TARTU RIIKLIK ÜLIKOOL

RESOLUTSIOONIMEETOD

1989

TARTU RIIKLIK ÜLIKOOL
Programmeerimise kateeder

RESOLUTSIOONIMEETOD

Koostanud M. Koit

TARTU 1989

Kinnitatud matemaatikateaduskonna nõukogus 17.06.1988. a.

РЕЗОЛЮЦИОННЫЙ МЕТОД.
Составитель Маре К о й т.
На эстонском языке.
Тартуский государственный университет.
ЭССР, 202400, г.Тарту, ул.Юликооли, 18.
Vastutav toimetaja R. Prank.
Paljundamisele antud 23.01.1989.
Formaat 60x84/16.
Rotaatoripaber.
Masinakiri. Rotaprint.
Tingtrükipoognaid 3,49.
Arvestuspoognaid 3,30. Trükipoognaid 3,75.
Trükiarv 200.
Tell. nr. 56.
Hind 10 kop.
TRÜ trükikoda. ENSV, 202400 Tartu, Tiigi t. 78.

Saateks

Kaasajal ei piirdu elektronarvutite rakendusvaldkond üksnes arvutusülesannetega. Sagedamini tuleb arvutite abil lahendada selliseid probleeme, kus arvutamisel on hoopis kõrvaline roll. Niisuguste ülesannete hulka kuulub ka teoreemide tõestamine. Olgu mainitud, et paljusid sisuliselt erinevaid ülesandeid saab sõnastada teoreemi tõestamise ülesannetena: näiteks programmide analüüs ja süntees, küsimustele vastamine küsimus-vastussüsteemis, graafide isomorfismi probleem jpm.

Teoreemide tõestamise teooriale panid aluse saksa matemaatiku David Hilberti (1862-1943) matemaatilise loogika alased tööd. Esimese teoreemide automaatse tõestamise meetodi lõi 1930. aastal prantsuse matemaatik Jacques Herbrand (1908-1931). Paraku oli see väga töömahukas ega leidnud seetõttu praktilist rakendamist isegi elektronarvutite ilmumisel.

1960. aastate keskpaigaks töötati välja lihtsamad ja efektiivsemad tõestusmeetodid: resolutsioonimeetod (J. Robinson) ja pöördmeetod (S.J. Maslov). Kirjeldamise ja kasutamise lihtsuse tõttu on resolutsioonimeetod ja tema modifikatsioonid aluseks enamikule teoreemide tõestamise arvutiprogrammidele.

Käesolevas õppevahendis tutvustatakse teoreemide automaatse tõestamise probleeme, seejuures on põhitähelepanu suunatud resolutsioonimeetodile. Lugejalt eeldatakse matemaatilise loogika algmõistete tundmist. Õppevahend on ette nähtud rakendusmatemaatika V kursuse üliõpilastele erikursuses "Tehisintellektisüsteemid".

1. Teoreemi tõestamise ülesanne 1. järku predikaatarvutuses

Teoreemi tõestamise ülesande püstitamiseks tuleb eeldused ja väide esitada loogikavalemitena. Valime siin loogiliseks formalismiks 1. järku predikaatarvutuse. Alustame mõningate varasemast tuttavate mõistete meenutamisest.[1]

Koosnegu predikaatarvutuse alfabeet järgmistest sümbolitest:

1. eraldajad ( ) ,
2. loogiliste tehete märgid $\neg$ & $\vee$ $\rightarrow$
3. kvantorid $\forall$ $\exists$.
4. (indiviid-)muutujate sümbolid x_k $(k = 1,2,\ldots)$
5. n-kohaliste funktsioonide sümbolid f_k^n $(k \geqslant 1,\ n \geqslant 0)$; seejuures sümboleid f_k^0 nimetame konstantideks
6. n-kohaliste predikaatide sümbolid p_k^n $(k \geqslant 1,\ n \geqslant 1)$.

Edaspidi kasutame ka järgmisi tähistusi: x_k asemel u, v, w, x, y, z,...; f_k^0 asemel a, b, c, d,...; f_k^n $(n \neq 0)$ asemel f, g, h,...; p_k^n asemel P, Q, R, T, V, W,... .

Alfabeedi sümbolitest võib konstrueerida mitmesuguseid avaldisi. Vaatleme terme, elementaarvalemeid ja valemeid.

Termid:

a) iga indiviidmuutuja ja iga konstant on term.

b) Kui $t_1, \ldots, t_n$ on termid $(n \geqslant 1)$, siis ka $f_k^n(t_1, \ldots, t_n)$ on term.

c) Avaldis on term parajasti siis, kui ta on seda a) või b) põhjal.

Elementaarvalemid (ehk aatomid):

kui p_k^n on predikaatsümbol ja $t_1, \ldots, t_n$ on termid, siis $p_k^n(t_1, \ldots, t_n)$ on elementaarvalem.

----

[1] Vt. näit. I.Kull. Matemaatiline loogika. Tallinn, Eesti Riiklik Kirjastus, 1964; R.Prank. Matemaatiline loogika ja diskreetne matemaatika, III. Tartu, TRÜ, 1983.

Valemid:

a) iga elementaarvalem on valem.

b) Kui F ja G on valemid ning x on indiviidmuutuja, siis $(\neg F)$, $(F \& G)$, $(F \vee G)$, $(F \rightarrow G)$, $((\forall x)F)$, $((\exists x)F)$ on valemid.

c) Avaldis on valem parajasti siis, kui ta on seda a) või b) põhjal.

Valemites $((\forall x)F)$ ja $((\exists x)F)$ nimetatakse valemit F vastavalt üldsuskvantori ja olemasolukvantori *mõjupiirkonnaks*. Muutujat x nimetatakse kvantoriga *seotud muutujaks*. Valemeid üles kirjutades jätame edaspidi osa sulge ära, lugedes kvantoreid koos eitustega kõrgeima prioriteediga teheteks.

Öeldakse, et valem on *kinnine*, kui kõik temas esinevad muutujad on seotud. Meid huvitavad just kinnised valemid.

Et anda valemile sisu, interpreteeritakse teda kui teatavat väidet vaadeldava indiviidide piirkonna kohta. Selleks tuleb fikseerida indiviidide piirkond (indiviidmuutujate väärtuste piirkond) ning määrata valemis esinevate konstantide, predikaat- ja funktsionaalsümbolite tähendused.

Valemite (või valemite hulga) *interpretatsiooniks* nimetatakse paari, mis koosneb mittetühjast hulgast E (nn. interpretatsiooni kandjast) ja kujutusest, mis seab vastavusse

- igale predikaatsümbolile p_k^n mingi n-kohalise relatsiooni hulgas E,
- igale funktsionaalsümbolile f_k^n mingi n-kohalise funktsiooni hulgas E,
- igale konstandile f_k^0 mingi elemendi hulgast E.

Indiviidmuutujad omandavad väärtusi hulgast E.

Antud interpretatsiooni korral saab iga kinnine elementaarvalem $p_k^n(t_1, \ldots, t_n)$ tõeväärtuse "tõene" (t) või "väär" (v): kui hulga E elemendid, mis vastavad termidele $t_1, \ldots, t_n$, kuuluvad relatsiooni, mis on määratud selle interpretatsiooniga, siis loetakse elementaarvalemit tõeseks, vastasel korral aga vääraks.

Kvantoreid mittesisaldava mitteelementaarse valemi

2

väärtus arvutatakse tema koostisosade väärtustest nii, nagu on näidatud tõeväärtustabelis (F ja G on valemid).

F	G	$\neg$F	F $\vee$ G	F & G	F $\to$ G
v	v	t	v	v	t
v	t	t	t	v	t
t	v	v	t	v	v
t	t	v	t	t	t

Valem $(\forall x)F$ on tõene, kui x iga väärtuse korral hulgast E on valem F tõene; vastasel korral on valem $(\forall x)F$ väär. Valem $(\exists x)F$ on tõene, kui leidub selline x väärtus hulgast E, et valem F on tõene; vastasel juhul on valem $(\exists x)F$ väär. Lõpliku piirkonna E korral võib selliste valemite tõeväärtused määrata tõeväärtustabelist.

Näide 1.1. Vaatleme valemite $(\forall x)P(x)$ ja $(\exists x)\neg P(x)$ sellist interpretatsiooni, kus $E = \{1, 2\}$ ning predikaatsümbolile P vastab järgmine relatsioon:

P(1)	P(2)
t	v

Selles interpretatsioonis on esimene valem väär ja teine tõene.

Valemit F nimetatakse rahuldatavaks, kui leidub selline interpretatsioon, milles F on tõene. Kui valem F on tõene interpretatsioonis I, siis öeldakse, et I on F mudel ehk I rahuldab valemit F. Eelmises näites vaadeldud interpretatsioon on valemi $(\exists x)\neg P(x)$ mudel.

Kui valem F on väär interpretatsioonis I, siis öeldakse, et I ei rahulda valemit F. Eelmises näites vaadeldud interpretatsioon ei rahulda valemit $(\forall x)P(x)$.

Kui mingi valem on tõene kõikvõimalikes interpretatsioonides, siis nimetatakse teda samaselt tõeseks. Näiteks valem $P(a) \to (P(a) \vee P(b))$ on samaselt tõene.

Valemit nimetatakse samaselt vääraks (ehk mitterahuldatavaks), kui ta on väär kõikvõimalikes interpretatsioonides.

Kui valem F on samaselt tõene, siis tema eitus $\neg F$ on samaselt väär.

Viimati defineeritud mõisted võib üle kanda ka valemite hulgale. Seejuures eeldatakse, et kõik valemid on seotud konjunktsiooni märgiga.

Kui valemite hulk S on tõene interpretatsioonis I, siis öeldakse, et I on S mudel ehk I rahuldab hulka S.

Öeldakse, et valemite hulk $S = \{F_1, \ldots, F_n\}$ on vasturääkiv (ehk mitterahuldatav), kui konjunktsioon $F_1 \& \ldots \& F_n$ on samaselt väär.

Öeldakse, et valemite hulk $S = \{F_1, \ldots, F_n\}$ on rahuldatav, kui valemite konjunktsioon $F_1 \& \ldots \& F_n$ on rahuldatav (s.t. leidub interpretatsioon, milles iga valem F_i on tõene).

Öeldakse, et valemite hulk $S = \{F_1, \ldots, F_n\}$ on tõene (väär) interpretatsioonis I, kui valemite konjunktsioon $F_1 \& \ldots \& F_n$ on tõene (väär) interpretatsioonis I.

Valem G järeldub loogiliselt valemite hulgast $S = \{F_1, \ldots, F_n\}$, kui iga interpretatsioon, mis rahuldab valemite hulka S, rahuldab ka valemit G.

Näide 1.2. Vaatleme valemeid

$F_1 = (\forall x)(P(x) \rightarrow Q(x))$,

$F_2 = P(a)$.

Näitame, et valem Q(a) järeldub loogiliselt valemitest F_1 ja F_2.

Vaatleme suvalist interpretatsiooni I, mis rahuldab valemit $F_1 \& F_2$. Selles interpretatsioonis peab valem $F_2 = P(a)$ olema tõene. Oletame vastuväiteliselt, et valem Q(a) on interpretatsioonis I väär. Siis aga peab ka valem F_1 olema selles interpretatsioonis väär. See on vastuolus eeldusega. Järelikult on valem Q(a) tõene igas interpretatsioonis, mis rahuldab valemit $F_1 \& F_2$, s.t. Q(a) järeldub loogiliselt valemitest F_1 ja F_2.

Tõestame nüüd kaks edaspidise käsitluse jaoks olulist teoreemi.

Teoreem 1.1. Olgu antud valemid $F_1, \ldots, F_n$ ja valem G. Valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$ parajasti siis, kui valem $F_1 \& \ldots \& F_n \to G$ on samaselt tõene.

Tõestus. (=>) Järeldugu valem G loogiliselt valemitest $F_1, \ldots, F_n$. Olgu I suvaline interpretatsioon. Kui kõik valemid $F_1, \ldots, F_n$ on tõesed selles interpretatsioonis, siis definitsiooni kohaselt on seda ka G. Järelikult on ka valem $F_1 \& \ldots \& F_n \to G$ tõene. Kui aga kõik valemid $F_1, \ldots, F_n$ ei ole tõesed interpretatsioonis I (vähemalt üks on väär), siis on valem $F_1 \& \ldots \& F_n \to G$ ometi tõene selles interpretatsioonis. Seega on ta tõene igas interpretatsioonis, s.t. samaselt tõene.

(<=) Olgu valem $F_1 \& \ldots \& F_n \to G$ samaselt tõene. Vaatleme tema suvalist interpretatsiooni I. Kui valem $F_1 \& \ldots \& F_n$ on selles interpretatsioonis tõene, siis peab ka valem G olema tõene. Järelikult valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$.

Teoreem 1.2. Olgu antud valemid $F_1, \ldots, F_n$ ja valem G. Valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$ parajasti siis, kui valem $F_1 \& \ldots \& F_n \to \neg G$ on samaselt väär.

Tõestus. Tähistame valemite A ja B loogilist samaväärsust $A = B$. Kuna $\neg(F_1 \& \ldots \& F_n \to G) =$

$$= \neg(\neg(F_1 \& \ldots \& F_n) \vee G) =$$
$$= F_1 \& \ldots \& F_n \& \neg G,$$

siis teoreemi 1.1 kohaselt järeldub valem G loogiliselt valemitest $F_1, \ldots, F_n$ parajasti siis, kui valem $F_1 \& \ldots \& F_n \& \neg G$ on samaselt väär.

Kui valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$, siis nimetatakse valemit $F_1 \& \ldots \& F_n \to G$ *teoreemiks*. Valemeid $F_1, \ldots, F_n$ nimetatakse teoreemi *eeldusteks* ning valemit G teoreemi *väiteks*.

Näide 1.3. Näitest 1.2: kuna valem Q(a) järeldub loogiliselt valemite hulgast $\{(\forall x)(P(x) \to Q(x)), P(a)\}$, siis valem $(\forall x)(P(x) \to Q(x)) \& P(a) \to Q(a)$ on teoreem.

Ülesannet, mis seisneb selle asjaolu tõestamises, et teatav valem järeldub loogiliselt antud valemite hulgast, nimetatakse *teoreemi tõestamise ülesandeks* (TTÜ).

Teoreemi 1.1 kohaselt võib selle tõestamiseks, et valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$, tõestada, et valem $F_1 \& \ldots \& F_n \rightarrow G$ on samaselt tõene.

Teatavasti ei eksisteeri algoritmi, mis 1. järku predikaatarvutuse suvalise valemi korral selgitaks, kas see valem on samaselt tõene, s.t. 1. järku predikaatarvutus on mittelahenduv. Eksisteerib aga algoritm, mis iga samaselt tõese valemi korral teeb kindlaks, et see valem on samaselt tõene, s.t. predikaatarvutust võib nimetada *poollahenduvaks*.[1]

Praktikas osutub mugavamaks kindlaks teha mitte seda, kas valem on samaselt tõene, vaid hoopis kontrollida, kas ta on samaselt väär. Seepärast vaatleme teoreemi $F_1 \& \ldots \& F_n \rightarrow G$ tõestamiseks valemit $\neg(F_1 \& \ldots \& F_n \rightarrow G)$ ehk $F_1 \& \ldots \& F_n \& \neg G$ (lähtevalemi eitust) ja tõestame, et ta on samaselt väär, ehk, nagu öeldakse, kummutame valemi $F_1 \& \ldots \& F_n \& \neg G$. Selleks on vaja näidata, et ei eksisteeri ühtegi interpretatsiooni, mille korral valemid $F_1, \ldots, F_n, \neg G$ oleksid korraga tõesed.

Seoses predikaatarvutuse poollahenduvusega on tõestus (kummutamine) edukas (annab positiivse vastuse) ainult sel juhul, kui valem G järeldub loogiliselt valemitest $F_1, \ldots, F_n$. Vastasel korral võib kummutamisprotseduur töötada lõpmatuseni (või anda negatiivse vastuse).

Predikaatarvutuse valemi võimalike interpretatsioonide hulk pole lõplik, sest juba interpretatsiooni kandjat võib valida piiramatul arvul erinevatel viisidel. Seetõttu ei saa asjaolu, kas valem on samaselt väär, üldiselt välja selgitada valemi tõeväärtuse kontrollimise teel kõikvõimalikes interpretatsioonides.

Järgnevas asume tutvustama valemi samaselt vääruse väljaselgitamise Herbrandi meetodit. Enne aga vaatame, kuidas valemit teisendada nn. disjunktide hulgaks.

---

[1] Vt. näit. С. Клини. Введение в метаматематику. М., Издательство иностранной литературы, 1957, lk. 382.

