DISKREETIT MALLIT JA MENETELMÄT

Jorma K. Mattila

Lappeenrannan teknillinen yliopisto
Sovelletun matematiikan laitos

Sisältö

1 JOHDANTO **3**

2 KLASSISTA INTUITIIVISTA JOUKKO-OPPIA **5**
2.1 Alkio, joukko ja osajoukko 5
2.2 Operoiminen joukoilla 6
2.3 Karteesinen tulo eli tulojoukko 10
2.4 Potenssijoukko ja joukkokunta 10
2.5 Äärellisistä ja äärettömistä joukoista 11
2.6 Joukkojen alkiomääristä 12
2.7 Osajoukkojen algebra 13
2.8 Joukon karakteristinen funktio 14
2.9 Joukko-opin laajennuksesta 18

3 RELAATIOT **21**
3.1 Relaation määritelmä ja esitystapoja 21
3.2 Binääristen relaatioiden ominaisuuksia 24
3.3 Erityisiä relaatioita 26

4 KLASSISTA LOGIIKKAA **28**
4.1 Looginen päättely 28
4.2 Mahdolliset maailmat 30
4.3 Formaalisista teorioista 33

5 PROPOSITIOLOGIIKKAA **35**
5.1 Aakkosto ja lauseenmuodostus 35
5.2 Arkikielen propositioita 37
5.3 $\mathcal{L}$:n semantiikkaa 38
5.4 Todistusteoriaa 44
5.5 Eräitä usein esiintyviä tehtävätyyppejä 54
5.6 Resoluutiomenetelmä 55

6 PREDIKAATTILOGIIKKA **59**
6.1 Syntaksi 59

7 BOOLEN ALGEBROISTA **62**
7.1 Yleistä taustaa 62
7.2 Operaatioista 62
7.3 Boolen algebran määrittely ja perusominaisuudet 64
7.4 Osittainen järjestys Boolen algebrassa 69
7.5 Boolen kaavat ja funktiot 72
7.6 Normaalimuodot 73
7.7 Isomorfismit 74
7.8 Boolen algebrat ja propositiologiikka 75

7.9 Lisää Boolen funktioista . . . 76
7.10 Kytkinpiirit . . . 78
7.11 Kombinatoriset piirit . . . 80

8 GRAAFITEORIAA 87
8.1 Verkkorakenteiden perusominaisuuksia . . . 87
8.2 Eulerin ja Hamiltonin kierrokset . . . 90
8.3 Tasograafeista . . . 91
8.4 Graafien värityksistä . . . 94
8.5 Puista . . . 97
8.6 Optimointi- ja sovitustehtäviä . . . 99

9 KOMBINATORIIKKAA 104
9.1 Summa- ja tuloperiaate . . . 104
9.2 Variaatiot ja kombinaatiot . . . 105
9.3 Osittelut ja multinomikertoimet . . . 106

10 AUTOMAATTIEN TEORIA 108
10.1 Äärelliset automaatit . . . 108
10.1.1 Peruskäsitteitä . . . 108
10.1.2 Äärellinen puoliautomaatti . . . 108
10.1.3 Äärellinen automaatti . . . 116
10.2 Turing-kone . . . 118

11 FORMAALISET KIELET 126
11.1 Kielioppi ja kieli . . . 126
11.2 Kielioppien tyyppejä . . . 131
11.3 kielioppien ja automaattien välinen yhteys . . . 132

12 LUKUTEORIAA 134
12.1 Lukuteoreettisia probleemeja . . . 134
12.2 Kokonaislukujen kantaesitys . . . 137
12.3 Jaollisuus ja Eukleideen algoritmi . . . 138
12.4 Kongruenssi . . . 140

1 JOHDANTO

Tarkastelemme tässä muutamia perusasioita, joita tuonnempana tarvitaan. Ensinnäkin merkitsemme lukujoukkoja seuraavasti:

$\mathbb{N} = \{1, 2, \ldots, n, \ldots\}$	luonnollisten lukujen joukko
$\mathbb{N}_0 = \{0, 1, 2, \ldots, n, \ldots\}$	peruslukujen joukko ($\mathbb{N}$ lisättynä luvulla 0)
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	kokonaislukujen joukko
$\mathbb{Q} = \left\{\frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0\right\}$	rationaalilukujen joukko
$\mathbb{R}$	reaalilukujen joukko

Kukin lukujoukko on järjestetty joukko-operaatioiden '$<$' ja '$>$' suhteen. Lisäksi joukot sisältyvät toisiinsa seuraavalla tavalla:

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Jos rajoitumme tarkastelemaan jonkin lukujoukon joko pelkästään positiivista tai negatiivista osaa, ilmaisemme tämän etumerkillä, joka sijoitetaan lukkujoukon symbolin alaindeksiksi, esim $\mathbb{Z}_+$ tarkoittaa positiivisten kokonaislukujen joukkoa.

Lause 1.0.1 (induktioperiaate). *Kokonaislukua m koskeva väite voidaan todistaa kaikille kokonaisluvuille m, joka on suurempi tai yhtäsuuri kuin tietty kokonaisluku, sanokaamme a_0, seuraavalla kahdella askeleella:*

(i) Todistetaan, että väite pätee kokonaisluvulle a_0.

(ii) Todistetaan seuraava lemma: Olkoon k, $k \geq a_0$, mikä tahansa kokonaisluku. Jos väite on tosi k:lle, niin lause on tosi kokonaisluvulle $k + 1$.

Askel (ii) on ns. induktioaskel ja lemman oletusta kutsutaan induktio-oletukseksi. Sanomme, että väite on todistettu induktiolla m:n suhteen.
Tässä on toinen tapa tarkastella induktioperiaatetta. Oletetaan, että on väite, jonka väitetään pitävän paikkansa kaikille a_0:aa suuremmille tai yhtä suurille kokonaisluvuille. Jos näin ei ole, niin on oltava sellainen pienin kokonaisluku h, $h \geq a_0$, jolle väite ei päde. Nyt on selvästi $h \neq a_0$, koska olemme todistaneet askeleessa (i), että väite pätee a_0:lle. Täten $h > a_0$, ja $h - 1 \geq a_0$. Edelleen, koska h on pienin kokonaisluku, jolle väite ei päde, täytyy väitteen päteä luvulle $h-1$. Mutta jos asetamme $k = h - 1$ askeleessa (ii), jolle väite on todistettu, päättelemme, että väite on tosi kokonaisluvulle $k + 1$ eli h:lle. Täten vastaoletus väitteen pätemättömyydestä h:lle on väärä.

Esimerkki 1.0.2. *Määrätään lukujono (S_n) seuraavasti:*

$$S_n = \sum_{i=1}^{n} (2i - 1) = 1 + 3 + 5 + \ldots + (2n + 1).$$

Tarkastellaan tätä lukujonoa järjestyksessä alusta alkaen muutaman alkion verran. Saamme

$$
\begin{array}{lll}
S_1 = 1 & = 1 & = 1^2 \\
S_2 = 1 + 3 & = 4 & = 2^2 \\
S_3 = 1 + 3 + 5 & = 9 & = 3^2 \\
S_4 = 1 + 3 + 5 + 7 & = 16 & = 4^2 \\
S_5 = 1 + 3 + 5 + 7 + 9 & = 25 & = 5^2 \\
S_6 = 1 + 3 + 5 + 7 + 9 + 11 & = 36 & = 6^2
\end{array}
$$

Otaksuma: $S_n = n^2$ *kaikille* $n \in \mathbb{N}$*. Todistetaan tämä käyttäen matemaattista induktiota.*
Väite: $S_n = n^2$ *kaikille* $n \in \mathbb{N}$*.*
Tod. *(1) vasen puoli* $= S_1 = 1$*, oikea puoli* $= 1^2 = 1$
Siis väite on tosi, kun $n = 1$*.*
(2) Induktio-oletus: $S_k = k^2$
Induktioväite: $S_{k+1} = (k+1)^2$
Induktioväitteen todistus: $S_{k+1} = (2i-1) = \sum_{i=1}^{n}(2i-1)+(2(k+1)-1) = k^2+2k+1 = (k+1)^2$
Siis induktioväite on tosi. Tällöin induktioperiaatteesta seuraa, että myös alkuperäinen väite $S_n = n^2$ *kaikille* $n \in \mathbb{N}$ *on todistettu.*

2 KLASSISTA INTUITIIVISTA JOUKKO-OPPIA

$\mathrm{card}(X)$.
Klassisen joukko-opin pääpiirteittäinen tuntemus on välttämätöntä diskreettien rakenteiden ja mm. sumeiden joukkojen tutkimuksessa, mutta se toimii yleensäkin hyvin kielenä matemaattisia asioita esitettäessä. Lisäksi tiedämme paremmin, mistä on kysymys algebrassa, topologiassa, sumeissa joukoissa tai yhtälöiden ratkaisemisessa, kun hallitsemme klassista joukko-oppia, vaikkapa vain intuitiivisella tasolla.

2.1 Alkio, joukko ja osajoukko

Asetamme joukko-oppimme perustaksi (loogisesti hämärän) ilmauksen:

> *Joukko* on kokoelma objekteja, joita kutsutaan tämän joukon *alkioiksi*. Joukkoa ei saa asettaa itsensä alkioksi.

Joukon käsitteen pitää olla siinä mielessä selkeä, että jokaisesta alkiosta voidaan (ainakin periaatteessa) selvittää kuuluuko se annettuun joukkoon vai ei.
Joukon alkiot voivat itsekin olla joukkoja, mutta tässä tulee olla varovainen! Jos sallisimme joukon olevan itsensä alkio, saisimme muodostaa houkuttelevan ”kaikkien joukkojen joukon”. Toisaalta tämä johtaa ikävyyksiin, kuten osoittaa esittäjänsä filosofi ja matemaatikko Bertrand Russellin mukaan nimetty *Russellin paradoksi*: *Joukko, jonka alkioina ovat ne joukot, jotka eivät ole itsensä alkioita, on itsensä alkio, jos ja vain jos se ei ole itsensä alkio.*
Seuraavassa kuvataan erilaisia keinoja konkreettisen joukon ilmaisemiseksi:

- käytetään sovittua nimitystä tai muuta merkintätapaa; esimerkiksi $\mathbb{N}$ tai reaalilukuväli $[1, 5]$
- kuvataan joukon alkiot sanallisesti: ”parilliset luonnolliset luvut alta kymmenen”
- luetellaan joukon alkiot: $\{2, 4, 6, 8\}$
- esitetään joukon alkiot täysin määräävä ehto:

$$\{\, n \in \mathbb{N} \mid n = 2k < 10 \text{ jollekin } k \in \mathbb{N} \,\}. \tag{2.1}$$

- muodostetaan joukko-operaatioilla muista joukoista (ks. Luku 2.2).

Aina kun joukko ilmaistaan luettelona tai ehtomuodossa, **alkiot suljetaan aaltosulkujen sisälle**.
Ehtomuodossa tarvitaan jokin alkioita rajaava ominaisuus P; joukko

$$\{\, x \mid P(x) \,\}$$

on siten kaikkien niiden alkioiden x joukko, joille ominaisuus P pätee eli ehto $P(x)$ on tosi.

Esimerkki 2.1.1. *Joukko*

$$\{\, x \in \mathbb{R} \mid x^2 - 2x - 3 = 0 \,\}$$

on niiden reaalilukujen joukko, jotka ovat yhtälön $x^2 - 2x - 3 = 0$ *reaalisia ratkaisuja.*

Tehtävä 2.1. *Esitä esimerkkijoukon (2.1) alkiot määräävä ehto* P.

Joukossa $\{a\}$ alkio a on sen ainoa alkio; tällaista joukkoa kutsutaan nimellä *yksiö* (*singleton*). Kun $a \neq b$, on joukossa $\{a, b\}$ tarkalleen kaksi alkiota. Sitä kutsutaan *ei-järjestetyksi pariksi*, ja sille on tietenkin voimassa $\{a, b\} = \{b, a\}$. Ääretön joukko voidaan esittää joskus myös alkioiden luettelointiperiaatteella, esimerkiksi $\mathbb{N}$ muodossa $\{1, 2, 3, \ldots\}$.
Usein joukkoja tarkastellaan jonkin laajemman joukon $\mathbf{X}$ osajoukkoina. Tällöin joukkoa $\mathbf{X}$ sanotaan *perusjoukoksi* (*universal set, universe of discourse*).
Alkion kuuluminen joukkoon merkitään tavalliseen tapaan $\in$-symbolilla:

Merkintä $x \in A$ tarkoittaa, että alkio x kuuluu joukkoon A.

Määritelmä 2.1.2. Joukot A ja B ovat *identtiset* eli *samat* tarkalleen silloin, kun niillä on täsmälleen samat alkiot; tätä merkitään $A = B$. Muulloin merkitään $A \neq B$.

Määritelmä 2.1.3. Sanomme, että A on joukon B *osajoukko* (*subset*), jos kaikki joukon A alkiot ovat myös joukon B alkioita. Tällöin sanotaan myös, että A *sisältyy* joukkoon B; tätä merkitään $A \subseteq B$. Kun $A \subseteq B$ ja $A \neq B$, sanomme, että A on joukon B *aito* osajoukko (*proper subset*); merkitään $A \subset B$.

Määritelmä 2.1.4. Jos P on sellainen ominaisuus, että $P(x)$ ei päde millään alkiolla x, ei joukolla $\{x \mid P(x)\}$ ole yhtään alkiota. Tällöin joukko on *tyhjä*, merkitään $\emptyset$ (*void, empty set*). Tyhjä joukko sisältyy jokaiseen joukkoon, ts. $\emptyset \subseteq A$, kun A on mikä tahansa joukko.

Esimerkki 2.1.5. (a) Tyhjän joukon $\emptyset$ ainoa osajoukko on $\emptyset$ itse.
(b) Yksiön $\{x\}$ osajoukot ovat $\emptyset$ ja $\{x\}$. Niitä on siis kaksi.
(c) Kun $x \neq y$, on joukolla $\{x, y\}$ osajoukot $\emptyset$, $\{x\}$, $\{y\}$ ja $\{x, y\}$, siis neljä kappaletta.

2.2 Operoiminen joukoilla

Määritelmä 2.2.1. Olkoot A ja B joukkoja. Joukkojen A ja B
(a) *yhdiste* eli *unioni* (*union*) on joukko

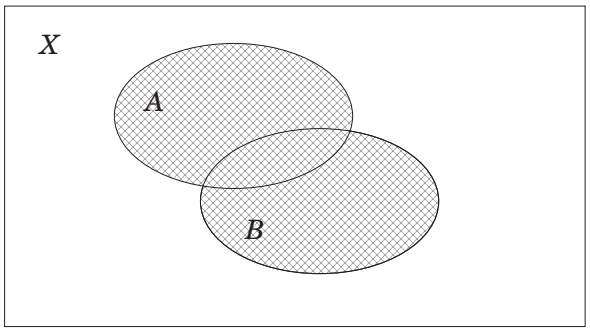
$$A \cup B = \{x \mid x \in A \text{ tai } x \in B\};$$

(b) *leikkaus* (*intersection*) on joukko

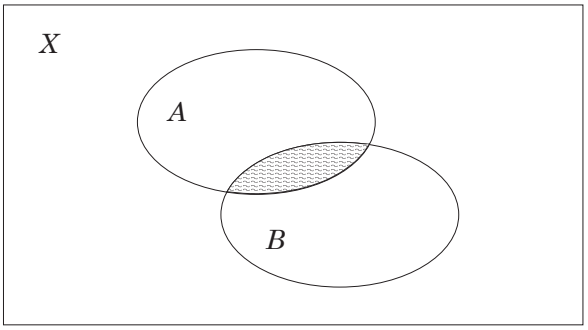
$$A \cap B = \{x \mid x \in A \text{ ja } x \in B\}.$$

Joukot A ja B ovat keskenään *alkiovieraita*, *pistevieraita* eli *erillisiä* (*disjoint*), jos $A \cap B = \emptyset$.

Kuvat 1 ja 2 havainnollistavat yhdistettä ja leikkausta nk. *Venn-diagrammin* avulla.



Kuva 1: Joukkojen A ja B yhdiste perusjoukossa $\mathbf{X}$.



Kuva 2: Joukkojen A ja B leikkaus perusjoukossa $\mathbf{X}$.

