

TARTU ÜLIKOOL

LOODUS- JA TÄPPISTEADUSTE VALDKOND

MATEMAATIKA JA STATISTIKA INSTITUUT

Aiden Madisson

Peano aritmeetika korrektsus

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendajad: PhD Danel Ahman

PhD Ülo Reimaa

TARTU 2025

PEANO ARITMEETIKA KORREKTSUS

Bakalaureusetöö

Aiden Madisson

Lühikokkuvõte

Antud bakalaureusetöös näidatakse, et Peano aritmeetika on korrektne. Selleks taandakse Peano aritmeetika korrektsuse näitamine Heytingi aritmeetika korrektsusele. Omakorda tehakse kindlaks, et igale Heytingi aritmeetikas tõestatavale valemile vastav Dialektika interpretatsiooni kvantoriteta valem on tõestatav Gödeli süsteemis **T**.

CERCS teaduseriala: P110 Matemaatiline loogika, hulgateooria, kombinatorika.

Märksõnad: Peano aritmeetika, Heytingi aritmeetika, korrektsus, intuitsionistlik loogika, lambda-arvutus.

CONSISTENCY OF PEANO ARITHMETIC

Bachelor thesis

Aiden Madisson

Abstract

This bachelor's thesis shows that Peano arithmetic is consistent. For that, the consistency of Peano arithmetic is reduced to show that Heyting arithmetic is consistent. In turn, it is demonstrated, that every formula that can be proved in Heyting arithmetic has a corresponding Dialectica interpretation quantifier-free formula, that can be proved in Gödel's system **T**.

CERCS research specialisation: P110 Mathematical logic, set theory, combinatorics.

Key Words: Peano arithmetic, Heyting arithmetic, consistency, intuitionistic logic, lambda calculus.

Sisukord

Sissejuhatus	4
1 Intuitsionistlik ja klassikaline loogika	6
1.1 Predikaatloogika	6
1.2 Peano aritmeetika	16
1.3 Klassikalise loogika interpreteerimine intuitsionistlikus loogikas . .	18
2 Dialektika interpretatsioon	24
2.1 Gödeli süsteem T	24
2.2 Dialektika interpretatsioon	28
3 Peano aritmeetika korrektsus	39
3.1 Church-Rosser'i teoreem	39
3.2 Peano aritmeetika korrektsus	41
Kokkuvõte	42
Kasutatud allikad	43

Sissejuhatus

Aastal 1958 ilmus ajakirjas *Dialectica* loogiku ja matemaatiku Kurt Gödeli intuitsionistliku aritmeetika interpretatsioon kvantoritevaba lõplike tüüpidega funktsionaalide teooriasse (süsteem \mathbf{T}), mida hiljem hakati kutsuma Dialektika interpretatsiooniks. Juba varasemalt oli teada tänu Gödeli enda mittetäielikkuse teoreemidele [8], et vähegi väljendusrikka teooria, see tähendab, teooria, milles on võimalik aritmeetikat väljendada, korrektsust ei ole võimalik selles teoorias endas tõestada (eeldusel, et antud teooria on korrektne). Sestap läheb ka Peano aritmeetika korrektsuse tõestamisel vaja tugevamat teooriat, kui Peano aritmeetika ise.

Antud bakalaureusetöö eesmärgiks on tutvustada lugejale ühte meetodit Peano aritmeetika korrektsuse tõestamisel.

Esimeses peatükis defineerime põhilised esimest järku predikaatloogika mõisted ning defineerime ühe konkreetse tuletussüsteemi intuitsionistliku predikaatloogika jaoks. Samuti kirjeldame ära, mida mõtleme teooria korrektsuse all. Esimese peatüki peamine tulemus on Heytingi aritmeetika ja Peano aritmeetika korrektsuse samaväärsuse näitamine.

Teises peatükis defineerime Gödeli süsteemi \mathbf{T} ning anname Dialektika interpretatsiooni definitsiooni. Põhitulemusena tõestame, et iga Heytingi aritmeetikas tõestatavale valemile vastav kvantoritevaba Dialektika interpretatsiooni valem on süsteemis \mathbf{T} tõestatav.

Kolmas peatükk annab tuginedes eelnevatest peatükkidest saadud tulemustele tõestuse, et Peano aritmeetika on korrektne. Suuresti tugineb tõestus Church-Rosser'i teoreemile süsteemi \mathbf{T} kohta.

Bakalaureusetöö lugejalt eeldatakse, et ta on mingilgi määral tuttav esimest järku predikaatloogika (näiteks on läbinud kursuse „Diskreetne matemaatika I“). Samuti tulevad kasuks varasemad teadmised lambda-arvutusest. Siiski saab tubli lugeja nendetagi hakkama.

Antud bakalaureusetöö on referatiivne ning ei sisalda uusi tulemusi.

1 Intuitsionistlik ja klassikaline loogika

Selles peatükis anname põhilised definitsioonid esimest järku predikaatloogika kohta, et hiljem oleks tekstis lihtsam orienteeruda. Samuti defineerime intuitsionistliku predikaatloogika tuletussüsteemi.

1.1 Predikaatloogika

Järgnevas alampeatükis defineerime peamised esimest järku predikaatloogika mõisted lähtudes allikast [10].

Esimest järku keele *tähestik* koosneb järgmistest osadest:

1. konstantsümbolid: a, b, c, d, \dots ,
2. funktsionaalsümbolid f, g, h, \dots ,
3. indiviidmuutujad: x, y, z, x_1, x_2, \dots ,
4. termisümbolid: t, u, v, t_1, t_2, \dots
5. predikaatsümbolid: P, Q, R, \dots ,
6. loogilised sümbolid: $\perp, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall$ ja \exists ,
7. võrdusesümbol: $=$;
8. piirajad: koma $,$ ja sulud $()$,
9. valemite tähistuseks mõeldud muutujad: $\varphi, \psi, \theta, \xi, \dots$ (kreeka tähed).

Antud lõputöö raames loeme predikaatloogika tähestiku hulka ka sümboli \perp , mida mõistame kui väärust või vastuolu süsteemis. Hiljem kasutame me vastuolu \perp saamiseks aru, mida täpselt mõistame teooria (mitte)korrektsuse all (definitsioon 1.18).

Sümboli \perp täpsem tähendus selgub, kui oleme defineerinud predikaatloogikale vastava tuletussüsteemi. Lisaks kasutame kokkuleppeliselt teada-tuntud sümboolikat hulgateooriast.

Kõigepealt aga anname signatuuri definitsiooni.

Definitsioon 1.1. Kolmikut $\Sigma = \langle \mathcal{C}; \mathcal{F}; \mathcal{P} \rangle$ nimetatakse esimest järku keele **signatuuriks**, kus:

1. \mathcal{C} on konstantsümbolite hulk,
2. \mathcal{F} on funktsionaalsümbolite hulk,
3. \mathcal{P} on predikaatsümbolite hulk.

Eeldatakse, et igal funktsionaalsümbolil ja igal predikaatsümbolil on fikseeritud argumentide arv. Funktsionaalsümboli juures eeldame, et argumentide arv on positiivne täisarv. Predikaatsümboli puhul eeldame, et argumentide arv on mittenegatiivne. Kõik kirjeldatud kolm hulka võivad olla nii lõplikud kui ka lõpmatud, kuid nad ei tohi omavahel lõikuda.

Enne valemi mõiste defineerimist läheb meil vaja termi mõistet.

Definitsioon 1.2. **Termid** signatuuris Σ on parajasti need avaldised, mida saab koostada järgmiste reeglite abil:

1. Iga individmuutuja x on term signatuuris Σ ,
2. Signatuuri Σ iga konstantsümbol c on term signatuuris Σ ,
3. Kui f on n -kohaline funktsionaalsümbol signatuuris Σ ja t_1, \dots, t_n on termid signatuuris Σ , siis $f(t_1, \dots, t_n)$ on term signatuuris Σ .

Näide 1.3. Signatuuris $\Sigma = \langle \mathbf{0}; \mathbf{s}, +, \cdot, ; \rangle$ on termideks näiteks $+(x, (\cdot(\mathbf{s}(y), z)), +(\mathbf{s}(\mathbf{0}), y))$ ja lihtsalt individmuutuja x .

Edaspidi kasutame lihtsuse huvides antud signatuuri $\Sigma = \langle \mathbf{0}; \mathbf{s}, +, \cdot \rangle$ (tegemist on Peano aritmeetika signatuuriga, vaata peatükk 1.2) funktsionaalsümboleid $+$ ja \cdot *infiks* kujul. See tähendab, et kirjepildi $+(x, y)$ ja $\cdot(x, y)$ asemel kirjutame lihtsalt $x + y$ ja $x \cdot y$. Samuti loeme tehete järjekorra mõttes funktsionaalsümboleid \mathbf{s} seotust tugevamaks kui sümboleid $+$ ja \cdot seotust. Ning \cdot seotust tugevamaks kui $+$ seotust; see võimaldab meil sulge ära jätta. Seega näiteks termi $x + \mathbf{s}x \cdot y$ all mõtleme avaldist $+(x, \cdot(\mathbf{s}(x), y))$.

Et saaksime antud keele kohta väiteid moodustada, peame defineerima *valemi* mõiste. Esmalt alustame *atomaarsest* valemist.

Definitsioon 1.4. Atomaarsed valemid on defineeritud kui:

1. vastuolu \perp on atomaarne valem signatuuris Σ ,
2. kui t ja s on termid signatuuris Σ , siis $t = s$ on atomaarne valem signatuuris Σ ,
3. Kui P on n -kohaline predikaatsümbol ja t_1, \dots, t_n on termid signatuuris Σ , siis $P(t_1, \dots, t_n)$ on atomaarne valem signatuuris Σ .

Definitsioon 1.5. Predikaatloogika valemid on parajasti need, mis on moodustatud järgmiste reeglite abil:

1. Iga atomaarne valem signatuuris Σ on valem selles signatuuris.
2. Kui φ ja ψ on valemid signatuuris Σ , siis $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Rightarrow \psi$ on valemid signatuuris Σ .
3. Kui φ on valem signatuuris Σ , siis $\forall x \varphi$ ja $\exists x \varphi$ on valemid signatuuris Σ .

Lühiduse mõttes defineerime valemi φ eituse $\neg\varphi$ kui

$$\neg\varphi := \varphi \Rightarrow \perp,$$

ning kahe valemi samaväärsuse kui

$$\varphi \Leftrightarrow \psi := (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi).$$

Üldtuntud kokkulepete järgi loeme loogilise sümboli \wedge seotust tugevamaks kui \vee seotust ning omakorda \vee seotust tugevamaks kui \Rightarrow seotust. Seega näiteks valemit $\varphi \vee \psi \wedge \theta \Rightarrow \theta$ loeme kui valemit $(\varphi \vee (\psi \wedge \theta)) \Rightarrow \theta$.

Kõigi esimest järku predikaatloogika valemite hulka signatuuris Σ tähistame sümboliga FO_{Σ} . Valemite süntaktilise võrduse tähistamiseks kasutame sümbolit \doteq , see tähendab, et valemid on süntaktiliselt võrdsed, kui nendele vastavad sümboljärjendid on identsed. Definiitsioonipõhist võrdust tähistame sümboliga $\stackrel{def}{=}$.

Näide 1.6. Valemid $x = y \Rightarrow y = x$ ja $x = y \Rightarrow x = y$ ei ole süntaktiliselt võrdsed. Valemid $\forall x(x + 0 = x)$ ja $\forall x(x + 0 = x)$ on süntaktiliselt võrdsed.

Definiitsioon 1.7. Olgu φ valem ja t term signatuuris $\Sigma = \langle \mathcal{C}, \mathcal{F}, \mathcal{P} \rangle$. Defneerime hulga $FV(t)$ ja $FV(\varphi)$ rekursiivselt sõltuvalt φ ja t kujust.

Termi t korral:

1. $FV(x) = \{x\}$,
2. $FV(c) = \emptyset, \quad c \in \mathcal{C}$,
3. $FV(f(t_1, \dots, t_n)) = FV(t_1) \cup \dots \cup FV(t_n). \quad f \in \mathcal{F}$

Valemi φ korral:

1. $FV(\perp) = \emptyset$,
2. $FV(t = s) = FV(t) \cup FV(s)$,
3. $FV(P(t_1, \dots, t_n)) = FV(t_1) \cup \dots \cup FV(t_n), \quad P \in \mathcal{P}$,
4. $FV(\psi \wedge \theta) = FV(\psi \Rightarrow \theta) = FV(\psi \vee \theta) = FV(\psi) \cup FV(\theta)$,

$$5. FV(\forall x \psi) = FV(\psi) \setminus \{x\},$$

$$6. FV(\exists x \psi) = FV(\psi) \setminus \{x\}.$$

Definitsioon 1.8. Olgu φ valem signatuuris Σ . Muutuja x on valemis φ **vaba** parajasti siis, kui $x \in FV(\varphi)$ või ta ei esine valemis φ . Muutuja on valemis φ **seotud** parajasti siis, kui ta ei ole vaba. Valemit φ , mille korral $FV(\varphi) = \emptyset$, nimetatakse **kinniseks**.

