Univerzitet u Beogradu

Matematički fakultet

STRATEGIJE U PRIMENI REŠAVAJUĆEG PRAVILA

magistarska teza

Beograd 1996

Dragan Kulezić

Mentor : dr Marica Prešić
Univerzitet u Beogradu
Matematički fakultet
Beograd

Članovi komisije : dr Marica Prešić
Univerzitet u Beogradu
Matematički fakultet
Beograd

dr Žarko Mijajlović
Univerzitet u Beogradu
Matematički fakultet
Beograd

dr Nedeljko Parezanović
Univerzitet u Beogradu
Matematički fakultet
Beograd

datum odbrane

MAGISTARSKA TEZA

PREDGOVOR

Ovaj rad predstavlja pokušaj da se na jednom mestu i sistematizovano izlože najvažnije strategije koje se primenjuju u rezolucijskom dokazivanju teorema, kao i da se kombinovanjem nekih strategija dobije nova, čije će se prednosti pokazati na nekim klasama formula.

Rad se sastoji iz šest glava i uvoda koji sadrži istorijski pregled najznačajnijih momenata u mehaničkom dokazivanju teorema, kao i pregled konkretnih računarskih programa i istraživača koji su ih razvijali.

Prva glava je najveća po obimu i sadrži najosnovnije pojmove koji su neophodni u mehaničkom dokazivanju teorema. Ona se sastoji iz devet delova. U prvom delu se uvode definicije atoma, literala, sastavka, jediničnog sastavka i praznog sastavka. Drugi deo se bavi algoritmima pripreme formula, tj. svođenjem formule na Skolemovu standardnu formu. U trećem delu se uvodi pojam Erbranovog prostora, zasićenja, interpretacije i modela, kao i fundamentalna rezolventa i fundamentalna rezolucija. Četvrti deo je posvećen teoremi Erbrana i njenom dokazu. Peti deo se bavi posledicama teoreme Erbrana. Erbranova metoda je metoda opovrgavanja. To znači da se umesto dokazivanja da je neka formula valjana, dokazuje da je njena negacija nezadovoljiva. Zatim se definiše metod zasićenja kao jedan mogući način mehaničke provere nezadovoljivosti. U šestom delu se dokazuje teorema o fundamentalnoj rezoluciji. Sedmi deo se bavi zamenom, kompozicijom zamena i nekim osobinama zamene i kompozicije zamena. U osmom delu se uvodi pojam unifikacije i najopštijeg zajedničkog unifikatora. Navodi se algoritam unifikacije i dokazuje teorema o korektnosti algoritma unifikacije. I na kraju, u devetom delu, uvodi se definicija rezolvente u opštem slučaju, kada sastavci sadrže i promenljive. Dokazana je osnovna lema o komutativnosti rezolucije i zasićenja, a zatim i lema o podizanju koja će kasnije biti mnogo korišćena u dokazima potpunosti najvažnijih strategija.

Druga glava se sastoji iz tri dela. U prvom delu se uvodi pojam strategije i na konkretnom primeru se pokazuje prednost u odnosu na metodu zasićenja nivoa. Drugi deo sadrži pojam literala čistog u skupu sastavaka. Na osnovu teoreme o čistim literalima uvodi se pravilo čistoće, koje predstavlja jednu od taktika pretraživanja. U trećem delu uvode se dve strategije, strategija upijanja i strategija brisanja. Navodi se algoritam upijanja i dokazuje njegova korektnost.. Takođe je dokazana i teorema o upijanju. Navodi se teorema koja karakteriše kada je strategija brisanja potpuna.

Treća glava je posvećena semantičkoj rezoluciji. Ona je podeljena na osam delova. U prvom delu se navodi primer kojim se motiviše potreba za sprečavanjem izvođenja dva identična sastavka. Drugo deo sadrži definiciju semantičke ili PI-rezolucije i definiciju PI-dedukcije. U trećem delu se dokazuje potpunost fundamentalne PI-rezolucije, a zatim i potpunost PI-rezolicije u opštem slučaju. Četvrti deo je posvećen hiperrezoliciji, a peti strategiji pomoćnog skupa, pri čemu je dokazana potpunost strategije pomoćnog skupa. U šestom delu se uvodi uređena rezolucija i uređena rezolventa. Sedmi deo sadrži definiciju uređene semantičke rezolucije, OI-rezolucije, dok se u osmom delu dokazuje nepotpunost OI-rezolucije navođenjem kontraprimera.

Četvrta glava obrađuje Lock-rezoluciji i sastoji se iz tri dela. U prvom delu se uvodi pojam Lock-rezolvente i Lock-dedukcije i na primerima pokazuje uspešnost uvedene strategije. Drugi deo sadrži dokaz potpunosti Lock-rezolucije, prvo za slučaj fundamentalnih sastavaka, a zatim i za opšti slučaj. U trećem delu se pokazuje da se Lock-rezolucija ne može uspešno kombinovati sa strategijom brisanja tautologija, jer se ne dobija potpuna strategija. Kontraprimer 4.7 je pronađen samostalno, dok se kontraprimer 4.8 nalazi u literaturi.

Peta glava obrađuje linearnu rezoluciju i sastoji se iz četiri dela. U prvom delu se definiše linearna rezolucija i linearna dedukcija. Drugi deo se bavi ulaznom i jediničnom rezolucijom. Dokazana je ekvivalentnost te dve rezolucije korišćenjem standardne tehnike dokazivanja za osnovni slučaj, a zatim i za opšti slučaj korišćenjem leme o podizanju. Treći deo je posvećen korišćenju isključenih literala. Uvodi se pojam redukcije, uređenog faktora, uređene rezolvente i uređenje linearne dedukcije (OL-dedukcije), da bi se učetvrtom delu dokazala potpunost OL-rezolucije.

Šesta glava predstavlja delimično samostalan rad. Zato se na njenom početku daje detaljan opis onoga šta je urađeno.

Zahvalnosti

**

ISTORIJSKI PREGLED

0.1. RAZVOJ TEORIJE MEHANIČKOG DOKAZIVANJA TEOREMA

Misao o stvaranju jednog opšteg postupka za rešavanje matematičkih problema javila se dosta rano. Nju najpre srećemo kod nemačkog matematičara LAJBNICA (Leibniz 1648-1716) koji je mnogo radio na formalizaciji jezika i mišljenja. Smatrao je da se može stvoriti logička mašina koja bi umesto nas vršila dokaze koristeći formalizovan jezik. Na žalost, veliki broj Lajbnicovih radova nije publikovan sve do početka ovog veka, tako da je njegov neposredni uticaj bio neznatan.

Dvadesetih godina ovog veka u Hilbertovoj školi se razvijao metod formalizacije. Predložen HILBERTOV PROGRAM zasnivanja matematike i entuzijazam Hilbertovih sledbenika uticali su na intenzivan razvoj aksiomatskog metoda. Tada dolazi do razvijanja teorije dokaza na bazi logičkog jezika razvijenog u radovima Fregea, Peana i Rasela.

1930. god. GEDEL je dokazao teoremu o potpunosti predikatskog računa prema kojoj se skup svih valjanih formula predikatskog računa prvog reda poklapa sa skupom svih izvodljivih formula, tj. predikatski račun je taj logički sistem na osnovu koga je moguće formalizovati matematiku. Ovim je težište interesovanja i istraživanja u oblasti teorije matematičkih dokaza preneseno na predikatski račun.

1930. god. ERBRAN (Herbrand) je u svojoj doktorskoj disertaciji ideji mehanizacije dokazivanja teorema dao realnu osnovu. Uprkos raznolikosti dokaza raznih teorema predikatskog računa prvog reda, definisan je opšti postupak pomoću koga se sve teoreme mogu da proveravaju na isti način. Time je omogućeno da se dokazivanje teorema svede na čisto mehanički rad proveravanja.

Veličina Erbranovog doprinosa je u tome što umesto da se tačnost teoreme proverava pri svakoj interpretaciji, kojih ima beskonačno mnogo, vrši se proveravanje da li je negacija teoreme kontradikcija na jednoj jedinoj interpretaciji koja se uvodi logično i zove se Erbranov prostor. Erbran pokazuje da ako je formula F teorema, tada postoji konačan podskup P Erbranovog prostora u kome je negacija formule F oslobođena od kvantifikatora (u oznaci skolem (-F)) kontradikcija. U slučaju da formula nije teorema traganje za takvim podskupom P se nikada ne bi završilo (jer on ne postoji).

1936. god. ČERČ i TJURING su nezavisno jedan od drugog dokazali neodlučivost predikatskog računa prvog reda. To je ujedno bio negativan odgovor o postojanju opšteg jedinstvenog postupka za rešavanje svih matematičkih problema. To znači, nemoguće je konstruisati algoritam koji bi za svaku formulu predikatskog računa prvog reda dao odgovor da li je ona teorema (valjana) ili nije, i koji bi završio rad posle konačno mnogo koraka, bez obzira da li je formula teorema ili nije.

U početku je ovaj rezultat bio veoma obeshrabrujući za dalji razvoj mehanizacije dokazivanja teorema, jer niko nije želeo da se upusti u traženje takvog opšteg algoritma za koji je dokazano da ne postoji.

Pa dobro, takav univerzalni algoritam ne postoji za predikatski račun prvog reda, ali zašto ne bi postojao za neki njegov deo.

1954. god. Akerman je dokazao postojanje klasa formula predikatskog računa prvog reda kod kojih je problem da li je neka formula iz klase teorema ili nije, odlučiv.

Teorija bi se dalje razvijala u pravcu traženja novih klasa formula koje su odlučive, da nije:

1965. god. JULIJA ROBINSON napravila veliki korak u oblasti dokazivanja teorema. Ona je uvela rešavajuće pravilo (rezoluciju) kao jedino pravilo izvođenja u postupku mehaničkog dokazivanja. Vrednost njene ideje je u tome što je pokazala da se kontradiktornost neke formule ne mora ispitivati redom po nivoima Erbranovog prostora. Rešavajućim postupkom je mnogo povećana efikasnost utvrđivanja kokntradikcije. Julija Robinson je dokazala i potpunost rešavajućeg postupka (metoda rezolucije) u tom smislu, da ako je formula teorema, možemo biti sigurni da ćemo posle izvršavanja konačnog broja koraka doći do potvrdnog odgovora, ali ako nije teorema, postupak se u opštem slučaju nikada ne bi završio. To je u skladu sa Čerč-Tjuringovim rezultatima o semiodlučivosti predikatskog računa prvog reda.

Posle 1965. god. pronađene su mnoge strategije koje poboljšavaju efikasnost rešavajućeg postupka. Veći deo ovog rada će se baviti upravo tim strategijama.

Dajemo sada pregled najznačajnijih strategija.

1965. Strategija pomoćnog skupa (Wos, Robinson i Carson).

1966. Melcerova preimenovana rezolucija.

1965. Robinsonova hiper-rezolucija.

1967. Slagle je predložio semantičku rezoluciju koja objedinjuje prethodne tri.

1971. Boyer-ova Lock-rezolucija.

1970. Linearna rezolucija nezavisno predložena od Lovelanda i Lukhama. Kasnije su data razna poboljšanja linearne rezolucije.

1970. Anderson i Bledsoa.

1971. Reiter.

1972. Loveland.

1971. Kovalski i Kuhner.

0.2.PREGLED RAČUNARSKIH PROGRAMA ZA DOKAZIVANJE TEOREMA

Sa pojavom prvih elektronskih računara stvorena je mogućnost za praktičnu primenu rezultata teorije mehaničkog dokazivanja teorema. Savremena istraživanja iz veštačke inteligencije su počela sa pokušajima Alena Noela, Gerberta Sajmona i Dž. Šoa koji su pisali programe za rešavanje zadataka. Poduhvat nije bio toliko važan sam za sebe, koliko to što je on dao ton mnogim drugim istraživanjima. Metodi programiranja razvijeni u tim radovima počeli su da se koriste u računarskim naukama uopšteno.

1957. god. NOEL i njegove kolege su prvo napravili program logičar-teoretičar (LT) namenjen za dokazivanje teorema u iskaznom računu. Program LT je radio sa rasprostranjenom formulacijom iskaznog računa, ali se ona pokazala krajnje neprimenljivom za pretraživanje izvođenja konkretnih teorema. Praktični rezultati ovog programa bili su skoro neznačajni. Jedino je korišćena metoda imala principijelnu vrednost za formiranje usmerenja koje se zove heurističko programiranje.

Pomoću LT je bilo uspešno dokazano 38 od 52 teoreme II glave knjige Vajtheda i Rasela PRINCIPIA MATEMATICA (PM). Rešenja 12 od 14 nedokazanih teorema nije bilo dovedeno do kraja zbog ograničenja fizičkih mogućnosti računara koji su postojali u to vreme. Preostale dve teoreme su izlazile iz logičkih mogućnosti samog algoritma. U programu je umesto algoritma Britanskog muzeja - tj. algoritma potpunog pretraživanja korišćen heuristički pristup (termin uveden od Poja 1954. god.). Većina matematičkih dokaza se izvodi na osnovu dosetke o karakteru rešenja, a zatim se proverava da li je ta dosetka ispravna. Noel je u stvari uveo niz pravila (tj. programa) za generisanje dosetki i zatim provere njihove upotrebljivosti. Rad Noela je podvrgnut kritici na osnovu toga što postoje efektivniji metodi potpunog pretraživanja nego algoritam Britanskog muzeja i da korišćenje savremenijih od njih može dati bolje rezultate.

1958. god. HAD WANG je napisao program (1960. god. je izašao članak) pomoću kojeg je dokazao skoro sve teoreme iz PRINCIPIA MATEMATIKA. Više od 200 teorema iz prvih pet poglavlja je dokazano za 37 min. od toga je oko 34 min. utrošeno na rad ulazno-izlaznih uređaja tako da je efektivno vreme (procesorsko vreme) iznosilo oko 3 min. Teoreme predikatskog računa sa jednakošću koje su zastupljene u sledećih pet poglavlja, oko 150 teorema, računar je dokazao za manje od jednog sata.

1963. god. STEFERUD je modifikovao program logičar-teoretičar i na moćnijem računaru dokazao sve 52 teoreme iz Principia matematica.

Algoritmi provere teoreme iskaznog računa nisu više interesantni. Jedino su in teresantni algoritmi izvođenja za neke račune koji su neodlučivi.

Među prvim programima koji dokazuju teoreme na jeziku predikatskog računa prvog reda imamo sledeće programe:

1960. god. GILMOR je napisao program koji se zasniva na Erbranovoj metodi zasićenja nivoa. Program je realizovan na računaru IBM-704. (Oznaka 704 računar je dobio jer je u njegovoj realizaciji učestvovalo tačno 704 saradnika). Program je dokazivao većinom elementarne teoreme. Davis /2/ npr. navodi da nije mogao da dokaže sledeću teoremu:

$$(\exists x)(\exists y)(\forall z)\{[F(x,y)\Rightarrow(F(y,z)\wedge F(z,z)]\wedge [F(x,y)\wedge G(x,y))\Rightarrow(G(x,z)\wedge G(z,z))\}$$

1960. god. PRAVIC je dao proceduru koja je uspešnija od procedure Gilmora.

1960. god. DAVIS i PATNAM poboljšavaju metod Gilmora. Kasnije 1963. god. daju novu metodu koja je znatno uspešnija. Na kraju rada saopštavaju: Procedura dokazivanja zasnovana na ovim idejama sada se programira na računaru IBM 7090 laboratorije kompanije Bell-telephone.

1962. Mc.CARTI je dao jezik za obradu spiskova LISP. Napisao je program na Lispu za dokazivanje teorema za računar IBM 7090.

1963. god. ABRAMS je sastavio program za proveru matematičkih dokaza na jeziku predikatskog računa. Program je u dokazima nekih od 63 teoreme u Principia Matematica otkrio nekorektnosti koje je Abrams uspeo da otkloni. Za proveru jedne teoreme bilo je potrebno u proseku 17 sec.

Kada je u radu Julije Robinskon formulisano pravilo rezolucije, otvoren je put ka moćnijim programima.

1967. god. CHANG i LEE su koristeći metod rezolucije (rešavajuće pravilo) napisali program za izvođenje posledica datog skupa aksioma. Centralno mesto u njemu zauzima kriterijum interesantnosti posledica. U njihovoj knjizi (73. god.) je dat listing programa koji je pisan na jeziku LISP. Interesantno je da je program pisan za korišćenje jedne strategije koja nije potpuna, ali se pokazala efikasnom.

Od ostalih programa koji koriste metod rezolucije treba spomenuti: 1969. god. program koji su napisali ROBINSON i WOS.

1970. god. program ALENA i LUKHAMA koji je bio korišćen za dokazivanje nekih teorema u teorije grupa.

Ovi programi su dalje usavršavani i varirani od strane niza autora.

Primena metoda rezolucije našla je mesto i u drugim programima koji nisu vezani direktno za dokazivanje matematičkih teorema. To su prvenstveno:

Programi za VOĐENJE DIJALOGA, Grina i Rafaela 1968. god. i Grina 1969.god.

PROVERA KOREKTNOSTI PROGRAMA, autora Zohar Mana.

AUTOMATSKO PROGRAMIRANJE, formalni sistem LUCID 1976.god. autora AKROFTA koji je namenjen za pisanje i proveru programa.

1. TEORIJSKI UVOD

1.1 UVODNI POJMOVI

Za formalni opis metoda koriste se oznake PREDIKATSKOG RAČUNA PRVOG REDA.

AZBUKU predikatskog računa prvog reda čine sledeći simboli:

KONSTANTE kojih ima prebrojivo mnogo i za koje dogovorno uzimamo: a, b, c, d, a_1, b_1, c_1, d_1, ...

PROMENLJIVE kojih ima prebrojivo mnogo i za koje dogovorno uzimamo: x, y, z, u, v, w, x_1, y_1, z_1,...

FUNKCIJSKI SIMBOLI dužine n ($n \geq 0$) za koje dogovorno uzimamo: f_i^n, g_j^n, h_k^n ,... (i, j, k= 0,1,2,...). Za n=0 izostavljamo donji indeks. Gornji indeks predstavlja dužinu funkcijskog simbola i biće izostavljen u onim slučajevima kada nema opasnosti od zabune. Često je podesno konstante smatrati funkcijskim simbolima dužine nula.

PREDIKATSKI (RELACIJSKI) SIMBOLI dužine n ($n \geq 0$) za koje dogovorno uzimamo: P_i^n, Q_j^n, R_k^n ,... (i, j, k= 0,1,2,...). I ovde će indeksi, i donji i gornji biti izostavljeni ako nema opasnosti od zabune. Iskazna slova su relacijski simboli dužine nula.

Sedam logičkih simbola za : negaciju, konjunkciju, disjunkciju, implikaciju, ekvivalenciju, univerzalni kvantor i egzistencijalni kvantor:

-, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$.

Četiri pomoćna simbola: leva, desna zagrada, zapeta i tačka: ( ) , . .

Definicije terma, elementarne formule i formule su uobičajene. Za formule koje imaju poseban oblik uvode se novi nazivi.

DEF 1.1 ATOM, LITERAL, IZRAZ, SASTAVAK, JEDINIČNI SASTAVAK, PRAZAN SASTAVAK.

ATOM (tj. atomna formula) je elementarna predikatska formula, tj. niz simbola koji se sastoji od simbola n-arnog predikata ($n \geq 0$) čiji su argumenti termi. LITERAL je atom ili njegova negacija. IZRAZI su termi ili literali. SASTAVAK je disjunkcija konačno mnogo literala.. Sastavak koji sadrži samo jedan literal zove se JEDINIČNI SASTAVAK. Prazna reč je PRAZAN SASTAVAK i označava se sa NIL

Raspored literala u sastavku je nebitan za njegovu istinitosnu vrednost (zbog zakona komutativnosti i asocijativnosti za disjunkciju). Ako se u sastavku pojavljuje više puta jedan isti literal, svako pojavljivanje sem prvog može se izostaviti (zbog zakona idempotencije za disjunkciju). Zato je sastavak određen skupom svojih literala.

DEF 1.2 KOMPLEMENTARNI LITERALI.

Ako je A atom, onda se dva literala A i -A nazivaju komplementarni literali (dopunjujući literali) i obrazuju u proizvoljnom poredku komplementaran par.

Od značaja su literali i sastavci koji ne sadrže promenljive, pa su uvedeni i nazivi za njih.

DEF 1.3 FUNDAMENTALNI ATOMI, FUNDAMENTALNI LITERALI, FUNDAMENTALAN SASTAVAK.
FUNDAMENTALNI ATOMI i FUNDAMENTALNI LITERALI (literali na osnovnom nivou) su oni atomi i literali koji ne sadrže promenljive. FUNDAMENTALNI SASTAVAK je sastavak čiji su svi članovi fundamentalni literali. Specijalno, prazan sastavak je fundamntalni literal (jer ne sadrži promenljive), a i fundamentalni sastavak.

1.2 ALGORITMI PRIPREME FORMULE

U daljem radu se koriste formule svedene na konjunktivnu normalnu formu bez kvantifikatora.

DEF 1.4 SKOLEMOVA STANDARDNA FORMA.
Formula F predikatskog računa prvog reda je u SKOLEMOVOJ STANDARDNOJ FORMI ako je ona oblika:
$(\forall X_1)\ (\forall X_2)\ \ldots(\forall X_n)\ (C_1 \wedge C_2 \wedge \ldots \wedge C_k)$
gde je svaki C_i sastavak $(1 \leq i \leq j)$ i $X_1, X_2, \ldots, X_n$ su sve različite promenljive koje se pojavljuju u sastavcima C_i. Niz $(\forall X_1)\ (\forall X_2) \ldots (\forall X_n)$ zove se PREFIKS a $C_1 \wedge C_2 \wedge \ldots \wedge C_k$ TELO FORMULE F.

Svaka formula predikatskog računa prvog reda može se transformisati u formulu koja je u Skolemovoj standardnoj formi primenom niza jednostavnih transformacija. Za to se koriste algoritmi pripreme formule. Dati algoritam sadrži korake 1-8 koji su opisani po redu izvršavanja. Svaki korak treba izvršavati sve dotle dok je to moguće. kad dati korak ne možemo više primeniti, prelazimo na sledeći.

ALGORITAM 1.4. ALGORITAM PRIPREME FORMULE.

ULAZ: Zatvorena formula F predikatskog računa prvog reda.

IZLAZ: Sastavci $C_1, \ldots, C_m$ bez kvantifikatora, ali sa novim funkcijskim simbolima.

Korak 1. Oslobađanje formule od implikacije i ekvivalencije. Svaki put kada se naiđe na implikaciju i ekvivalenciju treba izvršiti zamenu:

$A \Rightarrow B$ zameniti sa $-A \vee B$

$A \Leftrightarrow B$ zameniti sa $(A \wedge B) \vee (-A \wedge -B)$

Korak 2. Uvođenje negacije u formulu.
Gde god je moguće izvršiti zamene:

$-(A \wedge B)$ sa $-A \vee -B$

$-(A \vee B)$ sa $-A \wedge -B$

$-(\forall X)\ A$ sa $(\exists X)\ -A$

$-(\exists X)\ A$ sa $(\forall X)\ -A$

$\neg\neg A$ sa A.

Primenom ovih koraka dobija se formula kod koje se svaka negacija nalazi neposredno ispred atomne formule.

Korak 3. Preimenovanje promenljivih.

Eliminisati u F sve suvišne kvantifikatore. To znači eliminisati svaki kvantifikator $(\forall X_i)$ ili $(\exists X_i)$ u čijoj oblasti dejstva nema proneljive X_i. Promeniti imena promenljivih tako da u celoj formuli nema ni jedne koja je istovremeno i uz egzistencijalni i uz univerzalni kvantifikator, menjajući i imena odgovarajućih promenljivih koje su u polju dejstva tog kvantifikatora.

Na primer:

$(\forall X)\ P(X) * (\exists X)\ Q(X)$ zameniti sa $(\forall X)\ P(X) * (\exists Y)\ Q(Y)$

$(\exists X)\ P(X) * (\forall X)\ Q(X)$ zameniti sa $(\exists X)\ P(X) * (\forall Y)\ Q(Y)$

gde je Y nova promenljiva koja se ne pojavljuje ni u formuli P(X) ni u formuli Q(X), a * neki od simbola $\wedge$, $\vee$.