Lause 2.2.2. Yhdisteellä ja leikkauksella on seuraavat ominaisuudet:

(1) $A \cup A = A$; $A \cap A = A$ (idempotenssi)

(2) $A \cup B = B \cup A$; $A \cap B = B \cap A$ (kommutatiivisuus)

(3) $A \cup \emptyset = A$; $A \cap \emptyset = \emptyset$

(4) $(A \cup B) \cup C = A \cup (B \cup C)$ (assosiatiivisuus 1)

$(A \cap B) \cap C = A \cap (B \cap C)$ (assosiatiivisuus 2)

(5) $A \cup B = B$, jos ja vain jos $A \subseteq B$

$A \cap B = A$, jos ja vain jos $A \subseteq B$

(6) $A \subseteq A \cup B$ ja $B \subseteq A \cup B$

$A \cap B \subseteq A$ ja $A \cap B \subseteq B$

Unionin ja leikkauksen kesken vallitsevat myös *osittelu-* eli *distributiivisuuslait*:

(D1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributiivisuus 1)

(D2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributiivisuus 2)

Todistus. Esimerkiksi distributiivisuuslaki 1 todistuu seuraavasti:

$$\begin{aligned} A \cap (B \cup C) &= \{x \mid x \in A \text{ ja } x \in B \cup C\} = \{x \mid x \in A \text{ ja } (x \in B \text{ tai } x \in C)\} \\ &= \{x \mid (x \in A \text{ ja } x \in B) \text{ tai } (x \in A \text{ ja } x \in C)\} \\ &= \{x \mid x \in A \cap B \text{ tai } x \in A \cap C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

■

Seuraus 2.2.3. Distributiivisuuslait voidaan yleistää muotoon

(D1') $A \cap (B_1 \cup B_2 \cup \ldots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \ldots \cup (A \cap B_n)$

(D2') $A \cup (B_1 \cap B_2 \cap \ldots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \ldots \cap (A \cup B_n)$

Todistus. Todistus matemaattisella induktiolla; sopiva harjoitustehtäväksi. ■

Määritelmä 2.2.4. Perusjoukon $\mathbf{X}$ osajoukon A *komplementti* $\overline{A}$ on joukko

$$\overline{A} = \{x \mid x \in \mathbf{X} \text{ ja } x \notin A\}.$$

Lause 2.2.5. Joukon komplementilla on mm. seuraavia ominaisuuksia:

(C1) $\overline{\overline{A}} = A$ (kaksoiskomplementin laki)

(C2) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (DeMorganin laki 1)

(C3) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (DeMorganin laki 2)

(C4) $A \cap \overline{A} = \emptyset$, $A \cup \overline{A} = \mathbf{X}$

(C5) $\overline{\emptyset} = \mathbf{X}$, $\overline{\mathbf{X}} = \emptyset$

(C6) $A \subset B$ jos ja vain jos $\overline{B} \subset \overline{A}$

(C7) $A = B$ jos ja vain jos $\overline{A} = \overline{B}$

Todistus. Sopivia harjoitustehtäviä. ■

Määritelmä 2.2.6. Joukkojen A ja B *erotus* $A \setminus B$ on joukko

$$A \setminus B = \{x \mid x \in A \text{ ja } x \notin B\}$$

Lause 2.2.7. Joukkojen erotuksella on mm. seuraavia ominaisuuksia:

(E1) $A \setminus A = \emptyset$

(E2) $A \setminus \emptyset = A$

(E3) $\emptyset \setminus A = \emptyset$

(E4) $(A \setminus B) \setminus C = A \setminus (B \cup C) = (A \setminus C) \setminus B$

(E5) $A \setminus B = A \cap \overline{B}$

Todistus. Kuten edellä. ■

Määritelmä 2.2.8. Joukkojen A ja B *symmetrinen erotus* $A \triangle B$ on joukko

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

Lause 2.2.9. Symmetrisellä erotuksella on mm. seuraavia ominaisuuksia:

(SE1) $A \triangle A = \emptyset$

(SE2) $A \triangle B = B \triangle A$

(SE3) $A \triangle \emptyset = A$

(SE4) $A \triangle B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$

(SE5) $A \triangle B = (A \cup B) \setminus (A \cap B)$

Todistus. Kuten edellä. ■
Perusjoukon $\mathbf{X}$ osajoukkojen unioni, leikkaus, komplementti, erotus ja symmetrinen erotus ovat edelleen perusrjoukon $\mathbf{X}$ osajoukkoja. Näiden operaatioiden välillä löytyy riippuvuuksia. Voimme valita ns. perusoperaatioiksi esimerkiksi unionin, leikkauksen ja komplementin, kuten yleensä tehdäänkin. Muut joukko-operaatiot voidaan esittää näiden perusoperaatioiden avulla. Kuten edellä nähdään, riippuu symmetrinen erotus unionista ja erotuksesta. Se voidaan kuitenkin esittää komplementin avulla käyttämättä erotusta, koska erotus voidaan esittää leikkauksen ja komplementin avulla sekä komplementti erotuksen avulla; kun $A \subseteq \mathbf{X}$, on

$$\overline{A} = \mathbf{X} \setminus A$$

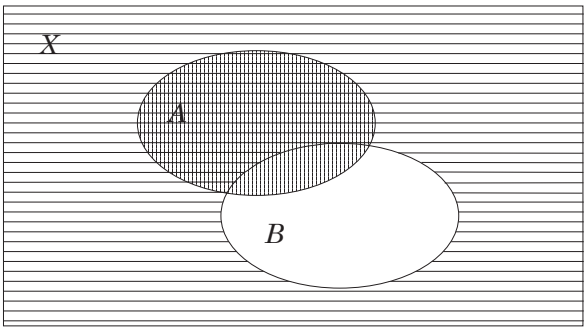
Perusoperaatiot unioni, leikkaus ja komplementin muodostus, jotka muodostavat joukoille ns. *hilaoperaatiot* (ks. Luku **??**).

Seuraus 2.2.10. DeMorganin laeilla (C2) ja (C3) on voimassa luonnolliset yleistykset:

(C2') $\overline{A_1 \cup A_2 \cup \ldots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_n}$

(C3') $\overline{A_1 \cap A_2 \cap \ldots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \ldots \cup \overline{A_n}$

Todistus. Induktioperiaatteella. ■



Kuva 3: Joukko $A \cap \overline{B}$

Esimerkki 2.2.11. *Väite*: $A \subseteq B$ jos ja vain jos $A \cap \overline{B} = \emptyset$.
Kuvassa 3 ristikoitu alue edustaa joukkoa $A \cap \overline{B}$. Se, että tämä joukko on tyhjä, on yhtäpitävä sen kanssa, että A on kokonaisuudessaan joukon B sisällä. Täsmällinen todistus on seuraava: joukolla A on esitys

$$A = A \cap \mathbf{X} = A \cap (B \cup \overline{B}) = (A \cap B) \cup (A \cap \overline{B})$$

Täten, jos $A \cap \overline{B} = \emptyset$, niin $A = A \cap B$. Tästä seuraa unionin ja leikkauksen ominaisuuden (5) nojalla, että $A \subseteq B$. Toisaalta, jos $A \subseteq B$, on em. ehdon (5) nojalla $A = A \cap B$ ja täten

$$A \cap \overline{B} = (A \cap B) \cap \overline{B} = A \cap (B \cap \overline{B}) = A \cap \emptyset = \emptyset.$$

2.3 Karteesinen tulo eli tulojoukko

Joukkoalgebraan saadaan lisäulottuvuutta ottamalla käyttöön tulojoukot. Näillä voidaan mallintaa tai kuvata rinnakkain kahta tai useampaakin ilmiötä.

Määritelmä 2.3.1. *Kahden joukon* $\mathbf{X}$ *ja* $\mathbf{Y}$ karteesinen tulo *eli* tulojoukko $\mathbf{X}\times\mathbf{Y}$ *on järjestettyjen parien* (a, b) *joukko, missä* $a \in \mathbf{X}$ *ja* $b \in \mathbf{Y}$*; siis*

$$\mathbf{X}\times\mathbf{Y} := \{\, (a, b) \mid a \in \mathbf{X}, b \in \mathbf{Y} \,\}.$$

Esimerkki 2.3.2. *Joukkojen* $\mathbf{X} := \{x_1, x_2, x_3\}$ *ja* $\mathbf{Y} := \{y_1, y_2\}$ *tulojoukossa on* $3 \cdot 2 = 6$ *alkiota*

$$\mathbf{X}\times\mathbf{Y} = \{\, (x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2), (x_3, y_1), (x_3, y_2)\}.$$

Tulojoukko voidaan muodostaa useammallekin joukolle. Tulojoukko toimii mm. relaation ja matriisien perusjoukkona, ks. luku "Relaatiot ja funktiot".
Suuntaamattoman verkon yhteydessä käytetään nk. *ei-järjestettyä tuloa,* ks. luku "Suuntaamattomat verkot".

2.4 Potenssijoukko ja joukkokunta

Olkoon $\mathcal{P}(\mathbf{X})$ joukon $\mathbf{X}$ kaikkien osajoukkojen joukko, ts.

$$\mathcal{P}(\mathbf{X}) = \{B \mid B \subseteq \mathbf{X}\}.$$

Joukkoa $\mathcal{P}(\mathbf{X})$ sanotaan joukon $\mathbf{X}$ *potenssijoukoksi* (*power set*).

Esimerkki 2.4.1. *Joukolla* $\mathbf{X} := \{1, 2, 3\}$ *on yhteensä* 8 *osajoukkoa ja*

$$\mathcal{P}(\mathbf{X}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\},$$

Esimerkki 2.4.1 havainnollistaa tuonnempana esitettävää lausetta 2.6.3.

Määritelmä 2.4.2. *Joukkojen* kunnalla $\mathcal{F}$ *joukossa* $\mathbf{X}$ *tarkoitetaan sellaista* $\mathbf{X}$*:n osajoukkojen kokoelmaa, että kun* A, $B \in \mathcal{F}$, *niin* $A \cup B$, $A \cap B$ *ja* $\overline{A} \in \mathcal{F}$. *Tällöin sanomme, että* $\mathcal{F}$ *on* suljettu *operaatioiden yhdiste, leikkaus ja komplementti suhteen.*

Koska DeMorganin lakien mukaan

$$A \cup B = \overline{(\overline{A} \cap \overline{B}} \text{ ja } A \cap B = \overline{\overline{A} \cup \overline{B}},$$

tämä seikka riittää osoittamaan sulkeutumisen sekä komplementin ja unionin että komplementin ja leikkauksen suhteen.

Esimerkki 2.4.3. *Joukkokuntia ovat esimerkiksi*
(a) Joukon $\mathbf{X}$ *potenssijoukko* $\mathcal{P}(\mathbf{X})$,
(b) Joukon $\mathbf{X}$ *kaikkien äärellisten osajoukkojen ja niiden komplementtien joukko, ja*
(c) $\{\emptyset, \mathbf{X}\}$.

Mikä tahansa perusjoukon $\mathbf{X}$ osajoukkojen kunta $\mathcal{F}$ sisältää joukot $\emptyset$ ja $\mathbf{X}$, sillä jos $A \in \mathcal{F}$, niin $\overline{A} \in \mathcal{F}$ ja täten $\emptyset = A \cap \overline{A} \in \mathcal{F}$, jolloin $\mathbf{X} = \overline{\emptyset} \in \mathcal{F}$.

2.5 Äärellisistä ja äärettömistä joukoista

Alkeisjoukko-opin lopuksi luomme pinnallisen katsauksen joukkojen kokovertailuun. Tarkempi koneisto esitellään luvussa "Mahtavuus ja kardinaliteetti".

Määritelmä 2.5.1. Äärellinen *joukko on joukko, joka on joko tyhjä tai sen alkiot voidaan numeroida* 1*:stä* n*:ään, missä* n *on äärellinen kokonaisluku. Täsmällisemmin tämä voidaan ilmaista siten, että on olemassa bijektio joukon* A *ja enintään* n*:n suuruisten ei-negatiivisten kokonaislukujen joukon välillä. Jos* $n = 0$, A *on tyhjä. Joukko* A *on* ääretön, *jos se ei ole äärellinen. Joukko* A *on* numeroituvasti ääretön, *jos ja vain jos* A*:n alkiot voidaan numeroida kaikilla positiivisilla kokonaisluvuilla, ts. on olemassa bijektio joukkojen* $\mathbb{N}$ *ja* A *välillä.*
On selvää, että äärellisen joukon osajoukko on äärellinen. Myös minkä tahansa joukon äärellisen joukon leikkaus on äärellinen. Selvää on myös, että kahden äärellisen joukon unioni on äärellinen. Selvästi jokainen joukko, jolla on ääretön osajoukko, on ääretön. Kuitenkaan kahden äärettömän joukon leikkauksen ei tarvitse olla ääretön. Esimerkiksi parittomien kokonaislukujen ja parillisten kokonaislukujen leikkaus on tyhjä.
Joukon alkioiden määrä ilmaisee joukon mahtavuuden *eli* kardinaalisuuden. *Joukon* X *mahtavuutta esittää ns.* kardinaaliluku, *jota merkitään symbolilla card*X.

Esimerkki 2.5.2. (a) Positiivisten parillisten kokonaislukujen joukko on numeroituvasti ääretön. Bijektio on tällöin muotoa $f(n) = 2n$.
(b) Kokonaislukujen joukko on numeroituvasti ääretön. Numeroiminen suoritetaan seuraavasti: $0, 1, -1, 2, -2, 3, -3, \ldots$. Bijektio on muotoa

$$g(n) = \begin{cases} \frac{n}{2}, & \text{kun } n \text{ on parillinen} \\ -\frac{n-1}{2}, & \text{kun } n \text{ on pariton} \end{cases}$$

Selvästi äärellisen joukon ja numeroituvasti äärettömän joukon unioni on numeroituvasti ääretön ja kahden numeroituvasti äärettömän joukon unioni on numeroituvasti ääretön. Jos numeroituvasti äärettömästä joukosta vähennetään äärellinen joukko, on erotus numeroituvasti ääretön. Joukko on numeroituva, jos ja vain jos se on joko äärellinen tai numeroituvasti ääretön. Selvästi numeroituvan joukon osajoukko on numeroituva. Siitä, mitä edellä sanottiin äärellisistä ja numeroituvasti äärettömistä joukoista, seuraa, että kahden numeroituvan joukon unioni on numeroituva.

2.6 Joukkojen alkiomääristä

Puetaan lauseiksi intuitiivisesti ilmeiset äärellisten joukkojen yhdisteiden ja tulojen alkiomääriä koskevat tulokset. Olkoon $\#\mathbf{X}$ äärellisen joukon $\mathbf{X}$ alkioiden lukumäärä.

Lause 2.6.1. *Äärellisille joukoille A ja B on voimassa*

$$\#(A \cup B) = \#A + \#B - \#(A \cap B)$$

Äärellisille joukoille A, B ja C on voimassa

$$\begin{aligned} \#(A \cup B \cup C) &= \#A + \#B + \#C \\ &\quad -\#(A \cap B) - \#(A \cap C) - \#(B \cap C) \\ &\quad +\#(A \cap B \cap C). \end{aligned}$$

Vastaava joukkojen yleinen yhteenlaskukaava johdetaan n:n joukon unionin alkioiden lukumäärälle luvussa "Mahtavuus ja kardinaliteetti".

Lause 2.6.2. *Äärellisten joukkojen $\mathbf{X}$ ja $\mathbf{Y}$ alkiomäärille on*

$$\#(\mathbf{X} \times \mathbf{Y}) = \#\mathbf{X} \cdot \#\mathbf{Y}.$$

Esimerkkien 2.1.5 ja 2.4.1 perusteella voitaneen arvata seuraava potenssijoukkojen alkiomääriä koskeva tulos, joka todistetaan induktiotodistusharjoitukseksi.

Lause 2.6.3. *Jokaiselle ei-negatiiviselle kokonaisluvulle n pätee: Jos joukossa A on n alkiota, niin sen potenssijoukossa $\mathcal{P}(A)$ on 2^n alkiota.*

Todistus. Perustellaan väite matemaattisella induktiolla joukon alkiomäärän n suhteen.
(1) Kun $n = 0$, on asia selvä Esimerkin 2.1.5 kohdan (a) nojalla.

(2) Oletetaan, että lauseen väite on tosi, kun $n = k > 0$. Olkoon A joukko, jossa on $k+1$ alkiota, ts.

$$A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}.$$

On osoitettava, että joukolla A on 2^{k+1} osajoukkoa. Olkoon $B = \{a_1, a_2, \ldots, a_k\}$. Koska joukossa B on k alkiota, on sillä 2^k osajoukkoa. Kun lisätään joukon B jokaiseen osajoukkoon alkio a_{k+1}, saadaan täten 2^k uutta osajoukkoa. Koska $B \subseteq A$, ovat joukon B osajoukot myös A:n osajoukkoja. Myös uudet joukot ovat konstruktionsa perusteella A:n osajoukkoja. Täten joukolla A on

$$2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

osajoukkoa. Täten induktioväite on tullut todistetuksi. Matemaattisen induktion periaatteen nojalla on täten lause tullut todistetuksi. ■

2.7 Osajoukkojen algebra

Olkoon $\mathbf{X}$ ei-tyhjä joukko. Tarkastellaan sen potenssijoukkoa $\mathcal{P}(\mathbf{X})$. Edellä esitettyjen tarkastelujen perusteella tiedämme, että mille tahansa joukolle $A \in \mathcal{P}(\mathbf{X})$ pätee mm. seikat $A \cup \overline{A} = \mathbf{X}$, $A \cap \overline{A} = \emptyset$, $A \cap \mathbf{X} = A$ ja $A \cup \emptyset = A$. Myös kommutatiivi- ja distributiivilait ovat voimassa $\mathbf{X}$:n osajoukoille leikkauksen ja unionin suhteen.
Näitä ei-tyhjän joukon ominaisuuksia käyttäen saamme seuraavan osajoukkojen algebran.

Määritelmä 2.7.1. *Olkoon $\mathbf{X}$ ei-tyhjä joukko. Olkoot $\cap$ (leikkaus) ja $\cup$ (unioni) sellaisia binäärisiä operaatioita ja $^-$ (komplementti) sellainen yksipaikkainen operaatio joukossa $\mathcal{P}(\mathbf{X})$ ja olkoot alkiot $\emptyset$ ja $\mathbf{X}$ joukon $\mathcal{P}(\mathbf{X})$ sellaisia alkioita, että seuraavat aksioomat ovat voimassa:*

(BA1) $\cap$ ja $\cup$ ovat kommutatiivisia, ts. kaikille alkioille $A, V \in \mathcal{P}(\mathbf{X})$ on voimassa

$$A \cup B = B \cup A \text{ ja } A \cap B = B \cap A.$$

(BA2) Jokaiselle alkiolla $A \in \mathcal{P}(\mathbf{X})$ on voimassa $A \cup \emptyset = A$ ja $A \cap \mathbf{X} = A$ eli $\emptyset$ ja $\mathbf{X}$ ovat vastaavasti identiteettialkioita operaatioiden $\cap$ ja $\cup$ suhteen.

(BA3) Operaatiot $\cap$ ja $\cup$ ovat distributiivisia, ts. kaikille alkioille $A, B, C \in \mathcal{P}(\mathbf{X})$ on voimassa

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \;\; A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

(BA4) Jokaista alkiota $A \in \mathcal{P}(\mathbf{X})$ kohti on olemassa sellainen alkio $\overline{A} \in \mathcal{P}(\mathbf{X})$, että

$$A \cup \overline{A} = \mathbf{X} \text{ ja } A \cap \overline{A} = \emptyset.$$

(BA5) B:n alkioille $\emptyset$ ja $\mathbf{X}$ pätee $\emptyset \neq \mathbf{X}$.

Tällöin joukko $\mathcal{P}(\mathbf{X})$ yhdessä joukko-operaatioiden kanssa muodostaa Boolen algebran

$$\langle \mathcal{P}(\mathbf{X}), \cap, \cup, ^-, \emptyset, \mathbf{X} \rangle. \tag{2.2}$$

Algebra (2.2) on erikoistapaus *Boolen algebrasta*. Boolen algebroja tarkastellaan lähemmin omassa luvussaan.

