe- ležja argumentnog dela tablice bulove funkcije i pokazuje da se taj deo tablice može kompaktno zapisati pomoću konkatenacije. Proširuju se bulove operacije sa $L_2 = \{0,1\}$ na skup $L_{2k}$ , $k \in N$. Operacije na $L_{2k}$ izražavaju se pomoću običnih aritmetičkih ope racija: sabiranje, oduzimanje i generalisane konjunkcije. Razmatra se mogućnost programske realizacije ove metode. Po ov oj metodi proces izvodjenja zamenjuje se izračunavanjem vredno sti aritmetičkog izraza. To daje mogućnost za jednostavno prog ramiranje primenom funkcijskih naredbi i funkcijskog potprogra ma za generalisanu konjunkciju. Osim toga, postižu se i uštede u memorijskom prostoru.

Glava II sadži teorijske osnove mehaničkog dokazivanja teorema u predikatskom računu. Na osnovu literature izlažemo razne pojmove i poznate rezultate koje koristimo u daljem iz- laganju. Osnovni sadržaji su: pravilo rezolucije, algoritam uni fikacije, specifične forme rezolucije i procedure traženja do- kaza. Osim sistematskog izlaganja rezultata, sačinjene su i blok sheme algoritama pobijanja za pojedine forme rezolucije. Ova glava ne sadrži nove rezultate, pa pod uslovom da su sadr- žaji koje obuhvata poznati, može se izostaviti pri čitanju rada.

Glava III sadrži rezultate o matematičkoj indukciji u dokazima reductio ad absurdum za teorije prvog reda sa aksiomom indukcije. Uvode se pravila indukcije koja su naročito pogodna za takve dokaze. Dokazuje se korektnost i potpunost ovih pravila kad se uz MP (modus ponens) i GEN (generalizacija) primenjuju u pomenutim teorijama. Pravilo za članove disjunkcije, uopštenje je ostalih pravila i pogodno je za primenu u mehaničkom dokazivanju teorema. Navode se primeri dokaza primenom uvedenih pravila. Osim formalizovanih dokaza, razmatraju se i neformalizovani dokazi od suprotnog matematičkom indukcijom. Za tu namenu formuliše se princip obratne indukcije, a njegova primena ilustruje se primerima.

Glava IV sadrži metode i pravila za mehaničko dokazivanje teorema u teorijama prvog reda koje dopuštaju primenu matematičke indukcije. Prvo se navode dovoljni uslovi za realizaciju matematičke indukcije primenom samo pravila rezolucije. Zatim izlažemo realizaciju matematičke indukcije po J.L.Darlingtonu [32]. Tehnika F-svodjenja, opisana u [32] koristi aksiome logike drugog reda. Osnovni nedostatak ovog prilaza je što se aksioma indukcije zadržava u polaznom skupu i tako omogućuje generisanje suvišnih posledica. Sličan nedostatak, kad je reč o aksiomama jednakosti, otklonili su Robinson i Wos [174], uvodjenjem pravila paramodulacije. Pravilo binarne indukcije koje uvodimo, otklanja pomenute nedostatke i shema-aksiomu matematičke indukcije eliminiše iz polaznog skupa. Time se smanjuje broj generisanih posledica i skraćuje dokaz.
Modifikuje se algoritam unifikacije. Dobijeni algoritam za odredjivanje zamene predstavlja uopštenje algoritma unifikacije.
Razmatra se ugradjivanje pravila binarne indukcije u postojeće procedure zasnovane na rezoluciji.
U završnom delu ove glave izlažu se rezultati o potpunosti pravila binarne indukcije u mehaničkom dokazivanju teorema, kad se za to koristi rezolucijsko-indukcijska procedura pobijanja.
Dokazan je stav potpunosti za jednu dovoljno opštu podteoriju teorije prvog reda i navedeni su uslovi pod kojima potpunost važi za celu teoriju.

Glava V sadrži informacije o programskoj realizaciji rezolucijsko-indukcijske procedure pobijanja, koja je zasnovana na uredjenoj linearnoj rezoluciji i pravilu binarne indukcije. Opisuju se karakteristike programskog modula izgrađenog za rezolucijsko-indukcijsko dokazivanje teorema u teorijama prvog reda i navode prvi test-primeri.
Ovaj programski moduo inkorporiran je u interaktivni sistem "Graph" za klasifikaciju i unapredjivanje znanja u oblasti teorije grafova, koji se razvija na Elektrotehničkom fakultetu u Beogradu pod rukovodstvom prof.dr Dragoša Cvetkovića.

Želim da izrazim posebnu zahvalnost prof.dr Mirku Stojakoviću, prof.dr Nedeljku Parezanoviću, prof.dr Slaviši Prešiću, dr Marici Prešić, dr Žarku Mijajloviću i mr Dragani Jemuović za sugestije, primedbe, uputstva i posvećeno vreme. Za podsticaje i pomoć pri koncipiranju i testiranju programskog modula za rezolucijsko-indukcijsko dokazivanje teorema, naročito sam zahvalan prof.dr Dragošu Cvetkoviću.

# U V O D N E  N A P O M E N E

## 1. O RAZVOJU VEŠTAČKE INTELIGENCIJE I MEHANIČKOG REŠAVANJA ZADATAKA

Na mogućnost spoznavanja i opisivanja zakonitosti mišljenja ukazano je još u antičko doba (dela Permenida, Zeno na, Aristotela). U XVII veku Lajbnic radi na projektima forma lizacije jezika i mišljenja i mašta o stvaranju mašine koja bi umesto ljudi mehanički vršila dokaze ( [162], str.142).

Pojavom računara 40-tih godina našeg veka i sintezom sa rezultatima matematičke logike, stvoreni su uslovi za dublje prodiranje u intelektualnu sferu. Saznanja i rezultati do ko jih je došao A. Tjuring naveli su ga da bezrezervno veruje u mogućnost stvaranja inteligentnih mašina. Za prepoznavanje inteligentnog ponašanja mašine Tjuring je 1950. godine pred-ložio sledeći test:

> "Ako je ponašanje mašine, koja odgovara na pitanja, nemoguće razlikovati od ponašanja čoveka, koji odgovara na analogna pitanja, onda ona poseduje inteligenciju." ( [158], str.21).

Pitanje ostvarljivosti "inteligentne mašine" izazvalo je žive, često polemičke diskusije. Na neplodotvornost takvih di skusija uticala je pre svega neprecizna formulacija "veštačke inteligencije", a s druge strane, zanemarivanje razlike izme-dju potencijalne ostvarljivosti i obima praktičnih teškoća na tom putu. Medjutim, kao posledica naučno-tehnološke revolucije javlja se nužnost automatizacije pojedinih intelektualnih ak-tivnosti. Tako je veštačka inteligencija, koja je još do sre-dine 60-tih godina imala dosta labilan naučni oslonac, privuk la veliki broj istraživača najrazličitijih profila. O naglom razvoju koji je usledio, indirektno govori i sledeća činjenica:

> "Za četiri godine, protekle od izlaska sjajne monografije N. Nilsona "Veštačka inteligencija" ( [143] ), ona je postala sa mo kanonski (i zato nezamenljivi) uvod u teoriju rešavanja zadataka, jer su u nizu pravaca dobijeni novi važni rezultati,

a niz centralnih problema veštačke inteligencije u njoj uopšte nije odražen... Većina ovih problema istaknuta je pre svega u intenzivnim istraživanjima 1970-1975.god. u oblasti robota koji poseduju inteligenciju."([158], str. 9)

Intenzivan razvoj jedan je od razloga što još uvek ne postoji jedinstvena i precizna definicija veštačke inteligencije. "Desetine definicija, razjašnjenja i preciziranja, koje su se pojavile u domaćoj[1)] i stranoj literaturi za poslednjih 10-12 godina, nisu pojasnile ovaj problem i krug ideja koje leže u njegovoj osnovi." (G.S.Pospelov i D.A.Pospelov,1974; [158],str. 21). Najopštije rečeno "to je rešavanje 'intelektualnih' zadataka primenom automatskih metoda, pre svega uz pomoć računara... Cilj radova u veštačkoj inteligenciji je stvaranje mašina, koje izvode takve aktivnosti, za koje je obično potrebna inteligencija čoveka. U osnovne pravce ove oblasti ubrajaju se automatske metode rešavanja zadataka, 'razumevanja' i prevodjenja jezika, dokazivanje teorema i prepoznavanje vizuelnih oblika i govora." ([143],str.5 i 7).

Umesto jedne opšte teorije veštačke inteligencije postoji niz teorijskih disciplina koje su u vezi sa njom. Sve češće se govori o sistemu veštačke inteligencije. Takav sistem odredjuje se u [158],str. 23, kao sistem sposoban za:

"- prikupljanje i korekciju znanja na osnovu aktivnog primanja informacije o svetu i generalisanog iskustva,
- svrsishodno ponašanje na osnovu prikupljenog znanja."

U razradi sistema veštačke inteligencije suštinsku ulogu ima mogućnost formalizacije neformalno postavljenih zadataka i nalaženje dovoljno efektivnih procedura pretraživanja u mnoštvu varijanata. Poseduju li takvi sistemi autonomni intelekt, pitanje je koje u sebi sadrži dosta neodredjenosti, a odgovor zavi si od pozicije (filozofske, posebno gnoseološke i psihološke) sa koje mu se pristupa. Neosporno je medjutim, da su postojeći sistemi sposobni da približno kao čovek, ponekad i uspešnije od čoveka, obavljaju pojedine aktivnosti koje su do nedavno smat-

---

1) Misli se na literaturu u SSSR.

rane isključivom privilegijom čoveka ili su mu čak bile nedostupne.

Veliki broj problema iz domena veštačke inteligencije može se predstaviti u obliku rešavanja zadataka, pa znanja sistema uključuju univerzalne i specijalne metode rešavanja zadataka. Osim numeričkih metoda koriste se metode logičke i heurističke prirode. Prihvaćeno je da se pod sopstvenim metodama veštačke inteligencije podrazumevaju upravo one koje se zasnivaju na raznim oblicima predstavljanja problema i raznim procedurama pretraživanja. Medjutim, primećena je obrnuta zavisnost izmedju opštosti predstavljanja i moćnosti metoda pretraživanja:

> "Pri pokušaju izgradjivanja opšteg rešavaoca zadataka bićemo prinudjeni da ga snabdemo opštim i zato relativno slabim metodama rešavanja." ([158] , str. 39).

Domen prvih istraživanja u oblasti veštačke inteligencije bile su razne igre i neki matematički zadaci. Razloge za takav izbor okarakterisao je M. Minski: "Igre i matematički zadaci uzimaju se ne zato što su prosti i jasni, već zato što oni pri minimalnim početnim strukturama daju najveću složenost ..." ([158], str. 23).

Medju prvim programima za rešavanje matematičkih zadataka ističu se: programi Gerlentera i dr. ([46], [47], 1959,1960 g.) za rešavanje geometrijskih zadataka izgradjeni na bazi heuristika koje koriste učenici uz oslanjanje na crtež kao model; program Slejgla ([179], 1963 g.) SAINT - simbolički automatski integrator, koji rešava elementarne integrale na bazi metoda i heuristika koje primenjuju studenti pri rešavanju analognih zadataka. Program ANALOGY T.Evansa ([41],1964 g.) otkriva geometrijske analogije sa crteža na nivou boljeg srednjoškolca. Program W.Martina ([119],1967 g.) i J.Mosesa ([138],1967 g.) operiše sa algebarskim izrazima, diferencira ih, odredjuje integral i rešava proste diferencijalne jednačine. Heuristički program regresione analize F.A.Milera ([126]) počev od 1964 godine našao je mnogobrojne primene u industrijskim kompanijama SAD, (videti [185], str. 132).

Svaki od navedenih programa odlikuje se specifičnošću metoda i heuristika. Osim parcijalnih pristupa rešavanju matematičkih zadataka javila se opštija ideja modeliranja na računaru deduktivne metode uz uvažavanje i primenu postojećih teorijskih rezultata. Za to poseban značaj imaju rezultati o algoritamskoj nerešivosti pojedinih tipova problema. Takav je problem prepoznavanja izvodljivosti, čiju je algoritamsku ne rešivost u opštem slučaju dokazao Čerč 1936 godine. Mada je ovaj rezultat Čerča učinio besmislenim sve dalje pokušaje izgradjivanja takvih algoritama, rezultati Erbrana iz 1930 god. upućuju na izgradjivanje algoritama koji završavaju rad i daju odgovor uvek kad je tvrdjenje izvodljivo iz polaznog skupa tvrdjenja. Za tvrdjenja koja nisu izvodljiva, takvi algoritmi u opštem slučaju ne daju odgovor i rade beskonačno. To je u vezi sa egzistencijom sledeće delimično rekurzivne funkcije:

$$\mathcal{C}(A) = \begin{cases} 1 \text{ , ako je A teorema} \\ \text{inače nedefinisana} \end{cases}$$

i u saglasnosti je sa rezultatom Čerča.
Tvrdjenje o egzistenciji takvih algoritama ne uzima u obzir praktične teškoće za njegovu realizaciju u ograničenom prostoru i konačnom vremenu, pa ima principijalni karakter. U vezi sa praktičnim mogućnostima računara je i rezultat o postojanju po volji složenih problema (videti[199],str.172-177).
Prostorno vremenska ograničenja računara upućuju na zaključak da se mogu formulisati zadaci za koje se zna da su rešivi u konačnom, ali koje računar neće moći rešiti za unapred fiksirano vreme. Upravo to nalaže potrebu za razlikovanje principijelnih i stvarnih mogućnosti računara. Medjutim, navedena ograničenja važe i kad se reč "računar" zameni sa "čovek", pa nisu prepreka za približavanje računara mogućnostima čoveka i njegovim potrebama. Zbog toga, poseban značaj imaju istraživanja na izgradjivanju efikasnih procedura za rešavanje zadataka praktičnog stepena složenosti.

## 2. O RAZRADI PROGRAMA ZA DOKAZIVANJE TEOREMA

Razrada programa za dokazivanje teorema stimulisana je iz više razloga. Sa stanovišta veštačke inteligencije ovaj problem u sebi sadrži važne komponente inteligentnog ponašanja. Mnogi zadaci koji se rešavaju u kibernetici mogu se formulisati kao teoreme koje treba dokazati, pa postoje raznovrsne mogućnosti za primenu. U matematičkom stvaralaštvu takvi programi mogu poslužiti kao sredstvo za proveru postojećih dokaza, zatim za testiranje hipoteza, a u sadejstvu sa čovekom i za dokazivanje novih teorema. Osim toga, iznalaženje adekvatnih pravila izvodjenja i mehaničkih procedura dokazivanja ima i samostalan teo rijski značaj.

Rezultati Hilberta, Čerča, Gedela, Genzena, Tarskog, Erbra na, Tjuringa, Markova i drugih logičara u vezi sa formalizacijom matematičkih teorija i logičkog izvodjenja, teorijom dokaza i teorijom algoritama sačinjavaju teorijsku osnovu za izgra djivanje praktičnih algoritama dokazivanja.
S ciljem okvirnog sagledavanja postignutih rezultata pomenućemo neke istaknute programe za mehaničko dokazivanje teorema.

Program LT Newella,Shaw i Simona ([140],1957 g.) dokazuje teoreme u iskaznom računu. Testiran na teoremama iz "Principia Mathematica" [211], od 52 teoreme dokazao je 38 teorema.

Program Wang Hao ([207], 1958 g.) dokazao je skoro sve teoreme iz "Principia Mathematica". Naime, više od 200 teorema u prvih pet poglavlja dokazano je za 37 min, od toga je oko 34 min utrošeno na rad ulazno-izlaznih uredjaja, tako da je stvarno vreme rada iznosilo oko 3 min. Teoreme predikatskog računa sa jednakošću koje su zastupljene u sledećih pet poglavlja PM, oko 150 teorema, računar je dokazao za manje od jednog sata.

Od programa i mehaničkih procedura za iskazni račun ističemo još sledeće: Amarel S.([5],1967 g.), Ehrenfeucht A.,Orlowska E. ([40],1967 g.), Anufriev F.V.,Kostjakov V.M.,Malašonok A.I. ([12],1972 g.), Mogilevskij G.L.,Ostrouhov D.A. ([135],1978 g.) i Rangaswamy S.V.,Chakrapani N.,Tikekar V.G. ([166], 1980 g.).

Medju prvim programima koji dokazuju teoreme na jeziku predikatskog računa prvog reda su programi Gilmora P.C. ([50],1960 g.), Davisa M.,Putnama H. ([34],1960 g.) i Prawit za ([161], 1960 g.).

Abrahams P. ([1], 1963 g.) je sastavio program za proveru matematičkih dokaza formulisanih na jeziku predikatskog računa. Program je u dokazima nekih od 63 teorema u "Principia Mathema tica" otkrio nekorektnosti koje je Abrahams uspeo da otkloni. Za proveru jedne teoreme trebalo je u proseku 17 sec.

Kad je u radu J.A.Robinson ([170],1965 g.) formulisano pravilo rezolucije otvoren je put ka moćnijim programima. Char-tung Lee ([94],1967 g.) je koristeći rezoluciju napisao program za izvodjenje posledica datog skupa aksioma. Centralno mesto u njemu zauzima kriterijum interesantnosti posledice. Programe za mehaničko dokazivanje teorema zasnovane na principu rezolucije napisali su Robinson G., Wos L. (1969 g., prema [143]), kao i Allen J.,Luckham D. ([4],1970 g.) Ovi programi su dalje usavršavani i varirani od strane niza autora.
Dokazivanje teorema na principu rezolucije primenjeno je u programima za vodjenje dijaloga Greena i Raphaela ([56],1968g.) i Greena ( [57],1969 g.). Druga značajna primena rezolucije razmatra se u radovima Waldinger R.J.,Lee C.T. ([206],1969 g.), Manna Z. Waldinger R. ([108], 1971 g.) u vezi sa proverom korektnosti programa, a i sa automatskim programiranjem. Formalni sistem LUCID Achcroft E.A.,Wadge W.W. ([2],1976 g.) namenjen je za pisanje i proveru programa.

Dalje povećavanje efikasnosti programa ostvaruje se uvodjenjem semantičke informacije i stvaranjem mogućnosti za intervencije spolja u procesu dokazivanja ( Henschen [65],1974 g.). Drugi prilaz je u ugradjivanju specifičnih svojstava konkretnih teorija u pravila izvodjenja i algoritme unifikacije (Slagle J. [183],[184],[187], 1972,1974 g.) Na tom putu su i rezultati o matematičkoj indukciji koje izlažemo u ovom radu.

Razradjuju se sistemi zasnovani na logikama višeg reda, intuicionističkoj logici i modalnostima. U radu J.L.Darlingtona [32], koriste se aksiome teorije drugog reda.

Osim prilaza zasnovanih na rezoluciji postoje i druge metode za mehaničko dokazivanje teorema koje se zasnivaju na obratnom metodu S.J.Maslova ([112]-[118], 1964-1979 g.), kao i na prirodnom izvodjenju (Šanin N.A.[193],1965 g.) i raznim heuristikama (Bledsoe [17],1971, Norton [146],1971, Bledsoe,Boyer,Henneman [18],1972, Bledsoe,Bruell [19],1974, Levins [139],1974 g.).

"Osim niza logičkih teorema dokazane su neke teoreme elementarne algebre, elementarne i projektivne geometrije, a takodje i elementarne teorije brojeva. Na primer takve: 'ako je kvadrat svakog elementa jednak jedinici, grupa je komutativna' , 'kvadratni koren iz prostog broja je iracio halan' , 'prostih brojeva je beskonačno mnogo'. Složenost dokaza poslednje dve teoreme, izgleda, približava se granici savremenih mogućnosti mašinskog traženja izvodjenja. Na taj način, zasad je malo nade za mašinsko dokazivanje zaista složenih teorema, tim pre teorema, koje čovek ne uspeva da dokaže... Drugi način - je sadejstvo matematičara i računara, pri čemu čovek principijelno usmerava dokaz i izriče hipoteze, a mašina... proverava hipoteze i daje materijal za formiranje novih hipoteza." (Enciklopedija kibernetiki, tom I,str.300,[221]).

"Program Garda ([60]) u nekoj meri uz pomoć čoveka, uspešno je savladao zadatak traženja prvog dokaza jedne hipoteze teorije modularnih struktura." ([143],str.234).

Osim za modeliranje dedukcije, izgradjuju se procedure i programi za modeliranje induktivne logike i induktivnog izvodjenja: Solomonov R.J.([190],1964), Hintikka J., Suppes P.([68],1966), Plotkin G.P.([153],[154],1969,1971), Poplseston R.J.([157],1969), Hintikka J., Niiniluoto I.([69],1976), Meltzer D.([123],1970), Kibner E.B.([79],1977), Manna Z.,Waldinger R.([110],1977), Von Henke F.W.([204],1977).

Na kraju ovog pregleda napominjemo da se u navedenim radovima koriste razne forme predstavljanja problema. Za opšte probleme izvodjenja i dokazivanje teorema koristi se deklarativno predstavljanje u formalno-logičkim sistemima. Za uže orijentisana istraživanja pogodnija su proceduralna predstavljanja u okviru posebnih problemski orijentisanih jezika, a takodje i semantička predstavljanja koja omogućuju operisanje sa semantičkom informacijom u okviru semantičkih mreža. O specifičnostima pojedinih tipova predstavljanja može se videti na primer, u [158], str.56-62. U ovom radu koristimo deklarativna predstavljanja.

## 3. PRECIZIRANJE ZADATKA MEHANIČKOG DOKAZIVANJA TEOREMA

Za predstavljanje problema koristićemo formalne teorije. U metateoriji uvode se definicije izvodjenja, teoreme i posledice skupa formula. Navodimo te definicije prema [162], str. 69-71.

Definicija 1. Konačan niz formula $B_1, B_2, \ldots, B_m$ formalne teorije $\tau$ zovemo IZVODJENJE (DEDUKCIJA, DOKAZ) u teoriji ako svaka formula $B_i$ $(1 \leqslant i \leqslant m)$ tog niza ispunjava uslov:

1° $B_i$ je aksioma, ili

2° $B_i$ je direktna posledica nekih prethodnih formula niza po izvesnom pravilu izvodjenja teorije $\tau$.

Definicija 2. Formulu $B_m$ formalne teorije zovemo TEOREMA u teoriji $\tau$, u oznaci $\vdash_{\tau} B_m$ ili $\vdash B_m$, ako postoji bar jedan niz $B_1, B_2, \ldots, B_m$ koji je izvodjenje u teoriji $\tau$. U ovom slučaju kažemo i da je taj niz izvodjenje teoreme $B_m$.

Definicija 3. Neka je F neki skup formula formalne teorije $\tau$ i neka je A odredjena formula iste teorije. Kažemo:

formula A je POSLEDICA skupa formula F ako postoji konačan niz formula $B_1, B_2, \ldots, B_m$ ($B_m$ je A), čija svaka formula $B_i$ ispunjava uslov:

$1^\circ$ $B_i$ je aksioma; ili
$2^\circ$ $B_i$ je iz skupa F; ili
$3^\circ$ $B_i$ je direktna posledica nekih prethodnih formula niza po izvesnom pravilu izvodjenja teorije $\tau$ .

Ako je A posledica skupa formula F, onda pišemo: $F \vdash_{\tau} A$, ili $F \vdash A$. Kad je F konačan skup, umesto $\{A_1, \ldots, A_k\} \vdash A$ pišemo: $A_1, \ldots, A_k \vdash A$ .

osnovu navedenih definicija, za dokaz da je formula A teorema (li posledica skupa formula F) u teoriji $\tau$ , dovoljno je odre ti bar jedno izvodjenje $B_1, \ldots, B_m$ , gde je $B_m$ formula A . redjivanje takvog niza formula za zadatu teoremu A, često hteva jaku intuiciju u pogledu odabiranja njegovih elemenata. djutim, konstrukcija traženog niza može se izvršiti, bar u rincipu, mehaničkim putem bez oslanjanja na intuiciju. To pre-iziramo u sledećoj tački.

1. <u>Metoda potpunog pregleda. Graf dokaza teorema</u>

Neka $R(S) \stackrel{def}{=} S \cup P(S)$ , gde je S neki skup formula eorije $\tau$ , a P(S) skup svih direktnih posledica formula iz S o pravilima izvodjenja teorije $\tau$ , i neka je za skup aksioma $\mathcal{A}$ eorije $\tau$ :

$$R_0(\mathcal{A}) \stackrel{def}{=} \mathcal{A} \quad .$$

$$R_{n+1}(\mathcal{A}) \stackrel{def}{=} R\,(\,R_n(\mathcal{A})\,) \text{ , za } n \geqslant 0 \text{ .}$$

ada, s obzirom da je izvodjenje teoreme A konačan niz, biće za eko konačno $k \geqslant 0 : A \in R_k(\mathcal{A})$ . Metoda potpunog pregleda sasto i se u uzastopnom generisanju skupova $R_i(\mathcal{A})$ , $i=1,2,\ldots,k$ . ad je skup $\mathcal{A}$ konačan, ovim postupkom moguće je odrediti mini-alan dokaz, tj. izvodjenje sa minimalnim brojem formula ili ravila izvodjenja. Preciziraćemo rečeno pomoću pojmova teorije rafova.

)efinišemo prvo, nivo formule C u datom izvodjenju:

(1) Ako $C \in \mathcal{A}$ , onda C ima nulti nivo,

(2) ako je S neki skup formula koje pripadaju datom izvodjenju i formula $D \in S$ ima najviši nivo u S, označen sa j ($j \geqslant 0$), i ako se formula C, koja ne pripada skupu S, izvodi iz D i možda još nekih formula skupa S po pravilu izvodjenja $\mathcal{C}$ , onda C ima nivo j+1 .

Kako formula C može imati više izvodjenja, formula C može imati nekoliko različitih nivoa (po jedan u svakom izvodjenju). Izvodjenjima koja su odredjena trojkom $(\mathcal{A}, \mathcal{R}, \mathcal{F})$ , gde je $\mathcal{A}$ - skup aksioma, $\mathcal{R}$ - skup pravila izvodjenja, $\mathcal{F}$ - skup terminalnih formula, pridružuje se orijentisani graf čiji su čvorovi formule iz $\mathcal{A}^*$ ( $\mathcal{A}^* = \bigcup_i R_i(\mathcal{A})$ ). Pri tome, formuli C koja ima m različitih izvodjenja odgovara na grafu m različitih čvorova, a svakom izvodjenju odgovara po jedan podgraf takvog grafa.

Definisaćemo prema [158] (str.85-87) apstraktni graf dokaza. Apstraktni graf dokaza teorema je uredjen par (G,s) , gde je G skup čvorova, a s funkcija nasledja definisana na podskupovima iz G, čije su vrednosti podskupovi u G, pri čemu su zadovoljeni sledeći uslovi:

1. $s(\emptyset) = \emptyset$
2. Ako $s(G') \neq \emptyset$ i $G' \subseteq G$ , onda je G' konačan skup
3. Ako za $G' \subseteq G$ i $G'' \subseteq G$ važi $G' \neq G''$, onda $s(G') \cap s(G'') = \emptyset$
4. Neka je $G_o = \{n \mid n \in G \text{ i } n \notin s(G') \text{ za svaki } G' \subseteq G\}$ i

$$G_{k+1} = \{n \mid n \in s(G') \text{ za } G' \subseteq \bigcup_{i \leqslant k} G_i \text{ i } G' \cap G_k \neq \emptyset\} ,$$

tada je: a) $G_o \neq \emptyset$

b) $G = \bigcup_{o \leqslant i} G_i$

c) $G_i \cap G_j = \emptyset$ za $i \neq j$ .

Uslov 3 obezbedjuje da različiti skupovi čvorova imaju različite skupove sledbenika. Sledbenici se definišu na sledeći način.

efinicija neposrednog sledbenika:

Ako je $G' \subseteq G$, $n \in G'$ i $n' \in s(G')$ , onda je n' neposredni sledbenik za n.

efinicija sledbenika:

Čvor $m \in G$ je sledbenik za $n \in G$, u oznaci $m > n$ , ako

(1) m je neposredni sledbenik za n , ili

(2) m je neposredni sledbenik nekog sledbenika za n .

slov 4 obezbedjuje da u grafu (G,s) svaki čvor ima jedinstven ivo, tj. za $i \neq j$ ako $n \in G_i$, onda $n \notin G_j$ .

Graf (G,s) interpretira se u domenu dokazivanja teorema la sledeći način:

Preslikavanje f: $G \longrightarrow \mathcal{A}^*$ svakom čvoru $n \in G$ pridružuje formulu $f(n) \in \mathcal{A}^*$ ; skup čvorova $s(G')$, gde $G' \subseteq G$, preslikava se u skup formula $R(\{f(n) \mid n \in G'\})$ odredjen primenom svih pravila izvodjenja iz skupa $\mathcal{R}$ na formule skupa $\{f(n) \mid n \in G'\}$.

Pri takvoj interpretaciji grafa (G,s) izvodjenje formule f(m) sadrži sve formule f(n) za koje je $m \geq n$ .

Sada se zadatak dokazivanja teorema može predstaviti kao uredjena četvorka (G,s,F,g) , gde je $F \subseteq G$ skup terminalnih čvorova, a g: $G \longrightarrow C$ (C je skup realnih brojeva) funkcija ocene kojom se izražava složenost izvodjenja. Po metodi potpunog pregleda generišu se svi čvorovi iz $G_1, G_2, \ldots$ , pa se za $n \in G_i$ funkcija g(n) obično izražava brojem i, tj. nivoom čvora n .

Jasno je da zbog brojnosti skupova $G_i$ algoritam potpunog pregleda daje ograničene, gotovo neznatne, mogućnosti za praktičnu realizaciju. U takvoj situaciji primenjuje se sledeći izlaz:

Ako nas interesuje samo da li je data formula teorema u formalnoj teoriji $\mathcal{T}$ , zadovoljavamo se mogućnošću, kad takva postoji, efektivnog utvrdjivanja činjenice da izvodjenje postoji, ne nastojeći da to izvodjenje i nadjemo.

" ... kad je lakše dobiti neformalizovani dokaz o postojanju formalnog dokaza, nego navesti sam formalni dokaz, i pri

tome se neformalizovani dokaz može izvesti 'finitnim' metodama..., skloni smo da se njime potpuno zadovoljimo. Ako je reč o primeni računara na probleme traženja ili provere dokaza, onda je umesan još jedan korak. Neki izbor dovoljno brzih i pogodnih metoda koje su već poznate u matematici, ili (za zadatke mašinskog traženja izvodjenja) nekih novih metoda,..., fiksira se u svojstvu novog formalnog sistema, u čijim okvirima računar treba da ostvari traženje ili proveru dokaza." (Klini,[82],str. 254-255).

3.2. Napomene o terminologiji

Za razlikovanje formalnih od neformalizovanih dokaza u literaturi postoje različiti termini: "proof" i "demonstration" a engleskom, "vivod" i "dokazateljstvo" na ruskom jeziku. stina, oni se često ne razlikuju (videti na pr. Klini [82], tr. 248, ili Mendelson [124], str. 39), a značenje im se odre juje kontekstom. Slično je i sa upotrebom termina: teorema, tav, metateorema, lema i njima srodnih. Trudeći se da ostanemo to bliže uobičajenoj terminologiji, preciziraćemo značenje ledećih termina, koje koristimo u ovom radu.

ermin "teorema" koristimo
- za teoreme formalne teorije u smislu definicije 2 ,
- za stavove ili leme matematičke teorije kad je reč o njihovom mehaničkom dokazivanju.

a tvrdjenja koja izričemo u ovom radu koristimo termine "stav" "lema".

ermin "izvodjenje" koristimo za niz formula u smislu definicija -3, a takodje i za takav niz snabdeven numeracijom formula i ko mentarima.

"Dokaz" zavisno od konteksta ima sledeća značenja:
- obrazlaganje tačnosti stava ili leme izrečene u tekstu, ili
- utvrdjivanje egzistencije izvodjenja za datu formulu, ili
- konstruisanje izvodjenja.

od "mehaničkim dokazivanjem teorema - u užem smislu"
odrazumevamo primenu računara za
konstruisanje izvodjenja u nekoj formalnoj teoriji,
utvrdjivanje egzistencije izvodjenja,
dokazivanje stavova ili lema neke matematičke teorije u
okviru odgovarajućeg formalizma prilagodjenog računaru.

Mehaničko dokazivanje teorema - u širem smislu" podrazumeva
azradu metoda, pravila, strategija, procedura, algoritama i
rograma, tj. celokupan sistem koji obezbedjuje realizaciju
ehaničkog dokazivanja teorema u užem smislu.

# G L A V A  I

## MEHANIČKO DOKAZIVANJE TEOREMA ISKAZNOG RAČUNA

Metode i programi za mehaničko dokazivanje teorema iskaznog računa razmatraju se u [5], [12], [40], [43], [135], [166], [193], [207]. ovoj glavi izlažemo jednu aritmetičku metodu za prepoznavanje izvodljivosti u iskaznom računu.

### ARITMETIČKA METODA PREPOZNAVANJA IZVODLJIVOSTI

Zbog odlučivosti iskaznog računa dokaz teoreme konstrukcijom njenog izvodjenja može se zameniti ispitivanjem odgovarajućeg kriterijuma. Dokazom da je taj kriterijum zadovoljen za datu formulu, dokazana je egzistencija njenog izvodjenja. Za dokazivanje teorema u ovom smislu postoje razni kriterijumi i postupci za njihovu proveru (tautologije, konjunktivne normalne forme, razni postupci opovrgavanja). Ovde, u tač. 1.3. izlažemo metodu zasnovanu na numeričkom kriterijumu i na aritmetičkom postupku za njegovu proveru. Metoda dopušta jednostavnu programsku realizaciju na FORTRAN-u. Pomoćne rezultate izlažemo u tač. 1.1. i 1.2. Ovi rezultati, zbog veze sa bulovim funkcijama, odnosno sa k-značnim logikama mogu predstavljati i samostalan interes.

### 1.1. NEKA OBELEŽJA ARGUMENTNOG DELA TABLICE BULOVE FUNKCIJE

Neka je bulova funkcija $f(x_1,\ldots,x_n)$ predstavljena tablicom 1., gde su $X_1,\ldots,X_n$ pomoćne promenljive. Postoji veza:

$$x_i = X_{n+1-i} \quad , \; i=1,2,\ldots,n \; . \tag{1}$$

Tablica 1.

| $x_n\ x_{n-1}\ \dots\ x_2\ x_1$ | $f(x_1,\dots,x_n)$ |
|---|---|
| $x_1\ x_2\ \dots\ x_{n-1}\ x_n$ | |
| 0 0 .... 0 0 | $f^1$ |
| 0 0 ... 0 1 | $f^2$ |
| ⋮ ⋮ ⋮ ⋮ | ⋮ |
| 1 1 ... 1 1 | $f^{2^n}$ |

Jedno obeležje ove tablice je da se j-ta vrsta njenog argumentnog dela odredjuje binarnim zapisom broja (j-1), $j=1,2,\dots,2^n$. Razmotrićemo karakteristike vezane za kolone - vektore koji odgovaraju promenljivima.

Neka je konkatenacija $\overset{m}{\underset{i=0}{\mathop{\Large\mathsf{K}}}} a_i = a_0 a_1 \dots a_m$ definisana sa

$$\text{(i)}\quad \overset{0}{\underset{i=0}{\mathop{\Large\mathsf{K}}}} a_i = a_0 \quad ;\quad \text{(ii)}\quad \overset{k+1}{\underset{i=0}{\mathop{\Large\mathsf{K}}}} a_i = \left(\overset{k}{\underset{i=0}{\mathop{\Large\mathsf{K}}}} a_i\right) a_{k+1} \quad ,$$

tada važi sledeća lema.

Lema 1. Svaki vektor $X_i$, $1 \leqslant i \leqslant n$ tablice 1 može se zapisati u obliku:

$$X_i = \overset{2^{n-i}-1}{\underset{j=0}{\mathop{\Large\mathsf{K}}}} \left( \overset{2^{i-1}}{\underset{r=1}{\mathop{\Large\mathsf{K}}}} 0^{j2^i + r} \quad \overset{2^i}{\underset{r=2^{i-1}+1}{\mathop{\Large\mathsf{K}}}} 1^{j2^i + r} \right) \qquad (2)$$

gde eksponent $(j2^i + r)$ odredjuje redni broj koordinate, posmatrano odozgo na niže u tablici 1.

Dokaz. Niz oblika 00 ... 011 ... 1 zvaćemo p e r i o d a. Perioda vektora $X_1$ je 01, njena dužina je $d_1=2$, a $X_1$ sadrži $2^{n-1}$ perioda. Tada svakoj komponenti neparnih perioda vektora $X_{i-1}$ $(i>1)$ u $X_i$ odgovara komponenta 0, a svakoj komponenti parnih perioda vektora $X_{i-1}$, odgovara u $X_i$ komponenta 1. Zato za dužinu perioda važi: $d_i = 2d_{i-1}$, $i>1$. Kako je $d_1=2$, sledi $d_i = 2^i$, $i=\overline{1,n}$, a broj perioda vektora $X_i$ je $2^n/2^i = 2^{n-i}$.

komponente (j+1)-ve po redu periode vektora $X_i$ , $0 \leqslant j \leqslant 2^{n-i}-1$, imaju redni broj od $j2^i+1$ do zaključno sa $j2^i+2^i$, pa se ova perioda može zapisati u obliku:

$$\overset{2^{i-1}}{\underset{r=1}{K}} {}_0{}^{j2^i+r} \; \overset{2^i}{\underset{r=2^{i-1}+1}{K}} {}_1{}^{j2^i+r}$$

Kako se pri prelazu na sledeću, (j+2)-gu periodu ne narušava redosled komponenata, jer prva sledeća komponenta ima redni broj $(j+1)2^i+1 = (j2^i+2^i)+1$ , vektor $X_i$ se može zapisati u obliku konkatenacije uzastopnih perioda, tj. u obliku (2) .

Posledica 1. Svaki vektor $X_i$ , $i=\overline{1,n}$ , tablice 1 može se generisati izrazom:

$$X_i = \overset{2^{n-i}-1}{\underset{j=0}{K}} \; \overset{2^i}{\underset{r=1}{K}} \left[r/(2^{i-1}+1)\right]^{j2^i+r} \qquad (3)$$

gde je [ ] - oznaka za ceo deo.

Zaista, za $r \leqslant 2^{i-1}$ biće $[r/(2^{i-1}+1)] = 0$ , a za $2^{i-1} < r \leqslant 2^i$ je $[r/(2^{i-1}+1)] = 1$ , pa je (3) ekvivalentno zapisu (2) .

Posledica 2. Izraz

$$\overset{n}{\underset{i=1}{K}} \; \overset{2^{n-i}-1}{\underset{j=0}{K}} \; \overset{2^i}{\underset{r=1}{K}} \left[r/(2^{i-1}+1)\right]^{j2^i+r} \qquad (3')$$

reprezentuje argumentni deo tablice 1.

Neka je $K_i$ dekadni ekvivalent binarnog zapisa odredjenog formulom (2), odnosno (3). Odredićemo $K_i$ tako što binarnu cifru sa eksponentom k pomnožimo sa $2^{2^n-k}$ i saberemo proizvode za $k=1,\ldots,2^n$ :

$$K_i = \sum_{j=0}^{2^{n-i}-1} \; \sum_{r=1}^{2^i} \left[r/(2^{i-1}+1)\right]^{j2^i+r} \cdot 2^{2^n-(j2^i+r)} =$$

$$= \sum_{j=0}^{2^{n-i}-1} \sum_{r=2^{i-1}+1}^{2^i} 2^{2^n - j2^i - r} = 2^{2^n} \sum_{j=0}^{2^{n-i}-1} (2^{2^i})^{-j} \cdot \sum_{r=2^{i-1}+1}^{2^i} 2^{-r} =$$

$$= \frac{2^{2^n} - 1}{(2^{2^{i-1}} - 1) + 2} \quad . \quad \text{Neka je } I(n) = 2^{2^n} - 1 \text{ , tada je}$$

$$K_i = \frac{I(n)}{I(i-1)+2} \quad , \; i=1,\ldots,n \; . \qquad (4)$$

Na osnovu veza (1) svakoj promenljivoj $x_i$ odgovara broj

$$k_i = K_{n+1-i} \quad , \text{ tj. } \quad k_i = \frac{I(n)}{I(n-i)+2} \quad , \; i=1,\ldots,n \; . \qquad (5)$$

Primetimo da broj I(n) odgovara funkciji konstanti f=1 . [1)]

<u>Primer za ilustraciju obeležja u slučaju n=3</u>

Odredićemo vektore $x_1, x_2, x_3$ i karakteristike $k_1, k_2, k_3$ .

