TARTU ÜLIKOOL
Arvutiteaduse instituut

Reimo Palm, Rein Prank

SISSEJUHATUS MATEMAATILISSE LOOGIKASSE

TARTU 2004

TARTU ÜLIKOOL
ARVUTITEADUSE INSTITUUT

Reimo Palm Rein Prank

SISSEJUHATUS MATEMAATILISSE LOOGIKASSE

Tartu 2004

Käesoleva raamatu väljaandmist on toetanud Eesti Infotehnoloogia Sihtasutus projekti „Tiigriülikool“ raames.

Toimetaja Härmel Nestra

Kaanekujundaja Aita Linnas

Õpiku digiversioonis on parandatud trükiversioonis avastatud vead.

ISBN 9985-56-867-2

Tartu Ülikooli Kirjastus
http://www.tyk.ut.ee/
Tellimus nr 202

SISUKORD

Eessõna **5**

I. Lausearvutus **7**
§ 1. Lausearvutuse põhimõisted 7
§ 2. Valemite omadused 12
§ 3. Järeldumine 18
§ 4. Samaväärsus 20
§ 5. Normaalkujud 24
§ 6. Normaalkujude minimeerimine 31
§ 7. Ülesanded 37

II. Predikaatarvutus **44**
§ 1. Predikaadid ja kvantorid 44
§ 2. Predikaatarvutuse süntaks 48
§ 3. Predikaatarvutuse semantika 52
§ 4. Valemite omadused 59
§ 5. Samaväärsus 64
§ 6. Valemi prefikskuju 70
§ 7. Ülesanded 74

III. Aksiomaatilised teooriad **83**
§ 1. Aksiomaatilise teooria üldskeem 83
§ 2. Sekventsiaalne lausearvutus 88
§ 3. Sekventsiaalne predikaatarvutus 97
§ 4. Esimest järku aksiomaatilised teooriad 101
§ 5. Ülesanded 107

IV. Turingi masinad **112**
§ 1. Turingi masina mõiste 112
§ 2. Kompositsioon ja hargnemine 119
§ 3. Mittearvutatavad funktsioonid 122
§ 4. Ülesanded 127

Aineregister **130**

EESSÕNA

Matemaatiline loogika on loogika haru, milles loogikaprobleemide käsitlemiseks kasutatakse matemaatilisi meetodeid. Kirjeldades mingi valdkonna mõisteid ja väiteid, tuuakse sisse formaliseeritud keel, mis on matemaatiliseks uurimiseks piisavalt täpne, ühemõtteline ja lihtne. Seejuures tehakse vahet keele süntaktilistel aspektidel, mis käsitlevad objekte kui teatavate reeglite järgi koostatud sümbolijärjendeid, ning semantilistel aspektidel, mis annavad süntaktilistele objektidele interpretatsiooni ehk „tähenduse“.

Matemaatilise loogika ajalugu võib alustada Gottfried Wilhelm Leibnizist (1646—1716), kes püüdis luua ühtset teaduskeelt (*lingua universalis*), milles saaks väljendada kõiki teadustõdesid, ning arutlusarvutust (*calculus ratiocinator*), mille abil võiks olemasolevatest tõdedest mehaaniliselt tuletada uusi. Hoo sai matemaatilise loogika areng sisse 19. sajandi keskel, kui George Boole (1815—1864) avaldas tööd *The Mathematical Analysis of Logic* (1847) ja *An Investigation of the Laws of Thought* (1854), milles klassikalise loogika seaduspärasused on esitatud algebraliste võrrandite kujul ühtse matemaatilise süsteemina. Boole'i ja temaga samal ajal tegutsenud Augustus De Morgani (1806—1871) ideedest kujunes välja lausearvutus. Gottlob Frege (1848—1925) raamatus *Begriffsschift* (1879) on esmakordselt esitatud üks tänapäeva loogika tähtsamaid süsteeme, predikaatarvutus. Frege hakkas ka matemaatika (aritmeetika) ülesehitamisel kasutama matemaatilist loogikat, mis muutus kiiresti täiemõõduliseks matemaatika keeleks ning omandas nüüdisaegse kuju Bertrand Russelli (1872—1970) ja Alfred North Whiteheadi (1861—1947) kolmeköitelises kapitaalses teoses *Principia mathematica* (1910—1913). Matemaatilise loogika järgnev areng on seotud matemaatika aluste aksiomatiseerimisega, sellealase töö suunajaks oli David Hilbert (1862—1943). Aksiomaatilise meetodi võimaluste kohta andsid selgust Kurt Gödeli (1906—1978) teoreemid predikaatarvutuse täielikkusest (1930) ja formaalse aritmeetika mittetäielikkusest (1931). Seoses matemaatilisest loogikast tulenevate küsimustega, näiteks predikaatarvutuse valemite samaselt tõesuse kontrollimine ja aksiomaatilistes teooriates tuletatavate valemite hulga kirjeldamine, hakkas 1930. aastatel, pärast algoritmi mõistele sobiva definitsiooni andmist, arenema algoritmiteooria. Tänaseks on matemaatiline loogika jagunenud paljudeks harudeks. Et aga matemaatilises loogikas kasutatavad formaliseeritud keeled on osutunud väga sobivaks programmide koostamise ja analüüsimise juures, siis on kogu valdkonna areng üha tihedamini seotud arvutiteadusega.

Õpiku esimese kahe peatüki teemad, lausearvutus ja predikaatarvutus, moodustavad matemaatilise loogika aluse. Lausearvutuse eesmärk on uurida lausete omavahelist kombineerumist liitlauseks, näiteks kuidas tekkinud liitlause tõeväärtus sõltub komponentlausete tõeväärtusest. Predikaatarvutus on lausearvutuse üldistus, kus fikseeritud tõeväärtusega lausete asemel vaadeldakse selliseid lauseid, mille tõeväärtus võib sõltuda argumentide väärtustest. Nende abil saab väidete struktuuri esitada täpsemalt. Kolmas peatükk on sissejuhatus aksiomaatilistesse teooriatesse. Esitatakse lausearvutuse ja predikaatarvutuse aksiomaatika sekventsiaalse süsteemina ning tutvustatakse esimest järku aksiomaatiliste teooriate konstrueerimist. Paljude distsipliinide aksiomaatika saab üles ehitada esimest järku teooriana. Aksiomaatilised teooriad moodustavad üldse matemaatilise loogika peamise uurimisobjekti. Peale valdkonna mõistete, väidete ja nende tõeväärtuste määramise formaliseeritakse aksiomaatilises teoorias lisaks veel tõestuse mõiste, väidete tõestamine taandub nende ümberkirjutamisele etteantud reeglite järgi. Lõpuks on õpiku neljandas peatükis antud lühike ülevaade algoritmiteooria põhimõistetest, lähtudes algoritmi ühest võimalikust matemaatilisest vastest, Turingi masinast. Tõestatakse ka teoreemid mõnede funktsioonide mittearvutatavuse kohta.

Käesolev õpik on välja kasvanud Rein Prangi loengute konspektist, mille koostas Kristel Õunapuu aastal 1994 ning mida levitati elektrooniliselt ja paljundistena. Lisatud on uut materjali, kõige rohkem lause- ja predikaatarvutuse osas, ning ülesanded, samuti materjali korrastatud. Autorid soovivad avaldada tänu Marju Mikkelile mitmete paranduste eest ning iseäranis toimetaja Härmel Nestrale, kes lisaks teksti läbivaatamisele tegi hulgaliselt mitmesuguseid sisulisi märkusi ja ettepanekuid.

I. LAUSEARVUTUS

§ 1. Lausearvutuse põhimõisted

Lausearvutus on matemaatilise loogika lihtsaim osa ja moodustab koos predikaatarvutusega enamiku matemaatilise loogika suundade aluse. Lihtsusele vaatamata puudutab lausearvutus mitmeid olulisi aspekte loogikas ning ka paljud praktilised küsimused taanduvad sageli ühele või teisele lausearvutuse probleemile.

Põhilised uuritavad objektid lausearvutuses on *laused*, mis võivad pärineda ükskõik millisest valdkonnast. Oluline on, et igale lausele saaks vastavusse seada *tõeväärtuse*, mis kirjeldab lause tegelikkusele vastavuse määra. Meie vaatleme klassikalist kahevalentset loogikat, kus lause tõeväärtus võib olla ainult üks kahest alternatiivist: „tõene“ või „väär“. Täpsemalt, eeldame, et käsitletavad laused rahuldavad järgmisi tingimusi.

1) *Välistatud kolmanda seadus.* Iga lause on kas tõene või väär.
2) *Mittevasturääkivuse seadus.* Ükski lause ei saa olla nii tõene kui ka väär.

Nende nõuete põhjal kuuluvad vaadeldavate hulka ainult niisugused laused, mis midagi väidavad, kusjuures sellel väitel on olemas ühene tõeväärtus. Näiteks leidub tõeväärtus lausetel „Réunioni saar asub India ookeanis“ ja „Arv 391 on algarv“, lausetel „Kas Eestis pesitseb toonekurgi?“ ja „Maja mere ääres“ aga mitte. Välistatud kolmanda seaduse nõudel jäävad kõrvale kõik küsilaused ja paljud hüüdlaused, samuti kõik käsud ning mõttetud sõnaühendid. Mittevasturääkivuse seadus välistab mitmesugused paradoksid, näiteks „See lause siin on väär“, ja muud taolised väited, mille tõeväärtust pole võimalik üheselt määrata. Teha kindlaks, kas mingi lause sisu poolest vastab tegelikkusele, ei ole lausearvutuse ülesanne, vajaliku informatsiooni peavad andma teised allikad.

Lausearvutuses jagatakse keerulisemad laused komponentlauseteks (lihtlauseteks) ja neid ühendavateks grammatilisteks seosteks. Seejärel tuuakse sisse tähised komponentlausete ja seoste märkimiseks ning pannakse vaadeldav lause kirja sümbolkujul. Komponentlausete tähistamiseks kasutame suuri ladina tähti A, B, C jne, mida nimetame *lausemuutujateks*, grammatilistele seostele vastavad *lausearvutuse tehted*. Tähtsamad lausearvutuse tehted on järgmised.[1]

- *Eitus* (märk $\neg$). Igapäevakeeles väljendab eitus lause mittekehtimist, näiteks „Lehis ei ole okaspuu“. Selle lause võib kirja panna valemiga $\neg A$, kus A = „Lehis on okaspuu“.
- *Konjunktsioon* (märk &) tähendab seost „ja“. Näiteks „Puhub tuul ja sajab vihma“ on valemkujul $A \,\&\, B$.
- *Disjunktsioon* (märk $\vee$) väljendab seost „või“. Näiteks „Helen laulab või Mart laulab“ on valemkujul $A \vee B$. Sidesõna „või“ kasutatakse siin mittevälistavas tähenduses: „Kas A või B või mõlemad“. Igapäevases keeles on käibel ka välistav „või“: „Kas A või B, aga mitte mõlemad“, näiteks „Ma külvan põllule rukist või panen põllule kartulid“. Disjunktsiooni all mõistame mittevälistavat „võid“.
- *Implikatsioon* (märk $\rightarrow$) väljendab tingimuslikku konstruktsiooni „kui ..., siis ...“. Näiteks „Kui Sven terve aasta korralikult õpib, siis suudab ta kevadel eksamid hõlpsasti ära teha“ või „Kui kehtib teoreem P, siis kehtib teoreem Q“. Mõlemad laused võib kirja panna valemiga $A \rightarrow B$.
- *Ekvivalents* (märk $\leftrightarrow$) tähendab matemaatikas sagedasti kasutatavat seost „parajasti siis, kui“ ehk „siis ja ainult siis, kui“. Näiteks lause „hulk X on kinnine parajasti siis, kui X ühtib oma sulundiga“ on valemkujul $A \leftrightarrow B$.

Olles piiritlenud lausearvutuse tehted, võime lisaks lausete komponentideks lahutamisele tegutseda ka vastupidises suunas: koostada lihtsamatest lausetest keerulisemaid, ühendades neid omavahel lausearvutuse tehete abil. Niisugustes operatsioonides eeldame järgmiste tingimuste täidetust.

3) Tehteid võib teostada ükskõik milliste lausetega.
4) Tehte tulemuseks saadud lause tõeväärtus sõltub ainult komponentlausete tõeväärtustest.

Nendest tingimustest järeldub vahetult, et lausetega tehete sooritamisel on oluline mitte lausete sisu, vaid tõeväärtus.

[1] Lisaks siintoodud tehtemärkidele kasutatakse ka teistsuguseid. Näiteks $\neg A$ asemel kirjutatakse mõnikord $\overline{A}$, $-A$ või $\sim A$, konjunktsiooni võib tähistada ka märk $\wedge$, implikatsiooni märgid $\supset$, $\Rightarrow$, ekvivalentsi märgid $\sim$, $\equiv$, $\Leftrightarrow$ jne.

Kirjutades laused üles sümbolkujul, saame lausearvutuse valemid. Kui see on tehtud, siis võime edasise uurimise aluseks võtta valemid ja jätta kõrvale laused, millest need valemid saadi. Täpse eeskirja valemite kirjapanemiseks määrab kindlaks *lausearvutuse süntaks*, mis väljendub järgmises definitsioonis.

Definitsioon 1. *Lausearvutuse valemid on parajasti need, mida saab koostada alltoodud reeglite abil.*

1) *Iga lausemuutuja on lausearvutuse valem.*
2) *Kui $\mathcal{F}$ on lausearvutuse valem, siis ka $\neg\mathcal{F}$ on lausearvutuse valem.*
3) *Kui $\mathcal{F}$ ja $\mathcal{G}$ on lausearvutuse valemid, siis ka $(\mathcal{F} \mathbin{\&} \mathcal{G})$, $(\mathcal{F} \vee \mathcal{G})$, $(\mathcal{F} \rightarrow \mathcal{G})$ ja $(\mathcal{F} \leftrightarrow \mathcal{G})$ on lausearvutuse valemid.*

Lausearvutuse valemi definitsioon näitab, kuidas lihtsamatest valemitest saab järk-järgult moodustada keerulisemaid. Niisugust tüüpi definitsioonid esinevad loogikas üsna sageli, neid nimetatakse *induktiivseteks*, sest vormi poolest meenutavad nad matemaatilise induktsiooni printsiipi. Tingimus 1) kujutab seejuures induktsiooni baasi, tingimused 2) ja 3) aga induktsiooni sammu.

Lähtudes lausemuutujatest, saame koostada valemid, mis sisaldavad ühte lausearvutuse tehet; lähtudes lausemuutujatest ja ühe tehtega valemitest, saame koostada kahe tehtega valemid jne. Kõiki antud valemi konstrueerimise käigus tekkinud valemeid nimetatakse selle valemi *osavalemiteks* ehk *alamvalemiteks*, konstrueerimise viimasel sammul kasutatud tehet aga valemi *peatehteks*.

Näide 1. Lausemuutujad A, B, C on lausearvutuse valemid definitsiooni esimese punkti põhjal. Teise punkti põhjal on lausearvutuse valemid ka näiteks $\neg A$ ja $\neg B$ ning kolmanda punkti põhjal $(B \vee A)$. Edasi on lausearvutuse valemid $(A \mathbin{\&} \neg B)$, $(C \rightarrow \neg A)$ ja $((A \mathbin{\&} \neg B) \mathbin{\&} (C \rightarrow \neg A))$ ning samuti $(((A \mathbin{\&} \neg B) \mathbin{\&} (C \rightarrow \neg A)) \leftrightarrow (B \vee A))$. Viimase valemi peatehe on $\leftrightarrow$ ja tema osavalemid on parajasti kõik loetletud valemid.

Et vähendada valemis sulgude arvu, teeme veel kolm kokkulepet.

1) *Tehete prioriteet* kõrgemast madalamani on $\neg$, $\&$, $\vee$, $\rightarrow$, $\leftrightarrow$.
2) *Vasakassotsiatiivsus*: kui mitme liikme konjunktsioonis või disjunktsioonis sooritatakse tehteid vasakult paremale, siis võib tehete järjekorda täpsustavatest sulgudest loobuda.
3) Valemi välimised sulud võib ära jätta.

Näide 2. Vaatleme taas eelmise näite viimast valemit

$$(((A \mathbin{\&} \neg B) \mathbin{\&} (C \to \neg A)) \leftrightarrow (B \vee A)).$$

Jättes ära välimised sulud, saame

$$((A \mathbin{\&} \neg B) \mathbin{\&} (C \to \neg A)) \leftrightarrow (B \vee A).$$

Tehete prioriteeti arvestades võime loobuda sulgudest valemi peatehte kummagi poole ümber:

$$(A \mathbin{\&} \neg B) \mathbin{\&} (C \to \neg A) \leftrightarrow B \vee A.$$

Vasakassotsiatiivsuse reegli põhjal pole tarvis ka esimesi sulge:

$$A \mathbin{\&} \neg B \mathbin{\&} (C \to \neg A) \leftrightarrow B \vee A.$$

Kokkuvõttes on valem omandanud hoopis ülevaatlikuma kuju.

Lausearvutuse süntaks fikseerib eeskirja, kuidas koostada lausearvutuse valemeid. Kirjeldame nüüd *lausearvutuse semantikat*, mis määrab kindlaks, kuidas leida valemi tõeväärtust, ehk annab valemile tähenduse tõesuse ja vääruse mõttes.

Iga lausemuutuja võib olla kas tõene või väär. Kui näiteks muutuja A on tõene, siis kirjutame[2] $A = 1$, vastasel korral, kui muutuja A on väär, kirjutame $A = 0$. Juhul, kui vaatluse all on korraga hulk lausemuutujaid ja me omistame tõeväärtuse igale muutujale, siis nimetatakse sellist tõeväärtuste komplekti muutujate *väärtustuseks*. Näiteks muutujakomplekti A, B, C üks võimalik väärtustus on $A = 1$, $B = 0$, $C = 1$ ehk lühemalt $(1, 0, 1)$.

Olgu antud mingi lausearvutuse valem. Omistame kõigile selles valemis esinevatele lausemuutujatele tõeväärtused, s.o anname neile muutujatele mingi väärtustuse. Valemi tõeväärtuse leidmiseks sellel väärtustusel tuleb sooritada kõik valemi tehted, milleks annab reeglid järgmine definitsioon.

Definitsioon 2. *Lausearvutuse valemi $\mathcal{F}$ tõeväärtus etteantud väärtustusel leitakse järgmiste reeglite abil.*

1) *Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 0$.*
2) *Kui $\mathcal{F} = \mathcal{G} \mathbin{\&} \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{F} = 1$ ja $\mathcal{G} = 1$.*
3) *Kui $\mathcal{F} = \mathcal{G} \vee \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{F} = 1$ või $\mathcal{G} = 1$.*
4) *Kui $\mathcal{F} = \mathcal{G} \to \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{F} = 0$ või $\mathcal{G} = 1$.*
5) *Kui $\mathcal{F} = \mathcal{G} \leftrightarrow \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{F} = 1$ ja $\mathcal{G} = 1$ või $\mathcal{F} = 0$ ja $\mathcal{G} = 0$.*

[2] Tõeväärtusi tähistatakse numbrite 1 ja 0 asemel mõnikord ka tähtedega t ja v (sõnadest „tõene“ ja „väär“) või tähtedega t ja f (sõnadest „true“ ja „false“).

Eituse puhul on tegemist lihtsa postulaadiga, et teineteist eitavate lausete tõeväärtused on vastupidised. Konjunktsioon on tõene ainult juhul, kui mõlemad komponentlaused on tõesed. Disjunktsioon on tõene, kui on tõene vähemalt üks komponentlause. Seega realiseerib disjunktsioon sõna „või“ mittevälistavat tähendust. Implikatsioon on väär ainult siis, kui eesliige on tõene ja tagaliige väär. Kuigi tavakeeles kipume väära eesliikmega implikatsiooni (näiteks „Kui $1 = 2$, siis täna on neljapäev“) pidama rohkem vääraks kui tõeseks, peetakse tõeväärtuse arvutamise reeglites silmas pigem järeldumist matemaatilises mõttes. Näiteks pole meil mingit põhjust lugeda järeldust „Kui arv x on positiivne, siis arvu x ruut on positiivne“ vääraks juhul, kui vaadeldav arv on negatiivne või null. Lõpuks, ekvivalents kehtib siis, kui pooled on võrdse tõeväärtusega.

Lausearvutuse semantika ja lausearvutuse süntaks on struktuurilt väga sarnased. Süntaks näitab, kuidas elementaarsetest detailidest, lausemuutujatest, ehitada üles valemeid, semantika järgib sama protseduuri, võttes oma detailide ossa tõeväärtused.

Näide 3. Leida valemi $A \mathbin{\&} \neg B \mathbin{\&} (C \to \neg A) \leftrightarrow B \vee A$ tõeväärtus muutujate A, B, C väärtustusel $(1, 0, 1)$.

Järgime sama skeemi nagu näites 1 valemi konstrueerimisel. Kõigepealt teame, et $A = 1$, $B = 0$, $C = 1$. Eelneva definitsiooni esimese punkti põhjal saame $\neg A = 0$ ja $\neg B = 1$ ning kolmanda punkti põhjal $B \vee A = 1$. Edasi leiame analoogilisel viisil $A \mathbin{\&} \neg B = 1$ ning $C \to \neg A = 0$, mistõttu $A \mathbin{\&} \neg B \mathbin{\&} (C \to \neg A) = 0$. Lõpuks näeme, et $A \mathbin{\&} \neg B \mathbin{\&} (C \to \neg A) \leftrightarrow B \vee A = 0$. Vaadeldaval väärtustusel on valem järelikult väär.

Tehete toimet võib ülevaatlikumalt kirjeldada *tõeväärtustabeliga*, mille vasakus osas on valemi argumentide kõikvõimalikud väärtustused, paremas osas aga tehete tulemused. Definitsioonis 2 antud reeglid võib seega esitada ka järgmiste tabelitena:

$\mathcal{F}$	$\neg\mathcal{F}$
1	0
0	1

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{F} \mathbin{\&} \mathcal{G}$	$\mathcal{F} \vee \mathcal{G}$	$\mathcal{F} \to \mathcal{G}$	$\mathcal{F} \leftrightarrow \mathcal{G}$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Väärtustused tabeli vasakus osas on soovitatav panna kirja kindlas järjekorras (meie valime selleks vastavate kahendarvude kahanemise järjekorra). Kui on vaja loetleda tehte tulemused kõikvõimalikel väärtustustel, siis piisab selleks ainult tõeväärtuste veerust.

Keerukama valemi tõeväärtustabelis kirjutatakse tehte tulemused iga tehtemärgi alla omaette veergu. Näites 1 konstrueeritud valemi tõeväärtustabeliks saame niiviisi

			4	2	6	5	1	7	3
A	B	C	$A\,\&$	$\neg B$	$\&\,(C$	$\to$	$\neg A)$	$\leftrightarrow B$	$\vee A$
1	1	1	0	0	0	0	0	0	1
1	1	0	0	0	0	1	0	0	1
1	0	1	1	1	0	0	0	0	1
1	0	0	1	1	1	1	0	1	1
0	1	1	0	0	0	1	1	0	1
0	1	0	0	0	0	1	1	0	1
0	0	1	0	1	0	1	1	1	0
0	0	0	0	1	0	1	1	1	0

Numbrid tähistavad järjekorda, milles tehted on sooritatud. Valemi tõeväärtused leiame viimasena (antud juhul seitsmendana) arvutatud ehk peatehtele vastavast veerust.

Tõeväärtustabel on lausearvutuse valemi analüüsimise universaalne meetod. Enamiku ülesannetest, mis puudutavad lausearvutuse valemi tõesust või väärust, saab lahendada tõeväärtustabeliga, kuigi mõnede spetsiaalsete ülesannete lahendamiseks on olemas ka teisi meetodeid. Et aga n muutujaga valemi tõeväärtustabel sisaldab 2^n rida, siis kasvab tõeväärtustabeli maht muutujate arvu suurenedes väga kiiresti.

§ 2. Valemite omadused

Järgnevas vaatleme lausearvutuse valemite „globaalseid" omadusi, jälgides valemi tõeväärtust seal esinevate lausemuutujate erinevatel väärtustustel.

Definitsioon 3. *Lausearvutuse valemit $\mathcal{F}$ nimetatakse*

- *samaselt tõeseks, kui ta on igal väärtustusel tõene;*
- *samaselt vääraks, kui ta on igal väärtustusel väär.*

Samaselt tõest valemit nimetatakse ka *tautoloogiaks* või *loogiliselt tõeseks valemiks* ning samaselt väära valemit *kontradiktsiooniks* või *loogiliselt vääraks valemiks*. Üks samaselt tõene valem on näiteks $A \vee \neg A$, see väljendab välistatud kolmanda seadust. Mittevasturääkivuse seadust kirjeldab aga samaselt väär valem $A \,\&\, \neg A$.

Samaselt tõesed valemid väljendavad üldkehtivaid loogikaseadusi ning pakuvad seetõttu loogikas suurt huvi. Asendades niisuguses valemis kõik lausemuutujad mingite lausetega, saame liitlause, mis on alati tõene. Näiteks kui valemis $A \vee \neg A$ võtta $A =$ „Homme on ilus ilm“, siis saame lause „Homme on ilus ilm või homme ei ole ilus ilm“, mis on tõene sõltumata sellest, milline ilm homme on.

Et samaselt tõene valem on igas olukorras tõene, siis ei sisalda ta informatsiooni. Kui viimane vaadeldud lause esineb näiteks ilmateates, siis pole sellest homse ilma kohta võimalik midagi teada saada. Teinekord esineb taolise struktuuriga väiteid igapäevases keeles, näiteks „Seadus võetakse Riigikogus vastu või ei võeta“. Kuigi niisugune väide otsest informatsiooni ei kanna, saab järeldada lause esitamise faktist, et tegemist on mingi seadusega, mille vastuvõtmise suhtes pole kõik saadikud ühel meelel. Selline kaudne tõlgendamine jääb aga väljapoole lausearvutuse piire.

Samaselt väärad valemid esitavad väiteid, mis mingil tingimusel tõesed olla ei saa. Vaatleme näiteks valemit $A \,\&\, \neg A$ ja valime jällegi $A =$ „Homme on ilus ilm“. Saame lause „Homme on ilus ilm ja pole ilus ilm“, mis ei saa olla tõene, sest siis peaks homne ilm olema ühtaegu nii ilus kui ka halb.

Iga valemi samaselt tõesust saab kontrollida tõeväärtustabeliga: valemi tõeväärtuste veerus peab esinema ainult väärtus 1. Et tõeväärtustabel on lõplik, siis saab lausearvutuse valemi samaselt tõesust (erinevalt edaspidi vaadeldavatest predikaatarvutuse valemitest) alati kindlaks teha lõpliku arvu sammudega ehk, algoritmiteooria terminites, lausearvutuse samaselt tõeste valemite hulk on lahenduv. Analoogilised märkused kehtivad samaselt väärade valemite kohta.

Näide 4. Näidata, et valem $A \,\&\, B \vee A \,\&\, \neg B \vee \neg A \,\&\, B \vee \neg A \,\&\, \neg B$ on samaselt tõene.

Koostame tõeväärtustabeli

		1	9	3	2	10	4	5	11	6	8	7
A	B	$A \,\&\, B$	$\vee$	$A \,\&$	$\neg B$	$\vee$	$\neg A$	$\&\, B$	$\vee$	$\neg A$	$\&$	$\neg B$
1	1	1	1	0	0	1	0	0	1	0	0	0
1	0	0	1	1	1	1	0	0	1	0	0	1
0	1	0	0	0	0	1	1	1	1	1	0	0
0	0	0	0	0	1	0	1	0	1	1	1	1

Et antud valemi tõeväärtuste veerus esinevad ainult tõesed väärtused, siis on valem samaselt tõene. Seda valemit võib pidada välistatud kolmanda seaduse üldistuseks kahe lausemuutuja juhule.

Näide 5. Näidata, et valem $\neg(A \lor B) \,\&\, \neg(\neg A \lor \neg B)$ on samaselt väär.

Koostame tõeväärtustabeli

		2	1	7	6	3	5	4
A	B	$\neg($	$A \lor B)$	$\&$	$\neg($	$\neg A$	$\lor$	$\neg B)$
1	1	0	1	0	1	0	0	0
1	0	0	1	0	0	0	1	1
0	1	0	1	0	0	1	1	0
0	0	1	0	0	0	1	1	1

Et antud valemi tõeväärtuste veerus esinevad ainult väärad väärtused, siis on valem samaselt väär.

Kui kaks valemit ei ole neis esinevate lausemuutujate ühelgi väärtustusel korraga tõesed, siis nimetatakse neid valemeid *vasturääkivateks.* Näite 5 põhjal võime öelda, et valemid $\neg(A \lor B)$ ja $\neg(\neg A \lor \neg B)$ on vasturääkivad. Analoogiliselt mõistetakse vasturääkivust kolme, nelja ja enama valemi puhul: valemite konjunktsioon on alati väär.

Vaatleme veel ühte valemiklassi.

Definitsioon 4. *Lausearvutuse valemit $\mathcal{F}$ nimetatakse kehtestatavaks, kui ta on vähemalt ühel väärtustusel tõene.*

Näiteks valem $A \,\&\, \neg B$ on kehtestatav, sest tema tõeväärtuste veerus esineb 1. Otse definitsioonist järeldub, et iga samaselt tõene valem on kehtestatav, sest selline valem on samuti vähemalt ühel väärtustusel tõene.

Sissetoodud valemiklasside vahel kehtivad järgmised seosed.

Teoreem 1. *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt väär.*

Tõestus. Andes valemis $\mathcal{F}$ esinevatele lausemuutujatele suvalise väärtustuse, näeme, et valemite $\mathcal{F}$ ja $\neg\mathcal{F}$ tõeväärtused on vastupidised. Järelikult kui $\mathcal{F}$ on igal väärtustusel tõene, siis $\neg\mathcal{F}$ on igal väärtustusel väär ja ümberpöördult. □

Teoreem 2. *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eitus $\neg\mathcal{F}$ ei ole samaselt tõene.*

Tõestus. Kui $\mathcal{F}$ on kehtestatav, siis väärtustusel, kus $\mathcal{F}$ on tõene, on valem $\neg\mathcal{F}$ väär ja ei saa seetõttu olla samaselt tõene. Ümberpöördult, kui $\neg\mathcal{F}$ ei ole samaselt tõene, siis leidub väärtustus, kus $\neg\mathcal{F}$ on väär ja $\mathcal{F}$ järelikult tõene. □

Nende omaduste valguses võib valemiklasside struktuuri kujutada järgmise joonisega:

Üleminek valemilt $\mathcal{F}$ valemile $\neg\mathcal{F}$ tähendab peegeldamist keskristsirge suhtes: samaselt tõene valem teiseneb samaselt vääraks valemiks, kehtestatav valem aga valemiks, mis ei ole samaselt tõene.

Mõnikord defineeritakse eraldi ka *kummutatav valem*, mis on vähemalt ühel väärtustusel väär, ja *kontingentne valem*, mis on vähemalt ühel väärtustusel tõene ja vähemalt ühel väärtustusel väär.

Valemi omaduste tuvastamisel tuleb tüüpiliselt otsustada, kas leidub väärtustus, millel valem on tõene, või väärtustus, millel valem on väär. Alati saab seda küsimust lahendada tõeväärtustabeliga, kuid mõnikord võib kiiremini sihile jõuda valemi struktuuri analüüsides. Näiteks kui on vaja kindlaks teha, kas etteantud valem saab olla mingil väärtustusel tõene, siis uurime kõigepealt, millised peavad olema valemi peatehte poolte tõeväärtused, et valem oleks tõene, seejärel püüame leida väiksemate komponentide tõeväärtused, siis omakorda veel väiksemate omad jne, liikudes valemi struktuuris järk-järgult üha sügavamale. Kui sellise analüüsi käigus satume alati vastuolule, siis valem ühelgi väärtustusel tõene ei ole ning on järelikult samaselt väär. Kui aga jõuame ilma vastuolu kohtamata välja lausemuutujateni, siis saame kätte väärtustuse, millel valem on tõene.

Olukorrast parema ülevaate saamiseks ja analüüsi käigus tekkivate variantide süstematiseerimiseks võib kasutada erilist skeemi, mida nimetatakse *tõesuspuuks*. Puu tipuks on uuritav valem koos kontrollitava tõeväärtusega. Kui oleme kindlaks teinud valemi mingi osa tõeväärtuse, siis kirjutame tulemuse valemi alla, selle alla omakorda valemi osa analüüsimisel saadud tulemuse jne. Kui osutub, et mingil sammul on valemi osadel mitu sobivat varianti tõeväärtusi, siis jaguneb analüüs sellel sammul harudeks, mida jätkatakse üksteisest sõltumatult.

Järgmises tabelis on toodud lausearvutuse tehete analüüsimise elementaarsammud.

- Eitus:

$$\begin{array}{c} \neg\mathcal{F}=1 \\ | \\ \mathcal{F}=0 \end{array} \qquad \begin{array}{c} \neg\mathcal{F}=0 \\ | \\ \mathcal{F}=1 \end{array}$$

- Konjunktsioon ja disjunktsioon:

$$\begin{array}{c} \mathcal{F}\,\&\,\mathcal{G}=1 \\ | \\ \mathcal{F}=1 \\ | \\ \mathcal{G}=1 \end{array} \qquad \begin{array}{ccc} & \mathcal{F}\,\&\,\mathcal{G}=0 & \\ \diagup & & \diagdown \\ \mathcal{F}=0 & & \mathcal{G}=0 \end{array} \qquad \begin{array}{ccc} & \mathcal{F}\vee\mathcal{G}=1 & \\ \diagup & & \diagdown \\ \mathcal{F}=1 & & \mathcal{G}=1 \end{array} \qquad \begin{array}{c} \mathcal{F}\vee\mathcal{G}=0 \\ | \\ \mathcal{F}=0 \\ | \\ \mathcal{G}=0 \end{array}$$

- Implikatsioon ja ekvivalents:

$$\begin{array}{ccc} & \mathcal{F}\to\mathcal{G}=1 & \\ \diagup & & \diagdown \\ \mathcal{F}=0 & & \mathcal{G}=1 \end{array} \qquad \begin{array}{c} \mathcal{F}\to\mathcal{G}=0 \\ | \\ \mathcal{F}=1 \\ | \\ \mathcal{G}=0 \end{array} \qquad \begin{array}{ccc} & \mathcal{F}\leftrightarrow\mathcal{G}=1 & \\ \diagup & & \diagdown \\ \mathcal{F}=1 & & \mathcal{F}=0 \\ | & & | \\ \mathcal{G}=1 & & \mathcal{G}=0 \end{array} \qquad \begin{array}{ccc} & \mathcal{F}\leftrightarrow\mathcal{G}=0 & \\ \diagup & & \diagdown \\ \mathcal{F}=1 & & \mathcal{F}=0 \\ | & & | \\ \mathcal{G}=0 & & \mathcal{G}=1 \end{array}$$

Nende reeglite abil jagame uuritava valemi järk-järgult väiksemateks osadeks. Kui oleme mingi komponendi tõeväärtusest tulenevad järeldused kirja pannud, siis märgistame selle komponendi tärniga, mis tähendab, et tema analüüs on lõppenud. Hargnemisega reegli puhul jaguneb analüüs kaheks haruks. Valemi lahutamist jätkame kuni kõige väiksemate komponentideni — lausemuutujateni. Kui puu mingis harus on kõik valemid tükeldatud lausemuutujateks, siis nimetatakse seda haru *lõpetatuks*. Võib juhtuda, et mingi valem esineb harus nii tõesena kui ka väärana, sel juhul oleme komponentideks lahutamise käigus sattunud vastuolule. Niisugust haru nimetatakse *vastuoluliseks* või *suletuks* ja tema alla kirjutatakse märk $\times$. Haru, milles vastuolu ei ole, nimetatakse *avatuks*. Tõesuspuu on valmis, kui iga tema haru on lõpetatud või vastuoluline.

Näide 6. Teha kindlaks, kas valem $\neg(A\to B)\vee\neg(B\to A)$ saab olla mingil väärtustusel väär.

Koostame tõesuspuu tingimusest $\neg(A\to B)\vee\neg(B\to A)=0$ lähtudes. Disjunktsiooni reeglite kohaselt peab olema $\neg(A\to B)=0$ ja $\neg(B\to A)=0$. Sellega oleme puu tipus asuva tingimuse osadeks lahutanud ning me võime ta tähistada tärniga. Saadud seostest esimene annab $A\to B=1$ ning teine $B\to A=1$. Vaatleme nüüd tingimust

$A \to B = 1$. Vastavalt implikatsiooni reeglile jaguneb puu siinkohal kaheks haruks: $A = 0$ ja $B = 1$. Tingimus $B \to A = 1$ kandub mõlemasse harusse. Et harusid pikendatakse üksteisest sõltumatult, siis tuleb see tingimus komponentideks lahutada kummaski harus eraldi. Sellega tekib joonisel näidatud tõesuspuu:

$$
\begin{array}{c}
\neg(A \to B) \vee \neg(B \to A) = 0 \quad \star \\
| \\
\neg(A \to B) = 0 \quad \star \\
| \\
\neg(B \to A) = 0 \quad \star \\
| \\
A \to B = 1 \quad \star \\
| \\
B \to A = 1 \quad \star \\
\swarrow \qquad \searrow \\
\begin{array}{cc}
A = 0 & B = 1 \\
\begin{array}{cc} \swarrow & \searrow \\ B = 0 & A = 1 \\ & \times \end{array} & \begin{array}{cc} \swarrow & \searrow \\ B = 0 & A = 1 \\ \times & \end{array}
\end{array}
\end{array}
$$

Kaks keskmist haru on vastuolulised, sest üks neist sisaldab vastuolulisi tingimusi lausemuutuja A, teine lausemuutuja B kohta. Ülejäänud kaks haru on lõpetatud, ent mitte vastuolulised. Nendest saame väärtustused, millel valem on väär: $A = 0$, $B = 0$ ja $A = 1$, $B = 1$.

Näide 7. Näidata, et valem $\neg B \& \neg(\neg C \to \neg B \vee A)$ on samaselt väär.

Püüame leida väärtustust, millel see valem on tõene. Koostame alljärgneva tõesuspuu, kus numbritega on tähistatud osavalemite käsitlemise järjekord.

$$
\begin{array}{c}
\neg B \,\&\, \neg(\neg C \to \neg B \vee A) = 1 \quad (1) \; \star \\
| \\
\neg B = 1 \\
| \\
\neg(\neg C \to \neg B \vee A) = 1 \quad (2) \; \star \\
| \\
\neg C \to \neg B \vee A = 0 \quad (3) \; \star \\
| \\
\neg C = 1 \\
| \\
\neg B \vee A = 0 \quad (4) \; \star \\
| \\
\neg B = 0 \\
| \\
A = 0 \\
\times
\end{array}
$$

Tõesuspuu ainus haru on vastuoluline, sest ta sisaldab vastuolulisi tingimusi $\neg B = 1$ ja $\neg B = 0$, seega pole võimalik, et valem on mingil väärtustusel tõene. See tähendab, valem on tõepoolest samaselt väär.

Märgatava eelise tõeväärtustabeli ees annab tõesuspuu siis, kui valemi komponentideks lahutamisel tekib vähe hargnemisi. Ka üldiselt on analüüsi mahu mõttes tihtipeale kasulikum lahutada valemeid osadeks nii, et hargnemist tekitavaid reegleid rakendatakse alles viimases järjekorras, kui muid reegleid enam kasutada ei saa.

Näide 8. Näidata, et valem $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ on samaselt tõene.

Püüame leida väärtustust, millel valem on väär:

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) = 0 \qquad (1)\ \star$$
$$A \to (B \to C) = 1 \qquad (5)\ \star$$
$$(A \to B) \to (A \to C) = 0 \qquad (2)\ \star$$
$$A \to B = 1 \qquad (4)\ \star$$
$$A \to C = 0 \qquad (3)\ \star$$
$$A = 1$$
$$C = 0$$
$$\begin{array}{cccc}
A = 0 & B = 1 & & \\
\times & A = 0 & B \to C = 1 \quad (6)\ \star & \\
 & \times & B = 0 & C = 1 \\
 & & \times & \times
\end{array}$$

Et tõesuspuu kõik harud viivad vastuolule, siis ei leidu väärtustust, millel valem oleks väär, ehk teisiti öeldes, valem on samaselt tõene.

§ 3. Järeldumine

Uurime küsimust, millal on lausearvutuse valem tõene, kui mingite teiste lausearvutuse valemite tõesus on teada.

Definitsioon 5. *Ütleme, et valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, kui igal neis valemeis esinevate muutujate väärtustusel, millel $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{G}$ tõene.*

Asjaolu, et valemitest $\mathcal{F}_1$, $\mathcal{F}_2$, ..., $\mathcal{F}_n$ järeldub valem $\mathcal{G}$, tähistatakse kirjutisega

$$\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \models \mathcal{G}.$$

Järeldumist saab kindlaks teha tõeväärtustabeli abil. Valime tõeväärtustabelist välja read, milles valemid $\mathcal{F}_1$, $\mathcal{F}_2$, ..., $\mathcal{F}_n$ on kõik tõesed, ja selgitame, kas nendes ridades on ka valem $\mathcal{G}$ tõene. Kui on, siis järeldumine kehtib; kui aga leidub rida, milles valemid $\mathcal{F}_1$, $\mathcal{F}_2$, ..., $\mathcal{F}_n$ on tõesed, kuid valem $\mathcal{G}$ on väär, siis oleme leidnud väärtustuse, mis väidetava järeldumise ümber lükkab.

Näide 9. Teha kindlaks, kas valemitest $\neg(A \& B)$ ja $B \to A$ järeldub valem $\neg B$.

Koostame tõeväärtustabeli

A	B	$\neg(A \& B)$		$B \to A$	$\neg B$
1	1	0	1	1	0
1	0	1	0	1	1
0	1	1	0	0	0
0	0	1	0	1	1

Kaks esimest valemit on mõlemad tõesed ainult teises ja neljandas reas. Et ka kolmas valem on nendes ridades tõene, siis järeldumine kehtib ehk

$$\neg(A \& B), B \to A \models \neg B.$$

Näide 10. Tõestada, et valemitest $A \to B$ ja $B \to C$ järeldub valem $A \to C$.

Oletame, et mingil väärtustusel on eeldused tõesed ja väide väär. See tähendab, $A \to B = 1$ ja $B \to C = 1$, kuid $A \to C = 0$. Viimasest võrdusest saame $A = 1$ ja $C = 0$. Edasi esimesest võrdusest $B = 1$, kuid teine võrdus ei saa nüüd enam kehtida.

Näide 11. Olgu antud lausemuutujad, mille tähendus on järgmine: A = „Kiiruste liitmisseadus kehtib“, B = „Valgus liigub kinnistähtedega seotud taustsüsteemis kõigis suundades sama kiirusega“ ning C = „Valgus liigub Maal kõigis suundades sama kiirusega“.

Kehtib valem $A \& B \to \neg C$ ehk tekstikujul „Kui kiiruste liitmisseadus kehtib ja valgus liigub kinnistähtedega seotud taustsüsteemis kõigis suundades sama kiirusega, siis pole Maal valguse liikumiskiirus kõigis suundades sama“, sest Maa ilmselt liigub kinnistähtedega seotud taustsüsteemi suhtes. Peale selle kehtib valem B, sest see on Einsteini relatiivsusteooria põhipostulaate, ja valem C, sest see järeldub Michelson-Morley katsest (1887). Vaatleme niisiis kolme valemit

$$A \& B \to \neg C, \quad B, \quad C.$$

Eeldame, et need kõik on tõesed. Esimeses valemis peab siis osavalem $A \& B$ olema väär. Et B on tõene, siis peab A olema väär ja $\neg A$ tõene. Sellega oleme näidanud, et toodud kolmest valemist järeldub valem $\neg A$ ehk sõnades „Kiiruste liitmisseadus ei kehti“.

Teine võimalus järeldumist kindlaks teha on kasutada alljärgnevat teoreemi, mis taandab järeldumise kontrollimise üheainsa valemi samaselt tõesuse kontrollimisele. Niisugust lähenemist kasutatakse eriti siis, kui valemit analüüsitakse arvutil, sest lausearvutuse standardülesannete, nagu samaselt tõesuse kontroll, lahendamiseks on koostatud hulgaliselt tavalisi ja heuristilisi efektiivseid algoritme.

Teoreem 3. *Valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$ parajasti siis, kui valem $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \to \mathcal{G}$ on samaselt tõene.*

Tõestus. Kui valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, siis neil väärtustustel, millel valemid $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene, mistõttu $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \to \mathcal{G}$ on tõene. Väärtustustel, millel mõni valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ on väär, on valem $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \to \mathcal{G}$ tõene seetõttu, et implikatsiooni eesliige on väär.

Ümberpöördult, kui valem $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \to \mathcal{G}$ on samaselt tõene, siis igal väärtustusel, millel valemid $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n$ tõene, mistõttu valem $\mathcal{G}$ on samuti tõene. □

Vastavalt sellele teoreemile tuleb näites 9 anda samaselt tõesuse kontrollijale ette valem $\neg(A \& B) \& (B \to A) \to \neg B$ ning näites 10 valem $(A \to B) \& (B \to C) \to (A \to C)$.

Järeldumise kindlakstegemiseks on võimalik kasutada ka tõesuspuid, näiteks kontrollides teoreemis antud kujuga valemi samaselt tõesust või võttes aluseks otse järeldumise definitsiooni.

§ 4. Samaväärsus

Koostades valemite $\neg(A \& B)$ ja $\neg A \vee \neg B$ tõeväärtustabelid, näeme, et valemite tõeväärtusveerud langevad kokku:

A	B	$\neg$	$(A \& B)$	$\neg A$	$\vee$	$\neg B$
1	1	0	1	0	0	0
1	0	1	0	0	1	1
0	1	1	0	1	1	0
0	0	1	0	1	1	1

Igapäevase keele abil on lihtne veenduda, et need valemid väljendavad ühte ja sama: esimene valem tähendab „Pole nii, et laused A ja

B on mõlemad tõesed“ ning teine valem „Vähemalt üks lausetest A ja B on väär“. Ühesuguse tõeväärtusveeruga valemeid ei ole võimalik sisu järgi teineteisest eristada, ehkki neil võib olla erinev väliskuju. Niisugustest kaalutlustest lähtudes anname järgmise definitsiooni.

Definitsioon 6. *Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse samaväärseteks, kui nende tõeväärtused on võrdsed igal neis valemeis esinevate muutujate väärtustusel.*

Asjaolu, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed, märgib kirjutis

$$\mathcal{F} \equiv \mathcal{G}.$$

Samaväärsed võivad olla ka erinevaid muutujaid sisaldavad valemid, nagu näiteks $(B \to A)\&(\neg B \to A)$ ja $(A \vee C)\&(A \vee \neg C)$. Kõik samaselt tõesed valemid on üksteisega samaväärsed, sest sellised valemid on igal väärtustusel tõesed. Analoogilisel põhjusel on omavahel samaväärsed kõik samaselt väärad valemid.

Kui $\mathcal{F} \equiv \mathcal{G}$, siis suvalisel valemites $\mathcal{F}$ ja $\mathcal{G}$ esinevate lausemuutujate väärtustusel on need valemid kas mõlemad tõesed või mõlemad väärad. Seepärast kehtivad seosed $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$. Ümberpöördult, kui viimased seosed kehtivad, siis ei saa leiduda väärtustust, kus $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused oleksid erinevad, mistõttu $\mathcal{F} \equiv \mathcal{G}$. Seega, *valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ ja valemist $\mathcal{G}$ järeldub valem $\mathcal{F}$*. Niisugust omadust kasutatakse tihti valemite samaväärsuse tõestamisel.

Kahe valemi samaväärsuse kontrolli saab samuti taandada teatava ühe valemi samaselt tõesuse kontrollile, nii nagu nägime järeldumise puhul.

Teoreem 4. *Valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valem $\mathcal{F} \leftrightarrow \mathcal{G}$ on samaselt tõene.*

Tõestus. Eeldame, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed. Valime valemites $\mathcal{F}$ ja $\mathcal{G}$ esinevatele muutujatele suvalise väärtustuse. Kui valitud väärtustusel kehtib $\mathcal{F} = 1$ ja $\mathcal{G} = 1$, siis $\mathcal{F} \leftrightarrow \mathcal{G} = 1$, kui aga valitud väärtustusel kehtib $\mathcal{F} = 0$ ja $\mathcal{G} = 0$, siis samuti $\mathcal{F} \leftrightarrow \mathcal{G} = 1$. Järelikult on valem $\mathcal{F} \leftrightarrow \mathcal{G}$ tõene sõltumata väärtustusest ehk samaselt tõene.

Eeldame nüüd ümberpöördult, et valem $\mathcal{F} \leftrightarrow \mathcal{G}$ on samaselt tõene. Valime selles valemis esinevatele muutujatele suvalise väärtustuse. Et ekvivalents on tõene, siis kas $\mathcal{F} = 1$, $\mathcal{G} = 1$ või $\mathcal{F} = 0$, $\mathcal{G} = 0$. See tähendab, valemite $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused on suvalisel väärtustusel samad. Vastavalt definitsioonile on valemid $\mathcal{F}$ ja $\mathcal{G}$ samaväärsed. □

On olemas hulk *lausearvutuse põhisamaväärsusi*, mida kasutatakse lausearvutuses teistest rohkem. Tähtsamad neist on järgmised.

