Tallinna Tehnikaülikool
Eesti TA Küberneetika Instituut

Loogika arvutiteaduses

Jaan Penjam

Tallinn • Detsember 1995

Sisukord

1. Sissejuhatus formaalloogikasse

Loogika on teadus mõtlemise üldistest seadustest ja vormidest. Eelkõige tegeleb loogika "õige mõtlemisega", s.t. püüab leida vastust küsimusele, kuidas arutleda nii, et kehtivate algteadmiste põhjal saada ainult tõeseid järeldusi.

Mõtlemine on inimaju olulisim funktsioon, mida uurivad mitmed teadusharud, nagu näiteks meditsiin, psühholoogia jt., aga ka tehisintellekt. Viimane tegeleb mõtteprotsesside modelleerimisega arvutil. Tehisseadme "arutlemise" tulemuste võrdlemisel inimese poolt tehtavate järeldustega saadakse muu hulgas väärtuslikke andmeid inimmõistuse olemusest.

Loogika peamiseks uurimismeetodiks on vaatlus ja arutluskäikude (teksti) analüüs. Ajuprotsesside füsioloogiliste alustega ning ümbritseva keskkonna tunnetamise (teadmiste hankimise) probleemidega loogika ei tegele. Selle asemel püütakse üldistada nende arutluskäikude ja mõtlemisaktide seaduspärasusi, mida argielus oleme harjunud nimetama loogilisteks. Võrreldes psühholoogiaga on loogikal veel üks tähtis iseärasus: loogika tegeleb inimese mõttetegevuse nn. verbaalse osaga, s.t. vaadeldakse vaid teksti kujul esitatavaid teadmisi ja mõttekäike. Kõrvale jääb alateadvusega seotud mõttetegevuse komponent. Seega saab loogikat vaadelda ka kui teadust tekstide analüüsimise ja teisendamise meetoditest.

Juba pealiskaudsel analüüsimisel võib märgata, et ühe inimese jaoks loogiline arutluskäik pole seda sageli teise jaoks. Niisiis mingit ühtset, kõigile sobivat "õige" mõtlemise reeglistikku pole olemas. Enim üksmeelsed ollakse vahest teaduslike, eriti täppisteaduslike arutluste loogiliseks tunnistamisel. Paraku aga ilmneb, et isegi matemaatikas leidub tõestusi, mida osa teadlasi tunnustab, osa aga mitte.

Järgnevas tuleb meil teha tegemist mitmete loogika arutlussüsteemidega: klassikalise lause- ja predikaatarvutuse, modaal- ja intuitsionistliku loogika süsteemidega (mida eadspidi nimetame **arvutuseks**). Ühtlasi antakse ülevaade teaduses enamkasutatavatest loogilise arutluse meetoditest.

Loogika kui teadusharu ajalugu ulatub vanadesse Idamaadesse ja Vana-Kreekasse. Ajaliselt vanim kirjalikult formuleeritud loogilise tuletuse süsteem oli Aristotelese süllogistika. Aristotelesele kuuluvad ka enamikus loogikaarvutustes järgitavad "õige mõtlemise seadused" (nende seaduste kaasaegsed sõnastused on välja töötanud G.W. Leibniz, A.Schopenauer jt.):

- *samasuse seadus*: iga mõiste või lause peab jääma ühe arutluse raames iseendaga identseks;
- *vasturääkivuste lubamatuse seadus*: ühe ja sma objekti kohta ei tohi ühes ja samas suhtes midagi üheaegselt eitada ega jaatada;
- *välistatud kolmanda seadus*: kahest teineteisele vasturääkivast väitest on üks tõene ja teine väär, kolmandat võimalust ei ole;
- *küllaldase aluse seadus*: iga väidet on vaja põhjendada mingi teise väitega, mille tõesus on kontrollitud.

Loetletud neli mõtlemisseadust on tavamõistusele hästi vastuvõetavad ning nende järgimine kindlustab stabiilsetes olukordades ka tulemusliku arutlemise. Traditsioonilise loogika seadusi järgib enamik loogikaarvutusi, kuid mitte kõik. Neid reegleid ei saa vahetult rakendada näiteks arutlustes, kus väidetel ja otsustustel on enam kui kaks tõeväärtust, s.o. kus väite tõesuse aste võib olla antud teatud tõenäosusega. Mõned loogikasüsteemid ei tunnista aga üksikuid loetletud seadustest. Näiteks intuitsionistlik loogika ei tunnista sellist argimõistusele hästi vastuvõetavat reeglit nagu välistatud kolmanda seadus.

Erinevused loogikate vahel võivad olla tingitud ka Aristotelese "mõtlemisseaduste" erinevast tõlgendamisest. Näiteks võib siinkohal tuua küllaldase aluse seaduse erinevad käsitlused, võtted, mille abil väiteid üksteise abil põhjendada.

Kontrollitud väidete kasutamisel uute väidete põhjendamiseks tuntakse kolme meetodit: *deduktsiooni*, *induktsiooni* ja *abduktsiooni*. Deduktsiooni korral rakendatakse üldisi seaduspärasusi üksikjuhtudele ning tuletatakse teadaolevatest üldistest väidetest uusi üldisi väiteid. Induktsiooni korral toimitakse vastupidi: üksikobjektide kohta käivaid väiteid üldistatakse kõigile sama klassi objektidele. Abduktsiooni e. analoogia raames loetakse teatud üksikobjekti kohta käiv väide tõeseks mingi teise (mitte tingimata samasse klassi kuuluva) objekti kohta.

Formaalselt esitatakse põhjendusi (tuletuskäike) harilikele murdudele sarnaneva kirjapildi abil - "murrujoone" kohale kirjutatakse eeldused, "nimetajasse" aga tehtav järeldus.

Illustreerime deduktsiooni, induktsiooni ja abduktsiooni erinevusi klassikalise näite varal. Olgu antud kolm lauset:

A: Sokrates oli inimene.
B: Kõik inimesed on surelikud.
D: Sokrates oli surelik.

Deduktiivse järelduse korral on väide D põhjendatav väidete A ja I kehtivusega, s.o. Sokratese kui üksikindiviidi kohta tehakse järeldus üldisemate väidete põhjal.

Toodud arutluskäik formaliseeritud kujul on järgmine:

$$\frac{A \quad I}{D}.$$

Induktiivse järelduse näiteks on kõigi inimeste surelikkuse tuletamine tõsiasjust, et Sokrates oli inimene ja suri:

$$\frac{A \quad D}{I}.$$

Abduktsiooni korral tehakse aga järeldus, et Sokrates oli inimene, eeldusest, et ta oli surelik, ning üldisest teadmisest, et kõik inimesed on surelikud:

$$\frac{D \quad I}{A}.$$

Juba antud näidetest on selge, et ainult deduktiivne meetod võib anda järeldatavatele väidetele täielikke põhjendusi. See on ka põhjus, miks järgnevas on põhirõhk asetatud just deduktsiooniteooriale - deduktsioon on kõigi algandmete suhtes korrektsete programmide ja täielike tõestuste koostamisel ainus meetod. Samas ei tohi alahinnata induktsiooni ja abduktsiooni olukorras, kus puuduvad üldisemad teadmised või deduktiivse meetodi rakendamine on mõnel muul põhjusel võimatu. Abduktsiooni kasutatakse näiteks mudeli omaduste ülekandmisel uuritavale objektile. Teatud juhtudel - tuumareaktsioonide, lennukite aerodünaamiliste jt. omaduste selgitamisel - ongi modelleerimine peamine meetod.

Lisakitsenduste korral võivd ka induktsioon ja abduktsioon anda täielikke tulemusi. Näiteks matemaatiline induktsioon on täielik naturaalarvude omaduste tõestamisel.

Mistahes tulemusliku mõtlemisprotsessi raames jälgitakse teatud fikseeritud mõtlemisreegleid (loogika süsteemi). Järjekindla loogilise aruteluta on mõeldamatu matemaatiline tõestamine. Sama tuleb öelda ka arvutiprogrammi koostamise kohta. Seepärast võib väita, et loogika on nii matemaatika kui ka arvutiteaduse alus.

Käesolevas konspektis vaadeldakse mitmeid loogikaarvutusi ning nende seost matemaatika ja arvutitaduse teoreetiliste alustega. Täpsemalt - vaadeldakse matemaatilist loogikat, s.o. loogikat, mis esitab mõtlemisstruktuure matemaatiliste sümbolite keeles.

Võrreldes kogu loogika ajalooga on matemaatiliste meetodite kasutamine loogilise mõtlemise uurimises suhteliselt noor. Esimesed matemaatilise loogika arvutused koostati alles möödunud sajandi keskpaiku, peamiselt A. De Morgani ja G. Boole'i töödes.

Tänapäeval uuritakse loogilist mõtlemist valdavalt matemaatilise loogika meetoditega. Matemaatilise loogika formaliseeritud esitus võimaldab modelleerida arutluskäike (näiteks tõestada matemaatikateoreeme) arvutil.

Järgnevates peatükkides vaadeldakse klassikalist deduktsiooniteooriat e. tuletusõpetust. Pearõhk on asetatud tuletusmeetoditele, mis on efektiivselt realiseeritavad arvutil. Antakse ka põgus ülevaade mudelite teooriast (käsitletakse arutluses esinevate väidete, otsustuste jne. tõestuse küsimusi) ning mitteklassikalistest loogikatest ja nende seosest arvutiteaduse erinevate valdkondadega.

Kursuse eesmärk on selgitada:

- programmide koostamisel kasutatavate otsustuste olemust;
- orgaanilist seost programmide koostamise ja matemaatika teoreemide tõestamise vahel;
- algoritmide automaatse koostamise formaalset meetodit;
- piire, mil määral võib arvuti modelleerida inimese mõttetegevust.

Kursuse matemaatilist ja kompuuterloogikat käsitlev osa annab teoreetilise ja metodoloogilise baasi arvutiteaduse teoretiliste aluste edaspidiseks õppimiseks. Koostamisel on kasutatud G. Mintsi loengumaterjale Tartu ja Stanfordi ülikoolide jaoks. Ülesannete valikul on tuginetud mitmete tuntud loogikaõpikute materjalidele.

2. Lausearvutus

Lausearvutus on lihtsaim logikasüsteem, mis käsitleb väidete ja otsustuste vahelisi sõltuvusi lahus lausete grammatilisest ja semantilisest struktuurist. Seega vaadeldakse siin lauseid jagamatute tervikutena, eeldades, et nende tõesusele vastavuse määr (mis klassikalise lausearvutuse korral võib olla ainult kas *tõene* või *väär*) on põhimõtteliselt kindlaks tehtav. Piltlikult võib kujutleda, et lausearvutuses vaadeldavad elementaarlaused (aatomid) on jutustavad lihtlaused, mille jaoks saab (konteksti arvestades) otsustada, kas nad kehtivad või mitte.

Lausearvutuse aatomitena võib käsitleda näiteks lauseid *Päikese ümber tiirleb 9 planeeti, Lapsed mängivad õues palli* või $5 < 3$. Paneme seejuures tähele, et esimene väide on tõene (kui mitte lugeda asteroide planeetideks), teine väide võib olla tõene kui ka väär, kuid põhimõtteliselt võib alati kontrollida, kas see väide peab paika. Viimane väide on aga väär.

Lausearvutue aatomeid nimetatakse vahel ka propositsioonideks (lad. k. *propositio* - esitus, ettepanek). Seepärast nimetatakse käesolevas vaadeldavat arutlussüsteemi ka propositsionaalloogikaks. Vastav ingliskeelne termin on *propositional calculus*.

Termini "lausearvutus" teine pool - "arvutus" - rõhutab asjaolu, et tegemist on formaliseeritud süsteemiga. Sõna "arvutus" tähistabki matemaatikas formaalset süsteemi. Arvutus on määratud, kui on antud

1. tähestik;
2. lubatud väljendite e. valemite hulk (arvutuse keel);
3. aksioomid (*a priori* tõesed valemid);
4. tuletusreeglid uute valemite moodustamiseks aksioomide baasil.

Lausearvutuse tähestik sisaldab sümboleid atomaarsete lausete tähistamiseks ning loogikatehteid, mis väljendavad aatomitevahelisi seoseid.

Näide 1. Vaatleme järgmist arutelu.
"Ma maksaksin teleri parandamise eest (m), kui ta hakkaks tööle (t). Teler aga ei tööta. Seepärast ma ei kavatse maksta".

Sümbolid m ja t tähistavad lauseid :

m : "ma maksan teleri parandamise eest";
t : "teler töötab".

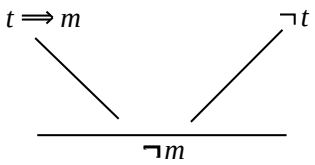
Eelnev arutelu on siis esitatav järgmiste avaldiste abil:

$t \Longrightarrow m$ (kui teler hakkab tööle, siis ma maksan ta parandamise eest;
sümbol $\Longrightarrow$ tähistab lausekonstruktsiooni "kui ..., siis ...";
$\neg\, t$ (teler ei tööta; sümbol $\neg$ tähistab eitust);
$\neg\, m$ (ma ei maksa teleri parandamise eest).

Kokkuvõttes on arutluskäigu formaliseering järgmine:

"Kuna $t \Longrightarrow m$ ja $\neg\, t$, siis $\neg\, m$".

Enamasti esitatakse see konstruktsioon järgmise puuna:



□

Toodud näide illustreerib traditsiooniliste arutluskäikude formaliseerimist; lausearvutus annab aga vahendid selliste formaliseeritud arutluskäikude analüüsimiseks. Arutluses kasutatavad järeldamismallid väljendavad arvutuse tuletusreeglid. Loogika eesmärk on leida sellised "universaalsed" tuletusreeglid, mis ei sõltu konkreetsetest lausetest.

Järgnevas on esitatud klassikalise lausearvutuse keel ja tuletusreeglid.

Tähestik:

- ladina väiketähed a, b, c, ...;
- märgid $\neg$ ja $\Longrightarrow$;
- ümarsulud (ja).

Valemid:

1. kõik ladina tähed on valemid;
2. kui A on valem, siis on valem ka (A);
3. kui A on valem, siis on valem ka $\neg A$;
4. kui A ja B on valemid, siis on ka valem $A \Longrightarrow B$;
5. rohkem valemeid ei ole.

Siin ja edaspidi on suured ladina tähed A, B, ... kasutusel kui metasümbolid, mille asemele võib panna mistahes valemi.

Aksioomideks on kõik valemid, mis vastavad järgmistele skeemidele:

$A1 : A \Longrightarrow (B \Longrightarrow A)$
$A2 : (A \Longrightarrow (B \Longrightarrow C)) \Longrightarrow ((A \Longrightarrow B) \Longrightarrow (A \Longrightarrow C))$
$A3 : (\neg\, B \Longrightarrow \neg\, A) \Longrightarrow ((\neg\, B \Longrightarrow A) \Longrightarrow B)$

Tuletusreegel: kui on tuletatavad valemid A ja $A \Longrightarrow B$, siis on tuletatav ka valem B. Formaalne tuletusreegli esitus

$$\frac{A \quad A \Longrightarrow B}{B}$$

Seda tuletusreeglit tähistatakse MP (lühend ladinakeelsetest sõnadest *moduns ponens*.

Sellele põhilisele tuletusreeglile lisanduvad reeglid syulgude sissetoomiseks ning kustutamiseks:

$$\frac{A}{(A)}$$

ja

$$\frac{(A)}{A}$$

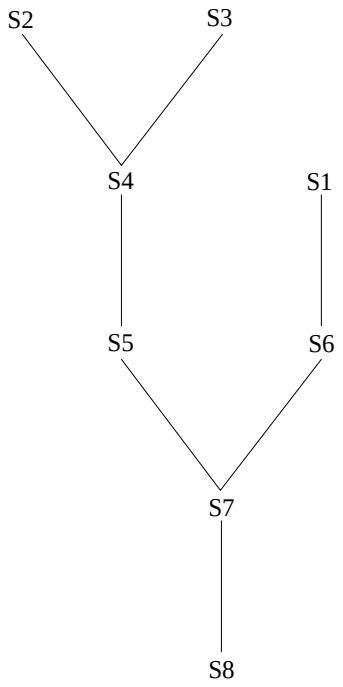
Tõestus on lõplik valemite jada $T_1, \ldots, T_n$, kus igs liige on kas aksioom või on saadud talle eelnevatest liikmetest tuletusreegli abil. Tuletuse viimast valemit nimetatakse **teoreemiks**. Vaadeldavas arvutuses on tõestuse leidmine võrdlemisi vaevaline, kasutada tuleb "kunstlikke võtteid".

Näide 2. Valemi $a \Longrightarrow a$ tuletus.

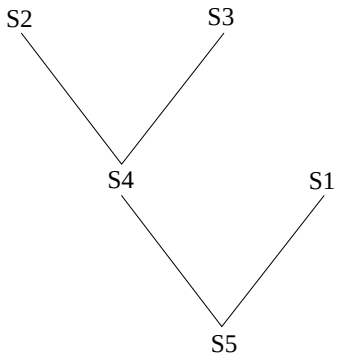
$S1.\ a \Longrightarrow (a \Longrightarrow a)$	$[A1 : \quad A \ldots a, B \ldots a]$
$S2.\ a \Longrightarrow ((a \Longrightarrow a) \Longrightarrow a)$	$[A1 : \quad A \ldots a, B \ldots (a \Longrightarrow a)]$
$S3.\ (a \Longrightarrow ((a \Longrightarrow a) \Longrightarrow a)) \Longrightarrow ((a \Longrightarrow (a \Longrightarrow a)) \Longrightarrow (a \Longrightarrow a))$	$[A2 : \quad A, C \ldots a, B \ldots (a \Longrightarrow a)]$
$S4.\ ((a \Longrightarrow (a \Longrightarrow a)) \Longrightarrow (a \Longrightarrow a))$	$[S2,\ S3]$
$S5.\ (a \Longrightarrow (a \Longrightarrow a)) \Longrightarrow (a \Longrightarrow a)$	$[S4]$
$S6.\ (a \Longrightarrow (a \Longrightarrow a))$	$[S1]$
$S7.\ (a \Longrightarrow a)$	$[S5,\ S6]$
$S8.\ a \Longrightarrow a$	$[S7]$

□

Tõestuse võib esitada ka puu kujul, see on ülevaatlikum:



Üleskirjutuse lihtsustamise eesmärgil ei kasuta me edaspidi sulgudega opereerimise reegleid. Nende ärajätmine ei muuda tuletuskäigu jlgimist oluliselt keerukamaks. Toodud näite korral sulureeglite vahelejätmine annab tuletuspuu kujul:



Ülesanne 1. *Ehitada valemi* $(\neg\, a \Longrightarrow a) \Longrightarrow a)$ *tuletus.*

Tuletuse ehitamist lihtsustab mõnevõrra nn. deduktsiooniteoreem.

Deduktsiooniteoreem (J. Herbrand, 1930): Kui valemite (hüpoteeside) hulgast $\Gamma \cup \{A\}$ on tuletatav valem B, siis on hulgast Γ tuletatav valem $A \Longrightarrow B$.

Tõestus. Olgu jada $B_1 \ldots, B_n$ valemi B tuletus, arvestades hüpoteese $\Gamma \cup \{A\}$.
Vaja on näidata, et $\forall i \in \{1, \ldots, n)$ korral kehtib $\Gamma \vdash A \Longrightarrow B_i$.
Tõestusmeetodina kasutame matemaatilist induktsiooni.

Induktsiooni baas: Näitame, et $\Gamma \vdash A \Longrightarrow B_1$.
Kuna B_1 on tuletuse $B_1, \ldots, B_n$ esimene element, siis ta on kas aksioom või hüpotees, s.o. valem hulgast Γ või $B_1 \equiv A$. Kahel esimesel juhul (B_1 on aksioom või $B_1 \in \Gamma$) saab ehitada tuletuse

$$\frac{[A1]\ :\ B_1 \Longrightarrow (A \Longrightarrow B_1) \qquad B_1}{A \Longrightarrow B_1}$$

Juhul kui $B_1 \equiv A$, on võimalik tuletada valem $A_1 \Longrightarrow B$ ($\equiv A \Longrightarrow A$) lähtudes aksioomidest, hüpoteese kasutamata (vt. näide 2).
Kokkuvõttes oleme tuletanud valemi $A \Longrightarrow B_1$, lähtudes aksioomidest, ning hüpoteeside hulgast Γ.
Induktsiooni samm: Oletame, et iga $k < i$ korral kehtib $\Gamma \vdash A \Longrightarrow B_k$ ning näitame, et leidub tuletus $\Gamma \vdash A \Longrightarrow B_i$.
Kui B_i on kas aksioom, hüpotees hulgast Γ või $B_i \equiv A$, on valemi $A \Longrightarrow B_i$ tuletus analoogne induktsiooni baasi tuletustega. Antud juhul tuleb aga käsitleda veel neljandat juhtu: valem B_i on saadud reegli MP abil temast tuletuses $B_1, B_2, \ldots, B_i, \ldots, B_n$ eespool astsevatest valemitest B_j ja B_m. Seega

$$\frac{B_j \qquad B_m}{B_i}, \tag{1}$$

nii et $j < i$ ja $m < i$.

Vastavalt induktsiooni eeldusele peavad sel juhul kehtima:

$$\Gamma \vdash A \Longrightarrow B_j$$

ja

$$\Gamma \vdash A \Longrightarrow B_m.$$

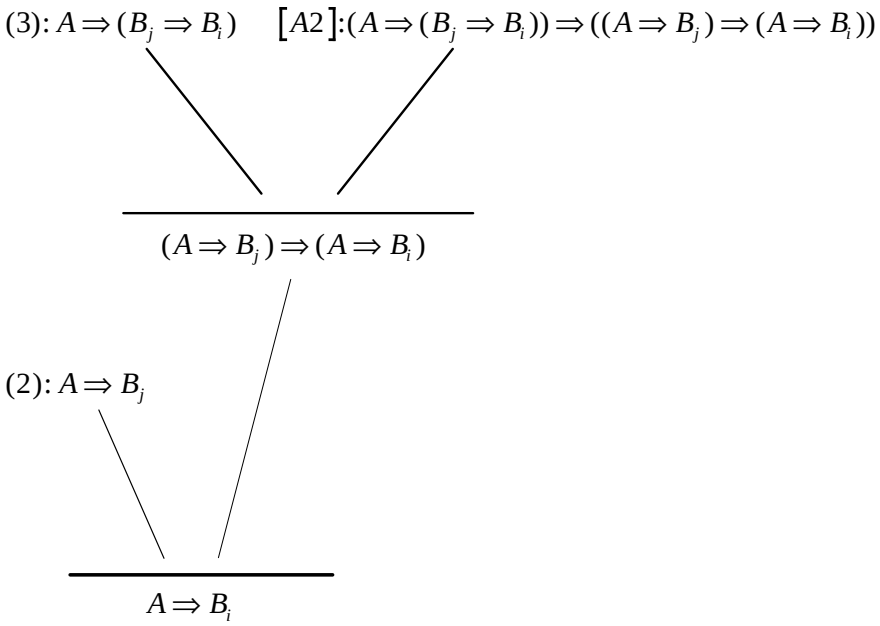
Selleks, et tuletuse samm (1) oleks üldse võimalik, peab näiteks valem B_m olema kujul $B_j \Longrightarrow B_i$. Tähendab, induktsiooni eeldusest järeldub järgmise kahe väite kehtivus:

$$\Gamma \vdash A \Longrightarrow B_j \tag{2}$$

ja

$$\Gamma \vdash A \Longrightarrow (B_j \Longrightarrow B_i) \tag{3}$$

Nendel eeldustel võib tuletuse $\Gamma \vdash A \Longrightarrow B_i$ koostada alljärgnevalt:



Sellega ongi induktsiooni abil näidatud, et iga $i = 1, \ldots, n$ korral $\Gamma \vdash A \Longrightarrow B_i$, seega ka erijuhul $B_n = B$ kehtib $\Gamma \vdash A \Longrightarrow B$.

□

Järeldus 1. $A \Longrightarrow B, \quad B \Longrightarrow C \vdash A \Longrightarrow C$.

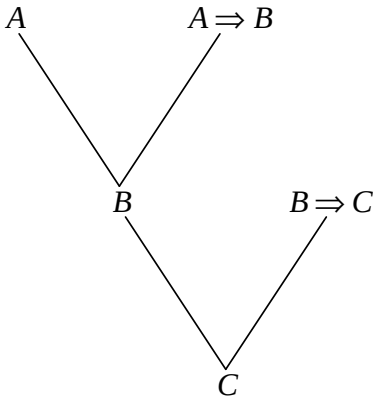
Tõestus.
Seega $A \Longrightarrow B, \quad B \Longrightarrow C, \quad A \vdash C$, millest deduktsiooniteoreemi põhjal järeldubki tõestatav väide.

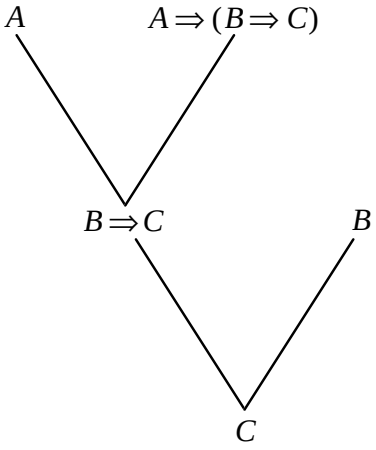
Järeldus 2. $A \Longrightarrow (B \Longrightarrow C), \quad B \vdash A \Longrightarrow C$.

Tõestus.
Seega $A \Longrightarrow (B \Longrightarrow C), \quad B, \quad A \vdash C$, millest deduktsiooniteoreemi järgi järeldubki tõestatav väide.

Oleme tõestanud kaks täiendavat tuletusreeglit:

$$\frac{A \Longrightarrow B \qquad B \Longrightarrow C}{A \Longrightarrow C}$$

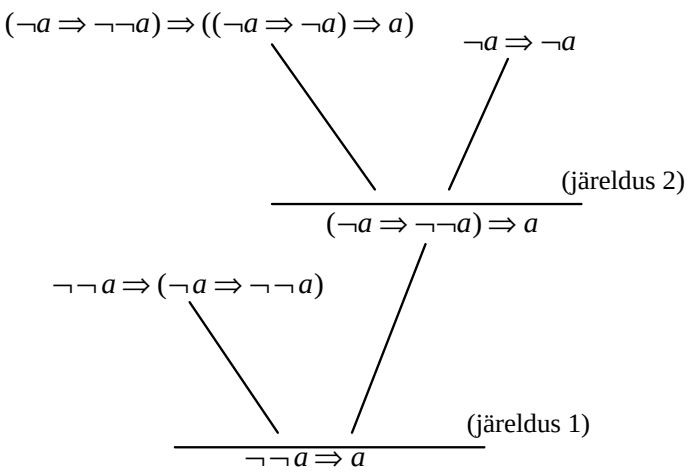




ja

$$\frac{A \Longrightarrow (B \Longrightarrow C) \quad B}{A \Longrightarrow C}.$$

Näide 3. Valemi $\neg\neg\, a \Longrightarrow a$ tuletus.