Na osnovu (1) i (3) je

$$x_1 = X_3 = \overset{0}{K}_{j=0} \; \overset{8}{K}_{r=1} [r/5]^{8j+r} = 0^1 0^2 0^3 0^4 1^5 1^6 1^7 1^8 = 00001111$$

$$x_2 = X_2 = \overset{1}{K}_{j=0} \; \overset{4}{K}_{r=1} [r/3]^{4j+r} = 0^1 0^2 1^3 1^4 0^5 0^6 1^7 1^8 = 00110011$$

$$x_3 = X_1 = \overset{3}{K}_{j=0} \; \overset{2}{K}_{r=1} [r/2]^{2j+r} = 0^1 1^2 0^3 1^4 0^5 1^6 0^7 1^8 = 01010101$$

---

1) Za odredjivanje $k_i$ mogu se koristiti i formule:

$$k_1^{(n)} = 2^{2^{n-1}} - 1 \quad ; \; k_i^{(n)} = k_{i-1}^{(n-1)} \cdot (2^{2^{n-1}} + 1) \; , \quad i=2,3,\ldots,n \; .$$

Očevidno, formula (5) omogućuje neposredno i nezavisno odredjivanje ovih brojeva.

Može se još primetiti i sledeća karakteristika:

$$\prod_{i=1}^{n} k_i = \prod_{i=1}^{n} K_i = (I(n))^{n-1} \; .$$

$$\varsigma_1 = \frac{I(3)}{I(2)+2} = 15 \quad ; \quad k_2 = \frac{I(3)}{I(1)+2} = 51 \; ; \; k_3 = \frac{I(3)}{I(0)+2} = 85 \; .$$

$$\prod_{i=1}^{3} k_i = (I(3))^2 = 255^2 \; .$$

## L.2. PROŠIRENJE BULOVIH OPERACIJA SKUPA $L_2$ NA $L_{2k}$

Na skupu $L_2 = \{0,1\}$ operacije disjunkcija (V) , konjunkcija ($\wedge$) i negacija ($\neg$) definisane su tablicama:

| V | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| | 0 | 1 |
|---|---|---|
| $\neg$ | 1 | 0 |

Za njih je $L_2$ regularna bulova algebra.[1)]

Neka je preslikavanje: $L_2^k \longrightarrow L_{2k}$ definisano na sledeći način

$$\varphi(x_1,x_2,\ldots,x_k) = 2^{k-1}x_1 + 2^{k-2}x_2 + \ldots + 2^0 x_k \; ; \; x_i \in \{0,1\} \; ,$$

gde je $L_{2k} = \{0,1,2,3,\ldots,2^k-1\}$ .

<u>Definicija 1.</u> Neka je $x = \varphi(a_1,a_2,\ldots,a_k)$ , $y = \varphi(b_1,b_2,\ldots,b_k)$ $a_i,b_i \in L_2$ , $i=1,2,\ldots,k$ i $*$ jedna od operacija $V, \wedge$ .

$$x * y \stackrel{\text{def}}{=\!=} \varphi(a_1 * b_1,\ a_2 * b_2,\ \ldots\ ,\ a_k * b_k)$$

$$\neg x \stackrel{\text{def}}{=\!=} \varphi(\neg a_1\ ,\ \neg a_2\ ,\ \ldots\ ,\ \neg a_k\ )$$

Neposredno se dokazuje da je za ove operacije $L_{2k}$ regularna bulova algebra. Ulogu istaknutih elemenata imaju 0 i $(2^k - 1)$ . Kako se sva svojstva operacija čuvaju na $L_{2k}$, analogno se proširuju i druge operacije skupa $L_2$.[2)]

---

1) Pojmovi bulove operacije, bulove algebre i regularne bulove algebre uzimaju se u smislu definicija u [51] , str. 37-45 .

2) Operacije max(x,y), min(x,y) i $(2^k-1)$-x pretvaraju $L_{2k}$ u bulovu algebru, ali ona nije regularna ([51], str.246).

Na $L_2$ važi: $\neg x = 1-x$ ; $xVy = x+y-x\cdot y$ ; $x \Rightarrow y = 1-x+x\cdot y$ ;

$$x \Leftrightarrow y = 1-(x+y)+2\cdot x\cdot y \quad .$$

Na osnovu ovih veza i prirode funkcije $\mathcal{C}$, u $L_{2k}$ važe sledeće jednakosti:

$$\neg x = (2^k-1) - x$$

$$\begin{aligned} x \vee y &= x + y - x\wedge y = x + \neg x\wedge y \\ x \Rightarrow y &= \neg x + x\wedge y = (2^k-1) - x + x\wedge y \\ x \Leftrightarrow y &= \neg x\wedge\neg y + x\wedge y = (2^k-1)-(x+y)+2(x\wedge y) = \neg(x+y)+2(x\wedge y) \end{aligned} \qquad (6)$$

gde su $x,y \in L_{2k}$ , " $\Rightarrow$ " i " $\Leftrightarrow$ " simboli za implikaciju i ekvivalenciju, a " + " , " - " i " $\cdot$ " obične aritmetičke operacije.

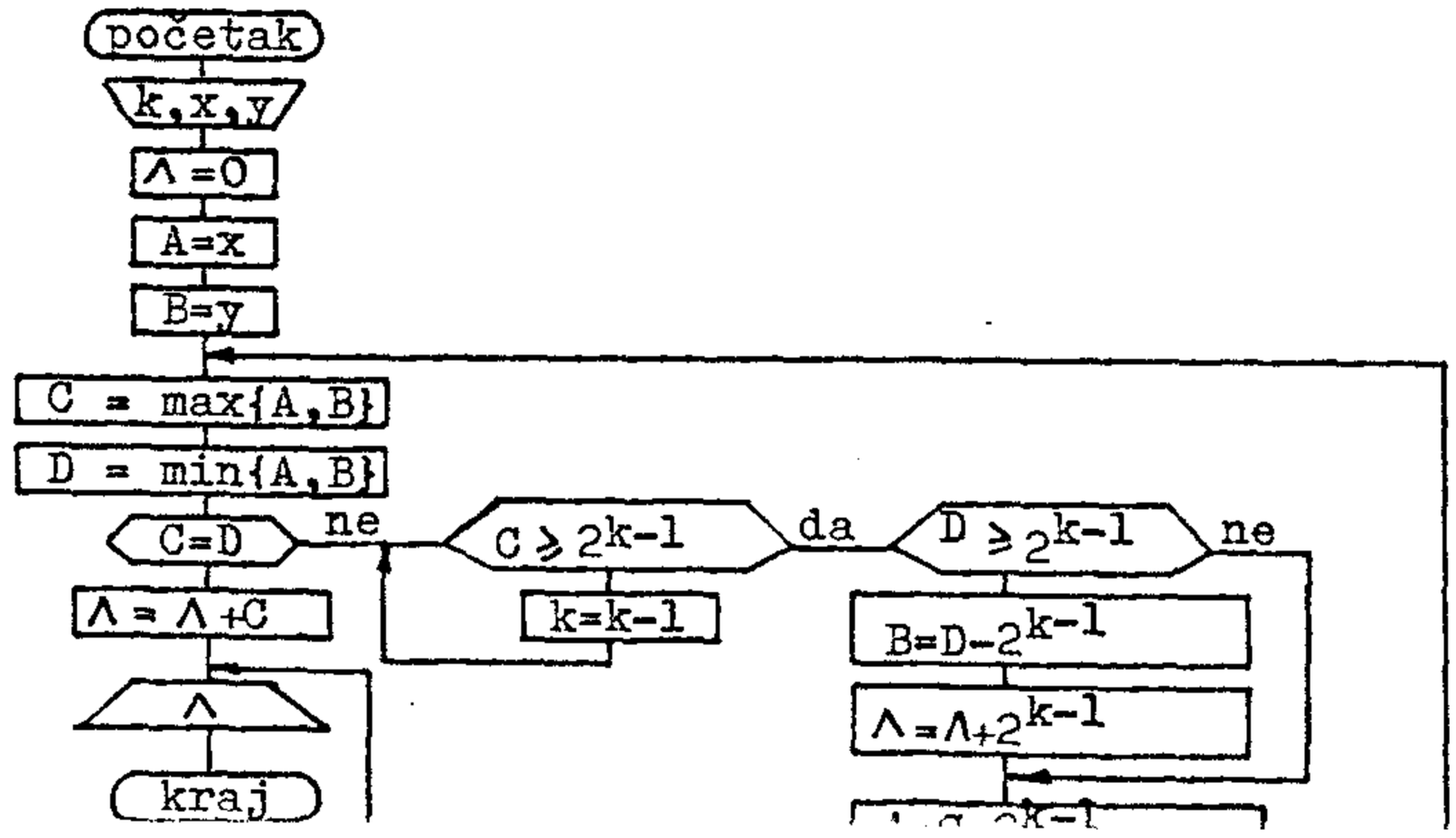
Za izvršavanje ovih operacija dovoljno je imati tablicu konjunkcije na skupu $L_{2k}$ . Tablica se jednostavno ispisuje po sledećem algoritmu.

Neka je matrica $T_{2m}$ odredjena sadržajem tablice konjunkcije na skupu $L_{2m}$ i neka je $K_{2m}$ kvadratna matrica reda $2^m$ čiji su elementi konstante $2^m$ , tada

$$T_{2m+1} = \begin{bmatrix} T_{2m} & T_{2m} \\ T_{2m} & T_{2m} + K_{2m} \end{bmatrix} ; \; T_1 = [0] \; ; \; m=0,1,\ldots,k-1 \; .$$

Primetimo da pri ručnoj upotrebi nema potrebe zapamćivanja ove tablice, već je dovoljno zapamtiti samo ovaj jednostavan postupak za njeno ispisivanje.

Izračunavanje konjunkcije $x\wedge y$ na $L_{2k}$ na računaru, može se izvršiti po sledećem algoritmu:



## .3. KARAKTERIZACIJA TEOREMA ISKAZNOG RAČUNA - ARITMETIČKA METODA PREPOZNAVANJA IZVODLJIVOSTI

Neka je H bijektivno preslikavanje skupa iskaznih lova $\{p_1,\dots,p_n\}$ na skup $\{k_1,\dots,k_n\}$, gde su $k_i = \frac{I(n)}{I(n-i)+2}$, $(n) = 2^{2^n} - 1$, karakteristični brojevi promenljivih $x_i$, i=1,..,n, tablici 1.

Tada svakoj iskaznoj formuli $F(p_1,\dots,p_n)$ odgovara izraz $(k_1,\dots,k_n)$ u bulovoj algebri $L_{2^{2^n}}$ .

Na osnovu stava potpunosti iskaznog računa i regularnosti ulove algebre $L_{2^{2^n}}$ važi stav:

TAV 1. Formula $F(p_1,\dots,p_n)$ iskaznog računa je teorema ako i samo ako $f(k_1,\dots,k_n) = I(n)$ .

Utvrdjivanje da li je data formula iskaznog računa teorema ože se realizovati po sledećem postupku:

1. Izborom preslikavanja H odredjuje se izraz $f(k_1,\dots,k_n)$
2. Pomoću tablice, ili algoritma za izračunavanje konjunkcije na $L_{2^{2^n}}$ ,kao i jednakosti (6), izračunava se $f(k_1,..,k_n)=k$
3. Ako je $k \neq I(n)$, formula nije teorema. U ovom slučaju na osnovu broja k može se odrediti kolona vrednosti bulove funkcije odredjene datom iskaznom formulom. Ustvari, k je dekadni ekvivalent te kolone.
4. Ako je $k=I(n)$, formula je teorema.

Primer 1. Dokazaćemo da je formula ✱ 5.21 iz PM

$$(\neg p \wedge \neg q) \Rightarrow (p \Leftrightarrow q)$$ teorema.

Kako je n=2 računamo u $L_{16}$ .

Neka je $H = \begin{pmatrix} p & q \\ 3 & 5 \end{pmatrix}$, pomoću tablice konjunkcije za $L_{16}$ jednakosti (6) računamo:

$$f(3,5) = (\neg 3 \wedge \neg 5) \Rightarrow (3 \Leftrightarrow 5) = (12 \wedge 10) \Rightarrow (15-8+2(3 \wedge 5)) =$$
$$= 8 \Rightarrow (7+2) = 8 \Rightarrow 9 = 15-8+8 \wedge 9 = 7 + 8 = 15 .$$

Kako je $I(2) = 2^4 - 1 = 15$ , na osnovu stava 1, formula je teorema.

Sa rastom n naglo se povećavaju brojevi sa kojima se računa u $L_{22^n}$ . Rad sa velikim brojevima može se izbeći primenom sledećeg postupka "deljenja na pruge".

Neka sva izračunavanja treba izvoditi u algebri $L_{22^c}$ , $c<n$. Izdelimo kolone tablice 1. na pruge od po $2^c$ komponenata i za svaku prugu odredimo odgovarajući dekadni ekvivalent.
Dobija se matrica karakterističnih brojeva:

$$\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & & \vdots \\ k_{s1} & k_{s2} & \cdots & k_{sn} \end{bmatrix} \qquad s = 2^{n-c} \qquad (7)$$

Sada se postupak primenjuje na vrste matrice (7), tj. izračunava se $f(k_{i1},\ldots,k_{in}) = k_i$ , $i=1,2,\ldots,s$ .
Pri tome, potrebno je voditi računa da izbor preslikavanja

$$H_i: \{p_1,\ldots,p_n\} \longrightarrow \{k_{i1},\ldots,k_{in}\}$$

ostane ne promenjen u odnosu na indeks j brojeva $k_{ij}$, za svako i.
Formula $F(p_1,\ldots,p_n)$ je teorema ako i samo ako za $i=1,2,\ldots,s$ važi $k_i = I(c)$ .

U računu su moguće razne olakšice. S obzirom da se prilikom izračunavanja f neki argumenti ne menjaju, mogu se koristiti dobijeni medjurezultati. Izračunavanja se znatno skraćuju ako se uzmu u obzir identiteti u regularnoj bulovoj algebri, posebno oni u kojima učestvuju istaknuti elementi.

Primer 2. Za formulu $p \Longrightarrow (q \vee r \Longrightarrow (r \Longrightarrow \neg p))$ izračunavanja ćemo izvoditi u $L_{16}$ . Matrica (7) ima oblik $\begin{bmatrix} 0 & 3 & 5 \\ 15 & 3 & 5 \end{bmatrix}$ .

$k_1 = f(0,3,5) = 0 \Longrightarrow (3 \vee 5 \Longrightarrow (5 \Longrightarrow \neg 10)) = 15$ ;

iskoristili smo identitet $0 \Rightarrow x = 15$ .

$k_2 = f(15,3,5) = 15 \Longrightarrow (3 \vee 5 \Longrightarrow (5 \Longrightarrow \neg 15)) = 3 \vee 5 \Longrightarrow (5 \Longrightarrow 0) =$

$= 7 \Longrightarrow 10 = 15-7+7 \wedge 10 = 8 + 2 = 10$.

ako je $k_2 \neq 15$ formula nije teorema. Njoj u tablici 1 odgovara ledeći vektor vrednosti: 11111010 odredjen konkatenacijom bi arnih zapisa brojeva $k_1$ i $k_2$ .

Navedeni postupci predstavljaju jedan oblik "kolektivne ritmetike", omogućuju kompaktan zapis i brzo iračunavanje prime om identiteta algebre $L_{2^{2^n}}$ .

Ako se realizuju na računaru, prednost je što se računa sa rojevima koji odgovaraju nizovima logičkih konstanti, a ne sa osebnim logičkim konstantama. To daje mogućnost racionalnog koišćenja memorije računara. Optimalno popunjavanje registara mo- se postići postupkom cepanja na pruge. Primetimo još da ne oraju sve pruge sadržati po $2^c$ binarnih komponenata. Naime, moće je cepanje na pruge sa po $s_1, s_2, \ldots, s_m$ komponenata, tako da $\sum_{i=1}^{m} s_i = 2^n$ , pa se može raditi u algebrama $L_{2^{s1}}, L_{2^{s2}}, \ldots, L_{2^{sm}}$ .

## .4. MOGUĆNOST PROGRAMSKE REALIZACIJE

Izložena metoda dopušta vrlo jednostavno programiranje a FORTRANU upotrebom funkcijskih naredbi i funkcijskog potprogama za izračunavanje konjunkcije. Proces izvodjenja zamenjuje e izračunavanjem vrednosti aritmetičkog izraza, pridruženog da oj formuli, tj. svodi se na izvršavanje jedne aritmetičke nared e.

a primer, za formulu $\neg(pVq) \Longleftrightarrow \neg p \wedge \neg q$ dovoljno je formulu zapiati u modifikovanoj poljskoj notaciji:

$$\Longleftrightarrow ( \neg ( V (p,q) ) , \wedge ( \neg p, \neg q ) )$$

oformiti sledeću FORTRAN-naredbu:

```
NF = MEQ(NEG(MDIS(3,5)),KON(2,NEG(3),NEG(5)))
```

ri čemu se koristi pridruživanje:

n ⟶ 2 (broj različitih iskaznih slova u formuli)
p ⟶ 3 (karakteristični broj $k_1$)
q ⟶ 5 (karakteristični broj $k_2$)

$\neg \longrightarrow$ NEG
$\vee \longrightarrow$ MDIS
$\wedge \longrightarrow$ KON
$\Rightarrow \longrightarrow$ IMPL
$\Leftrightarrow \longrightarrow$ MEQ

;ao prvi argument konjunkcije navodi se vrednost n.
;a izvršavanje ove aritmetičke naredbe potrebne su još i
;ledeće funkcijske naredbe:

```
 NEG(K) = 2 ** 2 ** N - 1 - K
DIS(K,L)= K - KON(N,K,L) + L
MPL(K,L)= NEG(K) + KON(N,K,L)
MEQ(K,L)= NEG(K+L) + 2 * KON(N,K,L)
```

;ao i funkcijski potprogram KON(N,K,L) , koji se može napisati
;eposredno na osnovu navedenog dijagrama na str. 23 .
'o izračunatoj vrednosti NF odlučuje se da li je data formula
;eorema (NF = 2 ** 2 ** N - 1), ili ne.

Ja detaljnijem opisu kompletnog FORTRAN programa se ne zadržava
;o, s obzirom na njegovu jednostavnost, a takodje i iz razloga
;to su u središtu naše pažnje u ovom radu metode dokazivanja
;eorema u predikatskom računu. Tim pre, što su metode koje se
;zlažu u narednim glavama ovog rada primenljive i na iskazni
;ačun.

# G L A V A II

## TEORIJSKE OSNOVE MEHANIČKOG DOKAZIVANJA TEOREMA U PREDIKATSKOM RAČUNU PRVOG REDA

U ovoj glavi na osnovu literature [124] , [82] , [194] , ] , [170] , [158] i [143] izlažemo osnovne rezultate o doka- anju teorema u predikatskom računu prvog reda. Stavove navodi- bez dokaza uz pozivanje na literaturu u kojoj se dokazi mogu i.

Istićemo sledeću notaciju:

Zagrade i interpunkcijski znaci ) ( ,

Propozicioni veznici $\neg$ $\vee$ $\wedge$ $\Rightarrow$ $\Leftrightarrow$

Kvantifikatori $\forall$ $\exists$

Promenljive $x_k$ , k=1,2,...

U konkretnim slučajevima pišemo i x,y,z,u,v,w,...

n-arni ($n \geqslant 0$) funkcijski simboli $f_k^n$ , k=1,2,...

U konkretnim slučajevima za $n > 0$ pišemo f,g,h,...

Za n=0 umesto konstanti $f_k^0$ pišemo a,b,c,...

n-arni ($n \geqslant 1$) predikatski simboli $p_k^n$ , k=1,2,...

U konkretnim slučajevima pišemo P,Q,R,...

## NEODLUČIVOST I OGRANIČENJA NA MEHANIČKE PROCEDURE DOKAZIVANJA

Predikatski račun se može izgraditi kako na bazi sintaksnih, o i na bazi semantičkih koncepcija. Prema Gedelovom stavu punosti obe koncepcije su ekvivalentne:

Formula predikatskog računa prvog reda je teorema ako i samo ako je valjana, tj.: $\vdash A \longleftrightarrow \models A$

inicija 1. (Hilbert i Bernajs [67], str.192.)

Formula A je deduktivno jednaka formuli B, ako je A izvodljiva iz B i B izvodljiva iz A po pravilima predikatskog računa.[1)]

primer, formula A(a), gde je A(a) proizvoljna formula u koju

---

Zahtev $\vdash A \Leftrightarrow B$ jači je od $A \vdash B$ i $B \vdash A$, tj. od zahteva za deduktivnu jednakost formula A i B.

lazi konstanta a , deduktivno je jednaka formuli ∀xA(x).
vaj primer se uopštava do stava ( [67], str.192.):

Ma koja formula A sa jednom ili više slobodnih promenljivih, deduktivno je jednaka formuli koja je univerzalno zatvorenje formule A.

bog toga, kad je reč o dokazivanju teorema, može se raditi
mo sa zatvorenim formulama.
zatvorene formule važi stav ( [162], str. 56. i 125.):
) Formula A je semantička posledica skupa formula
$A_1,A_2,\ldots,A_k$ , akko $A_1 \wedge A_2 \ldots \wedge A_k \Rightarrow A$ je valjana formula,
tj. $A_1,A_2,\ldots,A_k \models A \longleftrightarrow \models A_1 \wedge A_2 \ldots \wedge A_k \Rightarrow A$
) Formula A je (sintaksna) posledica skupa formula
$A_1,A_2,\ldots,A_k$ , akko je A semantička posledica tog skupa formula[1)], tj. $A_1,A_2,\ldots,A_k \vdash A \longleftrightarrow A_1,A_2,\ldots,A_k \models A$ .
osnovu stava potpunosti i ovog stava, zadatak dokazivanja
je data zatvorena formula teorema (ili posledica skupa zatvorenih formula), svodi se na dokazivanje da je odgovarajuća
ormula valjana. Iz rezultata Čerča ( [82], str.312.) sledi
a ne postoji opšta procedura za utvrdjivanje da li je data
ormula valjana ili nije. Sa sintaksnog stanovišta ovo je
karakterisano u [67] ,str. 172:
U predikatskom računu mi ne možemo, kao u iskaznom, zameniti izvodjenje formule primenom neke odlučive procedure. Naprotiv, mi smo u principu prinudjeni da se zaustavimo na deduktivnoj metodi."
edjutim, za formule koje su valjane postoji mehanička procedura pomoću koje se u konačnom broju koraka potvrdjuje da je ormula valjana ( [82], str.365.). Postojanje takve procedure aje osnovu da se predikatski račun smatra poluodlučivim ([158], tr. 81.).

efinicija 2. ([158], str.80., [67], str.168.)

Zatvorena formula A je zadovoljiva ako postoji interpretacija pri kojoj A ima vrednost ⊤ (tj. pri kojoj je A tačna). Takva interpretacija je model formule A.
A je nezadovoljiva ako za sve interpretacije ima vrednost ⊥ , (tj. ako za A ne postoji model).

---

) [illegible] formula ne mora biti konačan

Definicija 3. ([158], str. 81)

Skup S zatvorenih formula je zadovoljiv ako je zadovoljiva konjunkcija svih formula iz S.

Skup S je nezadovoljiv ako je nezadovoljiva konjunkcija svih formula iz S.

Na osnovu definicije 2., valjanost i nezadovoljivost su dualni: formula je valjana akko je njena negacija nezadovoljiva. Sledi, umesto dokazivanja valjanosti, može se dokazivati nezadovoljivost negacije date formule. Na primer, umesto dokazivanja valjanosti formule $A_1 \wedge \ldots \wedge A_k \Rightarrow A$, dokazuje se nezadovoljivost formule $A_1 \wedge \ldots \wedge A_k \wedge \neg A$. Na osnovu definicije 3., ovaj zadatak svodi se na dokazivanje da je skup $\{A_1, \ldots, A_k, \neg A\}$ nezadovoljiv.

Metode dokazivanja nezadovoljivosti datog skupa formula zovu se metode pobijanja (opovrgavanja).

Navedene definicije nisu konstruktivne, jer nije moguće razmotriti sve interpretacije na svim domenima. U posebnim slučajevima moguće je odrediti interpretaciju pri kojoj formula $\neg A$ ima vrednost $T$, pa tada sledi da $A$ nije valjana. Zbog toga, metoda gradjenja modela služi kao dobra dopuna metodi izvodjenja, jer se konstrukcijom izvodjenja utvrdjuje dokazivost tvrdjenja, a gradjenjem odgovarajućeg modela (za negaciju tvrdjenja) utvrdjuje se nedokazivost tvrdjenja, ([67], str.37.).

Iz egzistencije konačne procedure koja daje odgovor u slučaju kad je formula valjana, sledi egzistencija konačne procedure za utvrdjivanje da je negacija formule nezadovoljiva. Prvi korak na putu izgradjivanja takvih procedura je Skolem-Levenhajmov stav ([124], str.79):

Ako proizvoljna formula predikatskog računa prvog reda ima model, onda ima prebrojiv model.

Sledi, za dokaz da je formula nezadovoljiva dovoljno je dokazati da nema prebrojiv model.

Dalje, iz rezultata Erbrana sledi da je za utvrdjivanje nezadovoljivosti, umesto svih interpretacija nad raznim domenima, dovoljno posmatrati samo interpretacije nad jednim domenom: Erbranovim univerzumom.

# ERBRANOVA TEOREMA ZA KONAČAN NEZADOVOLJIV SKUP SASTAVAKA

## .1. Skolemizacija i skup sastavaka

Neka je $A_x(t)$ oznaka za formulu odredjenu iz formule (x) zamenom svakog slobodnog ulaženja promenljive $x$ termom , pri čemu je $t$ slobodan za $x$ u $A(x)$ .

uvodimo prvo, prema *[194]* i *[124]* , opis procesa skolemizaci-e:

Formula u preneksnoj formi je univerzalna, ako su svi kvantifikatori u njenom prefiksu univerzalni.
Neka je A zatvorena formula u preneksnoj normalnoj formi.
Formula $A^*$ , koja ne sadrži kvantifikatore odredjuje se na sledeći način:

$1^o$ Ako je A univerzalna, tj. oblika $\forall x_1 \ldots \forall x_n B$ , gde $n \geq 0$ i B ne sadrži kvantifikatore, onda je $A^*$ formula B .

$2^o$ Ako je A oblika $\forall x_1 \ldots \forall x_n \exists y B$ , $n \geq 0$, uvodi se nov n-arni funkcijski simbol $f$ ; u slučaju $n=0$ $f$ je nova konstanta. Neka je $A^o$ oznaka za formulu $\forall x_1 \ldots \forall x_n B_y(f(x_1,\ldots,x_n))$ . Formula $A^o$ sadrži jedan egzistencijalni kvantifikator manje od formule A. Ako $A^o$ nije univerzalna, postupak se ponavlja, tj. grade se formule $A^{oo}$ , $A^{ooo}$ itd., sve dok se ne dobije univerzalna formula. Iz nje se $A^*$ odredjuje prema $1^o$.

Kažemo da je $A^*$ dobijena iz A skolemizacijom.

Svaka zatvorena formula predikatskog računa prvog reda može se transformisati u skup sastavaka primenom sledećeg postupka ( [158] , str.83., *[143]*, str.181.):

(1) Vrši se preoznačavanje promenljivih tako da različita ulaženja kvantifikatora vezuju različite promenljive

(2) Eliminišu se simboli $\Leftrightarrow$ i $\Rightarrow$ uzastopnom primenom zamena $A \Leftrightarrow B \longleftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$ i $A \Rightarrow B \longleftrightarrow \neg A \vee B$

(3) Negacija se dovodi neposredno ispred predikatskih simbola primenom zamena:
$\neg(\neg A) \longleftrightarrow A$ ; $\neg(A \vee B) \longleftrightarrow \neg A \wedge \neg B$ ; $\neg(A \wedge B) \longleftrightarrow \neg A \vee \neg B$ ;
$\neg \forall x A \longleftrightarrow \exists x \neg A$ i $\neg \exists x A \longleftrightarrow \forall x \neg A$ .

(4) Formula se dovodi u preneksnu formu primenom zamena:

$KxA(x) \wedge B$ zamenjuje se sa $Kx(A(x) \wedge B)$

$KxA(x) \vee B$ zamenjuje se sa $Kx(A(x) \vee B)$, x ne ulazi u B.

$K_1xA(x) \wedge K_2yB(y)$ zamenjuje se sa $K_1xK_2y(A(x) \wedge B(y))$

$K_1xA(x) \vee K_2yB(y)$ zamenjuje se sa $K_1xK_2y(A(x) \vee B(y))$

gde $K, K_1, K_2 \in \{\forall, \exists\}$ .

5) Izvrši se skolemizacija preneksne forme

6) Formula (bez kvantifikatora) dovodi se u konjunktivnu normalnu formu

7) Eliminišu se simboli $\wedge$ zamenom $A \wedge B$ sa dve formule A,B .

menom (1)-(7) odredjuje se konačan skup formula od kojih je
ka disjunkcija konačnog broja atomičnih formula ili njihovih
acija.

Atomičnu formulu ili njenu negaciju zovemo literal.

Sastavak je disjunkcija literala. Prema tome, primenom
-(7) na datu formulu odredjuje se skup sastavaka. Iako sastav
ne sadrže kvantifikatore, smatramo ih zatvorenim formulama.
se opravdava sledećom valjanom formulom:

$\forall x(D_1 \wedge \ldots \wedge D_k) \Longleftrightarrow \forall xD_1 \wedge \ldots \wedge \forall xD_k$ , gde su $D_i$ sastavci.

Neka je S′ neki skup zatvorenih formula i S skup
stavaka odredjen primenom (1)-(7) na svaki element iz S′.
la važi stav ([158], str.84., [143], str.185., [124], str.93.):

Skup S′ je nezadovoljiv akko je nezadovoljiv skup S .

## 2. Erbranov univerzum i Erbranova teorema

Neka je S konačan skup sastavaka.

Erbranov univerzum H , kao domen interpretacije za S ,
iniše se na sledeći način ( [158], str.182., [143], str.185.):

Definicija 4.

) Svaka konstanta sadržana u S pripada H.

Ako S ne sadrži konstante, onda H sadrži neku konstantu,
recimo a .

) Ako termi $t_1, \ldots, t_n$ pripadaju H, onda term $f^n(t_1, \ldots, t_n)$
pripada H, gde je $f^n$ funkcijski simbol iz S.

) H sadrži one i samo one terme koji zadovoljavaju a) ili b)
ove definicije.

branov univerzum je konačan akko u S nema funkcijskih simbo-
, u suprotnom H je prebrojiv.

finicija 5.

Term koji ne sadrži promenljive je fundamentalan term.
Fundamentalna instanca sastavka $D(x_1,\ldots,x_k)$ nad skupom fundamentalnih terma P, gde su $x_1,\ldots,x_k$ sve različite promenljive u sastavku D, je sastavak $D_{x_1,\ldots x_k}(t_1,\ldots,t_k)$ odredjen zamenom svakog ulaženja promenljivih $x_i$ u D termima $t_i$ , $t_i \in P$ , $i=1,2,\ldots,k$.
Fundamentalna instanca sastavka D koji ne sadrži promenljive je D.
Evidno, fundamentalna instanca nad H je konstantan primer stavka $D(x_1,\ldots,x_k)$.

finicija 6.

Erbranova baza skupa sastavaka S je skup svih fundamentalnih instanci atomičnih formula iz S, nad Erbranovim univerzumom i za S.
Fundamentalna instanca atomične formule zove se atom.
ma tome, elementi Erbranove baze su atomi.
primer, za skup $S = \{P(x), Q(g(y)) \vee \neg R(z)\}$ Erbranov univer- je $H = \{a, g(a), g(g(a)), \ldots\}$ . Jedna fundamentalna instan- sastavka $Q(g(y)) \vee \neg R(z)$ u odnosu na H je $Q(g(a)) \vee \neg R(g(g(a)))$.
branova baza konačnog skupa S je skup
$\{P(a), Q(g(a)), R(a), P(g(a)), Q(g(g(a))), R(g(a)), \ldots\}$
branova baza konačnog skupa S je konačna ako je H konačan i ako S ne sadrži promenljive; u suprotnom je prebrojiva.

finicija 7.

H-interpretacija skupa S je interpretacija S nad H koja zadovoljava uslove:

(1) Svaka konstanta interpretira se kao ona sama
(2) Svaki n-arni funkcijski simbol f iz S interpretira se kao funkcija $H^n \longrightarrow H$, takva da se $(h_1,\ldots,h_n) \in H^n$ preslikava u $f(h_1,\ldots,h_n) \in H$ .
(3) Svaki predikatski simbol $p^n$ interpretira se kao relacija dužine n skupa H .

eka je $A = \{A_1,\ldots,A_n,\ldots\}$ Erbranova baza za skup S.
ada je H-interpretacija J odredjena skupom:
$J = \{m_1,\ldots,m_n,\ldots\}$ , gde je $m_i$ istinitosna vrednost za $A_i$.
običajeno je da se umesto $m_i$ piše $A_i$ kad $m_i = T$, odnosno $\neg A_i$
ad $m_i = \bot$.

H-interpretacija J ne zadovoljava sastavak $D(x_1,\ldots,x_k)$
ko postoji fundamentalna instanca $D_{x_1,\ldots,x_k}(t_1,\ldots,t_k)$ nad H
oja pri interpretaciji J ima vrednost $\bot$ .
-interpretacija J ne zadovoljava skup sastavaka S ako ne zado-
oljava bar jedan sastavak iz S.
a primer, H-interpretacija $J_1 = \{P(a), \neg Q(g(a)), R(a),\ldots\}$
e zadovoljava skup $S = \{P(x), Q(g(y)) \vee \neg R(z)\}$ , jer fundamental-
a instanca $Q(g(a)) \vee \neg R(a)$ sastavka $Q(g(y)) \vee \neg R(z)$ pri interpreta
lji $J_1$ ima vrednost $\bot$ .

aži sledeći <u>stav</u> ([25], prema [158], str.184.):

Skup sastavaka S je nezadovoljiv akko je S nezadovoljiv pri svim H-interpretacijama.

ledi, za utvrdjivanje nezadovoljivosti skupa sastavaka dovoljno
e razmotriti samo H-interpretacije.
edjutim, kako Erbranova baza može biti beskonačna, odredjivanje
-interpretacije je u tom slučaju beskonačan proces. Osim toga,
roj različitih H-interpretacija ne mora biti konačan. Ove teš-
oće otklonjene su zahvaljujući znamenitoj teoremi Erbrana ([82],
tr. 450.).
<u>eorema Erbrana</u> ima nekoliko ekvivalentnih formulacija. Za sa-
ržaje koje izlažemo najpogodnija je formulacija J.A.Robinson
[170], engl., str.27.)

Konačan skup sastavaka S je nezadovoljiv akko za neki konačan podskup P Erbranovog univerzuma je nezadovoljiv skup P(S), gde je P(S) skup svih fundamentalnih instanci sastavaka iz S nad P.

kup P(S), tzv. zasićenje S nad P, je konačan.

Navedeni oblik teoreme Erbrana omogućuje da se nezadovolji
ost konačnog skupa sastavaka S utvrdi primenom sledeće konačne
procedure ([170], str.27., [158], str.184.):

Neka su $P_o, P_1, P_2, \ldots$ konačni podskupovi Erbranovog univer zuma H za konačan skup sastavaka S, takvi da $P_i \subseteq P_{i+1}$ , za svako $i \geq 0$ i $\bigcup_I P_i = H$ .

Proverava se da li su skupovi $P_o(S), P_1(S), P_2(S), \ldots$ nezadovoljivi. Za ma koji konačan podskup P od H za neko j va- ži $P \subseteq P_j$ i zato $P(S) \subseteq P_j(S)$ .
Sledi, ako je S nezadovoljiv, onda je za neko konačno j nezado- voljiv $P_j(S)$, pa procedura završava rad na koraku j.

Kao konačni podskupovi Erbranovog univerzuma mogu se uzeti nivoi $H_o, H_1, \ldots$ koji se definišu na sledeći način:

(1) $H_o$ je skup svih konstanti u H

(2) Ako termi $t_1, \ldots, t_n$ pripadaju nivou $H_j$ skupa H, onda term $f^n(t_1, \ldots, t_n)$ pripada nivou $H_{j+1}$ i $H_j \subset H_{j+1}$ , $j \geq 0$ .

Procedura zasićenja nivoa odredjuje skupove $H_o(S), H_1(S), \ldots$ sve dok se za neko konačno j ne utvrdi da je $H_j(S)$ nezadovoljiv. Ako S nije nezadovoljiv, procedura ne završava rad.

Na metodi zasićenja nivoa zasnovane su procedure za mehanič ko dokazivanje teorema Gilmora [50], Davisa-Putnama [34] i razna njihova poboljšanja ( [35] ). Medjutim, nagli rast brojnosti sku- pova $H_j$ i $H_j(S)$ sa rastom j, i pored pokušaja poboljšanja, činio je ove procedure praktično neefikasnim.

## 3. PRAVILO REZOLUCIJE. ALGORITAM UNIFIKACIJE

Osnovne rezultate o rezoluciji izlažemo prema [170].

### 3.1. Fundamentalna rezolucija

Definicija 8. Ako je A atomična formula, onda su literali A i $\neg A$ komplementarni i obrazuju komplementaran par.

Definicija 9. Sastavak je konačan skup literala.
Prazan skup literala je prazan sastavak, u oznaci $\square$ .

Prema ovoj definiciji disjunkcija literala shvata se kao skup literala. Treba razlikovati prazan sastavak od praznog skupa sa-

tavaka. Prazan skup sastavaka je zadovoljiv, dok prazan sastak nije zadovoljiv.

efinicija 10.

Literal koji ne sadrži promenljive je fundamentalan literal. Sastavak čiji su elementi fundamentalni literali je fundamentalan sastavak. Posebno, $\square$ je fundamentalan sastavak.

rema ovoj definiciji svaka fundamentalna instanca sastavka D ad Erbranovim univerzumom H, je fundamentalan sastavak.

efinicija fundamentalne rezolvente

Ako su C i D fundamentalni sastavci, $L \subseteq C$ , $M \subseteq D$ i L,M jednočlani skupovi čiji elementi obrazuju komplementaran par, onda je fundamentalna rezolventa R sastavaka C i D sledeći fundamentalan sastavak: $\mathcal{R} = (C \setminus L) \cup (D \setminus M)$ .

a primer, za $P(a) \vee Q(b)$ i $\neg P(a) \vee \neg R(f(a))$ , gde su a i b konstane i f funkcijski simbol, fundamentalna rezolventa je $(b) \vee \neg R(f(a))$, tj. u skupovnoj notaciji: $C = \{P(a), Q(b)\}$ , $= \{P(a), \neg R(f(a))\}$ , pa je $\mathcal{R} = \{Q(b), \neg R(f(a))\}$ .

Neka je S skup fundamentalnih sastavaka. Skup $R_n(S)$, $n \geq 0$, efiniše se na sledeći način:

(1) $R_0(S) \stackrel{def}{=\!=} S$ ; (2) $R_{n+1}(S) \stackrel{def}{=\!=} R(R_n(S))$

pri čemu je $R(C) \stackrel{def}{=\!=} C \cup F$ , F – skup svih fundamentalnih rezolventi sastavaka iz skupa C.

ada važi sledeći stav (teorema o fundamentalnoj rezoluciji, *170]*, str.28.):

Konačan skup fundamentalnih sastavaka S je nezadovoljiv akko za neko $n \geq 0$ skup $R_n(S)$ sadrži prazan sastavak.

ada važi sledeći poseban oblik teoreme Erbrana ([*170*] , str.29.):

Ako je S proizvoljan konačan skup sastavaka, onda je S nezadovoljiv akko za neki konačan podskup P Erbranovog univerzuma za S i neko $n \geq 0$ skup $R_n(P(S))$ sadrži prazan sastavak. (P(S) – zasićenje S nad P).

Pravilo fundamentalne rezolucije je poseban slučaj opštijeg pravila - pravila rezolucije koje se može primeniti i kad sastavci sadrže promenljive. U sledećoj tački navodimo pojmove koji se koriste za definisanje pravila rezolucije.

## 3.2. Zamene, unifikacija i algoritam unifikacije

*Definicija 11.* ([170] , str.31.)

Zapis oblika $t/x$ , gde je x promenljiva i t term različit od x, zove se zamenska komponenta; x je promenljiva i t je term zamenske komponente $t/x$ .

Konačan skup zamenskih komponenti

$$\Theta = \{ t_1/x_1, \ldots, t_n/x_n \} \quad , \text{ gde } x_i \neq x_j \text{ za } i \neq j \ ,$$

zove se zamena.

Prazan skup zamenskih komponenti je prazna zamena.

Neka je E konačna reč obrazovana konkatenacijom simbola predikatskog računa i $\Theta$ neka zamena.

$\Theta$-primer reči E, u oznaci $E\Theta$, je reč odredjena iz reči E jednovremenim zamenjivanjem svakog ulaženja promenljivih $x_i$ u E za koje $t_i/x_i \in \Theta$, termima $t_i$ .

Na primer, za $P(f(x,y),z)$ i $\Theta = \{ y/x, a/y, b/u \}$ , $\Theta$-primer je $P(f(y,a),z)$ , a za zamenu $\Theta_1 = \{ a/x, a/y, b/u \}$ , $\Theta_1$-primer je $P(f(a,a),z)$ .