2.8 Joukon karakteristinen funktio

Tarkastelemme joukon esittämistä ns. *karakteristisella funktiolla*. Tämä vastaa sitä tapaa, jolla sumeita joukkoja esitetään, ts. käytetään jäsenyysfunktiota.
Jos $\mathbf{X}$ on tavallinen numeroituva joukko ja $\#\mathbf{X} = n$ ($n = 1, 2, \ldots$), on tunnettua, että $\mathbf{X}$:n kaikista osajoukoista koostuva joukkosysteemi $\mathcal{P}(\mathbf{X})$ on numeroituva, ja siinä on 2^n alkiota. Jos $A \subset \mathbf{X}$, ts. $A \in \mathcal{P}(\mathbf{X})$, niin joukon A karakteristinen funktio on

$$f_A : \mathbf{X} \to \{0, 1\}, \tag{2.3}$$

missä jokaiselle X:n alkiolle x pätee

$$f_A(x) = \begin{cases} 1, & \text{kun } x \in A \\ 0, & \text{kun } x \notin A \end{cases} \tag{2.4}$$

On helppoa osoittaa, että $\mathcal{P}(\mathbf{X})$ ja kaikkien karakteristisen funktioiden joukko

$$Ch(\mathbf{X}) = \{f \mid f : \mathbf{X} \to \{0, 1\}\} \tag{2.5}$$

ovat *isomorfiset*, ts. $\mathcal{P}(\mathbf{X})$ ja $Ch(\mathbf{X})$ vastaavat struktuuriltaan täysin toisiaan. Tämä tarkoittaa sitä, että on olemassa sellaiset bijektiiviset kuvaukset $\varphi : \mathcal{P}(\mathbf{X}) \to Ch(\mathbf{X})$ ja $\psi : Ch(\mathbf{X}) \to \mathcal{P}(\mathbf{X})$, että niiden yhdistetyt kuvaukset ovat identiteettikuvauksia, ts.

$$\varphi \circ \psi = I_{Ch(\mathbf{X})} \text{ ja } \psi \circ \varphi = I_{\mathcal{P}(\mathbf{X})}, \tag{2.6}$$

missä I_M on kuvaus $I_M : M \to M$, $I_M(x) = x$ kaikille $x \in M$. Tällaisia kuvauksia ovat esim.

$$\varphi(A) = f_A \text{ ja } \psi(f) = \{x \in \mathbf{X} \mid f(x) = 1\} \tag{2.7}$$

Nämä konstruktiot osoittavat, kuinka klassisessa joukko-opissa voidaan joukko korvata karakteristisella funktiollaan. Voimme sanoa tarkastelemalla isomorfisuutta

$$\mathcal{P}(\mathbf{X}) \cong Ch(\mathbf{X}), \tag{2.8}$$

että intuitiivinen malli $\mathcal{P}(\mathbf{X})$ korvataan matemaattisella mallilla $Ch(\mathbf{X})$. Käyttämällä $Ch(\mathbf{X})$:ää hylkäämme intuitiivisen pohjan, jota $\mathcal{P}(\mathbf{X})$ esittää, ja saavutamme enemmän abstraktisuutta. Tämä tarkastelu korostaa tavallisen joukon terävyyttä siinä mielessä, että annettu alkio täsmällisesti joko kuuluu tiettyyn joukkoon tai ei kuulu siihen.
Joukkoon $Ch(\mathbf{X})$ kuuluvien funktioiden arvojen joukko on siis $\{0, 1\}$. Tarkastelemme $\mathbf{X}$:n osajoukoille määriteltyjen joukko-operaatioiden unioni, leikkaus ja komplementti vastineita karakteristisen funktioiden joukossa $Ch(\mathbf{X})$ ja niiden arvojoukossa $\{0, 1\}$.
Olkoot $A, B \subseteq \mathbf{X}$. Tällöin myös $A \cup B \subseteq \mathbf{X}$. Tutkimme, miten voimme yhdistää funktiot f_A ja f_B siten, että tulos kuuluu joukkoon $Ch(\mathbf{X})$ eli on unionin $A \cup B$ karakteristinen funktio. Jos alkio $x \in \mathbf{X}$ on sellainen, että $x \in A \cup B$, niin $x \in A$ tai $x \in B$, tai $x \in A$ ja $x \in B$, sekä kääntäen. Joukko-opillista unionia vastaa siis ns. 'mukaanlukeva tai', eli sovimme, että ei ole välttämätöntä merkitä näkyviin erityisesti sitä seikkää, että tapaus '$x \in A$ ja $x \in B$' on myös mahdollinen. Sovimme siis, että 'tai' ilman "lisukkeita" on mukaanlukeva tai. Jos meillä

Unionin $A \cup B$ karakteristinen funktio.

f_A	f_B	$f_A \vee f_B$
0	0	0
0	1	1
1	0	1
1	1	1

on tilanne, jossa tapaus '$x \in A$ ja $x \in B$' ei ole mahdollinen, sanomme, että *joko* $x \in A$ *tai* $x \in B$. Tätä ei joukko-opissa vastaakaan unioni vaan symmetrinen erotus. Siis unionin kohdalla meillä on tilanne $x \in A \cup B$, jos ja vain jos $x \in A$ tai $x \in B$. Sama asia ilmaistuna karakteristisilla funktioilla on

$$f_A(x) = 1 \text{ tai } f_B(x) = 1. \tag{2.9}$$

Merkitsemme tätä symbolisesti ilmaisulla

$$f_A(x) \vee f_B(x) = 1. \tag{2.10}$$

Jos alkio $x \in \mathbf{X}$ on sellainen, että $x \neq A$ ja $x \neq B$, vastaa tämä tarkalleen tilannetta $x \neq A \cup B$. Siis kun $x \neq A \cup B$, niin $f_A(x) = 0$ tai $f_B(x) = 0$ ja kääntäen. Tästä seuraa edellisen kaavan symboliikkaa käyttäen

$$f_A(x) \vee f_B(x) = 0. \tag{2.11}$$

Voimmekin määritellä joukon $A \cup B$ karakteristisen funktion muodossa 'f_A tai f_B' eli muodossa

$$f_{A \cup B} = f_A \vee f_B \tag{2.12}$$

kaikille joukoille $A, B \subseteq \mathbf{X}$, jolloin $f_A, f_B \in Ch(\mathbf{X})$. Koska $A \cup B \subseteq \mathbf{X}$ eli $A \cup B \in \mathcal{P}(\mathbf{X})$, niin myös $f_A \vee f_B \in Ch(\mathbf{X})$. (2.11):n perusteella siis sekä $f_A(x) = 0$ että $f_B(x) = 0$ tarkalleen silloin, kun $x \neq A \cup B$. Jos olisi joko $f_A(x) = 1$ ja $f_B(x) = 0$ tai $f_A(x) = 0$ ja $f_B(x) = 1$, olisi tilanne (2.10):n mukainen, eli $f_{A \cup B}(x) = 1$. Kokoamme yhteen funktion $f_A \vee f_B$ arvot esitettynä f_A:n ja f_B:n arvojen avulla taulukon 2.8 mukaisesti.
Perusjoukon $\mathbf{X}$ osajoukkojen A ja B leikkaukselle $A \cap B$ saamme karakteristisen funktion seuraavasti. Olkoon alkio $x \in \mathbf{X}$ sellainen, että $x \in A \cap B$. Tämä on yhtäpitävä sen kanssa, että $x \in A$ ja $x \in B$. Siis $f_A(x) = 1$ ja $f_B(x) = 1$. Jos $x \notin A$ tai $x \notin B$, niin $x \notin A \cap B$, ts. jos $f_A(x) = 0$ tai $f_B(x) = 0$, niin $f_{A \cap B}(x) = 0$. Voimme siis ilmaista leikkauksen $A \cap B$ karakteristisen funktion muodossa 'f_A ja f_B', jota symbolisesti merkitsemme ehdolla

$$f_{A \cap B} = f_A \wedge f_B. \tag{2.13}$$

Funktion $f_{A \cap B}$ arvot riippuvat funktioiden f_A ja f_B arvoista taulukon 2.8 osoittamalla tavalla
Perusjoukon $\mathbf{X}$ osajoukon A komplementin $\overline{A}$ karakteristinen funktio saadaan seuraavasti. Olkoon ensin alkio $x \in \mathbf{X}$ sellainen, että $x \in \overline{A}$ eli $x \in \mathbf{X} \setminus A$ eli $x \notin A$. Tämä on yhtäpitävä sen kanssa, että $f_{\overline{A}}(x) = 1$. Jos taas $x \in A$, niin $x \notin \overline{A}$, jolloin $f_{\overline{A}}(x) = 0$. Määrittelemme

Leikkauksen $A \cap B$ karakteristinen funktio.

f_A	f_B	$f_A \wedge f_B$
0	0	0
0	1	0
1	0	0
1	1	1

Komplementin $\overline{A}$ karakteristinen funktio.

f_A	$\neg f_A$
0	1
1	0

siis komplementin $\overline{A}$ karakteristisen funktion muodossa 'ei f_A', jota merkitsemme symbolisesti ehdolla

$$f_{\overline{A}}(x) = \neg f_A. \tag{2.14}$$

Taulukko 2.8 antaa funktion $f_{\overline{A}}(x)$ arvon, kun funktion f_A arvo tiedetään.
Eo. taulukoita vastaavat seuraavat laskennalliset kaavat, joiden avulla joukkojen unionin, leikkauksen ja komplementin karakteristisen funktoiden arvot voidaan laskea, kun ko. joukkojen karakteristisen funktioiden arvot tiedetään. Nämä laskukaavat ovat vastaavasti muotoa

$$f_A \vee f_B = \max(f_A, f_B) \tag{2.15}$$
$$f_A \wedge f_B = \min(f_a, f_B) \tag{2.16}$$
$$\neg f_A = 1 - f_A \tag{2.17}$$

Kaavojen (2.15), (2.16) ja (2.17) mukaisia ilmauksia tarkastelemme vielä runsaasti tuonnempana. Kun vertaamme näitä kaavoja edellä olleisiin vastaaviin taulukoihin, havaitsemme, että ne ovat täysin yhteensopivat. Kaavojen (2.15), (2.16) ja (2.17) esittämät operaatiot muodostavatkin ensimmäisen ja vielä paljon käytetyn yleistyksen loogisille operaatioille '$\vee$', '$\wedge$' ja '$\neg$', jotka edellä esitetyllä tavalla sidottuna arvojoukkoon $\{0, 1\}$ esittävät klassisen logiikan operaatioita. Näitä operaatioita kutsutaan *konnektiiveiksi*, koska ne yhdistävät toisiinsa yksittäisiä ilmaisuja, jotka tässä ovat karakteristisia funktioita. Edellä olemmekin saaneet muodostettua muotoa '$x \in A$' ja '$x \notin A$' olevia väitteitä koskevan klassisen propositiologiikan. Kun laajennamme arvojoukkoa siten, että siihen kuuluu lukujen 0 ja 1 lisäksi lukuja esim. mainittujen lukujen väliltä, olemme karakteristisen funktioidemme kanssa jossakin ei-klassisessa logiikassa, joka tällöin on jokin moniarvologiikka. Jos määrittelemme konnektiivit kaavojen (2.15), (2.16) ja (2.17) mukaisesti, saamme jonkin Lukasiewiczin moniarvologiikan riippuen mm. siitä, miten arvo-joukkoon valitaan lukuja 0:n ja 1:n väliltä ja mitä muita ominaisuuksia moniarvoisella systeemillämme on.
Pitäydymme kuitenkin vielä klassisissa joukoissa ja karakteristisissa funktioissa. $\mathcal{P}(\mathbf{X})$ yhdessä perusoperaatioiden unioni, leikkaus ja komplementti muodostaa erään algebrallisen struk-

tuurin, jota merkitsemme symbolijonolla

$$\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{-}, \emptyset, \mathbf{X} \rangle.$$

Tämä struktuuri on jo edeltä tuttu Boolen algebra. Vastaava algebrallinen struktuuri karakteristisen funktioiden joukolle $Ch(\mathbf{X})$ on $\langle Ch(\mathbf{X}), \vee, \wedge, \neg, 0, 1 \rangle$. Koska on tunnettua, että (2.7):ssä määritelty kuvaus φ toteuttaa ehdot

(i) $\varphi(A \cup B) = \varphi(A) \vee \varphi(B)$

(ii) $\varphi(A \cap B) = \varphi(A) \wedge \varphi(B)$

(iii) $\varphi(\overline{A}) = \neg\varphi(A)$

(iv) $\varphi(\emptyset) = 0, \;\; \varphi(X) = 1$

ovat $\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{-}, \emptyset, \mathbf{X} \rangle$ ja $Ch(\mathbf{X})$ on $\langle Ch(\mathbf{X}), \vee, \wedge, \neg, 0, 1 \rangle$ isomorfiset, mikä seikka algebrallisesti perustelee, että tavallinen joukko voidaan esittää karakteristisella funktiolla.
Yleisesti ottaen Boolen algebra määritellään seuraavasti: Olkoot $\wedge$ (kohtaus) ja $\vee$ (yhdiste) sellaisia binäärisiä operaatioita ja $'$ (komplementti) sellainen yksipaikkainen operaatio joukossa $B(\neq \emptyset)$ ja olkoot alkiot $\mathbf{0}$ ja $\mathbf{1}$ joukon B sellaisia alkioita, että seuraavat aksioomat ovat voimassa:

(BA1) $\wedge$ ja $\vee$ ovat kommutatiivisia, ts. kaikille alkioille $x, y \in B$ on voimassa

$$x \vee y = y \vee x \text{ ja } x \wedge y = y \wedge x.$$

(BA2) Jokaiselle alkiolla $x \in B$ on voimassa $x \vee \mathbf{0} = x$ ja $x \wedge \mathbf{1} = x$ eli $\mathbf{0}$ ja $\mathbf{1}$ ovat vastaavasti identiteettialkioita operaatioiden $\vee$ ja $\wedge$ suhteen.

(BA3) Operaatiot $\wedge$ ja $\vee$ ovat distributiivisia, ts. kaikille alkioille $x, y, z \in B$ on voimassa

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \;\; x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

(BA4) Jokaista alkiota $x \in B$ kohti on olemassa sellainen alkio $x' \in B$, että

$$x \vee x' = \mathbf{1} \text{ ja } x \wedge x' = \mathbf{0}.$$

(BA5) B:n alkioille $\mathbf{0}$ ja $\mathbf{1}$ pätee $\mathbf{0} \neq \mathbf{1}$.

Tällöin joukko B yhdessä mainittujen operaatioiden kanssa muodostaa Boolen algebran

$$\mathcal{B} = \langle B, \wedge, \vee, ', \mathbf{0}, \mathbf{1} \rangle. \tag{2.18}$$

On helppoa todeta tämän määritelmän perusteella, että

$$\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{-}, \emptyset, \mathbf{X} \rangle$$

ja

$$\langle Ch(\mathbf{X}), \vee, \wedge, \neg, 0, 1 \rangle$$

ovat todella Boolen algebroja.

Emme syvenny sen tarkemmin nyt Boolen algebroihin, mutta tämä olkoon linkkinä logiikan algebralliselle tarkastelutavalle. Tässä kappaleessa esitetyt asiat muutenkin antavat lähtökohdan laajempaan matemaattiseen tarkasteluun, johon tässä luvussa ei kuitenkaan vielä mennä.

2.9 Joukko-opin laajennuksesta

Laajennamme karakteristisen funktioiden joukkoa $Ch(\mathbf{X})$ siten, että lisäämme näiden funktioiden kuvajoukkoon $\{0,1\}$ lukujen 0 ja 1 välillä olevia reaalilukuja sopivasti. Kutsumme näin saatavia funktioita *yleistetyiksi karakteristisiksi funktioiksi* eli *jäsenyysfunktioiksi*. Kun jäsenyysfunktioiden arvojoukoksi valitaan suljettu yksikköväli $[0,1]$, meillä on jäsenyysfunktioiden joukko

$$\mathcal{F}(\mathbf{X}) = \{\, \mu \mid \mu : \mathbf{X} \longrightarrow [0,1] \,\}. \tag{2.19}$$

Miten on tulkittavissa esimerkiksi sellainen tapaus, että $\mathbf{X}$:n osajoukon A kohdalla eräs alkio $x_0 \in \mathbf{X}$ suhtautuu A:han seuraavasti:

$$\mu_A(x_0) = 0,7\,?$$

Luonnollinen tulkinta on se, että x_0 kuuluu joukkoon A jäsenyysasteella 0,7. A ei ole siis tavallinen ns. 'terävä' joukko. Se ei ole ns. 'hyvinmääritelty' siinä mielessä, että perusjoukon $\mathbf{X}$ jokaisesta alkiosta voidaan yksiselitteisesti todeta, että alkio joko kuuluu tai ei kuulu joukkoon A. Esimerkkinä lällaisesta tapauksesta voidaan mainita vaikkapa $\mathbf{X}$ = *ihmisten joukko,* jolla on osajoukkona A = *kookkaiden ihmisten joukko*. Tällöin mm. tietty henkilö x_0 saattaa hyvinkin kuulua kookkaiden ihmisten joukkoon jäsenyysasteella 0,7. Siis terävää rajaa ei kookkaiden ihmisten joukolle voida määrittää. Reaalimaailmassa tämän kaltaisia ilmiöitä on lukemattomia. Jos perusjoukkoon $\mathbf{X}$ sisältyy tällaisia ei-hyvinmääriteltyjä osajoukkoja, voimme merkitä intuitiivisessa mallissa $\mathbf{X}$:n potenssijoukkoa vaikkapa ilmaisulla $\mathcal{FP}(\mathbf{X})$. Otamme nyt ns. *metaaksioomaksi* joukkojen $\mathcal{FP}(\mathbf{X})$. ja $\mathcal{F}(\mathbf{X})$ välisen isomorfian

$$\mathcal{FP}(\mathbf{X}) \cong \mathcal{F}(\mathbf{X}). \tag{2.20}$$

Tätä ei luonnollisestikaan voida todistaa, niinkuin $\mathcal{P}(\mathbf{X})$:n ja $Ch(\mathbf{X})$:n välinen isomorfia tavallisten joukkojen kohdalla voidaan tehdä. Tämä johtuu siitä, että intuitio ei riitä sellaisen riittävän helpon intuitiivisen mallin $\mathcal{FP}(\mathbf{X})$:n muodostamiseen, jossa joukkoja A voitaisiin käsitellä ja niillä operoida vastaavalla tavalla kuin intuitiivisessa klassisessa joukko-opissa voidaan tehdä. Siis laajentaessamme klassista joukko-oppia meidän on jo heti aluksi hylättävä intuitiivinen malli ja käytettävä jäsenyysfunktioille rakentuvaa mallia.
Annamme edellä esitettyyn tarkasteluun ja isomorfiaan (2.20) perustuen *sumean joukon* määritelmän.

Määritelmä 2.9.1. *Ei-tyhjän joukon* $\mathbf{X}$ $sumeaa\ osajoukkoa\ A$ *esittää jäsenyysfunktio*

$$\mu : \mathbf{X} \longrightarrow [0,1].$$

Sumean (osa)joukon A jäsenyysfunktiota $\mu_A(x)$ merkitään usein suoraan A:ta käyttämällä muodossa $A(x)$. Jäsenyysfunktioiden joukko $\mathcal{F}(\mathbf{X})$ on ääretön.
Määrittelemme seuraavaksi $\mathcal{F}(\mathbf{X})$:ssä määritellyt operaatiot.