Näide 1.9. Signatuuri $\Sigma = \langle \mathbf{0}; \mathbf{s}, +, \cdot \rangle$ valemis $\forall x \exists y (x + y = z)$ on muutujad x ja y seotud, z on aga vaba muutuja, sest

$$\begin{aligned} FV(\forall x \exists y (x + y = z)) &= FV(\exists y (x + y = z)) \setminus \{x\} \\ &= (FV(x + y = z) \setminus \{y\}) \setminus \{x\} \\ &= ((FV(x + y) \cup FV(z)) \setminus \{y\}) \setminus \{x\} \\ &= ((FV(x) \cup FV(y) \cup FV(z)) \setminus \{y\}) \setminus \{x\} \\ &= ((\{x\} \cup \{y\} \cup \{z\}) \setminus \{y\}) \setminus \{x\} \\ &= \{z\}. \end{aligned}$$

Edaspidi kasutame kvantoritega valemite kirjaviiside $\forall z \forall x \dots \forall y \varphi$ ja $\exists z \exists x \dots \exists y \psi$ asemel ka lühendatud kirjaviise $\forall z, x, \dots, y \varphi$ ja $\exists z, x, \dots, y \psi$.

Samuti läheb meil vaja substitutsiooni mõistet.

Definitsioon 1.10. Olgu φ valem ja t term signatuuris Σ . Muutuja x **substitutsiooniks** termiga t nimetatakse muutuja x kõigi vabade esinemiste asendamist valemis φ termiga t (tähistame $\varphi[t/x]$) järgnevalt:

1. Kui φ on atomaarne valem, tähistab $\varphi[t/x]$ valem, kus asendame kõik temas esinevad muutujad x termiga t .
2. Kui φ on kujul $\psi \wedge \theta$, $\psi \vee \theta$ või $\psi \Rightarrow \theta$, siis

- * $(\psi \wedge \theta)[t/x] := \psi[t/x] \wedge \theta[t/x]$
- * $(\psi \vee \theta)[t/x] := \psi[t/x] \vee \theta[t/x]$
- * $(\psi \Rightarrow \theta)[t/x] := \psi[t/x] \Rightarrow \theta[t/x]$

3. Kui φ on kujul $\forall y \psi$ või $\exists y \psi$, siis

$$\begin{aligned}
 * (\forall y \psi)[t/x] &:= \begin{cases} \forall y \psi, & \text{kui } x = y \\ \forall y (\psi[t/x]), & \text{kui } y \notin FV(t) \\ (\forall z \psi[z/y])[t/x], & \text{muud juhud; } z \notin FV(\psi) \text{ ja } z \notin FV(t) \end{cases} \\
 * (\exists y \psi)[t/x] &:= \begin{cases} \exists y \psi, & \text{kui } x = y \\ \exists y (\psi[t/x]), & \text{kui } y \notin FV(t) \\ (\exists z \psi[z/y])[t/x], & \text{muud juhud; } z \notin FV(\psi) \text{ ja } z \notin FV(t) \end{cases}
 \end{aligned}$$

Näide 1.11. Selgitame substituutsiooni mõistet kahe näitega:

1. Olgu φ kujul $\forall x \exists y (x + y = z)$, siis

$$\begin{aligned}
 \varphi[0/z] &\doteq (\forall x \exists y (x + y = z))[0/z] \stackrel{def}{=} \forall x ((\exists y (x + y = z))[0/z]) \\
 &\stackrel{def}{=} \forall x ((\exists y ((x + y = z)[0/z]))) \\
 &\stackrel{def}{=} \forall x ((\exists y ((x + y = 0)))) \\
 &\stackrel{def}{=} \forall x \exists y (x + y = 0).
 \end{aligned}$$

2. Olgu ψ kujul $\forall x (x = y)$, siis

$$\begin{aligned}
 \psi[x + 1/y] &\doteq \forall x (x = y)[x + 1/y] \\
 &\stackrel{def}{=} \forall z (z = y)[x + 1/y] \\
 &\stackrel{def}{=} \forall z ((z = y)[x + 1/y]) \\
 &\stackrel{def}{=} \forall z (z = x + 1).
 \end{aligned}$$

Enne teooria mõiste defineermist anname mitteformaalse definitsiooni tuletusreegli ja loogilise aksiomi kohta.

Definitsioon 1.12. Olgu $\varphi_1, \dots, \varphi_n, \psi$ valemid signatuuris Σ . **Tuletusreegliks** nimetame eeskirja saamaks valemitest $\varphi_1, \dots, \varphi_n$ valem ψ , mida tähistame sümboliga

$$\frac{\varphi_1 \dots \varphi_n}{\psi},$$

valemeid $\varphi_1, \dots, \varphi_n$ nimetame tuletusreegli **eeldusteks** ja valemit ψ **järelduseks**. Juhul kui tuletusreegli eelduste hulk on tühi, ütleme, et tegemist on **loogilise aksiomiga**.

Definitsioon 1.13. Olgu Σ signatuur ning \mathcal{A} esimest järku predikaatloogika valemite hulk signatuuris Σ , kus \mathcal{A} võib olla ka tühi. **Teooriaks** \mathcal{T} nimetame kolmikut $\langle \Sigma; \mathcal{A}; \mathcal{R} \rangle$, kus \mathcal{R} on mittetühi tuletusreeglite ja loogiliste aksiomide hulk koos reegliga **Ax**, mille defineerime kui:

$$\frac{\varphi \in \mathcal{A}}{\varphi} \mathbf{Ax}$$

See tähendab, et kui $\varphi \in \mathcal{A}$, siis φ on vahetult tuletatav ilma eeldusteta. Hulga \mathcal{A} valemite nimetame teooria \mathcal{T} **omaaksiomideks**.

Edaspidi teeme eelduse, et teoorias $\mathcal{T} = \langle \Sigma; \mathcal{A}; \mathcal{R} \rangle$ on hulgas \mathcal{R} olemas vähemalt tuletussüsteem \mathcal{I} ilma kvantorite kohta käivate reegliteta, s.t. nii öelda lausearvutuslik tuletussüsteem.

Näide 1.14. Olgu $\Sigma = \langle \mathbf{1}; \cdot; \cdot \rangle$. Rühmateoorias $\langle \Sigma; \mathcal{A}; \mathcal{I}_{\text{LEM}} \rangle$ (vaata \mathcal{I}_{LEM} jaoks definitsiooni 1.17) on omaaksiomideks parajasti valemid:

- * $\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$,
- * $\forall x (x \cdot \mathbf{1} = x)$,
- * $\forall x (\mathbf{1} \cdot x = x)$,

$$* \forall x \exists y (x \cdot y = \mathbf{1}),$$

$$* \forall x \exists y (y \cdot x = \mathbf{1}).$$

Definitsioon 1.15. Tuletuseks ehk formaalseks tõestuseks teoorias \mathcal{T} nimetatakse lõplikku valemite jada $\varphi_1, \dots, \varphi_n$, kus iga valem φ_i ($1 \leq i \leq n$) on kas loogiline aksiom, omaaksiom või vahetult tuletatav mõnedest selle jada eelmistest valemitest teooria \mathcal{T} mingi tuletusreegliga.

Definitsioon 1.16. Valemit φ nimetatakse **tuletatavaks** teoorias \mathcal{T} (tähistame $\mathcal{T} \vdash \varphi$ või ka $\vdash_{\mathcal{T}} \varphi$), kui leidub tuletus, mille viimaseks valemiks on φ .

Mõnikord võime kasutada ka kirjaviisi $\varphi_1, \dots, \varphi_n \vdash \psi$ ütlemaks, et eeldades valemite $\varphi_1, \dots, \varphi_n$ kehtivust, saame tuletada valemi ψ . Siiski proovime sellisest kirjapildist hoiduda ning üldiselt märgime ära, kas sümbolis $H \vdash \psi$ tähistab H teooriat või valemite hulka. Lühiduse mõttes tähistame mõnikord lõplikku valemite jada $\varphi_1, \dots, \varphi_n$ sümboliga Γ .

Järgnevalt formuleerime konkreetse tuletussüsteemi intuitsionistliku esimest järku predikaatloogika jaoks, mille pakkus välja Gödel [6].

Definitsioon 1.17. Intuitsionistlikus esimest järku predikaatloogikas on parajasti järgnevad tuletusreeglid ja loogilised aksiomid:

Tuletusreeglid:

$$\frac{\varphi \quad \varphi \Rightarrow \psi}{\psi} \text{ R1}$$

$$\frac{\varphi \Rightarrow \psi \quad \psi \Rightarrow \theta}{\varphi \Rightarrow \theta} \text{ R2}$$

$$\frac{\varphi \Rightarrow \psi}{\theta \vee \varphi \Rightarrow \theta \vee \psi} \text{ R3}$$

$$\frac{\varphi \Rightarrow (\psi \Rightarrow \theta)}{\varphi \wedge \psi \Rightarrow \theta} \text{ R4}$$

$$\frac{\varphi \wedge \psi \Rightarrow \theta}{\varphi \Rightarrow (\psi \Rightarrow \theta)} \text{ R5}$$

$$\frac{\varphi \Rightarrow \psi}{\varphi \Rightarrow \forall x \psi} \text{ R6, } x \notin FV(\varphi)$$

$$\frac{\varphi \Rightarrow \psi}{\exists x \varphi \Rightarrow \psi} \text{ R7, } x \notin FV(\psi)$$

Loogilised aksioomid:

$$\frac{}{\varphi \vee \varphi \Rightarrow \varphi} \text{ A1} \quad \frac{}{\varphi \Rightarrow \varphi \wedge \varphi} \text{ A2} \quad \frac{}{\varphi \Rightarrow \varphi \vee \psi} \text{ A3} \quad \frac{}{\varphi \wedge \psi \Rightarrow \varphi} \text{ A4}$$

$$\frac{}{\varphi \vee \psi \Rightarrow \psi \vee \varphi} \text{ A5} \quad \frac{}{\varphi \wedge \psi \Rightarrow \psi \wedge \varphi} \text{ A6} \quad \frac{}{\forall x \varphi \Rightarrow \varphi[t/x]} \text{ A7}$$

$$\frac{}{\varphi[t/x] \Rightarrow \exists x \varphi} \text{ A8} \quad \frac{}{\perp \Rightarrow \theta} \text{ A9}$$

Võrdusaksioomid:

1. $\frac{}{t = t} \text{ V1}$
2. $\frac{}{s_1 = t_1 \wedge \dots \wedge s_n = t_n \Rightarrow f(s_1, \dots, s_n) = f(t_1, \dots, t_n)} \text{ V2}$
3. $\frac{}{s = t \Rightarrow (\varphi[s/z] \Rightarrow \varphi[t/z])} \text{ V3}$

kus $s, t, s_1, \dots, s_n, t_1, \dots, t_n$ on termid, f on funktsionaalsümbol ja φ valem. On võimalik näidata, et selliseid võrdusaksioome rahudav seos on sümmeetriline ja transitiivne. Lühiduse mõttes kirjutame mõnikord ka $\neg(x = y)$ asemel $x \neq y$.

Intuitsionistlikust loogikasüsteemist saadakse klassikaline, kui lisatakse veel aksiomina **väljastatud kolmanda seadus** (ingl *Law of the Excluded Middle*):

$$\frac{}{\varphi \vee \neg\varphi} \text{ LEM}$$

Tähistamaks kõigi eelnevalt sissetoodud intuitsionistliku tuletussüsteemi reegleid ja aksioome, kasutame sümbolit \mathcal{I} (definiitsioon 1.17). Rõhutamiseks, et tegemist on klassikalise tuletussüsteemiga, kirjutame \mathcal{I}_{LEM} .

Siinkohal kommenteerime, et aksiom A9 täpsustab vastuolu \perp tähendust. See tähendab, et kui teoorias \mathcal{T} tuletussüsteemiga \mathcal{I} või \mathcal{I}_{LEM} on tuletatav vastuolu, siis kasutades aksiomi A9 ja tuletusreeglit R1, on võimalik tuletada iga suvaline

valem. See aga muudab antud teooria triviaalseks. Seega saame rääkida teooria (mitte)korrektsusest.

Definitsioon 1.18. Teooriat \mathcal{T} nimetatakse **vasturääkivaks** ehk **mittekorrekts**eks, kui leidub selline valem φ (teoorias \mathcal{T}), et $\mathcal{T} \vdash \varphi$ ja $\mathcal{T} \vdash \neg\varphi$.

Nimelt kui teooria \mathcal{T} on mittekorrektne, siis kuna defineerisime $\neg\varphi$ kui $\varphi \Rightarrow \perp$, saame tuletada teoorias vastuolu $\mathcal{T} \vdash \perp$. Teooriat nimetatakse **korrekts**eks, kui ta pole vasturääkiv.