1) Idempotentsuse seadused:

$$\mathcal{F} \,\&\, \mathcal{F} \equiv \mathcal{F}, \qquad \mathcal{F} \vee \mathcal{F} \equiv \mathcal{F}.$$

2) Kommutatiivsuse seadused:

$$\mathcal{F} \,\&\, \mathcal{G} \equiv \mathcal{G} \,\&\, \mathcal{F}, \qquad \mathcal{F} \vee \mathcal{G} \equiv \mathcal{G} \vee \mathcal{F}.$$

3) Assotsiatiivsuse seadused:

$$(\mathcal{F} \,\&\, \mathcal{G}) \,\&\, \mathcal{H} \equiv \mathcal{F} \,\&\, (\mathcal{G} \,\&\, \mathcal{H}), \quad (\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H} \equiv \mathcal{F} \vee (\mathcal{G} \vee \mathcal{H}).$$

4) Distributiivsuse seadused:

$$\mathcal{F} \,\&\, (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \,\&\, \mathcal{G} \vee \mathcal{F} \,\&\, \mathcal{H},$$
$$\mathcal{F} \vee \mathcal{G} \,\&\, \mathcal{H} \equiv (\mathcal{F} \vee \mathcal{G}) \,\&\, (\mathcal{F} \vee \mathcal{H}).$$

5) Neelamisseadused:

$$\mathcal{F} \,\&\, (\mathcal{F} \vee \mathcal{G}) \equiv \mathcal{F}, \qquad \mathcal{F} \vee \mathcal{F} \,\&\, \mathcal{G} \equiv \mathcal{F}.$$

6) De Morgani seadused:

$$\neg(\mathcal{F} \,\&\, \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}, \qquad \neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \,\&\, \neg\mathcal{G}.$$

7) Kahekordse eituse seadus:

$$\neg\neg\mathcal{F} \equiv \mathcal{F}.$$

8) Liikmete elimineerimise reeglid, kus $\mathcal{T}$ on suvaline samaselt tõene valem ja $\mathcal{V}$ on suvaline samaselt väär valem:

$$\mathcal{F} \,\&\, \mathcal{T} \equiv \mathcal{F}, \qquad \mathcal{F} \vee \mathcal{T} \equiv \mathcal{T},$$
$$\mathcal{F} \,\&\, \mathcal{V} \equiv \mathcal{V}, \qquad \mathcal{F} \vee \mathcal{V} \equiv \mathcal{F}.$$

9) Implikatsiooni avaldis konjunktsiooni ja disjunktsiooni kaudu:

$$\mathcal{F} \to \mathcal{G} \equiv \neg(\mathcal{F} \,\&\, \neg\mathcal{G}), \qquad \mathcal{F} \to \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}.$$

10) Konjunktsiooni ja disjunktsiooni avaldis implikatsiooni kaudu:

$$\mathcal{F} \,\&\, \mathcal{G} \equiv \neg(\mathcal{F} \to \neg\mathcal{G}), \qquad \mathcal{F} \vee \mathcal{G} \equiv \neg\mathcal{F} \to \mathcal{G}.$$

11) Ekvivalentsi avaldis teiste tehete kaudu:

$$\mathcal{F} \leftrightarrow \mathcal{G} \equiv \mathcal{F} \,\&\, \mathcal{G} \vee \neg\mathcal{F} \,\&\, \neg\mathcal{G}, \quad \mathcal{F} \leftrightarrow \mathcal{G} \equiv (\mathcal{F} \to \mathcal{G}) \,\&\, (\mathcal{G} \to \mathcal{F}).$$

Kõiki neid samaväärsusi saab kontrollida tõeväärtustabeli abil. Kuid nende kehtivust võib tõestada ka otsese arutlemise teel. Tõestame näiteks esimese distributiivsuse seaduse.

Kui $\mathcal{F} \,\&\, (\mathcal{G} \vee \mathcal{H}) = 1$, siis $\mathcal{F} = 1$ ja $\mathcal{G} \vee \mathcal{H} = 1$. Kui viimases seoses $\mathcal{G} = 1$, siis $\mathcal{F} \,\&\, \mathcal{G} = 1$. Kui aga $\mathcal{H} = 1$, siis $\mathcal{F} \,\&\, \mathcal{H} = 1$.

Mõlemal juhul on parempoolne valem tõene. Ümberpöördult, olgu $\mathcal{F} \,\&\, \mathcal{G} \vee \mathcal{F} \,\&\, \mathcal{H} = 1$. Kui $\mathcal{F} \,\&\, \mathcal{G} = 1$, siis $\mathcal{F} = 1$, $\mathcal{G} = 1$, millest $\mathcal{F} = 1$, $\mathcal{G} \vee \mathcal{H} = 1$. Seetõttu on vasakpoolne valem tõene. Kui aga $\mathcal{F} \,\&\, \mathcal{H} = 1$, siis $\mathcal{F} = 1$, $\mathcal{H} = 1$, millest $\mathcal{F} = 1$, $\mathcal{G} \vee \mathcal{H} = 1$. Ka sel juhul on vasakpoolne valem tõene. Niisiis oleme näidanud, et vasakpoolsest valemist järeldub parempoolne ning parempoolest vasakpoolne. See tähendab, et need valemid on samaväärsed.

Samaväärsused etendavad lausearvutuses sarnast osa nagu samasused algebras. Nii nagu algebras kasutatakse samasusi avaldiste lihtsustamiseks, nii võib ka lausearvutuse valemeid teisendada ja lihtsustada lausearvutuse samaväärsustega, kusjuures tekkiv valem jääb igal sammul samaväärseks esialgsega. Üks teisendussamm tähendab valemi enda või tema osavalemi asendamist teise, samaväärse valemiga. Kui asendame valemis $\mathcal{F}$ mingi osavalemi $\mathcal{F}_1$ samaväärse valemiga $\mathcal{F}_2$, siis on tulemuseks saadav valem ja valem $\mathcal{F}$ igal väärtustusel ühesuguse tõeväärtusega, sest uus osavalem $\mathcal{F}_2$ annab igal väärtustusel sama tõeväärtuse nagu osavalem $\mathcal{F}_1$, edasised tehted valemi tõeväärtuse arvutamisel tehakse juba ühtemoodi.

Tavaliselt on lihtsustamisel otstarbekas elimineerida kõik tehted peale eituse, konjunktsiooni ja disjunktsiooni, sest nende tehete vahel kehtivad kõige lihtsamad seosed. Mõnikord on parem enne tehete elimineerimist lihtsustada antud valemi mingit osavalemit.

Näide 12. Lihtsustada valem $\neg A \vee B \to A \,\&\, B$.

Tähistame

$$\mathcal{F} = \neg A \vee B \to A \,\&\, B.$$

Avaldades vaadeldavas valemis implikatsiooni eituse ja disjunktsiooni kaudu, saame

$$\mathcal{F} \equiv \neg(\neg A \vee B) \vee A \,\&\, B.$$

De Morgani seaduse abil viime eituse sulgude sisse:

$$\mathcal{F} \equiv \neg\neg A \,\&\, \neg B \vee A \,\&\, B.$$

Kahekordse eituse võime ära jätta:

$$\mathcal{F} \equiv A \,\&\, \neg B \vee A \,\&\, B.$$

Nüüd võime rakendada distributiivsuse seadust ja tuua ühise teguri sulgude ette:

$$\mathcal{F} \equiv A \,\&\, (\neg B \vee B).$$

Viimases valemis on liige $\neg B \vee B$ samaselt tõene ning me võime ta liikmete elimineerimise reegli põhjal välja jätta. Kokkuvõttes saame

$$\mathcal{F} \equiv A.$$

§ 5. Normaalkujud

Normaalkuju mõte on kahandada lausearvutuse valemite süntaktilist mitmekesisust, andes neile lihtsa väliskujuga ühtse vormi. Normaalkujusid kasutatakse teoreetilistes arutlustes näiteks tõestamaks, et mingi väide kehtib kõigi lausearvutuse valemite kohta, ning samuti praktikas, kui on vaja näiteks välja kirjutada valem, millel on teatavad iseloomulikud omadused.

Lausemuutujat või selle eitust nimetame *literaaliks*. Näiteks on A, B, C, D, $\neg A$, $\neg B$, $\neg C$, $\neg D$ literaalid. Literaali loetakse *positiivseks* või *negatiivseks* vastavalt sellele, kas ta on puhas lausemuutuja või koos eitusega. Ülaltoodud literaalidest on esimesed neli positiivsed ja viimased neli negatiivsed.

Ühest lausemuutujast saab seega moodustada kaks literaali. Olgu meil nüüd vaatluse all komplekt lausemuutujaid $A_1, A_2, \ldots, A_n$, milleks võib olla näiteks ühe valemi kõigi muutujate hulk. Lisades vajaduse järgi eitusi, moodustame neist literaalid $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$ (igast muutujast ühe) ning koostame valemi

$$\mathcal{L}_1 \,\&\, \mathcal{L}_2 \,\&\, \ldots \,\&\, \mathcal{L}_n.$$

Sellist valemit nimetatakse *täielikuks elementaarkonjunktsiooniks.*

Definitsioon 7. *Lausearvutuse valemi $\mathcal{F}$ täielikuks disjunktiivseks normaalkujuks (TDNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate täielike elementaarkonjunktsioonide disjunktsiooni.*

Normaalkujusse kuuluvaid täielikke elementaarkonjunktsioone nimetatakse ka selle normaalkuju *liikmeteks.*

Olgu meie käsutuses neli lausemuutujat A, B, C, D. Siis võime moodustada näiteks järgmised täielikud elementaarkonjunktsioonid

$$A \,\&\, B \,\&\, C \,\&\, D, \qquad A \,\&\, \neg B \,\&\, \neg C \,\&\, \neg D, \qquad \neg A \,\&\, B \,\&\, \neg C \,\&\, D.$$

Üks täielikul disjunktiivsel normaalkujul olev valem on näiteks

$$A \,\&\, B \,\&\, C \,\&\, D \vee A \,\&\, \neg B \,\&\, \neg C \,\&\, \neg D \vee \neg A \,\&\, B \,\&\, \neg C \,\&\, D.$$

Definitsiooni kohaselt peavad normaalkuju liikmed olema üksteisest erinevad, see tähendab, koosnema erinevatest literaalikomplektidest. Täielikke elementaarkonjunktsioone, mida on võimalik üksteisest saada literaalide järjekorda vahetades, loeme samadeks — nagu näiteks $A \,\&\, \neg B \,\&\, C \,\&\, D$ ja $C \,\&\, D \,\&\, A \,\&\, \neg B$.

Sarnaselt täieliku elementaarkonjunktsiooniga defineeritakse ka *täielik elementaardisjunktsioon*, mis on literaalidest $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$

koostatud valem

$$\mathcal{L}_1 \vee \mathcal{L}_2 \vee \ldots \vee \mathcal{L}_n.$$

Valemi $\mathcal{F}$ *täielikuks konjunktiivseks normaalkujuks* (TKNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate täielike elementaardisjunktsioonide konjunktsiooni.

Samast neljast muutujast võime koostada näiteks täielikud elementaardisjunktsioonid

$$A \vee B \vee C \vee D, \qquad A \vee \neg B \vee \neg C \vee \neg D, \qquad \neg A \vee B \vee \neg C \vee D$$

ning täielikul konjunktiivsel normaalkujul oleva valemi

$$(A \vee B \vee C \vee D) \,\&\, (A \vee \neg B \vee \neg C \vee \neg D) \,\&\, (\neg A \vee B \vee \neg C \vee D).$$

Võtame nüüd käsile normaalkujude tõesuse küsimuse. Täieliku normaalkuju hea omadus ja põhjus, miks teda üldse kasutatakse, seisneb selles, et tema puhul saab kergesti kindlaks teha, millistel väärtustustel on ta tõene ja millistel väärtustustel väär.

Vaatleme näiteks järgmist täielikul disjunktiivsel normaalkujul esitatud valemit:

$$A \,\&\, \neg B \,\&\, \neg C \,\&\, D \vee A \,\&\, B \,\&\, C \,\&\, \neg D.$$

Pidades silmas esimest liiget, valime väärtustuse $A = 1$, $B = 0$, $C = 0$, $D = 1$. Sellel väärtustusel on valem tõene, sest esimeses liikmes on kõik literaalid tõesed ning järelikult on tõene kogu liige. Valemi teise liikme järgi valime väärtustuse $A = 1$, $B = 1$, $C = 1$, $D = 0$. Ka sellel väärtustusel on valem tõene. Kui aga võtame väärtustuse, mis erineb neist kahest, näiteks väärtustuse $A = 1$, $B = 1$, $C = 0$, $D = 1$, siis on kummaski liikmes vähemalt üks literaal väär.

Üldiselt, suvalise täieliku disjunktiivse normaalkuju lausemuutujatest $A_1, A_2, \ldots, A_n$ võib kirja panna kujul

$$A_1^{\alpha_{11}} \,\&\, A_2^{\alpha_{12}} \,\&\ldots\&\, A_n^{\alpha_{1n}} \vee A_1^{\alpha_{21}} \,\&\, A_2^{\alpha_{22}} \,\&\ldots\&\, A_n^{\alpha_{2n}} \vee \ldots$$
$$\ldots \vee A_1^{\alpha_{m1}} \,\&\, A_2^{\alpha_{m2}} \,\&\ldots\&\, A_n^{\alpha_{mn}},$$

kus $(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n})$, $(\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2n})$, $\ldots$, $(\alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{mn})$ on teatavad tõeväärtuste järjendid pikkusega n, seejuures tähistab A_i^1 positiivset literaali A_i ning A_i^0 negatiivset literaali $\neg A_i$. Otsese kontrolliga võib veenduda, et $A_i^{\alpha_i} = 1$ parajasti siis, kui $A_i = \alpha_i$. Seetõttu on vaadeldava normaalkuju esimene liige tõene parajasti muutujate A_1, A_2, $\ldots$, A_n väärtustusel $(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n})$, teine liige väärtustusel $(\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2n})$ jne kuni viimane liige väärtustusel $(\alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{mn})$. Kõigil nendel väärtustustel on normaalkuju niisiis tõene. Kui aga valida muutujatele $A_1, A_2, \ldots, A_n$ selline väärtustus $(\beta_1, \beta_2, \ldots, \beta_n)$, mis ei lange kokku ühegi nimetatud väärtustusega, siis on normaalkuju kõik liikmed väärad, mistõttu normaalkuju on väär. Täielik disjunktiivne normaalkuju on seega tõene parajasti nendel väärtustustel, mis vastavad normaalkuju liikmetele.

Selline omadus annab võimaluse kirjutada valemiga samaväärne täielik disjunktiivne normaalkuju välja tõeväärtustabeli abil. Leiame tõeväärtustabelist kõik väärtustused, millel valem on tõene, ja moodustame iga sellise väärtustuse kohta ühe liikme, täieliku elementaarkonjunktsiooni. Väärtustusel tõesed lausemuutujad lähevad vastavasse liikmesse positiivse literaalina, väärad aga negatiivsena. Lõpuks ühendame kõik tekkinud liikmed disjunktsioonidega.

Näide 13. Leida valemi

$$\neg B \leftrightarrow \neg A \vee \neg B \to C \,\&\, A$$

täielik disjunktiivne normaalkuju.

Valemi viimiseks täielikule disjunktiivsele normaalkujule koostame tõeväärtustabeli

A	B	C	$\neg B$	$\leftrightarrow$	$\neg A$	$\vee$	$\neg B$	$\to$	$C \,\&\, A$
1	1	1	0	0	0	0	0	1	1
1	1	0	0	0	0	0	0	1	0
1	0	1	1	1	0	1	1	1	1
1	0	0	1	0	0	1	1	0	0
0	1	1	0	1	1	1	0	0	0
0	1	0	0	1	1	1	0	0	0
0	0	1	1	0	1	1	1	0	0
0	0	0	1	0	1	1	1	0	0

Valemi tõeväärtused saame tabeli parempoolse osa teisest veerust. Tõeseid väärtustusi on kolm: $(1, 0, 1)$, $(0, 1, 1)$ ja $(0, 1, 0)$. Valemi täielik disjunktiivne normaalkuju on järelikult

$$A \,\&\, \neg B \,\&\, C \vee \neg A \,\&\, B \,\&\, C \vee \neg A \,\&\, B \,\&\, \neg C.$$

Kirjeldatud meetodit ei saa rakendada juhul, kui valem on samaselt väär. Samaselt vääral valemil ei leidugi täielikku disjunktiivset normaalkuju, sest viimane peab olema alati mingil väärtustusel tõene (mõnikord loetakse küll ühtsuse mõttes, et samaselt väära valemi täielik disjunktiivne normaalkuju on tühi valem, mis ei sisalda ühtegi liiget). Kokkuvõttes oleme saanud järgmise tulemuse.

Teoreem 5. *Kui valem $\mathcal{F}$ ei ole samaselt väär, siis tal leidub täielik disjunktiivne normaalkuju.*

Järeldus 1. *Kui valem $\mathcal{F}$ ei ole samaselt tõene, siis tal leidub täielik konjunktiivne normaalkuju.*

Tõestus. Et valem $\neg\mathcal{F}$ ei ole samaselt väär, siis leidub tal täielik disjunktiivne normaalkuju, mis literaalide kaudu avaldatult on

$$\neg\mathcal{F} \equiv \mathcal{L}_{11} \,\&\, \mathcal{L}_{12} \,\&\ldots\&\, \mathcal{L}_{1n} \vee \mathcal{L}_{21} \,\&\, \mathcal{L}_{22} \,\&\ldots\&\, \mathcal{L}_{2n} \vee \ldots \\ \ldots \vee \mathcal{L}_{m1} \,\&\, \mathcal{L}_{m2} \,\&\ldots\&\, \mathcal{L}_{mn}.$$

Leiame mõlemast poolest eituse, seejärel viime paremal eituse sissepoole De Morgani seaduste abil. Nii saame

$$\mathcal{F} \equiv (\neg\mathcal{L}_{11} \vee \neg\mathcal{L}_{12} \vee \ldots \vee \neg\mathcal{L}_{1n}) \,\&\, (\neg\mathcal{L}_{21} \vee \neg\mathcal{L}_{22} \vee \ldots \vee \neg\mathcal{L}_{2n}) \,\&\ldots \\ \ldots\&\, (\neg\mathcal{L}_{m1} \vee \neg\mathcal{L}_{m2} \vee \ldots \vee \neg\mathcal{L}_{mn}).$$

Paremal poolel võis lausemuutujate ette tekkida kahekordseid eitusi. Jättes need ära, ongi tulemuseks valemi $\mathcal{F}$ täielik konjunktiivne normaalkuju. □

Ka konjunktiivsete normaalkujude kohta kehtib eelnevaga analoogiline käsitlus. Suvaline täielik konjunktiivne normaalkuju lausemuutujatest $A_1, A_2, \ldots, A_n$ avaldub kujul

$$(A_1^{\alpha_{11}} \vee A_2^{\alpha_{12}} \vee \ldots \vee A_n^{\alpha_{1n}}) \,\&\, (A_1^{\alpha_{21}} \vee A_2^{\alpha_{22}} \vee \ldots \vee A_n^{\alpha_{2n}}) \,\&\ldots \\ \ldots\&\, (A_1^{\alpha_{m1}} \vee A_2^{\alpha_{m2}} \vee \ldots \vee A_n^{\alpha_{mn}}),$$

kus tähistused on samad nagu eespool. Arvestades, et $A_i^{\alpha_i} = 0$ parajasti siis, kui $A_i = \neg\alpha_i$ (kus $\neg\alpha_i$ tähistab siin tõeväärtuse α_i vastandväärtust), on vaadeldava normaalkuju esimene liige väär parajasti muutujate $A_1, A_2, \ldots, A_n$ väärtustusel $(\neg\alpha_{11}, \neg\alpha_{12}, \ldots, \neg\alpha_{1n})$, teine liige väärtustusel $(\neg\alpha_{21}, \neg\alpha_{22}, \ldots, \neg\alpha_{2n})$ jne kuni viimane liige väärtustusel $(\neg\alpha_{m1}, \neg\alpha_{m2}, \ldots, \neg\alpha_{mn})$. Kõigil nendel väärtustustel on normaalkuju väär, ülejäänud väärtustustel, mis nendest erinevad, on kõik liikmed tõesed, mistõttu normaalkuju on samuti tõene.

Antud valemiga samaväärse täieliku konjunktiivse normaalkuju väljakirjutamiseks otsime tõeväärtustabelist üles kõik väärtustused, millel valem on väär, ja moodustame iga väära väärtustuse kohta ühe liikme, täieliku elementaardisjunktsiooni. Väärtustusel väärad lausemuutujad lähevad vastavasse liikmesse positiivse literaalina, tõesed aga negatiivsena. Lõpuks ühendame liikmed konjunktsioonidega.

Näide 14. Leida näites 13 vaadeldud valemi täielik konjunktiivne normaalkuju.

Koostatud tõeväärtustabelist näeme, et valem on väär väärtustustel $(1,1,1)$, $(1,1,0)$, $(1,0,0)$, $(0,0,1)$, $(0,0,0)$, millele normaalkujus vastab viis liiget. Valemi täielik konjunktiivne normaalkuju on

$$(\neg A \vee \neg B \vee \neg C) \,\&\, (\neg A \vee \neg B \vee C) \,\&\, (\neg A \vee B \vee C) \,\&\\ \&\, (A \vee B \vee \neg C) \,\&\, (A \vee B \vee C).$$

Paneme tähele, et literaalide märgid on võrreldes väärtustustes esinevate tõeväärtustega vastupidised.

Eespool vaadeldud tabelimeetod täieliku normaalkuju leidmiseks pole otstarbekas või üldse võimalikki, kui valem sisaldab suure hulga lausemuutujaid. Sel juhul võib püüda valemit lausearvutuse samaväärsustega teisendada, seades eesmärgiks mitte täieliku, vaid üldise normaalkuju.

Olgu antud lausemuutujate hulk $A_1, A_2, \ldots, A_n$. Vaatleme literaale $\mathcal{L}_{i_1}, \mathcal{L}_{i_2}, \ldots, \mathcal{L}_{i_k}$, mis on saadud vastavalt lausemuutujatest $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, kusjuures $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$. Valemit $\mathcal{L}_{i_1} \,\&\, \mathcal{L}_{i_2} \,\&\ldots\&\, \mathcal{L}_{i_k}$ nimetatakse *elementaarkonjunktsiooniks* ehk lühidalt *konjunktiks*. Valemi $\mathcal{F}$ *disjunktiivseks normaalkujuks* (DNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate elementaarkonjunktsioonide disjunktsiooni. Analoogiliselt defineeritakse *elementaardisjunktsioon* ehk *disjunkt*, mis on valem kujul $\mathcal{L}_{i_1} \vee \mathcal{L}_{i_2} \vee \ldots \vee \mathcal{L}_{i_k}$, ja valemi $\mathcal{F}$ *konjunktiivne normaalkuju* (KNK), mis on valemiga $\mathcal{F}$ samaväärne erinevate elementaardisjunktsioonide konjunktsioon.

Vastupidiselt täielikule normaalkujule võib samal valemil olla mitu disjunktiivset ja mitu konjunktiivset normaalkuju. Näiteks valemi $\mathcal{F} = (A \leftrightarrow C) \rightarrow \neg A \,\&\, B$ disjunktiivseks normaalkujuks sobib nii

$$\mathcal{F} \equiv A \,\&\, \neg C \vee \neg A \,\&\, C \vee B \,\&\, \neg C$$

kui ka

$$\mathcal{F} \equiv A \,\&\, \neg C \vee \neg A \,\&\, B \vee \neg A \,\&\, C.$$

Suvaline disjunktiivne normaalkuju muutujatest $A_1, A_2, \ldots, A_n$ koosneb liikmetest üldkujuga

$$A_{i_1}^{\alpha_{i_1}} \,\&\, A_{i_2}^{\alpha_{i_2}} \,\&\ldots\&\, A_{i_k}^{\alpha_{i_k}}.$$

Niisugune liige on tõene vaadeldavate muutujate kõigil väärtustustel, kus $A_{i_1} = \alpha_{i_1}, A_{i_2} = \alpha_{i_2}, \ldots, A_{i_k} = \alpha_{i_k}$. Need tingimused fikseerivad k lausemuutuja väärtused, ülejäänud $n - k$ muutujat, nimelt need, mis selles liikmes ei esine, võivad omandada suvalisi väärtusi. Seega on vaadeldav liige tõene parajasti 2^{n-k} väärtustusel. Disjunktiivses normaalkujus võib üks väärtustus muuta tõeseks rohkem kui ühe liikme, täieliku disjunktiivse normaalkuju puhul niisugune olukord võimalik ei ole.

Etteantud valemi saab teisendada disjunktiivsele normaalkujule järgmiste sammudega. Kirjeldatav meetod annab muu hulgas ka teise tõestuse teoreemile 5.

1) Elimineerime implikatsioonid ja ekvivalentsid, kasutades näiteks samaväärsusi

$$\mathcal{F} \to \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}, \qquad \mathcal{F} \leftrightarrow \mathcal{G} \equiv \mathcal{F} \,\&\, \mathcal{G} \vee \neg\mathcal{F} \,\&\, \neg\mathcal{G}.$$

Tulemuseks saadud valem sisaldab ainult eitust, konjunktsiooni ja disjunktsiooni.

2) Viime eitused vahetult lausemuutujate ette, kasutades De Morgani seadusi

$$\neg(\mathcal{F} \,\&\, \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}, \qquad \neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \,\&\, \neg\mathcal{G}.$$

Kui kuskile tekib kahekordne eitus, siis jätame selle ära. Tulemuseks on valem, kus pole ühtegi eitust sulgude ees.

3) Viime konjunktsioonid disjunktsioonidest sügavamale, kasutades distributiivsuse seadusi

$$\mathcal{F} \,\&\, (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \,\&\, \mathcal{G} \vee \mathcal{F} \,\&\, \mathcal{H},$$
$$(\mathcal{F} \vee \mathcal{G}) \,\&\, \mathcal{H} \equiv \mathcal{F} \,\&\, \mathcal{H} \vee \mathcal{G} \,\&\, \mathcal{H}.$$

Nii saame valemi, mis koosneb omavahel disjunktsiooniga seotud liikmetest, millest igaüks on literaalide konjunktsioon. See ei pruugi veel olla vajalik kuju, sest mõnes liikmes võib mõni muutuja esineda mitu korda, korduda võivad ka liikmed ise.

4) Eemaldame liikmed, mis sisaldavad vastandlikke literaalipaare (st sama muutujat ilma eituseta ja koos eitusega), sest need liikmed on samaselt väärad. Igast järelejäänud liikmest kaotame literaalide kordused. Jätame välja korduvad liikmed. Niisuguse korrastamise tulemuseks ongi valemi disjunktiivne normaalkuju, kus kõik liikmed on elementaarkonjunktsioonid.

5) Vajaduse korral võime siit edasi leida ka täieliku disjunktiivse normaalkuju. Lisame igale elementaarkonjunktsioonile täiskomplektist puuduvad muutujad, kasutades seost

$$\mathcal{F} \equiv \mathcal{F} \,\&\, (A \vee \neg A).$$

Seejärel rakendame uuesti distributiivsuse seadusi ja korrutame sulud lahti. Tulemuseks on mitme liikme disjunktsioon, kus kõik liikmed on täielikud elementaarkonjunktsioonid.

6) Jätame välja täielike elementaarkonjunktsioonide korduvad eksemplarid, kasutades idempotentsuse seadust

$$\mathcal{F} \vee \mathcal{F} \equiv \mathcal{F}.$$

Näide 15. Teisendada valem $\mathcal{F} = \neg B \leftrightarrow \neg A \vee \neg B \to C \,\&\, A$ disjunktiivsele normaalkujule.

Kõigepealt elimineerime ekvivalentsid ja implikatsioonid:

$$\begin{aligned}\mathcal{F} &\equiv \neg B \,\&\, (\neg A \vee \neg B \to C \,\&\, A) \vee \neg\neg B \,\&\, \neg(\neg A \vee \neg B \to C \,\&\, A) \equiv \\ &\equiv \neg B \,\&\, (\neg(\neg A \vee \neg B) \vee C \,\&\, A) \vee \neg\neg B \,\&\, (\neg A \vee \neg B) \,\&\, \neg(C \,\&\, A).\end{aligned}$$

Viime eitused sulgude sisse ja jätame kahekordsed eitused ära:

$$\begin{aligned}\mathcal{F} &\equiv \neg B \,\&\, (\neg\neg A \,\&\, \neg\neg B \vee C \,\&\, A) \vee B \,\&\, (\neg A \vee \neg B) \,\&\, (\neg C \vee \neg A) \equiv \\ &\equiv \neg B \,\&\, (A \,\&\, B \vee C \,\&\, A) \vee B \,\&\, (\neg A \vee \neg B) \,\&\, (\neg C \vee \neg A).\end{aligned}$$

Viime konjunktsioonid disjunktsioonidest sügavamale:

$$\begin{aligned}\mathcal{F} &\equiv \neg B \,\&\, A \,\&\, B \vee \neg B \,\&\, C \,\&\, A \vee B \,\&\, \neg A \,\&\, (\neg C \vee \neg A) \vee \\ &\qquad \vee B \,\&\, \neg B \,\&\, (\neg C \vee \neg A) \equiv \neg B \,\&\, A \,\&\, B \vee \neg B \,\&\, C \,\&\, A \vee \\ &\qquad \vee B \,\&\, \neg A \,\&\, \neg C \vee B \,\&\, \neg A \,\&\, \neg A \vee B \,\&\, \neg B \,\&\, \neg C \vee B \,\&\, \neg B \,\&\, \neg A.\end{aligned}$$

Teisendame konjunktsioonid elementaarseks. Viimases valemis on esimene, viies ja kuues liige samaselt väärad, mistõttu need jätame välja. Ülejäänutes korrastame muutujad. Pärast seda rahuldavad (endised) kolmas ja neljas liige neelamisseadust, mille põhjal võib ka kolmanda liikme välja jätta:

$$\mathcal{F} \equiv A \,\&\, \neg B \,\&\, C \vee \neg A \,\&\, B \,\&\, \neg C \vee \neg A \,\&\, B \equiv A \,\&\, \neg B \,\&\, C \vee \neg A \,\&\, B.$$

Saadud valemit võime edasi teisendada täielikuks disjunktiivseks normaalkujuks. Selleks tuleb liikmetesse lisada puuduvad muutujad. Et teises liikmes puudub muutuja C, siis lisame teisele liikmele samaselt tõese avaldise $C \vee \neg C$ ning avame uuesti sulud:

$$\begin{aligned}\mathcal{F} &\equiv A \,\&\, \neg B \,\&\, C \vee \neg A \,\&\, B \,\&\, (C \vee \neg C) \equiv \\ &\equiv A \,\&\, \neg B \,\&\, C \vee \neg A \,\&\, B \,\&\, C \vee \neg A \,\&\, B \,\&\, \neg C.\end{aligned}$$

Korduvaid liikmeid tulemuses ei esine, nii et ühtegi liiget enam ära jätta pole vaja. Sellega oleme leidnud valemi täieliku disjunktiivse normaalkuju, mis langeb ühte näites 13 saadud täieliku disjunktiivse normaalkujuga sama valemi jaoks.

Kogu eelneva käsitluse saab jällegi lihtsasti üle kanda konjunktiivsetele normaalkujudele. Näiteks kui eesmärgiks on teisendada valem konjunktiivsele normaalkujule, siis tuleb vaadeldud meetodis vahetada sõnad „konjunktsioon“ ja „disjunktsioon“ ning alates kolmandast punktist tehtemärgid & ja $\vee$.

Kolme lausemuutuja puhul ei anna valemi teisendamine tõeväärtustabeli arvutamisega võrreldes erilist efekti, ent kui muutujaid on mitukümmend, siis võib teisendamine normaalkuju leidmiseks olla ainuvõimalik meetod. Valemi normaalkujule viimist saab lihtsasti automatiseerida ja anda täitmiseks arvutile. Seetõttu eeldab näiteks suur osa lausearvutuse valemeid analüüsivaid algoritme, et sisendiks antav valem on juba mingil normaalkujul.

§ 6. Normaalkujude minimeerimine

Mõnikord, näiteks digitaallülituste koostamisel, seatakse valemi normaalkujule viimisel tingimuseks, et tulemus peab olema võimalikult lühike. Normaalkuju pikkuse mõõduks võime võtta selles sisalduvate literaalide arvu. Järgnevas tegeleme ainult disjunktiivsete normaalkujudega, sümmeetria põhjal saab loomulikult kõike laiendada ka konjunktiivsetele normaalkujudele.

Definitsioon 8. *Valemi $\mathcal{F}$ minimaalseks disjunktiivseks normaalkujuks (MDNK) nimetatakse valemi $\mathcal{F}$ disjunktiivset normaalkuju, mis sisaldab kõige vähem literaale.*

Normaalkuju võib ebaefektiivne olla mitmel põhjusel. Näiteks kui üks liige *katab* teist ehk ühe liikme literaalid kuuluvad kõik teise liikme koosseisu nagu normaalkujus

$$A \,\&\, B \vee A \,\&\, B \,\&\, \neg C,$$

siis võib neelamisseaduse põhjal teise liikme ära jätta. Samuti võib normaalkuju sisaldada *ühilduvaid liikmeid*, st niisugust kahte liiget, milles kõik literaalid peale ühe on samad, üks literaal aga esineb ühes liikmes positiivsena ning teises negatiivsena. Näiteks on omavahel ühilduvad elementaarkonjunktsioonid $B \,\&\, C \,\&\, D$ ja $B \,\&\, \neg C \,\&\, D$. Ühilduvad liikmed saab normaalkujus kokku võtta:

$$B \,\&\, C \,\&\, D \vee B \,\&\, \neg C \,\&\, D \equiv B \,\&\, (C \vee \neg C) \,\&\, D \equiv B \,\&\, D.$$

Kuid ainult kattuvuste kõrvaldamine ja ühilduvate liikmete ühendamine ei tarvitse anda minimaalset normaalkuju. Olgu näiteks

$$\mathcal{F} = A \,\&\, B \vee A \,\&\, B \,\&\, \neg C \vee A \,\&\, \neg B \,\&\, C \vee A \,\&\, C \vee \neg A \,\&\, B \,\&\, \neg C.$$

Siin võime ära jätta teise liikme, mida katab esimene liige, ning kolmanda liikme, mida katab neljas. Tulemuseks saame

$$\mathcal{F} \equiv A \,\&\, B \vee A \,\&\, C \vee \neg A \,\&\, B \,\&\, \neg C.$$

Alternatiivne võimalus on esialgses valemis ühendada teine ja viies liige ning jätta ära kolmas, nii tekib normaalkuju

$$\mathcal{F} \equiv A \,\&\, B \vee B \,\&\, \neg C \vee A \,\&\, C,$$

mis on eelmisest ühe literaali võrra lühem. Siiski pole ka viimane normaalkuju minimaalne, selleks on hoopis normaalkuju

$$\mathcal{F} \equiv B \,\&\, \neg C \vee A \,\&\, C,$$

kuigi nimetatud teisendustega pole seda valemit võimalik esialgsest valemist saada.

Järgnevas vaatleme võimalusi valemi minimaalse disjunktiivse normaalkuju leidmiseks. Väiksema muutujate arvu puhul sobib hästi *Karnaugh' diagramm*, mille ameerika matemaatik Maurice Karnaugh pakkus välja aastal 1950. Karnaugh' diagramm on tabel, mille igale lahtrile vastab üks valemi muutujate väärtustus ehk teiste sõnadega, üks liige valemi täielikus disjunktiivses normaalkujus. Kahe, kolme ja nelja muutuja jaoks näevad need tabelid välja järgmiselt:

	B	$\neg B$
A		
$\neg A$		

	B	B	$\neg B$	$\neg B$
A				
$\neg A$				
	C	$\neg C$	$\neg C$	C

	B	B	$\neg B$	$\neg B$	
A					D
A					$\neg D$
$\neg A$					$\neg D$
$\neg A$					D
	C	$\neg C$	$\neg C$	C	

Diagrammi read ja veerud on tähistatud nii, et täielikud elementaarkonjunktsioonid, mis vastavad kahele naaberlahtrile, erinevad alati täpselt ühe literaali märgi poolest, st on omavahel ühilduvad. Peale selle loeme, et diagrammi vasak serv on ühendatud paremaga ning ülemine serv alumisega. Liikudes näiteks üle parema serva tabelist välja, satume vasaku serva kaudu uuesti tabelisse sisse. Niiviisi on näiteks 4×4-tabeli igal lahtril neli erinevat naabrit.

Tabeli ridade ja veergude tähistusviisist tuleneb, et suvalist elementaarkonjunktsiooni (täielikku või mitte) esitab seotud lahtrite plokk, ristkülik või ruut, mille mõõtmed avalduvad kujul $2^a \times 2^b$. Näiteks elementaarkonjunktsioonile $A \,\&\, \neg C \,\&\, \neg D$ vastab nelja muutuja tabelis teise rea kaks keskmist lahtrit, see liige on parajasti täielike elementaarkonjunktsioonide $A \,\&\, B \,\&\, \neg C \,\&\, \neg D$ ja $A \,\&\, \neg B \,\&\, \neg C \,\&\, \neg D$ disjunktsioon. Kehtib ka vastupidine: iga selline plokk määrab mingi elementaarkonjunktsiooni. Näiteks neli lahtrit tabeli keskel esitavad elementaarkonjunktsiooni $\neg C \,\&\, \neg D$, sest nii C kui ka D on kõigis neljas lahtris negatiivse märgiga, seevastu A ja B märgid muutuvad kõikvõimalikes kombinatsioonides. Vastasservade samastamise tõttu võib mõni plokk kujutuda joonisel eraldiasuvateks lahtriteks, näiteks liikmele $C \mathbin{\&} D$ vastab nelja muutuja tabeli neli nurka.

Etteantud valemi minimaalse disjunktiivse normaalkuju leidmiseks määrame tõeväärtustabeli või täieliku disjunktiivse normaalkuju abil väärtustused, mil valem on tõene, ja märgime tabeli vastavatesse lahtritesse väärtused 1. Seejärel püüame need katta võimalikult suurte plokkidega, mille mõõtmed on arvu 2 astmed. Mida suuremad on plokid ja mida vähem neid on, seda lühem on leitav normaalkuju.

Näide 16. Leida valemi $(C \to A) \mathbin{\&} (A \to \neg B)$ minimaalne disjunktiivne normaalkuju.

Valem on tõene väärtustustel $(1, 0, 1)$, $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 0)$. Koostame Karnaugh' diagrammi ja märgime vastavad lahtrid:

	B	B	$\neg B$	$\neg B$
A			1	1
$\neg A$		1	1	
	C	$\neg C$	$\neg C$	C

Kõigi ühtede katmiseks vajame kahte 1×2-plokki, üks esimeses reas, teine teises reas. Esimene neist vastab elementaarkonjunktsioonile $A \mathbin{\&} \neg B$, teine aga elementaarkonjunktsioonile $\neg A \mathbin{\&} \neg C$. Valemi minimaalne disjunktiivne normaalkuju on järelikult

$$\mathcal{F} \equiv A \mathbin{\&} \neg B \vee \neg A \mathbin{\&} \neg C.$$

Näide 17. Diagrammi

	B	B	$\neg B$	$\neg B$
A		1	1	
$\neg A$	1	1	1	1
	C	$\neg C$	$\neg C$	C

katmiseks kasutame kahte plokki: üks mõõtmetega 1×4 haarab terve alumise rea, teine mõõtmetega 2×2 hõlmab neli keskmist ruutu. Minimaalseks disjunktiivseks normaalkujuks saame niisiis

$$\neg A \vee \neg C.$$

Näide 18. Diagrammil

	B	B	$\neg B$	$\neg B$	
A			1	1	D
A					$\neg D$
$\neg A$				1	$\neg D$
$\neg A$	1		1	1	D
	C	$\neg C$	$\neg C$	C	

leiame 2×2-ploki, mis katab korraga esimese ja viimase rea kaks viimast ruutu. Kahe ülejäänud väärtuse katmiseks ei ole otstarbekas kasutada mitte kahte 1×1-plokki, millega saaksime normaalkuju

$$\neg B \,\&\, D \vee \neg A \,\&\, B \,\&\, C \,\&\, D \vee \neg A \,\&\, \neg B \,\&\, C \,\&\, \neg D,$$

vaid kahte 1×2-plokki: üks neist haarab viimase rea esimese ja viimase lahtri, teine aga viimase veeru kaks viimast lahtrit. Valemi minimaalne normaalkuju on seega

$$\neg B \,\&\, D \vee \neg A \,\&\, C \,\&\, D \vee \neg A \,\&\, \neg B \,\&\, C.$$

Näeme, et plokid, millega Karnaugh' diagrammil tõeseid väärtusi kaetakse, võivad kattuda ka üksteisega, kui see on vajalik nende mõõtmete suurendamiseks.

Karnaugh' diagramm võimaldab leida minimaalset normaalkuju ka juhul, kui valemi tõeväärtus mõnel väärtustusel on määramata. Määramata tõeväärtus tähendab seda, et me võime ta lugeda tõeseks või vääraks oma äranägemise järgi. Niisugune olukord esineb näiteks siis, kui valem kirjeldab mingi loogilise seadme sisendite ja väljundi vahelist seost, kusjuures mõni sisendite väärtuste kombinatsioon kas pole võimalik või ei huvita meid sellele vastav väljundi väärtus. Minimeerimisülesandes püütakse määramata tõeväärtused fikseerida nii, et lõpuks tekkiv normaalkuju oleks lühim.

Näide 19. Leida valem, mille tõeväärtuste veerg (ülevalt alla lugedes) on 0, 1, 1, 0, 0, 1, x, x, kus x tähistab määramata väärtust.

	B	B	$\neg B$	$\neg B$
A	0	1	0	1
$\neg A$	0	1	x	x
	C	$\neg C$	$\neg C$	C

	B	B	$\neg B$	$\neg B$
A	0	1	0	1
$\neg A$	0	1	0	1
	C	$\neg C$	$\neg C$	C

Joonisel vasakul on kujutatud selle valemi Karnaugh' diagramm, mis on saadud tõeväärtuste veerust. Diagrammi teise veeru ühed tuleb katta ühe 2×1-plokiga. Neljanda veeru ühe saame katta maksimaalse plokiga siis, kui defineerime neljanda veeru x väärtuseks 1. Kolmanda veeru x väärtuseks võtame 0, siis piisabki kahest plokist. Tulemus on kujutatud joonisel paremal. Valemi minimaalne disjunktiivne normaalkuju on selle põhjal

$$B \,\&\, \neg C \vee \neg B \,\&\, C.$$

Karnaugh' diagramm on küll piltlik, ent sobib ainult väikese muutujate arvuga valemi minimeerimiseks ega ole hästi arvutil realiseeritav. Diagrammimeetodi teatavas mõttes algebraline vaste, mis ka programmeerimiseks paremini sobib, on *Quine-McCluskey meetod.*

Olgu antud valem $\mathcal{F}$ täielikul disjunktiivsel normaalkujul. Quine-McCluskey meetod koosneb kahest etapist: 1) leiame valemi kõik lihtimplikandid ja 2) leiame lihtimplikantide hulga minimaalse katte. *Lihtimplikant* on normaalkuju liige, millest ei saa jätta välja ühtegi literaali, ilma et muudetud normaalkuju kaotaks samaväärsust esialgsega. Karnaugh' diagrammil vastab lihtimplikandile maksimaalne plokk, st selline plokk, mis ei sisaldu üheski suuremas plokis. Quine-McCluskey meetodi ideed on kõige lihtsam selgitada näite abil.

Vaatleme täielikul disjunktiivsel normaalkujul esitatud valemit

$$\mathcal{F} = A\&B\&C\&\neg D \vee A\&\neg B\&\neg C\&D \vee A\&\neg B\&\neg C\&\neg D \vee \neg A\&B\&C\&D \vee$$
$$\vee \neg A\&B\&\neg C\&D \vee \neg A\&\neg B\&\neg C\&D \vee \neg A\&\neg B\&\neg C\&\neg D.$$

Kõigepealt tuleb leida lihtimplikandid. Selleks kirjutame välja kõik normaalkujus esinevad elementaarkonjunktsioonid ning otsime üles ühilduvad paarid. Tabelis on ühilduvad liikmed märgitud tärniga:

$A\&B\&C\&\neg D$						
$A\&\neg B\&\neg C\&D$	⋆	⋆				
$A\&\neg B\&\neg C\&\neg D$	⋆		⋆			
$\neg A\&B\&C\&D$				⋆		
$\neg A\&B\&\neg C\&D$				⋆	⋆	
$\neg A\&\neg B\&\neg C\&D$		⋆			⋆	⋆
$\neg A\&\neg B\&\neg C\&\neg D$			⋆			⋆

Et esimene liige $A\&B\&C\&\neg D$ ei ühildu ühegi teisega, siis on ta lihtimplikant. Ülejäänud liikmetest moodustame uued liikmed, võttes kokku ühilduvate paaride komponendid. Tekkinud liikmed kirjutame välja ning määrame jälle ühilduvad paarid:

$A\&\neg B\&\neg C$		⋆
$\neg B\&\neg C\&D$	⋆	
$\neg B\&\neg C\&\neg D$	⋆	
$\neg A\&B\&D$		
$\neg A\&\neg C\&D$		
$\neg A\&\neg B\&\neg C$		⋆

Sellest tabelist saame kaks lihtimplikanti $\neg A\&B\&D$ ja $\neg A\&\neg C\&D$, ühilduvad liikmed võtame jälle kokku. Praegusel juhul annavad mõlemad ühilduvate liikmete paarid $\neg B\&\neg C$, mis viimase järelejäänud liikmena on ise lihtimplikant. Kokkuvõttes leidsime neli lihtimplikanti, valemi $\mathcal{F}$ võib järelikult esitada nende disjunktsioonina kujul

$$\mathcal{F} \equiv A\&B\&C\&\neg D \vee \neg A\&B\&D \vee \neg A\&\neg C\&D \vee \neg B\&\neg C.$$

Ilmselt on saadud valem esialgse valemiga samaväärne, sest liikmepaaride ühendamisel samaväärsus säilib.

Nüüd elimineerime viimasest disjunktsioonist liiasused ehk leiame minimaalse komplekti liikmeid, mis esitab valemit $\mathcal{F}$. Selleks koostame jälle tabeli, mille ridades on algse täieliku disjunktiivse normaalkuju liikmed ning veergudes äsjasaadud lihtimplikandid. Tabeli lahtrisse kirjutame tärni, kui lihtimplikant katab vastavat liiget:

	$A \& B \& C \& \neg D$	$\neg A \& B \& D$	$\neg A \& \neg C \& D$	$\neg B \& \neg C$
$A \& B \& C \& \neg D$	$\star$			
$A \& \neg B \& \neg C \& D$				$\star$
$A \& \neg B \& \neg C \& \neg D$				$\star$
$\neg A \& B \& C \& D$		$\star$		
$\neg A \& B \& \neg C \& D$		$\star$	$\star$	
$\neg A \& \neg B \& \neg C \& D$			$\star$	$\star$
$\neg A \& \neg B \& \neg C \& \neg D$				$\star$

Et esimest liiget katab ainult esimene lihtimplikant, siis peab see lihtimplikant kuuluma minimaalsesse normaalkujusse. Samamoodi peab sinna kuuluma neljas lihtimplikant, sest see katab ainsana teist, kolmandat ja seitsmendat liiget. Ülejäänud liikmed saab katta teise lihtimplikandiga. Kolmas lihtimplikant osutus üleliigseks. Valemi minimaalne disjunktiivne normaalkuju on järelikult

$$\mathcal{F} \equiv A \& B \& C \& \neg D \vee \neg A \& B \& D \vee \neg B \& \neg C.$$

Näitame, et Quine-McCluskey meetodiga leitud disjunktiivne normaalkuju on tõepoolest kõigist võimalikest lühim. Olgu $\mathcal{F}$ mingi valem täielikul disjunktiivsel normaalkujul ning $\mathcal{F}'$ selle valemi minimaalne disjunktiivne normaalkuju. Kui valemi $\mathcal{F}'$ mingis liikmes on täiskomplektist puudu k muutujat, siis valemis $\mathcal{F}$ vastab sellele disjunktsioon 2^k täieliku elementaarkonjunktsioonist. Viimaste paarikaupa ühildamisel tekib pärast Quine-McCluskey meetodi esimest sammu 2^{k-1} liiget, milles puudub üks muutuja, nendest omakorda pärast teist sammu 2^{k-2} liiget, milles puudub kaks muutujat jne kuni pärast k-ndat sammu saame vaadeldava liikme. See liige peab olema lihtimplikant, sest kui ta ühilduks mingi teise sellel sammul tekkinud liikmega, siis võiksime selle liikme valemis $\mathcal{F}'$ asendada ühildamise tulemusega ning saada lühema disjunktiivse normaalkuju. Seega on pärast Quine-McCluskey algoritmi esimest etappi leitud kõik minimaalse disjunktiivse normaalkuju liikmed. Et teisel etapil valitakse liikmete hulgast välja need, mis annavad kõige väiksema literaalide arvuga normaalkuju, siis ei saa meetodis leitud disjunktiivne normaalkuju sisaldada rohkem literaale kui valemi minimaalne disjunktiivne normaalkuju.