Ako je C neki skup reči i $\Theta$ zamena, onda je $\Theta$-primer skupa C,, u oznaci $C\Theta$, skup svih reči $E\Theta$, gde $E \in C$ .

*Definicija 12.*

Neka su $\Theta = \{ t_1/x_1, \ldots, t_n/x_n \}$ i $\lambda$ dve zamene.

Kompozicija redom zamena $\Theta$ i $\lambda$ , u oznaci $\Theta\lambda$ , je skup $\Theta' \cup \lambda'$, gde je $\Theta' = \{ t_1/x_1, \ldots, t_n/x_n \} \setminus \{ x_1/x_1, \ldots, x_n/x_n \}$

i $\lambda' = \lambda \setminus \{ u/x \mid t/x \in \Theta \}$ .

U [170] , str.32. dokazane su sledeće jednakosti:

1. $(E\sigma)\lambda = E(\sigma\lambda)$ , za ma koju reč E i ma koje zamene $\sigma$ i $\lambda$ .
2. $(\sigma\lambda)\mu = \sigma(\lambda\mu)$ , za ma koje zamene $\sigma$ , $\lambda$ , $\mu$ .
3. $(C_1 \cup C_2)\lambda = C_1\lambda \cup C_2\lambda$ , za ma koje skupove reči $C_1$ i $C_2$ .

Neka je C neki skup terma i literala.

Leksikografski poredak uvodi se u C na sledeći način:

$1^o$ $A \in C$ je ispred $B \in C$, ako A sadrži manje simbola od B .

$2^o$ Ako $A \in C$ i $B \in C$ sadrže isti broj simbola i ako su a iz A i b iz B prvi po redu (s leva na desno) različiti simboli, onda je A ispred B akko a prethodi b u sledećem poretku:

$$x_1, x_2, \ldots, f_1^o, f_2^o, \ldots, f_1^1, f_2^1, \ldots, \ldots, p_1^1, p_2^1, \ldots, \ldots, \neg$$

gde su $x_i$ promenljive, $f_i^o$ konstante, $f_i^j$ funkcijski simboli dužine j, $p_i^j$ predikatski simboli dužine j, $\neg$ znak negacije.

)efinicija 13.

Neka je A neki, najmanje dvočlan skup literala.

Skup neslaganja B za skup A je skup svih literala, odnosno terma, koji na r-tom mestu u literalu $L_i \in A$ počinju simbolom $\delta_i^r$ , i=1,2,..., gde je r najmanji redni broj takav da u nizu $\delta_1^r, \delta_2^r, \ldots$ postoje različiti simboli.

čevidno, ako B nije prazan, onda sadrži bar dva elementa.

a primer, za skup $A = \{P(x,f(x,y),y), P(x,g(y),z), P(x,a,z)\}$ kup neslaganja $B = \{f(x,y), g(y), a\}$ .

efinicija 14.

Zamena $\Theta$ je unifikator skupa C, gde je C skup terma ili skup literala, ako je $C\Theta$ jednočlan skup.

Ako za skup C postoji unifikator $\Theta$, kaže se da $\Theta$ unificira skup C, odnosno da je C unifikativan skup.

čevidno, ako je $\Theta$ unifikator za skup A, onda $\Theta$ unificira i skup eslaganja B za skup A.

nifikativan skup A može imati više unifikatora.

efinicija 15.

Neka su $\Theta$ i $\sigma$ unifikatori skupa literala A.

Unifikator $\sigma$ je najopštiji unifikator (NOU) skupa A, ako za ma koji unifikator $\Theta$ skupa A postoji zamena $\lambda$ takva da je $\Theta = \sigma\lambda$

)stoji algoritam unifikacije ( [170] , str.32.) koji odredjuje )U za unifikativan skup literala i daje odgovor o nepostojanju nifikatora u slučaju da skup nije unifikativan.

Algoritam unifikacije za konačan neprazan skup literala

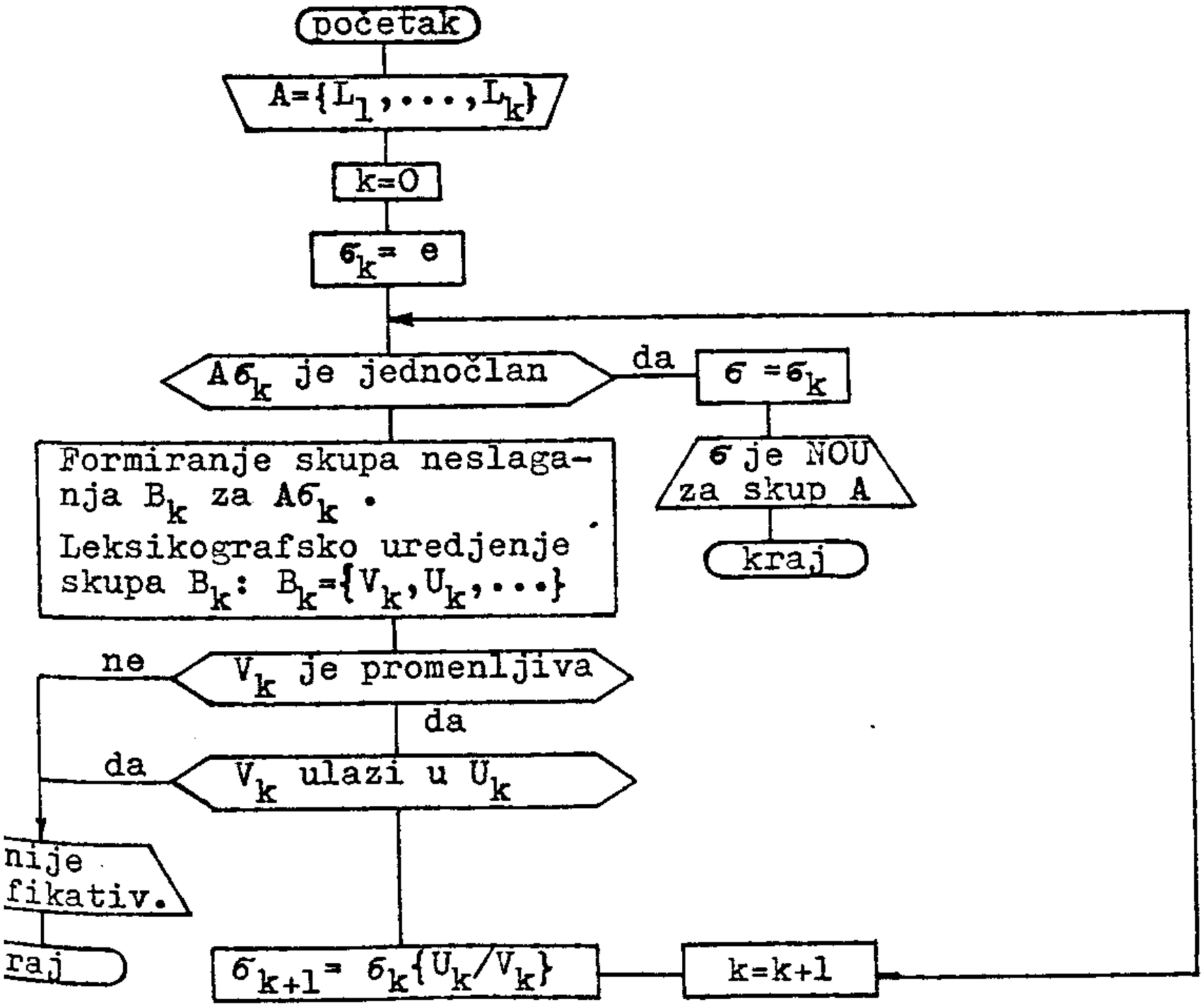
1.korak Staviti k=0 i $\sigma_k$= e (e-prazna zamena).Preći na 2.

2.korak Ako $A\sigma_k$ nije jednočlan skup, preći na 3. U suprotnom, staviti $\sigma = \sigma_k$ i završiti rad.

3.korak Neka je $V_k$ prvi, a $U_k$ sledeći element u leksikografskom poretku uredjenog skupa nesłaganja $B_k$ za $A\sigma_k$ .
Ako je $V_k$ promenljiva, koja ne ulazi u $U_k$, onda odrediti $\sigma_{k+1} = \sigma_k \{U_k/V_k\}$ (kompozicija $\sigma_k$ i $\{U_k/V_k\}$), uvećati k za 1 i preći na 2. U suprotnom, prekinuti rad i saopštiti da unifikator za skup A ne postoji.

U *[170]*, str.32-34 dokazano je da algoritam unifikacije završava rad za svaki neprazan konačan skup literala i da je u slučaju kad algoritam završava rad na 2.koraku, zamena $\sigma$ NOU .

SHEMA ALGORITMA ODREDJIVANJA NOU ZA KONAČAN SKUP LITERALA



## 3.3. Pravilo rezolucije

Navodimo prema [170], str.33 i [158], str.187 definicije rezolvente i pravila rezolucije. Sastavci se tretiraju kao skupovi literala.

Definicija rezolvente

Neka za sastavke $D_1$ i $D_2$, koji ne sadrže zajedničke promenljive (to se uvek može postići preoznačavanjem promenljivih), i za $L_1 \subseteq D_1$, $L_2 \subseteq D_2$ važe uslovi:

(1) Skupovi $L_1$ i $L_2$ nisu prazni,

(2) Za skup A svih atomičnih formula sadržanih u $L_1 \cup L_2$ postoji NOU $\sigma_A$,

(3) Elementi jednočlanih skupova $L_1\sigma_A$ i $L_2\sigma_A$ obrazuju komplementaran par[1].

Rezolventa sastavaka $D_1$ i $D_2$ je sastavak

$$(D_1 \setminus L_1)\sigma_A \cup (D_2 \setminus L_2)\sigma_A .$$

Na primer, za sastavke $D_1$: $P(x) \vee \neg Q(f(x)) \vee P(z)$ i $D_2$: $\neg P(a) \vee R(y)$ rezolventa je: $\neg Q(f(a)) \vee R(y)$. U skupovnoj notaciji: $D_1 = \{P(x), \neg Q(f(x)), P(z)\}$, $D_2 = \{\neg P(a), R(y)\}$, $L_1 = \{P(x), P(z)\}$, $L_2 = \{\neg P(a)\}$, $A = \{P(x), P(z), P(a)\}$; $\sigma_A = \{a/x, a/z\}$; $L_1\sigma_A = \{P(a)\}$, $L_2\sigma_A = \{\neg P(a)\}$; $(D_1 \setminus L_1)\sigma_A = \{\neg Q(f(a))\}$, $(D_2 \setminus L_2)\sigma_A = \{R(y)\}$, pa je rezolventa: $\{\neg Q(f(a)), R(y)\}$.

Kako sastavci $D_1$ i $D_2$ mogu imati najviše konačan broj različitih podskupova $L_1, L_2$ za koje važe uslovi (1)-(3), sledi da je broj rezolventi najviše konačan.

Definicija rezolucije

Neka su $D_1$ i $D_2$ sastavci za koje su ispunjeni uslovi (1)-(3) i R njihova rezolventa.

Pravilo izvodjenja: $\dfrac{D_1, D_2}{R}$ ZOVE SE REZOLUCIJA.

---

1) videti definiciju 8. tač. 3.1. str. 35.

Neka je $\mathcal{R}(C) \overset{\text{def}}{=\!=} C \cup \mathcal{F}$ , gde je $\mathcal{F}$ skup svih rezolventi elemenata skupa C.

Za skup sastavaka S, skup $\mathcal{R}_n(S)$ definiše se na sledeći način: $1^o\ \mathcal{R}_o(S) = S$ ; $2^o\ \mathcal{R}_{n+1}(S) = \mathcal{R}(\mathcal{R}_n(S))$ , $n \geq 0$ .

Važi <u>lema</u> ([170], str.34.):

> Ako je S skup sastavaka, P neki podskup Erbranovog univerzuma H za S i P(S) skup fundamentalnih instanci sastavaka iz S nad P (zasićenje S nad P), onda je
>
> $$\mathcal{R}(P(S)) \subseteq P(\mathcal{R}(S)) .$$

Njena posledica je: $\mathcal{R}_n(P(S)) \subseteq P(\mathcal{R}_n(S))$ .

Sada se poseban oblik Erbranove teoreme (videti tač.3.1. str.36.) transformiše u sledeći <u>stav</u> ([170] ,str.29.):

> Ako je S proizvoljan konačan skup sastavaka, onda je S nezadovoljiv akko za neki konačan podskup P Erbranovog univerzuma za S i neko $n \geq 0$, skup $P(\mathcal{R}_n(S))$ sadrži prazan sastavak.

Dalje, kako bilo koja zamena terma umesto promenljivih ne može transformisati neprazan sastavak u prazan sastavak, sledi: $P(\mathcal{R}_n(S))$ sadrži prazan sastavak akko $\mathcal{R}_n(S)$ sadrži prazan sastavak.
To omogućuje da se gore navedeni stav transformiše u sledeći konačan oblik - teoremu o rezoluciji.

<u>Teorema o rezoluciji</u> ( [170] , str.30.):

> Konačan skup sastavaka S je nezadovoljiv akko skup $\mathcal{R}_n(S)$ za neko konačno $n \geq 0$ sadrži prazan sastavak.

Očevidno, kad je S konačan skup fundamentalnih sastavaka, teorema o rezoluciji poklapa se sa teoremom o fundamentalnoj rezoluciji (videti tač.3.1. str.36.) .

Na osnovu teoreme o rezoluciji definiše se pobijanje datog skupa sastavaka ([170], str.35.):

<u>Pobijanje (opovrgavanje) datog skupa sastavaka S</u> je konačan niz sastavaka $B_1,\dots,B_k$ , takav da za svaki član $B_i$, $1 \leqslant i < k$, važi:

$1^\circ$ $B_i \in S$ ili $B_i$ je rezolventa neka dva prethodna člana niza

$2^\circ$ $B_k$ je prazan sastavak .

Sledi, pobijanje datog skupa sastavaka S je izvodjenje praznog sastavka iz skupa S, pri čemu skup pravila izvodjenja sadrži samo pravilo rezolucije.

Iz teoreme o rezoluciji sledi:

Konačan skup sastavaka S je nezadovoljiv akko postoji pobijanje za S.

Zato je teorema o rezoluciji ujedno i teorema o potpunosti ovog logičkog sistema.

## 4. PROCEDURE MEHANIČKOG DOKAZIVANJA TEOREMA ZASNOVANE NA REZOLUCIJI

Na osnovu teoreme o rezoluciji može se izgraditi sledeća <u>procedura pobijanja</u> ( *[170]*, str.37.):

Za konačan skup sastavaka S primenom pravila rezolucije odredjuju se skupovi $\mathcal{R}_1(S)$ , $\mathcal{R}_2(S)$ , . . . pri čemu može nastati jedan od sledećih ishoda:

1. Za neko konačno $n \geqslant 0$ skup $\mathcal{R}_n(S)$ sadrži prazan sastavak, pa je S nezadovoljiv ;
2. Za neko konačno $n \geqslant 0$ $\mathcal{R}_n(S) = \mathcal{R}_{n+1}(S)$ , pa je S zadovoljiv;
3. Procedura beskonačno generiše rezolvente, što je u vezi sa neodlučivošću predikatskog računa prvog reda.
   Prepoznavanje beskonačnog procesa moguće je samo u nekim posebnim slučajevima.

Procedura pobijanja može se primeniti za dokazivanje teorema u teorijama prvog reda (specijalnim kvantifikatorskim računima) sa konačnim brojem sopstvenih aksioma i za dokazivanje teorema predikatskog računa.

U slučaju teorija prvog reda skup S se formira na sledeći način:

$$S = A_1^s \cup A_2^s \cup \ldots \cup A_k^s \cup (\neg A)^s$$

gde $A_i^s$ su skupovi sastavaka odredjeni iz sopstvenih aksioma $A_i$ , i=1,2,...,k , a $(\neg A)^s$ je skup sastavaka odredjen iz negacije zatvorene formule A za koju se traži dokaz.
Za dokaz da je formula A teorema predikatskog računa, u S nije potrebno navoditi aksiome predikatskog računa. Zaista, ako je A teorema predikatskog računa i A zatvorena formula, onda je formula $\neg A$ nezadovoljiva, pa je nezadovoljiv i skup $S = (\neg A)^s$, gde $(\neg A)^s$ je skup sastavaka odredjen iz negacije zatvorene formule A.

Procedura pobijanja koja se gradi neposredno na osnovu teoreme o rezoluciji ima više teorijski nego praktičan značaj, jer brojnost skupova $\mathcal{R}_i(S)$ sa povećanjem i naglo raste. Skraćivanje i usmeravanje procesa izvodjenja postiže se ograničavanjem primene pravila rezolucije i primenom efektivnijih strategija pretraživanja. Procedura koju smo naveli zasnovana je na strategiji potpunog pregleda, kaže se još i pregleda u širinu ili zasićenja nivoa, tj. na generisanju rezolventi svih parova sastavaka iz $\mathcal{R}_i(S)$ , i=0,1,...

U sledećoj tački navodimo informativan pregled važnijih ograničenja primene pravila rezolucije, a u tački 4.2. kratko izlažemo ideje nekih strategija pretraživanja. U tački 4.3. navodimo opšte blok sheme algoritama pobijanja zasnovanih na raznim formama rezolucije.

## 4.1. Specifične forme rezolucije (informativan pregled)

4.1.1. Semantička rezolucija ([158] , str.191.), zasniva se na ideji "klaša" koji se definiše na sledeći način:

Neka je I interpretacija i P neki poredak predikatskih simbola sadržanih u skupu sastavaka S.

Konačan skup sastavaka $\{E_1,\ldots,E_q,N\}$ , $q \geq 1$, zove se

**s e m a n t i č k i  k l a š** u odnosu na P i I (PI - klaš) akko $E_1,\ldots,E_q$ (tzv.sateliti) i N (tzv. jedro) zadovoljavaju uslove:

(1) I ne zadovoljava $E_i$ , i=1,2,...,q

(2) $R_1$=N i postoji rezolventa $R_{i+1}$ za $R_i$ i $E_i$ ,i=1,2,...,q

(3) Rezolucija se vrši po literalu $L_1 \in E_i$ koji je najveći u $E_i$ u odnosu na poredak P: $P_1 < P_2 < \ldots < P_k$ , gde $P_j$ su predikatski simboli koji ulaze u sastavke skupa S.

(4)Interpretacija I ne zadovoljava rezolventu $R_{q+1}$.

Rezolventa $R_{q+1}$ zove se PI - rezolventa. S obzirom na (1)-(4), PI-rezolventa nastaje uzastopnom primenom pravila rezolucije.

Semantička rezolucija (PI-rezolucija) je pravilo izvodjenja koje iz datog skupa sastavaka S generiše PI-rezolvente.

Izvodjenje iz S je PI-izvodjenje ako je svaki sastavak u izvodjenju element iz S ili je PI-rezolventa prethodnih članova izvodjenja.

Primer ( [158] ,str.192.):

Neka je $E_1$= P(x)VQ(x), $E_2$=Q(x)VR(x), N=¬P(x)V¬Q(x)VR(x) [={¬P,¬Q,¬R} , gde ¬P,¬Q,¬R znači da su atomične formule koje sadrže simbole P,Q,R netačne pri interpretaciji I . Neka je P sledeći poredak predikatskih simbola: P> Q >R . Tada je $\{E_1,E_2,N\}$ PI-klaš, a PI-rezolventa ovog klaša je R(x). Ovde ni $\{E_1,N\}$ ni $\{E_2,N\}$ nije PI-klaš, jer I zadovoljava rezolvente, pa uslov (4) nije zadovoljen.

PI-rezolucija je potpuna u sledećem smislu (Čeng,Li,1973., prema [158], str.194.):

Ako je P poredak predikatskih simbola u konačnom nezadovoljivom skupu sastavaka S i I interpretacija, onda postoji PI-izvodjenje praznog sastavka iz S .

Izborom specijalnih interpretacija dobijaju se posebni slučajevi semantičke rezolucije: hiperrezolucija i rezolucija potpornog skupa. Prethodno izlažemo uredjenu rezoluciju, koja se koristi za definisanje hiperrezolucije.

4.1.2. Uredjena rezolucija ([158],str.196.)

Poredak predikatskih simbola uveden za PI-rezoluciju, u opštem slučaju ne obezbedjuje jedinstven izbor literala u satelitu, koji je kandidat za unifikaciju i rezoluciju. Da bi se obezbedio jedinstven izbor literala uvodi se poredak u sastavke (Reiter,1971).
Za razliku od sastavaka, koji se tretiraju kao skupovi literala, uredjeni sastavci su uredjene k-torke literala odredjene poretkom literala u sastavcima s leva na desno. Prvi literal u sastavku je najmladji, a poslednji je najstariji. Od dva literala u uredjenom sastavku mladji je onaj koji stoji levo.

Ako za dva ili više literala uredjenog sastavka D postoji NOU $\Theta$ , onda uredjen sastavak koji se dobija iz D$\Theta$ isključivanjem ma kojeg literala identičnog mladjem literalu, zove se uredjen faktor sastavka D.

Uredjena binarna rezolventa sastavka $D_1$ i sastavka $D_2$, koji ne sadrže zajedničke promenljive, odredjuje se na sledeći način: Neka su $L_1$ i $L_2$ literali u $D_1$ i $D_2$ , respektivno.
Ako za $L_1$ i $L_2$ postoji NOU $\Theta$ , onda se formira konkatenacija nizova $D_1\Theta$ i $D_2\Theta$ i iz nje se odstranjuju komplementarni literali $L_1\Theta$ i $L_2\Theta$ . Zatim se iz tako odredjenog uredjenog sastavka isključuju literali koji su identični nekom mladjem literalu. Tako odredjeni uredjeni sastavak D je uredjena binarna rezolventa redom za $D_1$ i $D_2$.
Uredjena binarna rezolventa $D_1$ i $D_2$ različita je od uredjene binarne rezolvente za $D_2$ i $D_1$.

Uredjena rezolventa uredjenih sastavaka $D_1$ i $D_2$ je jedna od sledećih uredjenih binarnih rezolventi:

a) $D_1$ i $D_2$ ,
b) $D_1$ i uredjenog faktora $D_2$ ,
c) Uredjenog faktora $D_1$ i $D_2$ ,
d) Uredjenog faktora $D_1$ i uredjenog faktora $D_2$.

Uredjena rezolucija je pravilo izvodjenja koje generiše uredjene rezolvente iz skupa uredjenih sastavaka.

uredjena rezolucija je potpuna (Kovaljski,Heis 1969,prema [158],str. 197.). Medjutim, semantička rezolucija za uredjene nastavke, koja se odredjuje na osnovu uredjenog semantičkog klaša za interpretaciju I (OI-klaš), tzv. OI-rezolucija nije potpuna (Anderson,1971, prema [158],str.199.).

4.1.3. Hiperrezolucija ([158],str.199.)

Neka je svaki element skupa I negacija predikatskog simbola (kao u primeru na str. 44.). Za takvu interpretaciju I, PI-rezolucija zove se pozitivna hiperrezolucija akko svi sateliti i sve PI-rezolvente (hiperrezolvente) su pozitivni uredjeni sastavci (sastavci koji ne sadrže ¬ ), jedro nije pozitivan uredjen sastavak i u svakom nepozitivnom uredjenom sastavku literali bez negacije prethode svim literalima sa negacijom.
Analogno se odredjuje negativna hiperrezolucija.
Postoji algoritam pobijanja koji za nezadovoljiv konačan skup sastavaka S generiše prazan sastavak generišući pozitivne hiperrezolvente ([158],str.200.). Blok shemu tog algoritma navodimo u tački 4.3.

4.1.4. Rezolucija potpornog skupa ([143],str.243,[158],str.194.)

Neka je S konačan nezadovoljiv skup sastavaka i $K \subseteq S$, takav da je skup $S \setminus K$ zadovoljiv.
Neka je I interpretacija koja zadovoljava skup $S \setminus K$ i P neki poredak predikatskih simbola u S. Iz potpunosti PI-rezolucije sledi da postoji PI-izvodjenje praznog sastavka iz S. Prema tome, u svakom PI-klašu interpretacija I ne zadovoljava satelite pa nijedan sastavak iz $S \setminus K$ nije satelit. Sledi, u svakoj binarnoj rezoluciji u procesu odredjivanja PI-rezolvente, bar jedan sastavak pripada skupu K. Kaže se da je K potporni skup i da njegovi elementi imaju podršku. Smatra se da i svaka rezolventa ima podršku.
Binarna rezolucija u kojoj bar jedan sastavak ima podršku zove se rezolucija potpornog skupa.

Razlaganjem svakog PI-klaša u PI-izvodjenju praznog sastavka na niz binarnih rezolucija dobija se izvodjenje sa potpornim skupom. Na osnovu potpunosti PI-rezolucije sledi da je rezolucija potpornog skupa potpuna.

Ako je S konačan nezadovoljiv skup sastavaka koji potiču od sopstvenih akşioma neke neprotivrečne teorije prvog reda i od negacije teoreme koju treba dokazati, onda se za potporni skup K mogu uzeti sastavci koji potiču od negacije teoreme ($S \setminus K$ je u tom slučaju zadovoljiv).
Opšta blok shema za binarnu rezoluciju koju navodimo u tački 4.3 obuhvata rezoluciju potpornog skupa.
Rezolucija potpornog skupa često se razmatra i kao posebna strategija - strategija potpornog skupa ( a ne kao zasebna forma rezolucije).

4.1.5. a) Linearna rezolucija ([158],str.202.)

Elementi polaznog skupa S zovu se ulazni sastavci.
Ulazna rezolucija je binarna rezolucija para sastavaka od kojih je bar jedan ulazni sastavak.
Linearno izvodjenje iz S je niz sastavaka $D_1,\ldots,D_n$ , gde je $D_1 \in S$ , a svaki član $D_{i+1}$ ,i=1,2,...,n-1 , je rezolventa sastavka $D_i$ (tzv. centralnog sastavka) i sastavka B (tzv. bočnog sastavka) koji zadovoljava jedan od uslova:

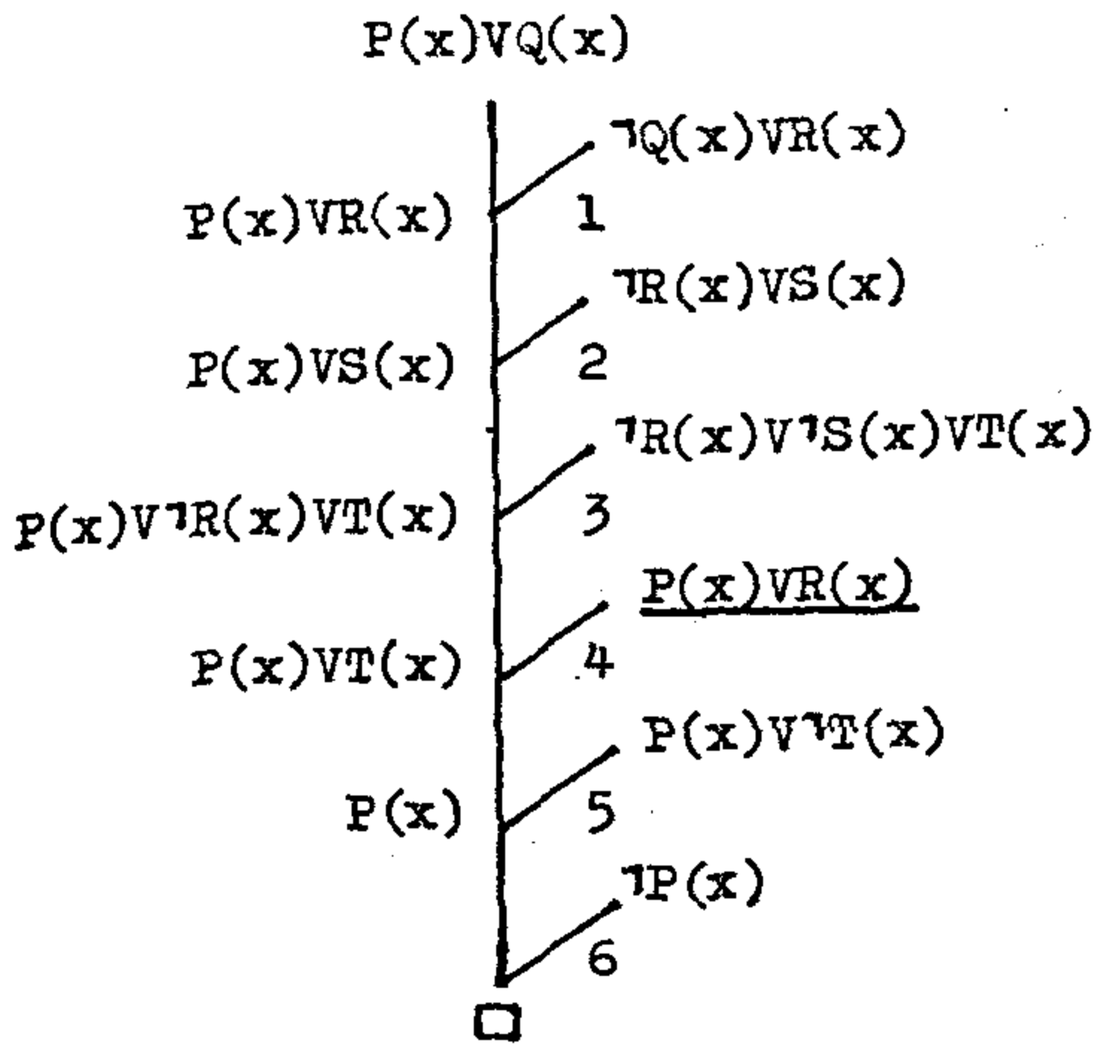
(1) $B \in S$ , ili

(2) B je $D_j$ za neko j , $1 < j < i$ .

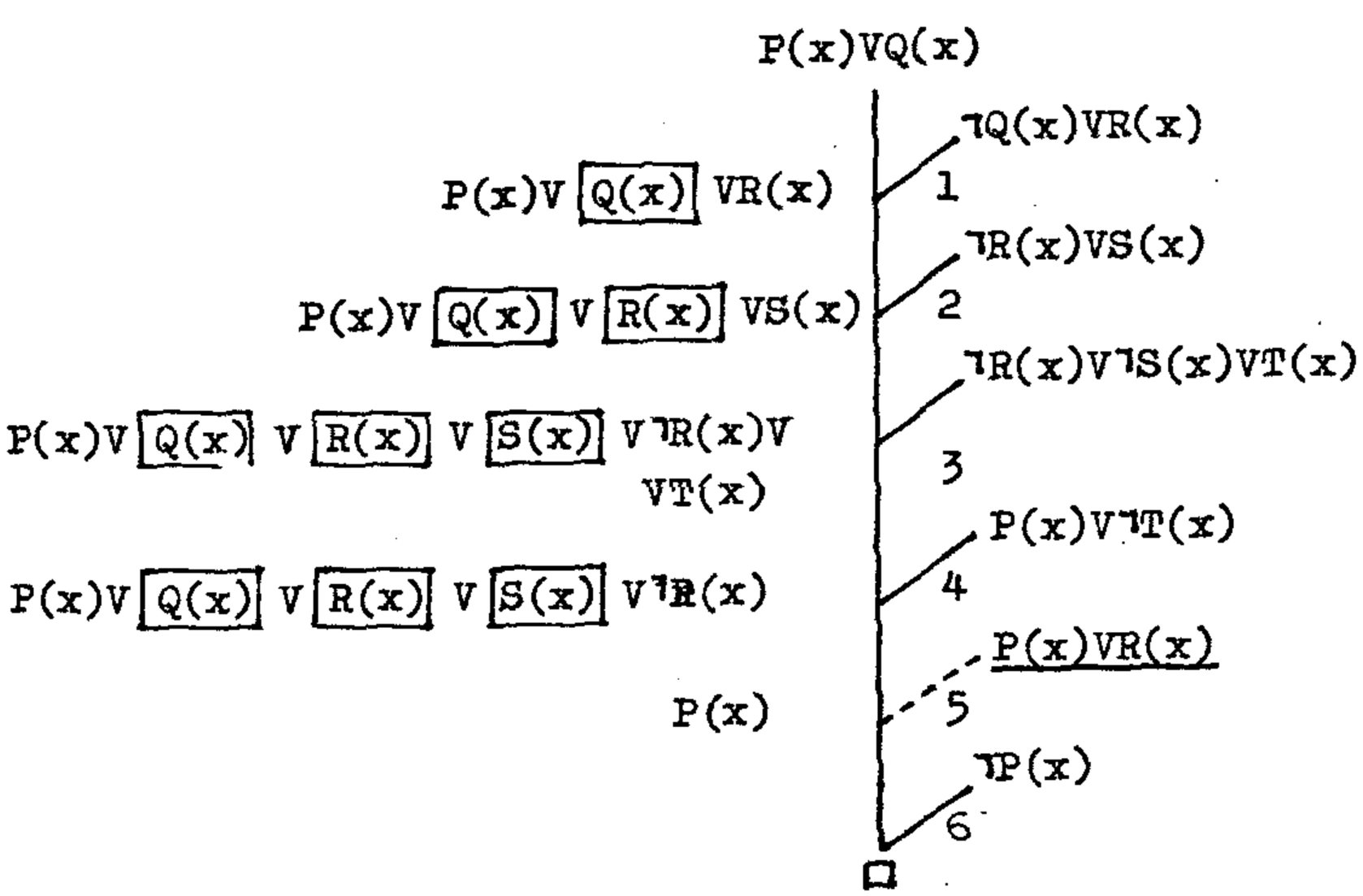
Primer ([158], str.202.)

Za skup $S = \{\neg P(x), P(x) \vee Q(x), \neg Q(x) \vee R(x), \neg R(x) \vee S(x), \neg R(x) \vee \neg S(x) \vee T(x), P(x) \vee \neg T(x)\}$

graf pobijanja koji zadovoljava uslove linearnog izvodjenja prikazan je slikom 1a.
Rezolvente 1,2,3,5,6 (6 je prazan sastavak) odredjene su ulaznom rezolucijom, a rezolventa 4 rezolucijom prethodnika, tj. iz 3 i 1 .




Slika 1a




Slika 1b

Važi sledeći stav potpunosti linearnog izvodjenja (Lokhem,197o, prema [158],str.204.):

> Neka je $D_1 \in S$ sastavak koji figuriše u nekom grafu pobijanja za skup S. Tada postoji graf pobijanja za skup S koji zadovoljava uslove linearnog izvodjenja sa početnim sastavkom $D_1$ .

Sledi, početni sastavak se bira iz $K \subseteq S$ , gde K sadrži sastavke koji se pojavljuju u nekom pobijanju za S. Za K se može uzeti skup sastavaka koji potiču iz negacije teoreme koja se dokazuje.

4.1.5. b) OL - rezolucija ( [158], str.205.)

Povećanje efikasnosti linearne rezolucije, bez narušavanja potpunosti, postiže se uvodjenjem uredjenih sastavaka i informacije o rezolviranim literalima ( [89] , [101] ) .

Informacija o rezolviranim literalima čuva se tako što se prilikom rezolucije ne odbacuju komplementarni literali, već se u rezolventi zadržava literal koji pripada prvom sastavku. Taj literal se na neki način markira. Ovde smo markiranje izvršili stavljanjem literala u okvir (slika 1b ). Markirani literali zovu se A-literali , a svi ostali literali zovu se B-literali.

Operacija sažimanja uredjenog sastavka D je brisanje poslednjeg literala L iz D akko za L i negaciju nekog A-literala iz D postoji NOU $\Theta$ .

Značaj operacije sažimanja je u tome što se eliminiše potreba za rezolucijom prethodnika, pa u izvodjenju ne treba memorisati prethodne rezolvente. To je veoma značajno za realizaciju na računaru.

Operacija skraćivanja uredjenog sastavka D je brisanje svih A-literala iz D iza kojih nema B-literala.

<u>OL - izvodjenje</u> je linearno izvodjenje sastavka $D_n$ iz skupa uredjenih sastavaka S sa početnim sastavkom $D_1 \in S$ akko su zadovoljeni sledeći uslovi:

(1) $D_{i+1}$ , za i=1,...,n-1 je uredjena rezolventa sastavka $D_i$ i sastavka $B_i$ , pri čemu je rezolvirani literal iz $D_i$ ili iz uredjenog faktora od $D_i$ , poslednji literal u $D_i$

(2) $B_i$ je sastavak $D_j$ za neko j , $1 \leq j < i$, ili je $B_i \in S$. Kad je $B_i$ sastavak $D_j$, $j < i$, onda se $D_{i+1}$ dobija iz $D_i$ operacijom sažimanja (bez rezolucije sa $B_i$).

(3) U izvodjenju nema tautologija.

Uredjena rezolventa se za slučaj OL-izvodjenja definiše na isti način kao i uredjena rezolventa uredjenih sastavaka za slučaj uredjene rezolucije (videti str. 45. ), ali se pojam uredjenog faktora i pojam uredjene binarne rezolvente, koji učestvuju u toj definiciji, sada odredjuju na sledeći način:
Uredjeni faktor sastavka D za slučaj OL-rezolucije odredjuje se kao uredjeni faktor sastavka D za uredjenu rezoluciju (videti str. 45.) uz dopunu da se pri obrazovanju uredjenog faktora primenjuje operacija skraćivanja.

<u>Uredjena binarna rezolventa</u> sastavka $D_1$ i sastavka $D_2$, koji ne sadrže zajedničke promenljive, odredjuje se za OL-izvodjenje na sledeći način:

Neka su $L_1$ i $L_2$ literali u uredjenim sastavcima $D_1$ i $D_2$, respektivno. Ako za $L_1$ i $\neg L_2$ postoji NOU $\theta$ i D je uredjen sastavak dobijen iz konkatenacije nizova $D_1\theta$ i $D_2\theta$ putem

1) isključivanja $L_2\theta$ ,
2) markiranja $L_1\theta$ ,
3) isključivanja iz preostalog niza svakog B-literala koji je identičan mladjem B-literalu u nizu ,
4) primene operacije skraćivanja ,

onda je D uredjena binarna rezolventa za $D_1$ i $D_2$ .

Na slici 1b prikazan je graf OL-izvodjenja za razmatrani primer.

OL - rezolucija je potpuna u sledećem smislu (Loveland 1972, Kovaljski,Kjuner 1971; prema [158],str 207.):

Ako je D uredjen sastavak u nezadovoljivom skupu S uredje-
ih sastavaka i ako je $S \setminus \{D\}$ zadovoljiv skup, onda postoji
L-izvodjenje praznog sastavka iz S sa početnim sastavkom D .

U tački 4.3. navodimo blok shemu algoritma pobijanja za
L - rezoluciju.

.2. Strategije pretraživanja (skice osnovnih ideja)

Procedura dokazivanja može se razmatrati kao par $(T,\Sigma)$
de je T polazni skup sastavaka i pravila izvodjenja, a $\Sigma$
trategija pretraživanja za T ([158], str.180.).
trategijom pretraživanja sužava se skup sastavaka i odredjuju
e oni sastavci na koje u konkretnom koraku procedure treba pri-
eniti pravilo izvodjenja. Specifičnim formama rezolucije, raz-
atranim u prethodnom odeljku, takodje se sužava izbor sastavaka
kandidata za rezoluciju, ali redosled izvršavanja rezolucije
ije u potpunosti preciziran.
obzirom da detaljno i strogo izlaganje raznih strategija, kao
oseban problem, zahteva dosta prostora, a kako to nije osnovni
ilj ovog rada, ograničićemo se grubom skicom osnovnih ideja.
zdvajamo strategije uprošćavanja i strategije zasnovane na funk
ijama ocene, koje mogu uključivati sintaksnu ili semantičku in-
ormaciju. Poseban pravac u razvoju strategija pretraživanja,ko-
i ovde ne razmatramo, je "slučajno pretraživanje" i primena re-
ultata teorije verovatnoća.

.2.1. Strategije uprošćavanja

Strategije uprošćavanja primenjuju se za sužavanje polaznog
kupa sastavaka S, kao i za eliminisanje suvišnih sastavaka ge-
erisanih u toku rada. Takve su na primer, strategije isključi-
anja tautologija, isključivanja azbučnih varijanata sastavaka,
trategija tzv. čistih literala ([170] ), strategija apsorpcije
strategija potpornog skupa. Pomenute strategije su ili ugradje
e u specifične forme rezolucije ili se sa njima mogu kombinova-
i. Na primer, sa hiperrezolucijom bez gubitka potpunosti može
e kombinovati strategija apsorpcije.

kaže se da sastavak $D_1$ apsorbuje sastavak $D_2$ , ako postoji zamena $\Theta$ , takva da je $D_1\Theta \subseteq D_2$ . U tom slučaju se sastavak $D_2$ isključuje. Medjutim,za binarnu rezoluciju (ili semantičku rezoluciju) i sve strategije zasićenja nivoa, isključivanje $D_2$ ne narušava potpunost izvodjenja samo ako se $D_2$ isključuje nakon zasićenja nivoa. Kad je reč o hiperrezoluciji, korak (*) algoritma (videti blok shemu 4.3.2. str. 55) može se dopuniti isključivanjem svakog sastavka iz skupova T ili M, koji je apsorbovan nekim drugim sastavkom iz T, odnosno M.