Olgu siinkohal mainitud, et eelnevalt formuleeritud tuletussüsteem \mathcal{I} ei ole üheselt määratud. See tähendab, et leidub teistsuguste reeglite ja loogiliste aksioomidega tuletussüsteeme, mis siiski teooria tugevuse mõttes on samaväärsed ehk tuletatavate valemite hulk on sama.

Samuti kehtivad tuletussüsteemis \mathcal{I} mõned head omadused.

Teoreem 1.19 (Deduktsiooniteoreem [11]). *Olgu Γ valemite hulk signatuuris Σ ja φ valem signatuuris Σ . Kui $\Gamma, \varphi \vdash_{\mathcal{I}} \psi$, siis $\Gamma \vdash_{\mathcal{I}} \varphi \Rightarrow \psi$.*

Sisuliselt ütleb deduktsiooniteoreem meile, et juhul kui tahame tõestada valemit kujul $\varphi \Rightarrow \psi$, piisab eeldada, et φ kehtib, ning seejärel näidata, et sellest järel-dub ψ . Selline argumenteerimine lubab meil järgnevaid tõestusi lihtsutada. Veelgi enam, tuleb välja, et tuletussüsteem \mathcal{I} on samaväärne niinimetatud *loomuliku tuletussüsteemiga*. Seda tuletussüsteemi me defineerima ei hakka, kuid lugeja võib selle leida allikast [11].

Lause 1.20. Kehtib järgnev:

$$\vdash_{\mathcal{I}} \varphi(y) \Rightarrow \forall x \varphi(x),$$

kus $x \notin FV(\varphi)$, $y \in FV(\varphi)$.

Tõestus. Eeldame, et $\varphi(y)$ kehtib. Kuna

$$\vdash_{\mathcal{I}} \varphi(y) \Rightarrow \varphi(y) \wedge \varphi(y) \text{ ja } \vdash_{\mathcal{I}} \varphi(y) \wedge \varphi(y) \Rightarrow \varphi(y)$$

vastavalt aksioomidele A2 ja A4, siis rakendades neile tuletusreeglit R2, saame, et

$$\vdash_{\mathcal{I}} \varphi(y) \Rightarrow \varphi(y). \quad (1)$$

Nüüd rakendades tuletusele (1) reeglit R6, saame, et

$$\varphi(y) \Rightarrow \forall x \varphi(x). \quad (2)$$

Kuna eeldasime, et $\varphi(y)$ kehtib, saame reegluga R1 valemitest $\varphi(y)$ ja $\varphi(y) \Rightarrow \forall x \varphi(x)$ tuletada valemi $\forall x \varphi(x)$, täpselt nii nagu tahtsime. ■

Eelnev lause annab meile viisi, kuidas tõestada valemeid, mis on kujul $\forall x \varphi(x)$. Sisuliselt piisab näitada, et valem $\varphi(y)$ kehtib, kus $y \in FV(\varphi)$ ehk y on nii öelda suvaline.

1.2 Peano aritmeetika

Vaatleme edasises ühte tuntumat formaalset aksiomaatilist teooriat nimega **Peano aritmeetika** (edaspidi ka lihtsalt **PA**). Peano aritmeetika on teooria $\langle \Sigma, \mathcal{A}, \mathcal{I}_{\text{LEM}} \rangle$, kus signatuur $\Sigma = \langle \mathbf{0}; \mathbf{s}, +, \cdot; \rangle$ ¹ ning omaaksioomideks on parajasti valemid:

P1. $\forall x \neg(\mathbf{0} = \mathbf{s}x),$

P2. $\forall x \forall y (\mathbf{s}x = \mathbf{s}y \Rightarrow x = y),$

P3. $\forall x (x + \mathbf{0} = x),$

¹Tihti kohtab kirjanduses **PA** signatuurina $\Sigma = \langle \mathbf{0}; \mathbf{s}, +, \cdot, = \rangle$, kuid kuna me oleme predikaatarvutuses võrdusmärgi = juba sisse arvestanud, kasutame signatuuri $\langle \mathbf{0}; \mathbf{s}, +, \cdot; \rangle$.

P4. $\forall x \forall y (x + sy = s(x + y))$,

P5. $\forall x (x \cdot \mathbf{0} = \mathbf{0})$,

P6. $\forall x \forall y (x \cdot sy = (x \cdot y) + x)$,

ja induktsiooniskeem

P7. $(\varphi(\mathbf{0}) \wedge \forall y (\varphi(y) \Rightarrow \varphi(sy))) \Rightarrow \forall x \varphi(x)$;

nimelt on **P7** aksioomiskeem ja defineerib ära lõpmatu hulga valemeid, seejuures konkreetse valemi saamiseks asendame omakorda valemi φ mingi konkreetse valemiga. Konstandist $\mathbf{0}$ mõtleme, kui tavalisest naturaalarvust 0. Funktsionaalsümbol s tähistab järgmise elemendi võtmist; seega sellise signatuuriga saame kirja panna kõik naturaalarvud, mõeldes sümbolist $\mathbf{0}$ kui arvust 0, sümbolist $s\mathbf{0}$ kui arvust 1, sümbolist $ss\mathbf{0}$ kui arvust 2 jne. Sellisel juhul näeme, et aksioom **P1** ütleb, et arv 0 ei järgne ühelegi arvule. Aksioom **P2** ütleb, et s on injektiivne tehe. Aksioomid **P3** kuni **P6** defineerivad liitmistehte $+$ ja korrutamistehte \cdot .

Näitame, et Peano aritmeetikas saab tõestada mõningaid teadatud omadusi naturaalarvude kohta.

Lause 1.21. $\mathbf{PA} \vdash \forall x (\mathbf{0} + x = x)$.

Tõestus. Tõestame väite rakendades induktsiooniskeemi valemile $\varphi(x) := \mathbf{0} + x = x$.

Induktsiooni baas. $\varphi(\mathbf{0})$ on valem $\mathbf{0} + \mathbf{0} = \mathbf{0}$, mis kehtib tänu aksioomile **P3**.

Induktsiooni samm. Näitamaks, et $\forall y (\varphi(y) \Rightarrow \varphi(sy))$ kehtib, piisab lause 1.20 põhjal näidata, et kehtib valem $\varphi(z) \Rightarrow \varphi(sz)$. Eeldame, et $\mathbf{PA} \vdash \varphi(z)$ ehk

$$\mathbf{PA} \vdash \mathbf{0} + z = z. \tag{3}$$

Nüüd saame, et

$$\mathbf{0} + sz \stackrel{\mathbf{P4}}{=} s(\mathbf{0} + z) \stackrel{3}{=} sz.$$

Seega kokkuvõttes kehtib valem $\forall y(\varphi(y) \Rightarrow \varphi(\mathbf{s}y))$. Rakendades induktsiooniskeemi valemitele $\varphi(\mathbf{0})$ ja $\forall y(\varphi(y) \Rightarrow \varphi(\mathbf{s}y))$, olemegi saanud, et $\mathbf{PA} \vdash \forall x (\mathbf{0} + x = x)$. ■

Järgmine lause ütleb meile, et $\mathbf{s0}$ on korrutamise suhtes ühikelement ehk $x \cdot 1 = x$.

Lause 1.22. $\mathbf{PA} \vdash \forall x (x \cdot \mathbf{s0} = x)$.

Tõestus. Tõestame väite rakendades induktsiooniga valemi $\psi(x) := x \cdot \mathbf{s0} = x$ peal.

Induktsiooni baas.

$$\mathbf{0} \cdot \mathbf{s0} \stackrel{\mathbf{P6}}{=} \mathbf{0} \cdot \mathbf{0} + \mathbf{0} \stackrel{\mathbf{P5}}{=} \mathbf{0} + \mathbf{0} \stackrel{\mathbf{P3}}{=} \mathbf{0}.$$

Induktsiooni samm. Induktsiooni samm on ilmne, sest

$$\mathbf{s}y \cdot \mathbf{s0} \stackrel{\mathbf{P6}}{=} \mathbf{s}y \cdot \mathbf{0} + \mathbf{s}y \stackrel{\mathbf{P5}}{=} \mathbf{0} + \mathbf{s}y \stackrel{1.21}{=} \mathbf{s}y,$$

seega kokkuvõttes $\forall x (x \cdot \mathbf{s0} = x)$. ■

1.3 Klassikalise loogika interpreteerimine intuitsionistlikus loogikas

Enne \mathbf{PA} korrektsuse tõestamist kirjeldame selle tõestuse ideed. Sisuliselt interpreteeritakse \mathbf{PA} teooriat Gödeli süsteemis \mathbf{T} , mille kohta saab näidata, et see rahuldab Church-Rosser'i printsiipi 3.5, mille tagajärjel saame teooria \mathbf{T} enda korrektsuse. Seega peab ka \mathbf{PA} ise olema korrektne. Tõestuses taandub \mathbf{PA} korrektsus vastava intuitsionistliku versiooni korrektsusele nimega Heytingi aritmeetika (edaspidi ka \mathbf{HA}). Seega $\mathbf{HA} = \langle \Sigma, \mathcal{A}, \mathcal{I} \rangle$, kus Σ ja \mathcal{A} on samad, mis teoorias \mathbf{PA} . Et interpreteerida Peano aritmeetikas tuletatavaid valemteid teooria \mathbf{HA} tuletatavateks valemiteks, on meil vaja kõigepealt N -interpretatsiooni mõistet.

Definitsioon 1.23 (N -interpretatsioon [1]). Olgu Σ signatuur. N -interpretatsioon on kujutus $(-)^N : FO_\Sigma \rightarrow FO_\Sigma$, mille defineerime rekursiivselt:

1. $\varphi^N := \neg\neg\varphi$, kui φ on atomaarne; $\perp^N := \perp$,
2. $(\varphi \wedge \psi)^N := \varphi^N \wedge \psi^N$,
3. $(\varphi \vee \psi)^N := \neg(\neg\varphi^N \wedge \neg\psi^N)$,
4. $(\varphi \Rightarrow \psi)^N := \varphi^N \Rightarrow \psi^N$,
5. $(\forall x \varphi(x))^N := \forall x \varphi(x)^N$,
6. $(\exists x \varphi(x))^N := \neg\forall x \neg\varphi(x)^N$.

Et saaksime tõestada teoreemi 1.27, läheb meil vaja Harropi valemi mõistet.

Definitsioon 1.24 (Harropi valem [11]). Harropi valemite klass defineeritakse järgnevalt:

1. iga atomaarne valem on Harropi valem,
2. kui φ ja ψ on Harropi valemit, siis $\varphi \wedge \psi$ on Harropi valem,
3. kui φ on Harropi valem, siis $\forall x \varphi$ on Harropi valem,
4. kui ψ on Harropi valem, siis $\varphi \Rightarrow \psi$ on Harropi valem, suvalise valemi φ korral.

Kuigi intuitsionistlikus loogikas (erinevalt klassikalisest) ei kehti iga suvalise valemi φ korral valem $\neg\neg\varphi \Rightarrow \varphi$, kehtib aga järgmine tulemus.

Lemma 1.25 ([11]). Olgu $H = \langle \Sigma, \mathcal{A}, \mathcal{I} \rangle$, s.t. teooria intuitsionistliku tuletussüsteemiga, kus valem φ_H on Harropi valem, mis on konstrueeritud valemitest kujul $\neg\neg\psi$, kus ψ on atomaarne, siis kehtib $H \vdash \varphi_H \Leftrightarrow \neg\neg\varphi_H$.

Lihtne on näha, et iga valemi ξ korral ξ^N rahuldab lemma 1.25 eeldusi, seega kehtib ka $H \vdash \xi^N \Leftrightarrow \neg\neg\xi^N$.

Lemma 1.26 (kontrapositiiv). Olgu $H = \langle \Sigma, \mathcal{A}, \mathcal{I} \rangle$, siis iga valemi φ ja ψ korral $H \vdash (\varphi^N \Rightarrow \psi^N) \Leftrightarrow (\neg\psi^N \Rightarrow \neg\varphi^N)$.

Tõestus. TARVILIKKUS. Eeldame, et

$$H \vdash \varphi^N \Rightarrow \psi^N \tag{4}$$

ning näitame, et $H \vdash \neg\psi^N \Rightarrow \neg\varphi^N$. Selleks oletame, et $H \vdash \neg\psi^N$ ehk

$$H \vdash \psi^N \Rightarrow \perp, \tag{5}$$

nüüd rakendades reeglit $R2$ tuletuste (4) ja (5) peal saame, et $H \vdash \varphi^N \Rightarrow \perp$ ehk $H \vdash \neg\varphi^N$, mida tahtsimegi näidata.