3

2. Valemi teisendamine disjunktide hulgaks

2.1. Valemi teisendamine prefiksiga normaalkujule

Tõestusprotseduuri lihtsustamise huvides teisendatakse kummutatav valem nn. d̲i̲s̲j̲u̲n̲k̲t̲i̲d̲e̲ hulgaks. Selleks esitatakse valem kõigepealt nn. prefiksiga normaalkujul

$$(Q_1 x_1)(Q_2 x_2)\ldots(Q_n x_n)M, \tag{2.1}$$

kus iga Q_i $(i = 1,2,\ldots,n)$ on kas $\exists$ või $\forall$ (seejuures $(Q_1 x_1)(Q_2 x_2)\ldots(Q_n x_n)$ on nn. p̲r̲e̲f̲i̲k̲s̲) ning M on valem, mis ei sisalda kvantoreid (nn. m̲a̲a̲t̲r̲i̲k̲s̲).

1. järku predikaatarvutuse valemi teisendamisel normaalkujule kasutatakse järgmisi samasusi, nn. seadusi (rõhutamaks asjaolu, et valem F sisaldab vaba muutujat x, tähistame valemit F[x]; valem G ei sisalda muutujat x):

$$QxF[x] \vee G = (Qx)(F[x] \vee G) \tag{2.2}$$

$$QxF[x] \,\&\, G = (Qx)(F[x] \,\&\, G) \tag{2.3}$$

$$\neg((\forall x)F[x]) = (\exists x)(\neg F[x]) \tag{2.4}$$

$$\neg((\exists x)F[x]) = (\forall x)(\neg F[x]) \tag{2.5}$$

$$(\forall x)F[x] \,\&\, (\forall x)H[x] = (\forall x)(F[x] \,\&\, H[x]) \tag{2.6}$$

$$(\exists x)F[x] \vee (\exists x)H[x] = (\exists x)(F[x] \vee H[x]) \tag{2.7}$$

Seadused (2.2) ja (2.3) kehtivad, sest valem G ei sisalda muutujat x ja seetõttu võib teda kanda kvantori Q mõjupiirkonda.[1]

Seaduse (2.4) tõestamiseks (analoogilisel viisil tõestatakse ka (2.5), (2.6) ja (2.7)) vaatleme suvalist interpretatsiooni I, milles vasakpoolne valem $\neg((\forall x)F[x])$ on tõene. Siis aga on valem $(\forall x)F[x]$ väär. Järelikult leidub selline element e interpretatsiooni kandjas, et F[e] on väär, s.t. $\neg F[e]$ on tõene interpretatsioonis I. Järelikult on valem $(\exists x)(\neg F[x])$ tõene interpretatsioonis I. Teiselt poolt, kui $\neg(\forall x)F[x]$ on väär interpretatsioonis I, siis

----

[1] Vt. näit. I.Kull. Matemaatiline loogika. Tallinn, Eesti Riiklik Kirjastus, 1964, lk. 108.

$F[x]$ on tõene iga x väärtuse korral ja $\neg F[x]$ on väär iga x väärtuse korral interpretatsiooni kandjast. Siis ka $(\exists x)(\neg F[x])$ on väär interpretatsioonis I. Järelikult on mõlema vaadeldava valemi tõeväärtused võrdsed suvalises interpretatsioonis ning need valemid on loogiliselt samaväärsed.

Seaduse (2.6) põhjal võib konjunktsioonist üldsuskvantori tuua sulgude ette. Seaduse (2.7) põhjal võib sama teha olemasolukvantoriga disjunktsioonis. Seevastu üldsuskvantorit ei tohi sulgude ette tuua disjunktsioonis ning olemasolukvantorit konjunktsioonis, s.t.

$$(\forall x)F[x] \vee (\forall x)G[x] \neq (\forall x)(F[x] \vee G[x]),$$

$$(\exists x)F[x] \mathbin{\&} (\exists x)G[x] \neq (\exists x)(F[x] \mathbin{\&} G[x]).$$

Niisugustel juhtudel tuleb ühes valemis seotud muutuja ümber nimetada. Nii näiteks kui muutuja z ei esine valemis $F[x]$, siis

$$(\forall x)F[x] \vee (\forall x)H[x] = (\forall x)F[x] \vee (\forall z)H[z]$$

ja seaduse (2.2) põhjal saame

$$(\forall x)F[x] \vee (\forall x)H[x] = (\forall x)(\forall z)(F[x] \vee H[z]). \qquad (2.8)$$

Analoogiliselt

$$(\exists x)F[x] \mathbin{\&} (\exists x)H[x] = (\exists x)(\exists z)(F[x] \mathbin{\&} H[z]). \qquad (2.9)$$

Lisaks seadustele (2.2) kuni (2.9) kasutatakse valemi teisendamiseks normaalkujule veel järgmisi lausearvutusest tuttavaid seadusi:

$$F \rightarrow G = \neg F \vee G \qquad (2.10)$$

$$\neg(\neg F) = F \qquad (2.11)$$

$$\neg(F \vee G) = \neg F \mathbin{\&} \neg G \qquad (2.12)$$

$$\neg(F \mathbin{\&} G) = \neg F \vee \neg G \qquad (2.13)$$

Valemi teisendamine prefiksiga normaalkujule võib toimuda järgmiste tegevuste järjest rakendamise teel.

1. Implikatsiooni märkide elimineerimine. Iga valem $F \rightarrow G$ asendatakse loogiliselt samaväärse valemiga $\neg F \vee G$.

2. Eituse märkide viimine elementaarvalemiteni. Kõikjal, kus võimalik, tehakse järgmised asendused:

$\neg\neg F$ asemel F,

$\neg(F \vee G)$ asemel $\neg F \mathbin{\&} \neg G$,

$\neg(F \mathbin{\&} G)$ asemel $\neg F \vee \neg G$,

$\neg(\forall x F)$ asemel $\exists x(\neg F)$,

$\neg(\exists x F)$ asemel $\forall x(\neg F)$,

kasutades seadusi (2.11), (2.12), (2.13), (2.4), (2.5). Nii saadakse lõpuks valem, milles eituse märgid asuvad vahetult elementaarvalemite ees.

3. Muutujate ümbernimetamine. Tehakse sellised muutujavahetused, et kõik kvantoritega seotud muutujad oleksid erinevad. Näiteks valem $\forall x R(x) \vee \forall x T(x)$ kirjutatakse ümber kujul $\forall x R(x) \vee \forall y T(y)$.

4. Kvantorite tõstmine valemi algusesse, kasutades seadusi (2.2), (2.3), (2.6)-(2.9). Teisendamise tulemusel saame esialgsega loogiliselt samaväärse valemi.

Näide 2.1. Teisendame prefiksiga normaalkujule valemi F:

$$(\forall x)(\forall y)((\exists z)(P(x,z) \ \& \ P(y,z)) \rightarrow (\exists u)Q(x,y,u)).$$

Sulgudes näitame kasutatud seaduse numbri:

$$F = (\forall x)(\forall y)(\neg(\exists z)(P(x,z) \ \& \ P(y,z)) \vee (\exists u)Q(x,y,u)) =$$
(2.10)
$$= (\forall x)(\forall y)((\forall z)(\neg P(x,z) \vee \neg P(y,z)) \vee (\exists u)Q(x,y,u)) =$$
(2.5), (2.13)
$$= (\forall x)(\forall y)(\forall z)(\exists u)(\neg P(x,z) \vee \neg P(y,z) \vee Q(x,y,u)).$$
(2.2)

2.2. Valemi teisendamine prefiksiga normaalkujult disjunktide hulgaks

Äsja kirjeldatud tegevuste 1 kuni 4 sooritamise tulemusel saab suvalise 1. järku predikaatarvutuse valemi teisendada prefiksiga normaalkujule (2.1)

$$(Q_1 x_1)\ldots(Q_n x_n)M.$$

Edasi teisendatakse maatriks M, mis ei sisalda kvantoreid, temaga loogiliselt samaväärsele konjunktiivsele normaalkujule.[1] Seejärel elimineeritakse kõik olemasolukvantorid, kasutades Skolemi funktsioone.[2] See toimub järgmiselt.

---

[1] Vt. näit. I.Kull. Matemaatiline loogika. Tallinn, 1964, lk. 33.

[2] Vt. sealsamas, lk. 125.

Olgu valem esitatud prefiksiga normaalkujul (2.1), milles maatriks M on juba esitatud konjunktiivsel normaalkujul. Olgu Q_r olemasolukvantor ($1 \leqslant r \leqslant n$). Kui kvantorist Q_r vasakul ei asu ühtegi üldsuskvantorit, siis valime uue konstandi c (mis erineb valemis M sisalduvatest konstantidest) ja asendame valemis M kõik muutuja x_r esinemised konstandiga c. Lõpuks tõmbame maha ($Q_r x_r$).

Kui olemasolukvantorist Q_r vasakul paiknevad üldsuskvantorid $Q_{s_1}, \ldots, Q_{s_m}$ ($1 \leqslant s_1 < s_2 < \ldots < s_m < r$), siis valime uue m-kohalise funktsiooni sümboli f (mis ei sisaldu valemis M), asendame valemis M kõik muutuja x_r esinemised termiga $f(x_{s_1}, x_{s_2}, \ldots, x_{s_m})$ ja tõmbame maha ($Q_r x_r$).

Seda protsessi rakendame kõigi olemasolukvantorite korral. Lõpuks saame antud valemi nn. standardkuju.

Konstante ja funktsioone, mida kasutatakse olemasolukvantori muutujate asemel, nimetatakse *Skolemi funktsioonideks*.

Näide 2.2. Teisendame standardkujule näites 2.1 vaadeldud valemi F, lähtudes tema prefiksiga normaalkujust

$(\forall x)(\forall y)(\forall z)(\exists u)(\neg P(x,z) \vee \neg P(y,z) \vee Q(x,y,u))$.

Maatriks on juba konjunktiivsel normaalkujul. Elimineerinud ainsa olemasolukvantori, saame valemi F standardkuju

$(\forall x)(\forall y)(\forall z)(\neg P(x,z) \vee \neg P(y,z) \vee Q(x,y,f(x,y,z)))$.

Näide 2.3. Teisendame standardkujule prefiksiga normaalkujul esitatud valemi F:

$(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(x,y,z,u,v,w)$.

Elimineerides olemasolukvantoreid, asendame muutuja x konstandiga a, muutuja u Skolemi funktsiooniga f(y,z) ning muutuja w Skolemi funktsiooniga g(y,z,v). Saame valemi F standardkuju

$(\forall y)(\forall z)(\forall v)P(a,y,z,f(y,z),v,g(y,z,v))$.

Näide 2.4. Teisendame standardkujule prefiksiga normaalkujul esitatud valemi F:

$(\forall x)(\exists y)(\exists z)((\neg P(x,y) \,\&\, Q(x,z)) \vee R(x,y,z))$.

Kõigepealt teisendame maatriksi konjunktiivsele normaalkujule:

$(\neg P(x,y) \vee R(x,y,z))\ \&\ (Q(x,z) \vee R(x,y,z))$.

Elimineerinud olemasolukvantorid, saame valemi F standardkuju:

$(\forall x)((\neg P(x,f(x)) \vee R(x,f(x),g(x)))\ \&$
$\&\ (Q(x,g(x)) \vee R(x,f(x),g(x))))$.

Elementaarvalemit või selle eitust nimetatakse *literaaliks*. Literaalide disjunktsiooni (milles erijuhul võib olla ka 0 literaali või 1 literaal) nimetatakse *disjunktiks*.

Kui disjunkt ei sisalda ühtki literaali, siis nimetatakse teda *tühidisjunktiks* ja tähistatakse []. Kuna tühidisjunkt ei sisalda ühtki literaali, mis võiks suvalises interpretatsioonis olla tõene, siis on tühidisjunkt alati väär.

Loeme disjunktide hulka S kõigi temasse kuuluvate disjunktide konjunktsiooniks. Kõiki hulga S disjunktides esinevaid muutujaid loeme üldsuskvantoriga seotuiks.

Selle kokkuleppe kohaselt võib valemi standardkuju esitada disjunktide hulgana (jättes niisiis ära üldsuskvantorid ja konjunktsiooni märgid).

Näide 2.5. Näidetes 2.1 ja 2.2 vaadeldud valemi standardkuju võib esitada üheelemendilise disjunktide hulgana

$\{\neg P(x,z) \vee \neg P(y,z) \vee Q(x,y,f(x,y,z))\}$.

Näites 2.4 vaadeldud valemi standardkuju esitub disjunktide hulgana

$\{\neg P(x,f(x)) \vee R(x,f(x),g(x)),\ Q(x,g(x)) \vee R(x,f(x),g(x))\}$.

Kui samaselt vääras valemis elimineerida olemasolukvantorid, siis saadud valem on ikka samaselt väär ja vastav disjunktide hulk on vasturääkiv. Kehtib järgmine

teoreem 2.1. Olgu S disjunktide hulk, mis esitab valemi F standardkuju. Valem F on samaselt väär parajasti siis, kui hulk S on vasturääkiv.

Tõestus. Üldsust kitsendamata võib eeldada, et valem F on esitatud normaalkujul:

$F = (Q_1 x_1) \ldots (Q_n x_n) M[x_1, \ldots, x_n]$.

Olgu Q_r vasakpoolseim olemasolukvantor. Tähistame
$F_1 = (\forall x_1)\ldots(\forall x_{r-1})(Q_{r+1}x_{r+1})\ldots(Q_n x_n)M[x_1,\ldots,x_{r-1},f(x_1,\ldots,x_{r-1}),x_{r+1},\ldots,x_n]$,
kus f on muutujale x vastav Skolemi funktsioon ($1 \leqslant r \leqslant n$). Tõestame, et valem F on samaselt väär parajasti siis, kui F_1 on samaselt väär.

Oletame vastuväiteliselt, et F_1 ei ole samaselt väär. Siis leidub interpretatsioon I, nii et F_1 on tõene interpretatsioonis I, s.t. iga $x_1,\ldots,x_{r-1}$ korral leidub vähemalt üks element (ja nimelt $f(x_1,\ldots,x_{r-1})$), mille korral valem

$(Q_{r+1}x_{r+1})\ldots(Q_n x_n)M[x_1,\ldots,x_{r-1},f(x_1,\ldots,x_{r-1}),x_{r+1},\ldots,x_n]$

on tõene. Ka valem F peaks siis olema tõene interpretatsioonis I, mis aga on vastuolus eeldusega. Järelikult peab valem F_1 olema samaselt väär.

Oletame nuud vastuväiteliselt, et valem F ei ole samaselt väär. Siis leidub interpretatsioon I, kandjaga D, milles F on tõene, s.t. iga $x_1,\ldots,x_{r-1}$ korral leidub selline element x_r, et valem

$(Q_{r+1}x_{r+1})\ldots(Q_n x_n)M[x_1,\ldots,x_{r-1},x_r,x_{r+1},\ldots,x_n]$

on tõene. Laiendame interpretatsiooni I, lisades funktsiooni f, mis kujutab $(x_1,\ldots,x_{r-1})$ elemendiks x_r iga $x_1,\ldots,x_{r-1}$ korral piirkonnast D, s.t. $f(x_1,\ldots,x_{r-1}) = x_r$. Tähistame saadud interpretatsiooni I'. Iga $x_1,\ldots,x_{r-1}$ korral on valem

$(Q_{r+1}x_{r+1})\ldots(Q_n x_n)M[x_1,\ldots x_{r-1},f(x_1,\ldots,x_{r-1}),x_{r+1},\ldots,x_n]$

tõene interpretatsioonis I', s.t. valem F on tõene interpretatsioonis I'. See aga on vastuolus eeldusega. Järelikult peab valem F olema samaselt väär.

Oletame nüüd, et valemis F on m olemasolukvantorit, ja olgu $F_0 = F$. Olgu valem F_k saadud valemist F_{k-1} esimese olemasolukvantori asendamise teel Skolemi funktsiooniga ($k = 1,\ldots,m$). Analoogiliselt eelnevaga saab näidata, et valem F_{k-1} on samaselt väär parajasti siis, kui F_k on samaselt väär. Aga $F_m = S$. Seega F on samaselt väär parajasti siis, kui disjunktide hulk S on vasturääkiv.

Valemi F teisendamine disjunktide hulgaks toimub niisiis järgmiste tegevuste järjest rakendamise teel:

1. implikatsiooni märkide elimineerimine,

2. eituse märkide viimine elementaarvalemiteni,

3. seotud muutujate ümbernimetamine,

4. kvantorite ettetoomine,

5. maatriksi teisendamine konjunktiivsele normaalkujule,

6. olemasolukvantorite elimineerimine, kasutades Skolemi funktsioone,

7. prefiksi ärajätmine,

8. konjunktsiooni märkide ärajätmine.

Näide 2.6. Teisendame disjunktide hulgaks valemi F:

$(\exists x)(\neg((\exists y)P(x,y)) \rightarrow ((\exists z)Q(z) \rightarrow R(x)))$

(ühtlasi näidates kasutatud tegevuse numbri).

$$F \overset{1,2}{=} (\exists x)(((\exists y)P(x,y)) \vee ((\forall z)\neg Q(z) \vee R(x))) \overset{4}{=}$$

$$= (\exists x)(\exists y)(\forall z)(P(x,y) \vee \neg Q(z) \vee R(x)) \overset{6}{=}$$

$$= (\forall z)(P(a,b) \vee \neg Q(z) \vee R(a)),$$

7: $\{P(a,b) \vee \neg Q(z) \vee R(a)\}$.

