

Diskreetne matemaatika I

Kevad 2019

Loengukonspekt

Lektor: Valdis Laan

20. juuni 2019. a.

Sisukord

1	Matemaatiline loogika	7
1.1	Lausearvutus	7
1.1.1	Põhimõistete meeldetuletamine	7
1.1.2	Tõesuspuud	13
1.2	Lausearvutuse valemite normaalkujud	17
1.2.1	Valemite teisendamine	17
1.2.2	Normaalkujudest üldiselt	18
1.2.3	Täielik disjunktiiivne normaalkuju	18
1.2.4	Täielikule disjunktiiivsele normaalkujule teisendamine	22
1.2.5	TDNK omadused ja rakendused	23
1.2.6	Mittetäielik disjunktiiivne normaalkuju	24
1.2.7	Konjunktiivsetest normaalkujudest	25
1.3	Predikaatarvutus	27
1.3.1	Indiviidid ja predikaadid	27
1.3.2	Kvantorid	29
1.3.3	Predikaatarvutuse süntaks	30
1.3.4	Signatuuri interpretatsioonid	34
1.3.5	Valemite omadused	39
1.3.6	Tõesuspuu predikaatarvutuses	40
1.3.7	Valemite samaväärsus. Predikaatloogika põhisamaväärsused	43
1.3.8	Valemi prefikskuju	49
1.4	Teoreem ja tõestus. Tõestustaktikad	52
1.4.1	Teoreemidest ja tõestustest	52
1.4.2	Väide on kujul $\mathcal{F} \& \mathcal{G}$	53
1.4.3	Eeldus on kujul $\mathcal{F} \& \mathcal{G}$	54
1.4.4	Väide on kujul $\mathcal{F} \vee \mathcal{G}$	54
1.4.5	Eeldus on kujul $\mathcal{F} \vee \mathcal{G}$	54
1.4.6	Väide on kujul $\mathcal{F} \Rightarrow \mathcal{G}$	54
1.4.7	Eeldus on kujul $\mathcal{F} \Rightarrow \mathcal{G}$	55
1.4.8	Väide on kujul $\neg \mathcal{F}$	55
1.4.9	Eeldus on kujul $\neg \mathcal{F}$	56
1.4.10	Väide on kujul $\mathcal{F} \Leftrightarrow \mathcal{G}$	56
1.4.11	Eeldus on kujul $\mathcal{F} \Leftrightarrow \mathcal{G}$	56
1.4.12	Väide on kujul $\forall x \mathcal{F}(x)$	57

1.4.13	Eeldus on kujul $\forall x \mathcal{F}(x)$	57
1.4.14	Väide on kujul $\exists x \mathcal{F}(x)$	57
1.4.15	Eeldus on kujul $\exists x \mathcal{F}(x)$	57
1.4.16	Näide tõestustaktikate kasutamisest	58
1.5	Aksiomaatilised teooriad. Peano aksiomaatika	60
1.5.1	Aksiomaatilised teooriad	60
1.5.2	Peano aritmeetika	61
2	Graafiteooria	69
2.1	Graafi mõiste	69
2.2	Ahelad ja tsüklid	75
2.3	Graafi sidusus	78
2.4	Graafide isomorfism	83
2.5	Euleri ja Hamiltoni graafid	85
2.6	Puud	89
2.6.1	Puude põhiomadused	89
2.6.2	Toespuid	92
2.7	Suunatud graafid	98
2.7.1	Suunatud graafide põhiomadused	98
2.7.2	Lühima tee leidmise ülesanne	106

Eessõna

Tegemist on Tartu Ülikooli 2019. a. kevadsemestri kursuse “Diskreetne matemaatika I” loengukonspektiga. Lisaks sellele konspektile on kasulik tutvuda ka muude õppematerjalidega. Iseäranis kasulik on lugeda õpikuid [9] ja [10].

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, Ago-Erik Rieti ja Uno Hämarikku arvukate asjalike märkuste eest, mis on aidanud konspekti kvaliteeti parandada. Ka mitmed üliõpilased on konspektist vigu leidnud ja parandusettepanekuid teinud, tänud neilegi.

Peatükk 1

Matemaatiline loogika

Kursuse esimeses pooles tutvume mõnede teemadega matemaatilise loogikast. Kordame üle lausearvutuse põhimõisted, teeme sissejuhatuse predikaatloogikasse, vaatame, kuidas matemaatilist loogikat saab kasutada teoreemide tõestamisel ning lõpuks tutvume aksiomaatilise teooria ideega, muuhulgas näitame, kuidas saab aksiomaatiliselt konstrueerida naturaalarvud (nn. Peano aksiomaatika).

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 nimeatakse **lausemuutujateks**. Grammatilistele seostele vastavad **lausearvutuse tehted**.

Liitlausete kohta tehakse veel järgmised eeldused.

- Liitlauseid võib moodustada suvalistest komponentlausetest, eeldamata nende vahelist 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 sümboolitega. Matemaatilise maailmapildi kursuses kasutati tähiseid $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Raamatus [9] on kasutusel komplekt $\neg, \&, \vee, \rightarrow, \leftrightarrow$. Käesolevas kursuses me eelistame sümboleid $\neg, \&, \vee, \Rightarrow, \Leftrightarrow$.

Lausearvutuse valemid on teatud formaalsed avaldised, mis moodustatakse lausemuutujatest ja tehtemärkidest $\neg, \&, \vee, \Rightarrow, \Leftrightarrow$. Täpne definitsioon on järgmine.

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 kirjanekus, 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 valemide 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 $X_1, X_2, \dots, X_n$ 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 $\mathcal{H} = 0$.

Definitsioonis 1.4 esitatud reeglid võib esitada tabeli kujul järgmiselt:

$\mathcal{G}$	$\mathcal{H}$	$\mathcal{G} \& \mathcal{H}$	$\mathcal{G} \vee \mathcal{H}$	$\mathcal{G} \Rightarrow \mathcal{H}$	$\mathcal{G} \Leftrightarrow \mathcal{H}$	$\neg\mathcal{G}$
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

Näide 1.5 Leiame valemi

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

tõeväärtuse väärtustusel $A = 1, B = 0$. Definitsiooni 1.4 punkti 2 põhjal on $A \& B = 0$. Sama definitsiooni punkti 4 põhjal on $A \Rightarrow A \& B = 0$, s.t. valem $\mathcal{F}$ on väär sellel väärtustusel. Põhimõtteliselt võiks selle arutluskäigu sümbolkujul kirja panna järgmiselt:

$$\mathcal{F}(1, 0) = 1 \Rightarrow 1 \& 0 = 1 \Rightarrow 0 = 0,$$

s.t. võiksime lausemuutujate asemele kirjutada nende tõeväärtused ja sooritada tõeväärtuste vahel vajalikud tehted vastavalt eelnevale tabelile.

Märkus 1.6 Mainime, et lausearvutuse valemi tõeväärtuse leidmine on väga sarnane sellega, kuidas leitakse algebralise avaldise väärtus muutujate mingite konkreetsete väärtuste korral. Näiteks kui meil on avaldis

$$f(x, y) = x + x \cdot y,$$

siis tema väärtus $x = 2, y = 5$ korral on reaalarv

$$f(2, 5) = 2 + 2 \cdot 5 = 2 + 10 = 12.$$

Selle väärtuse saame asendades avaldisse muutujate asemele nende väärtused ja sooritades teh-
ted.

Kui kirjutame lausearvutuse valemi 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	0	0	0	0	0	1	0
1	0	1	0	0	0	0	1	0
1	0	0	0	0	0	0	1	1
0	1	1	1	1	1	1	0	0
0	1	0	1	0	1	1	0	0
0	0	1	1	0	1	1	0	0
0	0	0	1	0	1	0	1	1

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

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

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

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

nimetatakse n -kohalisteks **Boole'i¹ funktsioonideks**.

Näide 1.7 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 $f(1, 0) = 1 \& 0 = 0$.

¹George Boole (1815–1864) — inglise matemaatik

Märkus 1.8 Formaalselt võib lausemuutujate $X_1, \dots, X_n$ väärtustust vaadelda kui kujutust

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

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 $\alpha(\mathcal{F}) = \alpha(\mathcal{G}) \oplus \alpha(\mathcal{H})$.

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 1.9 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 1.10 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 1.11 ([7, lause 3.13]) *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eituse $\neg \mathcal{F}$ on samaselt väär.*

Teoreem 1.12 ([7, lause 3.14]) *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eituse $\neg \mathcal{F}$ ei ole samaselt tõene.*

Definitsioon 1.13 Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **samaväärseteks**, kui nende tõeväärtused on võrdsed igal neis valemis 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.

Näide 1.14 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. Kui vaatleme kõigi lausearvutuse valemite hulka, milles esinevad lausemuutujad kuuluvad hulka $\{X_1, X_2, X_3, \dots\}$, siis samaväärsuse seos $\equiv$ on binaarne seos sellel hulgal. On võimalik näidata, et see seos on ekvivalentsiseos.

Teoreem 1.15 ([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. $\mathcal{F} \& (\mathcal{F} \vee \mathcal{G}) \equiv \mathcal{F}$ | LS8. $\mathcal{F} \vee \mathcal{F} \& \mathcal{G} \equiv \mathcal{F}$ |
| 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 1.16 Öeldakse, et valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ **järeldub** valem $\mathcal{G}$, kui igal neis valemis esinevate muutujate väärtustusel, millel $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{G}$ tõene. Sellisel juhul kirjutatakse

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

Teoreem 1.17 ([7, teoreem 4.7]) *Valemitest $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$ parajasti siis, kui valem $\mathcal{F}_1 \& \mathcal{F}_2 \& \dots \& \mathcal{F}_n \Rightarrow \mathcal{G}$ on samaselt tõene.*

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

Näide 1.18 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 1.19 Lihtne on veenduda, et mistahes valemite $\mathcal{F}$ ja $\mathcal{G}$ korral

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

Teoreem 1.20 ([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:

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

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 lahenduseeni 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:

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

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

- Konjunktsioon ja disjunktsioon:

$$\begin{array}{c} \mathcal{F} \& \mathcal{G} = 1 \\ | \\ \mathcal{F} = 1 \\ | \\ \mathcal{G} = 1 \end{array}$$

$$\begin{array}{cc} \mathcal{F} \& \mathcal{G} = 0 & \\ / & \backslash \\ \mathcal{F} = 0 & \mathcal{G} = 0 \end{array}$$

$$\begin{array}{cc} \mathcal{F} \vee \mathcal{G} = 1 & \\ / & \backslash \\ \mathcal{F} = 1 & \mathcal{G} = 1 \end{array}$$

$$\begin{array}{c} \mathcal{F} \vee \mathcal{G} = 0 \\ | \\ \mathcal{F} = 0 \\ | \\ \mathcal{G} = 0 \end{array}$$

- Implikatsioon ja ekvivalents:

$$\begin{array}{cc} \mathcal{F} \Rightarrow \mathcal{G} = 1 & \\ / & \backslash \\ \mathcal{F} = 0 & \mathcal{G} = 1 \end{array}$$

$$\begin{array}{c} \mathcal{F} \Rightarrow \mathcal{G} = 0 \\ | \\ \mathcal{F} = 1 \\ | \\ \mathcal{G} = 0 \end{array}$$

$$\begin{array}{cc} \mathcal{F} \Leftrightarrow \mathcal{G} = 1 & \\ / & \backslash \\ \mathcal{F} = 1 & \mathcal{F} = 0 \\ | & | \\ \mathcal{G} = 1 & \mathcal{G} = 0 \end{array}$$

$$\begin{array}{cc} \mathcal{F} \Leftrightarrow \mathcal{G} = 0 & \\ / & \backslash \\ \mathcal{F} = 1 & \mathcal{F} = 0 \\ | & | \\ \mathcal{G} = 0 & \mathcal{G} = 1 \end{array}$$

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 valem $\mathcal{F} \Leftrightarrow \mathcal{G}$ saab olla väär täpselt kahel juhul: kui $\mathcal{F}$ on tõene ja $\mathcal{G}$ on väär või kui $\mathcal{F}$ on väär ja $\mathcal{G}$ on tõene.

Näide 1.21 Teha kindlaks, kas valem

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

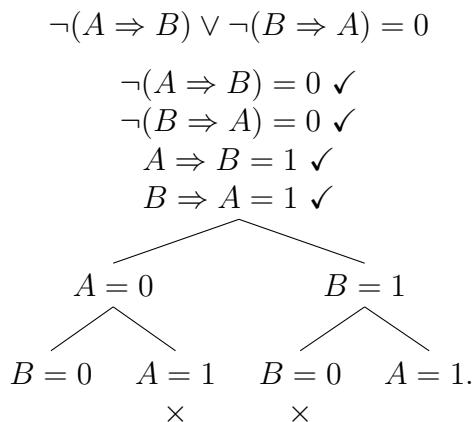
saab olla mingil väärtustusel väär.

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 analüüsimate 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



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, leidub väärtustusi, millel esialgne valem on väär”.

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 1.22 Teha kindlaks, kas valem

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

on samaselt tõene. Selleks kirjutame tõesuspuid 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”.) Tõesuspuid näeb välja järgmine:

$$\begin{array}{c} \neg(A \& B) \Rightarrow \neg A \vee \neg B = 0 \\ \neg(A \& B) = 1 \checkmark \\ \neg A \vee \neg B = 0 \checkmark \\ A \& B = 0 \checkmark \\ \neg A = 0 \checkmark \\ \neg B = 0 \checkmark \\ A = 1 \\ B = 1 \\ \swarrow \quad \searrow \\ A = 0 \quad B = 0 \\ \times \quad \times \end{array}$$

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 tõesuspuidude kohta võib leida raamatust [9], lk. 17–18.

Tõesuspuiduga saab valemi omadusi kontrollida järgmiselt.

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

Tõesuspuid abil saab kontrollida, kas valemitest $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ järeldeb valem $\mathcal{G}$. Selleks üritame leida valemities esinevate muutujate väärtustust, mille korral

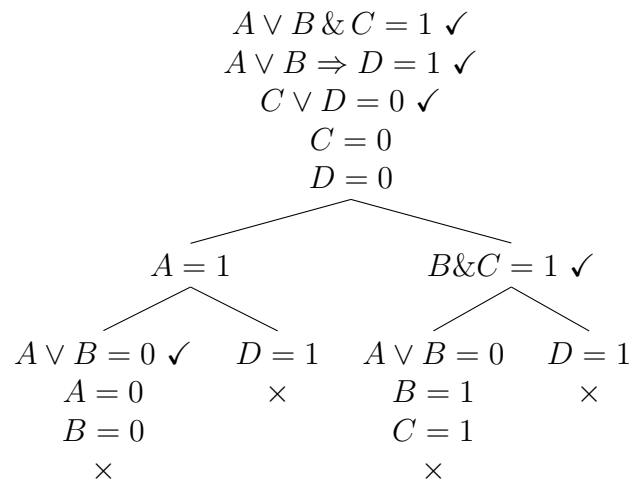
$$\mathcal{F}_1 = 1, \mathcal{F}_2 = 1, \dots, \mathcal{F}_n = 1 \quad \text{ja} \quad \mathcal{G} = 0.$$

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

Näide 1.23 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:



Kuna kõik harud on vastuolulised, siis järeldumine kehtib.

1.2 Lausearvutuse valemite normaalkujud

1.2.1 Valemite teisendamine

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

Lemma 1.24 *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 $\mathcal{H} \oplus \mathcal{F} \equiv \mathcal{H} \oplus \mathcal{G}$. $\square$

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 esialgsesga samaväärne.*

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

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

Näide 1.25 Kasutades lausearvutuse põhissamaväärsusi saame lihtsustada:

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

Paneme tähele, et selles samaväärsuste ahelas oleme teise ja neljanda samaväärsuse märgi juures kasutanud substitutsiooniprintsiipi. Kuna seos $\equiv$ on transitiivne, siis võime öelda, et $A \& B \& A \equiv A \& B$. Et valemis $A \& B$ on vähem lausemuutujaid, siis võime öelda, et see valem on lihtsam kui esialgne valem $A \& B \& A$.

Iga lausearvutuse valemi jaoks leidub temaga samaväärne valem, mis sisaldab ainult kahte tehet. Seega põhimõtteliselt lausearvutusega tegelemisel ei olegi tingimata viit tehet vaja.

Teoreem 1.26 ([7, lause 4.21]) *Iga lausearvutuse valemi jaoks leidub temaga samaväärne valem, mis sisaldab ainult järgmisi tehteid:*

- a) $\&$ ja $\neg$;
- b) $\vee$ ja $\neg$;
- c) $\Rightarrow$ ja $\neg$.

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

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0. \quad (1.1)$$

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 tunduvalt lihtsam teha. Samuti on kahe algebralise avaldise võrdsust kontrollida lihtsam, kui nad on esitatud polünoomi kujul — piisab vaid võrrelda vastavate polünoomide kordajaid. 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

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

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 (ellipsi puhul näiteks pooltelgede pikkusi). Teist järku joontest ja pindadest on juttu kursuses “Analüütiline geomeetria”.

Osutub, et ka lausearvutuse valemite puhul on olemas normaalkujud, mis on esialgsete valemitega samaväärsed (definiitsiooni 1.13 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

Definiitsioon 1.28 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 1.29 Lihtkonjunktsiooniks ehk elementaarkonjunktsiooniks nimetatakse lausearvutuse valemit, mis on moodustatud literaalidest kasutades ainult konjunktsiooni tehet, kusjuures ükski lausemuutuja ei esine selles valemis mitu korda.

Definitsioon 1.30 Lihtkonjunktsiooni nimetatakse **täielikuks**, kui vaadeldavatest muutujatest igaüks esineb selles täpselt ühe korra.