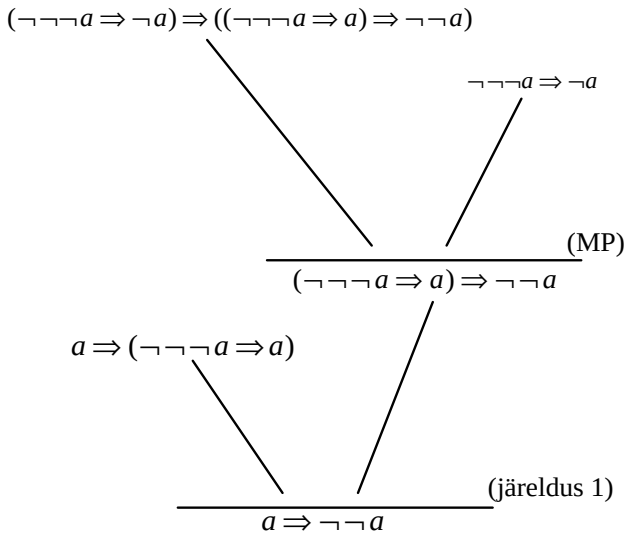


[A3: $A \ldots \neg a, B \ldots a$]
[Näide 1]

[A1: $A \ldots \neg a, B \ldots \neg a$]

□

Näide 4. Valemi $a \Longrightarrow \neg\neg\, a$ tuletus.



□

Järeldus 3. $a \equiv \neg\neg a$.

Ülesanne 2. *Tuletada valemid:*

1. $\neg\,((a \Longrightarrow b) \Longrightarrow \neg\,(b \Longrightarrow c)) \Longrightarrow (a \Longrightarrow c)$;
2. $\neg\, A \Longrightarrow (A \Longrightarrow B)$;
3. $(\neg\, B \Longrightarrow \neg\, A) \Longrightarrow (A \Longrightarrow B)$;
4. $(A \Longrightarrow B) \Longrightarrow (\neg\, B \Longrightarrow \neg\, A)$;
5. $(A \Longrightarrow B) \Longrightarrow ((\neg\, A \Longrightarrow B) \Longrightarrow B)$.

3. Predikaatarvutus

Predikaatarvutus on lausearvutuse laiendus, mis võimaldab opereerida üksikobjektidega. Predikaatarvutusega saab väljendada selliseid lauseid nagu "leidub selline arv, et ..." ja "iga elemendi korral kehtib ...", mis on matemaatilises tekstis sagedased. Predikaatarvutusele on iseloomulikud järgmised arutlused.

"Kõik koerad hauguvad. Muri on koer. Järelikult Muri haugub."

või

"Iga naturaalarvu N korral leidub algarv $x > N$. Kõik algarvud on naturaalarvud. 17 on algarv. Järelikult 17 on naturaalarv. Järelikult leidub algarv, mis on suurem kui 17".

Üksikobjektide (indiviidide) tähistamiseks kasutatakse predikaatarvutuses indiviidmuutujaid ja -konstante.

Indiviididevahelisi tehteid väljendavaid operatsioone tähistatakse **esimest järku predikaatarvutuse** puhul funktsionaalkonstantidega. Kõrgemat järku arvutuste korral võib kasutada ka funktsionaalmuutujaid.

Funktsioonide esitamiseks kasutatakse nn. prefiksnotatsiooni, s.t. tehtemärk kirjutatakse enne operande, näiteks $f(x, y)$, $+(5, z)$ jne. Iga funktsionaalkonstanti iseloomustab tema argumentide arv e. **kohalisus e. aarsus** ja funktsiooni tüüp. Nii võib rääkida 0-, 1-, 2-, jne. kohalistest funktsioonidest. Funktsiooni tüüp näitab aga, mis tüüpi on argumendid ja mis tüüpi on funktsiooni väärtus (s.t. millisesse hulka nad kuuluvad). Kui näiteks 3-kohalise funktsiooni g argumendid on vastavalt tüüpi τ_1, τ_2 ja τ_3 ning tulemus tüüpi τ, esitatakse funktsiooni g tüüp avaldisega

$$g : \tau_1 \times \tau_2 \times \tau_3 \longrightarrow \tau.$$

Argumente ja tulemust väljendavad tüübisümbolid $\tau, \tau_1, \tau_2, \ldots$ tähistavad objektide hulka, millest võivad olla valitud vastava suuruse konkreetsed väärtused. Näiteks reaalarvude liitmise operatsioon (funktsiooni) tüüp võib olle esitatud avaldisega

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \quad \text{e.} \quad + : \mathbf{real} \times \mathbf{real} \longrightarrow \mathbf{real}.$$

Ka programmeerimisest tuntud *if*-lauset võib vaadelda kui 3-kohalist funktsiooni. Eeldame lihsuse mõttes, et *if*-lauses kasutatakse vaid aritmeetikatehteid ning omistamisoperaatoreid; omistamine toimub mõlema alternatiivi korral ühele a samale muutujale. Selliseid tingimusi rahuldab näiteks tingimuslik lause

$$\mathbf{if}\ x > 5\ \mathbf{then}\ y : 4^*(x - z)\ \mathbf{else}\ y := -2^*x.$$

Selleks, et niisuguse lause "funktsionaalsus" paremini silma paistaks, võib ta esitada ka kujul

$$y := \ \mathbf{if}\ x > 5\ \mathbf{then}\ 4^*(x - z)\ \mathbf{else}\ -2^*x.$$

(Mõnes programmeerimiskeeles kasutataksegi just sellist *if*-lause vormi). Nagu näeme, on toodud näites tegu funktsiooniga, millelon kolm argumenti: üks tõeväärtuslik (tüüpi **bool** ja kaks reaalarvulist (tüüpi **real**) argumenti; tulemus on aga reaalarv (mida soovi korral võib omistada ka reaalarvulisele muutujale, nagu seda tehti eelnevas näites). Seega saab selle *if*-funktsiooni tüübi esitada avaldisena

$$\mathbf{if}\ : \mathbf{bool} \times \mathbf{real} \times \mathbf{real} \longrightarrow \mathbf{real}.$$

Lisaks indiviididele ja funktsioonidele kasutatakse esimest järku predikaatarvutuses veel indiviidide omadusi väljendavaid predikaate (predikaatkonstante). Need on

funktsioonid, mille väärtus on tõeväärtuse tüüpi. Eristamaks predikaate teistest funktsioonidest, kasutame nende tähistamiseks suurtähti P, Q, R jne.

Nii nagu funktsioonidegi korral, saab ka predikaatide puhul rääkida nende kohalisusest ja tüübist. Näitena võib tuua ühekohalise predikaadi $P(x)$, mille argument on reaalarvuline. Sellise predikaadi tüüp esitatakse avaldisena

$$P : \mathbf{real} \longrightarrow \mathbf{bool}.$$

Predikaati P võib interpreteerida kas näiteks tingimusena $x < 5$ või $\sin(x) = 30°$ või $x^2 + 3^*x - 4 = 0$ vms. viisil.

Esimest järku predikaatarvutuse klassikaline kuju on alljärgnev:

Tähestik:

- indiviidsümbolid (konstandid $a, b, c, \ldots, a_1, b_1, \ldots$ ja muutujad $x, y, z, \ldots, x_1, y_1, \ldots$);
- funktsionaalkonstandid ($f, g, h, \ldots$ - koos indeksitega, kui vaja);
- predikaatsümbolid ($P, Q, R, \ldots$ - koos indeksitega, kui vaja);
- loogikasümbolid (& - konjunktsioon, V - disjunktsioon, $\neg$ - eitus ja $\Longrightarrow$ - implikatsioon);
- kvantorid ($\forall$ - üldsuskvantor, $\exists$ - eksistentsikvantor);
- abisümbolid (sulud, koma).

Väljendid on tähestiku märkidest moodustatud stringid. Väljendeid tähistatakse enamasti ladina tähestiku alguse suurtähtedega $A, B, C, \ldots$ Sümbol $A(x)$ tähistab väljendit, mis sisaldab indiviidi x. Kui väljendi $A(x)$ ette on pandud sümbolid $\forall x$ või $\exists x$, s.t. tegu on väljenditega $\forall x A(x)$ või $\exists x A(x)$, nimetatakse muutujat x **seotud muutujaks**. Vastasel korral nimetatakse muutujat x **vabaks muutujaks** väljendis $A(x)$.

Term:

- iga indiviidsümbol määramispiirkonnaga τ on term tüüpi τ;
- kui f on k-kohaline funktsioonisümbol tüüpi $f : \tau_1 \times \ldots \times \tau_k \longrightarrow \tau$ ning $t_1, \ldots t_k$ on vastavalt termid tüüpi $\tau_1, \ldots, \tau_k$, siis on väljend $f(t_1, \ldots, t_k)$ term tüpi τ;
- muud väljendid ei ole termid.

Atomaarne valem e. aatom.

Väljend $P(t_1, \ldots, t_k)$ on atomaarne valem, kui P on k-kohaline predikaatsümbol tüüpi $\tau_1 \times \ldots \times \tau_k \longrightarrow \mathbf{bool}$ ning $t_1, \ldots, t_k$ on vastavalt termid tüüpi $\tau_1, \ldots, \tau_k$.

Valem:

- iga aatom on valem;
- kui A on valem, siis on valem ka $\neg A$;
- kui A ja B on valemid, siis on valemid ka $A\&B$, AVB ja $A \Longrightarrow B$;
- kui $A(x)$ on valem, kus x on vaba muutuja, siis on valemid ka $\forall x A(x)$ ja $\exists x A(x)$;
- muud väljendid ei ole valemid.

Predikaatarvutuse aksioomid:

A1. $A \Longrightarrow (B \Longrightarrow A)$
A2. $(A \Longrightarrow (B \Longrightarrow C)) \Longrightarrow ((A \Longrightarrow B) \Longrightarrow (A \Longrightarrow C))$
A3. $(A\&B) \Longrightarrow A$
A4. $(A\&B) \Longrightarrow B$
A5. $A \Longrightarrow (B \Longrightarrow (A\&B))$
A6. $(A \Longrightarrow C) \Longrightarrow ((B \Longrightarrow C) \Longrightarrow AVB \Longrightarrow C))$
A7. $A \Longrightarrow (AVB)$
A8. $B \Longrightarrow (AVB)$
A9. $\neg A \Longrightarrow (A \Longrightarrow B)$
A10. $(A \Longrightarrow B) \Longrightarrow ((A \Longrightarrow \neg B) \Longrightarrow \neg A)$
A11. $AV \neg A$
A12. $\forall x A(x) \Longrightarrow A[x := t]$
A13. $A[x := t] \Longrightarrow \exists x A(x)$
A14. $\forall x(A \Longrightarrow B(x)) \Longrightarrow (A \Longrightarrow \forall x B(x))$, kus A ei sisalda x-i vabalt
A15. $\forall x(B(x) \Longrightarrow A) \Longrightarrow (\exists x B(x) \Longrightarrow A)$, kus A ei sisalda x-i vabalt

Tuletusreeglid

Modus ponens (MP):

$$\frac{A \Longrightarrow B \quad A}{B}$$

ja üldistamine (Gen):

$$\frac{A}{\forall x A}$$

Ka predikaatarvutuse korral kehtib **deduktsiooniteoreem**.

Kui Γ, $A \vdash B$ ja leidub valemi A tuletus, milles ei kasutata reeglit Gen valemi A vabade muutujate suhtes, siis $\Gamma \vdash A \Longrightarrow B$. (Tõestus on toodud raamatus E. Mendelson "Introduction to Mathematical Logic", D. van Nostrad co inc., Princeton, 1964. Raamatu venekeelne tõlge on ilmunud Moskvas aastal 1984, kirjastuse "Nauka").

Näide 5. Tuletame valemi $\forall x \forall y A(x,y) \Longrightarrow \forall y \forall x A(x,y)$.

S1. $\forall x \forall y A(x,y)$	[hüpotees]
S2. $\forall x \forall y A(x,y) \Longrightarrow \forall y A(x,y)$	[A12, kus $t = x$]
S3. $\forall y A(x,y)$	[S1, S2, kasutades MP]
S4. $\forall y A(x,y) \Longrightarrow A(x,y)$	[A12, kus $t = y$]
S5. $A(x,y)$	[S3, S4, kasutades MP]
S6. $\forall x A(x,y)$	[S5, kasutades Gen]
S7. $\forall y \forall x A(x,y)$	[S6, kasutades Gen]

Seega oleme näidanud, et $\forall x \forall y A(x,y) \vdash \forall y \forall x A(x,y)$. Kuna tuletuses ei ole reeglit Gen rakendatud valemi $\forall x \forall y A(x,y)$ vabade muutujate suhtes, siis deduktsiooniteoreemi põhjal saabki järeldada soovitud valemi tuletatavuse.

□

Ülesanne 3. *Tuletada valem*

$$\forall x(A(x) \Longrightarrow B(x)) \Longrightarrow (\exists x A(x) \Longrightarrow \exists x B(x)).$$

4. Sekventsiaalarvutused

Matemaatikas kasutatakse tõestamismeetoditena induktsiooni (üksiknäidete üldistamine) ja deduktsiooni (järeldamine üldiste teadmiste põhjal). Deduktiivsed matemaatilised tõestused on formaliseerituna esitatavad loogika keeles. Seejuures saab iga deduktiivse arutluse kirja panna predikaatarvutuse (erandjuhtudel ka lausearvutuse) valemi tuletusena. Kõik matemaatilistes tuletustes kasutatavad valemid on implikatsiooni kujul (G. Gentzen, 1934):

$$A_1 \& \ldots \& A_m \Longrightarrow B_1 \vee \ldots \vee B_n . \tag{4}$$

Valemit kujul (4) nimetatakse **sekventsiks** ning esitatakse lühendatult avaldisena

$$A_1, \ldots, A_m \longrightarrow B_1, \ldots, B_n , \tag{5}$$

mida interpreteeritakse järgmiselt: "tingimustest $A_1, \ldots$ ja A_m järeldub B_1 või $\ldots$ B_n". Tingimused $A_1, \ldots, A_m$, $B_1, \ldots, B_n$ on esitatavad suvaliste predikaatarvutuse (või lausearvutuse) valemitena. Sekventsi (5) eeldusi $A_1, \ldots, A_m$ nimetatakse **antetsedendiks** ja järeldust $B_1, \ldots, B_n$ nimetatakse **suktsedendiks**. Sekventsi (5) antetsedent võib erijuhul ka puududa, s.t. $m = 0$. Sellisel juhul on valemid $B_1, \ldots, B_n$ tuletatavad aksioomidest lisaeeldusi (hüpoteese) kasutamata.

Sekventside esitamiseks kasutatakse ka kirjutist

$$\Gamma \longrightarrow \Delta,$$

kus kreeka tähed tähistavad valemite loetelusid. Juhul kui tahetakse rõhutada, et sekventsi antetsedent või suktsedent sisaldab muude valemite kõrval ka valemit A, esitatakse sekvents vastavalt kas kujul

$$\Gamma, A \longrightarrow \Delta$$

või

$$\Gamma \longrightarrow \Delta, A.$$

Suktsedendita sekvents ($n = 0$) näitab, et valemid $A_1, \ldots, A_m$ on vastuolulised.

Enamikku tuntud arvutustest saab esitada nn. sekventsiaalarvutustena, kus tuletuse "elementideks" on sekventsid.

Sekventsiaalarvutuse teoreemiks on iga valem A, mille korral on tuletatav antetsedendita sekvents $\longrightarrow A$. Tuletusreeglid kujul

$$\frac{S_1 \quad S_2 \quad \ldots \quad S_k}{S}$$

näitavad, et sekventside $S_1, \ldots, S_k$ tuletatavusest järeldub sekventsi S tuletatavus. Aksioomideks loetakse need sekventsid, mille antetsedendis ja suktsedendis on üks ja sama valem:

$$\Gamma, A \longrightarrow \Delta, A.$$

Iga sekventsiaalarvutuses kasutatava loogikatehte jaoks on kaks tuletusreeglit: üks tehtemärgi sissetoomiseks sekventsi S antetsedenti, teine märgi sissetoomiseks sekventsi S suktsedenti. Nimetatud asjaolu tõttu on sekventsiaalarvutuste konstrueerimine oluliselt lihtsam kui "klassikalistes" arvutustes. Näiteks lausearvutuse korral on tuletuse otsimine deterministlik.

Illustreerime toodud väiteid predikaatarvutuse sekventsiaalvariandi näitel.

1. järku predikaatarvutuse tuletusreeglid (arvutus G4):

1. Struktuurireeglid

   - Lõdvendus

$$\frac{\Delta \longrightarrow \Gamma}{D, \Delta \longrightarrow \Gamma} \qquad \frac{\Delta \longrightarrow \Gamma}{\Delta \longrightarrow \Gamma, G}$$

   - Taandamine

$$\frac{D, D, \Delta \longrightarrow \Gamma}{D, \Delta \longrightarrow \Gamma} \qquad \frac{\Delta \longrightarrow \Gamma, G, G}{\Delta \longrightarrow \Gamma, G}$$

   - Ümberjärjestamine

$$\frac{\Delta, A, B, \Gamma \longrightarrow \Pi}{\Delta, B, A, \Gamma \longrightarrow \Pi} \qquad \frac{\Delta \longrightarrow \Gamma, A, B, \Sigma}{\Delta \longrightarrow \Gamma, B, A, \Sigma}$$

   - Lõige

$$(\text{cut})\ \frac{\Delta \longrightarrow \Gamma, A \qquad A, \Pi \longrightarrow \Sigma}{\Delta, \Pi \longrightarrow \Gamma, \Sigma}$$

2. Loogikareeglid

$$(\neg \longrightarrow)\ \frac{\Gamma \longrightarrow \Delta, A}{\neg\, A, \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \neg)\ \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg\, A}$$

$$(\vee \longrightarrow)\ \frac{A, \Gamma \longrightarrow \Delta \quad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \vee)\ \frac{\Gamma \longrightarrow \Delta, A, B}{\Gamma \longrightarrow \Delta, A \vee B}$$

$$(\& \longrightarrow)\ \frac{A, B, \Gamma \longrightarrow \Delta}{A\&B, \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \&)\ \frac{\Gamma \longrightarrow \Delta, A \quad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A\&B}$$

$$(\Longrightarrow \longrightarrow)\ \frac{\Gamma \longrightarrow \Delta, A \quad B, \Gamma \longrightarrow \Delta}{A \Longrightarrow B, \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \Longrightarrow)\ \frac{A, \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \Longrightarrow B}$$

$$(\forall \longrightarrow)\ \frac{A[x := t],\ \forall x A(x),\ \Gamma \longrightarrow \Delta}{\forall x A(x), \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \forall)\ \frac{\Gamma \longrightarrow \Delta, A[x := b]}{\Gamma \longrightarrow \Delta, \forall x A(x)}$$

$$(\exists \longrightarrow)\ \frac{A[x := b], \Gamma \longrightarrow \Delta}{\exists x A(x), \Gamma \longrightarrow \Delta} \qquad (\longrightarrow \exists)\ \frac{\Gamma \longrightarrow \Delta,\ \ A[x := t], \exists x A(x)}{\Gamma \longrightarrow \Delta, \exists x A(x)}$$

Toodud tuletusreeglites tähistab t suvalist termi. Reeglites $(\longrightarrow \forall)$ ja $(\exists \longrightarrow)$ tähistab b vaba indiviidmuutujat, mis ei tohi esineda tuletatavas sekventsis, s.o. b ei tohi olla vaba muutuja üheski loetelu Γ, Δ valemis ega ka valemites $\exists x A(x)$ ja $\forall x A(x)$.

Näide 6. Tuletada valem $a \Longrightarrow \neg\, \neg\, a$.

$$\dfrac{\dfrac{\dfrac{\dfrac{a \longrightarrow a}{\neg\, a,\ a \longrightarrow}\ (\neg \longrightarrow)}{a \longrightarrow\ \neg\, \neg\, a}\ (\longrightarrow\ \neg)}{\longrightarrow a \Longrightarrow\ \neg\, \neg\, a}\ (\longrightarrow \Longrightarrow)$$

□

Märkus 1. Taandamis- ja ümberjärjestamise reeglid võimaldavad sekventsides esinevaid valemite loetelusid käsitleda hulkadena. Edaspidi eeldamegi, et valemite järjekord antetsedendis või suktsedendis pole oluline. Samuti ei pööra me tähelepanu asjaolule, kas mõni valem esineb sekventsi ühel poolel üks või mitu korda.

Märkus 2. Arvestades lõdvendusreegleid, võib aksioome käsitleda lihtsustatud kujul:

$$A \longrightarrow A.$$

Arvutuse $G4$ tuletusreeglid on saadud matemaatika deduktiivsete tuletuste formaliseerimisel.

Vaatame näiteks predikaati $P(x) = (x^2 < r)$. Siis $r > 0$ korral on lõpmata palju arve, mis seda predikaati rahuldavad, (s.t. on tõene valem $\exists x P(x)$); $r \leq 0$ korral ei leidu aga ühtegi arvu, mis rahuldaksid vaadeldavat predikaati.

Teiselt poolt kehtib predikaat $\neg\, P(y) = (y^2 \geq r)$ iga y jaoks, kui $r \leq 0$, vastasel juhul aga ei rahulda seda predikaati ükski y väärtus.

Kahe viimase lõigu põhjal saab teha üldistava järelduse, et sõltumata r väärtusest kehtib väide $\exists x \forall y (P(x) \vee \neg\, P(y))$ (edasises tähistame seda valemit tähega A). Selgub, et predikaadi P interpretatsioon pole antud juhul oluline: valem A on tuletatav iga predikaadi P jaoks. Matemaatikud kasutavad selle väite tuletamiseks sageli järgmist võtet.

Eeldame, et kehtib $\exists P(x)$. Siis võib leida konstandi a, nii et kehtib $P(a)$. Arvestades disjunktsiooni omadusi, saame, et kehtib seos

$$\forall y (P(a) \vee \neg\, P(y)) \text{ e. } \exists x \forall y (P(x) \vee \neg\, P(y)).$$

Eeldame nüüd, et $\exists x P(x)$ ei kehti, s.t. kehtib valem $\neg\, (\exists x P(x))$. Siis kehtib iga muutuja d väärtuse korral $\neg\, P(d)$. Analoogiliselt eelmiase juhuga saab siingi näidata, et

$$\exists x (P(x) \vee \neg\, P(d)) \text{ e. } \exists x \forall y (P(x) \vee \neg\, P(y)).$$

Seega oleme mõlema alternatiivi korral tõestanud, et kehtib valem A. Kuna rohkem võimalusi eelduse valikuks pole, võime väita, et valem A kehtib tingimusteta. Sisuliselt oleme kasutanud lõikereeglit:

$$\frac{\longrightarrow \exists x P(x) \vee \neg\, \exists x P(x) \qquad \longrightarrow \exists x P(x) \vee \neg\, \exists x P(x) \Longrightarrow \exists x \forall y (P(x) \vee \neg\, P(y))}{\exists x \forall y (P(x) \vee \neg\, P(y))}$$

Toodud juhul on lõikereegli variandi mõlemad eeldused suhteliselt lihtsalt tuletatavad (vt. näide 7). Lõikereegli kasutamise raskus seisneb sellise "lõigatava" valemi leidmises, mis annaks lihtsalt tõestatavad eeldused.

Lõikereeglit kasutatakse paljudes matemaatika arutluskäikudes.

Näide 7. $\exists x \forall y (P(x) \vee \neg\, P(y)) \equiv A.$

$$\begin{array}{lll}
 & & \dfrac{P(d) \longrightarrow A, P(c), P(d), \exists x P(x)}{\longrightarrow A, P(c), \neg\, P(d), P(d), \exists x P(x)} \\
 & \dfrac{P(a) \longrightarrow A, P(a) \neg\, P(b)}{P(a) \longrightarrow A, P(a) \vee \neg\, P(b)} & \dfrac{\longrightarrow A, P(c), \neg\, P(d), \exists x P(x)}{\longrightarrow A, P(c) \vee \neg\, P(d), \exists x P(x)} \\
 & \dfrac{P(a) \longrightarrow A, \forall y (P(a) \vee \neg\, P(y))}{S_3 :\ P(a) \longrightarrow A} & \dfrac{\longrightarrow A, \forall y (P(c) \vee \neg\, P(y)), \exists x P(x)}{S_2 : \longrightarrow A,\ \exists x P(x)} \\
\exists x P(x) \longrightarrow \exists x P(x) & S_1 :\ \exists x P(x) \longrightarrow a & \neg\, (\exists x P(x)) \longrightarrow a \\
\hline
\longrightarrow x P(x), \neg\, (\exists x P(x)) & \exists x P(x) \vee \neg\, (\exists x P(x)) \longrightarrow A & \\
\hline
\longrightarrow \exists x P(x) \vee \neg\, (\exists x P(x)) & & \\
\hline
S :\ \longrightarrow A & &
\end{array}$$

□

Järgnevas tõestame teoreemi, mis näitab, et nn. **siledate** sekventside korral saab kõiki lõikereegli abil tuletatavaid valemeid tõestada ka ilma selle reeglita. Siledaks nimetatakse sekventsi, milles üks ja sama muutuja ei esine ühtaegu nii seotud kui ka vaba muutujana. Näiteks sekvents

$$\forall x \forall y (P(x) \& Q(y)) \longrightarrow P(y) \tag{6}$$

pole sile, sest muutuja y on antetsedendis seotud, suktsedendis aga vaba.

Tegelikult ei kujuta sekventside sileduse nõue mingit piirangut, sest seotud muutujate ümbernimetamine ei muuda valemi tuletatavust. (Harjutusena on soovitatav tõestada viimast väidet kinnitavad valemid $\forall x A(x) \Longrightarrow \forall y A(y)$ ja $\exists x A(x) \Longrightarrow \exists y A(y)$). Näiteks sekventsiga (6) on samaväärne sile sekvents

$$\forall x \forall z (P(x) \& P(z)) \longrightarrow P(y).$$

Lõikereegli elimineeritavusest järeldub, et selle kasutamist saaks arutluskäikudes vältida. Sel asjaolul on suur metodoloogiline tähendus: lõikereegli abil saaks iga tuletatava lause jaoks tuletada ka tema eituse. Teiste sõnaega, mitteelimineeritavat lõikereeglit sisaldav arvutus pole **kooskõlaline**.

Lõikereegel on ainus reegel, mille järeldusena saadav sekvents ei pruugi sisaldada ühtegi valemit (veenduge selles!). Seega saab lõikereegliga põhimõtteliselt tuletada tühja sekventsi:

$$\longrightarrow .$$

Tühjast sekventsist saab aga lõdvendusreegliga tuletada nii $\longrightarrow A$ kui ka $\longrightarrow \neg A$. Kehtib ka vastupidine: juhul kui arvutuses saab tuletada vastuolu, s.t. sekventsid $\longrightarrow A$ ja $\longrightarrow \neg A$, saab tuletada ka tühja sekventsi

$$\dfrac{\begin{array}{ll} \longrightarrow A & \\ \neg A \longrightarrow & \longrightarrow \neg A \end{array}}{\longrightarrow} \text{ cut}$$

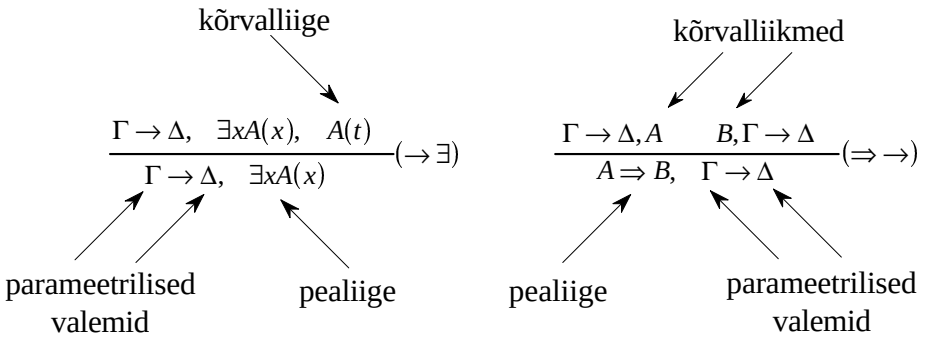
Järeldus 4. *Arvutus on mittekooskõlaline parajasti siis, kui tema tuletusreeglid lubavad tuletada tühja sekventsi. Predikaatarvutuses aga ei saagi tühja sekventsi tuletada, kui lõikereeglit ei kasutata.*

Teoreem 1. Teoreem lõike elimineerimisest *(G. Gentzen). Iga sile sekvents on tuletatav arvutuses G4 lõikereeglit kasutamata.*

Tegelikult tõestame veelgi tugevama väite: iga lõikereeglit kasutava tuletuse saab lõpliku arvu sammudega transformeerida tuletuseks, mis ei sisalda lõikereegli kasutamisi.