Näide 2.7. Teisendame disjunktide hulgaks valemi F:

$(\forall x)(\forall y)((\exists z)P(x,y,z) \ \& \ ((\exists u)Q(x,u) \rightarrow (\exists v)Q(y,v)))$.

$$F \overset{1,2}{=} (\forall x)(\forall y)((\exists z)P(x,y,z) \ \& \ ((\forall u)\neg Q(x,u) \vee$$
$$\vee (\exists v)Q(y,v))) \overset{4}{=}$$

$$= (\forall x)(\forall y)(\exists z)(\forall u)(\exists v)(P(x,y,z) \ \& \ (\neg Q(x,u) \vee$$
$$\vee Q(y,v))) \overset{6}{=}$$

$$= (\forall x)(\forall y)(\forall u)(P(x,y,f(x,y)) \ \& \ (\neg Q(x,u) \vee$$
$$\vee Q(y,g(x,y,u)))),$$

7,8: $\{P(x,y,f(x,y)), \ \neg Q(x,u) \vee Q(y,g(x,y,u))\}$.

Siitpeale eeldame, et kummutamisprotseduuri sisendil on antud valemile F vastav disjunktide hulk S. Tõestuse, et valem F on samaselt väär, asendame tõestusega, et disjunktide hulk S on vasturääkiv.

3. Disjunktide hulga H-interpretatsioon. Herbrandi teoreem

3.1. Herbrandi universum ja H-interpretatsioon

Teoreemi F_1 &...& $F_n \to G$ tõestamiseks tuleb näidata, et vastav disjunktide hulk S on vasturääkiv. Valemite hulk on aga vasturääkiv parajasti siis, kui temasse kuuluvate valemite konjunktsioon on väär kõikvõimalikes interpretatsioonides kõikvõimalike kandjatega. Kuna võimatu on vaadelda kõiki interpretatsioone kõikide kandjatega, siis on meie järgmiseks eesmärgiks leida üks "hea" kandja, mis esindaks kõikvõimalikke ja mida saaks hõlpsasti konstrueerida kummutatava valemi põhjal. Selline kandja leidub tõepoolest, teda nimetatakse disjunktide hulga Herbrandi universumiks.

Disjunktide hulga Herbrandi universum konstrueeritakse järgmiselt.

Def. Olgu H_0 hulga S disjunktides esinevate konstantide hulk. Kui S ei sisalda konstante, siis paigutatakse hulka H_0 suvaline konstant, näiteks $H_0 = \{a\}$. Seejärel olgu i=0,1,... korral

$$H_{i+1} = H_i \cup \{f^n(t_1,\dots,t_n) \mid f^n \text{ on hulgas S esinev n-kohaline funktsioon, } t_j \in H_i,\ j = 1,\dots,n\}.$$

Hulka $H = \bigcup_{i=0}^{\infty} H_i$ nimetatakse disjunktide hulga S *Herbrandi universumiks*, iga hulka H_i aga Herbrandi universumi *i-ndaks tasemeks* (i = 0,1,...).

Näide 3.1. Olgu S = {P(x) ∨ Q(y), ¬P(a), ¬Q(b)}. Siis $H = H_0 = H_1 = \dots = \{a,b\}$.

Näide 3.2. Olgu S = {R(x), P(g(x)) ∨ Q(y)}. Siis

$H_0 = \{a\}$,

$H_1 = H_0 \cup \{g(a)\}$,

$H_2 = H_1 \cup \{g(g(a))\}$,

....

$H = \{a, g(a), g(g(a)), g(g(g(a))), \dots\}$.

Def. Disjunktide hulga S *Herbrandi baasiks* H_B nimetatakse kõigi elementaarvalemite hulka kujul $P^n(h_1, \ldots, h_n)$, kus predikaatsümbol P^n sisaldub hulga S disjunktides ja $h_1, \ldots, h_n \in H$.

Näide 3.3. Näites 3.1 toodud disjunktide hulga Herbrandi baasiks on hulk

$H_B = \{P(a), P(b), Q(a), Q(b)\}$.

Näide 3.4. Näites 3.2 toodud disjunktide hulga Herbrandi baasiks on hulk

$H_B = \{R(a), P(a), Q(a), R(g(a)), P(g(a)), Q(g(a)), R(g(g(a))), P(g(g(a))), Q(g(g(a))), \ldots\}$.

Vaatleme nüüd interpretatsioone, mille kandjaks on Herbrandi universum, ning eraldame nende hulgast nn. H-interpretatsioonid.

Def. Interpretatsiooni I nimetatakse disjunktide hulga S *H-interpretatsiooniks* parajasti siis, kui kehtivad järgmised tingimused.

1. I kujutab hulga S iga konstandi iseendaks.

2. Olgu f suvaline n-kohalise funktsiooni sümbol, mis sisaldub hulga S disjunktides, ja olgu $h_1, \ldots, h_n$ hulga S Herbrandi universumi H elemendid. Interpretatsioon I seab funktsionaalsümbolile f vastavusse funktsiooni, mis kujutab (hulga H^n elemendi) $(h_1, \ldots, h_n)$ (hulga H elemendiks) $f(h_1, \ldots, h_n)$.

Hulgas S sisalduvaid predikaatsümboleid võib väärtustada suvaliselt.

Disjunktide hulga S iga H-interpretatsiooni võib vaadelda kui hulga S Herbrandi baasi elementide väärtustamist. Olgu $H_B = \{A_1, \ldots, A_n, \ldots\}$ disjunktide hulga S Herbrandi baas. Suvalise H-interpretatsiooni võib siis esitada kujul $I = \{m_1, \ldots, m_n, \ldots\}$, kus m_j on kas A_j või $\neg A_j$ $(j = 1,2,\ldots)$. Kui m_j on A_j, siis on elementaarvalemile A_j omistatud tõeväärtus "tõene", vastupidisel juhul aga "väär".

Näide 3.5. Vaatleme näites 3.1 toodud disjunktide hulka S. Tema Herbrandi universum on $H = \{a, b\}$. H-interpretatsioon seab konstandile a vastavusse a ja konstandile b vastavusse b. Hulga S H-interpretatsioonid on näiteks

$$I_1 = \{P(a),\ P(b),\ Q(a),\ Q(b)\}$$

(s.o. H-interpretatsioon, milles kõik elementaarvalemid P(a), P(b), Q(a), Q(b) on tõesed);

$$I_2 = \{\neg P(a),\ \neg P(b),\ \neg Q(a),\ \neg Q(b)\}$$

(s.o. H-interpretatsioon, milles kõik elementaarvalemid on väärad);

$$I_3 = \{P(a),\ P(b),\ \neg Q(a),\ \neg Q(b)\}$$

jne. Määrates erinevaid tõeväärtusi elementaarvalemitele, saame kokku 16 antud disjunktide hulga H-interpretatsiooni.

Näide 3.6. Vaatleme näites 3.2 toodud disjunktide hulka. H-interpretatsiooni kandjaks on hulk $H = \{a, g(a), g(g(a)), \ldots\}$. Kujutus (definitsiooni kohaselt):

$a \rightarrow a$,

$g \rightarrow g$ nii, et $g(h) \rightarrow g(h)$ iga $h \in H$ korral.

Hulga S H-interpretatsioone:

$I_1 = \{R(a),\ P(a),\ Q(a),\ R(g(a)),\ P(g(a)),\ Q(g(a)), \ldots\}$

(s.o. interpretatsioon, milles iga elementaarvalem on tõene);

$I_2 = \{\neg R(a),\ \neg P(a),\ \neg Q(a),\ \neg R(g(a)),\ \neg P(g(a)),\ \neg Q(g(a)), \ldots\}$;

$I_3 = \{\neg R(a),\ P(a),\ Q(a),\ \neg R(g(a)),\ P(g(a)),\ Q(g(a)), \ldots\}$

jne.

Disjunktide hulga igale interpretatsioonile saab vastavusse seada teatava H-interpretatsiooni.

Olgu I interpretatsioon, mille kandja on D. *Interpretatsioonile I vastavaks H-interpretatsiooniks* I* nimetatakse interpretatsiooni, mis konstrueeritakse järgmiselt:

olgu $h_1, \ldots, h_n$ Herbrandi universumi H elemendid. Olgu termile h_i interpretatsioonis I* vastav element $d_i \in D$. Kui $P(d_1, \ldots, d_n)$ omandab interpretatsioonis I väärtuse t (vastavalt v), siis ka $P(h_1, \ldots, h_n)$ omandab interpretatsioonis I* väärtuse t (vastavalt v).

Kehtib järgmine

teoreem 3.1. Disjunktide hulk on vasturääkiv parajasti siis, kui ta on väär kõigis oma H-interpretatsioonides.

<u>Tõestus</u>. (=>) Kui S on vasturääkiv, siis peab ta olema väär kõigis interpretatsioonides igasuguste kandjatega, sealhulgas ka kõigis oma H-interpretatsioonides.

(<=) Olgu S väär kõigis oma H-interpretatsioonides. Oletame vastuväiteliselt, et S ei ole vasturääkiv. Siis leidub selline interpretatsioon I, kandjaga D, milles S on tõene. Olgu I* interpretatsioonile I vastav H-interpretatsioon. S on tõene interpretatsioonis I*. See aga on vastuolus eeldusega. Järelikult peab hulk S olema vasturääkiv.

Seega piisab hulga S vasturääkivuse väljaselgitamiseks tema H-interpretatsioonide läbivaatamisest. Kui H-interpretatsioonide hulk on lõplik (nagu näites 3.5), siis on selle teoreemi alusel võimalik tõestada disjunktide hulga vasturääkivust.

3.2. Semantilised puud

Hulga S kõik H-interpretatsioonid võib esitada graafina, mida nimetatakse semantiliseks puuks. Disjunktide hulga vasturääkivuse tõestamist võib siis vaadelda kui tema semantilise puu konstrueerimist.

Esitame kõigepealt mõned definitsioonid.

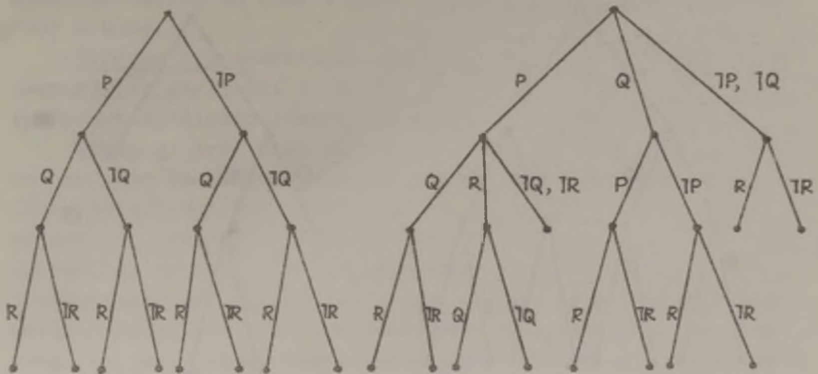
<u>Def</u>. Olgu A elementaarvalem. Literaale A ja $\neg A$ nimetatakse <u>kontraarseteks</u>, hulka $\{A, \neg A\}$ nimetatakse <u>kontraarseks paariks</u>.

<u>Def</u>. Olgu S disjunktide hulk ning olgu H_B tema Herbrandi baas. Hulga S <u>semantiliseks puuks</u> nimetatakse puud, milles igale kaarele on vastavusse seatud lõplik hulk literaale hulgast H_B nii, et

(i) igast tipust N väljub ainult lõplik hulk kaari L_1, ..., L_n. Olgu Q_i kaarele L_i vastavate literaalide konjunktsioon ($i = 1, \ldots, n$). Siis $Q_1 \vee \ldots \vee Q_n$ on samaselt tõene valem.

(ii) Tähistagu iga tipu N korral I(N) kõikide hulkade ühendit, mis vastavad tippu N viiva tee kaartele. Siis I(N) ei sisalda kontraarseid paare.

Näide 3.7. Olgu $H_B = \{P, Q, R\}$ hulga S Herbrandi baas. Joonisel on kujutatud hulga S kaks semantilist puud.



Def. Olgu $H_B = \{A_1, \ldots, A_n, \ldots\}$ disjunktide hulga S Herbrandi baas. Öeldakse, et hulga S semantiline puu on täielik parajasti siis, kui iga i = 1, 2, ... ja iga rippuva tipu N korral sisaldab I(N) kas A_i või $\neg A_i$.

Eelmises näites toodud semantilised puud on täielikud.

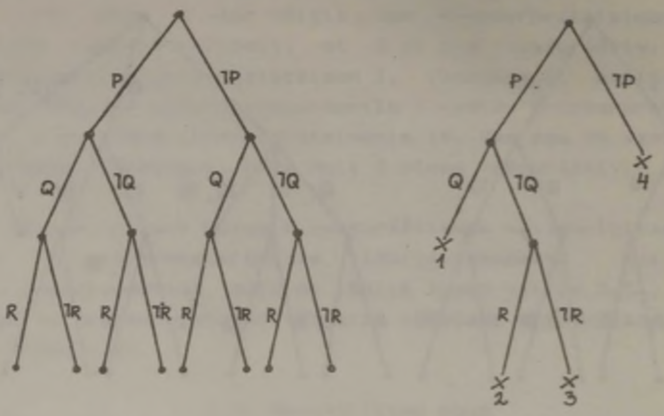
Kui hulga S Herbrandi baas on lõpmatu, siis on ka S iga täielik semantiline puu lõpmatu.

Täielik semantiline puu esitab hulga S kõikvõimalikud H-interpretatsioonid.

Iga tipu N korral moodustab I(N) osa hulga S mingist interpretatsioonist.

Kui S on vasturääkiv, siis ta peab olema väär igas H-interpretatsioonis. Me võime semantilise puu haru konstrueerimise peatada tipus N, kui I(N) ei rahulda hulka S.

Näide 3.8. Olgu $S = \{P,\ Q \vee R,\ \neg P \vee \neg Q,\ \neg P \vee \neg R\}$. Hulga S Herbrandi baas on $H = \{P, Q, R\}$. Joonisel on vasakul näidatud hulga S täielik semantiline puu, mille konstrueerimine on peatatud igas niisuguses tipus N, kus selgub, et I(N) ei rahulda hulga S mingit disjunkti. Tipus 1 selgub



nimelt, et väärtuse v saab disjunkt $\neg P \vee \neg Q$, tipus 2 - disjunkt $\neg P \vee \neg R$, tipus 3 - disjunkt $Q \vee R$, tipus 4 - disjunkt P.

3.3. Herbrandi teoreem

Herbrandi teoreem on aluseks enamikule kaasaegsetele masinalgoritmidele, mis on välja töötatud teoreemide tõestamiseks. Herbrandi teoreem põhineb eespol tõestatud teoreemil 3.1, s.t. selleks et selgitada, kas disjunktide hulk on vasturääkiv, on tarvilik ja piisav kontrollida ainult H-interpretatsioone. Kuna disjunktide hulga S H-interpretatsioone võib olla lõpmatu hulk, siis tuleb neid teataval viisil süstematiseerida. Selleks saab kasutada semantilist puud.

Def. Disjunkti C *fundamentaalnäiteks* nimetatakse disjunkti, mis on saadud C kõigi muutujate asendamisel Herbrandi universumi elementidega (samad muutujad asendatakse samade elementidega).

Näide 3.9. Vaatleme näites 3.1 toodud disjunktide hulka $S = \{P(x) \vee Q(y),\ P(a),\ Q(a)\}$. Disjunkti $P(x) \vee Q(y)$ fundamentaalnäited on $P(a) \vee Q(a)$, $P(a) \vee Q(b)$, $P(b) \vee Q(a)$, $P(b) \vee Q(b)$.

Teoreem 3.2 (Herbrandi teoreem). Disjunktide hulk S on vasturääkiv parajasti siis, kui eksisteerib tema disjunktide fundamentaalnäidete lõplik vasturääkiv hulk S'.

Tõestus. (=>) Olgu disjunktide hulk S vasturääkiv. Siis on ta väär oma kõikides interpretatsioonides, sealhulgas H-interpretatsioonides. Hakkame juurest alates läbima hulga S täielikku semantilist puud. Selle puu iga haru läbimise katkestame niipea, kui järjekordses tipus selgub, et vastav interpretatsioon ei rahulda hulga S mingi disjunkti C fundamentaalnäidet C'. Ühtlasi eemaldame veel läbimata osa sellest harust. Saame semantilise puu, milles on lõplik arv tippe ja lõplik arv kaari (see järeldub Kőnigi lemmast[1]). Järelikult leidub fundamentaalnäidete lõplik hulk, kus iga fundamentaalnäide C' on väär vähemalt ühes H-interpretatsioonis. Seetõttu on ka hulk S' vasturääkiv.