Seega lihtkonjunktsioon on valem kujul

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

kus $\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_n$ on literaalid, mis sisaldavad erinevaid lausemuutujaid. Näiteks valem $A \& \neg B \& C$ on täielik lihtkonjunktsioon lausemuutujatest A, B ja C , kuid $\neg A \& C$ on mitetäielik lihtkonjunktsioon muutujatest A, B ja C . Valem $A \& \neg B \& A \& C$ ei ole lihtkonjunktsioon.

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

Näide 1.32 Valem

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

on TDNK-l. Sellel TDNK-l on kolm liiget: $A \& B \& C$, $A \& \neg B \& C$ ja $A \& B \& \neg C$. Valem

$$\mathcal{G} = A \vee B \& \neg C \vee \neg A \& C$$

on DNK-l, aga mitte TDNK-l.

Lepime kokku, et mistahes lausemuutuja X korral kasutame tähistusi

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

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

Näide 1.33 Arvestades seda kokkulepet võime valemi $\mathcal{F}$ näitest 1.32 kirja panna kujul

$$\mathcal{F} = A^1 \& B^1 \& C^1 \vee A^1 \& B^0 \& C^1 \vee A^1 \& B^1 \& C^0.$$

Lemma 1.34 Iga $\alpha \in \{0, 1\}$ korral

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

(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 $X = 0$. $\square$

Uurime nüüd, millistel väärtustustel on TDNK-l olev valem tõene ja millistel väär.

Teoreem 1.35 Täielike lihtkonjunktsioonide disjunktsioon

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

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

TÕESTUS. TARVILIKKUS. Eeldame, et valem $\mathcal{F}'$ on tõene mingil väärtustusel

$(\beta_1, \dots, \beta_n) \in \{1, 0\}^n$. Valemi tõeväärtuse definitsiooni (vt. definitsiooni 1.4 punkti 3) tõttu leidub siis selline $i \in \{1, \dots, m\}$, et sellel väärtustusel $X_1^{\alpha_{i1}} \& \dots \& X_n^{\alpha_{in}} = 1$. Sama definitsiooni punkti 2 põhjal peavad siis kehtima võrdused

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

Tänu lemmale 1.34

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

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

PIISAVUS. Andes muutujatele $X_1, \dots, X_n$ väärtustuse $(\alpha_{i1}, \dots, \alpha_{in})$, kus $i \in \{1, \dots, m\}$, ja kasutades lemmat 1.34 võime kirjutada, et

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

Seega ka

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

ja vastavalt definitsioonile 1.4 on valem $\mathcal{F}'$ tõene sellel väärtustusel. $\square$

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 disjunktiiivsel 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. Teoreemi 1.35 põhjal saame siis valemi $\mathcal{F}'$ välja kirjutada.

Näide 1.36 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 (täpsemalt selle 6. veerust, mis annab valemi $\mathcal{F}$ tõeväärtused) näeme, et $\mathcal{F}$ on tõene viiel väärtustusel kaheksast. 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

$$\mathcal{F}' = A \& B \& C \vee \neg A \& B \& C \vee \neg A \& B \& \neg C \vee \neg A \& \neg B \& C \vee \neg A \& \neg B \& \neg C. \quad (1.2)$$

1.2.4 Täielikule disjunktiiivsele normaalkujule teisendamine

Teine võimalus TDNK leidmiseks on kasutada järgmist algoritmi.

Täielikule disjunktiiivsele 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 disjunkttsiooni.

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 disjunkttsioonide konjunktsioonid konjunktsioonide disjunkttsioonidega.

4. Kui esineb samaselt väärraid 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 disjunktiiivse normaalkuju.

5. Täieliku disjunktiiivse normaalkuju saamiseks tuleb iga lihtkonjunktsioon teha täielikuks. Kui näiteks lihtkonjunktsioonis $\mathcal{K}$ puudub 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 1.37 Sammul 4 võib juhtuda, et kõik konjunktsioonid on samaselt väärad. Selisel juhul peaksime nad kõik ära jätma ning tegemist on samaselt väärade valemiga. Selles olukorras öeldakse, et antud valemil puudub TDNK. Mõnikord öeldakse teooria ühtsuse huvides, et samaselt väärade valemite TDNK on tühi valem — valem, mis ei sisalda ühtegi liiget.

Näide 1.38 Leiame TDNK valemile

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

Rakendame algoritmi:

$$\mathcal{F} \equiv (\neg A \vee B \& C) \vee \neg(A \vee \neg(B \vee C)) \quad (\text{Samm 1})$$

$$\equiv \neg A \vee B \& C \vee \neg A \& \neg \neg(B \vee C) \quad (\text{Samm 2})$$

$$\equiv \neg A \vee B \& C \vee \neg A \& (B \vee C) \quad (\text{Samm 2})$$

$$\equiv \neg A \vee B \& C \vee \neg A \& B \vee \neg A \& C. \quad (\text{Samm 3})$$

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

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

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

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

$$\equiv \neg A \& B \& C \vee \neg A \& B \& \neg C \vee \neg A \& \neg B \& C \vee \neg A \& \neg B \& \neg C \vee A \& B \& C. \quad (\text{Samm 6})$$

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 tehete 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:

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

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

Teoreem 1.39 *Iga Boole'i funktsiooni $f : \{0, 1\}^n \rightarrow \{0, 1\}$ jaoks leidub lausearvutuse valem $\mathcal{F}(X_1, \dots, X_n)$, mis ei sisalda muid tehtemärke kui $\&$, $\vee$ ja $\neg$, ning mille poolt määratud Boole'i funktsioon on f .*

TÕESTUS. Olgu antud Boole'i funktsioon $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Leiame kõik järjendid $(\alpha_1, \dots, \alpha_n) \in \{0, 1\}^n$, mille korral $f(\alpha_1, \dots, \alpha_n) = 1$. Kui selliseid järjendeid leidub vähemalt üks, siis teoreemi 1.35 abil saame moodustada TDNK-l oleva lausearvutuse valemi $\mathcal{F} = \mathcal{F}(X_1, \dots, X_n)$, nii et $\mathcal{F}$ on tõene parajasti nendel väärtustustel $(\alpha_1, \dots, \alpha_n)$, mille korral $f(\alpha_1, \dots, \alpha_n) = 1$. Seega f on valemi $\mathcal{F}$ poolt määratud Boole'i funktsioon.

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

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 1.38 nägime, et valem

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

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 1.40 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 1.41 Võib veenduda (nt. tõeväärtustabeli abil), et valemi

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

disjunktiiivseks 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 Konjunktiiivsetest normaalkujudest

Vahetades ära konjunktsiooni ja disjunkttsiooni rollid võib rääkida valemi (täielikust) konjunktiiivsest normaalkujust.

Definitsioon 1.42 Lausemuutujate $X_1, \dots, X_n$ **täielikuks lihtdisjunkttsiooniks** ehk **täielikuks elementaardisjunkttsiooniks** nimetatakse literaalide disjunkttsiooni

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

Definitsioon 1.43 Valemi $\mathcal{F}$ **konjunktiiivseks normaalkujuks** (lühidalt KNK) nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate lihtdisjunkttsioonide konjunktsiooni. Kui kõik selles normaalkujus esinevad lihtdisjunkttsioonid on täielikud, siis öeldakse, et on tegemist **täieliku konjunktiiivse normaalkujuga** (lühidalt TKNK).

Niisiis TKNK-l olev valem näeb välja nii:

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

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

Näide 1.44 Näiteks valem

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

muutujate A ja B suhtes on täielikul konjunktiiivsel normaalkujul.

Analoogiliselt teoreemiga 1.35 saab tõestada järgmise tulemuse.

Teoreem 1.45 *Täielik konjunktiiivne normaalkuju*

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

on väär väärtustustel $(\neg\alpha_{i1}, \dots, \neg\alpha_{in})$, $i \in \{1, \dots, m\}$, 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 $(\alpha_1, \dots, \alpha_n)$ korral lisame TKNK-sse täieliku lihtdisjunktsiooni $X_1^{\neg\alpha_1} \vee \dots \vee X_n^{\neg\alpha_n}$. Näiteks kui valem $\mathcal{F} = \mathcal{F}(A, B, C)$ on väär väärtustustel

$$(1, 1, 1), (1, 0, 0), (0, 0, 1),$$

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 konjunktiiivse normaalkuju.

Konjunktiiivseid normaalkujusid kasutatakse tihti teoreemide automaattõestamisel, s.t. teoreemide tõestamisel arvutiprogrammide abiga.

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 lihtlauseid 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	$\dots + \dots = \dots$
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 hulgal² $\mathbb{N}$ 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 1.46 Olgu M mittetühi hulk. Hulgal M määratud **n -kohaliseks predikaadiks** nimetatakse kujutust $P : M^n \rightarrow \{1, 0\}$. Hulka M nimetatakse sellise predikaadi **indiviidide piirkonnaks**.

Definitsioon 1.47 Predikaadi $P : M^n \rightarrow \{1, 0\}$ **tõesuspiirkonnaks** nimetatakse hulka

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

Vaatleme veel näiteid.

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

Näide 1.48 Naturaalarvude hulgal $\mathbb{N}$ võib vaadelda ühekohalist predikaati $P(x) = “x \text{ on algarv}”$. See on siis kujutus

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

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

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

Selle predikaadi tõesuspiirkond on kõigi algarvude hulk.

Näide 1.49 Olgu M kõigi maailmajagude hulk

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

ning vaatleme kahekohalist predikaati

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

Siis näiteks

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

Märkus 1.50 Põhimõtteliselt võivad individid kuuluda ka erinevatesse hulkadesse, s.t. predikaat võib olla kujutus $M_1 \times \dots \times M_n \rightarrow \{1, 0\}$. Sellisel juhul räägitakse *mitmesordilistest predikaatidest*. Käesolevas kursuses me selliseid predikaate ei vaatle. Selles kursuses vaatleme ainult ühesordilist predikaatarvutust, kus eeldatakse, et komponentlausestes esinevad predikaadid on defineeritud ühel ja samal piirkonnal.

Märkus 1.51 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 lauseid vaadelda kui nullkohalisi predikaate, s.t. kujutusi $M^0 \rightarrow \{0, 1\}$. 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 $P(x_1, \dots, x_n)$ ja $Q(y_1, \dots, y_m)$ moodustada predikaadi

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

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

Näide 1.52 Vaatleme naturaalarvude hulgal $\mathbb{N}$ predikaate

$$\begin{aligned} P(x) &= \text{"}x \text{ on algarv"}, \\ Q(x, y) &= \text{"}y \text{ jagub arvuga } x". \end{aligned}$$

Siis võime moodustada kahekohalise predikaadi

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

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

Võib aga moodustada ka kolmekohalise predikaadi

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

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 1.53 Olgu $P(x_1, \dots, x_i, \dots, x_n)$ hulgal M määratud n -kohaline predikaat, kus $n \geq 1$, ning olgu $i \in \{1, \dots, n\}$.

1. Kirjutis

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

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

2. Kirjutis

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

tähistab $(n - 1)$ -kohalist predikaati, mis on tõene parajasti siis, kui argumentide $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ väärtused on sellised, et hulgas M leidub element m , mille korral on $P(x_1, \dots, m, \dots, x_n)$ 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 1.54 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 1.55 Vaatleme predikaati $Q(x, y)$ näitest 1.49. 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 1.56 Vaatleme hulgal $\mathbb{N}$ ühekohalist predikaati $P(x) = “x \text{ on algarv}”$. 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 1.57 Vaatleme hulgal $\mathbb{N}$ kolmekohalist predikaati

$$P(x, y, z) = “x + y = z”.$$

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

$$\forall y \forall z \exists x P(x, y, z) = \forall y \forall z “y \leq z” = \forall y “y = 0”$$

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 sümbolitena kasutatavatele tähtedele võib vajaduse korral lisada indekseid (näiteks võib vaadelda indiviidmuutujaid $x_1, \dots, x_n$). Funktsionaalsümboli ja predikaatsümboli argumentide arv peab selguma kontekstist.

Definitsioon 1.58 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 1.59 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 1.60 Naturaalarvude aritmeetikat saab kirja panna signatuurides

$$\begin{aligned} &\langle 0; ', +, \cdot; = \rangle, \\ &\langle 0, 1; +, \cdot; = \rangle, \\ &\langle 0, 1, 2, 3, \dots; +, \cdot; = \rangle. \end{aligned}$$

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

Näide 1.61 Rühmateooria jaoks võib kasutada signatuure

$$\begin{aligned} &\langle e; \cdot; = \rangle, \\ &\langle e; \cdot, {}^{-1}; = \rangle. \end{aligned}$$

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

Definitsioon 1.62 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 $t_1, t_2, \dots, t_n$ on termid, siis ka $f(t_1, t_2, \dots, t_n)$ on term.

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

Näide 1.63 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

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

Neist kaks esimest on muutujateta termid.

Näide 1.64 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:

$$46 \quad 3,14 \cdot y \quad ((2 \cdot x) + 1) \cdot (y + (4 \cdot x)).$$

Näide 1.65 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

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

Märkus 1.66 Matemaatikas on kõige enam levinud kahekohalised funktsionaalsümbolid. Neid nimetatakse enamasti tehtemärkideks. Seega tüüpiline term on avaldis, mis on moodustatud konstantsümbolitest ja muutujatest tehtemärkide abil.

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

Definitsioon 1.67 Predikaatarvutuse valemid on parajasti need avaldised, mis on moodustatud järgmiste reeglite abil.

1. Kui P on n -kohaline predikaatsümbol ja $t_1, \dots, t_n$ on termid, siis $P(t_1, \dots, t_n)$ on predikaatarvutuse valem.
2. Kui $\mathcal{F}$ on predikaatarvutuse valem, siis $\neg \mathcal{F}$ on predikaatarvutuse valem.
3. Kui $\mathcal{F}$ ja $\mathcal{G}$ on predikaatarvutuse valemid, siis $(\mathcal{F} \& \mathcal{G}), (\mathcal{F} \vee \mathcal{G}), (\mathcal{F} \Rightarrow \mathcal{G}), (\mathcal{F} \Leftrightarrow \mathcal{G})$ 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 valemite nimetatakse **atomaarseteks valemiteks** ehk **elementaarvalemiteks**. Kõiki antud valemi konstrueerimise käigus tekkinud valemite 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 1.68 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

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

ja mitteatomaarseid valemeid

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

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 valemities $\forall x \mathcal{G}$ 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 sellele, 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 1.69 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 1.70 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 tarvita-takse tihti ühte ja sama sümbolit mitmes erinevas tähenduses. Näiteks tehtemärk $+$ võib märkida reaalarvude liitmist, jäägiklasside liitmist, vektorite liitmist, maatriksite liitmist või hoopis funktsioonide liitmist. Need kõik on erinevad tehted, mis on defineeritud eri-nevatel 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 1.71 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 $f^\alpha : M_\alpha^n \rightarrow M_\alpha$;
3. iga n -kohalise predikaatsümboli $P \in \mathbf{P}$ mingiks n -kohaliseks predikaadiks $P^\alpha : M_\alpha^n \rightarrow \{1, 0\}$.

Märkus 1.72 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. Võrdusmärgi interpreteeritakse alati võrduspredikaadina.

Näide 1.73 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \dots; +, \cdot; =, < \rangle$. Anname sellele kolm erinevat interpretatsiooni.

1. $M = \mathbb{N}$ ja signatuuri sümboleid interpreteerime standardset.
2. $M = \mathbb{R}$ ja signatuuri sümboleid interpreteerime standardset.
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

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array},$$

ning $<$ on kahekohaline predikaat hulgal $\{0, 1\}$, mille tõesuspriirkond on $\{(0, 1)\}$ (s.t. $0 < 1$ ja ülejäänud paarid ei ole selles seoses).

Näide 1.74 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. $M = \text{Mat}_2(\mathbb{R})$ (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 järjest-rakendamine).
4. $M = \mathbb{Z}$, $e^\alpha = 0$, $*^\alpha = +$.
5. M on mingi mittetühja hulga A kõigi alamhulkade hulk $\mathcal{P}(A)$, $e^\alpha = A$, $*^\alpha = \cap$.

Kui fikseerime signatuuri mingi interpretatsiooni $\alpha = \langle M_\alpha; I_\alpha \rangle$ ja anname individ-muutujatele konkreetseid väärtused, siis tekib ka igale termile väärtus, milleks on hulga M_α mingi element.

Definitsioon 1.75 Termi t **väärtus** t^α interpretatsioonis α individmuutujate fikseeritud väärtustel leitakse järgmiste reeglite abil.

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

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

Jämedalt öeldes toimub termi väärtuse leidmine nii: pane muutujate asemele nende väärtused ja soorita vajalikud tehted.

Näide 1.76 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \dots; +, \cdot, =, < \rangle$. 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

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

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

Definitsioon 1.77 Predikaatarvutuse valemi $\mathcal{F}$ tõeväärtus $\mathcal{F}^\alpha$ interpretatsioonis α vabade muutujate fikseeritud väärtustusel leitakse järgmiste reeglite abil.

1. Kui $\mathcal{F} = P(t_1, \dots, t_n)$, kus P on n -kohaline predikaatsümbol ja $t_1, \dots, t_n$ on termid, siis $\mathcal{F}^\alpha = 1$ parajasti siis, kui $P^\alpha(t_1^\alpha, \dots, t_n^\alpha) = 1$.
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 $\mathcal{G}_{[x/m]}^\alpha = 1$, 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 $\mathcal{G}_{[x/m]}^\alpha = 1$, kus $[x/m]$ tähendab, et muutuja x väärtuseks loetakse element m .

Märkus 1.78 Kui $\mathcal{F}(x_1, \dots, x_n)$ on predikaatarvutuse valem vabade muutujatega $x_1, \dots, x_n$, siis tema tõeväärtust interpretatsioonis α vabade muutujate väärtustusel $(m_1, \dots, m_n)$ võib tähistada $\mathcal{F}^\alpha(m_1, \dots, m_n)$. Nii tekib meil kujutus

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

Niisiis valemi iga interpretatsioon tekitab ühe predikaadi.