Enne teoreemi tõestamist veendume kolme lemma kehtivuses. Alustame aga sellest, et toome sisse mõned tõestuses vajalikud mõisted.

Kõigil tuletusreeglitel grupist B on nn. alamavaldiste omadus: tuletusreegli järelduses võetakse abiks uus valem (reegli pealiige), mis saadakse eeldustes esinevatest valemitest (reegli kõrvalliikmetest) loogikatehete rakendamisel. Kõiki ülejäänud (tuletussammul muutumatutena ümberkirjutatavaid) valemeid nimetatakse parameetrilisteks valemiteks. Niisiis oleme andnud igale tuletusreeglis esinevale valemile üldnime. Näiteks:



Eellased ja järglased. Tuletusreegli järelduses esineva parameetrilise valemi A esinemist reegli eelduses nimetatakse tema vahetuks eellaseks.

Valemi A **eellaseks** on kõik need tuletuses esinevad valemid B, mis on suhtes $(A, B) \in R^*$, kus R^* on vahetu eelnevuse suhte R transitiivne refleksiivne sulund. Kui valem A on valemi B eellane, siis valemit B nimetatakse valemi A **järglaseks**.

Ülesanne 4. *Leida näites 7 esitatud tuletuses valemi A kõik eellased.*

Valemi astak on valemis esinevate loogikamärkide $\vee, \&, \neg, \Longrightarrow, \forall$ ja $\exists$ arv. Näiteks valemi $\exists x P(x) \vee \neg\ (\exists x P(x))$ astak on 4.

Lõike astak on tuletuses kasutatavas lõikereeglis

$$\frac{\Gamma \longrightarrow \Delta, C \qquad C, \Sigma \longrightarrow \Pi}{\Gamma, \Sigma \longrightarrow \Delta, \Pi}$$

lõigatava valemi C astak.

Tuletuse korrutamine sekventsiga $\Gamma \longrightarrow \Delta$ (tähistus $d \cdot [\Gamma \longrightarrow \Delta]$, kus d on mingi tuletuspuu) on tuletus, milles iga sekvents $\Sigma \longrightarrow \Pi$ on asendatud sekventsiga $\Gamma, \Sigma \longrightarrow \Pi, \Delta$.

Omadus 1. *Tuletuse d korrutamine suvalise sekventsiga ei muuda tuletuse struktuuri (kasutatakse tuletusreeglite järjekorda ja pealiikmeid) ega korrektsust. Teiste sõnadega, kui d on tuletus, siis on ka $d \cdot [\Gamma \longrightarrow \Delta]$ tuletus.*

NB! Veenduge selle väite kehtivuses iseseisvalt!

Definitsioon 1. *Sekventsi $\Gamma \longrightarrow \Delta$ tuletust D nimetame (k, F)-tuletuseks, kui kasutatavates lõikereeglites on lõigete maksimaalne astak k ja kõigi lõigatavate maksimaalse astmega valemite hulk on F. (k, F)-tuletuse tähistamiseks kasutatakse järgmist kirjavisi:*

$$\vdash^{(k,F)} \Gamma \longrightarrow \Delta$$

Näites 7 on esitatud valemi A $(4, \{\exists x P(x) \vee \neg\ \exists x P(x)\})$-tuletus.

Lemma 1.

(Inversioonilemma):

1. *Kui $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, A\&B$, siis $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, A$ ja $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, B$;*
2. *Kui $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, \forall x A$, siis $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, A[x := t]$, kus t ei sisalda muutujaid, mis on Γ, Δ ja $\forall x A$ jaoks seotud muutujad;*

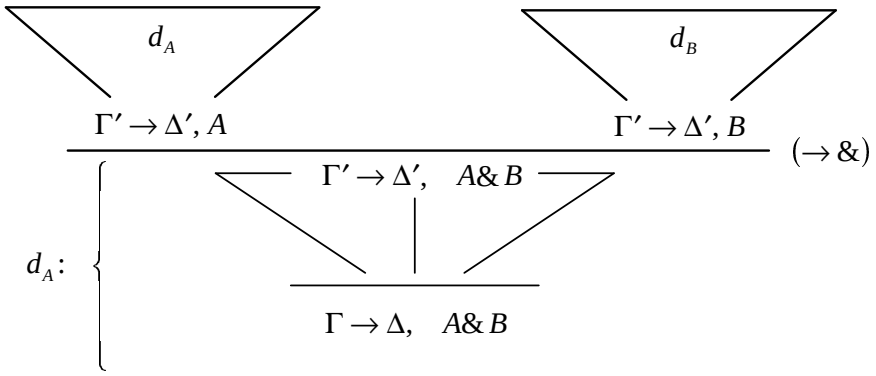
3. *Kui* $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, A \Longrightarrow B$, *siis* $\vdash^{(k,F)} A, \Gamma \longrightarrow \Delta, B$;
4. *Kui* $\vdash^{(k,F)} \Gamma \longrightarrow \Delta, \neg A$, *siis* $\vdash^{(k,F)} A, \Gamma \longrightarrow \Delta$;
5. *Kui* $\vdash^{(k,F)} A \vee B, \Gamma \longrightarrow \Delta$, *siis* $\vdash^{(k,F)} A, \Gamma \longrightarrow \Delta$ *ja* $\vdash^{(k,F)} B, \Gamma \longrightarrow \Delta$;
6. *Kui* $\vdash^{(k,F)} (\exists x A), \Gamma \longrightarrow \Delta$, *siis* $\vdash^{(k,F)} A[x := t], \Gamma \longrightarrow \Delta$, *kus* t *ei sisalda muutujaid, mis on* Γ, Δ *ja* $\exists x A$ *jaoks seotud muutujad.*

Tõestus.

Juhtum 1: Sekventsi $\Gamma \longrightarrow \Delta, A\&B$ tuletuses peab olema kasutatud kas

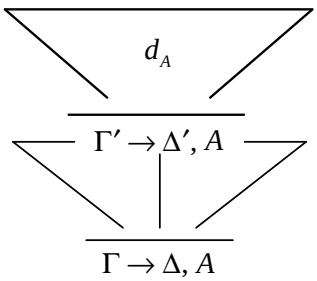
a) reeglit $(\longrightarrow \&)$,
b) lõdvendusreeglit valemi $A\&B$ sissetoomiseks või
c) aksioomi $A\&A \longrightarrow A\&A$.

Juhul 1a) on tuletus kujul:



Teisendame seda tuletust:

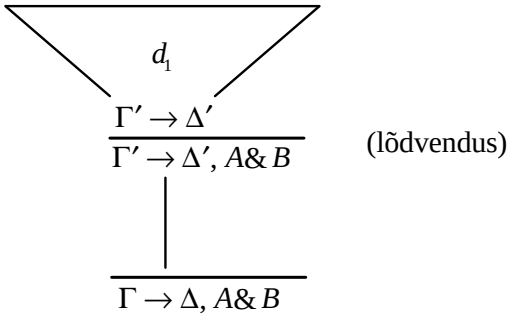
asendame tuletatavas sekventsis valemi $A\&B$ koos oma kõigi eellastega valemiga A (tuletuspuu osas D asendame parameetrilised valemid $A\&B$ uue valemiga A), jätame ära tuletussammu $(\longrightarrow \&)$ ning jätkame sekventsi $\Gamma' \longrightarrow \Delta', A$ tuletust puuga d_A. Saame



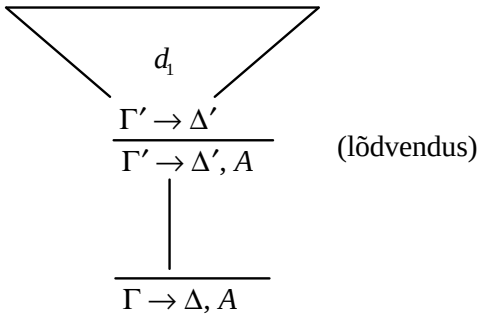
Samal viisil saame sekventsi $\Gamma \longrightarrow \Delta, B$ tuletuse.

Juhul 1b) on teisendus analoogne: parameetriline valem $A\&B$ tuleb koos kõigi oma eellastega asendada valemiga A (või valemiga B).

Seega tuletus

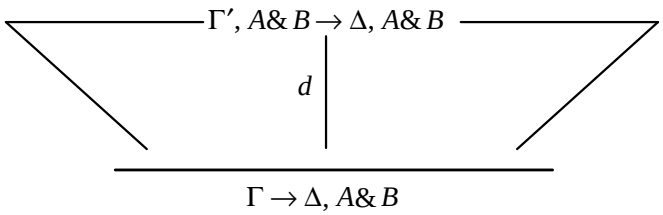


teisendatakse kujule

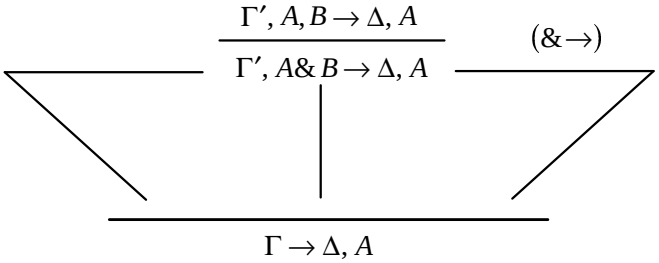


Juhul 1c) asendatakse sekventsis parameetrilised valemid $A\&B$ valemiga A (või valemiga B) ja seejärel tuletatakse sekvents $\Gamma', A\&B \longrightarrow \Delta'$, kasutades reeglit $(\& \longrightarrow)$.

Täpsemalt, tuletus



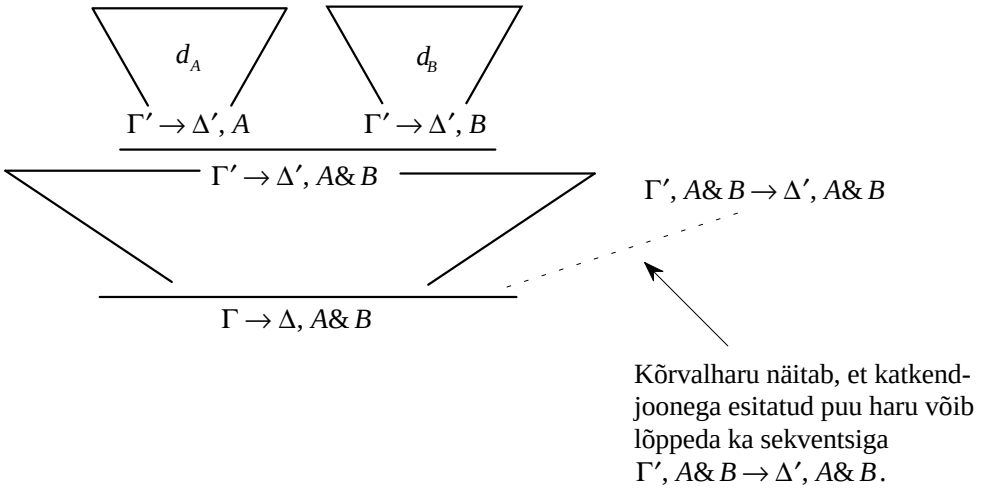
teisendatakse tuletuseks



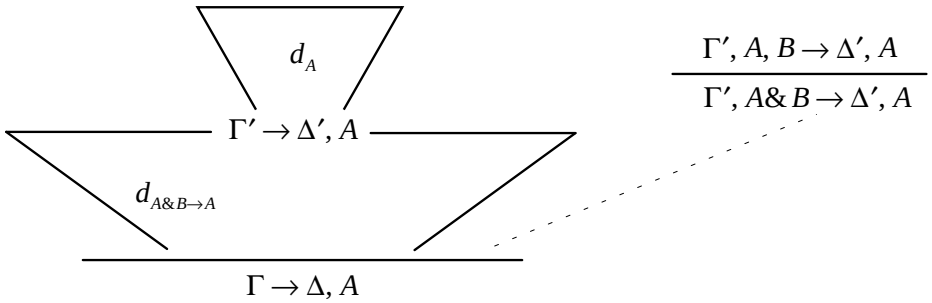
Märkus 3. Juhul 1b), kus valem toodi sisse lõdvendusreegliga, on teisendus rakendatav ka teiste loogikatehete korral, s.t. 1b), 2b), 3b), 4b), 5b) ja 6b) tõestatakse sama moodi.

Ülejäänud kaks teisendust saab esitada graafiliselt ühel joonisel.

Tuletuspuu enne teisendust:



Tuletuspuu pärast teisendust:



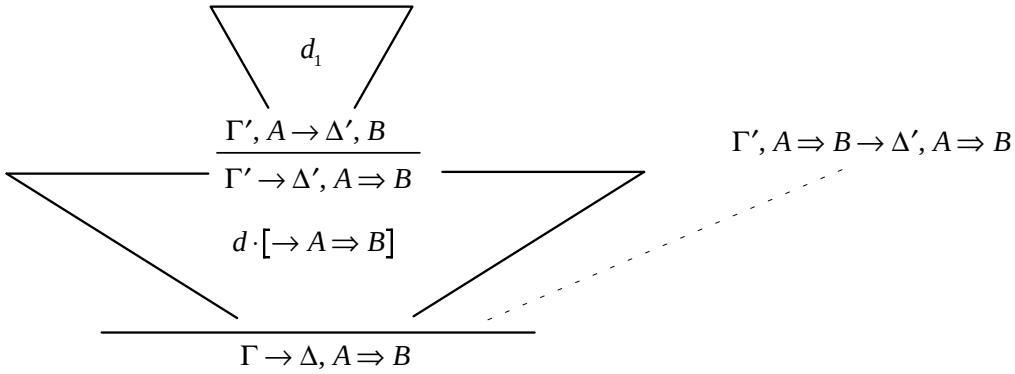
$d_{A\&B\to A}$ tähistab puud, mis on saadud puust d parameetrilise avaldise $A\&B$ ja tema kõigi eellaste asendamisel valemiga A.

(Märkuse lõpp).

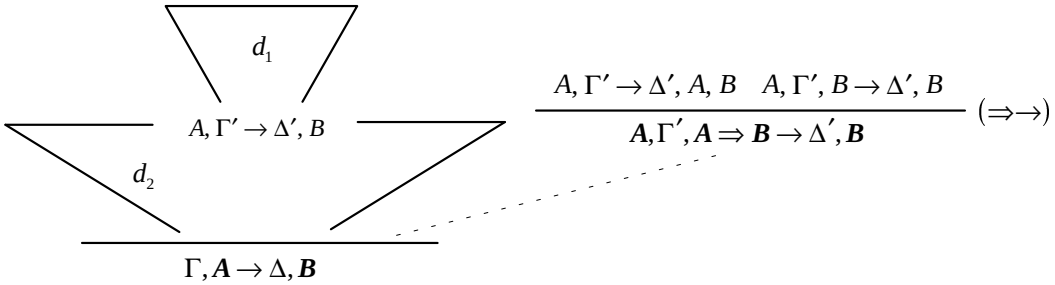
Juhtum 2 (jäetakse tõestada lugejal).

Juhtum 3. Esitame teisenduse graafiliselt.

Tuletuspuu enne teisendust:



ja pärast teisendust:



kus $d_2 = d \cdot [A \longrightarrow B]$.

Juhtumite 4, 5 ja 6 tõestused jäetakse lugejale harjutusülesanneteks.

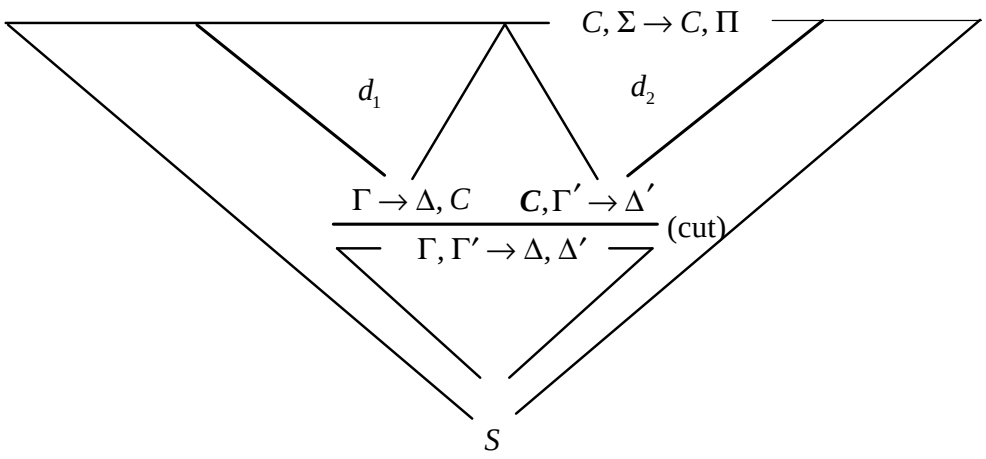
Lemma 2.

Kui $\vdash^{(0,F\cup\{C\})} S$, *siis* $\vdash^{(0,F)} S$.

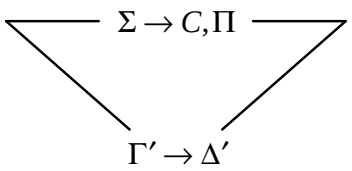
Tõestus.

Sekventsi S tuletus võib sisaldada mitut lõikereeglit astakuga 0. Valime neist kõige ülemise", s.o. sellise, mille eeldused on tuletatud ilma lõikereeglita. Väljavalitud lõike korral lõigatav reegel olgu C. Et lemma eeldustel on lõike astak 0, saab valemi tuletada vaid aksioomist. Seega on konstruktsioon, mis teisendab tuletuse $\vdash^{(0,F\cup\{C\})} S$ tuletuseks $\vdash^{(0,F)} S$, järgmine.

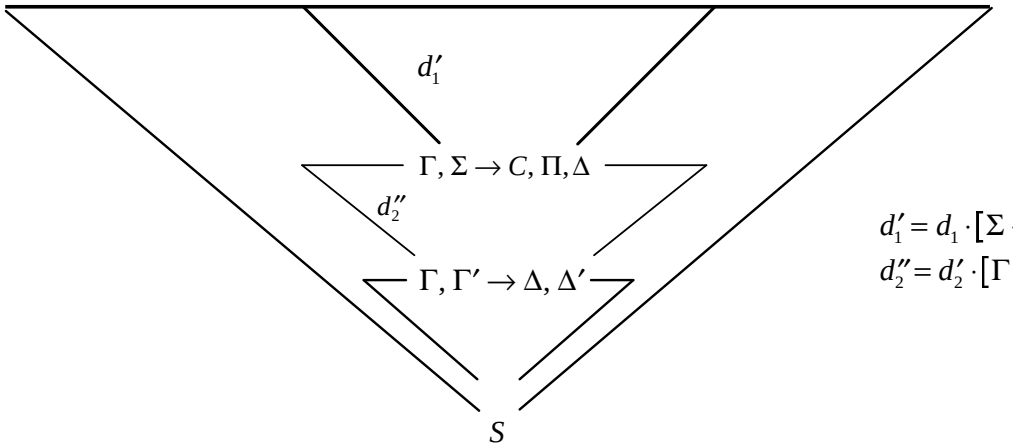
Tuletuspuu enne teisendust...



kus d_2':



... ja pärast:



$d_1' = d_1 \cdot [\Sigma \to \Pi]$
$d_2'' = d_2' \cdot [\Gamma \to \Delta]$

Lemma 3.

Kui $\vdash^{(k,F \cup \{C\})} S$, *siis* $\vdash^{(k,F)} S$.

Tõestus.

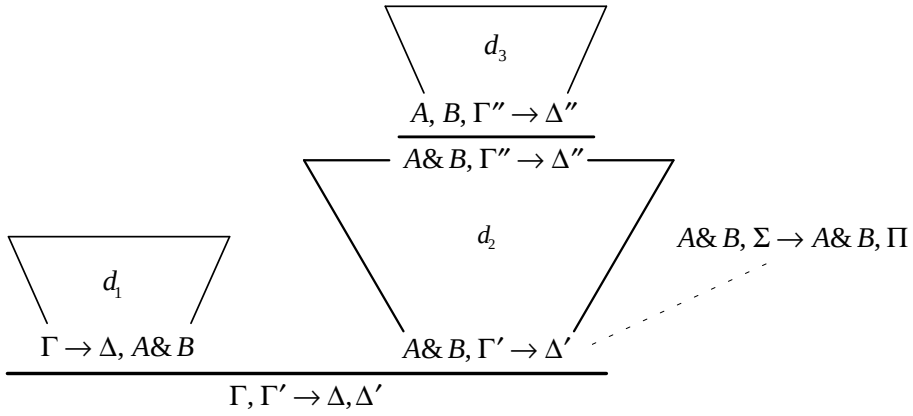
Kui $k = 0$, tuleneb väide otseselt lemmast 2.

Kui $k > 0$, tuleb vaadelda 6 juhtu: $C = A\&B$, $C = A \vee B$, $C = A \Longrightarrow B$, $C = \neg A$, $C = \exists x A$, $C = \forall x A$.

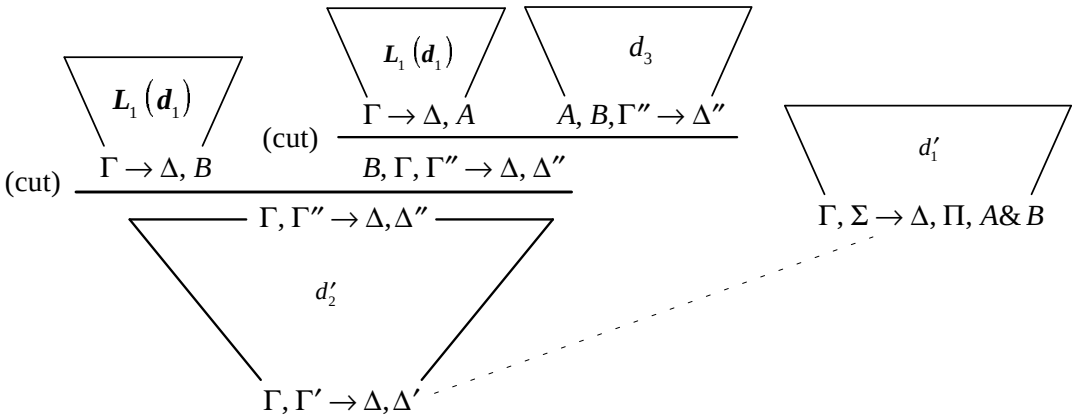
Esitame siin juhtude 1 ja 3 tõestused, jättes ülejäänud lugejale harjutusülesanneteks.

Juhtum 1: $C = A\&B$. Sekventsi S tuletuse alampuu, mille juureks on valemi C lõige, teiseneb järgmiselt.

Tuletuspuu enne teisendust...



... ja pärast teisendust:

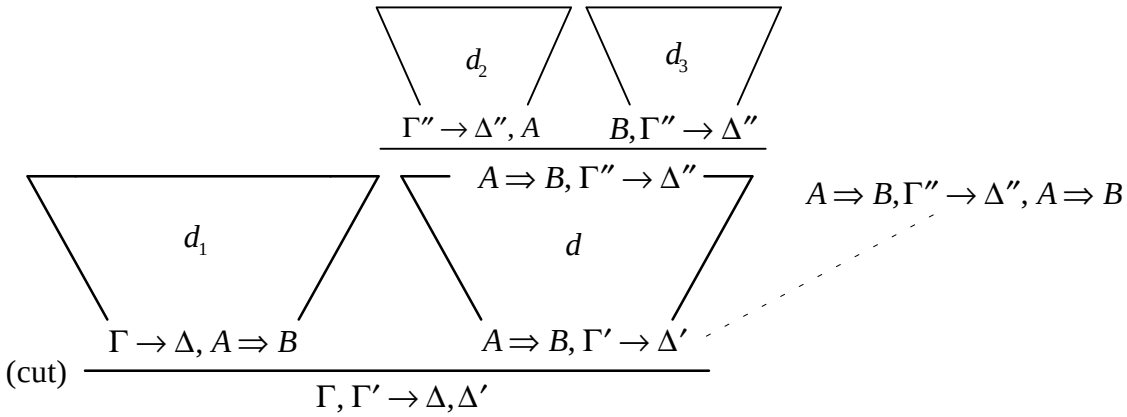


kus $L_1(d_1)$ tähistab puud, mis saadakse lemma 1 teisendusega puust d_1 :, d_2' on saadud d_2-st antetsedendis kõigi parameetriliste valemite $A\&B$ kustutamise ning seejärel sekventsiga $\Gamma' \longrightarrow \Delta'$ korrutamise tulemusena; $d_1' = d_1 \cdot [\Sigma \longrightarrow \Pi]$.

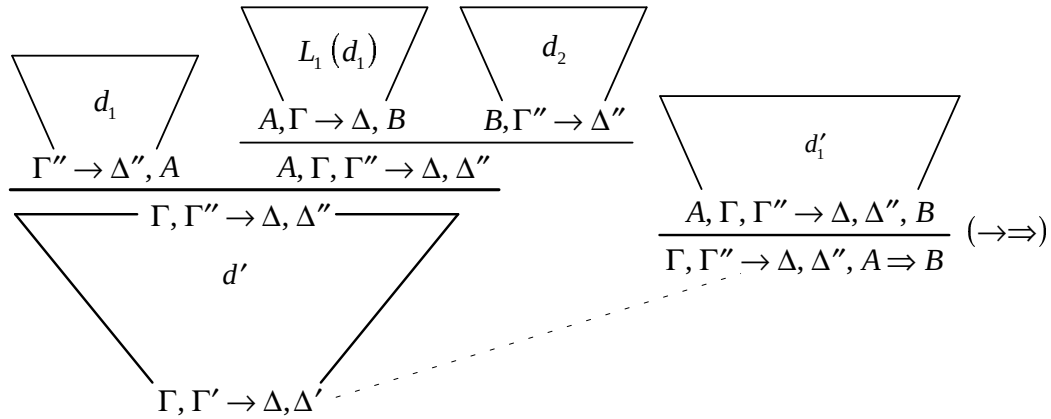
Teisenduse tulemusena saadud puus on üks lõige rohkem, kuid nende lõigete astak on väiksem kui k (lõigatavates valemites pole enam konjunktsiooni).

Juhtum 3: $C = A \Longrightarrow B$. Analoogselt eelmisega saab vaadeldavat lõiget sisaldavat alampuud teisendada järgmiselt.

Lähteseis:



tulemus:



kus d' on saadud tõestuse fragmendist d antetsedendist parameetrilise valemi $A \Longrightarrow B$ kustutamise ning sekventsiga $\Gamma \longrightarrow \Delta$ korrutamise teel; $d_1' = L_1(d_1) \cdot [\Gamma'' \longrightarrow \Delta'']$. Ülejäänud tähistused langevad kokku juhtumi 1 omadega.

Toodud lemmade põhjal saab tõestada ka lõike elimineerimise teoreemi (vt. lk. 19).

Oletame, et d on suvaline tuletus, milles k on maksimaalne lõike astak, F aga "lõigatavate" valemite hulk astakuga k. Järelikult on d (k, F)-tuletus.Kui $k > 0$, siis saab lemma 3 teisenduste kasutamisel lõplik arv kordi viia tuletuse kujule, milles lõigete maksimaalne astak ei ületa $k - 1$. Kui $k = 0$, saab lõplik arv kordi lemma 2 teisendust kasutades elimineerida kõik lõiked.