PIISAVUS. Eeldame, et

$$H \vdash \neg\psi^N \Rightarrow \neg\varphi^N \tag{6}$$

ning näitame, et $H \vdash \varphi^N \Rightarrow \psi^N$. Selleks oletame, et

$$H \vdash \varphi^N,$$

mis lemma 1.25 põhjal on samaväärne sellega, et $H \vdash \neg\neg\varphi^N$ ehk

$$H \vdash \neg\varphi^N \Rightarrow \perp. \tag{7}$$

Nüüd rakendades reeglit $R2$ tuletuste (6) ja (7) peal, saame, et $H \vdash \neg\psi^N \Rightarrow \perp$ ehk $H \vdash \neg\neg\psi^N$, mis lemma 1.25 kohaselt on samaväärne sellega, et $H \vdash \psi^N$, mida tahtsimegi näidata. ■

Märkus. Märgime ära, et intuitsionistlikus predikaatloogikas ei kehti valem $(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\psi \Rightarrow \neg\varphi)$ iga suvalise φ ja ψ korral.

Teoreem 1.27 ([11]). Olgu $H = \langle \Sigma; \emptyset; \mathcal{I} \rangle$, s.t. intuitsionistliku tuletussüsteemiga teooria, mille omaaksoomide hulk on tühi ja H^C olgu saadud lisades teooriale H

väljastatud kolmanda seaduse, s.t. $H^C = \langle \Sigma; \emptyset, \mathcal{I}_{LEM} \rangle$. Siis

$$H^C \vdash \xi \Leftrightarrow H \vdash \xi^N.$$

Tõestus. PIISAVUS. Ilmne, sest ξ^N ja ξ on klassikaliselt samaväärsed.

TARVILIKKUS. Eeldame, et $H^C \vdash \xi$ ning tõestame, et $H \vdash \xi^N$ induktsiooniga valemi ξ tuletuse pikkuse k järgi.

Induktsiooni baas. Olgu $k = 1$, siis ξ peab olema aksioom.

Kui $\xi \doteq \varphi \vee \varphi \Rightarrow \varphi$, siis $\xi^N \doteq \neg(\neg\varphi^N \wedge \neg\varphi^N) \Rightarrow \varphi^N$, mis on samaväärne valemiga $\neg\neg\varphi^N \Rightarrow \varphi^N$, see kehtib aga tänu lemmale 1.25.

Kui $\xi \doteq \varphi \Rightarrow \varphi \vee \psi$, siis $\xi^N \doteq \varphi^N \Rightarrow \neg(\neg\varphi^N \wedge \neg\psi^N)$, kust samaväärsed kontrapositiivi võtmisel saame $\neg\neg(\neg\varphi^N \wedge \neg\psi^N) \Rightarrow \neg\varphi^N$. Rakendades lemmat 1.25 saadud valemile, saame samaväärsed valemi $\neg\varphi^N \wedge \neg\psi^N \Rightarrow \neg\varphi^N$, mis kehtib aksioomi A4 tõttu.

Kui $\xi \doteq \varphi[t/x] \Rightarrow \exists x \varphi$, siis $\xi^N \doteq \varphi^N[t/x] \Rightarrow \neg\forall x \neg\varphi^N$, kust kontrapositiivi võtmisel saame $\neg\neg\forall x \neg\varphi^N \Rightarrow \neg\varphi^N[t/x]$. Jällegi lemma 1.25 põhjal on see samaväärne valemiga $\forall x \neg\varphi^N \Rightarrow \neg\varphi^N[t/x]$, mis kehtib tänu aksioomile A7.

Kui $\xi \doteq \varphi \vee \neg\varphi$, siis $\xi^N \doteq \neg(\neg\varphi^N \wedge \neg\neg\varphi^N)$, mis ilmselgelt kehtib. Ülejäänud juhud on triviaalsed ja on jäetud läbimõtlemiseks lugejale.

Induktsiooni samm. Induktsiooni sammus eeldame, et kui tuletuse $H^C \vdash \xi$ pikkus on k , siis $H \vdash \xi^N$. Eeldame, et tuletuse $H^C \vdash \xi$ pikkus on $k + 1$.

Kui viimane reegel mida rakendati on R3, siis $\xi \doteq \theta \vee \varphi \Rightarrow \theta \vee \psi$ ning induktsiooni eelduse kohaselt

$$H \vdash \varphi^N \Rightarrow \psi^N.$$

Siis $\xi^N \doteq \neg(\neg\theta^N \wedge \neg\varphi^N) \Rightarrow \neg(\neg\theta^N \wedge \neg\psi^N)$, kust kontrapositiivi võttes ja lemmat

1.25 rakendades saame, et ξ^N on samaväärne valemiga

$$\neg\theta^N \wedge \neg\psi^N \Rightarrow \neg\theta^N \wedge \neg\varphi^N.$$

Kasutades induktsiooni eeldust kehtib ka $\neg\psi^N \Rightarrow \neg\varphi^N$ ning valemitest $\neg\theta^N \wedge \neg\psi^N \Rightarrow \neg\theta^N$ ja $\neg\theta^N \wedge \neg\psi^N \Rightarrow \neg\psi^N$ saamegi, et

$$H \vdash \neg\theta^N \wedge \neg\psi^N \Rightarrow \neg\theta^N \wedge \neg\varphi^N.$$

Kui viimane reegel mida rakendati on *R7*, siis $\xi \doteq \exists x \varphi \Rightarrow \psi$ ning $\xi^N \doteq \neg\forall x \neg\varphi^N \Rightarrow \psi^N$ ning induktsiooni eelduse kohaselt

$$H \vdash \varphi^N \Rightarrow \psi^N.$$

Seega ka $H \vdash \neg\psi^N \Rightarrow \neg\varphi^N$ ning võttes valemist ξ^N kontrapositiivi saame, et $\neg\psi^N \Rightarrow \neg\neg\forall x \neg\varphi^N$, kus lemmat 1.25 rakendades saame, et ξ^N on samaväärne valemiga

$$\neg\psi^N \Rightarrow \forall x \neg\varphi^N.$$

Kasutades valemis $\neg\psi^N \Rightarrow \neg\varphi^N$ reeglit *R6*, saamegi, et $H \vdash \neg\psi^N \Rightarrow \forall x \neg\varphi^N$. Lihtne on näha, et ülejäänud reeglid on vahetult tuletavad. ■

Teoreem 1.28. *Kui $PA \vdash \varphi$, siis $HA \vdash \varphi^N$.*

Tõestus. Tänu teoreemile 1.27 piisab näidata, et väide kehtib, kui φ on **PA** omaaksioom. Aksioomide **P1** kuni **P6** korral on väide vahetult tuletatav kasutades lemmat 1.25. Näitame, et väide kehtib induktsiooniskeemi korral. Ka see on triviaalne, sest

$$\begin{aligned} (\varphi(\mathbf{0}) \wedge \forall y(\varphi(y) \Rightarrow \varphi(\mathbf{sy})) \Rightarrow \forall x \varphi(x))^N &\doteq (\varphi(\mathbf{0})^N \wedge \forall y(\varphi(y)^N \Rightarrow \varphi(\mathbf{sy})^N)) \Rightarrow \\ &(\forall x \varphi(x)^N) \end{aligned}$$

ning kuna induktsiooniskeem on **HA** aksiom, rakendame seda valemile $\varphi(x)^N$. ■

Järeldus 1.29. *PA* korrektsus on samaväärne *HA* korrektsusega.

Tõestus. Eelmisest teoreemist saame, et kui **PA** $\vdash \varphi$ ja **PA** $\vdash \neg\varphi$, siis **HA** $\vdash \varphi^N$ ja **HA** $\vdash \neg\varphi^N$, sest

$$(\neg\varphi)^N \doteq (\varphi \Rightarrow \perp)^N \doteq \varphi^N \Rightarrow \perp^N \doteq \varphi^N \Rightarrow \perp \doteq \neg\varphi^N.$$

Vastupidine on ilmne, ning seega saame taandada **PA** korrektsuse teooria **HA** korrektsusele. ■

2 Dialektika interpretatsioon

Selles peatükis anname ülevaate Gödeli süsteemist **T** ja Dialektika interpretatsioonist, lähtudes allikatest [1, 3, 5, 11].

2.1 Gödeli süsteem **T**

Definitsioon 2.1. Süsteemi **T** tüübid defineeritakse induktiivselt kui:

1. \mathbb{N} on tüüp², mida kutsutakse **naturaalarvude tüübiks**,
2. Kui σ ja τ on tüübid, siis $\sigma \rightarrow \tau$ on tüüp, mida kutsutakse **funktsiooni-tüübiks**,
3. Kui σ ja τ on tüübid, siis $\sigma \times \tau$ on tüüp, mida kutsutakse **korrutistüübiks** tüüpidest σ ja τ .

Tüüpe tähistame sümbolitega $\sigma, \tau, \rho, \sigma_1, \sigma_2, \dots$

Järgnevalt defineerime süsteemi **T** termid ning relatsiooni $t : \sigma$, mida loeme kui „ t on tüübiga σ “.

Definitsioon 2.2. Süsteemis **T** defineeritakse **tüübitud termid** induktiivselt:

1. Kõik muutujad $x^\tau, y^\tau, z^\tau \dots$ on termid tüübiga τ ,
2. Kui $s : \sigma$ ja $t : \sigma \rightarrow \tau$, siis $t(s) : \tau$,
3. $0 : \mathbb{N}$,
4. $s : \mathbb{N} \rightarrow \mathbb{N}$,
5. Kui $s : \sigma$ ja $t : \tau$, siis $(s, t) : \sigma \times \tau$,

²Kirjanduses võib ka kohata, et tähistuse \mathbb{N} asemel kasutatakse sümbolit 0 ; see aga võib segadust tekitada arvuga 0 ise. Seega meie kasutame sümboolikat \mathbb{N} .

6. Iga tüübi σ ja iga tüübi τ korral $\pi_1 : \sigma \times \tau \rightarrow \sigma$ ja $\pi_2 : \sigma \times \tau \rightarrow \tau$,
7. Iga tüübi σ ja iga tüübi τ korral $K_{\sigma,\tau} : \sigma \rightarrow \tau \rightarrow \sigma$,
8. Iga tüübi ρ , iga tüübi σ ja iga tüübi τ korral $S_{\rho,\sigma,\tau} : (\rho \rightarrow \sigma \rightarrow \tau) \rightarrow (\rho \rightarrow \sigma) \rightarrow (\rho \rightarrow \tau)$,
9. Iga tüübi σ korral $R_\sigma : \sigma \rightarrow (\mathbb{N} \rightarrow \sigma \rightarrow \sigma) \rightarrow \mathbb{N} \rightarrow \sigma$.

Terme tähistame sümbolitega $m, p, r, s, t, v, t_1, t_2, \dots$

Lühiduse mõttes kirjutame funktsiooni aplikatsiooni $t(s)$ asemel ka lihtsalt ts , kus $t : \sigma \rightarrow \tau$ ja $s : \sigma$. Funktsioonide mitmekordsel rakendamisel loeme assotsiatiivsust vasakpoolseks, see tähendab, et kui $t : \rho \rightarrow \sigma \rightarrow \tau$, $r : \rho$ ja $s : \sigma$, siis aplikatsiooni $t(r, s) : \tau$ või $trs : \tau$ all mõtleme kirjutist $(t(r))(s)$. Kui kontekstist on selge, mis tüüpi termidega me parasjagu tegeleme, jätame võrdusmärgi alaindeksi kirjutamata. Samamoodi toimime ka muutujate ülaindeksiga ja termide $K_{\sigma,\tau}$, $S_{\rho,\sigma,\tau}$ ning R_σ alaindeksitega.

Definitsioon 2.3. Valemid süsteemis **T** defineerime induktiivselt:

1. \perp on valem,
2. iga tüübi σ ja termide $t : \sigma$ ning $s : \sigma$ korral $s =_\sigma t$ on valem,
3. kui φ ja ψ on valemid, siis $\varphi \wedge \psi$, $\varphi \vee \psi$ ja $\varphi \Rightarrow \psi$ on valemid.

Gödeli süsteemi **T** loogiliseks aluseks võetakse kvantoritevaba intuitsionistliku loogika tuletusreeglid ja loogilised aksioomid ehk \mathcal{I} ilma kvantorite kohta käivate reeglitega, aga koos võrduspredikaadiga $=_\sigma$, mis on iga tüübi σ korral lahenduv. Sellist tuletussüsteemi tähistame sümboliga \mathcal{I}^- .

