Diskreetne matemaatika I

Kevad 2018

Loengukonspekt

Lektor: Valdis Laan

13. juuni 2018. a.

Eessõna

Tegemist on Tartu Ülikooli 2018. a. kevadsemestri kursuse “Diskreetne matemaatika I” loengukonspektiga. Lisaks sellele konspektile on kasulik tutvuda ka muude õppematerjalidega. Iseäranis kasulik on lugeda õpikuid [8] ja [9].

Kursus (nagu ka loengukonspekt) koosneb kahest poolest: sissejuhatusest matemaatilisse loogikasse ja graafiteooria elementidest. Kuna suur osa kursuse kuulajatest on informaatika eriala üliõpilased, siis on oluline osa selles kursuses algoritmidel. Samas on tegemist siiski matemaatika kursusega ja selle tõttu on enamus väiteid esitatud koos tõestusega. Lugejalt eeldatakse matemaatika põhimõistete (hulk, alamhulk, kujutus, binaarne seos, ekvivalentsiseos jt.) tundmist.

Konspekti tekstist võib leida mõned märkused, mille tekst on muust tekstist väiksem. Nende märkuste lugemine ei ole muust materjalist aru saamiseks hädavajalik. Need märkused on mõeldud eelkõige neile, kes soovivad materjaliga sügavamalt tutvuda.

Konspekti lõpust võib leida nimekirja allikatest, mida on selle teksti koostamisel kasutatud.

Soovin tänada Reimo Palmi ja Ago-Erik Rieti arvukate asjalike märkuste eest, mis on aidanud konspekti kvaliteeti parandada. Ka mitmed üliõpilased on konspektist vigu leidnud, tänud neilegi.

Loengute ja praktikumide ajakava

1. nädal. L. Sissejuhatus. Kordamine: lausearvutuse põhimõisted, lausearvutuse põhisamaväärsused, järeldumine. Tõesuspuud.

   P. Tingimuste ja olukordade analüüsimine lausearvutuse abil. Tõesuspuude koostamine lausearvutuses.

2. nädal. L. Lausearvutuse valemite normaalkujud.

   P. Valemite teisendamine. Normaalkujude leidmine.

3. nädal. L. Indiviidid ja predikaadid. Kvantorid. Esimest järku keeled.

   P. Predikaadid ja kvantorid. Lihtsamate lausete väljendamine valemiga. Predikaatarvutuse valemi tõeväärtuse leidmine.

4. nädal. L. Signatuuri interpretatsioonid. Predikaatide väljendamine. Samaselt tõesus.

   P. Matemaatiliste lausete väljendamine. Interpretatsioonide koostamine.

5. nädal. L. Tõesuspuu predikaatarvutuses. Järeldumine, samaväärsus. Predikaatloogika põhisamaväärsused.

   P. Lausete väljendamine. Tõesuspuude koostamine predikaatarvutuses.

6. nädal. L. Predikaatloogika põhisamaväärsuste tõestamine. Prefikskuju.

   P. Predikaatarvutuse samaväärsuste kasutamine. Tõestamine interpretatsioonide abil.

7. nädal. L. Teoreem ja tõestus. Tõestustaktikad.

   P. Väidete tõestamine.

8. nädal. L. Aksiomaatilised teooriad. Peano aksiomaatika.

   P. Loogika kordamine. Kontrolltöö.

9. nädal. L. Graafi mõiste. Tipu aste. Tipuastmete teoreem. Ahelad ja tsüklid.

   P. Graafiteooria abil lahenduvad ülesanded. Graafide põhiomadused. Tipuastmete teoreem.

10. nädal. L. Sidusus. Graafide isomorfism.

    P. Graafiteoreetiliste väidete tõestamine.

11. nädal. L. Euleri ja Hamiltoni tsüklid. Elementaarsete graafioperatsioonide algoritmid.

    P. Tõestusülesanded. Euleri ja Hamiltoni tsükli leidmine.

12. nädal. L. Puud. Puude põhiomadused.

    P. Arvulised ülesanded puudest. Tõestusülesanded puudest.

13. nädal. L. Algoritmi korrektsuse tõestamine. Toespuud. Kruskali ja Primi algoritm.

P. Puude omaduste kasutamine. Toespuu algoritmid.

14. nädal. L. Kruskali ja Primi algoritmi korrektsus. Suunatud graafid.

P. Suunatud graafide abil lahenduvad ülesanded. Tõestusülesanded suunatud graafidest.

15. nädal. L. Lühima tee leidmise ülesanne. Laiuti otsimise algoritm. Dijkstra algoritm.

P. Graafide kordamine. Kontrolltöö.

16. nädal. L. Floydi–Warshalli algoritm.

P. Tugev sidusus. Suunatud ahelad ja tsüklid.

Peatükk 1

Matemaatiline loogika

1.1 Lausearvutus

1.1.1 Põhimõistete meeldetuletamine

Lausearvutuse põhimõistetega on lugeja tutvunud kursuses “Matemaatiline maailmapilt”. Selles paragrahvis tuletame kõik olulisemad mõisted lühidalt meelde.

Lausearvutuse uurimisobjektideks on laused, millele saab vastavusse seada tõeväärtuse (“tõene” või “väär”), mida antud kursuse jooksul tähistame sümbolitega 1 ja 0 (levinud on ka tähistus t ja v). Eeldatakse, et vaadeldavad laused rahuldavad järgmisi tingimusi.

Välistatud kolmanda seadus. Iga lause on kas tõene või väär.

Mittevasturääkivuse seadus. Ükski lause ei saa olla korraga tõene ja väär.

Keerulisemad laused jagatakse lihtlauseteks ja neid ühendavateks grammatilisteks seosteks. Lihtlausete tähistamiseks kasutatakse suuri ladina tähti A, B, C jne., mida nimetatakse **lausemuutujateks**. Grammatilistele seostele vastavad **lausearvutuse tehted**.

Liitlausete kohta tehakse veel järgmised eeldused.

- Liitlauseid võib moodustada suvalistest komponentlausetest, eeldamata nendevahelist sisulist seost.
- Liitlause tõeväärtus sõltub ainult komponentlausete tõeväärtustest, mitte sisust.

Tähtsamad lausearvutuse tehted on ära toodud järgmises tabelis.

tehte nimi	tähis	grammatiline seos
eitus	$\neg$	ei
konjunktsioon	$\&, \wedge$	ja
disjunktsioon	$\vee$	või (mittevälistav)
implikatsioon	$\Rightarrow, \rightarrow, \supset$	kui ..., siis ...
ekvivalents	$\Leftrightarrow, \leftrightarrow, \sim$	... parajasti siis, kui ...

Märkus 1.1 Lausearvutuse tehteid märgitakse erinevates allikates erinevate sümbolitega. Matemaatilise maailmapildi kursuses kasutati tähiseid $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Raamatus [8] on kasutusel komplekt $\neg, \&, \vee, \rightarrow, \leftrightarrow$. Käesolevas kursuses me eelistame sümboleid $\neg, \&, \vee, \Rightarrow, \Leftrightarrow$.

Lausearvutuse tehete definitsioonid võib lühidalt esitada järgmise tabeli abil:

A	B	$A\&B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\neg A$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

.

Definitsioon 1.2 Lausearvutuse valemid on parajasti need avaldised, mida saab koostada järgmiste reeglite abil.

1. Iga lausemuutuja on lausearvutuse valem.

2. Kui $\mathcal{F}$ on lausearvutuse valem, siis ka $\neg\mathcal{F}$ on lausearvutuse valem.

3. Kui $\mathcal{F}$ ja $\mathcal{G}$ on lausearvutuse valemid, siis ka $(\mathcal{F}\&\mathcal{G}), (\mathcal{F} \vee \mathcal{G}), (\mathcal{F} \Rightarrow \mathcal{G})$ ja $(\mathcal{F} \Leftrightarrow \mathcal{G})$ on lausearvutuse valemid.

Valemi konstrueerimise viimasel sammul kasutatud tehet nimetatakse selle valemi **peatehteks**.

Mõnikord on otstarbekas lubada valemites ka konstante 1 ja 0. Sellisel juhul asendatakse valemi definitsioonis tingimus 1 tingimusega

$1'$. Iga lausemuutuja on lausearvutuse valem ning tõeväärtused 1 ja 0 on lausearvutuse valemid.

Et vähendada sulgude arvu valemi kirjapanekus, tehakse järgmised kokkulepped.

1) Tehete prioriteet kõrgeimast madalaimani on $\neg, \&, \vee, \Rightarrow, \Leftrightarrow$.

2) Kui mitme liikme konjunktsioonis või disjunktsioonis sooritatakse tehteid vasakult paremale, siis võib tehete järjekorda täpsustavatest sulgudest loobuda.

3) Valemi välimised sulud võib ära jätta.

Näide 1.3 Valem

$$A \wedge \neg B \wedge (C \Rightarrow \neg A) \Leftrightarrow B \vee A$$

on moodustatud valemitest $A \wedge \neg B \wedge (C \Rightarrow \neg A)$ ja $B \vee A$ tehte $\Leftrightarrow$ abil. Seega selle valemi peatehe on $\Leftrightarrow$.

Lausearvutuse valemeid tähistame harilikult tähtedega $\mathcal{F}$, $\mathcal{G}$ ja $\mathcal{H}$. Kui tahame rõhutada, et valem $\mathcal{F}$ on koostatud kasutades näiteks lausemuutujaid X, Y, Z, siis kirjutame $\mathcal{F}(X, Y, Z)$.

Kui lausemuutuja X on tõene, siis kirjutame $X = 1$. Kui lausemuutuja X on väär, siis kirjutame $X = 0$. Kui meil on vaatluse all mingi lõplik hulk lausemuutujaid ja me omistame igale muutujale kindla tõeväärtuse, siis sellist tõeväärtuste komplekti nimetatakse nende muutujate **väärtustuseks**. (Formaalselt võib öelda, et lausemuutujate $X_1, X_2, \ldots, X_n$

väärtustus on hulga $\{0,1\}^n$ element, s.t. n-elemendiline järjend nullidest ja ühtedest.) Kui lausemuutujaid on n-tükki, siis nende väärtustusi on sama palju, kui on hulgas $\{0,1\}^n$ elemente, s.t. 2^n tükki.

Valemi tõeväärtuse leidmiseks muutujate väärtustuse korral kasutame järgnevat definitsiooni.

Definitsioon 1.4 Olgu fikseeritud lausearvutuse valemis $\mathcal{F}$ leiduvate lausemuutujate mingi väärtustus. Kui $\mathcal{F}$ on lausemuutuja, siis **valemi $\mathcal{F}$ tõeväärtuseks** loetakse sellele muutujale antud tõeväärtus. Kui $\mathcal{F}$ sisaldab vähemalt ühte lausearvutuse tehet, siis **valemi $\mathcal{F}$ tõeväärtus** leitakse järgmiste reeglite abil.

1. Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 0$.
2. Kui $\mathcal{F} = \mathcal{G} \,\&\, \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ ja $\mathcal{H} = 1$.
3. Kui $\mathcal{F} = \mathcal{G} \vee \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ või $\mathcal{H} = 1$.
4. Kui $\mathcal{F} = \mathcal{G} \Rightarrow \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 0$ või $\mathcal{H} = 1$.
5. Kui $\mathcal{F} = \mathcal{G} \Leftrightarrow \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ ja $\mathcal{H} = 1$ või $\mathcal{G} = 0$ ja $\mathcal{H} = 0$.

Kui kirjutame muutujate kõikvõimalikud väärtustused üksteise alla ja arvutame iga väärtustuse korral välja valemi tõeväärtuse, siis saame tabeli, mida kutsutakse antud valemi **tõeväärtustabeliks**. Näiteks valemi

$$\mathcal{F} = (A \Rightarrow B\&C) \vee \neg(A \vee \neg(B \vee C))$$

tõeväärtustabel on

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

.

Sellest tabelist näeme näiteks, et valemi $\mathcal{F}$ tõeväärtus väärtustusel $(1,0,1)$ on 0.

Iga n muutujat sisaldav lausearvutuse valem $\mathcal{F}(X_1,\dots,X_n)$ määrab ära ühe kujutuse

$$f(X_1,\dots,X_n) : \{1,0\}^n \to \{1,0\},$$

mis igale muutujate väärtustusele $(\alpha_1,\dots,\alpha_n) \in \{1,0\}^n$ seab vastavusse valemi tõeväärtuse sellel väärtustusel. Kujutusi

$$\{1,0\}^n \to \{1,0\}$$

nimetatakse n-kohalisteks **Boole'i**[1] **funktsioonideks**.

[1] George Boole (1815–1864) — inglise matemaatik

Näide 1.5 Valem $\mathcal{F}(X,Y) = X\&Y$ määrab ära Boole'i funktsiooni

$$\begin{aligned}(1,1) &\mapsto 1,\\ (1,0) &\mapsto 0,\\ (0,1) &\mapsto 0,\\ (0,0) &\mapsto 0.\end{aligned}$$

Arvutamisel võiksime põhimõtteliselt kirjutada näiteks, et $f(1,0) = 1\&0 = 0$.

Märkus 1.6 Formaalselt võib lausemuutujate $X_1, \dots, X_n$ väärtustust vaadelda kui kujutust

$$\alpha : \{X_1, \dots, X_n\} \to \{1, 0\},$$

mis igale lausemuutujale X_i seab vastavusse tema tõeväärtuse $\alpha_i \in \{1, 0\}$. (Nii on väärtustusi käsitletud näiteks raamatus [6].) Sellisel juhul võiksime $X_i = 0$ asemel kirjutada $\alpha(X_i) = 0$ ja $X_i = 1$ asemel $\alpha(X_i) = 1$. Samuti saaksime valemi tõeväärtuse väärtustusel α defineerida järgmisel viisil.

a) Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\alpha(\mathcal{F}) = \neg(\alpha(\mathcal{G}))$.

b) Kui $\mathcal{F} = \mathcal{G} \oplus \mathcal{H}$, kus $\oplus \in \{\&, \vee, \Rightarrow, \Leftrightarrow\}$, siis $\alpha(F) = \alpha(\mathcal{G}) \oplus \alpha(\mathcal{H})$.

Sellises käsitluses on valemi $\mathcal{F}$ poolt ära määratud Boole'i funktsioon f defineeritud võrdusega

$$f(\alpha) = \alpha(\mathcal{F}).$$

Lausearvutuse valemitel võib olla mitmesuguseid omadusi. Neist olulisemad on järgmised.

Definitsioon 1.7 Öeldakse, et lausearvutuse valem $\mathcal{F}$ on

- **samaselt tõene**, kui ta on igal väärtustusel tõene,
- **samaselt väär**, kui ta on igal väärtustusel väär,
- **kehtestatav**, kui ta on vähemalt ühel väärtustusel tõene.

Näide 1.8 Valem $A \vee \neg A$ on samaselt tõene. Valem $A\&\neg A$ on samaselt väär. Valem $A \vee B$ ei ole samaselt tõene ega samaselt väär, kuid on kehtestatav.

Kehtivad järgmised teoreemid.

Teoreem 1.9 ([7, lause 3.13]) *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt väär.*

Teoreem 1.10 ([7, lause 3.14]) *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eitus $\neg\mathcal{F}$ ei ole samaselt tõene.*

Definitsioon 1.11 Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **samaväärseteks**, kui nende tõeväärtused on võrdsed igal neis valemeis esinevate muutujate väärtustusel. Kui valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed, siis kirjutatakse $\mathcal{F} \equiv \mathcal{G}$.

Valemite $\mathcal{F}$ ja $\mathcal{G}$ samaväärsuse kontrollimiseks saab kasutada tõeväärtustabeleid. Tabelites tuleb anda väärtustusi kõigile muutujatele, mis esinevad vähemalt ühes neist kahest valemist. Kui valemite tõeväärtused on samad iga väärtustuse korral, siis $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed, vastasel korral mitte. Näiteks valemid $\mathcal{F} = A$ ja $\mathcal{G} = A\&(B \vee \neg B)$ on samaväärsed, sest nende tõeväärtused on võrdsed muutujate A ja B mistahes väärtustuse (α, β) korral.

Juhime tähelepanu, et samaväärsus ei ole lausearvutuse tehe ja $\mathcal{F} \equiv \mathcal{G}$ ei ole lausearvutuse valem. Tegemist on hoopis binaarse seosega kõigi lausearvutuse valemite hulgal.

Teoreem 1.12 *Seos $\equiv$ on ekvivalentsiseos kõigi lausearvutuse valemite hulgal.*

Tõestus. See seos on refleksiivne, sest iga valem on samaväärne iseendaga. Samuti on selge, et kui valemite $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused on samad mistahes neis valemeis esinevate muutujate väärtustuse korral, siis ka $\mathcal{G}$ ja $\mathcal{F}$ tõeväärtused on samad mistahes väärtustuse korral. See tähendab, et seos $\equiv$ on sümmeetriline.

Oletame nüüd, et $\mathcal{F} \equiv \mathcal{G}$ ja $\mathcal{G} \equiv \mathcal{H}$. Siis $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused on samad igal väärtustusel ning $\mathcal{G}$ ja $\mathcal{H}$ tõeväärtused on samad iga väärtustuse korral. Seega ka $\mathcal{F}$ ja $\mathcal{H}$ tõeväärtused on samad iga väärtustuse korral ehk $\mathcal{F} \equiv \mathcal{H}$. Sellega on tõestatud transitiivsus.

Kokkuvõttes oleme näidanud, et $\equiv$ on ekvivalentsiseos. $\square$

Teoreem 1.13 ([7, teoreem 4.12]) *Valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valem $\mathcal{F} \Leftrightarrow \mathcal{G}$ on samaselt tõene.*

Tuletame meelde lausearvutuse põhisamaväärsused:

LS1. $\mathcal{F}\&\mathcal{F} \equiv \mathcal{F}$	**LS2.** $\mathcal{F} \vee \mathcal{F} \equiv \mathcal{F}$
LS3. $\mathcal{F}\&\mathcal{G} \equiv \mathcal{G}\&\mathcal{F}$	**LS4.** $\mathcal{F} \vee \mathcal{G} \equiv \mathcal{G} \vee \mathcal{F}$
LS5. $(\mathcal{F}\&\mathcal{G})\&\mathcal{H} \equiv \mathcal{F}\&(\mathcal{G}\&\mathcal{H})$	**LS6.** $(\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H} \equiv \mathcal{F} \vee (\mathcal{G} \vee \mathcal{H})$
LS7. $F\&(\mathcal{F} \vee \mathcal{G}) \equiv \mathcal{F}$	**LS8.** $\mathcal{F} \vee F\&\mathcal{G} \equiv \mathcal{F}$
LS9. $\mathcal{F}\&(\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F}\&\mathcal{G} \vee \mathcal{F}\&\mathcal{H}$	**LS10.** $\mathcal{F} \vee \mathcal{G}\&\mathcal{H} \equiv (\mathcal{F} \vee \mathcal{G})\&(\mathcal{F} \vee \mathcal{H})$
LS11. $\neg(\mathcal{F}\&\mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}$	**LS12.** $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F}\&\neg\mathcal{G}$
LS13. $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg(\mathcal{F}\&\neg\mathcal{G})$	**LS14.** $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$
LS15. $\mathcal{F}\&\mathcal{G} \equiv \neg(\mathcal{F} \Rightarrow \neg\mathcal{G})$	**LS16.** $\mathcal{F} \vee \mathcal{G} \equiv \neg\mathcal{F} \Rightarrow \mathcal{G}$
LS17. $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F}\&\mathcal{G} \vee \neg\mathcal{F}\&\neg\mathcal{G}$	**LS18.** $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv (\mathcal{F} \Rightarrow \mathcal{G})\&(\mathcal{G} \Rightarrow \mathcal{F})$
LS19. $\mathcal{F}\&\mathcal{T} \equiv \mathcal{F}$	**LS20.** $\mathcal{F} \vee \mathcal{T} \equiv \mathcal{T}$
LS21. $\mathcal{F}\&\mathcal{V} \equiv \mathcal{V}$	**LS22.** $\mathcal{F} \vee \mathcal{V} \equiv \mathcal{F}$
	LS23. $\neg\neg\mathcal{F} \equiv \mathcal{F}$,

kus $\mathcal{T}$ on suvaline samaselt tõene valem ja $\mathcal{V}$ on suvaline samaselt väär valem.

Definitsioon 1.14 Öeldakse, et valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$ **järeldub** valem $\mathcal{G}$, kui igal neis valemeis esinevate muutujate väärtustusel, millel $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{G}$ tõene. Sellisel juhul kirjutatakse

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

Teoreem 1.15 ([7, teoreem 4.7]) *Valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$ parajasti siis, kui valem $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \Rightarrow \mathcal{G}$ on samaselt tõene.*

Seega kontrollimaks, kas $\mathcal{F}_1, \ldots, \mathcal{F}_n \models \mathcal{G}$ võime välja arvutada valemi $\mathcal{F}_1 \& \mathcal{F}_2 \& \ldots \& \mathcal{F}_n \Rightarrow \mathcal{G}$ tõeväärtustabeli.

Näide 1.16 Valemitest $A \Rightarrow B$ ja $B \Rightarrow C$ järeldub valem $A \Rightarrow C$, s.t. võime kirjutada

$$A \Rightarrow B, B \Rightarrow C \models A \Rightarrow C\,.$$

Näide 1.17 Lihtne on veenduda, et mistahes valemite $\mathcal{F}$ ja $\mathcal{G}$ korral

$$\begin{gathered} \mathcal{F} \& \mathcal{G} \models \mathcal{F}, \\ \mathcal{F} \models \mathcal{F} \vee \mathcal{G}, \\ \mathcal{F} \& \neg \mathcal{F} \models \mathcal{G}. \end{gathered}$$

Teoreem 1.18 ([7, teoreem 4.11]) *Valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ ja valemist $\mathcal{G}$ järeldub valem $\mathcal{F}$.*

Sümbolites:

$$\mathcal{F} \equiv \mathcal{G} \quad \text{parajasti siis, kui} \quad \mathcal{F} \models \mathcal{G} \text{ ja } \mathcal{G} \models \mathcal{F}.$$

1.1.2 Tõesuspuud

Kui meil on vaja uurida, kas antud valemi puhul leidub muutujate väärtustus, millel see valem on tõene või väär, siis alati on seda võimalik teha tõeväärtustabeli abil. Teatud juhtudel võib siiski kiiremini lahenduseni jõuda valemi struktuuri uurides. Näiteks valemi

$$\neg A \& (B \Rightarrow C) \& A$$

puhul on ilma tõeväärtustabelitagi selge, et see on samaselt väär.

Valemite süstemaatiliseks analüüsimiseks võib kasutada järgmist skeemi, mida nimetatakse **tõesuspuuks**. Oletame näiteks, et me tahame kindlaks teha, kas valem $\mathcal{F}$ on kehtestatav. Paneme kirja rea $\mathcal{F} = 1$ ja hakkame uurima, millistel juhtudel selline asi on võimalik. Selleks leiame valemis üles peatehte ja osavalemid, mida see peatehe seob. Siis leiame need osavalemite tõeväärtused, mille korral $\mathcal{F}$ on tõene. Kui selliseid tõeväärtuste komplekte on üks, siis kirjutame need üksteise alla. Kui neid on mitu, siis tekib meil puule kaks allapoole hargnevat haru. Edasi jätkame harude analüüsimist sama skeemi alusel, kuni jõuame välja lausemuutujateni. Kui puu mingis harus tekib vastuolu (s.t. selles harus esineb mingi valem tõese ja väärana), siis ütleme, et see haru on vastuoluline ehk **suletud** ja kirjutame selle alla märgi $\times$. Vastasel korral ütleme, et haru on **avatud**.

Lausearvutuse tehete analüüsimisel kasutame järgmisi elementaarsamme.

- Eitus:

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

- Konjunktsioon ja disjunktsioon:

$$\begin{array}{c}\mathcal{F}\&\mathcal{G}=1\\ | \\ \mathcal{F}=1\\ | \\ \mathcal{G}=1\end{array}\qquad\begin{array}{cc}\multicolumn{2}{c}{\mathcal{F}\&\mathcal{G}=0}\\ / & \backslash \\ \mathcal{F}=0 & \mathcal{G}=0\end{array}\qquad\begin{array}{cc}\multicolumn{2}{c}{\mathcal{F}\vee\mathcal{G}=1}\\ / & \backslash \\ \mathcal{F}=1 & \mathcal{G}=1\end{array}\qquad\begin{array}{c}\mathcal{F}\vee\mathcal{G}=0\\ | \\ \mathcal{F}=0\\ | \\ \mathcal{G}=0\end{array}$$

- Implikatsioon ja ekvivalents:

$$\begin{array}{cc}\multicolumn{2}{c}{\mathcal{F}\Rightarrow\mathcal{G}=1}\\ / & \backslash \\ \mathcal{F}=0 & \mathcal{G}=1\end{array}\qquad\begin{array}{c}\mathcal{F}\Rightarrow\mathcal{G}=0\\ | \\ \mathcal{F}=1\\ | \\ \mathcal{G}=0\end{array}\qquad\begin{array}{cc}\multicolumn{2}{c}{\mathcal{F}\Leftrightarrow\mathcal{G}=1}\\ / & \backslash \\ \mathcal{F}=1 & \mathcal{F}=0\\ | & | \\ \mathcal{G}=1 & \mathcal{G}=0\end{array}\qquad\begin{array}{cc}\multicolumn{2}{c}{\mathcal{F}\Leftrightarrow\mathcal{G}=0}\\ / & \backslash \\ \mathcal{F}=1 & \mathcal{F}=0\\ | & | \\ \mathcal{G}=0 & \mathcal{G}=1\end{array}$$

Näiteks esimene konjunktsiooniga seotud skeem ütleb seda, et valem $\mathcal{F}\&\mathcal{G}$ saab tõene olla ainult siis, kui $\mathcal{F}$ on tõene ja $\mathcal{G}$ on tõene.

Teine ekvivalentsiga seotud skeem ütleb aga seda, et $\mathcal{F}\Leftrightarrow\mathcal{G}$ saab olla väär kahel juhul: kui $\mathcal{F}$ on tõene ja $\mathcal{G}$ on väär või kui $\mathcal{F}$ on väär ja $\mathcal{G}$ on tõene.

Näide 1.19 Teha kindlaks, kas valem

$$\neg(A\Rightarrow B)\vee\neg(B\Rightarrow A)$$

saab olla mingil väärtustusel väär.

Tõesuspuu koostamist alustame sellest, et paneme kirja tingimuse

$$\neg(A\Rightarrow B)\vee\neg(B\Rightarrow A)=0.$$

Vaadeldava valemi peatehe on disjunktsioon. Osavalemite $\neg(A\Rightarrow B)$ ja $\neg(B\Rightarrow A)$ disjunktsioon saab olla väär ainult siis, kui mõlemad osavalemid on väärad. Kirjutame vastavad tingimused üksteise alla. Nüüd võrdus $\neg(A\Rightarrow B)=0$ kehtib ainult siis, kui $A\Rightarrow B=1$. Lisame vastava rea tõesuspuusse. Sellega oleme kogu võrduses $\neg(A\Rightarrow B)=0$ sisalduva info ära kasutanud ja märgime vastava rea läbivaadatuks kirjutades rea lõppu näiteks linnukese. Järgmine analüüsimata rida on $\neg(B \Rightarrow A) = 0$. See annab meile tingimuse $B \Rightarrow A = 1$. Märgime ka rea $\neg(B \Rightarrow A) = 0$ läbivaadatuks.

Tingimuse $A \Rightarrow B = 1$ kehtimiseks on kaks võimalust: $A = 0$ või $B = 1$. See tekitab meil puus hargnemise. Mõlemas harus tuleb veel arvestada ka tingimust $B \Rightarrow A = 1$, mis kehtib parajasti siis, kui $B = 0$ või $A = 1$. Kui oleme vastavad hargnemised kirja pannud, siis saame puu

$$\neg(A \Rightarrow B) \vee \neg(B \Rightarrow A) = 0$$

$$\begin{array}{c} \neg(A \Rightarrow B) = 0 \checkmark \\ \neg(B \Rightarrow A) = 0 \checkmark \\ A \Rightarrow B = 1 \checkmark \\ B \Rightarrow A = 1 \checkmark \end{array}$$

$$\begin{array}{cccc} \multicolumn{2}{c}{A = 0} & \multicolumn{2}{c}{B = 1} \\ B = 0 & A = 1 & B = 0 & A = 1. \\ & \times & \times & \end{array}$$

Selles puus on kõik tehteid sisaldavad osavalemid läbi vaadatud ja igas harus oleme jõudnud lausemuutujateni. Kaks keskmist haru on suletud (ehk vastuolulised), sest ei A ega B saa olla korraga tõene ja väär. Vastava haru suletust märgime ristiga. Ülejäänud kaks haru annavad meile aga kõikvõimalikud väärtustused, mille korral esialgne valem on väär. Need on $A = 0, B = 0$ ja $A = 1, B = 1$. Seega vastus esialgsele küsimusele on "jah".

Ühtlasi näeme ka, et esialgne valem on kehtestatav, kuid mitte samaselt tõene, sest tema tõeväärtus neljast muutujate väärtustusest kahe korral peab olema tõene.

Märgime veel, et lihtne on kontrollida, kas tõesti esialgse valemi tõeväärtus väärtustusel $(0, 0)$ on 0. Selleks võime lihtsalt arvutada

$$\neg(0 \Rightarrow 0) \vee \neg(0 \Rightarrow 0) = \neg 1 \vee \neg 1 = 0 \vee 0 = 0.$$

Näide 1.20 Teha kindlaks, kas valem

$$\neg(A \& B) \Rightarrow \neg A \vee \neg B$$

on samaselt tõene. Selleks kirjutame tõesuspuu algusse rea $\neg(A \& B) \Rightarrow \neg A \vee \neg B = 0$. (Valem on samaselt tõene, kui ei õnnestu leida sellist väärtustust, mille korral tema tõeväärtus on "väär".) Tõesuspuu näeb välja järgmine:

$$\neg(A\&B) \Rightarrow \neg A \vee \neg B = 0$$

$$\begin{array}{c} \neg(A\&B) = 1 \checkmark \\ \neg A \vee \neg B = 0 \checkmark \\ A\&B = 0 \checkmark \\ \neg A = 0 \checkmark \\ \neg B = 0 \checkmark \\ A = 1 \\ B = 1 \end{array}$$

$$\begin{array}{cc} A = 0 & B = 0 \\ \times & \times \end{array}$$

Hargnemise selles puus tekitab rida $A\&B = 0$. Nagu näeme, on mõlemad harud vastuolulised, seega väärtustust, millel esialgne valem oleks väär, ei leidu. See tähendab, et esialgne valem on samaselt tõene.

Rohkem näiteid tõesuspuude kohta võib leida raamatust [8], lk. 17–18.

Tõesuspuuga saab valemi omadusi kontrollida järgmiselt.

- **Samaselt tõesuse** kontrollimiseks kirjutame tõesuspuu algusse $\mathcal{F} = 0$. Kui igas harus tekib vastuolu, siis valem on samaselt tõene.
- **Samaselt vääruse** kontrollimiseks kirjutame tõesuspuu algusse $\mathcal{F} = 1$. Kui igas harus tekib vastuolu, siis valem on samaselt väär.
- **Kehtestatavuse** kontrollimiseks kirjutame tõesuspuu algusse $\mathcal{F} = 1$. Kui leidub haru, kus vastuolu ei teki, siis valem on kehtestatav.

Tõesuspuu abil saab kontrollida, kas valemitest $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$. Selleks üritame leida valemites esinevate muutujate väärtustust, mille korral

$$\mathcal{F}_1 = 1, \mathcal{F}_2 = 1, \ldots, \mathcal{F}_n = 1 \quad \text{ja} \quad \mathcal{G} = 0.$$

Kui see ei õnnestu (s.t. tõesuspuu kõik harud on vastuolulised), siis järeldumine kehtib. Tõesuspuu algusse kirjutame need $n+1$ tingimust ja edasi tegutseme nii nagu harilikult.

Näide 1.21 Tõestada, et

$$A \vee B \,\&\, C,\ A \vee B \Rightarrow D \models C \vee D.$$

Püüame leida A, B, C, D väärtustust, mille korral $A \vee B \,\&\, C = 1$, $A \vee B \Rightarrow D = 1$ ja $C \vee D = 0$. Koostame tõesuspuu:

$$A \vee B \,\&\, C = 1$$

$$\begin{array}{c} A \vee B \Rightarrow D = 1 \ \checkmark \\ C \vee D = 0 \ \checkmark \\ C = 0 \\ D = 0 \end{array}$$

$$\begin{array}{cccc} \multicolumn{2}{c}{A = 1} & \multicolumn{2}{c}{B\&C = 1 \ \checkmark} \\ A \vee B = 0 \ \checkmark & D = 1 & A \vee B = 0 & D = 1 \\ A = 0 & \times & B = 1 & \times \\ B = 0 & & C = 1 & \\ \times & & \times & \end{array}$$

Kuna kõik harud on vastuolulised, siis järeldumine kehtib.

1.2 Lausearvutuse valemite normaalkujud

1.2.1 Valemite teisendamine

Lausearvutuses on tihti otstarbekas teisendada valemeid lihtsamale kujule. Eesmärgiks võib olla näiteks see, et valem oleks paremini arusaadav või et tema tõeväärtust antud väärtustusel oleks kergem leida.

Lemma 1.22 *Kui $\mathcal{F}, \mathcal{G}$ ja $\mathcal{H}$ on lausearvutuse valemid, $\mathcal{F} \equiv \mathcal{G}$ ning $\oplus \in \{\&, \vee, \Rightarrow, \Leftrightarrow\}$, siis*

$$\neg\mathcal{F} \equiv \neg\mathcal{G}, \quad \mathcal{F} \oplus \mathcal{H} \equiv \mathcal{G} \oplus \mathcal{H}, \quad \mathcal{H} \oplus \mathcal{F} \equiv \mathcal{H} \oplus \mathcal{G}.$$

TÕESTUS. Kui $\mathcal{F}$ ja $\mathcal{G}$ on igal väärtustusel sama tõeväärtusega, siis ka $\neg\mathcal{F}$ ja $\neg\mathcal{G}$ on igal väärtustusel sama tõeväärtusega, s.t. $\neg\mathcal{F} \equiv \neg\mathcal{G}$. Analoogilisel põhjusel ka $\mathcal{F} \oplus \mathcal{H} \equiv \mathcal{G} \oplus \mathcal{H}$ ja $\mathcal{H} \oplus \mathcal{F} \equiv \mathcal{H} \oplus \mathcal{G}$. □

Selle lemma abil saab tõestada järgmise kasuliku fakti (täieliku tõestuse võib leida näiteks raamatust [6], lk. 25–26).

Substitutsiooniprintsiip. *Kui asendada valemis mingi osavalem sellega samaväärse valemiga, siis saadud valem on esialgsega samaväärne.*

Näiteks kui vaatleme valemit $\mathcal{F}\&\mathcal{H}$ ning teame (näiteks põhisamaväärsuste põhjal), et $\mathcal{F} \equiv \mathcal{G}$, siis asendades valemi $\mathcal{F}$ valemiga $\mathcal{G}$ saame valemi $\mathcal{G}\&\mathcal{H}$, mis on esialgsega samaväärne:

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

Näide 1.23 Kasutades lausearvutuse põhisamaväärsusi saame lihtsustada:

$$\begin{aligned} A\&B\&A &= (A\&B)\&A \\ &\equiv A\&(B\&A) && \textbf{(LS5)} \\ &\equiv A\&(A\&B) && \textbf{(LS3)} \\ &\equiv (A\&A)\&B && \textbf{(LS5)} \\ &\equiv A\&B. && \textbf{(LS1)} \end{aligned}$$

Iga lausearvutuse valemi jaoks leidub temaga samaväärne valem, mis sisaldab ainult kahte tehet.

Teoreem 1.24 *Iga lausearvutuse valemi jaoks leidub temaga samaväärne valem, mis sisaldab ainult järgmisi tehteid:*

a) $\&$ *ja* $\neg$;

b) $\vee$ *ja* $\neg$;

c) $\Rightarrow$ *ja* $\neg$.

TÕESTUS. Tõestame osa a) (osade b) ja c) tõestused on analoogilised).

Kuna mistahes valemite $\mathcal{F}$ ja $\mathcal{G}$ korral $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F}\&\neg\mathcal{G}$ (vt. põhisamaväärsust **LS12**), siis lemma 1.22 ja **LS23** põhjal

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

Põhisamaväärsust **LS17** kasutades saame, et

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

Valemi võib teisendada kujule, mis sisaldab ainult eitust ja konjunktsiooni, järgmise algoritmiga.

Kuni valemis leidub veel tehtemärke $\vee$, $\Rightarrow$ või $\Leftrightarrow$, teha järgmist: valida suvaline osavalem, mille peatehe ei ole & ega $\neg$ ning

- kui see osavalem on kujul $\mathcal{F} \vee \mathcal{G}$, siis asendada ta samaväärse osavalemiga $\neg(\neg\mathcal{F}\&\neg\mathcal{G})$,
- kui see osavalem on kujul $\mathcal{F} \Rightarrow \mathcal{G}$, siis asendada ta samaväärse osavalemiga $\neg(\mathcal{F}\&\neg\mathcal{G})$,
- kui see osavalem on kujul $\mathcal{F} \Leftrightarrow \mathcal{G}$, siis asendada ta samaväärse osavalemiga $\neg(\neg(\mathcal{F}\&\mathcal{G})\&\neg(\neg\mathcal{F}\&\neg\mathcal{G}))$.

Selle algoritmi igal sammul väheneb valemis mittelubatud tehtemärkide arv ühe võrra. Varem või hiljem muutub see nulliks ja saadud valem on nõutaval kujul. □

1.2.2 Normaalkujudest üldiselt

Matemaatika üks üldine eesmärk on esitada keerulisi asju võimalikult lihtsal kujul.

Matemaatiliste objektide vaatlemisel tekib tihti selline küsimus: kas antud objekti jaoks on võimalik leida üks teine objekt, mis mingis mõttes on esialgsega samaväärne, kuid mingis mõttes esialgsest parem (näiteks lihtsam, paremini arusaadav). Vaatame selle kohta mõningaid näiteid.

Näide 1.25 1. Iga algebralise avaldise, mis on moodustatud muutujast x ja reaalarvudest kasutades liitmis-, lahutamis- ja korrutamistehet saab esitada polünoomi kujul, s.t. kujul

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0. \tag{1.1}$$

Näiteks avaldise $x + x(2x - 3) + 5$ saab pärast sulgude avamist ja koondamist viia kujule $2x^2 - 2x + 5$. Viimane kuju on esimesest märgatavalt lihtsam ja temaga opereerida on kergem. Näiteks tuletist on võimalik leida nii avaldisest $x+x(2x-3)+5$ kui ka avaldisest $2x^2 - 2x + 5$, kuid viimast kasutades on seda märksa lihtsam teha. Samuti on kahe algebralise avaldise võrdsust kontrollida lihtsam, kui nad on esitatud polünoomi kujul. Niisiis mainitud algebraliste avaldiste puhul on loomulik lugeda nii-öelda normaalkujuks esitust kujul (1.1). Ühe muutuja polünoomidest räägitakse põhjalikumalt kursuses “Algebra I”.