Näide 1.79 Vaatleme signatuuri $\sigma = \langle 0, 1, 2, 3, \dots; +, \cdot, =, < \rangle$. 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 vastavalt definitsiooni 1.77 punktile 8 on valem $\mathcal{F}$ tõene $y = 6$ korral. Viimast asjaolu võib kirja panna kujul $\mathcal{F}(6) = 1$. On lihtne aru saada, et

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

Ülesanne 1.80 Leida järgmiste valemite tõeväärtused kolmes interpretatsioonis, mida vaatlesime näites 1.73 (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 1.81 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 1.74 vaadeldud interpretatsioonides vabade muutujate kõigi väärtuste korral?

Definitsioon 1.82 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 1.83 Interpretatsiooni α nimetatakse valemite hulga $\{\mathcal{F}_1, \dots, \mathcal{F}_n\}$ **mudeliks**, kui see interpretatsioon on iga üksiku valemi mudel.

Näide 1.84 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 mudelitenä. Millise valemite hulga mudeliteks on näiteks rühmad või Abeli rühmad?

Näide 1.85 Vaatleme signatuuris $\sigma = \langle \top; ; =, \leq \rangle$ valemite hulka

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

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

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

Lühemalt võib öelda, et valem $\mathcal{F}$ väljendab predikaati P , kui tema poolt tekitatud kujutus, mida mainisime märkuses 1.78, langeb kokku kujutusega P .

Näide 1.87 Valem $\mathcal{F}(y)$, mida vaatlesime näites 1.79, väljendab naturaalarvude hulgal defineeritud predikaati $P(y) = “y \text{ on paarisarv}”$.

Näide 1.88 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 1.89 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 1.90 Predikaatarvutuse valemite $\mathcal{F}$ 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 tõe lausearvutuse valemi ja asendame iga lausemuutuja mingi predikaatarvutuse valemiga, siis saame samaselt tõe predikaatarvutuse valemi. Näiteks valem

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

on samaselt tõene. Sarnasel viisil saab samaselt väärast lausearvutuse valemist tule-
tada samaselt väärast predikaatarvutuse valemist. Kuid on ka selliseid samaselt tõe-
seid või väärast predikaatarvutuse valemist, millel puudub analoog lausearvutuses.

Näide 1.91 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 1.92 Predikaatarvutuse valemite nimetatakse **kehtestatavaks**, kui ta on tõene vähemalt ühes interpretatsioonis vabade muutujate mingitel väärtustel.

Näide 1.93 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 $Q(x, y) = "x \geq y"$. 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 (Church³, 1936). *Ei leidu algoritmi, mis suvalise predikaatarvutuse valemi puhul suudaks kindlaks teha, kas see on samaselt tõene või ei.*

Teoreem 1.94 *Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eituse $\neg\mathcal{F}$ on samaselt väär.*

TÕESTUS. Definitsiooni 1.77 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. $\square$

Teoreem 1.95 *Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eituse $\neg\mathcal{F}$ ei ole samaselt tõene.*

TÕESTUS. Vaatleme valemite $\mathcal{F}(x_1, \dots, x_n)$ 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. $\square$

1.3.6 Tõesuspüü predikaatarvutuses

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

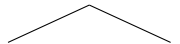
Järgnevas näites on vasakul ääres ridade numbrid ja paremal ääres on näidatud, millist eelnevast reast on antud rida saadud.

Näide 1.96 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 tõesuspüü.

³Alonzo Church (1903–1995) — ameerika matemaatik

1.	$\forall x P(x) \& \forall x Q(x) \Rightarrow \forall x (P(x) \& Q(x)) = 0 \checkmark$	
2.	$\forall x P(x) \& \forall x Q(x) = 1 \checkmark$	/1/
3.	$\forall x (P(x) \& Q(x)) = 0 \checkmark$	/1/
4.	$\forall x P(x) = 1$	/2/
5.	$\forall x Q(x) = 1$	/2/
6.	$P(c) \& Q(c) = 0 \checkmark$	/3/
		
7.	$P(c) = 0 \quad Q(c) = 0$	/6/
8.	$P(c) = 1 \quad P(c) = 1$	/4/
9.	$\times \quad Q(c) = 1$	/5/
		

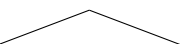
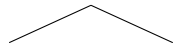
Selle puu read 2–5 on saadud definitsiooni 1.77 punktide 5 ja 3 põhjal. Rida 6 on saadud reast 3, mis ütleb, et $\forall x (P(x) \& Q(x)) = 0$. Definitsiooni 1.77 punkti 7 põhjal saame, et peab leiduma mingi element, tähistame seda sümboliga c , mille korral $P(c) \& Q(c) = 0$. Rea 7 saamiseks kasutame konjunktsiooni definitsiooni. Rea 8 saamiseks kasutame seda, et rea 4 tõttu peab iga x väärtuse korral $P(x)$ olema tõene, muuhulgas siis ka $P(c) = 1$. Rea 9 saame reast 5.

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

Näide 1.97 Uurime, kas valem

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

on samaselt tõene. Tekib järgmine tõesuspuu.

1.	$\exists x P(x) \& \exists x Q(x) \Rightarrow \exists x (P(x) \& Q(x)) = 0 \checkmark$	
2.	$\exists x P(x) \& \exists x Q(x) = 1 \checkmark$	/1/
3.	$\exists x (P(x) \& Q(x)) = 0$	/1/
4.	$\exists x P(x) = 1 \checkmark$	/2/
5.	$\exists x Q(x) = 1 \checkmark$	/2/
6.	$P(d) = 1$	/4/
7.	$Q(e) = 1$	/5/
8.	$P(d) \& Q(d) = 0 \checkmark$	/3/
9.	$P(e) \& Q(e) = 0 \checkmark$	/3/
		
10.	$P(d) = 0 \quad Q(d) = 0$	/8/
		
		
11.	$P(e) = 0 \quad Q(e) = 0$	/9/
		

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

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

Selles interpretatsioonis

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

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 1.98 Teha kindlaks, kas valem

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

on samaselt tõene.

Alustame tõesuspuu konstrueerimist:

- | | | |
|----|---|--------------|
| 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/ |

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

- | | | |
|----|---|--------------|
| 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/ |
| | $\times$ | |

Näeme, et valem on samaselt tõene.

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

Näide 1.99 Teha kindlaks, kas valem $\forall x \exists y P(x, y)$ on kehtestatav.

Konstrueerime tõesuspuu:

- | | | |
|----|-----------------------------------|-----|
| 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. | $\vdots$ | |

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 põhिसamaväärsused

Definitsioon 1.100 Predikaatarvutuse valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **samaväärseteks**, kui nende tõeväärtused on võrdsed igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel. Sellisel juhul kirjutatakse $\mathcal{F} \equiv \mathcal{G}$.

Kui vaatleme kõigi predikaatarvutuse valemite hulka, milles esinevad indiidmuutujad kuuluvad hulka $\{x_1, x_2, x_3, \dots\}$, siis on lihtne näha, et samaväärsuse seos $\equiv$ on ekvivalent-siseos sellel hulgal.

Definitsioon 1.101 Öeldakse, et valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ **järeldub** valem $\mathcal{G}$, kui igas interpretatsioonis valemite vabade muutujate kõikidel väärtustel, kus valemid $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene. Sellisel juhul kirjutatakse $\mathcal{F}_1, \dots, \mathcal{F}_n \models \mathcal{G}$.

Lause 1.102 Olgu $\mathcal{F}$ ja $\mathcal{G}$ predikaatarvutuse valemid. Siis

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

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 1.103 *Predikaatloogikas kehtivad järgmised põhisamaväärsused.*

PS1. *Kvantori ja eituse vahetamiseadus:*

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

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*

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

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

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

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

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

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

PS5. *Seotud muutujate ümbernimetamine:*

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

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

PS6. *Samaliigiliste kvantorite kommutatiivsus:*

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

TÕESTUS. Tõestame osa neist samaväärsusest. Selleks kasutame lauset 1.102.

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 element $m_0 \in M_\alpha$ nii, et $\mathcal{F}(m_0) = 0$. Siis aga $\neg \mathcal{F}(m_0) = 1$. Predikaatarvutuse valemi tõeväärtuse definitsiooni põhjal (vt. definitsiooni 1.77 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 $\mathcal{F}(m_0) = 0$. 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 oleme tõestanud, et $\neg \forall x \mathcal{F}(x) \models \exists x \neg \mathcal{F}(x)$ 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 1.77 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 1.77 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 järelneb, 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

definiitsiooni tõttu $\mathcal{F}(m_0) = 1$ või $\mathcal{G}(m_0) = 1$. Vastavalt valemi tõeväärtuse definiitsioonile 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 $\forall x \mathcal{F}(x) \& \mathcal{G} = 1$. Definiitsiooni 1.77 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 definiitsiooni 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 definiitsiooni 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 $\exists x \mathcal{F}(x) \& \mathcal{G} = 1$. Definiitsiooni 1.77 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. Demonst-

reerime siin teist võimalust:

$$\forall x (\mathcal{F}(x) \Rightarrow \mathcal{G}) \equiv \forall x (\neg \mathcal{F}(x) \vee \mathcal{G}) \quad (\text{LS14})$$

$$\equiv \forall x \neg \mathcal{F}(x) \vee \mathcal{G} \quad (\text{PS3b})$$

$$\equiv \neg \exists x \mathcal{F}(x) \vee \mathcal{G} \quad (\text{PS1b})$$

$$\equiv \exists x \mathcal{F}(x) \Rightarrow \mathcal{G}. \quad (\text{LS14})$$

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,

$$\exists x (\mathcal{F}(x) \Rightarrow \mathcal{G}) \equiv \exists x (\neg \mathcal{F}(x) \vee \mathcal{G}) \quad (\text{LS14})$$

$$\equiv \exists x \neg \mathcal{F}(x) \vee \mathcal{G} \quad (\text{PS3d})$$

$$\equiv \neg \forall x \mathcal{F}(x) \vee \mathcal{G} \quad (\text{PS1a})$$

$$\equiv \forall x \mathcal{F}(x) \Rightarrow \mathcal{G}. \quad (\text{LS14})$$

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. $\square$

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

Näide 1.104 Vaatleme signatuuri $\sigma = \langle e; *, \Rightarrow \rangle$ interpretatsiooni, mille kandja on teist järku reaalarvuliste elementidega ruutmaatriksite hulk $M = \text{Mat}_2(\mathbb{R})$ 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

$$\neg \forall x \mathcal{F}(x) = \text{“Ei ole nii, et kõik maatriksid on pööratavad”},$$

$$\exists x \neg \mathcal{F}(x) = \text{“Leidub maatriks, millel ei ole pöördmaatriksit”}.$$

Tänu teoreemi 1.103 punktile 1 teame, et need kaks väidet on samaväärsed.

Tekib loomulik küsimus, et kas teoreemi 1.103 punktis 2 võib konjunktsiooni asendada disjunktsiooniga ja vastupidi. Osutub, et vastus on eitav.

Lause 1.105 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 $\forall x (\mathcal{F}(x) \vee \mathcal{G}(x)) = 1$ (iga inimene on kas naissoost või meessoost), kuid $\forall x \mathcal{F}(x) \vee \forall x \mathcal{G}(x) = 0$, sest $\forall x \mathcal{F}(x) = 0$ ja $\forall x \mathcal{G}(x) = 0$ (ei ole nii, et kõik inimesed on naissoost või et kõik inimesed on meessoost). Seega

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

□

Ülesanne 1.106 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 1.103 punktis 6 nägime, et samaliigilisi kvantoreid võib ära vahetada. Kuidas on olukord eriliigiliste kvantoritega?

Lause 1.107 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 hulgaga $\mathbb{N}$ 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 1.108 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 1.109 Öeldakse, et predikaatarvutuse valem $\mathcal{F}$ on **prefikskujul**, kui ta ei sisalda kvantoreid või kui

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

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

Näide 1.110 Valem

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

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

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

aga ei ole prefikskujul.

Teoreem 1.111 Iga valemi jaoks leidub temaga samaväärne prefikskujul olev valem.

TÕESTUS. Vastavalt definitsioonile 1.67 saadakse predikaatarvutuse valemid atomaarsest valemist lausearvutuse tehete ja kvantorite abil. Tõestame induktsiooniga valemi struktuuri järgi, et iga selline valem on samaväärne prefikskujul oleva 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 tehete või kvantori rakendamise abil, on samuti samaväärne prefikskujul oleva valemiga. Niisiis olgu

$$\mathcal{F} \equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{F}_1, \quad \mathcal{G} \equiv Q'_1 y_1 Q'_2 y_2 \dots Q'_m y_m \mathcal{G}_1,$$

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 valemis 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

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

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

$$\begin{aligned} \mathcal{F} \& \mathcal{G} &\equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{F}_1 \& \mathcal{G} \\ &\equiv Q_1 x_1 (Q_2 x_2 \dots Q_n x_n \mathcal{F}_1 \& \mathcal{G}) & \text{(PS3)} \\ &\equiv Q_1 x_1 Q_2 x_2 (Q_3 x_3 \dots Q_n x_n \mathcal{F}_1 \& \mathcal{G}) & \text{(PS3)} \\ &\dots \\ &\equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n (\mathcal{F}_1 \& \mathcal{G}) & \text{(PS3)} \\ &\equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n (\mathcal{G} \& \mathcal{F}_1) & \text{(LS3)} \\ &\equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n (Q'_1 y_1 Q'_2 y_2 \dots Q'_m y_m \mathcal{G}_1 \& \mathcal{F}_1) \\ &\equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n Q'_1 y_1 Q'_2 y_2 \dots Q'_m y_m (\mathcal{G}_1 \& \mathcal{F}_1). & \text{(PS3)} \end{aligned}$$

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 tõestatud.

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

$$\forall x Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{F}_1 \quad \text{ja} \quad \exists x Q_1 x_1 Q_2 x_2 \dots Q_n x_n \mathcal{F}_1$$

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

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

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

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

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

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

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

ja vajaduse korral ka konjunktsiooni ja disjunktsiooni kommutatiivsust.

Näide 1.112 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 1.113 Vaatleme valemite

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

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 $\mathcal{E}_1, \dots, \mathcal{E}_n$, 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 $\mathcal{A}$ ”.

Näide 1.114 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”,
- $\mathcal{V}$ = “ $a^2 + b^2 = c^2$ ”.

Kui teoreemi eeldusi ja väiteid saab sobivas signatuuris esitada predikaatarvutuse valemite abil, siis sellise teoreemi võib loogika sümboolikat kasutades kirja panna kujul

$$\mathcal{E}_1, \dots, \mathcal{E}_n \models \mathcal{V}$$

või valemina

$$\mathcal{E}_1 \& \dots \& \mathcal{E}_n \Rightarrow \mathcal{V}.$$

Matemaatilises teoreemis on signatuur ja tema interpretatsioon α reeglina fikseeritud. See-
ga oleks tegelikult korrektsem kirjutada $\mathcal{E}_1, \dots, \mathcal{E}_n \models^\alpha \mathcal{V}$ ja tõlgendada seda sümboolikat
järgnevalt: interpretatsiooni α ja vabade muutujate mistahes väärtuste korral kui valemid
 $\mathcal{E}_1, \dots, \mathcal{E}_n$ on tõesed, siis ka valem $\mathcal{V}$ on tõene. Näiteks võib vaadelda teoreemi

$$(y : x), (z : x) \models^\alpha (y + z : x),$$

kus põhihulgaks on $\mathbb{N}$, kahekohalist tehtemärki $+$ interpreteerime naturaalarvude liitmis-
tehtena ja kahekohalist predikaatsümbolit $:$ tõlgendame kui jaguvusseost. Sõnades kõlaks
teoreem nii: *kui x, y, z on naturaalarvud, y jagub x -ga ja z jagub x -ga, siis ka $y + z$ ja-
gub x -ga*. Teoreemi tõestamiseks tuleks näidata, et järeldumine kehtib vabade muutujate
 x, y, z kõigi naturaalarvuliste väärtuste korral.

Järgnevas me siiski ei hakka kirjutama $\models^\alpha$ ja sümboolikat pisut kuritarvitades kasu-
tame lihtsalt sümbolit $\models$.

Selles paragrahvis räägime võimalikest tõestuse otsimise taktikatest. Täpsemalt öeldes
tuleb juttu sellest, milliseid tõestamise taktikaid pakub loogika: kuidas predikaatarvutuse
valemite abil kirja pandud 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.

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 valemite 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

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

Sellise teoreemi saab tõestada järgmise taktikaga: tõestame, et

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

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

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

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

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

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

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

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

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

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

$$\textit{Kui } n \textit{ on naturaalarv, siis } n(n+1) \textit{ on paarisarv}$$

tõestamiseks vaadelda eraldi juhte, kus n on paarisarv ($\mathcal{F}$) ja kus n on paaritu arv ($\mathcal{G}$), ning veenduda, et mõlemal juhul on $n(n+1)$ paarisarv ($\mathcal{V}$).

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

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

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Teoreemi tõestamiseks piisab, kui näitame, et

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

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 $\mathcal{E}_1, \dots, \mathcal{E}_{n-1}$ 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

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

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.

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

Sobiv väide $\mathcal{G}$ tuleb iga kord eraldi leida ja soovitatav 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

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

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

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

Näide 1.115 Tõestame teoreemi

Algarvude hulk ei ole lõplik.

Siin

$\mathcal{F} = \text{“algarvude hulk on lõplik”}$

ja eeldusteks on hästi tuntud faktid naturaalarvude aritmeetika kohta, mida me siin pikemalt välja kirjutama ei hakka.