Määritelmä 2.9.2. $\mathcal{F}(\mathbf{X})$*:ssä määritellään perusoperaatiot* unioni, leikkaus *ja* komplementti *vastaavasti ehdoilla*

$$(\mu \vee \nu)(x) = \max(\mu(x), \nu(x)); \tag{2.21}$$

$$(\mu \wedge \nu)(x) = \min(\mu(x), \nu(x)); \tag{2.22}$$

$$\overline{\mu}(x) = 1 - \mu(x). \tag{2.23}$$

Nämä määrittelyt vastaavat tarkalleen ko. operaatioiden määrittelyjä karakteristisen funktioiden joukossa. Tässäkin mielessä jäsenyysfunktiot ovat karakteristisen funktioiden laajennus. Operaatiot $\max$ ja $\min$ eivät ole ainoat operaatiot, jotka esittävät sumeiden joukkojen unionia ja leikkausta. Niitä on paljon muitakin (ns. *s-normit* ja *t-normit*). Niitä emme tässä käsittele.

Määritelmä 2.9.3. $\mathbf{X}$*:n sumeat joukot* A *ja* B *ovat* identtiset *tarkalleen silloin, kun*

$$A = B \iff \forall\, x \in \mathbf{X},\ A(x) = B(x). \tag{2.24}$$

Sumea joukko A sisältyy *sumeaan joukkoon* B *tarkalleen silloin, kun*

$$\forall\, x \in \mathbf{X},\ A(x) \leq B(x). \tag{2.25}$$

Merkitään seuraavassa $[0,1] = I$. I:n algebralliset omianisuudet siirtyvät myös jäsenyysfunktioiden joukkoon $\mathcal{F}(\mathbf{X})$. Korostettaessa tätä seikkaa jäenyysfunktioiden joukkoa merkitään usein myös $I^{\mathbf{X}}$:llä. Oikeastaan tämä joukko on tulojoukko $\prod_{x\in\mathbf{X}} I_x$, missä I_x on I indeksoituna $\mathbf{X}$:n yli.
Kokoamalla yhteen edellä esitetyt seikat jäsenyysfunktioista voimme muodostaa erään sumeiden joukkojen algebran. Se koostuu itse asiassa prof. Lotfi A. Zadehin (ks. [19]) vuonna 1965 esittämästä ensimmäisestä sumeiden joukkojen teoriasta. Hän ei tosin esittänyt sitä algebran muodossa, vaan algebralisointi on tehty jälkikäteen muiden toimesta. Täten kuitenkin nimitämme ko. algebraa *Zadeh-algebraksi*.

Määritelmä 2.9.4. (Zadeh-algebra). *Olkoon* $\mathbf{X}$ *ei-tyhjä joukko. Olkoot* $\wedge$ *ja* $\vee$ *sellaisia binäärisiä operaatioita ja* $\mu = \mathbf{1} - \mu$ *sellainen yksipaikkainen operaatio joukossa* $I^{\mathbf{X}}$*, että seuraavat aksioomat ovat voimassa:*

(QBA1) *operaatiot* $\wedge$ *ja* $\vee$ *ovat kommutatiivisia joukossa* $I^{\mathbf{X}}$*;*

(QBA2) *kaikille* $\mu \in I^{\mathbf{X}}, \mu \vee \mathbf{0} = \mu$ *and* $\mu \wedge \mathbf{1} = \mu$*;*

(QBA3) *operaatiot* $\wedge$ *ja* $\vee$ *ovat distributiivisia joukossa* $I^{\mathbf{X}}$*;*

(QBA4) *jokaista funktiota* $\mu \in I^{\mathbf{X}}$ *kohti on olemassa sellainen* $\mu' \in I^{\mathbf{X}}$*, että* $\mu' = \mathbf{1} - \mu$*;*

(QBA5) $\mathbf{0} \neq \mathbf{1}$.

Silloin $\langle I^{\mathbf{X}}, \wedge, \vee, \mathbf{1} - \mu, \mathbf{0}, \mathbf{1}\rangle$ *on* Zadeh-algebra.

0 ja **1** ovat vakiofunktioita $I^{\mathbf{X}}$:ssä saaden vastaavasti arvot 0 ja 1 kaikilla $x \in \mathbf{X}$.
Tällä algebralla on tutunomaisia piirteitä, kun vertaamme sitä Boolen algebraan. Se ei kuitenkaan ole varsinainen Boolen algebra, koska siinä ei ole varsinaista komplementtia, joka toteuttaa edellä esitetyt komplementin ehdot (C4), vaan ns. *kvasi-Boolen algebra*. Sitä kutsutaan myös *Morgan-algebraksi* tai *pehmeäksi algebraksi*. Ehto (QBA4) määrittelee erään *pseudokomplementin*. Pseudokomplementti ei toteuta yleisesti ehtoja (C4), mikä on helposti havaittavissa, kun tarkastellaan unionia ja leikkausta: $(A \vee \overline{A})(x) = \max(A(x), 1 - A(x))$ ja $(A \wedge \overline{A})(x) = \min(A(x), 1 - A(x))$. Jos nyt vaikkapa $A(x_0) = 0,6$, ei A:n ja $\overline{A}$:n unioni ole = 1 eikä leikkaus ole = 0 kohdassa x_0.

Esimerkki 2.9.5. *Tarkastellaan autojen joukon* $\mathbf{X}$ *osajoukkoa* A *= 'kalliden autojen joukko'. Otetaan käsittelyyn muutama automerkki: BMW, Buick, Ferrari, Fiat, Opel, Lada, Mersedes ja Rolls Royce. Jotkin näistä autoista, kuten ainakin Ferrari ja Rolls Royce, varmasti kuuluvat* A*:han, kun taas Lada tai Fiat eivät kuulu* A*:han. Sitten on kolmas ryhmä autoja, joista on vaikeampaa sanoa, kuuluvatko ne* A*:han vai eivät. Lisäksi eri ihmisillä on erilainen käsitys siitä, minkä hintainen auto on kallis. Jonkun mielestä em. autojen kuuluminen* A*:han voi olla seuraavanlainen:*

$$\begin{array}{rclrclrcl} A(\text{Ferrari}) & = & 1, & A(\text{Rolls Royce}) & = & 1, & A(\text{Mersedes}) & = & 0{,}8, \\ A(\text{BMW}) & = & 0{,}75, & A(\text{Buick}) & = & 0{,}7, & A(\text{Opel}) & = & 0{,}6, \\ A(\text{Fiat}) & = & 0, & A(\text{lada}) & = & 0. & & & \end{array}$$

Esimerkki 2.9.6. *Olkoon joukon* $\mathbb{R}$ *osajoukko* A *= 'likimain 6'. Se voidaan esittää vaikkapa seuraavalla jäsenyysfunktiolla:*

$$\begin{cases} 1 - \sqrt{\frac{|x-6|}{3}}, & \text{kun } 3 \leq x \leq 9, \\ 0 & \text{muulloin}. \end{cases}$$

Toisaalta joku saattaa olla sitä mieltä, että funktio

$$A(x) = \frac{1}{1 + (x-6)^2}$$

esittää paremmin A*:ta.*

3 RELAATIOT

3.1 Relaation määritelmä ja esitystapoja

Määrittelemme *järjestetyn parin* (x, y) siten, että jos $(x, y) = (u, v)$, niin $x = u$ ja $y = v$. Siis järjestetyn parin alkiot ovat määrätyssä järjestyksessä. Jos siis järjestetyn parin alkiot vaihtavat paikkaa keskenään, ei järjestetty pari ole enää sama kuin alkuperäinen pari.
Järjestetty kolmikko on järjestetty pari, jonka jompikumpi jäsen tilanteesta riippuen on järjestetty pari, ts. $(a, b, c) = ((a, b), c) = (a, (b, c))$.
Järjestetty n-jono voidaan määritellä vastaavalla tavalla järjestetyn parin laajennuksena

$$(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n). \tag{3.1}$$

Joukkojen A ja B karteesinen tulo $A \times B$ on kaikkien järjestettyjen parien joukko

$$A \times B = \{(a, b) \,|\, a \in A \text{ ja } b \in B\}. \tag{3.2}$$

Tämä voidaan laajentaa koskemaan yleisesti n:n joukon karteesista tuloa seuraavasti:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in A_i, i = 1, 2, \ldots, n\}. \tag{3.3}$$

Relaatio on joukko, johon liittyy tietty tulkinnallinen ominaisuus ominaisuuksien ja suhteiden universumissa. Joukko-oppi tarjoaa relaatioteorialle matemaattisen mallin, jota sovelletaan tutkittaessa ominaisuuksia ja suhteita. Relaatioita esiintyy kaikkialla. Niitä tapaamme yhteiskunnan, yhteisöjen, ryhmien jne. parissa. Esim. viinipullon oleminen pöydällä on viinipullon ja pöydän välinen relaatio, ja viinin kaataminen lasiin on pullon, viinin, lasin ja kaatajan välinen relaatio (viinipulloista yleensä: vrt. Kantin oppi oliosta sinänsä, ”das Ding an sich”, josta tieteenfilosofian uuskonkretisoijat ovat saaneet enemmän tai vähemmän loogisen johdannaisen ”das Ding am Tisch”.) Mm. sukulaisuussuhteet ovat hyviä esimerkkejä relaatioista.
Seuraavassa esitetään relaatioiden tavallisimpia merkintätapoja. Relaatioita merkitään, kuten joukkoja yleensäkin, isoilla kirjaimilla. Relaatiot ovat ns. n-paikkaisia, $n = 0, 1, 2, \ldots$. Nollapaikkainen relaatio kiinnittää vakion, ja sitä merkitään yleensä ko. vakion arvolla. Muita merkintätapoja relaatiolle R ovat mm. seuraavat:

yksipaikkaisia:	$Rx, R(x), x \in R, \ldots$
kaksipaikkaisia:	$xRy, Rxy, R(x, y), (y, x) \in R, \ldots$
kolmipaikkaisia:	$Rxyz, R(x, y, z), (x, y, z) \in R, \ldots$
$\vdots$	
n-paikkaisia:	$Rx_1x_2 \ldots x_n, R(x_1, x_2, \ldots, x_n), (x_1, x_2, \ldots, x_n) \in R$

Määrittelemme nyt n-paikkaisen relaation täsmällisesti tapauksissa $n \in \mathbb{N}$:

Määritelmä 3.1.1. *n-paikkainen relaatio $(n = 1, 2, \ldots)R$ joukossa S on joukon S^n osajoukko, ts. sellaisten järjestettyjen n-jonojen joukko, jotka koostuvat S:n alkioista.*

Tämän määritelmän mukaan yksipaikkainen relaatio R joukossa S on tietty S:n osajoukko. Yksipaikkainen relaatio nimeää usein jonkin ominaisuuden. Kaksipaikkainen eli binäärinen relaatio R joukossa S on määritelmän 3.1.1 mukaan järjestettyjen parien (a, b), $a, b \in S$, joukko, joka on joukon $S \times S$ osajoukko. Tällöin voidaan merkitä

$$R = \{(a, b) \mid a, b \in S, a \text{ ja } b \text{ liittyvät toisiinsa } R\text{:n ilmaisemalla tavalla}\} \tag{3.4}$$

Esimerkki 3.1.2. *Relaatio P = 'olla pienempi kuin' merkitään täsmällisesti seuraavalla tavalla:*

$$P = \{(a, b) \mid a, b \in S, a \textit{ on pienempi kuin } b\}$$

Kun nyt halutaan esim. ilmoittaa, että $_z$ on pienempi kuin z, voidaan tämä tehdä merkitsemällä $(_z, z) \in P$, tai $_zPz$, tai $P(_z, z$, tai P_zz, jolloin $_z$ ja z ovat koirien joukon S alkioita, missä joukossa P on määritelty. Yleensä lukujen keskinäisessä vertailussa käytetään tästä relaatiosta merkintää '$<$'. Esimerkiksi, kun $S = \mathbb{R}$, on

$$<= \{(a, b) \mid a, b \in \mathbb{R}, a \textit{ on pienempi kuin } b\}.$$

Tällöin yleensä merkitään $a < b$.

Esimerkki 3.1.3. *Tarkastellaan relaatiota xRy = 'x on y:n tekijä' joukossa $S = \{2, 3, 5, 6\}$. Tällöin $2R2, 2R6, 3R3, 3R6, 5R5$ ja $6R6$, jolloin relaatio R on joukko*

$$R = \{(2, 2), (2, 6), (3, 3), (3, 6), (5, 5), (6, 6)\}.$$

R on siis joukon $S \times S$ osajoukko.

Suoritamme tässä erilaisia tarkasteluja pääasiassa kaksipaikkaisille relaatioille, jolloin tietyt tarkastelut voidaan helposti laajentaa koskemaan myös useampipaikkaisia. Yksipaikkaisilla relaatioilla on täsmälleen samat ominaisuudet kuin tavallisilla joukoilla, ja *nollapaikkaisen* relaation tärkein ominaisuus on vakion arvon kiinnittäminen. Määrittelemme seuraavassa joitakin käsitteitä binäärisille eli kaksipaikkaisille relaatioille.

Määritelmä 3.1.4. *Olkoon S jokin ei-tyhjä joukko, A ja B sen osajoukkoja sekä $a \in A$ ja $b \in B$. Relaatiossa $R = \{(a, b) \mid a \in A, b \in B\}$ joukko A on relaation R* etualue *ja joukko B* takaalue. *A:n alkioita sanotaan R:n* etujäseniksi *ja B:n alkioita* takajäseniksi. *Tällöin relaation suunta on A:sta B:hen.*

Määritelmä 3.1.5. *Relaation R* käänteisrelaatio *R^{-1} joukossa S on sellainen, että se toteuttaa ehdon*

$$xRy \Rightarrow yR^{-1}x \tag{3.5}$$

Määritelmän 3.1.5 mukaan, kun relaatio R vallitsee S:n alkioiden x ja y välillä, vallitsee sen käänteisrelaatio R^{-1} y:n ja x:n välillä. Siis käänteisrelaatio vallitsee samojen alkioiden välillä kuin alkuperäinen relaatio, mutta sen *suunta* on vastakkainen.

Esimerkki 3.1.6. *(a) Olkoon xRy = 'x on y:n jälkeen'. Tällöin $yR^{-1}x$ = 'y on ennen x:ää'. (b) Olkoon aKb = 'a on oikealle b:stä'. Silloin $bK^{-1}a$ = 'b on vasemmalle a:sta'.*

Määritelmä 3.1.7. *(a) Relaation* R komplementti $\overline{R}$ *joukossa* S *määritellään ehdolla*

$$x\overline{R}y \Leftrightarrow xRy \textit{ ei päde}. \tag{3.6}$$

(b) Olkoot A *ja* B *relaatioita joukossa* S*. A:n ja B:n* tulo $A \cdot B$ *(voidaan myös merkitä* AB *tai* $A \cap B$*) joukossa* S *on relaatioiden* A *ja* B *leikkaus*

$$A \cdot B = \{(x, y) \mid xAy \textit{ ja } xBy\}. \tag{3.7}$$

(c) Olkoot A *ja* B *relaatioita joukossa* S*. A:n ja B:n* summa $A + B$ *(voidaan myös merkitä* $A \cup B$*) joukossa* S *on relaatioiden* A *ja* B *unioni*

$$A + B = \{(x, y) \mid xAy \textit{ tai } xBy\}. \tag{3.8}$$

Huom. Relaatioiden tulo ja summa ovat vastaavasti joukko-opillinen leikkaus ja unioni. Määritelmässä käytetyt nimitykset tarkoittavat tarkalleen ottaen ns. loogista tuloa ja loogista summaa.

Määritelmä 3.1.8. *Olkoot* A *ja* B *relaatioita joukossa* S*.*
(a) Jos ehto $xAy \Rightarrow xBy$ *on voimassa* S*:ssä, sanomme, että* A sisältyy B:hen *ja kirjoitamme* $A \subset B$*.*
(b) Jos $A \subset B$ *ja* $B \subset A$*, sanomme, että* A *ja* B *ovat identtiset, jolloin merkitsemme* $A = B$*.*

Määritelmä 3.1.9. *(a)* Universaalirelaatio $\mathbb{V}$ *joukossa* S *on relaatio*

$$\begin{aligned} \mathbb{V} \;=\; & \{(x, y) \in S \times S \mid \textit{kaikille } x, y \in S \textit{ pätee,} \\ & \textit{että on olemassa sellainen } R\textit{, että } xRy\}\,. \end{aligned} \tag{3.9}$$

(b) Tyhjä relaatio Λ *joukossa* S *on relaatio*

$$\begin{aligned} \Lambda \;=\; & \{(x, y) \in S \times S \mid \textit{kaikille } x, y \in S \textit{ pätee,} \\ & \textit{ettei ole olemassa sellaista } R\textit{:ää, että } xRy\}\,. \end{aligned} \tag{3.10}$$

Määritelmän 3.1.9 mukaan universaalirelaatio joukossa S vallitsee kaikkien S:n alkioiden välillä, ts. se muodostuu kaikista mahdollisista S:n alkioiden järjestetyistä pareista, siis $\mathbb{V} = S \times S$, kun taas tyhjä relaatio S:ssä ei vallitse yhdenkään S:n alkioparin välillä, eli $\Lambda = \emptyset$. Ilmeisesti $\Lambda = \overline{\mathbb{V}}$ ja $\mathbb{V} = \overline{\Lambda}$.

Määritelmä 3.1.10. *Olkoot* A *ja* B *relaatioita joukossa* S*. Relaatioiden* A *ja* B suhteellinen tulo $A|B$ *vallitsee* S*:n alkioiden* x *ja* y *välillä, jos ja vain jos on olemassa sellainen* S*:n alkio* z*, että ehto* xAz *ja* zBy *on voimassa.*

Esimerkki 3.1.11. *Relaatio '*x *on* y*:n setä' ihmisten joukossa on relaatioiden 'veli' ja 'isä' suhteellinen tulo, sillä* x *on* y*:n setä, jos ja vain jos on (tai on ollut) olemassa sellainen henkilö* z*, että* x *on* z*:n veli ja* z *on* y*:n isä.*

Määritelmä 3.1.12. *Relaation* R potensseja *ovat seuraavat ilmaisut:*

(i) $R^1 = R$

(ii) $R^2 = R|R$

(iii) $R^3 = (R|R)|R$.