(<=) Oletame, et leidub disjunktide hulga S fundamentaalnäidete lõplik hulk S', mis on vasturääkiv. Kuna S iga interpretatsioon I sisaldab hulga S' interpretatsiooni I' ning I' ei rahulda hulka S', siis interpretatsioon I ei rahulda samuti hulka S'. Kuid ükski interpretatsioon I' ei rahulda hulka S'. Järelikult ka ükski (hulga S) interpretatsioon I ei rahulda hulka S'. Seepärast ei rahulda hulka S ükski hulga S' interpretatsioon. Järelikult on S vasturääkiv.

Näide 3.10. Vaatleme valemit $(\forall x)P(x) \& (\exists x) \neg P(y)$. Tema standardkuju võib esitada disjunktide hulgana $S = \{P(x),\ \neg P(f(a))\}$. See on vasturääkiv disjunktide hulk, sest leidub tema fundamentaalnäidete vasturääkiv hulk

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

------

[1] Vt. näit. Д. Кнут. Искусство программирования для ЭВМ. Т. I. Основные алгоритмы. М., Мир, 1976, lk. 472.

Teoreemi 2.1 põhjal on valem $(\forall x)P(x)$ & $(\exists y)\neg P(y)$ samaselt väär.

Herbrandi teoreemi põhjal saab TTÜ konstruktiivselt lahendada: genereerime valemi standardkuju esitava disjunktide hulga S fundamentaalnäidete hulki $S'_0 \subseteq S'_1 \subseteq S'_2 \subseteq \ldots$. Iga hulga S'_i saamiseks $(i = 0,1,2,\ldots)$ asendame hulga S disjunktides muutujad (kõikvõimalikel viisidel) Herbrandi universumi i-nda taseme elementidega. Kontrollime, kas S'_i on vasturääkiv, kasutades selleks suvalist lausearvutuses sobivat meetodit (hulga S'_i disjunktides ei sisaldu muutujaid). Kui S'_i on vasturääkiv, siis Herbrandi teoreemi põhjal on ka S vasturääkiv. Vastasel korral genereerime järgmise hulga S'_{i+1}. Protsess võib predikaatarvutuse poollahenduvuse tõttu kesta lõpmatuseni. Kui aga S on vasturääkiv, siis garanteerib Herbrandi teoreem, et see protseduur avastab hulga S fundamentaalnäidete vasturääkiva hulga S'_i.

Herbrandi teoreem oli esimeste arvutil realiseeritud kummutamisprotseduuride aluseks.

Näide 3.11. Olgu $S = \{P(x), \neg P(f(y))\}$. Tõestame, et S on vasturääkiv, konstrueerides fundamentaalnäidete hulki. Kuna

$$H_0 = \{a\},$$

siis

$$S'_0 = \{P(a), \neg P(f(a))\}.$$

Hulk S'_0 ei ole vasturääkiv. Leiame Herbrandi universumi 1. taseme:

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

Siis

$$S'_1 = \{P(a), P(f(a)), \neg P(f(a)), \neg P(f(f(a)))\}.$$

Hulk S'_1 on vasturääkiv, sest sisaldab kontraarse paari $P(f(a))$, $\neg P(f(a))$, seega Herbrandi teoreemi kohaselt on ka hulk S vasturääkiv.

Näide 3.12. Vaatleme disjunktide hulka

$$S = \{P(x,a,g(x,b)), \neg P(f(y), z, g(f(a),b))\}.$$

Tõestame, et S on vasturääkiv, konstrueerides fundamentaalnäidete hulki. Kuna

$$H_0 = \{a,b\},$$

siis

$S_0' = \{ P(a,a,g(a,b)),\ P(b,a,g(b,b)), \neg P(f(a),a,g(f(a),b)), \neg P(f(a),b,g(f(a),b)),\ \neg P(f(b),a,g(f(a),b)), \neg P(f(b),b,g(f(a),b))\}$.

Hulk S_0' ei ole vasturääkiv. Leiame Herbrandi universumi 1. taseme:

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

Siis

$$S_1' = S_0' \cup \{P(f(a),a,g(f(a),b)),\ldots\}.$$

Hulk S_1' on vasturääkiv, sest sisaldab kontraarse paari $P(f(a),a,g(f(a),b))$ ja $\neg P(f(a),a,g(f(a),b))$.

Herbrandi teoreemi kohaselt on ka hulk S vasturääkiv.

<u>Näide 3.13</u>. Lahendame nüüd järgmise ülesande. Mõned patsiendid armastavad kõiki doktoreid. Ükski patsient ei armasta posijaid. Tõestada, et ükski doktor pole posija.

Kõigepealt esitame eeldused ja väite predikaatarvutuse valemitena. Tähistame

$P(x)$ - x on patsient,

$D(x)$ - x on doktor,

$Q(x)$ - x on posija,

$L(x,y)$ - x armastab y-t.

Eeldused võib siis esitada järgmiste valemitena:

$$F_1 = (\exists x)(P(x) \ \& \ (\forall y)(D(y) \rightarrow L(x,y)));$$

$$F_2 = (\forall z)(P(z) \rightarrow (\forall t)(Q(t) \rightarrow \neg L(z,t))).$$

Väide esitub valemina

$$G = (\forall u)(D(u) \rightarrow \neg Q(u)).$$

TTÜ lahendamiseks tuleb tõestada, et valem $(F_1 \ \& \ F_2) \rightarrow G$ on samaselt tõene, s.t. tema eitus $F_1 \ \& \ F_2 \ \& \ \neg G$ on samaselt väär. Teisendame viimase valemi disjunktide hulgaks (konjunktsiooni iga liikme võib seejuures muidugi teisendada eraldi):

$$F_1 \overset{1}{=} (\exists x)(P(x) \ \& \ (\forall y)(\neg D(y) \vee L(x,y))) =$$

$$\overset{4}{=} P(a) \ \& \ (\forall y)(\neg D(y) \vee L(a,y)) =$$

$$\overset{5}{=} (\forall y)(P(a) \ \& \ (\neg D(y) \vee L(a,y))) =$$

$$\overset{7}{=} P(a) \ \& \ (\neg D(y) \vee L(a,y)),$$

$8\colon \{P(a),\ \rceil D(y) \vee L(a,y)\}$;

$$F_2 \overset{1}{=} (\forall z)(\rceil P(z) \vee (\forall t)(\rceil Q(t) \vee \rceil L(z,t))) \overset{6}{=}$$
$$\overset{6}{=} (\forall z)(\forall t)(\rceil P(z) \vee \rceil Q(t) \vee \rceil L(z,t)) \overset{7}{=}$$
$$\overset{7}{=} \rceil P(z) \vee \rceil Q(t) \vee \rceil L(z,t);$$

$$G \overset{1}{=} ((\forall u)(\rceil D(u) \vee \rceil Q(u))) \overset{2}{=}$$
$$\overset{2}{=} (\forall u)(D(u) \,\&\, Q(u)) \overset{3}{=}$$
$$\overset{3}{=} D(b) \,\&\, Q(b),$$
$$8\colon \{D(b),\ Q(b)\}.$$

Seega teiseneb valem F_1 & F_2 & $\rceil G$ disjunktide hulgaks $S = \{P(a), \rceil D(y) \vee L(a,y), \rceil P(z) \vee \rceil Q(t) \vee \rceil L(z,t), D(b), Q(b)\}$. Tõestame, et hulk S on vasturääkiv, kasutades Herbrandi teoreemi. Kuna

$$H_0 = H = \{a,b\},$$

siis

$S_0' = S_1' = \ldots = \{P(a),\ \rceil D(a) \vee L(a,a),\ \rceil D(b) \vee L(a,b),\ \rceil P(a) \vee \rceil Q(a) \vee \rceil L(a,a),$
$\rceil P(a) \vee \rceil Q(b) \vee \rceil L(a,b),$
$\rceil P(b) \vee \rceil Q(a) \vee \rceil L(b,a),$
$\rceil P(b) \vee \rceil Q(b) \vee \rceil L(b,b),$
$D(b),\ Q(b)\}.$

See fundamentaalnäidete hulk on vasturääkiv. Tõepoolest. Oletame vastuväiteliselt, et leidub interpretatsioon I, mis rahuldab hulka S_0'. Selles interpretatsioonis peavad elementaarvalemid P(a), D(b) ja Q(b) olema tõesed. Ka L(a,b) peab olema tõene, sest muidu ei saaks valem $\rceil D(b) \vee L(a,b)$ olla tõene. Sel juhul on valem $\rceil P(a) \vee \rceil L(a,b) \vee \rceil Q(b)$ väär, s.t. interpretatsioon I ei rahulda hulka S_0'. See aga on vastuolus eeldusega. Järelikult peab hulk S_0' olema vasturääkiv. Siis on Herbrandi teoreemi põhjal ka hulk S vasturääkiv.

Seega ülesande eeldustel tõepoolest ükski doktor pole posija.

4. Resolutsioonimeetod

4.1. Üldidee

Põhiliseks raskuseks Herbrandi teoreemil põhinevate tõestusprotseduuride kasutamisel on hulkade S_i' kiire kasvamine i kasvades.

Näiteks vaatleme disjunktide hulka

$S = \{P(x,g(x),y,h(x,y),z,k(x,y,z), \neg P(u,v,e(v),w,f(v,w),x)\}$.

Siin

$H_0 = \{a\}$,

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

....

Fundamentaalnäidete hulgas S_0' on 2 elementi, hulgas S_1' juba $6\cdot(6\cdot6 + 6\cdot6\cdot6) = 1512$ elementi. Esimene vasturääkiv fundamentaalnäidete hulk on aga alles S_5'. Kuna Herbrandi universumi 5. tasemes on ligikaudu 10^{64} elementi, siis hulgas S_5' on ligikaudu 10^{256} elementi.

4.2. Resolutsioonimeetod lausearvutuse jaoks

Olgu disjunktid C_1 ja C_2 sellised, et C_1 sisaldab literaali L_1, C_2 aga sellega kontraarse literaali L_2. Kriipsutame maha disjunktides C_1 ja C_2 vastavalt literaalid L_1 ja L_2 ning moodustame allesjäänud literaalide disjunktsiooni. Nii konstrueeritud disjunkti nimetatakse disjunktide C_1 ja C_2 resolvendiks. Näiteks disjunktide

$P \vee R$

ja

$\neg P \vee Q$

resolvendiks on disjunkt

$R \vee Q$;

disjunktide

$\neg P \vee Q \vee R$

8

ja

$\neg Q \vee S$

resolvendiks aga disjunkt

$\neg P \vee R \vee S.$

Disjunktide

P

ja

$\neg P$

resolvendiks on tühidisjunkt [].

Teoreem 4.1. Olgu antud disjunktid C_1 ja C_2. Siis disjunktide C_1 ja C_2 resolvent C järeldub loogiliselt disjunktidest C_1 ja C_2.

Tõestus. Olgu $C_1 = L \vee C_1'$, $C_2 = \neg L \vee C_2'$ ja $C = C_1' \vee C_2'$, kus C_1' ja C_2' on literaalide disjunktsioonid. Oletame, et C_1 ja C_2 on tõesed interpretatsioonis I. Vaja on tõestada, et resolvent $C_1' \vee C_2'$ on samuti tõene interpretatsioonis I. Selles interpretatsioonis on kas L või $\neg L$ väär. Oletame, et L on väär. Siis C_1 ei saa koosneda ühestainsast literaalist ja C_1' peab olema interpretatsioonis I tõene. Seega resolvent $C_1' \vee C_2'$ on tõene interpretatsioonis I. Analoogiliselt võib näidata, et kui $\neg L$ on väär interpretatsioonis I, siis C_2' peab selles interpretatsioonis olema tõene. Järelikult $C_1' \vee C_2'$ on tõene interpretatsioonis I.

Edaspidi tõestame, et kui disjunktide hulk S on vasturääkiv, siis resolventide leidmise teel võib sellest hulgast tuletada tühidisjunkti.

Def. Tuletusreeglit, mis genereerib disjunktide hulgast S selle resolvendid, nimetatakse *resolutsiooniks*.

Def. Disjunkti *tuletuseks* disjunktide hulgast S *resolutsioonimeetodil* nimetatakse sellist disjunktide järjendit $C_1, C_2, \ldots, C_n$, kus iga C_i kas kuulub hulka S või on eelnevate disjunktide resolvent, ning $C_n = C$.

Tühidisjunkti tuletust disjunktide hulgast S nimetatakse hulga S *kummutamiseks* ehk *vasturääkivuse tõestuseks*.

Näide 4.1. Olgu $S = \{\neg P \vee Q, \neg Q, P\}$. Disjunktidest $\neg P \vee Q$ ja $\neg Q$ saame resolvendi $\neg P$ ning disjunktidest P ja $\neg P$

resolvendi []. Seega eksisteerib tühidisjunkti tuletus

$\neg P \vee Q$, $\neg Q$, $\neg P$, P, []

disjunktide hulgast S resolutsioonimeetodil.

4.3. Asendus ja unifikatsioon

Asume nüüd laiendama resolutsioonimeetodit lausearvutuselt 1. järku predikaatarvutusele.

Resolventide leidmisel on tarvis, et kahes disjunktis leiduksid kontraarsed literaalid. Kui disjunktid ei sisalda muutujaid, s.t. nad on põhidisjunktid, siis on resolventi lihtne leida. Näiteks põhidisjunktide

$P(a) \vee Q(b)$

ja

$\neg P(a) \vee R(a)$

resolvendiks on disjunkt

$Q(b) \vee R(a)$.

Resolvendi võib defineerida ka muutujaid sisaldavate disjunktide jaoks. Näiteks olgu

$C_1 = P(x) \vee Q(x)$,

$C_2 = \neg P(f(x)) \vee R(x)$.

Disjunktis C_1 pole ühtki literaali, mis oleks kontraarne mõne disjunktis C_2 esineva literaaliga. Kui aga asendame disjunktis C_1 muutuja x termiga f(x), siis saame disjunkti

$C_1^* = P(f(x)) \vee Q(f(x))$.

Disjunktidel C_1^* ja C_2 leidub resolvent

$C_3 = Q(f(x)) \vee R(x)$.

Disjunkti C_3 nimetatakse ka antud disjunktide C_1 ja C_2 resolvendiks.

Kuna resolventide moodustamiseks on tihti vaja muutujaid asendada, alustame järgmiste mõistete defineerimisest.

Def. Asenduskomponendiks nimetatakse avaldist t/x, kus x on muutuja, t aga term, mis ei ole x. Seejuures x nimetatakse asenduskomponendi muutujaks, t aga termiks.

Def. Asenduskomponentide hulka

$\alpha = \{t_1/x_1, \ldots, t_n/x_n\}$,

kus muutujad on erinevad, nimetatakse asenduseks.

8*

Asenduse α rakendamine mingile valemile F tähendab muutujate x_i $(1 \leqslant i \leqslant n)$ kõikide esinemiste asendamist valemis F termiga t. Saadud valemit tähistatakse $F\alpha$ ning nimetatakse valemi F *näiteks*.

Nii saadakse asenduse

$$\alpha = \{g(a)/x,\ f(z)/y\}$$

rakendamisel valemile

$$F = R(x, f(y))$$

valem

$$F\alpha = R(g(a),\ f(f(z)))$$

(valemi F näide).

Def. Asenduste α ja β *kompositsiooniks* $\alpha\beta$ nimetatakse asendust, mis saadakse asenduse β rakendamisel asenduse α kõigile termidele ning tulemusele selliste asenduskomponentide lisamisel asendusest β, mille muutujad puuduvad asenduses α.

Näiteks kui

$$\alpha = \{f(x,y)/z\},$$

$$\beta = \{a/x,\ b/y,\ c/w,\ d/z\},$$

siis

$$\alpha\beta = \{f(a,b)/z,\ a/x,\ b/y,\ c/w\}.$$

Resolventide leidmisel on mõnikord vaja unifitseerida (ühtsustada) kaks või enam avaldist, s.t. tuleb leida selline asendus, mis teeks mitu avaldist identseteks.

Def. Literaalide hulka $W = \{L_1, L_2, \ldots, L_n\}$ nimetatakse *unifitseeritavaks*, kui leidub selline asendus α, mille rakendamise tulemusel saadakse $L_1\alpha = L_2\alpha = \ldots = L_n\alpha$. Asendust α nimetatakse literaalide hulga *unifikaatoriks*.

Näiteks olgu antud literaalide hulk

$$W = \{R(f(y),x),\ R(f(b),f(a))\}.$$

Asendus $\alpha = \{f(a)/x,\ b/y\}$ on hulga W unifikaator, sest

$$(R(f(y),x))\alpha = R(f(b),f(a)),$$

$$(R(f(b),f(a)))\alpha = R(f(b),f(a)).$$

Def. Literaalide hulga $W = \{L_1, L_2, \ldots, L_n\}$ *lihtsaimaks unifikaatoriks* nimetatakse sellist unifikaatorit α, et kui β on hulga W unifikaator, siis leidub asendus γ nii, et

$$L_i\alpha\gamma = L_i\beta \qquad (i = 1,2,\ldots,n).$$

4.4. Unifitseerimisalgoritm

Algoritmi, mis leiab unifitseeritava literaalide hulga lihtsaima unifikaatori ja teatab ebaõnnestumisest, kui hulk pole unifitseeritav, nimetatakse _unifitseerimisalgoritmiks_. Algoritm põhineb järgmisel ideel.