Tõestamiseks oletame vastuväiteliselt, et algarvude hulk on lõplik ja koosneb algarvudest $p_1, \dots, p_n$. Vaatleme naturaalarvu $n = p_1 p_2 \dots p_n + 1$. See arv on suurem kui 1. Seega peab ta aritmeetika põhiteoreemi põhjal jaguma mingi algarvuga q . Kuna ainsad algarvud on $p_1, \dots, p_n$, siis peab leiduma selline $i \in \{1, \dots, n\}$, et $q = p_i$. Kuna arvud n ja $p_1 p_2 \dots p_n$ jaguvad q -ga, siis ka nende vahe, s.t. arv 1, jagub q -ga. Nii oleme näidanud, et eeldustest ja $\mathcal{F}$ -st järeljub väide

$$\mathcal{G} = \text{“arv 1 jagub algarvuga } q\text{”}.$$

Teisest küljest aga on hästi teada, et naturaalarvude omaduste tõttu kehtib $\neg \mathcal{G}$ (s.t. arv 1 ei jagu algarvuga q). Saadud vastuolu näitab, et $\mathcal{F}$ ei saa antud eelduste korral tõene olla. Seega peab tõene olema $\neg \mathcal{F}$.

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

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

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

Teoreemi tõestamiseks näidatakse harilikult, et

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

Mõnikord tõestatakse hoopis, et

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

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

Vaatleme olukorda, kus tõestatav teoreem on kujul

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

Ekvivalentsi kehtimist saab tõestamisel kasutada kahel viisil.

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

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

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

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

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

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

Elemendi a suvalisus tähendab seda, et eeldustes $\mathcal{E}_1, \dots, \mathcal{E}_n$ 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

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

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

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

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

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

Sellises olukorras tuleb lähtudes sellest, et kehtivad eeldused $\mathcal{E}_1, \dots, \mathcal{E}_n$ 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

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

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

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

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

1.4.16 Näide tõestustaktikate kasutamisest

Teeme üksikasjaliselt läbi ühe näidistõestuse, milles saame kasutada erinevaid tõestustaktikaid.

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 1.116 *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

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

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

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

Teoreemi väide on

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

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

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

Teoreem ise on seega kujul

$$\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3 \models \mathcal{V}_1 \& \mathcal{V}_2 \& \mathcal{V}_3.$$

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). Selle eelduse põhjal $(a \sqsubseteq a) \Leftrightarrow (a \sqsubset a) \vee (a = a)$. 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 disjunktsiooni definitsioonile peab tõene olema vähemalt üks järgnevast neljast lausest:
 - (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) Kui $a \sqsubset b$ ja $b \sqsubset a$, siis 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 võrdsused $a = b$ 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.

Ajalooliselt lõi esimese aksiomaatilise teooria vanakreeka matemaatik Eukleides (elas umbes aastatel 325–270 e.m.a.). Oma kuulsa teose “Elemendid” alguses sõnastas ta järgmised viis tasandi geomeetria aksioomi, millest lähtudes tõestas erinevaid teoreeme tasandi geomeetria kohta.

1. Igast punktist iga teise punktini saab tõmmata sirglõigu.
2. Iga sirglõigu saab pikendada sirgeks.
3. Saab joonistada mistahes raadiuse ja keskpunktiga ringjooni.
4. Kõik täisnurgad on omavahel võrdsed.
5. Kui mingi sirge lõikab kahte sirget nii, et samal pool tekkivad sisenurgad on kokku vähem kui kaks täisnurka, siis need kaks sirget lõikuvad samal pool, kus on need kaks sisenurka, mis on kokku väiksemad kui kaks täisnurka.

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. **Peano⁴ aritmeetika** aksioomid on järgmised:

$$\mathbf{P1.} \quad \forall x \neg(x' = 0);$$

$$\mathbf{P2.} \quad \forall x \forall y (x' = y' \Rightarrow x = y);$$

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

$$\mathbf{P4.} \quad \forall x \forall y (x + y' = (x + y)');$$

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

$$\mathbf{P6.} \quad \forall x \forall y (x \cdot y' = x \cdot y + x);$$

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 1.117 Me võime vaadelda hulka

$$\{0, 0', 0'', 0''', 0''', \dots\}$$

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 1.118 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?

⁴Giuseppe Peano (1858–1932) — itaalia matemaatik

Hulgateooria aksioomide põhjal (mida me selles kursuses küll ei käsitle) on olemas hulgad $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ jne., kusjuures need on kõik paarikaupa erinevad. Tähistame

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

Nagu näha,

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

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

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

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

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

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

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

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

$$\begin{aligned} n + 0 &:= n, & n + m' &:= (n + m)', \\ n \cdot 0 &:= 0, & n \cdot m' &:= n \cdot m + n. \end{aligned}$$

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

$0, 0', 0'', 0''', \dots$, 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 mittestandardised 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 selles teoreemid.

Teoreem 1.119 *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

$$\forall z ((a + b) + z = a + (b + z) \Rightarrow (a + b) + z' = a + (b + z')) \quad (1.3)$$

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

$$(a + b) + c = a + (b + c) \quad (1.4)$$

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. $\square$

Teoreem 1.120 *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 induktsiooniga, et valem $\forall x \mathcal{F}(x)$ on tõene.

Alus. Näitame, et valem

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

on tõene. Ka selleks kasutame induktsiooni. 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 1.121 *Naturaalarvudel on omadus*

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

TÕESTUS. Olgu a suvaline naturaalarv. Siis teoreemi 1.120 ja aksioomi P3 põhjal

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

□

Teoreem 1.122 *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,

$$a \cdot (b + 0) = a \cdot b \quad (\text{P3})$$

$$= a \cdot b + 0 \quad (\text{P3})$$

$$= a \cdot b + a \cdot 0. \quad (\text{P5})$$

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

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (1.8)$$

on tõene. Siis

$$a \cdot (b + c') = a \cdot (b + c)' \quad (\text{P4})$$

$$= a \cdot (b + c) + a \quad (\text{P6})$$

$$= (a \cdot b + a \cdot c) + a \quad (\text{eeldus (1.8)})$$

$$= a \cdot b + (a \cdot c + a) \quad (\text{teoreem 1.119})$$

$$= a \cdot b + a \cdot c'. \quad (\text{P6})$$

□

Teoreem 1.123 *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

$$a + c = b + c \Rightarrow a = b \quad (1.9)$$

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 $\forall z \mathcal{F}(z)$. $\square$

Ülesanne 1.124 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 $\leq$ järgmiselt:

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

Teoreem 1.125 *Seos $\leq$ 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 $a \leq a$.

Antisümmeetria. Peame näitama, et

$$\forall x \forall y ((x \leq y) \& (y \leq x) \Rightarrow (x = y)).$$

Tähistagu a, b suvalisi naturaalarve ning eeldame, et $a \leq b$ ja $b \leq a$. 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 1.123 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

$$\forall x \forall y \forall z ((x \leq y) \& (y \leq z) \Rightarrow (x \leq z)).$$

Tähistagu a, b, c suvalisi naturaalarve ning kehtigu võrratused $a \leq b$ ja $b \leq c$. 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 $\leq$ definitsiooni tõttu $a \leq c$. □

Ülesanne 1.126 Tõestada, et naturaalarvude järjestusseos $\leq$ on kooskõlas liitmise ja korrutamisega, s.t.

$$\begin{aligned} \forall x \forall y \forall z (x \leq y \Rightarrow x + z \leq y + z), \\ \forall x \forall y \forall z (x \leq y \Rightarrow x \cdot z \leq y \cdot z). \end{aligned}$$

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 [10], [3] ja [2].

Graafiteooria loojaks peetakse Leonhard Eulerit¹.

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). Mõnikord nimetatakse selliseid graafe **lihtgraafideks**.

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.

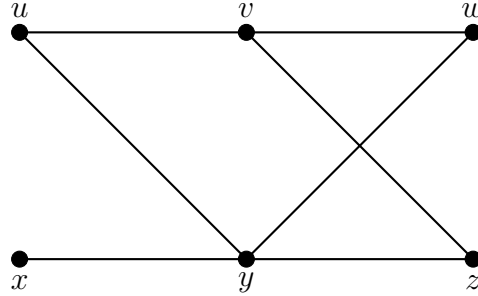
Definitsioon 2.2 Kui graafi tipp v kuulub servale e , siis öeldakse, et tipp v ja serv e on **intsidentsed**. Iga serv on intsidentne täpselt kahe tipuga, mida kutsutakse selle serva **otstippudeks**. Kahte tippu nimetatakse **naabertippudeks**, kui nad on servaga ühendatud. Kahte serva nimetatakse **naaberservadeks**,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

¹Leonhard Euler (1707–1783) — šveitsi matemaatik

²tipp = *vertex*

³serv = *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

$$V = \{u, v, w, x, y, z\}$$

$$E = \{uv, uy, vw, vz, wy, xy, yz\}.$$

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.

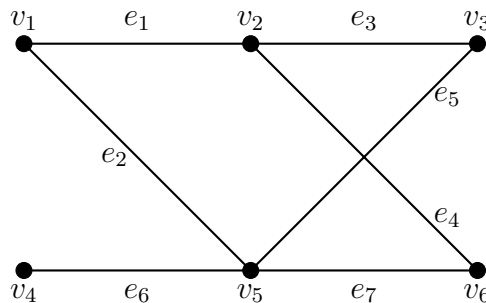
Definitsioon 2.4 Olgu $G = (V, E)$ graaf tippude hulgaga $V = \{v_1, \dots, v_n\}$. Graafi G **naabrusmaatriksiks** nimetatakse $n \times n$ -maatriksit $A = (a_{ij})$, kus

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

Definitsioon 2.5 Olgu $G = (V, E)$ graaf tippude hulgaga $V = \{v_1, \dots, v_n\}$ ja servade hulgaga $E = \{e_1, \dots, e_m\}$. 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:



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:



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 (see hulk võib olla ka tühi) seniste tippude vahele.

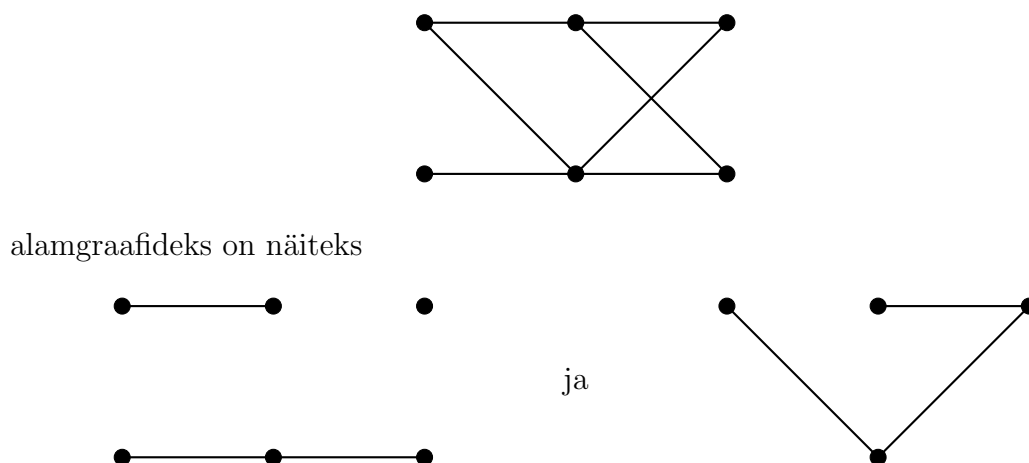
Definitsioon 2.15 Graafi $G' = (V', E')$ nimetatakse graafi $G = (V, E)$ **alamgraafiks**, kui $V' \subseteq V$ ja $E' \subseteq E$.

Teiste sõnadega: alamgraaf saadakse esialgsest graafist teatud hulga tippude ja servade kustutamisel.

Näide 2.16 1. Iga graaf on iseenda alamgraaf.

2. Nullgraaf O_n on iga n -tipulise graafi alamgraaf.

3. Graafi



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 $d(v) \in \{0, 1, \dots, n-1\}$.

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

$$d(u) = d(w) = d(z) = 2, \quad d(v) = 3, \quad d(x) = 1, \quad d(y) = 4.$$

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. $\square$

Järeldus 2.21 Igas graafis on paaritu astmega tippe paarisarv.

TÕESTUS. Kui paaritu astmega tippe oleks paaritu arv, siis summa

$$\sum_{v \in V} d(v)$$

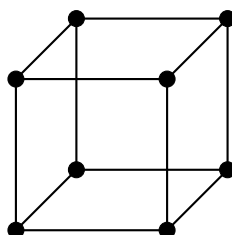
oleks paaritu arv, mis on vastuolus teoreemiga 2.20. Järelikult peab paaritu astmega tippe olema paarisarv. $\square$

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

$$|E| = \left(\sum_{v \in V} d(v) \right) / 2 = \frac{nk}{2}.$$

□

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 $v_0, v_1, \dots, v_k$, kus iga kaks järjestikust tippu on ühendatud servaga. Tippe v_0 ja v_k nimetatakse ahela **otstippudeks**, ülejäänud tipud on ahela **sisetipud**. Ahela $v_0, v_1, \dots, v_k$ **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 $v_0, v_1, \dots, v_k$ asemel lihtsalt $v_0v_1 \dots v_k$.

Kui meil on ahel $v_0, v_1, \dots, v_k$, siis öeldakse, et see ahel **läbib** tippe $v_0, v_1, \dots, v_k$ ja servi $v_0v_1, v_1v_2, \dots, v_{k-1}v_k$.

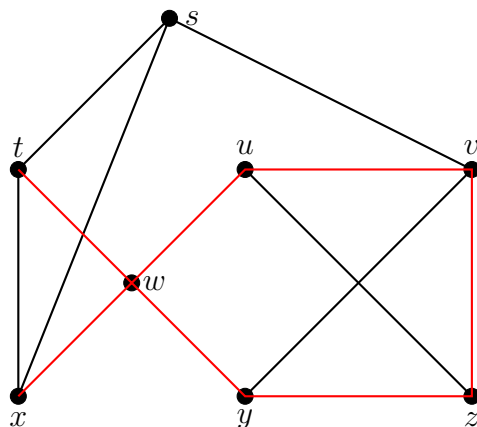
Ahelas võib mõni tipp või isegi mõni serv esineda mitu korda.

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].

Näide 2.29 Graafis



on ahel t, w, y, z, v, u, w, x (märgitud punasega) pikkusega 7 tippude t ja x vahel. See ahel ei ole lihtahel.

Teoreem 2.30 Kui graafis G leidub tippude u ja v vahel ahel, siis leidub nende vahel ka lihtahel.

⁴ahel = walk

⁵lihtahel = path

TÕESTUS. Eeldame, et tippude u ja v vahel leidub ahel

$$u = v_0, v_1, v_2, \dots, v_{k-1}, v_k = v.$$

Oletame, et selles ahelas esineb mingi tipp w vähemalt kaks korda. Otsime üles selle tipu esimese ja viimase esinemise ahelas:

$$v_0, v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_{j-1}, w, v_{j+1}, \dots, v_k.$$

Siis

$$v_0, v_1, \dots, v_{i-1}, w, v_{j+1}, \dots, v_k. \quad (2.1)$$

on ahel, milles tipp w esineb ainult ühe korra. Kui ahelas (2.1) esineb mõni tipp vähemalt kaks korda, siis toimime selle tipuga samamoodi nagu enne tegime tipuga w . Pärast lõplikku arvu selliseid samme saame tulemuseks ahela, kus ükski tipp ei esine mitu korda, s.t. tippe u ja v ühendava lihtahela. $\square$

Näide 2.31 Näites 2.29 vaadeldud graafis leidub tippude t ja x vahel lihtahel t, w, x . Aga leidub ka ühest servast koosnev lihtahel t, x .

Nagu nägime, graafis võib kahe tipu vahel leiduda mitmeid ja erineva pikkusega lihtahelaid.

Definitsioon 2.32 Graafi tippude u ja v , kus $u \neq v$, vaheliseks **kauguseks**⁶ 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.

Definitsioon 2.33 Kinnine ahel⁷ on ahel, mille esimene ja viimane tipp langevad kokku. **Kinnise ahela pikkus** on tema servade arv.

Definitsioon 2.34 Kinnist ahelat, milles on vähemalt kolm serva ja mis ei läbi ühtegi tippu kaks korda, kutsutakse **tsükliks**⁸.

Niisiis, tsükkel on ahel $v_0, v_1, \dots, v_{k-1}, v_0$, kus $k \geq 3$ ja tipud $v_0, v_1, \dots, v_{k-1}$ on paarikaupa erinevad. Tipu v_0 teistkordset esinemist järjendis $v_0, v_1, \dots, v_{k-1}, v_0$ ei loeta selle tipu teistkordseks läbimiseks.

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 tsükli.

Näide 2.35 Näites 2.3 vaadeldud graafis on 6 tippu ja 7 serva. Selles leidub näiteks tsükkel $uvzyu$ pikkusega 4. Lisaks sellele on selles graafis $uvwyzvu$ kinnine ahel, mis ei ole lihtahel ega tsükkel, ning $uvwyz$ on lihtahel, mis ei ole kinnine.

⁶kaugus = *distance*

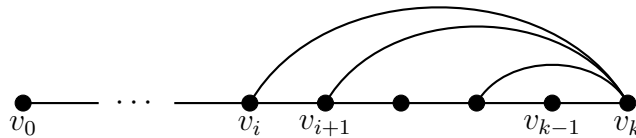
⁷kinnine ahel = *closed walk*

⁸tsükkel = *cycle*

Teoreem 2.36 Kui $l \geq 2$ on naturaalarv ja graafi iga tipu aste on vähemalt l , siis selles graafis leidub

1. lihtahel, mille pikkus on vähemalt l ,
2. tsükel, mille pikkus on vähemalt $l + 1$.

TÕESTUS. 1. Eeldame, et graafi G iga tipu aste on vähemalt l , kus $l \geq 2$. Olgu $v_0, v_1, \dots, v_k$ 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 $k \geq l$, s.t. vaadeldava lihtahela pikkus on vähemalt l .