Eliminisanje sastavaka može se izvršiti i na osnovu semantičke informacije. Ako je poznato da je u datoj interpretaciji neki literal sastavka tačan, onda se ceo sastavak može isključiti. Ako je neki literal netačan u konkretnoj interpretaciji, onda se taj literal može isključiti iz sastavaka u koje ulazi.

Kao poseban slučaj strategije uprošćavanja može se razmatrati prekidanje procesa izvodjenja u slučaju kad se beskonačan proces generisanja rezolventi može unapred prepoznati ([170] ).

Strategije uprošćavanja doprinose sužavanju skupa sastavaka, ali ne preciziraju redosled primene pravila rezolucije na preostale sastavke - kandidate za rezoluciju. Taj problem se rešava strategijama zasnovanim na funkcijama ocene.

### 4.2.2. Strategije zasnovane na funkcijama ocene

Funkcije ocene složenost izvodjenja izražavaju realnim brojem. U terminima grafa izvodjenja funkcija ocene g je preslikavanje $G \rightarrow R$, gde je G skup čvorova grafa, a R skup realnih brojeva,(videti str. 15.).

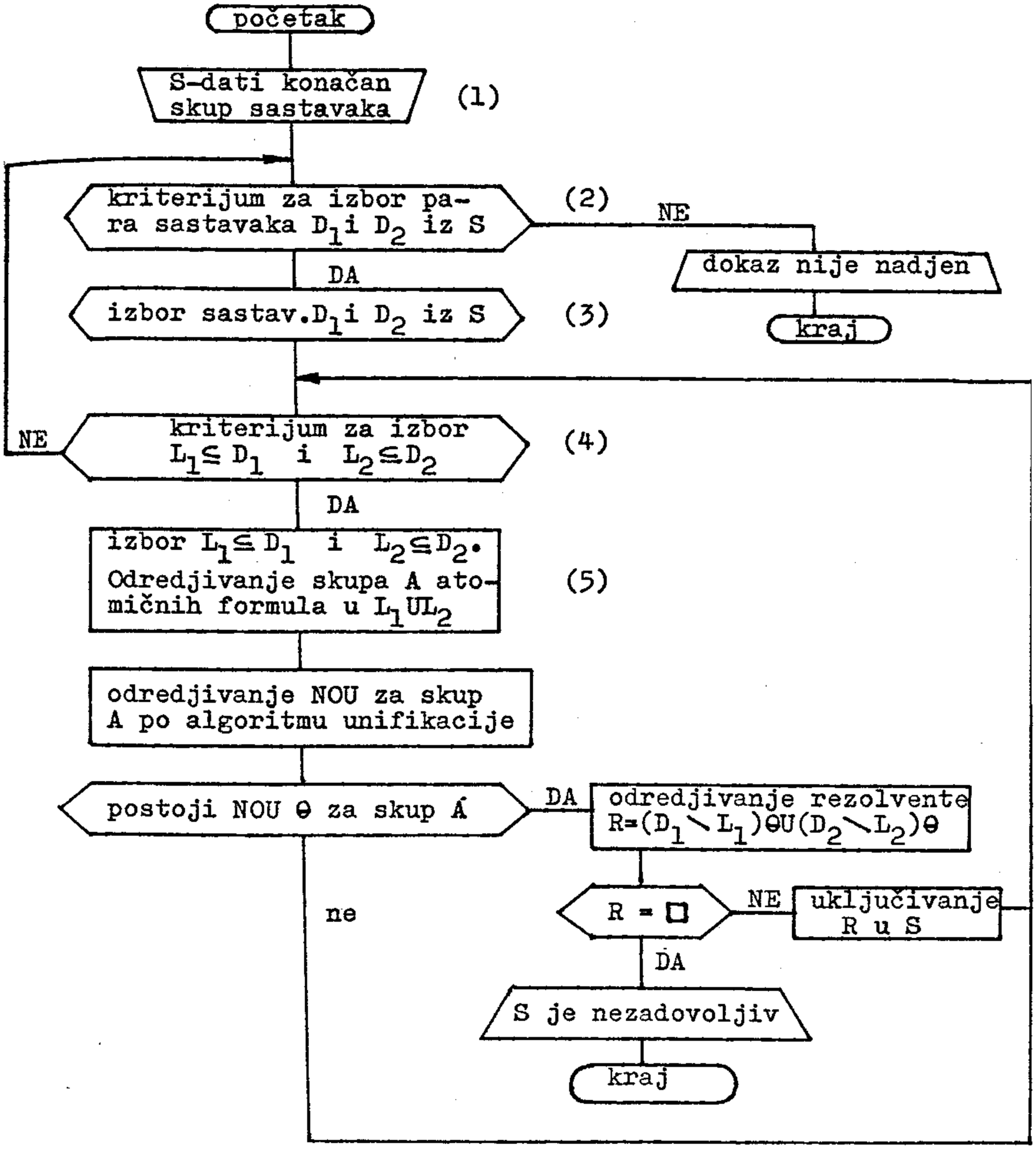
Za primenu pravila rezolucije uzimaju se oni sastavci za koje funkcija ocene ima najmanju vrednost. U praksi su najrasprostranjenije funkcije koje se odredjuju kao zbir funkcije složenosti izvodjenja i neke heurističke funkcije kojom se procenjuje složenost preostalog dela izvodjenja od datog sastavka do terminalnog sastavka. Tipičan primer strategije koja se zasniva samo na oceni složenosti i ne uzima u obzir heurističke ocene je strategija potpunog pregleda - zasićenja nivoa. U ovom slučaju složenost izvodjenja sastavka D odredjena je najmanjim brojem j, za koji važi $D \in \mathcal{R}_j(S)$ , (videti str. 13.).

Tipični primeri strategija zasnovanih na heurističkim funkcijama ocene su strategija jediničnih sastavaka (tzv. jedinična rezolucija) i strategija najmanjeg broja literala. Prema strategiji jediničnih sastavaka rezolucija se vrši na jednočlanim sastavcima, što neposredno generiše prazan sastavak. Kad to nije moguće vrše se rezolucije jednočlanih sa dvočlanim sastavcima itd. Ova strategija opravdava se skraćivanjem sastavaka, s obzirom da je cilj izvodjenje praznog sastavka. Da bi se izbeglo generisanje niza sastavaka koji se ne završava praznim sastavkom uvodi se granični nivo - dubina pretraživanja. Strategija pretraživanja u dubinu omogućuje izvodjenje praznog sastavka ako se on nalazi u okviru izabranog graničnog nivoa.
Strategija najmanjeg broja literala daje prednost onom paru sastavaka koji imaju najkraću rezolventu. Dužina rezolvente izračunava se po formuli: $d(R) \leqslant d(A)+d(B)-2$ , gde su A i B sastavci d(R) broj literala u rezolventi R.

Dijagonalna strategija (Kovaljski,1969) zasnovana je na funkciji ocene: $f(D)=g(D)+h(D)$ , gde je g(D) - nivo sastavka D u grafu izvodjenja, a h(D) - dužina sastavka (detaljnije videti u [158], str.221.). Ova funkcija ocene se uopštava (Minker i dr. 1974, Čeng Li 1973) i razmatra se kao linearna kombinacija funkcija, na primer: $f(D)=w_0g(D)+w_1h_1(D)+w_2h_2(D)$ , gde su $w_i$ koeficijenti, $\sum_i w_i = 1$ , g(D) nivo sastavka D, $h_1(D)$ dužina sastavka D , $h_2(D)$ najveći nivo složenosti terma u sastavku D. Medjutim, pri izboru funkcije ocene treba imati u vidu da u praktičnoj realizaciji, njeno izračunavanje može zahtevati više vremena i memorijskog prostora nego primena neke primitivnije strategije. Ovo ograničenje ističe u prvi plan strategiju potpornog skupa i strategiju jediničnih [illegible] sastavaka. Osim toga, stvaranjem mogućnosti za intervenciju spolja u procesu dokaza istraživač može da u zavisnosti od situacije menja strategiju i na osnovu sintaksne i semantičke informacije usmerava dalji tok izvodjenja.

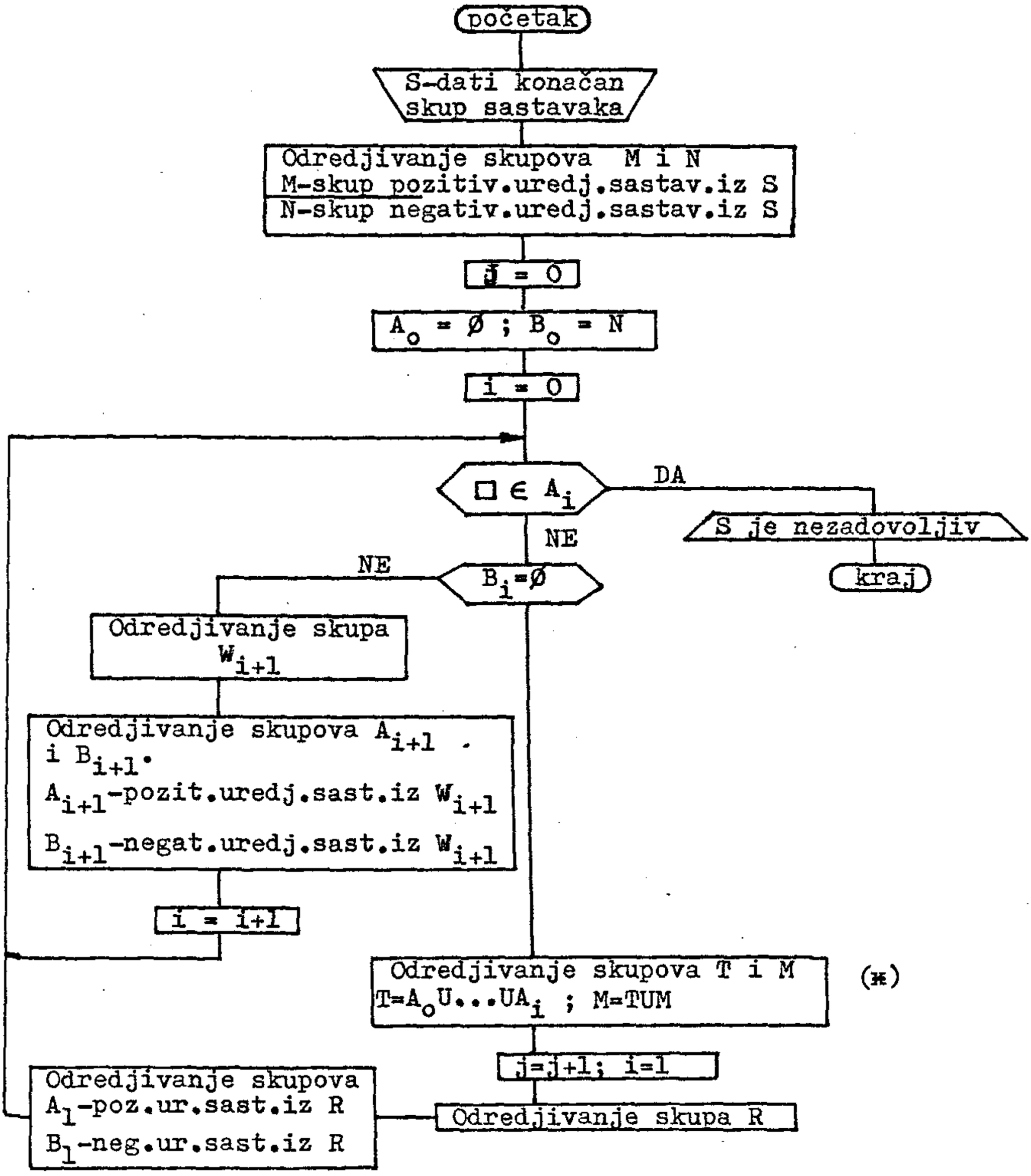
## 4.3. Blok sheme algoritama pobijanja zasnovanih na raznim formama rezolucije

### 4.3.1. Opšta blok shema algoritma pobijanja zasnovanog na b i n a r n o j rezoluciji



Komentar: (2),(3),(4),(5) zavise od ograničenja primene pravila rezolucije i od izabrane strategije generisanja sastavaka. Kriterijum (2) uključuje i odluku o prekidu rada kad je iscrpljeno predvidjeno vreme ili memorijski prostor kao i druge uslove za prekid rada u slučaju da dokaz nije nadjen.

4.3.2. Blok shema algoritma pobijanja za hiperrezoluciju

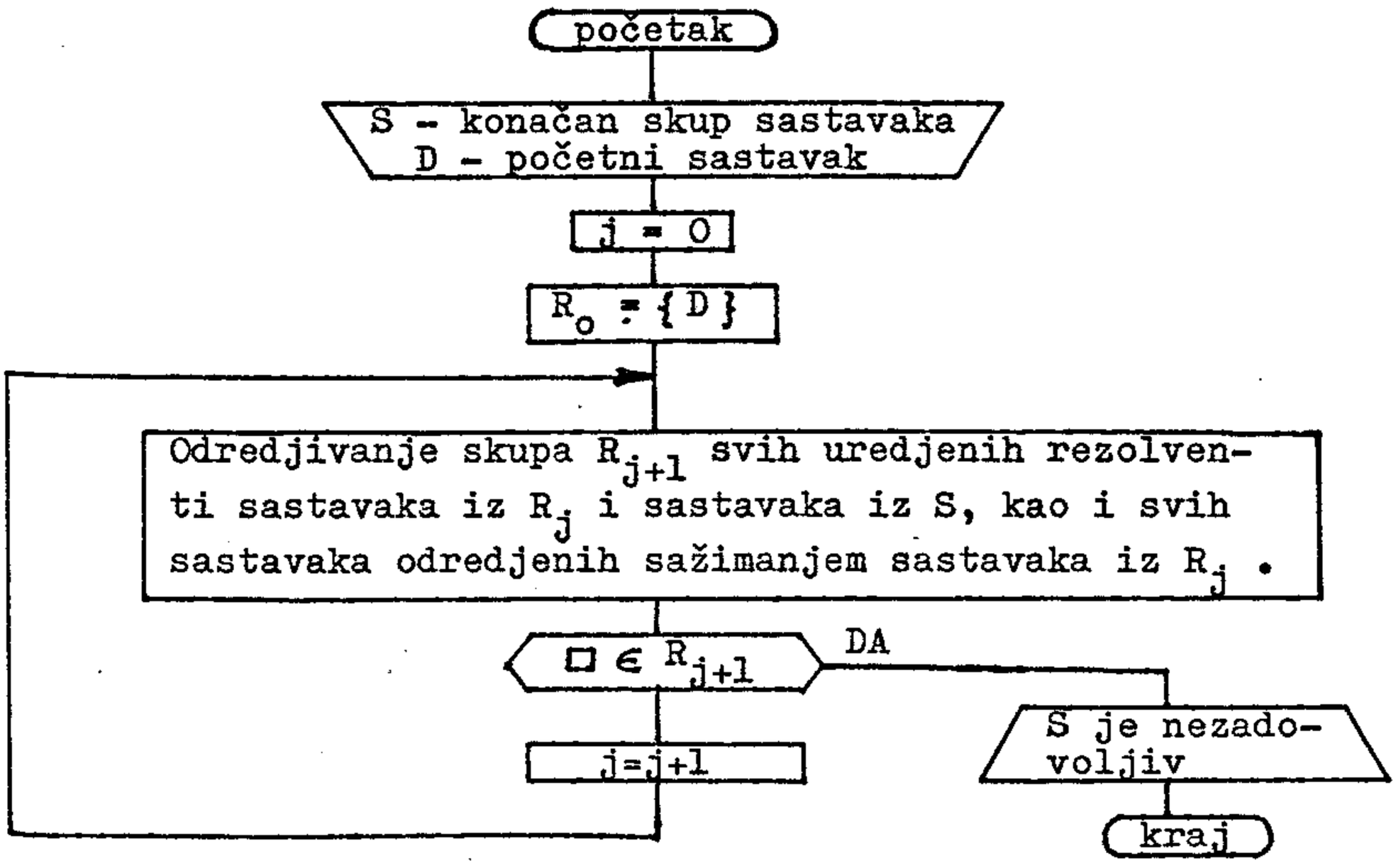


Komentar: j - brojač nivoa; $A_i$ sadrži hiperrezolvente generisane na nivou j; i - broj satelita koji učestvuju u formiranju hiperrezolvente. Na svakom nivou j, $B_i$ se smanjuje do praznog skupa, jer se maksimalan broj literala sa negacijom u ma kojem uredjenom sastavku u $B_i$ smanjuje za 1 pri povećanju i za 1 . Korak (*) je uveden da bi se na nivou (j+1) izbeglo generisanje rezolvente dobijene na nivou j.

$W_{i+1}$ je skup uredjenih rezolventi sastavaka $D_1$ i $D_2$ , gde je $D_1$ uredjeni sastavak iz M ili je uredjeni faktor uredjenog sastavka iz M, $D_2$ je uredjeni sastavak iz $B_i$. Rezolucija se vrši po literalu u $D_1$ sa najvećim predikatskim simbolom, a u $D_2$ najstarijim literalom. R je skup uredjenih rezolventi sastavaka $D_1$ i $D_2$ , gde je $D_1$ uredjen sastavak iz skupa T ili uredjen faktor uredjenog sastavka iz T, a $D_2$ je uredjen sastavak iz skupa N . Rezolucija se vrši po literalu u $D_1$ sa najvećim predikatskim simbolom i po ma kojem literalu iz $D_2$ .

U slučaju kad je S zadovoljiv skup, ovaj algoritam ne prekida rad, pa se to mora ostvariti intervencijom spolja.

### 4.3.3. Blok shema algoritma pobijanja za uredjenu linearnu OL-rezoluciju



Komentar: j - brojač nivoa. $R_{j+1}$ je skup uredjenih rezolventi koje se obrazuju od sastavaka iz $R_j$ (centralnih sastavaka) i sastavaka iz polaznog skupa S (ulaznih - bočnih sastavaka). U slučaju kad se sastavak $D \in R_j$ može sažeti, onda se sastavak $D^*$ odredjen sažimanjem sastavka D uključuje u $R_{j+1}$ i za D se ne traže rezolvente sa sastavcima iz S.

$\square$ - prazan sastavak.

S obzirom da se skup $R_{j+1}$ odredjuje samo na osnovu skupa $R_j$ i polaznog skupa S (primenom ulazne uredjene rezolucije i operacije sažimanja), nije potrebno memorisati skupove $R_o,\ldots,R_{j-1}$.

Navedena shema zasnovana je na strategiji zasićenja nivoa za OL-rezoluciju. Ako je ulazni skup S zadovoljiv, navedeni algoritam ne prekida rad, pa se u tom slučaju zaustavljanje ostvaruje intervencijom spolja.

# G L A V A  III

## MATEMATIČKA INDUKCIJA U DOKAZIMA "REDUCTIO AD ABSURDUM"

U ovoj glavi razmatramo dokaze "reductio ad absurdum" u teorijama prvog reda koje sadrže aksiomu matematičke indukcije i neformalizovane dokaze od suprotnog zasnovane na principu "obratne indukcije". Za teorije prvog reda sa aksiomom indukcije uvode se pravila indukcije pogodna za primenu u dokazima "reductio ad absurdum". Dokazuje se potpunost uvedenih pravila. Pravilo P5 za članove disjunkcije, koje je uopštenje ostalih pravila, pogodno je za primenu u mehaničkom dikazivanju teorema.

### 1. PRAVILA INDUKCIJE U TEORIJI PRVOG REDA

Neka teorija prvog reda sadrži sledeću shema-aksiomu indukcije:

$$A(0) \Longrightarrow (\forall x(A(x) \Longrightarrow A(Sx)) \Longrightarrow \forall xA(x)) \qquad (1)$$

gde je A(x) - proizvoljna formula u jeziku teorije, Sx - sukcesor od x, a formule A(0) i A(Sx) odredjene su iz A(x) zamenom svakog slobodnog ulaženja promenljive x termom 0, odnosno Sx , respektivno.

Neka je $A_x(t)$ - oznaka za formulu odredjenu iz A(x) zamenom svakog slobodnog ulaženja promenljive x termom t, pri čemu je term t slobodan za x u formuli A(x).

Neka promenljiva y ne ulazi u formulu A(x). Tada je formula (1) ekvivalentna formuli:

$$A_x(0) \Longrightarrow (\forall y(A_x(y) \Longrightarrow A_x(Sy)) \Longrightarrow \forall xA(x)) \qquad (2)$$

Nadalje, za sve formule smatramo da nijedna promenljiva u formulu ne ulazi i slobodno i vezano (to se uvek može postići preoznačavanjem promenljivih), kao i da različita ulaženja kvantifikatora vezuju različite promenljive.

Formula (2) ekvivalentna je formuli:

$$\forall x \exists y \, (A_x(0) \Longrightarrow (\neg A(x) \Longrightarrow (A_x(y) \wedge \neg A_x(Sy)))) \qquad (3)$$

Neka su $z_1,\ldots,z_s$ , $s \geqslant 0$, sve različite slobodne promenljive u formuli (3), tj. u formuli $A_x(0)$ . Tada je formula

$$\forall z_1 \ldots \forall z_s \forall x \exists y \, (A_x(0) \Longrightarrow (\neg A(x) \Longrightarrow (A_x(y) \wedge \neg A_x(Sy)))) \qquad (4)$$

deduktivno jednaka formuli (3), odnosno (1), pa se može uzeti za aksiomu.

Neka je $\mathcal{K}$ teorija prvog reda koja kao sopstvenu shema-aksiomu indukcije sadrži formulu (4) i čije su sve sopstvene aksiome zatvorene formule.
Neka je $\mathcal{K}^*$ teorija čije su aksiome odredjene skolemizacijom aksioma teorije $\mathcal{K}$ ,(postupak skolemizacije opisan je na str.31.)
Za $\mathcal{K}$ i $\mathcal{K}^*$ važi sledeći opšti stav, tzv."Druga $\varepsilon$-teorema" ([124] ,str.111.):

Neka je $\mathcal{T}^*$ teorija prvog reda, čije su sve sopstvene aksiome odredjene skolemizacijom sopstvenih aksioma teorije prvog reda $\mathcal{T}$ . Tada
a) ako je $\mathfrak{E}$ formula teorije $\mathcal{T}$ i $\vdash_{\mathcal{T}^*} \mathfrak{E}$ , onda $\vdash_{\mathcal{T}} \mathfrak{E}$
b) teorija $\mathcal{T}$ je neprotivrečna akko je neprotivrečna $\mathcal{T}^*$.

Teorija $\mathcal{K}^*$ je konzervativno proširenje teorije $\mathcal{K}$, jer su sve aksiome teorije $\mathcal{K}$ teoreme u $\mathcal{K}^*$.

Skolemizacijom shema-aksiome (4) dobija se sledeća shema-aksioma teorije $\mathcal{K}^*$:

$$A_x(0) \Longrightarrow (\neg A(x) \Longrightarrow (A_x(g(x,z_1,\ldots,z_s)) \wedge \neg A_x(Sg(x,z_1,\ldots,z_s)))) \qquad (4^*)$$

gde je g skolemova funkcija (s+1) argumenata i $z_1,\ldots,z_s$ sve različite promenljive u $A_x(0)$.[1)]

---

1) $A_x(g(x,z_1,\ldots,z_s))$ je $[A_x(y)]_y(g(x,z_1,\ldots,z_s))$ .

## 1.1. PRAVILA P1 i P2 . OSNOVNO PRAVILO INDUKCIJE

Iz (4*) pomoću MP (modus ponens) dobija se pravilo:

P1 $A_x(0), \neg A(x) \vdash_{\mathcal{K}^*} A_x(g(x,z_1,\ldots,z_s)) \wedge \neg A_x(Sg(x,z_1,\ldots,z_s))$

gde je g skolemova funkcija (s+1) argumenata i $z_1,\ldots,z_s$ sve različite slobodne promenljive u $A_x(0)$ .

Iz (4*) zamenom $x \rightarrow t$, term t je slobodan za x u A(x), izvodi se

$\vdash_{\mathcal{K}^*} A_x(0) \Rightarrow (\neg A_x(t) \Rightarrow (A_x(g(t,z_1,\ldots,z_s)) \wedge \neg A_x(Sg(t,z_1,\ldots,z_s))))$

i pomoću MP dobija se pravilo:

P2 $A_x(0), \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g(t,z_1,\ldots,z_s)) \wedge \neg A_x(Sg(t,z_1,\ldots,z_s))$

gde je term t slobodan za x u A(x); $z_1,\ldots,z_s$ sve različite slobodne promenljive u $A_x(0)$; g - skolemova funkcija (s+1) argumenata .

Posebno, kad je $A_x(0)$ zatvorena formula, tj. s=0 :

$$A_x(0), \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g(t)) \wedge \neg A_x(Sg(t)) \quad .$$

Pravilo P2 je uopštenje pravila P1 , jer kad je t slobodna promenljiva x , P2 postaje P1 .

Primer 1. Dokaz reductio ad absurdum pomoću P2 za teoremu $\forall x\,(x = 0 + x)$ u formalnoj abitmetici.

1. $a \neq 0 + a$ negacija i skolemiz.date formule;a-skol.konst.
2. $0 = 0 + 0$ teorema t=t+0 za 0 u svojstvu t
3. $ga = 0 + ga$ 2 i 1 po P2 za term a ;
4. $(ga)' \neq 0 + (ga)'$ Umesto Sg(a) stoji (ga)'
5. $(ga)' = (0 + ga)'$ iz 3, teorema $t=r \Rightarrow t' = r'$
6. $(ga)' = 0 + (ga)'$ iz 5, teoreme $(t+r)' = t+r'$ i $t=r \wedge r=s \Rightarrow t=s$
7. kontradikcija 4 i 6.

Primer 2. Neka su $F_x(0)$ i $\forall x(F(x)\Rightarrow F_x(Sx))$ teoreme teorije prvog reda sa indukcijom. Može se smatrati da je $F_x(0)$ zatvorena formula. Primenom pravila P2 dokazaćemo $\forall xF(x)$.

1) D i r e k t a n  d o k a z  (bez redukcije na apsurd):

| | |
|---|---|
| 1. $F_x(0)$ | date teoreme |
| 2. $\forall x(F(x)\Rightarrow F_x(Sx))$ | |
| 3. $\neg F(x)$ | hipoteza |
| 4. $F_x(g(x))\wedge\neg F_x(Sg(x))$ | 1 i 3 po P2 (ustvari P1) |
| 5. $\neg F(x)\Rightarrow(F_x(g(x))\wedge\neg F_x(Sg(x)))$ | 1,3 i 4 stav dedukcije i MP za 1 |
| 6. $(F_x(g(x))\Rightarrow F_x(Sg(x)))\Rightarrow F(x)$ | iz 5,kontrapozicija,tautologije |
| 7. $F_x(g(x))\Rightarrow F_x(Sg(x))$ | iz 2, zamena $x\rightarrow g(x)$ |
| 8. $F(x)$ | 6 i 7 po MP |
| 9. $\forall xF(x)$ | 8, pravilo GEN (generalizacija) |

2) D o k a z  r e d u c t i o  a d  a b s u r d u m

| | |
|---|---|
| 1. $F_x(0)$ | date teoreme |
| 2. $\forall x(F(x)\Rightarrow F_x(Sx))$ | |
| 3. $\neg F_x(a)$ | negacija i skolemizacija formule $\forall xF(x)$;a-skol.konst. |
| 4. $F_x(g(a))$ } | 1 i 3 po P2 |
| 5. $\neg F_x(Sg(a))$ } | |
| 6. $F_x(g(a))\Rightarrow F_x(Sg(a))$ | iz 2, zamena $x\rightarrow g(a)$ |
| 7. $F_x(Sg(a))$ | 4 i 6 po MP |
| 8.kontradikcija | 5 i 7 . |

Valjanost dokaza u primerima 1 i 2 neće se narušiti ako svuda umesto terma g(a) pišemo novu skolemovu konstantu u oznaci g. Takodje umesto skolemove funkcije jednog argumenta g(x), može se uzeti nova skolemova konstanta g. Uopšte, arnost skolemove funkcije se može smanjiti za jedinicu. To se obrazlaže na sledeći način. Formula (2) ekvivalentna je i sledećoj formuli[1)]

$$\exists y\forall x(A_x(0)\Rightarrow(\neg A(x)\Rightarrow(A_x(y)\wedge\neg A_x(Sy)))) \qquad (3')$$

---

1) U predikatskom računu važi: ako promenljiva x ne ulazi u formulu B(y) i promenljiva y ne ulazi u formulu C(x), onda
$\vdash\forall x\exists y(B(y)\Rightarrow C(x))\Leftrightarrow\exists y\forall x(B(y)\Rightarrow C(x))$ .

Zato se umesto shema-aksiome (3) za sopstvenu shema-aksiomu indukcije teorije $\mathcal{K}$ može uzeti formula

$$\forall z_1 \ldots \forall z_s \exists y \forall x (A_x(0) \Longrightarrow (\neg A(x) \Longrightarrow (A_x(y) \wedge \neg A_x(Sy)))) \qquad (4')$$

Skolemizacijom formule (4′) dobija se sledeća shema-aksioma teorije $\mathcal{K}^*$:

$$A_x(0) \Longrightarrow (\neg A(x) \Longrightarrow (A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s)))) \qquad (4'^*)$$

gde su $z_1,\ldots,z_s$ , $s \geqslant 0$, sva različite slobodne promenljive u $A_x(0)$ i g - skolemova funkcija s argumenata. Za s=0, g je skolemova konstanta.

Iz $(4'^*)$ zamenom $x \rightarrow t$ , term t je slobodan za x u A(x),izvodi se

$$\vdash_{\mathcal{K}^*} A_x(0) \Longrightarrow (\neg A_x(t) \Longrightarrow (A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s))))$$

i pomoću MP dobija se pravilo:

P2′ $A_x(0), \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s))$

gde je term t slobodan za x u A(x); $z_1,\ldots,z_s$ - sve različite slobodne promenljive u $A_x(0)$; g - skolemova funkcija s argumenata.

Za slučaj kad je $A_x(0)$ zatvorema formula,tj,s=0, pravilo glasi:

$$A_x(0), \neg A_x(t) \vdash_{\mathcal{K}^*} A_x(g) \wedge \neg A_x(Sg)$$

gde je g nova skolemova konstanta.

Pravilo P2′zovemo o s n o v n o pravilo indukcije.

Iz shema-aksiome $(4'^*)$ po MP izvodi se pravilo P1′:

$$A_x(0), \neg A(x) \vdash_{\mathcal{K}^*} A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s)).$$

Osnovno pravilo je uopštenje pravila P1′, jer kad je t slobodna promenljiva x , P2′ postaje P1′.

## 1.2. GENERALIZACIJA OSNOVNOG PRAVILA INDUKCIJE

U glavi II ,tač.3.2. navedene su opšte definicije zamene, kompozicije zamena, unifikatora i NOU za skup literala. Preciziraćemo ih za formule teorije prvog reda.

Definicija 1.

a) Skup zamenskih komponenti $\sigma = \{t_1/x_1,\ldots,t_n/x_n\}$
gde je $x_i \neq x_j$ za $i \neq j$ i nijedna od promenljivih $x_1,\ldots,x_n$ ne ulazi u terme $t_i$ , i=1,...,n , zove se zamena .

b) Primena zamene $\sigma$ na neku formulu A znači jednovremeno zamenjivanje svih slobodnih ulaženja promenljivih $x_i$ u A termima $t_i$ , i=1,...,n .

c) Formula $A\sigma$ , dobijena primenom zamene $\sigma$ na A, je $\sigma$-primer FORMULE A, u oznaci $A_\sigma$ , ako su termi $t_i$ zamene $\sigma$ slobodni za promenljive $x_i$ u formuli A, i=1,...,n .

d) Zamena $\sigma$ je unifikator za formule A i B ako se $\sigma$-primeri ovih formula poklapaju. Pišemo: $A_\sigma \equiv B_\sigma$ .

Očevidno, za formule A i A unifikator je prazna zamena. Takodje, ako u formuli A nema slobodnih promenljivih $x_i$ sadržanih u $\sigma$ , onda je $A_\sigma \equiv A$ .

STAV 1. Neka formule A i $\neg B_x(t)$ teorije $\mathcal{K}^*$ zadovoljavaju sledeće uslove:

(i) Postoji unifikator $\sigma$ za formule A i $B_x(0)$, tj. $A_\sigma \equiv (B_x(0))_\sigma$ (može se smatrati da promenljiva x ne ulazi u A, ni u $\sigma$ )

(ii) Primenom zamene $\sigma$ na formule $B_x(t)$ i $B_x(g(z_1,\ldots,z_s))$, gde je g skolemova funkcija s argumenata i $z_1,\ldots,z_s$ sve slobodne promenljive u $B_x(0)$, dobijaju se $\sigma$-primeri ovih formula, tj. $(B_x(t))_\sigma$ i $(B_x(g(z_1,\ldots,z_s)))_\sigma$ .

Tada se u teoriji $\mathcal{K}^*$ izvodi formula:

$$(B_x(g(z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(z_1,\ldots,z_s)))_\sigma \quad .$$

Dokaz. Saglasno sa definicijom 1, $\sigma$-primeri formula A, $B_x(t)$ i $B_x(g(z_1,\ldots,z_s))$ mogu se izvesti u teoriji $\mathcal{K}^*$. Zapisom $\neg B_x(t)$ obezbedjeno je da je term t slobodan za x u B(x). Zato u teoriji $\mathcal{K}^*$ postoji sledeće izvodjenje:

1. A
2. $\neg B_x(t)$
3. $(\neg B_x(t))_\sigma$ — $\sigma$-primer formule 2 (uslov (ii))
4. $(B_x(0))_\sigma$ — $\sigma$-primer formule 1 (uslov (i) )
5. $B_x(0) \Rightarrow (\neg B(x) \Rightarrow (B_x(g(z_1,\ldots,z_s)) \wedge \neg B_x(Sg(z_1,\ldots,z_s))))$
   aksioma $(4'^{*})$ za B(x); $z_1,..,z_s$ sve slobodne promenljive u $B_x(0)$
6. $B_x(0) \Rightarrow (\neg B_x(t) \Rightarrow (B_x(g(z_1,\ldots,z_s)) \wedge \neg B_x(Sg(z_1,\ldots,z_s))))$
   iz 5, zamena $x \to t$ , jer je t slobodan za x u $B(x)$ .
7. $(B_x(0))_\sigma \Rightarrow ((\neg B_x(t))_\sigma \Rightarrow ((B_x(g(z_1,..,z_s)))_\sigma \wedge (\neg B_x(Sg(z_1,..,z_s)))_\sigma))$
   $\sigma$-primer formule 6
8. $(B_x(g(z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(z_1,\ldots,z_s)))_\sigma$ iz 7,4 i 3 po MP .

Na osnovu stava 1 formuliše se sledeće pravilo:

P3 $A, \neg B_x(t) \vdash_{\mathcal{K}^*} (B_x(g(z_1,\ldots,z_s)))_\sigma \wedge (\neg B_x(Sg(z_1,\ldots,z_s)))_\sigma$
(pod uslovima (i) i (ii) )

U slučaju kad su A i $\neg B_x(t)$ literali, unifikator $\sigma$ se može odrediti po algoritmu unifikacije.

Primer 3. Dokaz reductio ad absurdum za teoremu formalne aritmetike $\forall x \forall y(x+y = y+x)$ , primenom pravila P3.

1. $a + b \neq b + a$ — neg.i skol.date formule;a,b -skol.konst.
2. $x + 0 = 0 + x$ — teorema
3. $a + g = g + a$ } 2 i 1 po P3 za term b i $\sigma = \{a/x\}$
4. $a + g' \neq g' + a$ } g - skolemova konstanta (s=0)
5. $(a + g)' = (g + a)'$ — 3, teorema $t=r \Rightarrow t' = r'$
6. $a + g' = (g + a)'$ — 5, teorema $(t+r)' = t+r'$ i teoreme o jednakosti
7. $g' + a = (g + a)'$ — teorema $t' + r = (t+r)'$
8. $a + g' = g' + a$ — 6 i 7, teoreme o jednakostima
9. kontradikcija — 4 i 8 .

Pravilo P3 je uopštenje osnovnog pravila (P2′), jer kad je $A \equiv B_x(0)$, onda je unifikator $\sigma$ prazna zamena, pa P3 postaje osnovno pravilo.

Primedba. S obzirom da promenljiva x ne ulazi u zamenu $\sigma$, $\sigma$-primer $(B(x))_\sigma$ je formula $B_\sigma(x)$, pa je $\sigma$-primer $(B_x(t))_\sigma$ formula $B_{\sigma x}(t\sigma)$ , Sledi, term $t\sigma$ je slobodan za x u $B_\sigma(x)$ . Sada se stav 1 može preformulisati, a pravilo P3 uprostiti, na sledeći način.

STAV 1′. Neka formule A i $\neg B_x(t)$ teorije $\mathcal{K}^*$ zadovoljavaju uslove:

(i) Postoji unifikator $\sigma$ za formule A i $B_x(0)$, tj. $A_\sigma \equiv B_{\sigma x}(0)$ (x ne ulazi u $\sigma$ ),

(ii)primenom zamene $\sigma$ na formulu $B_x(t)$ dobija se $\sigma$-primer te formule, tj. $B_{\sigma x}(t\sigma)$ .

Tada se u teoriji $\mathcal{K}^*$ izvodi formula

$$B_{\sigma x}(g(z_1,\ldots,z_s)) \wedge \neg B_{\sigma x}(Sg(z_1,\ldots,z_s))$$

gde su $z_1,\ldots,z_s$ sve slobodne promenljive u $B_{\sigma x}(0)$ i
g - skolemova funkcija s argumenata.

Dokaz. Saglasno definiciji 1, $\sigma$-primeri formula A i $B_x(t)$ mogu se izvesti u teoriji $\mathcal{K}^*$. Prema uslovu (ii) term $t\sigma$ je slobodan za x u formuli $B_\sigma(x)$. Zato u teoriji $\mathcal{K}^*$ postoji izvodjenje:

1. A
2. $\neg B_x(t)$
3. $\neg B_{\sigma x}(t\sigma)$ — $\sigma$-primer formule 2 (uslov (ii))
4. $B_{\sigma x}(0)$ — $\sigma$-primer formule 1 (uslov (i) )
5. $B_{\sigma x}(0) \Rightarrow (\neg B_\sigma(x) \Rightarrow (B_{\sigma x}(g(z_1,..,z_s)) \wedge \neg B_{\sigma x}(Sg(z_1,..,z_s))))$
   aksioma (4′*) za formulu B (x); $z_1,..,z_s$ -sve slob.prom.u $B_{\sigma x}(0)$
6. $B_{\sigma x}(0) \Rightarrow (\neg B_{\sigma x}(t\sigma) \Rightarrow (B_{\sigma x}(g(z_1,..,z_s)) \wedge \neg B_{\sigma x}(Sg(z_1,..,z_s))))$
   iz 5, zamena $x \to t\sigma$ , jer je $t\sigma$ slobodan za x u $B_\sigma(x)$
7. $B_{\sigma x}(g(z_1,\ldots,z_s)) \wedge \neg B_{\sigma x}(Sg(z_1,\ldots,z_s))$ iz 6, 4 i 3 po MP .

Na osnovu stava 1′formuliše se sledeće pravilo:

P3′ $A, \neg B_x(t) \vdash_{\mathcal{K}^*} B_{\sigma x}(g(z_1,\ldots,z_s)) \wedge \neg B_{\sigma x}(Sg(z_1,\ldots,z_s))$
(pod uslovima (i) i (ii))

Kad su A i $\neg B_x(t)$ literali unifikator $\sigma$ se može odrediti po algoritmu unifikacije.

Za razliku od pravila P3, argumenti skolemove funkcije g u pravilu P3′ su promenljive iz $B_{6x}(0)$, dok u pravilu P3 zbog primene zamene 6, argumenti skolemove funkcije mogu postati razni termi. Prednost pravila P3′ nad P3 sastoji se u manjem broju argumenata u skolemovoj funkciji.

Pravilo P3′ je uopštenje osnovnog pravila (P2′), jer kad je $A \equiv B_x(0)$, onda je unifikator 6 prazna zamena, pa P3′postaje P2′.

Pravilo P3′ se može dalje uopštiti na sledeći način.

STAV 2. Neka formule A i $\neg B$ teorije $\mathcal{K}^*$ zadovoljavaju uslov:

(i) postoji zamena 6 , takva da se na 6-primere $A_6$ i $\neg B_6$ može primeniti osnovno pravilo, tj. $A_6$ je oblika $F_x(0)$ i $\neg B_6$ je oblika $\neg F_x(t)$, term t je slobodan za x u F(x).

Tada se u teoriji $\mathcal{K}^*$ izvodi formula:

$$F_x(g(z_1,\ldots,z_s)) \wedge \neg F_x(Sg(z_1,\ldots,z_s))$$

gde su $z_1,\ldots,z_s$, $s \geqslant 0$, sve slobodne promenljive u formuli $F_x(0)$ i g - skolemova funkcija s argumenata.