Vaatleme avaldisi P(a) ja P(x). Need ei ole identsed, vaid erinevad teineteisest selle poolest, et esimeses avaldises on a, teises aga samal kohal muutuja x. Et ühtsustada avaldisi P(a) ja P(x), tuleb kõigepealt leida nende erinevus, seejärel aga püüda seda kõrvaldada. Vaadeldavas näites on erinevuste hulk {a,x}. Kuna x on muutuja, siis selle võib asendada konstandiga a ning erinevus ongi kõrvaldatud.

Defineerime alfabeetilise ja leksikograafilise järjestuse.

Def. Ütleme, et sümbolite hulk on _järjestatud alfabeetiliselt_, kui

1) sümbolid paiknevad järjekorras: muutujate, funktsioonide, predikaatide sümbolid ja eituse märk;

2) väiksema dimensiooniga funktsiooni (predikaadi) sümbol eelneb suurema dimensiooniga funktsioonide (predikaatide) sümbolitele; võrdsete dimensioonide korral aga on eespool alfabeetilises järjestuses varem esineva funktsiooni (predikaadi) sümbol;

3) muutujate sümbolid paiknevad alfabeetilises järjekorras.

Def. Terme ja literaale nimetame avaldisteks. Kõikide avaldiste hulk on _järjestatud leksikograafiliselt_, kui lühemad avaldised eelnevad pikematele, võrdse pikkusega avaldistest aga on eespool see, mille esimene sümbol (esimesed sümbolid) on alfabeetilises järjestuses eespool.

Avaldiste hulga W unifitseerimisalgoritm:

1. $k := 0$, $\sigma_k := \varepsilon$ (tühiasendus).
2. Kui $W\sigma_k$ ei ole üheelemendiline hulk, siis täita punkt 3. Vastasel korral $\sigma := \sigma_k$, töö lõpetada.
3. Hulgas $W\sigma_k$ vaadelda iga avaldist kui sümbolite korteeži

ja eraldada esimesed (vasakpoolseimad) osaavaldised, mis hulga $W\sigma_k$ kõigil elementidel ei ole identsed. Need osaavaldised järjestada leksikograafiliselt. Saadakse hulga $W\sigma_k$ nn. erinevuste hulk B_k. Tähistada hulga B_k 1. ja 2. elementi vastavalt v_k ja t_k. Kui v_k on muutuja, mis ei sisaldu avaldises t_k, siis

$$\sigma_{k+1} := \sigma_k\{t_k/v_k\},$$

$$k := k + 1,$$

täita punkt 2.

Vastasel korral teatada ebaõnnestumisest, töö lõpetada.

Märgime, et unifitseerimisalgoritm lõpetab töö igal lõplikul mittetühjal avaldiste hulgal W, sest vastupidisel juhul genereeriks ta lõplike mittetühjade hulkade lõpmatu jada $W\sigma_0$, $W\sigma_1$,..., kus iga järgmine hulk sisaldab ühe muutuja vähem kui eelmine. See on aga võimatu, sest W sisaldab ainult lõpliku hulga erinevaid muutujaid.

N<u>äide 4.2</u>. Rakendame unifitseerimisalgoritmi literaalide hulgale

$$W = \{P(x,z,v),\ P(x,f(y),y),\ P(x,z,b)\}.$$

Saame

$$k = 0,\ \sigma_0 = \varepsilon,\ W\sigma_0 = W.$$

Erinevuste hulk

$$B_0 = \{z,f(y)\}.$$

Siin

$$v_0 = z,\ t_0 = f(y).$$

Nüüd

$$\sigma_1 = \sigma_0\{f(y)/z\} = \{f(y)/z\},$$

$$k = 1.$$

Hulk

$$W\sigma_1 = \{P(x,f(y),v),\ P(x,f(y),y),\ P(x,f(y),b)\}$$

ei ole üheelemendiline, tema erinevuste hulk on

$$B_1 = \{v,y,b\}.$$

Siin

$$v_1 = v,\ t_1 = y$$

ning

$$\sigma_2 = \sigma_1\{y/v\} = \{f(y)/z\}\{y/v\} = \{f(y)/z,\ y/v\},$$

$$k = 2.$$

Hulk

$W\sigma_2 = \{P(x,f(y),y),\ P(x,f(y),b)\}$

ei ole üheelemendiline, erinevuste hulk on

$B_2 = \{y,\ b\}$,

kus

$v_2 = y,\ t_2 = b$.

Saame

$\sigma_3 = \sigma_2\{b/y\} = \{f(y)/z,\ y/v\}\{b/y\} = \{f(b)/z,\ b/v,\ b/y\}$,

$k = 3$.

Nüüd

$W\sigma_3 = \{P(x,f(b),b)\}$,

seega

$\sigma = \sigma_3 = \{f(b)/z,\ b/v,\ b/y\}$

on hulga W lihtsaim unifikaator.

Näide 4.3. Rakendame unifitseerimisalgoritmi literaalide hulgale

$W = \{Q(f(a),g(x)),\ Q(y,y)\}$.

Saame

$k = 0,\ \sigma_0 = \varepsilon,\ B_0 = \{y,\ f(a)\}$,

seega $\sigma_1 = \{f(a)/y\}$. Nüüd

$k = 1,\ W\sigma_1 = \{Q(f(a),g(x)),\ Q(f(a),f(a))\},\ B_1 = \{f(a),\ g(x)\}$.

Kuna f(a) ei ole muutuja, siis hulk W ei ole unifitseeritav.

Teoreem 4.2. Kui W on lõplik mittetühi unifitseeritav avaldiste hulk, siis unifitseerimisalgoritm lõpetab alati töö 2. sammul ning viimane σ_k on hulga W lihtsaim unifikaator.

Tõestus. Kuna W on unifitseeritav, siis olgu θ tema suvaline unifikaator. Induktsiooniga k järgi näitame, et leidub selline asendus λ_k, mille korral $\theta = \sigma_k\lambda_k$.

Olgu $k = 0$. Tähistame $\lambda_0 = \theta$. Siis $\theta = \sigma_0\lambda_0$, sest $\sigma_0 = \varepsilon$.

Oletame nüüd, et $\theta = \sigma_k\lambda_k$ $(0 \leq k \leq n)$. Kui hulk $W\sigma_k$ koosneb ühestainsast literaalist, siis peatub unifitseerimisalgoritm sammul 2. Kuna $\theta = \sigma_n\lambda_n$, siis σ_n on hulga W lihtsaim unifikaator.

Kui hulk $W\sigma_n$ koosneb enam kui ühest avaldisest, siis leiab unifitseerimisalgoritm hulga $W\sigma_n$ jaoks erinevuste hulga B_n. Kuna $\theta = \sigma_n\lambda_n$ on hulga W unifikaator, siis λ_n peab olema hulga B_n unifikaator. Kuna aga B_n on erinevuste hulk, siis peab selles hulgas leiduma muutuja v_n. Olgu t_n suvaline element hulgast B_n, kus $t_n \neq v_n$. Kuna λ_n unifitseerib B_n, siis $v_n\lambda_n = t_n\lambda_n$. Kui $v_n \in t_n$, siis $v_n\lambda_n \in t_n\lambda_n$. See aga pole võimalik, sest v_n ja t_n on erinevad ning $v_n\lambda_n = t_n\lambda_n$. Järelikult $v_n \notin t_n$. Seetõttu ei peatu algoritm sammul 3, vaid moodustab $\sigma_{n+1} = \sigma_n\{t_n/v_n\}$. Olgu $\lambda_{n+1} = \lambda_n - \{t_n\lambda_n/v_n\}$. Kuna $v_n \notin t_n$, siis

$$t_n\lambda_{n+1} = t_n(\lambda_n - \{t_n\lambda_n/v_n\}) = t_n\lambda_n.$$

Seega

$$\{t_n/v_n\}\lambda_{n+1} = \{t_n\lambda_{n+1}/v_n\} \cup \lambda_{n+1} = \{t_n\lambda_n/v_n\} \cup \lambda_{n+1} =$$
$$= \{t_n\lambda_n/v_n\} \cup (\lambda_n - \{t_n\lambda_n/v_n\}) = \lambda_n.$$

Järelikult

$$\theta = \sigma_n\lambda_n = \sigma_n\{t_n/v_n\}\lambda_{n+1} = \sigma_{n+1}\lambda_{n+1}.$$

Seepärast leidub iga $k \geqslant 0$ korral selline asendus λ_k, et $\theta = \sigma_k\lambda_k$. Kuna unifitseerimisalgoritm peab töö lõpetama ja kuna ta seda ei teinud sammul 3, siis peab töö lõppema sammul 2. Kuna $\theta = \sigma_k\lambda_k$ iga k korral, siis viimane σ_k on hulga W lihtsaim unifikaator.

4.5. Resolutsioonimeetod predikaatarvutuse jaoks

Def. Kui disjunkti C kaks või enam (samamärgilist) literaali on unifitseeritavad lihtsaima unifikaatoriga σ, siis disjunkti $C\sigma$ nimetatakse disjunkti C *kleebiseks*.

Näiteks disjunkti $C = P(x) \vee P(f(y)) \vee \neg Q(x)$ kleebis $P(f(y)) \vee \neg Q(f(y))$ saadakse hulga $\{P(x), P(f(y))\}$ lihtsaima unifikaatori $\sigma = \{f(y)/x\}$ rakendamise tulemusel disjunktile C.

Def. Olgu C_1 ja C_2 kaks disjunkti (vaatleme neid literaalide hulkadena), millel ei ole ühiseid muutujaid. Olgu L_1 ja L_2 sellised literaalid, et

1) $L_1 \subseteq C_1$,
   $L_2 \subseteq C_2$,

2) hulga $L_1 \cup \neg L_2$ jaoks eksisteerib lihtsaim unifikaator σ.

Siis öeldakse, et disjunktid C_1 ja C_2 *lahenevad* ning neist on tuletatav uus disjunkt, nende nn. *binaarne resolvent*

$(C_1 - L_1)\sigma \vee (C_2 - L_2)\sigma$.

Näide 4.4. Olgu

C_1: $R(y,g(a)) \vee R(y,g(x)) \vee P(x)$,

C_2: $\neg R(z,g(a)) \vee \neg P(z)$.

Tähistame $L_1 = R(y,g(a))$, $L_2 = \neg R(z,g(a))$. Hulk $\{L_1, \neg L_2\}$ on unifitseeritav lihtsaima unifikaatoriga

$\sigma = \{z/y\}$.

Disjunktide C_1 ja C_2 binaarseks resolvendiks on disjunkt

$(R(y,g(x)) \vee P(x) \vee \neg P(z))\sigma = R(z,g(x)) \vee P(x) \vee \neg P(z)$.

Binaarsed resolvendid on veel

$R(y,g(a)) \vee P(a) \vee \neg P(z)$

ja

$R(y,g(a)) \vee P(y,g(z)) \vee \neg R(z,g(a))$.

On disjunkte, mis ei lahene.

Def. Disjunktide C_1 ja C_2 resolvendiks nimetatakse binaarset resolventi, kus lahenevateks disjunktideks on kas

1) C_1 ja C_2,

2) C_1 kleebis ja C_2,

3) C_1 ja C_2 kleebis või

4) C_1 ja C_2 kleebised.

Näide 4.5. Näites 4.4 vaadeldud disjunktide C_1 ja C_2 resolvendiks on ka disjunkt

$R(z,g(a)) \vee P(a) \vee \neg P(z)$

- see on C_1 kleebise $R(z,g(a)) \vee P(a)$ ja disjunkti C_2 binaarne resolvent.

Nagu lausearvutuses, nii ka predikaatarvutuse korral nimetatakse tuletusreeglit, mis genereerib antud disjunktide hulgast selle resolvendid, resolutsiooniks.

Samuti nagu lausearvutuses defineeritakse ka disjunkti C tuletus disjunktide hulgast S resolutsioonimeetodil ning disjunktide hulga S kummutamine.

Olgu antud n disjunktist koosnev hulk S. Hulga S kõik resolvendid võib leida järgmise algoritmi kohaselt.

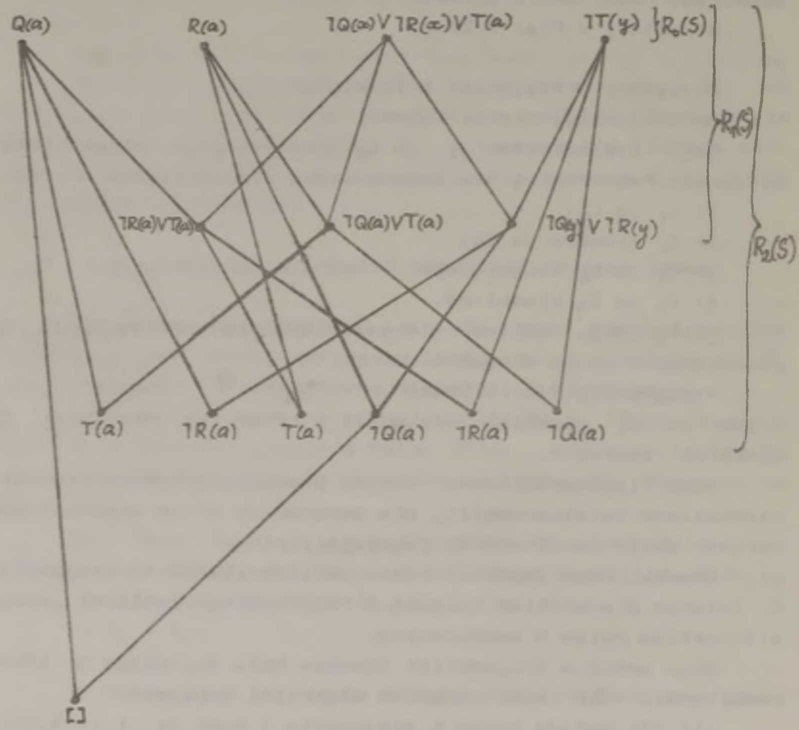
(i) Järjestada hulga S disjunktid 1 kuni n; i := 1.

(ii) Leida disjunkti number i kõikvõimalikud resolvendid disjunktidega number i+1,..., n.

(iii) i := i + 1. Kui i < n, siis täita (ii).

Tähistame $R(S)$ hulga S ühendit tema kõikvõimalike resolventide hulgaga. Olgu $R_0(S) = S$ ja $R_{i+1}(S) = R(R_i(S))$, $i \geqslant 0$.

<u>Näide 4.6.</u> Olgu $S = \{Q(a), R(a), \neg Q(x) \vee \neg R(x) \vee T(a), \neg T(y)\}$. Tuletame resolutsioonimeetodil hulgast S tühidisjunkti. Resolventide leidmisel rakendame äsja toodud algoritmi. Tuletuse esitame graafina, mille tippudele vastavad hulga S disjunktid ja resolvendid:



4.6. Resolutsioonimeetodi täielikkus

Näitame nüüd, et parajasti igast vasturääkivast disjunktide hulgast S saab resolutsioonimeetodil tuletada tühidisjunkti.

Lemma 4.4. Kui C_1' ja C_2' on disjunktide C_1 ja C_2 näited ning kui C' on C_1' ja C_2' resolvent, siis eksisteerib C_1 ja C_2 selline resolvent C, et C' on C näide.

Tõestus. Eeldame, et disjunktidel C_1 ja C_2 ei ole ühiseid muutujaid (seda võime saavutada vajaduse korral muutujaid ümber nimetades). Olgu L_1' ja L_2' resolveeritavad literaalid ning olgu

$$C' = (C_1'\nu - L_1'\nu) \cup (C_2'\nu - L_2'\nu),$$

kus ν on literaalide L_1' ja $\neg L_2'$ lihtsaim unifikaator. Kuna C_1' ja C_2' on vastavalt disjunktide C_1 ja C_2 näited, siis leidub selline asendus θ, et $C_1' = C_1\theta$ ja $C_2' = C_2\theta$. Olgu $L_i^1, \dots, L_i^{r_i}$ sellised literaalid disjunktis C_i, et

$$L_i^1\theta = \dots = L_i^{r_i}\theta = L_i'$$

$(i = 1, 2)$. Kui $r_i > 1$, siis olgu λ_i hulga $\{L_i^1, \dots, L_i^{r_i}\}$ lihtsaim unifikaator ja $L_i = L_i^1\lambda_i$ $(i = 1, 2)$. Siis on L_i literaal disjunkti C_i kleebises $C_i\lambda_i$. Kui $r_i = 1$, siis $\lambda_i = \varepsilon$ ja $L_i = L_i^1\lambda_i$. Olgu $\lambda = \lambda_1\lambda_2$. L_i' on L_i näide. Kuna L_1' ja $\neg L_2'$ on unifitseeritavad, siis on ka L_1 ja $\neg L_2$ unifitseeritavad. Olgu σ literaalide L_1 ja $\neg L_2$ lihtsaim unifikaator. Olgu

$$\begin{aligned} C &= ((C_1\lambda)\sigma - L_1\sigma) \cup ((C_2\lambda)\sigma - L_2\sigma) = \\ &= ((C_1\lambda)\sigma - \{L_1^1, \dots, L_1^{r_1}\}(\lambda\sigma)) \cup \\ &\cup (C_2(\lambda\sigma) - \{L_2^1, \dots, L_2^{r_2}\}(\lambda\sigma)). \end{aligned}$$

Disjunkt C on disjunktide C_1 ja C_2 resolvent. C' on C näide, sest

$$\begin{aligned} C' &= (C_1'\nu - L_1'\nu) \cup (C_2'\nu - L_2'\nu) = \\ &= ((C_1\theta)\nu - (\{L_1^1, \dots, L_1^{r_1}\}\theta)\nu) \cup \\ &\cup ((C_2\theta)\nu - (\{L_2^1, \dots, L_2^{r_2}\}\theta)\nu) = \\ &= (C_1(\theta\nu) - \{L_1^1, \dots, L_1^{r_1}\}(\theta\nu)) \cup \\ &\cup (C_2(\theta\nu) - \{L_2^1, \dots, L_2^{r_2}\}(\theta\nu)), \end{aligned}$$

ja $\lambda\sigma$ on lihtsam kui $\theta\nu$, mis tõestabki lemma.