2. Olgu v_i selline tipu v_k naaber, mis on tipule v_0 kõige lähemal (s.t. mille korral i on võimalikult väike). Siis $v_i, v_{i+1}, \dots, v_k, v_i$ on tsükel, kusjuures tema pikkus on vähemalt $l + 1$, sest ta sisaldab tippu v_k ja kõiki v_k naabertippe. $\square$

Järeldus 2.37 Kui graafis on servi vähemalt sama palju kui tippe, siis selles graafis leidub tsükel.

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 $|E| \geq |V|$. Kustutame ühekaupa graafist isoleeritud ja rippuvaid tippe, niikaua kuni neid leidub (ka neid, mis selle protsessi käigus juurde tekivad). Selle protsessi käigus on kustutamise järel saadaval graafil alati servi vähemalt sama palju kui tippe. Lõpuks jääb järele graafi G alamgraaf $G' = (V', E')$, kus $|E'| \geq |V'|$. Lisaks sellele $|V'| \geq 3$ ja G' iga tipu aste on vähemalt 2. Teoreemi 2.36 põhjal leidub graafis G' tsükel, mille pikkus on vähemalt 3. Sama tsükel esineb ka graafis G . $\square$

2.3 Graafi sidusus

Definitsioon 2.38 Graafi nimetatakse **sidusaks**, kui selle iga kahe tipu vahel leidub ahel.

Märkus 2.39 1. Muuhulgas loetakse ka ühetipuline graaf sidusaks.

2. Sidusas graafis saab mistahes tipust liikuda servipidi mistahes teise tippu.

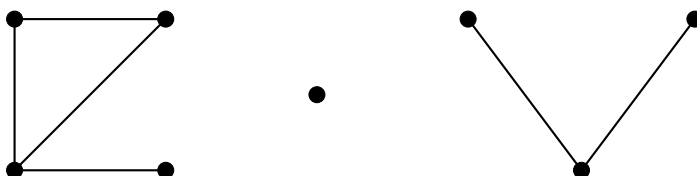
3. Kui u ja v on sidusa graafi kaks erinevat tippu, siis tänu teoreemile 2.30 leidub u ja v vahel lihtahel.

Kui graaf ei ole sidus, siis ta jaguneb sidusate alamgraafide lõikumatuks ühendiks.

Definitsioon. Graafi **sidususkomponentideks** ehk **sidusateks komponentideks** nimetatakse selle graafi maksimaalseid sidusaid alamgraafe.

Maksimaalsus selles definitsioonis tähendab seda, et antud sidus alamgraaf ei sisaldu üheski suurema tippude või servade arvuga sidusas alamgraafis. Graaf on sidus parajasti siis, kui tal on üks sidususkomponent.

Näide 2.40 Järgmisel graafil on kolm sidususkomponenti:

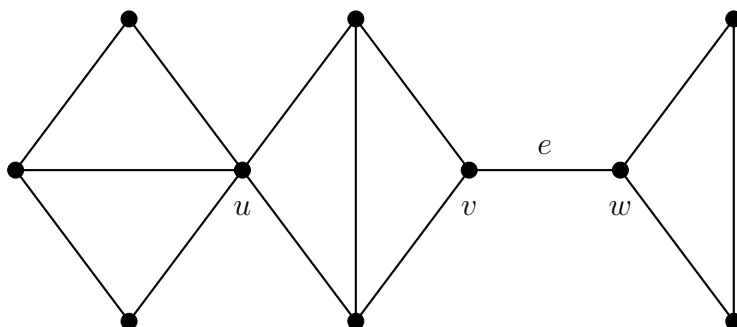


Definitsioon 2.41 Graafi serva nimetatakse **sillaks**, kui tema eemaldamisel graafist sidususkomponentide arv suureneb.

On selge, et serv uv on sild parajasti siis, kui pärast tema eemaldamist on otstipud u ja v erinevates sidususkomponentides.

Definitsioon 2.42 Kui tipu u ja temaga intsidentsete servade eemaldamisel graafi sidususkomponentide arv suureneb, siis öeldakse, et u on **eraldav tipp**.

Näide 2.43 1. Graafis



on üks sild e ja kolm eraldavat tippu u , v ja w .

2. Eesti maantee graafis on Muhu saart Saaremaaga ühendav maanteelõik sillaks. Selles graafis moodustavad Hiiumaa, Vormsi ja teised saared omaette sidususkomponendid.

Anneme nüüd tarviliku ja piisava tingimuse selleks, et graafi serv oleks sild.

Teoreem 2.44 *Graafi serv on sild parajasti siis, kui ta ei kuulu ühessegi tsüklisse.*

TÕESTUS. TARVILIKKUS. Olgu serv uv sild. Oletame vastuväiteliselt, et leidub tsükel 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 sidususkomponentis, 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 2.30 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. $\square$

Järgmine teoreem annab seosed graafi tippude, servade ja sidususkomponentide arvude vahel.

Teoreem 2.45 *Kui n -tipulisel graafil on m serva ja k sidususkomponenti, siis kehtivad võrratused*

$$n - k \leq m \leq \frac{(n - k)(n - k + 1)}{2}.$$

TÕESTUS. 1. Tõestame võrratuse $n - k \leq m$. Teeme seda matemaatilise induktsiooniga graafi servade arvu järgi. Täpsemalt öeldes tõestame, et iga naturaalarvu m ja iga m -servalise graafi G korral ei ületa tippude arvu ja sidususkomponentide arvu vahe servade arvu m .

Alus. Olgu $m = 0$. Siis on tegemist nullgraafiga O_n , milles sidususkomponente on n tükki. Võrratus on kujul $n - n \leq 0$ 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 n tippu, $m - 1$ serva ja $k + 1$ sidususkomponenti. Kasutades induktsiooni eeldust G' jaoks saame võrratuse $n - (k + 1) \leq m - 1$, kust $n - k \leq m$.

b) e ei ole sild. Siis graafis G' on n tippu, $m - 1$ serva ja k sidususkomponenti ning induktsiooni eelduse põhjal $n - k \leq m - 1$. Siis aga ka $n - k \leq m$.

2. Tõestame võrratuse

$$m \leq \frac{(n-k)(n-k+1)}{2}. \quad (2.2)$$

Selleks uurime, mitu serva saab maksimaalselt olla n -tipulisel graafil k sidususkomponendiga. Ilmselt peavad sellisel juhul kõik sidususkomponendid olema täisgraafid. Oletame, et meie m -servalisel graafil G on mitu sidususkomponenti, milles on rohkem kui 1 tipp. Teeme selle graafiga läbi järgmise konstruktsiooni.

- Jättes välja ühetipulised komponendid valime välja ühe minimaalse tippude arvuga komponendi,
- valime sellest komponendist välja ühe tipu v ,
- kustutame ära kõik servad tipust v tema komponendi teistesse tippudesse,
- lisame tipust v servad mingi maksimaalse tippude arvuga sidususkomponendi kõigisse tippudesse.

Selle konstruktsiooni tulemusena saame uue graafi G_1 , millel on graafiga G sama palju tippe ja sidususkomponente, kuid servade arv m_1 on suurem: $m < m_1$. Kordame graafiga G_1 sama mõttekäiku ja teeme seda seni kuni jõuame pärast lõplikku arvu samme graafini G^* , milles on

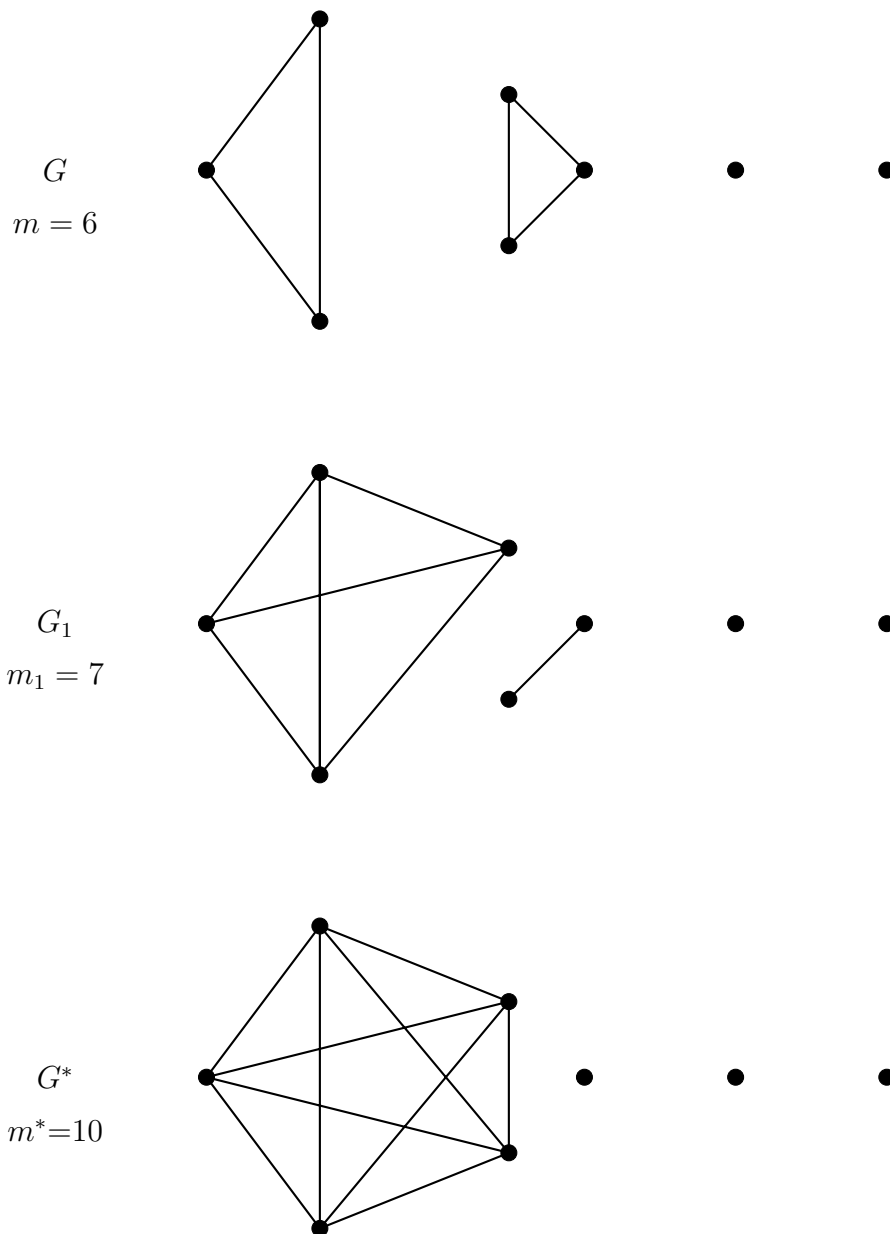
1. $k - 1$ ühetipulist sidususkomponenti,
2. üks $(n - k + 1)$ -tipuline täisgraafist sidususkomponent.

Märkuse 2.10 põhjal on sellise graafi servade arv

$$m^* = \frac{(n-k+1)(n-k+1-1)}{2} = \frac{(n-k)(n-k+1)}{2}.$$

Vastavalt meie arutluskäigule, kui meil on suvaline n -tipuline graaf m serva ja k sidususkomponendiga, siis $m \leq m^*$, mida oligi tarvis tõestada. $\square$

Näide 2.46 Võrratuse (2.2) tõestamisel kasutatud konstruktsiooni illustreerib järgmine näide.



Teeme mõned järeldused teoreemist 2.45.

Järeldus 2.47 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 2.45 põhjal $n - k \leq m < n - 1$, kust $n - k < n - 1$ ja seega $1 < k$. Kuna sidususkomponente on rohkem kui 1, siis on graaf mittesidus. $\square$

Järeldus 2.48 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 $n \geq 3$. Kui servade arv on m ja

$$m > \frac{(n-1)(n-2)}{2},$$

siis teoreemi 2.45 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

$$(k-2)(k-2n+1) > 0.$$

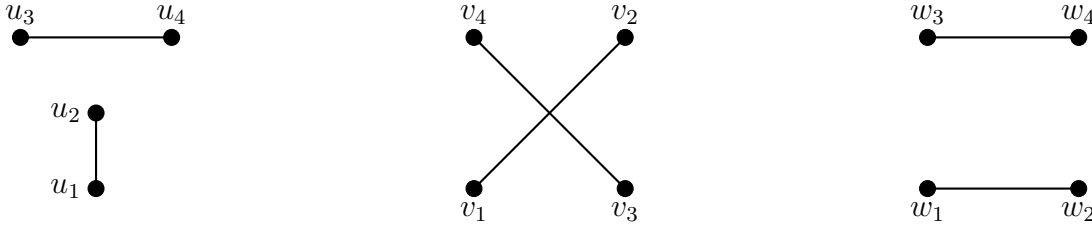
Arvestades võrratust $2 < 2n-1$ (sest $n \geq 3$) ja ruutparabooli omadusi peab $k < 2$ või $k > 2n-1$. Kui $k > 2n-1$, siis $k > n+n-1 > n$, mis ei ole võimalik (sidususkomponente ei saa olla rohkem kui tippe). Seega $k < 2$ ehk $k = 1$. Seda oligi tarvis tõestada. $\square$

2.4 Graafide isomorfism

Definitsioon 2.49 Graafe $G = (V, E)$ ja $G' = (V', E')$ nimetatakse **isomorfseteks**, kui leidub selline bijektiivne kujutus $\varphi : V \rightarrow V'$, et

$$uv \in E \text{ parajasti siis, kui } \varphi(u)\varphi(v) \in E'.$$

Näide 2.50 Graafid



on omavahel isomorfsed. Ükski neist graafidest ei ole isomorfne graafiga O_4 ega K_4 .

Graafide isomorfismi tõestamiseks 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 2.51 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 $\psi : E \rightarrow E'$, 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 $uv = v'u' = u'v'$.

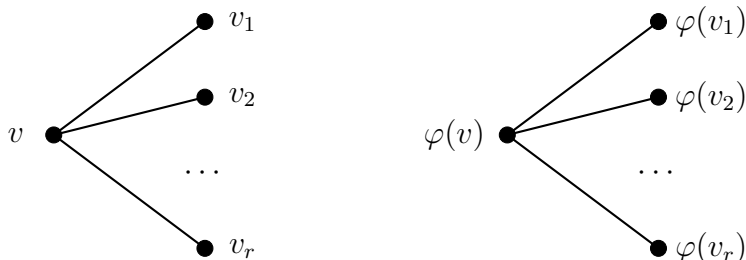
Sellega on näidatud, et ψ on injektiivne.

Veendume, et ψ on surjektiivne. Olgu $xy \in E'$. Tänu φ surjektiivsusele 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 surjektiivne.

Kuna kujutus ψ on bijektiivne, siis on graafides G ja G' sama palju servi. $\square$

Lause 2.52 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 $v_1, \dots, v_r$, siis $\varphi(v)\varphi(v_1), \dots, \varphi(v)\varphi(v_r) \in E'$. Tänu φ injektiivsusele on tipud $\varphi(v_1), \dots, \varphi(v_r) \in V'$ paarikaupa erinevad. Seega $d(\varphi(v)) \geq r$.



Kui oletada, et veel ka $\varphi(v)x \in E'$, kus $x \in V'$ ja $x \notin \{\varphi(v_1), \dots, \varphi(v_r)\}$, 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 $i \in \{1, \dots, r\}$, et $v_0 = v_i$. Siis aga $x = \varphi(v_0) = \varphi(v_i) \in \{\varphi(v_1), \dots, \varphi(v_r)\}$, vastuolu. Sellega oleme näidanud, et $\varphi(v)$ ainsad naabertipud graafis G' on $\varphi(v_1), \dots, \varphi(v_r)$. Järelikult $d(\varphi(v)) = r$. $\square$

Näide 2.53 Graafid



ei ole isomorfised, 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.

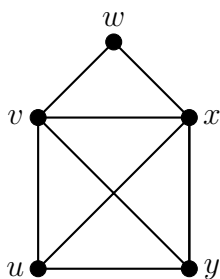
2.5 Euleri ja Hamiltoni graafid

Definitsioon 2.54 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 2.55 Euleri graaf on sidus graaf, milles leidub kinnine Euleri ahel.

Märkus 2.56 “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 2.57 Graafis



leidub Euleri ahel $uvyuxvwxxy$.

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, mille tõestas Leonhard Euler 1736. aastal.

Teoreem 2.58 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 induksiooniga 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 2.36 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 tsükklisse C kuuluvate servade kustutamisel. Graafis G' on vähem servi kui graafis G . Samuti on G' kõigi tippude astmed paarisarvud, sest kustutades tsükklisse 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 kinnise Euleri ahela ja jõuame tagasi tippu v_2 . Protseduuri korrates läbime niimoodi tsükli C . Tulemuseks on kinnine Euleri ahel G jaoks. $\square$

Järeldus. Täisgraaf K_n on Euleri graaf parajasti siis, kui n on paaritu arv.

TÕESTUS. Täisgraafis K_n on iga tipu aste $n - 1$, mis on paarisarv parajasti siis, kui n on paaritu. $\square$

Märkus. Eelmise teoreemi tõestus läheb läbi ka siis, kui graafis võib kahe tipu vahel olla mitu serva (selliseid graafe kutsutakse mõnikord **multigraafideks**). Paneme tähele, et selles tõestuses me kasutame teoreemi 2.36, mille tõestus läheb samuti multigraafide korral läbi, kui selle sõnastuses asendada fraas “iga tipu aste on vähemalt l ” fraasiga “igal tipul on vähemalt l naabertippu”. Multigraafis võib tipu aste (s.t. intsidentsete servade arv) olla suurem kui naabertippude arv.

Järeldus. Sidusas graafis leidub Euleri ahel tipust u tippu v parajasti siis, kui u ja v on selle graafi ainsad paaritu astmega tipud.

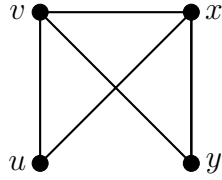
TÕESTUS. TARVILIKKUS. See on sarnane teoreemi 2.58 tarvilikkuse tõestusega.