2. On võimalik vaadelda mitme muutuja polünoome. Neid saab esitada üksliimete abil kasutades liitmis- ja lahutamistehet. Näiteks võib vaadelda kolme muutuja polünoomi

$$3x^2yz^7 - 2y^2z + 21.$$

Mitme muutuja polünoome käsitletakse kursuses “Algebra II”.

3. Ruutmaatriksitel on erinevaid normaalkujusid. Neist ühte kutsutakse Jordani normaalkujuks. Nimelt iga ruutmaatriksi A jaoks leidub temaga sarnane (siinkohal sõnal “sarnane” on täpne matemaatiline tähendus) maatriks $\mathcal{J}(A)$, mis on Jordani normaalkujul. Selles normaalkujus on palju nulle ja seetõttu on sellisel kujul maatriksitega lihtne arvutada. Jordani normaalkujust on juttu kursuses “Algebra II”.

4. Geomeetrias on igal teist järku joonel ja pinnal olemas kanooniline võrrand. Näiteks ellipsi kanooniline võrrand on $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$. Kanoonilise võrrandi põhjal on lihtne aru saada, millist tüüpi joone või pinnaga on tegu, ning tihti saab kanoonilisest võrrandist välja lugeda ka oluliste parameetrite väärtusi. Teist järku joontest ja pindadest on juttu kursuses “Analüütiline geomeetria”.

Osutub, et ka lausearvutuse valemite puhul on olemas normaalkujud, mis on esialgsete valemitega samaväärsed (definitsiooni 1.11 mõttes), kuid mingis mõttes esialgsetest valemitest paremad. Selles kursuses vaatleme põhjalikumalt valemi (täielikku) disjunktiivset normaalkuju, mis on mingis mõttes sarnane mitme muutuja polünoomide normaalkujuga.

1.2.3 Täielik disjunktiivne normaalkuju

Definitsioon 1.26 Lausemuutujat või selle eitust nimetatakse **literaaliks**. Lausemuutujat nimetatakse **positiivseks literaaliks** ja lausemuutuja eitust **negatiivseks literaaliks**.

Näiteks A, B, C, D on positiivsed literaalid ja $\neg A, \neg B, \neg C, \neg D$ on negatiivsed literaalid.

Definitsioon 1.27 **Lihtkonjunktsiooniks** ehk **elementaarkonjunktsiooniks** nimetatakse valemit, mis on moodustatud literaalidest kasutades ainult konjunktsiooni tehet, kusjuures ükski lausemuutuja ei esine selles valemis mitu korda.

Definitsioon 1.28 Lihtkonjunktsiooni nimetatakse **täielikuks**, kui vaadeldavatest muutujatest igaüks esineb selles täpselt ühe korra.

Seega lihtkonjunktsioon on valem kujul

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

kus $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$ on literaalid. Näiteks $A\&\neg B\&C$ on täielik lihtkonjunktsioon lausemuutujatest A, B ja C, kuid $\neg A\&C$ on mittetäielik lihtkonjunktsioon muutujatest A, B ja C.

Kahte lihtkonjunktsiooni loeme samadeks, kui nad erinevad ainult literaalide järjestuse poolest. Näiteks loeme, et $A\&\neg B\&C$ ja $C\&A\&\neg B$ on üks ja sama lihtkonjunktsioon. Enamasti loetakse, et lausemuutujate jaoks on fikseeritud kindel järjestus (nt. tähestikuline), ja lihtkonjunktsioonide kirjapanekul arvestatakse seda järjestust.

Lihtne on aru saada, et erinevaid täielikke lihtkonjunktsioone n muutujast on 2^n tükki.

Definitsioon 1.29 Valemi $\mathcal{F}$ **disjunktiivseks normaalkujuks** (lühidalt DNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate lihtkonjunktsioonide disjunktsiooni. Kui kõik selles normaalkujus esinevad lihtkonjunktsioonid on täielikud, siis öeldakse, et on tegemist **täieliku disjunktiivse normaalkujuga** (lühidalt TDNK). TDNK-s esinevaid lihtkonjunktsioone nimetatakse selle TDNK **liikmeteks**.

Näide 1.30 Valem

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

on TDNK-l. Valem

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

on DNK-l, aga mitte TDNK-l.

Lepime kokku, et mistahes lausemuutuja X korral kasutame tähistusi

$$X^1 = X \quad \text{ja} \quad X^0 = \neg X.$$

Seega iga literaali saab kirja panna kujul X^α, kus $\alpha \in \{0, 1\}$.

Lemma 1.31 *Iga $\alpha \in \{0,1\}$ korral*

$$X^\alpha = 1 \ \textit{parajasti siis, kui} \quad X = \alpha$$

(s.t. literaali X^α tõeväärtus on 1 parajasti siis, kui muutuja X tõeväärtus on α).

Tõestus. Vaatleme kahte juhtumit.

1) Olgu $\alpha = 1$. Siis võrdus $X^\alpha = 1$ on samaväärne võrdusega $X = 1$.

2) Olgu $\alpha = 0$. Siis võrdus $X^\alpha = 1$ on samaväärne võrdusega $\neg X = 1$, mis omakorda on samaväärne võrdusega $X = 0$. □

Teoreem 1.32 *Täielike lihtkonjunktsioonide disjunktsioon*

$$\mathcal{F}' = X_1^{\alpha_{11}}\&\ldots\&X_n^{\alpha_{1n}} \vee X_1^{\alpha_{21}}\&\ldots\&X_n^{\alpha_{2n}} \vee \ldots \vee X_1^{\alpha_{m1}}\&\ldots\&X_n^{\alpha_{mn}}$$

on tõene parajasti väärtustustel $(\alpha_{i1}, \ldots, \alpha_{in})$, kus $i = 1, \ldots, m$.

Tõestus. Tarvilikkus. Oletame, et valem $\mathcal{F}'$ on tõene mingil väärtustusel $(\beta_1, \ldots, \beta_n)$. Disjunktsiooni definitsiooni tõttu leidub siis selline $i \in \{1, \ldots, m\}$, et sellel väärtustusel $X_1^{\alpha_{i1}}\&\ldots\&X_n^{\alpha_{in}} = 1$. Vastavalt konjunktsiooni definitsioonile peavad siis kehtima võrdused

$$X_1^{\alpha_{i1}} = 1, \ldots, X_n^{\alpha_{in}} = 1.$$

Tänu lemmale 1.31

$$X_1 = \alpha_{i1}, \ldots, X_n = \alpha_{in},$$

mis tähendab, et väärtustus $(\beta_1, \ldots, \beta_n)$ langeb kokku väärtustusega $(\alpha_{i1}, \ldots, \alpha_{in})$.

Piisavus. Andes muutujatele $X_1, \ldots, X_n$ väärtustuse $(\alpha_{i1}, \ldots, \alpha_{in})$, kus $i \in \{1, \ldots, m\}$, ja kasutades lemmat 1.31 võime kirjutada, et

$$X_1^{\alpha_{i1}} = 1, \ldots, X_n^{\alpha_{in}} = 1.$$

Seega ka

$$X_1^{\alpha_{i1}}\&\ldots\&X_n^{\alpha_{in}} = 1$$

ja $\mathcal{F}' = 1$. □

Olgu meie ülesanne järgmine: leida valemi $\mathcal{F}$ TDNK, s.t. selline valem $\mathcal{F}'$, et

a) $\mathcal{F} \equiv \mathcal{F}'$,

b) $\mathcal{F}'$ on täielikul disjunktiivsel normaalkujul.

Selle ülesande lahendamiseks on kaks võimlust.

Esimene neist kasutab tõeväärtustabelit. Arvutades välja valemi $\mathcal{F}$ tõeväärtustabeli näeme, millised on muutujate väärtustused, millel $\mathcal{F}$ on tõene. Kuna $\mathcal{F}$ ja $\mathcal{F}'$ on samaväärsed, siis $\mathcal{F}'$ on tõene täpselt nendel samadel väärtustustel. Lause 1.32 põhjal saame siis valemi $\mathcal{F}'$ välja kirjutada.

Näide 1.33 Leiame valemi

$$\mathcal{F} = (A \Rightarrow B\&C) \vee \neg(A \vee \neg(B \vee C))$$

TDNK kasutades tõeväärtustabelit

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

.

Tabelist näeme, et $\mathcal{F}$ on tõene viiel väärtustusel. Nende väärtustuste abil kirjutame välja vastavad TDNK liikmed:

A	B	C	TDNK liige
1	1	1	$A\&B\&C$
0	1	1	$\neg A\&B\&C$
0	1	0	$\neg A\&B\&\neg C$
0	0	1	$\neg A\&\neg B\&C$
0	0	0	$\neg A\&\neg B\&\neg C$

.

Seega valemi $\mathcal{F}$ TDNK on

$$A\&B\&C \vee \neg A\&B\&C \vee \neg A\&B\&\neg C \vee \neg A\&\neg B\&C \vee \neg A\&\neg B\&\neg C. \qquad (1.2)$$

1.2.4 Täielikule disjunktiivsele normaalkujule teisendamine

Teine võimalus TDNK leidmiseks on kasutada järgmist algoritmi.

Täielikule disjunktiivsele normaalkujule teisendamise algoritm.

1. Elimineerime implikatsioonid ja ekvivalentsid, kasutades näiteks samaväärsusi

   $$\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}, \quad \mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F}\&\mathcal{G} \vee \neg\mathcal{F}\&\neg\mathcal{G}.$$

   Tulemuseks saadud valem sisaldab ainult eitust, konjunktsiooni ja disjunktsiooni.

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

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

   Kahekordsed eitused jätame ära. Tulemuseks on valem, kus ei ole ühtegi eitust sulgude ees.

3. Distributiivsuse seadust

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

   kasutades asendame disjunktsioonide konjunktsioonid konjunktsioonide disjunktsioonidega.

4. Kui esineb samaselt vääraid konjunktsioone (selliseid, kus esinevad korraga X ja $\neg X$), siis jätame need ära. Igast järelejäänud konjunktsioonist jätame ära literaalide kordused. Võrdsetest konjunktsioonidest jätame idempotentsuse omaduse

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

   tõttu alles ainult ühe.

   Tulemusena oleme saanud valemi disjunktiivse normaalkuju.

5. Täieliku disjunktiivse normaalkuju saamiseks tuleb iga lihtkonjunktsioon teha täielikuks. Kui näiteks lihtkonjunktsioonis $\mathcal{K}$ puutub muutuja X, siis samaväärsuse

   $$\mathcal{K} \equiv \mathcal{K}\&(X \vee \neg X) \equiv \mathcal{K}\&X \vee \mathcal{K}\&\neg X$$

   abil saame muutuja X lisada.

6. Korrastame valemi: järjestame literaalid konjunktsioonides ja kaotame ära korduvad konjunktsioonid.

Märkus 1.34 Sammul 4 võib juhtuda, et kõik konjunktsioonid on samaselt väärad. Sellisel juhul peaksime nad kõik ära jätma ning tegemist on samaselt väära valemiga. Selles olukorras öeldakse, et antud valemil puudub TDNK. Mõnikord öeldakse teooria ühtsuse huvides, et samaselt väära valemi TDNK on tühi valem — valem, mis ei sisalda ühtegi liiget.

Näide 1.35 Leiame TDNK valemile

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

Rakendame algoritmi:

$$\begin{aligned}
\mathcal{F} &\equiv (\neg A \vee B\&C) \vee \neg(A \vee \neg(B \vee C)) && \text{(Samm 1)}\\
&\equiv \neg A \vee B\&C \vee \neg A\&\neg\neg(B \vee C) && \text{(Samm 2)}\\
&\equiv \neg A \vee B\&C \vee \neg A\&(B \vee C) && \text{(Samm 2)}\\
&\equiv \neg A \vee B\&C \vee \neg A\&B \vee \neg A\&C. && \text{(Samm 3)}
\end{aligned}$$

Sellega on leitud valemi $\mathcal{F}$ DNK. TDNK leidmiseks tuleb konjunktsioonidesse lisada veel puuduvad muutujad ja valemit korrastada:

$$\begin{aligned}
\mathcal{F} &\equiv \neg A \vee B\&C \vee \neg A\&B \vee \neg A\&C\\
&\equiv \neg A\&(B \vee \neg B)\&(C \vee \neg C) \vee B\&C\&(A \vee \neg A)\\
&\quad \vee \neg A\&B\&(C \vee \neg C) \vee \neg A\&C\&(B \vee \neg B) && \text{(Samm 5)}\\
&\equiv (\neg A\&B \vee \neg A\&\neg B)\&(C \vee \neg C) \vee B\&C\&A \vee B\&C\&\neg A\\
&\quad \vee \neg A\&B\&C \vee \neg A\&B\&\neg C \vee \neg A\&C\&B \vee \neg A\&C\&\neg B && \text{(Samm 5)}\\
&\equiv \neg A\&B\&C \vee \neg A\&B\&\neg C \vee \neg A\&\neg B\&C \vee \neg A\&\neg B\&\neg C\\
&\quad \vee A\&B\&C \vee \neg A\&B\&C \vee \neg A\&B\&C \vee \neg A\&B\&\neg C\\
&\quad \vee \neg A\&B\&C \vee \neg A\&\neg B\&C && \text{(Samm 5, 6)}\\
&\equiv \neg A\&B\&C \vee \neg A\&B\&\neg C \vee \neg A\&\neg B\&C \vee \neg A\&\neg B\&\neg C \vee A\&B\&C. && \text{(Samm 6)}
\end{aligned}$$

Viimane valem ongi valemi $\mathcal{F}$ TDNK. Nagu näeme, on saadud TDNK liikmete järjekorra täpsuseni täpselt sama, mis tõeväärtustabeli põhjal leitud TDNK (1.2).

1.2.5 TDNK omadused ja rakendused

Vaatleme mõningaid loomulike küsimusi seoses TDNK-ga.

Kas igal valemil leidub TDNK? Me teame, et TDNK saame kirja panna tõeväärtustabeli põhjal, kui selles leidub vähemalt üks väärtustus, mille korral valem on tõene. Kui valem on samaselt väär, siis peaks tema TDNK olema tühi valem, aga seda reeglina valemite hulka ei loeta. Seega TDNK on olemas kõigil kehtestatavatel valemitel.

Kas valemi TDNK on üheselt määratud? Valemi tõeväärtustabel määrab üheselt ära, millised liikmed TDNK-sse kuuluvad, aga ta ei ütle, millises järjekorras need liikmed peavad olema. Seega TDNK on määratud üheselt liikmete järjekorra täpsusega.

Normaalkujude abil saab kindlaks teha, kas meil kasutusel olev tehete komplekt on piisav. Tehete defineerimisel võtsime viis tihti esinevat lausete ühendamise viisi ja formaliseerisime need. Võib küsida, kas on mingeid teisi lausete ühendamise viise, mida meie tehted ei väljenda?

Me leppisime kokku, et liitlause tõeväärtus sõltub ainult komponentlausete tõeväärtustest. Seega iga lausete ühendamise viis on kujutus, mis komponentlausete tõeväärtuste komplektile seab vastavusse liitlause tõeväärtuse:

$$f : \{0,1\}^n \to \{0,1\}.$$

Selliseid kujutusi nimetasime Boole'i funktsioonideks. Niisiis peame küsima, kas iga Boole'i funktsioon on määratud mingi lausearvutuse valemi poolt?

Teoreem 1.36 *Iga Boole'i funktsiooni $f : \{0,1\}^n \to \{0,1\}$ jaoks leidub lausearvutuse valem $\mathcal{F}(X_1, \ldots, X_n)$, mis ei sisalda muid tehtemärke kui &, $\vee$ ja $\neg$, ning mille poolt määratud Boole'i funktsioon on f.*

Tõestus. Olgu antud Boole'i funktsioon $f : \{0,1\}^n \to \{0,1\}$. Leiame kõik järjendid $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, mille korral $f(\alpha_1, \ldots, \alpha_n) = 1$. Kui selliseid on vähemalt üks, siis saame moodustada TDNK-l oleva lausearvutuse valemi $\mathcal{F} = \mathcal{F}(X_1, \ldots, X_n)$, nii et $\mathcal{F}$ on tõene parajasti nendel väärtustustel $(\alpha_1, \ldots, \alpha_n)$, mille korral $f(\alpha_1, \ldots, \alpha_n) = 1$. Seega f on valemi $\mathcal{F}$ poolt määratud Boole'i funktsioon.

Kui $f(\alpha_1, \ldots, \alpha_n) = 0$ iga $(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$ korral, siis f on võrdne suvalise samaselt väära valemi (näiteks $X_1 \& \neg X_1$) poolt määratud Boole'i funktsiooniga. □

Normaalkujude abil on lihtne kindlaks teha valemite põhiomadusi ja põhilisi seoseid valemite vahel.

- **Samaselt tõesus.** Valem on samaselt tõene parajasti siis, kui tema TDNK sisaldab kõiki 2^n täielikku lihtkonjunktsiooni, kus n on muutujate arv valemis.
- **Kehtestatavus.** Valem on kehtestatav parajasti siis, kui tal leidub TDNK.
- **Samaväärsus.** Kaks valemit on samaväärsed parajasti siis, kui neil on samad TDNK-d (liikmete järjekorra täpsusega).
- **Järeldumine.** Valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ parajasti siis, kui valemi $\mathcal{F}$ TDNK iga liige on ka valemi $\mathcal{G}$ TDNK liige.

1.2.6 Mittetäielik disjunktiivne normaalkuju

Mõnikord ei ole tingimata vajalik täielikku disjunktiivset normaalkuju leida, piisab juba mingi disjunktiivse normaalkuju leidmisest.

Näites 1.35 nägime, et valemi

$$\mathcal{F} = (A \Rightarrow B \& C) \vee \neg(A \vee \neg(B \vee C))$$

disjunktiivseks normaalkujuks on

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

Kui näiteks eesmärgiks on leida mingi muutujate A, B, C väärtustus, mille korral $\mathcal{F}$ on tõene, siis DNK $\mathcal{F}'$ järgi on seda väga lihtne teha: sobib näiteks iga väärtustus, kus A on väär, sest siis $\neg A = 1$ ja $\mathcal{F}' = 1$. Seega näiteks väärtustustel $(0,1,1), (0,1,0), (0,0,1)$ ja $(0,0,0)$ on $\mathcal{F}$ tõene. Arvestades veel teisi $\mathcal{F}'$ liikmeid saaksime põhimõtteliselt leida kõik väärtustused, millel $\mathcal{F}$ on tõene.

Erinevalt TDNK-st ei ole valemi DNK üheselt määratud.

Näide 1.37 Valem

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

on DNK-l. Arvestades põhisamaväärsust **LS8** saame kirjutada

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

kus ka $A\&B$ on DNK, seejuures esimesest DNK-st mõnevõrra lihtsam.

Näide 1.38 Võib veenduda (nt. tõeväärtustabeli abil), et valemi

$$\mathcal{F} = (A \Leftrightarrow B) \Rightarrow \neg A\&B$$

disjunktiivseks normaalkujuks sobib nii valem

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

kui ka valem

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

1.2.7 Konjunktiivsetest normaalkujudest

Vahetades ära konjunktsiooni ja disjunktsiooni rollid võib rääkida valemi (täielikust) konjunktiivsest normaalkujust.

Definitsioon 1.39 Lausemuutujate $X_1, \ldots, X_n$ **täielikuks lihtdisjunktsiooniks** ehk **täielikuks elementaardisjunktsiooniks** nimetatakse literaalide disjunktsiooni

$$X_1^{\alpha_1} \vee \ldots \vee X_n^{\alpha_n}.$$

Definitsioon 1.40 Valemi $\mathcal{F}$ **konjunktiivseks normaalkujuks** (lühidalt KNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate lihtdisjunktsioonide konjunktsiooni. Kui kõik selles normaalkujus esinevad lihtdisjunktsioonid on täielikud, siis öeldakse, et on tegemist **täieliku konjunktiivse normaalkujuga** (lühidalt TKNK).

Niisiis TKNK-l olev valem näeb välja nii:

$$(X_1^{\alpha_{11}} \vee \ldots \vee X_n^{\alpha_{1n}})\&(X_1^{\alpha_{21}} \vee \ldots \vee X_n^{\alpha_{2n}})\&\ldots\&(X_1^{\alpha_{m1}} \vee \ldots \vee X_n^{\alpha_{mn}}),$$

kus $\alpha_{ij} \in \{1, 0\}$.

Näide 1.41 Näiteks valem

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

muutujate A ja B suhtes on täielikul konjunktiivsel normaalkujul.

Analoogiliselt teoreemiga 1.32 saab tõestada järgmise tulemuse.

Teoreem 1.42 *Täielik konjunktiivne normaalkuju*

$$(X_1^{\alpha_{11}} \vee \ldots \vee X_n^{\alpha_{1n}}) \& (X_1^{\alpha_{21}} \vee \ldots \vee X_n^{\alpha_{2n}}) \& \ldots \& (X_1^{\alpha_{m1}} \vee \ldots \vee X_n^{\alpha_{mn}}).$$

on väär väärtustustel $(\neg\alpha_{i1}, \ldots, \neg\alpha_{in})$*,* $i \in \{1, \ldots, m\}$*, ja tõene kõigil ülejäänud väärtustustel.*

See teoreem võimaldab valemi TKNK välja kirjutada tõeväärtustabeli järgi. Leiame tabelist kõik väärtustused, millel meie valem on väär. Iga sellise väärtustuse $(\alpha_1, \ldots, \alpha_n)$ korral lisame TKNK-sse täieliku lihtdisjunktsiooni $X_1^{\neg\alpha_1} \vee \ldots \vee X_n^{\neg\alpha_n}$. Näiteks kui valem $\mathcal{F} = \mathcal{F}(A, B, C)$ on väär väärtustustel

$$(1, 1, 1), \quad (1, 0, 0), \quad (0, 0, 1),$$

ja ülejäänud väärtustustel tõene, siis tema TKNK on

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

Valemi TKNK võib leida ka teisendamise teel. Ei ole keeruline aru saada, mismoodi peaks eelmises paragrahvis toodud algoritmi modifitseerima selleks, et saaks leida valemi täieliku konjunktiivse normaalkuju.

1.3 Predikaatarvutus

1.3.1 Indiviidid ja predikaadid

Lausearvutuses vaadeldakse lauseid kui lihtlausetest moodustatud liitlauseid. Seejuures lihtlauseid käsitletakse kui tervikuid, mida enam osadeks jagada ei saa.

Predikaatloogikas jagatakse ka lihtlaused teatud osadeks. Täpsemalt öeldes jagatakse laused

- *indiviidideks* ehk *subjektideks*, mille kohta midagi väidetakse, ja
- *predikaadiks*, s.t. seoseks, milles indiviide väidetakse olevat.

Näiteks

lause	indiviid(id)	predikaat
3 on väiksem kui 7	3, 7	on väiksem kui
$2+4=6$	$2, 4, 6$	$\ldots + \ldots = \ldots$
3 on paaritu arv	3	on paaritu arv
lumi on valge	lumi	on valge

.

Nagu näeme võivad predikaadid sisaldada erineval arvul indiviide (eelmises näites on neid $1, 2$ või 3). Kui indiviide on predikaadis n tükki, siis räägitakse *n-kohalisest predikaadist*.

Predikaadi puhul on oluline ära näidata, milline on see hulk, kuhu võivad kuuluda tema indiviidid. Näiteks predikaati "on väiksem kui" võib vaadelda naturaalarvude hulgal, reaalarvude hulgal või hoopis päikesesüsteemi planeetide hulgal.

n-kohalist predikaati võib vaadelda kui n muutujast sõltuvat lauset, millel on muutujate konkreetsete väärtuste korral üheselt määratud tõeväärtus.

Nii näiteks võime naturaalarvude hulgal[2] $\mathbb{N}$ vaadelda kahekohalist predikaati

$$x \text{ on väiksem kui } y.$$

Kui $x = 3$ ja $y = 7$, siis selle lause tõeväärtus on 1, kui aga $x = 4$ ja $y = 2$, siis on tõeväärtus 0.

Predikaadi range definitsioon esitatakse harilikult järgmisel kujul.

Definitsioon 1.43 Olgu M mittetühi hulk. Hulgal M määratud **n-kohaliseks predikaadiks** nimetatakse kujutust $P : M^n \to \{1, 0\}$. Hulka M nimetatakse sellise predikaadi **indiviidide piirkonnaks**.

Definitsioon 1.44 Predikaadi $P : M^n \to \{1, 0\}$ **tõesuspiirkonnaks** nimetatakse hulka

$$T_P = \{(a_1, \ldots, a_n) \in M^n \mid P(a_1, \ldots, a_n) = 1\}.$$

Vaatleme veel näiteid.

[2]Käesolevas kursuses loeme, et $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Näide 1.45 Naturaalarvude hulgal $\mathbb{N}$ võib vaadelda ühekohalist predikaati $P(x) =$ "x on algarv". See on siis kujutus

$$P : \mathbb{N} \to \{1, 0\},$$

mis igale naturaalarvule seab vastavuse tõeväärtuse 1 või 0 vastavalt sellele, kas see naturaalarv on algarv või mitte. Muuhulgas

$$P(0) = 0,\ P(1) = 0,\ P(2) = 1,\ P(3) = 1,\ P(4) = 0, ...$$

Selle predikaadi tõesuspiirkond on kõigi algarvude hulk.

Näide 1.46 Olgu M kõigi maailmajagude hulk

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

ning vaatleme kahekohalist predikaati

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

Siis näiteks

$$\begin{array}{ll} Q(\text{Aafrika, Aasia}) = 1, & Q(\text{Ameerika, Aasia}) = 0, \\ Q(\text{Aafrika, Ameerika}) = 0, & Q(\text{Euroopa, Aasia}) = 1, \\ Q(\text{Aasia, Ameerika}) = 0, & Q(\text{Euroopa, Euroopa}) = 1. \end{array}$$

Märkus 1.47 Põhimõtteliselt võivad indiviidid kuuluda ka erinevatesse hulkadesse, s.t. predikaat võib olla kujutus $M_1 \times \ldots \times M_n \to \{1, 0\}$. Sellisel juhul räägitakse *mitmesordilistest predikaatidest*. Käesolevas kursuses me selliseid predikaate ei vaatle. Selles kursuses vaatleme ainult ühesordilist predikaatarvutust, kus eeldatakse, et komponentlausetes esinevad predikaadid on defineeritud ühel ja samal piirkonnal.

Märkus 1.48 Kuna predikaadi tõesuspiirkond on hulga M^n alamhulk, siis võime teda vaadelda n-kohalise seosena hulgal M. Näiteks iga kahekohaline predikaat määrab ära ühe binaarse seose.

Predikaatarvutus üldistab lausearvutust selles mõttes, et predikaadi tõeväärtus võib sõltuda argumentide väärtustest, samal ajal kui lausearvutuse lausel argumente ei ole ja tema tõeväärtus on kogu käsitluse jooksul ühesugune. Põhimõtteliselt võib lausearvutuse valemeid vaadelda kui nullkohalisi predikaate, s.t. kujutusi $M^0 \to \{0, 1\}$. Selline kujutus fikseerib hulgas $\{0, 1\}$ ühe elemendi (vaadeldava lause tõeväärtuse).

Predikaate võib siduda lausearvutuse tehete abil, et moodustada lihtsamatest predikaatidest keerulisemaid. Näiteks võib hulgal M defineeritud predikaatidest $P(x_1, \ldots, x_n)$ ja $Q(y_1, \ldots, y_m)$ moodustada predikaadi

$$R(x_1, \ldots, x_n, y_1, \ldots, y_m) = P(x_1, \ldots, x_n) \,\&\, Q(y_1, \ldots, y_m),$$

mille väärtus kohal $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ on 1 parajasti siis, kui $P(x_1, \ldots, x_n) = 1$ ja $Q(y_1, \ldots, y_m) = 1$. Ülejäänud lausearvutuse tehete korral toimitakse analoogiliselt.

Näide 1.49 Vaatleme naturaalarvude hulgal $\mathbb{N}$ predikaate

$$P(x) = \text{“}x \text{ on algarv”},$$
$$Q(x,y) = \text{“}y \text{ jagub arvuga } x\text{”}.$$

Siis võime moodustada kahekohalise predikaadi

$$\begin{aligned} R(x,y) &= P(x)\&Q(x,y) \\ &= \text{“}x \text{ on algarv ja } y \text{ jagub arvuga } x\text{”} \\ &= \text{“}x \text{ on arvu } y \text{ algtegur”}. \end{aligned}$$

Näiteks $R(2,24) = 1$ ja $R(6,24) = 0$.

Võib aga moodustada ka kolmekohalise predikaadi

$$S(x,y,z) = P(x)\&Q(y,z) = \text{“}x \text{ on algarv ja } z \text{ jagub arvuga } y\text{”}.$$

Siis näiteks $S(2,6,24) = 1$ ja $S(2,6,7) = 0$.

1.3.2 Kvantorid

Lisaks lausearvutuse tehetele on predikaatide puhul olemas veel kaks spetsiifilist operatsiooni, mida kutsutakse kvantoriteks.

Definitsioon 1.50 Olgu $P(x_1,\ldots,x_i,\ldots,x_n)$ hulgal M määratud n-kohaline predikaat, kus $n \geqslant 1$, ning olgu $i \in \{1,\ldots,n\}$.

1. Kirjutis
$$\forall x_i\, P(x_1,\ldots,x_i,\ldots,x_n)$$
tähistab $(n-1)$-kohalist predikaati, mis on tõene parajasti siis, kui argumentide $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$ väärtused on sellised, et hulga M iga elemendi m korral on $P(x_1,\ldots,m,\ldots,x_n)$ tõene. Operaatorit $\forall$ nimetatakse **üldisuskvantoriks** ehk **universaalsuskvantoriks**.

2. Kirjutis
$$\exists x_i\, P(x_1,\ldots,x_i,\ldots,x_n)$$
tähistab $(n-1)$-kohalist predikaati, mis on tõene parajasti siis, kui argumentide $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$ väärtused on sellised, et hulgas M leidub element m, mille korral on $P(x_1,\ldots,m,\ldots,x_n)$ tõene. Operaatorit $\exists$ nimetatakse **olemasolukvantoriks** ehk **eksistentsikvantoriks**.

Kvantori rakendamisel tekkinud predikaat ei sõltu enam muutujast, mis kvantoriga seoti. Öeldakse, et selline muutuja on **seotud**. Saadud predikaadi argumentideks olevaid muutujaid nimetatakse **vabadeks**. Predikaadile kvantori rakendamist nimetatakse **kvantifitseerimiseks**.

Märkus 1.51 Põhimõtteliselt $\forall x_i$ ja $\exists x_i$ on kujutused n-kohaliste predikaatide hulgast $(n-1)$-kohaliste predikaatide hulka. Kui kvantorit rakendatakse ühekohalisele predikaadile, siis tulemuseks on lause, mis ei sõltu ühestki muutujast ning millel on kas tõeväärtus 1 või 0.

Näide 1.52 Vaatleme predikaati $Q(x,y)$ näitest 1.46. Siis kirjutis

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

väljendab ühekohalist predikaati $Q'(x)$, mida sõnades väljendab lause "maailmajaol x on maismaaühendus kõigi maailmajagudega". Avaldises $\forall y\, Q(x,y)$ on y seotud muutuja ja x vaba muutuja. Kirjutis

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

väljendab aga ühekohalist predikaati $Q''(x)$, mida sõnades väljendab lause "maailmajaol x on maismaaühendus mingi maailmajaoga."

Näide 1.53 Vaatleme hulgal $\mathbb{N}$ ühekohalist predikaati $P(x) =$ "x on algarv". Siis $\forall x P(x)$ on lause, mis väidab, et iga naturaalarv on algarv, ja $\exists x\, P(x)$ on lause, mis väidab, et leidub naturaalarv, mis on algarv. Neist esimene lause on väär ja teine tõene.

Näide 1.54 Vaatleme hulgal $\mathbb{N}$ kolmekohalist predikaati

$$P(x,y,z) = \text{“}x+y=z\text{”}.$$

Sellele predikaadile võime järjest rakendada mitut kvantorit saades näiteks
$\forall y \forall z \exists x\, P(x,y,z)$. Siis

$$\forall y \forall z \exists x\, P(x,y,z) = \forall y \forall z \text{ “}y \le z\text{”} = \forall y \text{ “y=0”}$$

on lause, mis ei sõltu ühestki argumendist. See lause on väär, sest mitte kõik naturaalarvud ei võrdu nulliga.

1.3.3 Predikaatarvutuse süntaks

Anname nüüd reeglid predikaatarvutuse valemite koostamiseks. Kuna predikaatarvutuse väljendusvõimalused on lausearvutuse omadest suuremad, siis on ka predikaatarvutuse valemite struktuur keerulisem.

Predikaatarvutuses kasutatakse avaldiste üleskirjutamisel järgmisi sümboleid.

- **Indiviidmuutujad**, mida märgime harilikult tähtedega u, v, w, x, y, z. Iga indiviidmuutuja võib tähistada vaadeldava hulga ükskõik millist elementi (indiviidi).

- **Konstantsümbolid** a, b, c, d jne. Konstantsümbol tähistab vaadeldava hulga mingit fikseeritud elementi.

- **Funktsionaalsümbolid** f, g, h jne. Need tähistavad vaadeldaval hulgal defineeritud funktsioone.

- **Predikaatsümbolid** P, Q, R jne.
- **Loogikasümbolid** $\neg, \&, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists$.
- **Kirjavahemärgid** (,) ja koma.

Kõigile sümbolitele võib vajaduse korral lisada indekseid. Funktsionaalsümboli ja predikaatsümboli argumentide arv peab selguma kontekstist.

Definitsioon 1.55 Signatuuriks nimetatakse järjestatud kolmikut $\sigma = \langle \mathbf{C};\ \mathbf{F};\ \mathbf{P} \rangle$, kus

- $\mathbf{C}$ on konstantsümbolite hulk,
- $\mathbf{F}$ on funktsionaalsümbolite hulk,
- $\mathbf{P}$ on predikaatsümbolite mittetühi hulk.

Märkus 1.56 Alati eeldatakse, et predikaatsümbolite hulk on mittetühi, sest vastasel korral ei saa selles signatuuris kirja panna ühtegi valemit. Hulgad $\mathbf{C}$ ja $\mathbf{F}$ võivad olla tühjad. Kõik kolm hulka võivad olla lõpmatud.

Näide 1.57 Naturaalarvude aritmeetikat saab kirja panna signatuurides

$$\langle 0;\ {}',+,\cdot;\ = \rangle,$$
$$\langle 0,1;\ +,\cdot;\ = \rangle,$$
$$\langle 0,1,2,3,\ldots;\ +,\cdot;\ = \rangle.$$

(Märgime, et harilikult jäetakse kirjapanekust $\langle \{0\};\ \{{}',+,\cdot\};\ \{=\} \rangle$ loogelised sulud ära.)

Näide 1.58 Rühmateooria jaoks võib kasutada signatuure

$$\langle e;\ \cdot;\ = \rangle,$$
$$\langle e;\ \cdot, {}^{-1};\ = \rangle.$$

Avaldiste kirjapanemiseks ei pea teadma sümbolite täpset tähendust, küll aga peavad olema fikseeritud reeglid, mille abil sümbolitest avaldisi koostatakse.

Definitsioon 1.59 Termid signatuuris σ on parajasti need avaldised, mida saab koostada järgmiste reeglite abil.

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

Termi, milles ei ole ühtegi indiviidmuutujat, nimetatakse **muutujateta termiks**. Selline term on moodustatud ainult konstantsümbolitest ja funktsionaalsümbolitest.

Näide 1.60 Vaatleme indiviidmuutujat x ja signatuuri $\langle c;\ f, g;\ =\rangle$, kus f on kolmekohaline funktsionaalsümbol ja g on kahekohaline funktsionaalsümbol. Siis võib vaadelda näiteks terme

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

Neist kaks esimest on muutujateta termid.

Näide 1.61 Vaatleme indiviidmuutujaid x, y ja signatuuri $\langle \mathbb{R};\ +, \cdot;\ =\rangle$, kus $+$ ja $\cdot$ on kahekohalised funktsionaalsümbolid. Harilikult kirjutatakse kahekohaline funktsionaalsümbol argumentide vahele, mitte nende ette. Seega näiteks $+(x, y)$ asemel kirjutatakse $x + y$. Selles signatuuris võib vaadelda näiteks järgmisi terme:

$$46 \qquad 3 \cdot y \qquad ((2 \cdot x) + 1) \cdot (y + (4 \cdot x)).$$

Näide 1.62 Kolmemõõtmelise ruumi vabavektoritest rääkides võib kasutada signatuuri $\langle \vec{i}, \vec{j}, \vec{k}, \vec{0};\ +, -, \times;\ =\rangle$ ja indiviidmuutujaid $\vec{x}, \vec{y}, \vec{z}$. Termideks on näiteks

$$\vec{j} \qquad \vec{z} \qquad (\vec{x} + \vec{y}) - \vec{z} \qquad ((\vec{x} \times \vec{i}) + (\vec{y} \times \vec{j})) + (\vec{z} \times \vec{k}).$$

Predikaatarvutuse valemid moodustatakse predikaatsümbolitest, termidest, lausearvutuse tehetest ja kvantoritest.

Definitsioon 1.63 Predikaatarvutuse valemid on parajasti need avaldised, mis on moodustatud järgmiste reeglite abil.

1. Kui P on n-kohaline predikaatsümbol ja $t_1, \ldots, t_n$ on termid, siis $P(t_1, \ldots, t_n)$ on predikaatarvutuse valem.

2. Kui $\mathcal{F}$ on predikaatarvutuse valem, siis $\neg\mathcal{F}$ on predikaatarvutuse valem.

3. Kui $\mathcal{F}$ ja $\mathcal{G}$ on predikaatarvutuse valemid, siis $(\mathcal{F} \& \mathcal{G}), (\mathcal{F} \vee \mathcal{G}), (\mathcal{F} \Rightarrow \mathcal{G}), (\mathcal{F} \Leftrightarrow \mathcal{G})$ on predikaatarvutuse valemid.

4. Kui x on indiviidmuutuja ja $\mathcal{F}$ on predikaatarvutuse valem, siis $\forall x\, \mathcal{F}$ ja $\exists x\, \mathcal{F}$ on predikaatarvutuse valemid.

Esimese punkti põhjal moodustatud valemeid nimetatakse **atomaarseteks valemiteks** ehk **elementaarvalemiteks**. Kõiki antud valemi konstrueerimise käigus tekkinud valemeid nimetatakse antud valemi **osavalemiteks**. Viimasel konstrueerimissammul kasutatud lausearvutuse tehet või kvantori rakendamist nimetatakse valemi **peatehteks**.

Predikaatarvutuse valemite kirjutamisel kasutame sulgude panekul samasuguseid kokkuleppeid nagu lausearvutuse korralgi. Kvantorite prioriteet loetakse võrdseks eituse omaga.