Süsteemi **T** aksioomideks on:

$$\mathbf{T1.} \quad \frac{t : \mathbb{N}}{\neg(st =_{\mathbb{N}} 0)}$$

$$\begin{array}{l}
\mathbf{T2.} \quad \frac{t : \mathbb{N} \quad u : \mathbb{N}}{st =_{\mathbb{N}} su \Rightarrow t =_{\mathbb{N}} u} \\
\mathbf{T3.} \quad \frac{s : \sigma \quad t : \tau}{K(s, t) =_{\sigma} s} \\
\mathbf{T4.} \quad \frac{(s, t) : \sigma \times \tau}{\pi_1(s, t) =_{\sigma} s} \quad \text{ja} \quad \frac{(s, t) : \sigma \times \tau}{\pi_2(s, t) =_{\tau} t} \\
\mathbf{T5.} \quad \frac{r : (\rho \rightarrow \sigma \rightarrow \tau) \quad s : (\rho \rightarrow \sigma) \quad t : \rho}{S(r, s, t) =_{\tau} (r(t))(s(t))} \\
\mathbf{T6.} \quad \frac{s : \sigma \quad g : (\mathbb{N} \rightarrow \sigma \rightarrow \sigma) \quad 0 : \mathbb{N}}{R(s, g, 0) =_{\sigma} s} \\
\mathbf{T7.} \quad \frac{s : \sigma \quad g : (\mathbb{N} \rightarrow \sigma \rightarrow \sigma) \quad n : \mathbb{N}}{R(s, g, sn) =_{\sigma} g(n, R(s, g, n))}
\end{array}$$

ja induktsiooniskeem:

$$\frac{x : \mathbb{N} \quad t : \mathbb{N}}{(\varphi(0) \wedge (\varphi(x) \Rightarrow \varphi(sx))) \Rightarrow \varphi(t)}$$

suvalise valemi φ jaoks.

Võrdusaksioomideks on:

$$\begin{array}{l}
\mathbf{V1_{T.}} \quad \frac{t : \sigma}{t =_{\sigma} t} \\
\mathbf{V2_{T.}} \quad \frac{s : \sigma \quad t : \sigma \quad x : \sigma}{s =_{\sigma} t \Rightarrow (\varphi[t/x] \Rightarrow \varphi[s/x])}
\end{array}$$

ning kui muutujatel x ja y on sama tüüp, siis $\varphi \Rightarrow \varphi[y/x]$.

Järgnevalt läheb meil vaja teoreemi, mida kasutame teoreemi 2.12 tõestuses, nimelt.

Teoreem 2.4 (lambda-operaator [11]). Iga termi t tüübiga τ ja muutuja x tüübiga σ korral saame defineerida termi $\lambda x^{\sigma}.t$ tüübiga $\sigma \rightarrow \tau$ nii, et suvalise termi s tüübiga σ korral kehtib võrdus

$$(\lambda x^{\sigma}.t)s = t[s/x^{\sigma}].$$

Sisuliselt võib mõelda termist $\lambda x^\sigma.t$ kui kujutusest $x^\sigma \rightarrow t(x^\sigma)$. Näiteks saame kirja panna matemaatilisi operatsioone vastavalt.

Näide 2.5. Funktsiooni $f(x) = x + 2$ saame lambda-operaatoriga kirjutada kui $\lambda x.(x + 2)$.

Definitsioon 2.6. Olgu t term süsteemis \mathbf{T} . Termi t vabade muutujate hulga $FV(t)$ defineerime rekursiivselt sõltuvalt t kujust:

1. $FV(x) = \{x\}$,
2. $FV(t_1 t_2) = FV(t_1) \cup FV(t_2)$, kus t_1 ja t_2 on termid,
3. $FV(\lambda x.t_1) = FV(t_1) \setminus \{x\}$, kus t_1 on term.

Termi substituiooni mõiste anname üpris analoogiliselt predikaatloogika substituiooni mõistele.

Definitsioon 2.7 ([2]). Olgu $t : \tau$ term süsteemis \mathbf{T} . Muutuja x^σ **substituiooniks** termiga $s : \sigma$ nimetatakse muutuja x^σ kõigi vabade esinemiste asendamist termis $t : \tau$ termiga $s : \sigma$ (tähistame $t[s/x^\sigma]$), mille defineerime rekursiivselt sõltuvalt t kujust:

$$y^\sigma[s/x^\sigma] := \begin{cases} s, & \text{kui } x^\sigma = y^\sigma \\ y, & \text{kui } x^\sigma \neq y^\sigma \end{cases}$$

$$(t_1 t_2)[s/x^\sigma] := (t_1[s/x^\sigma])(t_2[s/x^\sigma])$$

$$(\lambda y^\sigma.t_1)[s/x^\sigma] := \begin{cases} \lambda y.t_1, & \text{kui } x^\sigma = y^\sigma \\ \lambda y.t_1[s/x^\sigma], & \text{kui } y^\sigma \notin FV(s) \\ \lambda z^\sigma.(t_1[z^\sigma/y^\sigma])[s/x^\sigma], & \text{muidu} \end{cases}$$

Edaspidi kasutame kirjaviisi $\lambda x_1.\lambda x_2.\dots\lambda x_n.t$ jaoks ka lühendatud kirjaviisi $\lambda x_1 x_2 \dots x_n.t$.

2.2 Dialektika interpretatsioon

Järgneva peatüki jooksul kasutame järgnevat sümboolikat, et tähistada lõplikke muutujatejärjendeid ja terminejärjendeid (mis võivad olla ka tühjad) vastavalt $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_n)$ jne. Termine korral $\mathbf{t} = (t_1, \dots, t_n)$, $\mathbf{t}_1 = (t'_1, \dots, t'_n)$ jne. Tähistamiseks funktsioonitüübiga muutujatest järjendeid, kasutame suurtähti, s.t. $\mathbf{X} = (X_1, \dots, X_n)$. Sümboli \mathbf{s} tähistab jätkuvalt järgmise naturaalarvu võtmist, seega \mathbf{s} ei tähista terminejärjendit. Kirjaviise $\exists \mathbf{x}$ ja $\forall \mathbf{x}$ loeme kui $\exists x_1 \exists x_2 \dots \exists x_n$ ja $\forall x_1 \forall x_2 \dots \forall x_n$ vastavalt. Lambda-operaatori korral loeme sümbolit $\lambda \mathbf{x}.t$ kui $\lambda x_1.(\lambda x_2.(\dots (\lambda x_n.t) \dots))$.

Gödeli dialektika interpretatsioon määrab igale **HA** valemile φ vastava valemi φ^D , kus φ^D on kujul $\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y})$, s.t. kujul

$$\exists x_1 \dots \exists x_n \forall y_1 \dots \forall y_n \varphi_D(x_1, \dots, x_n, y_1, \dots, y_n)$$

ning $\varphi_D(\mathbf{x}, \mathbf{y})$ on kvantorite vaba valem süsteemis **T**. Kusjuures valemi φ^D vabad muutujad on samad, mis valemis φ ning muutujatejärjendite \mathbf{x} ja \mathbf{y} tüüp sõltub valemis φ loogilisest struktuurist, kusjuures \mathbf{x} ja \mathbf{y} võivad olla ka tühjad.

Märkus. Lugejal võib tekkida küsimus, mis teoorias asetseb valem $\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y})$, tõepoolest, kuna süsteem **T** on kvantoritevaba, on see küsimus õigustatud. Valemit $\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y})$ võime vaadelda kui teooria **T** kvantoritega laiendatud süsteemi valemite. Seda kvantoritega laiendatud teooriat tähistame sümboliga $\mathbf{T}^{\exists \forall}$, kus lisaks naturaalarvudele saame kvantoritega siduda funktsioonitüüpi terme $t : \sigma \rightarrow \tau$. Sellisel juhul on tuletussüsteemiks \mathcal{L} . Juhul, kui kvantori domeeniks on funktsioonitüübiga muutujad, kasutame muutujatena suurtähti X, Y, Z, U, \dots , s.t. kirjaviise $\forall X$ ja $\exists X$.

Definitsioon 2.8 (dialektika interpretatsioon). Olgu $\varphi^D := \exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y})$ ja $\psi^D := \exists \mathbf{u} \forall \mathbf{v} \psi_D(\mathbf{u}, \mathbf{v})$. Kui meile on antud valem θ teoorias **HA**, anname valemile dialektika interpretatsiooni rekursiivselt:

1. Kui θ on atomaarne valem, siis $\theta^D := \theta_D := \theta$, seega ka $\perp^D := \perp_D := \perp$.
2. $(\varphi \wedge \psi)^D := \exists \mathbf{x}, \mathbf{u} \forall \mathbf{y}, \mathbf{v} (\varphi_D(\mathbf{x}, \mathbf{y}) \wedge \psi_D(\mathbf{u}, \mathbf{v}))$.
3. $(\varphi \vee \psi)^D := \exists z, \mathbf{x}, \mathbf{u} \forall \mathbf{y}, \mathbf{v} ((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y})) \vee (z \neq 0 \wedge \psi_D(\mathbf{u}, \mathbf{v})))$.
4. $(\forall z \varphi(z))^D := \exists \mathbf{X} \forall z, \mathbf{y} \varphi_D(\mathbf{X}(z), \mathbf{y}, z)$.
5. $(\exists z \varphi(z))^D := \exists z, \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}, z)$.
6. $(\varphi \Rightarrow \psi)^D := \exists \mathbf{U}, \mathbf{Y} \forall \mathbf{x}, \mathbf{v} (\varphi_D(\mathbf{x}, \mathbf{Y}(\mathbf{x}, \mathbf{v})) \Rightarrow \psi_D(\mathbf{U}(\mathbf{x}), \mathbf{v}))$.

Siinkohal tasuks selgitada antud interpretatsiooni. Valem $(\varphi \wedge \psi)^D$ saadakse, andes kõigepealt valemile kuju $\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \wedge \exists \mathbf{u} \forall \mathbf{v} \psi_D(\mathbf{u}, \mathbf{v})$

ning seejärel tuues predikaatloogika põhisamaväärsustega kvantorid valemi ette.

Nimelt kehtivad samaväärsused:

$$\begin{aligned} (\exists \mathbf{x} \theta(\mathbf{x}) \wedge \eta) &\Leftrightarrow \exists \mathbf{x} (\theta(\mathbf{x}) \wedge \eta), & \mathbf{x} \notin FV(\eta) \\ (\forall \mathbf{x} \theta(\mathbf{x}) \wedge \eta) &\Leftrightarrow \forall \mathbf{x} (\theta(\mathbf{x}) \wedge \eta), & \mathbf{x} \notin FV(\eta) \end{aligned}$$

Samad samaväärsused kehtivad asendades konjunktsiooni \wedge disjunktsiooniga \vee . Valemist $(\varphi \vee \psi)^D$ on lihtne konstruktiiivselt aru saada, sest lisamuutuja z ütleb meile, milline juhtum disjunktsioonist realiseerub, üldine teisendus on analoogne konjunktsiooni juhuga.

Valem $(\forall z \varphi(z))^D$ saadakse, kui anda antud valemile kõigepealt kuju

$$\forall z \exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}, z)$$

ning seejärel *skolemiseerides* olemasolu kvantori, s.t. saades kuju

$$\exists \mathbf{X} \forall z, \mathbf{y} \varphi_D(\mathbf{X}(z), \mathbf{y}, z).$$

Viimane teisendus on õigustatud kasutades valikuaksioomi süsteemis $\mathbf{T}^{\exists\forall}$ ehk rakendades samaväärsust:

$$\forall \mathbf{x} \exists \mathbf{y} \varphi(\mathbf{x}, \mathbf{y}) \Leftrightarrow \exists \mathbf{Y} \forall \mathbf{x} \varphi(\mathbf{x}, \mathbf{Y}(\mathbf{x})), \quad (\text{AC})$$

suvalise valemi φ korral.

Valemi $(\varphi \Rightarrow \psi)^D$ saame kasutades süsteemis $\mathbf{T}^{\exists\forall}$ kehtivaid samaväärsusi:

$$\begin{aligned} & (\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \exists \mathbf{u} \forall \mathbf{v} \psi_D(\mathbf{u}, \mathbf{v})) \\ & \stackrel{PS1}{\Leftrightarrow} \forall \mathbf{x} (\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \exists \mathbf{u} \forall \mathbf{v} \psi_D(\mathbf{u}, \mathbf{v})) \end{aligned} \quad (8)$$

$$\stackrel{IP'}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{u} (\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \forall \mathbf{v} \psi_D(\mathbf{u}, \mathbf{v})) \quad (9)$$

$$\stackrel{PS2}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} (\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})) \quad (10)$$

$$\stackrel{M'}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} \exists \mathbf{y} (\varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})) \quad (11)$$

$$\stackrel{AC}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{u}, \mathbf{Y}_1 \forall \mathbf{v} (\varphi_D(\mathbf{x}, \mathbf{Y}_1(\mathbf{v})) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})) \quad (12)$$

$$\stackrel{AC}{\Leftrightarrow} \exists \mathbf{U}, \mathbf{Y} \forall \mathbf{x}, \mathbf{v} (\varphi_D(\mathbf{x}, \mathbf{Y}(\mathbf{x}, \mathbf{v})) \Rightarrow \psi_D(\mathbf{U}(\mathbf{x}), \mathbf{v})). \quad (13)$$

Seega $(\varphi \Rightarrow \psi)_D \doteq (\varphi_D(\mathbf{x}, \mathbf{Y}(\mathbf{x}, \mathbf{v})) \Rightarrow \psi_D(\mathbf{U}(\mathbf{x}), \mathbf{v}))$.