□

Järgnev näide illustreerib lõike elimineerimist valemi A tuletuses.

Näide 8. (Näite 7 jätk). Lõike elimineerimine valemi $A \equiv \exists x \forall y (P(x) \vee \neg\, P(y))$ tuletusest (lähtetuletus oli esitatud näites 7).

1. Asendame kõigepealt valemi $\exists x P(x) \vee \neg\ (\exists x P(x))$ lõike kahe lihtsama valemi lõikega:
   S_1 ja S_2 tähistavad näites 7 vastavate sekventside tuletusi.

$$\dfrac{\dfrac{\dfrac{\exists x\,P(x)\to\exists x\,P(x)}{\to\exists x\,P(x),\neg(\exists x\,P(x))}\;[Ax] \qquad S_1{:}\exists x\,P(x)\to A}{\to\exists x\,P(x),A} \qquad \dfrac{S_2{:}\to A,\exists x\,P(x)}{\neg(\exists x\,P(x))\to A}}{\to A}$$

2. Vastavalt lemmale 3 elimineerime suurima astakuga lõike, s.t. valemi $\neg\ (\exists x P(x))$ lõike:

$$\text{(cut)}\ \dfrac{S_2{:}\to A,\ \exists x\,P(x) \qquad \dfrac{[Ax{:}]\quad \exists x\,P(x)\to\exists x\,P(x)\quad S_1{:}\exists x\,P(x)\to A}{\exists x\,P(x)\to A}\ \text{(cut)}}{\to A}$$

Ülemise lõike võib nüüd ära jätta, kuna vasak eeldus on aksioom:

$$\dfrac{S_2 :\longrightarrow A,\exists x\,P(x) \qquad \dfrac{S_3 : P(a)\longrightarrow A}{\exists x P(x)\longrightarrow A}}{\longrightarrow A}$$

3. Elimineerime $\exists x P(x)$-lõike, asendades selleks sekventsis S_3 muutuja a muutujaga d. Tulemuseks saame tuletuse:

$$\dfrac{P(d)\longrightarrow A,\ P(c),\ P(d) \qquad S_5' : P(d)\longrightarrow A}{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(d)\longrightarrow A,\ P(c)}{\longrightarrow A, P(c),\neg\,P(d)}}{\longrightarrow A, P(c)\vee\neg\,P(d)}}{\longrightarrow A,\forall y(P(c)\vee P(y)}}{\longrightarrow A}}$$

4. Vastavalt lemmale 2 elimineerime viimase 0-astakuga lõike:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P\ (d)\longrightarrow A,\ P(d),\ \neg\,P(b),\ P(c)}{P(d)\longrightarrow A,\ P(d)\vee\ \neg\,P(b),\ P(c)}}{P(d)\longrightarrow A,\ \forall y(P(d)\vee\ \neg\,P(y)),\ P(c)}}{P(d)\longrightarrow A,\ P(c)}}{\longrightarrow A,\ P(c),\ \neg\,P(d)}}{\longrightarrow A,\ P(c)\vee\ \neg\,P(d)}}{\longrightarrow A,\ \forall y(P(c)\vee\ \neg\,P(y))}}{\longrightarrow A}$$

□

Lõike elimineerimist nimetatakse ka tuletuse **normaliseerimiseks**.

Sekventsiaalarvutuste tarvis on leitud mitmeid heuristilisi meetodeid normaliseeritud tuletuse vahetuks konstrueerimiseks, s.t. lõikereegli "vahepealse" kasutamiseta. Alljärgnevas esitame ühe sellise algoritmi, kus tuletus on konstrueeritud "alt-üles" meetodil, liikudes eesmärgilt (tuletatavalt sekventsilt) aksioomide suunas.

Algoritmi esitamiseks võtame kasutusele abitähistused.

S' ja S'' tähistagu sekventsi S eeldusi tuletusreeglis

$$\frac{S'}{S} \quad \text{või} \quad \frac{S' \quad S''}{S} \tag{7}$$

F_S, F'_S ja F''_S tähistagu vastavalt tuletusreeglite (7) pea- ja kõrvalliikmeid.

Kui on oluline rõhutada, et pealiige (kõrvalliige) asub antetsedendis, siis kasutame tähistuste F_S, F'_S ja F''_S asemel A_S, A'_S ja A''_S. Analoogiliselt pea- või kõrvalliikmete esinemisel suktsedendis olgu vastavad tähised S_S, S'_S ja S''_S.

Alljärgnev algoritm on kirja pandud PASCALile sarnases pseudokeeles. Muutuja L tähistab antud hetkel veel tõestamata sekventside nimistut. Algoritmi töö algab tuletatava sekventsi kirjutamisega nimistusse L. Järgnevas võetakse nimistust esimene element ning leitakse tuletusreegel, mille järelduseks vaadeldav sekvents võiks olla. Kui tuletusreegli eeldused pole aksioomid, lisatakse need nimistusse L. Kui algoritmi töö lõpeb nimist L tühjaks saamisega, on lähtesekvents tuletatav, vastasel juhul mitte. Nimistusse L jäävad need sekventsid, mida enam lihtsustada ei saa. Tähistagu S_1 järgnevas nimistu $L =< S_1, S_2, \ldots, S_n >$ esimest elementi, tehted $L - S_1$ ja $L + S$ aga vastavalt esimese liikme eemaldamist nimistust ja elemendi S lisamist nimistu lõppu.

Juhime veel tähelepnu, et **case**-lause on deterministlik, s.t. alternatiive vaadeldakse nende kirjutamise järjekorras ning i-s alternatiiv tuleb vaatluse alla vaid juhul, kui kõigi eelnevate alternatiivide rakendamise tingimused pole rahuldatud. Seega annab algoritm reeglite järjestuse (heuristika) - milliseid reegleid eelistada juhul, kui antud sekventsis on võimalik valida mitme reegli rakendamise vahel.

Algoritm {tuletuse ehitamine arvutuses $G4$}

Input: sekvents S

Method:

(1) $L :=< S >$
(2) **while** $L \neq <>$ **do**
$\{L =< S_1, S_2, \ldots, S_n >\}$
case S_1 **of**
axiom: $L := L - S$;
$F_{S_1} = A \vee B$, $F_{S_1} = A\&B$, $F_{S_1} = A \Longrightarrow B$:
$\{S'_1$ ja S''_2 leidmiseks kasutatakse vastavalt reegleid
$(\vee \longrightarrow), (\longrightarrow \vee), (\& \longrightarrow), (\longrightarrow \&), (\Longrightarrow \longrightarrow)$ või $(\longrightarrow \Longrightarrow)\}$
$L := (L - S_1) + S'_1 + S''_1$;
$F_{S_1} = \neg A$:
$\{S'_1$ leidmiseks kasutatakse reegleid$(\neg \longrightarrow)$ või $(\longrightarrow \neg)\}$
$A_{S_1} = \exists x A(x)$, $S_{S_1} = \forall x A(x)$:
$\{S'_1$ leitakse reeglite$(\exists \longrightarrow)$ või $(\longrightarrow \forall)$ abil,
kusjuures tuuakse sisse uus muutuja b,
mis ei esine pealiikmega samas sekventsis$\}$
$L := (L - S_1) + S'_1$;
$S_{S_1} = \exists x A(x)$, $S_{S_1} = \forall x A(x)$:
$\{S'_1$ leitakse reeglite $(\longrightarrow \exists)$ või $(\forall \longrightarrow)$ abil,
sisse tuuakse term $t\}$
$L := (L - S_1) + S'_1$
else
stop ('S pole tuletatav')
(3) **stop** ('S on tuletatav')
end.

Paneme tähele, et esitatud algoritm ei kasuta lõikereeglit (Cut). Järgnevas (vt. ptk.5) selgub, et see pole algoritmi määramispiirkonda kitsendav, sest iga lõikereeglit kasutava tuletuse saab asendada ekvivalentse "lõikevaba" tuletusega.

Näide 9. Tuletada valem $\exists x \forall y P(x,y \Longrightarrow \forall y \exists x P(x,y)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a,b), \forall y P(a,y) \to P(a,b), \exists x P(x,b)}{P(a,b), \forall y P(a,y) \to \exists x P(x,b)}\ (\to \exists)}{\forall y P(a,y) \to \exists x P(x,b)}\ (\forall \to)}{\forall y P(a,y) \to \forall y \exists x P(x,y)}\ (\to \forall)}{\exists x \forall y P(x,y) \to \forall y \exists x P(x,y)}\ (\exists \to)}{\to \exists x \forall y P(x,y) \,/\Rightarrow \forall y \exists x P(x,y)}\ (\to \Rightarrow)$$

□

Näide 10. Näidata, et valemil $(p \Longrightarrow q) \Longrightarrow (\neg\, p \longrightarrow \neg\, q)$ puudub tuletus.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{q \longrightarrow p, p}{\longrightarrow \neg q, p, p}\ \text{(ei ole aksioom)}}{\neg p \longrightarrow \neg q, p}}{\longrightarrow (\neg p \Longrightarrow \neg q), p} \qquad q \longrightarrow (\neg p \Longrightarrow \neg q)}{(p \Longrightarrow q) \longrightarrow (\neg p \Longrightarrow \neg q)}}{\longrightarrow (p \Longrightarrow q) \Longrightarrow (\neg p \Longrightarrow \neg q)}$$

□

Ülesanne 5. *Leida järgmiste valemite tuletused (kui võimalik).*

a) $(p \& (p \Longrightarrow q)) \Longrightarrow q$
b) $a \vee \neg a$
c) $(p \Longrightarrow q) \Longrightarrow (\neg q \Longrightarrow \neg p)$
d) $\exists x(A(x) \Longrightarrow B(x)) \Longrightarrow (\forall x A(x) \Longrightarrow \exists x B(x))$
e) $(\forall x(A(x) \vee \forall x B(x)) \Longrightarrow \forall x(A(x) \vee B(x))$
f) $\exists x \forall y P(x,y) \Longrightarrow \forall y \exists x P(x,y)$
g) $(p \Longrightarrow q) \Longrightarrow (\neg p \Longrightarrow \neg q)$
h) $\forall x(A \Longrightarrow B) \Longrightarrow (\forall x A \Longrightarrow \forall x B)$
i) $\forall x(A \Longrightarrow B) \Longrightarrow (\exists x A \Longrightarrow \exists x B)$
j) $\forall x A \Longleftrightarrow \neg \exists x \neg A$

Ülesanne 6. *(Näidata, et tuletusreeglid* $\longrightarrow \Longrightarrow), (\&\ \longrightarrow) ja (\longrightarrow\ \forall)$ *on pööratavad. See tähendab, et reegli* $(\longrightarrow \Longrightarrow)$ *asemel võib kasutada ka reeglit*

$$\dfrac{\Gamma \longrightarrow \Delta, A \Longrightarrow B}{\Gamma, A \longrightarrow \Gamma, B}.$$

Ülesanne 7. *Näidata, et arvutuses G4 tuletatavate valemite hulk langeb kokku peatükis 3 esitatud predikaatarvutuses tuletatavate valemitega.*

5. Herbrand'i teoreem

Sekventsiaalarvutuse eelisteks on tuletuste suhteline lihtsus, samuti asjaolu, et neid saab kergesti laiendada ka teistele loogika arvutustele. Puudusteks tuleb aga märkida tuletuspuude suurt mahtu ja raskusi kvantorreeglite rakendamisel (asendamiseks sobivate termide leidmisel). Loetletud puudustest aitab üle saada järgnevas toodav Herbrand'i teoreem.

Herbrand'i teoreem lubab kvantoreid sisaldavate sekventside tuletused asendada lihtsamate (ilma kvantoriteta) sekventside tuletustega. Kõigepealt vaatame tulemuse valemite üldkuju jaoks Herbrand'i teoreemi erikujuliste valemite korral, seejärel üldistame tulemuse.

5.1. Erijuht

Käsitleme sekventsi

$$\forall x_1 \forall x_2 \ldots \forall x_p A(x_1, x_2, \ldots, x_p) \longrightarrow \exists x_1 \exists x_2 \ldots \exists x_q B(y_1, y_2, \ldots, y_q).$$

Kasutades lühendust, võib selle sekventsi esitada ka kujul

$$\forall \underline{x} A(\underline{x}) \longrightarrow \exists \underline{y} B(\underline{y}), \tag{8}$$

kus $\underline{x}$ ja $\underline{y}$ tähistavad vastavalt vektoreid $(x_1, \ldots, x_p)$ ja $(y_1, \ldots, y_q)$. Eeldame, et valemid $A(\underline{x})$ ja $B(\underline{y})$ ei sisalda kvantoreid.

Lihtne on veenduda, et igasuguste termidest moodustatud vektorite $\underline{t}_1, \underline{t}_2, \ldots$ korral saab tuletada sekventsi $\forall \underline{x} A(\underline{x}) \longrightarrow A(\underline{t}_1), A(\underline{t}_2), \ldots$. Sekventsi (8) tõestamiseks tuleb leida termide vektor $\underline{u}_1, \ldots, \underline{u}_k$, nii et vabalt valitud valemitest $A(\underline{t}_1)$ järelduks valem $B(\underline{u}_1) \vee \ldots \vee B(\underline{u}_k)$. Loomulik oleks termid $\underline{t}_1, \ldots, \underline{u}_1, \ldots, \underline{u}_k$ koostada sekventsi (8) koosseisu kuuluvatest funktsioonisümbolitest ja konstantidest.

Definitsioon 2. *Sekventsi (8)* Herbrand'i universumiks *nimetatakse termide hulka, mis on moodustatud sekventsi (8) konstantidest ja funktsioonisümbolitest. Kui sekventsis (8) konstante pole, võetakse kasutusele konstant* 0.

Sekventsi S Herbrand'i universumit tähistatakse sümboliga U_S (kohtades, kus see ei tekita arusaamatusi, tähistab U_A sekventsi $\longrightarrow A$ Herbrand'i universumi, kusjuures räägime valemi A universumist).

Herbrand'i universumi moodustamiseks tuleb konstrueerida hulk H_∞ vastavalt järgmisele eeskirjale:

H_0 - sekventsi koosseisu kuuluvate indiviidkonstantide hulk või $\{0\}$;
$H_{I+1} H_i \cup \{f(t_1, \ldots, t_n) \mid t_j \in H_i$, f on sekventsis (8) esinev n-kohaline funktsioonisümbol$\}$.

Näide 11. Leida sekventsi $\longrightarrow \forall x \exists x (P(f(x), a) \Longrightarrow Q(g(y), b)$ Herbrand'i universum.

$H_0 = (a, b)$
$H_1 = \{a, b, f(a), f(b), g(a), g(b)\}$
$H_2 = \{a, b, f(a), f(b), g(a), g(b), f(f(a)), f(f(b)), f(g(a)), f(g(b)),$
$g(f(a)), g(f(b)), g(g(a)), g(g(b))\}$
.....
Antud juhul on Herbrand'i universum lõpmatu.

□

Definitsioon 3. *Sekventsi (8)* Herbrand'i arenduseks *nimetatakse sekventsi*

$$A(\underline{t}_1)\&A(\underline{t}_2)\&\ldots\&A(\underline{t}_m) \longrightarrow B(\underline{u}_1) \vee B(\underline{u}_2) \vee \ldots \vee B(\underline{u}_n),$$

kus termid $\underline{t}_1, \ldots, \underline{t}_m, \underline{u}_1, \ldots, \underline{u}_n$ *kuuluvad sekventsi (8) Herbrand'i universumisse.*

Näide 12. Vaatleme sekventsi

$$\forall x \forall y z \underbrace{\Big(\big((F(x,y)\&F(y,z)) \Rightarrow G(x,z)\big)\&F(i,a)\&F(j,i)\Big)}_{A(x,y,z)} \rightarrow \exists z\, G(j,z)$$

Juhul kui predikaati $F(x, y)$ interpreteerida kui "x on y isa" ja predikaati $G(x, y)$ kui "x on y vanaisa", esitab toodud valem väite, et kui isik i on a isa ja j on i isa, siis isikul j on lapselaps.

Kuna valemis ei kasutata funktsioone, on selle sekventsi universum lõplik: $U_S = \{a, i, j\}$. Ka Herbrand'i arenduste hulk on lõplik, koosnedes 27 erinevast elemendist. Maksimaalne arendus on

$$A(a,a,a)\&A(a,a,i)\&\ldots\&A(j,j,j) \longrightarrow G(j,a) \vee G(j,i) \vee G(j,j),$$

aga Herbrand'i arenduseks on ka sekvents

$$A(j,i,a) \longrightarrow G(j,a).$$

Mõlemad toodud Herbrand'i arendused on tuletatavad.

□

Näide 13. Valemi $\exists x(\neg P(x) \vee P(f(x))$ Herbrand'i universum on

$$U = \{0,\ f(0),\ f(f(0)),\ f(f(f(0))), \ldots\}.$$

Järelikult on lõpmatu ka arenduste hulk:

$$\begin{aligned} A = \{&\neg P(0) \vee P(f(0)),\ (\neg P(0) \vee P(f(0))) \vee (\neg P(f(0)) \vee P(f(f(0)))),\\ &(\neg P(0) \vee P(f(0))) \vee (\neg P(f(0)) \vee P(f(f(0)))) \vee (\neg P(f(f(0))) \vee\\ &\vee P(f(f(f(0))))), \ldots\}. \end{aligned}$$

□

Märkigem, et teine element hulgas A on tuletatav valem.

Teoreem 2. *(Herbrand'i teoreemi lihtsam juht).*

Sekvents $\forall \underline{x} A(\underline{x}) \longrightarrow \exists \underline{y} B(\underline{y})$ *on tuletatav parajasti siis, kui leidub tema Herbrand'i arendus*

$$\&_{i \le n} A(\underline{t}_i) \longrightarrow \vee_{j \le m} B(\underline{u}_j),$$

mis on tuletatav.

Tõestus. (Tarvilikkus). Olgu tõestatav valem

$$\forall \underline{x} A(\underline{x}) \longrightarrow \exists \underline{y} B(\underline{y}). \tag{9}$$

Sekvents

$$\&_{i \le n} A(\underline{t}_i) \longrightarrow \vee_{j \le m} B(\underline{u}_i)$$

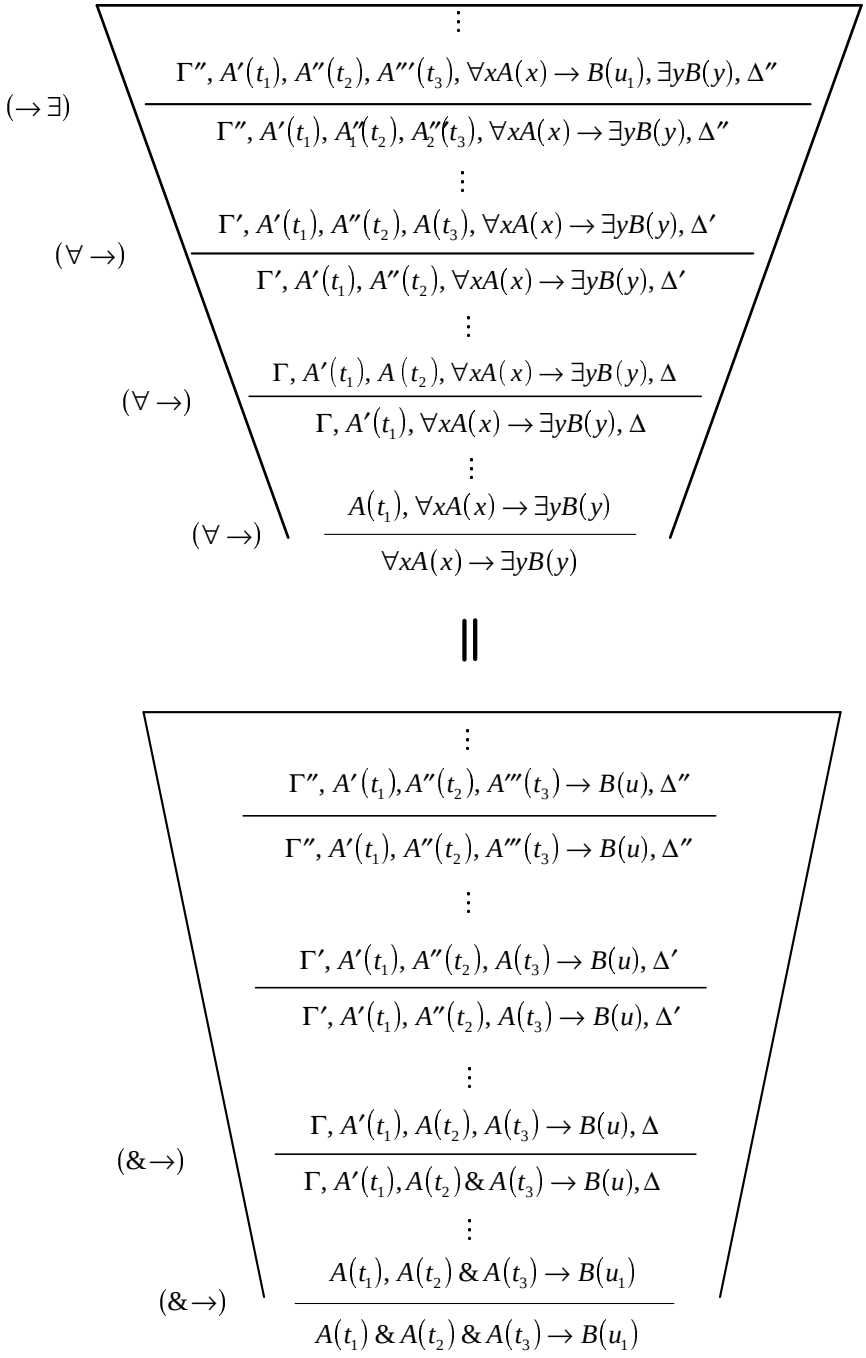
on saadav sekventsi (9) tuletusest, kui asendada tuletusreegite ($\forall \longrightarrow$) ja ($\longrightarrow \exists$) esinemised vastavalt reeglitega ($\& \longrightarrow$) ja ($\longrightarrow \vee$).

Selline teisendus annab sekventsi (9) tuletuse vaid siis, kui tuletuses pole kasutatud lõikereeglit.

Vaata ka kirjeldatud tuletuste teisenduse näidet (näide 14). (Piisavus ilma tõestuseta).

Näide 14. Sekventsi $\forall x A(x) \longrightarrow \exists y B(y)$ tuletuse teisendamine sekventsi $A(t_1)\&A(t_2)\&A(t_3) \longrightarrow B(u_1)$ tuletuseks.

□



Näide 15. Valem $\forall x P(x, f(x)) \longrightarrow \exists y P(f(y), y)$ pole tuletatav. Oletame vastuväiteliselt, et toodud valem on tuletatav. Siis peab vastavalt Herbrand'i teoreemile olema tuletatav selle valemi mingi Herbrand'i arendus $\&_i P(t_i, f(t)) \longrightarrow \vee_j P(f(u_j), u_j)$, kus t_i ja

u_i on termid. Selline tuletus peaks aga lõppema aksioomidega kujul, kus $P(t, f(t)) = P(f(u), u)$, mille korral $t = f(t)$. See pole aga võimalik ja seega ei saa ka lähtesekventsi tuletada.

Järeldus 5. *Sekvents kujul*

$$\forall \underline{x}_1 A_1(\underline{x}_1), \ldots, \forall \underline{x}_n A(\underline{x}_n) \longrightarrow \exists \underline{x}_1 B_1(\underline{y}_1), \ldots, \exists \underline{y}_m B_m(\underline{y}_m)$$

on tuletatav parajasti siis, kui on tuletatav tema mingi Herbrand'i arendus

$$A_1(\underline{t}_{11}), \ldots, A_1(\underline{t}_{1k_1}), \ldots, A_n(t_{nk_n}) \longrightarrow B_1(\underline{u}_{11}), \ldots, B_m(\underline{u}_{mk_m}).$$

5.2. Skolemiseerimine

Definitsioon 4. *Kaks sekventsi on* deduktiivselt võrdsed, *kui ühe tuletatavusest järeldub teise tuletatavus ja vastupidi.*

Teoreem 3. *Sekvents $\forall x \exists y A(x, y) \longrightarrow G$ on tuletatav parajasti siis, kui on tuletatav sekvents $\forall \underline{x} A(\underline{x}, f(\underline{x})) \longrightarrow G$, kus f on uus funktsioonisümbol ja G suvaline valem.*

Tõestus. (Tarvilikkus).

Eeldame, et sekvents $\forall \underline{x} \exists y A(\underline{x}, y) \longrightarrow G$ on tuletatav, s.t. leidub vastav tuletuspuu D. Sekventsi $\forall x A(\underline{x}, f(\underline{x})) \longrightarrow G$ tuletus on siis konstrueeritav lõikereegli abil:

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall \underline{x} A(\underline{x}, f(x)), A(\underline{a}, f(\underline{a})), \Gamma \to \exists y A(\underline{a}, y), A(\underline{a}, f(\underline{a}))}{\forall \underline{x} A(\underline{x}, f(x)), A(\underline{a}, f(\underline{a})), \Gamma \to \exists y A(\underline{a}, y)}(\to \exists)}{\forall \underline{x} A(\underline{x}, f(\underline{x})) \to \exists y A(\underline{a}, y)}(\forall \to)}{\forall \underline{x} A(\underline{x}, f(\underline{x})) \to \forall \underline{x} \exists y A(\underline{x}, y)}(\to \forall) \qquad \begin{array}{c} \triangledown \\ D \\ \forall \underline{x} \exists y A(\underline{x}, y) \to G \end{array}}{\forall \underline{x} A(\underline{x}, f(\underline{x})) \to G}$$

(Piisavust siinkohal ei tõesta).

Viimati vaadeldud teoreem lubab antetsedenti kuuluva valemi algusest ühe eksistentsikvantori "ära jätta". Rakendades toodud teoreemi korduvalt, võib iga valemi sekventsi antetsedendis viia kujule, kus kasutatakse vaid üldsuskvantoreid. Iga eliminеeritava eksistentsikvantori jaoks tuuakse valemisse uus k-kohaline funktsioonisümbol f, kus k on lähtevalemis antud eksistentsikvantorile eelnevate üldsuskvantorite arv. Eksistentsikvantoriga seotud muutuja asemele substitueeritakse aga valemisse term $f(x_1, \ldots, x_k)$, kus $x_1, \ldots, x_n$ on eelnevate üldsuskvantoritega seotud muutujad. Valemi muutmist sekventsi antetsedendis kirjeldatud viisil nimetatakse valemi *skolemiseerimiseks* (teisendust uurinud Rootsi loogiku Th. Skolemi nime järgi).
Näiteks sekventsi

$$\exists x \forall y \forall z \exists u \exists t \forall r (P(a, x, f(z)) \Longrightarrow Q(u, y, f(t), r)) \longrightarrow G$$

skolemiseerimisel saadakse

$$\forall y \forall z \forall r (P(a, b, f(z)) \Longrightarrow Q(g(y, z), y, f(h(y, z)), r)) \longrightarrow G.$$

(Põhjendage viimase teisenduse vastavust eelpool toodud teoreemile!)

Järeldus 6. *Sekventsid $A \longrightarrow G$ ja $S[A] \longrightarrow G$, kus $S[A]$ tähistab valemi A skolemiseerimise tulemust, on deduktiivselt võrdsed.*

5.3. Herbrand'i teoreemi üldjuht

Teoreem 4. *Sekventsid* $\longrightarrow \exists \underline{x} \forall y A(\underline{x}, y)$ *ja* $\longrightarrow \exists x A(\underline{x}, f(\underline{x}))$ *on deduktiivselt võrdsed.*

Tõestus. (Tarvilikkus).