§ 7. Ülesanded

1. Olgu antud lausemuutujad järgmises tähenduses: A = „On pühapäev“, B = „Kristjan läheb teatrisse“, C = „Kristjan läheb sõbrale külla“, D = „Kristjan läheb koeraga jalutama“, E = „Kristjan istub kodus“. Mida tähendavad järgmised valemid?

a) $A \to B$

b) $D \,\&\, A \to \neg B$

c) $\neg A \to \neg(B \vee C)$

d) $\neg B \,\&\, \neg C \,\&\, \neg D \to E$

e) $A \to \neg E \,\&\, (B \vee C \vee D)$

f) $(A \to \neg E) \,\&\, (\neg A \to \neg E)$

2. Panna järgmised väited kirja lausearvutuse valemiga. Püüda leida valem, mis väljendab olukorda võimalikult täpselt. Iga lause puhul hinnata, millised tähendusnüansid lähevad valemiks teisendamisel kaotsi.

a) Ostan pätsi leiba ja sinna juurde piima või keefirit.

b) Kui õnnetusi tuleb, siis tuleb neid uksest ja aknast.

c) Selleks, et sportlane oleks talvel edukas, on tal tarvis suvel omandada hea kehaline ettevalmistus.

d) Talvel pääsevad laevad sadamast välja ainult siis, kui jäälõhkuja on neile tee rajanud.

e) Kui ma nüüd vangerdan, siis ma kaotan lipu, kui jätan vangerdamata, siis saan mati.

f) Kui hr. Kask on õnnelik, siis pr. Kask on õnnetu, ja kui hr. Kask on õnnetu, siis pr. Kask on õnnelik.

g) Kommunism — see on nõukogude võim pluss kogu maa elektrifitseerimine.

h) Kui taevas läheb pilve, siis suvel hakkab sadama vihma, talvel aga lund.

3. Selgitada, kuidas tuleks lausearvutuse valemiga kirja panna järgmised väited.

a) Alari auto on must, aga Peetri auto on valge.

b) Näidendist leiab nii naeru kui ka pisaraid.

c) Tarvilik tingimus edukaks esinemiseks on hästi tehtud kodutöö.

d) Piisav tingimus diplomi saamiseks on vähemalt ühe ülesande õige lahendus.

e) Et sinine tapeet oli otsas, siis ostsime rohelist.

4. Lausearvutuse valemite kirjapanemiseks on käibel ka *poola kuju*, mille võttis 1928. aastal kasutusele poola loogik Jan Łukasiewicz. Selles ei panda tehtemärk mitte ühendatavate osavalemite vahele, vaid nende ette. Poola kuju iseärasusena pole valemites vaja kasutada sulge. Valemid $\neg A$, $A \& B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$, on poola kujul vastavalt Na, Kab, Aab, Cab, Eab, lausemuutujad kirjutatakse väikese tähega. Keerukamaid valemeid koostatakse analoogiliselt. Näiteks valemile $A \& B \vee C$ vastab valem $AKabc$, valemile $A \& (B \vee C)$ aga $KaAbc$. Alljärgnevatest valemitest teisendada a)—c) poola kujule ning d)—f) tavakujule.

a) $((A \vee B) \& (B \vee C)) \& (A \vee C)$ d) $EcNCbKad$

b) $\neg A \& (\neg A \to B) \to B$ e) $AaCKNababc$

c) $(A \vee B) \to (C \leftrightarrow D) \& A$ f) $KENAabcd$

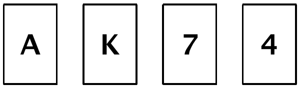
5. Koostada järgmiste valemite tõeväärtustabelid.

a) $\neg(\neg A \vee \neg(\neg B \vee \neg A))$ d) $C \to B \leftrightarrow A \to C \vee B \& A$

b) $(A \vee B) \& (B \vee C) \& (C \vee A)$ e) $\neg C \& \neg A \leftrightarrow (\neg C \to \neg B \vee A)$

c) $(A \to B \vee \neg C) \& (B \to A \vee \neg C)$ f) $C \leftrightarrow \neg A \vee (\neg C \& D \leftrightarrow (C \to D))$

6. Laual on neli kaarti. Iga kaardi ühele poole on kirjutatud täht ja teisele poole number. Kaardid paistavad nagu joonisel kujutatud. Millised nendest kaartidest tuleb kindlasti ümber pöörata, et teada saada, kas kehtib väide „Kui kaardi ühel pool on täishäälik, siis teisel pool on paarisarv“?



7. Maa-alust impeeriumit valitseb kaks kuningat: Päevakuningas ja Öökuningas. Päevakuningas räägib päeval tõtt ja öösel valetab, Öökuningas, vastupidi, räägib öösel tõtt ja päeval valetab. Et impeerium asub maa all, siis ainuke võimalus päevaaega kindlaks määrata on küsida seda emma-kumma kuninga käest, kes teavad täpselt, kas parajasti on päev või öö. Olles külaline sel kummalisel maal, kohtas rändur ühte kahest kuningast, kes asjakohasele küsimusele vastas: „Mina olen Päevakuningas ja praegu on öö.“ Kas on võimalik ainult selle lause põhjal otsustada, kas parajasti oli päev või öö? Kas on võimalik otsustada, kas see, keda rändur kohtas, oli Päeva- või Öökuningas?

8. Firma juhatusse kandideerib neli inimest — Arpson, Brauer, Cesany ja Dean —, kelle omavahelised suhted on võrdlemisi pingelised. Arpson teatas, et tema ei nõustu juhatusse kuuluma, kui sinna kuulub Brauer või Cesany. Brauer teatas, et tema ei soovi juhatusse kuuluda, kui sinna kuulub Dean. Dean ütles, et tema ei saa kuuluda juhatusse, kui sinna ei kuulu ka Cesany. Samal ajal on firma seisukohalt nõutav, et kui juhatusest puudub Arpson või Brauer, siis kuulub sinna Dean. Kas on võimalik moodustada juhatus nii, et kõik finessid arvestatud saaksid? Kes nendest neljast kandidaadist kuuluvad juhatusse?

9. Kolme väite A, B ja C kohta on teada järgmist.

- Kui A on tõene, siis on ka B ja C tõesed.
- Kui B on tõene, siis on vähemalt üks väidetest A ja C tõene.
- Kui C on tõene, siis on A tõene ja B väär.

Millised väidetest A, B, C on tõesed?

10. Määrata valemi liik (samaselt tõene, samaselt väär, kehtestatav).

a) $\neg C \,\&\, (\neg A \vee \neg C \,\&\, A) \leftrightarrow \neg C \to B$

b) $A \leftrightarrow B \to C \vee \neg A \,\&\, B \to A$

c) $(\neg B \,\&\, C \leftrightarrow (\neg A \to \neg B)) \vee A$

d) $(C \to D) \,\&\, (A \to C) \,\&\, (D \to \neg A) \,\&\, (A \to B \vee C) \,\&\, (B \to \neg D)$

11. Lausearvutuse valemist $\mathcal{F}$ on teada, et valem $\neg\mathcal{F} \vee \mathcal{G}$ ei saa olla samaselt tõene ega ka mitte samaselt väär. Kas siit saab midagi järeldada valemi $\mathcal{F}$ liigi kohta ja kui saab, siis mida?

12. Arvutis on realiseeritud lausearvutuse valemite samaselt tõesuse kontrollija, mis teeb kindlaks, kas etteantud valem on samaselt tõene või mitte. Arvutisse sisestati kaks valemit, mille üldkuju oli $\mathcal{F} \vee \mathcal{G}$ ja $\neg\mathcal{F} \vee \mathcal{G}$, ning kontrollija teatas vastuseks, et kumbki neist valemeist ei ole samaselt tõene. Mida saab sellest järeldada valemite $\mathcal{F}$ ja $\mathcal{G}$ liigi kohta?

13. Tõestada, et kui valem $\mathcal{F} \vee \mathcal{G} \to \mathcal{H}$ on kehtestatav, siis ka valemid $\mathcal{F} \to \mathcal{H}$ ja $\mathcal{G} \to \mathcal{H}$ on kehtestatavad.

14. Olgu $\mathcal{F} \to \mathcal{G}$ samaselt tõene valem, kus $\mathcal{F}$ ja $\mathcal{G}$ ei sisalda ühiseid lausemuutujaid. Tõestada, et siis $\mathcal{F}$ on samaselt väär või $\mathcal{G}$ on samaselt tõene. Näidata, et ühiste lausemuutujate puudumise eeldus on tarvilik.

15. *Craigi teoreem*. Tõestada, et kui $\mathcal{F} \to \mathcal{G}$ on samaselt tõene valem, kus $\mathcal{F}$ ja $\mathcal{G}$ sisaldavad vähemalt ühte ühist lausemuutujat, siis leidub valem $\mathcal{H}$, mis on moodustatud valemite $\mathcal{F}$ ja $\mathcal{G}$ ühistest muutujatest, nii et valemid $\mathcal{F} \to \mathcal{H}$ ja $\mathcal{H} \to \mathcal{G}$ on samaselt tõesed.

16. Tuua näide vasturääkivast n-valemilisest hulgast, mis ükskõik millise valemi eemaldamisel muutub mittevasturääkivaks.

17. Teha kindlaks, kas kehtivad järgmised järeldumised.

a) $A \to B, B \to C, \neg C \models \neg A$

b) $A \vee B, \neg B, C \to \neg A \models \neg C$

c) $A \vee B, \neg A \vee C, \neg B \models C$

d) $A \vee B \& C, A \vee B \to D \models C \vee D$

18. Antud on lausearvutuse valemid $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_m$ ja $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n$.

a) Tõestada, et kui mingi i ja mingi j korral valemist $\mathcal{F}_i$ järeldub valem $\mathcal{G}_j$, siis valemist $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_m$ järeldub valem $\mathcal{G}_1 \vee \mathcal{G}_2 \vee \ldots \vee \mathcal{G}_N$.

b) Tõestada, et kui iga i ja iga j korral valemist $\mathcal{F}_i$ järeldub valem $\mathcal{G}_j$, siis valemist $\mathcal{F}_1 \vee \mathcal{F}_2 \vee \ldots \vee \mathcal{F}_m$ järeldub valem $\mathcal{G}_1 \& \mathcal{G}_2 \& \ldots \& \mathcal{G}_n$.

19. Keegi ütles, et tal on niisugused lausearvutuse valemid $\mathcal{F}$ ja $\mathcal{G}$, et $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{F} \models \neg\mathcal{G}$. Kas selline asi on võimalik?

20. Panna järgmine arutlus kirja lausearvutuse valemitega ja tõestada, et see arutlus kehtib, st tõestada, et eeldustele vastavatest valemitest järeldub väitele vastav valem. „Õpilased on rõõmsad siis ja ainult siis, kui ei toimu kontrolltööd. Kui õpilased on rõõmsad, siis on õpetajal hea meel. Ent kui õpetajal on hea meel, siis ta ei taha pidada tundi, ning kui ta ei taha pidada tundi, siis toimub kontrolltöö. Järelikult õpilased pole rõõmsad.“

21. On teada järgmised faktid.

- Kui Mihkel köhib ja on näost valge, siis ta kas on haige või on käinud nurga taga suitsu tegemas.
- Kui Mihkel pole käinud suitsu tegemas ja ikkagi köhib või on näost valge, siis ta on haige.
- Kui Mihkel on haige, siis ta köhib, aga pole näost valge.

Pärast vahetundi klassi tulles oli Mihkel näost täiesti valge. Kas sellest järeldub, et ta käis nurga taga suitsu tegemas?

22. ÜRO rahukomitees on tekkinud järgmine keerukas seis. Almeraania keeldub uuele rahulepingule alla kirjutamast enne, kui Barmako ja Ceville on mõlemad sellele allkirja andnud. Et Ceville ja Doercenea on sõlminud vabakaubandusliidu, siis on nende otsused lepingule allakirjutamise suhtes ühesugused. Teiselt poolt keeldub Ceville, kartes Almeraania militaristlikku arengut, lepingule alla kirjutamast enne, kui Almeraania on sellele andnud oma allkirja. Tõestada, et kui Doercenead õnnestub veenda lepingule alla kirjutama, siis teevad seda ka kõik ülejäänud riigid.

23. Kui osapooled olid viimaks jõudnud kokkuleppele, kõik formaalsused täidetud ja leping allakirjutamiseks valmis, teatas Ceville äkitselt, et ühe Barmako diplomaadi käitumise tõttu pole ta nõus alla kirjutama ühtegi lepingut koos Barmakoga. Seepeale võttis Barmako valitsus jäiga positsiooni: Barmako ei allkirjasta ühtegi lepingut enne, kui seda teeb Doercenea. Tõestada, et kujunenud olukorras ei saa allakirjutamistseremooniat läbi viia, sest pole jäänud ainsatki riiki, mis oleks nõus lepingule alla kirjutama.

24. Leida, kas valemid järgmistes valemipaarides on samaväärsed.

a) $A \to B$ ja $\neg A \to \neg B$

b) $\neg(A \vee B)$ ja $\neg A \vee \neg B$

c) $A \vee \neg A$ ja $B \vee \neg B$

d) $(A \to B) \& (B \to C)$ ja $A \to C$

e) $\neg C \& \neg B \to \neg A \vee C \leftrightarrow \neg B \to A$ ja $(B \& C \leftrightarrow B) \to C \& A \vee B$

25. Teha kindlaks, kas lausearvutuses kehtib a) implikatsiooni assotsiatiivsus; b) ekvivalentsi assotsiatiivsus; c) distributiivsus konjunktsiooni ja implikatsiooni vahel.

26. *Duaalsusprintsiip.* Olgu $\mathcal{F}$ ja $\mathcal{G}$ samaväärsed valemid, mis sisaldavad tehtemärkidena ainult eitust, konjunktsiooni ja disjunktsiooni. Tõestada, et kui $\mathcal{F}'$ ja $\mathcal{G}'$ on saadud vastavalt valemitest $\mathcal{F}$ ja $\mathcal{G}$, asendades nendes iga tehtemärgi & märgiga $\vee$ ja vastupidi, siis valemid $\mathcal{F}'$ ja $\mathcal{G}'$ on samaväärsed.

27. Lihtsustada valemid lausearvutuse põhisamaväärsuste abil.

a) $\neg B \& (\neg C \vee A \to (B \leftrightarrow \neg C \& B))$

b) $B \leftrightarrow C \to \neg B \& A \vee (B \to \neg C)$

c) $C \to A \leftrightarrow A \& (B \vee A \to C)$

d) $\neg B \vee C \vee ((A \leftrightarrow \neg C) \to \neg B) \& A$

e) $(\neg A \to \neg C \leftrightarrow B) \leftrightarrow \neg C \vee \neg(\neg A \& C)$

28. Formuleerida algoritm, mille abil saab iga valemi avaldada a) eituse ja konjunktsiooni; b) eituse ja disjunktsiooni; c) eituse ja implikatsiooni kaudu.

29. Tõestada, et leidub lausearvutuse valem, mida ei saa avaldada eituse ja ekvivalentsi abil.

30. Tõestada, et on võimalik defineerida selline lausearvutuse tehe, et suvalise valemi saab avaldada ainult selle tehte abil.

31. Zen-budismi guru teatas oma õpilastele: „Kui ma olen Buddha, siis ma ei ole Buddha.“ Õpilased olid seda kuuldes hämmastunud. Väljendada väide valemiga, koostada tõeväärtustabel ja selgitada, millise lihtsama väitega on see väide samaväärne.

32. Uue hoone turvateenistuse lepingusse on sattunud üks esmapilgul võrdlemisi raskesti arusaadav punkt: „Alarm hakkab tööle, kui uks avatakse ja stopp-nupp pole alla vajutatud ajal, mil alarm on aktiivne, või kui ruumis on liikumine ja pole nii, et stopp-nupp on alla vajutatud või alarm pole aktiivne“. Lihtsustada seda.

33. Leida valemite täielik disjunktiivne ja täielik konjunktiivne normaalkuju.

a) $\neg A \& B \leftrightarrow C \vee A$ c) $(A \vee B) \& (C \vee \neg B) \leftrightarrow A \vee \neg C$

b) $(A \rightarrow B) \leftrightarrow C \& \neg A$ d) $\neg B \& (A \leftrightarrow \neg B) \& \neg(\neg C \rightarrow \neg B \vee A)$

34. Leida lausearvutuse valem $\mathcal{F}$, mis sisaldab kolme muutujat A, B, C ning mis on tõene parajasti siis, kui on tõene täpselt üks nendest muutujatest.

35. Komisjon, kuhu kuuluvad liikmed A, B, C ja D, otsustab olulisemaid küsimusi hääletades. Igal liikmel on üks hääl, välja arvatud komisjoni juht A, kellel on kaks häält. Otsus loetakse vastuvõetuks, kui tema poolt on antud vähemalt pool kõigist häältest. Leida valem, mis komisjoni liikmete hääletustulemuste järgi teeb kindlaks, kas otsus võeti vastu või mitte.

36. Koostada valem, mis on tõene parajasti siis, kui kahendarvude $\overline{AB}$ ja $\overline{CD}$ summa on ülimalt kahekohaline.

37. Leida valemite minimaalne disjunktiivne normaalkuju.

a) $A\&B\&\neg C \vee A\&B\&\neg C\&D \vee A\&\neg B\&D \vee C\&D \vee A\&\neg C\&\neg D$

b) $(A \& \neg C \rightarrow \neg A \vee \neg B) \leftrightarrow D$

c) $A \leftrightarrow \neg C \& (B \rightarrow \neg A) \leftrightarrow \neg B \vee C$

38. Leida järgmiste diagrammidega antud valemite minimaalne disjunktiivne normaalkuju, kus x tähistab määramata väärtust.

a)

	B	B	$\neg B$	$\neg B$	
A	x	0	1	1	D
A	0	1	x	1	$\neg D$
$\neg A$	0	0	1	x	$\neg D$
$\neg A$	0	0	1	x	D
	C	$\neg C$	$\neg C$	C	

b)

	B	B	$\neg B$	$\neg B$	
A	1	x	1	0	D
A	1	x	x	0	$\neg D$
$\neg A$	0	x	1	x	$\neg D$
$\neg A$	1	0	x	x	D
	C	$\neg C$	$\neg C$	C	

39. Lausearvutuse valemiga võib kirjeldada mitmesuguste süsteemide lubatavaid ja mittelubatavaid olekuid. Näiteks raadio olek on määratud kolme asjaoluga: kas voolujuhe on seinas, kas raadio on sisse lülitatud ning kas raadio mängib. Eeldame, et raadio on töökorras ja saab voolu ainult seinakontaktist.

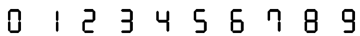
a) Võtta kasutusele lausemuutujad ning leida, millised lausemuutujate väärtuste kombinatsioonid on võimalikud ja millised võimatud.
b) Koostada lausearvutuse valem, mis on tõene parajasti siis, kui muutujate väärtustus esitab võimalikku olukorda.
c) Leida selle valemi minimaalne disjunktiivne normaalkuju.

40. Hoone temperatuuri reguleerimiseks paigaldati sinna kaks elektriradiaatorit: suur, võimsusega 3000 W, ning väike, võimsusega 1200 W. Kumbagi radiaatorit saab teisest sõltumatult sisse ja välja lülitada. Radiaatorite töötamise suhtes kehtib spetsiaalne režiim, mis arvestab välistemperatuuri. Täpsemalt,

- kui välistemperatuur on kõrgem kui $0\ ^\circ$C, siis peavad mõlemad radiaatorid olema välja lülitatud;
- kui välistemperatuur on $-6\ ^\circ$C ja $0\ ^\circ$C vahel, siis peab väiksem radiaator olema sisse ja suurem välja lülitatud;
- kui välistemperatuur on $-12\ ^\circ$C ja $-6\ ^\circ$C vahel, siis peab suurem radiaator olema sisse ja väiksem välja lülitatud;
- kui välistemperatuur on madalam kui $-12\ ^\circ$C, siis peavad mõlemad radiaatorid olema sisse lülitatud.

Temperatuuri fikseerivad kolm andurit A, B ja C hoone välisseinal. Seejuures A annab signaali siis, kui temperatuur langeb alla $0\ ^\circ$C, B annab signaali siis, kui temperatuur langeb alla $-6\ ^\circ$C ja C annab signaali siis, kui temperatuur langeb alla $-12\ ^\circ$C. Koostada loogilised seosed, mis väljendavad radiaatorite töötamist või mittetöötamist sõltuvalt andurite saadetud signaalidest.

41. Taskuarvuti vedelkristallekraanil koostatakse numbrid ristkülikukujulise võre ribadest, kus sisendiks antud numbri järgi lülitatakse vajalikud lõigud sisse:



Eeldame, et sisendnumbrid antakse ette kahendsüsteemis, st arvudena 0000 kuni 1001. Seega kulub sisendi esitamiseks neli kahendkohta. Leida võre iga lõigu jaoks minimaalsel disjunktiivsel normaalkujul valem, mis määrab kindlaks lõigu oleku (sisse või välja lülitatud) sõltuvalt sisendi kahendkohtade väärtustest.

II. PREDIKAATARVUTUS

§ 1. Predikaadid ja kvantorid

Lausearvutuses on vähim vaadeldav üksus lihtlause, mida enam osadeks ei jagata. Seetõttu võimaldab lausearvutus lahendada ainult neid probleeme, mis seostuvad lihtlausete kombineerumisega liitlauseteks, aga mitte lihtlausete struktuuriga. Näiteks laused „Markus on vallaline“, „Anu on vallaline“ ja „Kristjan on vallaline“, on lihtlaused ja neid peab lausearvutuses tähistama kolme erineva lausemuutujaga, näiteks A, B ja C. Siit aga ei tule nähtavale lausete sarnane kuju ehk see, et kolme inimese kohta antakse üks ja sama kirjeldus.

Lausearvutuse edasiarenduseks on predikaatarvutus, kus ka lihtlauset vaadeldakse koosnevana osadest, *indiviididest* ja *predikaadist*. Näiteks lause „Markus on vallaline“ võib jagada indiviidiks „Markus“ ja predikaadiks „. . . on vallaline“. Indiviide võib samas lauses olla suvaline arv, ka rohkem kui üks. Lauses „Markus armastab Anu“ on „Markus“ ja „Anu“ sarnaselt eelnevaga indiviidid ning konstruktsioon „. . . armastab . . . “ predikaat; lause „Oslo asub Tartust kaugemal kui Moskva“ sisaldab aga kolme indiviidi „Oslo“, „Tartu“ ja „Moskva“ ning predikaati „. . . asub . . . -st kaugemal kui . . . “. Tavaliselt märgivad indiviide lauses nimisõnad ja kõik ülejäänud lausekomponendid moodustavad predikaadi.

Indiviidide arvu järgi liigitatakse predikaadid ühekohalisteks, kahekohalisteks, kolmekohalisteks jne. Ühekohaline predikaat väljendab teatavat omadust, mis konkreetsel indiviidil võib olla või mitte olla. Rakendades näiteks predikaati „. . . on lauamäng“ erinevatele indiviididele, saame lihtlaused „Male on lauamäng“, „Go on lauamäng“, „Tennis on lauamäng“, „Võrkpall on lauamäng“. Iga niimoodi tekkinud lause võib olla tõene või väär, vastavalt sellele, kas indiviidil on predikaadiga antud omadus („olla lauamäng“) või mitte.

Kahe- ja enamakohaline predikaat väljendab seost indiviidide vahel, mis samuti võib kehtida või mitte kehtida. Näiteks predikaadist „$\ldots < \ldots$“ saame lihtlaused „$0 < 0$“, „$0 < 1$“, „$1 < 0$“, „$0 < 2$“ jne.

Kui kahest arvust on esimene väiksem kui teine, siis on predikaat nendel arvudel tõene, vastasel korral aga väär. Samamoodi tähendab kolmekohaline predikaat „$\ldots + \ldots = \ldots$“ seost kolme arvu vahel. Kui valime vabalt kolm arvu a, b, c ning leiame seejärel, et kehtib võrdus $a + b = c$, siis on predikaat nende kolme arvu puhul tõene.

Tavaliselt ei ole predikaatide argumendid ükskõik millised objektid, vaid kuuluvad teatavasse eelnevalt fikseeritud hulka. Rääkides mingist predikaadist, peame ühtlasi näitama, mis liiki objektide kohta see predikaat midagi väidab. Näiteks predikaadi „$\ldots$ on algarv“ puhul võime vaadeldavaks hulgaks valida naturaalarvud; igale naturaalarvule seatakse siis vastavusse lihtlause: „0 on algarv“, „1 on algarv“, „2 on algarv“ jne. Kahekohalise predikaadi puhul saame vastavalt ühe lause iga elemendipaari kohta, kolmekohalise predikaadi puhul iga elemendikolmiku kohta jne. Et loogikas on lausetest olulised ainult nende tõeväärtused, siis võime anda järgmise definitsiooni.

Definitsioon 1. *Hulgal M määratud n-kohaliseks predikaadiks nimetatakse kujutust $P\colon M^n \to \{1, 0\}$.*

Hulka, millel predikaat on määratud, nimetatakse selle predikaadi *indiviidide piirkonnaks*. Edaspidi võimegi mõista predikaadi all kujutust (funktsiooni), mis seab igale hulga M elementidest koostatud n-komponendilisele järjendile $(m_1, m_2, \ldots, m_n)$ vastavusse tõeväärtuse. Ühekohaline predikaat on siis kujutus, mis omistab hulga M igale elemendile tõeväärtuse 1 või 0.

Näide 1. Kui $M = \mathbb{N}$ ja predikaat $A(x) =$ „x on algarv“, siis kehtib $A(0) = 0$, $A(1) = 0$, $A(2) = 1$, $A(3) = 1$, $A(4) = 0$ jne.

Näide 2. Valime hulgaks M kõigi maailmajagude hulga

$$M = \{\mathit{Aafrika}, \mathit{Aasia}, \mathit{Ameerika}, \mathit{Antarktika}, \mathit{Austraalia}, \mathit{Euroopa}\}$$

ning vaatleme predikaati

$$B(x, y) = \text{„}x\text{-i ja } y\text{-i vahel on maismaaühendus“.}$$

Siis näiteks

$$\begin{aligned} &B(\mathit{Aafrika}, \mathit{Aasia}) = 1, && B(\mathit{Ameerika}, \mathit{Aasia}) = 0,\\ &B(\mathit{Aafrika}, \mathit{Ameerika}) = 0, && B(\mathit{Euroopa}, \mathit{Aasia}) = 1,\\ &B(\mathit{Aasia}, \mathit{Ameerika}) = 0, && B(\mathit{Euroopa}, \mathit{Euroopa}) = 1. \end{aligned}$$

Predikaatarvutus üldistab lausearvutust selles mõttes, et predikaadi tõeväärtus võib sõltuda argumentide väärtustest, samas kui lausearvutuse lausel argumendid puuduvad ja tema tõeväärtus on kogu käsitluse jooksul ühesugune. Teinekord vaadeldaksegi lausearvutuse lauseid kui erilisi „nullikohalisi“ predikaate, st „kujutusi“, millel on küll väärtus, aga pole ühtegi argumenti.

Predikaate kui tõeväärtusega lauseid võib omavahel siduda lausearvutuse tehete abil ning moodustada nii lihtsamatest lausetest keerulisemaid. Kui näiteks naturaalarvude hulgal on määratud predikaadid $A(x)$ = „x on paarisarv“ ja $B(x, y)$ = „$x < y$“, siis $A(x)\&B(x, y)$ tähendab „x on paarisarv ja $x < y$“. See on omaette kahekohaline predikaat, seos kahe arvu x ja y vahel, ning teda võib tähistada sümboliga $C(x, y)$. Omaette predikaat on ka $A(x) \,\&\, B(y, z)$, mis sõltub kolmest argumendist ja mida võime märkida sümboliga $D(x, y, z)$. Tähenduse poolest on $D(x, y, z)$ selline seos kolme arvu x, y ja z vahel, mis kehtib parajasti siis, kui x on paarisarv ja $y < z$: näiteks $D(0, 1, 2) = 1$ ja $D(1, 2, 3) = 0$. Samamoodi võib predikaate kombineerida muude lausearvutuse tehete abil, tulemuseks saame jälle mingi predikaadi. Lähtepredikaadid võivad sisaldada erineva arvu argumente, kuid nad peavad olema kõik määratud samal hulgal.

Lisaks lausearvutuse tehetele võib predikaatide puhul kasutada veel kahte spetsiifilist operatsiooni, *kvantoreid*, mis annavad predikaadi tõesuspiirkonna iseloomustuse teatava argumendi järgi.

Olgu $P(x_1, \ldots, x_i, \ldots, x_n)$ hulgal M määratud n-kohaline predikaat. Kirjutis

$$\forall x_i P(x_1, \ldots, x_i, \ldots, x_n)$$

tähistab $(n - 1)$-kohalist predikaati, mis on tõene parajasti siis, kui argumentide x_1, ..., x_{i-1}, x_{i+1}, ..., x_n väärtused on sellised, et hulga M iga elemendi m korral on $P(x_1, \ldots, m, \ldots, x_n)$ tõene. Operaatorit $\forall$ nimetatakse *üldisuskvantoriks* või ka *universaalsuskvantoriks*. Kvantori rakendamisel tekkinud predikaat ei sõltu enam muutujast, mis kvantoriga seoti.

Näide 3. Vaatleme predikaati $A(x, y)$ = „$x \leqslant y$“, kus argumentide väärtused on naturaalarvud. Siis on

$$\forall y A(x, y)$$

teatav ühekohaline predikaat $B(x)$. Sõnalisel kujul kirjapandult väljendab $B(x)$ omadust „x on selline naturaalarv, et iga naturaalarvu y korral $x \leqslant y$“. Näiteks $B(0)$ on tõene, sest iga naturaalarvu y korral tõepoolest $0 \leqslant y$, seevastu $B(1)$ on väär, $B(2)$ on väär, $B(3)$ on väär jne. Teisiti öeldes väljendab $B(x)$ seega omadust „$x = 0$“.

Analoogiliselt, kirjutis

$$\exists x_i P(x_1, \ldots, x_i, \ldots, x_n)$$

tähistab $(n-1)$-kohalist predikaati, mis on tõene parajasti siis, kui argumentide $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ väärtused on sellised, et hulgas M leidub element m, mille korral $P(x_1, \ldots, m, \ldots, x_n)$ on tõene. Operaatorit $\exists$ nimetatakse *olemasolukvantoriks* ehk *eksistentsikvantoriks*. Siingi ei sõltu tulemuseks saadud predikaat enam kvantoriga seotud muutujast.

Näide 4. Olgu nüüd $A(x,y) =$ „$x < y$“, kus argumentide väärtused on naturaalarvud. Siis esitab

$$\exists x A(x,y)$$

teatavat ühekohalist predikaati $B(y)$, mis sõnalisel kujul avaldub lausena „y on selline naturaalarv, et leidub naturaalarv x, mille korral $x < y$“. See predikaat on tõene argumendi y igal niisugusel väärtusel, mille puhul leidub sellest väärtusest väiksem naturaalarv. Näiteks $B(0)$ on väär, $B(1)$ on tõene, $B(2)$ on tõene jne.

Predikaadile kvantori rakendamist nimetatakse ka *kvantifitseerimiseks*. Et kvantori rakendamise tulemus on üldjuhul jällegi teatav predikaat, siis võib sellega sooritada samasuguseid operatsioone nagu teistegi predikaatidega, muu hulgas teda uuesti kvantifitseerida. Kõiki muutujaid kvantoriga sidudes saame lõpuks lause, mis ei sõltu ühestki argumendist ja kujutab seega lihtsalt tõeväärtust.

Näide 5. Vaatleme predikaati $A(x,y,z) =$ „$x + y = z$“ kõigi naturaalarvude hulgal. Siis

$$\exists x A(x,y,z)$$

on kahekohaline predikaat $B(y,z)$, mis väljendab seost „leidub naturaalarv, mida y-le liites saame z-i“. Ilmselt on see predikaat tõene, kui $y \leqslant z$, ja väär, kui $y > z$. Teiste sõnadega, $B(y,z) =$ „$y \leqslant z$“.

Vaatleme nüüd predikaati

$$\forall z B(y,z) = \forall z \exists x A(x,y,z).$$

Siin on vaba ainult muutuja y, seega on meil tegemist teatava predikaadiga $C(y)$. Lähtudes predikaadi $B(y,z)$ tähendusest, näeme, et $C(y)$ on tõene parajasti siis, kui kõikide naturaalarvude z puhul $y \leqslant z$. Järelikult esitab predikaat $C(y)$ lauset „$y = 0$“.

Veel ühe kvantori rakendamisel saame

$$\forall y C(y) = \forall y \forall z B(y,z) = \forall y \forall z \exists x A(x,y,z).$$

See on lause, mis ei sõltu ühestki argumendist ja millel on kindel tõeväärtus. Antud juhul on see tõeväärtus 0, sest ei kehti, et $C(y)$ on iga naturaalarvu y korral tõene.

§ 2. Predikaatarvutuse süntaks

Esitame nüüd reeglid predikaatarvutuse valemite koostamiseks. Predikaatarvutuse laiemate väljendusvõimaluste tõttu on need keerulisemad kui lausearvutuses. Selleks uurime kõigepealt, milliseid sümboleid väidete üleskirjutamiseks tavaliselt vaja läheb.

Algebralistes avaldistes kasutame muutujaid (nagu x, y, z jne), mis võivad tähistada ükskõik millised arve, konstante (näiteks 0, 1, 2 jne), mis märgivad üksikuid fikseeritud arve, ning tehtemärke ja funktsioonide tähiseid arvudega sooritatavate tehete jaoks. Elementaarsetest üksustest — muutujatest ja konstantidest — võime koostada kuitahes keerulisi avaldisi, ühendades neid tehtemärkide abil.

Lihtne on ette kujutada, et sarnasel viisil saame üles ehitada ka muud tüüpi avaldisi peale algebraliste. Seetõttu fikseerime edaspidise üldkujulise käsitluse tarbeks järgmised sümbolite klassid.

- *Indiviidmuutujad*, mida märgime tavaliselt tähtedega u, v, w, x, y, z. Iga indiviidmuutuja võib tähistada vaadeldava hulga ükskõik millist elementi (indiviidi).
- *Konstantsümbolid* a, b, c, d jne. Konstantsümbol tähistab vaadeldava hulga mingit kindlat elementi.
- *Funktsionaalsümbolid* f, g, h jne. Need tähistavad vaadeldaval hulgal määratud funktsioone.

Kõigile tähtedele võib vajaduse korral lisada ka indekseid. Funktsionaalsümboli argumentide arv selgub alati kontekstist.

Reaalarve puudutavates avaldistes on näiteks $+$, $-$ ja $\cdot$ kaheargumendilised funktsionaalsümbolid, sest liitmine, lahutamine ja korrutamine on reaalarvude hulgal määratud kahe muutuja funktsioonid. Komplikatsioonide vältimiseks vaadeldakse predikaatarvutuses enamasti ainult kõikjal määratud funktsioone, mille väärtus kuulub samasse hulka nagu argumendidki. Seega jätame praegu välja jagamise (tulemus pole alati määratud) ja juurimise (tulemus ei tarvitse olla reaalarv). Veel kasutatakse algebras näiteks funktsionaalsümboleid sin, cos, max, min jne. Hoolimata sellest, et taoline „sümbol“ koosneb mitmest märgist, käsitleme teda ikka ühtse tervikuna. Sama kehtib arve tähistavate konstantsümbolite $0, 1, \ldots, 9, 10, 11$ jne kohta.

Avaldiste kirjapanemiseks pole vaja teada sümbolite täpset tähendust, küll aga reegleid, kuidas sümboleid üksteisega ühendada. Nende reeglite rakendamisel saadud objekti nimetatakse termiks, täpsemalt määratleb selle järgmine definitsioon.

Definitsioon 2. *Termid on parajasti need, mida saab koostada alltoodud reeglite abil.*

1) *Iga indiviidmuutuja on term.*
2) *Iga konstantsümbol on term.*
3) *Kui f on n-kohaline funktsionaalsümbol ja $t_1, t_2, \dots, t_n$ on termid, siis $f(t_1, t_2, \dots, t_n)$ on term.*

Termi, milles ei esine ühtegi indiviidmuutujat, nimetatakse *muutujateta termiks*. Niisugune term on seega koostatud ainult konstantsümbolitest ja funktsionaalsümbolitest.

Näide 6. Indiviidmuutujast x, konstantsümbolist c, ühekohalisest funktsionaalsümbolist f ja kahekohalisest funktsionaalsümbolist g võime moodustada näiteks järgmised termid:

$$c \qquad f(c) \qquad g(f(c), f(c)) \qquad f(f(g(x, g(f(x), c))))$$

Neist kolm esimest on muutujateta termid.

Näide 7. Algebraterm on algebraline avaldis. Näiteks järgmised kirjutised on kõik algebratermid:

$$3 \qquad 7 \cdot x \qquad (2 \cdot x) + (5 \cdot y) \qquad (x + 10) \cdot ((2 \cdot x) + (20 \cdot y))$$

Tavaliselt lepitakse siin kokku tehete prioriteet, mille alusel saab osa sulge ära jätta. Samuti kirjutame funktsionaalsümbolid (tehtemärgid) traditsioonilisel viisil argumentide vahele, st mitte $+(x, y)$, nagu termi definitsioon rangelt võttes nõuab.

Näide 8. Kui tegeleme vektoritega kolmemõõtmelises ruumis, siis võime kasutada indiviidmuutujaid $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ (nende väärtusteks võivad olla suvalised vektorid), konstantsümboliteks on telgedesihilised ühikvektorid $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ ning nullvektor $\mathbf{0}$ ja funktsionaalsümboliteks märgid $+$, $-$ ja $\times$, viimane tähistab vektorkorrutise leidmist. Termid on kõik avaldised, mida saab nende tehete abil moodustada, näiteks

$$\boldsymbol{i} \qquad \boldsymbol{w} \qquad \boldsymbol{u} - (\boldsymbol{v} - \boldsymbol{w}) \qquad ((\boldsymbol{u} \times \boldsymbol{i}) + (\boldsymbol{v} \times \boldsymbol{j})) + (\boldsymbol{w} \times \boldsymbol{k})$$

Näide 9. Lausearvutuse valemeid võime samuti vaadelda termidena, kus indiviidmuutujateks on lausemuutujad ning funktsionaalsümboliteks lausearvutuse tehtemärgid $\neg$, &, $\vee$, $\to$, $\leftrightarrow$, kuid selline käsitlus on siiski mõnevõrra ebaharilik. Et lausearvutuse valemi definitsioonis võisid tehete argumentides esineda ainult lausemuutujatest koostatud valemid ja mitte tõeväärtused 1 ja 0, siis konstantsümbolid nendes termides puuduvad.

Kokkuvõttes, term on algebralise avaldise üldistus, kus indiviidmuutujate, konstantsümbolite ja funktsionaalsümbolite tähendusele kitsendusi ei seata. Igal konkreetsel juhul võib termi väärtus olla vaadeldava hulga teatav element. Selleks, et kirja panna elementide omadusi ja nendevahelisi seoseid, kasutame predikaate, märkides neid, nagu juba eelnevas teinud oleme, suurte ladina tähtedega A, B, C jne, mida nimetame *predikaatsümboliteks*. Predikaatsümboli argumentide kohale kirjutasime varem indiviidmuutujad, üldiselt võib aga sinna paigutada suvalise termi. Nii saadud kirjutistest moodustatakse lausearvutuse tehete ja kvantorite abil predikaatarvutuse valemid, nagu näitab järgmine definitsioon.

Definitsioon 3. *Predikaatarvutuse valemid on parajasti need, mida saab koostada alltoodud reeglite abil.*

1) *Kui P on n-kohaline predikaatsümbol ja $t_1, t_2, \dots, t_n$ on termid, siis $P(t_1, t_2, \dots, t_n)$ on predikaatarvutuse valem.*
2) *Kui $\mathcal{F}$ on predikaatarvutuse valem, siis $\neg\mathcal{F}$ on predikaatarvutuse valem.*
3) *Kui $\mathcal{F}$ ja $\mathcal{G}$ on predikaatarvutuse valemid, siis $(\mathcal{F} \,\&\, \mathcal{G})$, $(\mathcal{F} \vee \mathcal{G})$, $(\mathcal{F} \to \mathcal{G})$ ja $(\mathcal{F} \leftrightarrow \mathcal{G})$ on predikaatarvutuse valemid.*
4) *Kui x on indiviidmuutuja ja $\mathcal{F}$ on predikaatarvutuse valem, siis $\forall x\mathcal{F}$ ja $\exists x\mathcal{F}$ on predikaatarvutuse valemid.*

Definitsiooni esimese punkti põhjal koostatud valemeid nimetatakse *atomaarseteks valemiteks* või ka *elementaarvalemiteks*, sest need on kõige lihtsamad predikaatarvutuse valemid, millest koosnevad kõik ülejäänud. Kõiki antud valemi konstrueerimise käigus tekkinud valemeid nimetame nagu lausearvutuseski valemi *osavalemiteks* ehk *alamvalemiteks* ning viimasel konstrueerimissammul kasutatud lausearvutuse tehet või kvantori rakendamist valemi *peatehteks*.

Valemi sulgude suhtes teeme samasugused kokkulepped nagu lausearvutuse valemite puhul. Muu hulgas säilitame lausearvutuse tehete prioriteedi, kvantorid loeme prioriteedilt võrdseks eitusega.

Välja arvatud esinemised vahetult kvantori järel, jagunevad iga indiviidmuutuja kõik muud esinemised valemis seotuteks ja vabadeks. Nimelt, indiviidmuutuja x esineb valemis $\mathcal{F}$ *seotult*, kui ta asub mingi kvantori mõjupiirkonnas, st osavalemit $\forall x\mathcal{G}$ või $\exists x\mathcal{G}$ moodustavas valemis $\mathcal{G}$. Ülejäänud esinemisi nimetatakse *vabadeks*. Kui indiviidmuutuja x esineb valemis $\mathcal{F}$ vabalt, siis märgime sellist valemit mõnikord ka tähisega $\mathcal{F}(x)$. Valemit nimetatakse *kinniseks*, kui tema kõigi indiviidmuutujate kõik esinemised on seotud. Et predikaatarvutuse valemi definitsioon ei aseta indiviidmuutujate paiknemisele mingeid kitsendusi, siis võib üks ja sama indiviidmuutuja esineda valemis nii vabalt kui ka seotult: vaba esinemine jääb niisugusel juhul väljapoole kõigi seda muutujat siduvate kvantorite mõjupiirkondi.

Näide 10. Atomaarsed valemid algebras on näiteks kirjutised

$$y = x + 7 \qquad 2 \cdot x < 3 \cdot x \qquad (x + y) \cdot (y + z) > x + z$$

Predikaatsümboleid oleme siin tähistanud algebras tavaks saanud viisil nagu ka funktsionaalsümboleidki. Mõned mitteatomaarsed valemid on näiteks

$$x = 1 \vee x = 2 \qquad \forall x \forall y (x + y > x) \qquad \neg(y = 0) \rightarrow \exists z (x = y \cdot z)$$

Näide 11. Predikaatarvutuse valemis

$$\exists x (A(x) \rightarrow \neg B(y)) \,\&\, C(x)$$

on olemasolukvantori mõjupiirkonnaks konjunktsiooni vasak pool. Indiviidmuutuja x esinemine osavalemis $A(x)$ on seotud (sest ta asub kvantori mõjupiirkonnas), esinemine osavalemis $C(x)$ aga vaba. Indiviidmuutuja y esinemine osavalemis $B(y)$ on vaba, sest talle ei rakendu ühtegi kvantorit. Et valemis leidub vabu muutujaid, siis see valem ei ole kinnine.

Olgu $\mathcal{F}(x)$ valem, milles indiviidmuutuja x esineb vabalt, ning t muutujateta term või üldisemalt selline term, mis ei sisalda vabalt ühtegi sellist indiviidmuutujat, millele indiviidmuutuja x mõnes vaba esinemise kohas valemis $\mathcal{F}(x)$ ulatuks siduva kvantori mõjupiirkond. Kirjutisega $\mathcal{F}(t)$ märgime siis valemit, mis tekib pärast indiviidmuutuja x kõigi vabade esinemiste asendamist termiga t. Tingimus termi t vabade muutujate kohta garanteerib selle, et pärast niisugust asendamist ei satu ükski termis t vabalt esinev indiviidmuutuja kvantori alla.

Näide 12. Asendades valemis

$$\mathcal{F}(x) = \exists y (P(x, y) \,\&\, Q(y, x))$$

indiviidmuutuja x konstantsümboliga c, saame valemi

$$\mathcal{F}(c) = \exists y (P(c, y) \,\&\, Q(y, c)),$$

asendades aga indiviidmuutuja x termiga $f(z)$, saame valemi

$$\mathcal{F}(f(z)) = \exists y (P(f(z), y) \,\&\, Q(y, f(z))).$$

Pannes mitmesuguseid väiteid kirja predikaatarvutuse valemitega, võivad väidete tüübist sõltumatud sümbolid, nagu lausearvutuse tehtemärgid, kvantorid, sulud ja indiviidmuutujad, esineda ükskõik millistes valemites, olgu siis tegemist valemitega, mis puudutavad naturaalarve, reaalarve, vektoreid, alamhulki või muid objekte. Seevastu konstant-, funktsionaal- ja predikaatsümbolid võivad teooriati erineda. Tihtipeale fikseeritakse need kolm sümbolite klassi eelnevalt ning lubatakse valemites kasutada ainult sümboleid, mis kuuluvad kindlaksmääratud klassidesse. Kolmikut $\sigma = \langle C\,; F\,; P\rangle$, kus C on konstantsümbolite, F funktsionaalsümbolite ja P predikaatsümbolite hulk, nimetatakse *signatuuriks*; vastavalt nimetatakse predikaatarvutuse valemit, milles esinevad konstantsümbolid kuuluvad kõik hulka C, funktsionaalsümbolid hulka F ning predikaatsümbolid hulka P, *valemiks signatuuris* σ. Alati eeldatakse, et predikaatsümbolite hulk P pole tühi, sest muidu pole võimalik selles signatuuris kirja panna ühtegi valemit. Küll aga võivad hulgad C ja F olla tühjad, samuti võivad kõik kolm hulka olla lõpmatud.

Näide 13. Naturaalarve puudutavate väidete kirjapanemisel võime fikseerida signatuuri $\langle 0, 1\,; +, \cdot\,; =\rangle$. Iga valem selles signatuuris võib siis sisaldada ainult konstantsümboleid 0 ja 1, funktsionaalsümboleid $+$ ja $\cdot$ ning predikaatsümbolit $=$, näiteks

$$\neg\exists y(x \cdot y = 1) \qquad \text{või} \qquad \forall x \forall y(x + y = y + x)$$

Ükski valem ei tohi aga sisaldada muid erisümboleid nagu 2 või $<$.

Üldiselt püütakse signatuur valida nii, et ta sisaldaks käsitletava ainevalla tavalisemaid sümboleid. Kindel signatuur aitab väljendusvõimaluste paljususes teatavat korda luua ning sellest tulenevalt ka paremini uurida kõigi võimalike valemite hulga omadusi.

§ 3. Predikaatarvutuse semantika

Valemi tõeväärtus sõltub sellest, milliste objektide kohta ta midagi väidab ja kuidas temas esinevaid sümboleid mõistetakse. Näiteks valem $\forall x(x \geqslant 0)$ pole ise ei tõene ega väär, vaid tema tõeväärtus oleneb vaadeldavatest objektidest: kui nendeks on naturaalarvud, siis on valem tõene; kui aga vaadeldavad objektid on reaalarvud, siis on valem väär. Kuid lisaks sõltub valemi tõeväärtus ka sümbolite $\geqslant$ ja 0 tähendusest. Arvude puhul on neil küll olemas loomulik kindlakskujunenud tähendus, aga kui valem väljendab mingit väidet mitte arvude, vaid näiteks inimeste kohta, siis tuleb nimetatud sümbolite sisu ilmutatult ette anda. Näiteks kui loeme, et $\geqslant$ tähendab seost „on sündinud samal hetkel või hiljem“ ning 0 piiblitegelast Aadamat, siis (muidugi eeldusel, et piiblilegend paika peab) on kõnealune valem tõene. Kui aga $\geqslant$ tähendab seost „on vähemalt sama vana“ ja 0 käesoleva raamatu lugejat, siis on valem väär.

Objektide hulga fikseerib ja sümbolitele annab tähenduse interpretatsioon, mis defineeritakse järgmiselt.

Definitsioon 4. *Interpretatsioon on paar $\alpha = (M_\alpha, I_\alpha)$, kus M_α on mingi mittetühi hulk, mida nimetatakse põhihulgaks ehk interpretatsiooni kandjaks, ja I_α on interpreteeriv kujutus, mis teisendab*

1) *iga konstantsümboli hulga M_α mingiks elemendiks;*
2) *iga n-kohalise funktsionaalsümboli mingiks (kõikjal määratud) n-kohaliseks funktsiooniks hulgal M_α;*
3) *iga n-kohalise predikaatsümboli mingiks n-kohaliseks predikaadiks hulgal M_α.*

Predikaatsümbolile P vastavat predikaati interpretatsioonis α tähistame kirjutisega P^α või $\alpha(P)$. Kui interpretatsioon on eelnevalt fikseeritud ning ei ole karta segadust, siis võib interpretatsiooni tähise ära jätta. Taolise tähistusviisi kanname üle funktsionaal- ja konstantsümbolitele, laiendades seda edaspidi ka termidele ja valemitele.