Esimerkki 3.1.13. *Relaatio 'isoisä' on relaation 'isä' toinen potenssi, 'isoisänisä' kolmas potenssi jne.*

Määritelmä 3.1.14. *Sanomme, että R-ketju vallitsee x:n ja y:n välillä, jos niiden välillä vallitsee jokin R:n potenssi.*

Esimerkki 3.1.15. *Relaatio 'isänpuoleinen esi-isä' on yleisessä muodossa esitetty R-ketju, kun $R =$ 'isä'.*

3.2 Binääristen relaatioiden ominaisuuksia

Olkoon R binäärinen relaatio joukossa S. R:llä on seuraavia ominaisuuksia:

(1) R on *refleksiivinen* joukossa S, jos ja vain jos kaikille $x \in S$ pätee xRx.

(2) R on *irrefleksiivinen* joukossa S, jos ja vain jos jokaiselle $x \in S$ pätee $x\overline{R}x$.

(3) R on *non-refleksiivinen* joukossa S, jos ja vain jos on olemassa sellaisia alkioita $x \in S$, että xRx, ja on olemassa sellaisia alkioita $y \in S$, että $y\overline{R}y$. Tällöin S:llä on sellainen osajoukko, jossa R on refleksiivinen, sekä sellainen osajoukko, jossa R on irrefleksiivinen.

(4) R on *symmetrinen* joukossa S, jos ja vain jos jokaiselle alkioparille $x, y \in S$ pätee $xRy \Rightarrow yRx$.

(5) R on *asymmetrinen* joukossa S, jos ja vain jos jokaiselle alkioparille $x, y \in S$ pätee $xRy \Rightarrow y\overline{R}x$.

(6) R on *non-symmetrinen* joukossa S, jos ja vain jos on olemassa sellaisia alkiopareja $x, y \in S$, että sekä xRy että yRx, ja on olemassa sellaisia alkiopareja $r, s \in S$, että rRs mutta ei sRr.

(7) R on *antisymmetrinen* joukossa S, jos ja vain jos kaikille alkiopareille $x, y \in S$ pätee xRy ja $yRx \Rightarrow x = y$.

(8) R on *transitiivinen* joukossa S, jos ja vain jos kaikille $x, y, z \in S$ pätee ehto xRy ja $yRz \Rightarrow xRz$.

(9) R on *intransitiivinen* joukossa S, jos ja vain jos kaikille $x, y, z \in S$ pätee ehto xRy ja $yRz \Rightarrow$ ei ole niin, että xRz.

(10) R on *non-transitiivinen* joukossa S, jos ja vain jos on olemassa sellaiset alkiot $x, y, z \in S$, että xRy, yRz, xRz sekä on olemassa sellaiset alkiot $s, r, t \in S$, että rRs ja sRt mutta ei rRt.

(11) R on *yhtenäinen* joukossa S, jos ja vain jos jokaiselle alkioparille $x, y \in S, x \neq y$, pätee ehto xRy tai yRx.

(12) R on *vahvasti yhtenäinen*, jos ja vain jos kaikille alkioille $x, y \in S$ pätee ehto xRy tai yRx.

Esimerkkejä binääristen relaatioiden ominaisuuksista

(1) $xRy = x \geq y$ kokonaislukujen joukossa $\mathbb{Z}$. Koska $x \geq x$ kaikilla alkioilla $x \in \mathbb{Z}$, on R refleksiivinen $\mathbb{Z}$:ssa.

(2) $xRy =$ 'x on y:n äiti', S on ihmisten joukko. Koska kenen tahansa ihmisen kohdalla pätee, ettei hän ole itsensä äiti, on R irrefleksiivinen S:ssä.

(3) $xRy =$ 'x on y:n neliö' reaalilukujen joukossa $\mathbb{R}$. Esim. $1 = 1^2$, mutta $2 \neq 2^2$. Siis R on non-refleksiivinen $\mathbb{R}$:ssä.

(4) $xPy =$ 'x on y:n puoliso', S on yksiavioisten avioliitossa elävien ihmisten joukko. Tällöin, kun x ja y ovat mitä tahansa S:n alkioita, $xPy \Rightarrow yPx$ on voimassa. Siis P on symmetrinen S:ssä.

(5) $x\ddot{A}y =$ 'x on y:n äiti', S on ihmisten joukko. Tällöin, kun x ja y ovat ketä tahansa ihmisiä, pätee, että jos $x\ddot{A}y$, niin $y\ddot{A}x$ ei ole voimassa. Siis $\ddot{A}$ on asymmetrinen S:ssä.

(6) $xVy =$ 'x on y:n veli', S on ihmisten joukko. Tällöin, kun x ja y ovat sellaisia ihmisiä, että xVy on voimassa, joillekin alkiopareille x ja y pätee myös, että yVx, mutta ei kaikille. Siis V on non-symmetrinen S:ssä.

(7) $xRy = x \leq y$ joukossa $\mathbb{Z}$. Jos $x \leq y$ ja $y \leq x$, niin välttämättä $x = y$, mikä pätee yleisesti $\mathbb{Z}$:ssa. Siis R on $\mathbb{Z}$:ssa antisymmetrinen.

(8) $xEy =$ 'x on y:n esimies', S on sotilaiden joukko. Jos x, y ja z ovat keitä tahansa sellaisia henkilöitä, että xEy ja yEz, niin myös xEz. Siis E on transitiivinen S:ssä.

(9) $xTy =$ 'x on y:n tytär', S on ihmisten joukko. Olkoot x, y ja z keitä tahansa sellaisia henkilöitä, että xTy ja yTz. Tällöin relaatio xTz ei ole voimassa. Siis T on intransitiivinen S:ssä.

(10) $xYy =$ 'x on y:n ystävä', S on ihmisten joukko. Tällöin, jos xYy ja yYz, niin voi olla myös xYz, mutta ei välttämättä. Siis Y on non-transitiivinen S:ssä.

(11) $xRy = x > y$ joukossa $\mathbb{Z}$. Tällöin, kun x ja y ovat mitä tahansa erisuuria kokonaislukuja, $\mathbb{Z}$:ssa vallitsee $x > y$ tai $y > x$. Siis R on yhtenäinen $\mathbb{Z}$:ssa.

(12) $xRy = x \leq y$ $\mathbb{R}$:ssä. Tällöin kaikille luvuille $x, y \in \mathbb{R}$ pätee xRy tai yRx. Siis R on vahvasti yhtenäinen $\mathbb{R}$:ssä.

3.3 Erityisiä relaatioita

Määritelmä 3.3.1. *Relaatio R on* ekvivalenssirelaatio *joukossa S, jos R on (i) refleksiivinen, (ii) symmetrinen ja (iii) transitiivinen.*

Esimerkki 3.3.2. *Relaatio '$=$' on ekvivalenssirelaatio $\mathbb{R}$:ssä.*

Esimerkki 3.3.3. *Tarkastelemme relaatiota xSy = 'x:llä on sama sukunimi kuin y:llä' sukunimellisten ihmisten joukossa. Määritelmän 3.3.1 kohta (i) on triviaali ko. relaation suhteen, eli refleksiivisyys pätee selvästi. Lukija toteaa helposti, että myös kohdat (ii) ja (iii) ovat voimassa S:lle. Siis S on ekvivalenssirelaatio.*

Esimerkki 3.3.4. *Tarkastelemme relaatiota $x\mathcal{O}y$ = 'x opiskelee samaa pääainetta kuin y' opiskelijoiden joukossa X. On helposti todettavissa, että $\mathcal{O}$ on ekvivalenssirelaatio X:ssä. Relaatio $\mathcal{O}$ jakaa joukon X ns.* ekvivalenssiluokkiin *seuraavasti:*

$$\begin{aligned} A_1 &= \textit{kansantaloustiedettä pääaineenaan opiskelevat} \\ A_1 &= \textit{markkinointia pääaineenaan opiskelevat} \\ &\vdots \end{aligned}$$

Joukoilla A_i on mm. seuraavia ominaisuuksia: $A_i \subset X, i = 1, 2, \ldots; A_i \cap A_j = \emptyset$, kun $i \neq j, i, j = 1, 2, \ldots; A_1 \cup A_2 \cup \ldots = X$. Olkoon opiskelijan a pääaine talousmatematiikka. Tällöin relaatio $s\mathcal{O}a$ ilmaisee sen, että x opiskelee samaa pääainetta kuin a. Kaikkien opiskelijoiden joukko, jotka opiskelevat samaa pääainetta kuin a, voidaan ilmaista joukkona

$$A_k = \{x \mid x \in X \textit{ ja } x\mathcal{O}a\} \tag{3.11}$$

Joukko A_k on a:n määräämä $\mathcal{O}$-ekvivalenssiluokka.

Määrittelemme yleisesti ekvivalenssiluokan:

Määritelmä 3.3.5. *Jos R on ekvivalenssirelaatio joukossa S, niin S:n alkion a määräämä R-*ekvivalenssiluokka *on niiden S:n alkioiden joukko, jotka ovat relaatiossa R a:n kanssa, ts.*

$$[a]_R = \{x \mid x \in S \textit{ ja } xRa\}. \tag{3.12}$$

Esimerkki 3.3.6. *Olkoot xSy = 'x on saman värinen kuin y' kukkien joukossa K ja a = sinivuokko. Tällöin sinivuokon määräämä S-ekvivalenssiluokka on niiden kukkien joukko, jotka ovat sinivuokon värisiä, eli*

$$[a]_S = \{x \mid x \in K \textit{ ja } xSa\}.$$

Luokittelu perustuu yleisesti ekvivalenssirelaatiolle.

Järjestysrelaatiot määrittelevät tietyn järjestyksen joukossa.

Määritelmä 3.3.7. *(a) Relaatio R on* kvasijärjestys *joukossa S, jos ja vain jos R on S:ssä (i) refleksiivinen ja (ii) transitiivinen.*
(b) Relaatio R on joukossa S on (aito osittainen järjestys, *jos ja vain jos R on (i) refleksiivinen, (ii) antisymmetrinen ja (iii) transitiivinen S:ssä.*
(c) Relaatio R on (aito) kokonaisjärjestys *joukossa S, jos ja vain jos R on osittainen järjestys S:ssä ja yhtenäinen S:ssä.*

Esimerkki 3.3.8. *(a) '$\subset$' ei-tyhjän joukon S osajoukkojen joukossa $\mathcal{P}(S)$ on sekä kvasijärjestys että osittainen järjestys $\mathcal{P}(S)$:ssä.*
(b) '$<$' on kokonaisjärjestys $\mathbb{R}$:ssä.

Määritelmä 3.3.9. Funktio *eli* kuvaus *f joukosta A joukkoon B on keino liittää kuhunkin A:n alkioon jokin B:n alkio. Tämä voidaan sanoa täsmällisemmin esim. seuraavilla tavoilla:*
(i) f on sellaisten järjestettyjen parien joukko, että jos $(x, y) \in f$ ja $(x, z) \in f$, niin $y = z$;
tai
(ii) jokaista A:n alkiota x kohti on olemassa jokin sellainen B:n alkio y, että $(x, y) \in f$. Tällöin merkitään $y = f(x)$.

Koska funktiossa x:n vastineena oleva y määräytyy yksikäsitteisesti, on merkintä $y = f(x)$ perusteltu.

Määritelmä 3.3.10. *Alkiota y kutsutaan x:n* kuvaksi *eli* funktion arvoksi *pisteessä x. Alkiota x kutsutaan puolestaan y:n* alkukuvaksi *eli* argumentiksi.

Määritelmä 3.3.11. *Jos f on sellainen funktio A:sta B:hen, merk. $f : A \to B$, että B:n jokainen alkio on A:n jonkin alkion kuva, on f* surjektio *(eli funktio A:sta B:lle). Jos f liittää kuhunkin argumenttiin eri arvon, ts. $f(x) = f(y)$, jos ja vain jos $x = y$, on f* injektio *(eli* yksi yhteen, one-one*). Jos f on sekä surjektio että injektio, sanotaan f:ää* bijektioksi.

Esimerkki 3.3.12. *Olkoon $f : \mathbb{R} \to \mathbb{R}$ sellainen funktio, että $f(x) = x^2$. Tällöin f ei ole surjektio, koska kuvien joukko on $\mathbb{R}$:n aito osajoukko. Tämä f ei myöskään ole injektio, koska $f(-a) = a^2 = f(a)$, kun $a \in \mathbb{R}$. Jos f olisi funktio $f : \mathbb{R} \to \mathbb{R}_-$, olisi se injektio, koska identiteetistä $u^2 = v^2$ seuraa $u = v$, mikä on voimassa kaikille ei-negatiivisille reaaliluvuille u ja v. Lisäksi f olisi tällöin surjektio, koska kuvajoukko olisi sama kuin arvojoukko.*

4 KLASSISTA LOGIIKKAA

4.1 Looginen päättely

Päättelyn tuloksena syntyy *päätelmä* eli *argumentti*. Päätelmä koostuus siitä, että joistakin *oletuksista* eli *premisseistä* seuraa tietty *johtopäätös*. Siis päättely on johtopäätöksen muodostamista premisseistä tai sen osoittamista, että johtopäätös seuraa premisseistä. Päätelmä voi olla *oikea* eli (*loogisesti*) *pätevä* tai *epäpätevä*. Seuraava päättely näyttää pätevältä:

Oletukset eli premissit $\Longrightarrow$ Johtopäätös

Sokrates on ihminen.	oletus
Kaikki ihmiset ovat kuolevaisia.	oletus
Sokrates on kuolevainen.	johtopäätös

(4.1)

(4.1):ssä oletukset ovat tosia, samoin johtopäätös. Tällöin päätelmä on ilmeisesti oikea eli (loogisesti) pätevä.
Seuraava päätelmä ei ilmeisestikään ole pätevä.

Sokrates on ihminen.	oletus
Eräät ihmiset ovat kuolevaisia.	oletus
Sokrates ei ole kuolevainen.	johtopäätös

(4.2)

(4.2):ssa premissit ovat tosia, mutta johtopäätös on epätosi.
Välttämätön ehto päätelmän pätevyydelle:

Jos premissit ovat tosia, niin johtopäätös on tosi.

(4.3)

Tämä on tärkeä ominaisuus. Pätevä päättely ei sen mukaan johda 'totuuden ulkopuolelle', mikäli premissit ovat tosia. Sanomme, että pätevä päättely on *totuuden säilyttävä*.
Ehto (4.3) ei ole *riittävä ehto* pätevälle päättelylle, kuten seuraava esimerkki osoittaa.

Sokrates on ihminen.	oletus
Kaikki ihmiset ovat kuolevaisia.	oletus
Sokrates on filosofi.	johtopäätös

(4.4)

(4.4):ssä premissit ovat tosia ja johtopäätös on tosi, mutta päätelmä on silti epäpätevä. Ehto (4.3) onkin vaatimus, joka päätelmän täytyy vähintään toteuttaa, jotta se olisi pätevä.
Päättely saattaa olla pätevä myös seuraavissa tapauksissa.

Tosi premissi Epätosi premissi	$\Longrightarrow$	Epätosi johtopäätös

Epätodet premissit	$\Longrightarrow$	Tosi johtopäätös

Päätelmän pätevyydelle ei sinänsä ole merkitystä sillä, ovatko premissit tosia vai eivät, kuten seuraava esimerkki osoittaa

Sokrates on suomalainen.	oletus
Kaikki suomalaiset ovat kuolemattomia.	oletus
Sokrates on kuolematon.	johtopäätös

(4.5)

Sekä premissit että johtopäätös ovat epätosia (4.5):ssä.

Pekka on korppi.	oletus
Kaikki korpit ovat mustia.	oletus
Pekka on musta.	johtopäätös

(4.6)

Tarkastellaan päätelmiä (4.1), (4.5) ja (4.6). Niillä on selvästi sama *looginen muoto* eli sama *looginen rakenne*, joka voidaan alustavasti esittää seuraavasti:

a on A.	(a :lla on ominaisuus A)
Jokainen A on B.	(Kaikilla, joilla on ominaisuus A on ominaisuus B)
Siis: a on b.	(a :lla on ominaisuus B)

(4.7)

Syntaktinen kriteeri päätelmän pätevyydelle:

Päätelmän pätevyys ei niinkään riipu siinä esiintyvien lauseiden aktuaalisesta sisällöstä kuin niiden loogisesta muodosta.

(4.8)

Syntaktinen kriteeri (4.8) on yhteydessä semanttiseen kriteeriin (4.3). Tuonnempana tarkastellaan kysymystä, mitä loogisella muodolla tarkoitetaan ja miten päätelmän pätevyys riippuu siitä.
Edellä tarkastellun tapaisia päätelmiä kutsutaan *deduktioiksi*. Deduktiossa johtopäätös seuraa *välttämättä* premisseistä.
Päättely, jossa johtopäätös ei seuraa premisseistä välttämättä tai varmuudella, vaan esim. suurella todennäköisyydellä, on *induktiivinen* päätelmä.
Käytännöllisiä eli *jokapäiväisiä päättelyjä* ei useinkaan esitetä täydellisinä.

Kaikki ihmiset ovat kuolevaisia. Siis Sokrates on kuolevainen.

(4.9)

tai: ”Sokrates on ihmisenä kuolevainen.”

Pekka on korppi. Siis Pekka on musta.

(4.10)

tai: ”Pekka on musta, koska on korppi.”
Kysymys käytännöllisen päättelyn loogisesta pätevyydestä voi ratketa, jos löydetään puuttuvat premissit.