Kasutades lõikereeglit saab ehitada järgneva tuletuse. Eeldatakse, et D on sekventsi $\longrightarrow \exists \underline{x} \forall y A(\underline{x}, y)$ tuletus.

$$\dfrac{\dfrac{D}{\rightarrow \forall y \exists \underline{x} A(\underline{x}, y)} \qquad \dfrac{\forall y \exists \underline{x} A(\underline{x}, y), \exists \underline{x} A(\underline{x}, f(\underline{x})) \rightarrow \exists \underline{x}(\underline{x}, f(\underline{x}))}{\forall y \exists \underline{x} A(\underline{x}, y) \rightarrow \exists (\underline{x}, f(\underline{x}))} \; (\forall \rightarrow)}{\rightarrow \exists \underline{x} A(\underline{x}, f(\underline{x}))}$$

(Piisavus).

Ülesanne 8. *Näidata, et sekventsid* $\neg(\exists \underline{x} A(\underline{x}, f(\underline{x}))) \longrightarrow$ *ja* $\forall \underline{x}(\neg A(\underline{x}, f(\underline{x}))) \longrightarrow$ *on deduktiivselt võrdsed.*

Vastavalt tuletusreeglile ($\neg \longrightarrow$) ja viimase ülesande lahendusele on deduktiivselt võrdsed sekventsid

$$\longrightarrow \exists \underline{x} A(\underline{x}, f(\underline{x}))$$

ja

$$\forall \underline{x} \neg A(\underline{x}, f(\underline{x}))) \longrightarrow G.$$

Teoreemi 3 põhjal on siis tuletatav ka sekvents

$$\forall \underline{x} \exists y (\neg A(\underline{x}, y)) \longrightarrow .$$

Harjutuse ja reegli ($\neg \longrightarrow$) põhjal on viimasega deduktiivselt võrdsed sekventsid

$$\neg \exists \underline{x} \exists \forall y A(\underline{x}, y) \longrightarrow$$

ja

$$\longrightarrow \exists \underline{x} \forall y A(\underline{x}, y).$$

Sekventsi suktsedendis oleva valemi skolemiseerimine on antetsedendi skolemiseerimise duaalne operatsioon: elimineeritakse üldsuskvantorid, kusjuures nende asemele tuuakse uued funktsioonisümbolid. Sekventsi, mille antetsedent ja suktsedent on skolemiseeritud, öeldakse olevat *skolemi normaalkujul*. Teoreemidest 2 ja 3 järeldub, et iga sekvents on deduktiivselt võrdne om skolemi normaalkujuga. Kuna skolemiseerimise tulemusena saadakse sekvents kujul (8), siis kehtib üldjuhul ka teoreem 1.

Kokkuvõttes saab iga valemi viia kujule, kus kvantorid on valemi ees (tõestada vastavad üleminekureeglid!):

$$Q_1 u_1, \ldots, Q_n u_n M, \tag{10}$$

kus $Q_1, \ldots, Q_n$ on kvantorid, $u_1, \ldots, u_n$ on muutujad ja M valem, milles ei sisaldu enam kvantoreid. Iga valemit (10) saab skolemi mõttes normaliseerida ning seejärel konstrueerida tema Herbrand'i arendusi. Neid arendusi nimetatakse ka lähtevalemi Herbrand'i arendusteks. Vastavalt eeltoodule kehtib üldine Herbrand'i teoreem.

Teoreem 5. *Sekvents $\Gamma \longrightarrow \Delta$ on tuletatav parajasti siis, kui leidub tema tuletatav Herbrand'i arendus.*

Näide 16. Kas valem $\exists x \forall y(\neg P(x) \vee P(y))$ on teoreem?

Viime sekventsi $\longrightarrow \exists \forall y(\neg P(x) \vee P(y)$ normaalkujule:

$$\longrightarrow \exists x(\neg P(x) \vee P(f(x))).$$

Normaalkuju on tuletatav, kuna on tuletatav tema Herbrand'i arendus $(\neg P(0) \vee P(f(0))) \vee (\neg P(f(f(0))))$. (Vt. ka näide 13).

□

6. Resolutsioonimeetod

Iga predikaatarvutuse (lausearvutuse) valem A on viidav nn. **disjunktiivsele normaalkujule** $A = B_1 \vee B_2 \vee \ldots \vee B_k$, kus osavalemid B_i on atomaarsete valemite konjunktsioonid: $B_i = L_{i_1} \& L_{i_2} \& \ldots \& L_{i_{n_i}}$. *Literaalideks* nimetatavad "tegurid" L_{i_j} on kas atomaarsed valemid ($A, B, \ldots, P(x), Q(x,y), \ldots$) või nende eitused ($\neg A, \neg B, \ldots, \neg P(x), \neg Q(x,y), \ldots$). Eitusmärgiga algavat literaali nimetatakse negatiivseks, ilma eitusmärgita literaali aga positiivseks literaaliks.

Lihtsaim viis valemi teisendamiseks disjunktiivsele normaalkujule on kasutada samasusi:

$$A \Longrightarrow B \Longleftrightarrow \neg A \vee B \tag{11}$$

$$A \& (C \vee D) \Longleftrightarrow (A \& C) \vee (A \& D) \tag{12}$$

$$\neg(A \vee B) \Longleftrightarrow (\neg A \& \neg B) \tag{13}$$

$$\neg(A \& B) \Longleftrightarrow (\neg A \vee \neg B) \tag{14}$$

$$\neg\neg A \Longleftrightarrow A \tag{15}$$

Ülesanne 9. *Tõestage samaväärsused (11) - (15).*

Ülesanne 10. *Tõestage, et juhul kui valemid E ja F on samaväärsed ($E \Longleftrightarrow F$ on tuletatav), on sekventsid $\Gamma \longrightarrow \Delta, A[x := E]$ ja $\Gamma \longrightarrow \Delta, A[x := F]$ deduktiivselt võrdsed.*

Seostest (11) - (15) ning ülesande 10 lahendusest järeldub, et valemiga A (s.t. sekventsiga $\longrightarrow A$) on deduktiivselt võrdsed järgmised sekventsid:

$\longrightarrow B_1 \vee \ldots \vee B_k$
$\neg(B_1 \vee \ldots \vee B_k) \longrightarrow$
$\neg B_1 \& \ldots \& \neg B_k \longrightarrow$
$\neg B_1, \ldots, \neg B_k \longrightarrow$
$\neg(L_{1_1} \& \ldots \& L_{1_{n_1}}, \ldots, \neg(L_{k_1} \& \ldots \& L_{k_{n_k}}) \longrightarrow$
$D_1, \ldots, D_k \longrightarrow$

Literaalide disjunktsiooni $D_i = \neg L_{i_1} \vee \ldots \vee \neg L_{i_{n_i}}$ nimetatakse *disjunktiks*.

Järeldus 7. *Igale valemile A saab vastavusse seada disjunktide hulga D_A, mis on vastuoluline parajasti siis, kui A on tuletatav.*

Näide 17. Leida valemile $A = (p \Longrightarrow q) \Longrightarrow (\neg p \Longrightarrow \neg q)$ vastav disjunktide hulk D_A.

Viime valemi A disjunktiivsele normaalkujule, kasutades valemi järgmisi vahekujusid:

$\neg(p \Longrightarrow q) \vee (\neg p \Longrightarrow \neg q)$	(seose (11) abil)
$\neg(\neg p \vee q) \vee (\neg\neg p \vee \neg q)$	(seose (11) abil)
$(\neg\neg p \& \neg q) \vee (\neg\neg p \vee \neg q)$	(seose (13) abil)
$(p \& \neg q) \vee (p \vee \neg q)$	(seose (15) abil)
$(p \& \neg q) \vee p \vee \neg q$	

Järelikult on sekventsiga $\longrightarrow A$ deduktiivselt võrdne sekvents

$$\neg(p\&\neg q),\ \neg p,\ \neg\neg q \longrightarrow,$$

mille lihtsustamisel vastavalt seostele (14) ja (15) saame ekvivalentsse sekventsi

$$\neg p \vee q,\ \neg p, q \longrightarrow .$$

Seega on otsitav disjunktide hulk $D_A = (\neg p \vee q,\ \neg p, q)$.

□

Valemile vastava sekventside hulga saab koostada ka asendusvõtet kasutades, s.t. tuues sisse uusi muutujaid. Nimetatud võtet illustreerib järgmine näide.

Näide 18. Leida valemile $((a \Longrightarrow b) \Longrightarrow a) \Longrightarrow a$ vastav disjunktide hulk, mis on vastuoluline parajasti siis, kui lähtevalem on tuletatav.

Võtame kasutusele uued muutujad x, y ja z, mis tähistavad valemi $((a \Longrightarrow b) \Longrightarrow a) \Longrightarrow a$ osasid, s.t nad on ekvivalentsed valemi teatud osadega:

$$\begin{array}{l} x \Longleftrightarrow (a \Longrightarrow b); \\ y \Longleftrightarrow (x \Longrightarrow a); \\ z \Longleftrightarrow (y \Longrightarrow a). \end{array}$$

Toodud asenduste tulemusel vastab muutuja z kogu valemile

$$((a \Longrightarrow b) \Longrightarrow a) \Longrightarrow a.$$

Seose (11) abil võib toodud samasused teisendada disjunktideks:

valem $x \Longleftrightarrow (a \Longrightarrow b)$ on samaväärne kolme disjunktiga:

$$\neg x \vee \neg a \vee b \qquad a \vee x \qquad \neg b \vee x;$$

valem $y \Longleftrightarrow (x \Longrightarrow a)$ on samaväŕne kolme disjunktiga:

$$\neg y \vee x \vee a \qquad x \vee y \qquad \neg a \vee y;$$

valem $z \Longleftrightarrow (y \Longrightarrow a)$ on samaväärne kolme disjunktiga:

$$\neg z \vee \neg y \vee a) \qquad y \vee z \qquad \neg a \vee z.$$

Kõigi loetletud 9 valemi konjunktsioon on tuletatav parajasti siis, kui valem z on tuletatav. Selleks et saada tuletatava valemi jaoks vastuoluline disjunktide hulk, lisame veel valemi $\neg z$. Järelikult võib disjunktide hulga D_z esitada kujul

$$D_z = (\neg z,\ \neg x \vee \neg a \vee b,\ a \vee x,\ \neg b \vee x,\ \neg y \vee \neg x \vee a,\ x \vee y,\ \neg a \vee y,\ \neg z \vee \neg y \vee a,\ y \vee z,\ \neg a \vee z).$$

□

Ülesanne 11. *1. Näidata, et $x \Longleftrightarrow p\&q$ asendusele vastav disjunktide hulk on $(\neg x \vee p,\ \neg x \vee q,\ \neg p \vee \neg q \vee x)$.*

2. Näidata, et $x \Longleftrightarrow p \vee q$ asendusele vastav disjunktide hulk on $(\neg x \vee p \vee q,\ \neg p \vee x,\ \neg q \vee x)$.

3. Näidata, et $x \Longleftrightarrow \neg p$ asendusele vastav disjunktide hulk on $(\neg x \vee \neg p,\ \neg x \vee p)$.

Disjunktide hulga D_A vastuolulisuse tõestamiseks võib kasutada järgmist *resolutsioonireegliks* nimetatavat tuletusreeglit

$$\frac{A \vee L \qquad \neg L \vee B}{A \vee B}\ (Rp)$$

Resolutsioonireegel on kooskõlas predikaatarvutuse tuletusreeglitega, kuna sekvents $A \vee L, \quad \neg L \vee B \longrightarrow A \vee B$ on tuletatav (Kontrollige!).

Tähistagu avaldis $X \vdash C$ asjaolu, et disjunkt C on tuletatav disjunktide hulgast X ning loogilistest aksioomidest (disjunktidest, mis sisaldavad literaale L ja $\neg L$) resolutsioonireegli (Rp) abil.

Teoreem 6. *Olgu D_A valemile A vastavate disjunktide hulk. Valem A on teoreem parajasti siis, kui $D_A \vdash \emptyset$, kus $\emptyset$ tähistab tühja disjunkti.*

Tõestus.

Eelnevas nägime, et hulk D_A on vastuoluline parajasti siis, kui sekvents $\longrightarrow A$ on tuletatav. Seega on valem A teoreem parajasti siis, kui on tuletatav sekvents $D_A \longrightarrow$.

Näitame, et leidub üksühene kujutus, mis teisendab sekventsi $X, Y \longrightarrow Y'$ tuletuse resolutsioonimeetodil teostatud tuletuseks $X \vdash \neg Y \vee Y'$, kus X on disjunktide hulk, Y ja Y' on literaalide nimistud ja $\neg Y \vee Y'$ on disjunkt, mis sisaldab vaid nimistu Y elementide eitusi ning nimistu Y' literaale ja ainult neid. Sellest tulemusest järeldub teoreem 5, juhul kui Y ja Y' on tühjad nimistud.

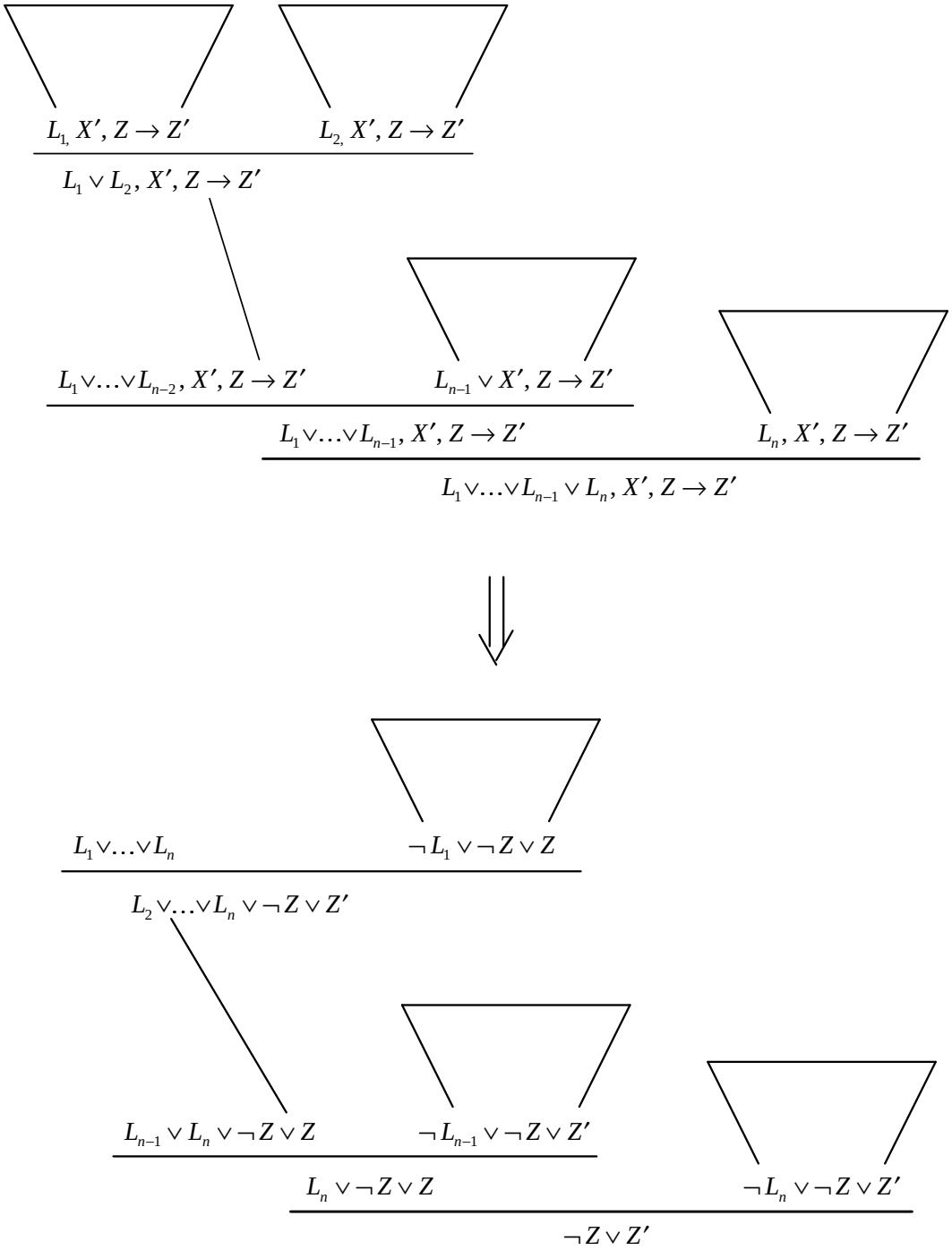
Sekventsi $X, Y \longrightarrow Y'$ tuletus saab sisaldada vaid sekventse kujul $X_1, Z \longrightarrow Z'$, kus X_1 on disjunktide hulga X alamhulk ja Z ja Z' on aatomite loetelud. Asendame kõik selliste sekventside tuletused resolutsioonimeetodil teostatud tuletusega $X_1 \vdash \neg Z \vee Z'$. Asenduse korrektsuse tõestame induktsiooni abil:

Baas. $X_1 = \emptyset$. Siis peab sekvents $Z \longrightarrow Z'$ olema aksioom, kuna ainult aatomeid sisaldavaid sekventse ei saa enam lihtsustada. Järelikult sisaldavad Z ja Z' vähemalt ühe ühise valemi ning disjunkt $Z' \vee \neg Z$ on resolutsioonimeetodi jaoks aksioom.

Samm. Oletame, et $X_1, \ Z \longrightarrow Z'$ ning $X_1 \vdash \neg Z \vee Z'$ on samaaegselt tuletatavad, kui hulk X_1 sisaldab vähem kui k elementi. Kui X_1 sisaldab täpselt k disjunkti, tuleb käsitleda 2 juhtu.

Esiteks: $X_1 = \{L_1, \ldots, L_n\} \cup X'$. Siis sekventside $L_1, X', Z \longrightarrow Z', \ldots, L_N, X', Z \longrightarrow Z'$ tuletatavusest järeldub tuletuste $X' \vdash \neg L_1 \vee \neg Z \neg Z', \ldots, X' \vdash \neg L_n \vee \neg Z \vee Z'$ korrektsus.

Seega annab järgnev teisendus korrektse tuletuse:



Teiseks: $X_1 = \{\neg p\} \cup X'$ korral on vastav asendus:

$$\dfrac{X', Z \to Z', p}{\neg p, X', Z \to Z'}$$

$$\Downarrow$$

$$\dfrac{\neg p\ \neg Z \vee Z' \vee p}{\neg Z \vee Z'}$$

□

Näide 19. Tõestame, et näites 18 esitatud disjunktide hulk on vasturääkiv ja seega valem $((a \Longrightarrow b) \Longrightarrow a) \Longrightarrow a$ tuletatav.

$$\dfrac{\dfrac{\dfrac{\dfrac{a \vee x \qquad\qquad a \vee y \vee \neg x}{a \vee \neg y} \qquad \neg a \vee z}{z \vee \neg y} \qquad y \vee z}{z} \qquad \neg z}{\emptyset}$$

□

Valemite unifitseerimine.

Substitutsiooniks nimetame asendust kujul $s = \{x_1 := t_1, \ldots, x_n := t_n\}$, kus $x_1, \ldots, x_n$ on paarikaupa erinevad muutujad ja $t_1, \ldots, t_n$ on termid, mis ei sisalda muutujat x_i, $(i = 1, 2, \ldots, n)$.

Kui s on substitutsioon, siis Es tähistab avaldist, mis on saadud avaldisest E kõigi vabade muutujate $x_1, \ldots, x_n$ samaaegsel asendamisel termidega $t_1, \ldots, t_n$. Avaldist Es nimetatakse avaldise E **näiteks**.

Olgu $s = \{x_1 := t_1, \ldots, x_n : t_n\}$ ja $r = \{y_1, \ldots, y_m := d_m\}$ asendused. Asenduste s ja r *kompositsiooniks* nimetame asendust

$$s \circ r = \{x_1 := t_1 r, \ldots, x_n := t_n r,\ y_1 := d_1, \ldots, y_m := d_m\},$$

millest on kustutatud elemendid, kus $x_i = t_i r$ ja elemendid $y_i := d_i$, mille korral $y_i \in \{x_1, \ldots, x_n\}$. Asenduste s ja r korral

$$E(s \circ r) = (Es) \circ r.$$

Näide 20. Olgu $s = \{z := f(y),\ y := z\}$ ja $r = \{x := a,\ y := b,\ z := y\}$.

Kompositsioon on seega

$$s \circ r = \{z := f(b),\ x := a\} = \{z := f(b),\ x := a\}.$$

□

Definitsioon 5. *Asendust s nimetatakse hulga $W = \{E_1, \ldots, E_n\}$* unifikaatoriks, *kui $E_1 s = \ldots = E_n s$. Avaldiste hulk W on unifitseeritav, kui sellel hulgal leidub unifikaator. Asendus s on avaldiste hulga W üldiseim unifikaator, kui iga unifikaatori v jaoks leidub asendus r, nii et $v = s \circ r$.*

Üldisema unifikaatori leidmise algoritm.

Vaatleme mittetühja valemite hulga elementide sümboleid alates esimesest. Fikseerime positsiooni, milles avastame esimese erinevuse. Moodustame hulga, mis sisaldab fikseeritud positsioonist algavad vähimad alamavaldised ja ainult need. Sellist avaldist nimetame *erinevuste hulgaks*. Näiteks valemite hulga

$$W = \{P(x, f(y, z)),\ \ P(x, a),\ \ P(x, g(h(k(x))))\}$$

elemendid erinevad alates viiendast positsioonist ja erinevushulgaks on

$$D = \{f(y,z), a, g(h(k(x)))\}.$$

Sümboliga e tähistame tühja asenduse.

Algoritm hulga V üldiseima unifikaatori leidmiseks.
IN: Valemite hulk V
OUT:

1. V on/ei ole unifitseeritav;
2. S on hulga V üldiseim unifikaator.

Meetod:

$S1.$ $k := 0$; $W_0 := V$; $s_0 := e$;
$S2.$ **if** $|W_k| = 1$ **then stop** (V on unifitseeritav, $s = s_k$);
$S3.$ **if** $|W_k| > 1$ **then** $D_k :=$ hulga W_k erinevushulk;
$S4.$ **if** $x_k \in D_k$ **and** $t_k \in D_k$ **and** $x_k \in t_k$
then goto $S5$
else stop (V ei ole unifitseeritav, e)
$S5.$ $s_{k+1} := s_k \cup \{x_k := t_k\}$; $W_{k+1} := W_k\{x_k := t_k\} = Vs_{k+1}$;
$S6.$ $k := k + 1$; **goto** $S2$.

Teoreem 7. *Kui avaldiste hulk V on lõplik ja unifitseeritav, lõpetab algoritm töö olekus $S2$.*

Ülesanne 12. *Leida hulga $W = \{P(a, x, f(g(y))),\ P(z, f(z),\ f(u))\}$ üldiseim unifikaator.*

Resolutsioonireegli üldjuht on

$$\frac{L \vee E \quad \neg L' \vee D}{(E \vee D)s}\ (R),$$

kus s on valemite L ja L' üldiseim unifikaator.

Valemite hulga X kõigi vabade muutujate sidumisel üldsuskvantoriga tekkivat hulka tähistatakse sümboliga $\forall X$.

Teoreem 8. *Olgu X disjunktide hulk. $\forall X$ on vastuoluline parajasti siis, kui $X \vdash \emptyset$, kasutades reeglit (R).*

Näide 21. Sekvents $\longrightarrow \exists x \forall y(P(x) \vee P(y))$ on deduktiivselt võrdne sekventsiga $\forall x P(x)$, $\forall y(\neg P(g(y))) \longrightarrow$ (Kontrollige!).

Valemite hulga vastuolulisus on tõestatav ühe reasolutsioonisammuga:

$$\frac{P(x) \quad \neg P(g(y))}{\emptyset},$$

kusjuures kasutatakse unifikaatorit $s = \{x := g(y)\}$.

□

Näide 22. Tõestada, et eeldustel

$$F1 : \forall x(C(x) \Longrightarrow (W(x) \& R(x))$$
$$F2 : \exists x(C(x) \& P(x))$$

kehtib valem

$$G : \exists x(P(x)\&R(x)).$$

On vaja tuletada sekvents

$$F1,\ F2 \longrightarrow G$$

ehk näidata, et hulk $D' = \{F1,\ F2,\ \neg G\}$ on vastuoluline. Teisendame hulga D' valemeid:

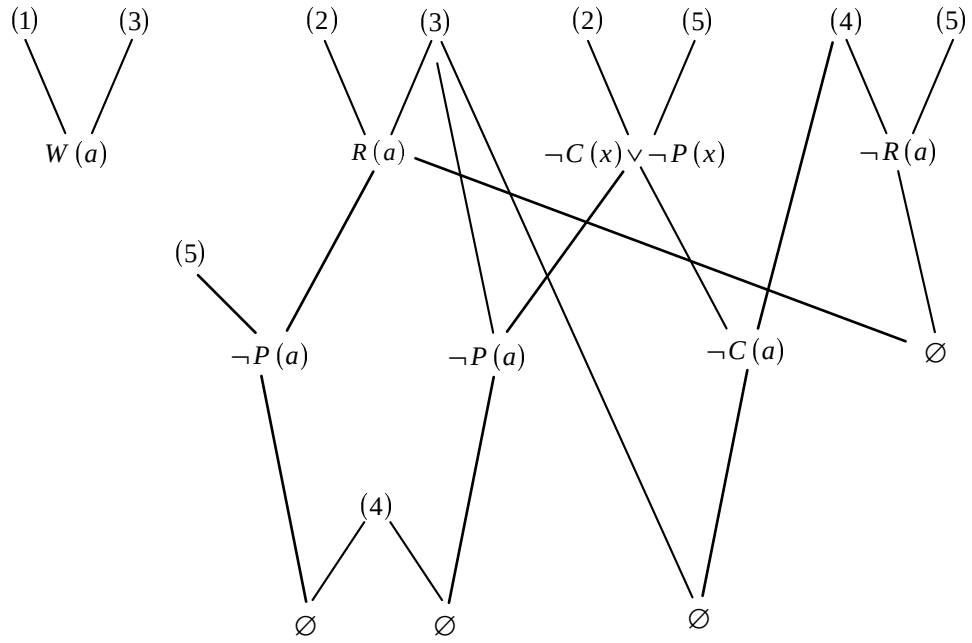
$$D'' = \Big\{ \underbrace{C(x) \Rightarrow \big(W(x)\&R(x)\big)}_{\text{(teisendus impl. jaoks)}},\quad \underbrace{\exists x\big(C(x)\&P(x)\big)}_{\text{(skolemiseerimine)}},\quad \underbrace{\forall x \neg \big(P(x)\&R(x)\big)}_{\text{(teisendus eituse jaoks)}} \Big\}$$

$$\neg C(x) \vee W(x),\quad \neg C(x) \vee R(x),\quad C(a),\quad P(a),\quad \neg P(x) \vee \neg R(x)$$

Järelikult on vaja tõestada järgmise disjunktide hulga vastuolulisus:

$$D = \{\underbrace{\neg C(x) \vee W(x)}_{(1)},\ \underbrace{\neg C(x) \vee R(x)}_{(2)},\ \underbrace{C(a)}_{(3)},\ \underbrace{P(a)}_{(4)},\ \underbrace{\neg P(x) \vee \neg R(x)}_{(5)}\}$$

Reegli (R) abil saab konstrueerida lõpliku hulga uusi disjunkte:



Nagu näha, saab tühja disjunkti tuletada mitmel viisil. Valemite hulga vastuolulisuse näitamiseks piisab tühja disjunkti ühe tuletuse leidmisest. Praktikas kasutatavad teoreemide tõestamise algoritmid läbivadki skeemi:

1. leida tuletatavale sekventsile S (valemile A) vastav disjunktide hulk $D := D_S$ ($D := D_A$);
2. seni kuni saab leida hulgal D uusi resolvente või kuni pole genereeritud tühja disjunkti, genereerida uus resolvent r ja $D := D \cup \{r\}$;
3. kui eelmine samm lõppes tühja disjunkti genereerimisega, on sekvents S tuletatav, vastasel juhul mitte.