Märkus. Märgime ära, et selline järjekord ei ole ainus viis, kuidas viia valem $\varphi \Rightarrow \psi$ niinimetatud $\exists\forall$ kujule. Üaltoodud samaväärsuste järjekorra motivatsiooniks on asjaolu, et tahame kasutada samaväärsusi **PS1** ja **IP'** võimalikult vähe, et esialgse valemi konstruktiivne kuju säiliks. Seda samaväärsuste järjekorda kasutame hiljem ka teoreemis 2.12. Kokkuleppeliselt nimetame samaväärsuste järjekorda **PS1**, **IP'**, **PS2**, **M'**, **AC** $\exists\forall$ -samaväärsuste ahelaks. Pikemaks aruteluks vaata allikat [11].

Samaväärsused (8) ja (10) kehtivad predikaatloogika põhisamaväärsuste tõttu:

$$(\exists \mathbf{x} \theta(\mathbf{x}) \Rightarrow \eta) \Leftrightarrow \forall \mathbf{x} (\theta(\mathbf{x}) \Rightarrow \eta), \quad \mathbf{x} \notin FV(\eta) \quad (\text{PS1})$$

$$\forall \mathbf{u} (\theta \Rightarrow \eta(\mathbf{u})) \Leftrightarrow (\theta \Rightarrow \forall \mathbf{u} \eta(\mathbf{u})). \quad \mathbf{u} \notin FV(\theta) \quad (\text{PS2})$$

Samaväärsused (12) ja (13) kehtivad (AC) tõttu. Samaväärsus (9) on erijuhtum järgnevast printsibist (inglise keelses kirjanduses *independence of premise*):

$$\exists \mathbf{u}(\theta \Rightarrow \eta(\mathbf{u})) \Leftrightarrow (\theta \Rightarrow \exists \mathbf{u} \eta(\mathbf{u})). \quad \mathbf{u} \notin FV(\theta) \quad (\text{IP})$$

Meie kasutame ainult ühte selle nõrgemat juhtu:

$$\exists u(\forall \mathbf{x} \theta(\mathbf{x}) \Rightarrow \eta(u)) \Leftrightarrow (\forall \mathbf{x} \theta(\mathbf{x}) \Rightarrow \exists \eta(u)) \quad (\text{IP}')$$

Samaväärsus (11) on õigustatud, kasutades Markovi printsipi:

$$\neg \neg \exists \mathbf{x} \varphi(\mathbf{x}) \Leftrightarrow \exists \mathbf{x} \varphi(\mathbf{x}), \quad (\text{M})$$

kus eeldame, et $\varphi(\mathbf{x})$ on kvantorite vaba valem. Nimelt on võimalik näidata, et intuitsionistlikus loogikas kehtib samaväärsus (vaata [9]):

$$\forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} (\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})) \Leftrightarrow \forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} \neg \neg \exists \mathbf{y} (\varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})),$$

seega rakendades nüüd Markovi printsipi valemile $\neg \neg \exists \mathbf{y} (\varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v}))$ saame valemi:

$$\forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} (\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})) \Leftrightarrow \forall \mathbf{x} \exists \mathbf{u} \forall \mathbf{v} \exists \mathbf{y} (\varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \psi_D(\mathbf{u}, \mathbf{v})), \quad (\text{M}')$$

mis ongi soovitud kujul.

Kuigi samaväärsused (PS1) ja (PS2) on ka intuitsionistlikus loogikas tõestatavad, peame teooria $\mathbf{T}^{\exists \forall}$ puhul samaväärsusi (AC), (M) ja (IP') võtma kui lisaeeslusi.

Järgmise teoreemi tõestamiseks läheb meil vaja kolme järgnevat lemmat.

Lemma 2.9 ([11]). Kui φ on valem teoorias **HA**, siis leidub term $t_\varphi : \mathbb{N}$ süsteemis **T** selliselt, et

$$\mathbf{T} \vdash t_\varphi(\mathbf{x}, \mathbf{y}) = 0 \Leftrightarrow \varphi_D(\mathbf{x}, \mathbf{y}).$$

Lemma 2.10 ([11]). Kui $\mathbf{T} \vdash \psi(0, \mathbf{v})$ ja $\mathbf{T} \vdash \psi(y^{\mathbf{N}}, t(y^{\mathbf{N}}, \mathbf{v})) \Rightarrow \psi(\mathbf{s}y^{\mathbf{N}}, \mathbf{v})$, siis $\mathbf{T} \vdash \psi(x^{\mathbf{N}}, \mathbf{v})$.

Lemma 2.11 ([11]). Olgu φ valem teoorias $\mathbf{T}^{\exists\forall}$. Siis $\mathbf{T}^{\exists\forall} + AC + M' + IP' \vdash \varphi \Leftrightarrow \varphi^D$. Seega kehtivad järgnevad samaväärsused:

- * $(\varphi \wedge \psi)^D \Leftrightarrow \varphi^D \wedge \psi^D$,
- * $(\varphi \vee \psi)^D \Leftrightarrow \varphi^D \vee \psi^D$,
- * $(\varphi \Rightarrow \psi)^D \Leftrightarrow \varphi^D \Rightarrow \psi^D$,
- * $(\forall z \varphi)^D \Leftrightarrow \forall z \varphi^D$,
- * $(\exists z \varphi)^D \Leftrightarrow \exists z \varphi^D$.

Järgnevas tõestuses on põhjalikult läbi tehtud juhud, mis osutusid keerulisemateks.

Teoreem 2.12 ([11]). Kui $\mathbf{HA} \vdash \xi$, siis leidub süsteemi \mathbf{T} termine jada \mathbf{t} selliselt, et $\mathbf{T} \vdash \xi_D(\mathbf{t}, \mathbf{y})$.

Tõestus. Eeldame, et $\mathbf{HA} \vdash \xi$ kehtib ning tõestame väite induktsiooniga valemi ξ tuletuse pikkuse kaudu.

Induktsiooni baas. Kui tuletuse pikkus on 1, siis peab ξ olema aksiom.

A1. Kui ξ on kujul $\varphi \vee \varphi \Rightarrow \varphi$, siis lemma 2.11 põhjal

$$\xi^D \doteq (\varphi \vee \varphi \Rightarrow \varphi)^D \Leftrightarrow ((\varphi \vee \varphi)^D \Rightarrow \varphi^D),$$

seega kasutades dialektika interpretatsiooni definitsiooni 2.8 saame, et

$$\xi^D \Leftrightarrow (\exists z, \mathbf{x}, \mathbf{x}' \forall \mathbf{y}, \mathbf{y}' ((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{y}')) \Rightarrow \exists \tilde{\mathbf{x}} \forall \tilde{\mathbf{y}} \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}})).$$

Nüüd kasutades $\exists\forall$ -samaväärsuste ahelat, saame anda valemile kuju:

$$\begin{aligned}
\xi^D &\stackrel{PS1}{\Leftrightarrow} \forall z, \mathbf{x}, \mathbf{x}' \left(\forall \mathbf{y}, \mathbf{y}' \left((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{y}')) \Rightarrow \exists \tilde{\mathbf{x}} \forall \tilde{\mathbf{y}} \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \right) \right) \\
&\stackrel{IP'}{\Leftrightarrow} \forall z, \mathbf{x}, \mathbf{x}' \exists \tilde{\mathbf{x}} \left(\forall \mathbf{y}, \mathbf{y}' \left((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{y}')) \Rightarrow \forall \tilde{\mathbf{y}} \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \right) \right) \\
&\stackrel{PS2}{\Leftrightarrow} \forall z, \mathbf{x}, \mathbf{x}' \exists \tilde{\mathbf{x}} \forall \tilde{\mathbf{y}} \left(\forall \mathbf{y}, \mathbf{y}' \left((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{y}')) \Rightarrow \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \right) \right) \\
&\stackrel{M'}{\Leftrightarrow} \forall z, \mathbf{x}, \mathbf{x}' \exists \tilde{\mathbf{x}} \forall \tilde{\mathbf{y}} \exists \mathbf{y}, \mathbf{y}' \left(((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{y}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{y}')) \Rightarrow \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \right) \\
&\stackrel{AC}{\Leftrightarrow} \forall z, \mathbf{x}, \mathbf{x}' \exists \tilde{\mathbf{x}} \exists \mathbf{Y}_1, \mathbf{Y}'_1 \forall \tilde{\mathbf{y}} \left(((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{Y}_1 \tilde{\mathbf{y}}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{Y}'_1 \tilde{\mathbf{y}})) \Rightarrow \varphi_D(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \right) \\
&\stackrel{AC}{\Leftrightarrow} \exists \tilde{\mathbf{X}}, \mathbf{Y}, \mathbf{Y}' \forall z, \mathbf{x}, \mathbf{x}', \tilde{\mathbf{y}} \left((z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{Y} z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{Y}' z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}})) \Rightarrow \right. \\
&\quad \left. \varphi_D(\tilde{\mathbf{X}} z \mathbf{x} \mathbf{x}', \tilde{\mathbf{y}}) \right).
\end{aligned}$$

Seega oleme jõudnud valemile ξ^D vastava kvantoritevaba valemieni $\xi_D(\tilde{\mathbf{X}}, \mathbf{Y}, \mathbf{Y}', z, \mathbf{x}, \mathbf{x}', \tilde{\mathbf{y}})$, kus

$$\begin{aligned}
\xi_D(\tilde{\mathbf{X}}, \mathbf{Y}, \mathbf{Y}', z, \mathbf{x}, \mathbf{x}', \tilde{\mathbf{y}}) &\doteq (z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{Y} z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}}) \vee z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{Y}' z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}})) \Rightarrow \\
&\quad \varphi_D(\tilde{\mathbf{X}} z \mathbf{x} \mathbf{x}', \tilde{\mathbf{y}}).
\end{aligned}$$

Seega peame valima $\tilde{\mathbf{X}}, \mathbf{Y}$ ja \mathbf{Y}' asemele sobivad termijadad, et kehtiks kvantoritevabas süsteemis $\mathbf{T} \vdash \xi_D(\mathbf{t}, \mathbf{y})$. Võttes \mathbf{Y} ja \mathbf{Y}' asemele termijadad \mathbf{t}_1 ja \mathbf{t}_2 , kus $\mathbf{t}_1 = \mathbf{t}_2 = \lambda z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} \cdot \tilde{\mathbf{y}}$ ja $\tilde{\mathbf{X}}$ asemele termijada \mathbf{t}_3 , kus $\mathbf{t}_3 = \lambda z \mathbf{x} \mathbf{x}' \cdot R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}')z$, saame valemikuju $\eta \vee \theta \Rightarrow \psi$, kus

$$\begin{aligned}
\eta &\doteq z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{t}_1 z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}}), \\
\theta &\doteq z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{t}_2 z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}}), \\
\psi &\doteq \varphi_D(\mathbf{t}_3 z \mathbf{x} \mathbf{x}', \tilde{\mathbf{y}}).
\end{aligned}$$

Paneme tähele, et näidata, et kehtib valem $\eta \vee \theta \Rightarrow \psi$, piisab näidata, et kui eeldada η kehtivust, jõuame valemieni ψ ning omakorda, kui eeldada θ kehtivust, jõuame valemieni ψ . Seega saame kaks juhtu:

* Eeldame, et valem $z = 0 \wedge \varphi_D(\mathbf{x}, \mathbf{t}_1 z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}})$ kehtib. Eelnevalt võetud termide järjenditest \mathbf{t}_1 ja \mathbf{t}_3 saame, et

$$\mathbf{t}_1 z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} = (\lambda z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} \cdot \tilde{\mathbf{y}}) z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} = \tilde{\mathbf{y}}$$

ning omakorda, kuna $z = 0$, siis

$$\mathbf{t}_3 z \mathbf{x} \mathbf{x}' = \mathbf{t}_3 0 \mathbf{x} \mathbf{x}' = (\lambda z \mathbf{x} \mathbf{x}' \cdot R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') z) 0 \mathbf{x} \mathbf{x}' = R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') 0 = \mathbf{x},$$

mis tähendab, et valem $\eta \Rightarrow \psi$ lihtsustub kujule $z = 0 \wedge \varphi_D(\mathbf{x}, \tilde{\mathbf{y}}) \Rightarrow \varphi_D(\mathbf{x}, \tilde{\mathbf{y}})$, mis kehtib tänu \mathcal{I}^- aksioomidele A4 ja A6, kus \mathcal{I}^- oli vastav tuletussüsteem ilma kvantorite kohta käivate reegliteta.