Dokaz. Na osnovu definicije 1, formule $F_x(0)$ i $\neg F_x(t)$ mogu se izvesti iz formula A i $\neg B$. Zato u teoriji $\mathcal{K}^*$ postoji izvodjenje:

. A

. $\neg B$

. $F_x(0)$ — 6-primer formule 1 (uslov (i))

. $\neg F_x(t)$ — 6-primer formule 2 (uslov (i))

. $F_x(g(z_1,\ldots,z_s)) \wedge \neg F_x(Sg(z_1,\ldots,z_s))$ — 3 i 4 po P2′

gde $z_1,\ldots,z_s$ su sve slobodne promenljive u $F_x(0)$ i g je skolemova funkcija s argumenata.

Na osnovu stava 2 formuliše se sledeće pravilo:

4 $A, \neg B \vdash_{\mathcal{K}^*} F_x(g(z_1,\ldots,z_s)) \wedge \neg F_x(Sg(z_1,\ldots,z_s))$

(pod uslovom (i))

ko je $F_x(0)$ zatvorena formula, (s=o), onda pravilo glasi:

$A, \neg B \vdash_{\mathcal{K}^*} F_x(g) \wedge \neg F_x(Sg)$ , gde je g nova skol.konst.

(pod uslovom (i))

Pravilo P4 je uopštenje osnovnog pravila, jer kad su A i $\neg B$ oblika $F_x(O)$ i $\neg F_x(t)$, zamena $\sigma$ je prazna, pa se P4 svodi na P2′. Pravilo P4 je uopštenje i pravila P3′ , jer kad je $\neg B$ formula oblika $\neg B_x(t_1)$ i formule $F_x(O)$, $\neg F_x(t)$ oblika $B_{\sigma x}(O)$, $\neg B_{\sigma x}(t_1\sigma)$ respektivno, onda je $\sigma$ unifikator za A i $B_x(O)$, pa se P4 svodi na P3′.

Specifičnost pravila P4 ilustrujemo na primeru formula na koje se može primeniti pravilo P4, ali se P3′ne može primeniti.

Primer 4. Neka je A: $P(O,h(x),x)$

$\neg B$: $\neg P(f(y,z),w,f(O,w))$

gde je P - predikatski simbol dužine tri; h,f - funkcijski simboli dužine jedan, odnosno dva; x,y,z,w - promenljive.

Uzmemo li u svojstvu terma t term w ili term f(O,w) iz $\neg B$, onda za A i $B_x(O)$ ne postoji unifikator, jer se O iz A ne unificira sa f(y,z) iz B .

Uzmemo li u svojstvu t preostali term f(y,z), onda je $B_x(O)$ formula: $P(O,w,f(O,w))$ , koja se ne može unificirati sa A iz sledećih razloga: skup neslaganja za A i $B_x(O)$ je $B_o = \{w,h(x)\}$ (o skupu neslaganja videti na str.38). Za skup $B_o$ algoritam unifikacije (videti str. 39.) generiše zamenu $\sigma_o = \{h(x)/w\}$ . Za $A\sigma_o$ : $P(O,h(x),x)$ i $(B_x(O))\sigma_o$ : $P(O,h(x),f(O,h(x)))$ skup neslaganja je $B_1 = \{x,f(O,h(x))\}$ . Kako promenljiva x ulazi u term f(O,h(x)) skup $B_1$ se ne može unificirati. Sledi, za A i $B_x(O)$ ne postoji unifikator $\sigma$ . Zato se na formule A i $\neg B$ ne može primeniti pravilo P3′.

Medjutim, ako na A i $\neg B$ primenimo sledeću zamenu

$$\sigma = \{O/y,h(O)/w,O/x,h(O)/z\}$$

dobijamo $\sigma$ -primere

$A_\sigma$: $P(\ O\ ,\ h(O)\ ,\ O\ )$

$\neg B_\sigma$: $\neg P(f(O,h(O)),\ h(O)\ ,\ f(O,h(O)))$

Ako sa F(x) označimo formulu $P(x,h(O),x)$ , onda se formule $A_\sigma$ i $\neg B_\sigma$ mogu označiti $F_x(O)$ i $\neg F_x(f(O,h(O)))$, respektivno. Zato se na A i $\neg B$ može primeniti pravilo P4 , što daje formulu:

$P(g,h(O),g) \wedge \neg P(Sg,h(O),Sg)$ , g je nova skol.konst.

U slučaju kad su A i ¬B literali zamena $\sigma$ se može odrediti po posebnom algoritmu koji je uopštenje algoritma unifikacije, (videti, u daljem tekstu, algoritam za odredjivanje zamene, str.87.).

## 1.3. PRAVILO INDUKCIJE ZA ČLANOVE DISJUNKCIJE

STAV 3.

Neka su $D_1$: A V $C_1$ i $D_2$: ¬B V $C_2$ formule teorije $\mathcal{K}^*$ koje zadovoljavaju sledeći uslov:

(i) postoji zamena $\sigma$ takva da se njenom primenom na $D_1$ i $D_2$ dobijaju $\sigma$-primeri oblika $D_{1\sigma}$: $F_x(0)$ V $C_{1\sigma}$ i $D_{2\sigma}$: ¬$F_x(t)$ V $C_{2\sigma}$ ,(term t je slobodan za x u F(x)).

Tada se u teoriji $\mathcal{K}^*$ izvode formule:

$F_x(g(z_1,\ldots,z_s))$ V $C_{1\sigma}$V $C_{2\sigma}$ i ¬$F_x(Sg(z_1,\ldots,z_s))$ V $C_{1\sigma}$V $C_{2\sigma}$ ,

gde su $z_1,\ldots,z_s$, $s \geq 0$, sve slobodne promenljive u formuli $F_x(0)$, a g skolemova funkcija s argumenata.

Dokaz. Na osnovu definicije zamene $\sigma$ i $\sigma$-primera (def. 1.), $\sigma$-primeri formula $D_1$ i $D_2$ mogu se izvesti u teoriji $\mathcal{K}^*$. Zato i teoriji $\mathcal{K}^*$ postoji sledeće izvodjenje:

1. $\neg C_1 \Rightarrow A$ formula $D_1$ zapisana pomoću implikacije
2. $\neg C_2 \Rightarrow \neg B$ formula $D_2$ zapisana pomoću implikacije
3. $\neg C_1 \wedge \neg C_2 \Rightarrow A \wedge \neg B$ 1 i 2, tautologija
4. $\neg C_{1\sigma} \wedge \neg C_{2\sigma} \Rightarrow F_x(0) \wedge \neg F_x(t)$ $\sigma$-primer formule 3 (uslov (i))
5. $F_x(0) \wedge \neg F_x(t) \Rightarrow F_x(g(z_1,\ldots,z_s)) \wedge \neg F_x(Sg(z_1,\ldots,z_s))$
   teorema iz koje je izvedeno osnovno pravilo P2′; $z_1,\ldots,z_s$ su sve slobodne promenljive u $F_x(0)$; g - skolemova funkcija s argumenata.
6. $\neg C_{1\sigma} \wedge \neg C_{2\sigma} \Rightarrow F_x(g(z_1,\ldots,z_s)) \wedge \neg F_x(Sg(z_1,\ldots,z_s))$
   4 i 5 tranzitivnost implikacije
7. $F_x(g(z_1,\ldots,z_s))$ V $C_{1\sigma}$V $C_{2\sigma}$ iz 6, tautologije
8. ¬$F_x(Sg(z_1,\ldots,z_s))$ V $C_{1\sigma}$V $C_{2\sigma}$

Na osnovu stava 3 formuliše se sledeće pravilo:

P5 $AVC_1, \neg BVC_2 \vdash_{\mathcal{K}^*} F_x(g(z_1,..,z_s))VC_{16}VC_{26}, \neg F_x(Sg(z_1,..,z_s))VC_{16}VC_{26}$
(pod uslovom (i))

Posebno, kad $A_6$ (tj. $F_x(0)$) ne sadrži slobodne promenljive, s=o, pravilo glasi:

$$AVC_1, \neg BVC_2 \vdash_{\mathcal{K}^*} F_x(g)VC_{16}VC_{26} \quad , \quad \neg F_x(Sg)VC_{16}VC_{26}$$

(pod uslovom (i))

gde je g nova skolemova konstanta.

Pravilo P5 je uopštenje pravila P4, jer kad u formulama $D_1$ i $D_2$ ne postoje članovi $C_1$ i $C_2$, onda se P5 svodi na P4. Kako je P4 uopštenje pravila P2, sledi P5 je uopštenje osnovnog pravila P2'.

## 1.4. PRIMERI DOKAZA REDUCTIO AD ABSURDUM PRIMENOM PRAVILA P5

Primer 5. Dokaz teoreme $\forall x \forall y(x + y = y + x)$ u formalnoj aritmetici. Dokaz se oslanja samo na teoreme koje se dokazuju bez indukcije.

| | | |
|---|---|---|
| 1. | $a+b \neq b+a$ | negacija date formule; a,b - skol. konst. |
| 2. | $z \neq y \vee z+0=y$ | teorema (dokazuje se bez indukcije) |
| 3. | $a \neq 0+a \vee a+g=g+a$ | iz 2 i 1 po P5 za term b |
| 4. | $a \neq 0+a \vee a+g' \neq g'+a$ | $\sigma = \{a/z, (0+a)/y\}$ ; $C_1$: $z \neq y$ ; $C_2$ ne postoji |
| 5. | $0=0+0$ | teorema (dokazuje se bez indukcije) |
| 6. | $h=0+h \vee a+g=g+a$ | iz 5 i 3 po P5 za term a; $\sigma = \emptyset$ ; |
| 7. | $h' \neq 0+h' \vee a+g=g+a$ | h - nova skolemova konstanta |
| 8. | $h'=(0+h)' \vee a+g=g+a$ | iz 6, teorema $t=r \Rightarrow t'=r'$ |
| 9. | $h'=0+h' \vee a+g=g+a$ | iz 8, teorema $(t+r)'=t+r'$ |
| 10. | $a+g=g+a$ | iz 7 i 9, tautologija $(p \vee q) \wedge (\neg p \vee q) \Rightarrow q$ |
| 11. | $a+g' \neq g'+a$ | koraci 6-9 za 4 umesto 3 u koraku 6 |
| 12. | $a+g'=g+a'$ | iz 10, teoreme korišćene u koracima 8 i 9 |
| 13. | $x+0'=x'+0$ | teorema (dokazuje se bez indukcije) |
| 14. | $g+a' \neq g'+a$ | iz 12 i 11, teorema $(t=r \wedge t \neq s) \Rightarrow r \neq s$ |
| 15. | $g+w'=g'+w$ | iz 13 i 14 po P5 za term a |
| 16. | $g+w'' \neq g'+w'$ | $\sigma = \{g/x\}$ ; w - nova skolemova konstanta |
| 17. | $g+w''=g'+w'$ | iz 15, teoreme korišćene pod 8 i 9 |

Primer 6. Dokaz teoreme $\forall x\forall y(x'+ y = (x+y)')$ u formalnoj aritm.

| | |
|---|---|
| 1. $a'+b \neq (a+b)'$ | negacija date formule; a,b -skol.konstante |
| 2. $x+0 = x$ | aksioma |
| 3. $x'+0=x'$ | teorema t+0=t za term x' |
| 4. $(x+0)'=x'$ | iz 2, teorema $t=r \Rightarrow t'= r'$ |
| 5. $x'+0=(x+0)'$ | iz 3 i 4, teorema $t=r \wedge s=r \Rightarrow t=s$ |
| 6. $a'+g=(a+g)'$ | 5 i 1 po P5 za term b; $\sigma = \{a/x\}$ |
| 7. $a'+g' \neq (a+g')'$ | g - nova skolemova konstanta |
| 8. $(a'+g)'=(a+g)''$ | iz 6, teorema $t=r \Rightarrow t'= r'$ |
| 9. $a'+g'=(a+g')'$ | iz 8, teoreme $(t+r)'=t+r'$ i $t=r \wedge r=s \Rightarrow t=s$, $t=r \Rightarrow r=t$ |
| 10. kontradikcija | 7 i 9 . |

Primer 7. Dokaz teoreme $\forall x\forall y\forall z((x+y)+z = x+(y+z))$ u formalnoj aritmetici.

| | |
|---|---|
| 1. $(a+b)+c \neq a+(b+c)$ | negacija date formule;a,b,c -skol.konst. |
| 2. $(x+y)+0 = x+y$ | teorema t+0=t |
| 3. $y+0 = y$ | - ii - |
| 4. $x+(y+0) = x+y$ | 3, teorema $t=r \Rightarrow s+t = s+r$ |
| 5. $(x+y)+0 = x+(y+0)$ | 2 i 4, teoreme o jednakosti |
| 6. $(a+b)+g = a+(b+g)$ | 5 i 1 po P5 za term c ; $\sigma = \{a/x, b/y\}$ |
| 7. $(a+b)+g' \neq a+(b+g')$ | g - nova skolemova konstanta |
| 8. $((a+b)+g)'=(a+(b+g))'$ | 6, teorema $t=r \Rightarrow t'= r'$ |
| 9. $(a+b)+g'= a+(b+g)'$ | 8, teorema $(t+r)'=t+r'$ i teoreme o jednakosti |
| 10. $(a+b)+g'= a+(b+g')$ | 9, - ii - |
| 11. kontradikcija | 7 i 10 . |

Primer 8. Neka su aksiome:

$x<y \Rightarrow (y<z \Rightarrow x<z)$

$x<x'$

$x \leqslant x$

$x<y \Rightarrow x \leqslant y$

$A_x(0) \Rightarrow (\forall y(A_x(y) \Rightarrow A_x(y')) \Rightarrow \forall x A(x))$.

Dokazaćemo $\forall x(0 \leqslant x)$ .

| | | |
|---|---|---|
| 1. | $\neg(0 \leqslant a)$ | negacija date formule; a skol.konst. |
| 2. | $x<y \Rightarrow (y<z \Rightarrow x<z)$ | |
| 3. | $x<x'$ | |
| 4. | $x \leqslant x$ | aksiome |
| 5. | $x<y \Rightarrow x \leqslant y$ | |
| 6. | $0 \leqslant g$ | 4 i 1 po P5 za term a; $\sigma = \{0/x\}$ |
| 7. | $\neg(0 \leqslant g')$ | g - nova skolemova konstanta |
| 8. | $\neg(x \leqslant y) \Rightarrow \neg(x<y)$ | 5, kontrapozicija |
| 9. | $\neg(0 \leqslant g') \Rightarrow \neg(0<g')$ | 8, $\theta = \{0/x, g'/y\}$ |
| 10. | $\neg(0<g')$ | 7 i 9 po MP |
| 11. | $0<g_1'$ | 3 i 10 po P5 za term g ; $\sigma = \{0/x\}$ |
| 12. | $\neg(0<g_1'')$ | $g_1$ - nova skolemova konstanta |
| 13. | $0<g_1' \Rightarrow (g_1'<z \Rightarrow 0<z)$ | 2, $\theta = \{0/x, g_1'/y\}$ |
| 14. | $g_1'<z \Rightarrow 0<z$ | 11 i 13 po MP |
| 15. | $\neg(0<z) \Rightarrow \neg(g_1'<z)$ | 14, kontrapozicija |
| 16. | $\neg(0<g_1'') \Rightarrow \neg(g_1'<g_1'')$ | 15, $\theta = \{g_1''/x\}$ |
| 17. | $\neg(g_1'<g_1'')$ | 12 i 16 po MP |
| 18. | $g_1'<g_1''$ | 3, $\theta = \{g_1'/x\}$ |
| 19. | kontradikcija | 17 i 18 . |

## 2. POTPUNOST PRAVILA INDUKCIJE

U tač. 1.2. i 1.3. dokazano je da su pravila P3,P3′, P4 i P5 uopštenja osnovnog pravila P2′ i da je osnovno pravilo P2′ uopštenje pravila P1′.

Korektnost uvedenih pravila sledi iz stavova 1,1′,2 i 3 - primenom pravila na teoreme teorije $\mathcal{K}^*$ izvode se teoreme teorije $\mathcal{K}^*$ 1).

Dokazaćemo potpunost pravila P5 u smislu izvodjenja u teoriji $\mathcal{K}^*$. Dokazi potpunosti ostalih pravila izvode se analogno.

---

1) Aksiome teorije $\mathcal{K}^*$ odredjene su skolemizacijom aksioma teorije $\mathcal{K}$ .

<u>STAV 4. (stav potpunosti)</u>

Neka je $\mathcal{A}^*$ skup sopstvenih aksioma i $\mathcal{T}^*$ skup teorema teorije prvog reda $\mathcal{K}^*$ koja sadrži formulu $(4'^{*})$ kao sopstvenu shema-aksiomu indukcije.

Ako je $\mathcal{T}_p$ skup teorema koje se izvode iz skupa aksioma $\mathcal{A}_1^* = \mathcal{A}^* \setminus \{ J \mid J \text{ je formula } (4'^{*}) \}$ kad se skup pravila izvodjenja teorije $\mathcal{K}^*$ proširi pravilom P5, onda je $\mathcal{T}_p = \mathcal{T}^*$.

<u>Dokaz.</u> Kako je P5 uopštenje pravila Pl', svaka teorema koja se izvodi primenom pravila Pl' može se izvesti primenom pravila P5. Zato je dovoljno dokazati da stav važi za pravilo Pl'.

Primenom pravila Pl' na formule $A_x(0)$ i $\neg A(x)$ izvodi se formula $A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s))$, pa se na osnovu stava dedukcije može izvesti aksioma $(4'^{*})$:

$$A_x(0) \Rightarrow (\neg A(x) \Rightarrow (A_x(g(z_1,\ldots,z_s)) \wedge \neg A_x(Sg(z_1,\ldots,z_s)))).$$

Sledi, P5 je potpuno u smislu izvodjenja u teoriji $\mathcal{K}^*$.

Valjanost dokaza reductio ad absurdum primenom P5 u teoriji $\mathcal{K}^*$ za teoreme teorije prvog reda $\mathcal{K}$, utvrdjuje sledeći

<u>STAV 5.</u>

Neka je B zatvorena formula neprotivrečne teorije prvog reda sa indukcijom $\mathcal{K}$. Neka je $\mathcal{A}$ skup sopstvenih aksioma teorije $\mathcal{K}$.

Formula B je teorema teorije $\mathcal{K}$ akko se u teoriji $\mathcal{K}^*$ iz koje je isključena aksioma indukcije $(4'^{*})$ i koja je proširena aksiomom $(\neg B)^{*}$, uz primenu pravila P5 može izvesti kontradikcija, tj.

$$\mathcal{A} \vdash_{\mathcal{K}} B \quad \text{akko} \quad \mathcal{A}_1^*, (\neg B)^{*} \vdash_{\mathcal{K}^* \text{ uz P5}} \perp$$

(formula $(\neg B)^{*}$ je skolemizirana negacija formule B).

<u>Dokaz.</u> Neka je formula B teorema teorije $\mathcal{K}$.
Kako je $\mathcal{K}$ neprotivrečna teorija, iz skupa aksioma $\mathcal{A}$ teorije $\mathcal{K}$

proširenog aksiomom $\neg B$ izvodi se kontradikcija, tj. teorija $\mathcal{K}$ proširena aksiomom $\neg B$ je protivrečna. Na osnovu Druge $\varepsilon$-teoreme (videti tač. 1.1. str. 59.) protivrečna je i teorija koja se dobija proširivanjem teorije $\mathcal{K}^*$ aksiomom $(\neg B)^*$ . Kako je pravilo P5 potpuno u smislu izvodjenja u teoriji $\mathcal{K}^*$ (potpunost je dokazana u stavu 4 nezavisno od ostalih aksioma u $\mathcal{K}^*$), sledi da se aksioma indukcije može isključiti iz proširene teorije $\mathcal{K}^*$ i uz primenu pravila P5 može se izvesti kontradikcija.

Obrnuto, neka se u teoriji $\mathcal{K}^*$, iz koje je isključena aksioma indukcije i koja je proširena aksiomom $(\neg B)^*$ , uz primenu pravila P5 može izvesti kontradikcija. Na osnovu Druge $\varepsilon$-teoreme i korektnosti pravila P5, protivrečna je i teorija $\mathcal{K}$ proširena aksiomom $\neg B$. Kako je $\mathcal{K}$ neprotivrečna, sledi formula B je teorema teorije $\mathcal{K}$.

NAPOMENA Uvedena pravila indukcije mogu se primeniti i u teorijama prvog reda koje medju sopstvenim aksiomama ne sadrže shema-aksiomu matematičke indukcije, ali koje uključuju matematičku indukciju. Takva je na primer, teorija čije su sopstvene aksiome odredjene Sistemom (A) Hilberta i Bernajsa [67], str. 322 i 330.

## 3. PRINCIP OBRATNE INDUKCIJE U NEFORMALIZOVANIM DOKAZIMA REDUCTIO AD ABSURDUM

Aksioma indukcije može se zapisati u obliku

$$A_x(0) \Rightarrow (\exists x \neg A(x) \Rightarrow \exists y(A_x(y) \wedge \neg A_x(Sy))) \qquad (2')$$

Formula (2′) do na prebrojiv skup svojstava formalizuje sledeći p r i n c i p o b r a t n e i n d u k c i j e :

> Ako prirodan broj 1 ima svojstvo P i postoji prirodan broj m koji nema svojstvo P, onda postoji prirodan broj k koji ima svojstvo P, takav da (k+1) nema svojstvo P .

Jednostavno se uveravamo u "prirodnost" ovog principa i u mogućnost njegove primene u neformalizovanim dokazima reductio ad absurdum.
Takav dokaz počinje sa: Postoji prirodan broj m takav da $\neg P(m)$, što se dobija iz pretpostavke da nije $\forall n P(n)$, n prirodan broj, tj. da tvrdjenje ne važi. Kad je dokazano P(1), iz P(1) i $\neg P(m)$ prema principu obratne indukcije izvodi se P(k) i $\neg P(k+1)$, za neki prirodan broj k , pa se iz toga izvodi komtradikcija. Princip obratne indukcije daje mogućnost da se kontradikcija izvede na osnovu P(1) i $\neg P(m)$ bez prethodnog izvodjenja $\forall n P(n)$.

Primetimo da je princip obratne indukcije varijanta principa najmanjeg broja[1]:

Ako postoji n da je Q(n), tada postoji najmanji n da je Q(n), tj. u formalnoj aritmetici:

$\vdash \exists x A(x) \Rightarrow \exists y (A_x(y) \wedge \forall z (z < y \Rightarrow \neg A_x(z)))$

Primer 9. Neka je P(n): $2+4+\ldots+2n = n(n+1)$ . Redukcijom na apsurd dokazaćemo: za svaki prirodan broj n važi P(n).

Neka tvrdjenje nije tačno. Tada postoji prirodan broj m da $\neg P(m)$. Kako je P(1) tačno, jer $2 \cdot 1 = 1 \cdot (1+1)$, prema principu obratne indukcije iz P(1) i $\neg P(m)$ sledi da postoji prirodan broj k takav da je P(k) i $\neg P(k+1)$, tj. $2+\ldots+2k = k(k+1)$ i $2+\ldots+2k+2(k+1) \neq (k+1)(k+1+1)$. Sledi, $k(k+1)+2(k+1) \neq (k+1)(k+2)$, pa $(k+1)(k+2) \neq (k+1)(k+2)$ što je kontradikcija. Dakle, dato tvrdjenje je tačno.

Primer 10. Neka je P(n): Ako je A prebrojiv skup, onda je $A^n$ prebrojiv skup, n prirodan broj.

Dokazaćemo: $\forall n P(n)$.

Pretpostavimo da tvrdjenje nije tačno. Tada postoji prirodan broj m da $\neg P(m)$ . P(1) je tačno, jer $A^1 = A$ je prebrojiv skup. Iz P(1) i $\neg P(m)$ prema principu obratne indukcije sledi da postoji prirodan broj k da je P(k) i $\neg P(k+1)$, tj. da je skup $A^k$ prebrojiv i skup $A^{k+1}$ nije prebrojiv. Kako je $A^{k+1} = A^k \times A$ , po definiciji direktnog proizvoda skup $A^k \times A$ je prebrojiv, pa je $A^{k+1}$ prebrojiv, što je kontradikcija. Time je dato tvrdjenje dokazano.

---

1) Ovo je primetio dr Žarko Mijajlović .

# G L A V A  IV

## MATEMATIČKA INDUKCIJA U MEHANIČKOM DOKAZIVANJU TEOREMA

Sadržaj ove glave posvećen je razradi metoda i pravila za mehaničko dokazivanje teorema u teorijama prvog reda koje dopuštaju primenu matematičke indukcije. Na osnovu izloženog u glavi II i rezultata glave III, uvodi se pravilo indukcije koje uz rezoluciju omogućuje mehaničko dokazivanje teorema metodom pobijanja.

### 1. O REALIZACIJI MATEMATIČKE INDUKCIJE U MEHANIČKOM DOKAZIVANJU

Na osnovu teoreme o rezoluciji (videti str. 41.) nezadovoljivost konačnog skupa sastavaka S može se utvrditi konačnom primenom pravila rezolucije. Zahtev da polazni skup sastavaka S bude konačan, predstavlja ograničenje za primenu rezolucijske procedure pobijanja na teorije sa shema-aksiomama. Za takve teorije rezolucijska procedura može se primeniti samo pod posebnim uslovima. U opštem slučaju, uvode se dopunske tehnike ili nova pravila.

### 1.1. DOVOLJNI USLOVI ZA REALIZACIJU MATEMATIČKE INDUKCIJE REZOLUCIJSKOM PROCEDUROM POBIJANJA

a) Neka je A teorema teorije prvog reda $\mathcal{K}$ sa indukcijom. Kako je svako izvodjenje teoreme A u teoriji $\mathcal{K}$ konačan niz formula teorije $\mathcal{K}$, aksioma indukcije u tom nizu pojavljuje se najviše konačan broj puta i to svaki put u vidu neke konkretne formule.
Ako su za formulu A unapred poznate sve konkretne aksiome indukcije, dovoljne za njeno izvodjenje, onda je skup sastavaka S

dobijen od konkretnih aksioma indukcije, ostalih sopstvenih aksioma teorije $\mathcal{K}$ i negacije formule A , konačan i nezadovoljiv. Prema teoremi o rezoluciji nezadovoljivost skupa S može se utvrditi konačnom rezolucijskom procedurom. S obzirom da ne poznajemo opšti postupak po kojem se na osnovu date formule A unapred mogu odrediti sve konkretne aksiome indukcije koje su dovoljne za izvodjenje formule A, navedeni uslov je zadovoljen kad je reč o mehaničkoj proveri postojećih doka za. Na taj način mogu se otkriti aksiome ili teoreme koje su suvišne, kao i nekorektnosti u postojećim dokazima.

b) Neka je $\mathcal{K}$ teorija prvog reda koja sadrži konačan broj sopstvenih aksioma i shema-aksiomu matematičke indukcije. Neka je $\mathcal{K}_1$ podteorija koja sadrži sve sopstvene aksiome teorije $\mathcal{K}$ osim aksiome indukcije.

<u>Lema 1.</u> Formula A(x) je teorema teorije $\mathcal{K}$ akko formule $A_x(0)$ i $\forall y(A_x(y) \Rightarrow A_x(Sy))$ su teoreme teorije $\mathcal{K}$ ,tj.

$$\vdash_{\mathcal{K}} A(x) \quad \text{akko} \quad \vdash_{\mathcal{K}} A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$$

<u>Dokaz.</u> Ako je $\vdash_{\mathcal{K}} A(x)$ , onda u teoriji $\mathcal{K}$ postoji izvodjenje:

| | | |
|---|---|---|
| 1. | A(x) | teorema |
| 2. | $\forall x A(x)$ | 1, GEN |
| 3. | $\forall x A(x) \Rightarrow A_x(0)$ | logička aksioma |
| 4. | $\forall x A(x) \Rightarrow A_x(y)$ | - ii - (y ne ulazi u A(x)) |
| 5. | $\forall x A(x) \Rightarrow A_x(Sy)$ | - ii - - ii - |
| 6. | $A_x(0)$ | 2 i 3 po MP |
| 7. | $A_x(y)$ | 2 i 4 po MP |
| 8. | $A_x(Sy)$ | 2 i 5 po MP |
| 9. | $A_x(y) \Rightarrow A_x(Sy)$ | 7 i 8, logička aksioma $p \Rightarrow (q \Rightarrow p)$ i MP |
| 10. | $\forall y(A_x(y) \Rightarrow A_x(Sy))$ | 9, GEN . |

Obrnuto, ako je $\vdash_{\mathcal{K}} A_x(0)$ i $\vdash_{\mathcal{K}} \forall y(A_x(y) \Rightarrow A_x(Sy))$, onda se u $\mathcal{K}$ iz aksiome indukcije pomoću MP izvodi $\forall x\, A(x)$, pa je $\vdash_{\mathcal{K}} A(x)$ .

Za bilo koju teoremu A(x) teorije $\mathcal{K}$ u odnosu na podteoriju $\mathcal{K}_1$ koja ne sadrži aksiomu indukcije, postoji tačno jedna od mogućnosti:

(1) $\vdash_{\mathcal{K}_1} A(x)$

(2) $\vdash_{\mathcal{K}_1} A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$ i A(x) nije teorema u $\mathcal{K}_1$, gde je x neka od promenljivih u formuli A

(3) $A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$ i A(x) nisu teoreme u $\mathcal{K}_1$, ni za koju promenljivu u formuli A .

Neka su $T_i$ skupovi teorema teorije $\mathcal{K}$ koje zadovoljavaju (i), i=1,2,3. Teoreme teorije $\mathcal{K}$ koje ne sadrže promenljive uključuju se ili u skup $T_1$, ili u skup $T_3$ . Tada je

$$\bigcap_{i=1}^{3} T_i = \emptyset \quad \text{i} \quad \bigcup_{i=1}^{3} T_i = T$$

gde je T skup teorema teorije $\mathcal{K}$ .

Teoreme iz $T_1$ mogu se dokazati rezolucijskom procedurom pobijanja, jer je skup sopstvenih aksioma teorije $\mathcal{K}_1$ konačan .

Za teoreme iz $T_3$ neposredna primena rezolucijske procedure ne dovodi do rezultata, s obzirom da skup sastavaka koji potiču od aksioma teorije $\mathcal{K}_1$ nije dovoljan, a skup sastavaka koji potiču od aksioma teorije $\mathcal{K}$ nije konačan.

Teoreme iz skupa $T_2$ mogu se dokazati primenom rezolucijske procedure pobijanja, jer važi sledeći stav.

<u>STAV 1.</u>

Neka je S konačan skup sastavaka odredjen iz sopstvenih aksioma neprotivrečne teorije $\mathcal{K}_1$ i negacije zatvorene formule $A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$ , gde je A(x) formula teorije $\mathcal{K}$ . Teorija $\mathcal{K}$ osim aksioma teorije $\mathcal{K}_1$ sadrži shema-aksiomu matematičke indukcije. Tada,
S je nezadovoljiv akko formula A(x) pripada skupu $T_1 \cup T_2$ .

<u>Dokaz</u>. Ako je S nezadovoljiv, onda s obzirom na neprotivrečnost teorije $\mathcal{K}_1$ sledi da je $\vdash_{\mathcal{K}_1} A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$, pa je

$A(x) \in T_1 \cup T_2$ .

Obrnuto, ako je $A(x) \in T_1 \cup T_2$ , onda je (i) $A(x) \in T_1$ ili (ii) $A(x) \in T_2$.

(i) Iz $\vdash_{\mathcal{K}_1} A(x)$ , na osnovu leme 1 sledi

$$\vdash_{\mathcal{K}_1} A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy)) ,$$

pa je s obzirom na neprotivrečnost teorije $\mathcal{K}_1$ , skup sastavaka S nezadovoljiv.

(ii) Iz $A(x) \in T_2$ , na osnovu definicije skupa $T_2$ je

$$\vdash_{\mathcal{K}_1} A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy)) ,$$

pa je skup sastavaka S nezadovoljiv.

Kako je S konačan skup, nezadovoljivost se može utvrditi konačnom rezolucijskom procedurom. Prema tome, za $A(x) \in T_1$ ili $A(x) \in T_2$ postoji konačno pobijanje zasnovano samo na rezoluciji.

U opštem slučaju, za datu formulu A(x) nije unapred izvesno da li pripada skupu $T_1 \cup T_2$ . Ako $A(x) \in T_3$ , ili nije teorema teorije $\mathcal{K}$ , rezolucijska procedura ne završava rad na praznom sastavku.

Medjutim, ponekad (na primer kad je reč o mehaničkoj proveri postojećih dokaza) moguće je polazni skup sastavaka S formirati tako da osim sastavaka koji potiču iz sopstvenih aksioma teorije $\mathcal{K}_1$ , S sadrži i sastavke koji potiču od nekih teorema teorije $\mathcal{K}$, takvih da se uključivanjem u S i sastavaka negacije zatvorene formule $A_x(0) \wedge \forall y(A_x(y) \Rightarrow A_x(Sy))$ dobije konačan nezadovoljiv skup sastavaka. Primetimo da se upravo na toj osnovi realizuju neformalizovani dokazi matematičkom indukcijom, zasnovani na dokazivanju baze indukcije P(1) i induktivnog koraka $P(k) \Rightarrow P(k+1)$, $k \in N$ . Zaista, u dokazu baze indukcije ili induktivnog koraka koriste se razne poznate teoreme, medju njima i one koje su (ranije) dokazane matematičkom indukcijom.

Primer 1. Mehanička provera dokaza teoreme $\forall x \forall y (x+y = y+x)$ primenom rezolucijske procedure pobijanja, na osnovu sledećeg polaznog skupa aksioma i teorema formalne aritmetike:

1. $x_1=x_2 \Rightarrow (x_1=x_3 \Rightarrow x_2=x_3)$ aksioma
2. $(x_1+x_2)' = x_1 + x_2'$ teorema (dokazuje se bez indukcije)
3. $x_1=x_2 \Rightarrow x_1' = x_2'$ aksioma
4. $(x_1+x_2)' = x_1'+x_2$ teorema (dokazuje se indukcijom)
5. $x_1+0 = 0+x_1$ teorema (dokazuje se indukcijom)

Neka je A(y) oznaka za formulu x+y=y+x. Tada je $A_y(0) \wedge \forall z(A_y(z) \Rightarrow A_y(z'))$ formula: $(x+0=0+x) \wedge \forall z(x+z=z+x \Rightarrow x+z' = z'+x)$ . U polazni skup uključujemo formulu:

6. $\neg \forall x((x+0=0+x) \wedge \forall z(x+z=z+x \Rightarrow x+z' = z'+x))$

Iz formula 1-6 odredjuje se sledeći skup sastavaka S:

1. $x_1 \neq x_2 \vee x_1 \neq x_3 \vee x_2 = x_3$
2. $(x_1+x_2)' = x_1 + x_2'$
3. $x_1 \neq x_2 \vee x_1' = x_2'$
4. $(x_1+x_2)' = x_1'+x_2$
5. $x_1+0 = 0+x_1$
6. $a+0 \neq 0+a \vee a+b=b+a$ iz formule 6; a,b - skol.konst.
7. $a+0 \neq 0+a \vee a+b' \neq b'+a$

Primenom binarne rezolucije iz sastavaka 1-7 izvodi se prazan sastavak:

8. $a+b=b+a$ 5,6 R (rezolucija)
9. $a+b' \neq b'+a$ 5,7 R
10. $(a+b)' = (b+a)'$ 3,8 R
11. $x_1 \neq a+b' \vee x_1 \neq b'+a$ 1,9 R
12. $(a+b)' \neq x_3 \vee (b+a)' = x_3$ 1,10 R
13. $(b+a)' \neq b'+a \vee (a+b)' \neq a+b'$ 11,12 R
14. $(a+b)' \neq a+b'$ 4,13 R
15. $\square$ (prazan sastavak) 2,14 R

## 1.2. REALIZACIJA MATEMATIČKE INDUKCIJE PO J.L.DARLINGTON-u

U radu J.L. Darlingtona [32] , uvodi se posebna tehnika f-svodjenja (f-matching technique) koja se uz rezoluciju koristi za dokazivanje teorema u teorijama sa jednakosnom supstitucijom i matematičkom indukcijom.

Tehnika f-svodjenja primenjuje se u slučaju da se u polaznom skupu sastavaka nalaze sledeći sastavci koji predstavljaju aksiomu jednakosne supstitucije (1), odnosno matematičke indukcije (2) i (3):

(1) $x \neq y \vee \neg f(x) \vee f(y)$

(2) $\neg f(0) \vee f(gx) \vee f(x)$ gde je gx skolemova funkcija,

(3) $\neg f(0) \vee \neg f(Sgx) \vee f(x)$ a Sx je sukcesor za x

Funkcija f(x) je funkcija drugog reda jednog argumenta, kojom se predikatski izraz predstavlja kao funkcija ne samo svojih slobodnih promenljivih, već kao funkcija ma koje (pravilno izgradjene) formule ili terma koje sadrži, ili kao funkcija ma koje formule ili terma koji se mogu unificirati sa (pravilno izgradjenom) formulom ili termom sadržanim u izrazu. Na taj način, funkcija f(x) je generalizacija pojma iskazne funkcije.

Demonstriračemo primenu f-tehnike prema [32].

Neka su dati sastavci:

(1) $x \neq y \vee \neg f(x) \vee f(y)$

(4) $.ez = z$

gde . posladnji predstavlja zapis leve neutralnosti u grupi. Rezolucijom (4) i prvog literala iz (1) generiše se zamena $\vartheta = \{.ez/x \ , \ z/y\}$ i izvodi se rezolventa: $\neg f(.ez) \vee f(z)$ . f-tehnika omogućuje svodjenje (4) sa drugim literalom iz (1) na sledeći način:

x iz f(x) može se unificirati redom sa: .ez , e , z , z (drugo ulaženje), pa se generišu sledeće zamene:

$\vartheta_1 = \{ .ez/x \ , \ (q=z)/f(q) \}$ $\vartheta_2 = \{ e/x \ , \ (.qz=z)/f(q) \}$

$\vartheta_3 = \{ z/x \ , \ (.eq=z)/f(q) \}$ $\vartheta_4 = \{ z/x \ , \ (.ez=q)/f(q) \}$.

Prve komponente ovih zamena odredjuju term kojim se zamenjuje argument od f , dok je druga komponenta pseudo-zamenska. Njome se odredjuje predikat kojim se zamenjuje f(q), pri čemu q markira mesto u predikatu na kojem se nalazi argument od f . Navedene zamene omogućuju generisanje sledećih rezolventi:

$\cdot ez \neq y \vee y=z$ za $\Theta_1$ ; $e \neq y \vee \cdot yz=z$ za $\Theta_2$

$z \neq y \vee \cdot ey=z$ za $\Theta_3$ ; $z \neq y \vee \cdot ez=y$ za $\Theta_4$ .

Rezolvente su "normalni" sastavci u tom smislu što ne sadrže f.

Uvodjenje sastavka (1) kao aksiome jednakosne supstitucije opravdava se u [32] mogućnošću generisanja primenom f-tehnike svojstava refleksivnost, simetričnost i tranzitivnost jednakosti u grupi.

Uvodjenje sastavaka (2) i (3) u svojstvu aksiome matematič ke indukcije opravdava se u [32] mogućnošću izvodjenja, primenom f-tehnike, jediničnog sastavka oblika f(x) iz dva sastavka oblika f(0) i $\neg f(x) \vee f(Sx)$ .

Uz primenu metode pobijanja dokaz za F(x,b) na osnovu F(0,b) i $\neg F(x,b) \vee F(Sx,b)$ u [32] ovako izgleda:

Primer 2.

1. $\neg f(0) \vee f(gx) \vee f(x)$ aksioma indukcije
2. $\neg f(0) \vee \neg f(Sgx) \vee f(x)$
3. F(0,b)
4. $\neg F(x,b) \vee F(Sx,b)$
5. $\neg F(a,b)$ negacija formule $\forall x F(x,b)$; a - skol.konst.
6. $F(gx,b) \vee F(x,b)$ 1,3 f-tehnika ; $\Theta = \{F(q,b)/f(q)\}$
7. $\neg F(Sgx,b) \vee F(x,b)$ 2,3 f-tehnika ; $\Theta = \{F(q,b)/f(q)\}$
8. F(ga,b) 5,6 R (rezolucija) ; $\Theta = \{a/x\}$
9. $\neg F(Sga,b)$ 5,7 R ; $\Theta = \{a/x\}$
10. F(Sga,b) 4,8 R ; $\Theta = \{ga/x\}$
11. kontradikcija 9,10 R

Navešćemo još jedan primer iz [32] .