Tuleb vahet teha sümbolil ja objektil, mida see sümbol tähistab. Näiteks on predikaatsümbol ja temale vastav hulgal M_α määratud predikaat erinevad asjad. Mõni teine interpretatsioon võib samale predikaatsümbolile seada vastavusse teise predikaadi. Niisugune vahetegemine tähise ja talle omistatava sisu vahel on kasulik selle poolest, et siis võib predikaatsümboleid ning samuti ka predikaatarvutuse valemeid käsitleda kui puhtalt süntaktilisi objekte ja rakendada nendega opereerimisel sisust sõltumatuid meetodeid.

Näide 14. Interpreteerime valemit $\forall x \exists y P(x, y)$ kolmel viisil.

1) Valime interpretatsiooni α, milles põhihulk on $M_\alpha = \mathbb{N}$ ning predikaatsümbolile P vastab predikaat $P^\alpha(x, y) =$ „$x > y$“. Valem omandab selles interpretatsioonis tähenduse „iga naturaalarvu jaoks leidub temast väiksem naturaalarv“. Et selline väide ei kehti, siis on valem selles interpretatsioonis väär.

2) Olgu nüüd antud interpretatsioon β põhihulgaga $M_\beta = \mathbb{R}^+$ ja $P^\beta(x, y) =$ „$xy = 1$“. Valemi tähendus on „igal positiivsel reaalarvul leidub positiivne reaalarvuline pöördarv“. Selline väide on tõene.

3) Valime interpretatsiooni γ, kus M_γ on kõigi geomeetriliste kehade hulk ning $P^\gamma(x, y)$ = „x mahub y-i sisse“. Interpretatsioonis γ on valemi tähenduseks „iga geomeetrilise keha jaoks leidub teda hõlmav keha“. See väide on samuti tõene.

Nagu näeme, võib ühel ja samal valemil olla eri interpretatsioonides erinev tähendus ja vastavalt sellele ka erinev tõeväärtus. Kui ütleme, et mingi valem on tõene või väär, tuleb seega kindlasti täpsustada, millises interpretatsioonis seda valemit vaatleme.

Valemi tõeväärtuse arvutamiseks etteantud interpretatsioonis tuleb kõigepealt kindlaks määrata valemis esinevate termide väärtused, nende põhjal saab leida atomaarsete valemite tõeväärtused ja edasi loogiliste tehetega kogu valemi tõeväärtuse. Analoogia süntaksi ja semantika vahel, nagu nägime lausearvutuse valemite juures, peab siingi paika, sest süntaktiliste üksuste (termide, valemite) induktiivne defineerimine toob kaasa võimaluse arvutada ka väärtus induktiivselt: kui on teada mingil sammul konstrueeritud termide või valemite väärtus, siis saab määrata järgmisel sammul konstrueeritavate termide või valemite väärtuse.

Et üldiselt võivad termid ja valemid sisaldada ka vabu indiviidmuutujaid, siis omistame viimastele kõigepealt mingid konkreetsed väärtused interpretatsiooni põhihulgast.

Definitsioon 5. *Termi t väärtus t^α interpretatsioonis α vabade muutujate fikseeritud väärtustel leitakse järgmiste reeglite abil.*

1) *Kui $t = x$, kus x on indiviidmuutuja, siis t^α on muutuja x väärtus.*
2) *Kui $t = c$, kus c on konstantsümbol, siis $t^\alpha = c^\alpha$.*
3) *Kui $t = f(t_1, t_2, \ldots, t_n)$, kus f on n-kohaline funktsionaalsümbol ja t_1, t_2, …, t_n on termid, siis $t^\alpha = f^\alpha(t_1^\alpha, t_2^\alpha, \ldots, t_n^\alpha)$.*

Kui term ei sisalda muutujaid, siis alustatakse tema väärtuse arvutamist konstantsümbolite väärtustest ehk põhihulga elementidest, mille interpretatsioon α konstantsümbolitele vastavusse seab. Seejärel rakendatakse samm-sammult funktsioone, mida interpretatsioon α seab vastavusse funktsionaalsümbolitele, kuni viimase funktsiooni väärtus annabki termi väärtuse. Kui term sisaldab muutujaid, siis saame niisugust protseduuri rakendada alles pärast seda, kui oleme muutujatele andnud väärtused. Muutujate väärtuste valimisel aga mingeid piiranguid ei ole, nad võivad olla interpretatsiooni põhihulga suvalised elemendid. Sisuliselt seatakse interpretatsiooni α kaudu igale muutujateta termile vastavusse põhihulga M_α element, muutujaid sisaldavale termile aga põhihulgal M_α määratud funktsioon, mille väärtus sõltub termis esinevate indiviidmuutujate väärtustest.

Termi väärtuse leidmisel tuleb esile ka olemuslik vahe konstantsümboli ja indiviidmuutuja vahel. Konstantsümboli väärtus on alati põhihulga mingi kindel element, mis on määratud interpretatsiooniga, indiviidmuutuja väärtus võib aga olla ükskõik milline. See vastab matemaatikas tavapärasele käsitlusele, kus konstandi väärtus on fikseeritud, muutuja väärtus aga võib vabalt muutuda. Põhjusel, et muutujal puudub vaadeldavate objektide mõttes konkreetne väärtus, jäetakse indiviidmuutujad, erinevalt konstantsümbolitest, tavaliselt välja ka signatuurist, kui see fikseeritakse mingi valdkonna valemite kirjapanemise tarbeks.

Näide 15. Vaatleme uuesti näidet 6. Valime interpretatsiooni α põhihulgaga $M_\alpha = \mathbb{N}$, kusjuures interpreteeriv kujutus I_α seab konstantsümbolile c vastavusse arvu 0, ühekohalisele funktsionaalsümbolile f vastavusse funktsiooni $f^\alpha(x) = x + 1$ ning kahekohalisele funktsionaalsümbolile g funktsiooni $g^\alpha(x, y) = x + y$. Näites toodud termide väärtused arvutatakse siis järgmiselt.

Term	Väärtus
c	0
$f(c)$	1
$g(f(c), f(c))$	2
$f(f(g(x, g(f(x), c))))$	$2x + 3$

Et viimane term sisaldab indiviidmuutujat x, siis sõltub tema väärtus muutuja x väärtusest. Näiteks juhul $x = 0$ on termi väärtus 3, juhul $x = 1$ on termi väärtus 5 jne.

Definitsioon 6. *Predikaatarvutuse valemi $\mathcal{F}$ tõeväärtus $\mathcal{F}^\alpha$ interpretatsioonis α vabade muutujate fikseeritud väärtustel leitakse järgmiste reeglite abil.*

1) *Kui $\mathcal{F} = P(t_1, t_2, \ldots, t_n)$, kus P on n-kohaline predikaatsümbol ja t_1, t_2, …, t_n on termid, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $P^\alpha(t_1^\alpha, t_2^\alpha, \ldots, t_n^\alpha) = 1$.*
2) *Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 0$.*
3) *Kui $\mathcal{F} = \mathcal{G}\&\mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ ja $\mathcal{H}^\alpha = 1$.*
4) *Kui $\mathcal{F} = \mathcal{G}\vee\mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ või $\mathcal{H}^\alpha = 1$.*
5) *Kui $\mathcal{F} = \mathcal{G}\rightarrow\mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 0$ või $\mathcal{H}^\alpha = 1$.*
6) *Kui $\mathcal{F} = \mathcal{G}\leftrightarrow\mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ ja $\mathcal{H}^\alpha = 1$ või $\mathcal{G}^\alpha = 0$ ja $\mathcal{H}^\alpha = 0$.*

7) *Kui $\mathcal{F} = \forall x\mathcal{G}$, siis $\mathcal{F}^{\alpha} = 1$ parajasti siis, kui põhihulga M_{α} iga elemendi m korral $\mathcal{G}^{\alpha}_{[x/m]} = 1$, kus $[x/m]$ tähendab, et muutuja x väärtuseks loetakse element m.*
8) *Kui $\mathcal{F} = \exists x\mathcal{G}$, siis $\mathcal{F}^{\alpha} = 1$ parajasti siis, kui põhihulgas M_{α} leidub selline element m, et $\mathcal{G}^{\alpha}_{[x/m]} = 1$, kus $[x/m]$ tähendab, et muutuja x väärtuseks loetakse element m.*

Termide väärtuste järgi määratakse definitsiooni punktis 1 atomaarsete valemite tõeväärtused. Predikaatarvutuse atomaarsed valemid on teatavas mõttes analoogilised lausemuutujatega lausearvutuses. Tõeväärtuste ülekandmine lihtsamatelt valemitelt keerulisematele punktides 2—6 toimub täpselt samamoodi nagu lausearvutuses. Kvantorreeglid 7 ja 8 annavad tingimused, millal on tõene kvantoriga valem: kvantori all asuv valem peab olema tõene, kui indiviidmuutuja x väärtuseks on kas ükskõik milline (üldisuskvantori korral) või mingi üks (olemasolukvantori korral) põhihulga element. Kinnise valemi korral saame loetletud reegleid rakendades tulemuseks valemi tõeväärtuse interpretatsioonis α. Kui aga valem sisaldab vabu muutujaid, siis võime nende reeglitega leida valemi tõeväärtuse vabade muutujate suvalistel väärtustel, nii et sel juhul seab interpretatsioon α valemile vastavusse teatava põhihulgal M_{α} määratud predikaadi.

Näide 16. Olgu antud signatuur $\sigma = \langle 0, 1, \ldots; +, \cdot; =, < \rangle$ (signatuur sisaldab omaette konstantsümboli iga naturaalarvu tähistamiseks). Vaatleme selles signatuuris kirjapandud valemite tõeväärtusi kolmes interpretatsioonis.

1) Interpretatsioon α, kus $M_{\alpha} = \mathbb{N}$ ning kõiki signatuuri sümboleid interpreteeritakse standardselt (nii, nagu on kombeks matemaatikas).
2) Interpretatsioon β, kus $M_{\beta} = \mathbb{R}$ ning signatuuri sümboleid interpreteeritakse standardselt.
3) Interpretatsioon γ, kus $M_{\gamma} = \{0, 1\}$. Konstantsümbolite puhul olgu
$$c^{\gamma} = \begin{cases} 0, & \text{kui } c \text{ on paarisarvu sümbol,} \\ 1, & \text{kui } c \text{ on paaritu arvu sümbol.} \end{cases}$$
Seega tähistavad sümbolid 0, 2, 4, ... kõik põhihulga M_{γ} elementi 0, sümbolid 1, 3, 5, ... aga kõik põhihulga elementi 1. Summamärki interpreteerime hulgal M_{γ} liitmisena mooduli 2 järgi: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 0$. Ülejäänud sümboleid interpreteerime standardselt.

Järgnevas tabelis on esitatud mõned valemid signatuuris σ ning nende tõeväärtused interpretatsioonides α, β ja γ.

Valem	α	β	γ
$0 = 2$	0	0	1
$1 + 2 = 3$	1	1	1
$\forall x(x < x + 1)$	1	1	0
$\forall x \exists y(x < y)$	1	1	0
$\forall x \exists y(y < x)$	0	1	0
$\forall x \forall y(x < y \to \exists z(x < z \,\&\, z < y))$	0	1	0
$\forall x \forall y_1 \forall y_2(x + y_1 = x + y_2 \to y_1 = y_2)$	1	1	1
$\forall x \forall y \exists z(x + z = y)$	0	1	1
$\forall x \forall y \exists z(x \cdot z = y)$	0	0	0
$\forall x \forall y(\neg(x = 0) \to \exists z(x \cdot z = y))$	0	1	1

Kui valime interpretatsiooni α puhul valemi $\mathcal{F}(x)$ vaba muutuja x väärtuseks põhihulga elemendi m, siis märgime valemi tõeväärtust edaspidi tähise $(\mathcal{F}(x))^{\alpha}_{[x/m]}$ asemel tähisega $\mathcal{F}(m)^{\alpha}$, või kui interpretatsioon on kontekstist selge, kirjutame lihtsalt $\mathcal{F}(m)$.

Interpretatsiooni α, milles valem $\mathcal{F}$ on tõene oma vabade muutujate kõikidel väärtustel, nimetatakse valemi $\mathcal{F}$ *mudeliks*. Sel juhul räägitakse, et valem $\mathcal{F}$ on tõene mudelis α. Analoogiliselt nimetatakse interpretatsiooni α valemite hulga $\{\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n\}$ mudeliks, kui see interpretatsioon on iga üksiku valemi mudel.

Tõeväärtuste leidmisel ja valemite analüüsimisel tuleb arvestada, et $\forall x\mathcal{F} = 0$ *ei tähenda*, et valem $\mathcal{F}$ on iga x korral väär. Valem $\forall x\mathcal{F}$ on väär parajasti siis, kui valem $\neg\forall x\mathcal{F}$ on tõene. Vaatleme näiteks valemit $\forall xA(x)$. Kui $\forall xA(x) = 1$, siis kehtib väide „Igal elemendil on omadus A“. Kui aga $\forall xA(x) = 0$, siis kehtib „Pole õige, et igal elemendil on omadus A“ ehk „Leidub element, millel pole omadust A“, selle tähendus pole sama mis väitel „Ühelgi elemendil pole omadust A“. Analoogiliselt ei tähenda $\exists x\mathcal{F} = 0$ mitte „Leidub element, mille korral $\mathcal{F}$ on väär“, vaid „Ei leidu elementi, mille korral $\mathcal{F}$ on tõene“, teisiti öeldes, „$\mathcal{F}$ on iga x korral väär“.

Valemile, mis sisaldab vabu muutujaid, vastab teatav põhihulgal määratud predikaat. Kui on fikseeritud signatuur, siis tuleb valemite koostamisel piirduda signatuuris näidatud sümbolitega. Seepärast tekib tihti küsimus, kuidas antud signatuuris panna kirja valem, mille interpretatsioon oleks etteantud predikaat. Kui valemi $\mathcal{F}$ interpretatsioon ja predikaat P on vabade muutujate kõikidel väärtustel sama tõeväärtusega, siis ütleme, et valem $\mathcal{F}$ *väljendab* predikaati P.

Näide 17. Vaatleme väiteid naturaalarvude kohta. Signatuur olgu $\langle 0, 1\,; +, \cdot\,; =\rangle$, kõiki sümboleid interpreteerime tavapärasel viisil.

Väide (predikaat) „$x = 2$“ tuleb väljendada näiteks valemiga

$$x = 1 + 1,$$

sest sümbol 2 pole signatuuriga lubatud.

Väite „$x \leqslant y$“ saab väljendada valemiga

$$\exists z(x + z = y).$$

Väite „x on paarisarv“ saab väljendada valemiga

$$\exists y(x = y + y).$$

Näide 18. Olgu nüüd tegemist väidetega, mis puudutavad naturaalarvude hulga $\mathbb{N}$ alamhulki, ning olgu antud signatuur $\langle\,;\,;\subseteq\rangle$, kus konstantsümbolite hulk ja funktsionaalsümbolite hulk on tühjad. Ainukese predikaatsümboli interpretatsioon olgu standardne.

Väidet „X on tühi hulk“ väljendab valem

$$\forall Y(X \subseteq Y).$$

Väite „Hulkade X ja Y ühend on Z“ saame väljendada valemiga

$$(X \subseteq Z)\,\&\,(Y \subseteq Z)\,\&\,\forall W((X \subseteq W)\,\&\,(Y \subseteq W) \to (Z \subseteq W)).$$

Sõnades on see „Z sisaldab hulka X ja Z sisaldab hulka Y ning suvaline hulk W, mis sisaldab hulki X ja Y, sisaldab ka hulka Z“ (ehk lühemalt „Z on vähim hulk, mis sisaldab hulki X ja Y“). Teine võimalus sama väidet kirja panna on valem

$$\forall W((X \subseteq W)\,\&\,(Y \subseteq W) \leftrightarrow (Z \subseteq W)).$$

Näeme, et mõne predikaadi väljendamiseks tuleb rakendada üsnagi kunstlikke võtteid, kuid sellised raskused tekivad üldse peaaegu alati, kui on vaja mingit ideed kirja panna eelnevalt kindlaksmääratud vahendite abil.

Kuigi predikaatarvutuse abil on võimalik väljendada paljusid selliseid seoseid, mida lausearvutuse abil ei saa, pole siiski ka predikaatarvutuse vahendid piisavad, et panna kirja üldse kõiki mõeldavaid väiteid näiteks matemaatikas. Järgmine samm väljendusvõimaluste laiendamise suunas on tuua indiviidmuutujate kõrval sisse funktsioon- ja predikaatmuutujad ning lubada kvantoritel siduda ka neid, nagu näiteks valemis $\forall P \exists f \forall x P(f(x))$. Sel juhul on tegemist teist järku predikaatarvutusega, vastandina käesolevas raamatus käsitletavale esimest järku predikaatarvutusele. Põhihulga elemente (mida valemites tähistavad indiviidmuutujad ja konstantsümbolid) mõistetakse esimest järku objektidena, põhihulgal määratud funktsioonid ja predikaadid on teist järku objektid.

§ 4. Valemite omadused

Analoogiliselt lausearvutusega võib ka predikaatarvutuses rääkida samaselt tõestest, samaselt vääradest ja kehtestatavatest valemitest, lausemuutujate väärtustusele vastab predikaatarvutuses interpretatsioon. Et üldiselt võib predikaatarvutuse valem sisaldada vabu indiviidmuutujaid, siis tuleb valemi tõeväärtuse üheseks fikseerimiseks ka nendele väärtused omistada.

Definitsioon 7. *Predikaatarvutuse valemit $\mathcal{F}$ nimetatakse*

- *samaselt tõeseks, kui ta on tõene igas interpretatsioonis oma vabade muutujate kõikidel väärtustel;*
- *samaselt vääraks, kui ta on väär igas interpretatsioonis oma vabade muutujate kõikidel väärtustel.*

Samaselt tõest predikaatarvutuse valemit nimetatakse ka *tautoloogiaks* või *loogiliselt tõeseks valemiks*, samaselt väära valemit aga *kontradiktsiooniks* või *loogiliselt vääraks valemiks*. Asjaolu, et valem $\mathcal{F}$ on samaselt tõene, märgitakse kirjutisega $\models \mathcal{F}$.

Kõigist predikaatarvutuse valemitest kuuluvad samaselt tõeste hulka kindlasti need, mille võib saada lausearvutuse samaselt tõestest valemitest, kui neis asendada iga lausemuutuja mingi predikaatarvutuse valemiga. Näiteks on valem $\exists x P(x) \vee \neg \exists x P(x)$ samaselt tõene. Sarnaselt saab lausearvutuse samaselt vääradest valemitest tuletada samaselt vääri predikaatarvutuse valemeid. Kuid predikaatarvutuses leidub ka selliseid samaselt tõeseid valemeid, millel puudub analoog lausearvutuses. Veendumaks, et niisugused valemid on samaselt tõesed, tuleb lähtuda otse ülaltoodud definitsioonist.

Näide 19. Tõestada, et valem

$$\forall x P(x) \vee \exists x \neg P(x)$$

on samaselt tõene.

Olgu α vabalt valitud interpretatsioon. Et valemis vabu muutujaid ei esine, siis nende väärtusi fikseerima ei pea. Kui disjunktsiooni vasak pool on interpretatsioonis α tõene, st $\forall x P(x) = 1$, siis on valem tõene. Kui aga $\forall x P(x) = 0$, siis peab põhihulgas M_α leiduma vähemalt üks element m, mille puhul $P(m) = 0$. Siis aga $\neg P(m) = 1$, mis tähendab, et $\exists x \neg P(x) = 1$. Seega on nüüd tõene disjunktsiooni parem pool ja ühtlasi kogu valem. Et interpretatsioon α oli suvaline, siis on valem $\mathcal{F}$ tõene igas interpretatsioonis ehk samaselt tõene.

Lausearvutuse valemi samaselt tõesust võisime kontrollida tõeväärtustabeliga, sest valemi lausemuutujatele saab anda ainult lõpliku hulga väärtustusi. Predikaatarvutuse valemi puhul tuleks otse definitsiooni järgides leida valemi tõeväärtus kõigis interpretatsioonides, neid aga on lõpmata palju. Et seda ei saa teha ka mingil muul moel, näitas ameerika matemaatik Alonzo Church (1903—1995), kes aastal 1936 tõestas *predikaatarvutuse mittelahenduvuse teoreemi*: pole olemas algoritmi, mis suudaks suvalise predikaatarvutuse valemi puhul kindlaks teha, kas valem on samaselt tõene või mitte. Seega tuleb valemi samaselt tõesuse määramiseks paratamatult kasutada meetodeid, mis annavad tulemuse vaid osade valemite korral.

Definitsioon 8. *Predikaatarvutuse valemit $\mathcal{F}$ nimetatakse kehtestatavaks, kui ta on tõene vähemalt ühes interpretatsioonis vabade muutujate mingitel väärtustel.*

Näide 20. Valem $\exists x A(x)$ on kehtestatav, sest leidub interpretatsioon, kus see valem on tõene: valime põhihulgaks kõigi naturaalarvude hulga ja predikaatsümboli A interpretatsiooniks predikaadi „... on paarisarv“, st $A(x)$ tähistab väidet „x on paarisarv“. Samuti on valem $\forall x B(x, y)$ kehtestatav: valime põhihulgaks jällegi naturaalarvude hulga, predikaatsümboli B interpretatsiooniks seose $\geqslant$ sellel hulgal ning anname vabale muutujale y väärtuse 0.

Predikaatarvutuse valemiklassid on üksteisega samasuguses vahekorras nagu lausearvutuses, ka tõestused on analoogilised.

Teoreem 1. *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt väär.*

Tõestus. Valemite $\mathcal{F}$ ja $\neg\mathcal{F}$ tõeväärtused on alati vastupidised, sõltumata interpretatsioonist ja valemites esinevate vabade muutujate väärtustest. Seega kui $\mathcal{F}$ on igas interpretatsioonis vabade muutujate kõikidel väärtustel tõene, siis on $\neg\mathcal{F}$ igas interpretatsioonis vabade muutujate kõikidel väärtustel väär ning ümberpöördult. □

Teoreem 2. *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eitus $\neg\mathcal{F}$ ei ole samaselt tõene.*

Tõestus. Kui $\mathcal{F}$ on kehtestatav, siis ta on mingis interpretatsioonis vabade muutujate mingitel väärtustel tõene. Valem $\neg\mathcal{F}$ on sel juhul aga väär ega saa olla samaselt tõene. Ümberpöördult, kui $\neg\mathcal{F}$ ei ole samaselt tõene, siis on ta mingis interpretatsioonis mingil vabade muutujate väärtustel väär. Siis on aga valem $\mathcal{F}$ tõene, mistõttu ta on kehtestatav. □

Ka predikaatarvutuse valemite puhul saab valemit tõeseks või vääraks muutva interpretatsiooni leidmiseks kasutada tõesuspuid. Lausearvutuse tehetele lisanduvad veel reeglid, mis näitavad valemi edasist analüüsi juhul, kui valem algab kvantoriga:

$$\begin{array}{cccc}
\forall x\mathcal{F}(x)=1 & \forall x\mathcal{F}(x)=0 & \exists x\mathcal{F}(x)=1 & \exists x\mathcal{F}(x)=0 \\
| & | & | & | \\
\mathcal{F}(t)=1 & \mathcal{F}(c)=0 & \mathcal{F}(c)=1 & \mathcal{F}(t)=0 \\
t\text{ on olemas-} & c\text{ on uus kons-} & c\text{ on uus kons-} & t\text{ on olemas-} \\
\text{olev term} & \text{tantsümbol} & \text{tantsümbol} & \text{olev term}
\end{array}$$

Tingimust $\forall x\mathcal{F}(x)=1$ saame kasutada alles siis, kui tõesuspuu uuritavas harus on olemas mingi term t, sest siis võime sooritada analüüsisammu: kui valem $\mathcal{F}(x)$ on tõene iga x korral, siis on ta tõene ka termi t korral. Sama olukord on tingimusega $\exists x\mathcal{F}(x)=0$, millest saame järeldada, et $\mathcal{F}(x)$ on suvalise olemasoleva termi korral väär. Et valemi osadeks lahutamise hilisematel etappidel võib tekkida uusi terme, siis võib olla vaja kasutada neid tingimusi mitu korda, mistõttu neid ei märgistata tärniga.

Tingimusi $\forall x\mathcal{F}(x)=0$ ja $\exists x\mathcal{F}(x)=1$ kasutatakse seevastu ainult üks kord, nende puhul tuleb sisse tuua uus konstantsümbol, mis erineb kõigist tõesuspuu vaadeldavas harus esinevatest termidest: näiteks kui $\exists x\mathcal{F}(x)=1$, siis pole alust ütelda, et element, mille leidumist see tingimus väidab, langeb kokku mõne olemasolevaga.

Näide 21. Näidata, et valem

$$(\exists xA(x)\to\forall xB(x))\to\forall x(A(x)\to B(x))$$

on samaselt tõene.

Kontrollime, kas valem saab olla väär. Moodustame tõesuspuu

$$\begin{array}{c}
(\exists xA(x)\to\forall xB(x))\to\forall x(A(x)\to B(x))=0 \quad {}^{(1)}\ \star \\
| \\
\exists xA(x)\to\forall xB(x)=1 \quad {}^{(4)}\ \star \\
| \\
\forall x(A(x)\to B(x))=0 \quad {}^{(2)}\ \star \\
| \\
A(a)\to B(a)=0 \quad {}^{(3)}\ \star \\
| \\
A(a)=1 \\
| \\
B(a)=0 \\
\swarrow \qquad \searrow \\
\begin{array}{cc}
\exists xA(x)=0 \quad {}^{(5)} & \forall xB(x)=1 \quad {}^{(6)} \\
| & | \\
A(a)=0 & B(a)=1 \\
\times & \times
\end{array}
\end{array}$$

Sammul (2) toome sisse uue konstantsümboli a, sellest tulenevalt on meil sammudel (5) ja (6) olemas term, nii et vastavat reeglit on võimalik rakendada. Et tõesuspuu mõlemad harud annavad vastuolu, siis ei saa valem üheski interpretatsioonis olla väär. Seega on valem tõepoolest samaselt tõene.

Näide 22. Näidata, et valem

$$\forall x(A(x) \to B(x)) \to (\exists x A(x) \to \forall x B(x))$$

ei ole samaselt tõene.

Analoogiliselt eelnevaga moodustame tõesuspuu

$$\forall x(A(x) \to B(x)) \to (\exists x A(x) \to \forall x B(x)) = 0 \quad {\scriptstyle (1)}\ \star$$
$$\forall x(A(x) \to B(x)) = 1 \quad {\scriptstyle ((5),\ (7))}\ \star$$
$$\exists x A(x) \to \forall x B(x) = 0 \quad {\scriptstyle (2)}\ \star$$
$$\exists x A(x) = 1 \quad {\scriptstyle (3)}\ \star$$
$$\forall x B(x) = 0 \quad {\scriptstyle (4)}\ \star$$
$$A(a) = 1$$
$$B(b) = 0$$
$$A(a) \to B(a) = 1 \quad {\scriptstyle (6)}\ \star$$
$$\begin{array}{cc} A(a) = 0 & B(a) = 1 \\ \times & \\ & A(b) \to B(b) = 1 \quad {\scriptstyle (8)}\ \star \\ & \begin{array}{cc} A(b) = 0 & B(b) = 1 \\ & \times \end{array} \end{array}$$

Paneme tähele, et sammudel (3) ja (4) võtame kasutusele kaks erinevat konstantsümbolit ning sammudel (5) ja (7) kasutame kummagi kohta valemi $\forall x(A(x) \to B(x))$ tõesust. Haru, mis lõpeb tingimusega $A(b) = 0$, enam jätkata ei saa, sest kõik valemid on jagatud elementaarvalemiteks. Et selles harus vastuolu ei tekkinud, siis oleme leidnud interpretatsiooni, kus valem on väär: valime põhihulgaks hulga $M_\alpha = \{a, b\}$ ning määrame predikaatsümbolite A ja B interpretatsiooni α seostega $A^\alpha(a) = 1$, $A^\alpha(b) = 0$, $B^\alpha(a) = 1$, $B^\alpha(b) = 0$. Antud valem on selles interpretatsioonis väär, järelikult pole tegemist samaselt tõese valemiga.

Mõnikord võib tõesuspuu koostamise juures tekkida tõrge seetõttu, et valemi struktuur nõuab edasise tegevusena kas tingimuse $\forall x \mathcal{F}(x) = 1$ või tingimuse $\exists x \mathcal{F}(x) = 0$ analüüsimist, aga ühtegi termi vaadeldavas puuharus varem ei esine. Taoline olukord tuleb ette näiteks valemi $\forall x A(x) \to \exists x A(x)$ puhul, kui püüame kindlaks teha, kas see valem saab olla mingis interpretatsioonis väär:

$$\begin{array}{c}
\forall x A(x) \to \exists x A(x) = 0 \quad {}^{(1)\ \star} \\
| \\
\forall x A(x) = 1 \\
| \\
\exists x A(x) = 0
\end{array}$$

Et aga interpretatsiooni põhihulk ei saa olla tühi, siis võime sellistel juhtudel eeldada, et mingi element on alati olemas ja tähise esimese elemendi jaoks ise sisse tuua. Pärast seda kulgeb analüüs standardsel viisil. Ülaltoodud näidet jätkates saame tõesuspuu

$$\begin{array}{c}
\forall x A(x) \to \exists x A(x) = 0 \quad {}^{(1)\ \star} \\
| \\
\forall x A(x) = 1 \quad {}^{(2)} \\
| \\
\exists x A(x) = 0 \quad {}^{(3)} \\
| \\
A(a) = 1 \\
| \\
A(a) = 0 \\
\times
\end{array}$$

mis näitab, et valem $\forall x A(x) \to \exists x A(x)$ on samaselt tõene.

Tõesuspuu abil saab leida interpretatsiooni, kus valemil on etteantud tõeväärtus, või näidata selle puudumist küll paljudel juhtudel, kuid siiski mitte alati.

Näide 23. Kontrollida, kas valem $\forall x \exists y P(x, y)$ on kehtestatav.

Eelnevas kirjeldatud võtetega tekib puu

$$\begin{array}{c}
\forall x \exists y P(x, y) = 1 \quad {}^{(1),\ (3)} \\
| \\
\exists y P(a, y) = 1 \quad {}^{(2)\ \star} \\
| \\
P(a, b) = 1 \\
| \\
\exists y P(b, y) = 1 \quad {}^{(4)\ \star} \\
| \\
P(b, c) = 1 \\
\vdots
\end{array}$$

Olemasolukvantorit lahti kirjutades tuleb iga kord sisse tuua uus konstantsümbol, pärast seda annab aga lähtetingimus uue olemasolukvantorit sisaldava valemi. Tõesuspuu ei saa seega kunagi valmis ega võimalda teha lõppjäreldust valemi kohta. Kui jätkaksime puu konstrueerimist piiramatult, siis annaks see küll interpretatsiooni lõpmatu põhihulgaga $M_\alpha = \{a, b, c, \dots\}$, kusjuures $P^\alpha(a, b) = 1$, $P^\alpha(b, c) = 1, \dots$, millest nähtub, et valem $\forall x \exists y P(x, y)$ on selles interpretatsioonis tõene, kuid meetodi tööaeg oleks sel juhul lõpmatu. Me võime püüda täiendada tõesuspuude meetodit nii, et ta arvestaks seda ja teisi analoogilisi juhte, kuid nagu Churchi teoreem predikaatarvutuse mittelahenduvuse kohta näitab, ei saa ükski täiendamine viia meetodini, mis annaks kõigi valemite puhul lõpliku aja jooksul õige vastuse.

§ 5. Samaväärsus

Kanname predikaatarvutuse valemitele üle ka järeldumise ja samaväärsuse mõiste.

Definitsioon 9. *Ütleme, et valemitest $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, kui igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel, kus valemid $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene.*

Täiesti sarnaselt lausearvutuse valemitega võib tõestada, et valemitest $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$ parajasti siis, kui valem $\mathcal{F}_1 \mathbin{\&} \mathcal{F}_2 \mathbin{\&} \dots \mathbin{\&} \mathcal{F}_n \to \mathcal{G}$ on samaselt tõene.

Definitsioon 10. *Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse samaväärseteks, kui nende tõeväärtused on võrdsed igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel.*

On selge, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ ja valemist $\mathcal{G}$ järeldub valem $\mathcal{F}$. Samuti on lihtne näha, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valem $\mathcal{F} \leftrightarrow \mathcal{G}$ on samaselt tõene.

Kõik lausearvutuse põhisamaväärsused kehtivad ka predikaatarvutuses. Näiteks De Morgani seadused

$$\neg(\mathcal{F} \mathbin{\&} \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}, \qquad \neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \mathbin{\&} \neg\mathcal{G}$$

kehtivad sõltumata sellest, kas $\mathcal{F}$ ja $\mathcal{G}$ on lause- või predikaatarvutuse valemid: vasak ja parem pool on samaväärsed tänu valemite erilisele kombineerimisviisile. Predikaatarvutuses leidub aga samaväärseid valemeid, mille samaväärsust ei ole võimalik tõestada ainuüksi lausearvutuse vahenditega. Vaatleme näiteks lauseid

$$\neg\forall x A(x) = \text{„Pole nii, et kõik on ausad“},$$
$$\exists x \neg A(x) = \text{„Leidub neid, kes pole ausad“}.$$

Ilmselt on nendel lausetel ühesugune sisu. Lausearvutuse seisukohalt on mõlemad laused aga lihtlaused ja nende struktuur avaneb alles predikaatarvutuses.

Predikaatarvutuse spetsiifilised samaväärsused käsitlevad kvantorite seost lausearvutuse tehete ja teiste kvantoritega. Olulisimad nendest samaväärsustest on järgmised.

1) Kvantori ja eituse vahetamisseadus:
$$\neg\forall x \mathcal{F}(x) \equiv \exists x \neg\mathcal{F}(x), \qquad \neg\exists x \mathcal{F}(x) \equiv \forall x \neg\mathcal{F}(x).$$

2) Kvantorite distributiivsus:
$$\forall x(\mathcal{F}(x) \mathbin{\&} \mathcal{G}(x)) \equiv \forall x \mathcal{F}(x) \mathbin{\&} \forall x \mathcal{G}(x),$$
$$\exists x(\mathcal{F}(x) \vee \mathcal{G}(x)) \equiv \exists x \mathcal{F}(x) \vee \exists x \mathcal{G}(x).$$

3) Kui indiviidmuutuja x ei esine valemis $\mathcal{G}$ vabalt, siis
$$\forall x(\mathcal{F}(x) \mathbin{\&} \mathcal{G}) \equiv \forall x \mathcal{F}(x) \mathbin{\&} \mathcal{G}, \quad \exists x(\mathcal{F}(x) \mathbin{\&} \mathcal{G}) \equiv \exists x \mathcal{F}(x) \mathbin{\&} \mathcal{G},$$
$$\forall x(\mathcal{F}(x) \vee \mathcal{G}) \equiv \forall x \mathcal{F}(x) \vee \mathcal{G}, \quad \exists x(\mathcal{F}(x) \vee \mathcal{G}) \equiv \exists x \mathcal{F}(x) \vee \mathcal{G}.$$

4) Kui indiviidmuutuja x ei esine valemis $\mathcal{G}$ vabalt, siis
$$\forall x(\mathcal{F}(x) \to \mathcal{G}) \equiv \exists x \mathcal{F}(x) \to \mathcal{G}, \quad \exists x(\mathcal{F}(x) \to \mathcal{G}) \equiv \forall x \mathcal{F}(x) \to \mathcal{G}.$$
Kui indiviidmuutuja x ei esine valemis $\mathcal{F}$ vabalt, siis
$$\forall x(\mathcal{F} \to \mathcal{G}(x)) \equiv \mathcal{F} \to \forall x \mathcal{G}(x), \quad \exists x(\mathcal{F} \to \mathcal{G}(x)) \equiv \mathcal{F} \to \exists x \mathcal{G}(x).$$

5) Seotud muutujate ümbernimetamine:
$$\forall x \mathcal{F}(x) \equiv \forall y \mathcal{F}(y), \qquad \exists x \mathcal{F}(x) \equiv \exists y \mathcal{F}(y),$$
kus y ei esine valemis $\mathcal{F}(x)$.

6) Samaliigiliste kvantorite kommutatiivsus:
$$\forall x \forall y \mathcal{F}(x, y) \equiv \forall y \forall x \mathcal{F}(x, y),$$
$$\exists x \exists y \mathcal{F}(x, y) \equiv \exists y \exists x \mathcal{F}(x, y).$$

Põhjendame mõne nendest samaväärsustest. Samaväärsuse tõestamiseks näitame, et kehtib järeldumine kummaski suunas.

1. rühma 1. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\neg\forall x \mathcal{F}(x) = 1$. Siis $\forall x \mathcal{F}(x) = 0$. Seega pole nii, et interpretatsiooni põhihulga iga elemendi $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$ (st $(\mathcal{F}(x))^{\alpha}_{[x/m]} = 1$), vaid leidub niisugune $m_0 \in M_\alpha$, et $\mathcal{F}(m_0) = 0$. Siis aga $\neg\mathcal{F}(m_0) = 1$ ja olemasolukvantori mõiste kohaselt $\exists x \neg\mathcal{F}(x) = 1$.

Ümberpöördult, eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\exists x \neg\mathcal{F}(x) = 1$. Siis peab leiduma element $m_0 \in M_\alpha$, et $\neg\mathcal{F}(m_0) = 1$ ehk $\mathcal{F}(m_0) = 0$. Kuna leidub element nii, et valem $\mathcal{F}(x)$ on väär, siis $\forall x\mathcal{F}(x) = 0$. Järelikult $\neg\forall x\mathcal{F}(x) = 1$.

Niisiis oleme saanud, et alati, kui valem $\neg\forall x\mathcal{F}(x)$ on tõene, on ka valem $\exists x \neg\mathcal{F}(x)$ tõene ja ümberpöördult. See tähendab, et need valemid on samaväärsed.

1. rühma 2. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\neg\exists x\mathcal{F}(x) = 1$. Näitame, et siis ka $\forall x\neg\mathcal{F}(x) = 1$. Valime suvalise elemendi $m \in M_\alpha$. Kui oleks $\neg\mathcal{F}(m) = 0$ ehk $\mathcal{F}(m) = 1$, siis oleks $\exists x\mathcal{F}(x) = 1$ ehk $\neg\exists x\mathcal{F}(x) = 0$, mis on vastuolus eeldusega. Järelikult peab kehtima $\neg\mathcal{F}(m) = 1$. Et m oli suvaline element, siis $\forall x\neg\mathcal{F}(x) = 1$.

Ümberpöördult, eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x\neg\mathcal{F}(x) = 1$. Oletame väitevastaselt, et $\neg\exists x\mathcal{F}(x) = 0$. Siis $\exists x\mathcal{F}(x) = 1$. Seega leidub põhihulgas M_α element m_0, mille korral $\mathcal{F}(m_0) = 1$ ehk $\neg\mathcal{F}(m_0) = 0$. Seetõttu $\forall x\neg\mathcal{F}(x) = 0$ (sest $\neg\mathcal{F}(x)$ ei ole iga x korral tõene). Viimane tulemus on vastuolus eeldusega. Järelikult meie oletus ei saa kehtida ja tõepoolest $\neg\exists x\mathcal{F}(x) = 1$.

2. rühma 1. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x(\mathcal{F}(x) \& \mathcal{G}(x)) = 1$. Näitame, et siis ka $\forall x\mathcal{F}(x) \& \forall x\mathcal{G}(x) = 1$. Konjunktsiooni tõesuseks piisab näidata, et mõlemad liikmed on tõesed. Tõestame, et $\forall x\mathcal{F}(x) = 1$. Selleks valime põhihulgast M_α suvalise elemendi m. Eeldusest saame, et elemendi m korral $\mathcal{F}(m) \& \mathcal{G}(m) = 1$, millest $\mathcal{F}(m) = 1$. Et m oli suvaline elementi, siis $\forall x\mathcal{F}(x) = 1$. Analoogiliselt põhjendame, et ka konjunktsiooni teine liige on tõene.

Eeldame nüüd, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x\mathcal{F}(x)\&\forall x\mathcal{G}(x) = 1$. Näitame, et siis ka $\forall x(\mathcal{F}(x)\&\mathcal{G}(x)) = 1$. Valime suvalise elemendi $m \in M_\alpha$. Eelduse põhjal $\forall x\mathcal{F}(x) = 1$ ja $\forall x\mathcal{G}(x) = 1$, mistõttu $\mathcal{F}(m) = 1$ ja $\mathcal{G}(m) = 1$. Seega $\mathcal{F}(m)\&\mathcal{G}(m) = 1$. Et m oli suvaline, siis $\forall x(\mathcal{F}(x)\&\mathcal{G}(x)) = 1$.

2. rühma 2. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel $\exists x(\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$. Siis leidub interpretatsiooni põhihulgas selline element $m_0 \in M_\alpha$, et $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$. Kui disjunktsioon on tõene põhjusel, et tema esimene liige on tõene, st $\mathcal{F}(m_0) = 1$, siis on $\exists x \mathcal{F}(x) = 1$ ja $\exists x \mathcal{F}(x) \vee \exists x \mathcal{G}(x) = 1$. Kui disjunktsioon on tõene seetõttu, et tema teine liige on tõene, siis saame analoogiliselt $\exists x \mathcal{F}(x) \vee \exists x \mathcal{G}(x) = 1$.

Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\exists x \mathcal{F}(x) \vee \exists x \mathcal{G}(x) = 1$. Kui selles valemis on $\exists x \mathcal{F}(x) = 1$, siis leidub element $m_0 \in M_\alpha$ nii, et $\mathcal{F}(m_0) = 1$. Järelikult $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$ ja $\exists x(\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$. Kui aga $\exists x \mathcal{G}(x) = 1$, siis leidub element $m_0 \in M_\alpha$, mille korral $\mathcal{G}(m_0) = 1$, järelikult $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$ ja $\exists x(\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$ ka sellel juhul.

Kvantoritega lausete puhul võib formuleerida kindlad üldised põhimõtted, kuidas nende lausetega tuleb tõestamisel ümber käia. Kui eeldus algab kvantoriga $\exists$ (nagu esimeses tõestuses paremalt vasakule ja 2. rühma 2. samaväärsuses vasakult paremale), siis teame, et põhihulgas leidub teatav element m_0, et kvantorialune avaldis on tõene, ja me võime kvantori ära jätta. Kui väide algab kvantoriga $\forall$, siis võime lähtuda väitest: püüame tõestada, et väite kvantorialune avaldis on tõene iga elemendi m korral. Keerulisemad on aga juhud, kus eeldus algab kvantoriga $\forall$ või väide algab kvantoriga $\exists$.

Eeldust kujul $\forall x \ldots$ saame kasutada alles siis, kui mingi element m on fikseeritud. Sel juhul järeldub eeldusest, et kvantorialune valem kehtib ka elemendi m korral. Samuti, kui väide on kujul $\exists x \ldots$, siis võime ütelda, et see väide kehtib, kui oleme suutnud leida mingi elemendi m_0, mille korral kvantorialune avaldis on tõene. Kui aga seda elementi pole, siis väidet otsese meetodiga tõestada ei saa.

Üldse on eelduse ja väite jaoks võimalikud neli kvantorite kombinatsiooni: $\forall$–$\forall$, $\forall$–$\exists$, $\exists$–$\forall$, $\exists$–$\exists$. Neist esimeses ja kolmandas on väide sobival kujul, võime võtta põhihulgast suvalise elemendi m ja asuda tõestama, et elemendi m korral kehtib väites kvantorialune avaldis. Kolmanda ja neljanda kombinatsiooni puhul on eeldus sobival kujul, sel juhul võime alustada tõestust eeldusest, tähistades sümboliga m_0 seda põhihulga elementi, mille korral on eelduses kvantorialune avaldis tõene. Kõige keerulisem on teine juht, kus ei saa otse lähtuda ei eeldusest ega väitest. Siin tuleb kasutada kaudseid tõestusmeetodeid, nagu näiteks vastuväiteline tõestus.

Kui eelduse või väite peatehteks pole mitte kvantor, vaid mingi lausearvutuse tehe, siis tuleb loomulikult kõigepealt rakendada lausearvutuse reegleid: näiteks kui eeldus avaldub kahe liikme disjunktsioonina, siis tuleb eraldi vaadelda juhte, mil tõene on emb-kumb disjunktsiooni pool.

Arusaadavalt ei seisa küsimus siinkohal ainult predikaatarvutuse samaväärsuste tõestamises, niisuguseid võtteid läheb vaja suvaliste matemaatiliste väidete tõestamiseks ja ka igapäevaelus ettetulevate arutluste kontrollimiseks.

3. rühma 1. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x(\mathcal{F}(x) \& \mathcal{G}) = 1$. Vaja on näidata, et $\forall x \mathcal{F}(x) \& \mathcal{G} = 1$ ehk $\forall x \mathcal{F}(x) = 1$ ja $\mathcal{G} = 1$. Tõestame esiteks, et $\forall x \mathcal{F}(x) = 1$. Valime põhihulgas suvalise elemendi $m \in M_\alpha$. Eeldusest saame siis $\mathcal{F}(m) \& \mathcal{G} = 1$, millest $\mathcal{F}(m) = 1$. Et m on suvaline, järeldub siit $\forall x \mathcal{F}(x) = 1$. Teiseks tõestame, et $\mathcal{G} = 1$. Kui $\mathcal{G}$ oleks väär, siis võttes põhihulgas vabalt mingi elemendi $m_0 \in M_\alpha$, näeme, et eelduses on kvantorialune avaldis $\mathcal{F}(m_0) \& \mathcal{G}$ väär ja seega oleks väär ka eeldus ise.

Ümberpöördult, eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x \mathcal{F}(x) \& \mathcal{G} = 1$. Näitame, et $\forall x(\mathcal{F}(x) \& \mathcal{G}) = 1$. Eeldusest leiame $\forall x \mathcal{F}(x) = 1$ ja $\mathcal{G} = 1$. Siit enam edasi minna ei saa, sest eelduse ees on üldisuskvantor. Kuid väide on sobival kujul. Olgu $m \in M_\alpha$ põhihulga suvaline element. Eelduse põhjal siis $\mathcal{F}(m) = 1$, mistõttu $\mathcal{F}(m) \& \mathcal{G} = 1$. Et m oli suvaline element, siis ka $\forall x(\mathcal{F}(x) \& \mathcal{G}) = 1$.

3. rühma 2. samaväärsus. Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x(\mathcal{F}(x) \vee \mathcal{G}) = 1$. Näitame, et $\forall x \mathcal{F}(x) \vee \mathcal{G} = 1$. Siin ei saa otse midagi ette võtta ei eelduse ega väitega. Väites esineb küll sobivalt kvantor $\forall$, kuid peatehe pole mitte kvantor, vaid disjunktsioon. Seega püüame tõestada vastuväiteliselt. Oletame, et väide ei kehti, st $\forall x \mathcal{F}(x) \vee \mathcal{G} = 0$. Siis peab olema $\forall x \mathcal{F}(x) = 0$ ja $\mathcal{G} = 0$. Et valem $\forall x \mathcal{F}(x)$ on väär, siis leidub element $m_0 \in M_\alpha$, et $\mathcal{F}(m_0)$ on väär. Selle elemendi korral on $\mathcal{F}(m_0) \vee \mathcal{G} = 0$, sest $\mathcal{G}$ on väär sõltumata elemendist m_0. Üldisuskvantori definitsiooni tõttu saame $\forall x(\mathcal{F}(x) \vee \mathcal{G}) = 0$, vastuolu.

Eeldame, et fikseeritud interpretatsioonis α ja valemite vabade muutujate väärtustel on $\forall x \mathcal{F}(x) \vee \mathcal{G} = 1$. Valime põhihulgast suvalise elemendi m. Kui disjunktsioonis on tõene esimene liige, st $\forall x \mathcal{F}(x) = 1$, siis ka $\mathcal{F}(m) = 1$ ja $\mathcal{F}(m) \vee \mathcal{G} = 1$. Kui disjunktsioonis on tõene teine liige, siis samuti $\mathcal{F}(m) \vee \mathcal{G} = 1$. Järelikult on suvalise elemendi m korral $\mathcal{F}(m) \vee \mathcal{G} = 1$, seega $\forall x(\mathcal{F}(x) \vee \mathcal{G}) = 1$.

Ülejäänud 3. rühma samaväärsused tõestatakse analoogiliselt ja nendel me enam pikemalt ei peatu. 4. rühma samaväärsusi saab tõestada samuti vahetu aruteluga, aga olles eelnevas kindlaks teinud mitmed samaväärsused, võime kasutada neid valemite teisendamisel.

4. rühma 1. samaväärsus. Lähtume vasakust poolest ja teisendame selle paremaks pooleks. Kõigepealt elimineerime lausearvutuse seaduste põhjal implikatsiooni:

$$\forall x(\mathcal{F}(x) \to \mathcal{G}) \equiv \forall x(\neg\mathcal{F}(x) \vee \mathcal{G}).$$

Tekkinud valemile võime rakendada 3. rühma 2. samaväärsust, sest valem $\mathcal{G}$ ei sisalda muutujat x vabalt. Saame

$$\forall x(\neg\mathcal{F}(x) \vee \mathcal{G}) \equiv \forall x\neg\mathcal{F}(x) \vee \mathcal{G}.$$

1. rühma 2. samaväärsuse abil toome eituse kvantori alt välja:

$$\forall x\neg\mathcal{F}(x) \vee \mathcal{G} \equiv \neg\exists x\mathcal{F}(x) \vee \mathcal{G}.$$

Kasutame uuesti implikatsiooni avaldist teiste tehete kaudu:

$$\neg\exists x\mathcal{F}(x) \vee \mathcal{G} \equiv \exists x\mathcal{F}(x) \to \mathcal{G}.$$

Sellega on samaväärsus tõestatud.