Korak 4. Izvlačenje kvantifikatora ispred formule redom zamenama, ako je to moguće

$((\forall X)\ A(X) \wedge (\forall X)\ B(X))$ zameniti sa $(\forall X)\ (A(X) \wedge B(X))$

$((\exists X)\ A(X) \vee (\exists X)\ B(X))$ zameniti sa $(\exists X)\ (A(X) \vee B(X))$

$((\forall X)\ A(X) \vee (\forall X)\ B(X))$ zameniti sa $(\forall X)(\forall Y)\ (A(X) \vee B(Y))$

$((\exists X)\ A(X) \wedge (\exists X)\ B(X))$ zameniti sa $(\exists X)(\exists Y)\ (A(X) \wedge B(Y))$

$(\exists X)\ A(X)*B$ zameniti sa $(\exists X)\ (A(X)*B)$

$B*(\exists X)\ A(X)$ zameniti sa $(\exists X)\ (B*A(X))$

$(\forall X)\ A(X)*B$ zameniti sa $(\forall X)\ (A(X)*B)$

$B*(\forall X)\ A(X)$ zameniti sa $(\forall X)\ (B*A(X))$.

Ovde A(X) označava da se promenljiva X pojavljuje slobodno u A, a samo B, da se promenljiva X koja se sa kvantifikatorom izvlači ispred zagrade ne pojavljuje slobodno u B, * je neki od simbola $\wedge$, $\vee$. Veoma je važno pridržavati se redosleda da bi se egzistencijalni kvantifikatori, ako je to moguće, izvukli ispred zagrade pre univerzalnih.

Višestrukim izvršavanjem ovih koraka, sve dok se podformule mogu zamenjivati prema napred navedenim koracima, formula se dovodi u **PRENEKS** oblik, tj. u oblik gde su svi kvantifikatori ispred formule.

Korak 5. Isključivanje egzistencijalnih kvantifikatora

Isključujemo redom egzistencijalne kvantifikatore na sledeći način:

Neka polazna formula ima oblik:

$(Q_1X_1)\ (Q_2X_2)\dots(Q_nX_n)\quad G(X_1, X_2, \dots, X_n)$

gde su Q_i, $i=1, \dots n$, univerzalni ili egzistencijalni kvantifikatori, a X_i, $i=1, \dots n$, su slobodne promenljive u G. Ako ni jedan od n kvantifikatora nije egzistencijalni, preći na korak 6, a ako jeste uraditi sledeće:

(1) Staviti $i=1$.

(2) Ako je Q_i univerzalni kvantifikator, preći na (3), a ako nije, zameniti polaznu formulu formulom u kojoj je iz navedenog niza kvantifikatora izostavljen član (Q_iX_i), a telo joj je jednako telu polazne formule u kome su sva pojavljivanja promenljive X_i zamenjena novom konstanom za tu formulu, zatim uvećati i za 1, pa ponoviti postupak (2) ako i nije veće od n, ako jeste, preći na korak 7 algoritma;

(3) Zameniti i sa i+1, pa ako i nije veće od n, proveriti da li je Q_i egzistencijalni kvantifikator. Ako jeste, i ako se ispred njega u nizu nalazi j univerzalnih kvantifiaktora koji vezuju redom promenljive $Xk_1, \ldots Xk_j$, izostaviti iz niza kvantifikatora član (Q_iX_i), a u telu formule zameniti svako pojavljivanje promenljive X_i termom $f(Xk_1, \ldots, Xk_j)$, gde je f nov funkcijski simbol dužine j. Polaznu formulu zameniti formulom koja je dobijena ovom transformacijom, zatim se vratiti na (3).

Ako je Q_i univerzalni kvantifikator, vratiti se na (3), ne menjajući ništa u polaznoj formuli.

Ako je i veće od n, preći na korak 6.

Korak 6. Oslobađanje od univerzalnih kvantifikatora.

Pošto su ispred formule ostali samo univerzalni kvantifikatori, prema konvenciji ih možemo odbaciti imajući u vidu da su formule sa kojima radimo zatvorene, a da je poredak univerzalnih kvantifikatora nebitan za istinitosnu vrednost formule. Zatim preći na korak 7.

Korak 7. Svođenje tela formule na konjunkciju sastavaka.

Koristeći distributivnost disjunkcije uraditi sledeće:

$(A\wedge B)\vee C$ zameniti sa $(A\vee C)\wedge(B\vee C)$,

$A\vee(B\wedge C)$ zameniti sa $(A\vee B)\wedge(A\vee C)$,

sve dok se formula ne svede na oblik $C_1 \wedge C_2 \wedge \ldots \wedge C_m$, gde su $C_1, C_2, \ldots C_m$ disjunkcije literala, čime je algoritam završen.

Rezultat primene ovog algoritma je formula bez kvantifikatora u kojoj se pojavljuju konstante i funkcije kojih ranije nije bilo. Pošto su svi koraci sem 5 generisali formulu ekvivalentnu datoj, to je jedini pitanje da li postupak primenjen u koraku 5 ima svojstvo saglasnosti i kompletnosti. Ovaj postupak je u literaturi dobro poznat, pa taj dokaz nećemo davati.

Za primenu ovog algoritma treba primetiti:

- Pojedini koraci mogu da se izvrše čisto mehanički, i prema tome pogodni su za programiranje na računaru. Ipak, prema Devisu /**/ praktičnije je da se ti pripremni koraci izvode ručno.
- Postojanje modela za neki skup formula ekvivalentno je postojanju modela skupa formula dobijenog primenom nekog od koraka datog algoritma.

Pored navedenog, postoje i drugi algoritmi pripreme formula. Imati pojednostavljenu formulu je velika prednost pri daljem mehaničkom radu sa njom. Zato je mnogo rađeno na algoritmima pripreme formula koji daju jednostavniju formulu.

Jedan od takvih algoritama koji daje jednostavniju formulu nego navedeni algoritam može se pronaći u magistarskom radu Dragane Jemuović /**/

Magistarski rad Gordane Jovanović /**/ bavi se algoritmom pripreme formula u kome se zadržava ekvivalencija između elementarnih formula, pri čemu se dokazuju neke prednosti tog algoritma.

1.3 SVOĐENJE SKUPA SASTAVAKA NA SASTAVKE BEZ PROMENLJIVIH

Za svođenje sastavaka na sastavke bez promenljivih potrebno je prethodno uvesti nove pojmove.

DEF 1.5 ERBRANOV PROSTOR.

Svakom skupu S sastavaka na sledeći način se pridružuje skup fundamentalnih terma koji se zove Erbranov prostor za S i označava sa H.

Neka je F skup svih funkcijskih simbola koje se pojavljuju u S. Ako F sadrži bar jednu konstantu (tj. simbol funkcije dužine nula), onda je F FUNKCIJSKI REČNIK za S. Ako F ne sadrži ni jednu konstantu, onda je funkcijski rečnik za S skup $F \cup \{a\}$, gde je a nova konstanta.

Erbranov prostor za S se sastoji iz svih terma koji se mogu izgraditi korišćenjem samo simbola iz funkcijskog rečnika za S.

DEF 1.6 ZASIĆENJE.

Ako je S skup sastavaka a P skup terma, tada je P[S] zasićenje S nad P, tj. skup svih fundamentalnih sastavaka dobijenih od elemenata iz S takvim zamenama promenljivih sa elementima iz P pri kojim se sva pojavljivanja jedne iste promenljive zamenjuju jednim istim termom.

DEF 1.7 INTERPRETACIJA i MODEL

INTERPRETACIJA nad nekim domenom D je svako preslikavanje atomnih formula koje ne sadrže promenljive u skup $\{T, \perp\}$ i koje se na uobičajen način (induktivno po složenosti formule) definiše za sve zatvorene formule, tj. formule bez slobodnih promenljivih).
(prvobitna definicija:** INTERPRETACIJA je skup fundamentalnih literala, koji ne sadrži komplementaran par literala. Interpretacija je definisana tako da u sebi ne sadrži kontradikciju (tj. par literala L i -L).**

MODEL skupa S zatvorenih formula je svaka interpretacija nad nekim domenom u kojoj su sve formule tog skupa istinite (tačne), tj. svaka interpretacija nad nekim domenom koja slika na $\{T\}$ sve formule skupa S.
VALJANA FORMULA je formula tačna u svakoj interpretaciji i svakom domenu, a ZADOVOLJIVA FORMULA je formula koja ima model, tj. koja je istinita u bar jednoj interpretaciji u nekom domenu.

Neka je S skup sastavaka (nekog skupa formula) H ERBRANOV prostor(univerzum) H[S] zasićenje nad H i neka je I interpretacija skupa S sastavaka sa domenom H. Interpretacija I je H-interpretacija skupa S ako ispunjava uslove:
1. I preslikava sve konstante iz S i sve fundamentalne terme iz H na same sebe.
2. Skup fundamentalnih atoma iz zasićenja S nad H interpretacija I preslikava u skup {T,⊥} čime se I induktivno definiše na celom zasićenju S nad H[S].

(prvobitna definicija: ** Neka je S skup fundamentalnih sastavaka, a A skup svih fundamentalnih atoma tih sastavaka. MODEL formula S po atomima iz A je svako preslikavanje skupa A u skup {T,⊥} tako da ma koja formula F skupa S u odnosu na to preslikavanje ima istinitosnu vrednost T. Dovoljno je poznavati samo skup onih atoma iz A koja se preslikavaju u T, da bi model bio potpuno određen. Zbog jednostavnosti zapisa uzima se da je model skupa S fundamentalnih sastavaka ona interpretacija I u odnosu na koju su svi sastavci iz S tačni. Neka je M interpretacija, a S skup fundamentalnih sastavaka. M je model za S ako svaki sastavak iz S sadrži neki član iz M. Kako je sastavak disjunkcija literala, tada ako sastavak sadrži neki član modela M, onda je on tačan u tom modelu.**

U opštem slučaju, biće pokazano da ako je S skup sastavaka koji nisu na osnovnom nivou, a H Erbranov prostor za S, M je model za S ako i samo ako je M model za H[S].

DEF 1.8 ZADOVOLJIVOST.

Skup sastavaka S je zadovoljiv ako postoji model za S. U protivnom slučaju S je nezadovoljiv.

Iz definicije zadovoljivosti je jasno da je proizvoljan skup sastavaka koji sadrži prazan sastavak nezadovoljiv, jer prazan sastavak ne sadrži nijedan član nijednog modela M. Prazan skup sastavaka je zadovoljiv jer se u njemu ne sadrži sastavak koji nije zadovoljiv. Ove dve pogodnosti će se pokazati veoma prirodne i korisne u daljem radu.

Posledica komutativnosti disjunkcije je da su dva sastavka koja sadrže iste literale, bez obzira na njihov redosled, ekvivalentni u odnosu na zadovoljivost. Zbog zakona idempotentnosti disjunkcije, svako višestruko pojavljivanje nekog literala u sastavku, može se (sem prvog) izostaviti. Navedene činjenice, zbog praktičnosti primene, omogućavaju da se sastavak posmatra kao skup svojih literala, a ne kao njihova disjunkcija.

DEF 1.9 FUNDAMENTALNA REZOLVENTA.

Za dva fundamentalna sastavka C_1 i C_2 koji sadrže komplementarne literale L i -L redom, fundamentalna rezolventa od C_1 i C_2, u oznaci $R(C_1, C_2)$, je disjunkcija sastavaka C_1' i C_2', gde je:

C_1' sastavak C_1 u kome je izostavljen literal L

C_2' sastavak C_2 u kome je izostavljen literal -L i svaki onaj literal koji se pojavljuje u C_1.

** prethodno definisati logičku posledicu**

TEOREMA 1.10 Za dva sastavka C_1 i C_2 njihova fundamentalna rezolventa R je njihova logička posledica.

DOKAZ: Neka C_1 i C_2 sadrže komplementarne literale L i -L redom. Neka su C_1 i C_2 tačni u interpretaciji I. Primetimo da se L i -L ne mogu istovremeno sadržati u I. Neka se L ne nalazi u I (tj. L je lažno pri interpretaciji I). Tada C_1 ne može biti sastavak koji se sastoji samo iz jednog literala. C_1 sadrži neki literal K (različit od L) koji se sadrži u I, inače bi C_1 bilo lažno u I. Međutim, i rezolventa C_1 i C_2 sadrži taj literal K, pa je prema tome ona tačna pri interpretaciji I. Slično se pokazuje i pri pretpostavci da se -L ne sadrži u I.

Treba primetiti da svaka dva fundamentalna sastavka ne moraju imati i fundamentalnu rezolventu, već samo ona koja sadrže parove komplementarnih literala. Neki sastavci imaju i više od jedne fundamentalne rezolvente. U svakom slučaju dva fundamentalna sastavka imaju konačan broj fundamentalnih rezolventi.

DEF 1.11 FUNDAMENTALNA REZOLUCIJA.
Ako je S skup fundamentalnih sastavaka, onda je fundamentalna rezolucija skupa S, u oznaci R(S), skup koji se sastoji od svih sastavaka iz S i svih fundamentalnih rezolventi svih parova sastavaka iz S.

$R(S)= S \cup \{R(C_1,C_2) \mid C_1,C_2 \in S\}.$

DEF 1.12 n-ta FUNDAMENTALNA REZOLUCIJA.
Ako je S skup fundamentalnih sastavaka, onda se n-ta fundamentalna rezolucija, u oznaci $R_n(S)$, definiše za svako $n \geq 0$ na sledeći način:

$R_0(S)= S$

$R_{n+1}(S)= R(R_n(S))$.

Ovim je uvedena prva grupa definicija.

1.4 TEOREMA ERBRANA

Sve metode mehaničkog dokazivanja teorema zasnivaju se na Erbranovoj teoremi, odnosno nekim njenim specijalnim oblicima.

TEOREMA 1.13 TEOREMA ERBRANA.
Neka su $A_1, \dots , A_m$ date aksiome i T teorema koju treba dokazati. Neka je $\{C_1, \dots , C_k\}$ skup sastavaka dobijenih iz $A_1, A_2, \dots , A_m$ i -T, pomoću nekog od algoritama za pripremu formula, i H odgovarajući Erbranov prostor. T je posledica $A_1, \dots , A_m$ ako i samo ako postoji takav skup sastavaka $Q_1, \dots , Q_n$ od kojih je

svaki dobijen od nekog sastavka C_i ($i=1, \dots, k$) zamenom promenljivih članovima iz H tako da je formula

$Q_1 \wedge Q_2 \wedge \dots \wedge Q_n$ kontradikcija.

DOKAZ:

Pretpostavimo da je $Q_1 \dots Q_n$ kontradikcija, ali da $A_1, \dots, A_m$, -T ima model. Kako $A_1, \dots, A_m$, -T ima model, onda i $C_1, \dots, C_k$ ima model sa univerzumom U. Pridružimo svakoj promenljivoj i svakom simbolu konstante u H neki fiksiran element iz U. Tada će svakom elementu skupa H biti dodeljen jedinstven element skupa U. Pri toj interpretaciji svako Q_i ($i=1, \dots, n$) je istinito. Zato $Q_1 \wedge \dots \wedge Q_n$ ne može biti kontradikcija jer je pronađen model u kome je istinito.

Obrnuto, pretpostavimo da $A_1, \dots, A_m$, -T nema model. Neka su $Q_1, Q_2, Q_3, \dots$ svi mogući sastavci dobijeni iz $C_1, \dots, C_k$ zamenom njihovih promenljivih članovima univerzuma H. Pri proizvoljnoj dodeli istinitosnih vrednosti atomnim formulama iz $Q_1, Q_2, Q_3, \dots$ najmanje jedan satavak Q_i biće lažan. Ako je tako, dokaz je završen, jer prema stavu kompaktnosti, beskonačna konjunkcija $Q_1 \wedge Q_2 \wedge \dots$ je kontradikcija ako je formula $Qs_1 \wedge Qs_2 \wedge \dots \wedge Qs_n \dots$ kontradikcija za neke $s_1, s_2, \dots, s_n$. Ukoliko pri proizvoljnoj dodeli istinitostnih vrednosti atomnim formulama ni jedan sastavak nije lažan, može se konstruisati model za $C_1, \dots, C_k$ sa univerzumom H. Interpretacija simbola konstanti i funkcija u tom modelu određuje se automatski: ako su date odgovarajuće istinitosne vrednosti atomnih formula iz $Q_1, Q_2, Q_3, \dots$ za koje su sve formule Q_i istinite, onda možemo interpretirati svaki predikatski simbol R, uzimajući $R(U_1, \dots, U_n)$ istinitim za $U_1, \dots, U_n$ iz H, ako i samo ako data zamena istinitosnih vrednosti daje atomnu formulu $R(U_1, \dots, U_n)$ koja je istinita u već postojećem modelu. Na taj način teorema je dokazana.

1.5 POSTUPAK ZASIĆENJA

Erbranova metoda je metoda opovrgavanja. To znači da se umesto dokazivanja da je neka formula valjana, dokazuje da je njena negacija nezadovoljiva. Mnogi problemi su formulisani tako da se utvrdi da li je neka činjenica posledica nekog skupa pretpostavki. Prevedeno na formulski jezik to je problem da li je neka formula T logička posledica jednog konačnog skupa formula S. Metodom opovrgavanja ovaj problem se svodi na problem: da li je skup formula $S \cup \{-T\}$ nezadovoljiv.

Zahvaljujući posledicama Erbranove teoreme moguće je mehanizovati proces ispitivanja da li je neki skup sastavaka nezadovoljiv.

1.11 POSLEDICA TEOREME ERBRANA.

Ako je S proizvoljan konačan skup sastavaka i H njegov Erbranov prostor onda je S nezadovoljiv ako i samo ako je neki KONAČAN PODSKUP P zasićenja ERBRANOVOG PROSTORA H[S] nezadovoljiv ($P \subseteq H[S]$).

Ova posledica se može izraziti i u sledećem obliku:

1.14' POSLEDICA TEOREME ERBRANA (Robinson /*/)

Ako je S proizvoljan konačan skup sastavaka, onda je S nezadovoljiv ako i samo ako je P [S] nezadovoljiv za neki KONAČAN PODSKUP P Erbranovog prostora za S ($P \subseteq H$).

Ova posledica Erbranove teoreme dozvoljava sledeći metod opovrgavanja koji se naziva POSTUPAK ZASIĆENJA:

Za dati konačan skup sastavaka bira se niz P_0, P_1, P_2, ... konačnih podskupova Erbranovog prostora H za S, takav da P_n pripada P_{n+1} za svako $n \geq 0$, i $\bigcup_0^\infty P_n = H$. Zatim se redom proveravaju skupovi $P_0[S]$, $P_1[S]$, $P_2[S]$, ... da li su zadovoljivi. Jasno je da P_n čini jedno pokrivanje H rastućim skupovima i da za proizvoljan konačan podskup P prostora H imamo da P pripada nekom P_i za neko i, pa prema tome i P[S], pripada $P_i[S]$. Prema posledici 1.14' teoreme Erbrana, ako je S nezadovoljiv, onda je za neko i podskup $P_i[S]$, nezadovoljiv.

Svakako, proizvoljan konkretan postupak ovog oblika treba da omogućava izbor P_0, P_1, P_2, ... na isti način za sve skupove sastavaka. Najprirodniji način takvog izbora je korišćenje nivoa H_0, H_1, H_2, ... Erbranovog prostora H, gde se H_0 sastoji iz svih konstanti, a H_n čine termi dubine najviše n. Ovaj postupak proveravanja teorema zove se postupak zasićenja po nivoima.

Osnovna kombinatorna smetnja za dostizanje efektivnosti postupka zasićenja po nivoima je ogromna brzina rasta konačnih skupova H_j i $H_j[S]$ sa povećanjem j. Za neke zanimljivije skupove S moguće je navesti primer sasvim prostih nezadovoljivih skupova sastavaka S za koje je prvi nezadovoljiv $H_j[S]$ toliko veliki da je daleko od svake moguće realizacije.

Interesantna heuristička primedba se sastoji u tome da za svaki konačan skup sastavaka, koji je nezadovoljiv, i za koji se faktički može da konstruiše opovrgavanje, postoji najmanje jedan konačan podskup Erbranovog prostora za S, koji ima prihvatljive dimenzije, takav da je P[S] nezadovoljiv, pri čemu je P minimalan u tom smislu da je Q[S] zadovoljiv za proizvoljan pravi podskup Q skupa P. Takav skup P se naziva OPOVRGAVAJUĆI SKUP za S. Ukoliko je poznat opovrgavajući skup za nezadovoljiv konačan skup sastavaka S, onda bi se procecura dokazivanja sastojala u konstruisanju P[S] zasićenja skupa S, i dokaza da je P[S], nezadovoljiv.

To bi u suštini bila osnovna shema mašinskog programa, gde se nalaženje opovrgavajućeg skupa prepušta snalažljivom matematičaru koji taj skup pogađa koristeći intuiciju, dok postupak proveravanja nezadovoljivosti izvodi računar. Nameće se misao da se i generisanje takvog skupa prepusti računaru, iako se na prvi pogled čini da o tome ne može biti ni govora.

1.6 REŠAVAJUĆI POSTUPAK

1.6. REŠAVAJUĆI POSTUPAK

POSTUPAK ZASNOVAN NA PRIMENI REZOLUCIJE SKUPA S

U ovom odeljku biće prikazan način proveravanja da li je neki skup fundamentalnih sastavaka zadovoljiv ili nije.

Neka je S konačan skup fundamentalnih sastavaka. Konstruišimo redom skupove: S, R(S), R(R(S)), ... dok neki $R_n(S)$ ne sadržI prazan sastavak NIL, ili se ne poklapa sa $R_{n+1}(S)$. U prvom slučaju S je nezadovoljiv, a u drugom je zadovoljiv. Pre ili kasnije jedan od ta dva uslova treba da se ispuni, pošto broj različitih sastavaka, sagrađenih od konačnog skupa literala koji ulaze u S mora biti konačan i prema tome, u beskonačnom nizu rastućih skupova S, R(S), R(R(S)), ..., $R_n(S)$, ... nisu sve inkluzije prave, jer rezolucijom se ne dobijaju novi literali. Na osnovu toga što se opisani proces pre ili kasnije završava sledi njegova korektnost.

TEOREMA 1.15 TEOREMA O FUNDAMENTALNOJ REZOLUCIJI (Robinson/*/).

Ako je S proizvoljan konačan skup fundamentalnih sastavaka, onda je S nezadovoljiv ako i samo ako $R_n(S)$ za neko $n \geq 0$ sadrži prazan sastavak NIL.

DOKAZ:

Neka je T završni skup u nizu R(S), ... , $R_n(S)$, odnosno T je zatvoren u odnosu na fundamentalnu rezoluciju. Treba pokazati da ako T ne sadrži prazan sastavak, onda je T zadovoljiv, i prema tome je i S zadovoljiv jer S se sadrži u T. Neka su L_1, L_2, ... , L_n svi različiti literali koji ulaze u T. Neka je M model definisan na sledeći način:

M_0 je prazan skup, a za svako $0 < j \leq k$, M_j je skup $M_{j-1} \cup \{L_j\}$ ako se ni jedan satavak iz T ne sastoji samo iz komplementarnih literala skupa $M_{j-1} \cup \{L_j\}$ u protivnom M_j je skup $M_{j-1} \cup \{-L_j\}$. Na kraju M je M_n. Ako T ne sadrži NIL, onda je M model za T. To je zato jer u protivnom postoji najmanji j, $0 < j \leq k$, tako da je neki sastavak C iz T satavljen ceo iz komplementarnih literala skupa M_j. Ali po definiciji M_j je $M_{j-1} \cup \{-L_j\}$. Zato uzimajući u obzir minimalnost j, sastavak C sadrži L_j. Ali pošto je M_j jednak po definiciji $M_{j-1} \cup \{-L_j\}$, onda postoji neki sastavak, recimo D iz T koji se sastoji ceo od literala koji su komplementarni literalima skupa $M_{j-1} \cup \{-L_j\}$. Zato zbog minimalnosti j sastavak D sadrži $-L_j$. U tom slučaju sastavak $B= (C-\{Lj\}) \cup (D-\{-Lj\})$ sastoji se ceo od komplementarnih literala skupa M_{j-1}, ako B nije NIL. No B je fundamentalna rezolucija C i D, zato B pripada skupu T i sledi da je B različito od NIL. Ali to protivreči minimalnosti j, čime je teorema dokazana.

Teorema o fundamentalnoj rezoluciji omogućava da se formuliše specifična forma teoreme Erbrana.

TEOREMA 1.16 TEOREMA ERBRANA-ROBINSONA (Robinson /8/).

Ako je S proizvoljan konačan skup sastavaka, onda je S nezadovoljiv ako i samo ako za neki konačan podskup P Erbranovog prostora H za S i za neko $n \geq 0$, $R_n(P[S])$ sadrži prazan sastavak.

PRIMER. Dokazati nezadovoljivost skupa sastavaka.

S= {Q(a), -Q(b), R(x), - R(f(b))}.

Funkcijski rečnik za S čini skup {a,b,f}.

Erbranov prostor za S je skup svih terma nad a, b, f.