□

Ülesanne 13. *(Tolliametnikud ja narkoäri).*

Olgu defineeritud järgmised predikaadid:

$S(x)$ - *riiki sõitis isik* x;
$V(x)$ - *isik* x *on* VIP;
$T(x)$ - x *on tolliametnik;*
$N(x)$ - x *on narkootikumidega kaubitseja;*
$L(x, y)$ - x *otsis läbi isiku* y.

On teada, et iga isik, kes pole VIP, *otsitakse läbi:*

$$F_1: \quad \forall x((S(x)\&\neg V(x)) \Longrightarrow \exists y(T(y)\&L(y,x)));$$

narkootikumidega kaubitseja võis maale pääseda vaid juhul, kui teda kontrollis narkoäri liige:

$$F_2 \quad \exists x(S(x)\&N(x)\&(\forall y(L(y,x) \Longrightarrow N(y))));$$

ükski VIP *ei kaubitse narkootikumidega:*

$$F_3 \quad \forall x(N(x) \Longrightarrow \neg V(x)).$$

Näidata, et leidub tolliametnik, kes tegeleb narkootikumide veoga, s.t. tuletada sekvents

$$F_1, F_2, F_3 \longrightarrow \exists x(T(x)\&N(x)).$$

Süsteem PROLOG (PROgramming in LOGic)

Programm PROLOG'is on nn. Horni lausete hulk:

$$A \longleftarrow B_1, \ldots, B_n \quad (n >= 0) \tag{16}$$

või

$$\longleftarrow B_1, \ldots, B_n \text{ ehk } B_1, \ldots, B_n \tag{17}$$

Horni laused esitavad vastavalt disjunkte:

(16) esitab disjunkti $A \vee \neg B_1 \vee \ldots \vee \neg B_n$

ja

(17) esitab disjunkti kujul $\neg B_1 \vee \ldots \vee \neg B_n$.

Uusi disjunkte tuletatakse PROLOG-süsteemis resolutsioonimeetodil, reegli (R) vaste, mis arvestab Horni lausete notatsiooni, on järgmine:

$$\frac{A' \longleftarrow Z \qquad A, X \longleftarrow}{(Z, X)s \longleftarrow} \tag{18}$$

kus (Z, X) on disjunktide hulkade Z ja X ühend ja s on hulga (A, A') üldiseim unifikaator.

Tüüpiline PROLOG-programm koosneb **väidetest** (Horni laused kujul $A \longleftarrow B_1, \ldots, B_n$) ja **eesmärgist** (lause kujul $\longleftarrow B$). Töö tulemusena kontrollib süsteem, kas eesmärk on antud väidete korral saavutatav, s.t. reegli (18) abil püütakse tuletada tühja disjunkti. Programmi väljund on *yes* (eesmärk on saavutatav) või *no* (eesmärk pole saavutatav), millele harilikult lisatakse info kasutatud unifitseerimiste kohta.

Näide 23. Horni lausetest

$G(x, z) \longleftarrow F(x, y), F(y, z)$ % vanaisa reegel
$F(i, a) \longleftarrow$ % i on a isa
$F(j, i) \longleftarrow$ % j on i isa

saab tuletada eesmärgi

$\longleftarrow G(j, z)$ % kas j-il on lapselapsi?

PROLOG-süsteemis oleks tuletus järgmine:

$$\dfrac{\dfrac{\dfrac{G(x,z) \leftarrow F(x,y), F(y,z) \qquad \leftarrow G(j,z)}{F(j,y), F(y,z) \leftarrow \qquad F(j,i) \leftarrow}}{F(i,z) \leftarrow \qquad F(i,a) \leftarrow}}{\varnothing}$$

$s_1 = \{x := j\}$
$s_2 = \{y := i\}$
$s_3 = \{z := a\}$

Seega on süsteemi vastus *yes* (j-il on lapselaps), kasutatav asendus $s = s_1 \circ s_2 \circ s_3 = \{x := j, y := i, z := a\}$. Viimast tuleb seose $G(x, z) \longleftarrow F(x, y), F(y, z)$ kohaselt interpreteerida järgmiselt: "j-i lapselaps on a".

□

Ülesanne 14. *Näidata, et näite 7 tingimustel i ei oma lapselapsi.*

7. Mudelite teooria

Seni vaatlesime valemite tuletamist kui süntaktilist teisendust. Küsimusele, milline on tuletatud valemi tähendus, me seni tähelepanu ei pööranud.

Matemaatilises loogikas käsitletakse valemi tähendust interpretatsiooni mõiste vahendusel. Valemeid võib interpreteerida erinevates keskkondades, s.t anda neile erinev semantika. Valemite interpreteerimise keskkonda nimetatakse loogikas *mudeliks*. Interpretatsioon seob valemis esinevate indiviidmuutujatega teatud hulga H elemendid, funktsioonisümbolitega operatsioonid hulgal H ja atomaarsete valemitega teatud suhteid hulga H elementide vahel. Teiste sõnadega, predikaatarvutuse valemeid interpreteeritakse alati mingil *algebralisel süsteemil*.

Definitsioon 6. Algebraliseks süsteemiks *nimetatakse struktuuri*

$$\mathcal{U} =< H; \Sigma >=< H; F_1, F_2, \ldots ; P_1, P_2, \ldots >,$$

kus

- H *on põhihulk e.* kandja*;*
- $F_1, F_2, \ldots$ *on vastavalt* $k_1-, k_2-, \ldots$ *-kohalised hulgal* H *kinnised funktsioonid (operatsioonid);*
- $R_1, R_2, \ldots$ *on vastavalt* $l_1-, l_2-, \ldots$ *-kohalised relatsioonid hulgal* H*.*

Algebralise süsteemi operatsioonide ja seoste tähiste hulka Σ nimetatakse algebralise süsteemi *signatuuriks*; korteeži $\tau =< k_1, k_2, \ldots ; l_1, l_2, \ldots >$ nimetatakse algebralise süsteemi *tüübiks*.

Definitsioon 7. *Algebralist süsteemi, mille signatuur sisaldab vaid operatsioone (s.t. mille tüüp on* $< k_1, k_2, \ldots ; >$*) nimetatakse* algebraks*. Algebralist süsteemi, mille signatuuris on vaid relatsioonid (s.t. mille tüüp on* $<; l_1, l_2, \ldots >$*), nimetatakse* mudeliks*.*

Näide 24. 1. Naturaalarvude mudel $< \mathbb{N}; ; =, S, P >$ esitab aritmeetika, mille tüüp on $<; 2, 3, 3 >$. Seejuures eeldatakse, et relatsioonid S ja P on antud järgmiste definitsioonidega:

$$S(x, y, z) \stackrel{\text{def}}{=} (x + y = z)$$

ja

$$P(x, y, z) \stackrel{\text{def}}{=} (x * y = z)$$

2. *Naturaalarvude algebra* sisaldab liitmise ja korrutamise operatsioonid: $< \mathbb{N}; \ + *; >$. Algebra tüüp on $\tau =< 2, 2; >$;
3. *Robinsoni algebra* $< F^{(1)}; *, +, ^{-1}; >$, kus kandja on ühekohaliste täisarvuliste funktsioonide hulk. Operaatorid $*$, $+$ ja $^{-1}$ tähendavad vastavalt funktsioonde korrutamist, liitmist ja pöördfunktsiooni leidmist. Seega on Robinsoni algebra tüüp $\tau =< 2, 2, 1; >$.

Definitsioon 8. *Hulka* $B \subseteq H$ *nimetatakse süsteemi* $\mathcal{U} =< H, \Sigma >$ baasiks*, kui hulga* H *kõik elemendid on saadavad hulga* B *elementidest signatuuri kuuluvate operatsioonide abil.*

Näide 25. Algebra $\mathcal{N} = < \mathbb{N}, + >$, kus "+" tähistab naturaalarvude liitmise operatsiooni, baasiks on hulk $B = \{0, 1\}$.

Robinsoni algebra baasi moodustavad ruutjäägi ja ühe liitmise funktsioonid.

□

Definitsioon 9. *Algebralist süsteemi* $\mathcal{U}' = < H', \Sigma >$ *nimetatakse süsteemi* $\mathcal{U} = < H, \Sigma >$ *alamsüsteemiks, kui kõik signatuuri operatsioonid on kinnised hulgal* $H' \subseteq H$.

Näide 26. Algebra $\mathcal{N} = < \mathbb{N}; + >$ alamalgebraks on näiteks $\mathcal{N}' = < 2\mathbb{N}, + >$, kus $2\mathbb{N}$ tähistab paarisarvuliste naturaalarvude hulka.

Algebraliste süsteemide võrdlemisel kasutatakse kujutusi.

Definitsioon 10. *Olgu* $\mathcal{U}_1 = < H_1, \Sigma_1 >$ *ja* $\mathcal{U}_2 = H_2, \Sigma_2 >$ *algebrad. Kujutust*

$$\varphi : \mathcal{U}_1 \longrightarrow \mathcal{U}_2$$

nimetatakse morfismiks, *kui* $\varphi(h_1) \in H_2$ *ja* $\varphi(f_1) \in F_2$ *iga* $h_1 \in H_1$ *ja* $f_1 \in F_2$ *korral.*

Definitsioon 11. *Üksühest homomorfismi nimetatakse* isomorfimiks.

7.1. Näiteid klassikalistest algebralistest süsteemidest

Näide 27. Poolrühm on algebra tüüpi $< 2; >$, mille ainus operatsioon $\oplus$ on assotsiatiivne.

Sama formaalselt: algebra $\mathcal{U} = < H; \oplus >$ on poolrühm, kui $\forall x \in H$, $\forall y \in H$ ja $\forall z \in H$ korral kehtib seos

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \text{(assotsiatiivsuse omadus).}$$

Poolrühmas leiduvad vasak- ja parempoolsed neutraliseerivad elemendid n_v ja n_p, kui $\forall x \in H$ korral kehtivad seosed $n_v \oplus x = x$ ja $x \oplus n_p = x$.

Teoreem 9. *Kui poolrühmas on neutraliseerivad elemendid* n_v *ja* n_p, *siis nad on üheselt määratud ja* $n_v = n_p$.

Näide 28. Rühm on täiendelementidega poolrühm tüübiga $< 2, 1; >$. Seega rühm on algebra $< H; *, \sim >$, nii et kehtivad seosed

$$\forall x, y, z \in H \quad x * (y * z) = (x * y) * z$$

$$\forall x, y \in H \quad \tilde{y} * (y * x) = x = (x * y) * \tilde{y}$$

Teoreem 10. *Igas rühmas leidub neutraliseeriv element.*

Rühma nimetatakse kommutatiivseks *e.* Abeli rühmaks, *kui kehtib seos*

$$\forall x, y \in H \quad x * y = y * x.$$

Näide 29. Ring on Abeli rühm, milles lisaks rühmaoperatsioonile on kasutusel veel teinegi kahekohaline operatsioon, mis osutub rühmaoperatsiooni suhtes distributiivseks. Seega ring on algebra $\mathcal{R} = < H; +, *, \sim >$ tüüpi $\tau =< 2, 2, 1; >$, nii et kehtivad seosed

– assotsiatiivsus:

$$\forall x, y, z \in H \quad x + (y + z) = (x + y) + z$$

$$\forall x, y \in H \quad \tilde{y} + (y + x) = x = (x + y) + \tilde{y}$$

– kommutatiivsus:

$$\forall x, y \in H \quad x + y = y + x$$

– distributiivsus:

$$\forall x, y, z \in H \quad x * (y + z) = (x * y) + (x * z)$$

Näide 30. Korpus on ring, mille nullelemendist erinevad elemendid moodustavad mõlema operatsiooni suhtes rühma. Seega korpus on algebra $\mathcal{X} = < H; +, *, \sim, ' >$ tüüpi $\tau = < 2, 2, 1, 1; >$, nii et kehtivad seosed

– assotsiatiivsus:

$$\forall x, y, z \in H \quad x + (y + z) = (x + y) + z$$

$$\forall x, y \in H \quad \tilde{y} + (y + x) = x = (x + y) + \tilde{y}$$

$$\forall x, y, z \in H \quad x * (y * z) = (x * y) * z$$

$$\forall x, y \in H \quad y' * (y * x) = x = (x * y) * y'$$

– kommutatiivsus:

$$\forall x, y \in H \quad x + y = y + x$$

– distributiivsus:

$$\forall x, y, z \in H \quad x * (y + z) = (x * y) + (x * z)$$

Näide 31. Võre on algebraline süsteem tüüpi $< 2, 2; >$, mille mõlemad operatsioonid on idempotentsed, kommutatiivsed ja teineteise suhtes distributiivsed. Seega kehtivad võre $\mathcal{V} = < H; +, * >$ korral järgmise seosed:

– idempotentsus:

$$\forall x \in H \quad x + x + x$$

$$\forall x \in H \quad x * x = x$$

– kommutatiivsus:

$$\forall x, y \in H \quad x + y = y + x$$

$$\forall x, y \in H \quad x * y = y * x$$

– assotsiatiivsus:

$$\forall x, y, z \in H \quad x + (y + z) = (x + y) + z$$

$$\forall x, y, z \in H \quad x * (y * z) = (x * y) * z$$

– distributiivsus:

$$\forall x, y \in H \quad x + (x * y) = x$$

$$\forall x, y \in H \quad x * (x + y) = x$$

Täiendelemendiga võre e. *Boole'i algebra* on võre, millel on üks lisaoperatsioon koos kahe täiendava tingimusega. Boole'i algebra $\mathcal{B} = < H; +, *, ' >$ tüüp on $< 2, 2, 1; >$ ning kehtivad seosed:

– idempotentsus

$$\forall x \in H \quad x + x = x$$

$$\forall x \in H \quad x * x = x$$

– kommutatiivsus:

$$\forall x, y \in H \quad x + y = y + x$$

$$\forall x, y \in H \quad x * y = y * x$$

– assotsiatiivsus:

$$\forall x, y, z \in H \quad x + (y + z) = (x + y) + z$$

$$\forall x, yx \in H \quad x * (y * z) = (x * y) * z$$

– distributiivsus:

$$\forall x, y \in H \quad x * (x * y) = x$$

$$\forall x, y \in H \quad x * (x + y) = x$$

– täiendelemendi omadused:

$$\forall x \in H \quad (x')' = x$$

$$\forall x, y \in H \quad (x + y)' = x' * y'$$

$$\forall x, y \in H \quad (x * y)' = x' + y'$$

Boole'i algebra näideteks on

– $\mathcal{B} = < \{\mathbf{true}, \mathbf{false}\}; \vee, \&, \neg, >$
– $S = < \mathcal{P}(H); \cup, \cap' >$, kus $\mathcal{P}(H)$ tähistab hulga H kõigi alamhulkade hulka ja A' hulga A täiendit hulgani H.

7.2. Interpretatsioon

Tähistame sümboliga $\mathcal{A}_p$ predikaatarvutuse aatomite hulga.

Definitsioon 12. Interpretatsioon *$\mathcal{I}$ on ühene kujutis, mis seab atomaarsete valemite hulgale $\mathcal{A}_p$ vastavusse algebralise süsteemi elemendid $\mathcal{M} = < M; \quad F_1, \ldots; R_1, \ldots >$, nii et kehtivad järgmised tingimused:*

– *igale indiviidile seatakse vastavusse element algebralise süsteemi kandjast M, s.t. $\mathcal{I}(x) \in M$;*
– *igale k-kohalisele funktsioonisümbolile f seatakse vastavusse k-kohaline operatsioon $\mathcal{I}(f) = g$ algebralise süsteemi signatuurist, nii et*

$$\begin{array}{l} \mathcal{I}(f(x_1, \ldots, x_k)) = g(m_1, \ldots, m_k) \text{ ja} \\ m_1 = \mathcal{I}(x_1); \\ \ldots\ldots\ldots\ldots \\ m_k = \mathcal{I}(x_k); \end{array}$$

– *igale k-kohalisele predikaadisümbolile P seatakse vastavusse selline algebralise süsteemi $\mathcal{M}$ signatuuri kuuluv relatsioon $\mathcal{I}(P) = R$, et*

$\mathcal{I}(P(x^1), \ldots, P(x^k)) = R(m^1, \ldots, m^k)$ *ja*
$m^1 = \mathcal{I}(x^1)$;
.....
$m^k = \mathcal{I}(x^k)$;

Asjaolu, et atomaarse valemi $A \in \mathcal{A}_p$ jaoks leiduvad algebraline süsteem $\mathcal{M}$ ja interpretatsioon $\mathcal{I}$, mis rahuldavad definitsiooni 12 tingimusi, tähistatakse $\mathcal{M} \models A[\mathcal{I}]$. Sel juhul nimetatakse süsteemi $\mathcal{M}$ valemi A mudeliks. Öeldakse ka, et valem A on **kehtestatav mudelil $\mathcal{M}$ interpretatsiooniga $\mathcal{I}$**.

Laiendame nüüd kehtestatavuse mõiste ka teistele predikaatarvutuse valemitele:

Definitsioon 13. $\mathcal{M} \models A[\mathcal{I}]$,

- *kui A on atomaarne valem ja leidub interpretatsioon $\mathcal{I}$, mille korral $\mathcal{I}(A)$ on rahuldatud mudelil $\mathcal{M}$;*
- *kui $\mathcal{A} = A \vee B$ ning $\mathcal{M} \vdash A[\mathcal{I}]$ või $\mathcal{M} \vdash B[\mathcal{I}]$;*
- *kui $\mathcal{A} = A\&B$ ning $\mathcal{M} \vdash A[\mathcal{I}]$ ja $\mathcal{M} \vdash B[\mathcal{I}]$;*
- *kui $\mathcal{A} = \neg A$ ning ei kehti $\mathcal{M} \vdash A[\mathcal{I}]$;*
- *kui $\mathcal{A} = A \Longrightarrow B$ ning $\mathcal{M} \vdash (\neg A \vee B)[\mathcal{I}]$;*
- *kui $\mathcal{A} = \forall x A(x)$, kui iga $m \in M$ korral on mudelil $\mathcal{M}$ rahuldatud $\mathcal{I}(A(x))(m)$;*
- *kui $\mathcal{A} = \exists x(A(x))$, kui leidub selline $m \in M$, et mudelil $\mathcal{M}$ on rahuldatud $\mathcal{I}(A(x))(m)$.*

Kui valem A on kehtestatav, öeldakse, et interpretatsiooni $\mathcal{I}$ korral on see valem mudelil $\mathcal{M}$ **tõene**. Seega jaotuvad fikseeritud interpretatsiooni ja mudeli korral valemid oma väärtuse järgi tõesteks ja väärateks. Eelnevad definitsioonid annavad meetodi valemite tõeväärtuse arvutamiseks.

Näide 32. Vaatleme predikaatarvutuse mudelite interpreteerimist naturaalarvude aritmeetikas, seega mudelil $\mathcal{N} = < \mathbb{N}; +, *, => $, kus tehtemärgid $+$ ja $*$ tähistavad vastavalt liitmise ja korrutamise operatsioone ning "=" - võrdlusrelatsiooni.

I Olgu antud valem

$$A(x) = \exists x(P(f(x,x),z) \Longrightarrow P(g(x,x),z))$$

Interpretatsioon $\mathcal{I}_1$ olgu selline, et

$$\mathcal{I}_1(x) = 2;$$

$$\mathcal{I}_1(f) = \ '*';$$

$$\mathcal{I}_1(g) = \ '+';$$

$$\mathcal{I}_1(P) = \ ' =' \ .$$

Vastavalt definitsioonile 13 kehtib seos $\mathcal{N} \models A(x)[\mathcal{I}_1]$, kui leidub selline naturaalarv m, et ei ole rahuldatud tingimus $2 * 2 = m$ või on rahuldatud tingimus $2 + 2 = m$. Niisugune olukord kehtib iga $m \in \mathbb{N}$ korral ja seega on valem $A(x)$ interpretatsiooni $\mathcal{I}_1$ korral kehtestatav (tõene).

Samal ajal ei ole valem $A(x)$ kehtestatav (on väär) interpretatsiooni $\mathcal{I}_2$ korral, mis erineb interpretatsioonist $\mathcal{I}_1$ selle poolest, et seab indiviididele vastavusse teised väärtused:

$$\mathcal{I}_2(x) = 5$$

ja

$$\mathcal{I}_2(z) = 25.$$

II Olgu antud valem

$$B = \forall x \forall y \forall z \forall u (P(f(x,y),z) \& P(f(x,y),u) \Longrightarrow P(x,y)).$$

Valem B on kehtestatav mudelil $\mathcal{N}$ iga interpretatsiooni korral, sealhulgas ka nende interpretatsioonide puhul, mis on saadud $\mathcal{I}_1$ ja $\mathcal{I}_2$ määramispiirkondade laiendamisel muutujaga u.

III Olgu antud valem

$$C = \forall x \forall y \forall z ((P(f(x,y),z) \& \neg P(x,y) \Longrightarrow P(g(x,y),z)).$$

Valem C pole kehtestatav ühegi interpretatsiooni korral.

□

Definitsioon 14. *Valem A on samaselt tõene e.* tautoloogia *mudelil $\mathcal{M}$, kui ta on iga interpretatsiooni korral sellel mudelil kehtestatav (tähistus $\mathcal{M} \models A$); Valem A on* üldkehtestatav *(tähistus $\models A$), kui ta on samaselt tõene igal mudelil.*

Teoreem 11. *Kõik prdikaatarvutuse teoreemid on üldkehtestatavad, s.t. iga valemi A korral on avaldised $\vdash A$ ja $\models A$ ekvivalentsed.*

Tõestus. Tõestame teoreemi lausearvutuse fragmendi korral. Kogu predikaatarvutuse kohta käiva analoogilise teoreemi jätame siinkohal tõestamata.

Olgu Γ ja Δ lõplikud valemite hulgad. Saab näidata, et järgmsied kaks väidet on ekvivalentsed:

(a) Kui mingi interpretatsiooni korral on tõesed kõik hulga Γ valemid, siis on tõene ka vähemalt üks valem hulgast Δ.
(b) Sekvents $\Gamma \longrightarrow \Delta$ on tuletatav.

Väidete (a) ja (b) ekvivalentsusest järeldub ka vaadeldava teoreemi kehtivus. Näitame kõigepealt, et väitest (b) järeldub väide (a). Tõestus on teostatav induktsiooniga, lähtudes sekventsi $\Gamma \longrightarrow \Delta$ tuletuspuu sügavusest.

- **Induktsiooni baas.** Kui $\Gamma \longrightarrow \Delta$ on aksioom, siis hulkadel Γ ja Δ leidub vähemalt üks ühine valem. Seega kui mingi interpretatsioon muudab tõeseks kõik antetsedendi Γ valemid, siis muudab ta tõeseks ka sekventsi mõlema poole ühise valemi. Järelikult kehtib väide (a);
- **Induktsiooni samm** eeldab kõigi tuletusreeglite läbianalüüsimist; vaatame siin vaid juhtu, kui sekvents on saadud reegli ($\Longrightarrow\longrightarrow$) abil.

NB! Kodune ülesanne. Tõestada teoreem teiste tuletusreeglite abil.

Niisiis, oletame, et sekvents $\Gamma \longrightarrow \Delta$ on saadud tuletusreegli ($\Longrightarrow\longrightarrow$) abil. Tarvis on näidata, et kui mingi interpretatsiooni korral on tõesed sekventside $\Gamma \longrightarrow \Delta, A$ ja $\Gamma, B \longrightarrow \Delta$ kõik vasaku poole valemid ja üks valem paremalt poolelt, siis sekventsis $\Gamma, A \Longrightarrow B \longrightarrow \Delta$ on tõene ka üks valem hulgast Δ. Interpretatsioon, mille korral sekventsis $\Gamma, B \longrightarrow \Delta$ on tõene valem hulgast Δ, on tõene ka üks valem tuletusreegli ($\Longrightarrow\longrightarrow$) järelduse $\Gamma, A \Longrightarrow B \longrightarrow \Delta$ suktsedendis. Järelikult kehtib väide (a).

Teiseks näitame, et väitest (a) järeldub väide (b). Olgu Γ ja Δ valemite hulgad, mis rahuldavad seost (a). Moodustame sekventsi $\Gamma \longrightarrow \Delta$. Leiame hulga $\Gamma \cup \Delta$ suurima astakuga valemi ja rakendame sellele valemile vastavat tuletusreeglit "tagurpidi", s.o. alt üles. Edasi kordame sama tegevust kasutatud reegli kõigi eelduste jaoks. Kui seda konstruktsiooni enam rakendada ei saa, s.t. tuletuspuud ei saa enam laiendada, on kaks võimalust:

1. konstrueeritud puu "lõpeb" aksioomidega (siis kehtibki väide (b));
2. konstrueeritud puus on lõpptipp $\Gamma' \longrightarrow \Delta'$, mis pole aksioom. Näitame, et võimalus 2. tegelikult kunagi ei realiseeru. Oletame väitevastaselt, et $\Gamma' \longrightarrow \Delta'$ pole aksioom, s.t. $\Gamma' \cap \Delta' = \emptyset$. Viimase seose korral on võimalik leida interpretatsioon, mille puhul kõik valemid hulgast Γ' on tõesed ja kõik valemid hulgast Δ' väärad. Kui nii, siis saab analoogselt tõestuse esimese osaga näidata, et sama kehtib ka tõestuse kõigi nende sõlmede jaoks, mis asuvad tõestuses teel tipust $\Gamma' \longrightarrow \Delta'$ puu juureni. Teiste sõnadega - kõigi sellele teele jäävate sekventside $\Gamma'' \longrightarrow \Delta''$ korral osutuvad antetsedentide kõik valemid tõesteks ja suktsedentide kõik valemid väärateks. Sama peab kehtima ka puu juure $\Gamma \longrightarrow \Delta$ kohta, mis on aga vastuolus eeldusega (a).

□

Viimasest teoreemist võib teha kaks lihtsat järeldust.

Järeldus 8. *Igal mittevastuolulisel valemite hulgal leidub mudel.*

Järeldus 9. *(Gödeli teoreem predikaatarvutuse täielikkusest). Kui valem A on samaselt tõene, siis ta on teoreem.*

7.3. Formaalsed teooriad

Praktikas kasutatakse loogilise arutluse käigus arvutusi, kus osa funktsioonisümboleid ja predikaate omavad kindlat tähendust, ning kaht liiki aksioome:

1. loogika aksioome;
2. spetsiifilisi aksioome, mis väljendavad vaadeldavale ainevaldkonnale omaseid postulaate.

Seetõttu on igas arutluses kasutatavad samaselt tõesed loogika valemid ja need valemid, mille kehtivus järeldub spetsiifilistest aksioomidest.

Definitsioon 15. *Valemite hulka T, mis on kinnine tuletatavuse relatsiooni suhtes, nimetatakse* teooriaks.

Teooriat nimetatakse *aksiomatiseeritavaks*, kui leidub loenduv hulk $\Gamma \subseteq T$, nii et iga valemi $X \in T$ korral $\Gamma \vdash X$. Hulga Γ elemente nimetatakse vastava teooria (spetsiifilisteks) *aksioomideks*.