PIISAVUS. Eeldame, et u ja v on ainsad paaritu astmega tipud. Lisame nende vahele serva (tulemusena võib tekkida multigraaf). Saadud graafis on kõigi tippude astmed paarisarvud. Seega teoreemi 2.58 tõttu leidub selles graafis kinnine Euleri ahel. Jättes sellest ahelast välja u ja v vahele lisatud serva saame Euleri ahela esialgses graafis. $\square$

Definitsioon 2.59 Tsükli, mis läbib graafi kõiki tippe täpselt ühe korra, nimetatakse **Hamiltoni**⁹ tsükliks. **Hamiltoni graaf** on graaf, milles leidub Hamiltoni tsükkel.

⁹William Rowan Hamilton (1805–1865) — iiri matemaatik, astronoom ja füüsik

Näide 2.60 Graafis



leidub Hamiltoni tsükkel $vuxyv$. Seega on tegemist Hamiltoni graafiga.

Järgmine, Diraci¹⁰ poolt tõestatud teoreem annab piisava tingimuse Hamiltoni tsükli leidumiseks graafis.

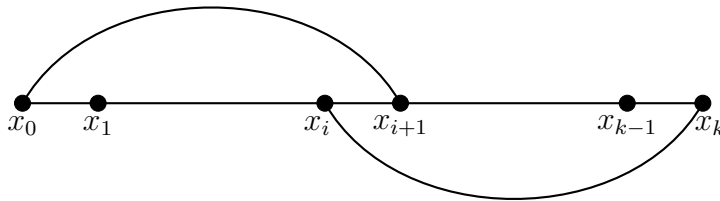
Teoreem 2.61 (Diraci teoreem) Olgu G n -tipuline graaf, kus $n \geq 3$ ja iga tipu aste on vähemalt $\frac{n}{2}$. Siis G on Hamiltoni graaf.

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 $\leq \frac{n}{2}$, 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). Kui oletaksime, et $k = 0$, siis graafis G pole servi ja seega sidususe tõttu $n = 1$, vastuolu. Kui $k = 1$, siis G ühegi tipu aste ei saa olla 2. Sidususe tõttu $G = K_2$ ja $n = 2$, vastuolu. Seega peab kehtima võrratus $k \geq 2$.

Paneme tähele, et 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

$$(\exists i \in \{0, 1, \dots, k-1\})(x_i x_k \in E \text{ ja } x_0 x_{i+1} \in E).$$



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

$$d(x_0) + d(x_k) + 1 \geq \frac{n}{2} + \frac{n}{2} + 1 = n + 1,$$

mis ei ole võimalik, sest graafil on n tippu ja ahela P tipud on kõik erinevad.

¹⁰ Gabriel Andrew Dirac (1925–1984) — ungari-briti matemaatik

Vaatleme nüüd kinnist ahelat

$$C = x_0 x_{i+1} x_{i+2} \dots x_{k-1} x_k x_i x_{i-1} \dots x_1 x_0.$$

Paneme tähele, et selles kinnises ahelas on $k+1$ tippu $(x_0, x_1, \dots, x_k)$, kusjuures iga tippu läbitakse üks kord. Järelikult on ahelas C ka $k+1 \geq 3$ (sest $k \geq 2$) serva ning tegemist on tsükliga. Oletame vastuväiteliselt, et C ei ole Hamiltoni tsükkel. Siis hulk $V \setminus \{x_0, \dots, x_k\}$ on mittetühi. Kuna G on sidus, siis hulgas $V \setminus \{x_0, \dots, x_k\}$ peab leiduma mingi tipp v , mis on serva abil ühendatud mingi tipuga x_j , kus $j \in \{0, 1, \dots, k\}$. 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. $\square$

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

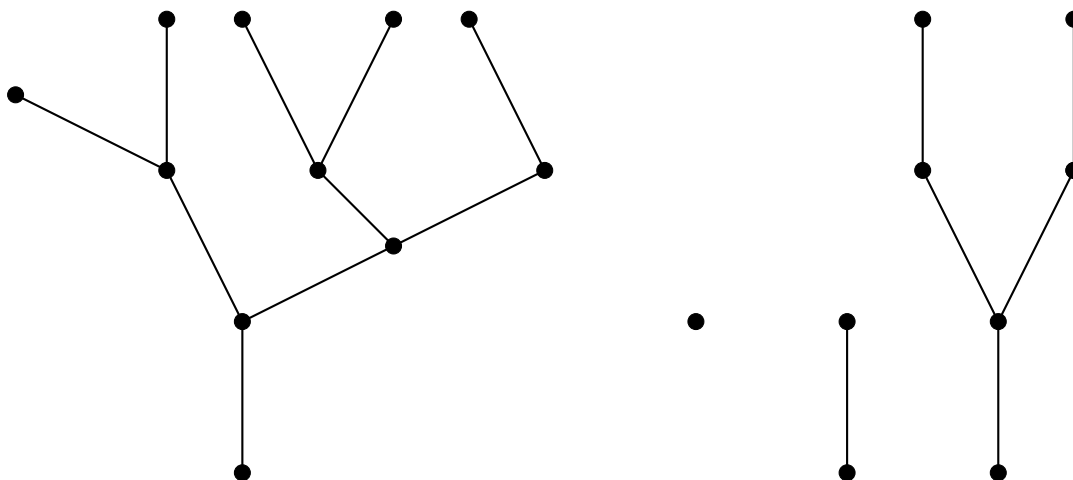
2.6.1 Puude põhiomadused

Puud moodustavad ühe olulise graafide klassi, millel on iseäranis palju rakendusi arvutiteaduses (näiteks andmestruktuuridena).

Definitsioon 2.62 Graafi nimetatakse **puuks**, kui ta on sidus ja ei sisalda tsükleid.

Definitsioon 2.63 Mets on graaf, mille kõik sidususkomponendid on puud.

Näide 2.64 Järgneval joonisel on mets, mis koosneb neljast puust:



Meenutame, et rippuvad tipud on need, mille aste on 1.

Definitsioon 2.65 Puu rippuvaid tippe nimetatakse **lehtedeks** ja mitterippuvaid tippe nimetatakse **sisetippudeks**.

Teoreem 2.66 *Vähemalt kahetipulisel puul on vähemalt kaks lehte.*

TÕESTUS. Olgu meil antud n -tipuline puu, kus $n \geq 2$. 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 vaadeldavas puus vähemalt kaks lehte. $\square$

Leidub kuitahes suure tippude arvuga puid, millel ongi ainult kaks lehte, nendeks on n -tipulised ahelad.

Teoreem 2.67 *Igal n -tipulisel puul on $n - 1$ serva.*

Seda teoreemi on võimalik tõestada vähemalt kahel viisil. Annamegi siin kaks erinevat tõestust.

TÕESTUS. Järelduse 2.47 põhjal ei saa puul olla vähem kui $n - 1$ serva. Järelduse 2.37 tõttu ei saa puul olla rohkem kui $n - 1$ serva. Seega peab puul olema $n - 1$ serva. $\square$

TÕESTUS. Tõestame väite induktsiooniga puu tippude arvu järgi.

Alus. Kui $n = 1$, siis on tegemist puuga, mille servade arv on 0.

Samm. Olgu $n \geq 1$ naturaalarv ja eeldame, et väide kehtib kõigi puude korral, millel on n tippu. Olgu G puu, millel on $n + 1$ tippu. Kuna graafil G on vähemalt kaks tippu, siis teoreemi 2.66 põhjal leidub tal leht. Kustutame selle ära koos intsidentse servaga. Järele jäävale n -tipulisele graafile saame rakendada induktsiooni eeldust, seega on temas $n - 1$ serva. Järelikult graafis G on n serva. $\square$

Teoreem 2.68 *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 2.44 põhjal kuulub e mingisse tsükklisse. 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. Selle lihtahela pikkus on vähemalt 2. Nüüd 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. $\square$

Järeldus 2.69 *Graafi G puhul, millel on n tippu ja m serva, on järgmised väited samaväärsed:*

1. G on puu;
2. G on sidus ja $m \leq n - 1$;
3. G ei sisalda tsükleid ja $m \geq n - 1$.

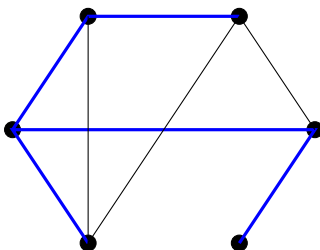
- a) meie kinnine ahel sisaldab vähemalt kolme erinevat tippu (x_r , x_{r+1} ja y_{r+1}) ning seega ka vähemalt kolme serva,
- b) vastavalt konstruktsioonile me ei läbi ühtegi tippu kaks korda.

PIISAVUS. Eeldame, et graafi G iga kahte erinevat tippu ühendab täpselt üks lihtahel. Siis G on sidus. Oletame vastuväiteliselt, et graafis G leidub tsükel ja valime selles tsükli 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. $\square$

2.6.2 Toespuid

Definitsioon 2.71 Sidusa graafi **toespooks**¹¹ ehk **aluspuuks** nimetatakse sellist alamgraafi, mis sisaldab kõiki tippe ja on puu.

Näide 2.72 Järgneval joonisel on üks graaf ja selle toespuu (toespuu servad on joonistatud paksema sinise joonega):



Lause 2.73 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 2.68 on T puu ja vastavalt definitsioonile 2.71 on ta graafi G toespuu. $\square$

Igal puul on ainult üks toespuu — see on ta ise. Kui sidus graaf ei ole puu, siis on tal mitu toespuid.

Toespude 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.

¹¹toespuu = *spanning tree*

Definitsioon 2.74 Kaalutud graafiks nimetatakse kolmikut (V, E, ω) , kus (V, E) on graaf ja $\omega : E \rightarrow \mathbb{R}^+$ on kujutus. Positiivset reaalarvu $\omega(e)$ nimetatakse serva e **kaaluks**.

Tüüpiline näide kaalutud graafist on maantee kaart, kus tippudeks on linnad, servadeks linnade vahelised maanteed ja servade kaaludeks teede pikkused.

Kaalutud graafi esitamisel joonise abil märgitakse servade kaalud harilikult joonisele servade juurde.

Definitsioon 2.75 Kaalutud graafi G toespuid T **kaaluks** $\omega(T)$ loetakse tema servade kaalude summat. Öeldakse, et graafi G toespuid T on **minimaalse kaaluga**, kui G iga toespuid T' korral $\omega(T) \leq \omega(T')$.

Näide 2.76 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 toespuid annab kõige odavam ehituskuluga võrgu.

Analoogiline ülesande püstitus tekib siis, kui on vaja välja ehitada elektri kõrgepingeliinid, veevõrgud või kanalisatsioonitrassid.

Hulgaliselt näiteid toespuid rakenduste kohta võib leida ingliskeelse Vikipeedia artiklist *Minimum spanning tree*.

Igal sidusal kaalutud graafil leidub minimaalse kaaluga toespuid. Kuna vaadeldavad graafid on lõplikud, siis võime antud graafi puhul leida kõik tema toespuid, arvutada välja kõigi toespuid kaalud ja leida kaalude hulgast minimaalse. Selliseid minimaalse kaaluga toespuid võib graafil olla mitu.

Graafi kõigi toespuid 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 toespuid leidmiseks. Esimese neist pakkus välja Joseph Kruskal¹² 1956. aastal.

Kruskali algoritm.

Antud: n -tipuline sidus kaalutud graaf $G = (V, E, \omega)$.

Leida: minimaalse kaaluga toespuid.

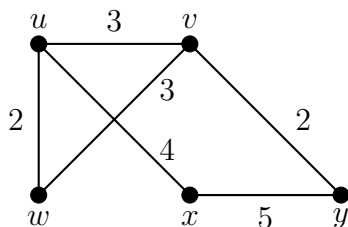
Idee: lisame minimaalse kaaluga servi nii, et ei tekiks tsükleid.

1. Vali servaks e_1 graafi G minimaalse kaaluga serv.
2. Iga $i = 2, 3, \dots, n - 1$ korral vali servaks e_i graafi G minimaalse kaaluga serv, mis erineb servadest $e_1, \dots, e_{i-1}$ ja ei moodusta koos servadega $e_1, \dots, e_{i-1}$ tsükli.
3. Tagasta graaf $T = (V, \{e_1, e_2, \dots, e_{n-1}\})$.

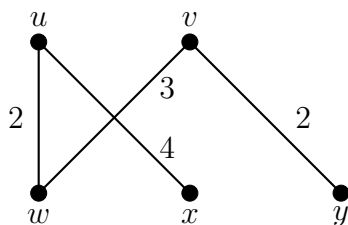
Märkus 2.77 Lause “Serv e_i koos servadega $e_1, \dots, e_{i-1}$ ei moodusta tsükli” all mõistame seda, et G alamgraaf, mis koosneb servadest $e_1, \dots, e_{i-1}, e_i$ ja nende otstippudest, ei sisalda ühtegi tsükli.

¹²Joseph Kruskal (1928–2010) — ameerika matemaatik

Näide 2.78 Leiame kaalutud graafi



minimaalse kaaluga toespuid Kruskali algoritmi abil. Selles graafis on kaks minimaalse kaaluga serva: uw ja vy . Esimesel sammul valime minimaalse kaaluga serva uw . Järgnevatel sammudel valime servad vy, vw, ux . Tulemuseks on toespuid



kaaluga $2 + 2 + 3 + 4 = 11$.

Tõestame, et Kruskali algoritm töötab korrektselt.

Teoreem 2.79 Kui G on sidus kaalutud graaf, siis Kruskali algoritm leiab graafi G minimaalse kaaluga toespuid.

TÕESTUS. Kõigepealt veendume, et sammul 2 on tõesti alati võimalik valida serv e_i , mis erineb varem valitud servadest $e_1, \dots, e_{i-1}$ ja ei moodusta koos nendega tsüklit. Selleks vaatleme graafi G alamgraafi $G' = (V, \{e_1, \dots, e_{i-1}\})$. Graafis G' on n tippu ja vähem kui $n - 1$ serva ($i - 1 < n - 1$). Vastavalt järeldusele 2.47 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 ühegi servadest $e_1, \dots, e_{i-1}$ ja samuti ei saa ta koos servadega $e_1, \dots, e_{i-1}$ moodustada tsüklit.

Olgu graafi G alamgraaf $T = (V, \{e_1, e_2, \dots, e_{n-1}\})$ leitud Kruskali algoritmi abil. Kuna T ei sisalda tsükleid ja tema servade arv on $n - 1$, siis järelduse 2.69 põhjal on T puu. Et ta sisaldab kõiki G tippe, siis on tegemist G toespuidga. Tuleb veel näidata, et T on minimaalse kaaluga toespuidude hulgas.

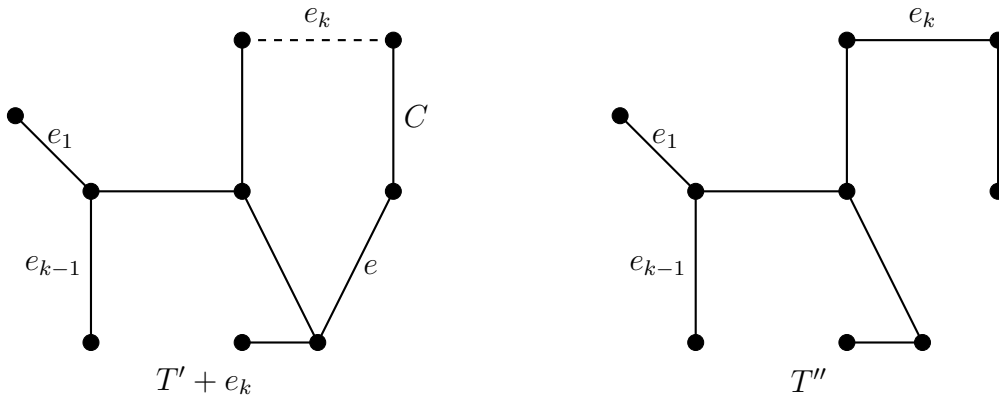
Oletame vastuväiteliselt, et T ei ole minimaalse kaaluga toespuid. Siis leidub toespuid, mille kaal on väiksem kui puul T . Olgu T' graafi G toespuid, mis

- on minimaalse kaaluga ja
- omab minimaalse kaaluga toespuidude 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 2.68 peab S sisaldama mingit tsüklit C . See tsükel 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 tsükli C). Kustutame graafist S serva e ja tähistame saadud graafi T'' . Tinglikult võiks kirjutada

$$S = T' + e_k \quad \text{ja} \quad T'' = S - e = T' + e_k - e.$$

Konstruksiooni illustreerib järgmine joonis.



Graaf T'' on ka G toespü, sest ta on sidus ja temas on $n-1$ serva (vt. järeldust 2.69). Vastavalt k valikule kuuluvad servad $e_1, \dots, e_{k-1}$ ka puusse T' . Serv e

- ei ole võrdne ühegi 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 algoritmi sammul 2 peab kehtima võrratus $\omega(e_k) \leq \omega(e)$. Kuna T'' on saadud puust T' serva e_k lisamisel ja serva e kustutamisel, siis $\omega(T'') \leq \omega(T')$. Et T' oli minimaalse kaaluga toespü, siis $\omega(T'') = \omega(T')$, mis tähendab, et ka T'' on minimaalse kaaluga toespü. Samas puul T'' on puuga T rohkem ühiseid servi kui puul T' (lisaks ülejäänutele ka serv e_k), mis on vastuolus T' valikuga. Saadud vastuolu näitab, et T peab olema minimaalse kaaluga toespü. $\square$

Tutvustame ka teist minimaalse toespü 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.