H= {a,b,f(a), f(b), f(f(a)), f(f(b)), ...}.

Korišćenjem metoda zasićenja nivoa:

H_0= {a,b}, H_0 je skup svih konstanti iz S.

H_0[S]= {Q(a), -Q(b), R(a), R(b), -R(f(b))}.

Zasićenje skupa Ho ne sadrži kontradikciju.

H_1= {a,b,f(a), f(b)}

H_1[S]= {Q(a), -Q(b), R(a), R(b), R(f(a)), R(f(b)), -R(f(b))}.

Jedina rezolucija koja se može izvesti je između C_1: R(f(b)) i C_2: -R(f(b)). R(C_1,C_2)= NIL. Otuda:

R(H_1[S])= H_1[S] $\cup$NIL

Ovim je dokazano da je S nezadovoljiv.

U ovom slučaju opovrgavajući skup je P={f(b)}.

Primetimo da ako imamo satavke C_1=P(x) i C_2=-P(f(b)) nije teško uočiti da njihova rezolventa postoji samo ako je x=f(b). Zamenom x sa f(b) preskače se proveravanje zadovoljivosti skupa H_0[S].

Interesantno i veoma važno pitanje je da li se može uvek ovako raditi, odnosno ne tražiti rezoluciju samo od fundamentalnih sastavaka, već i od sastavaka koji sadrže promenljive. Već se nazire predstava o opštem pojmu rezolvente i novim mogućnostima u dokazivanju teorema koji se zasnivaju na činjenici da je rezolventa polukomutativna sa zasićenjem. Tačnije, to svojstvo se može formulisati u obliku sledeće osnovne leme.

LEMA 1.17 Lema o polukomutativnosti rezolucije i zasićenja.

Ako je S proizvoljan skup sastavaka, a P proizvoljan podskup Erbranovog prostora za S, tada je R(P[S]) podskup od P[R(S)].

Na osnovu leme 1.17 svaki fundamentalni sastavak koji se može dobiti kao rezultat zamene promenljivih u paru sastavaka C i D sa termima iz P i nalaženjem fundamentalne rezolvente novodobijenih sastavaka, može takođe da se dobije kao rezultat zamene terma iz P u jednoj od konačno mnogo rezolventi (ali sada ne fundamentalnih) sastavaka C i D.

Lema će biti dokazana kasnije kada se uvede pojam zamene.

POSLEDICA 1.18 (posledica leme 1.17)

Ako je S proivoljan konačan skup sastavaka, a P proizvoljan podskup Erbranovog prostora za S, tada je:

R_n (P[S]) $\subseteq$ P[R_n(S)] za sve n $\geq$ 0.

DOKAZ se izvodi indukcijom po n.

Za n=0, tvrđenje je očigledno, jer je

R_0(P[S])= P[S]= P[R_0(S)]

Neka je tvrđenje tačno za n:

R_n(P[S]) $\subseteq$ P[R_n(S)].

Dokažimo da je tvrđenje tačno i za n+1.

$$\begin{aligned} R_{n+1}(P[S]) &= R(R_n(P[S])) && \text{po definiciji } R_{n+1} \\ &\subseteq R(P[R_n(S)]) && \text{po induktivnoj pretpostavci jer R čuva inkluziju} \\ &\subseteq P[R(R_n(S))] && \text{po lemi 1.17} \\ &= P[R_{n+1}(S)] && \text{po definiciji } R_{n+1}. \end{aligned}$$

Pomoću ove posledice i posledice Erbranove teoreme 1.14 može se neposredno dobiti:

TEOREMA 1.19 Posledica 1.18 i 1.14'

Ako je S proizvoljan konačan skup sastavaka, onda je S nezadovoljiv ako i samo ako za neki konačan podskup P Erbranovog prostora za S i neko $n \geq 0$, $P[R_n(S)]$ sadrži NIL.

Izmenom reda primenjivanja zasićenja i n-te rezolucije, postalo je moguće neočekivano uprošćenje primene rezolucije, jer zamena terma umesto promenljive ne može stvoriti prazan sastavak.

Prema tome, $P[R_n(S)]$ sadrži prazan sastavak ako i samo ako $R_n(S)$ sadrži prazan sastavak. Iz teoreme 1.19 dobija se osnovna teorema koja je glavni rezultat poznatog rada J.ROBINSON /**/.

TEOREMA 1.20 TEOREMA O REZOLUCIJI.

AKO JE S PROIZVOLJAN KONAČAN SKUP SASTAVAKA TADA JE S NEZADOVOLJIV AKO I SAMO AKO $R_n(S)$ SADRŽI PRAZAN SASTAVAK ZA NEKI $n \geq 0$.

Tvrđenje teoreme o rezoluciji je u stvari tvrđenje teoreme o fundamentalnoj rezoluciji bez spominjanja fundamentalnosti. Metod provere nezadovoljivosti konačnog skupa S sastavaka ostaje isti. U slučaju kada je S skup fundamentalnih sastavaka, on se svodi na raniji metod.

Ipak nije tačno da niz skupova S, R(S), R(R(S)), ... , $R_n(S)$ ... treba da se završava za svako S sa $R_n(S)= R_{n+1}(S)$, odnosno taj niza skupova nije obavezno konačan kao kod slučaja fundamentalne rezolucije. Po teoremi ČERČA, za svaki skup S postupak ne može da bude konačan, jer bi postojao odlučiv postupak za logiku prvog reda.

Problem nalaženja opovrgavajućeg skupa P je rešavan tako što ga je u početku zadavao matematičar rukovodeći se svojom intuicijom. Ukoliko bi bio poznat opovrgavajući skup P za nezadovoljiv skup sastavaka S, onda jedino ostaje da se računaju rezolvente, sve dotle dok se ne dobije prazan sastavak. Ali teorema o rezoluciji garantuje da će se iz nezadovoljivog skupa sastavaka dobiti prazan sastavak, bez obzira što nije poznat opovrgavajući skup. U tom smislu teorema o rezoluciji zamenjuje matematičara i njegovu intuiciju.

1.7 ZAMENA

Za nalaženje rezolvente dva sastavka koji sadrže promenljive, potrebno je definisati kako se zamenjuju termi umesto promenljivih.

DEF 1.21 KOMPONENTE ZAMENE su uređeni parovi (t,v), u oznaci t/v, gde je v promenljiva, a t term različit od v izgrađen od promenljivih i elemenata Erbranovog prostora.

DEF 1.22 ZAMENA je konačan (može biti i prazan) skup komponenata zamene oblika $\{t_1/x_1, \ldots, t_k/x_n\}$, sa međusobno različitim promenljivim.

Redosled komponenata zamene u zameni je nebitan. Zamene se označavaju sa $\alpha, \beta, \gamma, \ldots$ Oznaka za praznu zamenu je ε.

DEF 1.23 KONKRETIZACIJA

Rezultat primene zamene $\alpha = \{t_1/x_1, \ldots, t_k/x_n\}$ na proizvoljan konačan skup simbola E, koji se sastoji u zamenjivanju svih učestvovanja promenljive x_i, sa odgovarajućim termom t_i naziva se KONKRETIZACIJA E i označava sa $E\alpha$. Novodobijeni skup se naziva α primer E. Ako je $E= E_0x_{i1}\ E_1x_{i2} \ldots x_{ik}E_k$, pri čemu ni jedna od reči E_i ne sadrži promenljive x_i, (neke E_i mogu biti i prazne reči), tada α primer E je $E_0t_{i1}\ E_1t_{i2} \ldots t_{ik}E_k$.

DEF 1.24 STANDARDIZACIJA

Ako je C konačan skup reči, a $v_1, \ldots, v_n$, sve međusobno različite promenljive koje ulaze u C, i koje su poređane u leksikografskom poredku, ξ_C standardizacija je zamena sastavljena iz svih komponenata zamene oblika x_j/v_j, ($1 \leq j \leq n$ i $v_j \neq x_j$). Slično se definiše i η_C standardizacija, samo umesto x_j stoji y_j.

DEF 1.25 KOMPOZICIJA ZAMENA

Ako su $\alpha = \{t_1/x_1, \ldots, t_n/x_n\}$ i $\beta = \{s_1/y_1, \ldots, s_m/y_m\}$ dve proizvoljne zamene, tada je njihova KOMPOZICIJA, u oznaci $\alpha*\beta$, zamena koja se dobija iz skupa $\{t_1\beta/x_1, \ldots, t_n\beta/x_n, s_1/y_1, \ldots, s_m/y_m\}$ izostavljanjem svih elemenata $(t_j)\beta/x_j$ za koje je $(t_i)\beta=x_j$, i svih elemenata s_i/y_i za koje je $y_i \in \{x_1, x_2, \ldots, x_n\}$.

Iz definicije je jasno da se kompozicijom zamena opet dobija zamena, jer su izbačene komponente oblika x_j/x_j, dok se izbacivanjem komponenata oblika s_i/x_j sačuvao uslov da su sve promenljive međusobno različite. Neposredno se proverava da je $\varepsilon*\alpha= \alpha*\varepsilon=\alpha$ za proizvoljnu zamenu, gde je ε prazna zamena. Osobine kompozicije zamena istaknimo posebno.

TVRĐENJE 1.26 OSOBINE ZAMENE I KOMPOZICIJE ZAMENA

Neka su E i F skupovi reči i α, β, γ proizvoljne zamene.

Tada važi:

1. Ako je za svaku reč E $(E)\alpha=(E)\beta$, tada je $\alpha=\beta$.
2. $((E)\ \alpha)\ \beta= (E)\ (\alpha*\beta)$
3. $(\alpha*\beta)*\gamma= \alpha*(\beta*\gamma)$

4. $(E \cup F)\,\alpha = (E)\alpha \cup (F)\,\alpha$.

DOKAZ

1. Neka su $v_1, \ldots, v_k$ sve različite promenljive komponenata zamene iz α i β. Neka je E redom v_j $(1 \leq j \leq k)$. Tada je $(v_j)\,\alpha = (v_j)\beta$. Zato se α i β sastoje iz istih komponenata zamene, pa su jednake.

2. Dokazujemo $((E)\,\alpha)\,\beta = (E)\,(\alpha * \beta)$

Neka su $\alpha = \{t_1/x_1, \ldots, t_n/x_n\}$ i $\beta = \{s_1/y_1, \ldots, s_m/y_m\}$ dve proizvoljne zamene i reč E ima oblik $E = E_0 x_{i1} E_1 x_{i2} \ldots x_{ik} E_k$. Tada je $(E)\alpha = E_0 t_{i1} E_1 t_{i2} \ldots t_{ik} E_k$, a

$((E)\alpha)\beta = E_0' t_{i1}' E_1' t_{i2}' \ldots t_{ik}' E_k'$,

gde je svako $t_{ij}' = (t_{ij})\beta$, a svako $E_j' = (E_j)\beta_1$, gde je β_1 skup tih komponenata β čije promenljive nisu neke od $x_1, \ldots, x_n$ (zato što se ni jedna od tih promenljivih ne sadrži u nekoj od reči E_j). Ali $\alpha * \beta = \alpha_1 \cup \beta_1$ gde je svaka komponenta α_1 oblika $t_i\beta/x_i$ ako je $t_i\beta$ različito od x_i, a β_1 skup samo onih komponenata zamene s_i/y_i za koje je $y_i \notin \{x_1, \ldots, x_n\}$. Zato je $(E)\,(\alpha * \beta) = E_0' t_{i1}' E_1' t_{i2}' \ldots t_{ik}' E_k'$, čime je tvrđenje dokazano.

3. Neka je E proizvoljan reč. Tada je korišćenjem 26.2

$(E)\,((\alpha * \beta) * \gamma) = ((E)(\alpha * \beta))\gamma = (((E)\alpha)\beta)\gamma$

$(E)\,((\alpha * (\beta * \gamma)) = ((E)\alpha)(\beta * \gamma) = (((E)\alpha)\beta)\gamma$

Prema tvrđenju 1.26.1 je $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$

4. Ako izraz $A \in E \cup F$, onda $A \in E$ ili $A \in F$, što znači da $(A)\alpha \in (E)\,\alpha$ ili $(A)\,\alpha \in (F)\,\alpha$, iz čega sledi $(A)\alpha \in (E)\alpha \cup (F)\alpha$.

Obrnuto, ako neki izraz $B \in (E)\alpha \cup (F)\alpha$, onda $B \in (E)\alpha$ ili $B \in (F)\alpha$, u svakom slučaju postoji izraz A takav da je $(A)\alpha = B$ i $(A)\alpha \in (E)\alpha$ ili $(A)\alpha \in (F)\alpha$, što znači da $A \in E$ ili $A \in F$ što je ekvivalentno sa $A \in (E \cup F)$, a to znači da $B = (A)\alpha \in (E \cup F)\alpha$, čime je tvrđenje dokazano.

DEF 1.27 SKUP RAZLIČITOSTI

Neka je A konačan skup izraza. Skup različitosti za A je skup svih onih podizraza koji počinju od tog mesta gde neki izrazi imaju različit simbol.

Primer. Ako je A= {P(x, <u>h(x,y)</u> , y), P(x, <u>k(y)</u> ,y), P(x, <u>a</u>, b)} skup različitosti za A je {h(x,y), k(y), a}. Ako A nije jednočlan, tada ni skup različitosti od A nije jednočlan.

1.8 UNIFIKACIJA

DEF 1.28 UNIFIKACIJA I UNIFIKATIVAN SKUP

Zamena θ je unifikator skupa E, gde je E skup izraza (terma ili literala), ako je $(E)\theta$ jednočlan skup. Ako za skup E postoji unifikator θ, kaže se da θ unificira skup A, odnosno da je E unifikativan skup.

Unifikativan skup može imati više unifikatora. Jasno je da ako θ unificira A i A sadrži više od jednog elementa, onda θ unificira skup različitosti skupa A.

DEF 1.29 NAJOPŠTIJI ZAJEDNIČKI UNIFIKATOR

Neka su θ i σ unifikatori skupa izraza A. Unifikator σ je najopštiji unifikator skupa A, ako za ma koji unifikator θ skupa A postoji zamena α takva da je $\theta = \sigma * \alpha$.

ALGORITAM 1.30 ALGORITAM UNIFIKACIJE

Sledeći algoritam, primenjen na proizvoljan konačan neprazan skup izraza A naziva se algoritam unifikacije.

Korak 1. Staviti $\sigma(0) = \varepsilon$ i $k=0$ i preći na korak 2.

Korak 2. Ako $A\sigma(k)$ nije jednočlan skup preći na korak 3, u protivnom slučaju staviti $\sigma_A = \sigma(k)$ i završiti rad.

Korak 3. Neka su v_k i t_k dva prva iraza u leksikografskom poredku elemenata skupa različitosti $B(k)$ za skup $(A)\ \sigma(k)$. Ako je v_k promenljiva koja ne ulazi u t_k, staviti $\sigma(k+1) = \sigma(k) * \{t_k/v_k\}$, povećati k za jedan i vratiti se na korak 2. U protivnom prekinuti rad i saopštiti da unifikator za skup A ne postoji.

Definicija ovog algoritma ne sadrži dokaz da će se opisani proces uvek završiti za proizvoljan neprazan konačan skup pravilno konstruisanih izraza. U stvari ovaj algoritam uvek završava rad ili na koraku 2 ili na koraku 3, jer bi se u protivnom slučaju generisao beskonačan niz A, $(A)\sigma(1)$, $(A)\sigma(2)$, ... konačnih nepraznih skupova pravilno konstruisanih izraza u kome svaki sledeći član sadrži jednu promenljivu manje nego prethodni (tj. $(A)\sigma(k)$ sadrži v_k a $(A)\sigma(k+1)$ ne sadrži). Ali tako nešto je nemoguće, jer A sadrži samo konačan skup promenljivih.

DEF 1.31 VALJANOST ALGORITMA UNIFIKACIJE

Ako je A konačan neprazan skup izraza, za koji algoritam unifikacije završava rad na koraku 2, onda je A OPŠTEUNIFIKATIVAN skup. Dokazuje se da je konstruisana zamena σ najopštiji zajednički unifikator za A.

TEOREMA 1.32 TEOREMA O UNIFIKACIJI

Ako je A unifikativan, onda je A i opšteunifikativan. Ako je θ proizvoljan, a σ_A najopštiji zajednički unifikator, konstruisan primenom algoritma unifikacije, onda postoji zamena α takva da je $\theta = \sigma_A * \alpha$.

DOKAZ:

Dovoljno je dokazati da algoritam unifikacije završava rad nad A na koraku 2. i ako algoritam unifikacije još nije završio rad i konstruisana je zamena $\sigma(k)$, $k>0$, onda je jednakost (1) $\theta=\sigma(k)^*\ \alpha(k)$ ispravna na koraku 2 algoritma, za neku zamenu $\alpha(k)$. Dokaz se izvodi indukcijom po k.

Za k=0 tvrđenje je tačno, jer je $\sigma(0)=\varepsilon$, $\alpha(0)=\theta$.

Pretpostavimo da je za neko k>0 ispunjeno (i) za neku zamenu $\alpha(k)$. Tada, ako je (A) $\sigma(k)$ jednočlan skup, algoritam unifikacije će završiti rad na koraku 2. i pri tome je $\sigma_A=\sigma(k)$ najopštiji zajednički unifikator i $\alpha=\alpha(k)$ je tražena zamena. U protivnom algoritam prelazi na korak 3. Kako $\alpha(k)$ unificira $(A)\sigma(k)$, (zbog (1), jer θ unificira A), onda $\alpha(k)$ unificira skup neslaganja B(k) skupa $(A)\sigma(k)$. Zato v_k i t_k, definisani na koraku 3 algoritma unifikacije, zadovoljavaju jednakost (2) $(v_k)\alpha(k)=(t_k)\alpha(k)$.

Kako je B(k) skup različitosti, to izrazi iz B(k) ne mogu počinjati sa jednim istim simbolom. B(k) je unifikativan pa najmanje jedan izraz počinje sa promenljivom, i jednak je promenljivoj, jer je i promenljiva izraz. U leksikografskom poretku promenljive prethode svim drugim izrazima, a v_k je prvi izraz u B(k), onda je v_k promenljiva. Ako se v_k sadrži u t_k, onda se $(v_k)\alpha(k)$ sadrži u $(t_k)\alpha(k)$, što je nemoguće, jer v_k i t_k nisu identični jednaki i važi jednakost (2). Prema tome, v_k se ne sadrži u t_k. Zato algoritam unifikacije neće završiti rad na koraku 3, već će se vratiti na korak 2. i pri tome je $\sigma(k+1)=\sigma(k)^*\ \{t_k/v_k\}$. Stavimo $\alpha(k+1)=\alpha(k)-\{t_k\alpha(k)/v_k\}$.

Tada je

$\alpha(k)=\{(v_k)\alpha(k)/v_k\}\cup\alpha(k+1)$	po definiciji $\alpha(k+1)$
$=\{(t_k)\alpha(k)/v_k\}\cup\alpha(k+1)$	prema (2)
$=\{(t_k)\alpha(k+1)/v_k\}\cup\alpha(k+1)$	jer v_k se ne sadrži u t_k
$=\{t_k/v_k\}\cup\alpha(k+1)$	po def. 1.25

Odatle prema (1) je $\theta=\sigma(k+1)^*\ \alpha(k+1)$. Zato je jednakost (1) ispunjena za sve $\sigma(k)$. Kako algoritam unifikacije treba da se završi, i kako se ne završava na koraku 3, mora da se završi na koraku 2. Jednakost (1) važi za sve $\sigma(k)$, pa je poslednje $\sigma(k)=\sigma_A$ najopštiji zajednički unifikator, što je i trebalo dokazati.

1.9 REZOLVENTA I ZAMENA

DEF 1.33 DEFINICIJA BINARNE (STANDARDIZOVANE) REZOLVENTE

Neka za sastavke C i D, koji ne sadrže zajedničke promenljive (to se uvek može postići preoznačavanjem promenljivih korišćenjem ξ_C i η_D standardizacije), za njihove literale L i K redom, postoji najopštiji zajednički unifikator σ za L i ¬K

Tada je njihova BINARNA ili STANDARDIZOVANA rezolventa sastavak $C_1 \vee D_1$, gde je C_1 sastavak $(C)\sigma$ u kome su izostavljeni literali $(L)\sigma$, a D_1 sastavak $(D)\sigma$ u kome su izostavljeni literali $(K)\sigma$

Literali L i K se nazivaju ISKLJUČENI ili R-literali, a trojka $(L,K,(L)\sigma)$ se naziva KLJUČNA TROJKA.

DEF 1.34 FAKTOR

Ako dva ili više literala (sa istim znakom) sastavka D imaju najopštiji zajednički unifikator σ, onda se sastavak $(D)\sigma$ u kome su izbačena višestruka pojavljivanja istih literala naziva FAKTOR od D.

DEF 1.35 REZOLVENTA sastavaka C i D je jedna od sledećih binarnih (standardizovanih) rezolventi.

1) binarna rezolventa C i D
2) binarna rezolventa C i faktora od D
3) binarna rezolventa faktora od C i D
4) binarna rezolventa faktora od C i faktora od D.

Definicije REZOLUCIJE i n-te REZOLUCIJE se dobijaju iz DEF 1.11 i DEF 1.12 izostavljanjem fundamentalnosti.

DOKAZ 1.36 DOKAZ OSNOVNE LEME 1.17

Ako je S proizvoljan skup sastavaka, a P proizvoljan podskup Erbranovog prostora za S, onda je R(P[S]) podskup od P[R(S)].

Neka je A sastavak iz R(P[S]). Tada ili je A iz P[S] ili je A fundamentalna rezolventa dva fundamentalna sastavka $(C)\alpha$ i $(D)\beta$, gde su C i D iz S, $\alpha=\{t_1/v_1, \ldots, t_k/v_k\}$, $\beta=\{s_1/w_1, \ldots, s_m/w_m\}$, $v_1, \ldots, v_k$ spisak svih promenljivih koje ulaze u C a $w_1, \ldots, w_m$ spisak svih promenljivih koje ulaze u D navedenih u leksikografskom poredku, dok su $t_1, \ldots, t_k, s_1, \ldots, s_m$ elementi P. U tom slučaju $A=(C-L)\alpha \cup (D-M)\beta$ gde su L i M neprazni skupovi literala $L \subseteq C$, $M \subseteq D$, a $(L)\alpha$ i $(M)\beta$ su jednočlani skupovi, čiji elementi obrazuju komplementaran par. Neka je $\theta=\{ t_1/x_1, \ldots, t_k/x_k, s_1/y_1, \ldots, s_m/y_m\}$ Tada: $A=(C-L)(\xi_C*\theta)\cup(D-M)(\eta_D*\theta)$ i $(L)(\xi_C*\theta)=(L)\alpha$, $(M)(\eta_D*\theta)=(M)\beta$. Prema tome θ unificira skup N onih atomnih formula koje ili ulaze u skup $(L)\xi_C\cup(M)\eta_D$ ili su to formule komplementarne onim iz tog skupa. Prema teoremi o unifikaciji, N ima najopštiji unifikator σ_N, i postoji takva zamena γ nad P da je $\theta=\sigma_N*\gamma$. Odatle $(L)(\xi_C*\sigma_N*\gamma)=(L)\alpha$, $(M)(\eta_D*\sigma_N*\gamma)=(M)\beta$ i prema tome $(L)(\xi_C*\sigma_N)$ i $(M)(\eta_D*\sigma_N)$ su jednočlani skupovi, čiji su elementi komplementarni jedan drugom. Zato je (L,M,N) ključna trojka za (C,D) a sastavak $B=(C-L)(\xi_C*\sigma_N)\cup(D-M)(\eta_D*\sigma_N)$ je rezolventa C i D, prema tome B pripada R(S). Pošto je $\theta=\sigma_N*\gamma$, onda je $(B)\gamma=(C-L)(\xi_C*\theta)\cup(D-M)(\eta_D*\theta)$, $(B)\gamma=A$ i zato A pripada P[R(S)]. Ovim je dokaz leme završen.

Uslovi leme ne povlače obrnutu inkluziju: $P[R(S)] \subseteq R(P[S])$.

Primer: $S= \{ \{Q(x,f(y))\}, \{-Q(g(y),x))\} \}$, $P=\{a\}$.

Provera pokazuje da $P [R (S)]$ sadrži prazan sastavak NIL. Na taj način je S nezadovoljiv, a P nije opovrgavajući skup za S.

LEMA 1.37 LEMA O PODIZANJU (LIFTING LEMA)

Ako su C_1 i D_1 redom faktori C i D, i ako je R_1 rezolventa C_1 i D_1, tada postoji takva rezolventa R od C i D tako da je R_1 faktor od R.