Olgu $\mathcal{M}$ mingi algebraline süsteem. $Th(\mathcal{M})$-iga tähistame valemite hulka, mille elemendid väljendavad etteantud interpretatsiooni korral kõiki süsteemi $\mathcal{M}$ tõeseid väiteid ja ainult neid. Teooria T on mudelil $\mathcal{M}$ täielik, kui ta on ekvivalentne teooriaga $Th(\mathcal{M})$.

Täielikus teoorias on tuletatav kas valem A või tema eitus.

Täieliku teooria näitena võib vaadelda lausearvutust, mis on Boole'i algebra täielik teooria (ka hulgateooria on Boole'i algebra täielik teooria). Täielikud aksiomatiseeritavad teooriad on olemas paljudel algebralistel süsteemidel: rühmateoorial, ringide teoorial, järjestusega korpuste teoorial jne. Täielikke aksiomatiseeritavaid teooriaid omavate valdkondade kohta saab põhimõtteliselt kõiki väiteid tõestada automaatselt.

Näide 33. Naturaalarvude aritmeetika aksiomaatiline teooria A_0. Kasutatakse individkonstanti (0), kahekohalisi võrdlusrelatsioone ($<$ ja $=$), kahekohalisi liitmise ja korrutamise tehteid ($+$ ja $*$) ning ühekohalist järgmise naturaalarvu leidmise funktsiooni (s).

Teooria A_0 aksioomid:

1. $\neg(s(x) = 0)$
2. $(s(x) = s(y)) \Longrightarrow (x = y)$
3. $x + 0 = x$
4. $x + s(y) = s(x + y)$
5. $x * 0 = 0$
6. $x * s(y) = (x * y) + x$
7. $\neg(x < 0)$
8. $(x < s(y)) \Longrightarrow ((< y) \vee (x = y))$
9. $((x < y) \vee (x = y)) \Longrightarrow (x < s(y))$
10. $(\neg(x = y)) \Longrightarrow (x < y) \vee (y < x))$

□

Teoreem 12. *(Gödeli teoreem aritmeetika mittetäielikkusest). Iga aksiomatiseeritav Teooria T, mis sisaldab teooria A_0, on mittetäielik.*

8. Modaalloogika

Modaalsus on loogika, lingvistika ja filosoofia kategooria, mis iseloomustab väidete ja otsustuste tõesuse määra. Väide võib olla *paratamatult tõene* (alati kehtiv), *võimalikult tõene*, *juhuslikult tõene* (statistiline tõesus) jne. Modaalloogika on loogika haru, milles osa väiteid käsitletakse modaalsetena. Näiteks loodusseadusi väljendavatest aksioomidest loogilise arutlusega (s.t. predikaatarvutuse tuletusreeglite kasutamise teel) saadud väited loetakse paratamatult kehtivaiks. Enamik ühiskondliku olemise kohta käivad väited aga kehtivad vaid osaliselt või tõkestatud ajaintervalli jooksul. Enamasti tuleb aga tunnistada, et see või teine nähtus toimus hoopis juhuslikult, s.t. samade tingimuste korral oleks võinud juhtuda hoopis midagi muud.

Vanim modaalloogika süsteem pärineb Aristoteleselt. Esimesed formaliseeritud modaalloogilised arvutused esitas 1902. aastal inglise loogik C. Lewis. Hiljem on modaalloogikat arendanud G. Wright, J. Lukasiewicz jt. Tänapäeval puudub ühtne modaalloogika teooria.

Modaal- ja klassikalise loogika tuletusmehhanismidel pole põhimõtteliselt erinevust. Mõlemal juhul ehitatakse formaalsed teooriad üles etteantud spetsiifilistest ja loogilistest aksioomidest lähtudes, kasutades lõplikku arvu tuletusreegleid.

Enamasti on modaalloogika keel klassikalise loogika keeltega võrreldes täiendatud nn. modaalsusoperaatoritega $\Box$ (paratamatuse operaator) ja $\Diamond$ (võimalikkuse operaator). Enamikus modaalloogika arvutustes on nimetatud operaatorid duaalsed, s.t. üks nimetatud operaatoritest on väljendatav teise kaudu vastavalt seosele

$$\Box A \equiv \neg\Diamond\neg A.$$

Vaatleme allpool mõningaid modaalloogilise lausearvutuse näiteid.

8.1. Modaalse lausearvutuse keel

a) tähestik:

- ladina väiketähed a, b, c, ... (elementaarsete tõeväärtuslike lausete e. propositsioonide tähistamiseks);
- loogikaoperatsioonide märgid $\neg, \vee, \&, \Longrightarrow, \Box$ ja $\Diamond$;
- ümarsulud ().

b) valemid (metatähistena kasutame valemite esitamiseks ladina suurtähti):

- kõik ladina väiketähed on valemid;
- kui A on valem, siis on valemid ka (A), $\neg A$, $\Diamond A$ ja $\Box A$;
- kui A ja B on valemid, siis on valemid ka $A \vee B$, $A\&B$ ja $A \Longrightarrow B$;
- rohkem valemeid ei ole.

Kõigepealt vaatleme Lewise formaalseid modaalloogika süsteeme S1 - S5.

Arvutus S1.

Aksioomid:

1. $\Box A$, kui A on tuletatav klassikalises lausearvutuses;
2. $\Box(\Box A \Longrightarrow A)$;
3. $\Box(\Box(A \Longrightarrow B)\&\Box(B \Longrightarrow C)) \Longrightarrow \Box(A \Longrightarrow C)$;
4. $\Box A \Longrightarrow \neg\Diamond\neg A$;
5. $\neg\Box\neg A \Longrightarrow \Diamond A$.

Tuletusreeglid:

$$\frac{A \quad A \Longrightarrow B}{B}\,(MP)$$

$$\frac{\Box A}{A}$$

$$\frac{\Box(A \Longrightarrow B) \quad \Box(B \Longrightarrow A)}{\Box(\Box A \Longrightarrow \Box B)}$$

Lewise ülejäänud modaalarvutused on saadud süsteemile S1 aksioomiskeemide lisamise teel:

Arvutus S2: $S1 + \{\Box(\Box A \Longrightarrow \Box(A \vee B))\}$

Arvutus S3: $S2 + \{\Box(\Box A \Longrightarrow B)) \Longrightarrow \Box((\Box A \Longrightarrow \Box B))\}$

Arvutus S4: $S3 + \{\Box(\Box A \Longrightarrow \Box\Box A)\}$

Arvutus S5: $S4 + \{\Box(A \Longrightarrow \Box\Diamond A)\}$

Kuna uute arvutuste sissetoomisel lisati uusi aksioomiskeeme, siis on ilmne, et kui valem A on tuletatav arvutuses $\mathrm{S_i}$, siis on ta tuletatav ka kõigis arvutustes $\mathrm{S_j}$, kus $j > i$.

Teine modaalloogika tuntud arvutuste süsteem lähtub aksioomidest

1. A, kui A on tuletatav klassikalises lausearvutuses
2. $\Box(A \Longrightarrow B) \Longrightarrow (\Box A \Longrightarrow \Box B)$
3. $\Box A \Longrightarrow \neg\Diamond\neg A$
4. $\neg\Box\neg A \Longrightarrow \Diamond A$

ning tuletusreeglitest

$$\frac{A \quad A \Longrightarrow B}{B}\,(MP)$$

$$\frac{A}{\Box A}$$

Viimatikirjeldatud arvutust tähistatakse tavaliselt kui **Arvutust K**. Selle arvutuse laienditeks on

Arvutus T: $K + \{\Box A \Longrightarrow A\}$

Arvutus B: $T + \{A \Longrightarrow \Box\Diamond A\}$ - Brouweri aksioom.

Väide. Arvutus S4 on ekvivalentne arvutusega $T + \{\Box A \Longrightarrow \Box\Box A\}$.

Analoogiliselt klasikalise loogikaga saab modaalloogikat laiendada ka predikaatarvutuse juhule.

Modaalloogika arvutusi saab esitada ka sekventsiaalarvutustena. Sekvents esitatakse kujul

$$\Gamma \stackrel{k}{\longrightarrow} \Delta,$$

kus Γ ja Δ on valemite hulgd, k näitab sekventsi koosseisu kuuluvate valemite "modaalsuse taset". Aksioomideks on sekventsid kujul

$$\Gamma, A \stackrel{0}{\longrightarrow} A, \Delta.$$

Järgnevas tuuakse arvutuste $\mathrm{S2^n}$ tuletusreeglite süsteem. Valem A on tuletatav arvutuses $\mathrm{S2^n}$ parajasti siis, kui tuletusreeglite abil on tuletatav sekvents

$$\stackrel{l}{\longrightarrow} A,$$

nii et $l \leq n$.

Modaalloogika arvutuste $S2^n$ tuletusreeglid (sekventsiaalvariant):

$$(\neg \longrightarrow) \ \frac{\Gamma \stackrel{k}{\longrightarrow} \Delta, A}{\neg A,\ \Gamma \stackrel{k}{\longrightarrow} \Delta} \qquad (\longrightarrow \neg) \ \frac{A, \Gamma \stackrel{k}{\longrightarrow} \Delta}{\Gamma \stackrel{k}{\longrightarrow} \Delta,\ \neg A}$$

$$(\& \longrightarrow) \ \frac{A, B, \Gamma \stackrel{k}{\longrightarrow} \Delta}{A \& B,\ \Gamma \stackrel{k}{\longrightarrow} \Delta} \qquad (\longrightarrow \&) \ \frac{\Gamma \stackrel{k_1}{\longrightarrow} \Delta, A \quad \Gamma \stackrel{k_2}{\longrightarrow} \Delta, B}{\Gamma \stackrel{max(k_1,k_2)}{\longrightarrow} \Delta,\ A \& B}$$

$$(\vee \longrightarrow) \ \frac{A, \Gamma \stackrel{k_1}{\longrightarrow} \Delta \quad B, \Gamma \stackrel{k_2}{\longrightarrow} \Delta}{A \vee B,\ \Gamma \stackrel{max(k_1,k_2)}{\longrightarrow} \Delta} \qquad (\longrightarrow \vee) \ \frac{\Gamma \stackrel{k}{\longrightarrow} \Delta, A, B}{\Gamma \stackrel{k}{\longrightarrow} \Delta,\ A \vee B}$$

$$(\Longrightarrow \longrightarrow) \ \frac{\Gamma \stackrel{k_1}{\longrightarrow} \Delta, A \quad B, \Gamma \stackrel{k_2}{\longrightarrow} \Delta}{A \Longrightarrow B,\ \Gamma \stackrel{max(k_1,k_2)}{\longrightarrow} \Delta} \qquad (\longrightarrow \Longrightarrow) \ \frac{A, \Gamma \stackrel{k}{\longrightarrow} \Delta, B}{\Gamma \stackrel{k}{\longrightarrow} \Delta,\ A \Longrightarrow B}$$

$$(\Box \longrightarrow) \ \frac{A, \Gamma \stackrel{k}{\longrightarrow} \Delta}{\Box A,\ \Gamma \stackrel{k}{\longrightarrow} \Delta} \qquad (\longrightarrow \Box) \ \frac{\Gamma \stackrel{k}{\longrightarrow} \Delta, A}{\Box \Gamma \stackrel{k'}{\longrightarrow} \diamond \Delta,\ \Box A}$$

$$(\diamond \longrightarrow) \ \frac{A, \Gamma \longrightarrow \Delta}{\diamond A, \Box \Gamma \stackrel{k}{\longrightarrow} \diamond \Delta} \qquad (\longrightarrow \diamond) \ \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \stackrel{k}{\longrightarrow} \Delta, \diamond A}$$

$$(cut) \ \frac{\Gamma \stackrel{k}{\longrightarrow} \Delta, A \quad A, \Gamma' \stackrel{k_2}{\longrightarrow} \Delta'}{\Gamma, \Gamma' \stackrel{max(k_1,k_2)}{\longrightarrow} \Delta, \Delta'},$$

kus

$$k' = \begin{cases} k+1, \text{kui } \Gamma = \Delta = \emptyset \text{ või } k > 0 \\ 0, \text{vastasel juhul} \end{cases}$$

Näide 34. Valem $(\Box\Diamond p)\&\Box(p \Longrightarrow \neg q)) \Longrightarrow \neg\Box q$ on tuletatav arvutuses $S2$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Ax:\ \ p,q\xrightarrow{0}q}}{p,q,\neg q\xrightarrow{0}}}{A\quad p,q\xrightarrow{0}p}}{p,\quad p\Rightarrow\neg q,\quad q\xrightarrow{0}}}{\Diamond p,\Box(p\Rightarrow\neg q),\quad \Box q\xrightarrow{0}}}{\Box\Diamond p,\quad \Box(p\Rightarrow\neg q),\quad \Box q\xrightarrow{0}}}{(\Box\Diamond p)\&\Box(p\Rightarrow\neg q)\xrightarrow{0}\neg\Box q}}{\xrightarrow{0}(\Box\Diamond p)\&\Box(p\Rightarrow\neg q)\Rightarrow\neg\Box q}$$

$(\to\neg)$
$(\Rightarrow\to)$
$(\quad\to)$
$(\Box\to)$
$(\&\to),\ (\to\neg)$
$(\to\Rightarrow)$

□

Näide 35. Valem $(\Box\Diamond p)\&\Box(p \Longrightarrow \neg q)) \Longrightarrow \Diamond q$ pole tuletatav arvutuses S2.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Ax:\ \ p\to q,p}\qquad\dfrac{p\to q}{p,\neg q\to}}{p,\ \ p\Rightarrow\neg q\to q}}{p,\quad\Box(p\Rightarrow\neg q)\to q}}{\Box p,\quad\Box(p\Rightarrow\neg q)\to q}}{(\Box\Diamond p)\&\ \Box(p\Rightarrow\neg q)\to\Diamond q}}{\to(\Box\Diamond p)\&\ \Box(p\Rightarrow\neg q)\Rightarrow\neg\Diamond q}$$

(pole aksioom)
$(\to\neg)$
$(\Rightarrow\to)$
$(\quad\to)$
$(\Box\to)$
$(\&\to)$
$(\to\Rightarrow)$

□

Teoreem 13. *Modaalloogika arvutuste vahel kehtivad järgmised ekvivalentsiseosed:*

a) $S2^1 \equiv S2$;
b) $S2^\infty \equiv T$.

Vastavalt sellele teoreemile võib arvutuses T tõestuste koostamisel kasutada arvutuse $S2^n$ tuletusreegleid sekventsi astakuid arvestamata.

Arvutuse S4 sekventsiaalavariandi saame, kui asendame arvutuses T tuletusreeglid $(\longrightarrow\Box)$ ja $(\Diamond\longrightarrow)$ uutega:

$$(\longrightarrow\Box)\ \ \frac{\Box\Gamma\longrightarrow\Diamond\Delta,A}{\Box\Gamma\longrightarrow\Diamond\Delta,\Box A}$$

ja

$$(\Diamond\longrightarrow)\ \ \frac{A\Box\Gamma\longrightarrow\Diamond\Delta}{\Diamond A,\Box\Gamma\longrightarrow\Delta}$$

8.2. Modaalarvutuse semantika

Modaalloogika mudelina kasutatakse struktuuri $M = (W, V, R)$, kus

- W on maailmade hulk (*universum*);
- V on *väärtustus*, s.o. funktsioon

$$V;\ \ L \times W \longrightarrow B,$$

  mis seab kõigi lausemuutujate hulgale L ja universumile W vastavusse elemendi Boole'i algebra kandjast

$$B = \{\mathbf{true}, \mathbf{false}\};$$

- $R \subseteq W \times W$ on binaarne relatsioon universumil W.

Piltlikult võime enesele ette kujutada universumi kui maailmade (algebraliste süsteemide) süsteemi. Universumis esinevad objektid võivad liikuda erinevas arengustaadiumis olevate maailmade vahel. Maailmade w_1 ja w_2 vahel kehtib relatsioon R, kui objektid võivad maailmast w_1 liikuda maailma w_2. Objektide kohta käivad väited võivad ühtedes maailmades olla tõesed (**true**), teistes aga väärad (**false**).

Väärtustust V laiendatakse kõigile valemitele vastavalt järgmistele reeglitele:

- $V(\neg A, w) = \mathbf{true}$ parajasti siis, kui $V(A, w) = \mathbf{false}$;
- $V(A \vee B, w) = \mathbf{true}$ parajasti siis, kui $V(A, w) = \mathbf{true}$ või $V(B, w) = \mathbf{true}$;
- $V(\Box A, w) = \mathbf{true}$ parajasti siis, kui $V(A, w') = \mathbf{true}$ iga maailma $w' \in W$ mille puhul $R^*(w, w')$;
- $V(\Diamond A, w) = \mathbf{true}$ parajasti siis, kui $V(A, w') = \mathbf{true}$ vähemalt ühe maailma korral, mille puhul $R^*(w, w')$.

R^* tähistab relatsiooni R transitiivset-refleksiivset sulundit. See tähendab, et $(w, w') \in R^*$ parajasti siis, kui leidub maailmade jada $w = w_1, w_2, \ldots, w_k = w'$, kus $k > 0$ ja iga $j \in \{1, 2, \ldots, k-1\}$ korral $(w_j, w_{j+1}) \in R$.

Erinevate modaalarvutuste korral on mudelis $M = (W, V, R)$ maailmade "arenemise relatsioon" R erinev. Näiteks arvutuse S5 korral $(w, w') \in R$ iga kahe maailma $w, w' \in W$ puhul. Teisisõnu, antud maailmale võib järgneda mistahes teine maailm.

Teoreem 14. *Arvutus* S5 *on täielik mudelil* $M(W, V, R)$, *kus* $R = W \times W$.

Näide 36. 1. Kuna iga maailma $w \in W$ korral $V(p \vee \neg p, w) = \mathbf{true}$, siis teoreemist 14 järeldub, et

$$\vdash \Box(p \vee \neg p).$$

2. Valem $\Box p \vee \Box \neg p$ pole kehtestatav arvutuse S5 korral.

□

Ülesanne 15. *Tõestada, et süsteemis* S5 *kehtivad samaväärsused*

a) $\Box\Box A \Longleftrightarrow \Box A$
b) $\Box\Diamond A \Longleftrightarrow \Diamond A$
c) $\Diamond\Diamond A \Longleftrightarrow \Diamond A$
d) $\Diamond\Box A \Longleftrightarrow \Box A$

Järeldus 10. *Ülesandes 15 esitatud samasustest järeldub, et süsteemis* S5 *võib iga valem olla vaid paratamatu või võimalik.*

Arvutuse S4 maailmade vahel esitab relatsioon R järjestusseose omadustega:

1. $\forall w \in W$ korral $(w, w) \in R$;
2. $\forall w, w', w'' \in W$ korral $((w, w') \in R) \& ((w', w'') \in R) \Longrightarrow ((w, w'') \in R)$.

Teoreem 15. *Arvutus* S4 *on täielik mudelil* $M = (W, v, R)$, *mille korral relatsioon* R *rahuldab kitsendusi 1 ja 2.*

Ülesanne 16. *Näidata, et arvutuses* S4

- *on tuletatav valem* $\Box\Diamond A \Longleftrightarrow \Box\Diamond\Box\Diamond A$;
- *ei ole tuletatav valem* $\Box A \Longleftrightarrow \Box\Box A$.

Järeldus 11. *Arvutuses* S4 *võib valemil* A *olla 6 erinevat modaalsust:*

$$\Box A, \quad \Box\Diamond A, \quad \Box\Diamond\Box\Diamond A,$$
$$\Diamond A, \quad \Diamond\Box A, \quad \Diamond\Box\Diamond\Box A.$$

8.3. Seos modaalarvutuse S5 ja klassikalise predikaatarvutuse vahel

Definitsioon 16. *Predikaatarvutuse valemit nimetatakse* pseudomodaalseks, *kui tema iga alamvalem sisaldab ülimalt ühe vaba muutuja.*

Näide 37. Järgnevatest valemitest on A pseudomodaalne, B ja C aga mitte:

$A = (P(x) \vee Q(x)) \& \forall y(\neg P(y) \& \neg Q(y) \& \exists u(P(u) \vee Q(u)))$;
$B = P(x) \vee Q(y)$;
$C = P(x) \vee \forall x P(x) \vee Q(y)$.

□

Igale pseudomodaalsele predikaatarvutuse valemile saab vastavusse seada modaalarvutuse valemi A^{mod}, kasutades järgmist transleerimisskeemi.

1. Üldsuskvantor $\forall x$ asendatakse paratamatuse operaatoriga $\Box$ (sõltumata sellest, millise muutujaga antud kvantor seotud on).
2. Eksistentsikvantor $\exists y$ asendatakse võimalikkuse operaatoriga $\Diamond$ (sõltumata sellest, millise muutujaga antud kvantor seotud on).
3. Iga valemis A esineva predikaadi P jaoks võetakse kasutusele lausemuutuja p ning predikaatarvutuse aatom $P(x, y, \ldots)$ asendatakse vastava lausemuutujaga p (predikaadi argumendid jäetakse lihtsalt ära).
4. Kõik ülejäänud valemis A esinevad sümbolid kirjutatakse valemisse A^{mod} ümber muutmata kujul.

Näide 38. Näites 37 esitatud pseudomodaalsele valemile A vastav modaalne valem on

$$A^{mod} = (p \vee q) \& \Box(\neg p \& \neg q \& \Diamond(p \vee q)).$$

□

Teoreem 16. *Pseudomodaalne predikaatarvutuse valem on tuletatav parajasti siis, kui arvutuses S5 on tuletatav valem* A^{mod}.

Nii nagu predikaatarvutuse korral saab ka modaalarvutuste puhul näidata, et kui valem on tuletatav lõikereeglit kasutades, siis on ta tuletatav ka lõikereeglit kasutamata.

8.4. Modaalloogika mudel: temporaalloogika

Modaalloogikal on oluline roll teoreetilises informaatikas, kus teda kasutatakse programmide korrektsuse tõestmiseks. Modaalsusi interpreteeritakse enamasti järgmiselt:

$\Box$ – alati;

$\Diamond$ – mõnikord.

Arutlusse programmi kohta tuuakse sisse ajadimensioon ja avaldist $\Box A$ interpreteeritakse nii, et vaadeldud hetkest alates alati kehtib väide A, ja avaldist $\Diamond A$ nii, et aegajalt kehtib väide A. Arusaadavalt on tegu teineteise suhtes duaalsete modaalsustega, sest kehtib seos $A = \neg(\Box A)$.

Mitmetes käsitlustes kasutatakse lisaks nimetatud põhimodaalsustele veel operatsioone:

$\circ$ – järgmine;

$\cup$ – kuni.

Avaldisi $\circ A$ ja $A \cup B$ interpreteeritakse vastavalt kui "järgmisel ajahetkel kehtib A" ja "seni kehtib A, kuni hakkab kehtima B". Sellist spetsiifiliselt interpreteeritavat modaalloogikat nimetatakse *temporaalloogikaks*.

Lausearvutusliku temporaalloogika valem on:

- iga lausemuutuja p;
- $p\&q$ ja $\neg p$, kui p ja q on valemid;
- $p\&q$ ja $\circ p$, kui p ja q on valemid.

Ülejäänud valemeid võib vaadelda kui teatud lühendeid teistest lausetest:

$p \vee q \ldots \neg(\neg p \& \neg q)$
$p \Longrightarrow \ldots \neg p \vee q$
$p \equiv \ldots (p \Longrightarrow q)\&(q \Longrightarrow p)$
$\mathbf{true} \ldots p \vee \neg p$
$\mathbf{false} \ldots \neg\, \mathbf{true}$
$\Diamond p \ldots (\mathbf{true} \cup p)$
$\Box p \ldots \neg\Diamond(\neg p)$
$\Diamond^{\infty} p \ldots \Box\Diamond p$ (lõpmata tihti)
$\Box^{\infty} p \ldots \Diamond\Box p$ (peaaegu alati)
$pBq \ldots \neg((\neg p) \cup q)$ (p kehtib varem kui q)

Temporaalloogika aksioomid:

1. (eelnenud lühendusi väljendavad seosed)

$$\Box\neg p \equiv \neg\Diamond p \qquad \Diamond\neg p \equiv \Box p$$
$$\circ\neg p \equiv \neg \circ p$$
$$\Diamond^{\infty}\neg p \equiv \neg\Box^{\infty} p \qquad \Box^{\infty}\neg p \equiv \neg\Diamond^{\infty} p$$
$$((\neg p) \cup q) \equiv \neg(pBq)$$

2. (modaalsustevahelised seosed)

$$p \Longrightarrow \Diamond p \qquad \Box p \Longrightarrow p$$
$$\circ p \Longrightarrow \Diamond p \qquad \Box p \Longrightarrow \circ p$$
$$\Box p \Longrightarrow \Diamond p \qquad \Box p \Longrightarrow \circ\Box p$$
$$p \cup q \Longrightarrow \Diamond p \qquad \Box^{\infty} p \Longrightarrow \Diamond^{\infty} p$$

3. (põhimodaalsuste idempotentsus)

$$\Diamond\Diamond p \equiv \Diamond p \quad \Diamond^\infty\Diamond^\infty p \equiv \Diamond^\infty p \quad \Box\Box p \equiv \Box p \quad \Box^\infty\Box^\infty \equiv \Box^\infty p$$

4. (kommutatiivsus)

$$\circ\Diamond p \equiv \Diamond \circ p$$
$$((\circ p) \cup (\circ q)) \equiv \circ(p \cup q)$$
$$\circ\Box p \equiv \Box \circ p$$

5. (lõpmatuse aksioomid)

$$\Diamond^\infty p \equiv \circ\Diamond^\infty p \equiv \Diamond^\infty p \equiv \Box\Diamond^\infty p \equiv \Diamond^\infty\Diamond^\infty p \equiv \Box^\infty\Diamond^\infty p$$
$$\Box^\infty p \equiv \circ\Box^\infty p \equiv \Diamond\Box^\infty p \equiv \Box\Box^\infty p \equiv \Diamond^\infty\Box^\infty p \equiv \Box^\infty\Box^\infty p$$

6. (lausearvutuse tehted ja modaalsused)

$$\Diamond(p \vee q) \equiv (\Diamond p \& \Diamond q) \qquad \Diamond^\infty(p \vee q) \equiv \Diamond^\infty p \vee \Diamond^\infty q$$
$$\Box(p \& q) \equiv (\Box p \& \Box q) \qquad \Box(p \& q) \equiv (\Box^\infty p \& \Box^\infty q)$$
$$((p \& q) \cup r) \equiv ((p \cup r) \& (q \cup r))$$
$$(p \cup (q \vee r)) \equiv ((p \cup q) \vee (p \cup r))$$
$$\circ(p \vee q) \equiv \circ p \vee \circ q \qquad \circ(p \& q) \equiv (\circ p \& \circ q)$$
$$\circ(p \Longrightarrow q) \equiv (\circ p \Longrightarrow \circ q) \qquad \circ(p \equiv q) \equiv (\circ p \equiv \circ q)$$
$$(\Box p \vee \Box q) \Longrightarrow \Box(p \vee q)$$
$$\Diamond(p \& q) \Longrightarrow (p \vee q)$$
$$((p \cup r) \vee (q \cup r) \Longrightarrow ((p \vee q) \cup r \qquad (\Box^\infty p \vee \Box^\infty q) \Longrightarrow Box^\infty(p \vee q)$$
$$(p \cup (q \& r)) \Longrightarrow ((p \cup q) \& (p \cup r)) \qquad \Diamond^\infty(p \& q) \Longrightarrow (\Diamond^\infty p \& \Diamond^\infty q)$$

7. (monotoonsuse aksioomid)

$$\Box(p \Longrightarrow q) \Longrightarrow (\Box p \Longrightarrow \Box q) \qquad \Box(p \Longrightarrow q) \Longrightarrow (\Diamond p \Longrightarrow \Diamond q)$$
$$\Box(p \Longrightarrow q) \Longrightarrow (\circ p \Longrightarrow \circ q)$$
$$\Box(p \Longrightarrow q) \Longrightarrow (\Diamond^\infty p \Longrightarrow \Diamond^\infty q) \qquad \Box(p \Longrightarrow q) \Longrightarrow (\Box^\infty p \Longrightarrow Box^\infty q)$$
$$\Box(p \Longrightarrow q) \Longrightarrow (p \cup r) \Longrightarrow (q \cup r))$$
$$\Box(p \Longrightarrow q) \Longrightarrow ((r \cup p) \Longrightarrow (r \cup q))$$

8. (püsipunkti aksioomid)

$$\Diamond p \equiv p \vee \circ\Diamond p \qquad \Box p \equiv p \& \circ\Box p$$
$$(p \cup q) \equiv q \vee \circ(p \& (p \cup q)) \qquad (pBq) \equiv \neg q \& (pBq))$$

Tuletusreegel:

$$(MP)\ \frac{p \qquad p \Longrightarrow q}{q}$$

Loogika aksioomide ja tuletusreeglite "väärtuslikkust" uurib mudelite teooria, mis omistab loogikavalemitele semantika, s.o. interpretatsiooni, mille korral saab valemite paikapidavust vahetult kontrollida.