Teoreem 4.3 (resolutsioonimeetodi täielikkus). Disjunktide hulk S on vasturääkiv parajasti siis, kui resolutsioonimeetodil saab temast tuletada tühidisjunkti.

Tõestus. (=>) Tähistame

k(S) = (literaalide sisaldumiste arv hulga S disjunktides) − − (disjunktide arv hulgas S).

Tõestame induktsiooniga k(S) järgi.

Olgu k(S) = 0. Siis kas iga disjunkt sisaldab üheainsa literaali, või leidub disjunkt, milles on kaks literaali, kuid samas peab leiduma ka disjunkt, milles pole ühtegi literaali − tühidisjunkt. Viimasel juhul väide kehtib, seepärast vaatleme esimest juhtu. Olgu niisiis

$$S = \{L_1, L_2, L_3, \ldots\},$$

kus iga disjunkt kujutab endast ühtainsat literaali. Iga disjunkt on seega tõene parajasti siis, kui tema ainus literaal on tõene. Kuna eelduse kohaselt on S vasturääkiv, siis ei tohi teda rahuldada ükski interpretatsioon, s.t. hulgas S peab olema vähemalt üks paar literaale, mis kas ise või mille näited on kontraarsed. Olgu sellised literaalid näiteks L_1 ja L_2. Siis $L_2' = \neg L_1'$, kus L_1' ja L_2' on vastavalt literaalide L_1 ja L_2 näited. Nende resolvendiks on []. Lemmast 4.1 järeldub, et siis ka L_1 ja L_2 resolvendiks on []. Induktsiooni baas on tõestatud.

Oletame nüüd, et väide kehtib iga k(S) < n korral. Olgu k(S) = n ning olgu S vasturääkiv disjunktide hulk. Kui S sisaldab [], siis on teoreem tõestatud. Seepärast vaatleme juhtu, kus [] $\notin$ S. Kuna k(S) > 0, siis vähemalt üks disjunkt hulgas S sisaldab rohkem kui ühe literaali. Olgu selliseks disjunktiks C = A V L, kus L on literaal. Hulga S võib esitada kujul

$$S = S' \cup C,$$

kus S' = S − C. Hulgast S võib saada kaks hulka:

$$S_1 = S' \cup A,$$

$$S_2 = S' \cup L,$$

kusjuures $k(S_2) \leq k(S_1) < k(S) = n$. Induktiivse eelduse kohaselt võib hulkadest S_1 ja S_2, kui nad on vasturääkivad, tuletada tühidisjunkti. Tõestame, et S_1 ja S_2 on vasturääkivad.

Olgu M disjunkti C kõikide mudelite kogum. Kuna eelduse kohaselt on hulk S = S' U C vasturääkiv, siis ei saa teda rahuldada ka ükski interpretatsioon kogumist M . Seepärast peab igas interpretatsioonis $m \in M$ mingi valem $C^* \in S$ olema väär. Kõik väärtustused, mille korral A ja L on tõesed, kuuluvad kogumisse M ja igaühes neist on seega mingi valem $C^* \in S$ väär. Teiselt poolt, disjunkti C suvalises interpretatsioonis, mis ei kuulu kogumisse M , peavad mõlemad valemid A ja L olema väärad, sest muidu poleks $C = A \vee L$ väär. Seega ühegi interpretatsiooni korral pole hulgad S_1 ja S_2 rahuldatavad, s.t. nad on vasturääkivad.

Tähistame $R^k(S)$ disjunktide hulga, mis on saadud hulgast S k korda resolvente leides. Oleme tõestanud, et leiduvad sellised i ja j, et

$$[] \in R^i(S_1), \tag{4.1}$$

$$[] \in R^j(S_2). \tag{4.2}$$

Oletame nüüd, et i sammu, mis viivad suhteni (4.1), on rakendatud mitte hulgale S_1, vaid hulgale $S = S' \cup C$. Selle tulemusel saame kas $[]$ või L. Esimesel juhul on hulgast S tühidisjunkt resolutsioonimeetodil tuletatud. Vaatleme teist juhtu, kui saadakse L. Kuna $S' \subseteq S$, siis

$$S' \cup L = S_2 \subseteq R^i(S).$$

Nüüd võib $[]$ tuletamiseks rakendada hulgale S_2 kui hulga $R^i(S)$ osahulgale j korda resolventide leidmist ja saada suhte (4.2). See tõestabki tarvilikkuse.

($\Leftarrow$) Oletame, et eksisteerib $[]$ tuletus hulgast S. Olgu $R_1, R_2, \ldots, R_k$ resolvendid selles tuletuses. Oletame vastuväiteliselt, et leidub hulga S mingi mudel m. Kui m rahuldab hulga S disjunkte C_1 ja C_2, siis peab ta rahuldama ka nende suvalist resolventi (teoreemi 4.1 analoog predikaatarvutuse jaoks). Järelikult m rahuldab kõiki resolvente $R_1, \ldots, R_k$. See on aga võimatu, sest eelduse kohaselt on üks neist resolventidest $[]$. Seepärast peab hulk S olema vasturääkiv.

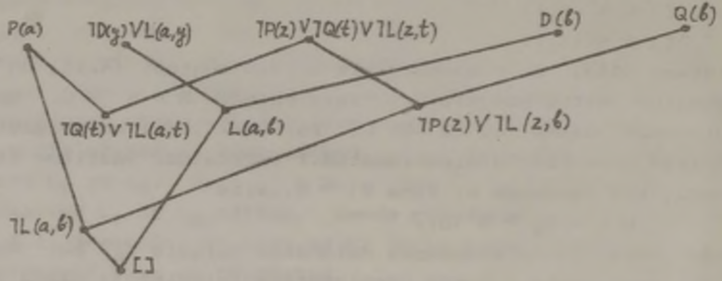
Resolutsioonimeetodi täielikkus tagab selle, et kui disjunktide hulk S on vasturääkiv, siis saab temast lõplik arv korda resolvente leides tuletada tühidisjunkti. Kui lõpliku arvu sammude järel pole osutunud võimalikuks tuletada tühidisjunkti, siis see ei tähenda veel, et S on rahuldatav: võib-olla õnnestuks tühidisjunkt tuletada suurema hulga sammude tulemusel.

4.7. Ülesannete lahendamine resolutsioonimeetodil

Vaatleme mõningaid näiteid resolutsioonimeetodi rakendamise kohta.

<u>Näide 4.7</u>. Lahendame resolutsioonimeetodil näites 3.13 lahendatud TTÜ, s.t. tõestame, et disjunktide hulk S ={P(a), ˥D(y) V L(a,y), ˥P(z) V ˥Q(t) V ˥L(z,t), D(b), Q(b)} on vasturääkiv.

Tõestuse (tühidisjunkti tuletuse) esitame graafina:



<u>Näide 4.8</u>. Iga tudeng on aus. Benno ei ole aus. Tõestada, et Benno ei ole tudeng.

Tähistame

T(x) - x on tudeng,

Q(x) - x on aus,

b - Benno.

Siis eeldused on

F_1 : (∀x)(T(x) → Q(x))

F_2 : ˥Q(b)

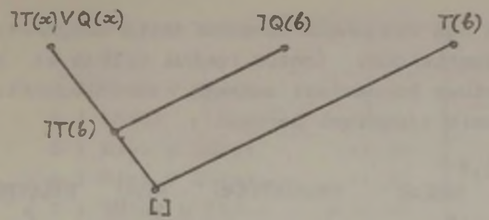
ja väide

G: ˥T(b).

Tuleb tõestada, et valem (F_1 & F_2) → G on samaselt tõene ehk, mis sellega samaväärne, et eitus F_1 & F_2 & ˥G on samaselt väär. Esitame selle valemi disjunktide hulgana:

S = {˥T(x) V Q(x), ˥Q(b), T(b)}.

Tuletame hulgast S resolutsioonimeetodil tühidisjunkti:



Järelikult tõepoolest Benno pole tudeng.

Näide 4.9. Modelleerime lihtsat küsimus-vastussüsteemi (KVS). Olgu KVS-s järgmised faktid:

F_1 : Benno on alati seal, kus on Clara.

F_2 : Clara on amfiteatris.

Kuidas KVS vastab küsimusele, kus on Benno?

Esitame faktid predikaatarvutuse valemitena. Tähistame

$P(x,y)$ - x paikneb kohal y,

a - amfiteater,

b - Benno,

c - Clara.

Siis

F_1 : $(\forall x)(P(c,x) \rightarrow P(b,x))$,

F_2: $P(c,a)$.

Selleks et vastata esitatud küsimusele, kasutab KVS järgmist võtet:[1] tõestab kõigepealt, et leidub koht, kus paikneb Benno, s.t. et valemitest F_1 ja F_2 järeldub loogiliselt valem

G: $(\exists y)(P(b,y))$.

Seejärel leiab KVS y väärtuse, mis ongi vastuseks küsimusele.

Näitame, et valem F_1 & F_2 & $\neg G$ on samaselt väär, s.o. disjunktide hulk

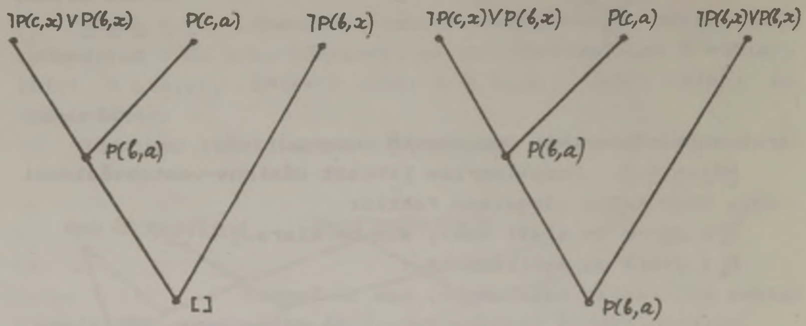
$S = \{ \neg P(c,x) \vee P(b,x), P(c,a), \neg P(b,y) \}$

on vasturääkiv. Tõestus on esitatud graafina (joonisel vasakul).

----

[1] Vt. näit. Л. Т. Кузин. Основы кибернетики. Т. 2. Основы кибернетических моделей. М., Энергия, 1979, lk. 494.

Nüüd võtame valemis ¬G iga disjunkti asemele selle disjunkti ja tema eituse disjunktsiooni (antud juhul ¬P(b,x) V V P(b,x)). Sama tõestuse kordamisel saamegi tühidisjunkti asemel vastuse küsimusele (joonisel paremal):



Vastus on P(b,a), seega Benno paikneb amfiteatris.

5. Semantiline resolutsioon

5.1. Näide

Resolutsioonimeetodi rakendamist teoreemide automaatsel tõestamisel piirab asjaolu, et resolventide hulgad kasvavad väga kiiresti. Lahendame veel ühe ülesande resolutsioonimeetodil, esitades lahenduse nüüd mitte graafina, vaid tabelina, ning seejärel hakkame otsima võtteid tõestuse lihtsustamiseks.

Näide 5.1. Tõestada, et disjunktide hulk
S = {R(x) V ¬Q(x) V ¬T(x), R(y) V T(y), R(z) V Q(z), ¬R(u)}
on vasturääkiv.

Kõiki hulga S disjunkte ja moodustatud resolvente järjest paarikaupa läbi vaadates saame tühidisjunkti genereerida 24. sammul:

```
         1 I R(x) V ¬Q(x) V ¬T(x)
         2 I R(y) V T(y)             S
         3 I R(z) V Q(z)
         4 I ¬R(u)
         5 I R(y) V ¬Q(y)        (1,2)
         6 I R(z) V ¬T(z)        (1,3)   R1(S)
         7 I ¬Q(u) V ¬T(u)       (1,4)          R2(S)
         8 I T(u)                (2,4)
         9 I Q(u)                (3,4)
 5 =    10 I R(u) V ¬Q(u)        (1,8)
 6 =    11 I R(u) V ¬T(u)        (1,9)
        12 I R(z)                (2,6)
 5 =    13 I R(u) V ¬Q(u)        (2,7)
12 =    14 I R(z)                (3,5)
 6 =    15 I R(u) V ¬T(u)        (3,7)
        16 I ¬Q(u)               (4,5)
        17 I ¬T(u)               (4,6)
12 =    18 I R(u)                (5,9)
12 =    19 I R(u)                (6,8)
        20 I ¬Q(u)               (7,8)
        21 I ¬T(u)               (7,9)
12 =    22 I R(u)                (2,17)
12 =    23 I R(u)                (3,16)
        24 I []                  (4,12)
```

Suur osa moodustatud resolventidest on tõestuse jaoks ülearused: hulga $R_1(S)$ resolventidest oleks vaja genereerida ainult kas nr. 5 või 6 ning hulga $R_2(S)$ resolventidest 12 ja 24.

Et vältida ülearuste resolventide moodustamist, seame resolutsioonile kitsendusi.

Esimene võte, mida kasutatakse resolventide hulga vähendamiseks, on disjunktide hulga S tükeldamine kaheks osahulgaks ja nõue, et resolventide moodustamisel võetaks disjunktid erinevatest osahulkadest. Hulga S tükeldamiseks kasutatakse interpretatsiooni: ühte osahulka (S_-) võetakse need disjunktid, mis valitud interpretatsioonis on väärad, ning teise (S_+) need, mis on tõesed.

Vaadeldavas näites kasutame sellist H-interpretatsiooni, milles kõik elementaarvalemid on väärad:

$I = \{ \neg R, \neg Q, \neg T\}.$

Saame järgmised osahulgad:

$S_- = \{2,3\}, \quad S_+ = \{1,4\}.$

Hulga $R_1(S)$ moodustamisel võimaldab selline täkeldus vältida ühe resolvendi (nr. 7) genereerimist.

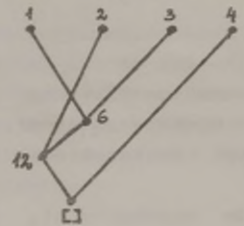
Teine võte, mida rakendatakse genereeritavate resolventide hulga vähendamiseks, on järjestuse sissetoomine predikaatsümbolite hulgas ja nõue, et resolveerida võib ainult sellise predikaadi esimesse osahulka kuuluvas disjunktis, mis temas sisalduvatest predikaatidest on suurim sissetoodud järjestuse mõttes.

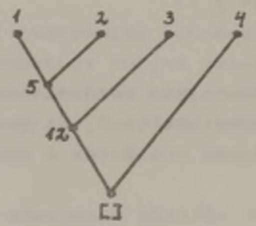
Vaadeldavas näites võtame kasutusele järgmise predikaatsümbolite järjestuse:

$P = (R < Q < T).$

Vaatame läbi resolvendid hulgast $R_1(S)$: täiendavalt võib nüüd vältida veel kahe resolvendi (nr. 8 ja 9) genereerimist.

Seega saame nimetatud kahte võtet kasutades vaadeldavas näites tühidisjunkti kaks tuletust:





Resolvendi nr. 12 moodustamisel kasutatakse mõlemal juhul kolme lähtedisjunkti (nr. 1, 2 ja 3).

Seame nüüd eesmärgiks laiendada resolvendi mõistet nii, et vaadeldavas näites saaks disjunktidest 1, 2 ja 3 kohe tuletada disjunkti 12, moodustamata vahepealseid resolvente 5 või 6.

5.2. Semantilise resolutsiooni definitsioon

Defineerime kõigepealt mõiste "semantiline klass".