4.2 Mahdolliset maailmat

Olemme todenneet, ettei päätelmän pätevyys kovin suuressa määrin riipu premissien aktuaalisesta totuudesta tai epätotuudesta eikä siitä, mikä niiden aktuaalinen tulkinta on. Se riippuu näistä seikoista ainoastaan siinä määrin kuin ehto (1.3) sanoo. Kun tässä yhteydessä puhutaan premissien 'aktuaalisesta totuudesta', 'aktuaalisesta sisällöstä' tai lyhyesti vain 'totuudesta', tarkoitetaan sen totuutta tai tulkintaa suhteessa tähän maailmaan tai siihen tilanteeseen tai asiaintilaan, jossa asianomaisella hetkellä olemme tai jota jostain syystä tarkastelemme. Jos esimerkiksi ollessani työhuoneessani sanon:

Tämän huoneen ovi on kiinni; (4.11)

niin *aktuaalinen tilanne* tai *aktuaalinen maailma* muodostuu niistä seikoista, tapahtumista jne., jotka liittyvät asianomaiseen huoneeseen ja siihen seikkaan, että olen siinä huoneessa. Mitä kaikkea täsmällisemmin sanottuna siihen liittyy, on ainakin osittain sopimuksenvarainen asia. Mutta ymmärrämme kuitenkin, mitä aktuaalinen tilanne tai maailma tässä yhteydessä suurinpiirtein tarkoittaa. Kun ajattelemme aktuaalisen maailman tällä tavoin kiinnitetyksi, ymmärrämme myös sen, mitä tarkoitetaan lauseen (4.11) aktuaalisella totuudella tai epätotuudella, ts. sillä, että se on tosi tai epätosi, tai mikä on sen aktuaalinen tulkinta. Tällaisten lauseiden yhteydessä puhutaan usein siitä *kontekstista* eli *asiayhteydestä*, jossa lause sanotaan.
Samoin, jos tarkastelemme lausetta

Helsinki on Suomen pääkaupunki; (4.12)

huomaamme, että se on tosi, siis tosi tässä aktuaalisessa maailmassamme, joka ehkä voidaan intuitiivisesti ajatella 'laajemmaksi' tai 'suuremmaksi' maailmaksi kuin äskeinen. Mitään tarkkoja rajojoa maailman koolle kummassakaan tapauksessa ei tarvitse kuitenkaan asettaa, jotta ymmärtäisimme näiden lauseiden merkityksen ja näkisimme, ovatko ne tosia vai eivät. Niinpä voimme esimerkiksi todeta, että tiettyyn historialliseen tilanteeseen nähden (4.12) ei ole tosi.
Osoitamme nyt, että pätevää päätelmää voidaan luonnehtia siinä esiintyvien lauseiden *merkityksien* avulla, kun 'merkitys' määritellään sopivalla tavalla. Saamme näin päättelylle semanttisen tulkinnan, joskin päättelyä, sikäli kuin sen muodosta on kysymys, voidaankin pitää syntaktisena toimituksena, kuten on jo aikaisemmin todettu.
Koska siis puhuminen aktuaalisesta totuudesta ei riitä, meidän on aktuaalisen maailman lisäksi tarkasteltava muitakin ns. *mahdollisia maailmoja, mahdollisia asiaintiloja* tai *tilanteita*. Voimme kuvitella esimerkiksi sellaisen tilanteen tai maailman, jossa Helsinki ei ole Suomen pääkaupunki, eli jossa lause (4.12) on epätosi. Se ei ole tämänhetkinen aktuaalinen maailma, mutta se on jossain mielessä mahdollinen; ja on jopa ollut tietyssä historian vaiheessa aktuaalinen. Tämän maailmamme tila esimerkiksi vuonna 2020 voisi edustaa nahdollista maailmaa, joka ei ole aktuaalinen, mutta tulee aktuaaliseksi eli *aktualisoituu* tai *realisoituu* tuona vuonna. Toisaalta voidaan myös puhua mahdollisista maailmoista (asiaintiloista, tilanteista jne.), jotka eivät koskaan aktualisoidu; esimerkiksi maailma, jossa on siivekkäitä hevosia, voisi ehkä olla sellainen. Se on mahdollinen jossain mielessä; se on esimerkiksi *loogisesti mahdollinen* maailma, vaikka se ei olisikaan *fyysisesti*, *biologisesti* tai *fysikaalisesti* mahdollinen. Meillä voi siis olla erilaisia kriteerejä sille, mikä on mahdollista, mikä ei; mutta logiikan yhteydessä tarkastellaan tavallisesti loogista mahdollisuutta (joka sekin on usein suhteessa annettuun logiikkaan).

Siitä, mitä mahdolliset maailmat tarkkaan ottaen ovat, meidän ei tarvitse tässä vaiheessa välittää. Silloin, kun tarkastellaan jonkin logiikan *formaalista semantiikkaa*, tarvittava mahdollisen maailman käsite määritellään aina täsmällisesti (matemaattisesti, joukko-opillisesti). Tällöin puhutaan usein *mallista* eikä niinkään maailmasta. Tässä vaiheessa riittää kuitenkin ajatella, että mahdollinen maailma on jotakin, jossa sopivan, tarkasteltavan *kielen* lauseet ovat tosia tai epätosia, ts. jossa niillä on *totuusarvo*. Toisaalta sovimme, että nimenomaan *lauseiksi* kutsutaan niitä kielen ilmaisuja, joilla on totuusarvo malleissa tai maailmoissa; lauseet ovat *totuudenkantajia*. Niinpä luonnollisen kielen lauseita tässä merkityksessä ovat ns. indikatiiviset ja muut väitelauseet, mutta eivät esimerkiksi kysymyslauseet. Usein luonnollista kieltä käytettäessä konteksti määrää, onko lause väitelause vai ei. Lauseet ovat kielen syntaksiin kuuluvia olioita, kun taas mahdolliset maailmat ja totuusarvot kuuluvat semantiikkaan.
olkoon A tarkasteltavan kielen lause ja u mahdollinen maailma. Merkitään

$$u \vDash A,$$

jos A on *tosi* maailmassa u. Jos se taas ei ole tosi maailmassa u, eli on *epätosi* tässä maailmassa, merkitään

$$u \nvDash A.$$

Totuus mailmassa (tai mallissa) voidaan määritellä formaalisessa semantiikassa, joskin sen merkitys riippuu tarkasteltavasta logiikasta.
Oletamme nyt, että voimme puhua sellaiseta kokonaisuudesta kuin kaikkien mahdollisten maailmojen kokoelma (luokka, avaruus) U. Tosiasiassa tällaista kokoelmaa ei kuitenkaan voida tarkasti rajata tai määritellä; se on epämääräinen, ja siitä puhuminen voi jopa johtaa ristiriitaan. Se on jo sinänsä epämääräinen, mutta toisaalta se on epämääräinen myös sen suhteen, missä mielessä maailmaa pidetään 'mahdollisena'; tällä voi olla eri merkityksiä, kuten edellä todettiin. Sitä voidaan paremmin rajata, jos tehdään sopivia oletuksia sen suhteen, millainen on mahdollisen maailman rakenne, mitä siihen ajatellaan kuuluvaksi ja millaista mahdollisuutta tarkoitetaan. Kun tarkastellaan jotakin *formaalista* logiikkaa, kysymykseen tulevat mahdolliset maailmat eli mallit ja niiden rakenne määritellään täsmällisesti. Tällöin U on hyvinmääritelty luokka, joskin tavallisesti hyvin suuri.
Seuraavia tarkasteluja varten tämä käsite on epämääräisenäkin hyödyllinen. Tällöin voimme puhua myös kaikkien niiden maailmojen kokoelmasta, joissa annettu tarkastelemamme kielen lause on tosi. Olkoon siis U annettu 'kaikkien' mahdollisten maailmojen kokoelma. Olkoon A tarkasteltavan kielen lause. Sovitaan seuraavista nimityksistä ja merkinnöistä:

$$\begin{aligned} P(A) &= \text{'kaikkien niiden } U\text{:hun kuuluvien} \\ &\quad\ \ \text{maailmojen luokka, joissa A on tosi'} \\ &= \{\, u \in U \mid u \vDash A \,\} \\ &= A\text{:n määrittämä } propositio \\ &= A\text{:n } intensio\ (merkitys). \end{aligned} \tag{4.13}$$

Siis $P(A)$ on aina avaruuden U osaluokka: $P(A) \subseteqq U$.
Voimme nyt määritellä eräitä tärkeitä semanttisia käsitteitä, jotka liittyvät lauseiden ominaisuuksiin ja keskinäisiin suhteisiin. Määritelmissä pitäisi avaruuden U olla parametrina, koska

se ei ole yksikäsitteisesti annettu kaikissa tapauksissa, kuten yllä todettiin. Ajatellaan kuitenkin seuraavassa, että U on kiinnitetty niin, että kaikki määritelmät on suljettu tähän annettuun mahdollisten maailmojen avaruuteen, jolloin sitä ei aina tarvitse erikseen mainita. Tämä on oerusteltua jo siitäkin syystä, että esimerkiksi formaalisessa semantiikassa tarkastellaan tavallisesti hyvinmääriteltyjä, ns. loogisesti mahdollisia maailmoja, joiden luokka on määrätty.
Oletetaan myös, että *kieli*, jonka lauseita tutkitaan, on annettu. Olkoon edelleen $u_0 \in U$ 'aktuaalinen' maailma jossakin tämän sanan merkityksessä.
Tarkastellaan ensin yhtä lausetta kerrallaan. Seuraavia lauseiden ominaisuuksia voidaan kutsua niiden *modaaliominaisuuksiksi*. Lause A on

tosi eli *aktuaalisesti tosi*, jos A on tosi aktuaalisessa maailmassa: $u_0 \vDash A$;

loogisesti tosi (*yleispätevä*) eli *välttämätön* (*välttämättä tosi*), jos A on tosi kaikissa mahdollisissa maailmoissa: $P(a) = U$;

loogisesti epätosi eli *mahdoton*, jos A ei ole tosi missään maailmassa, eli on epätosi kaikissa maailmoissa: $P(A) = \emptyset$.

satunnaisesti tosi eli *kontingentti*, jos A on tosi mutta ei välttämätön: $u_0 \vDash A$ ja $P(A) \neq U$;

toteutuva eli *mahdollinen* (*mahdollisesti tosi*), jos A on tosi jossakin maailmassa: $u \vDash A$ jollekin $u \in U$, eli $P(A) \neq \emptyset$;

kumoutuva, jos A on epätosi jossakin maailmassa: $u \nvDash A$ jollekin $u \in U$, eli $P(A) \neq U$.

Tarkastellaan seuraavaksi kahta tai useampaa lausetta. Sanomme, että

B on A:n *looginen seuraus* eli A:sta *seuraa loogisesti* B, jos B on tosi jokaisessa maailmassa, jossa A on tosi: $P(A)$ on $P(B)$:n osaluokka.

Jos A:sta seuraa loogisesti B, niin merkitään $A \vDash B$. Ylläolena määritelmä voidaan esittää myös muodossa

$$A \vDash B, \text{ jos aina, kun } u \vDash A, \text{ niin } u \vDash B.$$

Tämä merkitsee, että A 'sallii' vain osan (tai enintään samat) niistä maailmoista, jotka B sallii. Tässä mielessä voidaan sanoa, että A on 'loogisesti voimakkaampi' kuin B. Intuitiivisesti katsoen tuntuukin luonnolliselta ajatella, että mitä voimakkaamman ehdon lause ilmaisee, sitä 'vähemmän' voi olla maailmoja, joissa se on tosi.
Merkinnällä $A_1, A_2, \ldots, A_k \vDash B$ tarkoitetaan, että B on lauseiden $A_1, A_2, \ldots, A_k$ looginen seuraus. Loogisen seurauksen määritelmä voidaan yleistää seuraavasti:

$$A_1, \ldots, A_k \vDash B, \text{ jos aina, kun } u \vDash A_1 \text{ ja } \ldots \text{ ja } u \vDash A_k, \text{ niin } u \vDash B.$$

Määritelmä voidaan ilmeisellä tavalla yleistää myös tapaukseen, jossa lauseita $A_1, A_2, A_3, \ldots$ on ääretön määrä.
Merkitään $A_1, A_2, \ldots, A_k \vdash B$, jos premisseistä $A_1, A_2, \ldots, A_k$ voidaan päätellä B. Jotta looginen seuraus, joka on semanttinen käsite, ja pätevä päätelmä, joka on syntaktinen käsite, vastaisivat toisiaan, pitää seuraavan ehdon olla voimassa:

$$A_1, A_2, \ldots, A_k \vdash B, \text{ jos ja vain jos } A_1, A_2, \ldots, A_k \vDash B, \tag{4.14}$$

eli premisseistä voidaan päätellä johtopäätös täsmälleen silloin, kun johtopäätös on premissien looginen seuraus.
Voidaan osoittaa, että formaalisten logiikkojen yhteydessä tämä ehto on voimassa, kun mahdollisten maailmojen avaruutena on kussakin tapauksessa (kutakin logiikkaa vastaten) kaikkien loogisesti mahdollisten maailmojen luokka. Ehtoa ei voikaan osoittaa oikeaksi, ennen kuin siinä esiintyvät käsitteet on tehty täsmällisiksi. Tässä kurssissa tarkasteltavien logiikoiden yhteydessä ehtoa ei kuitenkaan todisteta.
Määrittelemme vielä lisää semanttisia käsitteitä:

- A ja B ovat *loogisesti ekvivalentteja* eli *loogisesti yhtäpitäviä,* jos ne määrittelevät saman proposition: $P(A) = P(B)$ eli $u \vDash A$, jos ja vain jos $u \vDash B$.

- A ja B ovat *yhteensopimattomia*, jos A:lla ja B:llä ei ole yhteisiä maailmoja, ts. maailmoja, joissa ne molemmat olisivat tosia: $P(A) \cap P(B) = \emptyset$.

- A ja B ovat *yhteensopivia*, jos on olemassa ainakin yksi sellainen maailma u, että $u \vDash A$ ja $u \vDash B$.

On vielä syytä muistuttaa, että nämä nimitykset on suhteutettu johonkin tiettyyn mahdollisten maailmojen avaruuteen U, vaikka tätä seikkaa ei määritelmissä erikseen mainita. Edelleen on huomattava, että mitä nimitystä kussakin määritelmässä annetuista vaihtoehdoista käytetään, riippuu jonkin verran käyttöyhteydestä. Niinpä ilmaisua 'välttämätön' ja 'välttämättä tosi' käytetään *modaalilogiikan* yhteydessä, kun taas ilmaisua 'loogisesti tosi' tai 'yleispätevä' käytetään tavallisen ei-modaalisen logiikan yhteydessä. Modaalilogiikka on juuri logiikkaa, joka tutkii välttämättömyyden ja mahdollisuuden käsitteitä. Usein myös käsitteen 'välttämättä tosi' ala katsotaan laajemmaksi kuin käsitteen 'loogisesti tosi'. Tämä tarkoittaa, että kaikkia loogisia totuuksia pidetään välttämättöminä totuuksina, mutta jotkin välttämättä todet lauseet eivät ole loogisesti tosia.

4.3 Formaalisista teorioista

Formaalinen kieli muodostuu joukosta primitiivisiä symboleja eli *aakkosia* sekä näistä lauseenmuodostussääntöjen avulla muodostettuja *kaavoja* tai *lauseita*. Formaalisen kielen aakkoset ovat merkkityyppejä, joiden esiintymät kaavoissa tai lauseissa ovat konkreettisia, esim. paperille kirjoitettuja merkkejä. Samalla aakkosella voi siten olla useampia *esiintymiä* formaalisen kielen kaavassa tai lauseessa.
Formaalisen kielen *syntaksilla* tarkoitetaan sen tutkimista kielen omassa piirissä - riippumatta kielen ilmausten merkityksistä tai käytöstä. Syntaksiin kuuluu siten formaalisen kielen "kielioppi", aakkoston ja lauseenmuodostussääntöjen spefisiointi sekä formaalisen kielen *todistusteoria,* sen kaavojen ja lauseiden väliset keskinäiset suhteet.
Formaalisen kielen todistusteoriassa valitaan jotkin kielen lauseet *aksioomiksi,* joista annettujen *päättelysääntöjen* avulla voidaan johtaa *teoreemoja.* Teoreemoja kutsutaan todistuviksi; niiden todistukset ovat kielen kaavojen äärellisiä jonoja. Todistusteorialla varustettua formaalista kieltä kutsutaan *kalkyyliksi.*
Formaalisiksi järjestelmiksi nimitetään sellaisia teorioita, joilla seuraavat ehdot ovat voimassa:

1. On annettu *muotosäännöt*, jotka ilmoittavat, mitkä merkit ovat teoriassa sallittuja.

2. On annettu *lauseenmuodostussäännöt*, jotka ilmoittavat, miten sallituista merkeistä muodostetaan teorian piirissä korrekteja ilmaisuja.

3. On annettu *aksioomat*, joista teorian muut ilmaisut voidaan johtaa.

4. On annettu *päättelysäännöt*, jotka ilmoittavat, miten teorian ilmaisuista voidaan johtaa uusia ilmaisuja.

Formaalinen kieli on täysin määrätty, kun ehdot (1)-(4) vallitsevat sen piirissä. Nämä ehdot määrittelevät *kalkyylin periaatteen.*

Objektikieli ja metakieli

Formaalinen kieli voi olla joko käytön välineenä tai tutkimuksen kohteena. Kun kieli on tutkimuksen kohteena, sitä kutsutaan *objektikieleksi.* Toisaalta tällaisen tutkimuksen välineenä tarvitaan myös kieltä. Tätä sanotaan *metakieleksi.* Metakielen avulla esitetään objektikieltä koskevia tuloksia. Näitä tuloksia kutsutaan *metateoreemoiksi* erotukseksi teoreemoista, joita voidaan todistaa objektikielessä.
David Hilbert pyrki kehittämään erityisesti logiikan järjestelmien aksiomaattisen teorian. Tästä käytetään nimitystä *todistusteoria,* matemaattisten todistusten yleinen teoria.
Todistusteorian neljä pääongelmaa ovat

1. Järjestelmän *ristiriidattomuuden* osoittaminen: osoitetaan, ettei järjestelmässä voida todistaa lausetta ja sen negaatiota.

2. Järjestelmän aksioomien *riippumattomuuden* osoittaminen. Vrt. esimerkiksi paralleeli aksiooman asemaa euklidisessa geometriassa.

3. Järjestelmän *täydellisyyden* osoittaminen: tutkitaan, voidaanko aksioomista johtaa järjestelmän kaikki todet lauseet.

4. *Ratkaisuongelma*: voidaanko järjestelmän lauseet todistaa jonkin äärellisen mekaanisen menetelmän avulla. Menetelmää, jos sellaista on, kutsutaan *ratkaisumenetelmäksi.*

Hilbert ajatteli, että kaikkien matemaattisten ongelmien ratkaisuun löytyy menetelmä.
Edellä esitetyt ongelmat voidaan ratkaista mm. propositiologiikan (eli lauselogiikan) osalta. Predikaattilogiikan osalta voidaan todistaa riippumattomuus, täydellisyys ja ristiriidattomuus. Ratkaisumenetelmää ei sen sijaan löydy (Church).
Aritmetiikan osalta tiedetään myös, ettei ratkaisumenetelmää ole olemassa. Aritmetiikka on myös epätäydellinen (Gödel). Ristiriidattomuuden osoittaminen tuottaa myös vaikeuksia monilla matematiikan alueilla.