Näide 1.64 Vaatleme indiviidmuutujaid x, y, z ja signatuuri $\langle \mathbb{R};\ +, \cdot;\ =, <, >\rangle$, kus kõik funktsionaal- ja predikaatsümbolid on kahekohalised. Ka kahekohalisi predikaatsümboleid on tavaks kirjutada argumentide vahele (seega $<(x,y)$ asemel $x<y$). Võime vaadelda atomaarseid valemeid

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

ja mitteatomaarseid valemeid

$$x = 0 \vee x = 1 \qquad \forall x \exists y\,(x+y > x) \qquad \neg(x=0) \Rightarrow \exists y\,(x \cdot y = 1).$$

Kui välja jätta indiviidmuutuja esinemised kvantori taga, siis tema ülejäänud esinemised valemis jagunevad seotuteks ja vabadeks. Indiviidmuutuja esineb valemis **seotult**, kui ta asub mingi kvantori mõjupiirkonnas. Ülejäänud esinemisi nimetatakse **vabadeks**. Seega kui x esineb valemis $\mathcal{G}$, siis valemites $\forall x\,\mathcal{G}$ ja $\exists x\,\mathcal{G}$ on tema esinemised seotud. Predikaatarvutuse valemit nimetatakse **kinniseks**, kui tema kõigi indiviidmuutujate kõik esinemised on seotud. Kui tahetakse juhtida tähelepanu sellel, et indiviidmuutuja x esineb valemis $\mathcal{F}$ vabalt, siis kirjutatakse vahel $\mathcal{F}(x)$.

Üks ja sama indiviidmuutuja võib valemis esineda nii vabalt kui seotult.

Näide 1.65 Predikaatarvutuse valemis

$$\exists x\,(P(x) \Rightarrow \neg Q(y)) \vee R(x)$$

on kvantori $\exists$ mõjupiirkonnaks osavalem $(P(x) \Rightarrow \neg Q(y))$. Selles osavalemis on muutuja x seotud, aga muutuja y vaba. Osavalemis $R(x)$ esineb muutuja x aga vabalt, sest ta ei asu ühegi kvantori mõjupiirkonnas. Kuna valemis leidub vabu muutujaid, siis see valem ei ole kinnine.

Märkus 1.66 Selles kursuses oleme defineerinud predikaatarvutuse valemi süntaksi rangelt ja sellest definitsioonist me kõrvale ei kaldu. Kui aga loogikasümboleid kasutatakse mõnedes konkreetsetes matemaatilistes tekstides, siis tihti suhtutakse kvantorite kirjutamisse pisut vabamalt. Allpool toome mõned näited selle kohta, kuidas mujal võidakse kvantoreid kirjutada ja kuidas sama sisuga väidet saaks kirja panna selle kursuse tähistustes.

mujal	selles kursuses
$\exists x \forall y > x : \mathcal{G}(x,y)$	$\exists x \forall y\,((y > x) \Rightarrow \mathcal{G}(x,y))$
$\forall x \exists y < x : \mathcal{G}(x,y)$	$\forall x \exists y((y < x) \& \mathcal{G}(x,y))$
$\forall x, y \exists z, w : \mathcal{G}(x,y,z,w)$	$\forall x \forall y \exists z \exists w\, \mathcal{G}(x,y,z,w)$

.

1.3.4 Signatuuri interpretatsioonid

Sümbolite arv, mida matemaatikas kasutatakse on suhteliselt piiratud. Selle tõttu tarvitatakse tihti ühte ja sama sümbolit mitmes erinevas tähenduses. Näiteks tehtemärk $+$ võib märkida reaalarvude liitmist, jäägiklasside liitmist, maatriksite liitmist või hoopis funktsioonide liitmist. Need kõik on erinevad tehted, mis on defineeritud erinevatel hulkadel. Millist märgi $+$ tähendust konkreetses olukorras silmas peetakse, peab selguma kontekstist.

Signatuur koosneb sümbolitest, mida me valemite kirja panemiseks soovime kasutada. Nendele sümbolitele võib aga vastavalt vajadusele anda erineva tõlgenduse, s.t. me võime neid erinevalt interpreteerida.

Definitsioon 1.67 Signatuuri $\sigma = \langle \mathbf{C};\ \mathbf{F};\ \mathbf{P}\rangle$ **interpretatsioon** on järjestatud paar $\alpha = \langle M_\alpha;\ I_\alpha\rangle$, kus M_α on mingi mittetühi hulk, mida nimetatakse **põhihulgaks** ehk **interpretatsiooni kandjaks**, ja I_α on **interpreteeriv kujutus**, mis teisendab

1. iga konstantsümboli $c \in \mathbf{C}$ hulga M_α mingiks elemendiks c_α;
2. iga n-kohalise funktsionaalsümboli $f \in \mathbf{F}$ mingiks n-kohaliseks funktsiooniks $f^\alpha : M_\alpha^n \to M_\alpha$;
3. iga n-kohalise predikaatsümboli P mingiks n-kohaliseks predikaadiks $P^\alpha : M_\alpha^n \to \{1, 0\}$.

Märkus 1.68 1. Kui interpretatsioon on fikseeritud ja ei ole karta segaduse tekkimist, siis võib interpretatsiooni tähise ära jätta.

2. On oluline teha vahet sümbolil ja tema interpretatsioonil. Erinevates interpretatsioonides võib üks ja sama sümbol tähendada väga erinevaid asju.

3. Võrdusmärki interpreteeritakse alati võrduspredikaadina.

Näide 1.69 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \ldots;\ +, \cdot;\ =, <\rangle$. Anname sellele kolm erinevat interpretatsiooni.

1. $M = \mathbb{N}$ ja signatuuri sümboleid interpreteerime standardselt.
2. $M = \mathbb{R}$ ja signatuuri sümboleid interpreteerime standardselt.
3. $M = \{0, 1\}$,
$$c_\alpha = \begin{cases} 0, & \text{kui } c \text{ on paarisarv,} \\ 1, & \text{kui } c \text{ on paaritu arv,} \end{cases}$$
$+$ ja $\cdot$ on kahekohalised tehted hulgal $\{0, 1\}$, mis on antud tabelitega
$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad\qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array},$$
ning $<$ on kahekohaline predikaat hulgal $\{0, 1\}$, mille tõesuspiirkond on $\{(0, 1)\}$ (s.t. $0 < 1$ ja ülejäänud paarid ei ole selles seoses).

Näide 1.70 Vaatleme signatuuri $\langle e;\ *;\ =\rangle$, kus $*$ on kahekohaline funktsionaalsümbol. Interpreteerime seda signatuuri järgmistel viisidel.

1. $M = \mathbb{R}^+$ (positiivsete reaalarvude hulk), $e^\alpha = 1$ ja $*^\alpha = \cdot$.
2. $M = Mat_2(\mathbb{R})$ (teist järku reaalarvuliste elementidega ruutmaatriksite hulk), e^α on teist järku ühikmaatriks ja $*^\alpha$ on maatriksite korrutamistehe.
3. $M = \mathbb{R}^\mathbb{R}$ (hulga $\mathbb{R}$ kõigi teisenduste hulk), $e^\alpha = 1_\mathbb{R}$ ja $*^\alpha = \circ$ (teisenduste järjestrakendamine).
4. $M = \mathbb{Z}$, $e^\alpha = 0$, $*^\alpha = +$.
5. M on mingi mittetühja hulga A kõigi alamhulkade hulk $\mathcal{P}(A)$, $e^\alpha = A$, $*^\alpha = \cap$.

Definitsioon 1.71 Termi t **väärtus** t^α interpretatsioonis α indiviidmuutujate fikseeritud väärtustel leitakse järgmiste reeglite abil.

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

Tänu sellele definitsioonile tekitab iga n muutujat sisaldav term ühe n-muutuja funktsiooni hulgal M_α.

Näide 1.72 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \ldots;\ +, \cdot;\ =, <\rangle$. Olgu interpretatsiooni kandja $M = \mathbb{N}$ ja interpretatsioon standardne. Siis võib vaadelda näiteks järgmisi terme:

term	x	2	$x+2$	$x \cdot x + 2 \cdot y$
vabade muutujate väärtused	$x = 3$	puuduvad	$x = 3$	$x = 3$, $y = 1$
termi väärtus	3	2	5	11

.

Näiteks term $x \cdot x + 2 \cdot y$ tekitab kahe muutuja funktsiooni

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N},\quad (k, l) \mapsto k^2 + 2l.$$

Ka predikaatarvutuse valemi tõeväärtus sõltub sellest, millisesse hulka kuuluvad temas sisalduvate muutujate väärtused ja kuidas me tõlgendame temas esinevaid sümboleid. Näiteks valem $\forall x\,(x \geqslant 0)$ on naturaalarvude korral tõene, kuid reaalarvude korral väär. Valemi tõeväärtuse etteantud interpretatsioonis ja vabade muutujate väärtuste korral saab leida järgmise definitsiooni abil.

Definitsioon 1.73 Predikaatarvutuse valemi $\mathcal{F}$ **tõeväärtus** $\mathcal{F}^\alpha$ interpretatsioonis α vabade muutujate fikseeritud väärtustusel leitakse järgmiste reeglite abil.

1. Kui $\mathcal{F} = P(t_1, \ldots, t_n)$, kus P on n-kohaline predikaatsümbol ja $t_1, \ldots, t_n$ on termid, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $P^\alpha(t_1^\alpha, \ldots, t_n^\alpha) = 1$.

2. Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 0$.
3. Kui $\mathcal{F} = \mathcal{G}\&\mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ ja $\mathcal{H}^\alpha = 1$.
4. Kui $\mathcal{F} = \mathcal{G} \vee \mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ või $\mathcal{H}^\alpha = 1$.
5. Kui $\mathcal{F} = \mathcal{G} \Rightarrow \mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 0$ või $\mathcal{H}^\alpha = 1$.
6. Kui $\mathcal{F} = \mathcal{G} \Leftrightarrow \mathcal{H}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $\mathcal{G}^\alpha = 1$ ja $\mathcal{H}^\alpha = 1$ või $\mathcal{G}^\alpha = 0$ ja $\mathcal{H}^\alpha = 0$.
7. Kui $\mathcal{F} = \forall x\, \mathcal{G}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui põhihulga M_α iga elemendi m korral $\mathcal{G}^\alpha_{[x/m]} = 1$, kus $[x/m]$ tähendab, et muutuja x väärtuseks loetakse element m.
8. Kui $\mathcal{F} = \exists x\, \mathcal{G}$, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui põhihulgas M_α leidub selline element m, mille korral $\mathcal{G}^\alpha_{[x/m]} = 1$, kus $[x/m]$ tähendab, et muutuja x väärtuseks loetakse element m.

Märkus 1.74 Kui $\mathcal{F}(x_1, \ldots, x_n)$ on predikaatarvutuse valem vabade muutujatega $x_1, \ldots, x_n$, siis tema tõeväärtust interpretatsioonis α vabade muutujate väärtustusel $(m_1, \ldots, m_n)$ võib tähistada $\mathcal{F}^\alpha(m_1, \ldots, m_n)$. Nii tekib meil kujutus

$$M_\alpha^n \to \{1, 0\}, \quad (m_1, \ldots, m_n) \mapsto \mathcal{F}^\alpha(m_1, \ldots, m_n).$$

Niisiis valemi iga interpretatsioon tekitab ühe predikaadi.

Näide 1.75 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \ldots;\ +, \cdot;\ =, < \rangle$. Olgu interpretatsiooni kandja $M = \mathbb{N}$ ja interpretatsioon standardne. Olgu meil valem

$$\mathcal{F}(y) = \exists x\, (2 \cdot x = y).$$

Milline on selle valemi tõeväärtus näiteks $y = 6$ korral? Kuna leidub selline $x \in \mathbb{N}$, et $2 \cdot x = 6$ (selleks x-ks on arv 3), siis $\mathcal{F}$ on tõene $y = 6$ korral. Viimast asjaolu võib kirja panna kujul $\mathcal{F}(6) = 1$. On lihtne aru saada, et

$$\mathcal{F}(k) = 1 \quad \text{parajasti siis, kui} \quad k \text{ on paarisarv.}$$

Ülesanne 1.76 Leida järgmiste valemite tõeväärtused kolmes interpretatsioonis, mida vaatlesime näites 1.69 (märgime, et siinsetes valemites pole vabu muutujaid):

valem	$\mathbb{N}$	$\mathbb{R}$	$\{1,0\}$
$0 = 2$	0	0	1
$\forall x\,(x < x + 1)$	1	1	0
$\forall x\,\exists y\,(x < y)$			
$\forall x\,\exists y\,(y < x)$			
$\forall x\,\forall y\,(x < y \Rightarrow \exists z\,(x < z\,\&\,z < y))$			
$\forall x\,\forall u\,\forall v\,(x + u = x + v \Rightarrow u = v)$			
$\forall x\,\forall y\,\exists z\,(x + z = y)$			
$\forall x\,\forall y\,\exists z\,(x \cdot z = y)$			
$\forall x\,\forall y\,(\neg(x = 0) \Rightarrow \exists z\,(x \cdot z = y))$			

Ülesanne 1.77 Olgu signatuur $\langle e;\ *;\ =\rangle$. See signatuur lubab muuhulgas näiteks kirja panna järgmisi abstraktse algebra jaoks olulisi valemeid

$$(x * y) * z = x * (y * z),\quad (e * x = x)\,\&\,(x = x * e),\quad \exists y((x * y = e)\,\&\,(y * x = e)).$$

Millised neist valemitest on tõesed näites 1.70 vaadeldud interpretatsioonides vabade muutujate kõigi väärtuste korral?

Definitsioon 1.78 Valemi $\mathcal{F}$ **mudeliks** nimetatakse sellist interpretatsiooni α, milles valem $\mathcal{F}$ on tõene oma vabade muutujate kõikidel väärtustel. Sel juhul öeldakse ka, et valem $\mathcal{F}$ **on tõene mudelis** α.

Definitsioon 1.79 Interpretatsiooni α nimetatakse valemite hulga $\{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ **mudeliks**, kui see interpretatsioon on iga üksiku valemi mudel.

Näide 1.80 Vaatleme signatuuri $\sigma = \langle 1;\ \cdot;\ =\rangle$ interpretatsiooni α, kus $M = \mathbb{N}$ ja sümboleid interpreteeritakse standardselt. Siis valem

$$\mathcal{F}(x, y, z) = ((x \cdot y) \cdot z = x \cdot (y \cdot z))$$

on tõene vabade muutujate x, y, z kõigil väärtustel ning seega antud interpretatsioon α on valemi $\mathcal{F}(x, y, z)$ mudel.

Valem

$$x \cdot x = x$$

aga ei ole tõene muutuja x väärtuse 2 korral ning seega interpretatsioon α ei ole selle valemi mudel.

Lihtne on ka aru saada, et interpretatsioon α on valemite hulga

$$\{(x \cdot y) \cdot z = x \cdot (y \cdot z),\quad x \cdot 1 = x,\quad 1 \cdot x = x\}$$

mudel. Sellise valemite hulga mudeleid kutsutakse algebras **monoidideks**. Väga paljud algebralised struktuurid saab defineerida mingite valemite hulkade mudelitena. Millise valemite hulga mudeliteks on näiteks rühmad või Abeli rühmad?

Näide 1.81 Vaatleme signatuuris $\sigma = \langle\top;\ ;\ =, \leqslant\rangle$ valemite hulka

$$\{x \leqslant x,\ \ (x \leqslant y) \,\&\, (y \leqslant x) \Rightarrow x = y,\ \ (x \leqslant y) \,\&\, (y \leqslant z) \Rightarrow x \leqslant z,\ \ x \leqslant \top\}.$$

Selle valemite hulga mudeliteks on osaliselt järjestatud hulgad, milles leidub suurim element.

Nagu nägime eespool, valemi interpretatsioon tekitab predikaadi. Võib püstitada ka vastupidise küsimuse: kas etteantud predikaadi, signatuuri ja selle interpretatsiooni korral õnnestub kirja panna valem, mille interpretatsioon oleks see predikaat.

Definitsioon 1.82 Olgu $\mathcal{F}(x_1, \ldots, x_n)$ valem signatuuris σ ja olgu $\alpha = \langle M_\alpha, I_\alpha\rangle$ selle signatuuri interpretatsioon. Öeldakse, et valem $\mathcal{F}(x_1, \ldots, x_n)$ **väljendab** predikaati $P : M_\alpha^n \to \{1, 0\}$, kui iga $m_1, \ldots, m_n \in M_\alpha$ korral

$$\mathcal{F}^\alpha(m_1, \ldots, m_n) = 1 \quad \text{parajasti siis, kui} \quad P(m_1, \ldots, m_n) = 1.$$

Lühemalt võib öelda, et valem $\mathcal{F}$ väljendab predikaati P, kui tema poolt tekitatud kujutus, mida mainisime eelnevas märkuses, langeb kokku kujutusega P.

Näide 1.83 Valem $\mathcal{F}(y)$, mida vaatlesime näites 1.75, väljendab naturaalarvude hulgal defineeritud predikaati $P(y) =$ "y on paarisarv".

Näide 1.84 Vaatleme signatuuri $\langle 0, 1;\ +;\ =\rangle$ standardset interpretatsiooni hulgal $\mathbb{N}$.

Predikaati "$x = 3$" saab väljendada valemiga

$$x = (1 + 1) + 1$$

(konstantsümbolit naturaalarvu 3 jaoks meil hetkel signatuuris pole).

Predikaati "$x < y$" saab väljendada valemiga

$$\exists z\, ((x + z = y) \,\&\, \neg(x = y))$$

või hoopis valemiga

$$\exists z\, ((x + z = y) \,\&\, \neg(z = 0)).$$

Predikaati "x on paarisarv" saab väljendada valemiga

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

(ka korrutamistehte jaoks ei ole praegu signatuuris sümbolit).

Näide 1.85 Vaatleme suvalise mittetühja hulga A kõigi alamhulkade hulka $\mathcal{P}(A)$ ja signatuuri $\langle\ ;\ \ ;\ \subseteq\rangle$, kus puuduvad konstantsümbolid ja funktsionaalsümbolid. Interpreteerime sümbolit $\subseteq$ sisalduvusseosena.

Predikaati "X on tühi hulk" väljendab valem $\forall Y\, (X \subseteq Y)$.

Predikaati "Alamhulkade X ja Y ühend on Z" saab väljendada valemiga

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

aga ka valemiga

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

1.3.5 Valemite omadused

Nii nagu lausearvutuseski saab ka predikaatarvutuses rääkida valemi samaselt tõesusest, samaselt väärusest ja kehtestatavusest.

Definitsioon 1.86 Predikaatarvutuse valemit $\mathcal{F}$ nimetatakse

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

Kui valem $\mathcal{F}$ on samaselt tõene, siis kirjutatakse $\models \mathcal{F}$.

Kui võtame mingi samaselt tõese lausearvutuse valemi ja asendame iga lausemuutuja mingi predikaatarvutuse valemiga, siis saame samaselt tõese predikaatarvutuse valemi. Näiteks valem

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

on samaselt tõene. Sarnasel viisil saab samaselt vääratest lausearvutuse valemitest tuletada samaselt vääraid predikaatarvutuse valemeid. Kuid on ka selliseid samaselt tõeseid või vääraid predikaatarvutuse valemeid, millel puudub analoog lausearvutuses.

Näide 1.87 Veendume, et signatuuris $\sigma = \langle\ ;\ \ ;\ P\rangle$ antud valem

$$\mathcal{F} = \forall x\, P(x) \vee \exists x\, \neg P(x)$$

on samaselt tõene.

Olgu meil fikseeritud signatuuri σ suvaline interpretatsioon $\alpha = \langle M_\alpha;\ I_\alpha\rangle$. Kuna valemis $\mathcal{F}$ pole vabu muutujaid, siis neile me väärtusi andma ei pea. On kaks võimalust.

1) $\forall x\, P(x) = 1$. Siis ka $\mathcal{F}^\alpha = 1$.

2) $\forall x\, P(x) = 0$. Seega ei kehti väide, et iga $m \in M_\alpha$ korral $P(m)$ on tõene. Järelikult leidub vähemalt üks element $m \in M_\alpha$, mille korral $P(m) = 0$ ehk $\neg P(m) = 1$. See tähendab, et $\exists x\, \neg P(x) = 1$, ning seega ka $\mathcal{F}^\alpha = 1$.

Kuna suvalise interpretatsiooni korral on valem $\mathcal{F}$ tõene, siis on ta samaselt tõene.

Definitsioon 1.88 Predikaatarvutuse valemit nimetatakse **kehtestatavaks**, kui ta on tõene vähemalt ühes interpretatsioonis vabade muutujate mingitel väärtustel.

Näide 1.89 Valem

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

on kehtestatav, sest me saame konstrueerida interpretatsiooni, kus see valem on tõene. Valime näiteks interpretatsiooni kandjaks hulga $\mathbb{N}$ ja ühekohalise predikaatsümboli P interpretatsiooniks olgu predikaat "... on käesoleva aasta arv".

Ka valem

$$\mathcal{G}(y) = \forall x\, Q(x, y)$$

on kehtestatav. Olgu põhihulk jälle $\mathbb{N}$ ja predikaatsümbolit Q interpreteerime kui predikaati $Q(x, y) =$ "$x \geqslant y$". Andes vabale muutujale y väärtuse 0 näeme, et $\forall x\, Q(x, 0) = 1$.

Lausearvutuse valemi samaselt tõesuse kontrollimiseks võib välja arvutada tema tõeväärtustabeli, milles on lõplik arv ridu. Et uurida predikaatarvutuse valemi samaselt tõesust, peaksime definitsioonist lähtudes vaatlema signatuuri kõikvõimalikke interpretatsioone. Neid on aga lõpmata palju, sest juba põhihulka M_α võib valida lõpmata paljudel viisidel.

Predikaatarvutuse mittelahenduvuse teoreem (Church[3], 1936). *Ei leidu algoritmi, mis suvalise predikaatarvutuse valemi puhul suudaks kindlaks teha, kas see on samaselt tõene või ei.*

Teoreem 1.90 *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt väär.*

Tõestus. Definitsiooni 1.73 punkti 2 põhjal on iga interpretatsiooni ja vabade muutujate mistahes väärtuste korral valemite $\mathcal{F}$ ja $\neg\mathcal{F}$ tõeväärtused erinevad. Seega kui $\mathcal{F}$ on igas interpretatsioonis ja vabade muutujate kõigil väärtustel tõene, siis $\neg\mathcal{F}$ on igas interpretatsioonis ja vabade muutujate kõigil väärtustel väär ning ka vastupidi. □

Teoreem 1.91 *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eitus $\neg\mathcal{F}$ ei ole samaselt tõene.*

Tõestus. Vaatleme valemit $\mathcal{F}(x_1,\dots,x_n)$ vabade muutujatega $x_1,\dots,x_n$. Kui $\mathcal{F}$ on kehtestatav, siis leidub mingi interpretatsioon α ja elemendid $m_1,\dots,m_n \in M_\alpha$ nii, et $\mathcal{F}^\alpha(m_1,\dots,m_n) = 1$. Siis aga $\neg\mathcal{F}^\alpha(m_1,\dots,m_n) = 0$, mis tähendab seda, et valem $\neg\mathcal{F}(x_1,\dots,x_n)$ ei ole samaselt tõene.

Kui valem $\neg\mathcal{F}(x_1,\dots,x_n)$ ei ole samaselt tõene, siis leidub interpretatsioon α ja elemendid $m_1,\dots,m_n \in M_\alpha$ nii, et $\neg\mathcal{F}^\alpha(m_1,\dots,m_n) = 0$. Siis aga $\mathcal{F}^\alpha(m_1,\dots,m_n) = 1$. See tähendab, et valem $\mathcal{F}(x_1,\dots,x_n)$ on kehtestatav. □

1.3.6 Tõesuspuu predikaatarvutuses

Ka predikaatarvutuse valemite puhul saab valemit tõeseks või vääraks muutva interpretatsiooni leidmiseks kasutada tõesuspuid. Vaatleme selle kohta mõningaid näiteid.

Järgnevas näites on vasakul ääres ridade numbrid ja paremal ääres on näidatud, millisest eelnevast reast on antud rida saadud.

Näide 1.92 Uurime, kas valem

$$\forall x\, P(x) \,\&\, \forall x\, Q(x) \Rightarrow \forall x\, (P(x) \,\&\, Q(x))$$

on samaselt tõene. Selleks proovime uurida, kas on võimalik, et see valem on mingis interpretatsioonis väär. Tekib järgmine tõesuspuu.

[3] Alonzo Church (1903–1995) — ameerika matemaatik

$$
\begin{array}{lccr}
1. & \multicolumn{2}{c}{\forall x\, P(x) \,\&\, \forall x\, Q(x) \Rightarrow \forall x\, (P(x) \,\&\, Q(x)) = 0 \checkmark} & \\
2. & \multicolumn{2}{c}{\forall x\, P(x) \,\&\, \forall x\, Q(x) = 1 \checkmark} & /1/ \\
3. & \multicolumn{2}{c}{\forall x\, (P(x) \,\&\, Q(x)) = 0 \checkmark} & /1/ \\
4. & \multicolumn{2}{c}{\forall x\, P(x) = 1} & /2/ \\
5. & \multicolumn{2}{c}{\forall x\, Q(x) = 1} & /2/ \\
6. & \multicolumn{2}{c}{P(c) \,\&\, Q(c) = 0 \checkmark} & /3/ \\
7. & P(c) = 0 & Q(c) = 0 & /6/ \\
8. & P(c) = 1 & P(c) = 1 & /4/ \\
9. & \times & Q(c) = 1 & /5/ \\
 & & \times &
\end{array}
$$

Selle puu read 2–5 on saadud lausearvutuse tehete definitsioonide põhjal. Rida 6 on saadud reast 3, mis ütleb, et $\forall x\, (P(x) \,\&\, Q(x)) = 0$. Üldisuskvantori definitsioonist saame, et peab leiduma mingi element, tähistame seda sümboliga c, mille korral $P(c) \,\&\, Q(c) = 0$. Rea 7 saamiseks kasutame konjunktsiooni definitsiooni. Rea 8 saamiseks kasutame seda, et rea 4 tõttu peab iga x korral $P(x)$ olema tõene, muuhulgas siis ka $P(c) = 1$.

Nagu näeme, on puu mõlemad harud vastuolulised, seega ei leidu interpretatsiooni, milles esialgne valem oleks väär. Järelikult on see valem samaselt tõene.

Näide 1.93 Uurime, kas valem

$$\exists x\, P(x) \,\&\, \exists x\, Q(x) \Rightarrow \exists x\, (P(x) \,\&\, Q(x))$$

on samaselt tõene. Tekib järgmine tõesuspuu.

$$
\begin{array}{lcccr}
1. & \multicolumn{3}{c}{\exists x\, P(x) \,\&\, \exists x\, Q(x) \Rightarrow \exists x\, (P(x) \,\&\, Q(x)) = 0 \checkmark} & \\
2. & \multicolumn{3}{c}{\exists x\, P(x) \,\&\, \exists x\, Q(x) = 1 \checkmark} & /1/ \\
3. & \multicolumn{3}{c}{\exists x\, (P(x) \,\&\, Q(x)) = 0} & /1/ \\
4. & \multicolumn{3}{c}{\exists x\, P(x) = 1 \checkmark} & /2/ \\
5. & \multicolumn{3}{c}{\exists x\, Q(x) = 1 \checkmark} & /2/ \\
6. & \multicolumn{3}{c}{P(d) = 1} & /4/ \\
7. & \multicolumn{3}{c}{Q(e) = 1} & /5/ \\
8. & \multicolumn{3}{c}{P(d) \,\&\, Q(d) = 0 \checkmark} & /3/ \\
9. & \multicolumn{3}{c}{P(e) \,\&\, Q(e) = 0 \checkmark} & /3/ \\
10. & P(d) = 0 & \multicolumn{2}{c}{Q(d) = 0} & /8/ \\
 & \times & & & \\
11. & & P(e) = 0 & Q(e) = 0 & /9/ \\
 & & & \times &
\end{array}
$$

Selles puus on kaks haru vastuolulised, kuid kolmas mitte. Selle kolmanda haru põhjal võime konstrueerida interpretatsiooni, kus põhihulk on $M = \{d, e\}$ ja ühekohalised predikaadid P ja Q on defineeritud võrdustega

$$P(d) = 1,\ P(e) = 0,\ Q(d) = 0,\ Q(e) = 1.$$

Selles interpretatsioonis

$$\exists x\, P(x) \,\&\, \exists x\, Q(x) = 1, \quad \text{kuid} \quad \exists x\, (P(x) \,\&\, Q(x)) = 0.$$

Seega esialgne valem ei ole samaselt tõene.

Märgime veel, et selles puus me ei märkinud rida 3 läbivaadatuks. Me küll kasutasime seda ridade 8 ja 9 saamiseks, aga sellega ei ole me veel kogu infot, mis reas 3 sisaldub, ära kasutanud.

Näide 1.94 Teha kindlaks, kas valem

$$\forall x\, P(x) \Rightarrow \exists x\, P(x)$$

on samaselt tõene.

Alustame tõesuspuu konstrueerimist:

$$\begin{array}{lcl}
1. & \forall x\, P(x) \Rightarrow \exists x\, P(x) = 0 \checkmark & \\
2. & \forall x\, P(x) = 1 & /1/ \\
3. & \exists x\, P(x) = 0 & /1/
\end{array}$$

Oleme olukorras, kus oleks vaja kasutada kas rida 2 või rida 3, aga me ei ole veel ühtegi tähist hulga M elemendi jaoks sisse toonud. Selles olukorras võime siiski kasutusele võtta tähise mingi elemendi jaoks (n.ö. esimese elemendi jaoks), sest definitsiooni kohaselt peab interpretatsiooni kandja M olema mittetühi hulk. Võtame selleks tähiseks näiteks c. Siis saame

$$\begin{array}{lcl}
1. & \forall x\, P(x) \Rightarrow \exists x\, P(x) = 0 \checkmark & \\
2. & \forall x\, P(x) = 1 & /1/ \\
3. & \exists x\, P(x) = 0 & /1/ \\
4. & P(c) = 1 & /2/ \\
5. & P(c) = 0 & /3/ \\
 & \times &
\end{array}$$

Näeme, et valem on samaselt tõene.

Tõesuspuu abil saame oma ülesande lahendada küll paljudel juhtudel, kuid mitte alati.

Näide 1.95 Teha kindlaks, kas valem $\forall x \exists y\, P(x, y)$ on kehtestatav.

Konstrueerime tõesuspuu:

$$\begin{array}{lcl}
1. & \forall x \exists y\, P(x, y) = 1 & \\
2. & \exists y\, P(a, y) = 1 & /1/ \\
3. & P(a, b) = 1 & /2/ \\
4. & \exists y\, P(b, y) = 1 & /1/ \\
5. & P(b, c) = 1 & /4/ \\
6. & \vdots &
\end{array}$$

Olemasolukvantorit lahti kirjutades tuleb iga kord sisse tuua uus sümbol, rida 1 annab siis aga uue olemasolukvantorit sisaldava valemi. Seega tõesuspuu ei saa kunagi valmis ja me ei saa selle põhjal teha järeldusi valemi kohta.

Siiski saab ka ilma tõesuspuuta näha, et see valem on kehtestatav. Võib näiteks P osas vaadelda suvalisel mittetühjal hulgal võrduspredikaati.

Lõpuks sõnastame ka tõesuspuu analüüsimise reeglid, mida vaadeldud näidetes juba kasutasime.

$$\begin{array}{cccc} \forall x\, \mathcal{F}(x) = 1 & \forall x\, \mathcal{F}(x) = 0 & \exists x\, \mathcal{F}(x) = 1 & \exists x\, \mathcal{F}(x) = 0 \\ | & | & | & | \\ \mathcal{F}(t) = 1 & \mathcal{F}(c) = 0 & \mathcal{F}(c) = 1 & \mathcal{F}(t) = 0 \end{array}$$

Siin c on uus konstantsümbol hulga M mingi elemendi tähistamiseks ja t on juba olemasolev (tõesuspuus varem sisse toodud) tähis.

1.3.7 Valemite samaväärsus. Predikaatloogika põhisamaväärsused

Definitsioon 1.96 Predikaatarvutuse valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **samaväärseteks**, kui nende tõeväärtused on võrdsed igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel. Sellisel juhul kirjutatakse $\mathcal{F} \equiv \mathcal{G}$.

On selge, et samaväärsuse seos $\equiv$ on ekvivalentsiseos (s.t. refleksiivne, sümmeetriline ja transitiivne) kõigi predikaatarvutuse valemite hulgal.

Definitsioon 1.97 Öeldakse, et valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$ **järeldub** valem $\mathcal{G}$, kui igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel, kus valemid $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene. Sellisel juhul kirjutatakse $\mathcal{F}_1, \ldots, \mathcal{F}_n \models \mathcal{G}$.

Lause 1.98 *Olgu $\mathcal{F}$ ja $\mathcal{G}$ predikaatarvutuse valemid. Siis*

$$\mathcal{F} \equiv \mathcal{G} \quad \textit{parajasti siis, kui} \quad \mathcal{F} \models \mathcal{G} \textit{ ja } \mathcal{G} \models \mathcal{F}.$$

TÕESTUS. TARVILIKKUS. Eeldame, et $\mathcal{F} \equiv \mathcal{G}$. Kui α on mingi interpretatsioon ja vabadele muutujatele on antud sellised väärtused, et $\mathcal{F}$ on tõene, siis ka $\mathcal{G}$ on tõene, ja vastupidi. Seega $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$.

PIISAVUS. Eeldame, et $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$. Olgu fikseeritud mingi interpretatsioon ja vabade muutujate mingid väärtused. On kaks võimalust.

1) $\mathcal{F} = 1$. Siis ka $\mathcal{G} = 1$, sest $\mathcal{F} \models \mathcal{G}$.

2) $\mathcal{F} = 0$. Siis ei ole võimalik, et $\mathcal{G} = 1$, sest see oleks vastuolus tingimusega $\mathcal{G} \models \mathcal{F}$. Järelikult $\mathcal{G} = 0$.

Kuna valemite $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused on igas interpretatsioonis ja vabade muutujate kõigi väärtuste korral samad, siis $\mathcal{F} \equiv \mathcal{G}$. $\square$

Kui võtame mingi lausearvutuse valemite samaväärsuse ja asendame selles lausemuutujad predikaatarvutuse valemitega, siis saame predikaatarvutuse samaväärsuse. Näiteks kehtivad samaväärsused

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

sõltumata sellest, kas $\mathcal{F}$ ja $\mathcal{G}$ on lausearvutuse või predikaatarvutuse valemid. Siiski on predikaatarvutuses ka selliseid samaväärsusi, mida ei saa tõestada puhtalt lausearvutuse vahenditega. Üheks selliseks on näiteks

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

Selliste samaväärsuste kirjapanekul loeme, et $\mathcal{F}$ on predikaatarvutuse valem, mis sisaldab vaba muutujat x, kuid põhimõtteliselt võib sisaldada ka veel mingeid teisi vabu muutujaid, mida me eraldi kirja panema ei hakka. Näiteks kui

$$\mathcal{F} = P(x)\&Q(y) \Rightarrow R(x,y,z),$$

siis võime öelda, et kehtib samaväärsus

$$\neg\forall x(P(x)\&Q(y) \Rightarrow R(x,y,z)) \equiv \exists x\neg(P(x)\&Q(y) \Rightarrow R(x,y,z)),$$

kus viimased kaks valemit sisaldavad vabu muutujaid y ja z.

Teoreem 1.99 *Predikaatloogikas kehtivad järgmised põhisamaväärsused.*

PS1. *Kvantori ja eituse vahetamisseadus:*

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

PS2. *Kvantorite distributiivsus:*

$$\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x)) \equiv \forall x\, \mathcal{F}(x) \,\&\, \forall x\, \mathcal{G}(x),$$

$$\exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) \equiv \exists x\, \mathcal{F}(x) \;\vee\; \exists x\, \mathcal{G}(x),$$

PS3. *Kui indiviidmuutuja x ei esine valemis $\mathcal{G}$ vabalt, siis*

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

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

PS4. *Kui indiviidmuutuja x ei esine valemis $\mathcal{G}$ vabalt, siis*

$$\forall x\, (\mathcal{F}(x) \Rightarrow \mathcal{G}) \equiv \exists x\, \mathcal{F}(x) \Rightarrow \mathcal{G}, \qquad \exists x\, (\mathcal{F}(x) \Rightarrow \mathcal{G}) \equiv \forall x\, \mathcal{F}(x) \Rightarrow \mathcal{G}.$$

Kui indiviidmuutuja x ei esine valemis $\mathcal{F}$ vabalt, siis

$$\forall x\, (\mathcal{F} \Rightarrow \mathcal{G}(x)) \equiv \mathcal{F} \Rightarrow \forall x\, \mathcal{G}(x), \qquad \exists x\, (\mathcal{F} \Rightarrow \mathcal{G}(x)) \equiv \mathcal{F} \Rightarrow \exists x\, \mathcal{G}(x).$$

PS5. *Seotud muutujate ümbernimetamine:*

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

kus y ei esine valemis $\mathcal{F}(x)$.

PS6. *Samaliigiliste kvantorite kommutatiivsus:*

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

TÕESTUS. Tõestame osa neist samaväärsusest. Selleks kasutame lauset 1.98.

PS1a. Näitame, et $\neg\forall x\, \mathcal{F}(x) \models \exists x\, \neg\mathcal{F}(x)$. Olgu meil fikseeritud mingi interpretatsioon $\alpha = \langle M_\alpha, I_\alpha \rangle$ ja vabade muutujate väärtused. Eeldame, et $\neg\forall x\, \mathcal{F}(x) = 1$. Siis $\forall x \mathcal{F}(x) = 0$. Järelikult ei ole nii, et iga elemendi $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$ (s.t. et kui anname muutujale x väärtuse m, siis valem $\mathcal{F}$ on tõene). See tähendab, et leidub mingi $m_0 \in M_\alpha$ nii, et $\mathcal{F}(m_0) = 0$. Siis aga $\neg\mathcal{F}(m_0) = 1$. Predikaatarvutuse valemi tõeväärtuse definitsiooni põhjal (vt. definitsiooni 1.73 punkti 8) $\exists x \neg\mathcal{F}(x) = 1$.

Näitame, et $\exists x\, \neg\mathcal{F}(x) \models \neg\forall x\, \mathcal{F}(x)$. Selleks eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral on $\exists x\, \neg\mathcal{F}(x) = 1$. Siis peab leiduma mingi element $m_0 \in M_\alpha$ nii, et $\neg\mathcal{F}(m_0) = 1$. Järelikult $F(m_0) = 0$. Siis aga ei ole nii, et iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$, s.t. $\forall x\, \mathcal{F}(x) = 0$ ehk $\neg\forall x\, \mathcal{F}(x) = 1$.

Kuna $\neg\forall x\, \mathcal{F}(x) \models \exists x\, \neg\mathcal{F}(x)$ ja $\exists x\, \neg\mathcal{F}(x) \models \neg\forall x\, \mathcal{F}(x)$, siis valemid $\neg\forall x\, \mathcal{F}(x)$ ja $\exists x\, \neg\mathcal{F}(x)$ on samaväärsed.