Ülejäänud selle rühma samaväärsusi saab tõestada samasuguse võttega. Kahe viimase rühma tõestused on sirgjoonelised.

Samaväärsuste puhul tuleb veel tähele panna, et mitmed eelnevatega sarnased seosed ei kehti. Näiteks ei tarvitse kehtida distributiivsus üldisuskvantori ja disjunktsiooni vahel, kui mõlemad valemid sisaldavad kvantori all asuvat muutujat vabalt. Teiste sõnadega,

$$\forall x(\mathcal{F}(x) \vee \mathcal{G}(x)) \qquad \text{ja} \qquad \forall x\mathcal{F}(x) \vee \forall x\mathcal{G}(x)$$

ei ole üldiselt samaväärsed. Selles veendumiseks piisab leida kasvõi üks interpretatsioon, kus nende valemite tõeväärtused erinevad.

Vaatleme näiteks juhtu, kus valemid $\mathcal{F}(x)$ ja $\mathcal{G}(x)$ kujutavad endast kõige lihtsama võimaliku juhuna atomaarseid valemeid, st olgu $\mathcal{F}(x) = A(x)$ ja $\mathcal{G}(x) = B(x)$. Valime interpretatsiooni α põhihulgaga $M_\alpha = \mathbb{N}$, kusjuures $A(x)$ tähistab väidet „x on paarisarv“ ja $B(x)$ väidet „x on paaritu arv“. Selles interpretatsioonis on

$$\forall x(A(x) \vee B(x)) = 1,$$

sest valemi tähendus on „Iga naturaalarv on kas paaris või paaritu“. Seevastu

$$\forall xA(x) \vee \forall xB(x) = 0,$$

sest selle valemi tähendus on „Iga naturaalarv on paaris või iga naturaalarv on paaritu“.

Sama interpretatsioon sobib ka näitamaks, et valemid

$$\exists x(\mathcal{F}(x) \mathbin{\&} \mathcal{G}(x)) \qquad \text{ja} \qquad \exists x\mathcal{F}(x) \mathbin{\&} \exists x\mathcal{G}(x)$$

ei tarvitse olla samaväärsed, ehk distributiivsus olemasolukvantori ja konjunktsiooni vahel ei kehti üldjuhul samuti.

Lisaks sellele ei tohi vahetada eriliigilisi kvantoreid, st alati ei ole samaväärsed ka valemid

$$\forall x \exists y \mathcal{F}(x,y) \qquad \text{ja} \qquad \exists y \forall x \mathcal{F}(x,y).$$

Eeldame, et valemi $\mathcal{F}(x,y)$ kujuks on jällegi teatav atomaarne valem $C(x,y)$, teiste sõnadega, võrdleme valemeid $\forall x \exists y C(x,y)$ ja $\exists y \forall x C(x,y)$. Valime predikaatsümboli C interpretatsiooniks põhihulgal $M = \{a,b\}$ määratud predikaadi, mida esitab tabel

y x	a	b
a	1	0
b	0	1

Valem $\forall x \exists y C(x,y)$ väidab siis, et selle tabeli igas veerus leidub väärtus 1, valem $\exists y \forall x C(x,y)$ väidab aga, et leidub rida, milles kõik väärtused on 1. Ilmselt on esimene valem tõene ja teine väär.

Veel üks interpretatsioon, mille abil saab näidata, et niisugune samaväärsus ei kehti, on selline, kus põhihulk on naturaalarvude hulk $\mathbb{N}$ ja $C(x,y)$ tähendab seost „$x < y$“. Esimese valemi tähendus on „Iga naturaalarvu korral leidub naturaalarv, mis on temast suurem“, teise valemi tähendus seevastu „Leidub naturaalarv, mis on suurem igast naturaalarvust“.

§ 6. Valemi prefikskuju

Predikaatarvutuse valemi prefikskuju on lähtekoht paljudele algoritmidele, teiste hulgas näiteks teoreemide automaattõestamises ning tehisintellektisüsteemides kasutatavale resolutsioonimeetodile. Prefikskujul olevas valemis on kõik kvantorid koondatud valemi ette.

Definitsioon 11. *Ütleme, et valem $\mathcal{F}$ on prefikskujul, kui*

$$\mathcal{F} = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \mathcal{F}',$$

kus $Q_1, Q_2, \ldots, Q_n$ on kvantorid, $x_1, x_2, \ldots, x_n$ indiviidmuutujad ja $\mathcal{F}'$ kvantoriteta valem, mida nimetatakse valemi $\mathcal{F}$ maatriksiks.

Järgnevas asume tegelema küsimusega, kuidas viia predikaatarvutuse valemit prefikskujule.

Teoreem 3. *Iga valemi jaoks leidub temaga samaväärne prefikskujul valem.*

Tõestus. Olgu $\mathcal{F}$ suvaline valem. Tõestame teoreemi induktsiooniga valemi struktuuri järgi.

Induktsiooni baas. Kui $\mathcal{F}$ on kujul $P(t_1, t_2, \ldots, t_n)$, kus P on n-kohaline predikaatsümbol ja t_1, t_2, …, t_n on termid, siis valemil $\mathcal{F}$ on juba nõutav kuju.

Induktsiooni samm. Vaatleme eraldi juhte valemi ehituse järgi.

Juht 1. Olgu valem $\mathcal{F}$ kujul $\neg\mathcal{F}_1$. Induktsiooni eelduse põhjal leidub valemiga $\mathcal{F}_1$ samaväärne prefikskujul valem $\mathcal{G}_1$. Olgu

$$\mathcal{G}_1 = Q_1x_1Q_2x_2\ldots Q_nx_n\mathcal{G}_1',$$

kus $\mathcal{G}_1'$ ei sisalda kvantoreid. Leides mõlemast poolest eituse, saame esialgse valemiga $\mathcal{F}$ samaväärse valemi. Kvantori ja eituse vahetamisseaduste põhjal

$$\mathcal{F} \equiv \neg(Q_1x_1Q_2x_2\ldots Q_nx_n\mathcal{G}_1') \equiv \overline{Q_1}x_1\overline{Q_2}x_2\ldots\overline{Q_n}x_n\neg\mathcal{G}_1',$$

kus

$$\overline{Q_i} = \begin{cases} \exists, & \text{kui } Q_i = \forall, \\ \forall, & \text{kui } Q_i = \exists. \end{cases}$$

Viimane valem on prefikskujul, sest $\neg\mathcal{G}_1'$ ei sisalda kvantoreid.

Juht 2. Olgu valem $\mathcal{F}$ kujul $\mathcal{F}_1 \,\&\, \mathcal{F}_2$. Induktsiooni eelduse põhjal leiduvad valemiga $\mathcal{F}_1$ samaväärne valem $\mathcal{G}_1$ ja valemiga $\mathcal{F}_2$ samaväärne valem $\mathcal{G}_2$, mis mõlemad on prefikskujul. Nimetades vajaduse korral valemites $\mathcal{G}_1$ ja $\mathcal{G}_2$ seotud muutujaid ümber, võime eeldada, et need valemid ei sisalda ühiseid seotud muutujaid ja et ükski kvantor ei seo muutujat, mis esineb valemis $\mathcal{G}_1$ või $\mathcal{G}_2$ vabalt. Olgu

$$\begin{aligned} \mathcal{G}_1 &= Q_{11}x_1Q_{12}x_2\ldots Q_{1n_1}x_{n_1}\mathcal{G}_1', \\ \mathcal{G}_2 &= Q_{21}y_1Q_{22}y_2\ldots Q_{2n_2}y_{n_2}\mathcal{G}_2', \end{aligned}$$

kus valemid $\mathcal{G}_1'$ ja $\mathcal{G}_2'$ ei sisalda kvantoreid. Siis valem $\mathcal{G}_1 \,\&\, \mathcal{G}_2$ on samaväärne valemiga $\mathcal{F}$ ning predikaatarvutuse samaväärsuste 3. rühma ja konjunktsiooni kommutatiivsuse abil saame

$$\begin{aligned} \mathcal{F} &\equiv Q_{11}x_1Q_{12}x_2\ldots Q_{1n_1}x_{n_1}\mathcal{G}_1' \,\&\, Q_{21}y_1Q_{22}y_2\ldots Q_{2n_2}y_{n_2}\mathcal{G}_2' \equiv \\ &\equiv Q_{11}x_1Q_{12}x_2\ldots Q_{1n_1}x_{n_1}(\mathcal{G}_1' \,\&\, Q_{21}y_1Q_{22}y_2\ldots Q_{2n_2}y_{n_2}\mathcal{G}_2') \equiv \\ &\equiv Q_{11}x_1Q_{12}x_2\ldots Q_{1n_1}x_{n_1}(Q_{21}y_1Q_{22}y_2\ldots Q_{2n_2}y_{n_2}\mathcal{G}_2' \,\&\, \mathcal{G}_1') \equiv \\ &\equiv Q_{11}x_1Q_{12}x_2\ldots Q_{1n_1}x_{n_1}Q_{21}y_1Q_{22}y_2\ldots Q_{2n_2}y_{n_2}(\mathcal{G}_2' \,\&\, \mathcal{G}_1'). \end{aligned}$$

Viimane valem ongi prefikskujul.

Juht 3. Olgu valem $\mathcal{F}$ kujul $\mathcal{F}_1 \vee \mathcal{F}_2$. Lausearvutuse samaväärsustega saame selle valemi teisendada valemiks $\neg(\neg\mathcal{F}_1 \,\&\, \neg\mathcal{F}_2)$. Juhtude 1 ja 2 põhjal leidub viimase valemiga samaväärne valem prefikskujul.

Juht 4. Olgu valem $\mathcal{F}$ kujul $\mathcal{F}_1 \to \mathcal{F}_2$. Teisendame selle valemi kujule $\neg\mathcal{F}_1 \vee \mathcal{F}_2$ ning rakendame juhte 1 ja 3.

Juht 5. Olgu valem $\mathcal{F}$ kujul $\mathcal{F}_1 \leftrightarrow \mathcal{F}_2$. Teisendame valemi kujule $\mathcal{F}_1 \& \mathcal{F}_2 \vee \neg \mathcal{F}_1 \& \neg \mathcal{F}_2$ ning rakendame juhte 1, 2 ja 3.

Juht 6. Olgu valem $\mathcal{F}$ kujul $\forall x \mathcal{F}_1$. Induktsiooni eelduse põhjal leidub valemiga $\mathcal{F}_1$ samaväärne prefikskujul valem $\mathcal{G}_1$, olgu

$$\mathcal{G}_1 = Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{G}_1',$$

kus $\mathcal{G}_1'$ ei sisalda kvantoreid. Siis

$$\mathcal{F} \equiv \forall x Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{G}_1',$$

mis ongi otsitav prefikskuju.

Juht 7. Olgu valem $\mathcal{F}$ kujul $\exists x \mathcal{F}_1$. Teisendame valemi kujule $\neg \forall x \neg \mathcal{F}_1$ ning rakendame juhte 1 ja 6. □

Saab formuleerida ka algoritmi valemi viimiseks prefikskujule. Variante selleks on mitmeid, järgnevas esitame ühe võimaluse.

Olgu antud valem $\mathcal{F}$, mis on vaja viia prefikskujule.

1) Elimineerime implikatsioonid ja ekvivalentsid, kasutades lausearvutuse samaväärsusi

$$\mathcal{G} \to \mathcal{H} \equiv \neg \mathcal{G} \vee \mathcal{H}, \qquad \mathcal{G} \leftrightarrow \mathcal{H} \equiv \mathcal{G} \& \mathcal{H} \vee \neg \mathcal{G} \& \neg \mathcal{H}.$$

2) Viime eitused kvantorite alla predikaatarvutuse põhisamaväärsuste

$$\neg \forall x \mathcal{G}(x) \equiv \exists x \neg \mathcal{G}(x), \qquad \neg \exists x \mathcal{G}(x) \equiv \forall x \neg \mathcal{G}(x)$$

abil. Kahekordsed eitused jätame ära.

3) Nimetame seotud muutujad ümber nii, et iga kvantor seoks erinevat muutujat ja et ükski kvantor ei seoks muutujat, mis esineb kuskil vabalt.

4) Kasutades seadusi

$$\forall x \mathcal{G}(x) \& \mathcal{H} \equiv \forall x (\mathcal{G}(x) \& \mathcal{H}), \quad \exists x \mathcal{G}(x) \& \mathcal{H} \equiv \exists x (\mathcal{G}(x) \& \mathcal{H}),$$
$$\forall x \mathcal{G}(x) \vee \mathcal{H} \equiv \forall x (\mathcal{G}(x) \vee \mathcal{H}), \quad \exists x \mathcal{G}(x) \vee \mathcal{H} \equiv \exists x (\mathcal{G}(x) \vee \mathcal{H})$$

ning vajaduse korral konjunktsiooni ja disjunktsiooni kommutatiivsust, toome kvantorid osavalemite eest valemi ette.

Näide 24. Teisendada prefikskujule valem

$$\mathcal{F} = \forall x \exists y P(x, y) \& (Q(z) \to \neg \forall x (R(x, y) \vee P(x, x))).$$

Avaldame implikatsiooni teiste tehete kaudu:

$$\mathcal{F} \equiv \forall x \exists y P(x, y) \& (\neg Q(z) \vee \neg \forall x (R(x, y) \vee P(x, x))).$$

Viimase kvantori eest viime eituse kvantori alla:

$$\mathcal{F} \equiv \forall x \exists y P(x, y) \& (\neg Q(z) \vee \exists x \neg (R(x, y) \vee P(x, x))).$$

Nüüd tuleb ümber nimetada seotud muutujad, et kõik seotud muutujad erineksid kõikidest vabadest muutujatest ja kõik kvantorid viitaksid erinevatele muutujatele. Muutuja x esineb kahes kvantoris, esimeses ja viimases. Muutuja y esineb seotult olemasolukvantoris ja vabalt konjunktsiooni paremas pooles. Muutuja z esineb ainult vabalt. Seega nimetame ümber muutuja x teise esinemise ja muutuja y ainsa seotud esinemise:

$$\mathcal{F} \equiv \forall x \exists u P(x,u) \,\&\, (\neg Q(z) \vee \exists v \neg (R(v,y) \vee P(v,v))).$$

Lõpuks toome kõik kvantorid sulgude ette:

$$\begin{aligned}\mathcal{F} &\equiv \forall x \exists u P(x,u) \,\&\, \exists v\, (\neg Q(z) \vee \neg (R(v,y) \vee P(v,v))) \equiv \\ &\equiv \forall x \exists u (P(x,u) \,\&\, \exists v\, (\neg Q(z) \vee \neg (R(v,y) \vee P(v,v)))) \equiv \\ &\equiv \forall x \exists u \exists v\, (P(x,u) \,\&\, (\neg Q(z) \vee \neg (R(v,y) \vee P(v,v)))).\end{aligned}$$

Viimane valem ongi prefikskujul.

Predikaatarvutuse valemi prefikskuju ei ole üheselt määratud. Valemi $\forall x A(x) \& \forall x B(x)$ puhul võime näiteks rakendada eeltoodud algoritmi ja saada tulemuseks valemi $\forall x \forall y (A(x) \,\&\, B(y))$. Samas võime kasutada ka predikaatarvutuse põhiseadusi, mille kohaselt on antud valem samaväärne valemiga $\forall x (A(x) \& B(x))$. Mõlemad kujud sobivad prefikskujuks, mõlemad on samaväärsed esialgse valemiga ja loomulikult ka omavahel.

Sageli teisendatakse teatavale standardkujule ka valemi maatriks Et maatriks kvantoreid ei sisalda, siis on selline teisendamine sisuliselt lihtsalt lausearvutuse valemi teisendamine, kus igale atomaarsele valemile vastab omaette lausemuutuja. Niisuguse valemi saab viia disjunktiivsele või konjunktiivsele normaalkujule.

Näide 25. Teisendada näites 24 saadud valemi maatriks konjunktiivsele normaalkujule.

Valemi maatriks sisaldab nelja atomaarset valemit $P(x,u)$, $Q(z)$, $R(v,y)$ ja $P(v,v)$. Tähistades neid lühiduse mõttes vastavalt tähtedega A, B, C ja D, võime valemi maatriksi üles kirjutada kujul

$$\mathcal{F}' = A \,\&\, (\neg B \vee \neg (C \vee D)).$$

Viime eituse De Morgani seaduste abil sulgude sisse:

$$\mathcal{F}' \equiv A \,\&\, (\neg B \vee \neg C \,\&\, \neg D)$$

ning teisendame tulemuse distributiivsuse seaduse põhjal elementaardisjunktsioonide konjunktsiooniks:

$$\mathcal{F}' \equiv A \,\&\, (\neg B \vee \neg C) \,\&\, (\neg B \vee \neg D).$$

Asendades tähed A, B, C ja D tagasi atomaarsete valemitega, saame maatriksi konjunktiivsel normaalkujul

$$P(x,u) \mathbin{\&} (\neg Q(z) \vee \neg R(v,y)) \mathbin{\&} (\neg Q(z) \vee \neg P(v,v)).$$

Valem ise koos konjunktiivsel normaalkujul maatriksiga on seega

$$\forall x \exists u \exists v (P(x,u) \mathbin{\&} (\neg Q(z) \vee \neg R(v,y)) \mathbin{\&} (\neg Q(z) \vee \neg P(v,v))).$$

§ 7. Ülesanded

1. Kõigi inimeste hulgal on antud predikaat $A(x,y)$ tähenduses „x armastab y-t“. Panna järgmised väited kirja predikaatarvutuse valemiga.

a) Igaüks armastab kedagi.

b) Igaüks armastab kedagi armunut.

c) Pole kedagi, keda ei armastata.

d) Leidub vastuseta armastust.

e) Kõik armunud armastavad iseennast.

2. Kõigi inimeste hulgal on antud predikaat $V(x,y)$ tähenduses „x on y-le võlgu“. Panna kirja järgmised väited.

a) Pole kedagi, kes kellelegi võlgu ei ole.

b) Leidub keegi, kellele kõik on võlgu.

c) Leidub keegi, kellele on võlgu ainult võlausaldajad.

d) Kõik, kellel on võlglasi, on võlgu kellelegi.

e) Mõned on võlgu ainult võlglastele.

3. Kui püüame väljendada lauset „Igaüks lahendas kõik ülesanded“, siis ei sobi selleks valem $\forall x \forall y A(x,y)$, sest kui $A(x,y)$ on „x lahendas y“, siis peab põhihulk sisaldama nii inimesi kui ülesandeid. Toodud valemi järgi kehtiks lahendamisseos nii kahe ülesande kui kahe inimese vahel. Seepärast toome sellel põhihulgal sisse predikaadid $B(x)$ ja $C(x)$ tähenduses $B(x) =$ „x on inimene“, $C(x) =$ „x on ülesanne“. Esitatud lause saab siis edasi anda valemiga $\forall x(B(x) \to \forall y(C(y) \to A(x,y)))$. Kasutades seda võtet, panna predikaatarvutuse valemiga kirja järgmised laused.

a) Mitte keegi ei lahendanud kõiki ülesandeid.

b) Iga ülesande puhul leidus keegi, kes selle lahendas.

c) Igaüks lahendas vähemalt ühe ülesande.

d) Mõned ei lahendanud ühtegi ülesannet.

4. Vaatleme naturaalarvude hulgal $\mathbb{N}$ määratud predikaate $A(x) =$ $=$ „x on algarv", $B(x,y) =$ „$x > y$" ja $C(x,y,z) =$ „$x + y = z$". Leida järgmiste valemite tõeväärtus.

a) $\forall x \forall y \forall z (C(x,y,z) \to B(z,x) \,\&\, B(z,y))$

b) $\exists y \forall z \exists x C(x,y,z)$

c) $\forall z \exists x C(x,x,z)$

d) $\forall y \exists x (A(x) \,\&\, B(x,y))$

e) $\exists x \exists y (\neg A(x) \,\&\, \neg A(y) \,\&\, \forall z (C(x,y,z) \to A(z)))$

5. Leida ülesande 4 valemite tõeväärtus juhul, kui predikaadid on määratud naturaalarvude hulga kõigi alamhulkade hulgal $\mathcal{P}(\mathbb{N})$ ning $A(x) =$ „x on üheelemendiline", $B(x,y) =$ „$x \subseteq y$" ja $C(x,y,z) =$ „$x \cap y = z$".

6. Leida ülesande 4 valemite tõeväärtus juhul, kui predikaadid on määratud positiivsete täisarvude hulgal $\mathbb{Z}^+$ ning $A(x) =$ „x on paarisarv", $B(x,y) =$ „$x \mid y$" ja $C(x,y,z) =$ „$\text{SÜT}(x,y) = z$".

7. Leida interpretatsioon, milles valem on tõene, ning interpretatsioon, milles valem on väär.

a) $\forall x \neg (A(x) \to B(x))$

b) $\forall x \exists y (A(x,y) \leftrightarrow \neg A(y,x))$

c) $\exists x (\forall y A(x,y) \vee \forall y \neg A(x,y))$

d) $\forall x \forall y (A(x,y) \to \forall z (A(y,z) \to A(z,x)))$

8. Vaatleme valemeid

$$\mathcal{F} = \exists x (A(x) \to B(x)) \qquad \text{ja} \qquad \mathcal{G} = \exists x (B(x) \to A(x)).$$

Kas on võimalik olukord, kus

a) täpselt üks valemitest $\mathcal{F}$ ja $\mathcal{G}$ on tõene;

b) valemid $\mathcal{F}$ ja $\mathcal{G}$ on mõlemad väärad;

c) valemid $\mathcal{F}$ ja $\mathcal{G}$ on tõesed, kuid valem $\exists x (A(x) \leftrightarrow B(x))$ on väär?

9. Konstrueerida iga tingimuste rühma rahuldamiseks võimalikult väikese põhihulgaga interpretatsioon.

a) $\forall x (P(x) \to Q(x)) = 1,$
$\forall x (Q(x) \to R(x)) = 1,$
$\exists x (P(x) \leftrightarrow R(x)) = 0$

b) $\forall x (P(x) \to Q(x)) = 0,$
$\forall x (Q(x) \to P(x)) = 0,$
$\exists x (P(x) \leftrightarrow Q(x)) = 1$

c) $\forall x (A(x) \leftrightarrow B(x)) = 0,$
$\forall x (B(x) \leftrightarrow C(x)) = 0,$
$\forall x (A(x) \leftrightarrow C(x)) = 0,$
$\forall x (A(x) \to B(x)) = 0,$
$\forall x (B(x) \to C(x)) = 0$

d) $\forall x \forall y (A(x,y) \to \neg A(y,x)) = 1$,
$\forall x \exists y A(x,y) = 1$,
$\exists x A(x,x) = 0$

10. Vaatleme valemit

$$\forall x \forall y \forall z (\forall u (R(x,u) \leftrightarrow R(y,u)) \vee \\ \vee \forall u (R(x,u) \leftrightarrow R(z,u)) \vee \forall u (R(y,u) \leftrightarrow R(z,u))).$$

Eeldame, et see valem on tõene kõigis interpretatsioonides, mille põhihulk on M. Milline võib olla hulga M elementide arv?

11. Tõestada, et leidub kehtestatav valem, mis on väär kõigis interpretatsioonides, mille põhihulgas on: a) vähem kui 3 elementi; b) vähem kui n elementi, kus n on fikseeritud naturaalarv.

12. Tõestada, et leidub kehtestatav valem, mis on väär kõigis interpretatsioonides, mille põhihulk on lõplik.

13. Olgu $\mathcal{F}$ valem, mis on tõene mingis interpretatsioonis, mille põhihulgas on n elementi. Tõestada, et iga $m \geqslant n$ korral on valem $\mathcal{F}$ tõene ka mingis sellises interpretatsioonis, mille põhihulgas on m elementi.

14. Olgu põhihulk $M = \mathbb{N}$ ja signatuur $\sigma = \langle 0, 1\,; +, \cdot\,; = \rangle$, sümbolite interpretatsioon standardne. Väljendada järgmised predikaadid.

a) $x < y$
b) $z = x - y$
c) $z = x/y$
d) x on täisruut
e) x jagub y-ga
f) x on algarv
g) z on jagatise x/y täisosa
h) z on jääk x jagamisel y-ga
i) $z = \text{SÜT}(x,y)$
j) $z = \text{VÜK}(x,y)$
k) x on arvu 2 aste
l) $z = x^y$

15. Vaatleme sama olukorda nagu eelmises ülesandes. Panna kirja järgmised väited.

a) Leidub kuitahes suuri algarve.
b) Leidub kuitahes suuri kaksikalgarve (st algarve, mis erinevad teineteisest 2 võrra).
c) Naturaalarvude jadas leidub kuitahes pikki lõike, mis koosnevad ainult kordarvudest.
d) Kui a ja b on ühistegurita, siis leidub lõpmata palju algarve kujul $an + b$ (Dirichlet' teoreem).

e) Arvude n ja $2n$ vahel leidub alati vähemalt üks algarv (Tšebõševi teoreem).

f) Iga arvust 2 suurem paarisarv on esitatav kahe algarvu summana (Goldbachi hüpotees).

16. Olgu põhihulk $M = \mathbb{R}$ ja signatuur $\sigma = \langle 0, 1\,; +, \cdot\,; =\rangle$. Väljendada järgmised predikaadid.

a) $x \geqslant 0$ b) $x \leqslant y$ c) $x < y$ d) $x \geqslant 1$

17. Olgu põhihulk $M = \mathcal{P}(\mathbb{N})$ ja signatuur $\sigma = \langle\,;\,;\subseteq\rangle$. Väljendada järgmised predikaadid.

a) $X = Y$
b) $X = \mathbb{N}$
c) $X \cap Y = Z$
d) $X \cup (Y \cap Z) = U$
e) $X \cap Y = \varnothing$
f) $\overline{X} = Y$
g) $X \setminus Y = Z$
h) $|X| = 1$
i) $|X| = 2$

18. Olgu põhihulk $M = \mathcal{P}(\mathbb{N})$ ja signatuur $\sigma = \langle\,;\cup, \cap\,; =\rangle$. Väljendada järgmised predikaadid.

a) $X = \varnothing$
b) $X = \mathbb{N}$
c) $X \subseteq Y$
d) $\overline{X} = Y$
e) $X \setminus Y = Z$
f) $|X| = 1$

19. Olgu põhihulk $M = \{1, 2, 4, 8, \dots\}$ ning signatuur $\sigma = \langle\,;\cdot\,;=\rangle$. Väljendada järgmised predikaadid.

a) $x > y$
b) $x = 1$
c) $x = 2$
d) $y = 2x$
e) $x = 4$
f) $x = 256$

20. Olgu põhihulk M tasandi sirgete hulk ning signatuur $\sigma = \langle\,;\,;\perp\rangle$, kus $\perp$ tähistab sirgete ristseisu (nendevaheline nurk on 90°). Panna kirja järgmised väited.

a) Sirged s ja t on paralleelsed.

b) Sirged s ja t lõikuvad.

c) Suvalised kaks sirget, mis on paralleelsed mingi kolmanda sirgega, on ka omavahel paralleelsed.

d) Kui sirge lõikab ühte kahest paralleelsest sirgest, siis lõikab ta ka teist.

e) Kui kaks sirget lõikuvad, siis tasandi iga sirge lõikab kas esimest või teist sirget.

21. Olgu antud põhihulk M, selle kolm alamhulka $A, B, C \subseteq M$ ning relatsioon $R \subseteq M \times M$. Signatuur olgu $\sigma = \langle\,;\,;A, B, C, R, =\rangle$, seejuures tähistagu $A(x)$, $B(x)$ ja $C(x)$ vastavalt väiteid „$x \in A$“, „$x \in B$“ ja „$x \in C$“ ning $R(x, y)$ väidet „$(x, y) \in R$“. Väljendada järgmised väited.

a) $A = B$
b) $A \subseteq B$
c) $A \subset B$
d) $A \cup B = C$
e) $A \cap B = C$
f) $A \setminus B = C$
g) $\overline{A} = B$
h) $A = \varnothing$
i) $A = M$
j) $A \cap B = \varnothing$
k) $|A| = 1$
l) $|A| = 2$
m) $A \times B \subseteq R$
n) $R \subseteq A \times B$
o) $A \times B = R$

22. Vaatleme sama olukorda nagu ülesandes 21. Väljendada järgmised väited.

a) R on refleksiivne
b) R on antirefleksiivne
c) R on sümmeetriline
d) R on antisümmeetriline
e) R on transitiivne
f) R on ekvivalents
g) R on mitterange järjestus
h) R on range järjestus

23. Vaatleme sama olukorda nagu ülesandes 21 eeldusel, et relatsioon $R \subseteq M \times M$ on ekvivalents. Väljendada järgmised väited.

a) A on elemendi x ekvivalentsiklass R järgi.
b) A on ekvivalentsiklass R järgi.
c) Kui x ja y on relatsioonis R, siis nende ekvivalentsiklassid ühtivad.
d) Kui x ja y ei ole relatsioonis R, siis nende ekvivalentsiklassid ei lõiku.

24. Vaatleme sama olukorda nagu ülesandes 21 eeldusel, et relatsioon $R \subseteq M \times M$ on mitterange järjestus. Väljendada järgmised väited.

a) x ja y on mittevõrreldavad järjestuse R mõttes
b) x on suurim element järjestuse R mõttes
c) x on maksimaalne element järjestuse R mõttes
d) R on tihe järjestus
e) R on lineaarne järjestus
f) x on hulga A ülemtõke
g) x on hulga A ülemraja
h) x on hulga A alamraja

25. Väljendada eelmise ülesande väited, kui relatsioon $R \subseteq M \times M$ on range järjestus.

26. Olgu põhihulk $M = \mathbb{R}$, millel on määratud funktsioon $f : \mathbb{R} \to \mathbb{R}$. Signatuur olgu $\sigma = \langle 0 ; +, f ; =, < \rangle$. Väljendada järgmised väited.

a) $y = -x$
b) f on paarisfunktsioon
c) f on paaritu funktsioon
d) f on perioodiline funktsioon

e) f on kasvav funktsioon

f) f on monotoonselt kasvav funktsioon

g) f on ülalt tõkestatud

h) f on pidev punktis x

i) f on vasakult (paremalt) pidev punktis x

j) f on pidev lõigul $[a,b]$ (vahemikus (a,b))

k) f on ühtlaselt pidev lõigul $[a,b]$

l) c on funktsiooni f maksimaalne väärtus lõigul $[a,b]$

m) c on funktsiooni f ülemraja lõigul $[a,b]$

27. Olgu antud põhihulk M, selle kaks alamhulka $A, B \subseteq M$ ja funktsioon $f\colon M \to M$. Signatuur olgu $\sigma = \langle ; f ; A, B, = \rangle$, kusjuures signatuuri sümbolite interpretatsioon on analoogiline ülesandega 21. Väljendada järgmised väited.

a) f on injektiivne

b) f on sürjektiivne

c) f on bijektiivne

d) $f(A) \subseteq B$

e) $f(A) = B$

f) $f^{-1}(B) \subseteq A$

g) $f^{-1}(B) = A$

h) $f(A) = f(B)$

i) $f^{-1}(f(M)) = M$

j) $f(f^{-1}(M)) = M$

28. Määrata valemi liik (samaselt tõene, samaselt väär, kehtestatav).

a) $\forall x(\neg A(x) \vee \neg B(x)) \to \forall x(A(x) \,\&\, B(x) \to C(x))$

b) $\forall x(P(x) \to \neg\exists y(P(y) \to Q(x,y)))$

c) $\exists x \forall y(P(y) \vee (P(x) \to Q(x,y)))$

d) $\forall x(P(x) \to Q(x)) \,\&\, \forall x(Q(x) \to R(x)) \to \forall x(P(x) \to R(x))$

29. Määrata valemi liik (samaselt tõene, samaselt väär, kehtestatav).

a) $\exists x \forall y(P(x,y) \,\&\, P(y,x) \leftrightarrow P(x,x) \,\&\, P(y,y))$

b) $\forall x \exists y(\neg P(x,y) \vee P(y,x) \to (P(x,x) \to \neg P(y,y)))$

c) $\forall x(P(x,x) \to \exists y \neg P(x,y) \,\&\, \exists y P(x,y))$

d) $\exists x \forall y P(x,y) \& \exists x \forall y \neg P(x,y) \& \exists x(\exists y P(x,y) \& \exists y \neg P(x,y))$

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

30. Olgu $\forall x_1 \ldots \forall x_n \mathcal{F}(x_1, \ldots, x_n)$ kinnine predikaatarvutuse valem, kus $\mathcal{F}$ on kvantoriteta valem, mis ei sisalda konstant- ega funktsionaalsümboleid. Tõestada, et kui selline valem on kehtestatav, siis on ta tõene mingis interpretatsioonis, mille põhihulk on üheelemendiline.

31. Olgu $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m \mathcal{F}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ kinnine predikaatarvutuse valem, kus $\mathcal{F}$ on kvantoriteta valem, mis ei sisalda konstant- ega funktsionaalsümboleid. Tõestada, et kui selline valem on kehtestatav, siis on ta tõene mingis interpretatsioonis, mille põhihulk koosneb n elemendist.

32. Olgu $\mathcal{F}$ kinnine predikaatarvutuse valem, mis ei sisalda konstant- ega funktsionaalsümboleid ning milles kõik predikaatsümbolid on ühekohalised. Tõestada, et kui selline valem on kehtestatav, siis on ta tõene mingis interpretatsioonis, mille põhihulk koosneb 2^n elemendist, kus n on valemi $\mathcal{F}$ erinevate predikaatsümbolite arv.

33. Tõestada, et leidub algoritm, millega saab kontrollida a) ülesandes 30; b) ülesandes 31; c) ülesandes 32 nimetatud tüüpi valemite kehtestatavust.

34. Teha kindlaks, kas kehtivad järgmised järeldumised.

a) $\exists x P(x), \exists x (P(x) \to Q(x)) \vDash \exists x Q(x)$

b) $\forall x (P(x) \to \neg Q(x)), \forall x (Q(x) \to R(x)) \vDash \forall x (P(x) \to \neg R(x))$

c) $\exists x (P(x) \,\&\, R(x)), \neg \exists x (P(x) \,\&\, Q(x)) \vDash \exists x (R(x) \,\&\, \neg Q(x))$

d) $\forall x \exists y P(x,y), \forall x \exists y \neg P(x,y) \vDash \forall y (\exists x P(x,y) \& \exists x \neg P(x,y))$

35. Süllogism Festino väidab järgmist: kui valemid $\forall x (P(x) \to \neg Q(x))$ ja $\exists x (R(x) \& Q(x))$ on tõesed, siis on ka valem $\exists x (R(x) \& \neg P(x))$ tõene. Näiteks kui ükski lind pole neljajalgne ja leidub elusolend, kes on neljajalgne, siis leidub elusolend, kes pole lind. Tõestada predikaatarvutuse abil, et süllogism Festino on korrektne.

36. Tõestada, et esimesest lausest järeldub teine.

- Professor on rõõmus, kui kõik tema õpilased armastavad loogikat.
- Professor on rõõmus, kui tal ei ole õpilasi.

37. Panna järgmine arutlus kirja predikaatarvutuse valemitega ning tõestada, et arutlus kehtib, st et eeldustele vastavatest valemitest järeldub väitele vastav valem: „Ühtegi akrobaatikatrikki, mida pole tsirkuse eeskavas välja kuulutatud, ei püüa trupp etenduse ajal sooritada. Ühtegi akrobaatikatrikki, mis sisaldab neljakordset saltot, pole üldse võimalik sooritada. Ühtegi akrobaatikatrikki, mida pole võimalik sooritada, ei ole tsirkuse eeskavas välja kuulutatud. Järelikult ühtegi akrobaatikatrikki, mis sisaldab neljakordset saltot, ei püüa trupp etenduse ajal sooritada.“

38. Kui antud indiviidi eellase iga eellane on ka antud indiviidi eellane ja ükski indiviid pole iseenda eellane, siis peab leiduma keegi, kellel pole eellasi. Kas selline järeldus on õige?

39. Kui muutuja x võib esineda vabalt nii valemis $\mathcal{F}(x)$ kui ka valemis $\mathcal{G}(x)$, siis üldiselt $\forall x(\mathcal{F}(x) \vee \mathcal{G}(x)) \not\equiv \forall x\mathcal{F}(x) \vee \forall x\mathcal{G}(x)$ ja $\exists x(\mathcal{F}(x) \& \mathcal{G}(x)) \not\equiv \exists x\mathcal{F}(x) \& \exists x\mathcal{G}(x)$. Tõestada, et siiski kehtivad alati järgmised järeldumised.

a) $\forall x\mathcal{F}(x) \vee \forall x\mathcal{G}(x) \vDash \forall x(\mathcal{F}(x) \vee \mathcal{G}(x))$

b) $\exists x(\mathcal{F}(x) \& \mathcal{G}(x)) \vDash \exists x\mathcal{F}(x) \& \exists x\mathcal{G}(x)$

40. Leida võimalikult väikese põhihulgaga interpretatsioon, millest selguks, et ei kehti samaväärsused

$$\forall x(\mathcal{F}(x) \to \mathcal{G}) \equiv \forall x\mathcal{F}(x) \to \mathcal{G} \quad \text{ja} \quad \exists x(\mathcal{F}(x) \to \mathcal{G}) \equiv \exists x\mathcal{F}(x) \to \mathcal{G},$$

kui muutuja x ei esine valemis $\mathcal{G}$ vabalt.

41. Tõestada, et kehtib järeldumine

$$\exists x\forall y\mathcal{F}(x,y) \vDash \forall y\exists x\mathcal{F}(x,y)$$

42. Kvantoritest $\exists x_1, \ldots, \exists x_k, \forall x_{k+1}, \ldots, \forall x_n$ moodustatakse suvaline ümberjärjestus $Q_{i_1}x_{i_1}, Q_{i_2}x_{i_2}, \ldots, Q_{i_n}x_{i_n}$. Tõestada, et iga valemi $\mathcal{F}$ korral kehtivad järeldumised

$$\exists x_1 \ldots \exists x_k \forall x_{k+1} \ldots \forall x_n \mathcal{F} \vDash Q_{i_1}x_{i_1} Q_{i_2}x_{i_2} \ldots Q_{i_n}x_{i_n}\mathcal{F},$$

$$Q_{i_1}x_{i_1} Q_{i_2}x_{i_2} \ldots Q_{i_n}x_{i_n}\mathcal{F} \vDash \forall x_n \ldots \forall x_{k+1} \exists x_k \ldots \exists x_1 \mathcal{F}.$$

43. Teha kindlaks, kas valemid on samaväärsed. Kui ei ole, siis kontrollida, kas ühest valemist järeldub teine.

a) $\forall x\exists y(P(x) \vee Q(y))$ ja $\exists y\forall x(P(x) \vee Q(y))$

b) $\forall x\exists y(P(x) \leftrightarrow Q(y))$ ja $\exists y\forall x(P(x) \leftrightarrow Q(y))$

c) $\neg\forall x(A(x) \to B(x))$ ja $\exists x\neg B(x) \to \neg\forall xA(x)$

44. Teha kindlaks, kas valemid on samaväärsed. Kui ei ole, siis kontrollida, kas ühest valemist järeldub teine.

a) $\forall x\exists y(P(x,y) \& P(y,x))$ ja $\forall x\exists y(P(x,x) \& P(y,y))$

b) $\forall x\forall y(A(x,y) \leftrightarrow B(x,y))$ ja $\forall x\forall y(A(x,x) \leftrightarrow B(y,y))$

c) $\exists x\forall y\forall zP(x,y,z)$ ja $\forall z\exists x\forall yP(x,y,z)$

45. Lihtsustada valemid predikaatarvutuse põhisamaväärsuste abil.

a) $\neg((\exists xP(x) \to \exists xQ(x)) \to \forall x\neg P(x) \& \forall x\neg Q(x))$

b) $\forall y(\exists xA(x) \to B(y)) \& \forall y(B(y) \to \forall xA(x))$

c) $\neg(\forall x(B(x) \to \neg A(x)) \& \neg\exists x(A(x) \& \neg B(x)))$

d) $\exists xA(x) \& \neg B \vee \forall x\neg A(x) \to (\exists xA(x) \leftrightarrow \forall x\neg A(x) \& B)$

46. Leida järgmiste lausete eitused ja lihtsustada neid.

a) Leidub arv, mis on väiksem kui suvaline positiivne arv.

b) Iga positiivse arvu jaoks leidub temast väiksem positiivne arv.

c) Igas külas leidub elanik, kes tunneb iga ülejäänud elanikku selles külas.

d) Leidub küla, kus vähemalt ühte inimest ei tunne ükski selle küla elanik.

47. Lausearvutuse tehtemärgid ja kvantorid ei ole sõltumatud, vaid neid võib avaldada üksteise kaudu. Milline on minimaalne komplekt tehtemärke ja kvantoreid, mille abil võib avaldada suvalise predikaatarvutuse valemi?

48. *Duaalsusprintsiip predikaatarvutuses.* Olgu $\mathcal{F}$ ja $\mathcal{G}$ samaväärsed valemid, mis võivad sisaldada ainult kvantoreid ja tehtemärke $\neg$, $\&$, $\vee$. Tõestada, et kui $\mathcal{F}'$ ja $\mathcal{G}'$ on saadud vastavalt valemitest $\mathcal{F}$ ja $\mathcal{G}$, asendades nendes iga tehtemärgi $\&$ märgiga $\vee$ ja vastupidi ning iga kvantori $\forall$ kvantoriga $\exists$ ja vastupidi, siis valemid $\mathcal{F}'$ ja $\mathcal{G}'$ on samaväärsed.

49. Teha kindlaks, kas iga predikaatarvutuse valemi korral leidub temaga samaväärne kinnine kvantoriteta valem.

50. Viia valemid prefikskujule.

a) $(\exists x A(x) \to \neg\forall x B(x) \vee \exists y C(x,y)) \to \forall x A(x)$

b) $(\forall y P(x,y) \,\&\, \neg\exists x \exists y R(x,y) \to \forall x P(x,x)) \to Q(y)$

c) $(\forall x P(x) \leftrightarrow \forall x Q(x)) \,\&\, \exists x (P(x) \,\&\, Q(x))$

51. Kas predikaatarvutuse samaväärsustega saab viia iga valemi kujule, kus kõik kvantorid asuvad atomaarsete valemite ees?

III. AKSIOMAATILISED TEOORIAD

§ 1. Aksiomaatilise teooria üldskeem

Väga mitmed teaduslikud teooriad on üles ehitatud aksiomaatiliselt. See tähendab, et on valitud teatav hulk väiteid, mida nimetatakse *aksioomideks* ja mis loetakse kehtivaks ilma tõestamata, ning kõik ülejäänud väited tõestatakse aksioomidest lähtudes. Aksiomaatilise lähenemisviisi alusepanijaks on vanakreeka matemaatik Eukleides (u 325 — u 265 e.m.a), kes korrastas sel viisil tolleaegse geomeetria. Rohkem kui kaks tuhat aastat kujutas Eukleidese geomeetria endast ranguse ja süstematiseerituse musternäidet ning ta oli kuni 19. sajandini ainus tõsiseltvõetav aksiomaatiline teooria. Tänaseks on koostatud aksiomaatika paljude distsipliinide jaoks, sealhulgas ka selliste jaoks, mis otseselt matemaatika valdkonda ei kuulu. Tuntumad aksiomaatilised teooriad on näiteks algebras rühmateooria, ringiteooria, võreteooria, vektorruumide teooria, funktsionaalanalüüsis meetriliste, topoloogiliste, Hilberti, Banachi jt ruumide teooriad, samuti Peano aritmeetika, Zermelo-Fraenkeli hulgateooria jne. Aksiomaatiliselt võib arendada ka elektrodünaamikat ja kvantmehaanikat.

Aksiomaatilise teooria ülesehitamisel tuleb muu hulgas selgus leida kahes küsimuses: mis on aksioom ja mis on tõestus. Tavaarusaama järgi tähendab aksioom väidet, mis on *silmnähtavalt õige*. Selliselt mõistis aksioomi arvatavasti ka Eukleides. Ta eeldas, et geomeetria laused kirjeldavad ümbritsevat ruumi, ja valis nende lausete hulgast välja niisugused, mis tundusid olevat kõige ilmsemad. Ülejäänud lausete kehtivus, mis nii ilmne ei olnud, tuli tõestada. Teadmiste arenedes aga tekkisid kahtlused ja 19. sajandil selgus, et need aksioomid ei tarvitse sugugi reaalse ruumiga vastavuses olla — ruum võib olla selline, et Eukleidese aksioomid seal ei kehti. Seepärast ei mõisteta tänapäeval aksioomi all enam silmnähtavalt õiget väidet. Tänapäeva aksioomid on enamasti *definitsiooni* rollis: nendega fikseeritakse uurimisobjektiks kõikvõimalike struktuuride klass, kus aksioomid kehtivad, väitmata midagi aksioomide ja materiaalse maa-ilma vahelise seose kohta. Näiteks kaasaegses geomeetrias tähendab ruum iga sellist struktuuri, kus kehtivad ruumi aksioomid. Mõnel juhul võivad aksioomideks olla *relatiivsed tõed*, mis on õiged sel määral, nagu nad on katseliselt kontrollitud. Niimoodi mõistetakse aksioome näiteks loodusteadustes, mis on süstemaatilisuse huvides aksiomaatiliselt üles ehitatud. Loodusteaduste mõne valdkonna aksiomatiseerimine aitab välja eraldada teatava hulga põhilisi väiteid, mille kehtivus tuleb selgitada katse või vaatlusega, kõik nendest tulenevad väited on juba automaatselt tõesed ega vaja katselist kontrolli.

Aja jooksul on olnud vaja täpsustada ka tõestuse mõistet. Jällegi tavaarusaamale tuginedes võime öelda, et esimesest väitest järeldub teine, kui teine väide on esimesega piisavalt põhjendatud. Erimeelsusi tekitab see, mida lugeda piisavaks põhjenduseks. Näiteks Eukleides kasutas oma teoreemide tõestamisel vaikimisi lauseid, mis reaalses ruumis küll kehtivad, kuid mis rangelt võttes aksioomidest ei järeldu. Võime ette kujutada ruume, kus kõik Eukleidese aksioomid on täidetud, aga need teoreemide tõestamisel kasutatud, kuid kirja panemata laused mitte. Vastavalt ei kehti sellistes ruumides ka nende lausete tõesusest sõltuvad teoreemid. Tänapäeval puudub matemaatikute hulgas üksmeel näiteks välistatud kolmanda seaduse suhtes. Kas võib ütelda, et kõigil meie poolt tõestamata ja isegi formuleerimata lausetel on alati olemas kindel tõeväärtus „tõene“ või „väär“? Kahtlusi tekitab ka nn olemasoluteoreemide tõestamine kaudsel viisil, näiteks vastuväiteliselt, ilma otsitavat objekti tegelikult kätte näitamata.

Eespool toodud kaalutlused sunnivad aksiomaatilise teooria ülesehitamisel täpselt määratlema laused, mida loetakse aksioomideks, ja sammud, mida lubatakse teoreemide tõestamisel teha. Nii jõuame *formaalse aksiomaatilise teooriani*, mis ehitatakse üles järgmise üldskeemi kohaselt.

1) Fikseeritakse tähestik ja antakse valemi definitsioon.
2) Osa valemeid loetakse aksioomideks. Neid pole teoorias vaja tõestada.
3) Fikseeritakse lõplik hulk *tuletusreegleid* kujul

$$\frac{\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n}{\mathcal{G}},$$

   mis lubavad valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ vahetult tuletada valemi $\mathcal{G}$.

Paneme tähele, et siin tegeldakse mitte enam lausete või väidetega, vaid valemitega. Valem, vastupidiselt lausele, on kindlapiiriline mõiste ja kujutab endast kasutatava tähestiku sümbolite järjendit. Erijuhul võib valem tähendada lause- või predikaatarvutuse valemit.

Üldskeem ei määra, millise printsiibi järgi loetakse valemeid aksioomideks, sest loogika seisukohalt pole see oluline. Tõestussamme saab teha ainult tuletusreeglite abil. Tuletusreegli alumise valemi võib lugeda tõestatuks ainult siis, kui vastavad ülemised valemid on tõestatud või aksioomid.

Definitsioon 1. *Tuletuseks ehk formaalseks tõestuseks nimetatakse valemite jada* $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$, *milles iga valem on kas aksioom või saadud mingi tuletusreegliga mõnedest temale eelnevatest valemitest.*

Valemit $\mathcal{F}$ nimetatakse *tuletatavaks*, kui leidub tuletus, mille viimane liige on valem $\mathcal{F}$.

Näide 1. Aksiomaatilise teooria näitena vaatleme teooriat MIU.

1) Tähestik on $\{\mathsf{M}, \mathsf{I}, \mathsf{U}\}$. Valemid on kõikvõimalikud sümbolijärjendid tähestiku sümbolitest.
2) Ainuke aksioom on MI.
3) Teoorias on neli tuletusreeglit:

$$\text{a)}\ \frac{*\mathsf{I}}{*\mathsf{IU}} \qquad \text{b)}\ \frac{\mathsf{M}*}{\mathsf{M}**} \qquad \text{c)}\ \frac{*\mathsf{III}\diamond}{*\mathsf{U}\diamond} \qquad \text{d)}\ \frac{*\mathsf{UU}\diamond}{*\diamond}$$

Sümbolid $*$ ja $\diamond$ tähistavad suvalisi valemeid (sümbolite järjendeid), ka tühje.