DOKAZ

Promenimo, ako je potrebno promenljive u C i D, tako da C i D ne sadrže iste promenljive. Neka su L_1 i K_1 isključeni literali u R_1 i neka je $R_1=((C_1)\sigma-(L_1)\sigma) \cup((D_1)\sigma-(K_1)\sigma)$, gde je σ najopštiji zajednički unifikator L_1 i $-K_1$. Kako su C_1 i D_1 faktori od C i D, to postoji takva zamena θ da je $C_1=(C)\theta$, $D_1=(D)\theta$. Neka su $L(1), \ldots, L(i)$ literali u C koji odgovaraju L_1, tj. $(L(1))\theta= L_1, \ldots L(i)) \theta= L_1$ i $K(1), \ldots, K(j)$ literali u D koji odgovaraju K_1, $(K(1))\theta=K_1, \ldots K(j))\theta= K_1$). Ako je $i>1$, postoji najopštiji zajednički unifikator α za $L(1), \ldots L(i)$ i neka je $L=(L(i))\alpha$. Ako je $i=1$, α=EPS. Slično za $K(1), \ldots, K(j)$ postoji najopštiji zajednički unifiaktor β i neka je $K=(K(j))\beta$. Neka je $\gamma=\alpha\cup\beta$. Tada je L literal u faktoru $(C)\alpha$ od C, i K literal u faktoru $(D)\beta$ od D. Jasno je da je L_1 faktor od L i K_1 faktor od K. Kako su L_1 i $-K_1$ unifabilni, to su i L i K unifabilni i neka je δ njihov najopštiji zajednički unifikator. Neka je:

$$R= (((C)\gamma)\delta-(L)\delta) \cup (((D)\gamma)\delta-(K)\delta)$$

$$= (((C)\gamma)\delta-(\{L(1),\ldots,L(i)\})\gamma)\delta) \cup (((D)\gamma)\delta-((\{K(1),\ldots,K(j)\})\gamma)\delta)$$

$$= ((C)(\gamma*\delta)-(\{L(1),\ldots,L(i)\})(\gamma*\delta) \cup (((D)(\gamma*\delta)-((\{K(1),\ldots,K(j)\})(\gamma*\delta))$$

R je rezolventa C i D. Jasno je da je R_1 faktor od R jer je

$$R_1= ((C_1)\sigma-(L_1)\sigma) \cup ((D_1)\sigma-(K_1)\sigma)$$

$$= (((C)\ \theta)\sigma-(\{L(1),\ldots L(i)\})\ \theta)\sigma \cup (((D)\ \theta)\sigma-((\{K(1),\ldots K(j)\})\ \theta)\sigma$$

$$= ((C)\ (\theta*\sigma)-(\{L(1),\ldots L(i)\})\ (\theta*\sigma) \cup ((D)\ (\theta*\sigma)-((\{K(1),\ldots K(j)\})\ (\theta*\sigma))$$

i $\gamma*\delta$ je opštiji nego $\theta*\sigma$.

Time je dokaz leme završen.

2. NEKE PROSTE STRATEGIJE

2.1 POJAM STRATEGIJE

U prethodnom odeljku izložen je rešavajući postupak (metod rezolucije). Pokazano je da je to dosta efikasan metod za dokazivanje teorema i dokazana je njegova potpunost. Direktno korišćenje rešavajućeg postupka za dokazivanje teoreme, tj. utvrđivanje nezadovoljivosti nekog skupa S sastavaka sastoji se u sledećem: izračunaju se sve rezolvente parova sastavaka iz S, dodaju se te rezolvente skupu S, izračunaju se sve dalje rezolvente parova sastavaka ovog skupa, dodaju se prethodnom skupu i ponavlja se ovaj proces sve dok se ne izvede prazan sastavak. Precizirajući rečeno generiše se jedan niz skupova $S_0, S_1, S_2, \ldots$ gde je $S_0=S$, $S_n=\{$rezolventa od $C_1, C_2 \mid C_1 \in S_0 \cup S_1 \cup \ldots \cup S_{n-1}, C_2 \in S_{n-1}\}$, sve dok se za neko n ne utvrdi da prazan sastavak pripada S_n. Ovaj postupak se naziva METOD ZASIĆENJA NIVOA.

Generišući sve moguće rezolvente skupa sastavaka, generiše se veliki broj rezolventi od kojih nisu sve značajne. Sve moguće rezolvente ne učestvuju u najkraćem izvođenju praznog sastavka. Mnoge od izvedenih rezolventi su nevažne, kao na primer tautologije, što je očigledno, jer dodavanjem tautologije nekom skupu sastavaka ne utiče se na njegovu nezadovoljivost. Neke izvedene rezovlente su prosto suvišne, ne učestvuju u direktnoj dedukciji praznog sastavka, nego samo stvaraju nove rezolvente koje su nebitne za dokaz. Osim toga, često se generiše nova rezolventa i dodaje spisku.

Sve ove nevažne generisane rezolvente, ne samo da opterećuju izvođenje kada ih izračunavamo i zapisujemo, nego i u sledećem koraku kod izračunavanja rezolventi sledećeg nivoa, troši se vreme na ispitivanje njihove interakcije sa drugim sastavcima, pri čemu se još i dalje dobijaju mnogobrojne neželjene, nevažne rezolvente. Pokažimo to na sledećem primeru.

PRIMER

Dokazati nezadovoljivost skupa sastavaka:

$S=\{P \vee Q, -P \vee Q, P \vee -Q, -P \vee -Q\}$.

Navedimo prvo najkraći dokaz u tom smislu da od njega ne postoji kraći:

(1)	$P \vee Q$	
(2)	$-P \vee Q$	
(3)	$P \vee -Q$	
(4)	$-P \vee -Q$	
(5)	Q	rezolventa od (1) i (2)
(6)	$-Q$	rezolventa od (3) i (4)
(7)	NIL	rezolventa od (5) i (6)

Direktno, metodom zasićenja nivoa dobija se dokaz koji sadrži 39 članova.

(1) $P \vee Q$

(2) $-P \vee Q$

(3) $P \vee -Q$

(4)	$\neg P \vee \neg Q$	
(5)	Q	od (1) i (2)
(6)	P	od (1) i (3)
(7)	$Q \vee \neg Q$	od (1) i (4)
(8)	$P \vee \neg P$	od (1) i (4)
(9)	$Q \vee \neg Q$	od (2) i (3)
(10)	$P \vee \neg P$	od (2) i (3)
(11)	$\neg P$	od (2) i (4)
(12)	$\neg Q$	od (3) i (4)
(13)	$P \vee Q$	od (1) i (7)
(14)	$P \vee Q$	od (1) i (8)
(15)	$P \vee Q$	od (1) i (9)
(16)	$P \vee Q$	od (1) i (10)
(17)	Q	od (1) i (11)
(18)	P	od (1) i (12)
(19)	Q	od (2) i (6)
(20)	$\neg P \vee Q$	od (2) i (7)
(21)	$\neg P \vee Q$	od (2) i (8)
(22)	$\neg P \vee Q$	od (2) i (9)
(23)	$\neg P \vee Q$	od (2) i (10)
(24)	$\neg P$	od (2) i (12)
(25)	P	od (3) i (5)
(26)	$P \vee \neg Q$	od (3) i (7)
(27)	$P \vee \neg Q$	od (3) i (8)
(28)	$P \vee \neg Q$	od (3) i (9)
(29)	$P \vee \neg Q$	od (3) i (10)
(30)	$\neg Q$	od (3) i (11)
(31)	$\neg P$	od (4) i (5)
(32)	$\neg Q$	od (4) i (6)
(33)	$\neg P \vee \neg Q$	od (4) i (7)
(34)	$\neg P \vee \neg Q$	od (4) i (8)
(35)	$\neg P \vee \neg Q$	od (4) i (9)
(36)	$\neg P \vee \neg Q$	od (4) i (10)
(37)	Q	od (5) i (7)
(38)	Q	od (5) i (9)
(39)	NIL	od (5) i (12)

Primena pravila rezolucije koja nije ničim sputavana, može generisati mnogo nevažnih sastavaka pored onih važnih (koji direktno učestvuju u dedukciji praznog sastavka). Prema tome da bi se dobila jedna efikasna procedura dokazivanja teorema, mora se na neki način sprečiti generisanje velikog broja tih nevažnih sastavaka, intuitivno, napraviti neki redosled u primeni pravila rezolucije.

Osnovno pitanje za građenje strategije je kako izabrati parove sastavaka, na koje treba primeniti pravilo rezolucije, jer očigledno, jedan dobar izbor mnogo poboljšava efikasnost metoda. Postoje mnogi radovi posvećeni ovom problemu i razrađene su mnoge, vrlo dobre strategije, tj. poboljšanja pravila rezolucije.

Sve strategije se u suštini sastoje:

(1) ili u postavljanju određenog kriterijuma, pa se rezolucija primenjuje samo na sastavke koje zadovoljavaju taj kriterijum (tako se ometa generisanje mnogih rezolventi)

(2) ili u određivanju primene rezolucije, tj. definiše se strogo kojim će se redosledom primenjivati rezolucija.

Jedna od bitnih osobina osim efikasnosti je da data strategija bude i potpuna što je i slučaj kod najvažnijih strategija.

2.2 ČISTI LITERALI

Prema teoremi Čerča o neodlučivosti predikatskog računa prvog reda, za neke skupove sastavaka ni jedna procedura opovrgavanja neće završiti rad, a izračunavanje rezolventi se može produžiti u beskonačnost. Ipak, u nekim slučajevima se može predvideti beskonačnost procesa.

PRIMER. Ispitati nezadovoljivost skupa sastavaka:

$S= \{ P(a), \ \neg P(x) \vee P(f(x)) \}$.

Procedura opovrgavanja generiše redom rezolvente:

$P(f(a)), P(f(f(a))), P(f(f(f(a)))), \ldots$

Navedeni primer navodi na pomisao o pravilu koje bi dozvoljavalo prepoznavanje beskonačnog procesa u slučaju njegovog nastanka, tako da bi se to pravilo moglo uključiti u proceduru opovrgavanja. Pri tome bi se procedura završila i u slučajevima koji analogno navedenom primeru proizvode beskonačan proces. Takvo pravilo je moguće uvesti, ono je osnovano na pojmu literala čistog u skupu sastavaka.

DEF 2.1 ČISTI LITERALI

Neka je S proizvoljan konačan skup sastavaka, C sastavak iz S i L literal iz C. L je ČIST u S ako ne postoji literal K iz $S-\{C\}$, i zamene α i β takve da je $(L)\alpha=(\neg K)\beta$.

Očigledno je da je literal L iz C čist u S, ako ne postoji rezolventa R(C,D), $C\neq D$, tako da je L isključeni literal.

TEOREMA 2.2 TEOREMA O ČISTIM LITERALIMA

Neka je S proizvoljan skup sastavaka, L literal iz C koji je čist u S. S je zadovoljiv ako i samo ako je $S-\{C\}$ zadovoljiv.

DOKAZ:

Ako je S zadovoljiv, tada je i $S-\{C\}$ zadovoljiv, jer je $S-\{C\}$ podskup od S.

Ako je $S-\{C\}$ zadovoljiv, tada postojoi model A za $S-\{C\}$, koji sadrži literale skup svih fundamentalnih literala oblika $(L)\theta$, gde je θ zamena nad H, i neka se K sastoji iz komplemenata svih literala iz N. Tada je skup $B=N\cup(A-K)$ model. Osim toga, to je model i za S, jer svaki sastavak u $H(\{C\})$ sadrži član iz B (ustvari bilo koji član iz N) i svaki sastavak iz $H(S-\{C\})$ sadrži član iz B, ustvari neki član iz A-K. Nijedan sastavak iz $H(S-\{C\})$ ne sadrži članove iz K, jer u protivnom slučaju, ako bi $(D)\beta$ bio takav sastavak, ($D\in S-\{C\}$), onda bi postojalo takvo M, da $M \subseteq D$, a $(M)\beta$ jednočlani skup koji sadrži član K. Tada bi postojala neka zamena α nad H takva da su skupovi $\{L\}\alpha$ i $\{M\}\beta$ jednočlani skupovi čiji elementi obrazuju komplementaran par. Međutim, to protivreči čistoći literala L u S. Time je teorema dokazana.

PRAVILO ČISTOĆE

Moguće je izostaviti iz konačnog skupa S sastavaka svaki sastavak koji sadrži literal čist u S.

Na taj način procedura opovrgavanja koja ujedinjuje pravilo rezolucije i pravilo čistoće "konvergira" za širi skup konačnih skupova sastavaka, nego procedura koja se zasniva samo na pravilu rezolucije. Takva pravila, kao što je pravilo čistoće, nazivaju se TAKTIKE PRETRAŽIVANJA, da bi se razlikovala od pravila izvođenja

2.3 STRATEGIJE UPIJANJA I BRISANJA

Pored strategija opovrgavanja, koje proširuju oblast konvergencije osnovne strategije, postoje i strategije koje povećavaju brzinu konvergencije. Jedna od takvih strategija je i strategija upijanja.

DEF 2.3 UPIJANJE, PODSASTAVAK, NADSASTAVAK.

Neka su C i D dva različita neprazna sastavaka. C UPIJA D ako postoji zamena α takva da je svaki literal iz $(C)\alpha$ istovremeno i u D. C se naziva PODSASTAVAK, a D NADSASTAVAK. Ako se sastavak posmatra kao skup svojih literala, može se koristiti oznaka $(C)\alpha\subseteq D$.

TEOREMA 2.4 TEOREMA O UPIJANJU

Neka je S proizvoljan konačan skup sastavaka, D nadsastavak iz S, a C sastavak iz $S-\{D\}$ koji upija D. S je zadovoljiv ako i samo ako je zadovoljiv $S-\{D\}$.

DOKAZ:

Dovoljno je dokazati da ako je M model za $S-\{D\}$, onda je M model za S. Neka je M model za $S-\{D\}$ i neka $C\in S-\{D\}$ upija D. Tada postoji takva zamena α tako da je svaki literal iz $(C)\alpha$ istovremeno i u D. Kako je D iz S, to su termi, komponenata zamene α izgrađeni iz simbola funkcija koje ulaze u funkcijski rečnik istovremeno fundamentalni faktor C nad H, i zato sadrži član iz M. Ali svaki fundamentalni faktor $(D)\beta$ sastavka D sadrži fundamentalni faktor $((C)\alpha)\beta$ sastavka C, i zato sadrži član iz M. Zato je M model za S, i teorema je dokazana.

STRATEGIJA UPIJANJA se formuliše na sledeći način:

Moguće je izostaviti iz konačnog skupa S sastavaka, svaki nadsastavak D koji je upijen nekim sastavkom C iz $S-\{D\}$.

Da bi se strategija upijanja mogla uključiti u proceduru opovrgavanja, potrebno je definisati algoritam koji proverava da li jedan sastavak upija drugi sastavak.

ALGORITAM 2.5 ALGORITAM UPIJANJA

ULAZ: sastavci C i D.

IZLAZ: odgovor da li C upija D.

KORAK 1. Neka su $v_1, \ldots, v_k$ sve promenljivih koje ulaze u D poređane po leksikografskom poretku, i $a_1, \ldots, a_k$ nove različite konstante koje se ne sadrže ni u C ni u D. Neka je $\beta=\{a_1/v_1, \ldots, a_k/v_k\}$. Ako je $D=L_1 \vee \ldots \vee L_m$, tada je $(D)\beta=(L_1)\beta \vee \ldots \vee (L_m)\beta$. Staviti $B=\{(-L_1)\beta, \ldots, (-L_m)\beta\}$ i preći na korak 2.

KORAK 2. Staviti $A(0)=C$, $k=0$ i preći na korak 3.

KORAK 3. Ako $A(k)$ sadrži NIL, zaustaviti se: C upija D. U protivnom slučaju staviti $A(k+1) = \{R(C_1,C_2) \mid C_1\in A(k), C_2\in B\}$.

KORAK 4. Ako je $A(k+1)$ prazan, zaustaviti se: C ne upija D. U protivnom, staviti $k=k+1$ i preći na korak 3.

Primetimo da u datom algoritmu svaki sastavak u $A(k+1)$ je za jedan literal kraći nego u $A(k)$ iz kojeg je dobijen. Zato u nizu $A(0), A(1) \ldots$ treba na kraju da se pojavi ili prazan skup ili skup koji sadrži NIL.

TEOREMA 2.6 KOREKTNOST ALGORITMA UPIJANJA

Sastavak C upija D ako i samo ako algoritam završava rad na koraku 3.

DOKAZ:

Neka C upija D. Tada postoji zamena α tako da je $(C)\alpha \subseteq D$. Zato je $((C)\alpha)\beta \subseteq (D)\beta$, i literali iz $((C)\alpha)\beta$ mogu biti isključeni korišćenjem jediničnih sastavaka iz B. To znači da će se na kraju pronaći $A(k)$ koji sadrži NIL. Tada algoritam završava rad na koraku 3.

Obrnuto, pretpostavimo da algoritam završava rad na koraku 3. Tada postoji izvođenje $R_1=R(C,B_0)$, $R_2=R(R_1,B_1)$, $\ldots$, $NIL=R(R_k,B_k)$, pri čemu su $B_0, \ldots B_k$ jedinični sastavci iz B. Neka je $\alpha(0)$ najopštiji zajednički unifikator dobijen pri traženju rezolvente C i B_0, $\alpha(i)$ najopštiji zajednički unifikator za R_i i B_i, $i=1, \ldots, k$. Tada $(\ldots((C)\alpha(0))\ldots\alpha(k))=\{-B_0, -B_1, \ldots, -B_k\} \subseteq (D)\beta$. Neka je $\gamma=\alpha(0)*\alpha(1)*\ldots*\alpha(k)$. Tada $(C)\gamma \subseteq (D)\beta$. Neka je δ zamena dobijena iz γ zamenom a_i u svakoj komponenti zamene sa x_i, $i=1,\ldots, n$. Tada $(C)\delta \subseteq D$, što znači da C upija D što je i trebalo dokazati.

Veoma korisna primena strategije upijanja je u sledećem slučaju. Neka rezolventa R sastavaka C i D, upija jedan od njih. Tada dodavši R po pravilu rezolucije, polaznom skupu sastavaka, istovremeno možemo izostaviti (korišćenjem taktike upijanja), onaj od sastavaka C ili D koji je upijen njihovom rezolventom. Ta operacija se svodi na zemenjivanje C ili D sa R. Odgovarajuće pravilo se naziva pravilo zamenjivanja, a strategija - STRATEGIJA ZAMENJIVANJA.

STRATEGIJA BRISANJA je strategija koja objedinjava brisanje tautologija i nadsastavaka. To je jednostavno strategija pojednostavljivanja. U njenoj primeni se ne ometa izvođenje svih rezolventi na jednom nivou, već se brišu neki od nevažnih sastavaka, pošto su oni već izvedeni pomoću rezolucije. Preciznije, novoizvedena rezolventa se briše ako je tautologija ili je nadsastavak nekog sastavka koja je već izveden.

Za primenu strategije brisanja potrebno je poznavati postupak za ispitivanje da li je neki sastavak tautologija. Sastsavak je tautologija ako sadrži komplementaran par literala, što je jednostavno ispitati. Za utvrđivanje da li je jedan sastavak nadsastavak drugog, može se koristiti algoritam upijanja.

POTPUNOST strategije brisanja zavisi od toga kako se brišu tautologije i nadsastavci. To je rezultat Kovalskog[**].

TEOREMA 2.7 POTPUNOST STRATEGIJE BRISANJA

Strategija brisanja je potpuna ako se u metodu zasićenja nivoa brišu sledeći sastavci: tautologije uvek i nadsastavak samo u slučaju kada je njegov podsastavak iz skupa istog ili nižeg nivoa.

3. SEMANTIČKA REZOLUCIJA

3.1 POJAM SEMANTIČKE REZOLUCIJE

Semantička rezolucija se prvi put pojavila 1967.god. u radu Slagle /*/. Ona sjedinjuje hiperrezoluciju Robinsona, preimenovanu rezoluciju Melcera /*/ i strategiju pomoćnog skupa Wosa, Robinsona i Carsona /*/. Ideja semantičke rezolucije se sastoji u podeli osnovnog skupa sastavaka na dve grupe, pri čemu se zahteva da sastavci koji učestvuju u rezoluciji ne budu iz iste grupe. Za podelu sastavaka na grupe koristi se neka interpretacija. Zato je ova rezolucija i dobila naziv semantička. Ako je S nezadovoljiv skup sastavaka, ni jedna interpretacija ne može zadovoljiti ili opovrgnuti sve sastavke. Zato svaka interpretacija deli S na dva neprazna skupa sastavaka, skup zadovoljivih (S_1) i skup nezadovoljivih sastavaka (S_2).

Drugi način onemogućavanja izvođenja suvišnih rezolventi je uređenje predikatskih simbola, i zahtev da pri primeni rezolucije na dva sastavka C i D, $C \in S_1$, $D \in S_2$, isljučeni literal iz D sadrži najveći predikatski simbol u tom sastavku.

Navedene ideje, korišćenje interpretacije za razbijanje sastavaka na dve grupe i uređivanje predikatskih simbola za smanjenje broja mogućih rezolventi su važni pojmovi u semantičkoj rezoluciji. Pored toga, poželjno je onemogućiti različita izvođenja jednog istog sastavka, kao u sledećem primeru.

PRIMER. Dokazati nezadovoljivost skupa sastavaka.

(1) $-P \lor -Q \lor R$

(2) $P \lor R$

(3) $Q \lor R$

(4) $-R$.

Neka je interpretacija $I = \{-P, -Q, -R\}$, i neka su predikatski simboli uređeni na sledeći način: $P > Q > R$. S_1 su sastavci (1) i (4), S_2 su (2) i (3). Primenivši ograničenja moguće je izvesti:

(5) $-Q \lor R$ iz (1) i (2)

(6) $-P \lor R$ iz (1) i (3).

Oba ova sastavka su zadovoljiva u interpretaciji I, zato ih dodajmo skupu sastavaka S_2. Primenom rezolucije sa sastavcima iz S_1 dobija se:

(7) R iz (3) i (5)

(8) R iz (2) i (6).

Primetimo da su dobijena dva različita izvođenja sastavka R. Kako je u dokazu dovoljno samo jedno izvođenje, uvodi se novi pojam kojim se poistovećuju različite varijante izvođenja istog sastavka.

3.2 DEFINICIJA PI-REZOLUCIJE

DEF 3.1 DEFINICIJA SEMANTIČKE REZOLUCIJE (PI REZOLUCIJE)

Neka je I interpretacija i P uređeni niz predikatskih simbola. **Konačan skup** sastavaka [illegible]

I (ili PI SUKOB), ako $E_1, \dots, E_q$ (nazvani elektroni) i N (nazvan nukleus) zadovoljavaju sledeće uslove:

(1) $E_1, E_2, \dots, E_q$ je lažno u I.

(2) Neka je R_1=N. Za svako i=2, ... , q postoji rezolventa R_{i+1} od R_i i E_i.

(3) Literal u E_i koji je primenjen u gornjoj rezoluciji sadrži najveći predikatski simbol u E_i (i=1, ... , q).

R_{q+1} je lažno u interpretaciji I.

R_{q+1} se naziva semantička ili PI-rezolventa (od PI sukoba $\{E_1, \dots, E_q, N\}$).

PRIMER. Neka je:

E_1= -Q(z) ∨ -Q(a)

E_2= R(b) ∨ S(c)

N= Q(x) ∨ Q(a) ∨ -R(y) ∨ -R(b) ∨ S(c).

Neka je I interpretacija {Q(a), Q(b), Q(c), -R(a), -R(b), -R(c), [illegible] S(c)}, i P sledeće uređenje predikatskih simbola Q > R > S.

Stavimo R_1=N.

Postoji rezolventa R_2 sastavaka R_1 i E_1 R_2=R(R_1, E_1)= -R(y) ∨ -R(b) ∨ [illegible]

Postoji rezolventa R_3 sastavaka R_2 i E_2. R_3= R(R_2,E_2)= S(c) ∨ S(c) [illegible] interpretaciji I.

Skup {E_1, E_2, N} zadovoljava sva četiri uslova, i zato je to PI sukob. PI rezolventa ovog sukoba je S(c).

DEF 3.2 PI-DEDUKCIJA

Neka je I interpretacija skupa sastavaka S, i P uređen niz predikatskih simbola koji se pojavljuju u S. Dedukcija iz S se naziva PI-dedukcija ako je svaki sastavak u dedukciji ili sastavak iz S ili PI-rezolventa.

Za semantičku rezoluciju je karakteristično da je moguće koristiti svaki niz i svaku interpretaciju. U stvari PI-rezolucija je potpuna, tako da se iz svakog nezadovoljivog skupa sastavaka uvek može izvesti prazan sastavak korišćenjem PI-rezolucije.