PS1b. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\neg\exists x\, \mathcal{F}(x) = 1$ ehk $\exists x\, \mathcal{F}(x) = 0$. Siis hulgas M_α ei ole sellist elementi m, mille korral $\mathcal{F}(m) = 1$. Järelikult iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 0$ ehk $\neg\mathcal{F}(m) = 1$. Valemi tõeväärtuse definitsiooni põhjal (vt. definitsiooni 1.73 punkti 7) $\forall x\, \neg\mathcal{F}(x) = 1$. Sellega oleme tõestanud, et $\neg\exists x\, \mathcal{F}(x) \models \forall x\, \neg\mathcal{F}(x)$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\forall x\, \neg\mathcal{F}(x) = 1$. Siis iga $m \in M_\alpha$ korral $\neg\mathcal{F}(m) = 1$ ehk $\mathcal{F}(m) = 0$. Järelikult ei leidu sellist hulga M_α elementi m, mille korral $\mathcal{F}(m) = 1$. Valemi tõeväärtuse definitsiooni põhjal $\exists x \mathcal{F}(x) = 0$ ehk $\neg\exists x \mathcal{F}(x) = 1$. Sellega oleme tõestanud, et $\forall x \neg\mathcal{F}(x) \models \neg\exists x \mathcal{F}(x)$.

PS2a. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x)) = 1$. Siis hulga M_α iga elemendi m korral $\mathcal{F}(m) \,\&\, \mathcal{G}(m) = 1$, kust konjunktsiooni definitsiooni abil saame, et $\mathcal{F}(m) = 1$ ja $\mathcal{G}(m) = 1$. Vastavalt valemi tõeväärtuse definitsioonile tähendab see, et $\forall x\, \mathcal{F}(x) = 1$ ja samuti $\forall x\, \mathcal{G}(x) = 1$. Definitsiooni 1.73 punkt 3 annab meile, et siis ka $\forall x\, \mathcal{F}(x) \,\&\, \forall x\, \mathcal{G}(x) = 1$. Sellega oleme tõestanud, et $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x)) \models \forall x\, \mathcal{F}(x) \,\&\, \forall x\, \mathcal{G}(x)$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\forall x\, \mathcal{F}(x) \,\&\, \forall x\, \mathcal{G}(x) = 1$. Siis $\forall x\, \mathcal{F}(x) = 1$ ja $\forall x\, \mathcal{G}(x) = 1$. Olgu nüüd $m \in M_\alpha$ suvaline element. Siis valemi tõeväärtuse definitsioonist järeldub, et $\mathcal{F}(m) = 1$ ja $\mathcal{G}(m) = 1$, seega ka $\mathcal{F}(m) \,\&\, \mathcal{G}(m) = 1$. Kuna viimane võrdus kehtib iga $m \in M_\alpha$ korral, siis $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x)) = 1$. Sellega oleme tõestanud, et $\forall x\, \mathcal{F}(x) \,\&\, \forall x\, \mathcal{G}(x) \models \forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x))$.

PS2b. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$. Siis leidub selline $m_0 \in M_\alpha$, et $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$. Disjunktsiooni definitsiooni tõttu $\mathcal{F}(m_0) = 1$ või $\mathcal{G}(m_0) = 1$. Vastavalt valemi tõeväärtuse definitsioonile esimesel juhul $\exists x\, \mathcal{F}(x) = 1$ ja teisel juhul $\exists x\, \mathcal{G}(x) = 1$. Järelikult ka $\exists x\, \mathcal{F}(x) \vee \exists x\, \mathcal{G}(x) = 1$. Sellega oleme tõestanud, et $\exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) \models \exists x\, \mathcal{F}(x) \vee \exists x\, \mathcal{G}(x)$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\exists x\, \mathcal{F}(x) \vee \exists x\, \mathcal{G}(x) = 1$. Siis on kaks võimalust.

1) $\exists x\, \mathcal{F}(x) = 1$. Siis leidub selline $m_0 \in M_\alpha$, et $\mathcal{F}(m_0) = 1$, Järelikult võib öelda, et ka $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$ ja $\exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$.

2) $\exists x\, \mathcal{G}(x) = 1$. Siis leidub selline $m_0 \in M_\alpha$, et $\mathcal{G}(m_0) = 1$. Järelikult võib öelda, et ka $\mathcal{F}(m_0) \vee \mathcal{G}(m_0) = 1$ ja $\exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$.

Sellega oleme tõestanud, et $\exists x\, \mathcal{F}(x) \vee \exists x\, \mathcal{G}(x) \models \exists x\, (\mathcal{F}(x) \vee \mathcal{G}(x))$.

PS3a. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) = 1$. Siis iga $m \in M_\alpha$ korral $\mathcal{F}(m) \,\&\, \mathcal{G} = 1$, kust $\mathcal{F}(m) = 1$ ja $\mathcal{G} = 1$. Järelikult $\forall x\, \mathcal{F}(x) = 1$ ja samuti $\forall x\, \mathcal{F}(x) \,\&\, \mathcal{G} = 1$. Sellega oleme tõestanud, et $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) \models \forall x\, \mathcal{F}(x) \,\&\, \mathcal{G}$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\forall x\, \mathcal{F}(x) \,\&\, \mathcal{G} = 1$. Definitsiooni 1.73 punkti 3 põhjal $\forall x\, \mathcal{F}(x) = 1$ ja $\mathcal{G} = 1$. Siis iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$. Seega iga $m \in M_\alpha$ korral ka $\mathcal{F}(m) \,\&\, \mathcal{G} = 1$, kust valemi tõeväärtuse definitsiooni abil saame, et $\forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) = 1$. Sellega oleme tõestanud, et $\forall x\, \mathcal{F}(x) \,\&\, \mathcal{G} \models \forall x\, (\mathcal{F}(x) \,\&\, \mathcal{G})$.

PS3b. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\exists x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) = 1$. Siis leidub selline $m \in M_\alpha$, et $\mathcal{F}(m) \,\&\, \mathcal{G} = 1$. Järelikult ka $\mathcal{F}(m) = 1$ ja $\mathcal{G} = 1$. Valemi tõeväärtuse definitsiooni põhjal $\exists x\, \mathcal{F}(x) = 1$ ja kuna $\mathcal{G} = 1$, siis ka $\exists x\, \mathcal{F}(x) \,\&\, \mathcal{G} = 1$. Sellega oleme tõestanud, et $\exists x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) \models \exists x\, \mathcal{F}(x) \,\&\, \mathcal{G}$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\exists x\, \mathcal{F}(x) \,\&\, \mathcal{G} = 1$. Definitsiooni 1.73 punkti 3 põhjal $\exists x\, \mathcal{F}(x) = 1$ ja $\mathcal{G} = 1$. Seega leidub selline $m \in M_\alpha$, et $\mathcal{F}(m) = 1$. Järelikult $\mathcal{F}(m) \,\&\, \mathcal{G} = 1$ ja samuti $\exists x\, (\mathcal{F}(x) \,\&\, \mathcal{G}) = 1$. Sellega oleme tõestanud, et $\exists x\, \mathcal{F}(x) \,\&\, \mathcal{G} \models \exists x\, (\mathcal{F}(x) \,\&\, \mathcal{G})$.

PS3c. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}) = 1$. Siis iga $m \in M_\alpha$ korral $\mathcal{F}(m) \vee \mathcal{G} = 1$. On kaks võimalust.

1) $\mathcal{G} = 1$. Siis ka $\forall x\, \mathcal{F}(x) \vee \mathcal{G} = 1$.

2) $\mathcal{G} = 0$. Siis peab iga $m \in M_\alpha$ korral $1 = \mathcal{F}(m) \vee \mathcal{G} = \mathcal{F}(m)$. Järelikult $\forall x\, \mathcal{F}(x) = 1$ ja $\forall x\, \mathcal{F}(x) \vee \mathcal{G} = 1$.

Sellega oleme tõestanud, et $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}) \models \forall x\, \mathcal{F}(x) \vee \mathcal{G}$.

Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral kehtib $\forall x\, \mathcal{F}(x) \vee \mathcal{G} = 1$. Siis on kaks võimalust

1) $\mathcal{G} = 1$. Siis iga $m \in M_\alpha$ korral $\mathcal{F}(m) \vee \mathcal{G} = 1$ ja seega $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}) = 1$.

2) $\forall x\, \mathcal{F}(x) = 1$. Siis iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$ ja seega ka $\mathcal{F}(m) \vee \mathcal{G} = 1$. Järelikult $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}) = 1$.

Sellega oleme tõestanud, et $\forall x\, \mathcal{F}(x) \vee \mathcal{G} \models \forall x\, (\mathcal{F}(x) \vee \mathcal{G})$.

PS3d. Selle tõestuse jätame lugejale iseseisvaks läbimõtlemiseks.

PS4a. Selle samaväärsuse tõestamiseks on kaks võimalust: teha seda otse (nii nagu eelmiste samaväärsuste tõestamisel) või kasutada juba varem tõestatud omadusi. Demonstreerime siin teist võimalust:

$$\begin{aligned}
\forall x\,(\mathcal{F}(x) \Rightarrow \mathcal{G}) &\equiv \forall x\,(\neg\mathcal{F}(x) \vee \mathcal{G}) && \text{(LS14)}\\
&\equiv \forall x\,\neg\mathcal{F}(x) \vee \mathcal{G} && \text{(PS3b)}\\
&\equiv \neg\exists x\,\mathcal{F}(x) \vee \mathcal{G} && \text{(PS1b)}\\
&\equiv \exists x\,\mathcal{F}(x) \Rightarrow \mathcal{G}. && \text{(LS14)}
\end{aligned}$$

Tänu seose $\equiv$ transitiivsusele võime kirjutada, et $\forall x\,(\mathcal{F}(x) \Rightarrow \mathcal{G}) \equiv \exists x\,\mathcal{F}(x) \Rightarrow \mathcal{G}$.

PS4b. Tõepoolest,

$$\begin{aligned}
\exists x\,(\mathcal{F}(x) \Rightarrow \mathcal{G}) &\equiv \exists x\,(\neg\mathcal{F}(x) \vee \mathcal{G}) && \text{(LS14)}\\
&\equiv \exists x\,\neg\mathcal{F}(x) \vee \mathcal{G} && \text{(PS3d)}\\
&\equiv \neg\forall x\,\mathcal{F}(x) \vee \mathcal{G} && \text{(PS1a)}\\
&\equiv \forall x\,\mathcal{F}(x) \Rightarrow \mathcal{G}. && \text{(LS14)}
\end{aligned}$$

PS4c ja **PS4d**. Need tõestused on analoogilised kahe eelnevaga.

PS5a ja **PS5b**. Nii $\forall x\,\mathcal{F}(x) = 1$ kui ka $\forall y\,\mathcal{F}(y) = 1$ parajasti siis, kui iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$. Seega on need kaks valemit samaväärsed. Analoogiliselt $\exists x\,\mathcal{F}(x) \equiv \exists y\,\mathcal{F}(y)$.

PS6a ja **PS6b**. Need järelduvad vahetult kvantorite definitsioonidest. □

Vaatleme ühte näidet sellest, kus me n.ö. igapäevaelus neid samaväärsusi kasutame.

Näide 1.100 Vaatleme signatuuri $\sigma = \langle e;\ *;\ =\rangle$ interpretatsiooni, mille kandja on $M = Mat_2(R)$ ning interpreteerime sümbolit e ühikmaatriksina ja sümbolit $*$ maatriksite korrutamistehtena. Olgu meil valem

$$\mathcal{F}(x) = \exists y((x * y = e)\,\&\,(y * x = e)),$$

mis sisaldab vaba muutujat x. Siis

$$\begin{aligned}
\neg\forall x\mathcal{F}(x) &= \text{“Ei ole nii, et kõik maatriksid on pööratavad”},\\
\exists x\neg\mathcal{F}(x) &= \text{“Leidub maatriks, millel ei ole pöördmaatriksit”}.
\end{aligned}$$

Tänu teoreemi 1.99 punktile 1 teame, et need kaks väidet on samaväärsed.

Tekib loomulik küsimus, et kas teoreemi 1.99 punktis 2 võib konjunktsiooni asendada disjunktsiooniga ja vastupidi. Osutub, et vastus on eitav.

Lause 1.101 *Predikaatarvutuse valemite $\mathcal{F}$ ja $\mathcal{G}$ korral*

$$\forall x\,\mathcal{F}(x) \vee \forall x\,\mathcal{G}(x) \models \forall x\,(\mathcal{F}(x) \vee \mathcal{G}(x)),$$

kuid vastupidine järeldumine üldjuhul ei kehti.

TÕESTUS. Eeldame, et fikseeritud interpretatsiooni α ja vabade muutujate väärtuste korral $\forall x\, \mathcal{F}(x) \vee \forall x\, \mathcal{G}(x) = 1$. Siis on kaks võimalust.

1) $\forall x\, \mathcal{F}(x) = 1$. See tähendab, et iga $m \in M_\alpha$ korral $\mathcal{F}(m) = 1$. Järelikult iga $m \in M_\alpha$ korral ka $\mathcal{F}(m) \vee \mathcal{G}(m) = 1$. Seega $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$.

2) $\forall x\, \mathcal{G}(x) = 1$. Sellisel juhul saame analoogiliselt, et $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$.

Sellega oleme tõestanud, et $\forall x\, \mathcal{F}(x) \vee \forall x\, \mathcal{G}(x) \models \forall x\, (\mathcal{F}(x) \vee \mathcal{G}(x))$.

Veendume, et vastupidine järeldumine ei kehti. Selleks tuleb konstrueerida mingi interpretatsioon. Vaatleme näiteks signatuuri $\sigma = \langle\ ;\ \ ;\ P, Q\rangle$ interpretatsiooni, kus M on kõigi inimeste hulk ja

$$P(x) = \text{“}x \text{ on naissoost”},$$
$$Q(x) = \text{“}x \text{ on meessoost”}.$$

Olgu $\mathcal{F}(x) = P(x)$ ja $\mathcal{G}(x) = Q(x)$. Siis $\forall x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$, kuid $\forall x\, \mathcal{F}(x) \vee \forall x\, \mathcal{G}(x) = 0$, sest $\forall x\, \mathcal{F}(x) = 0$ ja $\forall x\, \mathcal{G}(x) = 0$. Seega

$$\forall x\, (\mathcal{F}(x) \vee \mathcal{G}(x)) \not\models \forall x\, \mathcal{F}(x) \vee \forall x\, \mathcal{G}(x).$$

□

Ülesanne 1.102 Näidata, et

$$\exists x\, (\mathcal{F}(x) \,\&\, \mathcal{G}(x)) \models \exists x\, \mathcal{F}(x) \,\&\, \exists x\, \mathcal{G}(x),$$

kuid vastupidine järeldumine üldjuhul ei kehti.

Teoreemi 1.99 punktis 6 nägime, et samaliigilisi kvantoreid võib ära vahetada. Kuidas on olukord eriliigiliste kvantoritega?

Lause 1.103 *Predikaatarvutuse valemi $\mathcal{F}$ korral*

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

kuid vastupidine järeldumine üldjuhul ei kehti.

TÕESTUS. Oletame, et interpretatsioonis α on valem $\exists x\, \forall y\, \mathcal{F}(x, y)$ tõene. Siis leidub selline $m_0 \in M_\alpha$, et iga $n \in M_\alpha$ korral $\mathcal{F}(m_0, n) = 1$. Kui nüüd muutujal y on suvaline väärtus $n \in M_\alpha$, siis andes muutujale x väärtuse m_0 näeme, et $\mathcal{F}(m_0, n) = 1$. See tähendab, et valem $\forall y\, \exists x\, \mathcal{F}(x, y)$ on tõene.

Järeldumine

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

aga ei kehti. Selle näitamiseks interpreteerime signatuuri $\langle 0;\ +;\ <\rangle$ standardsel viisil hulgal $\mathbb{N}$ ja vaatleme valemit $\mathcal{F}(x, y) = (y < x)$. Siis valem $\forall y\, \exists x\, \mathcal{F}(x, y)$ on tõene selles interpretatsioonis, kuid valem $\exists x\, \forall y\, \mathcal{F}(x, y)$ ei ole tõene, sest ei leidu suurimat naturaalarvu. □

Märkus 1.104 Seotud muutujate ümbernimetamist võib kasutada näiteks järgmises olukorras:

$$\forall x\, (P(x) \vee Q(x, z)) \Rightarrow R(x) \equiv \forall y\, (P(y) \vee Q(y, z)) \Rightarrow R(x).$$

Esimeses valemis esineb x predikaatide P ja Q argumendina seotult, aga R argumendina vabalt. Segaduste vältimiseks võib olla otstarbekas tema seotud esinemised asendada muutujaga y.

1.3.8 Valemi prefikskuju

Nii nagu lausearvutuses võib rääkida valemi normaalkujudest, nii ka predikaatarvutuses on otstarbekas kasutada teatud normaalkuju, mida kutsutakse prefikskujuks. Prefikskujus on kõik kvantorid valemi alguses. Näiteks algoritmid, mida kasutatakse teoreemide automaattõestamiseks, eeldavad tihti, et valem on sellisel kujul.

Definitsioon 1.105 Öeldakse, et predikaatarvutuse valem $\mathcal{F}$ on **prefikskujul**, kui ta ei sisalda kvantoreid või kui

$$\mathcal{F} = Q_1x_1Q_2x_2 \dots Q_nx_n\mathcal{F}',$$

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

Näide 1.106 Valem

$$\forall y \exists x\,(f(x) = y)$$

on prefikskujul, kusjuures tema maatriks on valem $f(x) = y$ (sobivas signatuuris). Valemid

$$\neg\forall x\exists y\, P(x,y,z) \ \text{ ja } \ \exists x\forall y \neg P(x,y,z) \vee \forall x\exists y\, Q(x,y,z)$$

aga ei ole prefikskujul.

Teoreem 1.107 *Iga valemi jaoks leidub temaga samaväärne prefikskujul olev valem.*

TÕESTUS. Vastavalt definitsioonile 1.63 saadakse predikaatarvutuse valemid atomaarsetest valemitest lausearvutuse tehete ja kvantorite abil. Tõestame induktsiooniga valemi struktuuri järgi, et iga selline valem on samaväärne prefikskujul valemiga.

Induktsiooni alus. Atomaarsed valemid on kujul $P(t_1, \dots, t_n)$, kus P on n-kohaline predikaatsümbol ja $t_1, \dots, t_n$ on termid. Sellistes valemites kvantorid puuduvad ning seega on nad prefikskujul.

Induktsiooni samm. Eeldame, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed prefikskujul olevate valemitega ning näitame, et iga valem, mis on neist saadud lausearvutuse tehte või kvantori rakendamise abil, on samuti prefikskujul. Niisiis olgu

$$\mathcal{F} \equiv Q_1x_1Q_2x_2 \dots Q_nx_n\mathcal{F}_1, \qquad \mathcal{G} \equiv Q'_1y_1Q'_2y_2 \dots Q'_my_m\mathcal{G}_1,$$

kus $\mathcal{F}_1$ ja $\mathcal{G}_1$ on kvantoriteta valemid. (Juhtumid, kus $\mathcal{F}$ või $\mathcal{G}$ või mõlemad on kvantoriteta, on lihtsamad ning need jätame läbimõtlemiseks lugejale.) Kasutades seotud muutujate ümbernimetamise reeglit PS5 võime eeldada, et $\{x_1 \dots, x_n\} \cap \{y_1, \dots, y_m\} = \emptyset$, ja et ükski muutuja ei esine neis valemeis korraga seotult ja vabalt.

$\neg$. Iga $i \in \{1, \dots, n\}$ korral tähistame

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

Kasutades kvantori ja eituse vahetusseadusi PS1 n korda saame, et

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

kus valemis $\neg\mathcal{F}_1$ ei ole kvantoreid ja seega valem $\overline{Q_1}x_1\overline{Q_2}x_2 \dots \overline{Q_n}x_n\neg\mathcal{F}_1$ on prefikskujul.

&. Kasutades põhisamaväärsusi saame, et

$$\begin{aligned}
\mathcal{F} \,\&\, \mathcal{G} &\equiv Q_1x_1Q_2x_2\dots Q_nx_n\mathcal{F}_1 \,\&\, \mathcal{G} \\
&\equiv Q_1x_1(Q_2x_2\dots Q_nx_n\mathcal{F}_1 \,\&\, \mathcal{G}) && \text{(PS3)} \\
&\equiv Q_1x_1Q_2x_2(Q_3x_3\dots Q_nx_n\mathcal{F}_1 \,\&\, \mathcal{G}) && \text{(PS3)} \\
&\dots \\
&\equiv Q_1x_1Q_2x_2\dots Q_nx_n(\mathcal{F}_1 \,\&\, \mathcal{G}) && \text{(PS3)} \\
&\equiv Q_1x_1Q_2x_2\dots Q_nx_n(\mathcal{G} \,\&\, \mathcal{F}_1) && \text{(LS3)} \\
&\equiv Q_1x_1Q_2x_2\dots Q_nx_n(Q'_1y_1Q'_2y_2\dots Q'_my_m\mathcal{G}_1 \,\&\, \mathcal{F}_1) \\
&\equiv Q_1x_1Q_2x_2\dots Q_nx_nQ'_1y_1Q'_2y_2\dots Q'_my_m(\mathcal{G}_1 \,\&\, \mathcal{F}_1). && \text{(PS3)}
\end{aligned}$$

Viimane valem ongi prefikskujul, sest valem $\mathcal{G}_1 \,\&\, \mathcal{F}_1$ on kvantoriteta.

$\vee$. Teame, et

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

Tänu kahele eespool vaadeldud juhule võime öelda, et valem $\neg(\neg\mathcal{F} \,\&\, \neg\mathcal{G})$ (ja seega ka valem $\mathcal{F} \vee \mathcal{G}$) on samaväärne prefikskujul oleva valemiga.

$\Rightarrow$. Kuna $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$, siis ka see juhtum taandub eespool vaadeldud juhtudele.

$\Leftrightarrow$. Et $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F} \,\&\, \mathcal{G} \vee \neg\mathcal{F} \,\&\, \neg\mathcal{G}$, siis ka siin saame kasutada juba tõestatut.

$\forall, \exists$. On selge, et valemitega $\forall x\, \mathcal{F}$ ja $\exists x\, \mathcal{F}$ samaväärsed valemid

$$\forall x\, Q_1x_1Q_2x_2\dots Q_nx_n\mathcal{F}_1 \ \text{ ja } \ \exists x\, Q_1x_1Q_2x_2\dots Q_nx_n\mathcal{F}_1$$

on prefikskujul.

□

Valemi prefikskujule viimise all peame silmas temaga samaväärse prefikskujul oleva valemi leidmist. Seda on võimalik teha mitmel viisil. Esitame siin ühe võimaluse.

Predikaatarvutuse valemi prefikskujule viimise algoritm.
Olgu antud predikaatarvutuse valem $\mathcal{H}$, mis on vaja prefikskujule viia.

1. Elimineerime implikatsioonid ja ekvivalentsid kasutades samaväärsusi

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

2. Viime eitused kvantorite alla kasutades De Morgani seadusi ja samaväärsusi

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

Kahekordsed eitused jätame ära.

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

4. Toome kvantorid osavalemite eest valemi ette kasutades samaväärsusi

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

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

ja vajaduse korral ka konjunktsiooni ja disjunktsiooni kommutatiivsust.

Näide 1.108 Viime prefikskujule valemi

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

mis sisaldab vaba muutujat z. Kasutades eelnevat algoritmi saame

$$\begin{aligned}
\mathcal{F}(z) &\equiv \neg\forall x\exists y\, P(x,y,z)\,\&\,\neg\exists x\forall y\,\neg Q(x,y,z) && \text{(samm 2, LS12)}\\
&\equiv \exists x\forall y\,\neg P(x,y,z)\,\&\,\forall x\exists y\,\neg\neg Q(x,y,z) && \text{(samm 2, PS1)}\\
&\equiv \exists x\forall y\,\neg P(x,y,z)\,\&\,\forall x\exists y\, Q(x,y,z) && \text{(samm 2, LS23)}\\
&\equiv \exists x\forall y\,\neg P(x,y,z)\,\&\,\forall u\exists v\, Q(u,v,z) && \text{(samm 3, PS5)}\\
&\equiv \exists x\forall y\,(\neg P(x,y,z)\,\&\,\forall u\exists v\, Q(u,v,z)) && \text{(samm 4, PS3)}\\
&\equiv \exists x\forall y\,(\forall u\exists v\, Q(u,v,z)\,\&\,\neg P(x,y,z)) && \text{(samm 4, LS3)}\\
&\equiv \exists x\forall y\forall u\exists v\,(Q(u,v,z)\,\&\,\neg P(x,y,z)). && \text{(samm 4, PS3)}
\end{aligned}$$

Viimane valem on prefikskujul.

Predikaatarvutuse valemi prefikskuju ei ole üheselt määratud.

Näide 1.109 Vaatleme valemit

$$\forall x\,\mathcal{F}(x)\,\&\,\forall x\,\mathcal{G}(x).$$

Rakendades algoritmi saame

$$\forall x\,\mathcal{F}(x)\,\&\,\forall x\,\mathcal{G}(x) \equiv \forall x\,\mathcal{F}(x)\,\&\,\forall y\,\mathcal{G}(y) \equiv \forall x\forall y(\mathcal{F}(x)\,\&\,\mathcal{G}(y)).$$

Samas teame, et ka valem $\forall x(\mathcal{F}(x)\,\&\,\mathcal{G}(x))$ on esialgse valemiga samaväärne. Seega oleme esialgsele valemile saanud kaks erinevat prefikskuju.

1.4 Teoreem ja tõestus. Tõestustaktikad

1.4.1 Teoreemidest ja tõestustest

Matemaatilise loogika üks põhiline kasutusvaldkond on matemaatiliste teooriate loogiliselt range ülesehitamine. Matemaatilises teoorias (näiteks hulgateooria, eukleidiline geomeetria, naturaalarvude aritmeetika, rühmateooria) fikseeritakse mingid aksioomid ja nendest lähtudes asutakse loogikareeglite abil tõestama uusi teoreeme. Seejuures uute teoreemide tõestamisel võib kasutada (ja kasutataksegi) juba varem tõestatud teoreeme.

Mida mõeldakse matemaatikas tõestuse all? Harilikult loetakse tõestuseks teksti, kus sammude kaupa liikudes jõutakse arusaamiseni, et teoreem kehtib. Igal sammul

- esitatakse järjekordne väide,
- näidatakse ära, millistest eelmistest väidetest ta järeldub,
- öeldakse, millise tuletusreegli, teoreemi, samasuse vmt põhjal ta neist järeldub.

Sellist skeemi oleme järginud ka käesolevas kursuses mitmel pool, näiteks tõesuspuude juures või prefikskujule viimise puhul. Erinevates olukordades esitatakse tõestusi erineva üksikasjalikkuse astmega. Teadusartiklites jäetakse paljud lihtsad sammud kirja panemata, õpikutes esitatakse enamasti detailseid tõestusi. Matemaatiku töö põhisisu on uute teoreemide tõestamine, mitte arvutamine, näidete leidmine või uute mõistete defineerimine (kuigi ka kõike seda tuleb aeg-ajalt teha).

Harilikult esitatakse teoreemid matemaatikas kujul:

Kui kehtivad eeldused $\mathcal{E}_1, \ldots, \mathcal{E}_n$, siis kehtib väide $\mathcal{V}$.

Kui teoreem on sõnastatud mingil teisel kujul, siis saab teda sellisel kujul teoreemi(de)le taandada. Näiteks selleks, et tõestada "$\mathcal{A}$ kehtib parajasti siis, kui kehtib $\mathcal{B}$", piisab meil näidata, et "kui $\mathcal{A}$, siis $\mathcal{B}$" ja "kui $\mathcal{B}$, siis $\mathcal{A}$".

Kasutades loogika sümboolikat võib tüüpilise teoreemi kirja panna kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{V}.$$

Selline järeldumine on samaväärne sellega, et valem

$$\mathcal{E}_1 \,\&\, \ldots \,\&\, \mathcal{E}_n \Rightarrow \mathcal{V}$$

on samaselt tõene.

Näide 1.110 Võib vaadelda järgmist teoreemi: *kui kolmnurga külgede pikkused on a, b, c ning küljed pikkustega a ja b on risti, siis $a^2 + b^2 = c^2$.*

Selle teoreemi puhul

- $\mathcal{E}_1$ = "kolmnurga külgede pikkused on a, b, c",
- $\mathcal{E}_2$ = "küljed pikkustega a ja b on risti",
- $\mathcal{V}$ = "$a^2 + b^2 = c^2$".

Selles paragrahvis räägime võimalikest tõestuse otsimise taktikatest. Täpsemalt öeldes tuleb juttu sellest, milliseid tõestamise taktikaid pakub loogika: kuidas teoreemi eelduse või väite peatehe ütleb meile ette võimaliku järgmise sammu tõestuses.

Lisaks loogika poolt pakutavatele taktikatele on ka veel teisi, näiteks matemaatilise induktsiooni kasutamine, lemma sissetoomine jmt. Neid me siinkohal ei käsitle.

Paljudel juhtudel on võimalik teoreemi eeldused ja väide kirja panna predikaatarvutuse valemite abil. Taktikate leidmiseks uurime iga loogilise seose (s.t. lausearvutuse tehte ja kvantori) korral

1. kuidas tõestada väidet, milles see seos on peatehteks,
2. kuidas kasutada eeldust, milles see seos on peatehteks.

Taktikad, mida me vaatleme, aitavad valemeid lihtsustada: nad asendavad vaadeldava valemi tema osavalemi(te)ga ja jätavad ära välimise tehte või kvantori. See tähendab, et pärast lõplikku arvu samme on meil lootus jõuda atomaarsete valemiteni, mille puhul on loodetavasti kerge kindlaks teha, kas miski millestki järeldub.

1.4.2 Väide on kujul $\mathcal{F} \,\&\, \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Sellise teoreemi saab tõestada järgmise taktikaga: tõestame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{F} \text{ ja } \mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{G}.$$

Näiteks kui on antud mingi nelinurk külgedega a, b, c, d, siis selleks, et tõestada, et see nelinurk on rööpkülik, piisab, kui me näitame, et küljed a ja c on paralleelsed ($\mathcal{F}$) ning küljed b ja d on paralleelsed ($\mathcal{G}$).

1.4.3 Eeldus on kujul $\mathcal{F} \,\&\, \mathcal{G}$

Vaatleme olukorda, kus tõestatava teoreemi mingi eeldus, nt. viimane, on konjunktsioon, s.t. teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \,\&\, \mathcal{G} \models \mathcal{V}.$$

Kui $\mathcal{F} \,\&\, \mathcal{G} = 1$, siis ka $\mathcal{F} = 1$ ja $\mathcal{G} = 1$. Seega piisab näidata, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F}, \mathcal{G} \models \mathcal{V}.$$

1.4.4 Väide on kujul $\mathcal{F} \vee \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{F} \text{ või } \mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{G}.$$

1.4.5 Eeldus on kujul $\mathcal{F} \vee \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \vee \mathcal{G} \models \mathcal{V}.$$

Teoreemi tõestamiseks piisab, kui näitame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \models \mathcal{V} \text{ ja } \mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{G} \models \mathcal{V}.$$

Selle taktika kasutamiseks lisatakse mõnikord eeldustele mingi tõene disjunktsioon ja vaadeldakse selle põhjal kahte juhtu. Näiteks võime teoreemi

Kui n on naturaalarv, siis $n(n+1)$ on paarisarv

tõestamiseks vaadelda eraldi juhte, kus n on paarisarv ja kus n on paaritu arv, ning veenduda, et mõlemal juhul on $n(n+1)$ paarisarv.

1.4.6 Väide on kujul $\mathcal{F} \Rightarrow \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

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

1.4.7 Eeldus on kujul $\mathcal{F} \Rightarrow \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \Rightarrow \mathcal{G} \models \mathcal{V}.$$

Teoreemi tõestamiseks piisab, kui näitame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1} \models \mathcal{F} \text{ ja } \mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{G} \models \mathcal{V}.$$

Enamasti me ei pane teoreemi eeldustesse kirja kõiki juba varem teadaolevaid teoreeme, mida meil antud teoreemi tõestamisel vaja läheb, aga me siiski kasutame neid tõestuses. Need kasutatavad teoreemid on tihti ka kujul $\mathcal{F} \Rightarrow \mathcal{G}$. Antud tõestustaktika ütleb sisuliselt, et kui me tahame eeldust $\mathcal{G}$ väite $\mathcal{V}$ tõestamisel kasutada, siis peame kontrollima, et teoreemi $\mathcal{F} \Rightarrow \mathcal{G}$ eeldus $\mathcal{F}$ on antud eeldustel $\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}$ täidetud.

Näiteks kui tahame väite $\mathcal{V}$ tõestamisel kasutada mingi ruutmaatriksi A pöördmaatriksit, siis teoreemi

Kui ruutmaatriksi determinant ei ole 0, siis tal leidub pöördmaatriks.

kasutamiseks tuleb veenduda, et A determinant ei ole 0.

1.4.8 Väide on kujul $\neg\mathcal{F}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \neg\mathcal{F}.$$

Sellises olukorras on kõige levinum viis vastuolule viimine. Oletatakse vastuväiteliselt, et lisaks eeldustele kehtib ka $\mathcal{F}$. Näidatakse, et sellisel juhul saab mingi väite $\mathcal{G}$ jaoks tõestada, et kehtivad $\mathcal{G}$ ja $\neg\mathcal{G}$, s.t.

$$\mathcal{E}_1, \ldots, \mathcal{E}_n, \mathcal{F} \models \mathcal{G} \ \text{ ja } \ \mathcal{E}_1, \ldots, \mathcal{E}_n, \mathcal{F} \models \neg\mathcal{G}.$$

Sobiv väide $\mathcal{G}$ tuleb iga kord eraldi leida ja soovitav on ta valida nii, et kahe järeldumise tõestamine oleks võimalikult lihtne.

Vastuväitelist tõestamist võib kasutada ka siis, kui teoreemi väide ei ole eitus millestki. Siis teoreemi

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{F}$$

tõestamisel eeldatakse, et koos eeldustega $\mathcal{E}_1, \ldots, \mathcal{E}_n$ on tõene ka $\neg\mathcal{F}$. Näidatakse, et mingi $\mathcal{G}$ korral

$$\mathcal{E}_1, \ldots, \mathcal{E}_n, \neg\mathcal{F} \models \mathcal{G} \ \text{ ja } \ \mathcal{E}_1, \ldots, \mathcal{E}_n, \neg\mathcal{F} \models \neg\mathcal{G}.$$

1.4.9 Eeldus on kujul $\neg\mathcal{F}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \neg\mathcal{F} \models \mathcal{V}.$$

Eeldus $\neg\mathcal{F}$ tähendab, et me teame, et $\mathcal{F}$ on väär. Mingi väite väärus annab meile harilikult vähe informatsiooni.

Olukord, kus eitus on eelduste hulgas, tekib tüüpiliselt vastuväitelise tõestamise juures nii nagu eelmises punktis.

1.4.10 Väide on kujul $\mathcal{F} \Leftrightarrow \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks näidatakse harilikult, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models (\mathcal{F} \Rightarrow \mathcal{G}) \ \text{ ja } \ \mathcal{E}_1, \ldots, \mathcal{E}_n \models (\mathcal{G} \Rightarrow \mathcal{F}).$$

Mõnikord tõestatakse hoopis, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models (\mathcal{F} \Rightarrow \mathcal{G}) \ \text{ ja } \ \mathcal{E}_1, \ldots, \mathcal{E}_n \models (\neg\mathcal{F} \Rightarrow \neg\mathcal{G}).$$

1.4.11 Eeldus on kujul $\mathcal{F} \Leftrightarrow \mathcal{G}$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \Leftrightarrow \mathcal{G} \models \mathcal{V}.$$

Ekvivalentsi kehtimist saab tõestamisel kasutada kahel viisil.

1. Loogiline viis: vaadeldava teoreemi tõestamiseks piisab tõestada, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F} \Rightarrow \mathcal{G}, \mathcal{G} \Rightarrow \mathcal{F} \models \mathcal{V}.$$

2. Matemaatiline viis: kui tõestuses esineb üks valemitest $\mathcal{F}$ ja $\mathcal{G}$, siis võime ta asendada teisega.

1.4.12 Väide on kujul $\forall x\, \mathcal{F}(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \forall x\, \mathcal{F}(x).$$

Sellisel kujul teoreemi tõestuse esimene samm on harilikult selline: tähistagu a suvalist interpretatsiooni kandja elementi. Piisab, kui tõestame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \mathcal{F}(a).$$

Elemendi a *suvalisus* tähendab seda, et eeldustes $\mathcal{E}_1, \ldots, \mathcal{E}_n$ ei ole a kohta midagi väidetud, s.t. a ei esine neis valemeis vabalt. Konkreetse interpretatsiooniga tegeldes ei kasutata fraasi "interpretatsiooni kandja element", vaid öeldakse sõltuvalt olukorrast lihtsalt "Olgu a suvaline naturaalarv/reaalarv/tasandi punkt/...".

1.4.13 Eeldus on kujul $\forall x\, \mathcal{F}(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \forall x\, \mathcal{F}(x) \models \mathcal{V}.$$

Kui tõestuses on mingil sammul vaatluse all mingi element t, siis eeldusest $\forall x\, \mathcal{F}(x)$ saab järeldada, et peab kehtima ka $\mathcal{F}(t)$. Seega teoreemi tõestamiseks piisab, kui me oskame näidata, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F}(t) \models \mathcal{V}.$$

Kui vaja, siis võime eeldust $\forall x\, \mathcal{F}(x)$ kasutada ka veel mingite teiste elementide jaoks.

1.4.14 Väide on kujul $\exists x\, \mathcal{F}(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_n \models \exists x\, \mathcal{F}(x).$$

Sellises olukorras tuleb lähtudes sellest, et kehtivad eeldused $\mathcal{E}_1, \ldots, \mathcal{E}_n$ konstrueerida interpretatsiooni kandja selline element a, mille korral $\mathcal{F}(a)$ on tõene.

1.4.15 Eeldus on kujul $\exists x\, \mathcal{F}(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \exists x\, \mathcal{F}(x) \models \mathcal{V}.$$

Kui eeldus $\exists x\, \mathcal{F}(x)$ on tõene, siis leidub mingi element a, nii et $\mathcal{F}(a)$ on tõene. Seega piisab, kui tõestame, et

$$\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}, \mathcal{F}(a) \models \mathcal{V}.$$

Tähis a peab olema uus, ta ei tohi esineda teistes eeldustes ega väites.

1.4.16 Näide tõestustaktikate kasutamisest

Binaarset seost $\sqsubseteq$ hulgal X nimetatakse **järjestusseoseks**, kui ta on refleksiivne, antisümmeetriline ja transitiivne. Binaarset seost $\sqsubset$ hulgal X nimetatakse **rangeks järjestusseoseks**, kui ta on transitiivne ja iga $x \in X$ korral $x \not\sqsubset x$.