Lähtudes aksioomist ja kasutades antud nelja reeglit, saab konstrueerida järgmise tuletuse.

1.	MI	aksioom
2.	MII	reegel b)
3.	MIIII	reegel b)
4.	MUI	reegel c)
5.	MUIU	reegel a)
6.	MUIUUIU	reegel b)
7.	MUIIU	reegel d)

Kuigi valemiteks võtsime kõikvõimalikud sümbolite järjendid, ei ole sugugi mitte kõik valemid selles teoorias tuletatavad. Näiteks peavad kõik tuletatavad valemid algama sümboliga M, sest pole reeglit, millega selle sümboli valemi algusest eemaldada saaks.

Nagu lause- ja predikaatarvutuseski, mõistetakse ka käesolevas peatükis valemeid puhtalt süntaktiliste objektidena, millel enne vastavat määrangut puudub sisu. Tuletusreegleid kasutades saab olemasolevatest sümbolijadadest koostada uusi. Valemi tõestamiseks piisab, kui kirjutame aksioome reeglite kohaselt sobival viisil ümber.

Tähenduse annab valemitele semantika. Arusaadavalt võib samale valemikomplektile anda erinevaid tähendusi, st defineerida erinevaid semantikaid, mis ei tarvitse kuidagi üksteisega seoses olla. Ülalvaadeldud teooria valemeid võib interpreteerida näiteks kui arve kümnendsüsteemis, veduri ja vagunite lubatavaid järjestusi, aminohappeid valgus jne. Edaspidi piirdume aga selliste semantikatega, milles saab rääkida valemi tõeväärtusest. Näiteks lausearvutuse valemite puhul määrab iga lausemuutujate väärtustus ühe semantika. Predikaatarvutuse valemite puhul saab semantika defineerida interpretatsiooni või ka üldisemalt, interpretatsioonide klassi abil, näiteks seades igale valemile vastavusse väite, et valem on tõene igas sellesse klassi kuuluvas interpretatsioonis vabade muutujate kõigil väärtustel. Kui vaadeldav interpretatsioonide klass haarab üldse kõik võimalikud interpretatsioonid, siis seab niisugune semantika igale valemile vastavusse väite, et see valem on samaselt tõene.

Niisiis on meil ühelt poolt teooria *süntaks*, mis määrab kindlaks, kuidas valemeid kirja panna ja tuletusi koostada, ning teiselt poolt valemite *semantika*, mis annab igale valemile tõeväärtuse „tõene“ või „väär“. Süntaksi ja semantika vahekorra kirjeldamiseks defineerime järgmised kaks mõistet.

Definitsioon 2. *Aksiomaatilist teooriat $\mathcal{T}$ nimetatakse semantika S suhtes*

- *korrektseks, kui iga teoorias $\mathcal{T}$ tuletatav valem on semantikas S tõene;*
- *täielikuks, kui iga semantikas S tõene valem on teoorias $\mathcal{T}$ tuletatav.*

Näide 2. Vaatleme järgmist aksiomaatilist teooriat.

1) Tähestik on $\{\mathsf{I}, +\}$. Valemid on sellised tähestiku sümbolite järjendid, mis sisaldavad täpselt ühte sümbolit $+$.
2) Ainuke aksioom on $+$.
3) Ainuke tuletusreegel on
$$\frac{*}{\mathsf{I} * \mathsf{I}},$$
kus $*$ on suvaline valem.

Selles teoorias on tuletatavad parajasti need valemid, milles mõlemal pool sümbolit + on võrdne arv sümboleid I, näiteks +, I+I, II+II, III+III jne.

Omistame nüüd teooria valemitele tähenduse, defineerides kolm erinevat semantikat. Kõigis neis interpreteerime sümbolite I järjendit selle naturaalarvuna, mitu sümbolit järjendis on, sümboli + tähendus on aga igas semantikas erinev.

1) Semantika S_1: $m+n$ tähendab $m = n$.
2) Semantika S_2: $m+n$ tähendab $m \leqslant n$.
3) Semantika S_3: $m+n$ tähendab $m < n$.

Semantika S_1 suhtes on meie teooria korrektne ja täielik: iga tuletatav valem on selles semantikas tõene ja iga semantikas tõene valem on tuletatav. Semantika S_2 suhtes on teooria korrektne, kuid pole täielik: iga tuletatav valem on semantikas S_2 tõene, kuid leidub semantikas S_2 tõeseid valemeid, mis pole tuletatavad. Semantika S_3 suhtes pole teooria ei korrektne ega täielik.

Teooriat võib täiendada, lisades tuletusreegli

$$\frac{*}{*\mathsf{I}}$$

suvalise valemi $*$ korral. Saadud kahe tuletusreegliga teooria pole semantika S_1 suhtes korrektne, kuid on täielik. Semantika S_2 suhtes on uus teooria korrektne ja täielik, semantika S_3 suhtes pole teooria korrektne, on aga täielik.

Asudes mingit valdkonda aksiomatiseerima, on tavaliselt varasemast olemas teooria sisuline pool, st uuritavad objektid ja mingi hulk fakte nende kohta. Vastava formaalse teooria konstrueerimisel määratakse valemi mõiste nii, et oleks võimalik tähistada valdkonna põhilisi konstante, funktsioone ja predikaate. Valemite semantika tuleneb teooria sisust. Aksioomid ja reeglid püütakse valida nii, et teooria oleks selle semantika suhtes korrektne ja täielik, st tuletatavateks osutuksid parajasti need valemid, mis on semantikas tõesed. Nagu aga matemaatilise loogika uurimustest on selgunud, pole viimane eesmärk paljudel olulistel juhtudel (näiteks naturaalarvude aritmeetika korral) saavutatav. Korrektsuse nõudest loobumine, niisugune aksiomaatika, kus saaks tuletada ka teatavaid vääri valemeid, ei tule ilmselt kõne alla. Järelikult peame sellistel juhtudel rahulduma mittetäieliku aksiomaatilise teooriaga, kus mõned tõesed valemid ei ole tuletatavad, püüdes ainult selle poole, et tuletatavate valemitega oleks haaratud teooria sisust kõige olulisem osa.

§ 2. Sekventsiaalne lausearvutus

Võtame nüüd vaatluse alla lausearvutuse aksiomaatika. Lausearvutuse aksiomaatiliste süsteemide hulgas on ajalooliselt esimesed *Hilberti-tüüpi süsteemid*, kus teooria valemiteks, s.o tuletatavateks objektideks on parajasti lausearvutuse valemid. Teatavad valemid loetakse aksioomideks, nendest saab kindlaksmääratud reeglite abil tuletada teisi valemeid. Meie valime lausearvutuse ülesehitamiseks siiski *Gentzeni-tüüpi aksiomaatilise süsteemi*, mille saksa matemaatik Gerhard Gentzen (1909—1945) võttis kasutusele aastal 1935.

1) Tuletatavateks objektideks on *sekventsid*, avaldised kujul
$$\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G},$$
kus $\mathcal{F}_1$, $\mathcal{F}_2$, …, $\mathcal{F}_n$, $\mathcal{G}$ on lausearvutuse valemid, mis ei sisalda ekvivalentsi.

2) Aksioomid on sekventsid
$$\Gamma, \mathcal{F}, \Delta \vdash \mathcal{F},$$
kus $\mathcal{F}$ on mingi lausearvutuse valem ning Γ ja Δ tähistavad suvalisi valemite järjendeid, mis võivad olla ka tühjad.

3) Tuletusreeglid on järgmised.

Paremale sissetoomise reegel	Vasakule sissetoomise või paremalt eemaldamise reegel
$\dfrac{\Gamma \vdash \mathcal{F} \quad \Gamma \vdash \mathcal{G}}{\Gamma \vdash \mathcal{F} \mathbin{\&} \mathcal{G}}\ (\vdash \&)$	$\dfrac{\Gamma, \mathcal{F}, \mathcal{G} \vdash \mathcal{H}}{\Gamma, \mathcal{F} \mathbin{\&} \mathcal{G} \vdash \mathcal{H}}\ (\& \vdash)$
$\dfrac{\Gamma \vdash \mathcal{F}}{\Gamma \vdash \mathcal{F} \vee \mathcal{G}} \quad \dfrac{\Gamma \vdash \mathcal{G}}{\Gamma \vdash \mathcal{F} \vee \mathcal{G}}\ (\vdash \vee)$	$\dfrac{\Gamma, \mathcal{F} \vdash \mathcal{H} \quad \Gamma, \mathcal{G} \vdash \mathcal{H}}{\Gamma, \mathcal{F} \vee \mathcal{G} \vdash \mathcal{H}}\ (\vee \vdash)$
$\dfrac{\Gamma, \mathcal{F} \vdash \mathcal{G}}{\Gamma \vdash \mathcal{F} \to \mathcal{G}}\ (\vdash \to)$	$\dfrac{\Gamma \vdash \mathcal{F} \quad \Gamma \vdash \mathcal{F} \to \mathcal{G}}{\Gamma \vdash \mathcal{G}}\ (\vdash \not\to)$
$\dfrac{\Gamma, \mathcal{F} \vdash \mathcal{G} \quad \Gamma, \mathcal{F} \vdash \neg\mathcal{G}}{\Gamma \vdash \neg\mathcal{F}}\ (\vdash \neg)$	$\dfrac{\Gamma \vdash \neg\neg\mathcal{F}}{\Gamma \vdash \mathcal{F}}\ (\vdash \not\neg)$

Peale nende on olemas *struktuursed reeglid*
$$\frac{\Gamma \vdash \mathcal{F}}{\Gamma, \mathcal{G} \vdash \mathcal{F}}\ (S+) \qquad \frac{\Gamma, \Delta, \mathcal{F} \vdash \mathcal{G}}{\Gamma, \mathcal{F}, \Delta \vdash \mathcal{G}}\ (S\sim)$$
vasakule valemite juurdelisamiseks või seal valemite järjekorra vahetamiseks. Sümbolid Γ ja Δ tähistavad nagu ennegi suvalisi valemite järjendeid.

Sekvents esitab paremini matemaatiliste teoreemide ja lausete struktuuri, sest neid formuleeritakse sageli kujul, kus eeldustest järeldub väide. Samuti saab sekventside kaudu lihtsamini väljendada tavalisemaid tõestussamme, kus eelduste või väitega sooritatakse mingi operatsioon. Vajadusel võib aga iga sekventsi jaoks leida lausearvutuse valemi, mis väljendab sama väidet.

Sekventsi $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ vasakpoolset osa $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ nimetatakse sekventsi *eesliikmeks* ehk *antetsedendiks*, parempoolset osa $\mathcal{G}$ aga *tagaliikmeks* ehk *suktsedendiks*. Eesliige võib olla ka tühi. Sekventsi $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ mõistame väitena, et valemitest $\mathcal{F}_1$, $\mathcal{F}_2$, ..., $\mathcal{F}_n$ järeldub valem $\mathcal{G}$.

Aksioomideks olevad sekventsid väljendavad kõige ilmsemat järeldumist. Kindlasti võime eeldustest järeldada väite, kui väide esineb ise juba eelduste hulgas.

Teooria peamine tuletusaparaat on koondatud tuletusreeglitesse. Need vastavad enam-vähem matemaatikas kasutatavatele tõestusvõtetele. Näiteks kui on tehtud kindlaks, et eeldustel Γ kehtivad valemid $\mathcal{F}$ ja $\mathcal{G}$, siis võib konjunktsiooni paremale sissetoomise reegli järgi lugeda, et eeldustel Γ kehtib valem $\mathcal{F} \,\&\, \mathcal{G}$. Eituse paremale sissetoomise reegel tähendab, et kui eeldustel Γ viib valemi $\mathcal{F}$ kehtivuse eeldus vastuolule (saab järeldada teatava valemi $\mathcal{G}$ ja tema eituse), siis peab kehtima valem $\neg\mathcal{F}$.

Definitsiooni järgi on tuletus sellises süsteemis sekventside jada, kus järjekordse sekventsi saamiseks viidatakse tuletusreeglile ja sobivatele eespool asetsevatele sekventsidele. Ent tuletust otsida on käesolevas süsteemis otstarbekam mitte jada, vaid puu kujul. Etteantud sihtsekventsist lähtudes selgitame, millise reegliga see tekkida võib. Teinud reegli kindlaks, otsime järgmisi reegleid, millega saavad tekkida antud sekventsi eeldused jne. Puud konstrueerime seega alt üles liikudes, püüdes tükeldada sekventsi valemeid osavalemiteks.

Näide 3. Tuletada sekvents $A \,\&\, (B \vee C) \vdash A \,\&\, B \vee A \,\&\, C$.

Lähtudes antud sekventsist, konstrueerime järk-järgult talle eelnevad sekventsid, millega tekib tuletuspuu

$$
\dfrac{
\dfrac{\dfrac{\overline{\overline{A, B \vdash A}} \quad \overline{\overline{A, B \vdash B}}}{A, B \vdash A \,\&\, B}\,(\vdash \&)}{A, B \vdash A \,\&\, B \vee A \,\&\, C}\,(\vdash \vee)
\qquad
\dfrac{\dfrac{\overline{\overline{A, C \vdash A}} \quad \overline{\overline{A, C \vdash C}}}{A, C \vdash A \,\&\, C}\,(\vdash \&)}{A, C \vdash A \,\&\, B \vee A \,\&\, C}\,(\vdash \vee)
}{
\dfrac{A, B \vee C \vdash A \,\&\, B \vee A \,\&\, C}{A \,\&\, (B \vee C) \vdash A \,\&\, B \vee A \,\&\, C}\,(\& \vdash)
}\,(\vee \vdash)
$$

Puu lehtedeks on aksioomid, järelduste tegemine toimub „ülevalt alla“. Alati võib sellise puu kirja panna ka sekventside jadana nii, et iga sekventsi tuletamisel kasutatakse ainult jadas eespool paiknevaid sekventse: kõigepealt puu lehed (aksioomid), seejärel kõik need sekventsid, mis tulenevad vahetult aksioomidest jne.

Sekvents, mille vasakus pooles esineb mingi valem koos oma eitusega, on tuletatav paremal pool asuvast valemist sõltumata.

Näide 4. Tuletada sekvents $A, \neg A \vdash B$.

Tuletuspuuks saame

$$\dfrac{\dfrac{\overline{\overline{A, \neg A, \neg B \vdash A}} \qquad \overline{\overline{A, \neg A, \neg B \vdash \neg A}}}{A, \neg A \vdash \neg\neg B}\;(\vdash \neg)}{A, \neg A \vdash B}\;(\vdash \not\neg)$$

Eituse paremale sissetoomise reegli puhul tuleb joonepealsete sekventside paremates pooltes esinev valem määrata ise. See tuleb valida nii, et kummaski harus tekiks tuletatav sekvents, st et tuletuspuu haru oleks võimalik jätkata kuni aksioomideni. Enamasti sobib selleks mõni sekventsi vasakul pool asuvate valemite osavalem. Näites 4 pidime eituse paremale sissetoomise reegli rakendamiseks esimese sammuna kasutama kahekordse eituse reeglit.

Näide 5. Tuletada sekvents $\neg A \,\&\, \neg B \vdash \neg(A \vee B)$.

Koostame järgmise tuletuspuu:

$$\dfrac{\dfrac{\dfrac{\overline{\overline{\neg A, \neg B, A \vdash A}} \qquad \dfrac{\dfrac{\overline{\overline{\neg A, \neg B, B, \neg A \vdash B}} \qquad \overline{\overline{\neg A, \neg B, B, \neg A \vdash \neg B}}}{\neg A, \neg B, B \vdash \neg\neg A}\;(\vdash \neg)}{\neg A, \neg B, B \vdash A}\;(\vdash \not\neg)}{\neg A, \neg B, A \vee B \vdash A}\;(\vee \vdash) \qquad \overline{\overline{\neg A, \neg B, A \vee B \vdash \neg A}}}{\neg A, \neg B \vdash \neg(A \vee B)}\;(\vdash \neg)}{\neg A \,\&\, \neg B \vdash \neg(A \vee B)}\;(\& \vdash)$$

Näide 6. Tuletada sekvents $\vdash A \vee \neg A$.

Konstrueerime tuletuspuu

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\overline{\neg(A \vee \neg A), A \vdash A}}}{\neg(A \vee \neg A), A \vdash A \vee \neg A}\;(\vdash \vee) \qquad \overline{\overline{\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)}}}{\neg(A \vee \neg A) \vdash \neg A}\;(\vdash \neg)}{\neg(A \vee \neg A) \vdash A \vee \neg A}\;(\vdash \vee) \qquad \overline{\overline{\neg(A \vee \neg A) \vdash \neg(A \vee \neg A)}}}{\vdash \neg\neg(A \vee \neg A)}\;(\vdash \neg)}{\vdash A \vee \neg A}\;(\vdash \not\neg)$$

Seega saab tuletada ka selliseid sekventse, mille eesliige on tühi.

Iga aksiomaatilise teooria puhul huvitab meid küsimus, millised valemid on tuletatavad ja millised mitte. Eelnevate näidete põhjal võib oletada, et lausearvutuse aksiomaatilises teoorias on tuletatavad sekventsid, mille eesliikme valemitest järeldub tagaliikme valem, ning kõik ülejäänud sekventsid on mittetuletatavad. Käesolevas tõestame, et nii see tegelikult ongi. Täpsemalt, näitame, et sekventsiaalne lausearvutus on korrektne ja täielik sekventside samaselt tõesuse semantika suhtes.

Definitsioon 3. *Sekventsi $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ valemkujuks nimetatakse valemit $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \to \mathcal{G}$, kui $n > 0$, ja valemit $\mathcal{G}$, kui $n = 0$.*

Teoreem 1. *(Korrektsuse teoreem.) Kui sekvents $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ on tuletatav, siis tema valemkuju on samaselt tõene.*

Tõestus. Kasutame induktsiooni tuletuspuu struktuuri järgi.

Induktsiooni baas. Kui sekvents on aksioom, siis esineb tagaliikme valem eesliikme valemite hulgas ning sekventsil on kuju

$$\mathcal{F}_1, \ldots, \mathcal{F}_i, \ldots, \mathcal{F}_n \vdash \mathcal{F}_i.$$

Selle sekventsi valemkuju on

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_i \& \ldots \& \mathcal{F}_n \to \mathcal{F}_i.$$

Viimase valemi samaselt tõesus on ilmne.

Induktsiooni samm. Näitame iga reegli korral, et kui mingil valemites esinevate lausemuutujate väärtustusel on kõigi joonepealsete sekventside valemkujud tõesed, siis on sellel väärtustusel tõene ka joonealuse sekventsi valemkuju, st valemkuju tõesus antud väärtustusel levib mööda tuletuspuud allapoole. Et aksioomide valemkujud on samaselt tõesed, siis on järelikult samaselt tõesed ka kõigi tuletatud sekventside valemkujud. Vaatleme siinkohal implikatsiooni reegleid ja eituse paremale sissetoomise reeglit, piirdudes juhuga $n > 0$.

Implikatsiooni paremale sissetoomise reegel. Kui Γ koosneb valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$, siis joonepealse sekventsi valemkuju on

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \& \mathcal{F} \to \mathcal{G},$$

joonealuse sekventsi valemkuju aga

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \to (\mathcal{F} \to \mathcal{G}).$$

Oletame, et mingil väärtustusel on esimene valemkuju tõene ja teine väär. Sellel väärtustusel peab valem $\mathcal{F}_1 \& \ldots \& \mathcal{F}_n$ olema tõene ja valem $\mathcal{F} \to \mathcal{G}$ väär. Viimasest järeldub, et valem $\mathcal{F}$ on tõene ja valem $\mathcal{G}$ on väär. Nüüd aga saame, et esimene valemkuju on väär, sest implikatsiooni eesliige on tõene ja tagaliige väär, vastuolu.

Implikatsiooni paremalt eemaldamise reegel. Kui Γ koosneb valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$, siis joonepealsete sekventside valemkujud on

$$\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \to \mathcal{F} \qquad \text{ja} \qquad \mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \to (\mathcal{F} \to \mathcal{G})$$

ning joonealuse sekventsi valemkuju

$$\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \to \mathcal{G}.$$

Oletame, et mingil väärtustusel on esimesed kaks valemkuju tõesed, kuid kolmas on väär. Siis peab valem $\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n$ olema sellel väärtustusel tõene ja valem $\mathcal{G}$ väär. Et esimene valemkuju on tõene ja implikatsiooni eesliige on tõene, siis on ka valem $\mathcal{F}$ tõene. Nüüd on teise implikatsiooni eesliige vaadeldaval väärtustusel tõene, tagaliige väär ja kogu implikatsioon väär, vastuolu teise valemkuju tõesusega.

Eituse paremale sissetoomise reegel. Kui Γ koosneb valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$, siis joonepealsete sekventside valemkujud on

$$\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \mathbin{\&} \mathcal{F} \to \mathcal{G} \qquad \text{ja} \qquad \mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \mathbin{\&} \mathcal{F} \to \neg\mathcal{G}$$

ning joonealuse sekventsi valemkuju

$$\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n \to \neg\mathcal{F}.$$

Oletame, et mingil väärtustusel on esimesed kaks valemkuju tõesed, kuid kolmas on väär. Siis peab valem $\mathcal{F}_1 \mathbin{\&} \ldots \mathbin{\&} \mathcal{F}_n$ olema sellel väärtustusel tõene, valem $\neg\mathcal{F}$ väär ning valem $\mathcal{F}$ tõene. Järelikult on kahes esimeses valemkujus implikatsiooni eesliige tõene. Kui vaadeldaval väärtustusel on valem $\mathcal{G}$ väär, siis on esimene valemkuju samuti väär; kui aga valem $\mathcal{G}$ on tõene, siis on $\neg\mathcal{G}$ väär ja teine valemkuju väär. Mõlemal juhul saame vastuolu vastava valemkuju tõesusega.

Ülejäänud juhud vaadatakse läbi sarnasel viisil: oletame, et mingil väärtustusel on ülemiste sekventside valemkujud tõesed, kuid alumise sekventsi valemkuju väär. Sekventsi osadeks jaotades jõuame vastuoluni, mis tähendab, et alumise sekventsi valemkuju peab samuti olema tõene. □

Aksiomaatilise teooria oluline omadus, mida saab siduda korrektsusega, on mittevasturääkivus. Erinevalt korrektsusest ja täielikkusest on mittevasturääkivus puhtalt süntaktiline mõiste ega sõltu valitud semantikast. Kuid samas peavad tuletatavad objektid olema sellised, et on mõtet rääkida vähemalt nende osade eitustest. Olgu tuletatavateks objektideks sekventsid.

Definitsioon 4. *Aksiomaatilist teooriat $\mathcal{T}$ nimetatakse vasturääkivaks, kui leidub selline valem $\mathcal{F}$, et teoorias $\mathcal{T}$ on tuletatavad sekventsid $\vdash \mathcal{F}$ ja $\vdash \neg\mathcal{F}$. Vastasel korral nimetatakse teooriat $\mathcal{T}$ mittevasturääkivaks.*

Teoreem 2. *(Mittevasturääkivuse teoreem.) Sekventsiaalne lausearvutus on mittevasturääkiv.*

Tõestus. Oletame vastupidi, et leidub selline lausearvutuse valem $\mathcal{F}$, et on tuletatavad nii sekvents $\vdash \mathcal{F}$ kui ka sekvents $\vdash \neg\mathcal{F}$. Korrektsuse teoreemi põhjal on iga tuletatava sekventsi valemkuju samaselt tõene. See tähendab, et valemid $\mathcal{F}$ ja $\neg\mathcal{F}$ peaksid olema samaselt tõesed, mis aga on võimatu. □

Järgmisena võtame vaatluse alla lausearvutuse täielikkuse küsimuse. Meenutame, et lausemuutuja A puhul tähendab A^1 positiivset literaali A ning A^0 negatiivset literaali $\neg A$.

Teoreem 3. *Olgu $\mathcal{F}$ lausearvutuse valem ja $A_1, \ldots, A_n$ kõik temas esinevad lausemuutujad. Kui valem $\mathcal{F}$ on muutujate väärtustusel $(\alpha_1, \ldots, \alpha_n)$ tõene, siis on tuletatav sekvents*

$$A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{F};$$

kui valem $\mathcal{F}$ on muutujate väärtustusel $(\alpha_1, \ldots, \alpha_n)$ väär, siis on tuletatav sekvents

$$A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{F}.$$

Sisuliselt väidab teoreem seda, et me saame aksiomaatilises süsteemis välja arvutada valemi tõeväärtuse etteantud väärtustusel. Näiteks valemi $\neg A \vee B$ ja muutujate A, B väärtustuse $(1, 0)$ korral väidab teoreem, et tuletatav on sekvents $A, \neg B \vdash \neg(\neg A \vee B)$, sest vaadeldav valem on sellel väärtustusel väär.

Tõestus. Kasutame induktsiooni valemi $\mathcal{F}$ struktuuri järgi.

Induktsiooni baas. Kui $\mathcal{F}$ on lausemuutuja, näiteks A_1, ja $\alpha_1 = 1$, siis teoreemi väite kohaselt peab olema tuletatav sekvents $A_1 \vdash A_1$. Kui $\alpha_1 = 0$, siis peab olema tuletatav sekvents $\neg A_1 \vdash \neg A_1$. Mõlemad sekventsid on tuletatavad, sest nad on aksioomid.

Induktsiooni samm. Vaatleme eraldi juhte valemi ehituse järgi.

Juht 1. Olgu valem $\mathcal{F}$ kujul $\neg\mathcal{G}$. Eeldame, et valemi $\mathcal{G}$ jaoks teoreemi väide kehtib. Vaatleme väärtustust $(\alpha_1, \ldots, \alpha_n)$. Kui valem $\mathcal{F}$ on sellel väärtustusel tõene, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{F}$ ehk $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{G}$. Et valem $\mathcal{G}$ on vaadeldaval väärtustusel väär, siis on viimane sekvents tuletatav induktsiooni eelduse põhjal.

Kui valem $\mathcal{F}$ on antud väärtustusel väär, siis peame näitama, et tuletatav on sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{F}$ ehk $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\neg\mathcal{G}$. Et valem $\mathcal{G}$ on tõene, siis on induktsiooni eelduse põhjal tuletatav sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{G}$. Otsitava sekventsi saame tuletada järgmiselt:

$$\cfrac{\cfrac{\cfrac{\dots}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n},\neg\mathcal{G} \vdash \mathcal{G}}\,(S+) \qquad \overline{\overline{A_1^{\alpha_1},\dots,A_n^{\alpha_n},\neg\mathcal{G} \vdash \neg\mathcal{G}}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg\neg\mathcal{G}}\,(\vdash\neg)$$

Vasaku haru sekvents on tuletatav induktsiooni eelduse põhjal.

Juht 2. Olgu valem $\mathcal{F}$ kujul $\mathcal{G} \,\&\, \mathcal{H}$. Eeldame, et valemite $\mathcal{G}$ ja $\mathcal{H}$ jaoks teoreemi väide kehtib. Vaatleme väärtustust $(\alpha_1,\dots,\alpha_n)$. Kui $\mathcal{F}$ on antud väärtustusel tõene, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{F}$ ehk $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G} \,\&\, \mathcal{H}$. Et valemid $\mathcal{G}$ ja $\mathcal{H}$ peavad vaadeldaval väärtustusel olema tõesed, siis induktsiooni eelduse põhjal on tuletatavad sekventsid $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G}$ ja $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{H}$. Otsitava sekventsi saame tuletada järgmiselt:

$$\cfrac{\cfrac{\dots}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G}} \qquad \cfrac{\dots}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{H}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G} \,\&\, \mathcal{H}}\,(\vdash\&)$$

Kui valem $\mathcal{F}$ on sellel väärtustusel väär, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg\mathcal{F}$ ehk $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg(\mathcal{G} \,\&\, \mathcal{H})$. Valem $\mathcal{F}$ saab olla väär kahel juhul. Kui $\mathcal{G}$ on väär, siis induktsiooni eelduse põhjal on tuletatav $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg\mathcal{G}$ ja vajalik tuletus on

$$\cfrac{\cfrac{\overline{\overline{A_1^{\alpha_1},\dots,A_n^{\alpha_n},\mathcal{G},\mathcal{H} \vdash \mathcal{G}}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n},\mathcal{G} \,\&\, \mathcal{H} \vdash \mathcal{G}}\,(\&\vdash) \qquad \cfrac{\cfrac{\dots}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg\mathcal{G}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n},\mathcal{G} \,\&\, \mathcal{H} \vdash \neg\mathcal{G}}\,(S+)}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg(\mathcal{G} \,\&\, \mathcal{H})}\,(\vdash\neg)$$

Kui $\mathcal{H}$ on väär, siis on tõestus analoogiline.

Juht 3. Olgu valem $\mathcal{F}$ kujul $\mathcal{G} \vee \mathcal{H}$. Eeldame, et valemite $\mathcal{G}$ ja $\mathcal{H}$ jaoks teoreemi väide kehtib. Vaatleme väärtustust $(\alpha_1,\dots,\alpha_n)$. Kui $\mathcal{F}$ on antud väärtustusel tõene, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{F}$ ehk $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G} \vee \mathcal{H}$. Valem $\mathcal{F}$ saab olla tõene kahel juhul. Kui $\mathcal{G}$ on tõene, siis induktsiooni eelduse põhjal on tuletatav sekvents $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G}$ ning vajalik tuletus on

$$\cfrac{\cfrac{\dots}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G}}}{A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \mathcal{G} \vee \mathcal{H}}\,(\vdash\vee)$$

Kui $\mathcal{H}$ on tõene, siis on tõestus analoogiline.

Kui valem $\mathcal{F}$ on sellel väärtustusel väär, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg\mathcal{F}$ ehk $A_1^{\alpha_1},\dots,A_n^{\alpha_n} \vdash \neg(\mathcal{G} \vee \mathcal{H})$. Et valemid $\mathcal{G}$ ja $\mathcal{H}$ peavad olema väärad, siis induktsiooni eelduse põhjal on tuletatav nii sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{G}$ kui ka sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{H}$. Tähistades eelduste järjendi $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}$ lühiduse mõttes sümboliga Γ, saame otsitava sekventsi tuletada järgmiselt:

$$\dfrac{\dfrac{\dfrac{\cdots}{\Gamma \vdash \neg\mathcal{G}} \quad \dfrac{\cdots}{\Gamma \vdash \neg\mathcal{H}}}{\Gamma \vdash \neg\mathcal{G} \mathbin{\&} \neg\mathcal{H}}\,(\vdash \&) \qquad \dfrac{\dfrac{\cdots}{\Gamma, \neg\mathcal{G} \mathbin{\&} \neg\mathcal{H} \vdash \neg(\mathcal{G} \vee \mathcal{H})}}{\Gamma \vdash \neg\mathcal{G} \mathbin{\&} \neg\mathcal{H} \to \neg(\mathcal{G} \vee \mathcal{H})}\,(\vdash \to)}{\Gamma \vdash \neg(\mathcal{G} \vee \mathcal{H})}\,(\vdash \not\to)$$

Parempoolse haru ülemine sekvents on tuletatav näite 5 eeskujul.

Juht 4. Olgu valem $\mathcal{F}$ kujul $\mathcal{G} \to \mathcal{H}$. Eeldame, et valemite $\mathcal{G}$ ja $\mathcal{H}$ jaoks teoreemi väide kehtib. Vaatleme väärtustust $(\alpha_1, \ldots, \alpha_n)$. Kui $\mathcal{F}$ on sellel väärtustusel tõene, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{F}$ ehk $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{G} \to \mathcal{H}$. Valem $\mathcal{F}$ saab olla tõene kahel juhul. Kui $\mathcal{G}$ on väär, siis induktsiooni eelduse põhjal on tuletatav sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{G}$ ja vajalik tuletus on

$$\dfrac{\dfrac{\dfrac{\dfrac{\cdots}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{G}}}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}, \mathcal{G} \vdash \neg\mathcal{G}}\,(S+) \qquad \dfrac{\dfrac{\cdots}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}, \mathcal{G}, \neg\mathcal{G} \vdash \mathcal{H}}}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}, \mathcal{G} \vdash \neg\mathcal{G} \to \mathcal{H}}\,(\vdash \to)}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}, \mathcal{G} \vdash \mathcal{H}}\,(\vdash \not\to)}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{G} \to \mathcal{H}}\,(\vdash \to)$$

Parempoolse haru ülemine sekvents on tuletatav näite 4 eeskujul. Teisel juhul, kui $\mathcal{H}$ on tõene, siis induktsiooni eelduse põhjal on tuletatav sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{H}$ ja vajalik tuletus on

$$\dfrac{\dfrac{\dfrac{\cdots}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{H}}}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}, \mathcal{G} \vdash \mathcal{H}}\,(S+)}{A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{G} \to \mathcal{H}}\,(\vdash \to)$$

Kui valem $\mathcal{F}$ on sellel väärtustusel väär, siis on vaja näidata, et tuletatav on sekvents $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{F}$ ehk $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg(\mathcal{G} \to \mathcal{H})$. Et valem $\mathcal{G}$ peab siin olema tõene ja valem $\mathcal{H}$ väär, siis induktsiooni eelduse põhjal on tuletatavad sekventsid $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \mathcal{G}$ ning $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n} \vdash \neg\mathcal{H}$. Tähistades jällegi $A_1^{\alpha_1}, \ldots, A_n^{\alpha_n}$ sümboliga Γ, saame otsitava sekventsi tuletada järgmiselt:

$$\dfrac{\dfrac{\dfrac{\dfrac{\cdots}{\Gamma \vdash \mathcal{G}}}{\Gamma, \mathcal{G} \to \mathcal{H} \vdash \mathcal{G}}\,(S+) \qquad \overline{\overline{\Gamma, \mathcal{G} \to \mathcal{H} \vdash \mathcal{G} \to \mathcal{H}}}}{\Gamma, \mathcal{G} \to \mathcal{H} \vdash \mathcal{H}}\,(\vdash \not\to) \qquad \dfrac{\dfrac{\cdots}{\Gamma \vdash \neg\mathcal{H}}}{\Gamma, \mathcal{G} \to \mathcal{H} \vdash \neg\mathcal{H}}\,(S+)}{\Gamma \vdash \neg(\mathcal{G} \to \mathcal{H})}\,(\vdash \neg)$$

Sellega on kõik juhud läbi vaadatud. $\square$

Teoreem 4. *(Täielikkuse teoreem.) Kui sekventsi $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n \vdash \mathcal{G}$ valemkuju on samaselt tõene, siis sekvents on tuletatav.*

Tõestus. Eeldame kõigepealt, et $n = 0$. Siis on meil tegemist sekventsiga $\vdash \mathcal{G}$, kus $\mathcal{G}$ on samaselt tõene. Näitame, et $\vdash \mathcal{G}$ on tuletatav.

Olgu $A_1, \dots, A_n$ kõik lausemuutujad, mis sisalduvad valemis $\mathcal{G}$. Et valem $\mathcal{G}$ on samaselt tõene, siis järeldub eelmisest teoreemist, et suvalise väärtustuse $(\alpha_1, \dots, \alpha_n)$ korral saab tuletada sekventsi

$$A_1^{\alpha_1}, \dots, A_n^{\alpha_n} \vdash \mathcal{G}$$

ning järelikult, kui võtta $\alpha_n = 1$ ja $\alpha_n = 0$, ka sekventsid

$$A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}}, A_n \vdash \mathcal{G} \quad \text{ja} \quad A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}}, \neg A_n \vdash \mathcal{G}.$$

Konstrueerime nüüd tuletuspuu

$$\dfrac{\dfrac{\dots}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}} \vdash A_n \vee \neg A_n} \qquad \dfrac{\dfrac{\dfrac{\dots}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}}, A_n \vdash \mathcal{G}} \quad \dfrac{\dots}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}}, \neg A_n \vdash \mathcal{G}}}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}}, A_n \vee \neg A_n \vdash \mathcal{G}}\,(\vee\vdash)}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}} \vdash A_n \vee \neg A_n \to \mathcal{G}}\,(\vdash\to)}{A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}} \vdash \mathcal{G}}\,(\vdash\not\to)$$

Selle harud lõpevad kõik tuletatavate sekventsidega, vasaku haru ülemise sekventsi saab tuletada näite 6 eeskujul. Seega, suvalise tõeväärtuste komplekti $(\alpha_1, \dots, \alpha_{n-1})$ korral saab tuletada sekventsi

$$A_1^{\alpha_1}, \dots, A_{n-1}^{\alpha_{n-1}} \vdash \mathcal{G}.$$

Sama arutelu korrates eemaldame vasakust poolest ka ülejäänud literaalid, millega jõuame järelduseni, et sekvents $\vdash \mathcal{G}$ on tuletatav.

Olgu nüüd $n > 0$. Et sekventsi valemkuju $\mathcal{F}_1 \mathbin{\&} \dots \mathbin{\&} \mathcal{F}_n \to \mathcal{G}$ on samaselt tõene, siis on tõestuse eelmise osa põhjal tuletatav sekvents

$$\vdash \mathcal{F}_1 \mathbin{\&} \dots \mathbin{\&} \mathcal{F}_n \to \mathcal{G}.$$

Siis on ka sekvents $\mathcal{F}_1, \dots, \mathcal{F}_n \vdash \mathcal{G}$ tuletatav:

$$\dfrac{\dfrac{\dots}{\mathcal{F}_1, \dots, \mathcal{F}_n \vdash \mathcal{F}_1 \mathbin{\&} \dots \mathbin{\&} \mathcal{F}_n} \quad \dfrac{\dots}{\mathcal{F}_1, \dots, \mathcal{F}_n \vdash \mathcal{F}_1 \mathbin{\&} \dots \mathbin{\&} \mathcal{F}_n \to \mathcal{G}}}{\mathcal{F}_1, \dots, \mathcal{F}_n \vdash \mathcal{G}}\,(\vdash\not\to)$$

Vasakus harus oleva sekventsi saab tuletada konjunktsiooni komponentideks lahutades, parema haru sekvents on tuletatav ka ilma vasaku pooleta. □

Võttes korrektsuse ja täielikkuse teoreemi kokku, võime anda sekventsiaalse lausearvutuse tuletatavuse kirjelduse, st formuleerida tingimuse, millal sekvents on tuletatav ja millal mitte.

Järeldus 1. *Sekventsiaalses lausearvutuses on tuletatavad parajasti need sekventsid, mille valemkuju on samaselt tõene.*

§ 3. Sekventsiaalne predikaatarvutus

Samasuguse põhimõtte järgi nagu lausearvutuses konstrueerime nüüd predikaatarvutuse aksiomaatilise teooria.

1) Tuletatavateks objektideks on sekventsid, st avaldised kujul

$$\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G},$$

kus $\mathcal{F}_1$, $\mathcal{F}_2$, ..., $\mathcal{F}_n$, $\mathcal{G}$ on predikaatarvutuse valemid, mis ei sisalda lausearvutuse tehtena ekvivalentsi.

2) Aksioomid on sekventsid

$$\Gamma, \mathcal{F}, \Delta \vdash \mathcal{F},$$

kus $\mathcal{F}$ on mingi valem ning Γ ja Δ tähistavad suvalisi valemite järjendeid, mis võivad olla ka tühjad.

3) Tuletusreeglid on kõik lausearvutuse tuletusreeglid ja järgmises tabelis loetletud kvantorreeglid.

Paremale sissetoomise reegel	Vasakule sissetoomise reegel
$\dfrac{\Gamma \vdash \mathcal{F}(x)}{\Gamma \vdash \forall x \mathcal{F}(x)}\ (\vdash \forall)^*$	$\dfrac{\Gamma, \mathcal{F}(t) \vdash \mathcal{G}}{\Gamma, \forall x \mathcal{F}(x) \vdash \mathcal{G}}\ (\forall \vdash)$
$\dfrac{\Gamma \vdash \mathcal{F}(t)}{\Gamma \vdash \exists x \mathcal{F}(x)}\ (\vdash \exists)$	$\dfrac{\Gamma, \mathcal{F}(x) \vdash \mathcal{G}}{\Gamma, \exists x \mathcal{F}(x) \vdash \mathcal{G}}\ (\exists \vdash)^*$

Siin tähendab * tingimust, et muutuja x ei tohi esineda vabalt sekventsi üheski teises valemis, ning t on suvaline term.

Üldisuskvantori paremale sissetoomise reegel vastab matemaatilistes tõestustes sammule, kus selleks, et näidata mingi väite kehtivust kõigi objektide korral, valitakse vabalt üks objekt ja näidatakse väite kehtivus selle korral. Valitud objekti tähistatakse unikaalse muutujaga, mis on teistest muutujatest sõltumatu. Tingimus * garanteerib, et eeldusteks olevate valemite tõeväärtus jääb muutuja x erinevatel väärtustel samaks, mistõttu sellest, et väide kehtib vabalt valitud objekti x korral, võib järeldada, et väide kehtib kõigi objektide korral. Üldisuskvantori vasakule sissetoomisel seevastu ei ole kitsendavat tingimust vaja: eeldused Γ, $\mathcal{F}(t)$ on nõrgemad kui eeldused Γ, $\forall x \mathcal{F}(x)$ (sest valemist $\forall x \mathcal{F}(x)$ järeldub valem $\mathcal{F}(t)$ suvalise termi t korral). Kui mingitel eeldustel väide $\mathcal{G}$ kehtib, siis kehtib ta alati ka tugevamatel eeldustel.

Olemasolukvantori vasakule sissetoomise reegel vastab sammule, kus tõestamisel kasutatakse eeldust mingi objekti leidumise kohta ja tuuakse sisse sümbol selle tähistamiseks. Tingimus $*$ väljendab asjaolu, et üldiselt võib see objekt erineda kõigist nendest, millele selle hetkeni on tõestuses viidatud, seetõttu tuleb teda märkida erineva sümboliga. Tõestamine, et $\mathcal{G}$ järeldub eeldustest Γ, $\exists x\mathcal{F}(x)$, taandub siis tõestamisele, et $\mathcal{G}$ järeldub eeldustest Γ, $\mathcal{F}(x)$, kus x on tähis, mis kuskil mujal vabalt ei esine. Olemasolukvantori paremale sissetoomisel pole jällegi kitsendust vaja, sest kui eeldustest Γ järeldub väide $\mathcal{F}(t)$, siis järeldub samadest eeldustest ka nõrgem väide $\exists x\mathcal{F}(x)$, st kui objekt, mille korral väide $\mathcal{F}(x)$ kehtib, on otseselt kätte näidatud, siis selline objekt ilmselt leidub.

Kitsendusega reeglite joonepealsetes sekventsides esinev muutuja x võib omandada piiranguteta suvalisi väärtusi. Joonepealne sekvents tähendab seega järeldumist muutuja x iga väärtuse korral. Joonealustes sekventsides on see muutuja viidud kvantori alla. Võime näha teatavat analoogiat predikaatarvutuse samaväärsustega $\forall x(\mathcal{G}\to\mathcal{F}(x))\equiv\mathcal{G}\to\forall x\mathcal{F}(x)$ ja $\forall x(\mathcal{F}(x)\to\mathcal{G})\equiv\exists x\mathcal{F}(x)\to\mathcal{G}$.

Olgu veel näiteks toodud kaks ebakorrektset tuletust, kus esimeses ignoreeritakse kitsendavat tingimust üldisuskvantori, teises aga olemasolukvantori puhul:

$$\dfrac{\dfrac{\overline{\overline{P(x)\vdash P(x)}}}{P(x)\vdash\forall xP(x)}\;(\vdash\forall),\ {}^{*}\text{ ei kehti}}{\exists xP(x)\vdash\forall xP(x)}\;(\exists\vdash)^{*}\qquad\qquad \dfrac{\dfrac{\overline{\overline{P(x)\vdash P(x)}}}{\exists xP(x)\vdash P(x)}\;(\exists\vdash),\ {}^{*}\text{ ei kehti}}{\exists xP(x)\vdash\forall xP(x)}\;(\vdash\forall)^{*}$$

Mõlemal juhul väidab alumine sekvents, et kui leidub objekt, millel on omadus P, siis on omadus P kõigil objektidel. Niisugune järeldus ilmselt õige ei ole, viga tekkis reegli kitsenduse mittearvestamisest.

Näide 7. Tuletada sekvents $\forall xP(x)\vdash\forall yP(y)$.

Tuletuse otsimisel tasub püüda rakendada kitsendusega reegleid puu allosas ja ilma kitsenduseta reegleid ülaosas:

$$\dfrac{\dfrac{\overline{\overline{P(y)\vdash P(y)}}}{\forall xP(x)\vdash P(y)}\;(\forall\vdash)}{\forall xP(x)\vdash\forall yP(y)}\;(\vdash\forall)^{*}$$

Kvantorreegleid vastupidises järjekorras rakendades võime mingil sammul jõuda sekventsini, mille tuletamine on võimatu. Näiteks ülaltoodud tuletuses reeglite järjekorda vahetada püüdes tekib olukord

$$\dfrac{P(y)\vdash\forall yP(y)}{\forall xP(x)\vdash\forall yP(y)}\;(\forall\vdash)$$

Siin ei saa enam paremalt kvantorit eemaldada, sest tingimus * oleks rikutud. Kui valida esimesel sammul termiks t midagi muud peale indiviidmuutuja y, siis saaks ka paremalt kvantori eemaldada, kuid järele jääks mittetuletatav sekvents.

Näide 8. Tuletada sekvents $\forall x(P(x)\&Q(x)) \vdash \forall xP(x)\&\forall xQ(x)$.
Koostame tuletuspuu

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{\overline{P(x),Q(x)\vdash P(x)}}}{P(x)\&Q(x)\vdash P(x)}\,(\&\vdash)}{\forall x(P(x)\&Q(x))\vdash P(x)}\,(\forall\vdash)}{\forall x(P(x)\&Q(x))\vdash \forall xP(x)}\,(\vdash\forall)^* \qquad \dfrac{\dfrac{\dfrac{\overline{\overline{P(x),Q(x)\vdash Q(x)}}}{P(x)\&Q(x)\vdash Q(x)}\,(\&\vdash)}{\forall x(P(x)\&Q(x))\vdash Q(x)}\,(\forall\vdash)}{\forall x(P(x)\&Q(x))\vdash \forall xQ(x)}\,(\vdash\forall)^*}{\forall x(P(x)\&Q(x))\vdash \forall xP(x)\&\forall xQ(x)}\,(\vdash\&)$$

Predikaatarvutuse puhul huvitavad meid samad küsimused nagu lausearvutuses: korrektsus, mittevasturääkivus ja täielikkus. Ka siin valime semantikaks, mille suhtes korrektsust ja täielikkust vaatleme, samaselt tõesuse semantika.

Teoreem 5. *(Korrektsuse teoreem.) Kui sekvents $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ on tuletatav, siis tema valemkuju on samaselt tõene.*

Tõestus. Kasutame induktsiooni tuletuspuu struktuuri järgi.

Induktsiooni baas. Kui sekvents on aksioom, siis võime arutleda samamoodi nagu lausearvutuse korrektsuse teoreemis.

Induktsiooni samm. Näitame iga reegli korral, et kui mingis interpretatsioonis on joonepealsete sekventside valemkujud vabade muutujate kõikidel väärtustel tõesed, siis on selles interpretatsioonis vabade muutujate kõikidel väärtustel tõene ka joonealuse sekventsi valemkuju. Et aksioomide valemkujud on samaselt tõesed, siis on järelikult ka kõigi aksioomidest tuletatud sekventside valemkujud samaselt tõesed. Lausearvutuse reeglite korral saab tõestuse üle kanda vastavast teoreemist lausearvutuse kohta. Vaja on vaadelda veel kvantorreegleid. Piirdume siinkohal üldisuskvantoriga, olemasolukvantori puhul on tõestus analoogiline.

Üldisuskvantori paremale sissetoomise reegel. Joonepealse sekventsi valemkuju on

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \to \mathcal{F}(x),$$

joonealuse sekventsi valemkuju aga

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \to \forall x\mathcal{F}(x).$$

Oletame, et mingis interpretatsioonis α on esimene valemkuju oma vabade muutujate kõikidel väärtustel tõene, kuid teine valemkuju on oma vabade muutujate mingitel väärtustel väär. Sel juhul peab valem $\mathcal{F}_1 \& \ldots \& \mathcal{F}_n$ olema tõene ja valem $\forall x \mathcal{F}(x)$ väär. Järelikult leidub interpretatsiooni põhihulgas M_α element m nii, et vabade muutujate antud väärtustel on $\mathcal{F}(m)$ väär. Tingimuse * tõttu ei esine muutuja x osavalemis $\mathcal{F}_1 \& \ldots \& \mathcal{F}_n$. Seega kui esimeses valemkujus valida muutuja x väärtuseks element m ja ülejäänud vabadele muutujatele anda samad väärtused nagu teises valemkujus, siis on esimene valemkuju väär, vastuolu.