3.3 POTPUNOST PI-REZOLUCIJE

LEMA 3.3. POTPUNOST FUNDAMENTALNE PI-REZOLUCIJE

Neka je S konačan nezadovoljiv skup fundamentalnih sastavaka, P uređen niz predikatskih simbola, I interpretacija skupa S. Tada postoji PI-dedukcija sastavka NIL iz S.

DOKAZ:

Koristimo metod matematičke indukcije po broju atoma najdužeg sastavka.

Neka je A skup atoma iz S. Ako se A sastoji od jednog elementa na primer Q, onda među elementima u S postoje sastavci Q ili -Q. Rezolventa od Q i -Q je NIL. Kako je ili Q ili -Q lažno u I, i kako je NIL lažno u I, onda je NIL PI-rezolventa. Zato lema važi za ovaj slučaj.

Pretpostavimo da lema važi uvek kada se A sastoji od n elemenata $1 \leq i \leq n$. Da bi primenili indukciju, neka se A sastoji od tačno n+1 elemenata. Posmatrajmo sledeće slučajeve:

Slučaj 1.

S sadrži jedinični sastavak L koja je lažan u I (L je Literal). Neka je S_0 skup dobijen iz S izostavljanjem onih sastavaka koji sadrže literal L i izostavljanjem -L iz ostalih sastavaka. Jasno je da je So nezadovoljiv. Kako S_0 sadrži n ili manje od n atoma, prema indukcijskoj hipotezi postoji PI-dedukcija D_0 sastavka NIL iz S_0. Iz dedukcije D_0 možemo dobiti PI-dedukciju NIL iz S, na sledeći način:

Svaki PI sukob $\{E_1, \ldots, E_q, N\}$ zamenimo PI sukobom $\{E_1, E_2, \ldots, E_q, L, N_1\}$, ako je N dobijeno od sastavka N_1 iz S, izostavljanjem L iz N_1, gde su $E_1, \ldots, E_q$, N sastavci u izvođenju D_0, (sada su $E_1, \ldots, E_q$, L elektroni, a N_1 nukleus).

Ako je E_i dobijeno od sastavka F_i iz S, izostavljanjem -L iz F_i, odgovarajući P_i sukob za dobijanje E_i biće skup $\{L, F_i\}$. Tako se od dedukcije D_0 dobija PI-dedukcija D praznog sastavka NIL iz S.

Slučaj 2.

S ne sadrži jedinični sastavak koji je lažan u I. U tom slučaju izaberimo element B iz skupa A atoma iz S, tako da B sadrži najmanji predikatski simbol. Jedan od literala B ili -B je lažan u I. Neka je L onaj literal iz skupa $\{B,-B\}$ koji je lažan u I. Neka je S_0 skup dobijen iz S izostavljanjem onih sastavaka koje sadrže literal -L i izostavljanjem L iz ostalih sastavaka. S_0 je nezadovoljiv. Kako S_0 sadrži n ili manje od n atoma, prema indukcijskoj hipotezi postoji PI-dedukcija D_0 sastavka NIL iz S_0. Neka je D_1 dedukcija dobijena iz dedukcije D_0 vraćanjem literala L nazad u one sastavke odakle je izostavljen. D_1 je i PI-dedukcija, jer literal L sadrži najmanji predikatski simbol lažan u I. D_1 je ili PI-dedukcija NIL ili L.

Ako je D_1 dedukcija NIL, dokazali smo lemu. Ako je D_1 dedukcija L posmatrajmo skup $S \cup \{L\}$. Kako $S \cup \{L\}$ sadrži jedinični sastavak L koji je lažan u I, pomoću dokaza slučaja 1, postoji PI-dedukcija D_2, NIL iz $S \cup \{L\}$. Kombinovanjem D_1 i D_2, dobija se PI-dedukcija NIL iz S. Time je lema u potpunosti dokazana.

TEOREMA 3.4 POTPUNOST PI-REZOLUCIJE

Neka je S konačan nezadovoljiv skup sastavaka, P uređen niz predikatskih simbola, I interpretacija skupa S. Tada postoji PI-dedukcija sastavka NIL iz S.

DOKAZ:

Kako je S nezadovoljiv skup, prema teoremi ERBRANA postoji konačan nezadovoljiv skup S_0 fundamentalnih sastavaka, dobijen iz S zamenama promenljivih elemenata Erbranovog prostora. Prema lemi 3.3 postoji PI-dedukcija D_0 sastavka NIL iz skupa S_0. Pokažimo kako se može dedukcija D_0 transformisati u PI-dedukciju NIL iz S. Koristeći lemu o podizanju (LIFTING LEMA), ako su C_1 i D_1 faktori od C i D i ako je R_1 rezolventa od C_1 i D_1, tada postoji rezolventa R od C i D takva da je R_1 faktor od R. U dedukciji Do zamenimo svaki sastavak C_1 odgovarajućim sastavkom C, tako da je C_1 faktor od C.

Strategija brisanja se može koristiti zajedno sa PI-rezolucijom, ne narušavajući svojstvo potpunosti.

3.4 HIPERREZOLUCIJA

Neka je I interpretacija u kojoj je svaki literal negacija nekog atoma. U toj interpretaciji, svaki elektron i svaka PI-rezolventa mogu biti sastavljeni samo od atoma. Slično, ako je svaki literal u interpretaciji I atom, onda svaki elektron i svaka PI-rezolventa moraju da sadrže samo negacije atoma. Hiperrezolucija se zasniva na tim razmatranjima.

Sastavak se naziva POZITIVAN ako ne sadrži ni jedan znak negacije. NEGATIVAN sastavak je onaj čiji svi literali sadrže znak negacije. Sastavak je mešovit ako nije ni pozitivan ni negativan.

DEF 3.5 POZITIVNA I NEGATIVNA HIPERREZOLUCIJA

POZITIVNA HIPERREZOLUCIJA je specijalan slučaj PI-rezolucije, u kojoj svaki literal u interpretaciji I sadrži znak negacije. U tom slučaju svi elektroni i sve PI-rezolvente su pozitivni sastavci. NEGATIVNA HIPERREZOLUCIJA je specijalan slučaj PI-rezolucije, kada interpretacija I ne sadrži ni jedan znak negacije. Tada su svi elektroni i sve PI-rezolvente negativni sastavci.

Pozitivna i negativna hiperrezolucija su potpune jer su one specijalan slučaj semantičke rezolucije.

PRIMER. Za sledeći skup sastavaka.

$S = \{ Q(a) \vee R(x),\ \ -Q(x) \vee R(x),\ \ -R(a) \vee -S(a),\ \ S(x) \}$

Neka je P niz predikata $R < Q < S$. Onda dobijamo pozitivnu i negativnu hiperrezoluciju prikazanu na slici:

Čest je slučaj da se aksiome i teoreme predstavljaju pomoću nekih pozitivnih i mešovitih sastavaka, a negacija zaključka se predstavlja pomoću negativnog sastavka. U tom slučaju pozitivnoj hiperrezoluciji otprilike odgovara "razmišljanje unapred", dok negativnoj hierrezoluciji odgovara "razmišljanje unazad".

PRIMER. Neka su aksiome Q, R i $-Q \vee -R \vee S$, negacija zaključka $-S$, i neka je $R > S$ uređenje predikatskih simbola.

*
*
*
*
*
*
*
*
*
*

Prva dedukcija počinje sa aksiomama i izvodi S koje je kontradiktorno negaciji zaključka -S. Kod negativne hiperrezolucije dedukcija počinje iz negacije zaključka. Uzimajući da je zaključak lažan, izvodi se kontradikcija.

3.5 STRATEGIJA POMOĆNOG SKUPA

Strategiju pomoćnog skupa su predložili 1965. god. Wos, Robinson i Carson /**/.

Neka je teorema sastavljena od aksioma A_1, A_2, ... , A_n i zaključka B. Da bi dokazali teoremu, dokazujemo da je skup $\{A_1, A_2, \ldots , A_n, -B\}$ nezadovoljiv. Kako je A_1, ... , A_n obično zadovoljiv, nekorisno je tražiti rezolvente između A_1, A_2, ... , A_n. Na toj ideji se zasniva strategija pomoćnog skupa.

DEF 3.6 POMOĆNI SKUP

Podskup T skupa S sastavaka je POMOĆNI SKUP od S ako je S-T zadovoljiv. Rezolucija pomoćnog skupa je rezolucija dva sastavka koji nisu obe iz S-T. Dedukcija pomoćnog skupa je dedukcija u kojoj je svaka rezolucija rezolucija pomoćnog skupa.

Može se dokazati da je strategija pomoćnog skupa potpuna.

TEOREMA 3.7 POTPUNOST STRATEGIJE POMOĆNOG SKUPA

Ako je S konačan nezadovoljiv skup sastavaka i T podskup od S, tako da je S-T zadovoljv, onda postoji dedukcija pomoćnog skupa, praznog sastavka NIL iz S sa T kao pomoćnim skupom.

DOKAZ:

Kako je S-T zadovoljiv, postoji interpretacija I koja zadovoljava S-T. Izaberimo proizvoljno uređenje P predikatskih simbola u S. Koristeći teoremu 3.4 o potpunosti PI-rezolucije, postoji PI-dedukcija D praznog sastavka NIL iz S.

U dedukciji D posmatrajmo PI sukob $\{E_1, E_2, \ldots , E_q, N\}$.

PI-rezolventa ovog sukoba se dobija pomoću rezolucije E_1 i N, zatim rezolucije E_1 i izvedene rezolvente, i tako dalje. Svako primenjivanje rezolucije koristi neki elektron E_i. Međutim, elektron je lažan u interpretaciji I. Zato, za svaku način se PI-dedukcija može transformisati u dedukciju NIL iz S, koja je po konstrukciji dedukcija pomoćnog skupa.

PRIMER. Neka je S skup sastavljen od sledećih sastavaka:

(1) $P(g(x_1,y_1), x_1, y_1)$

(2) $-P(x_2, h(x_2, y_2), y_2)$

(3) $-P(x_3, y_3, u_3) \vee P(y_3, z_3, v_3) \vee -P(x_3, v_3, w_3) \vee P(u_3, z_3, w_3)$

(4) $-P(k(x_4), x_4, k(x_4))$

Neka je T skup koji sadrži sastavak (4). Tada je sledeća dedukcija, dedukcija pomoćnog skupa, sa T kao pomoćnim skupom. Primetimo da nije izvedena ni jedna rezolucija između aksioma.

(5) $-P(x_3, y_3, k(z_3)) \vee P(y_3, z_3, v_3) \vee -P(x_3, v_3, k(x_3))$ (4) i (3)

(6) $-P(x_3, y_3, k(k(y_3,v_3))) \vee -P(x_3, v_3, k(h(y_3, v_3)))$ (5) i (2)

(7) NIL (6) i (1)

3.6 UREĐENA REZOLUCIJA

Ideja uvođenja uređenih sastavaka se sastoji u posmatranju sastavka kao niza, a ne kao skupa literala. Time se određuje redosled literala u sastavku, koji se uvodi na prirodan način. Literal L_2 je veći od literala L_1 u sastavku C, ako se L_2 nalazi iza L_1 u nizu literala koji je određen sastavkom C. Na taj način poslednji literal u sastavku će uvek biti najveći literal.

DEF 3.8 UREĐENI SASTAVAK je niz različitih literala. Literal L_2 je VEĆI od literala L_1 u uređenom sastavku (ili L_1 je MANJI od L_2) ako se L_2 nalazi iza L_1 u nizu literala koji je određen uređenim sastavkom.

DEF 3.9 UREĐENI FAKTOR

Neka je C uređeni sastavak. Ako dva ili više literala u C (sa istim znakom) imaju najopštiji zajednički unifikator σ, uređeni faktor od C je sastavak dobijen iz $(C)\sigma$ izostavljanjem svakog literala koji je identičan nekom manjem literalu.

Jednostavno rečeno, ako se u sastavku zamenom može dobiti više identičnih literala, literal koji se prvi pojavljuje se zadržava, a ostali se izostavljaju.

DEF 3.10 UREĐENA BINARNA REZOLVENTA

Neka su C i D dva uređena sastavka bez zajedničkih promenljivih i L i K dva literala u C i D redom. Ako L i -K imaju najopštiji zajednički unifikator σ i ako je R sastavak dobijen od $(C)\sigma \vee (D)\sigma$ izostavljanjem $(L)\sigma$ i $(K)\sigma$ i izostavljanjem svakog literala koji se poklapa sa nekim manjim, onda se R naziva uređena binarna rezolventa od C i D. Literali L i K se nazivaju isključeni literali.

PRIMER. Neka su dati sastavci:

$C: P(x) \vee Q(x) \vee R(x)$ $\qquad$ $C_1: -P(a) \vee Q(a)$

Neka je $L=P(x)$ i $K=-P(a)$. L i -K imaju najopštiji unifikator $\sigma=\{a/x\}$. $(C)\sigma \vee (D)\sigma$ je $P(a)\vee Q(a)\vee -P(a)\vee Q(a)$. Izostavljanjem $(L)\sigma$ i $(K)\sigma$, dobija se $Q(a) \vee R(a) \vee Q(a)$. Izostavljanjem drugog pojavljivanja literala Q(a) dobija se sastavak $Q(a) \vee R(a)$ koji je uređena binarna rezolventa od C i D. Literali P(x) i -P(a) su isključeni literali.

DEF 3.11 UREĐENA REZOLVENTA

Naka su C_1 i C_2 dva uređena sastavka. Uređena rezolventa između C_1 i C_2 je jedna od sledećih binarnih uređenih rezolventi:

(1) uređena binarna rezolventa od C_1 i C_2

(2) uređena binarna rezolventa od C_1 i uređenog faktora od C_2

(3) uređena binarna rezolventa od uređenog faktora od C_1 i C_2

(4) uređena binarna rezolventa od uređenog faktora od C_1 i uređenog faktora od C_2.

3.7 DEFINICIJA OI-REZOLUCIJE

DEF 3.12 DEFINICIJA UREĐENE SEMANTIČKE REZOLUCIJE (ordered -uređen)

Neka je I interpretacija. Konačan skup uređenih sastavaka $\{E_1, E_2, \dots, E_q, N\}$ $q\geq 1$ naziva se UREĐENI SEMANTIČKI SUKOB u odnosu na I (ili OI SUKOB), ako $E_1, \dots, E_q$ (nazvani elektroni) i N (nazvan uređeni nukleus) zadovoljavaju sledeće uslove:

(1) $E_1, E_2 \dots, E_q$ je lažno u I.

(2) Neka je $R_q=N$. Za svako $i=q, q-1, \dots, 1$ postoji uređena rezolventa R_{i-1} od R_i i E_i.

(3) Isključeni literal u E_i je poslednji literal u E_i, $i=1, \dots, q$; isključeni literal u R_i je najveći literal koji ima faktor istinit u I.

(4) R_0 je lažno u interpretaciji I.

R_0 se naziva uređena semantička ili OI-rezolventa (od OI sukoba $\{E_1, \dots, E_q, N\}$).

DEF 3.13 OI-DEDUKCIJA

Neka je I interpretacija skupa uređenih sastavaka S. Dedukcija iz S se nazvia OI-dedukcija ako je svaki uređeni sastavak u dedukciji ili sastavak iz S ili OI-rezolventa.

Slagle i Norton /*/ su eksperimentisali sa OI rezolucijom. Njihovi rezultati govore da je to veoma efikasna strategija.

3.8 NEPOTPUNOST OI-REZOLUCIJE

Iako je OI rezolucija veoma efikasna, ona nije potpuna. Sledeći kontraprimer je naveo Anderson /21/.

KONTRAPRIMER 3.14 NEPOTPUNOST UREĐENE SEMANTIČKE REZOLUCIJE

Neka je S sledeći skup uređenih sastavaka:

(1) $P \vee Q$,

(2) $Q \vee R$,

(3) $R \vee W$,

(4) $-R \vee -P$,

(5) $-W \vee -Q$,

(6) $-Q \vee -R$.

Neka je I interpretacija u kojoj je svaki literal negativan. Tada sastavci (1) - (3) mogu biti korišćeni kao uređeni elektroni, a sastavci (4)-(6) kao uređeni nukleusi. Od sastavaka (4)-(6) mogu se dobiti sledeće OI rezolvente:

(7) $R \vee P$ iz OI sukoba ((3), (1), (5)),

(8) $P \vee Q$ iz OI sukoba ((1), (2), (6)).

Od sastavaka (1)-(8) može se dobiti sledeća OI rezolvena.

(9) $Q \vee R$ iz OI sukoba ((2), (7), (4)).

Sastavci (8) i (9) ne pripadaju S. Zato se od sastavaka (1)- 9) ne može dobiti ni jedna nova OI rezolventa. Drugim rečima, NIL se ne može dobiti pomoću OI rezolucije. Ali S je nezadovoljiv skup sastavaka. Zato OI rezolucija nije potpuna.

4. LOCK REZOLUCIJA

4.1 POJAM LOCK REZOLUCIJE

LOCK rezolucija se pojavila u doktorskoj disertaciji Boera 1971. god. /20/. Ideja LOCK rezolucije (lock - zabraviti, zaključati) se sastoji u onemogućavanju izvođenja svih rezolventi. To se postiže korišćenjem indeksa za sređivanje literala u skupu sastavaka S. Svako pojavljivanje literala u S je indeksirano. Pri tome razna pojavljivanja jednog istog literala u S mogu biti različito indeksirana. Rezolucija se primenjuje samo na literale najnižeg indeksa u svakom sastavku. Literali u rezolventi nasleđuju svoj indeks od sastavaka od kojih je nastala rezolventa (sastavci roditelji). Ako rezolventa sadrži više identičnih literala koji imaju različite indekse, literal najnižeg indeksa se čuva, a ostali se izostavljaju. Za indeksiranje je najzgodnije koristiti prirodne brojeve, mada se mogu koristiti elementi bilo kog uređenog skupa. Sastavak čiji su svi literali indeksirani naziva se INDEKSIRANI sastavak.

DEF 4.1 LOCK-FAKTOR

Neka je C indeksirani sastavak. Ako dva ili više literala u C (sa istim znakom) imaju najopštiji zajednički unifikator σ, Lock-faktor od C je sastavak dobijen iz $(C)\sigma$ izostavljanjem svakog literala koji je identičan literalu nižeg indeksa.

Jednostavno rečeno, ako se u sastavku zamenom može dobiti više identičnih literala, literal sa najnižim indeksom se zadržava, a ostali se izostavljaju. Ova operacija se naziva čuvanje nižeg za identične literale.

DEF 4.2 BINARNA LOCK-REZOLVENTA

Neka su C i D dva indeksirana sastavka bez zajedničkih promenljivih i L i K dva literala najnižih indeksa u C i D redom. Ako L i -K imaju najopštiji unifikator σ i ako je R sastavak dobijen iz $(C)\sigma \vee (D)\sigma$ izostavljanjem $(L)\sigma$ i $(K)\sigma$ i čuvanjem nižeg literala u ostalom delu sastavka, onda se R naziva binarna Lock-rezolventa od C i D.

PRIMER. Neka su dati sastavci:

C_1: ${}_1P(x) \vee {}_2Q(x) \vee {}_3R(x)$ $\quad$ C_2: ${}_4\text{-}P(a) \vee {}_5Q(a)$.

Kako ${}_1P(x)$ i ${}_4\text{-}P(a)$ imaju najniže indekse u C_1 i C_2 redom, biramo $L_1=P(x)$ i $L_2=\text{-}P(a)$. L_1 i L_2 imaju najopštiji unifikator $\sigma=\{a/x\}$. Zato je $(C_1)\sigma \vee (C_2)\sigma= {}_1P(a) \vee {}_2Q(a) \vee {}_3R(a) \vee {}_4\text{-}P(a) \vee {}_5Q(a)$.

Izostavljanjem $(L_1)\sigma$ i $(L_2)\sigma$, tj. ${}_1P(a)$ i ${}_4\text{-}P(a)$ dobija se: ${}_2Q(a) \vee {}_3R(a) \vee {}_5Q(a)$. Sada su ${}_2Q(a)$ i ${}_5Q(a)$ identični literali sa različitim indeksima. Čuvanjem nižeg dobija se: ${}_2Q(a) \vee {}_3R(a)$. To je binarna Lock-rezolventa sastavaka C_1 i C_2.

DEF 4.3 LOCK-REZOLVENTA

Neka su C_1 i C_2 dva indeksirana sastavka. Lock-rezolventa između C_1 i C_2 je jedna od sledećih binarnih Lock rezolventi:

(1) binarna Lock rezolventa od C_1 i C_2

(2) binarna Lock rezolventa od C_1 i Lock-faktora od C_2

(3) binarna Lock rezolventa od Lock-faktora od C_1 i C_2

(4) binarna Lock rezolventa od Lock-faktora od C_1 i Lock-faktora od C_2.

DEF 4.4 LOCK DEDUKCIJA

Neka je S skup sastavaka gde je svaki literal u S indeksiran. Dedukcija iz S je Lock-dedukcija ako je svaki sastavak koji u njoj učestvuje ili sastavak iz S ili Lock-rezolventa.

PRIMER. Dokazati nezadovoljivost sledećeg skupa sastavaka

(1) ${}_1P \lor {}_2Q$

(2) ${}_3P \lor {}_4\text{-}Q$

(3) ${}_6\text{-}P \lor {}_5Q$

(4) ${}_8\text{-}P \lor {}_7\text{-}Q$.

Iz sastavaka (1)-(4) moguće je izvesti samo jednu Lock rezolventu:

(5) ${}_6\text{-}P$ iz (3) i (4).

Iz sastavaka (1)-(5) moguće je izvesti dve Lock rezolvente:

(6) ${}_2Q$ iz (1) i (5),

(7) ${}_4\text{-}Q$ iz (2) i (5).

Na kraju se dobija prazan sastavak

(8) NIL iz (5) i (6).

U dokazu učestvuju samo tri Lock rezolvente. Ukoliko se koristi obična rezolucija, po metodu zasićenja nivoa (primer iz odeljka 2.1), u izvođenju praznog sastavka NIL učestvuje 35 rezolventi.

PRIMER. Dokazati nezadovoljivost sledećeg skupa sastavaka:

(1) ${}_5P(y,a) \lor {}_1P(f(y),y)$

(2) ${}_6P(y,a) \lor {}_2P(y,f(y))$

(3) ${}_8\text{-}P(x,y) \lor {}_3P(f(y),y)$

(4) ${}_9\text{-}P(x,y) \lor {}_4P(y,f(y))$

(5) ${}_{10}\text{-}P(x,y) \lor {}_7\text{-}P(y,a)$.

Iz S je moguće dobiti sledeću Lock dedukciju NIL:

(6) ${}_5P(a,a) \lor {}_{10}\text{-}P(x,f(a))$ iz (1) i (5)

(7) ${}_8\text{-}P(x,a) \lor {}_{10}\text{-}P(y,f(a))$ iz (3) i (5)

(8) ${}_{10}\text{-}P(x,f(a)) \lor {}_{10}\text{-}P(y,f(a))$ iz (6) i (7)

(9) ${}_6P(a,a)$ iz (8) i (2)

(10) ${}_7\text{-}P(x,a)$ iz (8) i (4)

(11) NIL iz (9) i (10).

4.2 POTPUNOST LOCK REZOLUCIJE

LEMA 4.5 POTPUNOST LOCK-REZOLUCIJE ZA OSNOVNI SLUČAJ

Neka je S skup fundamentalnih sastavaka gde je svaki sastavak u S indeksiran sa prirodnim brojem. Ako je S nezadovoljiv, tada postoji Lock-dedukcija praznog sastavka NIL iz S.

DOKAZ:

Neka je K(S) definisano kao:

K(S)= broj pojavljivanja literala u S - broj sastavaka u S.

K(S) se naziva suvišak literala. Lema se dokazuje matematičkom indukcijom po K(S). Ako je NIL u S lema je dokazana. Neka NIL nije u S.

Ako je K(S)=0, tada se S sastoji samo od jediničnih sastavaka. Kako je S nezadovoljiv, postoji literal L takav da su ${}_iL$ i ${}_j$-L u S, gde su i i j indeksi tih literala. Lock rezolventa od ${}_iL$ i ${}_j$-L je NIL. Time je pokazano da lema važi kada je K(S)=0.

Neka lema važi kada je K(S) manje od n. Dokažimo da važi i za K(S)=n. Kako je K(S) veće od 0, postoji najmanje jedan sastavak u S koji nije jedinični.