Teoreem 1.111 *Kui $\sqsubset$ on range järjestusseos hulgal X ja defineerime*

$$\forall x, y \in X\, (x \sqsubseteq y \Leftrightarrow (x \sqsubset y) \vee (x = y)),$$

siis $\sqsubseteq$ on järjestusseos hulgal X.

TÕESTUS. Teoreemi eeldused saab kirja panna kujul

$\mathcal{E}_1$) $\forall x\, \neg(x \sqsubset x)$ (antirefleksiivsus),

$\mathcal{E}_2$) $\forall x \forall y \forall z\, ((x \sqsubset y) \,\&\, (y \sqsubset z) \Rightarrow (x \sqsubset z))$ (transitiivsus),

$\mathcal{E}_3$) $\forall x \forall y\, ((x \sqsubseteq y) \Leftrightarrow (x \sqsubset y) \vee (x = y))$ ($\sqsubseteq$ definitsioon).

Teoreemi väide on

$\mathcal{V}_1$) $\forall x\, (x \sqsubseteq x) \,\&$ (refleksiivsus),

$\mathcal{V}_2$) $\forall x \forall y\, ((x \sqsubseteq y) \,\&\, (y \sqsubseteq x) \Rightarrow (x = y)) \,\&$ (antisümmeetria),

$\mathcal{V}_3$) $\forall x \forall y \forall z\, ((x \sqsubseteq y) \,\&\, (y \sqsubseteq z) \Rightarrow (x \sqsubseteq z))$ (transitiivsus).

Kuna teoreemi väide on kolme valemi konjunktsioon, siis kasutades tõestustaktikat 1.4.2 võime näidata, et eelduste tõesusest järeldub iga valemi tõesus eraldi.

$\mathcal{V}_1$ tõestus.

1. Vastavalt taktikale 1.4.12 tähistagu a hulga X suvalist elementi. Piisab, kui tõestame, et $a \sqsubseteq a$.

2. Kasutame eeldust $\mathcal{E}_3$ olukorras, kus $x = a$ ja $y = a$ (taktika 1.4.13). Seega $(a \sqsubseteq a) \Leftrightarrow (a \sqsubset a) \vee (a = a)$. Vastavalt taktikale 1.4.11 võime valemi $a \sqsubseteq a$ asendada valemiga $(a \sqsubset a) \vee (a = a)$. Seega piisab, kui näitame, et $(a \sqsubset a) \vee (a = a)$ on tõene.

3. Viimane disjunktsioon on tõene, sest tema teine liige on tõene (taktika 1.4.4).

$\mathcal{V}_2$ tõestus.

1. Tähistagu a ja b hulga X suvalisi elemente. Väite $\mathcal{V}_2$ tõestamiseks piisab tõestada, et $(a \sqsubseteq b) \,\&\, (b \sqsubseteq a) \Rightarrow (a = b))$ on tõene (taktika 1.4.12).
2. Eeldame, et lisaks eeldustele on tõene ka $(a \sqsubseteq b) \,\&\, (b \sqsubseteq a)$ ning tõestame, et $a = b$ (taktika 1.4.6).
3. Lisaks eeldustele peavad tõesed olema ka $a \sqsubseteq b$ ja $b \sqsubseteq a$ (taktika 1.4.3).
4. Eelduse $\mathcal{E}_3$ tõttu on tõesed $(a \sqsubset b) \vee (a = b)$ ja $(b \sqsubset a) \vee (b = a)$ (taktika 1.4.11).
5. Vastavalt taktikale 1.4.5 tuleb vaadelda nelja võimalust:
   (a) $a \sqsubset b$ ja $b \sqsubset a$,
   (b) $a \sqsubset b$ ja $b = a$,
   (c) $a = b$ ja $b \sqsubset a$,
   (d) $a = b$ ja $b = a$.
6. (a) Kasutades eeldust $\mathcal{E}_2$ saame, et $a \sqsubset a$, kuid see on vastuolus eeldusega $\mathcal{E}_1$. Ka juhtumid (b) ja (c) on vastuolus eeldusega $\mathcal{E}_1$. Seega peavad tõesed olema võrdused $a = b$ ja $b = a$, mida meil oligi vaja.

$\mathcal{V}_3$ tõestus.

1. Tähistagu a, b, c hulga X suvalisi elemente. Piisab tõestada, et $(a \sqsubseteq b) \,\&\, (b \sqsubseteq c) \Rightarrow (a \sqsubseteq c)$ on tõene.
2. Implikatsiooni tõestamiseks eeldame, et $(a \sqsubseteq b) \,\&\, (b \sqsubseteq c)$ on tõene ja näitame, et ka $a \sqsubseteq c$ on tõene.
3. Eelduse $\mathcal{E}_3$ põhjal kehtib $((a \sqsubset b) \vee (a = b)) \,\&\, ((b \sqsubset c) \vee (b = c))$ ning vaja on tõestada, et kehtib $(a \sqsubset c) \vee (a = c)$.
4. Disjunktsioonid tekitavad jälle neli varianti.
   (a) $a \sqsubset b$ ja $b \sqsubset c$ on tõesed. Siis $\mathcal{E}_2$ põhjal $a \sqsubset c$.
   (b) $a \sqsubset b$ ja $b = c$ on tõesed. Siis $a \sqsubset c$.
   (c) $a = b$ ja $b \sqsubset c$ on tõesed. Siis $a \sqsubset c$.
   (d) $a = b$ ja $b = c$ on tõesed. Siis $a = c$.

   Seega tõesti kõigil juhtudel $(a \sqsubset c) \vee (a = c)$ on tõene.

□

1.5 Aksiomaatilised teooriad. Peano aksiomaatika

1.5.1 Aksiomaatilised teooriad

Mitteformaalne aksiomaatiline teooria ehitatakse üles järgmise skeemi kohaselt.

1. Fikseeritakse mingi hulk antud teoorias uuritavaid objekte, nendel defineeritud seoseid ja funktsioone ning sümboolika nende tähistamiseks.

2. Teatud hulk väiteid loetakse tõeseks ilma tõestuseta. Neid väiteid nimetatakse selle teooria **aksioomideks**.

3. Teooria arendamine seisneb teoreemide tõestamises. **Teoreemideks** loetakse väiteid, mida saab tõestada lähtudes aksioomidest. Selleks, et uusi teoreeme oleks mugavam sõnastada, võidakse olemasolevate mõistete abil defineerida uusi mõisteid ja tuua sisse uusi tähistusi.

Teooria aksiomaatiline ülesehitus annab igale soovijale võimaluse kontrollida, kas mingi teoreem ikka kehtib või mitte. Selleks tuleks veenduda, et kõiki tõestussamme saab teha mingite aksioomide põhjal.

Tänapäeval on enamus matemaatilisi teooriaid üles ehitatud aksiomaatiliselt. Muuhulgas näiteks

- eukleidiline geomeetria,
- naturaalarvude aritmeetika (Peano aksiomaatika),
- hulgateooria (näiteks Zermelo-Fraenkeli aksiomaatika),
- algebraliste struktuuride (rühmad, vektorruumid jne.) teooriad,
- matemaatiline analüüs ja funktsionaalanalüüs.

1.5.2 Peano aritmeetika

Selles paragrahvis vaatleme küsimust, kuidas defineerida naturaalarvud ja tehted nendega.

Naturaalarvude aritmeetika aksiomaatiliseks käsitlemiseks vaatleme signatuuri

$$\sigma = \langle 0;\ ', +, \cdot;\ = \rangle,$$

kus $'$ on ühekohaline funktsionaalsümbol (seda tõlgendame kui "järgmise" elemendi leidmise operatsiooni) ning $+$ ja $\cdot$ on kahekohalised funktsionaalsümbolid. **Peano**[4] **aritmeetika** aksioomid on järgmised:

P1. $\forall x\, \neg(x' = 0)$;

P2. $\forall x \forall y (x' = y' \Rightarrow x = y)$;

[4] Giuseppe Peano (1858–1932) — itaalia matemaatik

P3. $\forall x(x+0=x)$;

P4. $\forall x \forall y(x+y'=(x+y)')$;

P5. $\forall x(x \cdot 0=0)$;

P6. $\forall x \forall y(x \cdot y'=x \cdot y+x)$;

P7. kõik valemid kujul $\mathcal{F}(0) \,\&\, \forall x(\mathcal{F}(x) \Rightarrow \mathcal{F}(x')) \Rightarrow \forall x \mathcal{F}(x)$, kus $\mathcal{F}(x)$ on suvaline valem signatuuris σ.

Märkus 1.112 Me võime vaadelda hulka

$$\{0, 0', 0'', 0''', 0'''', \ldots\}$$

Osutub, et kõik selle hulga elemendid on erinevad. Aksioomi P1 tõttu on 0 erinev kõigist teistest selle hulga elementidest. Kui näiteks oletaksime, et $0' = 0''$, siis aksioomi P2 tõttu $0 = 0'$, mis on vastuolus aksioomiga P1. Seega $0'$ ja $0''$ on erinevad. Analoogiliselt saaksime mistahes kahe elemendi korral näidata, et nad on erinevad.

Märkus 1.113 Induktsiooniaksioom P7 annab veel ühe taktika, mille abil saab Peano aritmeetikas tõestada väiteid kujul $\forall x\, \mathcal{F}(x)$. Vastavalt implikatsiooni definitsioonile piisab sellise väite tõesuse näitamiseks sellest, kui veendume, et

1. $\mathcal{F}(0)$ on tõene (induktsiooni alus ehk baas),
2. $\forall x(\mathcal{F}(x) \Rightarrow \mathcal{F}(x'))$ on tõene (induktsiooni samm).

Kas me saaksime defineerida naturaalarvude hulga, kui aksioomide P1–P7 mudeli? Tekib küsimus, et kas valemitest P1–P7 koosneval hulgal leidub üldse mõni mudel? Kui jah, siis milline see võiks olla?

Hulgateooria aksioomide põhjal (mida me selles kursuses küll ei käsitle) on olemas hulgad

$$\begin{aligned}
&0 := \emptyset,\\
&1 := \{0\} = \{\emptyset\},\\
&2 := \{0,1\} = \{\emptyset, \{\emptyset\}\},\\
&3 := \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\\
&\quad \ldots
\end{aligned}$$

kusjuures need on kõik paarikaupa erinevad. Nagu näha,

$$n+1 = n \cup \{n\} = \{0, 1, \ldots, n\},$$

s.t. selle jada iga järgmise hulga elementideks on kõik eelmised hulgad. Hulgateooria aksioomidest lähtudes saab tõestada, et kehtib järgmine tulemus (tõestuse võib leida näiteks raamtust [4], teoreem 3.1.1).

Teoreem. *Leidub täpselt üks hulk* $\mathbb{N}$*, mis rahuldab järgmisi tingimusi:*

1. $\emptyset \in \mathbb{N}$;

2. $\forall x\,(x \in \mathbb{N} \Rightarrow x \cup \{x\} \in \mathbb{N})$;

3. *kui* K *on selline hulk, et*

$$(\emptyset \in K)\,\&\,\forall x\,((x \in K) \Rightarrow (x \cup \{x\} \in K)),$$

siis $\mathbb{N} \subseteq K$.

Niisiis $\mathbb{N}$ on vähim hulk, mis sisaldab 0 ja mis koos iga hulgaga n sisaldab ka hulga $n \cup \{n\}$. See tähendab, et $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. Selle hulga elemente hakkame nimetama **naturaalarvudeks**.

Interpreteerime nüüd signatuuri σ järgnevalt. Põhihulgaks olgu hulk $\mathbb{N}$. Funktsiooni $' : \mathbb{N} \to \mathbb{N}$ defineerime võrdusega

$$n' := n \cup \{n\} = n + 1.$$

Kahekohalised funktsioonid (ehk kahekohalised algebralised tehted) $+$ ja $\cdot$ hulgal $\mathbb{N}$ defineerime võrdustega

$$n + 0 := n, \quad n + m' := (n + m)',$$

$$n \cdot 0 := 0, \quad n \cdot m' := n \cdot m + n.$$

On võimalik näidata, et selline interpretatsioon on aksioomide P1–P7 mudeliks. Seda mudelit nimetame Peano aritmeetika **standardseks mudeliks**.

Tuleb välja, et Peano aritmeetikal on olemas ka mittestandardseid mudeleid. Selliste mudelite leidumist võimaldab asjaolu, et mudeli kandja M peab küll sisaldama elemente $0, 0', 0'', 0''', \ldots$, aga aksioomid P1–P7 ei ütle midagi selle kohta, kas see kandja võib sisaldada ka mingeid teisi elemente. Mittestandardsete mudelite konstruktsioonid on üsna keerulised ja selles kursuses me neid ei käsitle.

Niisiis naturaalarvud (nagu ka mittestandardsed mudelid) rahuldavad Peano aksioome. Tuleb välja, et väga suure osa naturaalarvude aritmeetika kohta käivatest teoreemidest (kuid mitte kõik) saab tõestada lähtudes Peano aksioomidest. Tõestame mõned selised teoreemid.

Teoreem 1.114 *Naturaalarvude liitmine on assotsiatiivne:*

$$\forall x \forall y \forall z\,((x + y) + z = x + (y + z)).$$

Tõestus. Kahe välimise üldisuskvantori jaoks kasutame tõestamistaktikat 1.4.12. Tähistagu a ja b suvalisi naturaalarve. Teoreemi tõestamiseks piisab, kui tõestame, et

$$\forall z\,((a + b) + z = a + (b + z)).$$

Selleks kasutame aksioomi P7 olukorras, kus

$$\mathcal{F}(z) = ((a + b) + z = a + (b + z)).$$

Induktsiooni alus. Veendume, et $\mathcal{F}(0)$ on tõene. Tänu aksioomile P3

$$(a+b)+0=a+b \quad \text{ja} \quad a+(b+0)=a+b.$$

Järelikult

$$(a+b)+0=a+(b+0).$$

Induktsiooni samm. Peame näitama, et valem

$$\forall z\,((a+b)+z=a+(b+z) \;\Rightarrow\; (a+b)+z'=a+(b+z')) \tag{1.3}$$

on tõene. Selleks tähistagu c suvalist naturaalarvu ja eeldame, et

$$(a+b)+c=a+(b+c) \tag{1.4}$$

on tõene. Siis

$$\begin{aligned}
(a+b)+c' &= ((a+b)+c)' && \text{(P4)}\\
&= (a+(b+c))' && \text{(eeldus (1.4))}\\
&= a+(b+c)' && \text{(P4)}\\
&= a+(b+c'). && \text{(P4)}
\end{aligned}$$

Järelikult $(a+b)+c'=a+(b+c')$ ja sellega oleme näidanud, et valem (1.3) on tõene. □

Teoreem 1.115 *Naturaalarvude liitmine on kommutatiivne:*

$$\forall x\forall y\,(x+y=y+x).$$

TÕESTUS. Vaatleme valemit

$$\mathcal{F}(x)=\forall y\,(x+y=y+x).$$

Teoreemi tõestamiseks tõestame indunktsiooniga, et valem $\forall x\,\mathcal{F}(x)$ on tõene.

Alus. Näitame, et valem

$$\forall y\,(0+y=y+0)$$

on tõene. Ka selleks kasutame indunktsiooni. Täpsemalt öeldes näitame, et $\forall y\,\mathcal{G}(y)$ on tõene, kus $\mathcal{G}(y)=(0+y=y+0)$.

Alus. On ilmne, et $0+0=0+0$.

Samm. Näitame, et

$$\forall y\,(0+y=y+0 \;\Rightarrow\; 0+y'=y'+0)$$

on tõene. Tähistagu a suvalist naturaalarvu. Piisab tõestada, et

$$0+a=a+0 \;\Rightarrow\; 0+a'=a'+0 \tag{1.5}$$

on tõene. Eeldame, et $0 + a = a + 0$ on tõene. Siis

$$\begin{aligned} 0 + a' &= (0 + a)' && \text{(P4)} \\ &= (a + 0)' && \text{(eeldus)} \\ &= a' && \text{(P3)} \\ &= a' + 0. && \text{(P3)} \end{aligned}$$

Seega $0 + a' = a' + 0$ ja oleme tõestanud, et valem (1.5) on tõene.

Samm. Peame näitama, et

$$\forall x\,(\forall y\,(x + y = y + x) \;\Rightarrow\; \forall y\,(x' + y = y + x'))$$

on tõene. Tähistagu b suvalist naturaalarvu. Siis piisab tõestada, et

$$\forall y\,(b + y = y + b) \;\Rightarrow\; \forall y\,(b' + y = y + b')$$

on tõene. Selleks eeldame, et

$$\forall y\,(b + y = y + b) \tag{1.6}$$

on tõene. Vaja on näidata, et

$$\forall y\,(b' + y = y + b')$$

on tõene. Teeme seda induktsiooniga y järgi.

Alus. Kehtivad võrdused

$$\begin{aligned} b' + 0 &= b' && \text{(P3)} \\ &= (b + 0)' && \text{(P3)} \\ &= (0 + b)' && \text{(eeldus (1.6))} \\ &= 0 + b'. && \text{(P4)} \end{aligned}$$

Samm. Peame tõestama, et

$$\forall y\,((b' + y = y + b') \Rightarrow (b' + y' = y' + b'))$$

on tõene. Tähistagu c suvalist naturaalarvu. Piisab, kui tõestame, et

$$(b' + c = c + b') \Rightarrow (b' + c' = c' + b')$$

on tõene. Selleks eeldame, et

$$b' + c = c + b' \tag{1.7}$$

on tõene. Siis

$$\begin{aligned}
b' + c' &= (b' + c)' && \text{(P4)}\\
&= (c + b')' && \text{(eeldus (1.7))}\\
&= (c + b)'' && \text{(P4)}\\
&= (b + c)'' && \text{(eeldus (1.6))}\\
&= (b + c')' && \text{(P4)}\\
&= (c' + b)' && \text{(eeldus (1.6))}\\
&= c' + b'. && \text{(P4)}
\end{aligned}$$

Seega $b' + c' = c' + b'$, mida oligi tarvis tõestada.

□

Järeldus 1.116 *Naturaalarvudel on omadus*

$$\forall x\, (0 + x = x).$$

TÕESTUS. Olgu a suvaline naturaalarv. Siis teoreemi 1.115 ja aksioomi P3 põhjal

$$0 + a = a + 0 = a.$$

□

Teoreem 1.117 *Naturaalarvude puhul kehtib järgmine distributiivsuse seadus:*

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

TÕESTUS. Tähistagu a ja b suvalisi naturaalarve. Piisab, kui tõestame, et

$$\forall z\, (a \cdot (b + z) = a \cdot b + a \cdot z)$$

on tõene. Selle tõestamiseks kasutame induktsiooni z järgi.

Alus. Näitame, et $a \cdot (b + 0) = a \cdot b + a \cdot 0$. Tõepoolest,

$$\begin{aligned}
a \cdot (b + 0) &= a \cdot b && \text{(P3)}\\
&= a \cdot b + 0 && \text{(P3)}\\
&= a \cdot b + a \cdot 0. && \text{(P5)}
\end{aligned}$$

Samm. Tõestame, et

$$\forall z\, (a \cdot (b + z) = a \cdot b + a \cdot z \;\Rightarrow\; a \cdot (b + z') = a \cdot b + a \cdot z')$$

on tõene. Tähistagu c suvalist naturaalarvu. Piisab tõestada, et

$$a \cdot (b + c) = a \cdot b + a \cdot c \;\Rightarrow\; a \cdot (b + c') = a \cdot b + a \cdot c'$$

on tõene. Selleks eeldame, et

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{1.8}$$

on tõene. Siis

$$\begin{aligned} a \cdot (b + c') &= a \cdot (b + c)' && \text{(P4)} \\ &= a \cdot (b + c) + a && \text{(P6)} \\ &= (a \cdot b + a \cdot c) + a && \text{(eeldus (1.8))} \\ &= a \cdot b + (a \cdot c + a) && \text{(teoreem 1.114)} \\ &= a \cdot b + a \cdot c'. && \text{(P6)} \end{aligned}$$

□

Teoreem 1.118 *Naturaalarvudel on järgmine omadus:*

$$\forall x \forall y \forall z\, (x + z = y + z \;\Rightarrow\; x = y).$$

TÕESTUS. Tähistagu a ja b suvalisi naturaalarve. Teoreemi tõestamiseks piisab, kui tõestame, et

$$\forall z\, (a + z = b + z \;\Rightarrow\; a = b)$$

on tõene. Selleks kasutame aksioomi P7 olukorras, kus

$$\mathcal{F}(z) = (a + z = b + z \;\Rightarrow\; a = b).$$

Induktsiooni alus. Veendume, et $\mathcal{F}(0)$ on tõene. Olgu $a + 0 = b + 0$. Tänu aksioonile P3 saame võrduse $a = b$.
Induktsiooni samm. Tähistagu c suvalist naturaalarvu. Eeldame, et valem

$$a + c = b + c \;\Rightarrow\; a = b \tag{1.9}$$

on tõene. Oletame, et kehtib võrdus $a+c' = b+c'$. Siis aksioomi P4 põhjal $(a+c)' = (b+c)'$, kust aksioomi P2 abil saame võrduse $a + c = b + c$. Eeldust (1.9) kasutades saame, et $a = b$. Sellega oleme tõestanud, et

$$\forall z\, (\mathcal{F}(z) \Rightarrow \mathcal{F}(z'))$$

on tõene ning järelikult on tõene ka $\forall z\, \mathcal{F}(z)$. □

Ülesanne 1.119 Näidata, et naturaalarvudel on järgmised omadused:

- $\forall x \forall y \forall z\, ((x + y) \cdot z = x \cdot z + y \cdot z)$;
- $\forall x \forall y \forall z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z))$;
- $\forall x \forall y\, (x \cdot y = y \cdot x)$;
- $\forall x\, (x \cdot 1 = x)$.

Loomulikult ei pea naturaalarvude käsitlemisel piirduma ainult liitmis- ja korrutamistehte ning võrdusseosega. Võib defineerida ka uusi tehteid, seoseid ja mõisteid. Näiteks võime defineerida kahekohalise seose $\leqslant$ järgmiselt:

$$\forall x \forall y\, (x \leqslant y \Leftrightarrow \exists z(x + z = y)).$$

Teoreem 1.120 *Seos $\leqslant$ on järjestusseos naturaalarvude hulgal.*

Tõestus. Refleksiivsus. Tähistagu a suvalist naturaalarvu. Aksioomi P3 põhjal $a+0=a$. Järelikult $\exists z\,(a+z=a)$ on tõene. See tähendab, et kehtib ka $a \leqslant a$.

Antisümmeetria. Peame näitama, et

$$\forall x \forall y\,((x \leqslant y)\,\&\,(y \leqslant x) \Rightarrow (x = y)).$$

Tähistagu a, b suvalisi naturaalarve ning eeldame, et $a \leqslant b$ ja $b \leqslant a$. Siis leiduvad naturaalarvud c ja d nii, et $a + c = b$ ja $b + d = a$. Järelikult

$$(c + d) + a = a + (c + d) = (a + c) + d = b + d = a = 0 + a.$$

Teoreemi 1.118 põhjal saame, et $c + d = 0$. Oletame vastuväiteliselt, et $d \neq 0$. Siis leidub selline e, et $d = e'$. Järelikult

$$0 = c + d = c + e' = (c + e)',$$

mis on vastuolus aksioomiga P1. Seega $d = 0$ ja võrdusest $b + d = a$ saame, et $b = a$.

Transitiivsus. Peame näitama, et

$$\forall x \forall y \forall z\,((x \leqslant y)\,\&\,(y \leqslant z) \Rightarrow (x \leqslant z)).$$

Tähistagu a, b, c suvalisi naturaalarve ning kehtigu võrratused $a \leqslant b$ ja $b \leqslant c$. Siis leiduvad naturaalarvud u ja v nii, et $a + u = b$ ja $b + v = c$. Järelikult

$$c = b + v = (a + u) + v = a + (u + v),$$

kust seose $\leqslant$ definitsiooni tõttu $a \leqslant c$. □

Ülesanne 1.121 Tõestada, et naturaalarvude järjestusseos $\leqslant$ on kooskõlas liitmise ja korrutamisega, s.t.

$$\forall x \forall y \forall z\,(x \leqslant y \;\Rightarrow\; x + z \leqslant y + z),$$
$$\forall x \forall y \forall z\,(x \leqslant y \;\Rightarrow\; x \cdot z \leqslant y \cdot z).$$

Peatükk 2

Graafiteooria

2.1 Graafi mõiste

Selle kursuse teises osas käsitleme graafiteooriat. See on diskreetse matemaatika üks oluline haru, millel leidub ka palju praktilisi rakendusi. Loengukonspekti koostamisel on põhiliselt kasutatud raamatuid [9], [3] ja [2].

Graafiteooria loojaks peetakse Leonhard Eulerit[1].

Paljude päriselus esinevate olukordade modelleerimiseks on kasulik kasutada diagramme, millel on punktide abil ära märgitud teatud objektid ja punktidevaheliste joonte abil on välja toodud objektidevahelised seosed. Näiteks maanteede kaart (punktid – asulad, jooned – maanteed) või sugupuu (punktid – inimesed, jooned – sugulussidemed). Sedasorti diagrammide matemaatiliseks käsitlemiseks on kasutusele võetud graafi mõiste.

Definitsioon 2.1 **Graaf** on paar $G = (V, E)$, kus V on mittetühi hulk ja E on hulk, mille elementideks on hulga V mingid kaheelemendilised alamhulgad. Hulga V elemente nimetatakse graafi G **tippudeks**[2] ja hulga E elemente selle graafi **servadeks**[3].

Serva tippude u ja v vahel tähistatakse $\{u, v\}$ asemel tihti ka lihtsalt uv.

Antud definitsiooni mõttes ei tohi graafil olla silmuseid (servi, mille otspunktid langevad kokku) ega kordseid servi (s.t. kahe tipu vahel on ülimalt üks serv). Samuti ei ole oluline servade suund (suunatud graafe vaatleme selles kursuses hiljem).

Põhimõtteliselt võib graafis olla ka lõpmata palju tippe ja servi, aga **käesolevas kursuses käsitleme ainult lõplikke graafe**. Kui tekib vajadus rääkida lõpmatutest graafidest, siis juhime sellele eraldi tähelepanu.

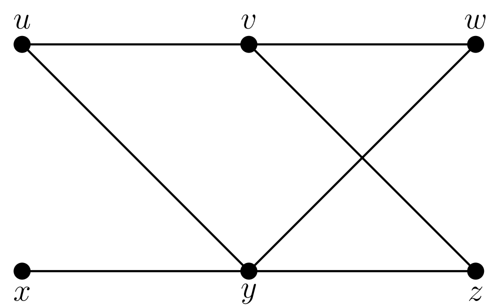
Definitsioon 2.2 Kui graafi tipp v kuulub servale e, siis öeldakse, et tipp v ja serv e on **intsidentsed**. Iga serv on intsidentne täpselt kahe tipuga, mida kutsutakse selle serva **otstippudeks**. Kahte tippu nimetatakse **naabertippudeks**, kui nad on servaga ühendatud. Kahte serva nimetatakse **naaberservadeks**, kui neil leidub ühine otstipp.

[1] Leonhard Euler (1707–1783) — šveitsi matemaatik

[2] tipp = *vertex*

[3] serv = *edge*

Näide 2.3 Graafe esitatakse tihti jooniste abil, kus täppidena on märgitud graafi tipud ja kaks tippu on ühendatud joonega parajasti siis, kui nende vahel on serv. Näiteks võime vaadelda järgmist kuuetipulist graafi:



Selle graafi puhul

$$
\begin{aligned}
V &= \{u, v, w, x, y, z\} \\
E &= \{uv, uy, vw, vz, wy, xy, yz\}.
\end{aligned}
$$

Selles graafis näiteks u ja y on naabertipud, aga u ja z ei ole. Servad uy ja wy on naaberservad, sest neil on ühine otspunkt y.

Graafide esitamisel ja uurimisel saab kasutada maatriksite abi. Graafidega seotud maatriksite defineerimiseks on oluline fikseerida tippude ja servade järjekord.

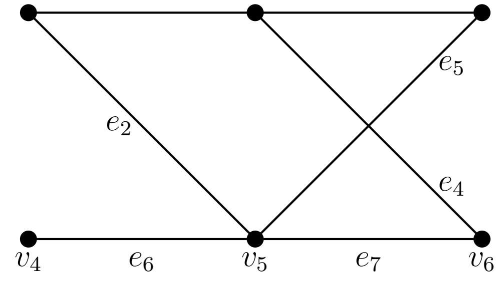
Definitsioon 2.4 Olgu $G = (V, E)$ graaf tippude hulgaga $V = \{v_1, \ldots, v_n\}$. Graafi G **naabrusmaatriksiks** nimetatakse $n \times n$-maatriksit $A = (a_{ij})$, kus

$$a_{ij} = \begin{cases} 1, & \text{kui } v_i v_j \in E, \\ 0, & \text{kui } v_i v_j \notin E. \end{cases}$$

Definitsioon 2.5 Olgu $G = (V, E)$ graaf tippude hulgaga $V = \{v_1, \ldots, v_n\}$ ja servade hulgaga $E = \{e_1, \ldots, e_m\}$. Graafi G **intsidentsusmaatriksiks** nimetatakse $n \times m$-maatriksit $B = (b_{ij})$, kus

$$b_{ij} = \begin{cases} 1, & \text{kui } v_i \text{ on serva } e_j \text{ otstipp}, \\ 0, & \text{kui } v_i \text{ ei ole serva } e_j \text{ otstipp}. \end{cases}$$

Näide 2.6 Vaatleme graafi



Selle graafi naabrusmaatriks on

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

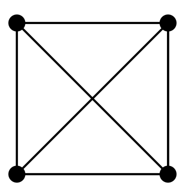
ja intsidentsusmaatriks on

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

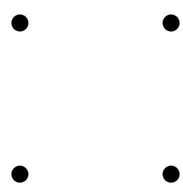
Definitsioon 2.7 Täisgraaf on graaf, mille iga kahe erineva tipu vahel on serv. n-tipulist täisgraafi tähistatakse sümboliga K_n.

Definitsioon 2.8 Nullgraaf on graaf, milles puuduvad servad. n-tipulist nullgraafi tähistatakse sümboliga O_n.

Näide 2.9 Neljatipuline täisgraaf ja nullgraaf:



K_4



O_4

Märkus 2.10 Graafil K_n on servi sama palju kui on n-elemendilisel hulgal 2-elemendilisi alamhulki. Seega on tema servade arv

$$C_n^2 = \frac{n(n-1)}{2}.$$

Näide 2.11 (Graafid kui mudelid) Vaatleme signatuuri, milles on üks kahekohaline predikaatsümbol R ja võrdussümbol $=$. Siis graafi $G = (V, E)$ võib vaadelda selle signatuuri interpretatsioonina põhihulgaga V, kus sümbolit R interpreteerime tippude naabrusseosena:

$$R(v_i, v_j) = a_{ij},$$

kus $A = (a_{ij})$ on graafi naabrusmaatriks. See interpretatsioon on valemite hulga

$$\{\forall x\, \neg R(x,x),\ \forall x \forall y\, (R(x,y) \Rightarrow R(y,x))\}$$

mudeliks. Täisgraaf on veel valemi

$$\forall x \forall y\, (\neg(x = y) \Rightarrow R(x, y))$$

mudeliks. Nullgraaf on valemi

$$\forall x \forall y\, \neg R(x, y)$$

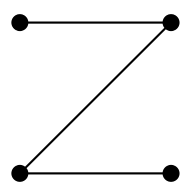
mudeliks.

Definitsioon 2.12 Graafi G **täiendgraaf** ehk **täiend** on graaf $\overline{G}$, mille tippude hulk on sama, mis G tippude hulk, aga servaga on ühendatud parajasti need tipud, mille vahel graafis G serv puudub.

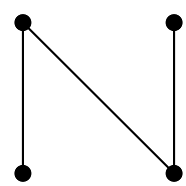
Näide 2.13 Lihtne on aru saada, et

$$\overline{K_n} = O_n \quad \text{ja} \quad \overline{O_n} = K_n\,.$$

Näide 2.14 Järgmised graafid on teineteise täiendgraafid:



ja



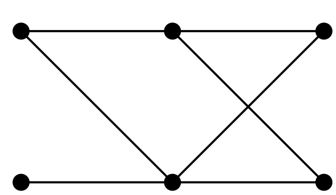
Graafidega tegeldes on meil aeg-ajalt vaja konstrueerida uusi graafe lähtudes olemasolevatest. Täiendgraafi moodustamine on üheks selliseks konstruktsiooniks. Lisaks sellele kasutame järgmisi operatsioone:

- serva kustutamine,
- serva lisamine kahe seniühendamata tipu vahele,
- tipu kustutamine koos kõigi temaga intsidentsete servadega,
- tipu lisamine koos servadega uue tipu ja teatava hulga seniste tippude vahele.

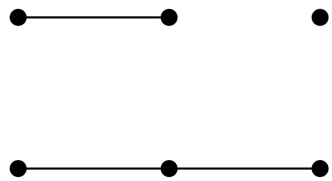
Definitsioon 2.15 Graafi $G' = (V', E')$ nimetatakse graafi $G = (V, E)$ **alamgraafiks**, kui ta on saadud graafist G teatud hulga tippude ja servade kustutamisel, s.t. $V' \subseteq V$ ja $E' \subseteq E$.

Näide 2.16

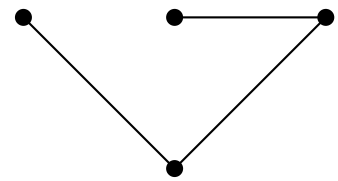
1. Iga graaf on iseenda alamgraaf.
2. Nullgraaf O_n on iga n-tipulise graafi alamgraaf.
3. Graafi



alamgraafideks on näiteks



ja



Definitsioon 2.17 Graafi tipu v **astmeks** ehk **valentsiks** nimetatakse selle tipuga intsidentsete servade arvu. Tipu v astet tähistatakse sümboliga $d(v)$.

Kui graafis on n tippu, siis iga tipu v korral $d(v) \in \{0, 1, \ldots, n-1\}$.

Definitsioon 2.18 Tippu, mille aste on 0, nimetatakse **isoleeritud tipuks**. Tippu, mille aste on 1, nimetatakse **rippuvaks tipuks**.

Näide 2.19 Näites 2.3 vaadeldud graafi tippude astmed on

$$d(u) = d(w) = d(z) = 2,\ d(v) = 3,\ d(x) = 1,\ d(y) = 4.$$

Selles graafis on üks rippuv tipp x ja mitte ühtegi isoleeritud tippu.

Teoreem 2.20 *Igas graafis on kõigi tippude astmete summa võrdne servade arvu kahekordsega.*

TÕESTUS. Olgu $G = (V, E)$ graaf. Me peame näitama, et

$$\sum_{v \in V} d(v) = 2 \cdot |E|.$$

Selle summa leidmisel vaatleme ühekaupa kõiki graafi tippe ja loeme kokku selle tipuga intsidentsed servad. Nii tehes oleme iga serva arvesse võtnud kaks korda: üks kord ühe otstipu juures ja teine kord teise otstipu juures. Seega peab tippude astmete summa olema kaks korda suurem kui servade arv. □

Järeldus 2.21 *Igas graafis on paaritu astmega tippe paarisarv.*

TÕESTUS. Kui paaritu astmega tippe oleks paaritu arv, siis summa

$$\sum_{v \in V} d(v)$$

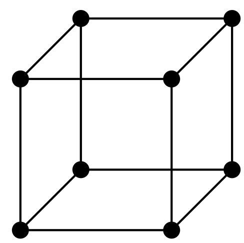
oleks paaritu arv, mis on vastuolus teoreemiga 2.20. Järelikult peab paaritu astmega tippe olema paarisarv. □

Definitsioon 2.22 Graafi nimetatakse **regulaarseks**, kui tema kõigi tippude astmed on võrdsed. Kui kõigi tippude astmed on võrdsed naturaalarvuga k, siis öeldakse, et graaf on k**-regulaarne**.

Näide 2.23 1. Täisgraaf K_n on $(n-1)$-regulaarne.

2. Nullgraaf O_n on 0-regulaarne.

3. Näide 3-regulaarsest graafist:



Järeldus 2.24 *n-tipulises k-regulaarses graafis on $\frac{nk}{2}$ serva.*

TÕESTUS. Olgu $G = (V, E)$ k-regulaarne graaf. Teoreemi 2.20 põhjal

$$|E| = \left(\sum_{v \in V} d(v)\right) / 2 = \frac{nk}{2}.$$

$\square$

Ülesanne 2.25 Kas leidub 5-tipuline 3-regulaarne graaf? Miks?

2.2 Ahelad ja tsüklid

Definitsioon 2.26 **Ahel**[4] graafis G on selline tippude järjend $v_0, v_1, \ldots, v_k$, kus iga kaks järjestikust tippu on ühendatud servaga. Tippe v_0 ja v_k nimetatakse ahela **otstippudeks**, ülejäänud tipud on ahela **sisetipud**. Ahela $v_0, v_1, \ldots, v_k$ **pikkuseks** loetakse arv k.

Niisiis, ahela pikkus on võrdne servade arvuga (mitte tippude arvuga!) selles ahelas. Muuhulgas on olemas ka ahel pikkusega 0 (see sisaldab ainult ühte tippu v_0). Tihti kirjutatakse $v_0, v_1, \ldots, v_k$ asemel lihtsalt $v_0 v_1 \ldots v_k$.

Kui meil on ahel $v_0, v_1, \ldots, v_k$, siis öeldakse, et see ahel **läbib** tippe $v_0, v_1, \ldots, v_k$ ja servi $v_0v_1, v_1v_2, \ldots, v_{k-1}v_k$.

Ahelas võib mõni tipp või isegi mõni serv esineda mitu korda.

Definitsioon 2.27 **Lihtahel**[5] on ahel, mille kõik tipud on erinevad.

Kuna lihtahelas ei saa tipud korduda, siis on selge, et lihtahelas ei saa ka ükski serv esineda mitu korda.

Märkus 2.28 Graafide puhul on erinevates keeltes ja erinevates raamatutes kasutusel üsna erinev terminoloogia, seetõttu tuleb hoolega jälgida, mida mingi termin mingis allikas tähendab. Siin oleme ära toonud mõnede terminite ingliskeelsed vasted, nii nagu neid on kasutatud raamatus [2].

Teoreem 2.29 *Kui graafis G leidub tippude u ja v vahel ahel, siis leidub nende vahel ka lihtahel.*

TÕESTUS. Eeldame, et tippude u ja v vahel leidub ahel

$$u = v_0, v_1, v_2, \ldots, v_{k-1}, v_k = v.$$

Oletame, et selles ahelas esineb mingi tipp w vähemalt kaks korda. Otsime üles selle tipu esimese ja viimase esinemise ahelas:

$$v_0, v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_{j-1}, w, v_{j+1}, \ldots, v_k.$$

Siis

$$v_0, v_1, \ldots, v_{i-1}, w, v_{j+1}, \ldots, v_k.$$

on ahel, milles tipp w esineb ainult ühe korra. Analoogilise lühendamise viime läbi kõigi kordselt esinevate tippude korral. Tulemuseks on tippe u ja v ühendav lihtahel. □

Graafis võib kahe tipu vahel leiduda mitmeid ja erineva pikkusega lihtahelaid.