5 PROPOSITIOLOGIIKKAA

Sanalle *propositiologiikka* on synonyymejä kuten *lauselogiikka, lausekalkyyli* ja *nollannen kertaluvun logiikka.* Propositiologiikka on eräs *formaalinen kieli*. Tässä tarkasteltavaa erityistä propositiologiikkaa kutsutaan nimellä *lauselogiikka*, merkitään $\mathcal{L}$.

5.1 Aakkosto ja lauseenmuodostus

Tarkastelemme tässä kielen $\mathcal{L}$ *syntaksin* peruskäsitteitä. Propositiologiikka formaalisena kielenä voidaan määritellä useilla eri tavoilla riippuen käytettävän aakkoston valinnasta.

Määritelmä 5.1.1. Lauselogiikan $\mathcal{L}$ *aakkosto* muodostuu seuraavista symboleista, joita kutsutaan $\mathcal{L}$:n *primitiivisiksi symboleiksi* eli *aakkosiksi*:

(1) numeroituva joukko $\{p_i \mid i \in \mathbf{N}\}$ symboleja (propositiokirjaimet),

(2) implikaation merkki $\rightarrow$,

(3) negaation merkki $\neg$,

(4) sulkumerkit $(,)$.

Mielivaltainen äärellinen jono $\mathcal{L}$:n aakkoston primitiivisiä symboleja on $\mathcal{L}$:n *ilmaisu*. Esimerkiksi jono $p_1 \Rightarrow \neg p_2$ on $\mathcal{L}$:n ilmaisu. se ei kuitenkaan ole ns. *"hyvinmuodostettu"*. Kielen $\mathcal{L}$ *hyvinmuodostetut kaavat*, merkitään *hmk* (wellformed formula, wff), määritellään seuraavan induktiivisen määritelmän avulla.

Määritelmä 5.1.2. $\mathcal{L}$:n hyvinmuodostetut kaavat *hmk* ovat seuraavat $\mathcal{L}$:n ilmaisut

(i) p_n on *hmk* kaikille $n \in \mathbf{N}$,

(ii) jos A ja B ovat lauseita, niin $(A \rightarrow B)$ on lause,

(iii) jos A on lause, niin $(\neg A)$ on lause,

(iv) ilmaisu on lause vain, jos se on lause edellisten ehtojen (i)-(iii) perusteella.

Määritelmän (5.1.2) ehdot (i)-(iv) ovat kielen $\mathcal{L}$ *lauseenmuodostussäännöt*. Ehto (i) määrittelee $\mathcal{L}$:n *atomilauseet*. Ehdot (ii) ja (iii) ilmaisevat, miten atomilauseista voidaan muodostaa *yhdistettyjä lauseita*.

Esimerkki 5.1.3. Ilmaisu $p_3 \rightarrow ((\neg p_2) \rightarrow p_1))$ on $\mathcal{L}$:n lause. Koska p_1, p_2 ja p_3 ovat määritelmän (5.1.2) kohdan (i) nojalla lauseita $\neg p_2$ on kohdan (iii) nojalla lause, niin tällöin ilmaisu $((\neg p_2) \rightarrow p_1))$ on lause kohdan (ii) nojalla, joten ko. alkuperäinen ilmaisu on siis $\mathcal{L}$:n lause kohdan (ii) nojalla.

Kielen $\mathcal{L}$ lauseiden joukko on yksikäsitteisesti määrätty, kuten seuraava tulos osoittaa.

Lause 5.1.4. On olemassa yksikäsitteinen joukko $\mathcal{W}$ sellaisia $\mathcal{L}$:n ilmaisuja, että

(1) $p_n \in \mathcal{W}$ kaikille $n \in \mathbf{N}$,

(2) jos $A \in \mathcal{W}$, niin $(\neg A) \in \mathcal{W}$,

(3) jos $A \in \mathcal{W}$, niin $(A \to B) \in \mathcal{W}$,

(4) jos $\mathcal{W}'$ toteuttaa ehdot (1)-(3), niin $\mathcal{W}$ sisältyy joukkoon $\mathcal{W}'$.

Todistus. Todistus seuraa määritelmistä (5.1.1) ja (5.1.2) täydellisen induktion nojalla. ■
Kun haluamme todistaa, että kaikilla $\mathcal{L}$:n lauseilla A on ominaisuus φ, voimme osoittaa tämän seuraavasti:

(1) Osoitetaan $\varphi(p_n)$ kaikille $n \in \mathbf{N}$,

(2) Osoitetaan $\varphi(\neg A)$, jos $\varphi(A)$,

(3) Osoitetaan $\varphi(A \to B)$, jos $\varphi(A)$ ja $\varphi(B)$.

Tällaista todistusmenetelmää kutsutaan *induktioksi lauseen pituuden suhteen*.
Metakielisessä määritelmässä (5.1.2) $\mathcal{L}$:n primitiivisiä symboleja p_n, $\neg$, $\to$,) ja (käytetään itseisesti. Tässä määritelmässä esiintyvät symbolit A ja B eivät ole $\mathcal{L}$:n, vaan sen metakielen symboleja, ns. *metamuuttujia*, jotka saavat arvoikseen $\mathcal{L}$:n lauseita.
Kun viittaamme metakielessä $\mathcal{L}$:n lauseisiin, noudatamme seuraavaa *sopimusta:*

(i) Lauseen uloin sulkumerkkipari voidaan jättää merkitsemättä,

(ii) Negaatiomuotoisen lauseen ympäriltä voidaan sulkumerkkipari jättää merkitsemättä *siinäkin* tapauksessa, että se esiintyy osana lausetta.

Sitomisjärjestys; Ensin sitoo negaatio ja sitten implikaatio.
Otamme käyttöön seuraavat **lyhennykset:**

$$A \vee B \overset{\text{merk.}}{=} \neg A \to B, \tag{5.1}$$

$$A \wedge B \overset{\text{merk.}}{=} \neg(\neg\neg A \to \neg B), \tag{5.2}$$

$$A \leftrightarrow B \overset{\text{merk.}}{=} \neg(\neg\neg(A \to B) \to \neg(B \to A)). \tag{5.3}$$

Merkinnät (5.1), (5.2) ja (5.3) esittävät vastaavasti konnektiiveja *disjunktio (ei)*, *konjunktio (ja)* sekä *ekvivalenssi (joss)*.
Kohdan (5.1) nojalla saadaan kohta (5.2) muotoon

$$A \wedge B \;=\; \neg(A \to \neg B).$$

Edelleen saamme kohtien (5.1) ja (5.2) nojalla kohta (5.3) muotoon

$$A \leftrightarrow B \;=\; (A \to B) \wedge (B \to A).$$

Huomautus 5.1.5. Valitsemamme aakkoston nojalla symbolit $\vee$, $\wedge$, ja $\leftrightarrow$ ovat metakielen merkkejä, joilla viitataan kielen $\mathcal{L}$ lauseisiin lyhennysmerkintöjen mukaisesti. Sitomisjärjestys, nämä uudet konnektiivit mukaanlukien, on nyt seuraava: ensin vahvimpana sitoo negaatio, sitten samanarvoisina disjunktio ja konjunktio, joiden keskinäinen sitomisjärjestys on osoitettava sulkumerkeillä, sekä viimeksi implikaatio ja ekvivalenssi, jotka ovat keskenään samanarvoiset. Näiden keskinäinen sitomisjärjestys täytyy myös osoittaa sulkumerkein.

Ilmausta, joka on lauseen A yhtenäinen osa ja joka itse on lause, kutsutaan lauseen A *osalauseeksi*. Jokainen yhdistetty lause voidaan täten kirjoittaa jossakin seuraavista muodoista: $\neg(A)$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, ja $(A \leftrightarrow B)$, jossa A ja B ovat annetun lauseen osalauseita. Tässä muodossa esiintyvää konnektiivia, ts. negaatiota tai lauseen uloimpia sulkumerkkejä vastaavaa konnektiivia, kutsutaan lauseen *pääkonnektiiviksi*. Em. lyhennysmerkintöjen lisäksi esitämme muut em. konnektiivien väliset keskinäiset riippuvuussuhteet:

$$\begin{aligned} A \vee B &\overset{\text{merk.}}{=} \neg(\neg A \wedge \neg B). \\ A \rightarrow B &\overset{\text{merk.}}{=} \neg(A \wedge \neg B), \\ A \leftrightarrow B &\overset{\text{merk.}}{=} \neg(A \wedge \neg B) \wedge \neg(B \wedge \neg A). \end{aligned}$$

5.2 Arkikielen propositioita

Propositioksi sanomme väitelausetta, johon voidaan liittää *totuusarvo*. Propositio siis väittää tietyn asiantilan tai tiettyjen asiantilojen vallitsevan.
Asiantila ja sen vallitseminen on propositiossa itse asian ydin. Jos sanomme ”Tänään on tiistai”, tai ”Eilen oli tiistai”, ilmaisevat ne saman proposition, jos ensimmäinen lause sanotaan tiistaina ja toinen keskiviikkona. Siis kielen kannalta sama propositio voidaan ilmaista eri lauseilla. Myös kielellisesti sama lause voi eri tilanteissa ilmaista eri propositioita. Jos esimerkiksi Josephine puhuessaan Napoleonista olisi sanonut 6.1.1806 klo 2: ”Hän on nyt nälkäinen”, hän olisi sanonut aivan muuta kuin Krupskaja olisi sanonut, jos hän olisi sanonut saman lauseen 7.1.1920 klo 3 viitaten Leniniin.
Kun arkikielessä haluamme osoittaa propositioita, käytämme usein että -lausetta. Jonkin verran yksinkertaistettuna voidaan sanoa, että perimmäinen ero suoran ja epäsuoran esityksen välillä vastaa eroa lauseesta puhumisen ja propositiosta puhumisen välillä. Tarkastelkaamme seuraavia esimerkkilauseita:

(a) John Lackland sanoi: ”Verot ovat hyviä talonpojille”.

(b) John Lackland sanoi, että verot ovat hyviä talonpojille.

Lause (a) on tosi ainoastaan, mikäli Lackland todella käytti sanoja *Verot ovat hyviä talonpojille*. Lause (b) on tosi, jos hän ilmaisi että -lauseen sisällön, *että verot ovat hyviä talonpojille*. Hän on voinut käyttää toisia sanoja ja jopa toista kieltä. Lauseessa (b), jossa on epäsuora esitys, sanomme siis, että Lackland esittää jonkin proposition eikä lausetta.
Ns. *klassisessa logiikassa*, jonka puitteissa pääasiassa liikumme, on kaksi totuusarvoa, *tosi* ja *epätosi*.

Kielen lauseiden muodollisia ominaisuuksia ja lainalaisuuksia voidaan tutkia *formalisoimalla* lause logiikan formaaliselle kielelle, jolloin lauseen sisällöllinen merkitys jää taka-alalle.

Esimerkki 5.2.1. Formalisoimme kielelle $\mathcal{L}$ seuraavan lauseen:

> ”Jos janoinen Mutikainen menee outoon soittoruokalaan, jossa lantrinki maksaa enemmän kuin viski, niin hän ei tilaa mitään, tai janoisuus käy ylivoimaiseksi ja Mutikainen pyytää lasillisen jäävettä”.

Merkitsemme atomilauseita seuraavasti:

j = janoinen Mutikainen menee outoon soittoruokalaan
l = siellä lantrinki maksaa enemmän kuin viski
h = hän tilaa jotakin
y = janoisuus käy ylivoimaiseksi
m = Mutikainen pyytää lasillisen jäävettä

Saamme siis

Jos j ja l, niin ei h, tai y ja m.

Kun korvaamme vielä sidesanat vastaavilla konnektiiveilla, saamme

$$j \wedge l \rightarrow \neg h \vee (y \wedge m).$$

Kuten esimerkissämme huomasimme, vastaa kutakin sidesanaa *ei*, *ja*, *tai*, *jos . . . niin* ja *joss* konnektiivit negaatio $\neg$, konjunktio $\wedge$, disjunktio $\vee$, implikaatio $\rightarrow$ ja ekvivalenssi $\leftrightarrow$.

5.3 $\mathcal{L}$:n semantiikkaa

Kieli on aina kieltä jostakin; se käsittelee, kuvaa, esittää tai merkitsee jotakin. Kielen *semantiikka* eli *malliteoria* on teoria kielen merkityksestä, siitä mitä kieli esittää.
Formaalisen kielen semantiikan teoria käyttää, kuten syntaktinen todistusteoriakin, matemaattisia käsitteitä ja menetelmiä, usein vaativampia kuin syntaktinen todistusteoria.
Keskeiset semanttiset käsitteet ovat *totuus* ja *epätotuus*. Jos lause kuvaa asiantilan, joka vallitsee, lause on *tosi*. Jos lause kuvaa asiantilan, joka ei vallitse, lause on *epätosi*. Seuraavsaa esitetään pääpiirteittäin $\mathcal{L}$:n semantiikkaa.
Ilmaisuja *tosi* ja *epätosi* voidaan merkitä mm. seuraavilla tavoilla:

(1) tosi $\overset{\text{merk.}}{=} T$ epätosi $\overset{\text{merk.}}{=} E$,

(2) tosi $\overset{\text{merk.}}{=} 1$ epätosi $\overset{\text{merk.}}{=} 0$.

$\mathcal{L}$:n lauseiden totuusarvot voidaan määrittää ns. *valuaation* avulla:

Määritelmä 5.3.1. $\mathcal{L}$:n *valuaatio* kiinnittää kuhunkin $\mathcal{L}$:n lauseeseen p_n, missä $n \in \mathbf{N}$, totuusarvon T tai E.

Määritelmä 5.3.2. Valuaatio laajennetaan $\mathcal{L}$:n lauseista muodostettujen yhdistettyjen $\mathcal{L}$:n lauseiden joukosta joukkoon $\{E, T\}$ seuraavasti: ■

1. Jos lause A on muotoa $B \to C$, niin $A := T$, jos $B := E$ tai $C := T$. Muussa tapauksessa $A := E$.
2. Jos A on muotoa $\neg B$, niin $A := T$, jos $B := E$. Muussa tapauksessa $A := E$.
3. Jos A on muotoa $B \wedge C$, niin $A := T$, jos sekä $B := T$ että $C := T$.
4. Jos A on muotoa $B \vee C$, niin $A := T$, jos vähintään toinen ehdoista $B := T$ ja $C := T$ pätee.
5. Jos A on muotoa $B \leftrightarrow C$, niin $A := T$ tarkalleen silloin, kun B ja C saavat saman arvon.

Esimerkki 5.3.3. Olkoon $P := T$ ja $Q := E$. Silloin $\neg P := E$. Minkä totuusarvon saa lause $P \Rightarrow (P \Rightarrow \neg Q)$? Määritelmän (5.3.2) nojalla $\neg Q := T$, $P \Rightarrow \neg Q := T$, joten $P \Rightarrow (P \Rightarrow \neg Q) := T$.

Seuraava Lause osoittaa„ että jokainen $\mathcal{L}$:n lause on joko tosi tai epätosi valuaation suhteen, eikä mikään lause ole sekä tosi että epätosi.

Lause 5.3.4. Jokainen $\mathcal{L}$:n lause A saa yksikäsitteisesti arvon T tai E.

Todistus. Määritelmän (5.3.2) nojalla voimme määrätä $\mathcal{L}$:n jokaisen yhdistetyn lauseen A totuusarvon, kun kaikkien A:ssa esiintyvien propositiokirjainten totuusarvot tunnetaan. Jokainen lause A määrittelee siten funktion

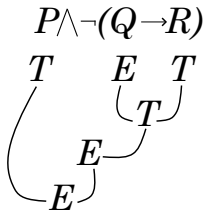
$$f_A : \{E, T\}^n \longrightarrow \{E, T\},$$

jossa n on A:ssa esiintyvien eri propositiokirjainten lukumäärä. Funktiota f_A kutsutaan lauseen A määräämäksi *totuusfunktioksi*. Yleisesti voidaan sanoa, että totuusfunktio on kuvaus *totuusarvojakeluiden* joukosta totuusarvojen joukkoon. Täten jokaisen totuusfunktionaalisen ilmaisun kohdalla pätee, että totuusfunktio liittää jokaiseen totuusarvojakeluun *yksikäsitteisesti* tietyn totuusarvon. ■

Esimerkki 5.3.5. Tarkastellaan ilmaisua $P \wedge \neg(Q \to R)$ puhtaasti totuusfunktionaalisena ilmaisuna. Tällöin se eräs kolmen muuttujan funktio $f(P, Q, R)$, ts. f on funktio

$$f : \{E, T\}^3 \longrightarrow \{E, T\}.$$

Joukon $\{E, T\}^3$ alkiot ovat järjestettyjä totuusarvokolmikoita. Sen kaikki alkiot muodostavat ko. ilmaisun totuusarvojakelut, joita tässä tapauksessa on $2^3 = 8$ kpl. Olkoon esimerkiksi $(P, Q, R) = (T, E, T)$. Tällöin saamme



Siis $f(T, E, T) = E$.

Huomautus 5.3.6. Totuusarvojakelut ovat funtioita lauseiden joukosta totuusarvojen joukkoon, ts. valuaatioita. Myös tätä seikkaa voidaan havainnollistaa totuustauluilla.

Toteutuvuus ja validisuus
Keskeisiä semantiikan käsitteitä ovat *toteutuvuuden* (satisfiability) ja *validisuuden* käsitteet.

Määritelmä 5.3.7. Ei-tyhjä joukko $\mathcal{M}$ kielen $\mathcal{L}$ lausemuuttujia (propositiokirjaimia) on $\mathcal{L}$:n *malli*.

Itse asiassa malli on asiantilojen kokonaisuus, joka ilmoitetaan niiden lauseiden joukkona, joiden ilmaisema asiantila vallitsee ko. mallissa. Lause on tosi joss lauseen ilmaisema asiantila vallitsee. Kun ilmaisemme tämän täsmällisemmin, saamme ns. *totuuden korrespondenssiteorian*: Lause P on tosi mallissa $\mathcal{M}$, joss sen ilmaisema asiantila vallitsee mallissa $\mathcal{M}$.

Määritelmä 5.3.8. Lause A on *toteutuva*, jos on olemassa sellainen $\mathcal{M}$, että $A := T$ joukossa $\mathcal{M}$, ts $A \in \mathcal{M}$, merk. $\mathcal{M} \models A$.

Määritelmä 5.3.9. Lause A on *validi*, joss $A \in \mathcal{M}$ pätee kaikille malleille $\mathcal{M}$, ts. $\mathcal{M} \models A$ pätee kaikille malleille $\mathcal{M}$, merk. $\models A$.