Primer 3. Dokaz primenom f-tehnike za teoremu:
$(x<0) \Rightarrow (Sx = 0 \vee Sx<0)$
u Sistemu (B) Hilberta-Bernajsa ( [67], str.335).

| | | | |
|---|---|---|---|
| 1. | $\neg(x<x)$ | | aksioma u Sistemu (B) |
| 2. | $\neg(x<y) \vee \neg(y<z) \vee x<z$ | | sastavak odredjen iz aksiome $x<y \wedge y<z \Rightarrow x<z$ Sistema (B) |
| 3. | $x<Sx$ | | aksioma u Sistemu (B) |
| 4. | $\neg f(0) \vee f(gx) \vee f(x)$ | | aksioma indukcije |
| 5. | $\neg f(0) \vee \neg f(Sgx) \vee f(x)$ | | |
| 6. | $a<0$ | } | sastavci odredjeni iz negacije date formule; a - skolemova konstanta |
| 7. | $Sa \neq 0$ | } | |
| 8. | $\neg(Sa<0)$ | } | |
| 9. | $a<gx \vee a<x$ | 4,6 f-tehnika ; | $\Theta = \{(a<q)/f(q)\}$ |
| 10. | $\neg(a<Sgx) \vee a<x$ | 5,6 f-tehnika ; | - ii - |
| 11. | $a<ga$ | 1,9 R ; | $\Theta = \{a/x\}$ |
| 12. | $\neg(a<Sga)$ | 1,10 R ; | - ii - |
| 13. | $\neg(ga<z) \vee a<z$ | 2,11 R ; | $\Theta = \{a/x , ga/y\}$ |
| 14. | $a<Sga$ | 3,13 R ; | $\Theta = \{ga/x , Sga/z\}$ |
| 15. | kontradikcija | 12,14 R | |

Primetimo da sastavci 7 i 8 ne učestvuju u izvodjenju kontradikcije. Ustvari, navedeni dokaz je dokaz i za teoremu $\neg(x<0)$. U navedenom primeru f-tehnika se primenjuje samo na jedinične sastavke - literale . To važi i za sve ostale primere navedene u [32] . U slučaju kad se pojavljuje nejedinični sastavak, kao na primer, $x=y \vee x<y$ , u [32] se za primenu f-tehnike uvodi novi predikat, $x \leqslant y \overset{def}{\Longleftrightarrow} x=y \dot{\vee} x<y$ , pa se sastavci dobijeni iz takve definicije uključuju u polazni skup sastavaka.

Za testiranje nove f-tehnike, prema navodu u [32] , ona je ugradjena u COMIT program za dokazivanje teorema napisan u Institutu za instrumentalnu matematiku u Bonu, i realizovana na računaru IBM 7090 .

### 1.2.1. Nedostaci f-tehnike. Pravilo paramodulacije.

Osnovni nedostatak ovog prilaza je prisustvo aksioma (1),(2) i (3) u polaznom skupu sastavaka. One ne samo što proširuju osnovni skup i doprinose povećanju dužine dokaza, nego omogućuju generisanje i nepotrebnih sastavaka iz kojih se dalje generišu novi nepotrebni sastavci. Time se proširuje i "zamagljuje" prostor traženja dokaza, što negativno utiče na efikasnost metode.

Na primer, ( [158], str.210) neka iz P(a) i a=b treba izvesti P(b). Primenom f-tehnike dobija se sledeće izvodjenje:

1. $x \neq y \vee \neg f(x) \vee f(y)$ aksioma
2. $P(a)$
3. $a=b$
4. $a \neq y \vee P(y)$ 1,2 f-tehnika ; $\Theta = \{a/x , P(q)/f(q)\}$
5. $P(b)$ 3,4 R

Prirodnije bi bilo ne izvoditi formulu pod 4 , već pomoću posebnog pravila izvodjenja dobiti kraći dokaz za P(b) neposredno na osnovu P(a) i a=b .

Kad je reč o teorijama sa jednakošću navedeni nedostaci su otklonjeni uvodjenjem pravila paramodulacije (Robinson,Wos [174]). Pravilo paramodulacije omogućuje izvodjenje bez pozivanja na shema-aksiome jednakosti. Navodimo prema [158] str.213 , formulaciju pravila paramodulacije:

> Iz sastavaka $D_1$: $P(t) \vee C_1$ i $D_2$: $r=s \vee C_2$ , koji ne sadrže zajedničke promenljive (gde su $C_1$ i $C_2$ sastavci, r i s termi, a P(t) literal koji sadrži term t) pod uslovom da postoji NOU $\sigma$ za t i r , izvodi se tzv. binarni paramodulant sastavaka $D_1$ i $D_2$:
>
> $$P_\sigma[s\sigma] \vee C_{1\sigma} \vee C_{2\sigma}$$
>
> gde $P_\sigma[s\sigma]$ označava rezultat zamene jednog ulaženja terma $t\sigma$ u $P_\sigma$ termom $s\sigma$ .

Kao posledica rečenog, javlja se potreba i za pravilom indukcije koje bi , po analogiji sa pravilom paramodulacije, omogućilo izvodjenje bez pozivanja na shema-aksiomu indukcije. Takvo pravilo uvodimo u sledećem odeljku.

## 2. PRAVILO INDUKCIJE U MEHANIČKOM DOKAZIVANJU TEOREMA

Pravilo indukcije koje ovde uvodimo omogućuje da se sastavci koji potiču od shema-aksiome matematičke indukcije eliminišu iz polaznog skupa sastavaka. To oslobadja od rada sa proizvoljnom formulom (formulskom promenljivom) koja figuriše u aksiomi indukcije, doprinosi smanjivanju broja generisanih sastavaka i skraćivanju dokaza. U izlaganju koristimo pojmove i rezultate navedene u glavi II i glavi III ovog rada.

Na osnovu pravila P5 (glava III , str. 69.) formuliše se sledeće pravilo indukcije za mehaničko dokazivanje teorema.

P r a v i l o b i n a r n e i n d u k c i j e (pravilo P):

Iz sastavaka $P_1 \vee C_1$ i $\neg P_2 \vee C_2$ (gde su $P_1$ i $P_2$ literali, $C_1$ i $C_2$ sastavci) koji ne sadrže zajedničke promenljive i zadovoljavaju uslov:

(i) postoji zamena $\sigma$ koja daje $\sigma$-primere $P_{1\sigma}$ i $\neg P_{2\sigma}$ oblika $L_x(0)$ i $\neg L_x(t)$ ,

izvode se sastavci:

$$L_x(g(z_1,\dots,z_s)) \vee C_{1\sigma} \vee C_{2\sigma} \quad \text{i} \quad \neg L_x(Sg(z_1,\dots,z_s)) \vee C_{1\sigma} \vee C_{2\sigma}$$

gde je g - skolemova funkcija s argumenata; $z_1,\dots,z_s$ sve različite promenljive u literalu $L_x(0)$; S - sukcesor .

Pišemo:

$$P \quad P_1 \vee C_1, \neg P_2 \vee C_2 \vdash L_x(g(z_1,\dots,z_s)) \vee C_{1\sigma} \vee C_{2\sigma} \ , \neg L_x(Sg(z_1,\dots,z_s)) \vee C_{1\sigma} \vee C_{2\sigma}.$$

(pod uslovom (i))

Skolemova funkcija g koja se uvodi prilikom primene pravila P, zavisi od literala u koji se uvodi, pa se za različite literale uvode različite skolemove funkcije.

U slučaju kad $L_x(O)$ ne sadrži promenljive, g je nova skolemova konstanta, pa se po pravilu P izvode sastavci:

$$L_x(g) \vee C_{16} \vee C_{26} \quad \text{i} \quad \neg L_x(Sg) \vee C_{16} \vee C_{26}\,.$$

Osnovni problem za primenu pravila P u mehaničkom dokazivanju teorema je odredjivanje potrebne zamene $\sigma$. On se rešava tako što se za to koristi modifikovani algoritam unifikacije. Izložićemo to u tački 2.1.

Neke prednosti primene pravila P u odnosu na tehniku f-svodjenja [32], ilustruju sledeći primeri.

Primer 4. Dokaz za $\forall x F(x)$ iz $F(O)$ i $\forall x(F(x) \Rightarrow F(Sx))$ primenom rezolucije i pravila P ($F(x)$ - literal u kojem je x jedina promenljiva).

1. $F(O)$
2. $\neg F(x) \vee F(Sx)$
3. $\neg F(a)$ — negacija formule $\forall x F(x)$; a - skolemova konstanta
4. $F(g)$ } 1 i 3 po pravilu P ; g - nova skol.konst.
5. $\neg F(Sg)$ } $\sigma = \emptyset$ ; $C_1$ i $C_2$ ne postoje
6. $F(Sg)$ — 2,4 R (rezolucija)
7. $\square$ — 5,6 R

Navedeni dokaz je za četiri koraka kraći od dokaza u [32] (uporediti sa primerom 2, str. 81.). U ovom jednostavnom primeru neposredno je uočljiva samo prednost u pogledu broja korisnih sastavaka, dok je prednost u pogledu ukupnog broja generisanih sastavaka ovde skrivena, pošto nismo razmatrali strategiju generisanja sastavaka.

Primer 5. Dokaz teoreme $\forall x(O+x=x)$ u formalnoj aritmetici.

1. $x_1 \neq x_2 \vee x_1 \neq x_3 \vee x_2 = x_3$
2. $y_1 \neq y_2 \vee y_1' = y_2'$ — aksiome zapisane u obliku sastavaka
3. $z+O=O$ — (uzeli smo samo neophodne)
4. $(z_1+z_2)' = z_1+z_2'$
5. $O + a \neq a$ — negacija date formule; a - skolemova konst.
6. $O + g = g$ } 3 i 5 po pravilu P; $\sigma = \{O/z\}$; $C_1$ i $C_2$ ne
7. $O + g' \neq g'$ } postoje; g - nova skolemova konstanta
8. $(O + g)' = g'$ — 2,6 R
9. $x_1 \neq O+g' \vee x_1 \neq g'$ — 1,7 R
10. $(O + g)' \neq O + g'$ — 8,9 R

Primer 6. Kompletan dokaz primenom rezolucije i binarne indukcije za teoremu $\forall x \forall y(x+y=y+x)$ u formalnoj aritmetici (dokaz je nešto duži, jer se polazi samo od aksioma, a ne i od teorema form.arit.).

1. $x_1 \neq x_2 \vee x_1 \neq x_3 \vee x_2 = x_3$
2. $z_1 + 0 = z_1$
3. $y_1 \neq y_2 \vee y_1' = y_2'$ aksiome (samo neophodne)
4. $z_2 + z_3' = (z_2 + z_3)'$
5. $a+b \neq b+a$ negacija date formule; a,b - skol. konstante
6. $z_1 + 0 \neq x_3 \vee z_1 = x_3$ 1,2 R
7. $z_1 = z_1$ 2,6 R
8. $z_1 \neq x_2 \vee x_2 = z_1$ 7,1 R
9. $z_1 = z_1 + 0$ 8,2 R
10. $(z_2+z_3)' = z_2+z_3'$ 8,4 R
11. $z_1 \neq x_3 \vee z_1 + 0 = x_3$ 9,1 R
12. $(z_1+0)' = z_1'$ 2,3 R
13. $(z_1+0)' \neq x_3 \vee z_1' = x_3$ 12,1 R
14. $z_1' = z_1 + 0'$ 13,10 R
15. $z_1' + 0 = z_1 + 0'$ 14,11 R uz preoznačavanje $z_1$ u 11
16. $a \neq 0+a \vee a+g=g+a$ } 5,11 P ; $\sigma = \{a/z_1 , (0+a)/x_3\}$
17. $a \neq 0+a \vee a+g' \neq g'+a$ } g je nova skolemova konstanta
18. $h = 0+h \vee a+g=g+a$ } 9,16 P ; $\sigma = \{0/z_1\}$
19. $h' = 0+h' \vee a+g=g+a$ } h je nova skolemova konstanta
20. $h' = (0+h)' \vee a+g=g+a$ 19,3 R
21. $(0+h)' = h' \vee a+g=g+a$ 20,8 R
22. $(0+h)' \neq x_3 \vee h' = x_3 \vee a+g=g+a$ 21,1 R
23. $h' = 0+h' \vee a+g=g+a$ 22,10 R
24. $a+g=g+a$ 23,19 R
25. $a+g' \neq g'+a$ koraci 18–24 uzimajući 17 umesto 16 u koraku 18
26. $(a+g)' = (g+a)'$ 24,3 R
27. $(a+g)' \neq x_3 \vee (g+a)' = x_3$ 26,1 R
28. $(g+a)' = a+g'$ 27,10 R
29. $(g+a)' \neq x_3 \vee a+g = x_3$ 28,1 R
30. $a+g' = g+a'$ 29,10 R
31. $g+a' = a+g'$ 30,8 R
32. $g+a' \neq x_3 \vee a+g' = x_3$ 30,1 R

| | | |
|---|---|---|
| 33. $g+a' \neq g'+a$ | 32,25 | R |
| 34. $g'+a \neq g+a'$ | 33,8 | R |
| 35. $g'+w = g+w'$ } | 34,15 | P ; $\sigma = \{ g/z_1 \}$ |
| 36. $g'+w' \neq g+w''$ } | | w nova skolemova konstanta |
| 37. $(g'+w)'=(g+w')'$ | 35,3 | R |
| 38. $(g'+w)' \neq x_3$ V $(g+w')'=x_3$ | 37,1 | R |
| 39. $(g+w')'=g'+w'$ | 38,10 | R |
| 40. $(g+w')'=x_3$ V $g'+w'=x_3$ | 39,1 | R |
| 41. $g'+w' = g+w''$ | 40,10 | R |
| 42. □ | 41,36 | R |

## 2.1. ALGORITAM ZA ODREDJIVANJE ZAMENE

Modifikovaćemo algoritam unifikacije (videti str.39.) tako da u slučaju kad za date literale ne postoji unifikator, odredjuje zamenu $\sigma$ , potrebnu za realizaciju pravila binarne indukcije, kad takva postoji.

Blok shema algoritma za odredjivanje zamene data je na figuri 1. Kako algoritam na izlazu daje NOU za dati par literala, ako NOU postoji, a u slučaju da NOU ne postoji na izlazu se dobija zamena $\sigma$ ili odgovor o njenom nepostojanju, algoritam predstavlja generalizaciju algoritma unifikacije.
Isprekidana linija na figuri 1 navedena je samo radi komparacije sa algoritmom unifikacije (da bi se bolje uočila dopuna) i ne pripada algoritmu za odredjivanje zamene.
U navedenoj shemi je:

n - brojač neslaganja koja se ne mogu otkloniti unifikacijom.
Kad je na izlazu n=0, onda je $\sigma$ NOU. Kad je na izlazu n>0, onda je $\sigma$ zamena koja obezbedjuje primenu pravila binarne indukcije.

k - brojač svih neslaganja

e - prazna zamena

BLOK SHEMA ALGORITMA ZA ODREDJIVANJE ZAMENE

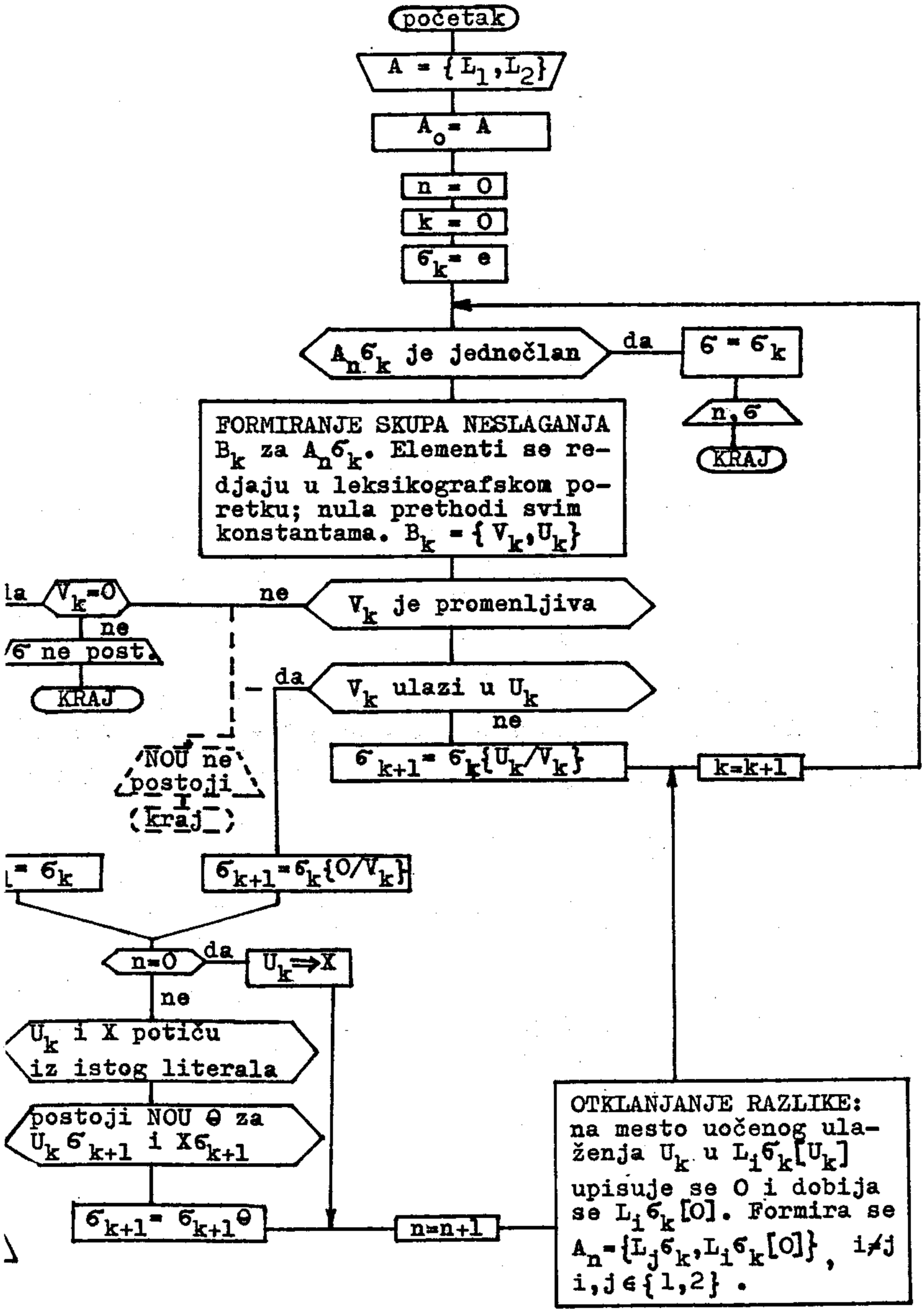



Figura 1.

$L_i\sigma_k$ - literal dobijen primenom zamene $\sigma_k$ na literal $L_i$

$A_n\sigma_k$ - skup dobijen iz skupa $A_n$ primenom $\sigma_k$ na literale iz $A_n$

$\sigma_{k+1}\theta$ - kompozicija zamena $\sigma_{k+1}$ i $\theta$

X - čuva prvi po redu term $U_k$ literala $L_i\sigma_k$ , $i\in\{1,2\}$ , koji se ne može unificirati sa odgovarajućim termom $V_k$ literala $L_j\sigma_k$ , $j\in\{1,2\}$ i $j\neq i$ . Taj term je kandidat za primenu pravila binarne indukcije.

Algoritam za odredjivanje zamene odredjuje najopštiju zamenu (NOZ) kad zamena postoji (to je posledica odgovarajućeg svojstva algoritma unifikacije) i daje informaciju o nepostojanju NOZ, kad zamena ne postoji.

Rad algoritma za odredjivanje zamene ilustruje sledeći primer.

Primer 7. Odredjivanje zamene (NOZ) $\sigma$ za skup:

$A = \{ P(0,h(x),x) , P(f(y,z),w,f(0,w))\}$

(to je skup iz primera 4 glave III , str. 67, na kojeg se pravilo P3′ ne može primeniti).

$A_0 = A$ , $B_0 = \{0,f(y,z)\}$ , pa NOU za A ne postoji.
Kako je $V_0 = 0$ i $U_0 = f(y,z)$ , biće $\sigma_1 = \sigma_0 = e$ , $X = f(y,z)$ i nakon otklanjanja uočene razlike, za n=1 biće

$$A_1 = \{P(0,h(x),x) , P(0,w,f(0,w))\}$$

Dalje, $B_1 = \{w,h(x)\}$ . Ova razlika je otklonjiva unifikacijom, pa je $\sigma_2 = \{h(x)/w\}$ i za k=2

$$A_1\sigma_2 = \{P(0,h(x),x) , P(0,h(x),f(0,h(x)))\}$$

Sada je $B_2 = \{x,f(0,h(x))\}$ , razlika nije otklonjiva unifikacijom, pa kako je $V_2 = x$ i ulazi u $U_2 = f(0,h(x))$ , biće

$$\sigma_3 = \sigma_2\{0/x\} = \{h(0)/w , 0/x\} .$$

Kako je n=1 i oba terma $U_2 = f(0,h(x))$ i $X = f(y,z)$ potiču iz drugog literala $P(f(y,z),w,f(0,w))$, traži se NOU $\theta$ za $U_2\sigma_3 = f(0,h(0))$ i $X\sigma_3 = f(y,z)$ .
Po algoritmu unifikacije odredjuje se: $\theta = \{0/y , h(0)/z\}$ , pa je nova zamena $\sigma_3$ jednaka $\sigma_3\theta = \{h(0)/w , 0/x , 0/y , h(0)/z\}$ .

Dakle, $\sigma_3 = \{h(0)/w , 0/x , 0/y , h(0)/z\}$

Za n=2, nakon otklanjanja razlike dobija se

$A_2 = \{P(0,h(x),x)\ ,\ P(0,h(x),0)\}$ i $A_2\sigma_3 = \{P(0,h(0),0),P(0,h(0),0)\} = \{P(0,h(0),0)\}$

Skup $A_2\sigma_3$ je jednočlan, pa je odredjena $\sigma = \sigma_3$ . Kako je na izlazu n=2, $\sigma$ je NOZ za skup A. Upravo ovu zamenu smo koristili u primeru 4 na str. 67 .

Zaista, primenom $\sigma$ na A dobija se $A\sigma = \{P(0,h(0),0),P(f(0,h(0)),h(0),f(0,h(0)))\}$ .

Kako je $P(0,h(0),0) = [P(X,h(0),X)]_X(0) = L_X(0)$ i

$P(f(0,h(0)),h(0),f(0,h(0))) = [P(X,h(0),X)]_X(f(0,h(0))) = L_X(t)$, za $t = f(0,h(0))$ , na sastavke

$D_1$: $P(0,h(x),x) \vee C_1$ i $D_2$: $\neg P(f(y,z),w,f(0,w)) \vee C_2$ , gde su $C_1$ i $C_2$ sastavci, može se primeniti pravilo P i izvesti:

$P(g,h(0),g) \vee C_{1\sigma} \vee C_{2\sigma}$ i $\neg P(g',h(0),g') \vee C_{1\sigma} \vee C_{2\sigma}$

gde je g nova skolemova konstanta; s=0 jer $L_x(0)$ ne sadrži promenljive.

## 2.2. UGRADJIVANJE PRAVILA BINARNE INDUKCIJE U PROCEDURE ZASNOVANE NA REZOLUCIJI

Ugradjivanje pravila binarne indukcije u rezolucijske procedure pobijanja može se ostvariti na bazi sledećeg principa:

> Pravilo binarne indukcije primenjuje se na date sastavke, samo ako se na date sastavke ne može primeniti pravilo rezolucije, a svi uslovi za primenu pravila indukcije su zadovoljeni.

Ovaj princip ne zavisi od konkretne forme rezolucije (binarna, hiperrezolucija, linearna rezolucija) ni od konkretne strategije pretraživanja, pa se može primeniti na svaku od njih.
Ilustrovaćemo to na opštoj blok shemi algoritma pobijanja zasnovanog na binarnoj rezoluciji i strategiji zasićenja nivoa.
Opšta blok shema za rezoluciju modifikuje se bez narušavanja osnovne strukture sheme uz sledeće dopune:

- dodaje se INDUKTIVNI BLOK u kojem se po pravilu P generišu novi sastavci u slučaju da za uočene literale ne postoji NOU, a postoji zamena $\sigma$ ,
- dodaje se algoritam za odredjivanje zamene $\sigma$ (Figura 1).

Opšta blok shema algoritma pobijanja sa binarnom rezolucijom i binarnom indukcijom data je Figurom 2. Isprekidana linija na Figuri 2 navedena je radi komparacije sa algoritmom koji se zasniva samo na rezoluciji, pa ne pripada algoritmu. Komentar uz Figuru 2 identičan je komentaru za rezoluciju na str. *55* , uz dopunu da u polazni skup sastavaka S ne ulaze sastavci koji potiču od shema-aksiome matematičke indukcije. Realizacija induktivnog bloka je očevidna, pa se na njenom komentarisanju ne zadržavamo. Potrebno je samo voditi računa da se pri svakoj novoj primeni pravila binarne indukcije uvodi nov simbol skolemove funkcije ili konstante, koji nije sadržan u skupu sastavaka generisanih do tog momenta. To se može postići uvodjenjem numeracije ovih simbola.

OPŠTA BLOK SHEMA ALGORITMA POBIJANJA ZASNOVANOG NA BINARNOJ REZOLUCIJI, BINARNOJ INDUKCIJI I STRATEGIJI ZASIĆENJA NIVOA

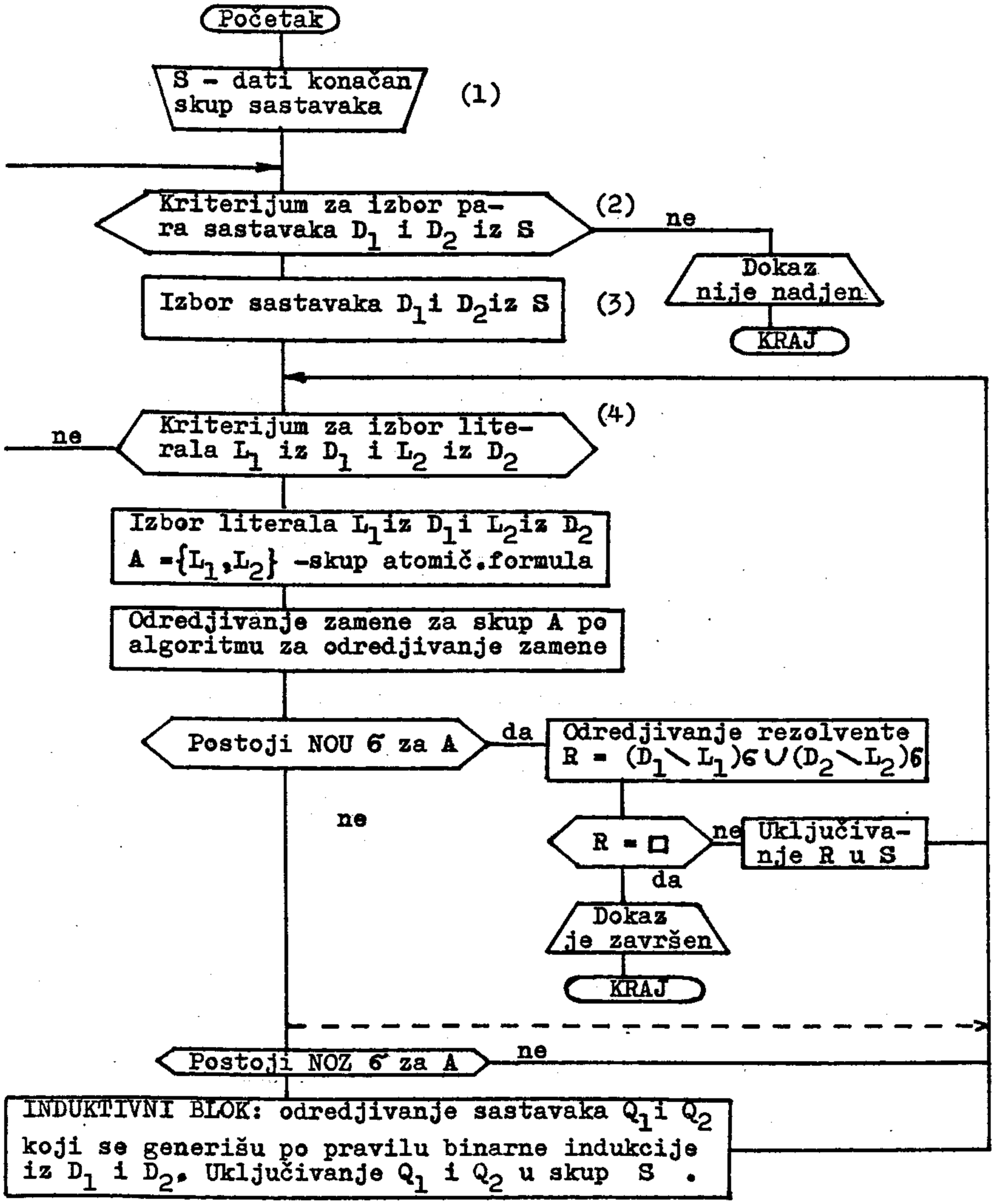



Figura 2.

## 3. O POTPUNOSTI PRAVILA BINARNE INDUKCIJE U MEHANIČKOM DOKAZIVANJU TEOREMA METODOM POBIJANJA

Neka je $\mathcal{K}$ teorija prvog reda koja sadži shema-aksiomu matematičke indukcije i neka je teorija $\mathcal{K}^*$ odredjena skolemizacijom sopstvenih aksioma teorije $\mathcal{K}$ . Teorija $\mathcal{K}^*$ sadrži sledeću shema-aksiomu indukcije (videti str. 62.):

$$A_x(0) \Rightarrow (\neg A(x) \Rightarrow (A_x(g(z_1,..,z_s)) \wedge \neg A_x(Sg(z_1,..,z_s)))) \qquad (1^*)$$

gde su $z_1,...,z_s$ sve različite slobodne promenljive u formuli $A_x(0)$; $A(x)$ je proizvoljna formula u $\mathcal{K}^*$ ; x je slobodna promenljiva u A(x); g - skolemova funkcija s argumenata; S -sukcesor. Zapisaćemo ovu aksiomu u obliku sastavaka:

$$\begin{array}{l} \neg A_x(0) \vee A_x(g(z_1,...,z_s)) \vee A(x) \\ \neg A_x(0) \vee \neg A_x(Sg(z_1,...,z_s)) \vee A(x) \end{array} \qquad (1^*_s)$$

Kako u opštem slučaju formula A(x) nije literal, formule $(1^*_s)$ imaju samo oblik sastavaka, pa ćemo ih zvati kvazi-sastavci.

Neka je $\mathcal{K}_L$ podteorija neprotivrečne teorije $\mathcal{K}$ , koja se od $\mathcal{K}$ razlikuje samo po tome što u shema-aksiomi indukcije A(x) nije proizvoljna formula već proizvoljan literal u jeziku teorije. Tada kvazi-sastavci $(1^*_s)$ u teoriji $\mathcal{K}_L$ postaju obični sastavci. Neka je A skup ostalih sopstvenih aksioma i neka je A konačan skup.

Dokazaćemo potpunost pravila binarne indukcije kad se uz rezoluciju primenjuje u dokazima pobijanjem za teoreme teorije $\mathcal{K}_L$.

Neka je $A_s$ skup sastavaka u $\mathcal{K}^*_L$ koji potiču od aksioma skupa A. Neka je F zatvorena formula teorije $\mathcal{K}_L$ i $\overline{F}_s$ skup sastavaka u $\mathcal{K}^*_L$ odredjen iz negacije formule F. Tada važi

STAV 2. Ako se konačnom primenom pravila rezolucije i pravila binarne indukcije iz skupa sastavaka $A_s \cup \overline{F}_s$ izvodi prazan sastavak, onda je F teorema u $\mathcal{K}_L$ , tj.

$$A_s \cup \overline{F}_s \vdash_{R,P} \square \rightarrow \vdash_L F$$

Dokaz. Stav ćemo dokazati oslanjanjem na potpunost rezolucije.

Ako $F \in T_1$ (videti str. 77.), onda je tvrdjenje tačno na osnovu potpunosti rezolucije (u tom slučaju prazan sastavak se izvodi samo rezolucijom).

Ostaje slučaj kad se pravilo binarne indukcije primenjuje bar jedanput. Neka je u izvodjenju praznog sastavka pravilo binarne indukcije primenjeno na sastavke $D_1$: $P_1 \vee C_1$ i $D_2$: $\neg P_2 \vee C_2$ (gde su $P_1$ i $P_2$ literali, $C_1$ i $C_2$ sastavci) koji su generisani iz polaznog skupa $A_s \cup \overline{F}_s$ ili mu pripadaju. Tada su po pravilu P generisani sastavci:

$$L_x(g(z_1,\ldots,z_s)) \vee C_{16} \vee C_{26} \quad \text{i} \quad \neg L_x(Sg(z_1,\ldots,z_s)) \vee C_{16} \vee C_{26} \qquad (2)$$

gde je $P_{16} = L_x(0)$ i $\neg P_{26} = \neg L_x(t)$; $z_1,\ldots,z_s$ su sve različite promenljive u literalu $L_x(0)$; g -skolemova funkcija s argumenata.

Sastavci (2) mogu se dobiti rezolucijom $D_1$, odnosno $D_2$ sa sledećim sastavcima:

$$\neg L_x(0) \vee L_x(g(z_1,\ldots,z_s)) \vee L(x)$$
$$\neg L_x(0) \vee \neg L_x(Sg(z_1,\ldots,z_s)) \vee L(x) \qquad (3)$$

Formule (3) su sastavci jedne konkretne aksiome indukcije u $\mathcal{K}^*_L$ (za literal L(x) ). Zato se primena pravila P na $D_1$ i $D_2$ može zameniti rezolucijom $D_1$, odnosno $D_2$ sa sastavcima konkretne aksiome indukcije.

Kako se pravilo P u izvodjenju praznog sastavka može primeniti najviše konačan broj puta i pošto se svaka primena binarne indukcije može zameniti rezolucijom sa sastavcima odgovarajućih konkretnih aksioma indukcije u $\mathcal{K}^*_L$ sledi da postoji izvodjenje praznog sastavka iz skupa $A_s \cup \overline{F}_s \cup I_s$ ($I_s$ - skup sastavaka konkretnih aksioma indukcije) samo po pravilu rezolucije.

Na osnovu potpunosti rezolucije skup $A_s \cup \overline{F}_s \cup I_s$ je nezadovoljiv, pa kako je $\mathcal{K}_L$ neprotivrečna teorija, formula F je posledica skupa A i nekih konkretnih aksioma indukcije u $\mathcal{K}_L$. Sledi, F je teorema u $\mathcal{K}_L$.

rimetimo, da s obzirom da je $\mathcal{K}_L$ podteorija teorije $\mathcal{K}$, je teorema i teorije $\mathcal{K}$.

ema 2. Ako se u teoriji $\mathcal{K}_L^*$ kao jedina pravila izvodjenja koriste pravilo rezolucije i pravilo binarne indukcije, onda se u $\mathcal{K}_L^*$ može dokazati aksioma indukcije teorije $\mathcal{K}_L$.

okaz. Neka je L(x) literal i $x, z_1, \ldots, z_s$ sve različite romenljive u L(x). Tada je formula

$$\forall z_1 \ldots \forall z_s \exists y \forall x (L_x(0) \Rightarrow (\neg L(x) \Rightarrow (L_x(y) \wedge \neg L_x(Sy))))$$

ksioma indukcije u teoriji $\mathcal{K}_L$. Njena negacija je

$$\exists z_1 \ldots \exists z_s \forall y \exists x (L_x(0) \wedge (\neg L(x) \wedge (\neg L_x(y) \vee L_x(Sy))))$$

kolemizacijom se dobija formula

$$L_x^c(0) \wedge \neg L_x^c(g(y)) \wedge (\neg L_x^c(y) \vee L_x^c(Sy))$$

ie je g skolemova funkcija argumenta y; gornji indeks c značava da je u literalima svaka od promenljivih $z_1, \ldots, z_s$ amenjena novom skolemovom konstantom.

z skupa sastavaka: $S = \{L_x^c(0), \neg L_x^c(g(y)), \neg L_x^c(y) \vee L_x^c(Sy)\}$

rimenom rezolucije i binarne indukcije izvodi se prazan sa-
tavak:

| | | |
|---|---|---|
| 1. | $L^c{}_x(0)$ | |
| 2. | $\neg L_x^c(g(y))$ | sastavci iz skupa S |
| 3. | $\neg L_x^c(y) \vee L_x^c(Sy)$ | |
| 4. | $L_x^c(h)$ | iz 1 i 2 po pravilu P ; $\sigma = \emptyset$ ; |
| 5. | $\neg L_x^c(Sh)$ | h - nova skolemova konstanta |
| 6. | $L_x^c(Sh)$ | 3,4 R |
| 7. | $\square$ | 5,6 R |

rimetimo da smo lemu dokazali nezavisno od ostalih aksioma $\mathcal{K}_L$.

osledica Sastavci aksiome indukcije se ne moraju navoditi u polaznom skupu sastavaka, koji potiču od ostalih sopstvenih aksioma teorije $\mathcal{K}_L$, kad se dokaz pobijanjem izvodi primenom pravila rezolucije i pravila binarne indukcije.

Zato važi sledeći stav.

STAV 3. Ako je zatvorena formula F teorema u $\mathcal{K}_L$, onda se iz konačnog skupa sastavaka $A_s U \bar{F}_s$ primenom pravila rezolucije i pravila binarne indukcije izvodi prazan sastavak, tj. $\vdash_{\mathcal{K}_L} F \longrightarrow A_s U \bar{F}_s \vdash_{R,P} \square$ .

Na osnovu stavova 2 i 3 važi sledeći

STAV POTPUNOSTI za teoriju $\mathcal{K}_L$

Zatvorena formula F je teorema u $\mathcal{K}_L$ akko konačnom primenom pravila rezolucije i pravila binarne indukcije iz skupa $A_s U \bar{F}_s$ generiše se prazan sastavak, tj. $\vdash_{\mathcal{K}_L} F \longleftrightarrow A_s U \bar{F}_s \vdash_{R,P} \square$ .

Razmotrimo pod kojim uslovima stav potpunosti važi za teoriju $\mathcal{K}$. Za teoriju $\mathcal{K}$ sastavci aksiome indukcije su kvazi-sastavci (jer A(x) je proizvoljna formula u jeziku teorije $\mathcal{K}$, a ne literal). Zbog toga na $A_x(0)$ i $\neg A_x(g(y))$ ne može se primeniti pravilo binarne indukcije, pa ni rezolucija kojom bi se izveo prazan sastavak (jer su oba pravila definisana samo za literale). Zato, u ovom slučaju ne važe lema 2 i stav 3. Medjutim, svaka konkretna formula Q(x) teorije $\mathcal{K}$, koja ulazi u svojstvu A(x) u aksiomu indukcije, odnosno u kvazi-sastavke koji su potrebni za dokaz teoreme F teorije $\mathcal{K}$, može se po definiciji zameniti novim predikatom R(x), tj. $R(x) \overset{def}{\Longleftrightarrow} Q(x)$. Ako sada formulu Q(x) u konkretnoj aksiomi indukcije zamenimo literalom R(x) i skupu polaznih sastavaka $A_s U \bar{F}_s$ priključimo sastavke odredjene nakon skolemizacije formule $R(x) \Longleftrightarrow Q(x)$, onda važi lema 2 i sledeći stav u kojem je $R_s$ oznaka za skup sastavaka koji potiču iz novouvedenih definicija.

STAV 3'. Ako je zatvorena formula F teorema teorije $\mathcal{K}$, onda postoji konačan skup sastavaka $R_s$ takav da se iz konačnog skupa sastavaka $A_s U \bar{F}_s U R_s$ konačnom primenom pravila rezolucije i pravila binarne indukcije generiše prazan sastavak, tj.

$$\vdash_{\mathcal{K}} F \longrightarrow A_s U \bar{F}_s U R_s \vdash_{R,P} \square$$

Sada važi sledeći (slabiji) STAV POTPUNOSTI za teoriju $\mathcal{K}$ :

Postoji konačan skup sastavaka $R_s$, takav da se po pravilu rezolucije i pravilu binarne indukcije generiše prazan sastavak iz konačnog skupa $A_s U \bar{F}_s U R_s$ akko je zatvorena formula F teorema teorije $\mathcal{K}$ , tj.

$$\vdash_{\mathcal{K}} F \longleftrightarrow A_s U \bar{F}_s U R_s \vdash_{R,P} \square$$

Ovde se radi o principijelnoj potpunosti, jer skup $R_s$ obično nije unapred poznat, niti je poznata procedura koja bi na osnovu skupa $A_s U \bar{F}_s$ generisala elemente skupa $R_s$ .
Primetimo da kad se radi o proveri postojećih dokaza , skup $R_s$ se može unapred odrediti. Prema tome, primenom pravila rezolucije i pravila binarne indukcije mogu se proveravati dokazi teorema teorije $\mathcal{K}$ koje pripadaju skupovima $T_1, T_2, T_3$ definisanim u tač. 1.1. ove glave (str.77.).