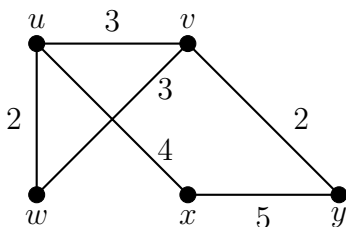
Antud: n -tipuline sidus kaalutud graaf $G = (V, E, \omega)$.

Leida: minimaalse kaaluga toespü.

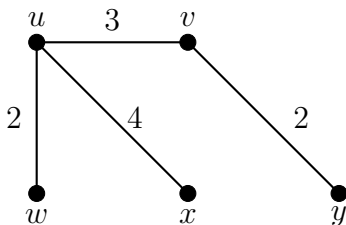
Idee: Konstrueerime alamgraafi T . Alustame suvalisest tipust ja ühendame puule järjest servi, mis viivad uude tippu (mis veel ei kuulu graafi T), valides igal sammul minimaalse kaaluga serva.

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 2.80 Vaatleme jälle kaalutud graafi



Leiame selle graafi minimaalse kaaluga toespuid Primi algoritmi abil. Esimesel sammul valime tipu v . Järgnevatel sammudel valime tipud y, u, w, x koos servadega vy, vu, uw, ux . Tulemuseks on toespuid



Paneme tähele, et selles näites ja näites 2.78 leitud minimaalse kaaluga toespuid on erinevad. Nende mõlema kaal on $2 + 2 + 3 + 4 = 11$.

Teoreem 2.81 Kui G on sidus kaalutud graaf, siis Primi algoritm leiab graafi G minimaalse kaaluga toespuid.

TÕESTUS. Kuna G on sidus, siis igal sammul leidub serv, mis ühendab alamgraafi T_{i-1} mõne hulka U kuuluva tipuga. Seega valikut sammul 2(a) on võimalik teha.

Olgu Primi algoritmi abil leitud servad $e_1, \dots, e_{n-1}$. Kuna ühelgi sammul ei saa serva e_i ja tipu w_i lisamisel tekkida tsüklid, siis kõik graafid T_i (servadega $e_1, \dots, e_i$), kus $i \in \{1, \dots, n - 1\}$, on tsükliteta. Samas on nad konstruktsiooni tõttu sidusad. Järelikult

T_i on puu iga $i \in \{0, 1, \dots, n-1\}$ korral. Muuhulgas T_{n-1} on puu. Ta sisaldab ka kõiki G tippe ning seega on toespüu. Tõestame, et T_{n-1} on minimaalse kaaluga toespüude hulgas.

Olgu $k \in \{0, 1, \dots, n-1\}$ maksimaalne arv, mille korral puu T_k sisaldub mingis minimaalse kaaluga toespüus. (Paneme tähele, et T_0 kindlasti sisaldub igas minimaalse kaaluga toespüus, seega on võimalik selline k leida.) On kaks võimalust.

a) $k = n-1$. Kuna T_{n-1} sisaldub mingis minimaalse kaaluga toespüus T ja kõigil toespüudel on $n-1$ serva, siis $T_{n-1} = T$, s.t. T_{n-1} on minimaalse kaaluga toespüu. Seda me soovisimegi näidata.

b) $k < n-1$. Näitame, et sel juhul tekib vastuolu. Niisiis T_k sisaldub mingis minimaalse kaaluga toespüus T . Seega T sisaldab servi $e_1, \dots, e_k$, aga mitte serva e_{k+1} (vastavalt k maksimaalsusele). Lisame puule T serva e_{k+1} . Saadud alamgraaf S sisaldab tänu teoreemile 2.68 mingit tsüklit C . See tsükel peab aga sisaldama serva e_{k+1} . Tsükel 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.

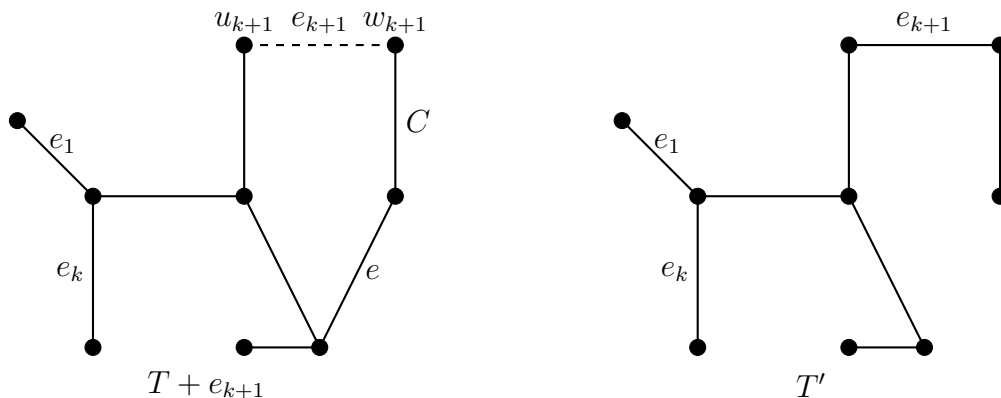
Alustame tipust u_{k+1} liikumist mööda tsüklit C , aga mitte tipu w_{k+1} suunas, vaid vastupidises suunas. Kuna u_{k+1} on alamgraafis T_k aga w_{k+1} ei ole, siis varem või hiljem jõuame mingi servani e , mille üks otstipp on graafis T_k ja teine väljaspool seda. See serv ei saa kuuluda graafi T_{k+1} , sest

- a) $e \notin \{e_1, \dots, e_k\}$ (kuna e ei kuulu graafi T_k),
- b) $e \neq e_{k+1}$ (kuna me liigume tsüklil C serva e_{k+1} vältides).

Moodustame graafi T' kustutades graafist S serva e . Tinglikult võime kirjutada

$$S = T + e_{k+1} \quad \text{ja} \quad T' = S - e = T + e_{k+1} - e.$$

Konstruktsiooni illustreerib järgmine joonis.



Siis $\omega(e_{k+1}) \leq \omega(e)$, sest hetkel kui Primi algoritm valis serva e_{k+1} , oli valitavate servade hulgas ka e . Seega $\omega(T') \leq \omega(T)$. Et T' on sidus graaf $n-1$ servaga, siis järelduse 2.69 tõttu on ta puu. Samuti sisaldab ta kõiki G tippe ja on seega G toespüu. Kuna T oli minimaalse kaaluga toespüu, siis $\omega(T') = \omega(T)$ ja ka T' on minimaalse kaaluga toespüu. 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 alg Tipp ja milline lõpptipp. Vaatleme nüüd graafe, mille servadel on suund.

Definitsioon 2.82 Suunatud graaf¹³ on järjestatud paar $G = (V, E)$, kus V on mit-tetühi 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**¹⁴ 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 2.83 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 2.84 Meenutame, et **binaarseteks seosteks** hulgal V nimetatakse hulga $V \times V$ alamhulki. Seega binaarne seos ja suunatud graaf on sisuliselt sama asi.

Näide 2.85 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.

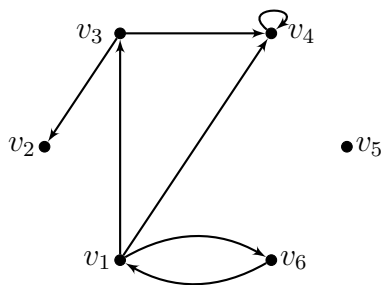
Definitsioon 2.86 Olgu $G = (V, E)$ suunatud graaf tippude hulgaga $V = \{v_1, \dots, v_n\}$. Siis G **naabrusmaatriksiks** nimetatakse $n \times n$ -maatriksit $A = (a_{ij})$, kus

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

Näide 2.87 Suunatud graafi

¹³suunatud graaf = *directed graph*, *digraph*

¹⁴kaar = *arc*



naabrusmaatriks on

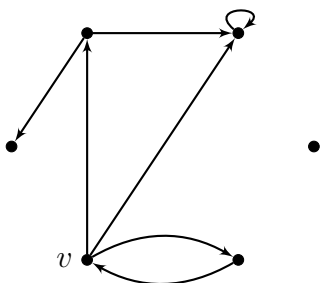
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Nagu näha, suunatud graafi naabrusmaatriks ei pea olema sümmeetriline ning tema peadiagonaalil võib olla ühtesid.

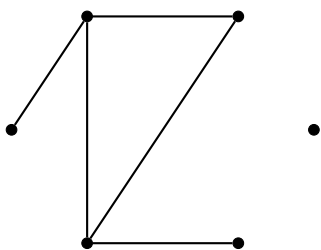
Kui asendame suunatud graafis kõik kaared suunamata servadega (nii-öelda unustame suuna ära), jätame välja kõik silmused ja kordsetest servadest jätame alles ühe, siis saame graafi, mida kutsutakse esialgse suunatud graafi **alusgraafiks**¹⁵.

Definitsioon 2.88 Suunatud graafi tipu v **sisendastmeks**¹⁶ (tähistus $d_-(v)$) nimetatakse sellesse tippu sisenevate kaarte arvu ning **väljundastmeks**¹⁷ (tähistus $d_+(v)$) nimetatakse sellest tipust väljuvate kaarte arvu.

Näide 2.89 Suunatud graafis



on $d_-(v) = 1$ ja $d_+(v) = 3$. Selle graafi alusgraaf on



¹⁵alusgraaf = *underlying graph*

¹⁶sisendaste = *indegree*

¹⁷väljundaste = *outdegree*

Teoreem 2.90 *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. $\square$

Definitsioon 2.91 Suunatud graafi **sisend** on tipp, mis pole ühegi kaare lõpptipp.

Definitsioon 2.92 Suunatud graafi **väljund** on tipp, mis pole ühegi kaare alg Tipp.

Näide 2.93 Näites 2.87 vaadeldud suunatud graafi sisendiks on tipp v_5 ning väljunditeks on tipud v_2 ja v_5 .

Ülesanne 2.94 Kuidas saab naabrusmaatriksi abil kindlaks teha, kas suunatud graafi mingi tipp on sisend või väljund?

Definitsioon 2.95 Suunatud graafi tippude järjendit $v_0, v_1, \dots, v_k$, 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.

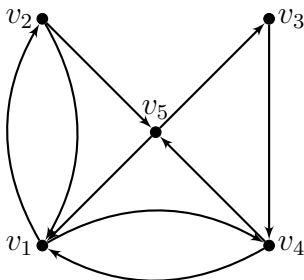
Definitsioon 2.96 **Suunatud tsükkel** on kinnine suunatud ahel, milles on vähemalt kaks kaart ja mis ei läbi ühtegi tippu kaks korda.

Märkus 2.97 Niisiis suunatud tsükkel on suunatud ahel $v_0, v_1, \dots, v_k$, kus $k \geq 2$, $v_0 = v_k$ ja tipud $v_0, v_1, \dots, v_{k-1}$ 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 2.98 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 tsükel.

Teoreem 2.99 *Kui suunatud graafis pole suunatud tsükleid ja silmuseid, siis leidub sellel graafil vähemalt üks sisend ja vähemalt üks väljund.*

TÕESTUS. Vaatleme suunatud graafi $G = (V, E)$, milles pole suunatud tsükleid ega silmuseid 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. Kuna silmuseid ei ole, siis leidub tipp $v_1 \neq v$ nii, et $(v, v_1) \in E$. Kui v_1 on väljund, siis lõpetame. Vastasel korral peab leiduma mingi kaar (v_1, v_2) , kus $v_2 \neq v_1$. Jätkame samamoodi. Paneme tähele, et ükski järgnev tipp v_i ei saa võrdsuda varem valitud tippudega $v, v_1, \dots, v_{i-1}$, sest graaf ei sisalda suunatud tsükleid. Kuna graafis on lõplik arv tippe, siis pärast lõplikku arvu samme peame jõudma mingisse 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 2.100 Suunatud graafi nimetatakse **tugevalt sidusaks**, kui iga kahe tipu u ja v korral leidub suunatud ahel tipust u tippu v .

Ka ühetipuline suunatud graaf loetakse tugevalt sidusaks.

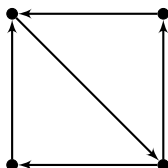
Definitsioon 2.101 Suunatud graafi nimetatakse **nõrgalt sidusaks**, kui tema alusgraaf on sidus.

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 2.102 Suunatud graaf



on nõrgalt sidus, kuid mitte tugevalt sidus. Suunatud graaf



on tugevalt sidus.

Näide 2.103 Vaatleme linnatänavate suunatud graafi näitest 2.85. Liikluse planeerimisel on loomulik nõuda, et see graaf oleks tugevalt sidus, sest liiklejad tahavad, et igalt ristmikult saaks liikluseeskirja rikkumata sõita igale teisele.

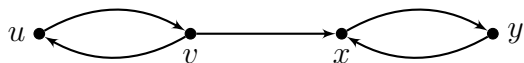
Lause 2.104 *Kui G on vähemalt kahetipuline tugevalt sidus graaf, siis tal ei ole sisendeid ega väljundeid.*

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. $\square$

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 2.105 Suunatud graafis



ei ole sisendeid ega väljundeid. See graaf ei ole tugevalt sidus, sest tipust x ei leidu suunatud ahelat tippu v .

Teoreem 2.106 *Kui sidusas suunamata graafis ei leidu ühtegi silda, siis saab graafi servadele määrata suunad nii, et tekkinud suunatud graaf on tugevalt sidus.*

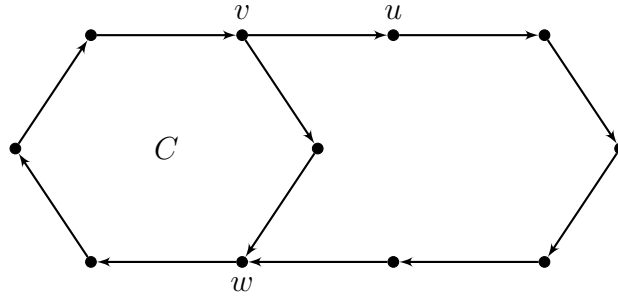
TÕESTUS. Ühetipulise graafi puhul on väide ilmne. Ainuke kahetipuline sidus suunamata graaf (isomorfismi täpsuseni) on



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 2.44 peab iga serv sisalduma mingis tsükli. Valime suvalise serva e (see leidub sidususe tõttu) ja vaatleme tsükli 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 tsükklisse C . Võib juhtuda, et mõni G serv ei kuulu tsükklisse C . Siis võime talle määrata suvalise suuna. Saadud suunatud graaf on tugevalt sidus.

2) Mõni G tipp ei kuulu tsükklisse C . Siis leidub sidususe tõttu G serv, mis ühendab tsükli C mingit tippu v mingi tipuga u väljaspool tsükli. Ka serv vu peab sisalduma mingis tsükli 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 tsükklisse C . Määrame ahela $v, u, \dots, w$ 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 tsükklisse. Kui mõni G serv jääb protsessi käigus kasutamata, siis võime talle anda suvalise suuna, sest see tugevat 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 2.107 Suunatud graafi $G' = (V', E')$ nimetatakse suunatud graafi $G = (V, E)$ **alamgraafiks**, kui $V' \subseteq V$ ja $E' \subseteq E$.

Definitsioon 2.108 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 2.109 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

$$V' \subseteq V'' \text{ \& } E' \subseteq E'' \implies V' = V'' \text{ \& } E' = E''.$$

Muuhulgas alamgraafi $G' = (V', E')$ 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:

$$u \equiv v \iff u \rightsquigarrow v \text{ ja } v \rightsquigarrow u.$$

Lihtne on veenduda, et seos $\equiv$ on ekvivalentsiseos. Ekvivalentsiklassid selle seose järgi on tipuhulga V alamhulgad.

Lause 2.110 *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 kui $v, v' \in K$, siis $u \equiv v$ ja $u \equiv v'$, kust sümmeetria ja transitiivsuse tõttu $v \equiv v'$ ning järelikult tipust v leidub suunatud ahel tippu v' (ja vastupidi).

Näitame, et G_K on maksimaalne tugevalt sidus alamgraaf. Oletame vastuväiteliselt, et G_K ei ole seda. Siis G_K sisaldub mingis tugevalt sidusas alamgraafis $G' = (V', E')$, kusjuures $K \subset V'$ või $E_K \subset E'$. Kuna juhtum $K = V'$ ja $E_K \subset E'$ ei ole võimalik, siis $K \subset V'$ ja leidub tipp $v_0 \in V' \setminus K$. Et alamgraaf G' on tugevalt sidus, siis $u \rightsquigarrow v_0$ ja $v_0 \rightsquigarrow u$. Järelikult $u \equiv v_0$, mis tähendab, et $v_0 \in K$, vastuolu.

Sellega oleme näidanud, et G_K on graafi G tugevalt sidus komponent. $\square$

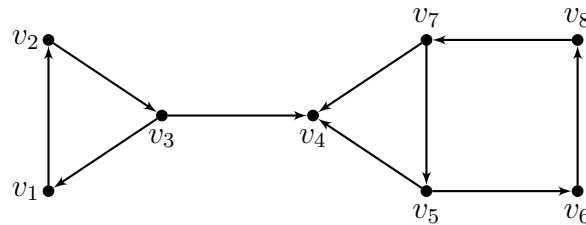
Kuna ekvivalentsiseos $\equiv$ tekitab hulga V tükelduse, siis G tugevalt sidusad komponendid on lõikumatud ja G iga tipp peab kuuluma mingisse tugevalt sidusasse komponenti. Lisaks sellele võime öelda, et tugevalt sidusate komponentide arv on võrdne ekvivalentsiklasside arvuga seose $\equiv$ järgi.