* Eeldame, et $z \neq 0 \wedge \varphi_D(\mathbf{x}', \mathbf{t}_2 \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}})$ kehtib. Analoogselt eelneva juhuga saame, et $\mathbf{t}_2 z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} = \tilde{\mathbf{y}}$ ning kuna $z \neq 0$, siis $z = \mathbf{s} z'$, seega

$$\begin{aligned} \mathbf{t}_3 z \mathbf{x} \mathbf{x}' &= \mathbf{t}_3 (\mathbf{s} z') \mathbf{x} \mathbf{x}' = (\lambda z \mathbf{x} \mathbf{x}' \cdot R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') z) (\mathbf{s} z') \mathbf{x} \mathbf{x}' \\ &= R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') (\mathbf{s} z') = (\lambda w \mathbf{u} \cdot \mathbf{x}') z' (R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') z') = \mathbf{x}', \end{aligned}$$

mis tähendab, et saame valemi $z \neq 0 \wedge \varphi_D(\mathbf{x}', \tilde{\mathbf{y}}) \Rightarrow \varphi_D(\mathbf{x}', \tilde{\mathbf{y}})$, mis jällegi tänu \mathcal{I}^- aksioomidele A4 ja A6 kehtib.

Kokkuvõttes oleme saanud, et $\mathbf{T} \vdash \xi_D(\mathbf{t}, \mathbf{y})$, kus

$$\mathbf{t} = (\lambda z \mathbf{x} \mathbf{x}' \cdot R\mathbf{x}(\lambda w \mathbf{u} \cdot \mathbf{x}') z, \lambda z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} \cdot \tilde{\mathbf{y}}, \lambda z \mathbf{x} \mathbf{x}' \tilde{\mathbf{y}} \cdot \tilde{\mathbf{y}}) \quad \text{ja} \quad \mathbf{y} = (z, \mathbf{x}, \mathbf{x}', \tilde{\mathbf{y}}).$$

A2. Kui ξ on kujul $\varphi \Rightarrow \varphi \wedge \varphi$, siis lemma 2.11 põhjal

$$\xi^D \doteq (\varphi \Rightarrow \varphi \wedge \varphi)^D \Leftrightarrow \varphi^D \Rightarrow (\varphi \wedge \varphi)^D,$$

seega jällegi kasutades dialektika interpretatsiooni definitsiooni, saame, et

$$\xi^D \Leftrightarrow (\exists \mathbf{x} \forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \exists \mathbf{x}', \mathbf{x}'' \forall \mathbf{y}', \mathbf{y}'' (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}''))).$$

Nüüd rakendades $\exists \forall$ samaväärsuste ahelat, et leida valem ξ_D , saame

$$\begin{aligned} \xi^D &\stackrel{PS1}{\Leftrightarrow} \forall \mathbf{x} \left(\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \exists \mathbf{x}', \mathbf{x}'' \forall \mathbf{y}', \mathbf{y}'' (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}'')) \right) \\ &\stackrel{IP'}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{x}', \mathbf{x}'' \left(\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow \forall \mathbf{y}', \mathbf{y}'' (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}'')) \right) \\ &\stackrel{PS2}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{x}', \mathbf{x}'' \forall \mathbf{y}', \mathbf{y}'' \left(\forall \mathbf{y} \varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}'')) \right) \\ &\stackrel{M'}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{x}', \mathbf{x}'' \forall \mathbf{y}', \mathbf{y}'' \exists \mathbf{y} \left(\varphi_D(\mathbf{x}, \mathbf{y}) \Rightarrow (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}'')) \right) \\ &\stackrel{AC}{\Leftrightarrow} \forall \mathbf{x} \exists \mathbf{x}', \mathbf{x}'' \exists \mathbf{Y}_2 \forall \mathbf{y}', \mathbf{y}'' \left(\varphi_D(\mathbf{x}, \mathbf{Y}_2 \mathbf{y}' \mathbf{y}'') \Rightarrow (\varphi_D(\mathbf{x}', \mathbf{y}') \wedge \varphi_D(\mathbf{x}'', \mathbf{y}'')) \right) \\ &\stackrel{AC}{\Leftrightarrow} \exists \mathbf{X}', \mathbf{X}'', \mathbf{Y} \forall \mathbf{x}, \mathbf{y}', \mathbf{y}'' \left(\varphi_D(\mathbf{x}, \mathbf{Y} \mathbf{x} \mathbf{y}' \mathbf{y}'') \Rightarrow (\varphi_D(\mathbf{X}' \mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{X}'' \mathbf{x}, \mathbf{y}'')) \right). \end{aligned}$$

Seega valemile ξ^D vastav kvantoritevaba valem ξ_D on kujul $\xi_D(\mathbf{X}', \mathbf{X}'', \mathbf{Y}, \mathbf{x}, \mathbf{y}, \mathbf{y}'')$, kus

$$\xi_D(\mathbf{X}', \mathbf{X}'', \mathbf{Y}, \mathbf{x}, \mathbf{y}, \mathbf{y}'') \doteq \varphi_D(\mathbf{x}, \mathbf{Y} \mathbf{x} \mathbf{y}' \mathbf{y}'') \Rightarrow \varphi_D(\mathbf{X}' \mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{X}'' \mathbf{x}, \mathbf{y}'').$$

Kasutades lemmat 2.9, leidub term t_φ selliselt, et

$$\mathbf{T} \vdash t_\varphi(\mathbf{x}, \mathbf{y}') = 0 \Leftrightarrow \varphi_D(\mathbf{x}, \mathbf{y}'), \quad (14)$$

seega piisab võtta \mathbf{X}' ja \mathbf{X}'' asemele termijadad \mathbf{t}_1 ja \mathbf{t}_2 , kus $\mathbf{t}_1 = \mathbf{t}_2 = \lambda \mathbf{x}. \mathbf{x}$ ja \mathbf{Y} asemele termijada \mathbf{t}_3 , kus

$$\mathbf{t}_3 = \lambda \mathbf{x} \mathbf{y}' \mathbf{y}'' . R \mathbf{y}'' (\lambda w \mathbf{u}. \mathbf{y}') t_\varphi(\mathbf{x}, \mathbf{y}')$$

ning seega saame valemi

$$(\varphi_D(\mathbf{x}, \mathbf{t}_3 \mathbf{x} \mathbf{y}' \mathbf{y}'') \Rightarrow (\varphi_D(\mathbf{t}_1 \mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{t}_2 \mathbf{x}, \mathbf{y}''))).$$

Kusjuures näeme, et $\mathbf{t}_1\mathbf{x} = \mathbf{t}_2\mathbf{x} = \mathbf{x}$. Juhul, kui $t_\varphi(\mathbf{x}, \mathbf{y}') = 0$, siis tingimusest (14) saame, et $\mathbf{T} \vdash \varphi_D(\mathbf{x}, \mathbf{y}')$ ning saame valemi

$$\varphi_D(\mathbf{x}, \mathbf{y}'') \Rightarrow (\varphi_D(\mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{x}, \mathbf{y}')),$$

sest

$$\begin{aligned} \mathbf{t}_3\mathbf{x}\mathbf{y}'\mathbf{y}'' &= (\lambda\mathbf{x}\mathbf{y}'\mathbf{y}'' . R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')t_\varphi(\mathbf{x}, \mathbf{y}'))\mathbf{x}\mathbf{y}'\mathbf{y}'' = R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')t_\varphi(\mathbf{x}, \mathbf{y}') \\ &= R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')0 = \mathbf{y}''. \end{aligned}$$

Seega valemi kehtimine on ilmne. Nüüd juhul kui $t_\varphi(\mathbf{x}, \mathbf{y}') \neq 0$, siis $t_\varphi = \mathbf{s}z$, $z : \mathbb{N}$, ning saame valemi

$$\varphi_D(\mathbf{x}, \mathbf{y}') \Rightarrow (\varphi_D(\mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{x}, \mathbf{y}')), \quad (15)$$

sest

$$\begin{aligned} \mathbf{t}_3\mathbf{x}\mathbf{y}'\mathbf{y}'' &= (\lambda\mathbf{x}\mathbf{y}'\mathbf{y}'' . R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')t_\varphi(\mathbf{x}, \mathbf{y}'))\mathbf{x}\mathbf{y}'\mathbf{y}'' = R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')t_\varphi(\mathbf{x}, \mathbf{y}') \\ &= R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')(\mathbf{s}z) = (\lambda w\mathbf{u}.\mathbf{y}')z(R\mathbf{y}''(\lambda w\mathbf{u}.\mathbf{y}')z) = \mathbf{y}''. \end{aligned}$$

Kuna $t_\varphi(\mathbf{x}, \mathbf{y}') \neq 0$, siis tingimusest (14) saame, et $\mathbf{T} \vdash \neg\varphi_D(\mathbf{x}, \mathbf{y}')$. Tõestamaks valemi (15) kehtivust, eeldame, et $\varphi_D(\mathbf{x}, \mathbf{y}')$ kehtib ja näitame, et sellest järeljub valemi $(\varphi_D(\mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{x}, \mathbf{y}''))$ kehtivus. Tõepoolest, eeldades, et $\varphi_D(\mathbf{x}, \mathbf{y}')$ kehtib, saame tingimusest, et $\mathbf{T} \vdash \neg\varphi_D(\mathbf{x}, \mathbf{y}')$ tuletada, et $\mathbf{T} \vdash \perp$. Nüüd kasutades aksioomi A9 saamegi tuletada valemi $(\varphi_D(\mathbf{x}, \mathbf{y}') \wedge \varphi_D(\mathbf{x}, \mathbf{y}''))$. Kusjuures siin kasutasime eeldust, et võrduspredikaat = on lahenduv.

Mitteloogilised aksioomid. Defineerides liitmise kui termi $p := \lambda x.\lambda y.Rx(\lambda w.\lambda z.\mathbf{s}z)y$

ehk $x + y := pxy$, on lihtne näha, et

$$\begin{aligned} px0 &= Rx(\lambda w.\lambda z.sz)0 = x, \\ px(\mathbf{s}y') &= Rx(\lambda w.\lambda z.sz)y' = (\lambda w.\lambda z.sz)y'(Rx(\lambda w.\lambda z.sz)y') = \\ &= \mathbf{s}(Rx(\lambda w.\lambda z.sz)y') = \mathbf{s}(pxy'), \end{aligned}$$

ehk $x + 0 = x$ ja $x + \mathbf{s}y = \mathbf{s}(x + y)$, mistõttu liitmise aksioomid on rahuldatud.

Korrutamise defineerime termina $m := \lambda x.\lambda y.R0(\lambda w.\lambda z.z + x)y$. Sellisel juhul

$$\begin{aligned} x \cdot 0 &= mx0 = (\lambda x.\lambda y.R0(\lambda w.\lambda z.z + x)y)x0 \\ &= R0(\lambda w.\lambda z.z + x)0 = 0, \\ x \cdot \mathbf{s}y &= mx(\mathbf{s}y) = (\lambda x.\lambda y.R0(\lambda w.\lambda z.z + x)y)x(\mathbf{s}y) \\ &= R0(\lambda w.\lambda z.z + x)(\mathbf{s}y) = (\lambda w.\lambda z.z + x)y(R0(\lambda w.\lambda z.z + x)y) \\ &= R0(\lambda w.\lambda z.z + x)y + x = (\lambda x.\lambda y.R0(\lambda w.\lambda z.z + x)y)xy + x \\ &= mxy + x = x \cdot y + x, \end{aligned}$$

ehk ka korrutamist defineerivad aksioomid on rahuldatud.

Piisab veel näidata, et väide kehtib induktsiooniskeemi korral. Selleks tõestame samaväärse induktsioonireegli

$$\frac{\varphi(0) \quad \forall y(\varphi(y) \Rightarrow \varphi(\mathbf{s}y))}{\forall z\varphi(z)} \text{ INDR}$$

Eeldame, et leiduvad termijadad $\mathbf{t}_1, \mathbf{t}_2$ ja \mathbf{t}_3 selliselt, et $\mathbf{T} \vdash \varphi_D(\mathbf{t}_1, \mathbf{v}, 0)$ ja $\mathbf{T} \vdash \varphi_D(\mathbf{x}', \mathbf{t}_2 u \mathbf{x}' \mathbf{y}'', u) \Rightarrow \varphi_D(\mathbf{t}_3 u \mathbf{x}', \mathbf{y}'', \mathbf{s}u)$. Tahame leida termijada \mathbf{t} selliselt, et $\mathbf{T} \vdash$

$\varphi_D(\mathbf{t}z, \mathbf{y}, z)$. Vöttes $\mathbf{t} := \lambda z. R\mathbf{t}_1(\lambda q\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))z$, näeme, et

$$\begin{aligned}\mathbf{t}0 &= R\mathbf{t}_1(\lambda q\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))0 = \mathbf{t}_1, \\ \mathbf{t}(\mathbf{s}z') &= R\mathbf{t}_1(\lambda q\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))(\mathbf{s}z') = (\lambda q\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))z'(R\mathbf{t}_1(\lambda q\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))z') \\ &= (\lambda q\mathbf{w}\mathbf{w}.\mathbf{t}_3q(\mathbf{t}q))z'(\mathbf{t}z') = \mathbf{t}_3z'(\mathbf{t}z'),\end{aligned}$$

seega term t on korrektselt defineeritud.