Neka je m najveći indeks kod svih onih sastavaka iz S koji nisu jedinični. Neka je C sastavak koji nije jedinični i koji sadrži literal ${}_mL$ indeksiran sa m, a C_0 sastavak dobijen od C izostavljanjem literala ${}_mL$. C_0 nije prazan sastavak jer C nije jedinični sastavak. Neka je:

S_1= (S- {C})∪{C_0} i S_2= (S- {C})∪{${}_mL$}.

Skupovi sastavaka S_1 i S_2 su nezadovoljivi. K(S_1) je manje od n, i K(S_2) je manje od n. Zato prema indukcijskoj hipotezi postoje Lock-dedukcije D_1' i D_2' praznog sastavka NIL iz S_1 i S_2. Neka je D_1 dedukcija dobijena iz D_1' stavljanjem ${}_mL$ nazad u C_0. Kako je m najveći indeks u sastavku C, jasno je da je D_1 takođe Lock dedukcija. Rezultat te Lock dedukcije je NIL ili ${}_mL$. Ako je to NIL, dokaz je završen. Ako je to ${}_mL$, kombinovanjem D_1 i D_2' dobija se Lock dedukcija NIL iz S. Ovim je dokaz leme završen.

TEOREMA 4.6 POTPUNOST LOCK-REZOLUCIJE

Neka je S konačan nezadovoljiv skup indeksiranih sastavaka. Tada postoji Lock-dedukcija praznog sastavka NIL iz S.

DOKAZ:

Kako je S nezadovoljiv skup, prema teoremi ERBRANA postoji konačan nezadovoljiv skup S_0 fundamentalnih literala, dobijen iz S zamenama promenljivih elementima Erbranovog prostora. Prema lemi 4.5 postoji Lock-dedukcija D_0 sastavka NIL iz skupa S_0. Koristeći lemu o podizanju (LIFTING lemu), i rasuđivanje slično onom koje je korišćeno u dokazu teoreme 3.4 od dedukcije D_0 može se konstruisati Lock dedukcija D praznog sastavka NIL. Time je teorema dokazana.

4.3 OGRANIČENOST LOCK REZOLUCIJE

Lock rezolucija je potpuna sama za sebe, ali se ne može kombinovati sa većinom drugih strategija. Sledeći primer pokazuje da sjedinjavanje Lock rezolucije i strategije brisanja tautologija u jednu strategiju ne daje potpunu strategiju.

PRIMER 4.7

(1) $_1P \vee {_2Q}$

(2) $_8P \vee {_7\text{-}Q}$

(3) $_4\text{-}P \vee {_3Q}$

(4) $_5\text{-}P \vee {_6\text{-}Q}$.

Za sastavke (1) i (2) ne postoji Lock-rezolventa, jer literali $_2Q$ i $_7\text{-}Q$ nemaju najmanji indeks u sastavcima (1) i (2) redom. Takođe za sastavke (1) i (3) ne postoji Lock-rezolventa, jer literal $_4P$ nema najmanji indeks u sastavku (3)

Za sastavke (1) i (4) Lock-rezolventa je $_2Q \vee {_6\text{-}Q}$ a to je tautologija. Ako bi se koristila strategija brisanja tautologija, onda se ne bi izvodila ni rezolventa sastavaka (1) i (4). Dalje je slično. Sastavci (2) i (3) imaju samo jednu Lock-rezolventu a to je $_8P \vee {_4\text{-}P}$ jer su $_7\text{-}Q$ i $_3Q$ literali sa najnižim indeksima u sastavcima (2) i (3) redom. Ali ta Lock-rezolventa je tautologija, pa se ne koristi u izvođenju. Sastavci (2) i (4) nemaju Lock-rezolventu jer $_8P$ nije literal sa najnižim indeksom u sastavku (2). Slično ne postoji Lock-rezolventa za sastavke (3) i (4) jer $_6\text{-}Q$ nije literal sa najnižim indeksom u sastavku (4).

Polazni skup sastavaka je nezadovoljiv. Korišćenjem strategije brisanja tautologija u Lock-rezoluciji nije se dobilo izvođenje praznog sastavka iz nezadovoljivog skupa sastavaka. Zato kombinovanje ove dve strategije ne daje potpunu strategiju.

PRIMER. 4.8 Ovaj primer je iz rada Kurerova. Neka su zadati indeksirani sastavci:

(1) $_1b \vee {_8a}$

(2) $_2a \vee {_3\text{-}b}$

(3) $_4c \vee {_5\text{-}a}$

(4) $_6a \vee {_7\text{-}c}$.

Lock dedukcija praznog sastavka NIL je:

(5) $_3\text{-}b \vee {_7\text{-}c}$	iz (2) i (4)
(6) $_8a \vee {_7\text{-}c}$	iz (1) i (5)
(7) $_5\text{-}a \vee {_8a}$	iz (3) i (6)
(8) $_3\text{-}b \vee {_8a}$	iz (2) i (7)
(9) $_8a$	iz (1) i (8)
(10) $_3b$	iz (2) i (9)
(11) $_7\text{-}c$	iz (4) i (10)
(12) $_5\text{-}a$	iz (3) i (11)
(13) NIL	iz (9) i (12).

Ukoliko bi se pomoću strategije brisanja tautologija sprečilo izvođenje sastavka (7), ne bi se mogao dobiti sastavak NIL iz nezadovoljivog skupa sastavaka, što znači da nova strategija nije potpuna.

Takođe je nepotpuna i kombinacija strategije pomoćnog skupa i Lock rezolucije.

PRIMER 4.7. Ovaj primer je konstruisan samostalno i ne nalazi se u [illegible]
Neka su zadati indeksirani sastavci:

(1) ${}_1P \vee {}_2Q$

(2) ${}_8P \vee {}_7\text{-}Q$

(3) ${}_4\text{-}P \vee {}_3Q$

(4) ${}_5\text{-}P \vee {}_6\text{-}Q$.

Za sastavke (1) i (2) ne postoji Lock-rezolventa, jer literali ${}_2Q$ i ${}_7\text{-}Q$ [illegible] najmanji indeks u sastavcima (1) i (2) redom. Takođe za sastavke (1) i (3) [illegible] Lock-rezolventa, jer literal ${}_4P$ nema najmanji indeks u sastavku (3).
Za sastavke (1) i (4) Lock-rezolventa je ${}_2Q \vee {}_6\text{-}Q$ a to je tautologija. [illegible] koristila strategija brisanja tautologija, onda se ne bi izvodila ni rezolventa [illegible] (1) i (4). Dalje je slično. Sastavci (2) i (3) imaju samo jednu Lock-rezolventu [illegible] ${}_8P \vee {}_4\text{-}P$ jer su ${}_7\text{-}Q$ i ${}_3Q$ literali sa najnižim indeksima u sastavcima (2) i (3) [illegible] Ali ta Lock-rezolventa je tautologija, pa se ne koristi u izvođenju. Sastavci [illegible] nemaju Lock-rezolventu jer ${}_8P$ nije literal sa najnižim indeksom u [illegible] Slično ne postoji Lock-rezolventa za sastavke (3) i (4) jer ${}_6\text{-}Q$ nije literal [illegible] indeksom u sastavku (4).
Polazni skup sastavaka je nezadovoljiv. Korišćenjem strategije brisanja [illegible] Lock-rezoluciji nije se dobilo izvođenje praznog sastavka iz nezadovoljivog [illegible] sastavaka. Zato kombinovanje ove dve strategije ne daje potpunu strategiju.

PRIMER. 4.8 Ovaj primer je iz rada Kurerova. Neka su zadati [illegible] sastavci:

(1) ${}_1b \vee {}_8a$

(2) ${}_2a \vee {}_3\text{-}b$

(3) ${}_4c \vee {}_5\text{-}a$

(4) ${}_6\text{-}a \vee {}_7\text{-}c$.

Lock dedukcija praznog sastavka NIL je:

(5) ${}_3\text{-}b \vee {}_7\text{-}c$	iz (2) i (4)
(6) ${}_8a \vee {}_7\text{-}c$	iz (1) i (5)
(7) ${}_5\text{-}a \vee {}_8a$	iz (3) i (6)
(8) ${}_3\text{-}b \vee {}_8a$	iz (2) i (7)
(9) ${}_8a$	iz (1) i (8)
(10) ${}_3b$	iz (2) i (9)
(11) ${}_7\text{-}c$	iz (4) i (10)
(12) ${}_5\text{-}a$	iz (3) i (11)
(13) NIL	iz (9) i (12).

Ukoliko bi se pomoću strategije brisanja tautologija [illegible] sastavka (7), ne bi se mogao dobiti sastavak NIL iz nezadovoljivog [illegible] što znači da nova strategija nije potpuna.

Nejasno je kako za zadati skup sastavaka unapred zadati indeksiranje literala da bi se dobio najkraći dokaz (ili najoptimalniji). U praksi se koristi indeksiranje koja će inicirati neku drugu strategiju (npr. uređenje predikatskih simbola). Ponekad je bilo kakvo indeksiranje pogodno da bi se izvođenje znatno skratilo, kao što pokazuje primer.

PRIMER. Neka je:

$S=\{P, Q, R, W, -P \vee -Q \vee -R \vee -W\}$

Korišćenjem obične rezolucije stvoriće se:

S_1 - 4 člana (od četiri slova -P, -Q, -R, -W biramo tri na 4 načina)

S_2 - 6 članova (od četiri slova biramo dva na 6 načina)

S_3 - 4 člana (od četiri slova biramo jedno na 4 načina)

S_4 = NIL.

U dedukciji učestvuje 5+14=19 sastavaka. Potrebno je stvoriti 14 sastavaka pre nego što dokaže nezadovoljivost S.

Indeksiranjem literala u S proizvoljnim, ali različitim indeksima i primenom Lock rezolucije, skupovi S_1, S_2, S_3 jednočlani, tako da će ukupno biti izvedena samo tri sastavka.

5. LINEARNA REZOLUCIJA
5.1 LINEARNA REZOLUCIJA

Metoda linearne rezolucije je slična jednom načinu dokazivanja indentiteta pri kome se jedna strana transformiše sve dotle dok se ne dobije druga strana identiteta. Linearna rezolucija počinje sa sastavkom koji se primenjuje u rezoluciji, da bi se dobila rezolventa koja se ponovo primenjuje u rezoluciji, i sve tako dok se ne dobije prazan sastavak NIL.

Dobra osobina linearne rezolucije je njena prosta struktura. Ona je potpuna i saglasna sa strategijom pomoćnog skupa, a može se kombinovati i sa heurističkim metodama.

Linearnu rezoluciju su nezavisno uveli u svojim radovima Loveland /1970/ i Luchkam /1970/, a kasnije je poboljšana: Anderson i Bledsoe /1970/, Yates /1970/, Reiter /1971/, Loveland /1972/ i Kowalski i Kuhner /1971/. Ovde će biti izložena verzija data kod Kovalskog i Lovelanda /1972/ pošto ona može biti lako primenjena na računaru.

DEF 5.1 LINEARNA DEDUKCIJA

Neka je S skup sastavaka i C_0 sastavak iz S. LINEARNA DEDUKCIJA sastavaka C_n od polaznog sastavka C_0 iz skupa S je dedukcija koja zadovoljava sledeće uslove:

(i) Za i=0, 1, ... , n-1, C_{i+1} je rezolventa od C_i (koji se naziva CENTRALNI ili GLAVNI sastavak) i B_i (koji se naziva SPOREDNI ili BOČNI sastavak)

(ii) B_i je ili u S, ili je već izvedeni sastavak C_j za neko j, j<i.

5.2 ULAZNA I JEDINIČNA REZOLUCIJA

POTPUNOST strategije je veoma važna u mehaničkom dokazivanju teorema, tj. poželjno je da je uvek moguće izvesti prazan sastavak iz nezadovoljivog skupa sastavaka. Zbog obimnosti dokaza pri takvim strategijama, nekada je važnija EFIKASNOST strategije, nego njena potpunost. Ako je rezolucijska procedura brza i uspešna pri dokazivanju velikog broja teorema, može biti korisna čak i kada nije potpuna. Ovde se razmatraju dve takve strategije: ULAZNA rezolucija i JEDINIČNA rezolucija

Ulazna rezolucija je podslučaj linearne rezolucije. Ona se mnogo lakše izvršava i mada nije potpuna, u nekim primerima uspešnija je od linearne rezolucije. Pokazaćemo i da je ulazna rezolucija ekvivalentna jediničnoj rezoluciji, što znači da teorema koja može biti dokazana ulaznom, može biti dokazana i jediničnom i obrnuto.

Za zadati polazni skup S sastavaka, svaki član skupa S se naziva ulazni sastavak.

DEF 5.2 ULAZNA rezolucija je rezolucija u kojoj je jedan od sastavaka ulazni sastavak. Ulazna dedukcija (koja daje značaj polaznom skupu S) je izvođenje u kojem je svaka rezolucija ulazna rezolucija. Ulazno pobijanje je ulazna dedukcija NIL iz S.

DEF 5.3 JEDINIČNA rezolucija je rezolucija u kojoj je bar jedan od sastavaka jedinični sastavak ili jedinični faktor nekog sastavka. Jedinična dedukcija je dedukcija u kojoj je svaka rezolucija jedinična rezolucija. Jedinično pobijanje je jedinična dedukcija NIL.

Jediničnu rezoluciju su veoma mnogo primenjivali Wos, Carson i Robinson.

LEMA 5.4. EKVIVALENTNOST ULAZNE I JEDINIČNE REZOLUCIJE ZA SLUČAJ FUNDAMENTALNIH SASTAVAKA

Neka je S skup fundamentalnih sastavaka. Tada postoji jedinično pobijanje ako i samo ako postoji ulazno pobijanje.

DOKAZ:

Lema se dokazuje indukcijom.

Neka je A skup atoma iz S. Ako se A sastoji od jednog elementa, na primer Q, onda među sastavcima u S postoje jedinični sastavci Q ili -Q. Jasno, rezolventa od Q i -Q je NIL. Dobijena dedukcija je i jedinična i ulazna. Zato lema važi za ovaj slučaj.

Pretpostavimo da lema važi kada se A sastoji od i elemenata $1 \leq i \leq n$. Da bi primenili indukciju, posmatrajmo A koji se sastoji od tačno n+1 elementa.

(=>) Neka postoji jedinično pobijanje iz S. S sadrži bar jedan jedinični sastavak L, gde je L literal. Neka je So skup dobijen iz S izostavljanjem onih sastavaka koji sadrže literal L i izostavljanjem -L iz ostalih sastavaka. Kako postoji jedinično pobijanje iz S, to postoji jedinično pobijanje i iz So. Ali So sadrži n ili manje od n atoma, pa prema indukcijskoj hipotezi postoji ulazna dedukcija Do sastavka NIL iz So. Neka je D dedukcija dobijena iz Do vraćanjem literala -L u sastavke iz kojih je izostavljen. Neka je T sastavak koji se dobija dedukcijom D. T je ili NIL ili -L. Ako je T NIL dokaz je završen. Ako je T jednako -L, rezolucijom sa L (koje je ulazni sastavak) dobija se NIL. Tako je dedukcija dobijena kombinovanjem dedukcije D i primene rezolucije na T i L, ulazna dedukcija iz S. Ovim je dokazan prvi deo leme.

(<=) Obrnuto, neka postoji ulazno pobijanje iz S. Tada S sadrži bar jedan jedinični sastavakL gde je L literal (to je na primer ulazni sastavak poslednje primenjene rezolucije). Neka je: So= $S \cup \{R(C,L) \mid C \in S\} - \{D$: D sastavak koji sadrže L ili -L$\}$. Kako postoji ulazno pobijanje iz S, to postoji i ulazno pobijanje iz So. Ali So sadrži n ili manje od n atoma, pa prema indukcijskoj hipotezi postoji jedinično pobijanje iz So. Svaki sastavak iz So je ili elemenat S ili je dobijen primenom jedinične rezolucije na sastavak L i neki sastavak iz S. Zato postoji jedinično pobijanje iz S, čime je završena druga polovina dokaza leme.

TEOREMA 5.4 EKVIVALENTNOST ULAZNE I JEDINIČNE REZOLUCIJE

Za zadati skup sastavaka S postoji jedinično pobijanje ako i samo ako postoji ulazno pobijanje.

DOKAZ:

(=>) Neka postoji jedinično pobijanje D iz skupa S. Iz D se može dobiti fundamentalno jedinično pobijanje Do zamenom svakog sastavka C odgovarajućim fundamentalnim sastavkom. Neka je So skup fundamentalnih sastavaka dobijen na ovaj način. Korišćenjem leme 5.4 postoji ulazno pobijanje Eo iz So. Koristeći [illegible] lemu, od Eo se može dobiti ulazno pobijanje E.

(<=) Dokaz drugog dela teoreme, dobija se iz dokaza prvog dela međusobnom zamenom reči jedinično i ulazno.

Ako za zadati skup sastavaka S postoji ulazno pobijanje, korišćenjem teoreme 5.4 moguće je dobiti NIL iz S korišćenjem jedinične rezolucije. Jediničnu rezoluciju je lakše realizovati nego ulaznu, i u tome je značaj teoreme 5.4.

5.3 KORIŠĆENJE ISKLJUČENIH LITERALA

Efikasnost linearne rezolucije se može povećati uvođenjem dva nova pojma. Jedan od njih je pojam uređenog sastavka, koji je uveden u 3.8. Korišćenje uređenog sastavka kod semantičke rezolucije je znatno povećalo njenu efikasnost, što će biti slučaj i kod linearne rezolucije. Za razliku od semantičke rezolucije koja zajedno sa uređenim sastavcima nije bila kompletna, linearna rezolucija korišćena sa uređenim sastavcima ostaje kompletna.

Drugi pojam koristi informaciju o isključenim literalima. Informacija koju daju ti literali može biti veoma korisna. Pri nalaženju rezolvente isključeni literali se ne izostavljaju već se uokviruju. Uokvireni literali se ne mogu koristiti za dalje nalaženje rezolventi, već samo za informaciju koji su literali do tog trenutka bili isključeni.

DEF 5.5 Uređeni sastavak C se može redukovati, ako je poslednji literal u C unifikativan sa negacijom nekog uokvirenog literala iz C.

DEF 5.6 REDUKCIJA

Neka je C uređeni sastavak koji se može redukovati. Neka je poslednji literal L unifikativan sa nekim uokvirenim literalom, i neka je σ njihov najopštiji zajednički unifikator. REDUKCIJA sastavka C je uređeni sastavak dobijen iz $(C)\sigma$ izostavljanjem literala $(L)\sigma$ i svih sledećih uokvirenih literala, za kojima ne slede neuokvireni literali.

Ako u uređenom sastavku postoji više od jednog učestvovanja neuokvirenog literala, tada se zadržava prvo (levo) učestvovanje, a ostala se izostavljaju. Ova operacija se naziva ČUVANJE LEVOG literala za identične neuokvirene literale

DEF 5.7 UREĐENI FAKTOR

Neka dva ili više neuokvirenih literala (istog znaka) u uređenom sastavku C imaju najopštiji zajednički unifikator σ. Tada je UREĐENI FAKTOR od C uređeni sastavak dobijen od $(C)\sigma$ izostavljanjem svakog višestrukog pojavljivanja neuokvirenog literala sem prvog levog i izostavljanjem svakog uokvirenog literala iza koga ne slede neuokvireni literali.

Jednostavno rečeno, ako se u sastavku zamenom može dobiti više identičnih neuokvirenih literala, prvi levi od njih se sačuva, a ostali se izostavljaju. Ako se uokvireni literali nalaze na kraju sastavka, oni se izostavljaju.

DEF 5.8 UREĐENA BINARNA REZOLVENTA

Neka su C i D dva indeksirana sastavka bez zajedničkih promenljivih i L i K dva neuokvirena literala u C i D redom. Neka L i -K imaju najopštiji zajednički unifikator σ. Neka je R_1 uređeni sastavak dobijen iz $(C)\sigma \vee (D)\sigma$ uokviravanjem literala $(L)\sigma$, izostavljanjem $(K)\sigma$ i čuvanjem levog literala za identične neuokvirene literale u ostalom delu sastavka. Neka je R sastavak dobijen od R_1 izostavljanjem svih uokvirenih literala za kojima ne slede neuokvireni literali. Tada se R naziva UREĐENA BINARNA rezolventa od C i D. Literali L i K se nazivaju isključeni literali.

DEF 5.9 UREĐENA REZOLVENTA

Neka su C_1 i C_2 dva uređena sastavka. Uređena rezolventa od C_1 i C_2 je jedna od sledećih uređenih binarnih rezolventi:

(1) uređena binarna rezolventa od C_1 i C_2

(2) uređena binarna rezolventa od C_1 i uređenog faktora od C_2

(3) uređena binarna rezolventa od uređenog faktora od C_1 i C_2

(4) uređena binarna rezolventa od uređenog faktora od C_1 i uređenog faktora od C_2.

DEF 5.10 UREĐENA LINEARNA DEDUKCIJA (OL-DEDUKCIJA)

Neka je S skup uređenih sastavaka i C_0 sastavak iz S. **UREĐENA** LINEARNA DEDUKCIJA sastavka C_n od polaznog uređenog sastavka C_0 iz skupa S je dedukcija koja zadovoljava sledeće uglove:

(i) Za i=0, ..., n-1, sastavak C_{i+1} je uređena rezolventa od C_i (koji se naziva CENTRALNI ili GLAVNI uređeni sastavak) i B_i (koji se naziva **SPOREDNI** uređeni sastavak). Isključeni literal u C_i (ili u uređenom faktoru C_i) je **POSLEDNJI** literal.

(ii) B_i je ili uređeni sastavak u S, ili uređeni faktor nekog već izvedenog sastavka C_j za neko j, j<i. B_i je specijalan slučaj nekog C_j, j<i, ako i samo ako je C_i uređeni sastavak koji se može redukovati. Tada je C_{i+1} redukcija sastavka C_i.

(iii) U dedukciju ne ulaze tautologije.

LEMA 5.11

Ako je u nekoj OL-dedukciji C_i redukcija uređenog sastavka, onda postoji centralni uređeni sastavak C_j, j<i, takav da je redukcija C_{i+1} sastavka C_i uređena rezolventa C_i i nekog uređenog faktora C_j.

Neka su C_1 i C_2 dva uređena sastavka. Uređena rezolventa od C_1 i C_2 je jedna od sledećih uređenih binarnih rezolventi:

(1) uređena binarna rezolventa od C_1 i C_2

(2) uređena binarna rezolventa od C_1 i uređenog faktora od C_2

(3) uređena binarna rezolventa od uređenog faktora od C_1 i C_2

(4) uređena binarna rezolventa od uređenog faktora od C_1 i uređenog faktora od C_2.

DEF 5.10 UREĐENA LINEARNA DEDUKCIJA (OL-DEDUKCIJA)

Neka je S skup uređenih sastavaka i C_0 sastavak iz S. **UREĐENA** LINEARNA DEDUKCIJA sastavka C_n od polaznog uređenog sastavka C_0 iz skupa S je dedukcija koja zadovoljava sledeće uglove:

(i) Za i=0, ..., n-1, sastavak C_{i+1} je uređena rezolventa od C_i (koji se naziva CENTRALNI ili GLAVNI uređeni sastavak) i B_i (koji se naziva **SPOREDNI** uređeni sastavak). Isključeni literal u C_i (ili u uređenom faktoru C_i) je **POSLEDNJI** literal.

(ii) B_i je ili uređeni sastavak u S, ili uređeni faktor nekog već izvedenog sastavka C_j za neko j, j<i. B_i je specijalan slučaj nekog C_j, j<i, ako i samo ako je C_i uređeni sastavak koji se može redukovati. Tada je C_{i+1} redukcija sastavka C_i.

(iii) U dedukciju ne ulaze tautologije.

LEMA 5.11

Ako je u nekoj OL-dedukciji C_i redukcija uređenog sastavka, onda postoji centralni uređeni sastavak C_j, j<i, takav da je redukcija C_{i+1} sastavka C_i uređena rezolventa C_i i nekog uređenog faktora C_j.

Koristeći lemu 5.11 OL-dedukciju je moguće definisati na sledeći način:

(1) Svaki sastavak B_i ili pripada S ili je uređeni faktor nekog C_j, j<i.

(2) Ako je C_i uređeni sastavak koji se može redukovati, onda je C_{i+1} redukcija sastavka C_i. U protivnom je C_{i+1} uređena rezolventa sastavka C_i i nekog B_i koji pripada S, pri čemu je isključeni literal u C_i poslednji.

(3) U dedukciju ne ulaze tautologije.

5.4 POTPUNOST OL REZOLUCIJE

LEMA 5.11 POTPUNOST FUNDAMENTALNE OL-REZOLUCIJE

Neka je C fundamentalni uređeni sastavak koji pripada nezadovoljivom skupu fundamentalnih uređenih sastavaka. Ako je S- {C} zadovoljiv, tada postoji OL-dedukcija sastavka NIL sa gornjim uređenim sastavkom C.