Üldisuskvantori vasakule sissetoomise reegel. Joonepealse sekventsi valemkuju on

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \& \mathcal{F}(t) \to \mathcal{G},$$

joonealuse sekventsi valemkuju aga

$$\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \& \forall x \mathcal{F}(x) \to \mathcal{G}.$$

Oletame, et mingis interpretatsioonis α on esimene valemkuju oma vabade muutujate kõikidel väärtustel tõene, kuid teine valemkuju on oma vabade muutujate mingitel väärtustel väär. Siis peab valem $\mathcal{F}_1 \& \ldots \& \mathcal{F}_n \& \forall x \mathcal{F}(x)$ olema tõene ja valem $\mathcal{G}$ väär. Konjunktsiooni omaduste põhjal on valemid $\mathcal{F}_1 \& \ldots \& \mathcal{F}_n$ ja $\forall x \mathcal{F}(x)$ tõesed. Anname esimeses valemkujus termi t nendele vabadele muutujatele, mis teises valemkujus ei esine, suvalised väärtused ja ülejäänud vabadele muutujatele samad väärtused nagu teises valemkujus. Et $\forall x \mathcal{F}(x)$ on tõene, siis on ka $\mathcal{F}(t)$ tõene. Järelikult on esimeses valemkujus implikatsiooni vasak pool tõene ja kogu valemkuju väär, vastuolu. □

Teoreem 6. *(Mittevasturääkivuse teoreem.) Sekventsiaalne predikaatarvutus on mittevasturääkiv.*

Tõestus. Tõestus on analoogiline lausearvutuse juhuga. □

Teoreem 7. *(Täielikkuse teoreem.) Kui sekventsi $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ valemkuju on samaselt tõene, siis sekvents on tuletatav.*

Selle teoreemi tõestas austria loogik ja matemaatik Kurt Gödel aastal 1930. Omal ajal oli see matemaatilise loogika üks silmapaistvamaid tulemusi. Meie seda teoreemi käesolevas kursuses ei tõesta.

Järeldus 2. *Sekventsiaalses predikaatarvutuses on tuletatavad parajasti need sekventsid, mille valemkuju on samaselt tõene.*

Teisiti öeldes, predikaatarvutuse aksiomaatiline teooria on, nagu lausearvutuse omagi, korrektne ja täielik samaselt tõesuse semantika suhtes.

§ 4. Esimest järku aksiomaatilised teooriad

Koostades mingi distsipliini aksiomaatikat, defineeritakse valemi mõiste valdaval enamikul juhtudest võrdusmärki sisaldava signatuuri kaudu, kusjuures võrdusmärgi soovitud tähenduseks on võrdus. Et kasutada tuletustes võrduse omadusi, vaatleme kõigepealt *võrdusega predikaatarvutust*, milles on eelnevas käsitletud nn *puhta predikaatarvutuse* tõestusvahenditele lisatud võrduse aksioomid.

Olgu σ signatuur, mis sisaldab võrdusmärki. Võrdusega predikaatarvutuse aksiomaatiline teooria signatuuris σ on järgmine.

1) Tuletatavateks objektideks on sekventsid $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$, kus $\mathcal{F}_1$, $\mathcal{F}_2$, …, $\mathcal{F}_n$, $\mathcal{G}$ on valemid signatuuris σ.
2) Aksioomid on kõik puhta predikaatarvutuse aksioomid ja lisaks neile kõik järgmist tüüpi sekventsid (võrduse aksioomid):
   - Re) $\Gamma \vdash t = t$, kus t on term signatuuris σ;
   - $=f$) $s_1 = t_1, \ldots, s_n = t_n \vdash f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)$, kus s_1, …, s_n ja t_1, …, t_n on termid signatuuris σ ning f on signatuuri σ funktsionaalsümbol;
   - $=P$) $s_1 = t_1, \ldots, s_n = t_n \vdash P(s_1, \ldots, s_n) \to P(t_1, \ldots, t_n)$, kus s_1, …, s_n ja t_1, …, t_n on termid signatuuris σ ning P on signatuuri σ predikaatsümbol.
3) Tuletusreeglid on kõik puhta predikaatarvutuse tuletusreeglid.

Sekventside tuletamine selles süsteemis toimub samamoodi nagu varemgi, tuletuspuu haru võib aga lõppeda ka loetletud kolme tüüpi aksioomidega. Aksioom Re väljendab võrduse refleksiivsust, aksioomid $=f$ ja $=P$ aga võimaldavad asendada vastavalt funktsionaal- ja predikaatsümboli argumentides terme võrdsete termidega. Võrduse sümmeetrilisus ja transitiivsus osutuvad selles süsteemis tuletatavateks omadusteks.

Näide 9. Tuletada sekvents $x = y \vdash y = x$.

Koostame tuletuspuu

$$\dfrac{\overline{\overline{x=y \vdash x=x}}\;(Re) \qquad \dfrac{\dfrac{\overline{\overline{x=y, x=x \vdash x=x}}\;(Re) \qquad \overline{\overline{x=y, x=x \vdash x=x \to y=x}}\;(=P)}{x=y, x=x \vdash y=x}\;(\vdash \not\to)}{x=y \vdash x=x \to y=x}\;(\vdash \to)}{x=y \vdash y=x}\;(\vdash \not\to)$$

Parempoolne ülemine sekvents on aksioom tüüpi $=P$, kus predikaatsümboli rollis on võrdusmärk.

Näide 10. Tuletada sekvents $x = y, y = z \vdash x = z$.

Tuletuspuu parempoolse haru taandame võrduse aksioomile $=P$, konstrueerides selleks sobiva ees- ja tagaliikmega sekventsi.

$$
\dfrac{
\overline{\overline{x=y,y=z \vdash x=y}}
\qquad
\dfrac{
\dfrac{
\dfrac{
\overline{\overline{y=z \vdash x=x}}\,(Re)
\qquad
\dfrac{
\dfrac{
\overline{\overline{x=x,y=z \vdash x=y\to x=z}}\,(=P)
}{
y=z,x=x \vdash x=y\to x=z
}\,(S\sim)
}{
y=z \vdash x=x\to(x=y\to x=z)
}\,(\vdash\to)
}{
y=z \vdash x=y\to x=z
}\,(\vdash\not\to)
}{
y=z,x=y \vdash x=y\to x=z
}\,(S+)
}{
x=y,y=z \vdash x=y\to x=z
}\,(S\sim)
}{
x=y,y=z \vdash x=z
}\,(\vdash\not\to)
$$

Kirjeldame nüüd üldkujuliselt, kuidas defineeritakse lihtsaimad konkreetsed matemaatikas uuritavaid teooriad, *esimest järku teooriad*. Nende abil saab aksiomatiseerida väga palju klassikalise matemaatika valdkondi. Teooriad võib seejuures üles ehitada nii, et nad erinevad ainult aksioomide poolest, tuletusreeglid on alati samad.

Olgu fikseeritud signatuur σ.

1) Tuletatavateks objektideks on sekventsid $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$, kus $\mathcal{F}_1$, $\mathcal{F}_2$, $\ldots$, $\mathcal{F}_n$, $\mathcal{G}$ on valemid signatuuris σ.
2) Aksioomid on kõik puhta predikaatarvutuse aksioomid ja lisaks neile teooria *omaaksioomid* ehk *eriaksioomid*.
3) Tuletusreeglid on kõik puhta predikaatarvutuse tuletusreeglid.

Nagu näeme, on iga esimest järku teooria määratud signatuuri ja omaaksioomidega. Esimest järku teooria mõiste haarab teiste hulgas ka puhta predikaatarvutuse (sel juhul on omaaksioomide hulk tühi), ning võrdusega predikaatarvutuse (omaaksioomideks on võrduse aksioomid). Peale nende vaatleme veel kahte esimest järku teooriat.

Rühmateooria võime formaalse aksiomaatilise teooriana esitada signatuuris $\sigma = \langle e\,;\circ\,;=\rangle$, kus e tähistab ühikelementi ja $\circ$ rühma tehet. Et signatuur sisaldab võrdusmärki, siis kuuluvad omaaksioomide hulka kõik võrdusega predikaatarvutuse aksioomid, millele võime lisada järgmised sekventsid.

$G1)$ $\vdash \forall x \forall y \forall z((x \circ y) \circ z = x \circ (y \circ z))$

$G2)$ $\vdash \forall x(x \circ e = x)$ $\qquad$ $G4)$ $\vdash \forall x \exists u(x \circ u = e)$

$G3)$ $\vdash \forall x(e \circ x = x)$ $\qquad$ $G5)$ $\vdash \forall x \exists u(u \circ x = e)$

Kui omaaksioomide hulka lugeda ka sekvents

$G6)$ $\vdash \forall x \forall y(x \circ y = y \circ x)$,

siis saame kommutatiivsete ehk Abeli rühmade teooria.

Näide 11. Tuletada sekvents $\forall x(x\circ y=x)\vdash y=e$, mis väljendab väidet, et rühma parempoolne ühikelement on üheselt määratud.

$$
\begin{prooftree}
\AxiomC{}
\doubleLine
\RightLabel{(Re)}
\UnaryInfC{$e\circ y=e\vdash e\circ y=e\circ y$}
\AxiomC{}
\doubleLine
\UnaryInfC{$\vdash G3$}
\RightLabel{$(S+)$}
\UnaryInfC{$e\circ y=e\vdash G3$}
\AxiomC{}
\doubleLine
\RightLabel{$(=P)$}
\UnaryInfC{$e\circ y=y, e\circ y=e\vdash e\circ y=e\circ y\to y=e$}
\RightLabel{$(S\sim)$}
\UnaryInfC{$e\circ y=e, e\circ y=y\vdash e\circ y=e\circ y\to y=e$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$e\circ y=e, G3\vdash e\circ y=e\circ y\to y=e$}
\RightLabel{$(\vdash\to)$}
\UnaryInfC{$e\circ y=e\vdash G3\to(e\circ y=e\circ y\to y=e)$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$e\circ y=e\vdash e\circ y=e\circ y\to y=e$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$e\circ y=e\vdash y=e$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$\forall x(x\circ y=x)\vdash y=e$}
\end{prooftree}
$$

Näide 12. Tuletada sekvents $\vdash\forall a\forall b\exists z(a\circ z=b)$, mis väljendab väidet, et rühmas on võrrand $a\circ z=b$ alati lahenduv.

$$
\begin{prooftree}
\AxiomC{}
\doubleLine
\UnaryInfC{$\vdash G4$}
\AxiomC{}
\doubleLine
\RightLabel{(Re)}
\UnaryInfC{$a\circ u=e\vdash b=b$}
\AxiomC{}
\doubleLine
\RightLabel{$(=f)$}
\UnaryInfC{$a\circ u=e, b=b\vdash (a\circ u)\circ b=e\circ b$}
\RightLabel{$(\vdash\to)$}
\UnaryInfC{$a\circ u=e\vdash b=b\to(a\circ u)\circ b=e\circ b$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$a\circ u=e\vdash (a\circ u)\circ b=e\circ b$}
\AxiomC{}
\doubleLine
\UnaryInfC{$\vdash G1$}
\AxiomC{}
\doubleLine
\UnaryInfC{$\vdash G3$}
\RightLabel{$(S+)$}
\UnaryInfC{$(a\circ u)\circ b=a\circ(u\circ b)\vdash G3$}
\AxiomC{}
\doubleLine
\RightLabel{$(=P)$}
\UnaryInfC{$(a\circ u)\circ b=a\circ(u\circ b), e\circ b=b\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$(a\circ u)\circ b=a\circ(u\circ b), G3\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\vdash\to)$}
\UnaryInfC{$(a\circ u)\circ b=a\circ(u\circ b)\vdash G3\to((a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b)$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$(a\circ u)\circ b=a\circ(u\circ b)\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$\forall z((a\circ u)\circ z=a\circ(u\circ z))\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$\forall y\forall z((a\circ y)\circ z=a\circ(y\circ z))\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$G1\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\vdash\to)$}
\UnaryInfC{$\vdash G1\to((a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b)$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(S+)$}
\UnaryInfC{$a\circ u=e\vdash (a\circ u)\circ b=e\circ b\to a\circ(u\circ b)=b$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$a\circ u=e\vdash a\circ(u\circ b)=b$}
\RightLabel{$(\vdash\exists)$}
\UnaryInfC{$a\circ u=e\vdash\exists z(a\circ z=b)$}
\RightLabel{$(\exists\vdash)$}
\UnaryInfC{$\exists u(a\circ u=e)\vdash\exists z(a\circ z=b)$}
\RightLabel{$(\forall\vdash)$}
\UnaryInfC{$G4\vdash\exists z(a\circ z=b)$}
\RightLabel{$(\vdash\to)$}
\UnaryInfC{$\vdash G4\to\exists z(a\circ z=b)$}
\RightLabel{$(\vdash\not\to)$}
\BinaryInfC{$\vdash\exists z(a\circ z=b)$}
\RightLabel{$(\vdash\forall)^*$}
\UnaryInfC{$\vdash\forall b\exists z(a\circ z=b)$}
\RightLabel{$(\vdash\forall)^*$}
\UnaryInfC{$\vdash\forall a\forall b\exists z(a\circ z=b)$}
\end{prooftree}
$$

Teiseks vaatleme formaalset aritmeetikat (ehk Peano aritmeetikat). Signatuur olgu klassikalisel viisil $\sigma = \langle 0\,;{}'\,, +, \cdot\,; = \rangle$, kus sümbol $'$ on ette nähtud tähistama arvule järgneva arvu leidmise funktsiooni, ning omaaksioomideks võrduse aksioomid ja sekventsid

$A1$) $\vdash \forall x \neg(x' = 0)$

$A2$) $\vdash \forall x \forall y (x' = y' \to x = y)$

$A3$) $\vdash \forall x (x + 0 = x)$

$A4$) $\vdash \forall x \forall y (x + y' = (x + y)')$

$A5$) $\vdash \forall x (x \cdot 0 = 0)$

$A6$) $\vdash \forall x \forall y (x \cdot y' = x \cdot y + x)$

$A7$) $\mathcal{F}(0), \forall x(\mathcal{F}(x) \to \mathcal{F}(x')) \vdash \forall x \mathcal{F}(x)$, kus $\mathcal{F}(x)$ on suvaline valem signatuuris σ.

Aksioomid $A1$ ja $A2$ määravad kindlaks funktsiooni $'$ omadused, nendega postuleeritakse, et elemendiga 0 algab jada 0, $0'$, $0''$, ..., mille liikmed on kõik üksteisest erinevad. Aksioomid $A3$ ja $A4$ defineerivad induktiivselt summa väärtused selle jada elementidel, aksioomid $A5$ ja $A6$ teevad sama korrutisega. Aksioomid $A1$—$A6$ on konkreetsed sekventsid, seevastu kujutab $A7$ aksioomiskeemi, mis haarab lõpmata palju sekventse, tema ülesanne on väljendada matemaatilise induktsiooni printsiipi.

Esimest järku teooriate puhul ei saa enam väita, et tuletatavad on parajasti sellised sekventsid, mille valemkuju on samaselt tõene, sest samaselt tõesed ei tarvitse olla juba kasvõi omaaksioomide valemkujud. Küll aga võime kõigist interpretatsioonidest välja eraldada viimaste mudelid, st interpretatsioonid, kus omaaksioomide valemkujud on tõesed, ning uurida sekventside tuletatavuse ja tõesuse vahekorda selliste interpretatsioonide klassi suhtes. Aksiomaatilise teooria ülesehitamisel soovime ju näiteks, et võrdusega predikaatarvutuses tuletatavad sekventsid oleksid tõesed kõigis mudelites, kus kehtivad võrduse aksioomid, rühmateoorias tuletatavad sekventsid peaksid olema tõesed kõigil rühmadel (interpretatsioonides, kus kehtivad rühmateooria aksioomid), võreteooria omad kõigil võredel jne.

Lihtsuse mõttes kõneleme siin ja järgnevas sekventside tõesusest, pidades selle all silmas nende valemkujude tõesust.

Teoreem 8. *(Korrektsuse teoreem.) Kui sekvents $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n \vdash \mathcal{G}$ on esimest järku teoorias tuletatav, siis ta on tõene teooria omaaksioomide kõikides mudelites.*

Tõestus. Selle teoreemi võib jällegi tõestada induktsiooniga tuletuspuu struktuuri järgi.

Induktsiooni baas. Puhta predikaatarvutuse aksioomid on samaselt tõesed, iga omaaksioom on aga ilmselt tõene teooria omaaksioomide kõikides mudelites.

Induktsiooni samm. Et tuletusreegliteks on puhta predikaatarvutuse tuletusreeglid, siis võib induktsiooni sammu üle võtta predikaatarvutuse korrektsuse teoreemi tõestusest, kus näidatakse, et iga fikseeritud mudeli puhul kandub sekventsi tõesus järk-järgult mööda tuletuspuud allapoole. □

Analoogilise relativiseerimisega kehtivad esimest järku teooriate puhul ka mittevasturääkivuse ja täielikkuse teoreem.

Teoreem 9. *(Mittevasturääkivuse teoreem.) Kui esimest järku teooria omaaksioomidel leidub mudel, siis on see teooria mittevasturääkiv.*

Tõestus. Kui teoorias oleksid tuletatavad sekventsid $\vdash \mathcal{F}$ ja $\vdash \neg\mathcal{F}$ ning teooria omaaksioomidel leidub mudel, siis peaksid valemid $\mathcal{F}$ ja $\neg\mathcal{F}$ olema selles mudelis mõlemad tõesed, mis on aga võimatu. □

Näiteks rühmateooria on mittevasturääkiv, sest omaaksioomidel leidub mudel: valime interpretatsiooni põhihulgaga $M = \{1\}$, konstantsümbol e tähistagu elementi 1 ja funktsionaalsümbol $\circ$ korrutamist. Selles interpretatsioonis on kõik omaaksioomid tõesed.

Analoogiliselt lause- ja predikaatarvutusega saab ka üldiste esimest järku teooriate kohta tõestada täielikkuse teoreemi järgneval kujul. Meie selle teoreemi tõestust käesolevas ei vaatle.

Teoreem 10. *(Täielikkuse teoreem.) Kui sekvents $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n \vdash \mathcal{G}$ on tõene esimest järku teooria omaaksioomide kõikides mudelites, siis sekvents on teoorias tuletatav.*

Võttes korrektsuse ja täielikkuse teoreemi kokku, saame, et esimest järku teoorias on tuletatavad parajasti need sekventsid, mis on teooria omaaksioomide kõikides mudelites tõesed.

Näiteks mingi sekventsi rühmateoorias saab tuletada parajasti siis, kui see sekvents on tõene kõigis rühmades, sekventsi formaalses aritmeetikas saab tuletada parajasti siis, kui sekvents on tõene formaalse aritmeetika aksioomide kõigis mudelites jne.

Formaalse aritmeetika aksioomid peavad silmas loomulikult ühte konkreetset mudelit põhihulgaga $\mathbb{N} = \{0, 1, 2, \dots\}$, kuid neil aksioomidel leidub ka teisi, standardsega mitteisomorfseid mudeleid. Sellest, et vaadeldavas interpretatsioonis kehtib induktsiooniaksiomiga $A7$ väljendatud väide „Iga valem $\mathcal{F}(x)$, mis on tõene elementidel $0, 0', 0'', \ldots,$ on tõene üldse kõigil elementidel“, ei piisa järelduseks, et põhihulgas pole muid elemente peale nimetatute. Formaalse aritmeetika aksioomidest saame tuletada ainult selliseid sekventse, mis on tõesed ühtviisi nii naturaalarvude hulgal kui ka aksioomide ülejäänud mittestandardsetes mudelites.

Eelmised teoreemid võrdlevad teoorias tuletatavate sekventside hulka teooria omaaksioomide kõikides mudelites tõeste sekventside hulgaga. Naturaalarvude keskse koha tõttu matemaatikas huvitab meid formaalse aritmeetika puhul aga rohkem võrdlus mudelis $\mathbb{N}$ tõeste sekventside hulgaga. Seni aluseks võetud kõikides mudelites tõesuse semantika asemel vaatleme seega nüüd ühes konkreetses mudelis tõesuse semantikat. Ka selle semantika suhtes võib püstitada küsimuse teooria korrektsusest ja täielikkusest.

Et ilmselt peavad formaalse aritmeetika aksioomid $A1$—$A7$ olema naturaalarvude puhul tõesed, siis kujutab $\mathbb{N}$ ühte nende aksioomide mudelit. Seega saame teoreemist 8, et kõik tuletatavad sekventsid on mudelis $\mathbb{N}$ tõesed ehk formaalne aritmeetika on korrektne. Täielikkuse kohta aga tõestas Kurt Gödel aastal 1931 järgmise *aritmeetika mittetäielikkuse teoreemi*: kui formaalne aritmeetika on mittevasturääkiv, siis 1) leidub valem, mis on mudelis $\mathbb{N}$ tõene, aga pole formaalses aritmeetikas tuletatav; 2) ka lõpliku (või üldiselt lahenduva) hulga mudelis $\mathbb{N}$ tõeste aksioomide lisamine ei muuda formaalset aritmeetikat täielikuks. Selleks konstrueeris Gödel valemi, mis väljendab iseenda mittetuletatavust, st juba vanadele kreeklastele tuntud valetajaparadoksi (kas lause „Ma valetan“ on tõene või väär?) tõestusteoreetilise variandi. Samuti näitas Gödel, et teatavatel loomulikel lisaeeldustel võib punktis 1) nimetatud omadustega valemiks võtta valemi, mis väljendab formaalse aritmeetika (või vastavalt laiendatud süsteemi) mittevasturääkivust. Hilisema aja uurimustes on selgunud, et taolised kontranäited ei tarvitse sugugi olla samavõrra kunstlikud ja tegelikest rakendustest kaugelseisvad, vaid juba 19. sajandil olid arvuteoorias olemas teoreemid, mis ei järeldu formaalse aritmeetika aksioomidest.

Formaalse aritmeetika mittevasturääkivuse probleem on matemaatika aluste uurimisel erilise tähtsusega. Kui tunnistada aksioomide $A1$—$A7$ tõesus mudelis $\mathbb{N}$ tuntuks ja mitteprobleemseks, siis on formaalne aritmeetika mittevasturääkiv teoreemi 9 põhjal. 19. sajandi lõpul asuti tõsisemalt tegelema matemaatika usaldusväärsuse põhjendamisega. Esimene katse teha seda hulgateooria abil luhtus, sest hulgateoorias endas avastati paradoksid. Järgmisena nähti võimalust formuleerida matemaatika alused aksiomaatilise süsteemina ning tõestada selle süsteemi mittevasturääkivus (nn Hilberti programm). Otsitav süsteem peab loomulikult sisaldama naturaalarvude aritmeetikat ja sealhulgas tuleks lahendada ka aritmeetika mittevasturääkivuse küsimus. Niisuguse eesmärgi korral aga ei saa *a priori* kasutada teadmisi lõpmatutest hulkadest (nagu $\mathbb{N}$), sest nii võiksime süsteemi sisse tuua paradoksid. Aritmeetika mittevasturääkivus tuleks tõestada võimalikult minimaalsete vahenditega (Hilberti väljenduse järgi finiitsete meetoditega). Gödeli tulemustest järeldub, et kui formaalne aritmeetika on mittevasturääkiv, siis tuleb selle tõestamiseks kasutusele võtta sinna mittekuuluvaid aksioome. Laiendatud teooria mittevasturääkivus vajaks omakorda põhjendamist uue laiendamise abil jne. Kaugema järeldusena tähendab see aga, et Hilberti programm kogu matemaatika aksiomatiseerimise põhjendamise kohta pole realiseeritav.

§ 5. Ülesanded

1. Konstrueerida teooria, mis on korrektne ja täielik lk 87 kirjeldatud semantika S_3 suhtes.

2. Leida semantika, mille suhtes teooria on korrektne ja täielik.

a) Tähestik on $\{\mathsf{p}, \mathsf{q}, -\}$, valemid on kõikvõimalikud sümbolijärjendid selles tähestikus. Aksioomid on kõik valemid kujul $x\mathsf{p}{-}\mathsf{q}x{-}$, kus x tähistab suvalist mittetühja sümbolite $-$ järjendit. Ainuke tuletusreegel on

$$\frac{x\mathsf{p}y\mathsf{q}z}{x\mathsf{p}y{-}\mathsf{q}z{-}},$$

kus x, y, z on suvalised mittetühjad sümbolite $-$ järjendid.

b) Tähestik on $\{\mathsf{T}, -\}$, valemid on selle kõikvõimalikud sümbolijärjendid. Aksioomid on kõik valemid kujul $-\mathsf{T}x$, kus x tähistab suvalist mittetühja sümbolite $-$ järjendit. Tuletusreeglid on

$$\frac{x\mathsf{T}y}{y\mathsf{T}x} \quad \text{ja} \quad \frac{x\mathsf{T}y}{x\mathsf{T}xy},$$

kus x ja y on suvalised mittetühjad sümbolite $-$ järjendid.

3. Käesolevas ülesandes tutvume sekventsiaalse lausearvutuse tuletusvõtetega. Tuletuspuu loomist alustatakse antud sekventsist, liikudes samm-sammult ülespoole. Puu iga haru tipus peab olema aksioom. Ainult *konjunktsiooni* ja *disjunktsiooni* sisaldavate sekventside tuletamiseks piisab kõige lihtsamast taktikast: lahutada vasaku ja parema poole valemid osadeks. Ettevaatlik tuleb olla disjunktsiooni paremale sissetoomise reegliga, mis võib joone peale tekitada mittetuletatavaid sekventse. Üldjuhul on kasulikum jagada vasak pool osadeks enne paremat. Iga järgneva sekventsi juures on antud tuletuspuu tippude ettenähtud arv.

a) $A \& (B \& C) \vdash (A \& B) \& C$ [7]
b) $(A \& B) \& C \vdash A \& (B \& C)$ [8]
c) $A \vee B \& C \vdash (A \vee B) \& (A \vee C)$ [12]
d) $(A \vee B) \& (A \vee C) \vdash A \vee B \& C$ [12]

Implikatsioone sekventsi paremas pooles saab käsitleda sarnaselt. Vasakul asuvat implikatsiooni saab tõestuses kasutada implikatsiooni paremalt eemaldamise reegli abil, valides valemi $\mathcal{F}$ nii, et $\mathcal{F} \to \mathcal{G}$ langeks kokku vasaku poole mingi valemiga või vasakul poolel oleva implikatsiooni tagaliikmega.

e) $A, A \to B \vdash B$ [3]
f) $A \to B, B \to C \vdash A \to C$ [6]
g) $A \& B \to C \vdash A \to (B \to C)$ [7]
h) $A \to (B \to C) \vdash A \& B \to C$ [7]
i) $A \to B, A \to (B \to C) \vdash A \to C$ [8]

Eituse paremale sissetoomise reeglis tuleb vasturääkivust tekitav valem $\mathcal{G}$ valida selliselt, et nii $\mathcal{G}$ kui $\neg\mathcal{G}$ oleksid vasakust poolest (kuhu on lisatud valem $\mathcal{F}$) järeldatavad, tihti sobib mõni vasaku poole valem või selle osa. Mõnikord tuleb selle reegli kasutamiseks luua võimalus sel teel, et parema poole ette lisatakse $\neg\neg$.

j) $\neg(A \vee B) \vdash \neg A$ [4]
k) $A \to B, \neg B \vdash \neg A$ [5]
l) $A, \neg B \vdash \neg(A \to B)$ [5]
m) $\neg A, \neg B \vdash \neg(A \vee B)$ [8]
n) $\neg A \to \neg B \vdash B \to A$ [7]

4. Tuletada sekventsid, mis väljendavad lausearvutuse tehete vahelisi seoseid.

a) $\neg(A \vee B) \vdash \neg A \& \neg B$ [9]
b) $\neg A \& \neg B \vdash \neg(A \vee B)$ [9]
c) $\neg(A \& B) \vdash \neg A \vee \neg B$ [12]
d) $\neg A \vee \neg B \vdash \neg(A \& B)$ [9]
e) $A \to B \vdash \neg A \vee B$ [10]
f) $\neg A \vee B \vdash A \to B$ [8]

g) $A \to B \vdash \neg(A \& \neg B)$ [7]

h) $\neg(A \& \neg B) \vdash A \to B$ [7]

i) $A \vee B \vdash \neg A \to B$ [8]

j) $\neg A \to B \vdash A \vee B$ [10]

k) $A \& B \vdash \neg(A \to \neg B)$ [6]

l) $\neg(A \to \neg B) \vdash A \& B$ [9]

m) $A \& B \vee \neg A \& \neg B \vdash (A \to B) \& (B \to A)$ [19]

n) $(A \to B) \& (B \to A) \vdash A \& B \vee \neg A \& \neg B$ [26]

5. Tuletada järgmised sekventsid.

a) $\vdash (A \to B) \vee (B \to A)$ [11]

b) $\vdash ((A \to B) \to A) \to A$ [11]

c) $\vdash (A \vee (A \to B) \to B) \to B$ [9]

d) $\neg A \to B, A \to B \vdash B$ [10]

e) $A \to \neg(B \to C) \vdash (A \to B) \& (A \to \neg C)$ [19]

f) $(A \to B) \to (\neg C \to \neg B) \vdash B \to C$ [10]

g) $(A \vee B) \& (\neg A \vee B) \& (A \vee \neg B) \vdash \neg(\neg A \vee \neg B)$ [25]

h) $(\neg A \vee \neg B) \& (\neg A \vee B) \& (A \vee \neg B) \& (A \vee B) \vdash C$ [38]

6. Vaatleme sekventsiaalse lausearvutuse analoogi, milles on standardsete aksioomide kõrvale lisatud aksioom $\vdash A \& \neg A$. Tõestada, et selles teoorias saab tuletada suvalise sekventsi $\vdash \mathcal{F}$.

7. Vaatleme sekventsiaalse lausearvutuse analoogi, milles sekventsid sisaldavad ainult lausemuutujatest A_1, A_2, ..., A_n koostatud valemeid. Olgu $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ nende muutujate fikseeritud väärtustus. Lisame teooriale standardsete lausearvutuse aksioomide kõrvale veel aksioomid $\vdash A_1^{\alpha_1}$, $\vdash A_2^{\alpha_2}$, ..., $\vdash A_n^{\alpha_n}$. Tõestada, et selles teoorias saab tuletada suvalise sekventsi $\vdash \mathcal{F}$, kus $\mathcal{F}$ on lausearvutuse valem, mis on väärtustusel $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ tõene.

8. Vaatleme sekventsiaalse lausearvutuse analoogi, milles sekventsid sisaldavad ainult lausemuutujatest A, B, C koostatud valemeid. Standardsete aksioomide kõrvale lisame veel aksioomid

$$\vdash A \vee B, \qquad \vdash B \vee C, \qquad \vdash A \vee C.$$

Tõestada, et selles teoorias saab tuletada suvalise sekventsi $\vdash \mathcal{F}$, kus $\mathcal{F}$ on lausearvutuse valem, mis on tõene muutujate A, B, C igal sellisel väärtustustel, kus vähemalt kaks muutujat on tõesed.

9. Vaatleme sekventsiaalse lausearvutuse analoogi, milles on standardsete tuletusreeglite kõrvale lisatud veel reeglid

$$\frac{\Gamma, \mathcal{F} \vee \mathcal{G} \vdash \mathcal{H}}{\Gamma, \mathcal{G} \vee \mathcal{F} \vdash \mathcal{H}} \quad \text{ja} \quad \frac{\Gamma \vdash \mathcal{F} \& \mathcal{G}}{\Gamma \vdash \mathcal{G} \& \mathcal{F}}.$$

Kas nende reeglite lisamisel tekib tuletatavaid sekventse juurde?

10. Predikaatarvutuse sekventside tuletusvõtted sarnanevad lausearvutuse omadega, arvestada tuleb veel kvantorreegleid. Lihtsamatel juhtudel piisab valemeid analüüsivate reeglite rakendamisest õiges järjekorras, st ülespoole liikudes rakendatakse kõigepealt kitsendusega reeglit.

a) $\exists x \exists y P(x,y) \vdash \exists y \exists x P(x,y)$ [5]

b) $\exists x \forall y P(x,y) \vdash \forall y \exists x P(x,y)$ [5]

c) $\exists x P(x) \vee \exists x Q(x) \vdash \exists x (P(x) \vee Q(x))$ [9]

d) $\forall x P(x) \vee \forall x Q(x) \vdash \forall x (P(x) \vee Q(x))$ [8]

Eituse paremale sissetoomise reegli ja implikatsiooni paremalt eemaldamise reegli korral tuleb valem valida nii, et saaks kitsendusega reeglit õigel ajal rakendada. Keerulisematel juhtudel tuleb tuua sisse valemi (nt mingi lausemuutuja) ja tema eituse disjunktsioon või tekitada parema poole ette $\neg\neg$.

e) $\neg \forall x P(x) \vdash \exists x \neg P(x)$ [9]

f) $\exists x \neg P(x) \vdash \neg \forall x P(x)$ [5]

g) $\neg \exists x P(x) \vdash \forall x \neg P(x)$ [5]

h) $\forall x \neg P(x) \vdash \neg \exists x P(x)$ [7]

11. Tuletada järgmised sekventsid, mis kujutavad predikaatarvutuse põhisamaväärsusi juhul, kui implikatsiooni pooltest üks ei sisalda kvantoriga seotud indiviidmuutujat vabalt.

a) $\forall x (P(x) \to Q) \vdash \exists x P(x) \to Q$ [7]

b) $\exists x P(x) \to Q \vdash \forall x (P(x) \to Q)$ [6]

c) $\exists x (P(x) \to Q) \vdash \forall x P(x) \to Q$ [6]

d) $\forall x P(x) \to Q \vdash \exists x (P(x) \to Q)$ [19]

e) $\forall x (P \to Q(x)) \vdash P \to \forall x Q(x)$ [7]

f) $P \to \forall x Q(x) \vdash \forall x (P \to Q(x))$ [9]

g) $\exists x (P \to Q(x)) \vdash P \to \exists x Q(x)$ [6]

h) $P \to \exists x Q(x) \vdash \exists x (P \to Q(x))$ [23]

12. Tuletada järgmised sekventsid.

a) $\forall x \exists y (P(x) \,\&\, Q(y)) \vdash \exists y \forall x (P(x) \,\&\, Q(y))$ [22]

b) $\vdash \forall x P(x) \vee \exists x \neg P(x)$ [11]

c) $\vdash \exists x \forall y (P(x) \to P(y))$ [27]

d) $\forall x \forall y \forall z (P(x,y) \,\&\, P(y,z) \to P(x,z)), \forall x \neg P(x,x) \vdash$
$\vdash \neg (P(x,y) \,\&\, P(y,x))$ [10]

e) $\forall x \forall y (P(x,y) \to P(y,x)), \forall x \forall y \forall z (P(x,y) \,\&\, P(y,z) \to$
$\to P(x,z)) \vdash \exists u P(u,w) \to P(w,w)$ [16]

13. Vaatleme sekventsiaalse predikaatarvutuse analoogi, milles on aksioomideks kõik standardsed aksioomid ning lisaks veel sekventsid $\vdash \forall x A(x)$ ja $\vdash \forall x \neg A(x)$. Tõestada, et niisuguses teoorias saab tuletada suvalise sekventsi $\vdash \mathcal{F}$.

14. Olgu vaatluse all sekventsiaalse predikaatarvutuse analoog, milles standardsete tuletusreeglite kõrvale on lisatud veel reegel

$$\frac{\Gamma \vdash \forall x \mathcal{F}(x) \vee \forall x \mathcal{G}(x)}{\Gamma \vdash \forall x(\mathcal{F}(x) \vee \mathcal{G}(x))}\,.$$

Näidata, et kui selles teoorias on konstrueeritud mingi sekventsi tuletuspuu, mis kasutab lisatud reeglit, siis saab konstrueerida sama sekventsi tuletuspuu, mis seda reeglit ei kasuta.

15. Tuletada võrdusega predikaatarvutuses sekventsid

a) $\vdash \forall x \forall y \forall z(x = z \,\&\, y = z \to x = y)$

b) $\vdash \forall x \forall y \forall z \forall u(x = y \,\&\, y = z \,\&\, z = u \to x = u)$

c) $\vdash \forall x \forall y \forall z(x = y \,\&\, \neg(z = x) \to \neg(z = y))$

d) $P(a), \forall x(P(x) \to Q(x)), a = b \vdash Q(b)$

e) $\forall x(P(x) \to x = a \vee x = b), \exists x(P(x) \& Q(x)) \vdash Q(a) \vee Q(b)$

16. Tuletada esimest järku rühmateoorias sekventsid

a) $\vdash \forall a \forall x \forall y(a \circ x = a \circ y \to x = y)$

b) $\vdash \forall a \forall x \forall y(x \circ a = y \circ a \to x = y)$

c) $\vdash \forall a \forall x \forall y(a \circ x = e \,\&\, y \circ a = e \to x = y)$

17. Tõestada, et rühmateoorias tuletatavate sekventside hulk jääb samaks, kui aksioomid $G1$—$G5$ asendada aksioomidega $G1$, $G2$, $G4$.

18. Tuletada formaalses aritmeetikas sekventsid

a) $\vdash \forall a \forall b(a = b \to a' = b')$

b) $\vdash \forall a \forall b \forall c(a = b \to a + c = b + c)$

c) $\vdash \forall a \forall b \forall c(a = b \to c + a = c + b)$

d) $\vdash \forall a \forall b \forall c((a + b) + c = a + (b + c))$

e) $\vdash \forall a \forall b(a' + b = (a + b)')$

f) $\vdash \forall a \forall b(a + b = b + a)$

g) $\vdash \forall a \forall b \forall c(a \cdot (b + c) = (a \cdot b) + (a \cdot c))$

19. Tõestada, et kui esimest järku teoorias on tuletatav valem $\mathcal{F}$, siis leidub valem $\mathcal{G}$, mis kujutab teooria teatavate aksioomide konjunktsiooni, nii et valem $\mathcal{G} \to \mathcal{F}$ on samaselt tõene.

IV. TURINGI MASINAD

§ 1. Turingi masina mõiste

Algoritm on eeskiri, mis määrab teatavat liiki ülesannete lahendamiseks vajalikud operatsioonid ja nende järjekorra. Üks vanemaid ja tuntumaid on antiikajast pärinev Eukleidese algoritm kahe naturaalarvu suurima ühisteguri leidmiseks. Sajandite vältel on algoritme koostatud palju — näiteks kuupvõrrandi lahendamiseks, arvude tegurdamiseks, esemete optimaalse valiku või paigutuse leidmiseks jne. Algoritmidest räägiti seejuures ainult konkreetselt ja positiivselt, tõestades, et antud eeskiri on antud ülesande lahendamise algoritm. Teiselt poolt aga kogunes ajapikku ülesandeid, mille lahendamiseks ei õnnestunud algoritmi leida. Üks niisugustest ülesannetest oli näiteks Hilberti kümnes probleem: teha kindlaks, kas täisarvuliste kordajatega n muutuja polünoomil leidub täisarvuline nullkoht. Tänaseks on teada, et selle ja paljude teiste ülesannete lahendamiseks ei olegi olemas üldist algoritmi.

Et oleks võimalik tõestada mingi algoritmi puudumist, tuleb kõigepealt täpselt määratleda, mida üldse algoritmi all mõista. Paljudest lähenemisviisidest on praeguseks välja kujunenud mitmeid väliselt erinevaid, kuid sisult ekvivalentseid algoritmi mõiste formalisatsioone. Meie vaatleme nendest nn Turingi masinat, mis kirjeldab algoritmi mõistet teatava idealiseeritud arvuti kujul ning mille tõid sisse inglise matemaatik Alan Turing (1912—1954) ning ameerika loogik ja matemaatik Emil Post (1897—1954) aastal 1936.

Turingi masin koosneb lindist, lugevast-kirjutavast peast, sisemälust ja käskude tabelist. Lint on mõlemas suunas lõpmatu ning jagatud ühesuurusteks pesadeks. Igasse pessa on kirjutatud üks sümbol lõplikust tähestikust $\{s_1, s_2, \ldots, s_m\}$ või tühik s_0. Eeldame, et alguses on lindil vaid lõplik hulk tühikust erinevaid sümboleid, kõik ülejäänud pesad on täidetud tühikutega. Lugev-kirjutav pea võib liikuda mööda linti pesast pesasse, lugeda pesas oleva sümboli või kirjutada sinna olemasoleva sümboli asemele uue. Sisemälu on igal ajamomendil ühes lõplikust hulgast seisunditest $q_0, q_1, \dots, q_k$, millest seisundeid $q_1, \dots, q_k$ nimetatakse aktiivseteks ning seisundit q_0 passiivseks. Masin alustab arvutusi esimeses aktiivses seisundis q_1, töö käigus võib ta üle minna ühest seisundist teise.

Instruktsioone pea tegevuse ja seisundite muutumise kohta esitatakse *käskudena*

$$s_a q_b \to s_c q_d K,$$

kus s_a ja s_c tähistavad sümboleid ($0 \leqslant a, c \leqslant m$), q_b ja q_d seisundeid ($1 \leqslant b \leqslant k$, $0 \leqslant d \leqslant k$) ning K on üks tähtedest L, R, C. Sama vasaku poolega käske ei tohi olla rohkem kui üks. Vasaku poole järgi koondatakse käsud *tabelisse*, mille read vastavad masina seisunditele, veerud aga tähestiku sümbolitele:

	s_0	s_1	$\dots$	s_a	$\dots$	s_m
q_1						
$\vdots$						
q_b				$s_c q_d K$		
$\vdots$						
q_k						

Mõned lahtrid võivad ka tühjaks jääda, kui vastava vasaku poolega käsku ei ole. Tabel määrab seega konkreetse Turingi masina, tihti nimetatakse tabelit ka Turingi masina *programmiks*.

Turingi masin töötab taktide kaupa, iga takti täitmine võtab ühe ajaühiku. Oletame, et pea all on sümbol s_a ning masin on seisundis q_b. Kui tabeli lahtris, mis vastab sümbolile s_a ning seisundile q_b, leidub käsk $s_c q_d K$, siis kirjutatakse lindile pea all olevasse pessa sümboli s_a asemele sümbol s_c, masin läheb seisundist q_b seisundisse q_d ning pea liigub ühe positsiooni võrra vasakule, ühe positsiooni võrra paremale või ei liigu üldse vastavalt K väärtusele L, R või C. Sellega on üks takt läbi, samasugune tegevus kordub igal järgmisel taktil. Masin lõpetab töö, kui ta mingi käsu toimel siirdub passiivsesse seisundisse q_0 või kui järgmisena täitmisele kuuluvat käsku pole olemas (täitmisjärg jõuab tühja lahtrisse). Kui aga kumbagi olukorda ette ei tule, siis jätkub masina töö lõpmatult.

Igal ajahetkel võib Turingi masina seisu kirjeldada kolme asjaoluga: millised sümbolid asuvad lindi pesades, kus asub lugev-kirjutav pea ning millises seisundis masin parajasti viibib. Masin alustab tööd mingis algseisus ja peatub mingis lõppseisus. Kui masina seis on teada, siis saab selle järgi leida kõik järgnevad seisud. Mõnikord nimetatakse Turingi masina seisu, st komplekti, mis koosneb lindi lahtrite sisust, pea asukohast ja masina seisundist üheskoos võetuna, ka *situatsiooniks*. Komplekti, mis koosneb lindi lahtrite sisust ja pea asukohast, nimetatakse *konfiguratsiooniks*. Masina seisu mingil hetkel määravad seega konfiguratsioon ja seisund, milles masin sellel hetkel asub.

Et Turingi masina mõiste on kasutusele võetud algoritmide teoreetiliseks uurimiseks, siis on tema praktilise kasutamisega seotud küsimused teisejärgulised, muu hulgas ka see, et üksikute sammude elementaarsuse tõttu tuleb lihtsatki ülesannet lahendava masina tabel üsna mahukas ja arvutus võib kesta suure hulga takte. Palju olulisemad on põhimõttelist ja fundamentaalset laadi küsimused. Konstruktsiooni lihtsuse tõttu saab Turingi masinate kohta hõlpsasti tõestada mitmeid üldisi teoreeme, mida võib siis pidada kehtivaks suvaliste algoritmide korral, sest siiamaani pole teada ühtegi algoritmi, mida ei saaks vähemalt põhimõtteliselt kirja panna Turingi masinana (jätame kõrvale niisugused, mis kasutavad näiteks juhuslikkust mingi füüsikalise protsessi näol). Samuti sobib algoritmi täitmiseks kulunud taktide arv sammude ühetaolisuse tõttu hästi algoritmi ajalise keerukuse mõõduks. Suur sammude arv pole keerukuse uurimisel takistuseks, sest sammu tegemise aeg pole fikseeritud; tähtsam on see, kuidas sammude arv muutub ülesande mahu kasvades.

Järgnevas käsitleme naturaalarvuliste argumentide ja väärtusega funktsioonide arvutatavuse küsimusi. Selleks tuleb kokku leppida, kuidas arve, st algandmeid ja arvutuse tulemust, Turingi masina lindil kujutada.

Fikseerime tähestiku järgmiselt: $s_0 = \texttt{-}$, $s_1 = \texttt{0}$, $s_2 = \texttt{1}$. Naturaalarvu x esitame lindil sümbolijadana

$$\texttt{0}\underbrace{\texttt{11...1}}_{x \text{ ühte}},$$

naturaalarvude järjendi $(x_1, \ldots, x_n)$ esitus olgu

$$\texttt{0}\underbrace{\texttt{11...1}}_{x_1 \text{ ühte}}\texttt{0}\underbrace{\texttt{11...1}}_{x_2 \text{ ühte}}\texttt{...0}\underbrace{\texttt{11...1}}_{x_n \text{ ühte}}.$$

Kõik arvud peavad siin olema kirjutatud üksteise järele ilma tühikuteta. Lisaks mõistame standardkonfiguratsiooni all niisugust konfiguratsiooni, kus lindil on ülaltoodud kujuga sümbolijada ning masina pea asub viimase nulli (viimase arvu algust tähistava nulli) kohal. Standardseks nimetame ka Turingi masina seisu, kui tema puhul on masina konfiguratsioon standardne.

Neid kokkuleppeid arvestades saab defineerida, mis on Turingi masina poolt arvutatav funktsioon ja mis on Turingi mõttes arvutatav funktsioon. Et ühte ja sama Turingi masinat võib rakendada erineva liikmete arvuga naturaalarvujärjenditele, siis seostub iga masinaga üks ühekohaline, üks kahekohaline jne funktsioon. Turingi masina töötamise spetsiifikale vastavalt ei tarvitse need funktsioonid olla kõikjal määratud.

Definitsioon 1. *Turingi masina $\mathcal{M}$ poolt arvutatav n muutuja funktsioon $f^n_{\mathcal{M}}$ defineeritakse järgmiselt. Eeldame, et masina töö alguses on lindil*

$$\mathtt{0}\underbrace{\mathtt{11...1}}_{x_1 \text{ ühte}}\mathtt{0}\underbrace{\mathtt{11...1}}_{x_2 \text{ ühte}}\mathtt{...0}\underbrace{\mathtt{11...1}}_{x_n \text{ ühte}}$$

ja pea asub viimase nulli kohal. Kui masin peatub lõpliku arvu sammude järel, töö lõpus on lindil

$$\mathtt{0}\underbrace{\mathtt{11...1}}_{x_1 \text{ ühte}}\mathtt{0}\underbrace{\mathtt{11...1}}_{x_2 \text{ ühte}}\mathtt{...0}\underbrace{\mathtt{11...1}}_{x_n \text{ ühte}}\mathtt{0}\underbrace{\mathtt{11...1}}_{y \text{ ühte}}$$

ja pea asub viimase nulli kohal, siis funktsiooni $f^n_{\mathcal{M}}$ väärtuseks argumentidel $x_1, x_2, \ldots, x_n$ on y. Vastasel korral on funktsiooni väärtus nendel argumentidel määramata.

Definitsioon 2. *Funktsiooni f nimetatakse Turingi mõttes arvutatavaks, kui leiduvad Turingi masin $\mathcal{M}$ ja naturaalarv n, et $f = f^n_{\mathcal{M}}$.*

Turingi masina mõiste ja viimaste definitsioonide selgituseks esitame mõned näited Turingi mõttes arvutatavatest funktsioonidest.

Näide 1. Konstantne funktsioon $f(x) = 3$ on Turingi mõttes arvutatav.

Seda funktsiooni arvutab näiteks järgneva tabeliga Turingi masin. Igast reast paremal on kirja pandud ka selgitus, mida masin selles seisundis teeb.

	-	0	1	
q_1	$0q_2R$	$0q_1R$	$1q_1R$	lõppu 0
q_2	$1q_3R$			kirjutada 1
q_3	$1q_4R$			kirjutada 1
q_4	$1q_5L$			kirjutada 1
q_5		$0q_0C$	$1q_5L$	pea õigesse kohta

Programmi toimel liigub pea argumendi nulli kohalt argumendi lõppu ning kirjutab sinna nulli ja kolm ühte. Seejärel liigub pea tagasi viimase nulli kohale, millega tekib standardne lõppseis.

Näide 2. Samasusfunktsioon $f(x) = x$ on Turingi mõttes arvutatav.

Siin ei saa iga ühe jaoks omaette seisundit reserveerida nagu eelmises näites, sest masin peab töötama suvalise arvu ühtede korral. Organiseerime seega töö nii, et masin kopeerib sümbolid 1 argumendist vastusesse ükshaaval, iga kord asendab argumendis järjekordse sümboli 1 tühikuga ja kirjutab vastuse lõppu ühe sümboli 1 juurde.

	-	0	1	
q_1	$0q_2L$	$0q_1R$	$1q_1R$	lõppu 0
q_2		$0q_3R$	$1q_2L$	argumendi algusesse
q_3		$0q_0C$	$-q_4R$	asendada 1 tühikuga
q_4	$1q_5L$	$0q_4R$	$1q_4R$	liikuda lõppu ja kirjutada 1
q_5	$1q_3R$	$0q_5L$	$1q_5L$	liikuda tagasi tühikuni

Tabeli põhiosaks on tsükkel seisundites q_3, q_4, q_5, kus argumendi sümboleid 1 asendatakse tühikuga järjekorras vasakult paremale. Kui kõik sümbolid 1 on vastusesse üle kantud ja järg jõudnud vastuse algust tähistava sümbolini 0, siis masin peatub.