Uopšte, konačnom primenom pravila rezolucije i pravila binarne indukcije mogu se dokazati sve teoreme iz skupova $T_1$ i $T_2$, kao i sve one teoreme iz $T_3$ koje pripadaju teoriji $\mathcal{K}_L$. Za dokazivanje teorema iz $T_3$ koje ne pripadaju teoriji $\mathcal{K}_L$ potrebno je ( i dovoljno) imati na raspolaganju skup $R_s$ .

Kao primer najprostije i potpune rezolucijsko-indukcijske procedure može se uzeti procedura zasnovana na strategiji potpunog pregleda (zasićenja nivoa) u kojoj se na svakom koraku odredjuju sve rezolvente i svi sastavci generisani po pravilu binarne indukcije. U praktičnoj realizaciji potrebno je primeniti neku efektivniju strategiju.

Želimo na kraju da naglasimo da potpunost izabrane procedure, koja daje garanciju o dokazu u konačnom broju koraka, ima više teorijski nego praktičan značaj, jer dokaz može izaći iz realno postavljenih prostorno-vremenskih ograničenja. Zato je za praktičnu realizaciju primarna korektnost pravila izvođenja.

# G L A V A V

## INFORMACIJE O PROGRAMSKOJ REALIZACIJI REZOLUCIJSKO-INDUKCIJSKE METODE DOKAZIVANJA TEOREMA

Za mehaničko dokazivanje teorema u teorijama sa konačnim skupom sopstvenih aksioma, kao i za teorije sa jednakošću , postoje programi zasnovani na rezoluciji ili paramodulaciji. Prve verzije ovih programa bile su malo efektivne, pa su poboljšavane od strane više autora. Povećanje efektivnosti ostvareno je ugradjivanjem posebnih formi rezolucije (hiperrezolucija, uredjena linearna rezolucija) i razradom posebnih strategija pretraživanja (videti str. *43-54*).

Na bazi blok shema navedenih na Fig.1 i 2 glave IV , moguće je u postojeće programe za rezoluciju, bez naročitih teškoća, ugraditi pravilo binarne indukcije.

Kako ni jedan od postojećih programa za rezoluciju nije bio dostupan autoru ovog rada, razradjen je iznova celovit programski sistem zasnovan na rezoluciji i binarnoj indukciji. Za razradu takvog sistema potrebno je dosta vremena i angažovanje više ljudi. Srećnu okolnost predstavlja Projekat interaktivnog sistema "Graph" za klasifikaciju i unapredjivanje znanja iz oblasti teorije grafova, koji se realizuje na Elektrotehničkom fakultetu u Beogradu pod rukovodstvom prof.dr Dragoša Cvetkovića. U okviru ovog projekta javlja se potreba za rezolucijsko-indukcijskim dokazivačem teorema, za šta su brojni saradnici ovog projekta obezbedili polazne osnove.

Koristeći već razradjen sistem kodiranja simbola predikatskog računa prvog reda i postojeće programske module za racionalno angažovanje memorijskog prostora (tzv. memory manager) i za izdavanje alfa-numeričkih poruka, autor je napisao sistem programa za rezolucijsko-indukcijsko dokazivanje teorema u teorijama prvog reda.

Ovaj programski moduo sastoji se iz programa za testiranje i skupa potprograma od kojih 37 pripada autoru ovog rada. Moduo je inkorporiran u Sistem "Graph". Informacije o Sistemu "Graph" mogu se naći u [28] - [31].
Svi programi ovog sistema pisani su na FORTRANU i za većinu je izvršeno testiranje.
Na taj način, zahvaljujući pre svega prof.dr Dragošu Cvetkoviću, koji mi je ukazao značajnu pomoć i podršku u procesu pisanja programa, dosta vremena posvetio obučavajući me radu na računaru PDP 11/34 za potrebe testiranja i razradio programe za komuniciranje sa spoljašnjom memorijom, izgradjen je u okviru Sistema "Graph" rezolucijsko-indukcijski dokazivač teorema.

# 1. PROGRAMSKI MODUO ZA REZOLUCIJSKO-INDUKCIJSKO DOKAZIVANJE TEOREMA U TEORIJAMA PRVOG REDA

## 1.1. OPŠTE INFORMACIJE

Moduo za rezolucijsko-indukcijsko dokazivanje teorema pisan je kao potpuno automatizovan programski sistem koji radi u dva režima: sa rezolucijom i indukcijom, ili samo sa rezolucijom. Moduo je zasnovan na uredjenoj linearnoj rezoluciji (OL-rezoluciji, videti glavu II str. 49 ovog rada) i na pravilu binarne indukcije (videti glavu IV str. 84 ovog rada).

Uredjena linearna rezolucija, koja uključuje strategiju potpornog skupa i udaljavanja tautologija, izabrana je zbog prednosti koja se ogleda u potrebi memorisanja samo onih sastavaka koji su generisani na uzastopnim (susednim) nivoima, a ne svih generisanih sastavaka u procesu traženja dokaza. Osim toga, jedan od sastavaka koji učestvuju u OL-rezoluciji je na svakom koraku unapred fiksiran u svojstvu "centralnog sastavka", a rezolucija (ili indukcija) vrši se samo po njegovom poslednjem literalu. Drugi sastavak uzima se iz skupa polaznih sastavaka i ima ulogu "bočnog sastavka".

S obzirom da primena pravila indukcije, u skladu sa principom navedenim na str. 91 , dovodi do generisanja dva sastavka, jedan od njih se zadržava u svojstvu kandidata za novi centralni sastavak na narednom nivou, a drugi se zapisuje u polazni skup bočnih sastavaka.

Polazni skup sastavaka sačinjavaju sastavci odredjeni pomoću skolemizacije iz negacije zatvorene formule koju treba dokazati i sastavci dobijeni na isti način iz sopstvenih aksioma (osim shema-aksiome matematičke indukcije), lema, ranije dokazanih teorema ili definicija teorije prvog reda.

Kao rezultat dobija se dokaz nezadovoljivosti polaznog skupa sastavaka u obliku odštampanog pobijanja, ili informacija da se pobijanje ne može naći u predvidjenim dimenzijama angažovane memorije računara. U takvom slučaju, signal za prekid rada je dostizanje predvidjenog maksimalnog broja generisanih sastavaka za poslednji početni sastavak iz niza početnih sastavaka koji potiču od negacije formule koja se dokazuje.

U toku rada koriste se ograničenja na dužinu literala, dužinu sastavaka i broj generisanih sastavaka na svakom nivou, kao i ograničenje dubine pretraživanja (broj nivoa) za svaki početni sastavak. Sastavci koji prelaze ova ograničenja se ne generišu.

Potrebno je naglasiti da štampani dokument na izlazu, u slučaju da računar ostvari pobijanje polaznog skupa sastavaka, sadrži samo sastavke koji pripadaju pobijanju, a ne sve generisane sastavke u toku rada. Time je korisniku omogućen pregledan uvid u dokaz pobijanjem, bez nepotrebnih detalja, a dokument dobijen na računaru ne predstavlja "knjigu" iz koje treba izdvojiti dokaz, već samo dokaz. To je postignuto memorisanjem izvesnih karakteristika o sastavcima koji učestvuju u rezolucijama ili indukcijama. Na osnovu tih karakteristika vrši se rekonstrukcija stabla dokaza, vraćanjem s kraja (od praznog sastavka) na početak i ponovnim generisanjem samo onih sastavaka koji pripadaju izdvojenom stablu.

U slučaju kad računar ostvari pobijanje štampani dokument ima sledeći izgled na svakom nivou:
CENTRALNI SASTAVAK:
BOČNI SASTAVAK:
REZOLUCIJSKA (odnosno INDUKCIJSKA) ZAMENA:
Na kraju takvog niza stoji:
PRAZAN SASTAVAK
DOKAZ JE ODŠTAMPAN .

Na osnovu sadržaja tač. 1.2.,1.3.,2.1. i 2.2. može se steći detaljniji uvid u strukturu i ograničenja, kao i funkcionisanje ovog programskog modula. Informacije o prvim rezultatima testiranja navedene su u odeljku 3.

U okviru daljeg usavršavanja i eksploatacije sistema "Graph" moguća su razna poboljšanja ove verzije programskog modula ( na pr. poboljšanje strategije pretraživanja, uvodjenje novih ograničenja na primenu pravila binarne indukcije, ugradjivanje pravila paramodulacije, kao i stvaranje mogućnosti za interaktivno pretraživanje).

## 1.2. OBLIK RAGISTROVANJA PODATAKA

Za registrovanje podataka koriste se celobrojne promenljive i jednodimenzioni nizovi čiji su članovi celi brojevi. Svaki simbol formule-teorije prvog reda kodira se celobrojnom konstantom u skladu sa kodnom listom.
Podaci se u memoriji računara registruju na sledeći način:

1. <u>Niz sastavaka</u> $D_1,D_2,\ldots,D_n$ registruje se kao jednodimenzioni niz A(I) u obliku:

$$\underbrace{A(1)\ \ldots\ A(s_1)}_{D_1}\ \underbrace{A(s_1+1)\ \ldots\ A(s_2)}_{D_2}\ \ldots\ \underbrace{A(s_{n-1}+1)\ \ldots\ A(s_n)}_{D_n}$$

pri čemu se u $A(s_1),A(s_2),\ldots,A(s_n)$ nalazi simbol za kraj sastavka.

2. <u>Sastavak</u> D (disjunkcija literala: $L_1 \vee L_2 \vee \ldots \vee L_k$) registruje se kao jednodimenzioni niz D(j) oblika:

$$\underbrace{D(1)\ldots D(l_1)}_{L_1}\underbrace{D(l_1+1)\ldots D(l_2)}_{L_2} \cdots \underbrace{D(l_{k-1}+1)\ldots D(l_k)}_{L_k} D(l_{k+1})$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad *$$

Simbol disjunkcije se ne registruje; * je simbol za kraj sastavka.

3. <u>Literal</u> (atomična formula ili njena negacija) registruje se tako što se svaki simbol sadržan u literalu registruje kao poseban element niza L(K). Zagrade i zarezi se zadržavaju i registruju. Po potrebi na kraj niza L(K) stavlja se simbol za kraj literala.

4. <u>Markirani literal</u> registruje se kao literal ispred kojeg je upisan specijalni simbol (/). Taj simbol se registruje kao prvi element niza L(K).

<u>Primer</u>: Sastavak $P(x) \vee \boxed{Q(f(x,y),z)} \vee \neg R(z) \vee \boxed{\neg Q(a,b)}$ , gde su markirani literali uokvireni, biće registrovan kao niz:

D: P(x)/Q(f(x,y),z)¬R(z)/¬Q(a,b)*
tj. u 30 članova niza D.

5. <u>Zamenska komponenta</u> t/x , gde je t term, a x promenljiva, registruje se kao niz T/X* , gde je T niz odredjen termom t bez simbola za kraj terma, X promenljiva, a * simbol za kraj zamenske komponente.

6. <u>Zamena</u> registruje se kao niz zamenskih komponenti (bez simbola za kraj komponente) razdvojenih zarezom, a na kraj se stavlja simbol za kraj zamene.

Primer: Zamena $\sigma = \{f(a,y)/z, b/x\}$ registruje se u 13 članova niza SIGMA: f(a,y)/z,b/x*

<u>Napomena</u>: Literal $(x+y)' \neq x+y'$ mora se transformisati u oblik:
=('(+(x,y)),+(x,'(y))) .

## 1.3. ULAZNI PODACI, NIZOVI I OGRANIČENJA

Kao ulazni podaci u programski moduo za rezolucijsko-indukcijsko dokazivanje teorema moraju se zadati vrednosti sledećih promenljivih i nizova:

Promenljive:

IND - za vrednost 0 odredjuje režim rada sa indukcijom, a za za vrednost 1 bez indukcije

M - broj sastavaka koji potiču iz negacije formule koja se dokazuje

N - broj sastavaka u polaznom skupu sastavaka

JMAX - maksimalan broj sastavaka u nizu AKS. Zbog indukovanih sastavaka treba da je (na početku) JMAX>N

LMAX - maksimalan broj sastavaka generisanih u nivou

DMAX - maksimalna dužina sastavka (uključujući i simbol za kraj)

LITMAX- maksimalna dužina literala (uključujući i simbol za kraj)

BUBMAX- maksimalna dubina dokaza (maksimalan broj nivoa u dokazu)

RNVMAX- maksimalan broj svih generisanih sastavaka za dati početni sastavak iz skupa KN uvećan za DUBMAX

K1 - ukupan broj simbola, koji se registruju, iz sastavaka koji potiču iz negacije teoreme (uključujući i simbol za kraj svakog sastavka, ali bez simbola disjunkcije). To je broj simbola u nizu KN

K2 - ukupan broj simbola (koji se registruju) u polaznom skupu sastavaka (sa simbolom za kraj svakog sastavka, ali bez simbola disjunkcije). To je ukupan broj simbola u ulaznom nizu AKS.

KRMAX - maksimalan broj članova (simbola) u nizu KR koji sadrži sastavke generisane na prethodnom nivou, a prepisane iz niza REZ, tj. sastavke koji predstavljaju kandidate za centralne sastavke na tekućem nivou. KRMAX≤LMAX•DMAX .

AKSMAX- maksimalan broj članova (simbola) niza AKS.
AKSMAX≤JMAX•DMAX .

Vrednosti KRMAX i AKSMAX koriste se i za dimenzionisanje nizova REZ i KR, odnosno AKS na ulazu.

Nizovi:

N(I) , I= $\overline{1,K1}$ - sadrži M sastavaka koji potiču od negacije teoreme i sastoji se od K1 članova (simbola) Početni centralni sastavak je element iz KN.

AKS(I) , I= $\overline{1,K2}$ - sadrži N sastavaka polaznog skupa (aksiome, leme, teoreme,definicije i sve članove iz KN) i sadrži K2 članova (simbola).
U režimu sa indukcijom u AKS se upisuje po jedan od indukovanih sastavaka u svakoj primeni pravila binarne indukcije.

Za dati centralni sastavak na jednom nivou generišu se svi sastavci rezolucijom ili indukcijom sa bočnim sastavcima iz AKS. Novogenerisani sastavci memorišu se u nizu REZ i poslužiće kao centralni sastavci na narednom nivou. Pri prelazu na naredni nivo, kad su iscrpeni svi sastavci iz niza KR kao centralni, odnosno kad je dostignut broj LMAX, niz REZ se oslobadja prepisivanjem u niz KR (na mesto starih centralnih sastavaka).
Kad broj generisanih sastavaka dostigne RNVMAX (za izabrani početni sastavak iz KN) prelazi se na sledeći početni sastavak iz niza KN. Ukoliko u KN više nema sastavaka (a nije generisan prazan sastavak) rad se prekida, USPEH = 0 i saopštava se da dokaz nije nadjen u predvidjenim dimenzijama nizova.
Ako je na nekom nivou generisan prazan sastavak, tada je USPEH=1, što znači da je teorema dokazana, pa se pristupa generisanju stabla i štampanju dokaza.

Osim nizova KN i AKS koji su ulazni podaci i nizova KR i REZ koji se formiraju u toku rada, za odredjivanje povratnog puta, generisanje stabla i štampanje dokaza formira se i niz

RNIV - niz brojevnih karakteristika svih generisanih sastavaka u toku rada sa fiksiranim početnim sastavkom iz niza KN .
Elementi niza RNIV su brojevi:

$$R \cdot 10^6 + J \cdot 10^4 + K \cdot 10^2 + INBR$$

gde R - ukazuje na centralni sastavak uzet kao R-ti sastavak iz niza KR koji je generisan na prethodnom nivou. Na prvom nivou R=1 ukazuje na I-ti po redu sastavak iz skupa KN koji je uzet kao početni sastavak i kao takav prepisan u niz KR kao njegov jedini sastavak;

J - ukazuje na bočni sastavak uzet kao J-ti sastavak iz AKS;

K - ukazuje na K-ti literal u bočnom sastavku

INBR - brojač primena pravila binarne indukcije (potreban je za numerisanje novih skolemovih funkcija ili konstanti).

Brojevne karakteristike sastavaka generisanih u raznim nivoima razdvojene su u nizu RNIV specijalnim simbolom. Svaka karakteristika kao i specijalni simbol memoriše se kao element niza RNIV. Na osnovu prethodnog, RNVMAX predstavlja maksimalan broj članova niza RNIV.

Ilustrovaćemo na jednom primeru kako se na osnovu karakteristika sadržanih u nizu RNIV vrši rekonstrukcija povratnog puta i stabla dokaza.

Radi jednostavnosti uzećemo da se karakteristika izračunava po izrazu: $R \cdot 10^3 + J \cdot 10^2 + K \cdot 10 + INBR$ .

Neka su karakteristike (zapisane po nivoima) u nizu RNIV:

1120 1130 1321 *

1130 1321 1430 2121 2321 3110 3131 *

1230 1320 2120 2410 3421 4320

pri čemu poslednja (4320) odgovara praznom sastavku.

Tada je $R = [4320/1000] = 4$

Karakteristika 4320-4000 = 320 memoriše se kao prvi član niza PUT. Na osnovu tako odredjenog R traži se R-ta po redu karakteristika u prethodnom nivou iz niza RNIV; to je 2121 .

Iz nje se odredjuje R = 2 i 2121-2000 = 121 memoriše se kao drugi član niza PUT.

Druga po redu karakteristika prethodnog nivoa iz niza RNIV je 1130 , a kako je to prvi nivo, R=1 ukazuje da treba uzeti I-ti po redu sastavak iz niza KN (vrednost I u tom trenutku je poznata). Broj 1130-1000=130 memoriše se kao treći član niza PUT. Kako je $J = [130/100] = 1$ treba uzeti J-tu (tj. prvu) aksiomu

niza AKS.
ko je K = $\lceil(130-100)/10\rceil$ = 3 , treba naći K-ti (tj.treći)
teral u J-toj (prvoj) aksiomi.
jzad, kako je INBR = 30-3•10 = 0 ne treba vršiti indukciju,
ć rezoluciju I-tog sastavka iz KN (kao centralnog) i J-te
siome iz AKS (kao bočnog sastavka) po K-tom literalu aksiome
poslednjem literalu centralnog sastavka.
d je rezolucija izvršena i kad su odštampani centralni i
čni sastavci i rezolucijska zamena, prelazi se na prethodnu
rugu) karakteristiku niza PUT. To je 121. Iz nje je

J = 1 ; K = 2 ; INBR = 1 ,

o znači da treba vršiti indukciju prethodno odredjene rezol-
nte (kao centralnog sastavka) sa K-tim (drugim) literalom J-te
rve) aksiome iz niza AKS (kao bočnog sastavka).
d je indukcija izvršena, nakon štampanja centralnog i bočnog
stavka i indukcijske zamene, prelazi se na prethodni član ni-
PUT. U ovom slučaju to je prvi član i on sadrži karakteristi-
: 320 . Iz nje je

J = 3 ; K = 2 ; INBR = 0 ,

se rezolucija vrši nad poslednjim literalom centralnog sas-
vka (indukovanog na prethodnom nivou) i K-tim (drugim) lite-
lom J-te (treće) aksiome iz niza AKS kao bočnim sastavkom,
ri tom to ne mora obavezno biti polazna aksioma, već može biti
ki od indukovanih sastavaka koji su upisani u niz AKS).
o rezultat dobija se prazan sastavak. Štampaju se centralni i
čni sastavak i rezolucijska zamena i informacija da je gene-
san prazan sastavak i da je dokaz završen.

POMENA

Zbog minimalne dužine registrovanja celobrojnih podataka
va podregistra, a ne četiri) u sistemu PDP 11/34, maksimalna
ednost celog broja je 32767, pa je zbog toga niz RNIV podeljen
dva niza RNIV1 i RNIV2 . Elementi niza RNIV1 čuvaju karakteri-
ike R i K , izračunavaju se izrazom $R\cdot10^2+K$ , a elementi niza
IV2 čuvaju karakteristike J i INBR , a izračunavaju se po izra-
$J\cdot10^2+$ INBR.
nalaže sledeća ograničenja na maksimalne vrednosti:

$R \leqslant 326$ ; $K \leqslant 99$ ; $J \leqslant 326$ ; $INBR \leqslant 99$ ,

što znači da broj sastavaka generisanih u nivou (broj sastavaka u nizu REZ, odnosno KR) mora biti najviše 326. Takodje, niz AKS može imati najviše 326 sastavaka, tj. $JMAX \leqslant 326$ i broj literala u sastavku ne prelazi 99, a broj primena pravila binarne indukcije za fiksirani početni sastavak ne prelazi 100 .

Nizovi KN , AKS , REZ , KR , RNIV1 , RNIV2 kao nizovi velikih dimenzija čuvaju se u spoljašnjoj memoriji, a sa njima se komunicira pomoću dva potprograma RGET i RSTOR (za učitavanje, odnosno upisivanje). Ostali nizovi koji se koriste kao pomoćni u okviru posebnih potprograma memorišu se kao delovi niza MEMOR koji predstavlja zajedničku zonu i angažuje se ili oslobadja pomoću posebnog programskog modula MEMORY MANAGER - a .

Svi nizovi u modulu za rezolucijsko-indukcijsko dokazivanje teorema imaju relativne dimenzije i dimenzionišu se pre ulaska u moduo u osnovnom programu.

## 2. PREGLED POTPROGRAMA MODULA ZA REZOLUCIJSKO-INDUKCIJSKO DOKAZIVANJE TEOREMA

### 2.1. KRATAK OPIS FUNKCIJA POJEDINIH POTPROGRAMA

Navodimo imena potprograma sa opisom funkcije koju ostvaruju.

RDOKAZ poziva se iz glavnog programa (odn. programa za test.). U njemu se vrši izbor centralnog i bočnog sastavka. Početni sastavak uzima se iz niza KN (I-ti sastavak u KN). Za komuniciranje sa spoljašnjom memorijom pozivaju se RGET i RSTOR. Bočni sastavak uzima se iz skupa polaznih sastavaka,tj. iz niza AKS.Formira se niz KR,kandidata za centralne sastavke. U početku KR sadrži samo izabrani početni sastavak iz KN. Za odredjivanje poslednjeg literala u izabranom centralnom sastavku iz niza KR poziva se RPOSLT. Zatim se poziva RADD12

u kojem se za izabrane sastavke D1 i D2 generišu moguće rezolvente i indukovani sastavci zajedno sa njihovim karakteristikama. Generisani sastavci memorišu se u nizu REZ.
Kad su za svaki centralni sastavak iz KR generisani novi sastavci, prelazi se na naredni nivo: niz REZ se oslobadja prepisivanjem u niz KR.(novo-generisani sastavci postaju kandidati za centralne sastavke). Ukoliko je generisan prazan sastavak, poziva se RPUT za odredjivanje povratnog puta na osnovu karakteristika koje su memorisane u nizu RNIV1 i u nizu RNIV2.Zatim se poziva RPOVRT za generisanje i štampanje dokaza.
Ukoliko za izabranu aksiomu nije generisan prazan sastavak, prelazi se na narednu aksiomu, ako postoji, a ako ne postoji više aksioma,prelazi se na nov centralni sastavak iz niza KR. Ukoliko u nizu KR nema više centralnih sastavaka, prelazi se na nov početni sastavak iz KN (na sledeći nivo). Ako su iscrpeni svi početni sastavci iz KN, a nije generisan prazan sastavak, saopštava se da pokušaj dokaza nije uspeo, odnosno da dokaz nije nadjen u predvidjenim dimenzijama nizova.

RGET i RSTOR služe za komuniciranje sa spoljašnjom memorijom. Autor ih je napisao u formi pozivanja, odnosno zapisivanja podnizova dužih nizova.
RGET vrši učitavanje I-tog sastavka iz jednodimenzionog niza A u jednodimenzioni niz B. LB je broj simbola u nizu B uključujući i simbol za kraj sastavka.
RSTOR vrši zapisivanje LB članova niza B u niz A počev od I-tog sastavka u A. Promenljiva LER je indikator nemogućnosti zapisivanja u A zbog prekoračenja maksimalne dimenzije AMAX niza A ( u tom slučaju LER = 1 , inače LER = 0).

RPRPIS vrši prepisivanje I-tog sastavka niza A u I-ti sastavak niza B. To se ostvaruje posredstvom pomoćnog niza PN. Promenljiva LER je indikator nemogućnosti prepisa zbog prekoračenja maksimalne dimenzije BMAX niza B (u tom slučaju LER=1,inače 0). Ovaj potprogram poziva RGET i RSTOR. Treba imati u vidu da prilikom zapisivanja ostatak niza u koji se upisuje može biti deformisan,ali za potrebe dokazivača teorema to nije bitno.

RADD12 vrši obradu izdvojenih sastavaka D1 i D2.
Poziva RBRLD za odredjivanje broja literala u sastavku D2.
Poziva RKLITK za odredjivanje k-tog literala iz D2 koji je komplementaran (u odnosu na negaciju predikatskog simbola) poslednjem literalu iz D1.
Poziva RPREOZ za preoznačavanje zajedničkih promenljivih u D1 i D2.
Poziva RFORL za formiranje skupa literala za potrebe odredjivanja unifikatora, odnosno indukcijske zamene.
U zavisnosti od izabranog režima rada (sa ili bez indukcije) poziva RUNIFI (za odredjivanje unifikatora), odnosno RIZAM (za odredjivanje indukcijske zamene). Ako takve zamene postoje poziva REZOL za generisanje rezolvente, odnosno RINDBL za generisanje indukovanih sastavaka. Ako odgovarajuće zamene ne postoje, prelazi se na izbor narednog literala u D2. Kad takav izbor više nije moguć, ili ako je dostignut maksimalan broj generisanig sastavaka u nivou LMAX, vraća se u RDOKAZ zajedno sa nizom generisanih sastavaka (REZ) i njihovim karakteristikama, koje su memorisane u nizovima IKJR1 i IKJR2. U slučaju da je generisanjem indukovanih sastavaka popunjen niz AKS, stavlja se Z=1 i ta vrednost se prenosi u RDOKAZ kao nova vrednost promenljive IND, što znači da se u daljem radu indukcija neće vršiti, pa do popune predvidjenih dimenzija nizova pokušava se naći dokaz samo rezolucijom.
Upisivanje generisanih sastavaka vrši se pozivanjem RSTOR.
Upisivanje se vrši u nizove REZ, odnosno kod primene indukcije u REZ i AKS.
Prilikom generisanja novih sastavaka vrši se eliminacija tautologija. Tautologije se ne upisuju u REZ niti se bilo gde memorišu.

RUNIFI odredjuje NOU ako postoji i saopštava ako NOU ne postoji.
Poziva RTERM za odredjivanje terma T u nizu A koji počinje simbolom u A(I).
Poziva RSUPST za supstituciju svakog ulaženja promenljive X u niz A termom T.

Poziva RKOMP za odredjivanje kompozicije niza A sa T/Xж u obliku A,T/Xж .
Poziva RTETPR za odredjivanje Θ-primera niza D (radi odredjivanja unifikatora).

RIZAM vrši odredjivanje indukcijske zamene, ako postoji, i saopštava ako zamena ne postoji.
Poziva RTERM , RSUPST , RKOMP , RTETPR , RUNIFI i RCOMP za odredjivanje kompozicije zamena IALFA i IBETA .

REZOL vrši odredjivanje OL-rezolvente, za sastavke D1 i D2 .
Poziva RFORMR za formiranje OL-rezolvente.
Poziva RSAŽ za izvršavanje operacije sažimanja nad rezultatom R dobijenim iz RFORMR : brisanje svakog nemarkiranog literala u R identičnog mladjem (koji stoji levo) nemarkiranom literalu u R, uz utvrdjivanje da li u R postoje komplementarni nemarkirani literali, tj. da li je R tautologija (ako da TAU=1,inače 0). M=1 znači da u R od I-te pozicije do kraja nema nemarkiranih literala, tj. da je sažimanje završeno.
Za ostvarivanje ovih funkcija RSAŽ poziva RNEMRL za nalaženje nemarkiranog literala L u nizu R od I-tog člana pa nadalje, i RBRIS za brisanje svakog ulaženja nemarkiranog literala L u niz D (ostatak niza R s desna od literala R; u RSAŽ ovaj niz imenovan je REST) i utvrdjivanje da li niz D sadrži komplementarne sa L literale, ako da T=1, što znači da je D tautologija (vrednost T pri povratku u RSAŽ postaje vrednost TAU).
Po izvršenju RSAŽ,REZOL poziva RSKR za izvršenje operacije skraćivanja: brisanje svakog markiranog literala u R iza kojeg nema nemarkiranih literala.
Ako je skraćeno R prazan sastavak, ili ako sadrži samo jedan nemarkirani literal koji je jedini u R, onda je M=0, što znači da se njegovo brisanje ne može izvršiti u potprogramu RBRLKM , tj. da je rezolventa odredjena. Inače M=1 i W čuva poziciju početka poslednjeg nemarkiranog literala (koji nije jedini literal u R). Kad je po povratku iz RSKR u REZOL M=1, onda se poziva RBRLKM za brisanje poslednjeg (nemarkiranog) literala koji se unificira NOU Θ (za šta RBRLKM poziva RUNIFI) sa nekim komplementarnim markiranim literalom. Ako se ovo brisanje

ne može izvršiti (IZVB = 0) rezolventa je odredjena, a ako je brisanje izvršeno (IZVB = 1) po povratku u REZOL ponovo se poziva RSKR. Ovo se ponavlja sve dok se na izlazu iz RSKR ne dobije M=0 ili dok se na izlazu iz RBRLKM ne dobije IZVB = 1 , što se posle konačnog broja ponavljanja ovog ciklusa mora dogoditi.

Kao što je rečeno, formiranje OL-rezolvente sastavaka D1 i D2 vrši se u RFORMR. RFORMR izvršava rezoluciju po poslednjem literalu u D1, koji se pri tome markira i zadržava u rezolventi R, i literalu L2 sastavka D2. Za formiranje R u RFORMR poziva se RTETPR za odredjivanje Oprimera i RMARK za markiranje poslednjeg literala u nizu D1. Na izlazu iz RMARK dužina starog niza uvećana je za jedinicu (za simbol markice).
Za formiranje rezolvente RFORMR zatim poziva RBRIS koji briše svako ulaženje literala L2 u niz D2. Tako odredjeni ostatak niza D2, po povratku u RFORMR, dopisuje se na niz D1 (u kojem je poslednji literal markiran) i tako dobijeni niz R predstavlja ulazni podatak za RSAŽ, a potom za RBRLKM, gde OL-rezolventa dobija definitivan oblik. Formirana rezolventa vraća se u RADD12 zajedno sa informacijom da li je tautologija ili ne.

RINDBL vrši generisanje indukovanih sastavaka iz sastavaka D1 i D2, a na osnovu prethodno odredjene indukcijske zamene. Poziva RNIZPR za odredjivanje niza različitih promenljivih koje ulaze u niz D. Različite promenljive memorišu se u nizu X dužine LX gde su zapisane u obliku: X1, ... ,XLX . To se čini nakon što je pozivanjem RTETPR , RPOSLT i RKLIT obezbedjena mogućnost primene pravila indukcije na poslednji literal iz D1 i k-ti literal iz D2.

U RPOSLT vrši se odredjivanje poslednjeg literala u sastavku D1 i prepisivanje tog literala u niz LIT; M je broj simbola u poslednjem literalu uključujući i simbol za kraj.
U RKLIT vrši se odredjivanje k-tog literala u nizu D2 za dato k.

Promenljiva Y u RINDBL koja dobija vrednost u RADDl2 (preciznije u RIZAM) za vrednost 1 odredjuje da se term po kojem treba vršiti indukciju nalazi u literalu L1, pa se niz promenljivih odredjuje iz literala L2, a za vrednost 2 obrnuto. Za odredjivanje terma sa novim skolemovim funkcijama (odnosno konstantama)oblika G(X1,...,XL)* i '(G(X1,...,XL))* , (odnosno G* i '(G)*), pri čemu je G numerisan nov simbol, koristi se RFRMTR. Kad su termi formirani iz RINDBL poziva se RZT1T2 u kojem se vrši zamenjivanje svakog ulaženja terma t u niz A termom T2 i svakog odgovarajućeg ulaženja O u niz B termom T1.

Odgovarajuće ulaženje znači: A: ... t ... t ...
B: ... O ... O ...

Rezultati se upisuju u nizove P1:...T2 ...T2 ...
i P2:...T1 ...T1 ...

Zatim RINDBL poziva RUPIS1 za upisivanje u niz A sastavka D1 do rednog broja I (početak poslednjeg literala u D1), na to se dopisuje D2 do simbola PK-tog (početak k-tog literala),pa se preskoči broj simbola koji pripadaju k-tom literalu (literalu L2) i dopiše se ostatak od D2; na to se dopiše P (P je P1 ili P2 zavisno od toga da li je Y=1 ili Y=2). Na taj način formiran je indukovani sastavak Q1 (koji će biti memorisan u nizu REZ i postaće kandidat za centralni sastavak na narednom nivou). Drugi indukovani sastavak formira se u RUPIS2 koji se od RUPIS1 razlikuje samo po tome što se upisivanje u niz A do rednog broja I vrši uz preskakanje markiranih literala u D1. S obzirom da će tako formirani sastavak Q2 biti memorisan u nizu AKS i nadalje će poslužiti kao bočni sastavak na narednim nivoima, markirani literali u Q2 nisu potrebni.

Za ostvarenje opisanih funkcija RUPIS1 i RUPIS2 pozivaju RZAPIS koji ostvaruje upisivanje u niz A počev od I-tog člana, članova niza D do J-tog člana, preskakanje (DL-1) članova u D i dopisivanje ostatka niza D, a zatim prepisivanje celog niza P.

'UT vrši odredjivanje povratnog puta (stabla dokaza) po indeksima koji se nalaze u nizu RNIV (ustvari RNIV1 i RNIV2) loženi po nivoima u kojim su generisani. Odredjivanje povratnog puta vrši se po postupku opisanom na str. 104-106.

OVRT vrši generisanje i štampanje dokaza. Za ostvarivanje te funkcije poziva se RPRAD. RPRAD ostvaruje istu funkciju kao RADD12 ali sada, pri ponovnom radu, generišu se samo sastavci koji pripadaju stablu dokaza, pa pojedini delovi RADD12 postaju suvišni. Ustvari, pre ulaska u RPRAD poznato je po kojem literalu u sastavku D2 treba vršiti rezoluciju, odnosno indukciju, a dobijeni rezultat predstavlja jedan nivo u dokazu. Na osnovu sačuvanih karakteristika poznate je i koju aksiomu na datom nivou dokaza treba uzeti za bočni sastavak. Centralni sastavak je takodje poznat; to je sastavak generisan na prethodnom nivou, a na samom početku to je I-ti sastavak iz niza KN (vrednost I pre ulaska u RPOVRT je poznata).

## 2. STRUKTURA PROGRAMSKOG MODULA

Povezanost potprograma u okviru programskog modula rezolucijsko-indukcijske dokazivanje teorema prikazana je Figuri 3. Imena potprograma koja su na Fig. 3 podvučena imena bazičnih potprograma (potprograma koji u sebi ne irže poziv drugih potprograma). Ne podvučeno ime podrazumeva se uključuju svi potpbogrami koje potprogram čije je to ime ziva.

tprogrami AUXVC i MDEL pripadaju MEMORY MANAGER-u , a potprogmi MESSAG i FDISPL ostvaruju štampanje poruka i rezultata. zultati se mogu štampati u kodiranom obliku ili uz pomoć FDISPL slovno-cifarskom (uobičajenom) obliku.

tprogramom CHFSD ispituje se vrsta uočenog simbola (promenljiva, ıstanta, predikatski simbol, funkcijski simbol ).

tprogrami AUXVC , MDEL , MESSAG , FDISPL i CHFSD napisani su strane drugih autora - saradnika na izgradnji Sistema "Graph", ne pripadaju autoru ovog rada. Isto važi i za nove verzije T i RSTOR adaptirane za komuniciranje sa spoljašnjom memorijom

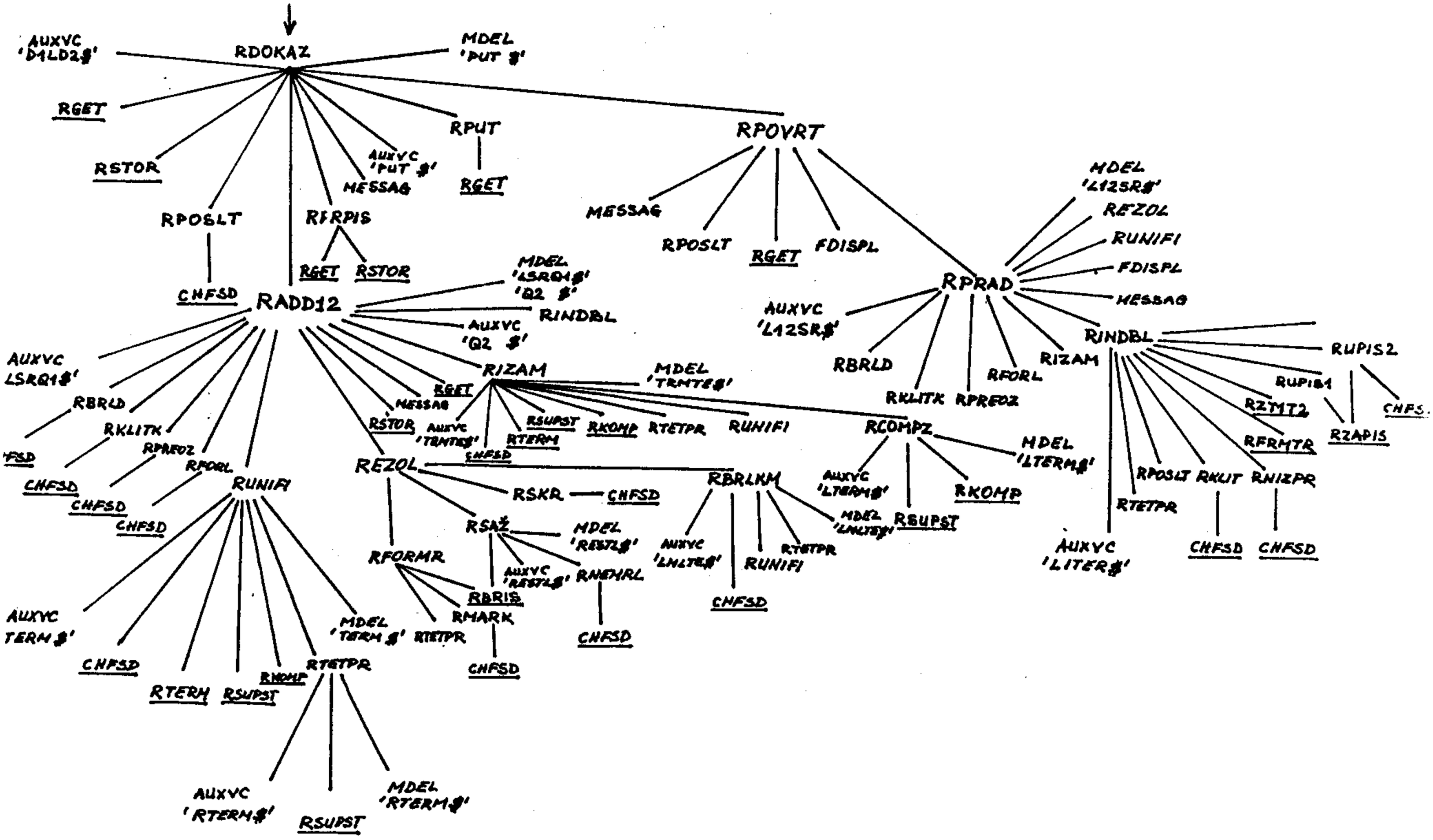

RDOKAZ
AUXVC 'D1LD2$'
MDEL 'PUT $'
RGET
RSTOR
RPOSLT
CHFSD
RFRPIS
RGET
RSTOR
AUXVC 'PUT $'
MESSAG
RPUT
RGET
RADD12
MDEL 'LSRQ1$' 'Q2 $'
RINDBL
AUXVC 'Q2 $'
AUXVC LSRQ1$'
RBRLD
RKLITK
RPREDZ
RFORL
RUNIFI
CHFSD
CHFSD
CHFSD
CHFSD
RIZAM
MDEL 'TRMTE$'
RGET
MESSAG
RSTOR
AUXVC 'TRMTE$'
RSUPST
RTERM
CHFSD
RKOMP
RTETPR
RUNIFI
REZOL
RSKR
CHFSD
RSAŽ
MDEL 'REZL$'
AUXVC 'REZL$'
RFORMR
RBRIS
RMARK
RNEMRL
RTETPR
CHFSD
CHFSD
AUXVC TERM$'
MDEL 'TERM $'
CHFSD
RTERM
RSUPST
RKOMP
RTETPR
AUXVC 'RTERM$'
RSUPST
MDEL 'RTERM$'
RPOVRT
MESSAG
RPOSLT
RGET
FDISPL
RBRLKM
AUXVC 'LNLTE$'
MDEL 'LNLTE$'
RUNIFI
CHFSD
RTETPR
RCOMPZ
AUXVC 'LTERM$'
RSUPST
MDEL 'LTERM$'
RKOMP
RPRAD
MDEL 'L12SR$'
REZOL
RUNIFI
FDISPL
MESSAG
AUXVC 'L12SR$'
RBRLD
RKLITK
RPREDZ
RFORL
RIZAM
RINDBL
RUPIS2
RUPIS1
RZMT2
RFRMTR
RZAPIS
CHFS.
RPOSLT
RTETPR
RKLIT
RNIZPR
AUXVC 'LITER$'
CHFSD
CHFSD

Figura 3.