DOKAZ:

Koristimo metod matematičke indukcije po broju elemenata u skupu A atoma za S. Ako se A sastoji od jednog elementa, na primer Q, onda među elementima u S postoje uređeni sastavci Q i -Q. Rezolventa od Q i -Q je NIL. Kako je S-{C} zadovoljiv, onda se ili Q ili -Q poklapa sa C. Zato lema važi u ovom slučaju.

Pretpostavimo da lema važi kada se A sastoji od i elemenata $1 \leq i \leq n$. Da bi primenili indukciju, posmatrajmo A koji se sastoji od tačno n+1 elemenata. Posmatrajmo sledeće slučajeve:

Slučaj 1.

C je jedinični sastavak. Neka je C=L, gde je L literal. Neka je So skup dobijen iz S izostavljanjem onih uređenih sastavaka koji sadrže L i izostavljanjem -L iz ostalih uređenih sastavaka. Jasno je da je So nezadovoljiv. Neka je To nezadovoljiv podskup od S, takav da je svaki pravi podskup od To zadovoljiv (takav skup je moguće dobiti proveravajući sve moguće podskupove skupa S). To mora da sadrži uređeni sastavak Eo, koji je dobijen od nekog sastavka iz S izostavljanjem literala -L. U protivnom bi To bio podskup skupa S- {C} koji bi bio nezadovoljiv prema definiciji To. Ali S- {C} je zadovoljiv, pa bi se dobila kontradikcija.

Sada je Eo uređeni sastavak u nezadovoljivom skupu To sastavaka, pri čemu je To- {Eo} zadovoljiv. To sadrži n ili manje od n atoma, pa prema indukcijskoj hipotezi postoji OL-dedukcija Do (prikazana na slici (a)) sastavka NIL iz To sa polaznim uređenim sastavkom Eo. Vratimo literal -L NA KRAJ svih uređenih sastavaka iz kojih je bio izostavljen, osim polaznog sastavka Eo, koji ćemo dobiti rezolucijom L i E. Na taj način je dobijena dedukcija D sastavka NIL ili -L, predstavljena na slici (b).

Na slici (b) simbol ($\vee$-L) označava dodavanje literala -L na njegovo mesto na kraju uređenih sastavaka iz kojih je bio izostavljen.

Potrebno je dokazati da je D takođe OL dedukcija. Ni jedan sastavak u D nije tautologija, jer je D dobijena od dedukcije Do koja ne sadrži ni tautologije ni literale L. Ako -L nije poslednji literal u centralnom sastavku, onda je rezolucija u D ista kao i u Do. Ako je -L poslednji literal u nekom centralnom sastavku, onda se -L može izostaviti jer je jednak uokvirenom literalu L. U tom slučaju zamenimo deo izvođenja predstavljen na slici (a) sa odgovarajućim izvođenjem predstavljenim na slici (b). Očigledno se sastavak $L \vee C_i$ ($\vee$-L) može redukovati i njegova redukcija je $L \vee C_i$.

Posle transformacije polazne dedukcije prema shemi predstavljenoj na slici (b) dobija se OL-dedukcija D' ili sastavka NIL ili L $\vee$ -L, iz S sa gornjim uređenim sastavkom C. Ako je D' dedukcija sastavka NIL, tvrđenje je dokazano. Ako je D' dedukcija sastavka L $\vee$-L primenom rezolucije na sastavke L $\vee$-L i L dobija se NIL. Na taj način se dedukcija D' može dodavanjem OL-rezolucije između L $\vee$-L i L dopuniti do OL-dedukcije praznog sastavka NIL, što je i trebalo dokazati.

Slučaj 2.

C nije jedinični sastavak. U tom slučaju neka je L prvi levi literal u C, odnosno C = L$\vee$Co, gde je Co neprazan uređeni sastavak. Neka je So skup dobijen iz S izostavljanjem onih uređenih sastavaka koje sadrže literal -L i izostavljanjem L iz ostalih uređenih sastavaka. So je nezadovoljiv. Pokažimo da je So-{Co} zadovoljiv. Neka je I interpretacija koja zadovoljava S-{C}. Takva interpretacija postoji jer je [illegible] skup S-{C} zadovoljiv prema uslovima leme. Kako je S nezadovoljiv, onda je C lažno u I. Zato je i L lažno u interpretaciji I. Tada je So- {Co} istinito u I i So-{Co} je zadovoljiv skup.

Kako So sadrži n ili manje od n atoma, prema indukcijskoj hipotezi postoji OL-dedukcija Do sastavka NIL iz So sa gornjim uređenim sastavkom Co. Neka je D_1 dedukcija dobijena iz dedukcije Do vraćanjem literala L nazad u one sastavke odakle je izostavljen. D_1 je OL-dedukcija sastavka L iz S sa gornjim uređenim sastavkom C. Skup $L \cup (S-\{C\})$ je nezadovoljiv i sadrži jedinični sastavak, pri čemu je skup S-{C} zadovoljiv. Koristeći prvi slučaj dokaza leme, postoji OL-dedukcija D_2 sastavka NIL iz $L \cup (S- \{C\})$ sa gornjim uređenim sastavkom L. Kombinovanjem D_1 i D_2, dobija se OL-dedukcija NIL iz S sa gornjim uređenim sastavkom C. Time je lema u potpunosti dokazana.

TEOREMA 5.12 POTPUNOST OL-REZOLUCIJE

Neka je C uređeni sastavak koji pripada uređenom skupu S uređenih sastavaka i neka je S- {C} zadovoljiv skup. Tada postoji OL-dedukcija sastavka NIL iz S sa gornjim uređenim sastavkom C.

DOKAZ:

Kako je S nezadovoljiv skup a S- {C} zadovoljiv, prema teoremi ERBRANA postoji konačan nezadovoljiv skup So fundamentalnih uređenih sastavaka, dobijen iz S zamenom promenljivih elementima Erbranovog prostora. Tada postoji faktor Co sastavka C takav da je So nezadovoljiv, Co pripada So i So-{Co} je zadovoljiv. Prema lemi 5.11 postoji OL-dedukcija Do sastavka NIL iz skupa So sa gornjim uređenim sastavkom Co. Koristeći LIFTING lemu 1.37 dedukcija Do se može transformisati u OL dedukciju NIL iz S sa gornjim uređenim sastavkom C. Time je teorema dokazana.

6. REZOLUCIJSKA PROCEDURA ODLUČIVA ZA NEKE KLASE FORMULA

6.1 UVODNI PRIMERI

Ova glava predstavlja delimično samostalan rad. U prvom delu su navedena dva prosta primera gde rezolucijska procedura stvara beskonačan proces. U prvom primeru se u rezolventi stvaraju termi sve veće složenosti. u drugom primeru se stvaraju sve duže rezolvente. To je motiv za traženje strategije koje će u nekim primerima onemogućiti beskonačan proces stvaranja rezolventi.

U drugom delu se uvodi uređenje nad atomnim formulama. koristeći definiciju sličnosti terma i definiciju dominantnosti terma. Zatim se definiše rezolucijska procedura $R_{<a}$ za koju se dokazuje da je kompletna. Dokaz je izveden samostalno, iako mnogo podseća na lemu 4.5.

Treći deo je motivisan strategijom upijanja, samo što se zahteva da sastavak upija sam sebe. Definiše se kondenzacija i uvodi rezolucijska procedura R_c za koju se dokazuje da čuva svojstvo kompletnosti. Dokaz je elementaran.

U četvrtom delu se pokazuje da rezolucijska procedura nastala kombinovanjem prethodne dve strategije predstavlja odlučivu proceduru za monadičnu klasu. što i nije neki veliki rezultat, jer je odlučivost monadične klase formula dokazao Lowenheim još 1915 god. Koristeći rezultate iz doktorske disertacije Friedman-a [..] pokušano je da se ispita da li je $R_{<ac}$ rezolucijska procedura odlučiva za još neku klasu formula.

6.1 UVODNI PRIMERI

Navedimo ponovo primer iz 2.2 koji pokazuje da Robinsonova rezolucijska procedura. primenjena bez ograničenja, neće dati odgovor o nezadovoljivosti, čak i u slučaju jednostavne formule.

PRIMER 1.
Neka je F formula:
F: $(\exists z)(\forall x)(\exists y)(\ P(z)\wedge\ P(x)\Rightarrow P(y)\ )$
Primenom algoritma 1.4 za pripremu formula dobija se skup sastavaka:
$\{P(a), -P(x) \vee P(f(x))\}$

Ukoliko a interpretiramo kao broj "0", funkciju f(x) kao "sledbenik prirodnog broja x". onda je ovo formulacija fragmenta aksiome peana za prirodne brojeve.

Primenom rezolucije na sastavke nastaju rezolvente:
$P(f(a))$, $P(f(f(a)))$, ... , $P(f_n(a))$, ...

$P(a)$ $\qquad$ $-P(x) \vee P(f(x))$

$P(f(a))$ $\qquad$ $-P(x) \vee P(f(x))$

$P(f(f(a)))$ $\qquad$ $-P(x) \vee P(f(x))$

...

Očigledno je da u ovom primeru rezolucijska procedura stvara ... proces. Razlog je što se u rezolventi pojavljuju termi sve veće ... terma u rezolventi ni na koji način nije ograničena. Procedura koja bi ... za neku klasu formula, trebala bi da spreči stvaranje terma neograničene ... rezolventi. Za ograničavanje generisanja beskonačnog procesa, J.R... radu [**] uvodi pojam literala čistog u skupu sastavaka. Ovde će ... jedna drugačija tehnika za ograničenje dubine terma u rezolventi.

PRIMER 2. Neka je E formula

$(\forall x_1)\ (\forall x_2)\ (\forall x_3)\ (P(x_1,x_2) \vee Q(x_2,x_3) \vee R(x_1,x_3) \wedge (-R(x_1,x_2) \vee Q(x_2,x_3) \vee$ ...

Primenom algoritma 1.4 za pripremu formula dobija se skup sastavaka ...

$P(x_1,x_2) \vee Q(x_2,x_3) \vee R(x_1,x_3)$, $\quad -R(x_1,x_2) \vee Q(x_2,x_3) \vee -P(x_2,x_3)$ ...

Primenom rezolucije na polazni skup sastavaka dobijaju se rezolvente ...

$P(x_1,x_2) \vee Q(x_2,x_3) \vee R(x_1,x_3)$, $\qquad -R(y_1,y_2) \vee Q(y_2,y_3) \vee$ ...

$\theta=\{x_1/y_1, x_3/y_2,$ ...

$P(x_1,x_2) \vee Q(x_2,x_3) \vee Q(x_3,x_4) \vee -P(x_1,x_4)$ $\qquad -R(y_1,y_2) \vee Q(y_2,y_3) \vee$ ...

$\theta=\{x_1/y_1, x_4/y_2,$ ...

$P(x_1,x_2) \vee Q(x_2,x_3) \vee Q(x_3,x_4) \vee Q(x_4,x_5) \vee R(x_1,x_5)$ $\qquad -R(y_1,y_2) \vee Q(y_2,y_3) \vee$ ...

...

Nastavljajući proces primene rezolucijske procedure prema ... zaključujemo da se mogu generisati sastavci:

$P(x_1,x_2) \vee Q(x_2,x_3) \ \dots\ Q(x_{n-1}, x_n) \vee R(x_1,x_n)$ $\qquad n=5,7,9,$ ...

Rezolucijska procedura u ovom primeru stvara rezolvente sve ... je razlog zašto to nije odlučiva procedura.

Neka je H Erbranov prostor sastavljen od konstante a i dva ... f i g, dužine 1 odnosno 2. Tada:

$H_0 = \{a\}$

$H_1 = \{f(a), g(a,a)\}$

$H_2 = \{f(f(a)), f(g(a,a)), \ldots, g(g(a,a), g(a,a))\}$

Svet terma H je slabo uređen. Uporedivi su po složenosti samo termi iz različitih nivoa H_i i H_j.

Trebalo bi u svet terma uvesti jedno strožije uređenje, tako da se mogu po složenosti porediti i termi iz istog nivoa, npr. f(a) i g(a,a). Primenjujući rezolucijsku proceduru na tako uređene terme, može se zahtevati da se u rezolventi ne pojavljuje term koji je složeniji od svih terma isključenog literala L.

To znači da se prvo vrši rezolucija nad onim literalom koji sadrži najsloženiji term. Na taj način izbegava se stvaranje rezolvente sa termima sve veće složenosti, što je u puno primera razlog za neodlučivost rezolucijske procedure nad datim skupom sastavaka.

6.2 A-UREĐENJE

Pri definisanju rezolucijske procedure koja će ograničiti povećanje dubine terma u rezolventi, koristi se definicija slična onoj koja se prvi put pojavila u radu: Kowalski and Hayes: Semantic Trees in Automatic Theorem - proving (Machine Intelligence 4, 87-101, 69.god.).

DEF 6.1 A-UREĐENJE

A uređenje $<_a$ je IREFLEKSIVNA i TRANZITIVNA binarna relacija nad atomnim formulama takva da:

(1) za svaki skup sastavaka, $<_a$ je saglasna sa nekim uređenjem Erbranovog prostora (to znači da postoji neko uređenje Erbranovog prostora A_1, A_2,... tako da ako je $A_i <a\ A_j$, tada je i<j)

(2) Ako je $A <_a B$, tada je $(A)\alpha <_a (B)\alpha$ za svaku zamenu α.

DEF 6.2 SLIČNI TERMI

Definicija relacije sličnosti terma koju označavamo sa ~, uvodi se rekurzivno:

(1) Za svaku individualnu promenljivu x, x~x.

(2) Za bilo koje dve individualne konstante a i b, a~b.

(3) Ako je $t_1 \sim s_1, \ldots, t_n \sim s_n$ i f i g funkcijski simboli dužine n, tada je $f(t_1, \ldots t_n) \sim g(s_1, \ldots, s_n)$.

Relacija sličnosti terma je relacija ekvivalencije. Ako su dva terma slična, slični su i njihovi odgovarajući podtermi. Termi t i s su slični ako se rezlikuju samo u funkcijskim simbolima.

DEF 6.3 DOMINANTNI TERMI

Ako je $u=f(t_1, \ldots, t_n)$, $v=g(s_1, \ldots, s_n, \ldots, s_m)$, $0 \leq n < m$, pri čemu je $t_1 \sim s_1, \ldots, t_n \sim s_n$, tada je term v DOMINANTAN termu u.

Biti pravi podterm i dominantnost su relacije strogog uređenja, tj. irefleksivne, asimetrične i tranzitivne. Ako su u i v slični termi i w je dominantan u, tada je w dominantan i v. Ako je v dominantan u i v sličan w, tada je w dominantan u.

DEF 6.4 SLOŽENOST TERMA
Term v je složeniji od u, u oznaci $u <_t v$ ako:
(1) v je dominantan u, ili
(2) postoji term t koji je pravi podterm od v i sličan je u, ili
(3) postoji term t koji je pravi podterm od v i dominantan je u.

LEMA 6.5 SLOŽENOST TERMA JE RELACIJA UREĐENJA
DOKAZ:
Irefleksivnost i asimetričnost relacije složenosti je posledica irefleksivnosti i asimetričnosti relacija dominantnosti i relacije biti pravi podterm.

Tranzitivnost se dokazuje analizom devet slučajeva.

Neka je $u <_t v$ po (1) i $v <_t w$ po (1), (2) ili (3). Tada je $u <_t w$ po (3).

Neka je $u <_t v$ po (2) i $v <_t w$ po (1), (2) ili (3). Tada je $u <_t w$ po (2).

Neka je $u <_t v$ po (3) i $v <_t w$ po (1), (2) ili (3). Tada je $u <_t w$ po (3).

Korišćenjem relacije $<_t$ nad termima za koju je dokazano da je relacija uređenja koja se čuva supstitucijom, definiše se relacija $<_a$ nad atomima.

DEF 6.6 Neka su A i B atomi. $A <_a B$ ako postoji term u iz B, takav da za svaki term t iz A, u je složenije od t.

LEMA 6.7 Relacija $<_a$ je relacija strogog uređenja i čuva se supstitucijom.
DOKAZ:
Irefleksivnost relacije $<_a$ je posledica irefleksivnosti relacije $<_t$.
Neka je A atom $A(t_1, \ldots, t_n)$. Tada ne može biti $A <_a A$ jer bi to značilo da u atomu A postoji neki term, nazovimo ga t_j, tako da je t_j složeniji od svih t_1, $\ldots$, t_n. No to ne može biti jer nije t_j složenije od t_j, prema lemi 6.5.

Relacija $<_a$ je trazitivna. Neka su A,B,C, atomi takvi da je $A <_a B$ i $B <_a C$. Iz uslova da je $A <_a B$ sledi da postoji term v iz B takav da je za svaki term u iz A ispunjeno $u <_t v$. Slično, iz $B <_a C$ sledi da postoji term w iz C takav da je za svaki term iz B, pa i za v ispunjeno $v <_t w$. Koristeći tranzitivnost relacije $<_t$, odnosno da $u <_t v$ i $v <_t w$ povlači $u <_t w$, zaključujemo da postoji term w iz C takav da za svaki term u iz A važi $u <_t w$, odnosno $A <_a C$.

Relacija $<_a$ se čuva supstitucijom. Neka je $A <_a B$. To znači da postoji term v u B takav da za svaki term u iz A $u <_t v$. Koristeći osobinu relacije $<_t$ u odnosu na zamene: $u <_t v$ povlači $(u)\theta <_t (v)\theta$, zaključujemo da u atomu $(B)\theta$ postoji term $(v)\theta$ koji je složeniji od svakog terma $(u)\theta$ iz $(A)\theta$. Time je dokazano da se relacija $<_a$ čuva supstitucijom.

Pri definisanju rezolucijske procedure koja će ograničiti porast složenosti terma u rezolventi, koristi se sledeća definicija.

DEF 6.8 Neka je E rezolventa sastavaka C i D i L literal iz E. E zadovoljava <a ograničenje ako ne postoji atom M, takav da M ili -M pripada E, za koji je $L <_a M$.

R_a je rezolucijska procedura u kojoj svaka rezolventa zadovoljava $<_a$ ograničenje.

Koristeći definiciju relacije uređenja $<_a$ koja je uvedena ranije, to znači da u rezolventi E ne postoji literal M sa termom s koji je složeniji od svakog terma t koji se javlja u isključenom literalu L. Jednsotavnije, rezolucija se primenjuje tako da se prvo isključuju složeniji literali.

TEOREMA 6.9 Ra JE KOMPLETNA REZOLUCIJSKA PROCEDURA

DOKAZ:

Neka je S nezadovoljiv skup sastavaka. Izvršimo indeksiranje literala u S na sledeći način: koristeći relaciju uređenja $<_t$ nad termima, možemo prvo urediti terme, a zatim sa relacijom $<_a$ i atome. Kako je prema lemi 6.6 $<_a$ relacija strogog uređenja (irefleksivna i tranzitivna) dobijeni su lanci uređenih atoma. Atome iste dubine koji se ne mogu međusobno urediti uredimo leksikografski, ali tako da je uređenje indukovano sa $<_a$ očuvano. Na ovaj način je dobijeno indeksiranje svih literala.

Neka je K(S) definisano kao:

K(S)= broj pojavljivanja literala u S - broj sastavaka u S.

Teorema se dokazuje matematičkom indukcijom po K(S). Ako je NIL u S teorema je dokazana. Neka NIL nije u S.

Ako je K(S)=0, tada se S sastoji samo od jediničnih sastavaka. Kako je S nezadovoljiv, postoji literal L takav da su L i -L u S. Rezolventa od L i -L je NIL. Time je pokazano da teorema važi kada je K(S)=0.

Neka teorema važi kada je K(S) manje od n. Dokažimo da važi i za K(S)=n. Kako je K(S) veće od 0, postoji najmanje jedan sastavak u S koji nije jedinični.

Neka je m najmanji indeks onog literala, kod svih onih sastavaka iz S koji nisu jedinični. Neka je C sastavak koji nije jedinični i koji sadrži literal L indeksiran sa najmanjim indeksom, a C_0 sastavak dobijen od C izostavljanjem literala L. C_0 nije prazan sastavak jer C nije jedinični sastavak. Neka je:

$S_1 = (S- \{C\}) \cup \{C_0\}$ i $S_2 = (S- \{C\}) \cup \{L\}$.

Skupovi sastavaka S_1 i S_2 su nezadovoljivi. $K(S_1)$ je manje od n, i $K(S_2)$ je manje od n. Zato prema indukcijskoj hipotezi postoje R_a dedukcije D_1' i D_2' praznog sastavka NIL iz S_1 i S_2. Neka je D_1 dedukcija dobijena iz D_1' stavljanjem L nazad u C_0. Kako je literal L literal sa najmanjim indeksom u sastavku C, jasno je da je D_1 takođe R_a dedukcija. Rezultat te R_a dedukcije je NIL ili L. Ako je to NIL, dokaz je završen. Ako je to L, kombinovanjem D_1 i D_2' dobija se R_a dedukcija NIL iz S. Ovim je dokazano da je Ra kompletna rezolucijska procedura.

6.3 KONDENZACIJA

Ograničenje povećanja broja sastavaka u rezolventi uspešno se ostvaruje uvođenjem kondenzacije, gde pokušavamo da sažmemo u sastavak onoliko literala koliko je to zamenom moguće.

DEF 6.11 KONDENZACIJA

Neka je C sastavak i α zamena. Posmatrajmo sastavak kao skup svojih literala. Ako je $(C)\alpha$ podskup od C, kažemo da se sastavak C može kondenzovati. $(C)\alpha$ je KONDENZACIJA ako je $(C)\alpha \subseteq C$, i za svaku drugu zamenu β za koju je $(C)\beta \subseteq C$ važi $(C)\alpha \subseteq (C)\beta$.

PRIMER

Kondenzacija sastavka $P(x) \vee P(f(a))$ je $P(f(a))$.

Sastavak $P(x_1,x_2) \vee P(x_2,x_3) \vee P(x_3,x_4)$ je kondenzovan.

LEMA 6.12 Svake dve kondenzacije sastavaka su faktori jedna ...

DOKAZ: Neka je $(A)\alpha$ podskup od A i $(A)\beta$ podskup od A. ... podskup $(A)\beta$ podskup od A. Ali $((A)\alpha)\beta$ ne može imati manje ... β i zato je $((A)\alpha)\beta = (A)\beta$. Slično je $((A)\alpha)\beta = (A)\alpha$.

U ovom radu je dat algoritam 2.5 algoritam upijanja. Lako se ... algoritam koji za zadati sastavak pronalazi njegovu kondenzaciju. Ako ... sastavaka, tada je cond(S) skup u kome je svaki sastavak iz S zamenjen ... kondenzacijom.

DEF 6.13 Ako je R bilo koja rezolucijska procedura, R_c je ... slična R, osim što su svaki polazni sastavak i generisana rezolventa ... svojom kondenzacijom.

TEOREMA 6.14 KOMPLETNOST REZOLUCIJSKE PROC...

Ako je R kompletna rezolucijska procedura, tada je i R_c kompletna.

DOKAZ:

Neka je R kompletna rezolucijska procedura. To znači da postoji ... praznog sastavka NIL iz svakog nezadovoljivog skupa sastavaka S. Neka ... sastavci i E rezolventa u tom izvođenju. Neka su A_1 i B_1 kondenzacije ... B. Tada je rezolventa E_1 ako postoji nad istim isključenim literalom ...

A	B	$A\alpha = A_1$	$B\beta = B_1$
E		E_1	

Međutim, može se desiti da je u cond(A) ili u cond(B) isključeni literal ... i da ne postoji rezolventa A i B nad tim literalom. Kako je u deduk... postepeno gube isključeni literali, odaberimo umesto rezolvente onaj od ... ili B_1 u kome je isključeni literal kondenzovan (nestao). Ako su član... A i B dodeljeni sastavci A_1 i B_1 članu koji odgovara rezolventi E d... sastavaka A_1 ili B_1 koji ne sadrži isključeni literal L. Jasno je da je ... od E.

Na ovaj način je svakom članu dedukcije D dodeljen član deduk... dobijen ili kao rezolucija dva prethodna člana ili kao naslednik ... članova. Pri tome uvek važi da je E_1 podskup E.

Koristeći osobinu da se pomoću kondenzacije ne može dobiti ... u dedukcija Do će se pre ili kasnije pojaviti NIL, jer se NIL pojavljuje ... način je pokazano da je i R_c kompletna rezolucijska procedura.