Definitsioon 2.30 Graafi tippude u ja v, kus $u \neq v$, vaheliseks **kauguseks** loetakse miinimumi nende tippude vaheliste lihtahelate pikkustest. Kui nende tippude vahel ahelaid ei leidu, siis loetakse kokkuleppeliselt, et u ja v vaheline kaugus on lõpmatus. Tipu kaugus iseendast on 0.

[4] ahel = *walk*
[5] lihtahel = *path*

Definitsioon 2.31 **Kinnine ahel**[6] on ahel, mille esimene ja viimane tipp langevad kokku. **Kinnise ahela pikkus** on tema servade arv.

Definitsioon 2.32 Kinnist ahelat, milles on vähemalt kolm serva ja mis ei läbi ühtegi tippu kaks korda, kutsutakse **tsükliks**[7].

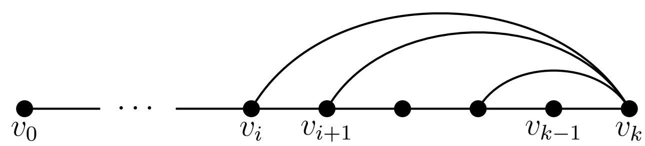
Niisiis, tsükkel on ahel $v_0, v_1, \ldots, v_{k-1}, v_0$, kus $k \geqslant 3$ ja tipud $v_0, v_1, \ldots, v_{k-1}$ on paarikaupa erinevad.

Tsükli (ja kinnise ahela) puhul ei ole oluline, millisest tipust me alustame selle kirja panemist. Seega näiteks *uvwu*, *vwuv* ja *wuvw* tähistavad ühte ja sama tsüklit.

Teoreem 2.33 *Kui $l \geqslant 2$ ja graafi iga tipu aste on vähemalt l, siis selles graafis leidub*

1. *lihtahel, mille pikkus on vähemalt l,*
2. *tsükkel, mille pikkus on vähemalt $l+1$.*

Tõestus. 1. Eeldame, et graafi G iga tipu aste on vähemalt l, kus $l \geqslant 2$. Olgu $v_0v_1\ldots v_k$ selline lihtahel graafis G, mille pikkus on maksimaalne (s.t. pikemaid lihtahelaid ei leidu). Siis tipu v_k kõik naabertipud peavad ka kuuluma sellesse ahelasse, sest muidu saaksime neid v_k järele lisades ahelat pikendada (vt. joonist). Kuna v_k naabertippe on vähemalt l, siis ka $k \geqslant l$, s.t. ahela pikkus on vähemalt l.



2. Olgu v_i selline tipu v_k naaber, mis on tipule v_0 kõige lähemal. Siis $v_iv_{i+1}\ldots v_kv_i$ on tsükkel, kusjuures tema pikkus on vähemalt $l+1$, sest ta sisaldab tippu v_k ja kõiki v_k naabertippe. □

Järeldus 2.34 *Kui graafis on servi vähemalt sama palju kui tippe, siis selles graafis leidub tsükkel.*

Tõestus. Paneme tähele, et 1- ja 2-tipulises graafis on servi vähem kui tippe. Vähim graaf, milles on servi vähemalt sama palju kui tippe, on 3-tipuline täisgraaf K_3.

Olgu nüüd $G = (V, E)$ suvaline graaf, kus $|E| \geqslant |V|$. Kustutame ühekaupa graafist isoleeritud ja rippuvaid tippe, niikaua kuni neid leidub (ka neid, mis selle protsessi käigus juurde tekivad). Selle protsessi käigus on graafil alati servi vähemalt sama palju kui tippe. Lõpuks jääb järele alamgraaf $G' = (V', E')$, kus servi on vähemalt sama palju kui tippe. Lisaks sellele $|V'| \geqslant 3$ ja G' iga tipu aste on vähemalt 2. Teoreemi 2.33 põhjal leidub graafis G' tsükkel, mille pikkus on vähemalt 3. □

Näide 2.35 Näites 2.3 vaadeldud graafis on 6 tippu ja 7 serva. Selles leidub näiteks tsükkel *uvzyu* pikkusega 4. Selles graafis veel *uvwyzvu* on kinnine ahel, mis ei ole lihtahel ega tsükkel, ning *uvwyz* on lihtahel, mis ei ole kinnine.

[6] kinnine ahel = *closed walk*
[7] tsükkel = *cycle*

2.3 Graafi sidusus

Definitsioon 2.36 Graafi nimetatakse **sidusaks**, kui selle iga kahe tipu vahel leidub ahel.

Märkus 2.37 1. Muuhulgas loetakse ka ühetipuline graaf sidusaks.

2. Sidusas graafis saab mistahes tipust liikuda servipidi mistahes teise tippu.

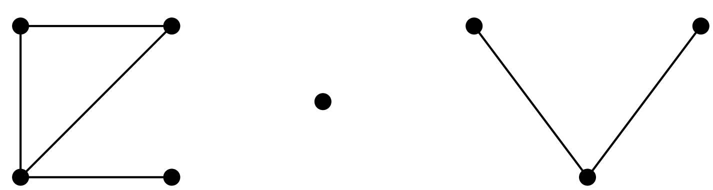
3. Kui u ja v on sidusa graafi kaks erinevat tippu, siis tänu teoreemile 2.29 leidub u ja v vahel lihtahel.

Kui graaf ei ole sidus, siis jaguneb ta sidusate alamgraafide lõikumatuks ühendiks.

Definitsioon. Graafi **sidususkomponentideks** ehk **sidusateks komponentideks** nimetatakse selle graafi maksimaalseid sidusaid alamgraafe.

Maksimaalsus selles definitsioonis tähendab seda, et mistahes tipu lisamisel antud sidusale alamgraafile saame mittesidusa alamgraafi. Graaf on sidus parajasti siis, kui tal on üks sidususkomponent.

Näide 2.38 Järgmisel graafil on kolm sidususkomponenti:

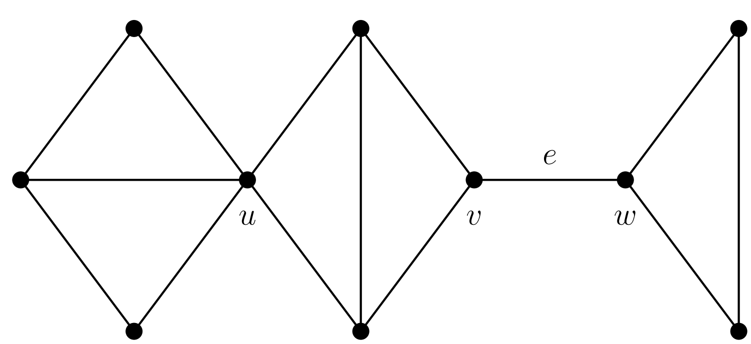


Definitsioon 2.39 Graafi serva nimetatakse **sillaks**, kui tema eemaldamisel graafist sidususkomponentide arv suureneb.

On selge, et serv uv on sild parajasti siis, kui pärast tema eemaldamist on otstipud u ja v erinevates sidususkomponentides.

Definitsioon 2.40 Kui tipu u ja temaga intsidentsete servade eemaldamisel graafi sidususkomponentide arv suureneb, siis öeldakse, et u on **eraldav tipp**.

Näide 2.41 Graafis



on üks sild e ja kolm eraldavat tippu u, v ja w.

Teoreem 2.42 *Graafi serv on sild parajasti siis, kui ta ei kuulu ühessegi tsüklisse.*

TÕESTUS. TARVILIKKUS. Olgu serv uv sild. Oletame vastuväiteliselt, et leidub tsükkel C, mis sisaldab serva uv. Siis serva uv eemaldamisel on ikkagi võimalik tsükli C ülejäänud servi pidi liikuda tipust u tippu v. Seega u ja v on uues graafis samas sidususkomponendis, mis on vastuolus sellega, et uv oli sild. Järelikult uv ei kuulu tsüklitesse.
PIISAVUS. Eeldame, et serv uv ei sisaldu üheski tsüklis. Siis iga ahel tipust u tippu v peab sisaldama serva uv, sest muidu sellele ahelale serva uv lisades saaksime kinnise ahela, millest saab välja eraldada tsükli kasutades samasugust mõttekäiku nagu teoreemi 2.29 tõestuses. Kui nüüd serv uv eemaldada, siis ei jää enam ühtegi ahelat u ja v vahele. Seega u ja v on erinevates sidususkomponentides ning järelikult on serv uv sild. □

Teoreem 2.43 *Kui n-tipulisel graafil on m serva ja k sidususkomponenti, siis kehtivad võrratused*

$$n-k \leqslant m \leqslant \frac{(n-k)(n-k+1)}{2}.$$

TÕESTUS. 1. Tõestame võrratuse $n-k \leqslant m$. Teeme seda induktsiooniga graafi servade arvu järgi.
Alus. Olgu $m=0$. Siis on tegemist nullgraafiga O_n, milles sidususkomponente on n tükki. Võrratus on kujul $n-n \leqslant 0$ ja see kehtib.
Samm. Olgu $m>0$, olgu graafis G n tippu ja k sidususkomponenti ning eeldame, et väide kehtib kõigi graafide korral, kus on vähem kui m serva. Valime graafis G välja ühe serva e (see leidub, sest $m>0$) ning kustutame selle ära, nii et tulemuseks saadav graaf on G'. On kaks võimalust.

a) e on sild. Siis graafis G' on $m-1$ serva ja $k+1$ sidususkomponenti. Kasutades induktsiooni eeldust G' jaoks saame võrratuse $n-(k+1) \leqslant m-1$, kust $n-k \leqslant m$.

b) e ei ole sild. Siis graafis G' on $m-1$ serva ja k sidususkomponenti ning induktsiooni eelduse põhjal $n-k \leqslant m-1$. Siis aga ka $n-k \leqslant m$.

2. Tõestame võrratuse

$$m \leqslant \frac{(n-k)(n-k+1)}{2}.$$

Selleks uurime, mitu serva saab maksimaalselt olla n-tipulisel graafil k sidususkomponendiga. Ilmselt peavad kõik sidususkomponendid olema täisgraafid. Kui võtame kõige väiksema tippude arvuga sidususkomponendist ühe tipu koos intsidentsete servadega ära ja lisame kõige suurema tippude arvuga komponenti ühe tipu juurde koos servadega kõigisse teistesse selle komponendi tippudesse, siis saadud graafis ei ole vähem servi kui esialgses. Korrates seda protsessi jõuame lõpuks graafini, milles on

1. $k-1$ ühetipulist sidususkomponenti,

2. üks $(n-k+1)$-tipuline täisgraafist sidususkomponent.

Vastavalt märkusele 2.10 on sellises graafis servi

$$\frac{(n-k+1)(n-k+1-1)}{2} = \frac{(n-k)(n-k+1)}{2}.$$

□

Järeldus 2.44 *Kui n-tipulisel graafil on vähem kui $n-1$ serva, siis see graaf on mittesidus.*

TÕESTUS. Olgu n-tipulisel graafil k sidususkomponenti ja m serva, kusjuures $m < n-1$. Teoreemi 2.42 põhjal $n-k \leqslant m < n-1$, kust $1 < k$. Kuna sidususkomponente on rohkem kui 1, siis on graaf mittesidus. □

Järeldus 2.45 *Kui n-tipulisel graafil on rohkem kui $(n-1)(n-2)/2$ serva, siis see graaf on sidus.*

TÕESTUS. Kui $n = 1$, siis graaf on sidus. Kui $n = 2$, siis peab graafil olema rohkem kui 0 serva ja seega on ta sidus. Edasises eeldame, et $n \geqslant 3$. Kui servade arv on m ja $m > \frac{(n-1)(n-2)}{2}$, siis teoreemi 2.43 tõttu

$$\frac{(n-1)(n-2)}{2} < \frac{(n-k)(n-k+1)}{2}.$$

Järelikult

$$n^2 - 3n + 2 < n^2 - kn + n - kn + k^2 - k,$$

kust

$$k^2 - (2n+1)k + 4n - 2 > 0.$$

Vaadeldes seda ruutvõrratusena k suhtes ja leides vastava ruutvõrrandi lahendid 2 ja $2n-1$ saame võrratuse

$$(k-2)(k-2n+1) > 0.$$

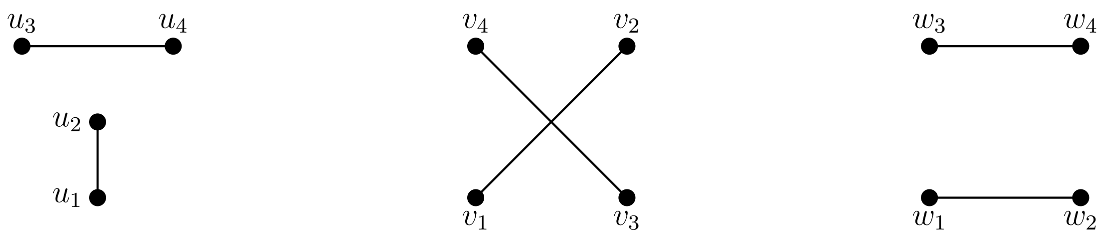
Arvestades seda, et $2 < 2n-1$ (sest $n \geqslant 3$) ja ruutparabooli omadusi peab $k < 2$ või $k > 2n-1$. Kui $k > 2n-1$, siis $k > n+n-1 > n$, mis ei ole võimalik (sidususkomponente ei saa olla rohkem kui tippe). Seega $k < 2$ ehk $k = 1$. Seda oligi tarvis tõestada. □

2.4 Graafide isomorfism

Definitsioon 2.46 Graafe $G = (V, E)$ ja $G' = (V', E')$ nimetatakse **isomorfseteks**, kui leidub selline bijektiivne kujutus $\varphi : V \to V'$, et

$$uv \in E \text{ parajasti siis, kui } \varphi(u)\varphi(v) \in E'.$$

Näide 2.47 Graafid



on omavahel isomorfsed.

Graafide isomorfismi kontrollimiseks tuleb konstrueerida üks sobiv kujutus tipuhulkade vahel. Kui on vaja näidata, et kaks graafi ei ole isomorfsed, siis harilikult näidatakse, et ühel graafidest on mingi omadus, mis isomorfismi all säilib, aga teisel seda ei ole. (Selliseid omadusi nimetatakse mõnikord **invariantideks**.) Toome siin kaks näidet sellistest omadusest.

Lause 2.48 *Kui kaks graafi on isomorfsed, siis on neil sama palju servi.*

TÕESTUS. Olgu φ isomorfism graafide $G = (V, E)$ ja $G' = (V', E')$ vahel. Siis võime vaadelda kujutust $\psi : E \to E'$, mis on defineeritud võrdusega

$$\psi(uv) = \varphi(u)\varphi(v)$$

iga $uv \in E$ korral. Näitame, et ψ on injektiivne. Selleks oletame, et $\psi(uv) = \psi(u'v')$. Siis $\varphi(u)\varphi(v) = \varphi(u')\varphi(v')$ ehk $\{\varphi(u), \varphi(v)\} = \{\varphi(u'), \varphi(v')\}$. On kaks võimalust.
a) $\varphi(u) = \varphi(u')$ ja $\varphi(v) = \varphi(v')$. Siis φ injektiivsuse tõttu $u = u'$ ja $v = v'$, kust $uv = u'v'$.
b) $\varphi(u) = \varphi(v')$ ja $\varphi(v) = \varphi(u')$. Siis $u = v'$ ja $v = u'$, kust $uv = v'u' = u'v'$.
Sellega on näidatud, et ψ on injektiivne.

Veendume, et ψ on sürjektiivne. Olgu $xy \in E'$. Tänu φ sürjektiivsusele leiduvad tipud $u, v \in V$ nii, et $x = \varphi(u)$ ja $y = \varphi(v)$. Kuna $\varphi(u)\varphi(v) \in E'$, siis $uv \in E$. Järelikult $\psi(uv) = \varphi(u)\varphi(v) = xy$. See tähendab, et ψ on sürjektiivne.

Kuna kujutus ψ on bijektiivne, siis on graafides G ja G' sama palju servi. $\square$

Lause 2.49 *Kui graafid $G = (V, E)$ ja $G' = (V', E')$ on isomorfsed ja graafis G leidub tipp, mille aste on r, siis ka graafis G' leidub tipp, mille aste on r.*

TÕESTUS. Olgu $v \in V$ ja $d(v) = r$. Eelduse põhjal leidub isomorfism φ graafist G graafi G'. Kui v naabertipud on $v_1, \ldots, v_r$, siis $\varphi(v)\varphi(v_1), \ldots, \varphi(v)\varphi(v_r) \in E'$. Tänu φ injektiivsusele on tipud $\varphi(v_1), \ldots, \varphi(v_r) \in V'$ paarikaupa erinevad. Seega $d(\varphi(v)) \geqslant r$.

Kui oletada, et veel ka $\varphi(v)x \in E'$, kus $x \in V'$ ja $x \notin \{\varphi(v_1), \ldots, \varphi(v_r)\}$, siis tänu φ sürjektiivsusele leidub tipp $v_0 \in V$ nii, et $x = \varphi(v_0)$. Kuna $\varphi(v)\varphi(v_0) \in E'$, siis ka $vv_0 \in E$. Järelikult leidub selline $i \in \{1, \ldots, r\}$, et $v_0 = v_i$. Siis aga $x = \varphi(v_0) = \varphi(v_i) \in \{\varphi(v_1), \ldots, \varphi(v_r)\}$, vastuolu. Sellega oleme näidanud, et $\varphi(v)$ ainsad naabertipud graafis G' on $\varphi(v_1), \ldots, \varphi(v_r)$. Järelikult $d(\varphi(v)) = r$. □

Näide 2.50 Graafid

ei ole isomorfsed, sest teises graafis leidub tipp astmega 1, aga esimeses mitte.

Lisaks kahele tõestatud lausele saab veel näidata, et isomorfsetel graafidel on

- sama palju sidususkomponente,
- samasugune tipuastmete mittekasvav järjend,
- sama lühima tsükli pikkus,
- sama pikima tsükli pikkus,
- jne.

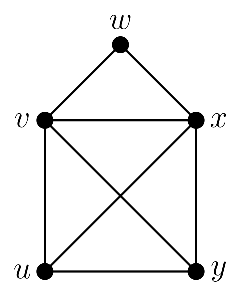
2.5 Euleri ja Hamiltoni graafid

Definitsioon 2.51 **Euleri ahel** on ahel, mis sisaldab graafi iga serva täpselt ühe korra. **Kinnine Euleri ahel** on Euleri ahel, mille esimene ja viimane tipp langevad kokku.

Definitsioon 2.52 **Euleri graaf** on sidus graaf, milles leidub kinnine Euleri ahel.

Märkus 2.53 "Kinnise Euleri ahela" asemel öeldakse mõnikord "Euleri tsükkel". Selle kursuse terminoloogias ei pruugi Euleri tsükkel olla tsükkel, sest selles võivad tipud korduda. Seetõttu me väldime termini "Euleri tsükkel" kasutamist.

Näide 2.54 Graafis



leidub Euleri ahel $uvyuxvwxy$.

Euleri ahela leidmise vajadus tekib praktikas näiteks siis, kui on vaja lumest puhastada teed mingis piirkonnas või laiali kanda post mingis linnas nii, et iga tänavat läbitaks üks kord.

Millistes graafides leidub kinnine Euleri ahel? Sellele küsimusele annab vastuse järgmine teoreem.

Teoreem 2.55 *Graaf on Euleri graaf parajasti siis, kui ta on sidus ja tema iga tipu aste on paarisarv.*

TÕESTUS. TARVILIKKUS. Olgu G Euleri graaf. Siis ta on sidus ja sisaldab kinnist Euleri ahelat. Olgu v selle graafi suvaline tipp. Iga kord kui ahel läbib seda tippu, kasutab ta ära kaks selle tipuga intsidentset serva (ühe sisenemiseks, teise väljumiseks). Et ahel saaks ära kasutada kõik tipu v juures olevad servad, peab tipu v aste olema paarisarv.

PIISAVUS. Tõestame, et kui sidusa graafi tippude astmed on paarisarvud, siis on see graaf Euleri graaf. Teeme seda induktsiooniga graafi servade arvu järgi.

Induktsiooni alus. Vaatleme juhtu, kus graafis on 0 serva. Sidususe tõttu tähendab see, et graafis on üksainus tipp v ja sobivaks kinniseks Euleri ahelaks on sellest ainsast tipust koosnev ahel, milles on 0 serva.

Induktsiooni samm. Olgu $G = (V, E)$ sidus graaf, mille tippude astmed on paarisarvud, ning olgu $|E| > 0$. Eeldame, et tõestatav väide kehtib kõigi graafide puhul, mille servade arv on väiksem kui $|E|$.

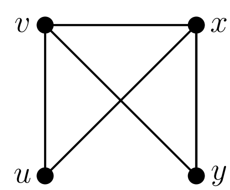
Graafi G ühegi tipu aste ei ole 0, sest muidu poleks ta sidus. Seega iga tipu aste on vähemalt 2. Teoreemi 2.33 põhjal sisaldab G mingit tsüklit C. Kui C sisaldab kõiki graafi G servi, siis ongi ta ise kinnine Euleri ahel ja tõestus on lõppenud.

Vastasel juhul vaatleme graafi G alamgraafi $G' = (V, E')$, mis on saadud kõigi tsüklisse C kuuluvate servade kustutamisel. Graafis G' on vähem servi kui graafis G. Samuti on G' kõigi tippude astmed paarisarvud, sest kustutades tsüklisse C kuuluvaid servi vähendame G iga tipu astet 0 või 2 võrra. Graaf G' ei pruugi olla sidus, küll aga on seda tema sidususkomponendid. Induktsiooni eelduse põhjal leidub G' iga sidususkomponendi jaoks kinnine Euleri ahel.

Konstrueerime nüüd G jaoks kinnise Euleri ahela järgmiselt. Hakkame liikuma mööda tsükli C servi. Kui jõuame tipuni v_1, mille aste graafis G' ei ole 0 (s.t. mille aste graafis G on vähemalt 4), siis läbime tippu v_1 sisaldavas G' sidususkomponendis leiduva kinnise Euleri ahela ning jõuame lõpuks tippu v_1 tagasi. Siis jätkame tsükli C läbimist kohast, kus see pooleli jäi, kuni jõuame järgmise tipuni v_2, mille juures on veel läbimata G' servi. Tippu v_2 sisaldavas G' sidususkomponendis läbime jällegi Euleri ahela ja jõuame tagasi tippu v_2. Protseduuri korrates läbime niimoodi tsükli C. Tulemuseks on kinnine Euleri ahel G jaoks. □

Definitsioon 2.56 Tsüklit, mis läbib graafi kõiki tippe täpselt ühe korra, nimetatakse **Hamiltoni[8] tsükliks**. **Hamiltoni graaf** on graaf, milles leidub Hamiltoni tsükkel.

Näide 2.57 Graafis



leidub Hamiltoni tsükkel $vuxyv$. Seega on tegemist Hamiltoni graafiga.

Järgmine, Diraci[9] poolt tõestatud teoreem annab piisava tingimuse Hamiltoni tsükli leidumiseks.

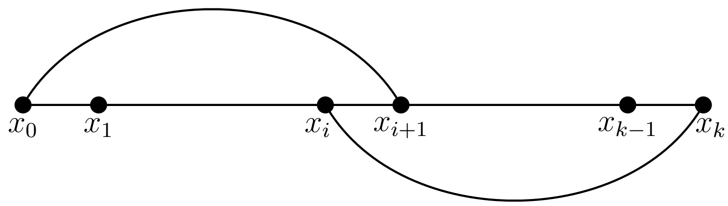
Teoreem 2.58 (Diraci teoreem) *Olgu G n-tipuline graaf, kus $n \geqslant 3$ ja iga tipu aste on vähemalt $\frac{n}{2}$. Siis G on Hamiltoni graaf.*

TÕESTUS. Rahuldagu graaf $G = (V, E)$ teoreemi eeldusi. Oletame, et G ei ole sidus. Siis on temas vähemalt kaks sidususkomponenti ja minimaalse tippude arvuga sidususkomponendis on tippude arv $\leqslant \frac{n}{2}$, mistõttu iga tipu aste on $< \frac{n}{2}$. See on vastuolus eeldusega. Järelikult G on sidus graaf.

Olgu $P = x_0x_1 \dots x_k$ maksimaalse pikkusega lihtahel graafis G (s.t. pikemaid lihtahelaid ei leidu). Siis kõik x_0 naabertipud ja kõik x_k naabertipud asuvad ahelal P, sest muidu saaksime ahelat pikendada. Seega $x_0, \dots, x_{k-1}$ hulgas on vähemalt $\frac{n}{2}$ tipu x_k naabertippu ja $x_1, \dots, x_k$ hulgas on vähemalt $\frac{n}{2}$ tipu x_0 naabertippu. Näitame, et

$$(\exists i \in \{0, 1, \dots, k-1\})(x_i x_k \in E \text{ ja } x_0 x_{i+1} \in E).$$

[8]William Rowan Hamilton (1805–1865) — iiri matemaatik, astronoom ja füüsik
[9] Gabriel Andrew Dirac (1925–1984) — ungari-briti matemaatik



Oletame vastuväiteliselt, et see tingimus ei kehti. Siis leidub ahelal P vähemalt $d(x_0)$ tippu, mis ei ole x_k naabrid (need on x_0 naabritele eelnevad tipud ja võib-olla veel mõned tipud). Lisaks sellele on ahelal P kõik $d(x_k)$ tipu x_k naabrit ja tipp x_k ise ka. Seega peaks ahelal olema vähemalt $d(x_0) + d(x_k) + 1$ tippu. Aga

$$d(x_0) + d(x_k) + 1 \geqslant \frac{n}{2} + \frac{n}{2} + 1 = n + 1,$$

mis ei ole võimalik, sest graafil on n tippu ja ahela P tipud on kõik erinevad.

Vaatleme nüüd tsüklit

$$C = x_0 x_{i+1} x_{i+2} \ldots x_{k-1} x_k x_i x_{i-1} \ldots x_1 x_0.$$

Paneme tähele, et selles tsüklis on $k+1$ tippu $(x_0, x_1, \ldots, x_k)$ ja seega ka $k+1$ serva. Oletame, et see ei ole Hamiltoni tsükkel. Siis hulk $V \setminus \{x_0, \ldots, x_k\}$ on mittetühi. Kuna G on sidus, siis hulgas $V \setminus \{x_0, \ldots, x_k\}$ peab leiduma mingi tipp v, mis on serva abil ühendatud mingi tipuga x_j, kus $j \in \{0, 1, \ldots, k\}$. Siis aga läbides serva vx_j ning seejärel alustades tipust x_j kõik tsükli C servad peale viimase saaksime lihtahela pikkusega $k+1$. See on vastuolus P maksimaalsusega. Järelikult C peab sisaldama kõiki G tippe ja olema Hamiltoni tsükkel. □

Hamiltoni tsüklid on seotud järgmise tuntud matemaatilise probleemiga.

Rändkaupmehe ülesanne. *On antud n linna koos nende vahel eksisteerivate teede ja nende pikkustega. Leida lühim marsruut, mis läbib kõiki linnu täpselt ühe korra ja jõuab alguspunkti tagasi.*

Sellise ülesande lahendamiseks vaadeldakse graafi, mille tippudeks on linnad, servadeks nendevahelised teed ja igale servale on omistatud kaal, mida väljendab vastava tee pikkus. Ülesande lahendamiseks tuleb leida selles graafis Hamiltoni tsükkel, mille puhul on servade kaalude summa vähim. Arvutuslikult loetakse selline ülesanne raskeks.

2.6 Puud

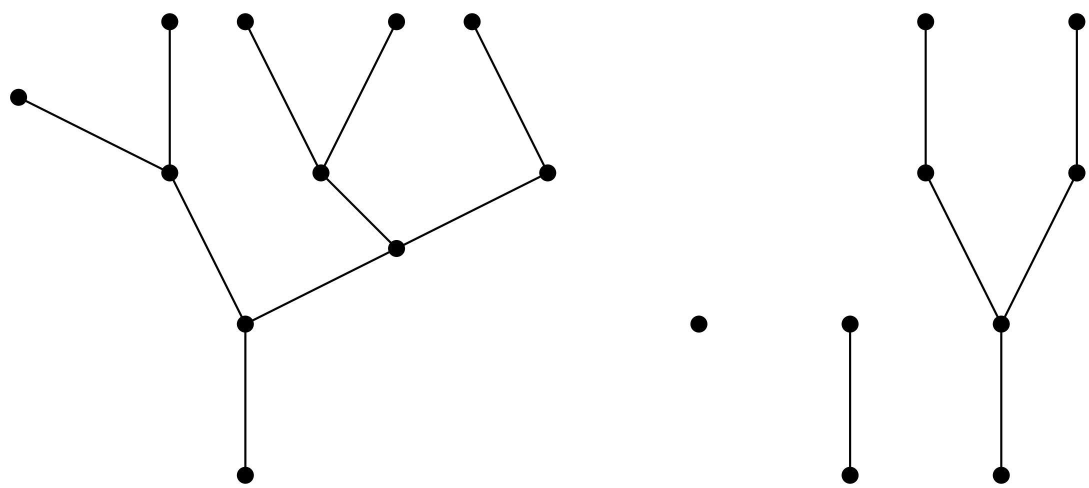
2.6.1 Puude põhiomadused

Puud moodustavad ühe olulise graafide klassi, millel on iseäranis palju rakendusi arvutiteaduses (näiteks andmestruktuuridena).

Definitsioon 2.59 Graafi nimetatakse **puuks**, kui ta on sidus ja ei sisalda tsükleid.

Definitsioon 2.60 **Mets** on graaf, mille kõik sidususkomponendid on puud.

Näide 2.61 Järgneval joonisel on mets, mis koosneb neljast puust:



Meenutame, et rippuvad tipud on need, mille aste on 1.

Definitsioon 2.62 Puu rippuvaid tippe nimetatakse **lehtedeks** ja mitterippuvaid tippe nimetatakse **sisetippudeks**.

Teoreem 2.63 *Vähemalt kahetipulisel puul on vähemalt kaks lehte.*

TÕESTUS. Olgu meil antud n-tipuline puu, kus $n \geqslant 2$. Valime graafis välja suvalise tipu, olgu see v_1, ja hakkame sellest tipust servi mööda liikuma nii, et me ei läbiks ühtegi tippu kaks korda. Tekkiv lihtahel peab kindlasti lõppema tipus, mille aste on 1. Kui see nii ei oleks, siis jõuaksime mingil sammul tipuni v_k, millest ei leidu enam serva ühtegi läbimata tippu, aga mille aste on vähemalt 2. Järelikult peab tipust v_k leiduma serv juba mõnda läbitud tippu v_i, kus $i \neq k-1$. See aga tähendab, et graaf sisaldab tsüklit, mis on vastuolus eeldusega. Seega graafis leidub vähemalt üks tipp v, mille aste on üks.

Võtame nüüd tipu v ja korrates sama mõttekäiku konstrueerime lihtahela alates temast. Ka see peab lõppema mingis tipus u, mille aste on 1. Järelikult on graafis vähemalt kaks lehte. □

Leidub kuitahes suure tippude arvuga puid, millel ongi ainult kaks lehte, nendeks on n-tipulised ahelad.

Teoreem 2.64 *Igal n-tipulisel puul on $n-1$ serva.*

Seda teoreemi on võimalik tõestada vähemalt kahel viisil. Annamegi siin kaks erinevat tõestust.

TÕESTUS. Järelduse 2.44 põhjal ei saa puul olla vähem kui $n-1$ serva. Järelduse 2.34 tõttu ei saa puul olla rohkem kui $n-1$ serva. Seega peab puul olema $n-1$ serva. □

TÕESTUS. Tõestame väite induktsiooniga puu tippude arvu järgi.
Alus. Kui $n = 1$, siis on tegemist puuga, mille servade arv on 0.
Samm. Eeldame, et väide kehtib kõigi puude korral, millel on k tippu. Olgu G puu, millel on $k+1$ tippu ($k \geqslant 1$). Kuna graafil G on vähemalt kaks tippu, siis teoreemi 2.63 põhjal leidub tal leht. Kustutame selle ära koos intsidentse servaga. Järele jäävale k-tipulisele graafile saame rakendada induktsiooni eeldust, seega on temas $k-1$ serva. Järelikult graafis G on k serva. □

Teoreem 2.65 *Graafi G puhul on järgmised väited samaväärsed:*

1. *G on puu;*
2. *G on sidus, kuid ükskõik millise serva kustutamisel muutub mittesidusaks;*
3. *G ei sisalda tsükleid, kuid ükskõik millise serva lisamisel tekib tsükkel.*

TÕESTUS. $1 \Rightarrow 2$. Eeldame, et G on puu. Siis on ta definitsiooni tõttu sidus. Oletame vastuväiteliselt, et mingi serva e kustutamise järel jääb G sidusaks. Siis serv e ei ole sild. Teoreemi 2.42 põhjal kuulub e mingisse tsüklisse. See on aga vastuolus eeldusega. Järelikult pärast mistahes serva kustutamist muutub G mittesidusaks.

$2 \Rightarrow 3$. Eeldame, et G rahuldab tingimust 2. Oletame, et G sisaldab mingit tsüklit. Siis sellest tsüklist ühe serva kustutamisel sidusus ei kao, mis on vastuolus eeldusega. Järelikult G ei saa sisaldada tsükleid.

Olgu u ja v graafi G suvalised tipud, mille vahel pole serva (seega nende vahele on võimalik serva lisada). Sidususe tõttu peab leiduma lihtahel tippude u ja v vahel. Siis serva uv lisamisel tekib tsükkel.

$3 \Rightarrow 1$. Eeldame, et G rahuldab tingimust 3. Siis ta ei sisalda tsükleid. Oletame vastuväiteliselt, et G ei ole sidus. Siis leiduvad tipud u ja v, mis asuvad erinevates sidususkomponentides. Serva uv lisamisel tsüklit tekkida ei saa, mis on vastuolus eeldusega. Järelikult G peab olema sidus. Sidusa tsükliteta graafina on ta puu. □

Järeldus 2.66 *Graafi G puhul, millel on n tippu ja m serva, on järgmised väited samaväärsed:*

1. *G on puu;*
2. *G on sidus ja $m \leqslant n-1$;*
3. *G ei sisalda tsükleid ja $m \geqslant n-1$.*

TÕESTUS. Kui G on puu, siis teoreemi 2.64 põhjal $m = n - 1$. Seega $1 \Rightarrow 2$ ja $1 \Rightarrow 3$.

$2 \Rightarrow 1$. Eeldame, et G on sidus ja $m \leqslant n-1$. Siis järelduse 2.44 põhjal saame mistahes serva kustutamisel mittesidusa graafi. Kuna G rahuldab teoreemi 2.65 tingimust 2, siis peab ta olema puu.

$3 \Rightarrow 1$. Eeldame, et G ei sisalda tsükleid ja $m \geqslant n - 1$. Siis mistahes serva lisamisel saame graafi, milles on servi vähemalt sama palju kui tippe. Vastavalt järeldusele 2.34 peab selline graaf sisaldama tsüklit. Kuna G rahuldab teoreemi 2.65 tingimust 3, siis peab ta olema puu. □

Teoreem 2.67 *Graaf G on puu parajasti siis, kui tema iga kahte erinevat tippu ühendab täpselt üks lihtahel.*

TÕESTUS. TARVILIKKUS. Olgu G puu ja u, v selle kaks erinevat tippu. Sidususe tõttu leidub u ja v vahel vähemalt üks lihtahel. Oletame vastuväiteliselt, et leidub kaks erinevat lihtahelat u ja v vahel:

$$u = x_0, x_1, \ldots, x_{k-1}, x_k = v,$$
$$u = y_0, y_1, \ldots, y_{l-1}, y_l = v.$$

Tõestuse lõpetamiseks näitame, et graafis G leidub tsükkel, mis annab vastuolu eeldusega, et G on puu.

Olgu r suurim indeks, mille korral

$$x_0 = y_0, x_1 = y_1, \ldots, x_r = y_r$$

ning olgu

$$m = \min(k, l).$$

Veendume, et $r < m$. On selge, et $r \leqslant m$. Oletame vastuväiteliselt, et $r = m$. Siis on kolm võimalust.

1. $m = k$ ja $l > k$. Siis peame teist ahelat pidi tipust $y_k = x_k = v$ edasi liikuma ja lõpuks jõudma uuesti tagasi tippu $y_l = v$. Seega tipp v esineb teises ahelas kaks korda, mis on vastuolus eeldusega, et tegemist on lihtahelaga.

2. $m = l$ ja $k > l$. See juhtum annab vastuolu analoogiliselt eelmisega.

3. $m = k = l$. Sellisel juhul vaadeldavad ahelad ei ole erinevad, mis on vastuolus eeldusega.

Niisiis $r < m$. See tähendab, et tipud x_{r+1} ja y_{r+1} on erinevad. Liigume nüüd tipust x_r alustades mööda esimest ahelat, kuni jõuame esimese tipuni, mis asub ka teisel ahelal (varem või hiljem peab see juhtuma, sest ahelad lõpevad samas tipus v). Tollest tipust liigume teist ahelat pidi tagasi tippu x_r. Nii oleme saanud tsükli, sest

a) meie kinnine ahel sisaldab vähemalt kolme erinevat tippu (x_r, x_{r+1} ja y_{r+1}) ning seega ka vähemalt kolme serva,

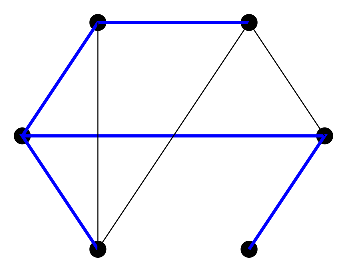
b) vastavalt konstruktsioonile me ei läbi ühtegi tippu kaks korda.

Piisavus. Eeldame, et graafi G iga kahte erinevat tippu ühendab täpselt üks lihtahel. Siis G on sidus. Oletame vastuväiteliselt, et graafis G leidub tsükkel ja valime selles tsüklis välja ühe serva uv. Siis tippe u ja v ühendab vähemalt kaks lihtahelat: servast uv koosnev lihtahel ja tsükli ülejäänud osast koosnev lihtahel. See on vastuolus eeldusega ning järelikult G ei saa sisaldada tsükleid. Seega on ta puu. □

2.6.2 Toespuud

Definitsioon 2.68 Sidusa graafi **toespuuks**[10] ehk **aluspuuks** nimetatakse sellist alamgraafi, mis sisaldab kõiki tippe ja on puu.

Näide 2.69 Järgneval joonisel on üks graaf ja selle toespuu (toespuu servad on joonistatud paksema sinise joonega):



Lause 2.70 *Igal sidusal graafil leidub toespuu.*

Tõestus. Olgu G sidus graaf. Hakkame ühekaupa kustutama selle graafi servi nii, et graaf ei kaotaks sidusust. Selle protsessi lõpuks jääb meile alles alamgraaf T, mis

- sisaldab kõiki G tippe,
- on sidus,
- ükskõik millise serva kustutamisel muutub mittesidusaks.