Niisuguse tabeliga määratud Turingi masin $\mathcal{M}$ arvutab iga $n \geqslant 1$ korral mingit funktsiooni $f^n_{\mathcal{M}}$. Et lugev-kirjutav pea ei liigu töö käigus viimase argumendi nullist vasakule, siis tegeleb masin ka juhul, kui talle antakse ette mitu argumenti, ikka viimase argumendi kopeerimisega. Järelikult on iga n korral $f^n_{\mathcal{M}}(x_1, x_2, \dots, x_n) = x_n$.

Näide 3. Funktsioon $f(x, y) = x + y$ on Turingi mõttes arvutatav.

Kahe arvu liitmiseks tuleb mõlema argumendi ühed kopeerida argumentide järele. Seisundid q_4, q_5, q_6 tegelevad esimese argumendi, seisundid q_7, q_8, q_9 aga teise argumendi ühtede ülekandmisega.

	-	0	1	
q_1	$0q_2L$	$0q_1R$	$1q_1R$	lõppu 0
q_2		$0q_3L$	$1q_2L$	teise argumendi algusesse
q_3		$0q_4R$	$1q_3L$	esimese argumendi algusesse
q_4		$0q_7R$	$-q_5R$	asendada 1 tühikuga
q_5	$1q_6L$	$0q_5R$	$1q_5R$	liikuda lõppu ja kirjutada 1
q_6	$1q_4R$	$0q_6L$	$1q_6L$	liikuda tagasi tühikuni
q_7		$0q_0C$	$-q_8R$	asendada 1 tühikuga
q_8	$1q_9L$	$0q_8R$	$1q_8R$	liikuda lõppu ja kirjutada 1
q_9	$1q_7R$	$0q_9L$	$1q_9L$	liikuda tagasi tühikuni

Selle tabeliga antud masin $\mathcal{M}$ arvutab juhul $n \geqslant 2$ funktsiooni $f^n_{\mathcal{M}}(x_1, x_2, \dots, x_n) = x_{n-1} + x_n$, juhul $n = 1$ aga satub masin pärast argumendi läbimist seisundis q_3 tühja lahtrisse ja peatub mittestandardses lõppseisus, mistõttu $f^1_{\mathcal{M}}(x_1)$ on kõikjal määramata.

Näide 4. Ka kahe arvu vahet saab Turingi masinaga arvutada. Et vahe võib olla negatiivne, lindil tohivad aga olla ainult mittenegatiivsed arvud, siis vaatleme tavalise vahe asemel nn lõigatud vahet

$$x \dot{-} y = \begin{cases} x - y, & \text{kui } x \geqslant y, \\ 0, & \text{kui } x < y. \end{cases}$$

Funktsiooni $f(x, y) = x \dot{-} y$ arvutamiseks sobib järgmine Turingi masin. See töötab samuti nagu eelmise näite masin, ainult teise argumendi iga sümboli 1 korral kustutatakse vastusest üks sümbol 1.

	-	0	1	
q_1	$0q_2L$	$0q_1R$	$1q_1R$	lõppu 0
q_2		$0q_3L$	$1q_2L$	teise argumendi algusesse
q_3		$0q_4R$	$1q_3L$	esimese argumendi algusesse
q_4		$0q_7R$	$-q_5R$	asendada 1 tühikuga
q_5	$1q_6L$	$0q_5R$	$1q_5R$	liikuda lõppu ja kirjutada 1
q_6	$1q_4R$	$0q_6L$	$1q_6L$	liikuda tagasi tühikuni
q_7		$0q_0C$	$-q_8R$	asendada 1 tühikuga
q_8	$-q_9L$	$0q_8R$	$1q_8R$	liikuda lõppu
q_9		$0q_{10}L$	$-q_{10}L$	kustutada 1
q_{10}	$1q_7R$	$0q_{10}L$	$1q_{10}L$	liikuda tagasi tühikuni

Definitsiooni järgi on Turingi masina $\mathcal{M}$ poolt arvutatav funktsioon $f^n_{\mathcal{M}}$ määratud argumentide $x_1, x_2, \ldots, x_n$ korral vaid siis, kui masin $\mathcal{M}$, alustades tööd standardsest algseisust, peatub lõpliku arvu sammude järel standardses lõppseisus. Seejuures peavad olema alles kõik algsed argumendid ja funktsiooni väärtus peab olema kirjas nende järel. Kui need nõuded ei ole täidetud, siis on funktsiooni $f^n_{\mathcal{M}}$ väärtus argumentide $x_1, x_2, \ldots, x_n$ korral määramata. Sisuliselt tähendab määramatus kolme võimalust:

1) masin ei peatu;
2) masin peatub, kuid lindil pole vajaliku kujuga sümbolijada;
3) masin peatub ja lindil on vajaliku kujuga sümbolijada, kuid pea ei asu õiges kohas.

Kahel viimasel juhul ei ole määramatus põhimõtteline, me võiksime funktsioonile anda samuti mingi väärtuse, näiteks nulli. Kõigi Turingi mõttes arvutatavate funktsioonide hulk sellest ei muutu: kui funktsioon f on arvutatav Turingi masinaga, mille poolt arvutatava funktsiooni väärtus juhtudel 2) ja 3) on määramata, siis on ta arvutatav ka sellise Turingi masinaga, mille poolt arvutatava funktsiooni väärtuseks nendel juhtudel loetakse null, ning ümberpöördult. Küll aga ei või juhul 1) omistada Turingi masina poolt arvutatava funktsiooni väärtuseks konkreetset arvu, sest siis tuleks Turingi mõttes arvutatavaks lugeda ka näiteks niisugune kõikjal määratud funktsioon, mille puhul iga seda funktsiooni arvutav Turingi masin töötab mõnel argumendi väärtusel lõpmata kaua, ja seega algoritmiliselt lahenduvaks ülesanne, mis intuitiivse arusaama järgi seda ei ole.

Et Turingi masin võib mõnel argumendil töötada lõpmatult, siis leidub Turingi mõttes arvutatavaid funktsioone, mis on vaid osaliselt määratud. Matemaatikas kasutatakse sellises olukorras mõnikord funktsiooni jätkamist, vaadeldes osaliselt määratud funktsiooni asemel kõikjal määratud funktsiooni, mille väärtused langevad kokku esialgse funktsiooni väärtustega kõigil argumentidel, millel esialgne funktsioon on määratud. Ent niisugusel üleminekul ei tarvitse säilida funktsiooni olulised omadused, praegusel juhul arvutatavus. Algoritmiteoorias tõestatakse, et leidub mitte kõikjal määratud Turingi mõttes arvutatavaid funktsioone, mida pole võimalik jätkata kõikjal määratud Turingi mõttes arvutatavateks funktsioonideks. Jätkamisel saadud funktsioon asuks siis kindlasti väljaspool arvutatavate funktsioonide klassi. Seega, kui meie eesmärgiks on uurida küsimusi, mis seostuvad funktsioonide arvutatavusega, peame paratamatult lubama käsitluses osaliselt määratud funktsioone.

Eelnevate definitsioonidega eraldatakse kõikide naturaalarvuliste funktsioonide hulgast välja need, mida saab arvutada mingi Turingi masinaga. Lihtne on veenduda, et Turingi masina tabeleid on loenduv hulk, mistõttu on ka Turingi mõttes arvutatavate funktsioonide hulk loenduv. Et aga kõigi naturaalarvuliste n muutuja funktsioonide hulk on kontiinumi võimsusega (juba naturaalarvude hulga alamhulkade karakteristlikke funktsioone on kontiinumi võimsusega hulk), siis leidub mittearvutatavaid funktsioone isegi rohkem kui arvutatavaid. Järgnevas näeme, et mittearvutatavad on ka mõned sellised funktsioonid, mis pakuvad otsest huvi algoritmiteooria seisukohalt.

Peale Turingi masina on olemas veel mitmeid algoritmi mõiste formalisatsioone, näiteks osaliselt rekursiivsed funktsioonid (S. C. Kleene), lambdaarvutus (A. Church), normaalalgoritmid (A. Markov). On aga osutunud, et kõik need formalisatsioonid on omavahel ekvivalentsed, st määravad ühe ja sama arvutatavate funktsioonide klassi. Seepärast on algoritmiteoreetikud arvamusel, et kõik nimetatud formalisatsioonid kirjeldavadki igaüks erineval viisil algoritmi mõiste intuitiivselt tajutavat sisu. Niisugust väidet nimetatakse Churchi teesiks. Formuleerime selle Turingi masinate jaoks.

Churchi tees. *Iga algoritmiliselt arvutatav funktsioon on arvutatav Turingi masina abil.*

Churchi teesi ei ole võimalik tõestada, sest „algoritmiliselt arvutatav“ on mittematemaatiline mõiste ja väljendab inimeste tavaarusaama algoritmidest. Vastupidiselt on „arvutatav Turingi masina abil“ defineeritud rangelt ja tal on kindel matemaatiline sisu. Küll aga on Churchi teesi võimalik ümber lükata, näiteks juhul, kui avastatakse funktsioon, mis on ilmselgelt algoritmiliselt arvutatav, kuid mida ei saa arvutada ühegi Turingi masinaga. Vaatamata pikaajalisele uurimistööle algoritmiteoorias, pole niisugust funktsiooni leitud.

§ 2. Kompositsioon ja hargnemine

Kanname Turingi masinatele üle kaks operatsiooni, mille analoogid igapäevaterminites on mitme algoritmi järjestrakendamine ja algoritmi täitmiskäigu hargnemine vastavalt mingi teise algoritmi töö tulemusele.

Eeldame, et kõik vaadeldavad masinad töötavad ühes ja samas tähestikus $\{s_0, s_1, \ldots, s_m\}$. Et masina kogu arvutuskäik on määratud konfiguratsiooniga töö alguses (algseisund on alati q_1), siis toome sisse järgmised tähised. Kui masin $\mathcal{M}$ alustab tööd konfiguratsioonis X ja peatub lõpliku arvu sammude järel konfiguratsioonis X', siis kirjutame $\mathcal{M}(X) = X'$. Kui aga masin $\mathcal{M}$ töötab konfiguratsiooni X puhul lõpmatult, siis märgime $\mathcal{M}(X) = \perp$.

Algoritmide järjestrakendamisele vastab Turingi masinate kompositsioon. Olgu teada lindi algseis ja pea algasend, st algkonfiguratsioon. Paneme kõigepealt tööle masina $\mathcal{M}_1$. Kui masin töö lõpetab, siis käivitame tekkinud konfiguratsioonis masina $\mathcal{M}_2$. Masin, mis annab alati sama tulemuse nagu masinad $\mathcal{M}_1$ ja $\mathcal{M}_2$ järjest rakendatult, on nende masinate kompositsioon.

Definitsioon 3. *Turingi masinat $\mathcal{M}$ nimetatakse masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ kompositsiooniks, kui iga algkonfiguratsiooni X korral kehtib võrdus $\mathcal{M}(X) = \mathcal{M}_2(\mathcal{M}_1(X))$.*

Suvalist masinat, mis on masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ kompositsioon, märgime tähisega $\mathcal{M}_2 \circ \mathcal{M}_1$, kus sarnaselt funktsioonide kompositsiooniga on $\mathcal{M}_2$ vasakul ja $\mathcal{M}_1$ paremal.

Definitsioonis nõutakse, et masina $\mathcal{M}$ töö lõppedes on lindi pesade sisu ja pea asend täpselt sama nagu pärast masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$

töö lõppu. Kui masin $\mathcal{M}$ töötab mingi konfiguratsiooni korral lõpmatult, siis peavad ka $\mathcal{M}_1$ ja $\mathcal{M}_2$ järjest rakendatult töötama selle konfiguratsiooni korral lõpmatult.

Masin $\mathcal{M}$, mis on masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ kompositsioon, ei pea modelleerima nende masinate tööd ega olema nendega muul moel seotud peale alg- ja lõppkonfiguratsioonide võrdsuse. Kui näiteks valida suvalised kolm masinat, mis kõik töötavad iga argumendi korral lõpmatult, kuid igaüks erineval viisil, siis on igaüks neist kahe ülejäänu kompositsioon. Siiski leidub ühtne võte, kuidas moodustada kahe etteantud masina tabelite põhjal nende kompositsioonmasina tabel nii, et saadud masina töö jäljendab antud masinate järjestikust tööd.

Teoreem 1. *Kui $\mathcal{M}_1$ ja $\mathcal{M}_2$ on samas tähestikus töötavad Turingi masinad, siis saab nende masinate tabelite järgi alati koostada kompositsioonmasina tabeli.*

Tõestus. Olgu masinal $\mathcal{M}_1$ aktiivsed seisundid $q_1, q_2, \ldots, q_k$ ning masinal $\mathcal{M}_2$ seisundid $r_1, r_2, \ldots, r_l$. Kirjutame masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ tabelid teineteise järele, andes esimese masina peatumiskohtades juhtimise teise masina esimesele seisundile. Selleks asendame igal pool seisundi q_0 seisundiga r_1, esimese masina tabeli igasse tühja lahtrisse $s_a q_b$ kirjutame aga $s_a r_1 C$. Niisugune teisendatud tabel ongi kompositsioonmasina tabel, sest kui esimese masina töö on valmis, siis suundub täitmisjärg alati teise masina avaseisundisse. $\square$

Eeldame nüüd, et masinad $\mathcal{M}_1$ ja $\mathcal{M}_2$ arvutavad vastavalt ühe muutuja funktsioone f ja g. Kas nende masinate kompositsioon $\mathcal{M}_2 \circ \mathcal{M}_1$ arvutab funktsioonide kompositsiooni $g \circ f$?

Olgu kompositsioonmasina töö alguses lindil

$$0\underbrace{11\ldots1}_{x \text{ ühte}},$$

kusjuures pea on nulli kohal. Kui masin $\mathcal{M}_1$ peatub, siis jääb lindile

$$0\underbrace{11\ldots1}_{x \text{ ühte}}0\underbrace{11\ldots1}_{f(x) \text{ ühte}}$$

ja pea on vastuse nulli kohal. Selles konfiguratsioonis rakendame masinat $\mathcal{M}_2$. Eeldades, et selle masina pea ei liigu arvutuste käigus argumendi nullist vasakule, jääb pärast masina töö lõppu lindile seis

$$0\underbrace{11\ldots1}_{x \text{ ühte}}0\underbrace{11\ldots1}_{f(x) \text{ ühte}}0\underbrace{11\ldots1}_{g(f(x)) \text{ ühte}},$$

kus pea on viimase nulli kohal. Liitfunktsiooni puhul peavad töö lõppedes aga lindile jääma ainult argument x ja väärtus $g(f(x))$.

Seetõttu tuleb tekkinud seisus rakendada veel ühte masinat $\mathcal{E}$, mis eemaldab vahetulemuse ja nihutab vastuse vasakule. Liitfunktsiooni arvutab seega kolme masina $\mathcal{M}_1$, $\mathcal{M}_2$ ja $\mathcal{E}$ kompositsioon. Masina $\mathcal{E}$ tabelit koostada pole raske.

Teiseks vaatleme, kuidas Turingi masinate puhul realiseerida algoritmi täitmiskäigu hargnemist. Selle olukorra formaliseerimiseks valime järgmise tee. Eeldame, et masinal $\mathcal{M}_0$ on kaks passiivset seisundit q_0^1 ja q_0^2. Kui masin $\mathcal{M}_0$ lõpetab töö passiivses seisundis q_0^1, siis rakendame tekkinud konfiguratsioonile masinat $\mathcal{M}_1$; kui aga masina $\mathcal{M}_0$ töö lõpeb seisundis q_0^2, siis rakendame masinat $\mathcal{M}_2$. Masinad $\mathcal{M}_1$ ja $\mathcal{M}_2$ kujutavad seega algoritmi täitmise alternatiivseid harusid.

Definitsioon 4. *Olgu Turingi masinal $\mathcal{M}_0$ kaks passiivset seisundit q_0^1 ja q_0^2. Masinat $\mathcal{M}$ nimetatakse masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ hargnemiseks masina $\mathcal{M}_0$ järgi, kui iga algkonfiguratsiooni X korral*

$$\mathcal{M}(X) = \begin{cases} \mathcal{M}_1(\mathcal{M}_0(X)), & \text{\textit{kui masin} } \mathcal{M}_0 \text{ \textit{lõpetab konfiguratsiooni} } X \\ & \text{\textit{korral töö seisundis} } q_0^1, \\ \mathcal{M}_2(\mathcal{M}_0(X)), & \text{\textit{kui masin} } \mathcal{M}_0 \text{ \textit{lõpetab konfiguratsiooni} } X \\ & \text{\textit{korral töö seisundis} } q_0^2, \\ \mathcal{M}_0(X), & \text{\textit{muudel juhtudel.}} \end{cases}$$

Mõnikord nõutakse ühtsuse mõttes veel, et $\mathcal{M}_0$ lõpetab alati töö emmas-kummas passiivses seisundis, st ei tööta lõpmatult ega satu tühja lahtrisse. Samuti eeldatakse sageli, et tingimus kontrollimine ei muuda konfiguratsiooni, st alati $\mathcal{M}_0(X) = X$.

Esitatud definitsioonis annab masin $\mathcal{M}_0$ vastuse tingimuse kehtivuse või mittekehtivuse kohta seisundi kujul. Teine tee hargnemist korraldada oleks leppida kokku, et masin $\mathcal{M}_0$ kirjutab midagi lindile. See aga tooks kaasa vajaduse seada kitsendusi lindi sisule ning oleks lõppkokkuvõttes keerulisem.

Analoogiliselt kompositsiooniga saab ka hargnemise puhul koostada komponentmasinate tabelite järgi sellise masina tabeli, mis vastab antud masinate hargnemisele.

Teoreem 2. *Kui $\mathcal{M}_0$, $\mathcal{M}_1$ ja $\mathcal{M}_2$ on samas tähestikus töötavad Turingi masinad, kusjuures masinal $\mathcal{M}_0$ on kaks passiivset seisundit q_0^1 ja q_0^2, siis saab nende masinate tabelite järgi alati koostada sellise masina tabeli, mis on masinate $\mathcal{M}_1$ ja $\mathcal{M}_2$ hargnemine masina $\mathcal{M}_0$ järgi.*

Tõestus. Kirjutame masinate $\mathcal{M}_0$, $\mathcal{M}_1$ ja $\mathcal{M}_2$ tabelid järjest. Asendame kõik seisundid q_0^1 masina $\mathcal{M}_1$ esimese seisundiga ning seisundid q_0^2 masina $\mathcal{M}_2$ esimese seisundiga. □

§ 3. Mittearvutatavad funktsioonid

Järgnevalt võtame endale eesmärgiks näidata, et mitmed programmeerimises huvipakkuvad ülesanded ei ole Turingi masinaga lahendatavad. Churchi teesi põhjal ei saa siis neid ülesandeid (üldkujuliselt) lahendada mitte ühegi algoritmiga.

Alustame sellest, et seame igale Turingi masinale vastavusse teatava unikaalse arvu, mida nimetatakse masina *Gödeli numbriks*. Vaatleme Turingi masinaid, mille lindil võivad olla sümbolid s_0, s_1, ..., s_m. Esmalt nummerdame kõik Turingi masina käsud: käsu

$$s_a q_b \to s_c q_d K$$

Gödeli numbriks loeme arvu

$$g(s_a q_b \to s_c q_d K) = 2^a 3^b 5^c 7^d 11^k,$$

kus k on 1, 2 või 3 vastavalt sellele, kas K on L, R või C.

Näide 5. Arvutada käsu $\mathtt{1}q_1 \to \mathtt{0}q_3L$ Gödeli number.

Et $s_1 = \mathtt{0}$ ja $s_2 = \mathtt{1}$, siis saame valemist

$$g(\mathtt{1}q_1 \to \mathtt{0}q_3L) = 2^2 3^1 5^1 7^3 11^1 = 226380.$$

Gödeli numbri järgi saab käsu üheselt taastada. Tuleb vaid number algteguriteks lahutada ja kirjutada algarvude 2, 3, 5, 7 ja 11 astmete järgi vajalik käsk välja. Iga naturaalarvu esitus algtegurite korrutisena on üheselt määratud. Leidub ka arve, mis pole ühegi käsu Gödeli numbriks, näiteks 13. Selleks, et arv oleks mingi käsu Gödeli number, peavad 2 ja 5 astmed asuma 0 ja m vahel, 3 aste peab olema vähemalt 1, sest käsu vasakul poolel on aktiivne seisund, ning 11 aste kas 1, 2 või 3. Kõik sammud numbri järgi käsu taastamisel on tehtavad algoritmiliselt, teiste sõnadega, leidub algoritm, mis kontrollib, kas antud naturaalarv on mingi käsu Gödeli number, ja kui on, siis leiab selle käsu.

Kui on määratud käskude numbrid, siis saab defineerida Turingi masina numbri. Eeldame, et Turingi masin $\mathcal{M}$ koosneb käskudest C_1, C_2, ..., C_t. Ühesuse saavutamiseks lepime kokku, et käsud on järjestatud asukoha järgi masina tabelis: igas reas vasakult paremale ja read ise ülevalt alla. Masina $\mathcal{M}$ Gödeli numbriks loeme arvu

$$G(\mathcal{M}) = 2^{g(C_1)} 3^{g(C_2)} \dots p_t^{g(C_t)},$$

kus p_t on t-s algarv (astendatavad on siin niisiis t esimest algarvu).

Masina numbri järgi saab üheselt taastada masina kõigi käskude numbrid ning viimaste abil omakorda kõik masina käsud. Seega kui on antud Turingi masina number, siis saab selle järgi välja kirjutada masina tabeli. Leidub arve, mis pole ühegi masina numbriks. Samuti nagu käskude puhul, võib ka siin leida tingimused, mida arv rahuldama peab, et ta oleks mingi Turingi masina Gödeli number, ning samuti leidub algoritm, mis kontrollib, kas naturaalarv on mingi Turingi masina number ning jaataval juhul leiab selle masina käsud.

Teoreetiliste küsimustega tegeledes on otstarbekam selline numeratsioon, milles ei esine tühimikke. Seetõttu defineerime Gödeli numbrite alusel uue, tihendatud numeratsiooni, kus iga arv on mingi Turingi masina number. Olgu nimelt $\mathcal{T}_0$ vähima Gödeli numbriga Turingi masin ning iga $i = 0, 1, \ldots$ korral $\mathcal{T}_{i+1}$ vähima Gödeli numbriga Turingi masin, mis ei kuulu hulka $\{\mathcal{T}_0, \ldots, \mathcal{T}_i\}$.

Teisendused Gödeli numbrist uueks numbriks ja vastupidi on samuti algoritmiliselt teostatavad. Kui on antud Gödeli number, siis võime üle kontrollida kõik sellest väiksemad arvud ja teha kindlaks, kui mitu neist osutub mingi Turingi masina numbriks. Ümberpöördult, kui on antud masina järjekorranumber i, siis võime üksteise järel naturaalarve läbi vaadates välja selgitada suuruselt i-nda Gödeli numbri. Kokkuvõttes, masina tabeli põhjal on võimalik välja arvutada tema järjekorranumber tihendatud numeratsioonis, järjekorranumbri põhjal aga leida vastava masina tabel, st ka kõiki üleminekuid Turingi masina tabeli ja masina järjekorranumbri vahel saab teha algoritmiliselt.

Üldiselt huvitab meid niisuguse algoritmi olemasolu, mis kontrollib Turingi masina $\mathcal{M}$ tabeli järgi, kas masinal $\mathcal{M}$ on teatav omadus R või mitte. Uuritavad omadused võivad olla mitmesugused, näiteks

1) masinal $\mathcal{M}$ on ainult kaks seisundit;
2) masina $\mathcal{M}$ tabelis ei ole tühje ruute;
3) masin $\mathcal{M}$ töötab iga algkonfiguratsiooni puhul ülimalt kaks takti;
4) masin $\mathcal{M}$ lõpetab töö iga algkonfiguratsiooni korral;
5) masin $\mathcal{M}$ arvutab mingit kõikjal määratud funktsiooni;
6) masin $\mathcal{M}$ arvutab funktsiooni $f(x) = 2x$.

Omadusi, mis on defineeritud otseselt masina tabeli terminites (nagu ülaltoodud omadustest kaks esimest), on lihtne kontrollida. Küsimus on huvitavam, kui vaatleme omadusi, mis puudutavad Turingi masina arvutusprotsessi või masina poolt arvutatavat funktsiooni (ülejäänud näidetes).

Et üleminekud masina tabelilt masina järjekorranumbrile ning vastupidi on algoritmilised, siis on teatava omaduse R äratundmine tabeli järgi samaväärne omaduse R äratundmisega masina numbri järgi. Seetõttu eeldame, et Turingi masinad on nummerdatud eelnevas näidatud viisil $\mathcal{T}_0, \mathcal{T}_1, \ldots$, ning otsime algoritmi, mis kontrolliks naturaalarvu x järgi, kas masinal $\mathcal{T}_x$ on omadus R või mitte. Algoritm tähendab meie formalisatsioonis Turingi masinat, seega otsime ka omadust tuvastavat algoritmi Turingi masina kujul.

Definitsioon 5. *Ütleme, et Turingi masin $\mathcal{M}$ lahendab omadust R, kui tema poolt arvutatav ühe muutuja funktsioon on*

$$f_{\mathcal{M}}(x) = \begin{cases} 1, & \textit{kui masinal } \mathcal{T}_x \textit{ on omadus } R, \\ 0, & \textit{kui masinal } \mathcal{T}_x \textit{ ei ole omadust } R. \end{cases}$$

Vaatleme nüüd olukorda, kus uuritava omaduse rollis on eneselerakendatavus. Turingi masinat $\mathcal{T}_x$ nimetatakse *eneselerakendatavaks*, kui ta peatub sisendargumendil x. Teiste sõnadega, kui masin $\mathcal{T}_x$ lõpetab töö (ükskõik, kas standardses lõppseisus või mitte) omaenda numbril lõpliku arvu sammude järel, siis on ta eneselerakendatav; kui aga arvutus kestab lõpmatult, siis pole.

Teoreem 3. *Ei leidu Turingi masinat, mis lahendaks eneselerakendatavuse omadust.*

Tõestus. Oletame väitevastaselt, et leidub masin $\mathcal{M}$, mille korral

$$f_{\mathcal{M}}(x) = \begin{cases} 1, & \text{kui masin } \mathcal{T}_x \text{ on eneselerakendatav}, \\ 0, & \text{kui masin } \mathcal{T}_x \text{ ei ole eneselerakendatav}. \end{cases}$$

Siis võime konstrueerida sellise masina $\mathcal{N}$, mis argumendil x ei peatu, kui $f_{\mathcal{M}}(x) = 1$, ja peatub, kui $f_{\mathcal{M}}(x) = 0$. Masinaks $\mathcal{N}$ sobib kompositsioon $\mathcal{E} \circ \mathcal{M}$, kus masina $\mathcal{E}$ tabel on

	-	0	1
q_1	$\texttt{-}q_0L$	$\texttt{0}q_1R$	$\texttt{1}q_1C$

Kui masin $\mathcal{M}$ annab argumendil x vastuseks $\texttt{1}$, st pärast tema töö lõppu jääb lindile $x\texttt{01}$, siis käivitatakse lõpmatu tsükkel $\texttt{1}q_1 \to \texttt{1}q_1C$. Kui aga masin $\mathcal{M}$ annab vastuseks $\texttt{0}$, st lindile jääb $x\texttt{0}$, siis lõpeb töö kahe takti pärast lindi sisu muutmata.

Uurime, kas masin $\mathcal{N}$ on eneselerakendatav. Olgu n selle masina number, st $\mathcal{N} = \mathcal{T}_n$. Oletame, et $\mathcal{N}$ on eneselerakendatav. Siis $f_{\mathcal{M}}(n) = 1$, millest saame, et masin $\mathcal{N}$ ei peatu argumendil n ja järelikult pole eneselerakendatav. Jõudsime vastuolule. Oletame nüüd, et $\mathcal{N}$ ei ole eneselerakendatav. Siis $f_{\mathcal{M}}(n) = 0$, millest saame, et $\mathcal{N}$ peatub argumendil n ehk on eneselerakendatav. Jällegi saime vastuolu. Seega peame tegema järelduse, et masinat $\mathcal{M}$, mis kontrollib eneselerakendatavuse omadust, ei saa olemas olla. $\square$

Tõestatud teoreemil iseenesest kuigi suurt praktilist väärtust ei ole, ta lihtsalt kujutab esimest näidet ühest mittearvutatavast funktsioonist. Küll aga saab tema abil tõestada *peatumise probleemi* mittelahenduvuse. Peatumise probleem formuleeritakse järgmiselt.

Antud: naturaalarvud x ja y.

Küsimus: kas Turingi masin $\mathcal{T}_x$ peatub argumendil y?

Sellist laadi küsimustega tuleb praktilises programmeerimises tihti tegeleda, näiteks siis, kui soovime teada saada, kas programm jääb käivitamisel tsüklisse või mitte.

Teoreem 4. *Ei leidu Turingi masinat, mis kontrolliks argumentide x ja y järgi, kas masin $\mathcal{T}_x$ lõpetab argumendil y töö lõpliku arvu sammudega.*

Tõestus. Oletame väitevastaselt, et leidub masin $\mathcal{M}$, mille korral

$$f_{\mathcal{M}}(x, y) = \begin{cases} 1, & \text{kui masin } \mathcal{T}_x \text{ peatub argumendil } y, \\ 0, & \text{kui masin } \mathcal{T}_x \text{ ei peatu argumendil } y. \end{cases}$$

Siis võime konstrueerida masina $\mathcal{N}$, et

$$f_{\mathcal{N}}(x) = \begin{cases} 1, & \text{kui masin } \mathcal{T}_x \text{ on eneselerakendatav,} \\ 0, & \text{kui masin } \mathcal{T}_x \text{ ei ole eneselerakendatav.} \end{cases}$$

Masinaks $\mathcal{N}$ sobib kompositsioon järgmisest kolmest masinast.

1) Masin, mis arvutab funktsiooni $f(x) = x$. Selle masina tabel on toodud näites 2.
2) Masin $\mathcal{M}$.
3) Masin, mis eemaldab vahepealt teise argumendi ja kirjutab vastuse (0 või 1) esimese argumendi järele. Selle masina tabel on

	-	0	1	
q_1	-q_4L	1q_1R	-q_2L	kas paremal on 0 või 1
q_2		0q_3R	-q_2L	1 puhul kustutada ühed
q_3	1q_0L			ja kirjutada vastuse 1
q_4		0q_0C	-q_4L	0 puhul kustutada ühed

Olgu alguses lindil arv x. Kõigepealt see dubleeritakse, nii et lindile jääb xx, kusjuures pea asub teise nulli kohal. Seejärel rakendatakse masinat $\mathcal{M}$, mis jätab lindile xx01, kui $\mathcal{T}_x$ peatub argumendil x, ja xx0, kui $\mathcal{T}_x$ ei peatu argumendil x. Lõpuks kustutatakse x üleliigne eksemplar ja lindile jääb vastavalt kas x01 või x0.

Nüüd aga saame vastuolu teoreemiga 3, mis väidab, et masinat $\mathcal{N}$ ei ole olemas. Järelikult ei saa olemas olla ka masinat $\mathcal{M}$. □

Lisaks kahele viimasele teoreemile on võimalik tõestada teisigi analoogilisi tulemusi teatud omadusi kontrollivate Turingi masinate mitteleidumise kohta. Põhilise informatsiooni annab ja teatavas mõttes keskset kohal seisab nende hulgas 1953. aastast pärinev *Rice'i teoreem*, mille esitame tõestuseta.

Teoreem 5. *Olgu A kõigi Turingi mõttes arvutatavate funktsioonide hulga mittetühi pärisalamhulk. Ei leidu Turingi masinat, mis kontrolliks argumendi x järgi, kas Turingi masina $\mathcal{T}_x$ poolt arvutatav funktsioon kuulub hulka A.*

Funktsioonide hulgad, millesse kuulumist saab Turingi masina numbri järgi kontrollida, võivad olla ainult kas tühi hulk või üldse kõigi arvutatavate funktsioonide hulk. Seega järeldub Rice'i teoreemist, et algoritmiliselt (Turingi masinaga) ei saa kindlaks teha ühtegi Turingi masinate omadust, mis on väljendatud masinate poolt arvutatavate funktsioonide kaudu, välja arvatud kaks triviaalset omadust, millest üks kehtib kõigi funktsioonide, teine aga mitte ühegi funktsiooni kohta. Näiteks ei leidu Turingi masinat, mis kontrolliks argumendi x väärtuse järgi, kas masin $\mathcal{T}_x$ arvutab funktsiooni $f(x) = 2x$: selleks piisab hulgaks A valida hulk, mis ainsa elemendina sisaldab nimetatud funktsiooni. Ühe ja sama funktsiooni arvutamiseks võib leida palju erinevaid masinaid ning väita, et konkreetne masin arvutab antud funktsiooni, saab alles siis, kui oleme võrrelnud masina töö tulemust ja funktsiooni väärtust kõigil argumentidel.

Kõiki vaadeldud negatiivseid tulemusi on võimalik üle kanda Turingi masinatelt suvalisele programmeerimiskeelele. Sel juhul tähendavad nad, et arvuti (programmi) abil ei saa kontrollida ühtegi programmide omadust, mis programmeerijale tegelikult huvi pakub, näiteks kas programm arvutab seda funktsiooni, mille jaoks ta on kirjutatud, või kas ta lõpetab töö igasuguse sisendi korral. Niisugusel interpretatsioonil on olemas pessimistlik ja optimistlik aspekt. Pessimistlikust vaatepunktist on arvuti väga piiratud võimalustega. Ta mitte ainult ei suuda teha midagi, mida talle täpselt ette kirjutatud pole, vaid paljude oluliste ülesannete lahenduskäiku pole üldse võimalikki ette kirjutada. Optimistlikust seisukohast võib neid tulemusi aga interpreteerida nii, et programmeerimises leidub ülesandeid, mida ei saa lahendada puhtmehaaniliselt, arvuti abil, vaid mis sisaldavad arvuti jaoks kättesaamatuid loomingulisi momente. Selliste ülesannete lahendamine nõuab järelikult intuitsiooni ja loovust, mida käesoleva hetkeni suudab ilmutada ainult inimene.

§ 4. Ülesanded

1. Koostada Turingi masinad, mis arvutavad järgmisi funktsioone.

a) $f(x) = 2x$

b) $f(x) = \left[\dfrac{x}{3}\right]$

c) $f(x) = x \bmod 3$

d) $f(x) = 2x + \left[\dfrac{x}{3}\right] + 1$

e) $f(x, y) = \left[\dfrac{x}{y}\right]$

f) $f(x, y) = x \bmod y$

g) $f(x, y) = 2x \dot{-} 3y$

h) $f(x, y, z) = 3y \dot{-} 2x + 4z$

i) $f(x, y) = |x - y|$

j) $f(x, y) = |x - 4y|$

k) $f(x, y) = \min(x, y)$

l) $f(x, y) = \max(x, y)$

m) $f(x) = x^2$

n) $f(x) = x^3$

o) $f(x) = 2^x$

p) $f(x, y) = x^y$

q) $f(x) = x!$

r) $f(x) = [\sqrt{x}]$

s) $f(x, y) = \text{SÜT}(x, y)$

t) $f(x, y) = \text{VÜK}(x, y)$

u) $f(x) = \begin{cases} 1, & \text{kui } x \text{ on algarv} \\ 0, & \text{kui } x \text{ ei ole algarv} \end{cases}$

2. Kirjeldada võimalikult detailselt, mida peab Turingi masin, et arvutada järgmiste funktsioonide väärtusi, kus a, b, c on teatavad naturaalarvulised konstandid.

a) $f(x) = |ax - by| + cz$

b) $f(x) = |ax - by| \dot{-} cz$

c) $f(x) = ax \dot{-} cz + by$

d) $f(x) = ax + cz \dot{-} by$

3. Arvestades, et lint on mõlemast suunast lõpmatu, koostada selline Turingi masin $\mathcal{M}$, et iga $n \geqslant 1$ korral oleks

a) $f^n_{\mathcal{M}}(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n$

b) $f^n_{\mathcal{M}}(x_1, x_2, \ldots, x_n) = x_1 + 2x_2 + \ldots + nx_n$

c) $f^n_{\mathcal{M}}(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$

4. Koostada Turingi masin $\mathcal{E}$, mis etteantud argumentide (x, y) korral kustutab esimese argumendi ja nihutab teise argumendi vasakule esimese asemele (vt lk 121).

5. Konstrueerida funktsioone $f(x) = 0$ ja $f(x) = 2x$ arvutavate Turingi masinate tabelite järgi sellise Turingi masina tabel, mis arvutab funktsiooni $f(x) = x + (-1)^x x$. Selleks organiseerida nende masinate hargnemine, koostades lisaks sobiva kolmanda masina tabeli.

6. Koostada ülimalt 5-seisundiline Turingi masin, mis argumendi 0 puhul kirjutab lindile nii suure väljundi kui võimalik ja peatub standardses lõppseisus.

7. Koostada Turingi masinad, mis arvutavad järgmisi funktsioone. Masina tähestik koosneb sümbolitest s_0 = -, s_1 = ,, s_2 = 0, s_3 = 1, arve esitatakse lindil kahendsüsteemis. Iga arv algab sümboliga , ning sellele järgneb teatud hulk sümboleid 0 ja 1, mis moodustavad arvu kahendkuju. Lindi ülejäänud lahtrid on täidetud tühikutega.

a) $f(x) = 0$

b) $f(x) = 20$

c) $f(x) = x$

d) $f(x) = x + 1$

e) $f(x) = x + 2$

f) $f(x) = x + 3$

g) $f(x) = x + 20$

h) $f(x) = x \dot{-} 1$

i) $f(x) = x \dot{-} 2$

j) $f(x) =$ arvu x pikkus

k) $$f(x, y) = \begin{cases} 1, & \text{kui } x = y \\ 0 & \text{vastasel korral} \end{cases}$$

l) $$f(x, y) = \begin{cases} 1, & \text{kui } x < y \\ 0, & \text{vastasel korral} \end{cases}$$

m) $f(x, y) = \max(x, y)$

n) $f(x, y) = \min(x, y)$

o) $f(x) = x \bmod 3$

p) $f(x, y) = x + y$

q) $f(x, y) = x \dot{-} y$

r) $f(x) = 2x$

s) $f(x) = 3x$

t) $f(x, y) = xy$

u) $f(x) = \left[\dfrac{x}{y}\right]$

8. Koostada ülesandes 7 kirjeldatud tähestikus töötav Turingi masin, mis teisendab etteantava arvu

a) tavakujult kahendsüsteemi;

b) kahendsüsteemist tavakujule.

9. Kas leidub Turingi masin, mis alustab tööd standardses algseisus, töötab iga argumendi $x \geqslant 1$ korral täpselt $3x + 1$ takti ja peatub standardses lõppseisus? Kui jah, siis esitada selle masina tabel, vastasel korral tõestada, et sellist masinat pole.

10. Kas leidub Turingi masin, mis alustab iga argumendi x korral tööd standardses algseisus ja peatub $3x + 2$ takti järel täpselt samas seisus, kus alustas?

11. Kas leidub Turingi masin, mis arvutab funktsiooni $f(x) = 0$ ja töötab iga x korral paarisarvu takte?

12. Turingi masin $\mathcal{M}$ alustab tööd standardsest algseisust ja peatub fikseeritud argumendi n korral $3(n+3)$ takti järel standardses lõppseisus. Kui suur võib maksimaalselt olla masina $\mathcal{M}$ poolt arvutatud funktsiooni väärtus $f_{\mathcal{M}}(n)$?

13. Tõestada, et ei leidu Turingi masinat $\mathcal{M}$, mis argumendi x puhul tagastab väärtuse 1, kui Turingi masin $\mathcal{T}_x$ *ei ole* eneselerakendatav, ning väärtuse 0, kui Turingi masin $\mathcal{T}_x$ on eneselerakendatav (st masin $\mathcal{M}$ kontrollib mitte-eneselerakendatavuse omadust).

14. Tõestada, et ei leidu Turingi masinat $\mathcal{M}$, mis argumendi x puhul peatub (ükskõik millises lõppseisus), kui masin $\mathcal{T}_x$ ei ole eneselerakendatav, ning ei peatu, kui masin $\mathcal{T}_x$ on eneselerakendatav.

15. Kirjeldada tõestuse ideed, kuidas peatumise probleemile taandamise teel saab näidata, et ei leidu Turingi masinat, mis naturaalarvude x ja y järgi teeks kindlaks, kas Turingi masinate $\mathcal{T}_x$ ja $\mathcal{T}_y$ poolt arvutatavad funktsioonid $f^1_{\mathcal{T}_x}$ ja $f^1_{\mathcal{T}_y}$ langevad kokku.

16. Turingi masina omadust võime identifitseerida naturaalarvude hulga alamhulgaga, mis sisaldab arvu x parajasti siis, kui masinal $\mathcal{T}_x$ on vaadeldav omadus. Tõestada, et kui leiduvad Turingi masinad, mis lahendavad omadusi R ja S, siis leidub Turingi masin, mis lahendab omadust: a) R'; b) $R \cup S$; c) $R \cap S$; d) $R \setminus S$.

AINEREGISTER

ühilduvad liikmed, 31
üldisuskvantor, 46

aksiomaatiline teooria, 84
aksiomaatilise teooria üldskeem, 84
aksiomaatilise teooria korrektsus, 86
aksiomaatilise teooria mittevasturääkivus, 92
aksiomaatilise teooria täielikkus, 86
aksiomaatilise teooria vasturääkivus, 92
aksioom, 83, 84
aktiivne seisund, 113
alamvalem, 9, 50
algebraterm, 49
algoritm, 112
algoritm valemi viimiseks prefikskujule, 72
algoritm valemi viimiseks TDNK-le, 28
antetsedent, 89
aritmeetika mittetäielikkuse teoreem, 106
arvu esitus lindil, 114
arvutatav funktsioon, 115
assotsiatiivsuse seadused, 22
atomaarne valem, 50
avatud haru, 16

Churchi tees, 119
Churchi teoreem predikaatarvutuse mittelahenduvusest, 60

Craigi teoreem, 39

De Morgani seadused, 22
disjunkt, 28
disjunktiivne normaalkuju, 28
disjunktsioon, 8, 11
distributiivsuse seadused, 22
DNK, 28
duaalsusprintsiip, 41, 82

eitus, 8, 11
eksistentsikvantor, 47
ekvivalents, 8, 11
elementaardisjunktsioon, 28
elementaarkonjunktsioon, 28
elementaarvalem, 50
eneselerakendatav Turingi masin, 124
eriaksioomid, 102
esimest järku aksiomaatiline teooria, 102
esimest järku predikaatarvutus, 58
esimest järku teooria korrektsuse teoreem, 104
esimest järku teooria mittevasturääkivuse teoreem, 105
esimest järku teooria täielikkuse teoreem, 105

formaalne aksiomaatiline teooria, 84
formaalne aritmeetika, 104
formaalne tõestus, 85
funktsionaalsümbol, 48

Gödeli number, 122
Gödeli teoreem aritmeetika mittetäielikkusest, 106
Gödeli teoreem predikaatarvutuse täielikkusest, 100
Gentzeni-tüüpi süsteem, 88

hargnemine, 121
Hilberti kümnes probleem, 112
Hilberti-tüüpi süsteem, 88

idempotentsuse seadused, 22
implikatsioon, 8, 11
indiviid, 44
indiviidide piirkond, 45
indiviidmuutuja, 48
indiviidmuutuja seotud esinemine, 50
indiviidmuutuja vaba esinemine, 50
induktiivne definitsioon, 9
interpretatsioon, 53
interpretatsiooni kandja, 53
interpreteeriv kujutus, 53

järeldumine, 18, 64

käsu Gödeli number, 122
kahekordse eituse seadus, 22
kahendsüsteemis arv, 128
Karnaugh' diagramm, 32
katmine, 31
kehtestatav valem, 14, 60
kinnine valem, 50
KNK, 28
kommutatiivsuse seadused, 22
kompositsioon, 119
konfiguratsioon, 114
konjunkt, 28
konjunktiivne normaalkuju, 28
konjunktsioon, 8, 11
konstantsümbol, 48
kontingentne valem, 15
kontradiktsioon, 12, 59
korrektne aksiomaatiline teooria, 86
korrektsuse teoreem, 91, 99, 104
kummutatav valem, 15
kvantifitseerimine, 47
kvantor, 46
kvantori ja eituse vahetamisseadus, 65
kvantori mõjupiirkond, 50
kvantorite distributiivsus, 65
kvantorite kommutatiivsus, 65

lõigatud vahe, 117
lõpetatud haru, 16
lahendatav omadus, 124
lause, 7
lausearvutuse aksiomaatika, 88
lausearvutuse korrektsuse teoreem, 91
lausearvutuse mittevasturääkivuse teoreem, 93
lausearvutuse põhisamaväärsused, 22
lausearvutuse süntaks, 9
lausearvutuse semantika, 10
lausearvutuse täielikkuse teoreem, 96
lausearvutuse tehe, 8
lausearvutuse tuletusreeglid, 88
lausearvutuse valem, 9
lausemuutuja, 8
lihtimplikant, 35
liikmete elimineerimise reeglid, 22
literaal, 24
loogiliselt tõene valem, 12, 59
loogiliselt väär valem, 12, 59

määramata tõeväärtus, 34
maatriks, 70
MDNK, 31
minimaalne disjunktiivne normaalkuju, 31

mittevasturääkiv aksiomaatiline teooria, 92
mittevasturääkivuse seadus, 7, 12
mittevasturääkivuse teoreem, 93, 100, 105
mudel, 57, 104
muutujateta term, 49

naturaalarvu esitus lindil, 114
neelamisseadused, 22
negatiivne literaal, 24
normaalkuju liikmed, 24

olemasolukvantor, 47
omaaksioomid, 102
osavalem, 9, 50

põhihulk, 53
põhitehete tõeväärtustabelid, 11
passiivne seisund, 113, 121
Peano aritmeetika, 104
peatehe, 9, 50
peatumise probleem, 125
poola kuju, 38
positiivne literaal, 24
predikaadi väljendamine, 57
predikaat, 44, 45
predikaatarvutuse aksiomaatika, 97
predikaatarvutuse korrektsuse teoreem, 99
predikaatarvutuse mittelahenduvuse teoreem, 60
predikaatarvutuse mittevasturääkivuse teoreem, 100
predikaatarvutuse põhisamaväärsused, 65
predikaatarvutuse süntaks, 48
predikaatarvutuse semantika, 52
predikaatarvutuse täielikkuse teoreem, 100
predikaatarvutuse tuletusreeglid, 97
predikaatarvutuse valem, 50
predikaatsümbol, 50
prefikskuju, 70
puhas predikaatarvutus, 101

Quine-McCluskey meetod, 34

rühmateooria, 102
Rice'i teoreem, 126

süntaks, 9, 48, 86
samaliigiliste kvantorite kommutatiivsus, 65
samaselt tõene valem, 12, 59
samaselt väär valem, 12, 59
samaväärsed valemid, 21, 64
seisund, 113
sekvents, 88, 97, 101
sekventsi eesliige, 89
sekventsi tagaliige, 89
sekventsi valemkuju, 91
sekventsiaalne lausearvutus, 88
sekventsiaalne predikaatarvutus, 97
semantika, 10, 52, 86
seotud muutuja, 50
seotud muutujate ümbernimetamine, 65
signatuur, 52
situatsioon, 114
struktuursed reeglid, 88
suktsedent, 89
suletud haru, 16
sulureeglid, 9, 50

täielik aksiomaatiline teooria, 86
täielik disjunktiivne normaalkuju, 24
täielik elementaardisjunktsioon, 24
täielik elementaarkonjunktsioon, 24
täielik konjunktiivne normaalkuju, 25
täielikkuse teoreem, 96, 100, 105

tühik, 112
tõene, 7, 10
tõene mudelis, 57
tõestusvõtted, 67
tõesuspuu, 15
tõesuspuu reeglid, 16, 61
tõeväärtus, 7
tõeväärtuse arvutamine, 10, 55
tõeväärtustabel, 11
tautoloogia, 12, 59
TDNK, 24
tehete prioriteet, 9, 50
tehted predikaatidega, 46
tehtemärgid, 8
teist järku predikaatarvutus, 58
term, 49
termi väärtus, 54
tihendatud numeratsioon, 123
tingimus * (kvantorreeglites), 97
tingimused lausete kohta, 7, 8
TKNK, 25
tuletatav valem, 85
tuletus, 85
tuletuspuu, 89
tuletusreegel, 84
Turingi mõttes arvutatav funktsioon, 115
Turingi masin, 112
Turingi masina Gödeli number, 122
Turingi masina käsk, 113
Turingi masina poolt arvutatav funktsioon, 115
Turingi masina programm, 113
Turingi masina seis, 113
Turingi masina tabel, 113
Turingi masinate hargnemine, 121
Turingi masinate kompositsioon, 119

universaalsuskvantor, 46

väär, 7, 10
väärtustus, 10
välistatud kolmanda seadus, 7, 12, 84
välistav „või“, 8
väljendamine, 57
võrdusega predikaatarvutus, 101
vaba muutuja, 50
valem, 9, 50
valem signatuuris, 52
valemi maatriks, 70
valemi prefikskuju, 70
valemi tõeväärtus, 10, 55
valemite hulga mudel, 57
vasakassotsiatiivsus, 9
vastuoluline haru, 16
vasturääkiv aksiomaatiline teooria, 92
vasturääkivad valemid, 14