6.4 ODLUCIVOST R_{AC} ZA NEKE KLASE FORMULA

Monadična klasa formula predikatskog računa prvog reda je ona koja sadrži samo predikate dužine jedan.

TEOREMA 6.15 $R_{<ac}$ je rezolucijska procedura koja je odlučiva za monadičnu klasu.

DOKAZ:

Neka je G formula predikatskog računa prvog reda koja sadrži n univeralnih kvantifikatora i $k \geq 1$ monadičnih predikatskih simbola.

$(\exists a_1,\ldots,a_{l_0})(\forall x_1)(\exists y_1,\ldots,y_{l1})(\forall x_2)(\exists z_1,\ldots,z_{l2})\ldots(\forall x_n)(\exists w_1,\ldots,w_{ln})F(a_1,\ldots,a_{lo},x_1,y_1,\ldots, w_{ln})$

Primenom algoritma 1.4 za pripremu formula dobija se

$F(a_1,\ldots,a_{lo},\ \underline{x_1},\ f_1(x_1),\ldots,\ f_{l1}(x_1),\ \underline{x_2}\ ,\ g_1(x_1,x_2),\ldots,\ g_{l1}(x_1,x_2),\ \ldots,\ \underline{x_n},\ h_1(x_1,\ldots,x_n),\ldots, h_{ln}(x_1,\ldots,x_n)\qquad l_1,\ldots,l_n \geq 0.$

U svakom sastavku se nalazi najviše n-promenljivih. (To je očigledno ako posmatramo pripremljenu formulu, gde su promenljive podvučene). Ako se neka od promenljivih, recimo x_i, $1 \leq i \leq n$ uopšte ne pojavljuje u sastavku (ni kao slobodna promenljiva, ni kao argument nekog funkcijskog simbola) tu promenljivu možemo izbaciti ali na sledeći način: Na sastavak $C(\ x_1,\ldots x_{i-1},x_{i+1},\ldots,\ x_n)$ primenimo zamenu $\theta=\{\ x_i/x_{i+1}\ ,\ldots,\ x_{i-1}/x_n\}$. U novom sastavku $(C)\theta\ =\ C(\ x_1,\ldots x_{i-1},x_i,\ldots,\ x_{n-1})$ izvršeno je pomeranje promenljivih prema napred. Na sličan način promenljive u svakom sastavku (koje nisu na osnovnom nivou) mogu biti uređene:

$V_1,\ \ldots\ ,\ V_m\ ,\qquad m \leq n.$

tako da je lista argumenata svakog funkcijskog simbola početni segment od $V_1,\ldots V_m$.

Argumenti predikatskog simbola P mogu biti:

$X_1,\ X_2,\ldots X_n,\ a_1,\ \ldots,\ a_{lo},\ f_1(X_1),\ \ldots,\ f_{l1}(X_1),\ldots,\ h_i\ (X_i,\ \ldots,\ X_n),\ldots,\ h_{l1}\ (X_1,\ldots X_n)$

U sastavku se literal sa simbolom P (tj. P ili -P) može pojaviti najviše

$2(n+L_0+L_1+\ldots+L_n)$ puta, inače se sastavak može kondenzovati.

Kako po pretpostavci imamo ukupno k predikatskih simbola, to je najveći broj literala koji se mogu pojaviti u sastavku $2*(n+L_0+L_1+\ldots L_n)*k$.

Ovim je određena granica dužine sastavaka koji se može pojaviti u izvođenju.

Kako je broj sastavaka ograničene složenosti (sa termima čija dubina nije veća od 2) i ograničene dužine konačan, to je $R_{<ac}$ rezolucijska procedura koja je odlučiva za monadičnu klasu.

Akermanova klasa funkcija je klasa sa prefiksom $\exists^m\forall\exists^n$.

TEOREMA 6.16 $R_{<ac}$ je rezolucijska procedura koja je odlučiva za Akermanovu klasu.

DOKAZ:

Neka je E formula sa prefiksom $\exists^m\forall\exists^n$ koja sadrži k predikatskih simbola P_i

$(\exists a_1,\ldots a_m)(\forall x)\ (\exists y_1,\ldots,y_n)F(a_1,\ldots,a_m,x,\ y_1,\ldots,y_n).$

Primenom algoritma 1.4za pripremu formule, formula E se [illegible] $F(a_1,\ldots,a_m, x, f_1(x),\ldots,f_n(x))$.

Za sastavke koji se dobijaju primenom algoritma 1.4 je očigledno [illegible]

a) U svakom sastavku koji nije na osnovnom nivou javlja se [illegible] promenljiva.

b) U sastavku sa promenljivom v, argumenti literala su termi iz [illegible] $\{a_1,\ldots,a_m, v, f_1(v),\ldots,f_n(v))$.

Dokažimo da se čuva svojstvo uređenja $<_a$. Neka su C i D [illegible] Akermanove klase koji sadrže tačno po jednu promenljivu. Onda su oni [illegible]

$C(a_1, \ldots, a_m, x, f_1(x), \ldots , f_n(x))$

$D(a_1, \ldots, a_m, x, f_1(x), \ldots , f_n(x))$

Potrebno je dokazati da i njihova rezolventa koja zadovoljava $<_a$ ograničenje [illegible] najviše jednu promenljivu. U sastavku, pa ni u literalu se ne može pojaviti [illegible] jedne promenljive. Zato, ako se term $f_i(v)$ javlja kao argument predikatskog [illegible] onda se ni jedan term oblika $f_j(a_k)$ ne može pojaviti u tom literalu. [illegible] odrezane literale M i N koji učestvuju u rezoluciji ne može biti oblika [illegible] čemu bar jedan od argumenata $f_i(y)$ stvarno učestvuje u nekom literalu [illegible] jer bi rezolventa bila oblika:

$E(a_1, \ldots, a_n, x, f_1(x), \ldots , f_n(x) , \ldots, f_1(f_i(x), \ldots , f_n(f_i(x)))$ ·

pri čemu $f_k(f_i(x))$ za neko k stvarno učestvuje u E, jer bi time bio narušen [illegible] $<_a$ ograničenje.

Ukoliko se ni za jedno k ne bi pojavljivao term $f_k(f_i(x))$, rezolventa [illegible] sadržala samo jednu promenljivu.

Slično, ako je unifikator za odrezane literala M i N iz C i D oblika [illegible] $\{x/y\}$ u rezolventi će se pojaviti samo jedna promenljiva. Razmatranjem [illegible] koji su se pojavili, zaključujemo da rezolventa E sadrži samo jednu promenljivu [illegible]

Neka je dužina predikatskog simbola P_i označena sa arnost(P_i). [illegible] koji se mogu konstruisati od predikatskog simbola P_i, čiji su argumenti a_1,[illegible] $f_1(v),\ldots, f_n(v)$ je:

$$(m+1+n)^{\text{arnost}(Pi)}$$

Broj literala ne može biti veći od

$$2^*(m+1+n)^{\text{arnost}(Pi)}$$

Sastavak C ne može imati više od

$$\sum_{i=1}^{k} 2^*(m+1+n)^{\text{arnost}(Pi)} \text{ različitih literala.}$$

Nalaženjem granice za dužinu sastavaka dobijena je odlučivost Akermanove [illegible] jer postoji samo konačan broj nevarijabilnih sastavaka ograničene [illegible] argumenti termi dubine ne veće od dva.

Nije jasno da li je ovako definisana rezolucijska procedura [illegible] odlučivanja za još neku odlučivu klasu predikatskih formula.

7. REZOLVENTA U FAZI LOGICI

REZOLVENTA U FAZI LOGICI

DEF 7.1 FAZI LOGIKA je uređena četvorka $([0,1], \wedge, \vee, -)$, gde su operacije I ($\wedge$), ILI ($\vee$) i NE ($-$) definisane na sledeći način $A \wedge B = \min(A,B)$, $A \vee B = \max(A,B)$, $-A = 1-A$, $A,B \in [0,1]$.

DEF 7.2 Promenljiva x_i ($i=1,\dots n$) ili njena negacija $-x_i$ naziva se slovna promenljiva. Slovna promenljiva x_i i $-x_i$ su komplementarne. Definicija iskaza je uobičajena. Sastavak je disjukcija slovnih promenljivih.

U fazi logici ne važe zakoni $-x \vee x = 1$, $-x \wedge x = 0$. U običnoj logici sastavak koji sadrži istovremeno x i -x je tautologija. U fazi logici takvi sastavci se nazivaju KOMPLEMENTARNI.

DEF 7.3 INTERPRETACIJA je preslikavanje T skupa promenljivih u $[0,1]$. Istinitosna vrednost sastavka C se označava sa T(C). Ako je S skup sastavaka $S=\{C_1, \dots C_n\}$, tada je istinitosna vrednost za S, $T(S)=T(C_1 \wedge \dots \wedge C_n)$.

Svaki iskaz se može korišćenjem zakona mreže, uz uobičajeno definisanje implikacije i ekvivalencije, napisati kao konjukcija sastavaka. Koristeći osobine komutativnog zakona i zakona idempotentnosti za I i ILI, sastavak se može posmatrati kao skup svojih (različitih) slovnih promenljivih.

DEF 7.4 FAZI REZOLVENTA

Neka su dva sastavka C_1 i C_2 redom jednaka $C_1 = x_i \vee L_1$, $C_2 = -x_i \vee L_2$, gde L_1 i L_2 ne sadrže slovne promenljive x_i i $-x_i$, i ne sadrže komkplementarni par promenljivih. Tada se sastavak $L_1 \vee L_2$ naziva fazi rezolventa od C_1 i C_2 i označava $Rf(C_1,C_2)$. X_i se naziva ključna promenljiva (slovo).

Neka je C pretpostavka i D njena logička posledica. Tada je $T(C) \leq T(D)$. Prema lemi 1.10 rezolventa (obična) sastavaka C_1 i C_2 je njihova logička posledica. Zato je $T(C_1,C_2) \leq T(R(C_1,C_2))$ i $T(C_1,C_2)=T(C_1,C_2,R(C_1,C_2))$. To znači da se u iskaznom računu istinitosna vrednost skupa sastavaka pri svim interpretacijama neće promeniti ako tom skupu dodamo rezolventu neka dva sastavka iz skupa. U slučaju fazi logike to nije tačno, što pokazuje sledeći primer.

LEMA 7.5 Za fazi rezolventu ne važi $T(C_1,C_2) \leq T(Rf(C_1,C_2))$.

DOKAZ.Neka je $C_1 = xi \vee L_1$, $C_2 = -xi \vee L_2$, i neka je za neku interpretaciju $T(x_i)=0.3$, $T(L_1)=0.1$, $T(L_2)=0.2$. Tada je $T(C_1)=0.3$. $T(C_2)=0.7$, $T(C_1,C_2)=0.3$, dok je $T(Rf(C_1,C_2)) = T(L_1 \vee L_2)=0.2$. Kako nije $0.3 \leq 0.2$, navedeni kontraprimer dokazuje lemu.

DEF 7.6 Neka je D iskaz dobijen iz skupa iskaza S korišćenjem nekog od pravila izvođenja. D je ZNAČAJNA logička posledica ako je $T(S) \leq T(D)$.

Sledeća teorema određuje uslove pod kojima je rezolventa u fazi logici značajnja logička posledica skupa sastavaka od kojih je nastala.

TOREMA 7.7 Neka su C_1 i C_2 dva sastavka i $Rf(C_1,C_2)$ njihova fazi rezolventa sa ključnim slovom x_i. Tada važi:

(1) ako $T(x_i,-x_i) \leq T(Rf(C_1,C_2)$, tada $T(C_1,C_2) \leq T(Rf(C_1,C_2)$

(2) ako $T(x_i,-x_i) \geq T(Rf(C_1,C_2)$, tada $T(C_1,C_2) \geq T(Rf(C_1,C_2)$

DOKAZ. Neka je $C_1=x_i \vee L_1$, $C_2=-x_i \vee L_2$, i $L_1 \vee L_2$ ne sadrži x_i, ni $-x_i$, niti neke komplementarne promenljive. Tada je $C_1 \wedge C_2= x_i \wedge -x_i \vee x_i \wedge L_2 \vee -x_i \wedge L_i \vee L_1 \wedge L_2$, $Rf(C_1,C_2)=L_1 \vee L_2$.

Uvek su ispunjene sledeće tri nejednakosti

(1) $T(x_i \wedge L_2) \leq T(L_1 \vee L_2)$,

(2) $T(-x_i \wedge L1) \leq T(L_1 \vee L_2)$,

(3) $T(L_i \wedge L_2) \leq T(L_1 \vee L_2)$.

Tada je $T(x_i \wedge L_2 \vee -x_i \wedge L_1 \vee L_1 \wedge L_2) \leq T(L_1 \vee L_2)$. Zato, ako

$T(x_i, -x_i) \leq T(L_1 \vee L_2)= T(Rf(C_1,C_2)$, tada $T(C_1,C_2) \leq T(Rf(C_1,C_2)$ i

$T(x_i,-x_i) \geq T(L_1 \vee L_2)= T(Rf(C_1,C_2)$, tada $T(C_1,C_2) \geq T(Rf(C_1,C_2)$,

što je i trebalo dokazati.

Na osnovu teoreme 7.7, fazi rezolventa ne mora biti značajna logička posledica sastavaka od kojih je nastala, što zavisi od istinitosne vrednosti ključne promenljive. U fazi logici, za dobijanje logičke posledice koja je tačnija od pretpostavki, treba izabrati ključnu promenljivu koja zadovoljava uslov (1) teoreme 7.5. Pri korišćenju proizvoljne ključne promenljive ne može se uvek dobiti značajna logička posledica. Zato je provera uslova (1) kod nalaženja fazi rezolvente bitna.

7.8 PRVA POSLEDICA TEOREME 7.7

Neka su C_1 i C_2 dva sastavka. Ako je $T(Rf(C_1,C_2) \geq 0.5$, tada je $T(C_1,C_2) \leq T(Rf(C_1,C_2))$.

DOKAZ. Neka je $Rf(C_1,C_2)$ fazi rezolventa C_1 i C_2 sa klju!nom promenljivom x_i. Za svaku interpretaciju je uvek ispunjeno $T(x_i,-x_i) \leq 0.5$. Zato ako $T(Rf(C_1,C_2)) \geq 0.5$, onda $T(x_i,-x_i) \leq T(Rf(C_1,C_2))$ i prema teoremi 7.6 je $T(C_1,C_2) \leq T(Rf(C_1,C_2))$, što je trebalo dokazati.

Prema ovoj posledici, ako istinitosna vrednost fazi rezolvente nije manja od 0.5, fazi rezolventa je značajna logička posledica.

7.9. DRUGA POSLEDICA TEOREME 7.7

Neka su C_1 i C_2 dva sastavka. Ako je $T(C_1, C_2) \geq 0.5$, tada je $T(C_1,C_2) \leq T(Rf(C_1,C_2))$.

DOKAZ. Neka je $C_1= x_i \vee L_1$, $C_2= -x_i \vee L_2$, i $L_1 \vee L_2$ ne sadrži x_i, ni $-x_i$, niti neke komplementarne promenljive. Tada je

$$C_1 \wedge C_2= x_i \wedge -x_i \vee x_i \wedge L_2 \vee -x_i \wedge L_1 \vee L_1 \wedge L_2$$

Uvek je ispunjeno $T(x_i, -x_i) \leq 0.5$. Ako je $T(C_1, C_2)>0.5$, onda je ili $T(L_1)>0.5$ ili $T(L_2)>0.5$ i $T(L_1 \vee L_2)= T(Rf(C_1,C_2))>0.5$. Zato $T(x_i, -x_i) \leq T(Rf(C_1,C_2)$ i prema teoremi 7.7 $T(C_1,C_2) \leq T(Rf(C_1,C_2))$.

Ako je istinitosna vrednost sastavaka veća od 0.5, prema posledici 7.9 njihova fazi rezolventa je značajna logička posledica.

7.10 TREĆA POSLEDICA TEOREME 7.7

Neka su C_1 i C_2 dva sastavka i $Rf(C_1,C_2)$ njihova fazi rezolventa sa ključnom promenljivom x_i. Ako je $T(x_i, -x_i)=T(Rf(C_1,C_2))$, tada je $T(C_1,C_2)=T(Rf(C_1,C_2))$.

DOKAZ neposredno sledi iz 7.7 i njenih posledica.

Tvrđenje koje je obratno 7.10 nije uvek istinito.

Ako je S skup satavaka, onda se n-ta fazi rezolucija, u oznaci Rn(S), definiše za svako $n \geq 0$ na sledeći način:

$Ro(S)= S$

$R_{n+1}(S)= Rf(R_n(S))$.

TEOREMA 7.12 Neka je S skup sastavaka i G sastavak iz $R_n(S)$. Ako je $T(G) \leq 0{,}5$, tada u S postoji sastavak C, takav da je $T(C) \leq 0.5$.

TEOREMA 7.13 Neka je S skup sastavaka i G sastavak iz $R_n(S)$. Ako je $T(G) \geq 0.5$, tada u S postoji sastavak C, takav da je $T(C) \leq T(G)$.

TEOREMA 7.14 Neka je S skup sastavaka i S sasavak iz Rn(S). Ako je $T(C) \geq 0.5$ za sve sastavke C iz S, tada je $T(S) \leq T(G)$.

POSLEDICA 7.15 Neka je S skup sastavaka. Ako je za sve sastavke C iz S, $T(C) \geq 0.5$, tada je $T(R_n(S))= T(S)>0.5$, za svako n.

POSLEDICA 7.16 Neka je S skup sastavaka i G sastavak iz $R_n(S)$. Ako je $T(G)<T(C)$ za sve sastavke C iz S, tada u S postoji sastavak C' takav da je $T(C') \leq 0.5$.

DEF 7.18 Neka su a i b elementi intervala $[0,1]$. $a>>b$ ako je $0.5 \geq a \geq b$ ili $0.5 \leq a \leq b$.

TEOREMA 7.19 Neka je S skup sastavaka i G fazi rezolventa dva sastavka iz S. Tada za svaku interpretaciju $T(S)>>T(S,G)$. S, tada je $T(S) \leq T(S)$.

TEOREMA 7.20 Neka je S skup sastavaka. Tada za sve $n \in M$ i za svaku interpretaciju $T(S)>>T(Rn(S))$.

LITERATURA

e

1. Aanderaa S.O., Lewis H.R., Linear sampling and the $\forall\exists\forall$ case of the decision problem, J.Symbolic Logic 39, 3 (1974), 519-548.

2. Anderson R., Bledsoe W., A linear format for resolucion with merging and a new technique for establishing completenes, J.ACM 17 (1970), 525-534.

3. Barwise J. (ed.) Handbook of Mathematical Logic, North-Holand, Amsterdam, 1977.

4. Bouer R.S., Locking: A Restriction of resolucion, Ph.D. Thesis, University of Texas at Austin, Texas, 1971.

5. Chang C.L., Lee R.C. SYMBOLIC LOGIC AND MEHANICAL THEOREM PROVING, Academic Press, 1973.

6. Chang C.L., The unit proof and the input proof in theorem proving, J.ACM 17 (1970), 698-707.

6. Church A. Introduction to Metamathematical Logic, Princeton Univ. Press, Princeton, 1956.

7. Davis M. Eliminating the irrelevant from mechanical proofs, Proceeding of Symposium in Applied Mathematics, American Mathematical Society, v.15, 1963.

8. Davis M., Putnam H., A computing procedure for quantification theory, J.ACM 7 (1960), 201-215.

9. Hunt E.B. Artificial Intelligence. New York, Academic Press 1975.

10. Herbrand J., Recherches sur la theorie de la demonstration, Thesis, Paris 1930.

11. Herbrand J., Recherches sur la theorie de la demonstration, Travaux de la Societe des Sciences et des Lettres de Varsovie, C1.III, Math.Phys., 33 (1930).

12. Hilbert D., Bernays P. Grundlagen der Mathematik, I-II, Springer-Verglar, 1968, 1970.

13. Jackson P.C. Introduction to Artificial Intelligence. New York, Petrocelli Bookss 1974.

14. Jennović D. Mehaničko dokazivanje teorema sa primenom u [illegible] formiranju hipoteza, magistarski rad, Beograd 1979.

15. Jovanović G. Jedno uopštenje rešavajućeg postupka za mehaničko dokazivanje teorema, magistarski rad, Beograd 1979.

16. Joyner W.H., Automatic theorem-proving and the decison problem, Tehn. Rep. 7-73, Center for Research in Computing tehnology, Harvard U., Cambridge, 197[illegible]

17. Joyner W.H., Automatic theorem-proving and the decison problem, 14th Annual Symp. on Swiching and Automata theory, Iowa City, Iowa, 1973, 159-166

18. Kallick B., A decision procedure based on the resolution method, Proc. IFIP Cong. 1968, North-Holland Pub.Co., Amsterdam, 269-275.

19. Kleene S.C. Introduction to Metamathematic, North-Holand, Amsterdam, 1952

20. Kleene S.C. Mathematical Logic, John Wiley & Sons, 1967.

21. Knuth D.E. The art of computer programming, Vol.1, Addison-Wesley Publishing Companu 1968.

22. Kowalsi R., Studies in the completness and efficienci of theorem proving by resolution. Ph.D. Thesis, Univ. of Edinburgh, 1970.

23. Kowalski R., Kuehner D., Linear resolution with selection function. Artificial Intelligence 2 (1971), 227-260.

24. Krom M.R., The decision problem for formulas in prenex conjunctive normal form with binary disjunctions, J.Symbolic logic 35 (1970), 210-216.

25. Lewis H.R., Program shemata and the first-order decision problem. J.Comput.Syst.Scis. 8, 1 (1974), 71-83.

26. Loveland D.W., Mechanical theorem proving by model elimination. J.ACM 15 (1968), 236-251.

27. Loveland D.W., A.Simplified format for the model elimination theorem-proving procedure. J.ACM 16 (1969), 349-363.

28. Loveland D.W., Theorem provers combining model elimination and resolution. Machine intelligence, 4/Ed. Melcer and Michie, American Elsevier, 1969, 73-86.

29. Loveland D.W., A linear format for resolucion, Proc. IRIA Symp. Automatic Demonstration, Versailles, France 1968, N.Y. 1970, 147-162.

30. Loveland D.W., Some linear Herbrand proof procedures, an analysis, Depth. of Computer Science, Carnegie-Mellon University, 1970.

31. Loveland D.W., A unifying view of some linear Herbrand procedures, J.ACM. 19 (1972), 366-384.

32. Lucham D., Refinement theorems in resolution theory, Proc. IRIA Symp. Automatic Demonstration, Versailles, France 1968, N.Y. 1970, Springer, 163-190.

33. Nilsson N.J. Principles of Artificial Intelligence, Tioga Publishing Co., 1980.

34. Melcer B., Theorem proving for computers: some results on resolution and renaming, Computer J. 8 (1966), 341-343.

35. Mendelson E. Introduction to Mathematical Logic, Van Nostrand Co., Princeton, 1963.

36. Prešic M., Prešic S., Uvod u matematičku logiku (teorija i zadaci), Matematički institut 1979.

37. Prešic S., Elementi matematičke logike, Zavod za izdavanje udžbenika, Beograd, 1972.

38. Reiter R., Two results on ordering for resolution with merging and linear format, J.ACM. 18 (1971), 630-646.

39. Robinson J.A. Theorem-proving on the computer, J.ACM 10 (1963), 163-174.

40. Robinson J.A. A machine oriented logic based on the resolucion principle, J.ACM 12 (1965), 23-41.

41. Robinson J.A., Automatic deduction with hyper-resolution, Internat.J. Comput. Math., 1965 (1) 227-234.

42. Robinson J.A., The generalized resolution principle, Machine Intelligence, 3/Ed. Melcer and Michie, Edinburgh U.Press, 1968, 77-93.

43. Shoenfield J.R. Mathematical Logic, Addison-Wesley Publishing Companu 1967.

44. Slagle J.R., Automatic theorem proving with renable and semantic resolution, J.ACM 14 (1967), 687-697.

45. Slagle J.R., Norton L., Experiments with an automated theorem prover having partial ordering rules, Division of Computer Research and Tehnology, National Inst., Health, Bethesda, Maryland, 1971.

46. Slagle J.R., Farrell C.D., Experiments in automatic learning for a multipurpose heuristic program, Comm.Assoc.Comput. Mach., 1971, 14, 91-99.

47. Wos L., Robinson G.A., Carson D.F., The unit preference strategy in theorem proving, Proc. AFIPS 1964 Fall Joint Computer Conf., 1964, 26, 616-621

48. Wos L., Robinson G.A., Carson D.F., Efficiency and completeness of the set support strategy in theorem proving, J.ACM 12 (1965), 536-541.

49. Whitehead A. N. Rusell B. Principia Mathematica, Cambridge Univ. Press 1927.