Def. Olgu I interpretatsioon ja P predikaatsümbolite järjestus. Lõplikku disjunktide järjendit

$\{E_1, \ldots, E_q, N\}$,

kus $q \geqslant 1$, nimetatakse *semantiliseks klassiks* P ja I suhtes ehk *PI-klassiks*, disjunkte $E_1, \ldots, E_q$ semantilise klassi *elektronideks* ja N tema *tuumaks*, kui kehtivad järgmised 4 tingimust:

1. elektronid $E_1, \ldots, E_q$ on väärad interpretatsioonis I.
2. Olgu $R_1 = N$. Iga $i = 1, \ldots, q$ korral leidub resolvent R_{i+1}, mille moodustavad disjunktid E_i ja R_i.
3. Resolveeritav literaal on disjunktis E_i suurim predikaatsümbolite järjestuse P mõttes.
4. Resolvent R_{q+1} on väär interpretatsioonis I.

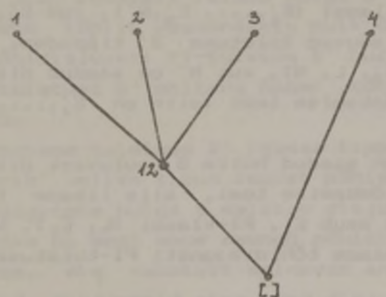
Resolventi R_{q+1} nimetatakse PI-klassi $\{E_1, \ldots, E_q, N\}$ *PI-resolvendiks*.

Vaadeldavas näites moodustavad PI-klassi disjunktid {2,3,1}. (Elektronid võib võtta ka vastupidises järjekorras: {3,2,1}).

Def. Tuletusreeglit, mis genereerib disjunktide hulgast PI-resolvendid, nimetatakse *semantiliseks resolutsiooniks*.

Tuletust disjunktide hulgast S nimetatakse *PI-tuletuseks*, kui iga disjunkt selles kas kuulub hulka S või on eelnevate disjunktide mingi PI-klassi PI-resolvent.

Vaadeldavas näites saame PI-tuletuse esitada puuna:



5.3. Semantilise resolutsiooni täielikkus

Semantilise resolutsiooni täielikkuse näitamiseks tõestame kõigepealt lemma.

<u>Lemma 5.1</u>. Kui P on predikaatsümbolite järjestus põhidisjunktide lõplikus vasturääkivas hulgas S ning I hulga S interpretatsioon, siis on olemas tühidisjunkti PI-tuletus hulgast S.

<u>Tõestus</u>. Tõestame induktsioonimeetodil. Hulga S disjunktid ei sisalda muutujaid, kuna nad on põhidisjunktid.

Olgu A hulga S elementaarvalemite hulk. Kui A koosneb ühestainsast valemist Q, siis peavad hulka S kuuluma nii Q kui ka ꓶQ. Nende resolvent on []. Üks disjunktidest Q ja ꓶQ peab olema väär interpretatsioonis I ja [] on väär igas interpretatsioonis. Seetõttu on tühidisjunkt PI-resolvent.

Oletame nüüd, et lemma kehtib juhul, kui hulk A koosneb i elemendist ($1 \leqslant i \leqslant n$). Vaatleme juhtu, kus hulk A koosneb n+1 elemendist. Võimalikud on kaks alljuhtu.

1) Hulka S kuulub literaal L, mis on väär interpretatsioonis I. Olgu S′ hulk, mis on saadud hulgast S nende disjunktide väljajätmise teel, mis sisaldavad literaali L, ning literaali ꓶL mahakriipsutamise teel ülejäänud disjunktidest. Hulk S′ on vasturääkiv. Kuna S′ sisaldab ülimalt n elementaarvalemit, siis induktsiooni eelduse tõttu eksisteerib tühidisjunkti PI-tuletus D′ hulgast S′ (olgu see esitatud graafina). Sellest tuletusest lähtudes võime saada tühidisjunkti PI-tuletuse hulgast S järgmisel viisil.

Esiteks, iga PI-klassi $\{E_1', \dots, E_q', N'\}$, kus $E_1', \dots, E_q'$, N' on disjunktid, mis asuvad tuletuse D′ tippudes, asendame PI-klassiga $\{E_1', \dots, E_q', L, N\}$, kui N' on saadud disjunktist N literaali L mahatõmbamise teel (siin on $E_1', \dots, E_q'$, L elektronid ja N tuum).

Teiseks, kui E_i' on saadud hulka S kuuluvast disjunktist E_i literaali ꓶL mahatõmbamise teel, siis lisame tuletuses selle tipu kohale, kus asub E_i', PI-klassi $\{L, E_i\}$. Niisuguse protsessi tulemusel saame tühidisjunkti PI-tuletuse hulgast S.

2) Hulka S ei kuulu literaali, mis oleks väär

interpretatsioonis I. Sel juhul valime elemendi B hulga S elementaarvalemite hulgast nii, et B sisaldaks järjestuse P mõttes vähima predikaatsümboli. Üks literaalidest B ja $\neg B$ on väär interpretatsioonis I. Olgu L hulga $\{B, \neg B\}$ see element, mis interpretatsioonis I on väär. Olgu S' hulk, mis on saadud hulgast S nende disjunktide väljajätmise teel, mis sisaldavad literaali $\neg L$, ja literaali L mahatõmbamise teel ülejäänud disjunktidest. Hulk S' on vasturääkiv. Kuna S' sisaldab ülimalt n elementaarvalemit, siis induktsiooni eelduse kohaselt eksisteerib tühidisjunkti PI-tuletus D' hulgast S'. Olgu D_1 tuletus, mis on saadud tuletusest D' literaali L tagasipaigutamise teel nendesse disjunktidesse, millest ta oli maha kriipsutatud. D_1 on samuti PI-tuletus, sest literaal L sisaldab vähima predikaatsümboli ja on interpretatsioonis I väär. D_1 on kas tühidisjunkti või L PI-tuletus. Esimesel juhul ongi tõestus sellega lõppenud. Teisel juhul vaatleme hulka S U {L}. Kuna see hulk sisaldab literaali L, mis on väär interpretatsioonis I, siis alljuhu 1 tõestuse kohaselt leidub tühidisjunkti PI-tuletus D_2 hulgast S U {L}. Kombineerides tuletusi D_1 ja D_2, saame tühidisjunkti PI-tuletuse hulgast S. Sellega on lemma tõestatud.

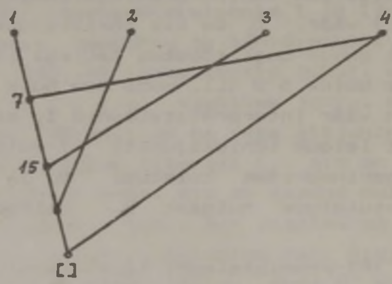
<u>Teoreem 5.1</u> (PI-resolutsiooni täielikkus). Kui P on predikaatsümbolite järjestus lõplikus vasturääkivas disjunktide hulgas S ning I on hulga S interpretatsioon, siis leidub tühidisjunkti PI-tuletus hulgast S.

<u>Tõestus</u>. Kuna S on vasturääkiv, siis Herbrandi teoreemi (teoreem 3.2) kohaselt leidub hulga S disjunktide fundamentaalnäidete lõplik vasturääkiv hulk S'. Lemma 5.1 kohaselt leidub tühidisjunkti PI-tuletus D' hulgast S'. Näitame nüüd, kuidas tuletust D' ehitada ümber tühidisjunkti tuletuseks hulgast S.

Paigutame tuletuse D' igasse tippu mingi disjunkti, mis "majoreerib" selles tipus asuvat põhidisjunkti. Igasse algtippu paigutame hulga S sellise disjunkti, mille fundamentaalnäiteks on seal enne asunud põhidisjunkt. Kui kõikidesse tippudesse, mis vahetult eelnevad antud tipule, on juba paigutatud disjunktid ning need disjunktid moodustavad PI-klassi, siis paigutame vaadeldavasse tippu PI-resolvendi, mille fundamentaalnäiteks on seal enne asunud põhidisjunkt. Viimasesse tippu paigutatav disjunkt peab olema tühi, sest seal enne asunud disjunkt on tühi. See tuletuspuu koos sinna paigutatud disjunktidega esitabki tühidisjunkti PI-tuletuse hulgast S. Sellega on teoreem tõestatud.

Märgime, et semantilise resolutsiooni puhul võib kasutada mistahes järjestust ja mistahes interpretatsiooni.

Näide 5.2. Kui valime näites 5.1 vaadeldud disjunktide hulga puhul predikaatsümbolite järjestuse $P = (T < Q < R)$ ja interpretatsiooni $I = \{ \neg R, Q, T\}$, siis saame tühidisjunkti PI-tuletuse disjunktide hulgast S esitada järgmise graafina:



Järgnevas käsitleme semantilise resolutsiooni kahte erijuhtu, seades täiendavaid kitsendusi PI-resolventide moodustamisele.

5.4. Hüperresolutsioon

Vaatleme interpretatsiooni I, milles suvaline literaal on elementaarvalemi eitus. Sellise interpretatsiooni korral peab iga elektron ja iga PI-resolvent sisaldama ainult elementaarvalemeid (eitusteta). Analoogiliselt, kui mingis interpretatsioonis I on iga literaal elementaarvalem, siis peab suvaline elektron ja suvaline PI-resolvent sisaldama ainult elementaarvalemite eitusi. Nendel kaalutlustel põhineb hüperresolutsioon.

Def. Disjunkti, mis ei sisalda eituse märke, nimetatakse *positiivseks disjunktiks*.

Disjunkti, milles iga literaal sisaldab eituse märgi, nimetatakse *negatiivseks disjunktiks*.

Disjunkti, mis ei ole positiivne ega negatiivne, nimetatakse *segadisjunktiks*.

Näiteks R(x) ∨ T(x) on positiivne disjunkt, ¬R(x) ∨ ∨ ¬T(x) on negatiivne disjunkt, R(x) ∨ ¬Q(x) ∨ ¬T(x) on segadisjunkt.

Def. Olgu I interpretatsioon, milles iga elementaarvalem on väär:

I = { ¬Q, ¬R,...}.

PI-resolutsiooni sellises interpretatsioonis nimetatakse *positiivseks hüperresolutsiooniks*.

Positiivse hüperresolutsiooni korral on kõik elektronid ja kõik PI-resolvendid positiivsed disjunktid.

Näites 5.1 kasutasime tühidisjunkti tuletamiseks positiivset hüperresolutsiooni, sest valitud interpretatsioonis olid kõik elementaarvalemid väärad.

Analoogiliselt positiivse hüperresolutsiooniga defineeritakse negatiivne hüperresolutsioon, lähtudes interpretatsioonist, milles kõik elementaarvalemid on tõesed. Elektronid ja PI-resolvendid osutuvad siis negatiivseteks disjunktideks.

Järgmise näiteülesande lahendamisel kasutame kõigepealt tavalist resolutsiooni ning siis negatiivset ja positiivset hüperresolutsiooni.

Näide 5.3. Tõestada, et põiknurgad, mis tekivad trapetsi diagonaali lõikumisel trapetsi alustega, on võrdsed.

Kasutame tõestamisel järgmisi teadmisi:

- trapets on nelinurk, mille kaks vastaskülge on paralleelsed;

- kahe paralleelse sirge lõikamisel kolmandaga tekkivad põiknurgad on võrdsed.

Et esitada teadmised predikaatarvutuse valemitena, toome sisse järgmised tähistused:

T(x,y,u,v) - nelinurk xyuv on trapets (x on ülemine vasakpoolne tipp, y ülemine parempoolne tipp, u alumine parempoolne tipp, v alumine vasakpoolne tipp);

Q(x,y,u,v) – lõik [x,y] on paralleelne lõiguga [u,v];

E(x,y,zu,v,w) – nurk xyz võrdub nurgaga uvw.

Siis eeldused on

F_1 : $(\forall x)(\forall y)(\forall u)(\forall v)(T(x,y,u,v) \rightarrow Q(x,y,u,v))$,

F_2 : $(\forall r)(\forall s)(\forall t)(\forall z)(Q(r,s,t,z) \rightarrow E(r,s,z,t,z,s))$,

F_3 : T(a,b,c,d)

ja väide

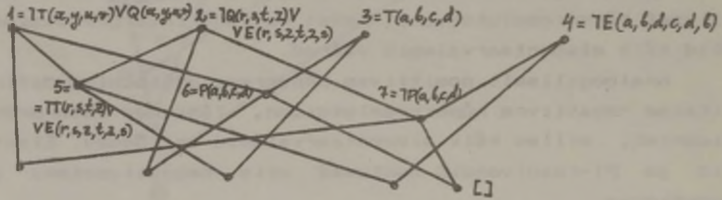
G: E(a,b,d,c,d,b).

Teoreemi F_1 & F_2 & F_3 $\rightarrow$ G tõestamiseks tuleb tõestada, et disjunktide hulk

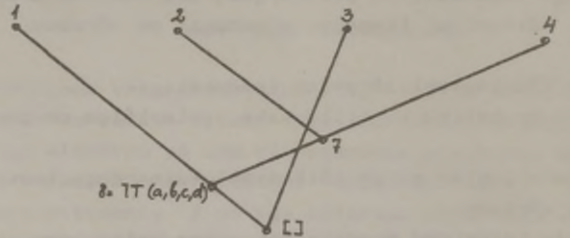
S = { ⅂T(x,y,u,v) V Q(x,y,u,v), ⅂Q(r,s,t,z) V V E(r,s,z,t,z,s), T(a,b,c,d), ⅂E(a,b,d,c,d,b)}

on vasturääkiv.

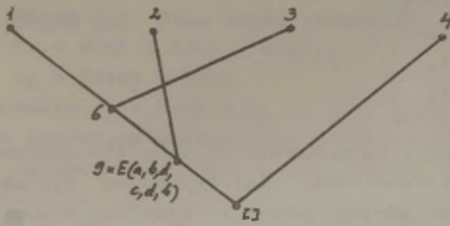
Tõestus resolutsioonimeetodil:



Tõestus negatiivse hüperresolutsiooniga (interpretatsioon I = {T, Q, E}, predikaatsümbolite järjestus suvaline, tuletuspuu tippudes on disjunktide järjekorranumbrid):



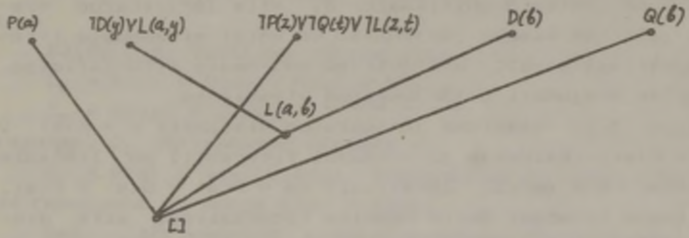
Tõestus positiivse hüperresolutsiooniga (I = { ⅂T, ⅂Q, ⅂E}, predikaatsümbolite järjestus suvaline):



Selles näites on kõigi PI-resolventide moodustamisel igas PI-klassis üksainus elektron (ja üks tuum).

Näide 5.4. Lahendame positiivse hüperresolutsiooniga ülesande patsientidest ja doktoritest (vt. näited 3.13, 4.7).

Olgu I = { ¬P, ¬D, ¬Q, ¬L} ning olgu predikaatsümbolite järjestus suvaline. PI-tuletuse saab esitada järgmise graafina:



Disjunktid P(a), L(a,b), Q(b) ja ¬P(z) ∨ ¬Q(t) ∨ ¬L(z,t) moodustavad PI-klassi, mille PI-resolvendiks on tühidisjunkt. Esimesed kolm disjunkti on selle PI-klassi elektronid, neljas aga tuum.

5.5. Järjestatud disjunkte kasutav semantiline resolutsioon

PI-tuletuses kasutatav predikaatsümbolite järjestus P ei võimalda üldjuhul valida elektronis literaali, mida resolveerida (juhul kui on mitu kandidaati).

Näide 5.5. Olgu S = {R(a) ∨ R(b) ∨ R(c) ∨ R(d), ¬R(x)}. Olgu antud interpretatsioon I = { ¬R} ja suvaline predikaatsümbolite järjestus P.

Antud kaks disjunkti moodustavad PI-klassi, millel on neli erinevat PI-resolventi:

$R(b) \vee R(c) \vee R(d)$,

$R(a) \vee R(c) \vee R(d)$,

$R(a) \vee R(b) \vee R(d)$,

$R(a) \vee R(b) \vee R(c)$.

Seame nüüd eesmärgiks täiendavate kitsenduste asetamise teel saada üksainus PI-resolvent. Selleks toome disjunkti literaalide hulgas sisse järjestuse, s.t. vaatleme disjunkte kui literaalide järjestatud hulki.

Def. Olgu C järjestatud disjunkt ning olgu L_1 ja L_2 literaalid disjunktis C. Öeldakse, et literaal L_1 on *noorem* kui literaal L_2 (ehk: literaal L_2 on *vanem* kui literaal L_1), kui L_1 esineb disjunktis C varem kui literaal L_2.

Näiteks järjestatud disjunktis $R(a) \vee R(b) \vee R(c)$ on literaal $R(c)$ vanem kui literaalid $R(a)$ ja $R(b)$ ning literaal $R(b)$ on noorem kui literaal $R(c)$.