Temporaal- e. *ajaloogikate* korral kasutatakse mitmeid mudeleid, mis eelkõige erinevad aja mõiste erineva käsitlemise poolest. Enamkasutatav temporaalloogika mudel kasutab nn. lineaarset aega, mille korral eeldatakse, et

- aeg on diskreetne;
- ajaarvamisel on algmoment, millele eelnevaid sündmusi ei saa vaadelda;
- aeg on tulevikus lõpmatu.

Oma väidete kehtivust vaadeldakse ajateljel. Ajatelg on kolmik $M = (S, L, X)$, kus S on olekute hulk; $x : \mathbb{N} \longrightarrow S$ on lõpmatu olekute jada ja $L : S \longrightarrow 2^{AP}$. AP on atomaarsete lausete hulk ning L on funktsioon, mis esitab antud olekus tõeste atomaarsete lausete hulga. Ajamomentidele vastavate olekute jada esitatakse sageli kujul $x = (s^0, s^1, \dots)$. Sümboliga X_i tähistame olekute alamjada $x_i = (s^i, s^{i+1}, \dots)$.

Ütleme, et valem p kehtib lineaaraja mudelil $M = (S, L, X)$ ja kirjutame $M, x \models p$, kui p on tõene jada x teatud olekute korral. Seos $\models$ on defineeritav induktiivselt:

1. $x \models P$ parajasti siis, kui $P \in L(s_0)$ atomaarse lause $P \in AP$ korral;
2. $x \vdash p\&q$ parajasti siis, kui $x \models p$ ja $x \models q$;
   $x \models \neg p$ parajasti siis, kui ei kehti $x \models p$;
3. $x \models (p \cup q)$ parajasti siis, kui leidub selline j, et $x_j \models q$ ja iga $k < j$ korral $x_k \models p$;
   $x \models \circ p$ parajasti siis, kui $x_1 \models p$.

Valem p on kehtestatav, kui leidub struktuur $M = (S, L, X)$, nii et $M, x \models p$. Valem p on üldkehtestatav (kirjutame $\models p$), kui ta on kehtestatav igal mudelil M.

Valem p on tuletatav (kirjutame $\vdash p$), kui ta on tuletatav ülalloetletud aksioomidest tuletusreeglite abil. Tuletussüsteem on kooskõlaline, kui iga tuletatav valem on ka üldkehtestatav. Tuletussüsteem on täielik, kui iga üldkehtestatav valem on tuletatav.

Teoreem 17. *Proportsionaalse temporaalloogika tuletussüsteem on mittevasturääkiv ja täielik.*

Käsitletud temporaalloogika variant baseerub lineaarsel ajal. Märkigem, et kasutusel on ka mitmeid teisi ajamudeleid, mis võimaldavad modelleerida arvutisüsteemide erinevaid aspekte. Aeg võib olla pidev või nn. hargnev, s.t. erinevate paralleelselt toimuvate protsesside kirjeldamisel kasutatakse aja erinevat kvantimist. Mõnedes loogikates on aeg ka pööratav. Osa loogikaid kasutab ajamomentide asemel ajaintervalle.

9. Intuitsionistlik loogika

20. saj. matemaatika aluste uuringutes valitseb peamiselt kaks erinevat lähenemist: formalism ja intuitsionism. Mõlemad suunad püüavad ületada matemaatika alustes avastatud **paradokse**. Viimaseid esineb matemaatika eriharudes ning nende tekke peamiseks põhjuseks on lõplike hulkade omaduste ülekandmine lõpmatutele hulkadele (nn. hulgateoreetiline käsitlus).

Formalismi (D. Hilbert, J. von Neumann) idee on matemaatiliste teooriate formaliseerimine ja nende mittevasturääkivuste tõestamine. Hulk teooriaid ongi aksiomatiseeritavad (näiteks rühmateooria, hulgateooria jt.), paraku on aga matemaatika raames ka selliseid teooriaid, mida ei saa täielikult formaliseerida. Näiteks võib tuua aritmeetika, mille jaoks (vastavalt Gödeli teoreemile) ei leidu täielikku formaalset teooriat.

Intuitsionism on formalismile teatud mõttes vastandlik suund, mis peab matemaatikas tõeseks vaid intuitsiooniga kooskõlas olevaid väiteid. Näiteks saab inimene intuitiivselt aru konkreetsete naturaalarvude tähendusest, suudab konstrueerida iga naturaalarvu n, lähtudes arvust $n-1 (n = 0, 1, 2, \ldots)$ või loendades piisavalt suure (kuid lõpliku) hulga elemente. Hulki, mille uusi elemente on võimalik moodustada tõkestamatult, nimetatakse **potentsiaalselt lõpmatuteks hulkadeks**. Kõigi naturaalarvude hulka aga, veel enam reaalarvude hulka kui tervikut, on tunduvalt raskem ette kujutada. Tervikuna antud lõpmatut hulka nimetatakse matemaatikas **aktuaalselt lõpmatuks**.

Intuitsionism kui filosoofiline suund matemaatikas tunnustab vaid potentsiaalset, mitte aga aktuaalset lõpmatust. Intuitsionistide jaoks kehtivad vaid need väited, mille puhul saab leida konkreetset väidet kinnitava objekti (arvu, lõpliku hulga jne.). Kui mingil põhjusel pole otstarbekas vastavat objekti leida (näiteks on tegu nii suure naturaalarvuga, et selle üleskirjutamine võtaks liiga kaua aega), peab olema antud vähemalt konstruktsioon (algoritm) sellise objekti saamiseks. Väite tõesust kinnitavat objekti või tema konstruktsiooni nimetatakse ka väite *realisatsiooniks*.

Intuitsionistlikus loogikas on tuletatavad vaid need väited, mille jaoks leidub realisatsioon. Näiteks väide $\exists x A(x)$ on tõestatav vaid juhul, kui saab konstrueerida muutuja x konkreetse väärtuse $x = x_0$, nii et $A(x_0)$ on tõene. Implikatsioonile $A \Longrightarrow B$ peab vastama kujutus (funktsioon), mis leiab valemi A realisatsiooni põhjal valemi B realisatsiooni ning valem $A \Longrightarrow B$ on tuletatav parajasti siis, kui selline kujutus eksisteerib. $A \vee B$ on tuletatav vaid sel juhul, kui on leitav kas valemi A või valemi B realisatsioon. Näiteks valemit $A \vee \neg A$ ei saa lugeda seni tõeseks, kui pole antud valemi A või tema eituse realisatsiooni. Seega ilmneb oluline erinevus klassikalise ja intuitsionistliku lausearvutuse vahel: valem $A \vee \neg A$ on klassikalises lausearvutuses esmaselt tõene, intuitsionistlikus lausearvutuses ei pruugi ta alati kehtida (ja ei ole seega ka lisaeeldusteta tuletatav). Siit tulenevalt ei kehti intuitsionistlikus loogikas ka nn. välistatud kolmanda seadus.

Välistatud kolmanda seaduse mittekehtimine intuitsionistlikus loogikas tingib ka asjaolu, et ei tohi kasutada vastuväitelisi tõestusi. Nii ei ole mitmed klassikalise matemaatika teoreemid intuitsionistliku matemaatika seisukohalt kehtivad. Näiteks matemaatilise analüüsi tuntud teoreem, et iga tõkestatud lõigus pidev reaalmuutuja funktsioon omab sellel lõigul maksimumi. Põhjuseks on siin asjaolu, et "küllalt keerulise" funktsiooni jaoks ei leidu meetodit maksimumi leidmiseks. Teise intuitsionistide jaoks mittekehtiva teoreemi näitena võib tuua järgmise von Dahleni teoreemi.

Näide 39. Teoreem 18. *Leiduvad irratsionaalarvud a ja b nii, et a^b on ratsionaalarv.*

Tõestus. Oletame, et $\sqrt{2}^{\sqrt{2}}$ on ratsionaalarv. Siis võib valida $a = \sqrt{2}$ ja $b = \sqrt{2}$. Kui aga $\sqrt{2}^{\sqrt{2}}$ on irratsionaalarv, siis võib võtta $a = \sqrt{2}$ ja $b = \sqrt{2}^{\sqrt{2}}$. Ka sel juhul on a^b ratsionaalarv:

$$a^b = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^2 = 2.$$

Vaadeldav tõestus on klassikalises mõttes korrektne, kuid pole intuitsionistlikus mõttes üldse võetav tõestusena, sest tulemusena ei tea me ikkagi, millisel arvupaaril on tegelikult teoreemis väidetav omadus.

Kõigil intuitsionistlikus tõestuses esinevatel valemitel peab leiduma realisatsioon. Seega tõestustes kasutatavad tuletusreeglid peavad muu hulgas konstrueerima oma järelduste realisatsioonid. Seejuures võib kasutada muidugi tuletusreegli eelduste realisatsioone. Teiste sõnadega, kui valemitest $A, B, \ldots, D$ on tuletatav valem E, kasutades reeglit

$$\frac{A, B, \ldots D}{E},$$

siis peab leiduma konstruktsioon f, nii et $e = f(a, b, \ldots, d)$, kus $a, b, \ldots d$ ja e on vastavalt valemite $A, B, \ldots, D$ ja E realisatsioonid.

Järgnevas esitatavad intuitsionistliku lausearvutuse tuletusreeglid tagavad oma järelduste realiseeritavuse. Seega esitavad tõestused ühtlasi ka teoreemi realisatsiooni e. konstruktsiooni algoritmi vastava objekti ehitamiseks. Seetõttu kasutatakse sellist loogikat programmide automaatseks sünteesimiseks: lähtudes vastavast teoreemist (programmi spetsifikatsioonist) ehitatakse teoreemi intuitsionistlik tõestus, mille struktuuri põhjal saadakse seejärel teoreemile vastav programm. Saab näidata, et sel viisil võib konstrueerida mistahes (lõplikus ajas töötava) programmi.

Intuitsionistliku lausearvutuse keel ühtib klassikalise lausearvutuse keelega.

Aksioomiskeeme on intuitsionistlikus lausearvutuses 10 (A. Heyting, 1930):

1. $A \Longrightarrow (B \Longrightarrow A)$
2. $(A \Longrightarrow B) \Longrightarrow ((A \Longrightarrow (B \Longrightarrow C)) \Longrightarrow (A \Longrightarrow C)$
3. $A \Longrightarrow (B \Longrightarrow A\&B)$
4. $A\&B \Longrightarrow A$
5. $A\&B \Longrightarrow B$
6. $A \Longrightarrow A \vee B$
7. $B \Longrightarrow A \vee B$
8. $(A \Longrightarrow C) \Longrightarrow ((B \Longrightarrow C) \Longrightarrow (A \vee B \Longrightarrow C))$
9. $(A \Longrightarrow B \Longrightarrow ((A \Longrightarrow \neg B) \Longrightarrow \neg A)$
10. $A \Longrightarrow (\neg A \Longrightarrow B)$

Tuletusreeglina kasutatakse MP.

Nagu eespool deklareeritud, vastab igale tuletatavale valemile tema realisatsioon. Realisatsioonide esitamiseks defineerime termide keele L (sisuliselt funktsionaalne programmeerimiskeel). Keel sisaldagu indiviidsümboleid (konstante ja muutujaid) objektide tähistamiseks. Iga indiviidsümboli jaoks olgu defineeritud ka muutuja määramispiirkond. Keele L laused e. termid olgu määratud järgmiste seostega:

- iga indiviidsümbol x tüüpi s on term;
- avaldis $t(x_1, \ldots, x_n)$ on term tüübiga s, kui t on term tüübiga $s_1, \ldots, s_n \longrightarrow s$ ja $x_1, \ldots, x_n$ on termid vastavalt tüüpidega $s_1, \ldots, s_n$;
- $\lambda x.t$ on term tüüpi $s' \longrightarrow s$, kui t on term tüübiga s ja x on termis t sidumata sümbol, mille tüüp on s'. (Seotud sümboliteks loetakse kõiki neid tekstimärke y, mis avaldises $\lambda y.t$ esinevad termi t koosseisus. Siinses tähistuses tõlgendatakse kõiki seotud sümboleid muutujatena, vabad sümbolid tähistavad konstante).

Asjaolu, et valemit A realiseerib objekt, mille konstruktsioon on määratud termiga t, tähistame valemiga $A(t)$. Näiteks lausemuutuja p korral on teda realiseeriv objekt - täpsemini üks objektidest, mille jaoks väide p kehtib - tähistatav indiviidsümboliga. Erijuhul, kui valem on kujul $A \Longrightarrow B$, vastab talle realisatsioon $f = \lambda a.b$, kus term b esitab osavalemi B realisatsiooni. Muutuja a väärtusteks võivad aga olla valemi A mistahes realisatsioonid. Seega on implikatsiooni realisatsiooniks (konstantne) funktsioon f. Lühiduse mõttes kasutame avaldist $A \underset{f}{\Longrightarrow} B$ tähistamaks seda, et implikatsiooni $A \Longrightarrow B$ realiseerib funktsioon f. Kui viimases implikatsioonis valemid A ja B on atomaarsed, siis saab implikatsioonile anda ka järgmise interpretatsiooni (kooskõlas eelpool esitatud tõlgendusega): olgu muutuja b väärtus arvutatav muutuja a väärtusest funktsiooni f abil.

Intuitsionistliku lausearvutuse tuletusreeglit võib modifitseerida, näidates ära ka konstruktsiooni, mis esitab tuletusreegli järelduse realisatsiooni:

$$\frac{A \Longrightarrow B \qquad A(a)}{B(f(a))}.$$

Programmide struktuurne süntees. Praktikas kasutatakse intuitsionistlikku lausearvutust programmide automaatseks konstrueerimiseks tõestuste struktuuri põhjal. Enamasti kasutatakse seejuures intuitsionistlikku lausearvutuse sekventsiaalvarianti.

Vaatleme järgnevalt üht sellistest sünteesimeetoditest, kus lausearvutuse valemites kasutatakse vaid kaht loogikaoperatsiooni: konjunktsiooni & ja implikatsiooni $\Longrightarrow$. Seega on lausearvutuse valemid defineeritud järgmisel viisil:

- iga lausemuutuja $p, q, r, \ldots$ on valem;
- kui A ja B on valemid, siis on valemiteks ka $A\&B$ ja $A \Longrightarrow B$;
- rohkem avaldisi ei ole.

Vajaduse korral võib muidugi kasutada ka teisi loogikaoperatsioone, defineerides need konjunktsiooni ja implikatsiooni kaudu.

Sekvents on, nagu klassikaliseski loogikas, avaldis kujul

$$A, \ldots, B \longrightarrow C, \ldots, D.$$

Valemite üleskirjutuste lühendamiseks kasutame konjunktsiooni $A_1\& \ldots \&A_k$ asemel kirjutist $\overline{A}$.

Loogilised aksioomid on need sekventsid, mille antetsedent ja suktsedent sisaldavad üht ja sama valemit (aatomit). Selle ühise atomaarse valemi (lausemuutuja) realisatsiooniks võib valida suvalise väärtuse talle vastava muutuja lubatud väärtuste hulgast. Seega on loogilise aksioomi kuju

$$\Gamma, A(a) \longrightarrow A(a), \Delta.$$

Spetsiifilised aksioomid, mis esitavad formaalse teooria teatud ainevaldkonna kirjeldamiseks (nimetatakse ka vastava valdkonna **arvutusmudeliks**), on implikatsioonid kujul

$$\longrightarrow \overline{A} \underset{f}{\Longrightarrow} B \quad \text{(arvutuslause)}$$

või

$$\longrightarrow \overline{(\overline{A} \underset{\overline{\mu}}{\Longrightarrow} B)} \Longrightarrow (\overline{C} \underset{F(\overline{\mu})}{\Longrightarrow} D) \quad \text{(tingimuslik arvutuslause)}$$

Arvutuslaused näitavad käsitletava valdkonna objektide vahel kehtivaid arvutatavaid (efektiivselt realiseeritavaid) seoseid. Seejuures tingimusliku arvutuslause realisatsioon

sõltub objektide $a_1, \ldots, a_k$ ja b vahelisest arvutusseosest (siin on arvestatud, et objektid a_i, b, c_j ja d on seatud vastavusse lausemuutujatele A_i, B, C_j ja D.

Tingimuslikule arvutuslausele võib anda järgmise intuitiivse interpretatsiooni: objekti d väärtus on arvutatav (konstantse) funktsiooniga F, lähtudes objektide c_j väärtusest ja objektide a_i ja b vahelistest sõltuvustest μ_i. Funktsioonid μ_i sõltuvad omakorda arvutusmudeli teistest arvutuslausetest ega ole ühe aksioomi raames vahetult esitatavad. Seepärast tuleb sümboleid μ_i vaadelda kui funktsionaalmuutujaid (funktsiooni F jaoks on need "protseduuri" tüüpi argumendid).

Programmide struktuurse sünteesi korral kasutatavad tuletusreeglid on:

1.
$$\frac{\longrightarrow \overline{A} \underset{f}{\Longrightarrow} V \quad ; \quad \overline{\Gamma \longrightarrow A(a)}}{\Gamma \longrightarrow V(f(\overline{a}))} \ (\Longrightarrow --),$$
kus $\overline{a} = (a_1, \ldots, a_k)$;

2.
$$\frac{\Gamma, \overline{A} \longrightarrow B(b)}{\Gamma \longrightarrow \overline{A} \underset{\lambda a_1 \ldots \lambda a_k . b}{\longrightarrow} B} \ (\Longrightarrow +)$$

3.
$$\frac{\longrightarrow \overline{(\overline{A} \underset{\overline{\varphi}}{\Longrightarrow} B)} \Longrightarrow (\overline{C} \underset{F(\overline{\varphi})}{\Longrightarrow\!\Longrightarrow} D) \quad ; \quad \overline{\Gamma, \overline{A} \longrightarrow B(b)} \quad ; \quad \overline{\Sigma \longrightarrow C(c)}}{\Gamma, \Sigma \longrightarrow D(F(\overline{(\lambda \overline{a}.b)}, \overline{c}))} \ (\Longrightarrow --),$$
kus $\overline{c} = (c_1, \ldots, c_k)$ ja $(\lambda \overline{a}.b)$ on $\lambda a_1 \ldots \lambda a_k . b$ termide hulk kõigi $(\overline{A} \Longrightarrow B)$ implikatsioonide jaoks konjunktsioonis $\overline{(\overline{A} \Longrightarrow B)}$.

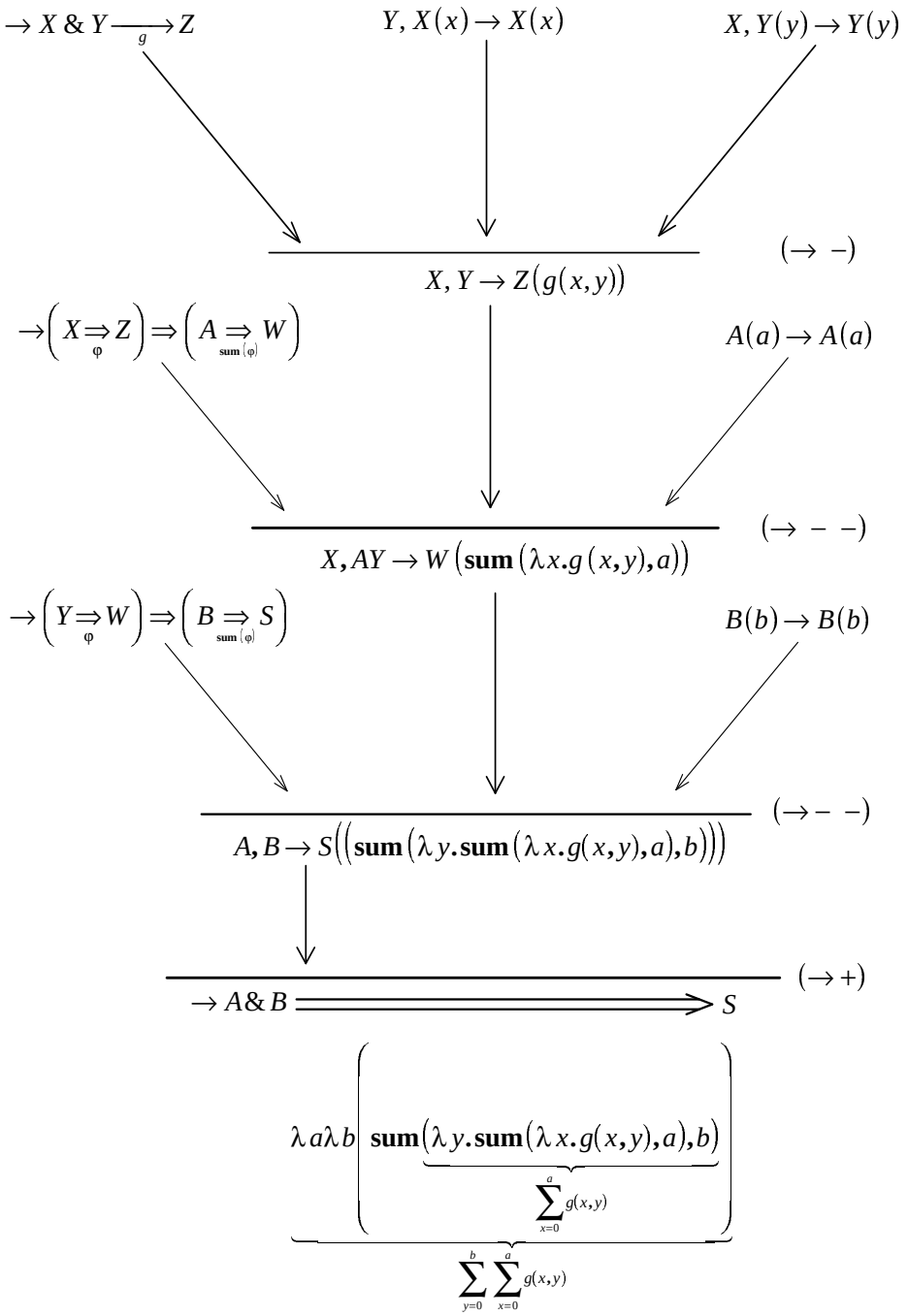
Programmi P sünteesimiseks, mis arvutaks muutuja x põhjal muutuja y väärtuse, tuleb vastaval arvutusmudelil tõestada sekvents
$$\longrightarrow X \underset{\lambda x . t}{\Longrightarrow\!\Longrightarrow} Y.$$
Kui selline tuletus on leitav, siis seda sekventsi realiseeriv term ongi otsitavaks programmiks.

Näide 40. Programmi sünteesimine kahekordse summa $S = \sum_{y=0}^{b} \sum_{x=0}^{a} g(x,y)$ arvutamiseks. Programmi konstrueerimiseks kasutatakse alamprogrammina eelnevalt programmeeritud funktsiooni $\mathbf{sum}(\varphi, a)$ ühekordse summa $\varphi(a) = \sum_{x=1}^{a} Z(x) = \mathbf{sum}(Z, a)$ arvutamiseks.

Järgnevalt on esitatud vaadeldavat ülesannet kirjeldav arvutusmudel ja sünteesi kirjeldav tuletus.

$$S = \sum_{y=o}^{b} \sum_{x=0}^{a} g(x,y)$$

$$\begin{array}{ll}
S = \sum_{y=o}^{b} w(y) & \longrightarrow (Y \underset{\varphi}{\Longrightarrow} W) \longrightarrow (B \underset{\mathbf{sum}(\varphi)}{\Longrightarrow\!\Longrightarrow} S) \\
w(y) = \sum_{x=0}^{a} z & \longrightarrow (X \underset{\mathbf{sum}(\varphi)}{\Longrightarrow\!\Longrightarrow} Z) \longrightarrow (A \underset{\mathbf{sum}(\varphi)}{\Longrightarrow\!\Longrightarrow} W) \\
z = g(x,y) & \longrightarrow x \& Y \underset{g}{\Longrightarrow} Z)
\end{array}$$



Lemma 4. *Olgu $F[E]$ valem, mis on saadud valemist $F(x)$ vaba muutuja x asendamisel valemiga E. Siis on intuitsionistlikus lausearvutuses deduktiivselt samaväärsed ($\overset{\diamond}{=}$) järgmised sekventside paarid:*

$$
\begin{array}{ll}
(a) & \Sigma \longrightarrow F[E] \stackrel{\circ}{=} (x \Longrightarrow E), (E \Longrightarrow x), \Sigma \longrightarrow F[x] \\
(\&) & \Sigma \longrightarrow F[A\&B] \stackrel{\circ}{=} (x \Longrightarrow A), (x \Longrightarrow B), (A \Longrightarrow (B \Longrightarrow x)), \Sigma \longrightarrow F[x] \\
(\Longrightarrow) & \Sigma \longrightarrow F[A \Longrightarrow B] \stackrel{\circ}{=} (x \Longrightarrow (A \Longrightarrow B)), ((A \Longrightarrow B) \Longrightarrow x), \Sigma \longrightarrow F[x] \\
(\vee) & \Sigma \longrightarrow F[A \vee B] \stackrel{\circ}{=} (x \Longrightarrow (A \Longrightarrow B)), (A \Longrightarrow x), (B \Longrightarrow x), \Sigma \longrightarrow F[x] \\
(\Longleftrightarrow) & \Sigma \longrightarrow F[A \Longleftrightarrow B] \stackrel{\circ}{=} (x \Longrightarrow (A \Longrightarrow B)), (x \Longrightarrow (B \Longrightarrow A)), \\
 & \qquad\qquad (A \Longrightarrow B) \Longrightarrow ((B \Longrightarrow A) \Longrightarrow x), \Sigma \longrightarrow F[x]
\end{array}
$$

Teoreem 19. *Iga lausearvutuse valemile vastava sekventsi* $\longrightarrow A$ *jaoks leidub temaga deduktiivselt ekvivalentne sekvents* $A_1, \ldots, A_k \longrightarrow V$, *kus* V *on muutuja ja* $A_1, \ldots, A_k$ *on lihtne või tingimuslik arvutuslause.*

Teoreem 20. *Iga arvutuslause, mis on tuletatav intuitsionistlikus lausearvutuses, on tuletatav programmide struktuurse sünteesi reeglite järgi ja vastupidi.*

Järeldus 12. *Programmide struktuurne süntees on täielik intuitsionistlikus lausearvutuses.*

Märkus 4. Intuitsionistlik lausearvutus on ka samaväärne modaalse lausearvutusega S4. (Vt. üksikasjalikumalt A. Grzegorczyk, "Fundam. Math.", 1967, V. 60, No. 2, pp. 223-231).