Vastavalt teoreemile 2.65 on T puu ja vastavalt definitsioonile 2.68 on ta graafi G toespuu. □

Igal puul on ainult üks toespuu — see on ta ise. Kui sidus graaf ei ole puu, siis on tal mitu toespuud.

Toespuude leidmine on tihti kasulik sellises olukorras, kus graaf on kaalutud. Kaalutud graafi all peetakse silmas sellist graafi, mille igale servale on omistatud nn. kaal, mida väljendatakse harilikult positiivse reaalarvu abil. Formaalselt võib kaalutud graafi defineerida järgmiselt.

Definitsioon 2.71 **Kaalutud graafiks** nimetatakse kolmikut (V, E, ω), kus (V, E) on graaf ja $\omega : E \to \mathbb{R}^+$ on kujutus. Positiivset reaalarvu $\omega(e)$ nimetatakse serva e **kaaluks**.

[10]toespuu = *spanning tree*

Tüüpiline näide kaalutud graafist on maanteede kaart, kus tippudeks on linnad, servadeks linnade vahelised maanteed ja servade kaaludeks teede pikkused.

Definitsioon 2.72 Kaalutud graafi G toespuu T **kaaluks** $\omega(T)$ loetakse tema servade kaalude summat. Öeldakse, et graafi G toespuu T on **minimaalse kaaluga**, kui G iga toespuu T' korral $\omega(T) \leqslant \omega(T')$.

Näide 2.73 Oletame, et riik tahab ehitada välja valguskaablivõrgu, mis jõuaks iga Eesti linna, alevi ja alevikuni. Võime vaadelda graafi, mille tippudeks on asulad, servaga on ühendatud need asulad, mille vahele on põhimõtteliselt võimalik mõistliku kuluga kaabel paigaldada, ja serva kaaluks on vastava kahe asula vahele kaabli paigaldamise maksumus eurodes. Minimaalse kaaluga toespuu annab kõige odavama ehituskuluga võrgu.

Analoogiline ülesande püstitus tekib siis, kui on vaja välja ehitada elektri kõrgepingeliinid, veevõrgud või kanalisatsioonitrassid.

Hulgaliselt näiteid toespuude rakenduste kohta võib leida ingliskeelse Vikipeedia artiklist *Minimum spanning tree*.

Igal sidusal kaalutud graafil leidub minimaalse kaaluga toespuu. Kuna vaadeldavad graafid on lõplikud, siis võime antud graafi puhul leida kõik tema toespuud, arvutada välja kõigi toespuude kaalud ja leida kaalude hulgast minimaalse. Selliseid minimaalse kaaluga toespuid võib graafil olla mitu.

Graafi kõigi toespuude leidmine on väga töömahukas ja arvutuslikult ebaefektiivne. Õnneks on olemas ka paremaid algoritme. Selles paragrahvis toome ära kaks algoritmi antud sidusa kaalutud graafi minimaalse kaaluga toespuu leidmiseks. Esimese neist pakkus välja Joseph Kruskal[11] 1956. aastal.

Kruskali algoritm.

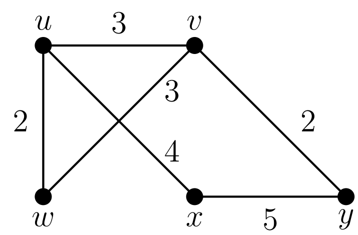
Antud: n-tipuline sidus kaalutud graaf $G = (V, E, \omega)$.
Leida: minimaalse kaaluga toespuu.
Idee: lisame minimaalse kaaluga servi nii, et ei tekiks tsükleid.

1. Vali servaks e_1 graafi G minimaalse kaaluga serv.
2. Iga $i = 2, 3, \ldots, n-1$ korral vali servaks e_i graafi G minimaalse kaaluga serv, mis erineb servadest $e_1, \ldots, e_{i-1}$ ja ei moodusta koos servadega $e_1, \ldots, e_{i-1}$ tsüklit.
3. Tagasta graaf $T = (V, \{e_1, e_2, \ldots, e_{n-1}\})$.

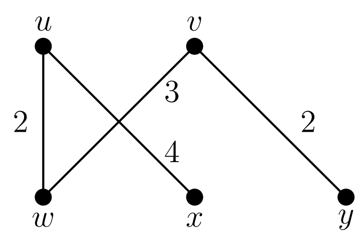
Märkus 2.74 Lause "Serv e_i koos servadega $e_1, \ldots, e_{i-1}$ ei moodusta tsüklit" all mõistame seda, et G alamgraaf, mis koosneb servadest $e_1, \ldots, e_{i-1}, e_i$ ja nende otstippudest, ei sisalda ühtegi tsüklit.

[11] Joseph Kruskal (1928–2010) — ameerika matemaatik

Näide 2.75 Leiame kaalutud graafi



minimaalse kaaluga toespuu Kruskali algoritmi abil. Esimesel sammul valime minimaalse kaaluga serva uw. Järgnevatel sammudel valime servad vy, vw, ux. Tulemuseks on toespuu



Näitame, et Kruskali algoritm töötab korrektselt.

Teoreem 2.76 *Kui G on sidus kaalutud graaf, siis Kruskali algoritm leiab graafi G minimaalse kaaluga toespuu.*

TÕESTUS. Kõigepealt veendume, et sammul 2 on tõesti alati võimalik valida serv e_i, mis erineb servadest $e_1, \ldots, e_{i-1}$ ja ei moodusta koos nendega tsüklit. Selleks vaatleme graafi G alamgraafi $G' = (V, \{e_1, \ldots, e_{i-1}\})$. Graafis G' on n tippu ja vähem kui $n-1$ serva ($i-1 < n-1$). Vastavalt järeldusele 2.44 on graaf G' mittesidus. Järelikult peab tal leiduma vähemalt kaks sidususkomponenti. Võtame kaks tippu u ja v, mis asuvad G' erinevates sidususkomponentides. Kuna G on sidus, siis peab graafis G leiduma ahel u ja v vahel. See ahel peab sisaldama vähemalt ühte serva e_i, mille otstipud on erinevates komponentides. Selline serv e_i ei saa langeda kokku ühegagi servadest $e_1, \ldots, e_{i-1}$ ja samuti ei saa ta koos servadega $e_1, \ldots, e_{i-1}$ moodustada tsüklit.

Olgu graafi G alamgraaf $T = (V, \{e_1, e_2, \ldots, e_{n-1}\})$ leitud Kruskali algoritmi abil. Kuna T ei sisalda tsükleid ja tema servade arv on $n-1$, siis järelduse 2.66 põhjal on T puu. Et ta sisaldab kõiki G tippe, siis on tegemist G toespuuga. Tuleb veel näidata, et T on minimaalse kaaluga toespuude hulgas.

Oletame vastuväiteliselt, et T ei ole minimaalse kaaluga toespuu. Siis leidub toespuid, mille kaal on väiksem kui puul T. Olgu T' graafi G toespuu, mis

- on minimaalse kaaluga ja
- omab minimaalse kaaluga toespuude hulgas puuga T maksimaalset arvu ühiseid servi.

Siis $\omega(T') < \omega(T)$ ning järelikult ka $T' \neq T$. Olgu $k \in \{1, \dots, n-1\}$ vähim arv, mille korral serv e_k ei kuulu puusse T' (see leidub, sest $T' \neq T$). Olgu S graafi G alamgraaf, mis saadakse serva e_k lisamisel puule T'. Siis vastavalt teoreemile 2.65 peab S sisaldama mingit tsüklit C. See tsükkel C peab sisaldama serva e_k, kuid ta peab sisaldama ka mingit serva e, mis ei kuulu puusse T (sest vastasel korral sisaldaks puu T tsüklit C). Kustutame graafist S serva e ja tähistame saadud graafi T''. Siis T'' on ka G toespuu, sest ta on sidus ja temas on $n-1$ serva (vt. järeldust 2.66).

Vastavalt k valikule kuuluvad servad $e_1, \dots, e_{k-1}$ ka puusse T'. Serv e

- ei ole võrdne ühegagi servadest $e_1, \dots, e_{k-1}$ (sest e ei kuulu puusse T) ja
- ei moodusta koos servadega $e_1, \dots, e_{k-1}$ tsükleid (sest T' on puu ja $e_1, \dots, e_{k-1}, e$ on tema servade hulgas).

Vastavalt serva e_k konstruktsioonile Kruskali algoritmis peab $\omega(e_k) \leqslant \omega(e)$. Kuna T'' on saadud puust T' serva e_k lisamisel ja serva e kustutamisel, siis $\omega(T'') \leqslant \omega(T')$. Et T' oli minimaalse kaaluga toespuu, siis $\omega(T'') = \omega(T')$, mis tähendab, et ka T'' on minimaalse kaaluga toespuu. Samas puul T'' on puuga T rohkem ühiseid servi kui puul T', mis on vastuolus T' valikuga. Saadud vastuolu näitab, et T peab olema minimaalse kaaluga toespuu. $\square$

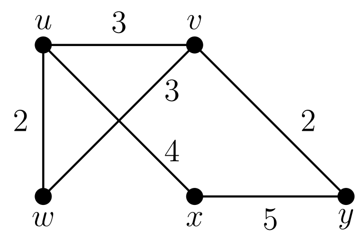
Tutvustame ka teist minimaalse toespuu leidmise algoritmi, mille töötas 1930. aastal välja tšehhi matemaatik Vojtěch Jarník. Hiljem taasavastasid selle algoritmi ameerika matemaatik ja arvutiteadlane Robert Prim (aastal 1957) ja hollandi arvutiteadlane Edsger Dijkstra (aastal 1959). Kuigi seda algoritmi oleks õigem kutsuda Jarníku algoritmiks, kasutame käesolevas kursuses rahvusvaheliselt enam levinud nimetust *Primi algoritm.*

Primi algoritm.

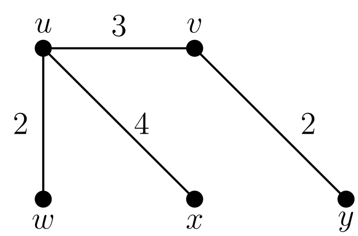
Antud: n-tipuline sidus kaalutud graaf $G = (V, E, \omega)$.
Leida: minimaalse kaaluga toespuu.
Idee: Konstrueerime alamgraafi T. Alustame suvalisest tipust ja ühendame puule järjest servi, mis viivad uude tippu (mis veel ei kuulu graafi T), valides igal sammul minimaalse kaaluga serva.

1. Vali graafist G välja suvaline tipp v. Olgu T_0 graaf ainsa tipuga v ja olgu $U := V \setminus \{v\}$.
2. Iga $i = 1, \dots, n-1$ korral:
   (a) leia graafist G vähima kaaluga serv e_i, mis ühendab mingit graafi T_{i-1} tippu mingi U tipuga w_i;
   (b) lisa alamgraafile T_{i-1} serv e_i ja tema teine otstipp w_i, tähista saadud graafi T_i;
   (c) eemalda tipp w_i hulgast U.
3. Tagasta graaf T_{n-1}.

Näide 2.77 Vaatleme jälle kaalutud graafi



Leiame selle graafi minimaalse kaaluga toespuu Primi algoritmi abil. Esimesel sammul valime tipu v. Järgnevatel sammudel valime tipud y, u, w, x koos servadega vy, vu, uw, ux. Tulemuseks on toespuu



Paneme tähele, et selles näites ja näites 2.75 leitud minimaalse kaaluga toespuud on erinevad. Nende mõlema kaal on $2 + 2 + 3 + 4 = 11$.

Teoreem 2.78 *Kui G on sidus kaalutud graaf, siis Primi algoritm leiab graafi G minimaalse kaaluga toespuu.*

TÕESTUS. Kuna G on sidus, siis igal sammul leidub serv, mis ühendab alamgraafi T_{i-1} mõne hulka U kuuluva tipuga.

Olgu Primi algoritmi abil leitud servad $e_1, \ldots, e_{n-1}$. Kuna ühelgi sammul ei saa serva e_i ja tipu w_i lisamisel tekkida tsükkel, siis kõik graafid T_i (servadega $e_1, \ldots, e_i$), kus $i \in \{1, \ldots, n-1\}$, on tsükliteta. Samas on nad konstruktsiooni tõttu sidusad. Järelikult T_i on puu iga $i \in \{0, 1, \ldots, n-1\}$ korral. Muuhulgas T_{n-1} on puu. Ta sisaldab ka kõiki G tippe ning seega on toespuu. Tõestame, et T_{n-1} on minimaalse kaaluga toespuude hulgas.

Olgu $k \in \{0, 1, \ldots, n-1\}$ maksimaalne arv, mille korral puu T_k sisaldub mingis minimaalse kaaluga toespuus. (Paneme tähele, et T_0 kindlasti sisaldub igas minimaalse kaaluga toespuus, seega on võimalik selline k leida.) On kaks võimalust.
a) $k = n-1$. Kuna T_{n-1} sisaldub mingis minimaalse kaaluga toespuus T ja kõigil toespuudel on $n-1$ serva, siis $T_{n-1} = T$, s.t. T_{n-1} on minimaalse kaaluga toespuu.
b) $k < n-1$. Näitame, et sel juhul tekib vastuolu. Niisiis T_k sisaldub mingis minimaalse kaaluga toespuus T. Seega T sisaldab servi $e_1, \ldots, e_k$, aga mitte serva e_{k+1} (vastavalt k maksimaalsusele). Lisame puule T serva e_{k+1}. Saadud alamgraaf S sisaldab tänu teoreemile 2.65 mingit tsüklit C. See tsükkel peab aga sisaldama serva e_{k+1}. Tsükkel C peab sisaldama ka mingit serva, mis ei kuulu puusse T_{k+1} (sest T_{k+1} ei saa tsüklit C sisaldada). Olgu $e_{k+1} = u_{k+1}w_{k+1}$, siis vastavalt konstruktsioonile on tipp u_{k+1} alamgraafis T_k ja tipp w_{k+1} väljaspool seda.

Alustame tipust u_{k+1} liikumist mööda tsüklit C, aga mitte tipu w_{k+1} suunas, vaid vastupidises suunas. Nii jõuame mingi servani e, mis ei kuulu graafi T_{k+1}, mille üks otstipp on graafis T_k ja teine väljaspool seda. Moodustame graafi T' kustutades graafist S serva e. Siis $\omega(e_{k+1}) \leqslant \omega(e)$, sest hetkel kui Primi algoritm valis serva e_{k+1}, oli valitavate servade hulgas ka e. Seega $\omega(T') \leqslant \omega(T)$. Et T' on sidus graaf $n-1$ servaga, siis järelduse 2.66 tõttu on ta puu. Samuti sisaldab ta kõiki G tippe ja on seega G toespuu. Kuna T oli minimaalse kaaluga toespuu, siis $\omega(T') = \omega(T)$ ja ka T' on minimaalse kaaluga toespuu. Samas T' sisaldab puud T_{k+1}, mis on vastuolus k valikuga. $\square$

2.7 Suunatud graafid

2.7.1 Suunatud graafide põhiomadused

Siiani oleme vaadelnud graafe, kus servade suund pole oluline, s.t. me ei ole teinud vahet, milline tipp on serva algtipp ja milline lõpptipp. Vaatleme nüüd graafe, mille servadel on suund.

Definitsioon 2.79 **Suunatud graaf**[12] on järjestatud paar $G = (V, E)$, kus V on mittetühi hulk ja E on hulga $V \times V$ alamhulk.

Seega hulga E elementideks on järjestatud paarid (u, v), kus $u, v \in V$. Suunatud graafi puhul räägitakse servade asemel harilikult **kaartest**[13] ning joonistel kujutatakse neid tavaliselt nooltena. Tippu u nimetatakse kaare (u, v) **algtipuks** ja tippu v selle kaare **lõpptipuks**. Öeldakse, et kaar (u, v) **väljub** tipust u ja **siseneb** tippu v.

Kui edaspidises tahame mingil hetkel rõhutada, et vaatleme graafi definitsiooni 2.1 mõttes, siis ütleme, et vaatleme suunamata graafi. Nii nagu suunamata juhulgi vaatleme selles kursuses ainult lõplikke suunatud graafe.

Märkus 2.80 Suunatud graafis võib definitsiooni järgi kahe tipu vahel olla kas 0, 1 või 2 kaart. Meie definitsiooni järgi on lubatud ka silmused, s.t. kaared kujul (v, v). (Mõnikord silmuseid suunatud graafi definitsioonis ei lubata.) Kui u ja v on erinevad tipud, siis kaared (u, v) ja (v, u) on erinevad. Mõnikord tähistatakse suunatud graafi kaarte hulka tähega A (sõnast *arc*, vt. näiteks monograafiat [1]).

Märkus 2.81 Meenutame, et **binaarseteks seosteks** hulgal V nimetatakse hulga $V \times V$ alamhulki. Seega binaarne seos ja suunatud graaf on sisuliselt sama asi.

Näide 2.82 Olgu meil antud mingi linna tänavate kaart. Seda võib vaadelda suunatud graafina, mille tippudeks on ristmikud ja kahe ristmiku u ja v vahel on kaar (u, v), kui need on ühendatud tänavaga, millel on lubatud sõita ristmikult u ristmiku v suunas. Seega kahesuunalise liiklusega tänavad annavad graafi kaks kaart ja ühesuunalise liiklusega tänavad ühe.

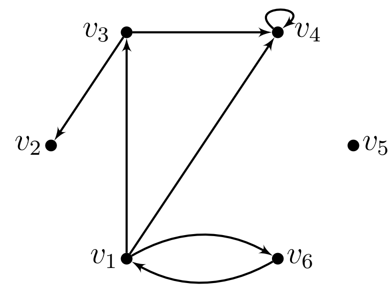
Definitsioon 2.83 Olgu $G = (V, E)$ suunatud graaf tippude hulgaga $V = \{v_1, \ldots, v_n\}$. Siis G **naabrusmaatriksiks** nimetatakse $n \times n$-maatriksit $A = (a_{ij})$, kus

$$a_{ij} = \begin{cases} 1, & \text{kui } (v_i, v_j) \in E, \\ 0, & \text{kui } (v_i, v_j) \notin E. \end{cases}$$

Näide 2.84 Suunatud graafi

[12] suunatud graaf = *directed graph, digraph*

[13] kaar = *arc*



naabrusmaatriks on

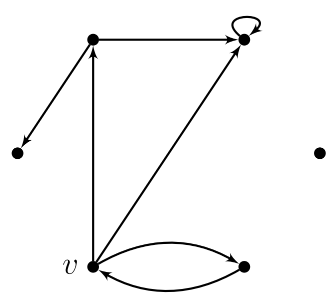
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Nagu näha, suunatud graafi naabrusmaatriks ei pea olema sümmeetriline ning tema peadiagonaalil võib olla ühtesid.

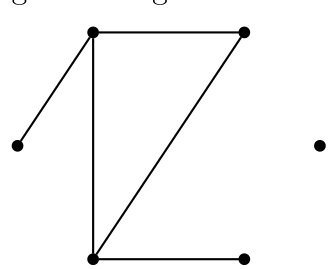
Kui asendame suunatud graafis kõik kaared suunamata servadega (nii-öelda unustame suuna ära), jätame välja kõik silmused ja kordsetest servadest jätame alles ühe, siis saame graafi, mida kutsutakse esialgse suunatud graafi **alusgraafiks**[14].

Definitsioon 2.85 Suunatud graafi tipu **sisendastmeks**[15] (tähistus $d_+(v)$) nimetatakse sellesse tippu sisenevate kaarte arvu ning **väljundastmeks**[16] (tähistus $d_-(v)$) nimetatakse sellest tipust väljuvate kaarte arvu.

Näide 2.86 Suunatud graafis



on $d_+(v) = 1$ ja $d_-(v) = 3$. Selle graafi alusgraaf on



[14]alusgraaf = *underlying graph*
[15]sisendaste = *indegree*
[16]väljundaste = *outdegree*

Teoreem 2.87 *Suunatud graafis on tippude sisendastmete summa võrdne tippude väljundastmete summaga:*

$$\sum_{v \in V} d_+(v) = \sum_{v \in V} d_-(v).$$

TÕESTUS. Tippude sisendastmete summa on võrdne graafi kaarte arvuga, sest selle summa leidmisel arvestame iga kaart ühe korra. Samamoodi on väljundastmete summa võrdne kaarte arvuga. Järelikult on need summad võrdsed. □

Definitsioon 2.88 Suunatud graafi **sisend** on tipp, mis pole ühegi kaare lõpptipp. Suunatud graafi **väljund** on tipp, mis pole ühegi kaare algtipp.

Definitsioon 2.89 Suunatud graafi tippu nimetatakse **isoleerituks**, kui ta ei ole ühegi kaare alg- ega lõpptipp.

Seega iga isoleeritud tipp on samaaegselt nii sisend kui väljund.

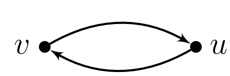
Näide 2.90 Näites 2.84 vaadeldud suunatud graafi sisendiks on tipp v_5 ning väljunditeks on tipud v_2 ja v_5.

Ülesanne 2.91 Kuidas saab naabrusmaatriksi abil kindlaks teha, kas suunatud graafi mingi tipp on sisend või väljund?

Definitsioon 2.92 Suunatud graafi tippude järjendit $v_0, v_1, \ldots, v_k$, kus iga kaks järjestikust tippu v_i ja v_{i+1} on ühendatud kaarega (v_i, v_{i+1}), nimetatakse **suunatud ahelaks**. Kui ükski tipp suunatud ahelas ei kordu, siis on tegemist **suunatud lihtahelaga**. **Kinnine suunatud ahel** on suunatud ahel, mille esimene ja viimane tipp langevad kokku.

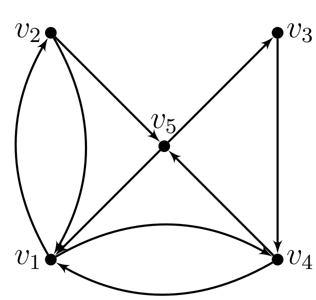
Definitsioon 2.93 **Suunatud tsükkel** on kinnine suunatud ahel, milles on vähemalt kaks kaart ja mis ei läbi ühtegi tippu kaks korda.

Märkus 2.94 Niisiis suunatud tsükkel on ahel $v_0, v_1, \ldots, v_k$, kus $k \geqslant 2$, $v_0 = v_k$ ja tipud $v_0, v_1, \ldots, v_{k-1}$ on erinevad. Definitsiooni järgi ei loe me silmuseid tsükliteks, kuid suunatud graafides võib olla kahest kaarest koosnevaid tsükleid kujul v, u, v:



Selline terminoloogia on kooskõlas raamatus [1] kasutatavaga (vt. lk. 11). Mõnes teises allikas võidakse lubada ka silmust suunatud tsüklina.

Näide 2.95 Vaatleme suunatud graafi



Selles graafis

- v_1, v_2, v_5, v_1, v_4 on suunatud ahel, mis ei ole suunatud lihtahel,
- $v_1, v_2, v_5, v_1, v_4, v_1$ on kinnine suunatud ahel,
- v_5, v_3, v_4, v_1, v_2 on suunatud lihtahel,
- v_5, v_3, v_4, v_5 on suunatud tsükkel.

Teoreem 2.96 *Kui suunatud graafis pole suunatud tsükleid, siis leidub graafil vähemalt üks sisend ja vähemalt üks väljund.*

TÕESTUS. Kui suunatud graafis leidub isoleeritud tippe, siis on need korraga nii sisendid kui väljundid.

Vaatleme suunatud graafi G, milles pole suunatud tsükleid ega isoleeritud tippe ja näitame, et selles graafis leidub väljund. Valime selles graafis välja ühe tipu v. Kui v on väljund, siis on vajalik tipp leitud. Vastasel korral leidub kaar, millele v on algtipuks. Liigume mööda seda kaart naabertippu v_1. Kui v_1 on väljund, siis lõpetame. Vastasel korral peab leiduma mingi kaar (v_1, v_2). Jätkame samamoodi. Paneme tähele, et ükski järgnev tipp v_i ei saa võrduda varem valitud tippudega $v, v_1, \ldots, v_{i-1}$, sest graaf ei sisalda suunatud tsükleid. Kuna graafis on lõplik arv tippe, siis pärast lõplikku arvu samme peame jõudma tippu u, kust ei välju ühtegi kaart. Seega u on väljund.

Sisendi leidmiseks saame kasutada analoogilist arutelu liikudes kaari pidi lõpptipu poolt algtipu poole. $\square$

Definitsioon 2.97 Suunatud graafi nimetatakse **tugevalt sidusaks**, kui iga kahe tipu u ja v korral leidub suunatud ahel tipust u tippu v.

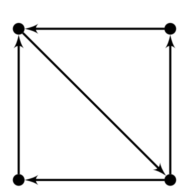
Ka ühetipuline suunatud graaf on tugevalt sidus.

Definitsioon 2.98 Suunatud graafi nimetatakse **nõrgalt sidusaks**, kui tema alusgraaf on sidus.

Kui suunatud graaf G on tugevalt sidus, siis on ta ka nõrgalt sidus. Tõepoolest, kui mistahes tippude u ja v korral leidub suunatud ahel tipust u tippu v, siis ka G alusgraafis on u ja v ühendatud ahelaga.

Näide 2.99 Suunatud graaf

on nõrgalt sidus, kuid mitte tugevalt sidus. Suunatud graaf



on tugevalt sidus.

Näide 2.100 Vaatleme linnatänavate suunatud graafi näitest 2.82. Liikluse planeerimisel on loomulik nõuda, et see graaf oleks tugevalt sidus, sest liiklejad tahavad, et igalt ristmikult saaks liikluseeskirja rikkumata sõita igale teisele.

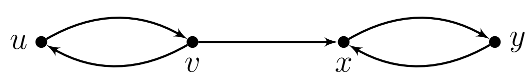
Lause 2.101 *Kui G on vähemalt kahetipuline tugevalt sidus graaf, siis tal ei ole sisendeid ega väljundeid.*

Tõestus. Olgu u graafi G mingi suvaline tipp. Valime veel ühe tipu v, mis erineb tipust u. Tugeva sidususe tõttu peavad leiduma suunatud ahelad tipust u tippu v ja tipust v tippu u. Järelikult peab leiduma nii tipust u väljuvaid kui ka tippu u sisenevaid kaari. See tähendab, et u ei saa olla ei sisend ega väljund. □

Seega kui vähemalt kahetipulises suunatud graafis leidub sisend või väljund, siis see graaf ei saa olla tugevalt sidus.

Kui suunatud graafis puuduvad sisendid ja väljundid, siis sellest veel ei järeldu tugev sidusus.

Näide 2.102 Suunatud graafis



ei ole sisendeid ega väljundeid. See graaf ei ole tugevalt sidus, sest tipust x ei leidu suunatud ahelat tippu v.

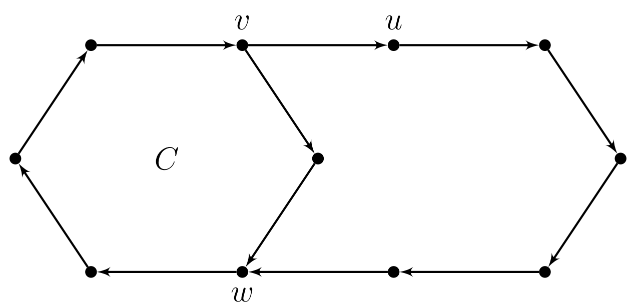
Teoreem 2.103 *Kui sidusas suunamata graafis ei leidu ühtegi silda, siis saab graafi servadele määrata suunad nii, et tekkinud suunatud graaf on tugevalt sidus.*

Tõestus. Ühetipulise graafi puhul on väide ilmne. Ainuke kahetipuline sidus suunamata graaf (isomorfismi täpsuseni) on

ja selle ainus serv on sild. Edasises vaatleme suvalist teoreemi eeldusi rahuldavat graafi G, milles on vähemalt kolm tippu. Kuna ükski serv pole sild, siis tänu teoreemile 2.42 peab iga serv sisalduma mingis tsüklis. Valime suvalise serva e (see leidub sidususe tõttu) ja vaatleme tsüklit C, mis seda serva sisaldab. Orienteerime selle tsükli kõik servad ühes suunas, siis saab igast tsükli tipust liikuda igasse teise. On kaks võimalust.

1) Kõik G tipud kuuluvad tsüklisse C. Võib juhtuda, et mõni G serv ei kuulu tsüklisse C. Siis võime talle määrata suvalise suuna. Saadud suunatud graaf on tugevalt sidus.

2) Mõni G tipp ei kuulu tsüklisse C. Siis leidub sidususe tõttu G serv, mis ühendab tsükli C mingit tippu v mingi tipuga u väljaspool tsüklit. Ka serv vu peab sisalduma mingis tsüklis ja seega peab lisaks ahelale v, u leiduma veel üks suunamata ahel tippude u ja v vahel.



Liigume seda pikemat ahelat pidi tipust u tippu v ja olgu w esimene ahela tipp, mis kuulub tsüklisse C. Määrame ahela $v, u, \ldots, w$ servadele suuna tipu v poolt tipu w poole. Omavahel kaartega ühendatud tippude hulgas pääseb nüüd endiselt igast tipust igasse teise. Nii jätkame kuni kõik G tipud on ühendatud mingisse suunatud tsüklisse. Kui mõni G serv jääb protsessi käigus kasutamata, siis võime talle anda suvalise suuna, sest see tugevalt sidusust ära ei kaota. $\square$

Suunamata graafide korral saime rääkida sidususkomponentidest. Ka suunatud graafide korral on see võimalik, aga olukord on veidi keerulisem. Anname kõigepealt mõned definitsioonid.

Definitsioon 2.104 Suunatud graafi $G' = (V', E')$ nimetatakse suunatud graafi $G = (V, E)$ **alamgraafiks**, kui $V' \subseteq V$ ja $E' \subseteq E$.

Definitsioon 2.105 Olgu $G = (V, E)$ suunatud graaf ja $U \subseteq V$. **Tippude hulga** U **poolt tekitatud** G **alamgraafiks** nimetatakse suunatud graafi $G_U = (U, E_U)$, kus

$$E_U = \{(x, y) \mid x, y \in U, (x, y) \in E\}.$$

Seega hulga U poolt tekitatud alamgraaf saadakse, kui kaarteks võetakse kõik kaared, mis hulka U kuuluvate tippude vahel graafis G olemas on.

Definitsioon 2.106 Suunatud graafi **tugevalt sidus komponent** on maksimaalne tugevalt sidus alamgraaf.

Seega suunatud graafi $G = (V, E)$ tugevalt sidus alamgraaf $G' = (V', E')$ on selle graafi tugevalt sidus komponent, kui mistahes tugevalt sidusa alamgraafi $G'' = (V'', E'')$ korral

$$V' \subseteq V'' \;\&\; E' \subseteq E'' \Longrightarrow V' = V'' \;\&\; E' = E''.$$

Muuhulgas alamgraafile $G' = (V', E')$ mistahes tipu $v \in V \setminus V'$ ja seda tippu G' tippudega ühendavate G kaarte lisamisel saame alamgraafi, mis ei ole enam tugevalt sidus.

Olgu $G = (V, E)$ suunatud graaf. Kui tipust u leidub suunatud ahel tippu v, siis kirjutame $u \rightsquigarrow v$. Defineerime hulgal V binaarse seose $\equiv$ järgmiselt:

$$u \equiv v \Longleftrightarrow \quad u \rightsquigarrow v \text{ ja } v \rightsquigarrow u.$$

Lihtne on veenduda, et seos $\equiv$ on ekvivalentsiseos.

Lause 2.107 *Ekvivalentsiklassid seose $\equiv$ järgi tekitavad suunatud graafi alamgraafid, mis on selle suunatud graafi tugevalt sidusateks komponentideks.*

TÕESTUS. Olgu $G = (V, E)$ suunatud graaf ja vaatleme suvalise tipu $u \in V$ ekvivalentsiklassi

$$K = \{v \in V \mid u \equiv v\}$$

poolt tekitatud alamgraafi $G_K = (K, E_K)$. See alamgraaf on tugevalt sidus, sest vastavalt seose $\equiv$ definitsioonile saab ekvivalentsiklassi piires liikuda igast tipust igasse teise mööda suunatud ahelat.

Näitame, et G_K on maksimaalne tugevalt sidus alamgraaf. Oletame vastuväiteliselt, et G_K ei ole seda. Siis peab leiduma mingi tipp $v_0 \in V \setminus K$ nii, et tipu v_0 lisamisel saadav alamgraaf $G_{K \cup \{v_0\}}$ on ka tugevalt sidus. Muuhulgas $u \rightsquigarrow v_0$ ja $v_0 \rightsquigarrow u$. Siis aga $u \equiv v_0$, mis tähendab, et $v_0 \in K$, vastuolu.

Sellega oleme näidanud, et G_K on graafi G tugevalt sidus komponent. $\square$

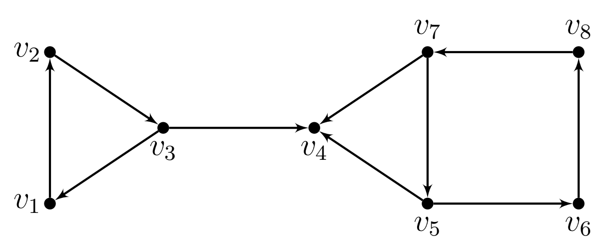
Kuna ekvivalentsiseos $\equiv$ tekitab hulga V tükelduse, siis G tugevalt sidusad komponendid on lõikumatud ja G iga tipp peab kuuluma mingisse tugevalt sidusasse komponenti. Lisaks sellele võime öelda, et tugevalt sidusate komponentide arv on võrdne ekvivalentsiklasside arvuga seose $\equiv$ järgi.

Järeldus 2.108 *Suunatud graaf on tugevalt sidus parajasti siis, kui tal on üks tugevalt sidus komponent.*

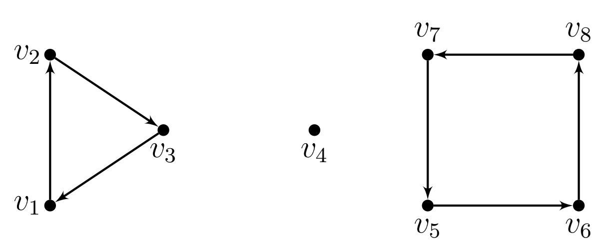
TÕESTUS. Suunatud graaf on tugevalt sidus parajasti siis, kui seose $\equiv$ järgi on ainult üks ekvivalentsiklass, milleks on hulk V. Viimane on samaväärne sellega, et tugevalt sidusaid komponente on üksainus. $\square$

Lause 2.107 tõestuse põhjal saab anda ka algoritmi tugevalt sidusate komponentide leidmiseks. Valime suunatud graafis G välja suvalise tipu u. Otsime üles kõik tipud v, mille korral $u \rightsquigarrow v$ ja $v \rightsquigarrow u$. Need tipud tekitavad G esimese tugevalt sidusa komponendi. Siis valime ülejäänud tippude hulgast välja suvalise ja kordame protsessi niikaua kui see on võimalik.

Näide 2.109 Suunatud graafi



tugevalt sidusad komponendid on



.

2.7.2 Lühima tee leidmise ülesanne

Praktilistest ülesannetest tekkivates suunatud graafides on tihti kaartele omistatud mingid positiivse arvuna väljendatavad kaalud.

Definitsioon 2.110 Kaalutud suunatud graafiks[17] nimetatakse kolmikut (V, E, ω), kus (V, E) on suunatud graaf ja $\omega : E \to \mathbb{R}^+$ on kujutus. Positiivset reaalarvu $\omega(e)$ nimetatakse kaare e **kaaluks** ehk **pikkuseks**.

Definitsioon 2.111 Kaalutud suunatud graafi suunatud ahela **kaaluks** ehk **pikkuseks** nimetatakse selle ahela kaarte kaalude summat.

Kui $T = v_0, v_1, \ldots, v_k$ on mingi suunatud ahel, siis tema kaalu tähistame $\omega(T)$ või $\omega(v_0, v_1, \ldots, v_k)$. Niisiis

$$\omega(T) = \sum_{i=1}^{k} \omega(v_{i-1}, v_i).$$

Lühima tee leidmise ülesanne[18] seisneb selles, et antud kaalutud suunatud graafi G kahe tipu puhul leida minimaalse kaaluga suunatud ahel ühest tipust teise (juhul kui see olemas on).

Edasises ütleme "minimaalse kaaluga suunatud ahela" asemel lühidalt ka "lühim tee".

Niisiis tee T tipust u tippu v on lühim, kui iga tee T' korral tipust u tippu v on $\omega(T) \leqslant \omega(T')$.

Definitsioon 2.112 Kaalutud suunatud graafi tippude u ja v vaheliseks **kauguseks**[19] (tähistus $d(u, v)$) nimetatakse minimaalse kaaluga suunatud ahela pikkust tipust u tippu v, kui tipust u leidub suunatud ahelaid tippu v. Kui selliseid ahelaid ei leidu, siis loetakse, et $d(u, v) = \infty$.

Seega lühima tee leidmise ülesande lahendamise käigus leitakse graafi tippude vahelisi kaugusi.

Näide 2.113 1. Vaatleme jälle linnatänavate suunatud graafi näitest 2.82. Omistame selle graafi kaartele kaalud, mis näitavad, kui palju aega kulub keskmiselt ühelt ristmikult naaberristmikule jõudmiseks. Lühima tee leidmine tähendab sellisel juhul minimaalse ajakuluga marsruudi leidmist.

2. Olgu meil graafi tippudeks linnad, servadeks nendevahelised maanteed ja kaaludeks maanteede pikkused. Lühima tee leidmine tähendab sellisel juhul sõna otseses mõttes lühima tee leidmist linnast A linna B.

3. Olgu graafi tippudeks linnad ja servadeks ühistranspordiliinid. Kui servade kaaludeks on ajakulu, siis lühima tee leidmine tähendab minimaalse ajakuluga marsruudi leidmist. Kui aga servade kaaludeks on piletihinnad, siis lühima tee leidmine tähendab võimalikult odava marsruudi leidmist.

[17] kaalutud suunatud graaf = *weighted directed graph*

[18] lühima tee leidmise ülesanne = *shortest path problem*

[19] kaugus = *distance*

Lühima tee leidmise ülesannet võib sõltuvalt silmas peetavast rakendusest püstitada väga erinevatel viisidel. Konkreetsest püstitusest sõltub ka see, milline peaks olema ülesande lahendamiseks kasutatav algoritm. Ülesande püstitus võib sõltuda näiteks järgmistest asjaoludest.

- Kas graaf on suunatud või suunamata?
- Kas servade kaalud peavad olema positiivsed arvud või on lubatud ka negatiivsed kaalud?
- Kas tahame leida lühimat teed tipust a tippu z, tipust a kõigisse teistesse tippudesse, või hoopis kõigi tipupaaride vahel?
- Kas meid huvitab ainult lühima tee pikkus või ka sinna teesse kuuluvad tipud?
- Kas tahame leida ühe lühima tee või kõikvõimalikud lühimad teed kahe tipu vahel?