Def. Kui kahel või enamal literaalil järjestatud disjunktis C on lihtsaim unifikaator σ, siis järjestatud disjunkti, mis on saadud järjendist $C\sigma$ kõigi niisuguste literaalide väljajätmisel, mis ühtivad nooremate literaalidega, nimetatakse disjunkti C *järjestatud kleebiseks*.

Näide 5.6. Vaatleme järjestatud disjunkti $C = P(x) \vee \vee Q(x) \vee P(a)$. Esimesel ja viimasel literaalil on lihtsaim unifikaator $\sigma = \{a/x\}$. Järelikult $C\sigma = P(a) \vee Q(a) \vee P(a)$. Kuna viimane literaal ühtib noorima literaaliga, siis disjunkti C järjestatud kleebiseks on $P(a) \vee Q(a)$. (Märgime, et järjend $Q(a) \vee P(a)$ ei ole disjunkti C järjestatud kleebis.)

Def. Olgu C_1 ja C_2 järjestatud disjunktid ühiste muutujateta. Olgu L_1 literaal disjunktis C_1 ning L_2 literaal disjunktis C_2, kusjuures L_1 ja $\neg L_2$ olgu unifitseeritavad lihtsaima unifikaatoriga σ. Olgu C järjestatud disjunkt, mis on saadud järjestatud disjunktide $C_1\sigma$ ja $C_2\sigma$ disjunktsioonist literaalide $L_1\sigma$ ja $L_2\sigma$ kõrvaldamisel ning järelejäänud järjendist kõikide selliste literaalide mahakriipsutamisel, mis on identsed järjendi noorima literaaliga. Siis öeldakse, et C on järjestatud disjunktide C_1 ja C_2 *binaarne järjestatud resolvent*. Literaale L_1 ja L_2 nimetatakse *resolveeritavateks literaalideks*.

Näide 5.7. Olgu antud järjestatud disjunktid

$C_1 = R(x) \vee Q(x) \vee T(x)$,

$C_2 = \neg R(a) \vee Q(a)$.

Literaalid $L_1 = R(x) \in C_1$ ja $L_2 = \neg R(a) \in C_2$ on unifitseeritavad lihtsaima unifikaatoriga $\sigma = \{a/x\}$.

Leiame disjunktide C_1 ja C_2 binaarse järjestatud resolvendi:

$(R(x) \vee Q(x) \vee T(x))\{a/x\} \vee (\neg R(a) \vee Q(a))\{a/x\} = Q(a) \vee \vee T(a) \vee Q(a) = Q(a) \vee T(a)$.

Def. Järjestatud disjunktide C_1 ja C_2 järjestatud resolvendiks nimetatakse kas

I) C_1 ja C_2 järjestatud resolventi või

2) C_1 järjestatud kleebise ja C_2 järjestatud resolventi või

3) C_1 ja C_2 järjestatud kleebise järjestatud resolventi või

4) C_1 ja C_2 järjestatud kleebiste järjestatud resolventi.

Näide 5.8. Vaatleme järjestatud disjunkte

$C_1 = P(x) \vee Q(x) \vee R(x) \vee P(a)$,

$C_2 = \neg P(a) \vee Q(a)$.

Disjunkti C_1 järjestatud kleebis on

$C_1' = P(a) \vee Q(a) \vee R(a)$. Disjunktide C_1 ja C_2 järjestatud resolvent on seega $Q(a) \vee R(a)$.

Def. Järjestatud resolutsiooniks nimetatakse tuletusreeglit, mis genereerib järjestatud disjunktide hulgast järjestatud resolvente.

Võib tõestada, et järjestatud resolutsioon on täielik.

Vaatleme nüüd semantilist resolutsiooni järjestatud disjunktide jaoks. Defineerime mõiste "järjestatud semantiline klass" ehk "OI-klass" eespool defineeritud semantilise klassi (PI-klassi) eeskujul.

Def. Olgu antud interpretatsioon I. Disjunktide järjendit

$E_1, \ldots, E_q, N$,

kus $q \geq 1$, nimetatakse OI-klassiks, disjunkte $E_1, \ldots, E_q$ selle klassi elektronideks ja N tuumaks, kui kehtivad järgmised tingimused:

1. I ei rahulda elektrone $E_1, \ldots, E_q$.

2. Olgu $R_q = N$. Iga $i = q, \ldots, 1$ korral leidub järjestatud disjunktide järjestatud resolvent

$R_{i-1} = R(E_i, R_i)$.

3. Resolveeritav literaal on elektronis E_i vanim ja resolvendis R_i vanim neist, mida I rahuldab.

4. R_0 on väär interpretatsioonis I.

Resolventi R_0 nimetatakse OI-klassi OI-resolvendiks.

Näide 5.9. Vaatleme järjestatud disjunktide paari

$\{\neg R(x), R(a) \vee R(b) \vee R(c) \vee R(d)\}$.

Olgu $I = \{\neg R\}$. Vaadeldav disjunktide paar moodustab OI-klassi, mille OI-resolvendiks on järjestatud disjunkt

$R(a) \vee R(b) \vee R(c)$.

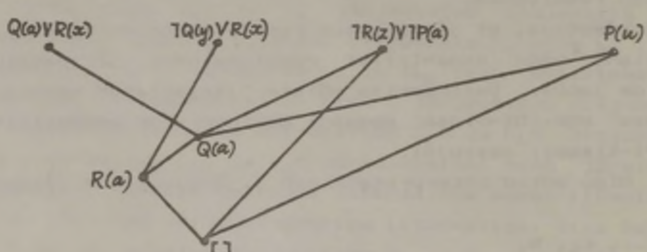
Tavalisi resolvente on sellel disjunktide paaril 4 (vt. näide 5.5).

Näide 5.10. Olgu $I = \{\neg R, \neg Q, \neg S\}$. Järjestatud disjunktide järjend $\{Q(a) \vee R(x), S(x), \neg R(x) \vee \neg S(a)\}$ moodustab OI-klassi, mille OI-resolvendiks on disjunkt $Q(a)$.

Def. Olgu S järjestatud disjunktide hulk ning I tema interpretatsioon. Tuletust hulgast S nimetatakse OI-tuletuseks, kui iga järjestatud disjunkt selles tuletuses on kas hulgast S või eelnevate järjestatud disjunktide mingi OI-klassi OI-resolvent.

Näide 5.11. Leiame tühidisjunkti OI-tuletuse järjestatud disjunktide hulgast $S = \{Q(a) \vee R(x), \neg Q(y) \vee R(y), \neg R(z) \vee \neg P(a), P(u)\}$.

Olgu $I = \{\neg Q, \neg R, \neg P\}$. OI-tuletuse esitame graafina:



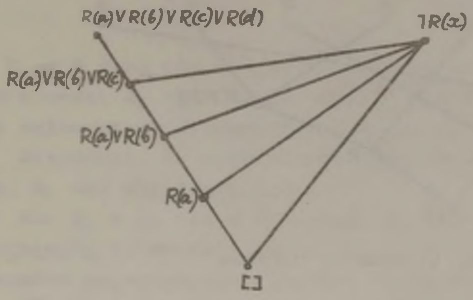
Siin disjunktide järjend $\{Q(a) \vee R(x), P(u), \neg R(z) \vee \neg P(a)\}$

moodustab OI-klassi, mille elektronid on Q(a) ∨ R(x) ja P(u), tuum ¬R(z) ∨ ¬R(a) ning OI-resolvent Q(a). OI-klassid on veel {Q(a), ¬Q(y) ∨ R(y)} (OI-resolvent R(a)) ja {R(a), P(u), ¬R(z) ∨ ¬P(a)} (OI-resolvent []).

Näide 5.12. Vaatleme järjestatud disjunktide hulka

{R(a) ∨ R(b) ∨ R(c) ∨ R(d), ¬R(x)}

(vt. näide 5.5). Olgu I = { ¬R}. Tühidisjunkti OI-tuletus sellest hulgast on esitatud graafina:



Juba neljas OI-resolvent osutub tühidisjunktiks. Tavalisi resolvente oleks aga tulnud genereerida $4 + 4\cdot3 + 4\cdot3\cdot2 + 1 = 41$.

Nagu eksperimendid kinnitavad, on OI-tuletus efektiivne teoreemide tõestamise meetod. Kahjuks pole ta aga täielik: igast vasturääkivast disjunktide hulgast ei saa OI-tuletuse teel genereerida tühidisjunkti. Toome selle kohta näite.

Näide 5.13. Kuulugu hulka S järjestatud disjunktid

(1) P ∨ Q,

(2) Q ∨ R,

(3) R ∨ W,

(4) ¬R ∨ ¬P,

(5) ¬W ∨ ¬Q,

(6) ¬Q ∨ ¬R.

Olgu I = { ¬P, ¬Q, ¬R, ¬W}. Siis disjunkte (1)-(3) võib kasutada järjestatud elektronidena, disjunkte (4)-(6) aga järjestatud tuumadena. Saame järgmised OI-resolvendid:

(7) R ∨ P - OI-klassist {(3), (1), (5)},

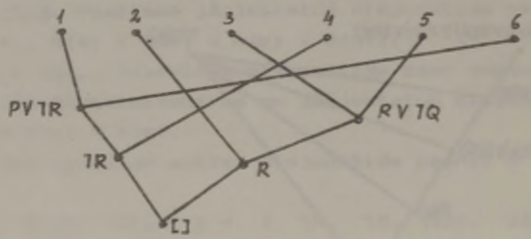
(8) P V Q - OI-klassist {(1), (2), (6)}.

Disjunktide hulgast (1)-(8) saame OI-resolvendi

(9) Q V R (OI-klassist {(2), (7),(4)}).

Disjunktid (8) ja (9) ei kuulu hulka S. Seetõttu ei saa disjunktidest (1)-(9) tuletada ühtki uut OI-resolventi, sealhulgas ka mitte tühidisjunkti.

Ometi on hulk S vasturääkiv, sest resolutsioonimeetodil saab temast tuletada tühidisjunkti:



6. Lineaarne tuletus

Vaatleme lihtsa ülesehitusega ja ülevaatlikku lineaarset tuletust, mis saadakse teatavate kitsenduste asetamisega resolventide moodustamisele.

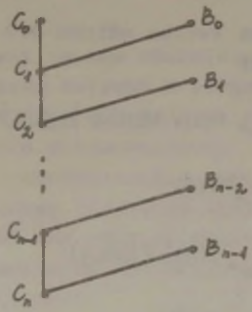
Defineerime algul lihtsa ja efektiivse tuletusreegli - sisendresolutsiooni.

Def. Sisendresolutsiooniks nimetatakse sellist resolutsiooni, milles vähemalt üks lahenevatest disjunktidest on lähtedisjunkt (s.o. kuulub antud disjunktide hulka S).

Kui kasutada tavalise resolutsiooni asemel ainult sisendresolutsiooni, siis väheneb oluliselt genereeritavate resolventide hulk. Kahjuks pole aga sisendresolutsioon täielik.

Lubades tuletuses kasutada lisaks sisendresolutsioonile ka nn. eelnevusresolutsiooni, saame lineaarse tuletuse, mis on täielik.

Def. Disjunkti C_n lineaarseks tuletuseks disjunktide hulgast S nimetatakse tuletust $C_0, B_0, C_1, B_1, \ldots, C_{n-1}, B_{n-1}, C_n$ kujul

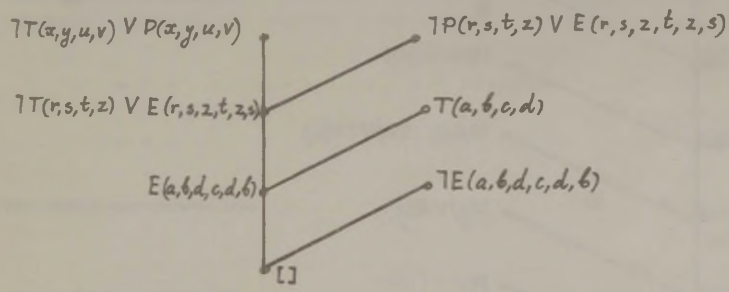


kus $C_0 \in S$ ning iga $i=0,1,\ldots,n-1$ korral on C_{i+1} disjunkti C_i ja disjunkti B_i resolvent, kus B_i kas kuulub hulka S või on mõni eelnevatest disjunktidest C_j mingi $j < i$ korral.

Disjunkti C_i nimetatakse resolvendi C_{i+1} *keskdisjunktiks*, B_i aga *külgdisjunktiks*.

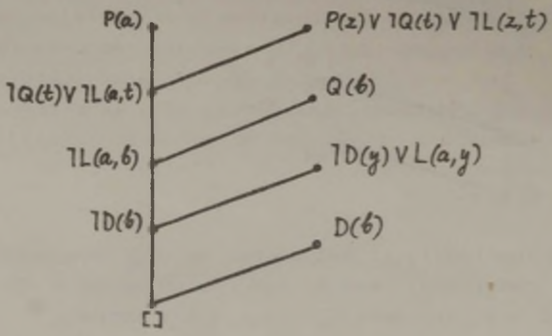
Kui $B_i \in S$, siis öeldakse, et C_{i+1} on saadud *sisendresolutsiooni* tulemusel; kui $B_i = C_j$, siis öeldakse, et C_{i+1} on saadud *eelnevusresolutsiooni* tulemusel.

Näide 6.1. Lahendame näites 5.3 vaadeldud ülesande trapetsist, kasutades lineaarset tuletust:



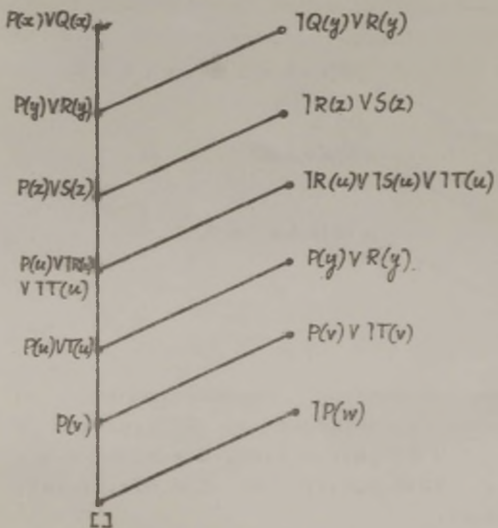
Kõik selles tuletuses kasutatud resolutsioonid on sisendresolutsioonid. Keskdisjunktideks on $\neg T(x,y,u,v) \vee$ $\vee\, Q(x,y,u,v)$, $\neg T(r,s,t,z) \vee E(r,s,z,t,z,s)$, $E(a,b,d,c,d,b)$, külgdisjunktideks aga $\neg Q(r,s,t,z) \vee E(r,s,z,t,z,s)$, $T(a,b,c,d)$, $\neg E(a,b,d,c,d,b)$.

Näide 6.2. Lahendame veel näites 3.13 toodud ülesande patsientidest ja doktoritest (vt.ka näited 4.7 ja 5.3), kasutades lineaarset tuletust:



Ka selles lineaarses tuletuses on kasutatud ainult sisendresolutsiooni.

<u>Näide 6.3.</u> Tõestame, et disjunktide hulk
$S = \{P(x) \lor Q(x),\ \neg Q(y) \lor R(y),\ \neg R(z) \lor S(z),\ \neg R(u) \lor S(u) \lor$
$\lor\ T(u),\ P(v) \lor \neg T(v),\ \neg P(w)\}$
on vasturääkiv, kasutades lineaarset tuletust:



sisendresolutsioon

– " –

– " –

eelnevusresolutsioon

sisendresolutsioon

– " –

Praktiliselt toimub tühidisjunkti lineaarse tuletuse otsimine disjunktide hulgast S järgmisel viisil. Võtame mingi disjunkti $C_0 \in S$ ja leiame tema kõikvõimalikud resolvendid hulga S ülejäänud disjunktidega. Kõik saadud resolvendid on keskdisjunkti kandidaadid. Neist igaühe puhul toimime samuti, nagu varem toimisime disjunktiga C_0, ainult külgdisjunktideks võivad nüüd olla mitte ainult hulga S disjunktid, vaid ka eelnevad keskdisjunktid. Tõestus lõpeb, kui saadakse tühidisjunkt.

Lõpetuseks

Teoreemide automaatse tõestamise alal võib täheldada märkimisväärset progressi. Hoolimata sellest kalduvad olemasolevad tõestusprogrammid genereerima liialt palju resolvente ning uurima ülearuseid tuletusteid. Seetõttu on konkreetsete ülesannete puhul kasutatud spetsiifilisi tõestusmeetodeid või rakendatud lihtsamaid, kuigi mitte täielikke tuletusreegleid. On kasutatud ka kõrgemat järku predikaatarvutust. Programmeerimise seisukohalt tähendab see, et lihtsad tehted suurel valemite hulgal asendatakse keeruliste tehetega väikesel valemite hulgal. Tõestusprogrammid on enamasti koostatud keeles LISP (või INTERLISP).

Sisukord