Järeldus 2.111 *Suunatud graaf on tugevalt sidus parajasti siis, kui tal on üks tugevalt sidus komponent.*

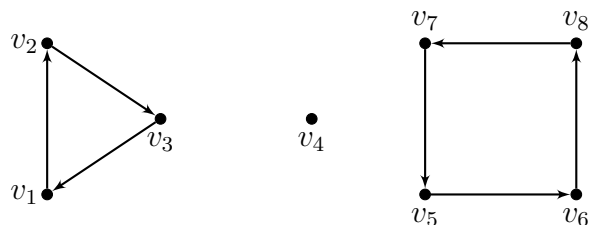
TÕESTUS. Suunatud graaf on tugevalt sidus parajasti siis, kui seose $\equiv$ järgi on ainult üks ekvivalentsiklass, milleks on hulk V . Viimane on samaväärne sellega, et tugevalt sidusaid komponente on üksainus. $\square$

Lause 2.110 tõestuse põhjal saab anda 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 suvalise ja kordame protsessi kuni see on võimalik.

Näide 2.112 Suunatud graafi



tugevalt sidusad komponendid on



Märkus. Suunatud graafi nimetatakse **Euleri graafiks**, kui leidub kinnine suunatud ahel, mis läbib kõiki selle graafi kaari täpselt ühe korra. Saab tõestada järgmise tulemuse:

Suunatud graaf on Euleri graaf parajasti siis, kui ta on tugevalt sidus ja iga tipu korral tema sisendaste võrdub väljundastmega.

2.7.2 Lühima tee leidmise ülesanne

Praktilistest ülesannetest tekkivates suunatud graafides on tihti kaarte omistatud mingid positiivse reaalarvuna väljendatavad kaalud.

Definitsioon 2.113 Kaalutud suunatud graafiks¹⁸ nimetatakse kolmikut (V, E, ω) , kus (V, E) on suunatud graaf ja $\omega : E \rightarrow \mathbb{R}^+$ on kujutus. Positiivset reaalarvu $\omega(e)$ nimetatakse kaare e **kaaluks** ehk **pikkuseks**.

Definitsioon 2.114 Kaalutud suunatud graafi suunatud ahela **kaaluks** ehk **pikkuseks**¹⁹ nimetatakse selle ahela kaarte kaalude summat.

Kui $T = v_0, v_1, \dots, v_k$ on mingi suunatud ahel, siis tema kaalu tähistame $\omega(T)$ või $\omega(v_0, v_1, \dots, v_k)$. Niisiis

$$\omega(T) = \sum_{i=1}^k \omega(v_{i-1}, v_i).$$

Lühima tee leidmise ülesanne²⁰ 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 $\omega(T) \leq \omega(T')$.

Definitsioon 2.115 Kaalutud suunatud graafi tippude u ja v vaheliseks **kauguseks**²¹ (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 2.116 1. Vaatleme jälle linnatänavate suunatud graafi näitest 2.85. Omistame selle graafi kaarte 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 maanteed 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 pileti hinnad, siis lühima tee leidmine tähendab võimalikult odava marsruudi leidmist.

¹⁸kaalutud suunatud graaf = *weighted directed graph*

¹⁹Erinevalt suunamata graafide juhust ei tähenda suunatud ahela pikkus selle kaarte arvu. Loodetavasti siin segadust ei teki.

²⁰lühima tee leidmise ülesanne = *shortest path problem*

²¹kaugus = *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 2.117 *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 . $\square$

Järgnevalt vaatleme kahte lühima tee leidmise algoritmi. Nendes algoritmides kasutame järgmisi kokkuleppeid.

- Eeldame, et kaalutud suunatud graafi G tippude hulgaks on

$$V = \{1, 2, \dots, n\}.$$

- Meil on olemas kujutus $\omega : E \rightarrow \mathbb{R}^+$ 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 algoritmide 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).

Esimese algoritmi töötasid üksteisest sõltumatult välja prantsuse matemaatik Bernard Roy ning ameerika arvutiteadlased Robert Floyd ja Stephen Warshall. Teise algoritmi autor on hollandi arvutiteadlane Edsger Wybe Dijkstra.

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 teist tippu (s.t. tippu, kuhu peaksime tipust i suunduma). 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 $k = 1, \dots, n$ do

 for $i = 1, \dots, n$ do

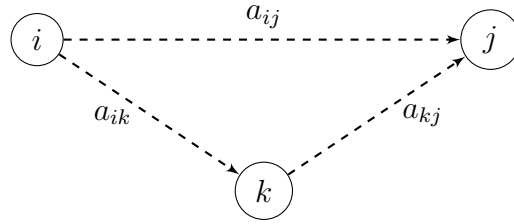
 for $j = 1, \dots, n$ do

 if $a_{ik} + a_{kj} < a_{ij}$ then

$a_{ij} := a_{ik} + a_{kj}$

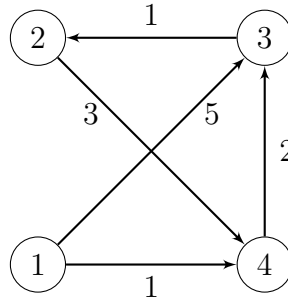
$b_{ij} := b_{ik}$

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 (sest $a_{kk} = 0$) ja seega omistamist ei toimu. Sama kehtib $j = k$ korral. See tähendab, et etapil k matriksi A ja B k -s rida ja k -s veerg ei muutu.

Näide 2.118 Rakendame Floyd–Warshalli algoritmi suunatud kaalutud graafile



Siis matriksi A elemendid muutuvad k väärtuste 1, 2, 3 ja 4 korral järgmiselt:

$$\begin{aligned}
 A : \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & 2 & 0 \end{pmatrix} &\longrightarrow \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & \infty & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & 4 \\ \infty & \infty & 2 & 0 \end{pmatrix} \longrightarrow \\
 &\longrightarrow \begin{pmatrix} 0 & 6 & 5 & 1 \\ \infty & 0 & \infty & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 4 & 3 & 1 \\ \infty & 0 & 5 & 3 \\ \infty & 1 & 0 & 4 \\ \infty & 3 & 2 & 0 \end{pmatrix}.
 \end{aligned}$$

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 matriksi A k -ndast veerust (a_{ik}) elemendiga k -ndast reast (a_{kj}). Elemendid $a_{kk} = 0, a_{kj}, a_{ij}, a_{ik}$ asuvad matriksis 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 matriks (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.

Matriksi B elemendid muutuvad järgmiselt:

$$B : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \longrightarrow$$

$$\longrightarrow \begin{pmatrix} 1 & 3 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 2 \\ 1 & 3 & 3 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 4 & 4 & 4 \\ 1 & 2 & 4 & 4 \\ 1 & 2 & 3 & 2 \\ 1 & 3 & 3 & 4 \end{pmatrix}.$$

Viimasest maatriksist saab välja lühimad teed kõigi tipupaaride vahel. Näiteks lühim tee tipust 1 tippu 2 sisaldab tippe

$$1, 4(=b_{12}), 3(=b_{42}) \text{ ja } 2(=b_{32}).$$

Tõestame, et Floyd-Warshalli algoritm töötab korrektselt.

Teoreem 2.119 *Pärast Floyd-Warshalli algoritmi täitmist kehtivad iga $i, j \in \{1, \dots, n\}$ 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 k -ahelateks tipust i tippu j kõiki suunatud ahelaid tipust i tippu j , mille vahetipud kuuluvad hulka $\{1, \dots, k\}$ ($k \geq 1$ on naturaalarv). 0-ahelateks tipust i tippu j nimetame suunatud ahelaid, millel sisetipud puuduvad. Seega 0-ahel on lihtsalt kaar (i, j) . Paneme tähele, et iga $(k-1)$ -ahel tipust i tippu j on ka k -ahel tipust i tippu j . Teoreemi tõestamiseks näitame, et kehtib järgmine väide:

(*) iga $k \in \{0, 1, \dots, n\}$ ja $i, j \in \{1, 2, \dots, n\}$ 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 $k = 0$. Siis k -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. Olgu $k > 0$. 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.

(1) Oletame, et leidub k -ahelaid tipust i tippu j . Olgu T üks minimaalse pikkusega k -ahel tipust i tippu j . Siis

$$\omega(T) \leq a_{ik} + a_{kj}. \quad (2.3)$$

Kuna induktsiooni eelduse põhjal on a_{ij} mingi minimaalse $(k-1)$ -ahela pikkus või ∞ ning iga $(k-1)$ -ahel on ka k -ahel, siis kehtib võrratus

$$\omega(T) \leq a_{ij}. \quad (2.4)$$

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 tipust i tippu j . Seega $a_{ij} = \omega(T)$. Võrratusest (2.3) saame võrratuse

$$a_{ij} \leq a_{ik} + a_{kj},$$

mistõttu etapil k a_{ij} -le ja b_{ij} -le uut väärtust ei omistata. Minimaalsed k -ahelad ja minimaalsed $(k-1)$ -ahelad tipust i tippu j on sama pikkusega (see pikkus on a_{ij}). Pärast etappi k on b_{ij} väärtuseks mingi sellise $(k-1)$ -ahela T' teise tipu number. See ahel T' on ka minimaalne k -ahel ja seega a_{ij} ja b_{ij} väärtused on sellised nagu vaja.

b) T sisaldab tippu k . Siis ta sisaldab tippu k täpselt ühe korra, sest minimaalne ahel peab olema lihtahel. Olgu

$$T = i, u, \dots, v, k, x, \dots, y, j.$$

Siis

$$T_1 = i, u, \dots, v, k \text{ ja } T_2 = k, x, \dots, y, j$$

on $(k-1)$ -ahelad, kusjuures nende pikkused peavad olema minimaalsed, sest muidu ei oleks T minimaalne k -ahel. Induktsiooni eelduse ja võrratuse (2.4) tõttu peab

$$a_{ik} + a_{kj} = \omega(T_1) + \omega(T_2) = \omega(T) \leq a_{ij}.$$

Kui $\omega(T) = a_{ij}$, siis a_{ij} -le ja b_{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 nii juhul a) kui ka juhul b) elemendi a_{ij} väärtuseks ahela T pikkus ning b_{ij} väärtuseks on tipust i tippu j viiva minimaalse pikkusega k -ahela teise tipu number. See tähendab, et (1) kehtib pärast etappi k .

(2) Oletame nüüd, et k -ahelaid tipust i tippu j ei leidu. Siis ei leidu ka $(k-1)$ -ahelaid ja seega induktsiooni eelduse põhjal pärast etappi $k-1$ kehtib võrdus $a_{ij} = \infty$. Lisaks sellele kas $a_{ik} = \infty$ või $a_{kj} = \infty$ (kui mõlemad arvud oleksid lõplikud, siis peaks leiduma k -ahel tipust i tippu j). Järelikult võrratus

$$a_{ik} + a_{kj} < a_{ij}$$

ei saa kehtida ning a_{ij} -le ja b_{ij} -le uut väärtust ei omistata. Niisiis ka (2) kehtib pärast etappi k . $\square$

Dijkstra algoritm

Antud: kaalutud suunatud graaf $G = (V, E, \omega)$, algtip 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 väljavali 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 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 tsükel

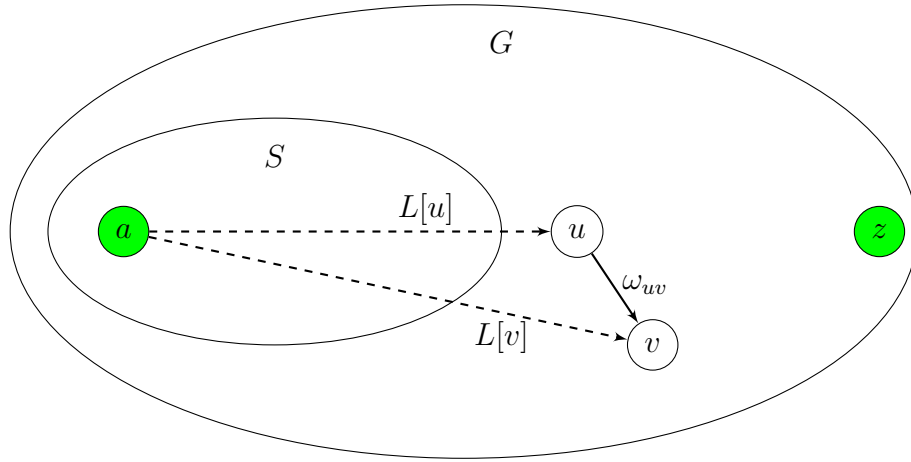
while $z \notin S$ do

$u :=$ 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 2.120 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 .

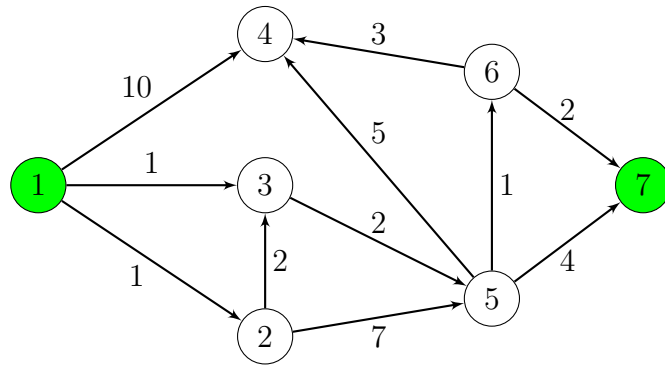
2. Võib juhtuda, et u valimisel on kõigi vaadeldavate tippude $i \notin S$ korral $L[i] = \infty$ (vt. näidet 2.122). Siis me valimegi ühe neist tippudest.

3. Kui $\omega_{uv} = \infty$, siis tingimus $L[u] + \omega_{uv} < L[v]$ ei ole täidetud (isegi siis, kui $L[v] = \infty$). Seega for-tsükliks 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 tahaksime leida lühimad teed kõigisse teistesse tippudesse (mitte ainult tippu z), siis tuleks while-tsükliks tingimus $z \notin S$ asendada tingimusega $S \neq V$. Nii vaadatakse u osas läbi kõik graafi tipud.

Näide 2.121 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

$$S = \{1, 2, 3, 5, 6, 7\}.$$

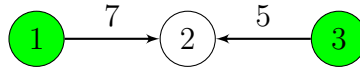
Järgnevas tabelis on ära toodud $L[i]$ -de väärtused igal sammul (sammu 0 all on mõeldud algväärtustamist). Tabeli iga veeru põhjal valitakse uus element u nende tippude i hulgas,

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 2.122 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 2.123 *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 pidi olema $L[v] \neq \infty$ 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 $k + 1$. $\square$

Teoreem 2.124 *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. Väite 2 kehtimine järeldub lemmast 2.123. Tõestame väite 1.

Eeldame, et pärast algoritmi täitmist $v \in S$ ja tipust a leidub suunatud ahelaid tippu v . Siis $d(a, v) \neq \infty$. Kui õnnestub tõestada võrratus

$$L[v] \leq d(a, v), \quad (2.5)$$

siis $L[v] \neq \infty$ ja lemma 2.123 põhjal on $L[v]$ mingi suunatud ahela pikkus tipust a tippu v . Järelikult $d(a, v) \leq L[v]$ ja me saame vajaliku võrduse $L[v] = d(a, v)$.

Tõestame võrratuse (2.5) 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 $v \neq a$, mis pärast algoritmi täitmist kuulub hulka S ja kuhu leidub tipust a suunatud ahelaid. Olgu T mingi 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 $L[i] \leq d(a, i)$ 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 2.117(3) peab kehtima võrratus $d(a, y) \leq d(a, v)$.
- Kuna $a, \dots, x, y$ ja $a, \dots, x$ on minimaalse pikkusega 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: $L[x] \leq d(a, x)$. Järelikult

$$L[x] + \omega_{xy} \leq d(a, x) + \omega_{xy}.$$

- Kuna tipp x lisati hulka S mingil varasemal etapil, siis kõik temast väljuvad kaared (muuhulgas $e = (x, y)$) on for-tsükliks läbi vaadatud. Seega $L[y] \neq \infty$ ja

$$L[y] \leq L[x] + \omega_{xy}.$$

- Samal etapil, kus u väärtuseks valiti v , jäeti valimata y , mis oli ka väljaspool hulka S . Seega valiku hetkel peab kehtima võrratus

$$L[v] \leq L[y].$$

- Eelnevat kokku võttes näeme, et

$$L[v] \leq L[y] \leq L[x] + \omega_{xy} \leq d(a, x) + \omega_{xy} = d(a, y) \leq d(a, v),$$

mida oligi vaja.

□

Märkus 2.125 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 2.126 Millises järjekorras lisatakse tipud hulka S ? Olgu pärast Dijkstra algoritmi täitmist

$$S = \{v_1, v_2, \dots, v_r\},$$

kusjuures esimesena on lisatud v_1 (s.t. $v_1 = a$), teisenä v_2 jne. Tuleb välja, et

$$d(a, v_1) \leq d(a, v_2) \leq \dots \leq d(a, v_r),$$

s.t. tippe lisatakse hulka S tipule a läheduse järjekorras. Selle näitamiseks vaatleme iga $i \in \{1, \dots, r-1\}$ korral seda hetke, kui u -ks valitakse v_i . Sel hetkel kehtib iga $j \in \{i+1, \dots, r\}$ jaoks võrratus

$$L[v_i] \leq L[v_j].$$

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 $L[v_i] \leq L[v_{i+1}]$. while-tsükli järgmisel läbimisel valitakse u ossa v_{i+1} ja $L[v_{i+1}]$ väärtust enam ei muudeta. Seega

$$d(a, v_i) = L[v_i] \leq L[v_{i+1}] = d(a, v_{i+1}).$$

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 $L(v_i) \geq \delta$, siis võib algoritm töö lõpetada ja teatada, et sellist teed ei leidu.

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] O. Ore, Graafid ja nende kasutamine, “Valgus”, Tallinn, 1976.
- [9] R. Palm, R. Prank, Sissejuhatus matemaatilisse loogikasse, Tartu Ülikooli Kirjastus, 2004.
- [10] R. Palm, Diskreetse matemaatika elemendid, Tartu Ülikooli Kirjastus, 2003.
- [11] R. Prank, kursuse “Graafid ja matemaatiline loogika” loengute slaidid, Tartu, 2017.
- [12] R. Prank, Lausearvutuse kordamine, õppematerjal, Tartu, 2017.