## 5. INFORMACIJA O PRVIM REZULTATIMA TESTIRANJA

Prvo testiranje programskog modula za rezolucijsko-indukcijsko dokazivanje teorema u teorijama prvog reda sa matematičkom indukcijom izvršeno je na računaru PDP 11/34 , bez korišćenja spoljašnje memorije. To je uslovilo izbor jednostavnih test primera.

Za ilustraciju navodimo dva primera realizovana na PDP 11/34 u procesu testiranja.

Primer 1. Dokaz $\forall x P(x)$ pobijanjem iz $P(0)$ i $\forall x(P(x) \Rightarrow P(Sx))$
($P(x)$ - literal u kojem je x jedina promenljiva).

Polazni skup sačinjavaju sastavci: $\neg P(C)$ ; $P(0)$ ; $\neg P(x) \vee P(Sx)$.

Ulazni podaci su:

IND=0 ; M=1 ; N=3 ; JMAX=10; LMAX=10; DMAX=20; LITMAX=10;
SUBMAX=5; RNVMAX=10; K1=6 ; K2=24 ; KRMAX=200 ; AKSMAX=120 ;

Iz KN sadrži 6 članova:

$\neg P(C)$※ negacija i skolemizacija formule $\forall x P(x)$, C Skol.konst.

Iz AKS sadrži 24 člana:

$P(0)$※$\neg P(X) P(S(X))$※$\neg P(C)$※

Na računaru PDP 11/34 dobijeno je sledeće pobijanje:

DOKAZ JE NADJEN

POBIJANJE JE SLEDEĆI NIZ SASTAVAKA:

CENTRALNI SASTAVAK:

$P(C)$※

BOČNI SASTAVAK:

$P(0)$※

INDUKCIJSKA ZAMENA:(nou):

※ (prazna)

CENTRALNI SASTAVAK:

$P(S(G1))$※

BOČNI SASTAVAK:

$\neg P(X) P(S(X))$※

REZOLUCIJSKA ZAMENA (nou):

G1/X※

CENTRALNI SASTAVAK:

$\neg P(S(G1)) \neg P(G1)$※

ČNI SASTAVAK:
(Gl)*
EZOLUCIJSKA ZAMENA (nou):
    * (prazna)
ENTRALNI SASTAVAK:
RAZAN SASTAVAK
KAZ JE ODŠTAMPAN
KAZANA JE NEZADOVOLJIVOST POLAZNOG SKUPA

omentar: Svaki sledeći centralni sastavak je rezultat primene avila rezolucije ili pravila binarne indukcije na prethodne - ntralni i bočni sastavak. Simbol * označava kraj niza koji edstavlja sastavak ili zamenu. U procesu pobijanja simbol dis- nkcije se ne koristi, pa su sastavci predstavljeni samo litera- ma u nizu. Simbol: / ispred literala u sastavku znači da je edeći literal markiran.

imer 2. Dokaz $\forall x(0+x=x)$ pobijanjem iz $\forall x(x+0=x)$ i
$\forall x(0+x=x \Rightarrow 0+Sx=Sx)$ .

lazni skup sačinjavaju sastavci:
+0=x ; $0+x\neq x \vee 0+Sx=Sx$ ; $0+a\neq a$
azni podaci su:
D=0 ; M=1 ; N=3 ; JMAX=4 ; LMAX=5 ; DMAX=40 ; LITMAX=20 ;
BMAX=5 ; RNVMAX=10 ; K1=13 ; K2=55 ; KRMAX=200 ; AKSMAX=120 ;
z KN sadrži 13 članova:
=(+(0,a),a)*
z AKS sadrži 55 članova:
+(x,0),x)*¬=(+(0,x),x)=(+(0,S(x)),S(x))*¬=(+(0,a),a)*

računaru PDP 11/34 dobijeno je sledeće pobijanje:

KAZ JE NADJEN
BIJANJE JE SLEDEĆI NIZ SASTAVAKA:
NTRALNI SASTAVAK:
(+(0,a),a)*
ČNI SASTAVAK:
+(x,0),x)*
DUKCIJSKA ZAMENA:
x*

```
CENTRALNI SASTAVAK:
¬=(+(0,S(Gl)),S(Gl))*
BOČNI SASTAVAK:
¬=(+(0,x),x)=(+(0,S(x)),S(x))*
REZOLUCIJSKA ZAMENA:
Gl/x*
CENTRALNI SASTAVAK:
/¬=(+(0,S(Gl)),S(Gl))¬=(+(0,Gl),Gl)*
BOČNI SASTAVAK:
=(+(0,Gl),Gl)*
REZOLUCIJSKA ZAMENA:
     * (prazna)
CENTRALNI SASTAVAK:
PRAZAN SASTAVAK
DOKAZ JE ODŠTAMPAN
DOKAZANA JE NEZADOVOLJIVOST POLAZNOG SKUPA
```

Videti komentar uz primer 1.

Kao što je već naglašeno, jednostavnost prvih test-primera uslovljena je malim kapacitetom slobodnog dela operativne memorije korišćenog računara.
U okviru Sistema "Graph" na računaru veće snage, uz korišćenje spoljašnje memorije, mogu se očekivati dokazi i složenijih teorema.

# BIBLIOGRAFIJA


1. Abrahams P. , Machine Verification of Mathematical Proof, doc.dis.Dept. of Math, MIT,Cambridge,Mass, 1963.
2. Achcroft E.A.,Wadge W.W. , LUCID - a formal System for writing and proving programs. SIAM J.Comp.5 N°3,336-354, 1976.
3. Aleksandrov E.A. , Osnovi teorii evrističeskih rešenij, "Sov. radio" Moskva 1975.
4. Allen J.,Lucham D., An Interactive Theorem-Proving Program. "Machine Intelligence" 5 , 321-336, New York 1970.
5. Amarel S., An Approach to Heuristic Problem-Solving and Theorem Proving in the Propositional Calculus. "Sistems and Computer Science", Toronto 1967.
6. Amosov N.M., K voprosu ob algoritme intellekta i ego evolucii. Kibernetika, No 2, 49-56, Kiev 1979.
7. Anderson R.,Bledsoe W., A Linear Format for Resolution with Merging and a New Technique for Establishing Completeness. J. ACM. 17, No 3, 1970.
8. Anderson R., Completeness results for E-resolution. Proc. of the AFIPS, SJCC, pp 653-656, 1970.
9. Anufriev F.V. i dr., Ob odnom algoritme poiska dokazateljstv v teorii grupp. Kibernetika No 1, Kiev 1966.
0. Anufriev F.V., Algoritm poiska dokazateljstv v teorii množestv. Sb."Teorija avtomatov" vip.4, IKAN USSR, Kiev 1967.
1. Anufriev F.V., Algoritm poiska dokazateljstv teorem v logičeskih isčislenijah. Sb."Teorija avtomatov"vip.5,IKANUSSR 1969.
2. Anufriev F.V.,Kostjakov V.M.,Malašonok A.I., Algoritm i mašinij eksperiment poiska dokazateljstv teorem v isčislenii viskazivanij. Kibernetika No 5, 68-73, Kiev 1972.
3. Anufriev F.V.,Aseljderov Z.M., Algoritm očevidnosti. Kibernetika No 5, 29-60, Kiev 1972.
4. Aseljderov Z.M.,Anufriev F.V.,Kapitanova J.V., Organizacija dannih dlja algoritma očevidnosti v poiske dokazateljstv teorem v formalizovannih teorijah. Kibernetika No 5,61-67, Kiev 1972.

15. Aubin Raymond , Mechanizing structural induction I,II. Theoret. Comput.Sci.9,No 3, 329-362, 1979.
16. Banerji,Ranan B., Artificial intelligence (A theoretical approach), North-Holland,New York-Oxford 1980.
17. Bledsoe W.W., Splitting and Reduction Heuristics in Automatic theorem Proving. Artificial Intelligence 2,No 1,55-77,1971.
18. Bledsoe W.W.,Boyer R.S.,Henneman W.H., Computer Proofs of Limit Theorems. Artificial Intelligence 3,No 1,27-60, 1972.
19. Bledsoe W.W.,Bruell P. , A Man-Machine Theorem-Proving Sistem. Artificial Intelligence 5, 51-72, 1974.
20. Bublik V.V., Obobščennaja strukturnaja indukcija. Kibernetika No 3, Kiev 1977.
21. Buzurkanov V.,Abdullasova M.,Kasimov N.H., Ob odnom podhode k realizacii metoda rezolucii. "Vopr.vičisl.i prikl.mat." No 65, 149-157, Taškent 1981.
22. Ceitin G.S., O složnosti vivoda v isčislenii viskazivanij. Zap.nauč.seminarov LOMI ANSSSR, t.8.,1968.
23. Chang C.L., Renamable Paramodulation for Automatic Theorem Proving with Equality. Artificial Intelligence 1,247-256,1970.
24. Chang C.L.,Slagle J.R., Completness of Linear Refutation for Theories with Equality. J.ACM 18, 126-136 , 1971.
25. Chang C.,Lee R., Simbolic Logic and Mechanical Theorem Proving. Academical Press, New York-London 1973.
26. Churh A., Introduction to Mathematical Logic,I,Princeton 1956. Ruski prevod IL Moskva 1961.
27. Cook S.A., Soundness and Completeness of on Axiom Sistem for Program Verification."SIAM J.on Comp."v.7,No 1, 1978.
28. Cvetković D., A project for using computers in further development of graph theory. Proc.of the 4-th Internat.Conf. on the Theory and Appl. of Graphs, Kalamazoo 1980,Wiley 1981 .
29. Cvetković D.M.,Kraus L.L.,Simić S.K., Discussing graph theory with a computer. I Implementation of graph theoretical algorithms. "Publ.Elektrotehn.fak.Univ.Beograd.Ser.mat.fiz.",1981.
30. Cvetković D.,Prevodjenje matematičkog teksta na jezik formula kvantifikatorskog računa pomoću računara, Beograd 1981.
31. Cvetković D.,Pevac I., Interaktivni dokazivač teorema,(saopštenje). Beograd 1982.

2 . Darlington J.L., Automatic Theorem Proving with Equaliti Substitutions and Mathematical Induction. "Machine Intelligence 3", Michie D.(ed.), Edinburgh Univ.Press,113-127,1968.
3. Darlington J.L., Theorem Provers as Question Ansverers. Proc.Intern.Joint Conf.Artificial Intelligence 1969.
4. Davis M.,Putnam H., A Computing Procedure for Quantification Theory. J.ACM 7, no 3, 201-215, 196o.
5. Davis M., Elimination the Irrelevant From Mechanical Proofs. Proc.of the Fefteenth Simp.in Applied Math. of American Math. Siety., 15-30, 1963. Ruski pr. u Kibernetičeskij sb. 7, 1970.
6. Davis M.,Schwark J.T., Mathematical extensibility for theorem verifiers and proof checkers. Comput.Math. Appl.5,no 3, 1979.
7. Davidov G.V. , Sintez metoda rezoljucij s obratnim metodom. "Zap.nauč.semin.Lenjingradskogo otdel.Mat.in-ta ANSSSR" 20, Lenjingrad 1971.
8. Dell'orco Pietro, A syntactic approach to automatic theorem proving. "APL Congr 1973", Amsterdam a.a.,75-82, 1973.
9. Devide V., Matematička logika (Ideo).Posebno izd.Mat.in-ta Beograd 1972.
0. Ehrenfeucht A.,Orlowska E., Mehanical Proof Procedure for Propositional Calculus. Bull.Acad.Polon.Sci.Ser. "Math., Astronom.,Fhys." 15, no 1, 25-30, 1967.
1. Evans T., A Heuristic Program to Solve Geometric Analogy Problems. Proc.AFIPS Ann.Spring Joint Computer Conf., 327-338, 1964.
2. Evans T., A Program for the Solution of a Class of Geometrie-Analogy Intelligence - Test Questions. "Semantic information processing", 271-353, 1968.
3. Fiby R.,Sokol J.,Sudolsky M, Efficient resolution theorem proving in the propositional logic. CL&CL-Comput Linquist. Comput.Lang. 13, 1979.
4. Fikes R.E.,Nilson N.J., STRIPS: A New Approach to the Application Theorem Proving to Problem Solving. II Intern.Joint Conf.Artif.Intell. The British Comput.Soc.,608-619,London 971. Ruski prevod u "Integraljnije roboti", Mir 1973.

45. Gallaire H., Controle de la deduction et retour arriere intelligent en resolution de problemes. "Inf.Logical et math. Appl. et implications Actes Congr.FCET,Nancy 1980", S.I., 4-14, 1980.
46. Gerlernter H., Realisation of a Geometry Theorem proving Machine. Proc.Intern.Conf. Informat.Processing, 1959.
47. Gerlernter H.,Hansen J.R.,Loveland D.W., Empirical Explora tion of the Geometry Theorem Machine. Proc.Western Joint Comput.Conf., 143-147, 1960.
48. Gerlernter H., Realisation of a Geometry Theorem-proving Machine. Proc.Internat.Proc.,273-282, UNESCO Hous,Paris1969.
49. Gentzen G., Untersuchungen über das Logische Schliessen. Math.Z. 39, 176-210, 405-431, 1934.
50. Gilmore P.C., A proof Method for Quantification Theory: Its Justification and Realization. IBM J.Res.Develop,28-35,1960.
51. Gindinkin S.G., Algebra logiki v zadačah."Nauka"Moskva 1972.
52. Gladun V.P.,Vaščenko N.D., Metodi formirovanija ponjatij na CVM. Kibernetika no 2, Kiev 1975.
53. Gluškov V.M.,Kapitanova J.V. i dr., K postroeniju praktiče-skogo formaljnogo jazika dlja zapisi matematičeskih teorij. Kibernetika no 5, Kiev 1972.
54. Gluškov V.M.,Kapitanova J.V., Avtomatizacija poiska dokaza-teljstv teorem matematičeskih teorij i intellektualjnije ma šini. Kibernetika no 5, Kiev 1972.
55. Gluškov V.M., Teorema o nepolnote formaljnih teorij s pozi-cij programista. Kibernetika no 2,1-5, Kiev 1979.
56. Green C.C.,Raphael B., The Use Theorem-Proving Techniques in Question-Answering Systems. Proc.MCM 23 rd Nath.Conf. Bran-don System Press, Princeton, New Jersey, 169-181, 1968.
57. Green C.C., Theorem-proving by Resolution as a Basis for Question-Answering Sistems. "Machine Intelligence 4", 183-205, New York 1969.

58. Green C.C., Application of Theorem-proving to Problem Solving. In Proc.Intern.Jount Conf.Artificial Intelligence, Walker and Norton (eds.), 219-239 , Washington 1969.
59. Gross M.,Lanten A., Teorija formaljnih grammatik. "Mir", Moskva 1971.
60. Guard J.R.,Oglesbi F.C.,Bennett J.H.,Settle L.G., Semi-automated Mathematics. J.ACM 16, no 1, 49-62, 1969.
61. Hant E., Iskusstvenij intellekt. Pr.sa engl."Mir"Moskva 1978.
62. Harrison,Malcom,Rubin,Norman, Another generalization of resolution. "J.Assoc.Comput Mach" no 3, 341-351, 1978.
63. Hennessy,Matthew C.B., A proof system for the first-order relation calculus. J.Comp.Syst.Sci.20, 96-110, 1980.
64. Henschen L.,Wos L., Unit refutations and Horn sets. J.ACM 21, no 4, 590-605, 1974.
65. Henschen L., A Theorem-Proving Lanquage for Experimentation. Comm.ACM 17,no 6, 308-314, 1974.
66. Hewitt C., Planer:A Language for Proving Theorems in Robots. Int.Joint Conf.Artif.Intell.,295-301, Washington 1969.
67. Hilbert D.,Bernays P., Grundlagen der Mathematik. Ruski prevod: "Nauka" Moskva 1979.
68. Hintikka J.,Suppes P., Aspects of Inductive Logic. North Holland Publ.Co., Amsterdam 1966.
69. Hintikka J.,Niiniluoto I., An axiomatic foundation for the logic of inductive generalization. Formal methods in the methodology of empirical sciences. (Proc.Conf.Wasav 1974), 57-81, Synthese Library 103. Reidel, Dordrecht 1976.
70. Hotomski P., Odin sposob otiskanija značenij formul isčislenija viskazivanij. Matematički vesnik 12(27), Beograd 1975.
71. Jablonski S.V., Funkcionaljnije postroenija v k-značnoj logike. Trudi mat. in-ta V.A.Steklova, t.51, AN SSSR 1958.
72. Jablonski S.V.,Ljapunov O.B.(redaktori), Diskretnaja matematika i matematičeskije voprosi kibernetiki."Nauka"M.1974.
73. Jablonski S.V., Vvedenije v diskretnuju matematiku."Nauka" Moskva 1979.
74. Jovanović G., magistarski rad, PMF Beograd 1981.

75. Kanger S. , Uproščenij metod dokazateljstva dlja elementarnoj logiki. Sb. "Matem.teorija log.vivoda",Nauka Moskva 1967.
76. Kapetanović M.,Mijajlović Ž., Modeli aritmetike - pregled osnovnih rezultata. Seminar za konstruktivnu matematiku i teoriju modela "Beograd-Zagreb",Beograd juna 1979.(rukopis).
77. Kapitanova J.V. i dr., Kratkij obzor i bibliografija rabot po avtomatizacii poiska dokazateljstv teorem v formaljnih teorijah. Kibernetika no 5, Kiev 1972.
78. Kellerman E., Unification Algorithm for Theorem Proving. "IBM Technical Disclosure Bull" 13, 3533-3536,April 1971.
79. Kibner E.V., On a theory of inductive inference. Fund. of Comp. Theory (Proc.Int.Conf.Poznan-Kornik 1977),435-440, Berlin 1977.
80. King J.,Floyd R.W., Interpretation Oriented Theorem Prower over Integers. "II ACM Simp.on Theory of Comp."Northampton 70.
81. Kirsanov G.M.,Cejtlin G.E.,Juščenko E.L., Analist - paket program dlja dokazateljstva toždestv (teorem) v aksiomatizirovannih SAA. Kibernetika no 4, 1979.
82. Kleene S.C., Mathematical Logic. John Wiley and Sons,Inc, New York-London-Sydney 1967. Ruski prev."Mir" Moskva 1973.
83. Kleščev A.S., Predstavlenije znanij- metodologija i formalizmi. Dalekovostočnij naučnij centr AN SSSR.Prepr.no 21,42,1981.
84. Korotkova M.A.,Popov S.V., Čeredničenko N.D., Programa poiska vivoda. Prepr.no 54(77).Inst.prikl.mat.ANSSSR 36,Moskva 1977.
85. Kowalski R.,Hayes P.J., Semantic Trees in Automatic Theorem Proving. "Machine Intelligence 4",87-101,New York 1969.
86. Kowalski R., Search Strategies for Theorem-Proving. "Machine Intelligence 5",181-201,New York 1969.
87. Kowalski R., And-or Graphs, Theorem-proving Graphs and Bi-Directional Search."Machine Intell.7",167-194,New York 1972.
88. Kowalski R., Studies in the Completeness and Efficiency of Theorem-Proving by Resolution. Doc.Thesis. Univer. of Edinburgh 1970.
89. Kowalski R.,Kuchner D., Linear Resolution with Selection Function. Artificial Intelligence 2, 227-260, 1971.

90. Koževnikova G.P.,Stognij A.A., Predstavlenije analitičeskih viraženij pri vipolnenii na CVM formuljnih preobrazovanij. Kibernetika no 4, Kiev 1975.
91. Krupko N.A., Ob odnoj avtomatičeskoj sisteme logičeskogo vivoda. Programmirovanije ž.AN SSSR no 3, 28-40, 1978.
92. Kurjerov J.N., Taktika vzaimnogo pogloščenija i ee normaljnaja forma. Kibernetika no 6, Kiev 1979.
93. Lakatos I., Dokazateljstva i oproverženija."Nauka"Moskva 1967.
94. Lee R.Char-tung, A Completness Theorem and a Computer Program for Finding Theorems Derivable from Given Axioms". Doc.diss. Univ. of California, Berkley 1967.
95. Lee R.C.T., Fuzzy Logic and the Resolution Principle. Jour. ACM 19, 109-119, 1972.
96. Levitan G.I., Primenenije deduktivnogo vivoda v sistemah situacionogo upravlenija. Tehničeskaja kibernetika ž. AN SSSR no 1, 1977.
97. Lifšic V.A., Normaljnaja forma dlja vivodov v isčislenii predikatov s ravenstvom i funkcionaljnimi simvolami. "Zap.nauč.seminarov" t.4, LOMI, Lenjingrad 1967.
98. Lifšic V.A., Specijalizacija formi vivodov v isčislenii predikatov s ravenstvom. Trudi Mat in-ta ANSSSR XCVIII,M-L.,1968.
99. Logičeskij vivod. AN SSSR, "Nauka" Moskva 1979.
100. Loveland D.W., Theorem-Provers Combining Model Elimination and Resolution. "Machine Intelligence 4",73-86, 1969.
101. Loveland D.W., A Unifying View of Some Linear Herbrand Procedures. J. ACM 19, 366-384, 1972.
102. Loveland D.W., Automated theorem proving: a logical basis. N.Holl.Publ.Co. XIV , Amsterdam 1978.
103. Luckham D., The Resolution Principle in Theorem-Proving. "Machine Intelligence 1", 47-61, 1967.
104. Luckham D., Refinement Theorems in Resolution Theory. Simp. on Automatic Demonstration, Lecture Notes on Mathematics no 125, Springer-verlag, Berlin and New York 1970.
105. Luckham D.,Nilsson N.J., Extracting Information from Resolution Proof Trees. Artificial Intelligence 2, 27-54, 1971.

106. Ljalecky A.V., Malašonok A.I., K- disjunkt calculus with a latent clash resolution rule (Russian). Mathematical questi ons of theory of machine intelligence, AN USSR, Instit. Kibernetiki, 3-33, Kiev 1975.

107. Mak-Karti Dž., Programmi vičisliteljnih mašin dlja proverki matematičeskih dokazateljstv. Prev. sa engl. IKAN USSR 1966.

108. Manna Z.,Waldinger R., Towards Automatic Program Synthesis. Commun ACM, 1971.

109. Manna Z., Mathematical Theory of Computation. N.Y.Mc Graw-Hill Book Co, 1974.

110. Manna Z.,Waldinger R., Studies in Automatic Programming Logic. North-Holland, New York-Amsterdam-Oxford 1977.

111. Manna Z.,Waldinger R., The logic of computer programming. IEEE Trans. Software Engrg. 4, no 3, 199-229, 1978.

112. Maslov S.J., Obratnij metod ustanovlenija vivodimosti v klasičeskom isčislenii. "Dokladi ANSSSR" 159,no 1, Moskva 1964.

113. Maslov S.J., Svjaz meždu taktikami obratnogo metoda i metoda rezoljucij. "Zap.nauč.semin." LOMI ANSSSR, 16, Lenjingrad 1969.

114. Maslov S.J.,Mintz G.E.,Orevkov V.P., Mechanical proof-search and the theory of logical deduction in the USSR. Rev.Internat.Philos. 25, no 4, 575-584, 1971.

115. Maslov S.J., Obratnij metod i taktiki ustanovlenija vivodimosti dlja isčislenija s funkcionaljnimi znakami. Trudi Mat. in-ta im. Steklova CXXI,. Moskva-Lenjingrad 1972.

116. Maslov S.J., Norgela S.A., O pravilah tipa sečenija obščego vida. "Zap. nauč.semin." LOMI ANSSSR, 40, Lenjingrad 1974.

117. Maslov S.J., Teorija poiska vivoda i ee primenenija. Kibernetika no 4, Kiev 1975.

118. Maslov S.J., Informacija v isčislenii i racionalizacija pereborov. Kibernetika no 2, Kiev 1979.

119. Martin W.A., Simbolic Mathematical Laboratory. Doct.diss., MIT Cambrigge 1967.

120. Matrosov V.M.,Vasiljev S.N., Princip sravnenija dlja vivoda teorem I i II. Izv.ANSSSR Tehnič.kibernetika no 2,4; 1978.
121. Meltzer B. Theorem-Proving for Computers: Some Results on Resolution and Renaming. Comp.J. 8, 341-343, 1966.
122. Meltzer B., Some Notes on Resolution Strategies. "Machine Intelligence 3", 71-75, New York 1968.
123. Meltzer B., The Semantics of Induction and the Possibility of Complete Systems of Inductive Inference. "Artificial Intell." 1 , 189-192, 1970.
124. Mendelson E., Introduction to Mathematical Logic. D.Van Nostrand Company, Inc, 1964. Ruski pr."Nauka" Moskva 1976.
125. Meyer R.K., Career induction for quantifiers. Notre Dame J. Formal Logic 21, no 3, 539-548, 1980.
126. Miller F.A., Improving Heuristic Regression Analysis. Presented at the 6-th Annual Southeastern Regional Meeting of the ACM. Chapel Hill, North Caroline, June 1967.
127. Minker J.,Fishman D.H.,Mc Skimin J.R., The $Q^{*}$ Algorithm - A Search Strategy for a Deductive Question-Answering System. Artificial Intelligence 4, 225-243 , 1973.
128. Minker J. i dr., MRPPS -An Interactive Refutation Proof Procedure System for Question-Answering. Internat. J. of Computer and Information Sciences 3, no 2, 105-122, 1974.
129. Minsky M., Steps Toward Artificial Intelligence. Proc.IRE,49, 8-30, 1961. Ruski pr. u knj."Vičisliteljnije mašini i mišljenije", "Mir" Moskva 1967.
130. Minsky M., Semantic Information Processing. Cambridge 1968.
131. Minc G.E., Varirovanije faktik poiska vivoda v sekvencijalnih isčislenijah. "Zap.nauč.semin." LOMI AN SSSR 4, 1967.
132. Minc G.E., Teorija dokazateljstv. Arifmetika i analiz. Lenjingrad 1975.
133. Minc G.E., Finitnoe issledovanije transfinitnih vivodov. "Zap.nauč. semin." LOMI AN SSSR 49, Lenjingrad 1975.
134. Mitrinović D.S., Indukcija.Binomna formula.Kombinatorika. "Mat.biblioteka",Zavod za izd.udžb.SRS Beograd 1970.

135. Mogilevskij G.L., Ostrouhov D.A., K mehaničeskomu isčisleniju viskazivanij s ispoljzovanijem analitičeskih tablic Šmuljana. Kibernetika,no 4, Kiev 1978.
136. Morris J.B., E-resolution: Extension of Resolution to Include the Equality Relation. Intern.Joint Conf. on Artif. Intelligence, Washington D.C. 1969.
137. Morris J.B., Another recursion induction principle. Comm. ACM 14, 351-354, 1971.
138. Moses J., Symbolic Integration. MAC-TR-47, Project MAC,MIT, Cambridge 1967.
139. Nevins A.J., A Human Oriented Logic for Automatic Theorem Proving. J. ACM 21, no 4, 606-621, 1974.
140. New ll A.,Shaw J.,Simon H., Empirical Explorations of the Logic Theory Machine. Proc.West.Joint Comp.Conf. 1957.
141. Newell A., Shaw J.,Simon H., A General Problem-Solving Prog ram for a Computer."Computer and Automation"v.8,no 7,1959.
142. Njuel A.,Saimon G., GPS-programma mod lirujuščaja proces čelovečeskogo mišlenija. Sb."Vičisl.mašini i mišlenije", "Mir" Moskva 1967.
143. Nilson N.J., Iskusstvennij intellekt - metodi poiska rešenij. Prevod sa engleskog "Mir" Moskva 1973.
144. Nilsson N.J., A production system for automatic deduction. Machine Intelligence, Vol 9, 101-126, Horwood Chichester 1979.
145. Nilsson N.J., Principles of artificial intelligence. Tioga Publishing Co., Palo Alto, Calif. 1980.
146. Norton L.W., Experiments with a Heuristic Theorem Proving Program for Predicate Calculus with Equality. "Artificial Intelligence 2", 261-284, 1971.
147. Oshiba Takeshi, A method for obtaining proof figures of valid formulas in the first order predicate calculus. "Comment math.Univ.St.Pauli" 30, no 1,49-62, 1981.
148. Overbeek R.A.,Lusk E.L., Data structures and control architecture for implementation of theorem proving programs. "Lect. Notes Comp. Sci" 87, 232-249 , 1980.

149. Parezanović N., Algoritmi i programski jezik FORTRAN IV. Matematički institut Beograd 1972.
150. Paterson M.S., Wegman M.N., Linear Unification. J.Comp.System.Sci. 16, no 2, 158-167, 1978.
151. Peterson J.G., An automatic theorem prover for substitution and detachment systems. Notre Dame,J.Formal Logic 19,no 1, 119-122, 1978.
152. Petrov J.A., Matematičeskaja logika i materijalističeskaja dialektika. Izd. Moskovskogo univ. 1974.
153. Plotkin G.P., A Note on Inductive Generalization. "Machine Intelligence 5", 153-164, 1969.
154. Plotkin G.P., A Further Note on Inductive Generalization. "Machine Intelligence 6", 101-124, 1971.
155. Pljuškevičene A.J., O specijalizacii ispoljzovanija aksiom pri poiske vivoda v aksiomatičeskih teorijah s ravenstvom. "Zap.nauč.semin." Izd Mat.In-ta im.Steklova,Lenjingrad 1971.
156. Pogosjan E.M., Obučenije kak raznovidnost induktivnogo vivoda. Tehničeskaja kibernetika IAN SSSR no 3, 1978.
157. Poplsestone R.J., An Experiment in Automatic Induction. Machine Intelligence 5 , 203-216, 1969.
158. Popov E.V.,Firdman G.R., Algoritmičeskije osnovi intellektualjnih robotov i iskusstvennogo intellekta."Nauka" Moskva 1976.
159. Pospelov D.A.,Puškin V.N., Mišljenije i avtomati. Izd. "Sovetskoje radio", Moskva 1972.
160. Pospelov G.S., Pospelov D.A., Iskusstvennij intellekt: sostojanija i problemi. U Sb."Iskusstvennij intellekt - itogi i perspektivi", materijali seminara MDNTP, 1974.
161. Prawitz D.,Prawitz H.,Voghera N., A mechanical proof procedure and its realization in an electronic computer. J. ACM, Baltimore-New York, v.7, no 2, 196o.
162. Prešić B.S., Elementi matematičke logike. "Mat.biblioteka", Zavod za izd. udžbenika SRS Beograd 1968.
163. Prešić M.,Prešić S., Uvod u matematičku logiku -teorija i zadaci. Matematički institut Beograd 1979.

164. Pšeničnikova S.V. , K modelirovaniju na EVCM poiska dokazateljstv nekotorih teorem analiza. Sb. "Teorija avtȯmatov", vip. 4, izd AN USSR 1969.

165. Quinlan J.R.,Hunt E.B., A Formal Deductive Problem-Solving System. J.ACM 15, 625-646, 1968.

166. Rangaswamy S.V.,Chakrapani N.,Tikekar V.G., A computational algorithm for the verification of tautologies in propositio nal calculus. J.Indian Inst.Sci. 62,no 3, 71-81, 1980.

167. Raseva H.,Sikorskij R., Matematika metamatematiki. "Nauka" Moskva 1972.

168. Reiter R., Two results on Ordering for Resolution with Merging and Linear Format. J. ACM 18, 630-646, 1971.

169. Reiter R., A Semantic Guided Deductive System for Automatic Theorem Proving. Third Internat.Joint.Conf.Artificial Intelli gence, Stanford Univ., 41-46 , 1973.

170. Robinson J.A., A Machine-Oriented Logic Based on the Resolution Principle. J. ACM 12, no 1, 23-41, 1965.
Ruski prevod "Kibernetičeskij sbornik" no 7, Novaja serija, "Mir" Moskva 1970.

171. Robinson J.A., Automatic Deduction with Hyper-Resolution. Intern.J.Comp.Math. 1, 227-234, 1965.

172. Robinson J.A., The Generalized Resolution Principle. "Machine Intelligence 3" New York, 77-94, 1968.

173. Robinson J.A., An Overview of Mechanical Theorem Proving. "Theoretical Approaches to Non-Numerical Problem Solving", 2-20, New York 1970.

174. Robinson G.,Wos L., Paramodulation and Theorem-Proving in First Order Theories with Equality. "Machine Intelligence 4" 135-150, Edinburgh 1969.

175. Robinson G.,Wos L., Completeness of Paramodulation. J. of Simbolic Logic 34, March 1969.

176. Robitašvili N.T., Sovmeščenije obratnogo metoda i metoda rezoljucij. "Soobšč. AN GSSR" 64,no 2, Tbilisi 1971.

177. Ryll-Nardzewski C., The role of the axiom of induction in elementary aritmetic. Fundam.Math. 39, 239-263, 1953.

178. Sickel,Sharon , Variable range restrictions in resolution theorem proving. Machine Intelligence, Vol.8,73-85, Ellis Horwood, Chichester, 1977.

179. Slagle J., A Heuristic Program that Solves Symbolic Integration Problems on Freshman Calculus.J.ACM 10,no 4, 507-520, 1963.

180. Slagle J., Automatic Theorem Proving with Renamable and Semantic Resolution. J.ACM 14, 687-697, 1967.

181. Slagle J.R.,Chang G.L.,Lee R.Č.T., Completeness Theorems for Semantic Resolution in Consequence-Finding. "Proc.Intern. Joint Conf. on Arificial Intelligence", 281-285, 1969.

182. Slagle j.,Koniver D., Finding Resolution Proofs and Using Duplicate Goals in AND-OR Trees. Heuristics Lab.Div. of Computer Res. a Technol., Nat.inst.of Health, Bethesdam Md 1970.

183. Slagle J., Automatic Theorem Proving with Built-in Theories Including Equality, Partial Ordering and Sets.
J. ACM 19,no 1, 120-135, 1972.

184. Slagle J.R.,Norton L.M., Experiments with automatic theorem-prover having partial orderung inference rules.
Communs ACM 16, no 11, 682-688, 1973.

185. Slagle J., Artificial Intelligence: the Heuristic Programing Approach. Mc Graw Hill Book Co. New York 1971.
Ruski prevod "Mir" Moskva 1973.

186. Slagle J.,Norton L., Automated Theorem-proving for the Theories of Partial and Total Ordering. Computer J. 1974.

187. Slagle J.R., Automated Theorem Proving for Theories with Simplifiers, Commutativity and Associativity.
J. ACM 21, no 4, 622-642, 1974.

188. Smirnov V.V., Formaljnij vivod i logičeskie isčislenija.
"Nauka" Moskva 1972.

189. Smullyan R., First-order Logic. Springer-Verlag N.Y., 1968.

190. Solomonoff R.J., A Formal Theory of Inductive Inference.
"Information and Control" 7, no 1-2, 1964.

191. Stojaković M., Algoritmi i automati. Novi Sad 1972.
192. Subje-Kami, Dvoičnaja tehnika i obrabotka informacii. "Mir" Moskva 1964.
193. Šanin N.A. i dr., Algorifm mašinogo poiska estestvenogo logičeskogo vivoda v isčislenii viskazivanij."Nauka"M-L.1965.
194. Šenfild J., Matematičeskaja logika, "Nauka" Moskva 1975.
195. Štedron B., Doing Arithmetic with Resolution. Sctipta Fac.Sci.Natur UJEP Brunensis - Math.8,no 10,63-67,1978.
196. Takeuti G., Proof Theory. North-Holland Publ.Co.N.Y. 1975. Ruski prevod "Mir" Moskva 1978.
197. Tarski A., Uvod u matematičku logiku i metodologiju matematike. Prevod sa engl. "Rad" Beograd 1973.
198. Townley J.A., A pragmatic approach to resolution-based theorem proving. Internat.J.Comput.Inform.Sci.9,no 2, 93-116, 1980.
199. Trahtenbrot B.A., Što su algoritmi.Algoritmi i rač.automati. "Školska knjiga" Zagreb 1978.
200. Turchin V.F., The use of metasystem transition in theorem proving and program optimization. Automata,Lanquages and programing. Lecture Notes in Comput.Sci. 85,Springer, Berlin 1980.
201. Turing A.M., Computer Machinery and Intelligence. Mind 59, 433-460, 1950. Ruski prevod "Fizmatgiz" 1960.
202. Vander Burg Cordon, Minker Jack, Statespace, problem deduction and theorem proving- some relationships. Communs ACM 18, no 2, 107-115, 1975.
203. Voevodin V.V.,Gaisorjan S.S.,Kabanov M.I., Avtomatizirovanaja generacija programm. Sb."Čislenij analiz na FORTRANE" vip. 1, Izd. MGU 1973.
204. Von Henke F.W., Towards automation of proof by induction. Lecture Notes in Comput.Sci. Vol 48, Springer Berlin 1977.
205. Voprosi teorii matematičeskih mašin."Mašinostroenije" M.1964.
206. Waldinger R.J.,Lee C.T., PROW: A Step toward Automatic Program Writing. Proc.Internat.Joint.Conf. Artif.Intell., 1969.
207. Wang Hao, Toward mechanical Mathematics. IBM J.Res.Devel. no 1, 2-22, 1960. Ruski pr. "Kibernet. sb." no 5,Moskva 1962.

208. Wang Hao, Mechanical Mathematics and Inferential Analysis. "Computer Programming and Formal Systems",North Holl.,1963.
209. Wang Hao, Formalization and Axiomatic Theorem Proving. Proc.IFIP Congr. 1965,vol. 1, Spartan Books,Washington 1965.
210. Wang Hao, Logic of Many Sortid Theories. J. of Simbolic Logic V, 17, no 2, 1972.
211. Whitehead A.N., Russel B., Principia Mathematica. 2 d.ed., vol I, Cambridge Univ. Press 1935.
212. Winston P.H., Artificial Intelligence. Addison-Wesley Series in Comp.Sci. Mass-London-Amsterdam 1977.
213. Woodall D.R. , Inductio ad absurdum ? The Mathematical gazette 59, no 408, 64-70, 1975.
214. Wos L.,Robinson G.,Carson D., Efficiency and Completeness of the Set of Support Strategy in Theorem-proving. J. ACM 12, no 4, 536-541, 1965.
215. Wos L.,Robinson G., Paramodulation and Set of Support. Proc.Simp.Automatic Demonstration, Springer-Verlag, 276-310, New York 1970.
216. Yates R.,Raphael B., Hart T., Resolution Graphs. Artificial Intelligence 1, no 4, 1970.
217. Youse B.K., Mathematical induction. Prentice-Hall 1964.
218. Zahar´jaščev M.V.,Popev S.V., A deduction search procedure based on the Syntactic tree method. AN SSSR, Inst.Prikl.Mat. Preprint no 111, pp,51, 1978.
219. Zamov N.K.,Šaronov V.I., Ob odnom klasse strategij, primenjaemih pri ustanovlenii dokazuemosti metodom rezolucii. "Zap.naučč.semin." 16, LOMI, Lenjingrad 1969.
220. Zamov N.K.,Šaronov V.I., Decision strategies for finding the derivation in the resolution method (Russian). Issled. Prikl. Mat., vyp 4, 31-34, 1977.
221. Enciklopedija kibernetiki, t. I i II , Kiev 1975.

# I S P R A V K E

## U DOKTORSKOJ DISERTACIJI HOTOMSKI PETRA

| ana | red | stoji | treba da stoji |
|---|---|---|---|
| 28 | 1 odozdo | A(a) | A(x) |
| 29 | 1 odozgo | konstanta a | slobodna promenljiva x |
| 26 | 17 odozgo | $D=\{ P(a),\ldots\}$ | $D=\{\neg P(a),\ldots\}$ |
| 27 | 6 odozdo | $\Theta'=\{t_1/x_1,\ldots,t_n/x_n\}$ | $\Theta'=\{t_1^{\lambda}/x_1,\ldots,t_n^{\lambda}/x_n\}$ |
| 24 | 16 odozdo | $E_1= P(x) \vee Q(x)$ | $E_1= P(x)$ |
| 28 | 10 odozgo | dikazivanju | dokazivanju |
| 25 | 9 odozdo | $B (x)$ | $B_6(x)$ |
| 23 | 1 odozdo | $\vdash_L F$ | $\vdash_{\mathcal{K}_L} F$ |
| 21 | 12 odozdo | ragistrovanja | registrovanja |
| 28 | 14 odozgo | Ukoliko u nizu KR nema više centralnih sastavaka, prelazi se na nov početni sastavak iz KN (na sledeći nivo). | Ukoliko ukupan broj generisanih sastavaka dostigne RNVMAX ili ako je dostignut granični nivo DUBMAX, prelazi se na nov početni sastavak iz KN. |
| 10 | 16 odozdo | od literala R | od literala L |
| 11 | 5 odozgo | IZVB = 1 | IZVB = 0 |