Enne algoritmide juurde minekut teeme mõned lihtsad tähelepanekud lühimate teede kohta.

Lemma 2.114 *n-tipulises kaalutud suunatud graafis kehtivad järgmised väited.*

1. *Lühim tee ei tohi sisaldada silmuseid ja peab olema suunatud lihtahel.*
2. *Lühim tee sisaldab ülimalt $n-1$ kaart.*
3. *Lühima tee iga osatee on ka lühim oma otspunktide vahel.*

TÕESTUS. 1. Ahelast silmuse välja jätmisel saame samuti ahela, mis ei ole pikem kui esialgne. Kui ahelas on korduvaid tippe, siis saame korduvate tippude vahele jääva osa välja jätta ning pikkus kahaneb.

2. Kuna lühim tee peab olema lihtahel, siis on temas ülimalt n tippu ning järelikult ülimalt $n-1$ kaart.

3. Vaatleme lühimat teed

$$T = u, \dots, x, \dots, y, \dots, v$$

tippude u ja v vahel. Kui osatee $x, \dots, y$ ei oleks minimaalse pikkusega tippude x ja y vahel, siis saaksime ta asendada lühema teega ning tulemuseks oleks ka u ja v vahel lühem tee kui T. □

Järgnevalt vaatleme kolme lühima tee leidmise algoritmi. Kõigis nendes algoritmides kasutame järgmisi kokkuleppeid.

- Eeldame, et kaalutud suunatud graafi G tippude hulgaks on

$$V = \{1, 2, \dots, n\}.$$

- Meil on olemas kujutus $\omega : E \to \mathbb{R}^+$ ja me tähistame kaare (i,j) kaalu $\omega(i,j)$ asemel sümboliga ω_{ij}.

- Kui tipust i ei ole kaart tippu j (s.t. $(i,j) \notin E$), siis algoritmides me loeme, et $\omega_{ij} = \infty$. Praktikas on mõistlik ∞ ossa võtta mingi hästi suur arv, näiteks $n \cdot r$, kus n on tippude arv ja r on G servade kaaludest maksimaalne. Kuna lühimas tees on ülimalt $n-1$ kaart, siis ükski lühim tee ei saa olla pikkusega $n \cdot r$.

- Sõltumata sellest, kas graafis G on silmuseid või mitte, me loeme, et iga tipu i korral $\omega_{ii} = 0$ (s.t. lühim tee tipust i tippu i on pikkusega 0).

Laias laastus on nende kolme algoritmi idee selline, et leiame mingid esialgsed hinnangud võimalikele lühimate teede pikkustele ja hakkame siis neid samm-sammult parandama.

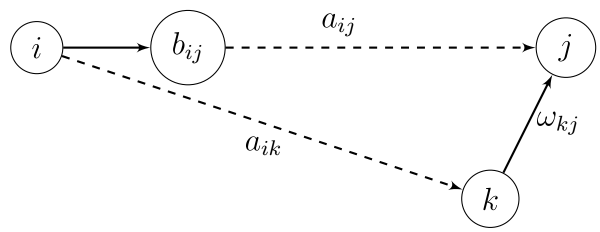
Märgime veel, et kuigi algoritmid on sõnastatud suunatud graafide jaoks, saab neid kasutada ka suunamata juhul. Nimelt suunamata graafi võib muuta suunatuks asendades iga serva kahe kaarega (mõlemas suunas).

Lühima tee laiuti otsimise algoritm

Antud: kaalutud suunatud graaf $G = (V, E, \omega)$.
Leida: lühimad teed kõigi tipupaaride vahel.
Idee: Moodustame kaks $n \times n$-maatriksit A ja B. Otsime järjest lühimaid $1, 2, \ldots, n-1$-kaarelisi teid tipust i tippu j. Maatriksi A element a_{ij} näitab seni leitud lühima tee kaalu tipust i tippu j. Maatriksi B element b_{ij} näitab tippu, kuhu tuleb selles lühimas tees tipust i esimese sammuga minna (s.t. lühima tee esimest vahetippu).

```
comment: Algväärtused
a_ij := ω_ij
b_ij := j
comment: Täidetakse 4-kordne tsükkel
for s = 2,...,n−1 do  (vaatleme s-tipulisi teid)
    for i = 1,...,n do  (i on algtipp)
        for j = 1,...,n do  (j on lõpptipp)
            for k = 1,...,n do  (k on eelviimane tipp tees)
                if a_ik + ω_kj < a_ij then
                                a_ij := a_ik + ω_kj
                                b_ij := b_ik
```

Asenduse idee on järgmine: kui tipust i tippu k ja sealt ühe sammuga tippu j liikudes on lühem tee kui seni leitud lühim tee tipust i tippu j, siis liigume tipust i tippu k ja sealt tippu j. Olukorda enne a_{ij} ja b_{ij} väärtuste uuendamist illustreerib järgnev joonis. Sellel on pidevate joontega tähistatud kaared ja katkendlike joontega suunatud ahelad.



Tõestame teoreemi laiuti otsimise algoritmi korrektsuse kohta.

Teoreem 2.115 *Pärast lühima tee laiuti otsimise algoritmi täitmist kehtivad iga $i, j \in \{1, \ldots, n\}$ korral järgmised väited.*

1. *Kui leidub suunatud ahel tipust i tippu j, siis a_{ij} väärtuseks on lühima tee pikkus tipust i tippu j ja b_{ij} väärtuseks sellise tee teise tipu number.*

2. *Kui ei leidu suunatud ahelaid tipust i tippu j, siis $a_{ij} = \infty$.*

TÕESTUS. Selles tõestuses nimetame s-*ahelateks* tipust i tippu j kõiki suunatud ahelaid tipust i tippu j, milles on ülimalt s kaart (s on naturaalarv). Teoreemi tõestamiseks näitame, et kehtib järgmine väide (nn. tsükli invariant):

(*) *iga $s \in \{1, 2, \ldots, n-1\}$ ja $i, j \in \{1, 2, \ldots, n\}$ korral pärast etapi s läbimist*

(1) kui leidub s-ahelaid tipust i tippu j, siis a_{ij} väärtuseks on minimaalse s-ahela pikkus tipust i tippu j ja b_{ij} väärtuseks on mingi sellise minimaalse s-ahela teise tipu number,

(2) kui ei leidu s-ahelaid tipust i tippu j, siis $a_{ij} = \infty$.

Kui oleme väite (*) ära tõestanud, siis teame, et pärast etappi $n-1$ annab maatriks A meile minimaalsete $(n-1)$-ahelate pikkused kõigi tipupaaride vahel. Samas lemma 2.114 põhjal me teame, et iga minimaalne ahel peab olema $(n-1)$-ahel. Seega oleme leidnud minimaalsete ahelate pikkused tipupaaride vahel ning maatriks B annab minimaalsetes ahelates teised tipud, s.t. oleme näidanud, et teoreem kehtib.

Väite (*) tõestamiseks kasutame matemaatilist induktsiooni s järgi, kusjuures etapi $s = 1$ all peame silmas algväärtustamist.

Alus. Olgu $s = 1$. 1-kaarelised ahelad tipust i tippu j on olemas siis, kui leidub kaar tipust i tippu j. Sellise ahela pikkus on ω_{ij} ja see arv omistatakse a_{ij}-le. Kui leidub kaar $(i, j) \in E$, siis ahela i, j teine tipp on j ning see omistatakse b_{ij}-le. Kui aga $(i, j) \notin E$, siis omistatakse $a_{ij} = \infty$. Seega (*) kehtib $s = 1$ korral.

Samm. Eeldame, et (*) kehtib pärast etapi s läbimist ja olgu maatriksite A ja B elemendid sellised, nagu nad on pärast etapi s läbimist. Uurime, mis juhtub etapil $s + 1$. Olgu

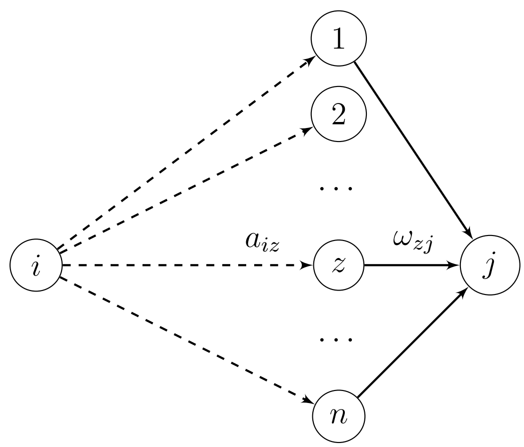
$$T = i, x, y, \ldots, z, j$$

minimaalne $(s+1)$-ahel tipust i tippu j. Siis $T' = i, x, y, \ldots, z$ peab tänu lemmale 2.114(3) olema minimaalne s-ahel tipust i tippu z. Induktsiooni eelduse põhjal on $\omega(T') = a_{iz}$ ja seega $\omega(T) = a_{iz} + \omega_{zj}$. Kuna a_{ij} on minimaalse s-ahela pikkus ja ükski $(s+1)$-ahel (muuhulgas ükski s-ahel) tipust i tippu j ei ole lühem kui T, siis

$$a_{iz} + \omega_{zj} \leqslant a_{ij}.$$

On kaks võimalust.
a) $a_{iz} + \omega_{zj} = a_{ij}$. Siis $k = z$ korral a_{ij}-le uut väärtust ei omistata.
b) $a_{iz} + \omega_{zj} < a_{ij}$. Siis $k = z$ korral omistatakse a_{ij}-le uus väärtus $a_{iz} + \omega_{zj}$. Lisaks sellele omistatakse $b_{ij} := b_{iz}$.

Ülejäänud tippude $k \in V \setminus \{z\}$ korral peab $a_{ik} + \omega_{kj} \geqslant a_{iz} + \omega_{zj}$, sest T on minimaalne $(s+1)$-ahel. Seega pärast k-ga seotud tsükli läbimist on a_{ij} väärtuseks $\omega(T)$ ning b_{ij} väärtuseks on tipust i tippu j viiva minimaalse pikkusega $(s+1)$-ahela teise tipu number. See tähendab, et (1) kehtib pärast etapi $s+1$ läbimist.

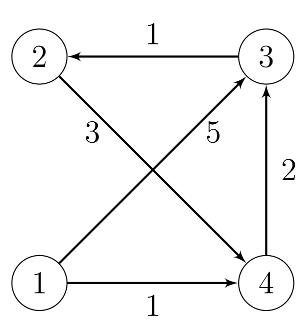


Oletame nüüd, et $(s+1)$-ahelaid tipust i tippu j ei leidu. Siis ei leidu ka s-ahelaid ja seega induktsiooni eelduse põhjal $a_{ij} = \infty$. Lisaks sellele iga tipu z korral kas $a_{iz} = \infty$ või $\omega_{zj} = \infty$ (vt. joonist). Järelikult võrratus

$$a_{iz} + \omega_{zj} < a_{ij}$$

ei kehti ja a_{ij}-le uut väärtust ei omistata. Seega (2) kehtib pärast etappi $s+1$. □

Näide 2.116 Rakendame lühima tee laiuti otsimise algoritmi suunatud kaalutud graafile (kaalud on märgitud kaarte juurde)



Siis maatriksite A ja B elemendid muutuvad s väärtuste 1 (algväärtustus), 2 ja 3 korral järgmiselt (punasega on märgitud elemendid, mis on võrreldes eelmise maatriksiga muutunud):

$$A: \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 6 & 3 & 1 \\ \infty & 0 & 5 & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 4 & 3 & 1 \\ \infty & 0 & 5 & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix}$$

$$B: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 & 4 & 4 \\ 1 & 2 & 4 & 4 \\ 1 & 2 & 3 & 2 \\ 1 & 3 & 3 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 4 & 4 & 4 \\ 1 & 2 & 4 & 4 \\ 1 & 2 & 3 & 2 \\ 1 & 3 & 3 & 4 \end{pmatrix}.$$

Maatriksi A viimane väärtus annab meile lühimate teede pikkused kõigi tipupaaride vahel. Näiteks näeme, et lühim tee tipust 2 tippu 3 on pikkusega 5. See, et mõned maatriksi elemendid on ∞, näitab, et vastavate tippude vahel suunatud ahelaid ei leidu. Näiteks tipust 2 ei ole võimalik liikuda tippu 1.

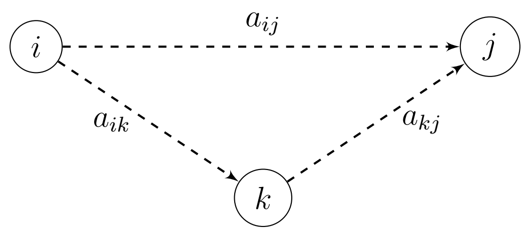
Maatriks B annab meile ka lühima tee tipud. Konstrueerime näiteks lühima tee tipust 1 tippu 2 maatriksi B põhjal. Kuna $b_{12} = 4$, siis tipust 1 peame liikuma tippu 4. Et $b_{42} = 3$, siis järgmine tipp on 3. Kuna $b_{32} = 2$, siis viimane tipp on 2 ja kogu suunatud ahel on $1, 4, 3, 2$.

Floydi–Warshalli algoritm

Antud: kaalutud suunatud graaf $G = (V, E, \omega)$.
Leida: lühimad teed kõigi tipupaaride vahel.
Idee: Moodustame kaks $n \times n$-maatriksit A ja B. Otsime lühimaid teid tipust i tippu j. Maatriksi A element a_{ij} näitab seni leitud lühima tee kaalu tipust i tippu j. Maatriksi B element b_{ij} näitab lühima tee esimest vahetippu. Vaadatakse läbi kõik tipud k ja uuritakse, milliste tipupaaride (i, j) korral saab k kaudu tipust i liikuda tippu j lühemini kui varem leitud lühimat teed pidi i ja j vahel.

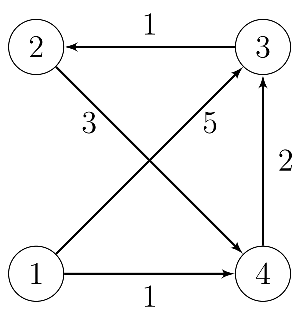
comment: Algväärtused
$a_{ij} := \omega_{ij}$
$b_{ij} := j$
comment: Täidetakse 3-kordne tsükkel
for $k = 1, \ldots, n$ do
    for $i = 1, \ldots, n$ do
        for $j = 1, \ldots, n$ do
            if $a_{ik} + a_{kj} < a_{ij}$ then
                $a_{ij} := a_{ik} + a_{kj}$
                $b_{ij} := b_{ik}$

Asenduse idee on järgmine: kui tipust i tippu k ja sealt tippu j liikudes on lühem tee kui seni leitud lühim tee tipust i tippu j, siis liigume tipust i tippu k ja sealt tippu j.



Paneme veel tähele, et kui $i = k$, siis võrratus $a_{kk} + a_{kj} < a_{kj}$ ei kehti ja seega omistamist ei toimu. Sama kehtib $j = k$ korral. See tähendab, et etapil k maatriksite A ja B k-s rida ja k-s veerg ei muutu.

Näide 2.117 Rakendame Floydi–Warshalli algoritmi juba varem vaadeldud suunatud kaalutud graafile



Siis maatriksi A elemendid muutuvad k väärtuste 1, 2, 3 ja 4 korral järgmiselt:

$$A: \quad \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & 4 \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow$$

$$\longrightarrow \begin{pmatrix} 0 & 6 & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 4 & 3 & 1 \\ \infty & 0 & 5 & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix}.$$

Sinisega on ära märgitud k-s rida ja k-s veerg enne k-ndat etappi. Nagu eespool öeldud k-nda etapi käigus need kindlasti ei muutu. Tingimuse $a_{ik} + a_{kj} < a_{ij}$ kontrollimisel liidetakse element k-ndast veerust (a_{ik}) elemendiga k-ndast reast (a_{kj}). Elemendid $a_{kk} = 0, a_{kj}, a_{ij}, a_{ik}$ asuvad maatriksis n.ö. ristküliku tippudes, kusjuures a_{ik} ja a_{kj} on teineteise vastandtipud ning a_{kk} ja a_{ij} on teineteise vastandtipud.

Paneme tähele, et teine maatriks (see, mis vastab väärtusele $k = 1$) on sama, mis esimene. Põhjuseks on see, et ei leidu tipupaare (i, j), mille vahel saaks tipu 1 kaudu liikuda.

Teoreem 2.118 *Pärast Floydi-Warshalli algoritmi täitmist kehtivad iga $i, j \in \{1, \ldots, n\}$ korral järgmised väited.*

1. *Kui leidub suunatud ahel tipust i tippu j, siis a_{ij} väärtuseks on lühima tee pikkus tipust i tippu j ja b_{ij} väärtuseks sellise tee teise tipu number.*

2. *Kui ei leidu suunatud ahelaid tipust i tippu j, siis $a_{ij} = \infty$.*

Anname ka selle algoritmi korrektsuse tõestuse, kuigi eksamil ei ole selle tõestuse teadmine vajalik.

TÕESTUS. Selles tõestuses nimetame *k-ahelateks* tipust i tippu j kõiki suunatud ahelaid tipust i tippu j, mille vahetipud kuuluvad hulka $\{1, \ldots, k\}$ (k on naturaalarv). Paneme tähele, et iga $(k-1)$-ahel on ka k-ahel. Teoreemi tõestamiseks näitame, et kehtib järgmine väide:

(*) *iga $k \in \{0, 1, \ldots, n\}$ ja $i, j \in \{1, 2, \ldots, n\}$ korral pärast etapi k läbimist*

1. *kui leidub k-ahelaid tipust i tippu j, siis a_{ij} väärtuseks on minimaalse k-ahela pikkus tipust i tippu j ning b_{ij} väärtuseks on mingi sellise minimaalse k-ahela teise tipu number,*

2. *kui ei leidu k-ahelaid tipust i tippu j, siis $a_{ij} = \infty$.*

Kui oleme väite (*) ära tõestanud, siis teame, et pärast etappi n annab maatriks A meile minimaalsete n-ahelate pikkused kõigi tipupaaride vahel ning maatriks B annab minimaalsetes ahelates teised tipud, s.t. oleme näidanud, et teoreem kehtib.

Väite (*) tõestamiseks kasutame matemaatilist induktsiooni k järgi, kusjuures etapi $k = 0$ all peame silmas algväärtustamist.

Alus. Olgu $k = 0$. Sellisel juhul loeme k-ahelateks selliseid ahelaid, millel ei ole vahetippe. Selline ahel on lihtsalt kaar tipust i tippu j ja selle ahela pikkus on ω_{ij}, mis omistatakse a_{ij}-le. Kui leidub kaar $(i, j) \in E$, siis ahela i, j teine tipp on j ning see omistatakse b_{ij}-le. Kui $(i, j) \notin E$, siis omistatakse $a_{ij} := \infty$. Seega (*) kehtib $k = 0$ korral.

Samm. Eeldame, et (*) kehtib pärast etapi $k-1$ läbimist ja olgu maatriksite A ja B elemendid sellised, nagu nad on pärast etapi $k-1$ läbimist. Näitame, et (*) kehtib ka pärast etapi k läbimist.

Olgu T mingi minimaalne k-ahel tipust i tippu j. Siis $\omega(T) \leqslant a_{ik} + a_{kj}$. Kuna iga $(k-1)$-ahel on ka k-ahel ja induktsiooni eelduse põhjal on a_{ij} mingi minimaalse $(k-1)$-ahela pikkus, siis $\omega(T) \leqslant a_{ij}$. On kaks võimalust.

a) T ei sisalda tippu k. Siis T on $(k-1)$-ahel. Kuna ta on minimaalne k-ahel, siis on ta ka minimaalne $(k-1)$-ahel. Induktsiooni eelduse põhjal on a_{ij} minimaalse $(k-1)$-ahela pikkus. Seega $a_{ij} = \omega(T)$. Järelikult

$$a_{ij} \leqslant a_{ik} + a_{kj},$$

mistõttu etapil k a_{ij}-le uut väärtust ei omistata.

b) T sisaldab tippu k. Siis ta sisaldab tippu k täpselt ühe korra, sest minimaalne ahel peab olema lihtahel. Olgu

$$T = i, u, \ldots, v, k, x, \ldots, y, j.$$

Siis $T_1 = i, u, \ldots, v, k$ ja $T_2 = k, x, \ldots, y, j$ on $(k-1)$-ahelad, kusjuures nende pikkused peavad olema minimaalsed, sest muidu ei oleks T minimaalne k-ahel. Induktsiooni eelduse tõttu peab

$$\omega(T) = \omega(T_1) + \omega(T_2) = a_{ik} + a_{kj}.$$

Teame, et $\omega(T) \leqslant a_{ij}$. Kui $\omega(T) = a_{ij}$, siis a_{ij}-le uut väärtust ei omistata. Kui aga $\omega(T) < a_{ij}$, siis omistatakse a_{ij}-le väärtus $\omega(T)$ ehk minimaalse k-ahela pikkus. Samuti omistatakse b_{ij}-le mingi sellise k-ahela teise tipu number.

Järelikult pärast k-ga seotud tsükli läbimist on a_{ij} väärtuseks ahela T pikkus ning b_{ij} väärtuseks on tipust i tippu j viiva minimaalse pikkusega ahela teise tipu number. See tähendab, et (1) kehtib pärast etappi k.

Oletame nüüd, et k-ahelaid tipust i tippu j ei leidu. Siis ei leidu ka $(k-1)$-ahelaid ja seega induktsiooni eelduse põhjal $a_{ij} = \infty$. Lisaks sellele kas $a_{ik} = \infty$ või $a_{kj} = \infty$. Järelikult võrratus

$$a_{ik} + a_{kj} < a_{ij}$$

ei kehti ja a_{ij}-le uut väärtust ei omistata. Seega (2) kehtib pärast etappi k. □

Dijkstra algoritm

Antud: kaalutud suunatud graaf $G = (V, E, \omega)$, algtipp a ja lõpptipp z.
Leida: lühim tee tipust a tippu z.
Andmed: S — selliste tippude hulk, kuhu on juba leitud lühim tee tipust a,
$L[i]$ — seni leitud vähim tee pikkus tipust a tippu i.

Idee on järgmine.

1. Võtame kasutusele hulga S, kuhu hakkame lisama tippe, millesse on juba leitud lühim tee tipust a. Töö alguses loeme, et S on tühi hulk.

2. Igale tipule omistame esialgse kauguse algtipust: algtipu a korral loeme, et see kaugus on 0, ülejäänud tippude korral loeme, et see on lõpmatus.

3. Igal sammul valime välja ühe seni vaatlemata tipu ja lisame hulka S. Esimesel sammul võtame selleks algtipu a.

4. Iga väljavalitud tipu u korral vaatleme tema naabreid v, kuhu saab kaart mööda liikuda ja mis ei ole veel vaadeldud tippude hulka S lisatud. Iga sellise v korral uurime, kas teekond a-st u kaudu v-sse on lühem, kui varem teada olnud lühim tee pikkusega $L[v]$. Kui on, siis omistame $L[v]$-le uue väärtuse. Vastasel korral jääb $L[v]$ muutmata.

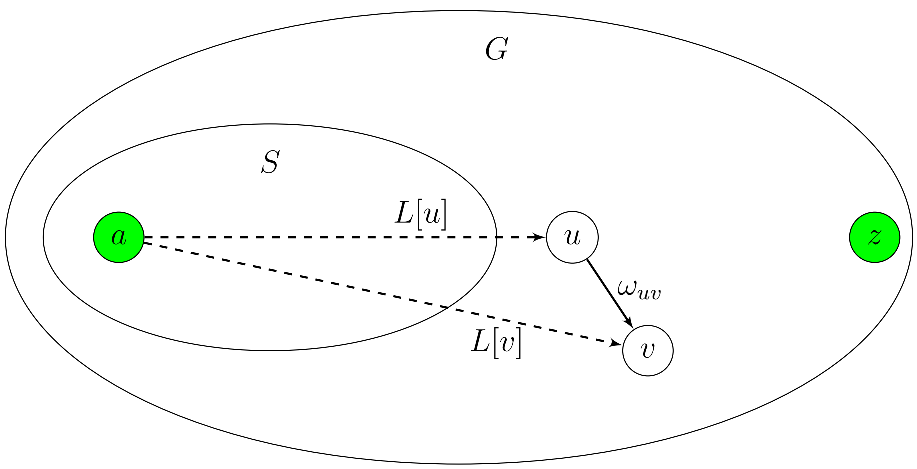
5. Kui kõik u naabrid on läbi vaadatud, siis me valime uue tipu u nende hulgast, mida me ei ole veel hulka S lisanud. Valimisel vaatame, millise tipu korral on seni leitud kaugus algtipust kõige väiksem. Uue tipu u jaoks kordame eelmises punktis mainitud samme.

6. Lõpetame siis, kui lõpptipp z saab hulka S lisatud.

7. Algoritmi töö lõpus annab $L[z]$ meile lühima tee pikkuse tipust a tippu z. Kui $L[z] = \infty$, siis see tähendab, et tipust a ei leidu suunatud ahelaid tippu z.

Algoritm ise näeb välja nii:

comment: Algväärtused
$L[a] := 0$
iga $i \in V \setminus \{a\}$ korral $L[i] := \infty$
$S := \emptyset$
comment: Täidetakse tsükkel
while $z \notin S$ do
  $u :=$ selline $i \notin S$, et $L[i]$ on minimaalne
  $S := S \cup \{u\}$
  for $v \notin S$ do
    if $L[u] + \omega_{uv} < L[v]$ then $L[v] := L[u] + \omega_{uv}$



Märkus 2.119 1. Algoritm lõpetab töö, sest while-tsükli igal sammul lisatakse hulka S üks tipp, mis seni sinna ei kuulunud. Kuna tippude arv graafis on lõplik, siis mingil hetkel lisatakse ka tipp z hulka S.

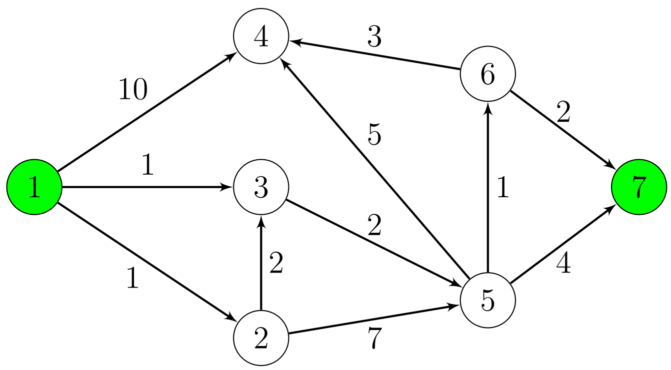
2. Võib juhtuda, et u valimisel on kõigi vaadeldavate tippude $i \notin S$ korral $L[i] = \infty$. Siis me valimegi ühe neist tippudest.

3. Kui $\omega_{uv} = \infty$, siis tingimus $L[u]+\omega_{uv} < L[v]$ ei ole täidetud (isegi siis, kui $L[v] = \infty$). Seega for-tsüklis on mõtet vaadelda vaid neid tippe $v \notin S$, mis on tipu u naabrid, s.t. mille korral leidub kaar $(u, v) \in E$.

4. Paneme tähele, et kui mingi tipp u on juba hulka S lisatud, siis $L[u]$ väärtust edasistel sammudel enam ei muudeta.

5. Kui me tahaksime leida lühimad teed kõigisse teistesse tippudesse (mitte ainult tippu z), siis tuleks while-tsüklis tingimus $z \notin S$ asendada tingimusega $V \setminus S \neq \emptyset$. Nii vaadatakse u osas läbi kõik graafi tipud.

Näide 2.120 Rakendame Dijkstra algoritmi suunatud kaalutud graafile



olukorras, kus $a = 1$ ja $z = 7$, s.t. otsime lühimat teed tipust 1 tippu 7. Algoritmi töö käigus lisatakse hulka S tippe ja lõpetatakse siis, kui on tipp 7 lisatud. Töö lõppedes on

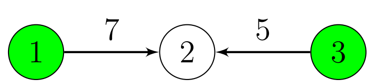
$$S = \{1, 2, 3, 5, 6, 7\}.$$

Järgnevas tabelis on ära toodud $L[i]$-de väärtused igal sammul (sammu 0 all on mõeldud algväärtustamist). Tabeli iga veeru põhjal valitakse uus element u nende tippude i hulgast, mis ei ole veel hulka S lisatud ja mille korral $L[i]$ väärtus on minimaalne (tabelis märgitud punase värviga). Näiteks sammul 1 on meil $S = \{1\}$ ja meil on minimaalse väärtusega 1 nii $L[2]$ kui ka $L[3]$. Antud juhul oleme u-ks valinud tipu 2, aga sama hästi oleks võinud valida ka tipu 3.

	samm 0	samm 1	samm 2	samm 3	samm 4	samm 5
$L[1]$	0	0	0	0	0	0
$L[2]$	∞	1	1	1	1	1
$L[3]$	∞	1	1	1	1	1
$L[4]$	∞	10	10	10	8	7
$L[5]$	∞	∞	8	3	3	3
$L[6]$	∞	∞	∞	∞	4	4
$L[7]$	∞	∞	∞	∞	7	6

Tabelist näeme, et lühima tee pikkus tipust 1 tippu 7 on 6. See tee on $1, 3, 5, 6, 7$.

Näide 2.121 Rakendame Dijkstra algoritmi suunatud kaalutud graafile



olukorras, kus $a = 1$ ja $z = 3$. Algoritmi käigus lisame hulka S esimesena tipu 1, siis tipu 2 ja lõpuks tipu 3. Lisaks sellele arvutame

	samm 0	samm 1	samm 2
$L[1]$	0	0	0
$L[2]$	∞	7	7
$L[3]$	∞	∞	∞

Töö lõppedes on $L[3] = \infty$, mis tähendab, et tipust 1 ei leidu suunatud ahelat tippu 3.

Hakkame nüüd uurima Dijkstra algoritmi korrektsust. Alustuseks tõestame ühe abitulemuse.

Lemma 2.122 *Dijkstra algoritmi töö igal etapil iga tipu v korral kui $L[v] \neq \infty$, siis leidub suunatud ahel tipust a tippu v, mille pikkus on $L[v]$.*

TÕESTUS. Tõestame induktsiooniga, et iga k korral pärast algoritmi töö k-ndat etappi väide kehtib.

Alus. Pärast etappi 0 (s.t. pärast algväärtustamist) on ainuke tipp, mille korral L väärtus ei ole ∞, tipp a, kusjuures $L[a] = 0$ ja 0 on ka lühima tee pikkus tipust a tippu a.

Samm. Eeldame, et väide kehtib pärast etappi k, s.t. pärast while-tsükli k-ndat läbimist, ja vaatleme suvalist tippu v. Olgu pärast etappi $k+1$ $L[v] \neq \infty$. Kui $L[v]$ väärtust etapil $k+1$ ei muudetud, siis juba pärast etappi k $L[v] \neq \infty$ ning ahel pikkusega $L[v]$ tipust a tippu v leidub tänu induktsiooni eeldusele.

Kui aga etapi $k+1$ käigus toimub omistamine

$$L[v] := L[u] + \omega_{uv},$$

siis enne omistamist peab kehtima võrratus $L[u] + \omega_{uv} < L[v]$. Järelikult $L[u] + \omega_{uv} < \infty$, kust $L[u] \neq \infty$ ja $\omega_{uv} \neq \infty$. Kuna $L[u]$ väärtust etapil $k+1$ ei muudeta, siis $L[u] \neq \infty$ juba pärast etappi k ja seega induktsiooni eelduse põhjal leidub suunatud ahel pikkusega $L[u]$ tipust a tippu u. Lisades sellele ahelale kaare (u, v) (see leidub, sest $\omega_{uv} \neq \infty$) saame ahela pikkusega $L[u] + \omega_{uv}$ tipust a tippu v. See on sama väärtus, mis on $L[v]$-l pärast etappi $k+1$. □

Sellest lemmast järeldub, et alati kui $L[v] \neq \infty$, siis

$$d(a, v) \leqslant L[v]. \tag{2.1}$$

Teoreem 2.123 *Pärast Dijkstra algoritmi täitmist kehtivad iga tipu $v \in S$ korral järgmised väited.*

1. *Kui leidub suunatud ahelaid tipust a tippu v, siis*

$$L[v] = d(a, v).$$

2. *Kui ei leidu suunatud ahelaid tipust a tippu v, siis*

$$L(v) = \infty.$$

TÕESTUS. Väide 2 järeldub lemmast 2.122. Tõestame väite 1.

Tänu võrratusele (2.1) piisab meil näidata, et kui $v \in S$ ja tipust a leidub suunatud ahelaid tippu v, siis

$$L[v] \leqslant d(a, v).$$

Teeme seda induktsiooniga selle järgi, kuidas tippe hulka S lisatakse.

Alus. Esimesena lisatakse hulka S alati tipp a. Tipu a korral $d(a,a) = 0 = L[a]$.

Samm. Vaatleme tippu v, mis pärast algoritmi täitmist kuulub hulka S ja kuhu leidub tipust a suunatud ahelaid. Olgu T minimaalse pikkusega suunatud ahel tipust a tippu v, seega $\omega(T) = d(a,v)$. Vaatleme seda hetke algoritmi töös, kui tipuks u valitakse v, ja eeldame, et varem hulka S lisatud tippude i jaoks võrratus $L[i] \leqslant d(a,i)$ kehtib. Sel hetkel $a \in S$, aga $v \notin S$. Seega peab ahelas T leiduma mingi kaar $e = (x,y)$, kus $x \in S$ ja $y \notin S$. Niisiis

$$T = a, \dots, x, y, \dots, v.$$

Teeme järgmised tähelepanekud.

- Tänu lemmale 2.114(3) peab kehtima võrratus $d(a,y) \leqslant d(a,v)$.
- Kuna $a, \dots, x, y$ ja $a, \dots, x$ on minimaalsed ahelad, siis

$$d(a,x) + \omega_{xy} = \omega(a, \dots, x) + \omega(x,y) = \omega(a, \dots, x, y) = d(a,y).$$

- Kuna tipp x lisati hulka S mingil varasemal etapil, siis tema jaoks kehtib induktsiooni eeldus: $L[x] \leqslant d(a,x)$. Järelikult

$$L[x] + \omega_{xy} \leqslant d(a,x) + \omega_{xy}.$$

- Kuna tipp x lisati hulka S mingil varasemal etapil, siis kõik temast väljuvad kaared (muuhulgas $e = (x,y)$) on for-tsüklis läbi vaadatud. Seega $L[y] \neq \infty$ ja

$$L[y] \leqslant L[x] + \omega_{xy}.$$

- Samal etapil, kus u väärtuseks valiti v, jäeti valimata y, mis oli ka väljaspool hulka S. Seega valiku hetkel peab kehtima võrratus

$$L[v] \leqslant L[y].$$

- Eelnevat kokku võttes näeme, et

$$L[v] \leqslant L[y] \leqslant L[x] + \omega_{xy} \leqslant d(a,x) + \omega_{xy} = d(a,y) \leqslant d(a,v),$$

  mida oligi vaja.

□

Märkus 2.124 Dijkstra algoritm leiab ainult lühimate teede pikkused tipust a hulka S kuuluvatesse tippudesse. Kui soovime leida ka lühimatesse teedesse kuuluvaid tippe, siis tuleks algoritmi pisut modifitseerida võttes iga tipu i jaoks kasutusele suuruse $P[i]$, mis näitab, milline on lühimas tees tipust a tippu i eelviimane tipp. Algväärtustamisel võib lugeda, et $P[i] := a$ ja kui if-lauses toimub $L[v]$ uuendamine, siis tuleks lisada ka omistamine $P[v] := u$. Pärast algoritmi töö lõppu saame tipust a tippu z viiva lühima tee tipud välja lugeda niiöelda vastupidises järjekorras:

$$z, P[z], P[P[z]], \dots, a.$$

Märkus 2.125 Millises järjekorras lisatakse tipud hulka S? Olgu pärast Dijkstra algoritmi täitmist

$$S = \{v_1, v_2, \ldots, v_r\},$$

kusjuures esimesena on lisatud v_1 (s.t. $v_1 = a$), teisena v_2 jne. Tuleb välja, et

$$d(a, v_1) \leqslant d(a, v_2) \leqslant \ldots \leqslant d(a, v_r),$$

s.t. tippe lisatakse hulka S tipule a läheduse järjekorras. Selle näitamiseks vaatleme iga $i \in \{1, \ldots, r-1\}$ korral seda hetke, kui u-ks valitakse v_i. Sel hetkel kehtib iga $j \in \{i+1, \ldots, r\}$ jaoks võrratus

$$L[v_i] \leqslant L[v_j].$$

Algoritmi edasises töös $L[v_i]$ ei muutu, kuid $L[v_{i+1}]$ võib väheneda. Nimelt kui kehtib võrratus $L[v_i] + \omega_{v_i v_{i+1}} < L[v_{i+1}]$, siis toimub omistamine

$$L[v_{i+1}] := L[v_i] + \omega_{v_i v_{i+1}}.$$

Kuna aga kaarte kaalud on positiivsed, siis ka pärast seda omistamist jääb kehtima võrratus $L[v_i] \leqslant L[v_{i+1}]$. while-tsükli järgmisel läbimisel valitakse u ossa v_{i+1} ja $L[v_{i+1}]$ väärtust enam ei muudeta. Seega

$$d(a, v_i) = L[v_i] \leqslant L[v_{i+1}] = d(a, v_{i+1}).$$

Tõestatud omadust võib kasutada näiteks sellises olukorras, kus ülesandeks on teha kindlaks, kas tipust a leidub suunatud ahel tippu z, mille pikkus on väiksem kui etteantud positiivne konstant δ. Kui pärast i-ndat sammu z ei ole veel hulgas S, aga $d(a, v_i) \geqslant \delta$, siis võib algoritm töö lõpetada ja teatada, et sellist teed ei leidu.

Sisukord

Kirjandus

[1] J. Bang-Jensen, G. Gutin, Digraphs: Theory, Algorithms and Applications, Springer-Verlag, 2007.

[2] B. Bollobás, Graph Theory: An Introductory Course, Springer-Verlag, 1985.

[3] A. Buldas, P. Laud, J. Willemson, Graafid, Tartu Ülikooli Kirjastus, 2008.

[4] K. Ciesielski, Set Theory for the Working Mathematician, Cambridge University Press, 1997.

[5] S. Even, Graph algorithms, Cambridge University Press, Cambridge, 2012.

[6] S. Hedman, A First Course in Logic, Oxford University Press, 2004.

[7] T. Hõim, J. Langemets, Matemaatiline maailmapilt, loengukonspekt, 2017.

[8] R. Palm, R. Prank, Sissejuhatus matemaatilisse loogikasse, Tartu Ülikooli Kirjastus, 2004.

[9] R. Palm, Diskreetse matemaatika elemendid, Tartu Ülikooli Kirjastus, 2003.

[10] R. Prank, kursuse "Graafid ja matemaatiline loogika" loengute slaidid, Tartu, 2017.

[11] R. Prank, Lausearvutuse kordamine, õppematerjal, Tartu, 2017.