Nüüd vöttes \mathbf{x}' asemel $\mathbf{t}u$ saame, et $\mathbf{T} \vdash \varphi_D(\mathbf{t}0, \mathbf{v}, 0)$ ja $\mathbf{T} \vdash \varphi_D(\mathbf{t}u, \mathbf{t}_2u(\mathbf{t}u)\mathbf{y}'', u) \Rightarrow \varphi_D(\mathbf{t}(\mathbf{s}u), \mathbf{y}'', \mathbf{s}u)$. Rakendades nüüd lemmat 2.10 valemile $\psi(u, \mathbf{y}) := \varphi_D(\mathbf{t}u, \mathbf{y}, u)$, saamegi soovitud tulemuse $\mathbf{T} \vdash \varphi_D(\mathbf{t}z, \mathbf{y}, z)$.

Induktsiooni samm. Eeldame, et kui tuletuse $\mathbf{H}\mathbf{A} \vdash \xi$ pikkus on k , siis $\mathbf{T} \vdash \xi_D(\mathbf{t}, \mathbf{y})$. Kehtigu $\mathbf{H}\mathbf{A} \vdash \xi$, mille tuletuse pikkus on $k + 1$.

Kui ξ saadi reegluga $R1$, siis ξ on kujul ψ ning induktsiooni eelduse kohaselt leiduvad termijärjendid $\mathbf{t}_1, \mathbf{t}_2$ ja \mathbf{t}_3 selliselt, et

$$\mathbf{T} \vdash \varphi_D(\mathbf{t}_1, \mathbf{y}) \text{ ja } \mathbf{T} \vdash \varphi_D(\mathbf{x}, \mathbf{t}_2\mathbf{x}\mathbf{v}) \Rightarrow \psi_D(\mathbf{t}_3\mathbf{x}, \mathbf{v}),$$

Meie eesmärgiks on leida termijärjend \mathbf{t} selliselt, et $\mathbf{T} \vdash \psi_D(\mathbf{t}, \mathbf{v})$. Näeme, et vöttes \mathbf{x} asemele termijärjendi \mathbf{t}_1 ja \mathbf{y} asemele $\mathbf{t}_2\mathbf{t}_1\mathbf{v}$ saame, et $\mathbf{T} \vdash \varphi_D(\mathbf{t}_1, \mathbf{t}_2\mathbf{t}_1\mathbf{v})$ ja $\mathbf{T} \vdash \varphi_D(\mathbf{t}_1, \mathbf{t}_2\mathbf{t}_1\mathbf{v}) \Rightarrow \psi_D(\mathbf{t}_3\mathbf{t}_1, \mathbf{v})$, mistõttu saame, et $\mathbf{T} \vdash \psi_D(\mathbf{t}_3\mathbf{t}_1, \mathbf{v})$, seega piisab võtta $\mathbf{t} = \mathbf{t}_3\mathbf{t}_1$. ■

3 Peano aritmeetika korrektsus

3.1 Church-Rosser'i teoreem

Definitsioon 3.1 ([4]). Term t on **normaalne**, kui ükski tema alamtermidest ei ole kujul $\pi_1(u, v)$, $\pi_2(u, v)$, $K(s, t)$, $S(r, s, t)$ või $R(s, g, n)$.

Definitsioon 3.2 ([4]). Defineerime binaarse seose \rightsquigarrow süsteemi \mathbf{T} termide peal vastavalt:

1. $\pi_1(u, v) \rightsquigarrow u$;
2. $\pi_2(u, v) \rightsquigarrow v$;
3. $K(s, t) \rightsquigarrow s$;
4. $S(r, s, t) \rightsquigarrow (r(t))(s(t))$;
5. $R(s, g, 0) \rightsquigarrow s$;
6. $R(f, g, sn) \rightsquigarrow g(n, R(f, g, n))$.

Juhul kui $t \rightsquigarrow t'$, siis termi t kutsutakse **reedeksiks** ja termi t' termi t **teisenduseks**.

Definitsioon 3.3 ([4]). Öeldakse, et term t **redutseerub** termiks u **ühe sammuga**, tähistame $t \rightarrow u$, kui u saadakse termist t selliselt, et t mingi alamterm t_1 asendatakse termiga t_2 , kus kehtib $t_1 \rightsquigarrow t_2$. Ütleme, et term t **redutseerub** termiks u ja tähistame $t \rightarrow^* u$, kui u saadakse termist t lõpliku arvu ühe sammu redutseerimistega. Loeme, et term redutseerub iseendaks 0-sammuga.

Definitsioon 3.4 ([4]). Termi t **normaalkujuks** nimetatakse termi u selliselt, et $t \rightarrow^* u$ ja u on normaalne.

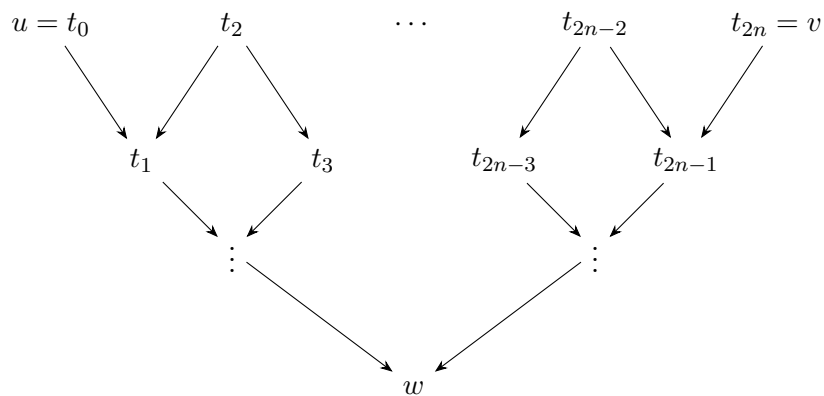
Paneme tähele, et kui u on normaalne, siis ei saa me tema peal ühtegi ühe sammulist reduktsiooni läbi viia, sest temas puuduvad reedeksid. Seega normaalkujul olev term saab redutseeruda ainult iseendaks. Siinkohal võib lugejal tekkida küsimus, kas igal süsteemi \mathbf{T} termil leidub normaalkuju. Vastus sellele küsimusele on jaatav. Nimelt kehtib ka veel tugevam väide, mis ütleb, et süsteem \mathbf{T} iga termi iga ühe sammuliste redutseerimiste jada jõuab normaalkujuni sõltumata redutseerimiste järjekorrast. Seda omadust tuntakse kui **tugevalt normaliseerituse omadust**.

Meil läheb vaja aga järgnevat teoreemi.

Teoreem 3.5 (Church-Rosser'i teoreem [1]). *Kui süsteemis \mathbf{T} kehtib, et $t \rightarrow^* u$ ja $t \rightarrow^* v$, siis leidub term w selliselt, et $u \rightarrow^* w$ ja $v \rightarrow^* w$.*

Järeldus 3.6 ([4]). *Kui süsteemis \mathbf{T} termide $u : \sigma$ ja $v : \sigma$ korral $u =_\sigma v$, siis leidub term $w : \sigma$ selliselt, et $u \rightarrow^* w$ ja $v \rightarrow^* w$.*

Nimelt, kui termide $u : \sigma$ ja $v : \sigma$ korral $u =_\sigma v$ ehk kasutades süsteemi \mathbf{T} omaaksioome (2.1) oleme saanud võrdustejada $u = t_0 = t_1 = \dots t_{2n} = v$, siis rakendades termidele t_{2i-2} ja t_{2i} , kus $i = 1, \dots, n$, Church-Rosser'i teoreemi, saame, et



kus nooled diagrammis tähistavad redutseerimisseost \rightarrow^* .

Church-Rosser'i teoreemi näol on tegemist väga tugeva väitega, mis annab arvutuslikult süsteemile väga häid omadusi. Kahjuks jääb selle teoreemi tõestus antud lõputöö mahust välja.

3.2 Peano aritmeetika korrektsus

Tuletame lugejale meelde, et teooria \mathcal{T} korrektsuse defineerisime, kui antud teoorias ei leidu valemit φ selliselt, et saame tuletused $\mathcal{T} \vdash \varphi$ ja $\mathcal{T} \vdash \neg\varphi$. Peano aritmeetika on sisemiselt kooskõlaline, nimelt saame lõpuks näidata, et kehtib järgnev teoreem.

Teoreem 3.7 (Peano aritmeetika korrektsus [7]). *Peano aritmeetika on korrektne, see tähendab, et ei leidu valemit φ , mille korral $PA \vdash \varphi$ ja $PA \vdash \neg\varphi$.*

Tõestus. Teoreemi 1.27 põhjal piisab näidata, et **HA** on korrektne. Oletame vastuväiteliselt, et leidub valem φ selliselt, et **HA** $\vdash \varphi$ ja **HA** $\vdash \neg\varphi$. Kuna $\neg\varphi \doteq \varphi \Rightarrow \perp$, saame, et **HA** $\vdash \perp$. Teoreemi 2.12 põhjal siis ka **T** $\vdash \perp_D$ ehk **T** $\vdash \perp$. Nüüd kasutades aksioomi A9 saame tuletada, et **T** $\vdash 0 =_{\mathbb{N}} s0$. Järelduse 3.6 põhjal leidub term w selliselt, et $0 \rightarrow^* w$ ja $s0 \rightarrow^* w$. Kuna termid 0 ja $s0$ on normaalsed, ei saa me nende peal ühtegi ühe sammulist reduktsiooni täide viia, mis annab vastuolu termi w olemasoluga. ■

Kokkuvõte

Antud bakalaureusetöös näitasime, et Peano aritmeetika on korrektne. Selleks defineerisime kõigepealt põhilised esimest järku predikaatloogika mõisted ning pakusime välja konkreetse tuletussüsteemi esimest järku intuitsionistlikule predikaatloogikale. Seejärel näitasime, et Peano aritmeetika korrektsus on samaväärne Heytingi aritmeetika korrektsusega teoreemide 1.27 ja 1.28 näol.

Samuti defineerisime Gödeli süsteemi \mathbf{T} ja Dialektika interpretatsiooni, mille puhul andsime põhjaliku selgituse selle interpretatsiooni motivatsioonist. Teoreemis 2.12 tõestasime põhilised juhud, näitamaks, et iga Heytingi aritmeetikas tõestatavale valemile vastav Dialektika interpretatsiooni kvantoriteta valem on tõestatav Gödeli süsteemis \mathbf{T} .

Lõpetuseks defineerisime termide redutseerimise mõiste ning tõestasime, et kasutades Church-Rosser'i teoreemi 3.5 ja selle järeldest 3.6 süsteemi \mathbf{T} kohta, on Peano aritmeetika korrektne.

Kasutatud allikad

- [1] Jeremy Avigad ja Solomon Feferman. „Gödel’s functional (“Dialectica”) interpretation“. Teoses: *Studies in Logic and the Foundations of Mathematics*. Kõide 137. Elsevier, 1998, lk. 337–405.
- [2] Hendrik Pieter Barendregt, Wil Dekkers ja Richard Statman. *Lambda calculus with types*. Cambridge University Press, 2013.
- [3] Solomon Feferman, John Dawson ja Stephen Kleene, toim. *Kurt Gödel: Collected Works Vol. II*. Oxford University Press, 1990.
- [4] Jean-Yves Girard, Paul Taylor ja Yves Lafont. *Proofs and types*. Kõide 7. Cambridge university press Cambridge, 1989.
- [5] Mireia González Bedmar. „On a game-theoretic semantics for the Dialectica interpretation of analysis“ (2018).
- [6] Kurt Gödel. „Über Eine Bisher Noch Nicht Benützte Erweiterung des Finiten Standpunktes“. *Dialectica* 12.3 (1958), lk. 280.
- [7] J Roger Hindley ja Jonathan P Seldin. *Lambda-calculus and combinators: an introduction (supplement to book)*. Cambridge University Press, 2008.
- [8] Juliette Kennedy. „Kurt gödel“ (2007).
- [9] Ulrich Kohlenbach. *Applied proof theory: proof interpretations and their use in mathematics*. Springer Science & Business Media, 2008.
- [10] Rein Prank. *Matemaatiline loogika ja algoritmiteooria*. Tartu Ülikooli Kirjastus, 2004.
- [11] Anne Sjerp Troelstra. *Metamathematical investigation of intuitionistic arithmetic and analysis*. Springer, 1973.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Aiden Madisson,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Peano aritmeetika korrektsus”, mille juhendajad on Danel Ahman ja Ülo Reimaa, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.
2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commons'i litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.
3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.
4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Aiden Madisson

29.05.2025