Esimerkki 5.3.10. Olkoon $\mathcal{M} = \{P, Q\}$. Tällöin $\mathcal{M} \models P \wedge Q$, koska $\mathcal{M} \models P$ ja $\mathcal{M} \models Q$. Myös $\mathcal{M} \models P \vee R$, koska $\mathcal{M} \models P$ ja $\mathcal{M} \models \neg(P \rightarrow \neg Q)$, koska $\mathcal{M} \models \neg P$ ei päde, jolloin myös $\mathcal{M} \models P \rightarrow \neg Q$ ei päde, josta seuraa, että $\mathcal{M} \models \neg(P \rightarrow \neg Q)$ pätee.

Lause P on toteutuva, koska se on tosi mm. eo. mallissa. Samoin lause $\neg P$ on toteutuva, koska se on tosi sellaisessa mallissa , jossa P on epätosi. Lause P ei ole validi, koska on olemassa sellainen malli, jossa se on tosi ja toisaalta sellainen malli, jossa se on epätosi. Siis lause P ja sen negaatio $\neg P$ voivat olla yhtä aikaa toteutuvia, mutta sama malli ei voi niitä tällöin toteuttaa. Mm. lause $\neg(P \rightarrow \neg Q)$ on toteutuva, koska $\mathcal{M} \models \neg(P \rightarrow \neg Q)$ pätee.
Lause $P \rightarrow P$ on validi, kosa se on tosi missä tahansa mallissa. Tämä voidaan todeta mm. totuustauluilla.
Seuraavat lauseet ovat selviä ja helppoja todistaa.

Lause 5.3.11. (a) Lause Q seuraa loogisesti lauseesta P, joss lause $P \rightarrow Q$ on validi. (b) Lauseet P ja Q ovat loogisesti ekvivalentteja, joss lause $P \leftrightarrow Q$ on validi.

Lause 5.3.12. Lause A on validi, joss $\neg A$ ei ole toteutuva.

Lause 5.3.13. Lause A on toteutuva, joss $\neg A$ ei ole validi.

Toteutuvuus ja validisuus voidaan määritellä koskemaan myös lausejoukkoja. Tällöin puhutaan *simultaanisesta toteutuvuudesta*.

Määritelmä 5.3.14. Olkoon Δ joukko $\mathcal{L}$:n lauseita ja ν mallin $\mathcal{M}$ valuaatio. Valuaatio ν *toteuttaa (simultaanisesti)* Δ:n, jos ν toteuttaa Δ:n jokaisen lauseen. Lausejoukko Δ, joka toteutuu simultaanisesti, on *toteutuva* eli *konsistentti*.

Esimerkki 5.3.15. Olkoon $\Delta = \{P \to Q,\ \neg Q,\ P \to P\}$ ja $\mathcal{M} = \{R\}$. Tällöin ei ole niin, että

$$\mathcal{M} \models P \text{ ja } \mathcal{M} \models Q,$$

jolloin joukon Δ lauseet saavat seuraavat totuusarvot: $P \to Q := T$, $\neg Q := T$ ja $P \to P := T$ ts. $\mathcal{M} \models P \to Q$, $\mathcal{M} \models \neg Q$ ja $\mathcal{M} \models P \to P$.

(Semanttinen) looginen seuraus
Semantiikassa voidaan tutkia, millä ehdoilla lause A seuraa jostakin lausejoukosta Δ. Sanomme, että Δ implikoi lauseen A, jos A on tosi aina, kun jokainen Δ:n lause on tosi. Määrittelemme tämän täsmällisesti:

Määritelmä 5.3.16. Olkoon Δ joukko $\mathcal{L}$:n lauseita. Lause A *seuraa loogisesti* lausejoukosta Δ (Δ *implikoi semanttisesti* A:n), jos A on tosi kaikissa niissä malleissa, joissa Δ:n jokainen lause on tosi. Tällöin merkitään $\Delta \models A$.

Esimerkki 5.3.17. Olkoon $\Delta = \{P, Q \to \neg P\}$ ja $\mathcal{M} = \{P, R\}$. Tällöin $\mathcal{M} \models \neg Q$ ja $\mathcal{M} \models Q \to \neg P$. Helposti havaitaan, että $\mathcal{M}$ on ainoa malli, joka toteuttaa simultaanisesti Δ:n. Koska se toteuttaa myös lauseen $\neg Q$, niin $\Delta \models \neg Q$.

Esimerkki 5.3.18. Olkoon $\Delta = \{P \to \neg P,\ \neg(P \to \neg P)\}$. Mikään malli ei toteuta joukkoa Δ. Δ on *(semanttisesti) ristiriitainen* (semanttisesti inkonsistentti). Silloin jokaisesta valuaatiosta pätee, että jos se simultaanisesti toteuttaa Δ:n, se toteuttaa myös lauseen Q. Siis $\Delta \models Q$, eli *inkonsistentti lausejoukko implikoi semanttisesti minkä lauseen hyvänsä.*

Lause 5.3.19. $\Delta \models A$, joss $\models A$. (Merkintä $\models A$ tarkoittaa, että A on validi.)

Lause 5.3.20. Jos $A \in \Delta$, niin $\Delta \models A$.

Lause 5.3.21. Jos $\Delta \models A$, niin $\Delta \cup \Omega \models A$.

Lause 5.3.22. Jos $\Delta \models A$ ja $\Omega \cup \{A\} \models B$, niin $\Delta \cup \Omega \models B$.

Lause 5.3.23. Jos $\Delta \models A \to B$, niin $\Delta \cup \{A\} \models B$.

Lause 5.3.24. Jos $\Delta \cup \{A\} \models B$, niin $\Delta \models A \to B$.

Vrt. Todistusteorian vastaavia tuloksia.
Semanttisen seurauksen määritelmän nojalla *päättely on validi,* jos johtopäätös on tosi kaikissa niissä malleissa, joissa premissit ovat tosia. Päättely ei ole validi, jos on olemassa sellainen malli, jossa premissit ovat tosia, mutta johtopäätös on epätosi.

Esimerkki 5.3.25. On osoitettava, että seuraava päättely ei ole validi.

> Jos käki kukkuu,
> kevät on pitkällä.
> Kevät on pitkällä.
> Siis käki kukkuu.

Formalisoidaan päättely seuraavasti: K = 'käki kukkuu', P = 'Kevät on pitkällä'. Saamme formaalisen päättelyn

1.	$K \to P$	pr.
2.	P	pr.
3.	K	J.(=johtopäätös)

On siis löydettävä sellainen malli, jossa lauseet $1.$ ja $2.$ ovat tosia, mutta lause $3.$ epätosi. Kokeilemme mallia $\mathcal{M} = \{P\}$, jolloin $P := T$ ja $K := E$. Tällöin $K \to P := T$, $P := T$, mutta $K := E$ eli juuri niin, että premissit ovat tosia ja johtopäätös epätosi.

Totuustaulut
$\mathcal{L}$:n lauseiden loogisen luonteen selvittämiseksi käytetään usein ns. *totuustaulumenetelmää*. Tässä esitämme pääkohdittain *Postin* totuustaulumenetelmän. Muodostamme ensin negaation, implikaation, konjunktion, diskonjunktion ja ekvivalenssin totuustaulut, joita kutsumme *perustotuustauluiksi*.

P	$\neg P$	P	Q	$P \to Q$	$P \wedge Q$	$P \vee Q$	$P \leftrightarrow Q$
T	E	T	T	T	T	T	T
E	T	T	E	E	E	T	E
		E	T	T	E	T	E
		E	E	T	E	E	T

Perustotuustaulut on konstruoitu etsimällä konnektiiveille kaikki mahdolliset valuaatiot. Näitä totuusarvokombinaatioita eli totuusarvojakeluja, joita vastaavat kunkin konnektiivin taulussa (myös lukumääräisesti) vaakarivit, on 2^k kpl, missä k ilmaisee propositiokirjainten määrän. Kaikki $\mathcal{L}$:n lauseiden totuustaulut voidaan konstruoida perustotuustaulujen avulla.

Esimerkki 5.3.26. Muodostamme lauseen $(P \to \neg Q) \vee (\neg Q \wedge Q)$ totuustaulun.

P	Q	$\neg Q$	$\neg P$	$P \to \neg Q$	$\neg Q \wedge Q$	$(P \to \neg Q) \vee (\neg Q \wedge Q)$
T	T	E	E	E	E	E
T	E	T	E	T	E	T
E	T	E	T	T	E	T
E	E	T	T	T	E	T

Totuusarvoja määrätessämme etenemme siis siten, että ensin merkitsemme näkyviin vasemmalle lauseiden P ja Q alle kaikki totuusarvokombinaatiot ja muodostamme konnektiivien totuusarvot vastaaville arvokombinaatioille katsomalla ne perustotuustauluista.

Määritelmä 5.3.27. Lause on *tautologia*, jos sen totuustaulu muodostuu pelkästään totuusarvoista T, ts. lause on tosi kaikilla totuusarvojakeluilla.

Määritelmästä (5.3.27) seuraa

Lause 5.3.28. $\mathcal{L}$:n lause on tautologia, joss se on validi.

Esimerkki 5.3.29. Tutkimme totuustaulun avulla, onko lause $\neg(P \wedge \neg Q) \rightarrow (\neg P \vee Q)$ tautologia.

P	Q	$\neg P$	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$	$\neg P \vee Q$	$\neg(P \wedge \neg Q) \rightarrow (\neg P \vee Q)$
T	T	E	E	E	T	T	T
T	E	E	T	T	E	E	T
E	T	T	E	E	T	T	T
E	E	T	T	E	T	T	T

Totuustauluilla voidaan tutkia, (i) onko lause tai lausejoukko toteutuva, kumoutuva vai ristiriitainen (eli inkonsistentti), (ii) onko lause validi, ja (iii) onko päättely validi.

Esimerkki 5.3.30. Tutkimme totuustauluilla, onko lause $(P \rightarrow Q) \wedge (P \wedge \neg Q)$ toteutuva.

P	Q	$\neg Q$	$(P \rightarrow Q)$	$P \wedge \neg Q$	$(P \rightarrow Q) \wedge (P \wedge \neg Q)$
T	T	E	T	E	E
T	E	T	E	T	E
E	T	E	T	E	E
E	E	T	T	E	E

Esimerkki 5.3.31. On tutkittava ovatko lauseet $\neg(P \vee \neg Q)$ ja $\neg P \wedge Q$ loogisesti ekvivalentteja. Tämä suoritetaan tutkimalla totuustauluilla, onko lauseen (5.3.11) ehto (b) voimassa eli päteekö

$$\models \neg(P \vee \neg Q) \leftrightarrow (\neg P \wedge Q).$$

Looginen päättely voidaan esittää, kuten edellä on nähty, luettelemalla premissit ja johtopäätös. Se voidaan esittää myös implikaatiomuodossa, jossa implikaation etujäsen muodostuu kaikkien premissien konjunktiosta ja takajäsen johtopäätöksestä. Siis päättely $P_1, P_2, \ldots, P_n \models Q$ voidaan esittää muodossa

$$P_1 \wedge P_2 \wedge \ldots \wedge P_n \rightarrow Q.$$

Kun päättelyn validisuutta tutkitaan esim. totuustauluilla, käytetään päättelystä implikaatiomuotoa.

Esimerkki 5.3.32. Tutkimme, onko seuraava päättely validi:

1.	$P \rightarrow \neg Q$	pr.
2.	$\neg Q \wedge P$	pr.
3.	$\neg P \vee Q$	J.(=johtopäätös)

Päättely implikaatiomuodossa on lause $(P \rightarrow \neg Q) \wedge (\neg Q \wedge P) \rightarrow (\neg P \vee Q)$. Jos tämä lause on validi, on myös alkuperäinen päättely validi. Lause taas on validi, jos se on tautologia. Muodostamalla totuustaulu todetaan, että tämä lause ei ole tautologia eikä siten validi, mitä myöskään alkuperäinen päättely ei ole.

Disproof -menetelmä

Tämä epäsuoran todistuksen säännön kanssa analoginen menetelmä soveltuu hyvin käytännön validisuustodistuksiin.

Yritetään osoittaa lause kumoutuvaksi. Jos toteamme sen mahdottomaksi, niin olemme osoittaneet ko. lauseen validiksi.

Esimerkki 5.3.33. On osoitettava, että lause
$(A \to B \vee C) \to (A \to (\neg C \to B))$ on validi.

1. Jos ko. lause olisi kumoutuva, niin on välttämätöntä, että $A \to (B \vee C)$ on tosi ja $A \to (\neg C \to B)$ on epätosi.
2. Jotta $A \to (\neg C \to B)$ olisi epätosi, niin on välttämätöntä, että A on tosi ja $\neg C \to B$ epätosi.
3. Jotta $\neg C \to B$ olisi epätosi, on välttämätöntä, että $\neg C$ on tosi ja B epätosi.
4. Jotta $\neg C$ olisi tosi, on välttämätöntä, että C olisi epätosi.

Siis välttämättä $A := T$, $B := E$ ja $C := E$. Mutta tällöin lause $A \to (B \vee C)$ on epätosi vastoin kohdan (1) vaatimusta. Siis ko. lausetta ei voida kumota, joten se on tosi kaikilla totuusarvojakeluilla ja täten validi.

Lause 5.3.34. Jos $\models P$ ja $\models P \to Q$, niin $\models Q$.

Todistus. Jos Q ei olisi tautologia, ts. $\models Q$ ei päde, niin Q saisi jollakin totuusarvojakelulla arvon E. Koska $P \to Q$ on tautologia oletuksen nojalla, niin P saa tällä totuusarvojakelulla arvon E. Tällöin P ei olisi tautologia, mikä on vastoin oletusta. ■

Huomautus 5.3.35. Eo. metateoreemaa voidaan tulkita siten, että modus ponens säilyttää tautologian.

Ratkaisuongelma
$\mathcal{L}$:n ratkaisuongelma on ratkeava, koska sillä on ratkaisumenetelmä, eli $\mathcal{L}$:llä on menetelmiä, joiden avulla voidaan tutkia jokainen $\mathcal{L}$:n lause mekaanisesti äärellisellä askelmäärällä, onko se validi vai ei. Mm. totuustaulut ovat $\mathcal{L}$:n eräs ratkaisumenetelmä. Muita menetelmiä ovat semanttiset puut, disproof -menetelmä sekä muut RAA:n sovellukset.

5.4 Todistusteoriaa

$\mathcal{L}$:n aksiomatisointi
$\mathcal{L}$:n aksiomatisointi suoritetaan spesifioimalla joukko aksioomia ja päättelysääntöjä. Seuraavassa esitettävä aksiomatisointi perustuu Lukasiewiczin esittämään aksioomasysteemiin, kuitenkin siten, että aksioomat Von Neumannin idean mukaisesti esitetään ns. *aksioomakaavioina*. Tämä systeemi on käyttökelpoinen erityisesti silloin, kun halutaan todistaa lauseita $\mathcal{L}$:ssä.
Lähestymistapaa, jossa logiikan tutkimisen menetelmän muodostavat aksiomatisointi ja todistaminen, kutsutaan *todistusteoreettiseksi*. Käytämme seuraavassa aksioomakaavioista lyhyesti nimitystä aksiooma.
$\mathcal{L}$:n **aksioomat**. Jos P, Q ja R ovat mitä tahansa $\mathcal{L}$:n lauseita, niin seuraavat kaavat ovat aksioomia:

$$
\begin{array}{ll}
(A1) & P \to (Q \to P) \\
(A2) & (P \to (Q \to R)) \to ((P \to Q) \to (P \to R)) \\
(A3) & (\neg Q \to \neg P) \to (P \to Q).
\end{array}
$$

Huomautus 5.4.1. Aksioomia on äärettömän monta, koska P, Q ja R voivat olla mitä tahansa $\mathcal{L}$:n lauseita. Aksioomat $(A1) - (A3)$ ovat ns. *aksioomakaavioita*.

Päättelysääntönä on *Modus (Ponendo) Ponens*, merk. MP, joka sanoo, että lauseista P ja $P \to Q$ päätellään P. Tämä esitetään ns. *päättelykaaviona* seuraavasti:

$$\frac{\begin{array}{l} P \\ P \to Q \end{array}}{Q} \qquad (MP)$$

Viiva on nimeltään ns. *päättelyviiva*, sen yläpuolella olevat lauseet ovat *premissejä* eli oletuksia ja viivan alapuolella oleva lause on *johtopäätös*.

Määritelmä 5.4.2. Olkoon joukko Δ kielen $\mathcal{L}$ lauseita (premissit). Äärellinen lausejono $S_1, \ldots, S_n$ on lauseen S_n **Δ-*päättely***, joss jokaisella indeksin i, $1 \leq i \leq n$ arvolla ainakin yksi seuraavista ehdoista on voimassa:

(i) S_i on aksiooma,

(ii) $S_i \in \Delta$,

(iii) On olemassa sellaiset luvut $j, k < i$, että S_k on $S_j \to S_i$. (Tällöin S_i päätellään MP:llä sitä edeltävistä lauseista S_j ja $S_j \to S_i$).

Ko. jono $S_1, \ldots, S_n$ on S_n:n *deduktio* eli *johto* joukosta Δ. Tällöin merkitään $\Delta \vdash S_n$, ja sanomme, että S_n on *johdettavissa* joukosta Δ. Jos erityisesti Δ on äärellinen, esim. $\Delta = \{A_1, \ldots, A_k\}$, merkitsemme

$$A_1, \ldots, A_n \vdash S_n.$$

Semanttisen implikaation ja johdettavuuden käsitteen välillä vallitsee selvä analogia;

$$\begin{array}{rl} \Delta \vdash A: & A \text{ on johdettavissa lausejoukosta } \Delta, \\ \Delta \models A: & A \text{ on } \Delta\text{:n semanttinen seuraus.} \end{array}$$

Määritelmä 5.4.3. Jos lause P on johdettavissa tyhjästä lausejoukosta Δ, niin P on $\mathcal{L}$:n *teoreema*, merk. $\vdash P$. Äärellinen jono $\mathcal{L}$:n lauseita $S_1, \ldots, S_n$ $(S_n = P)$ on P:n *todistus* $\mathcal{L}$:ssä, jos se täyttää määritelmän (5.4.2) ehdot (i) ja (iii). Sanomme tällöin, että P on *todistuva* $\mathcal{L}$:ssä.

Lause 5.4.4. $\vdash P \to P$.

Todistus.

1. $(P \to ((P \to P) \to P)) \to ((P \to (P \to P)) \to (P \to P))$ $A2$
2. $P \to ((P \to P) \to P)$ $A1$
3. $(P \to (P \to P)) \to (P \to P)$ $MP, 1, 2$
4. $P \to (P \to P)$ $A1$

5. $P \to P$ $MP, 4, 3$

■

Lause 5.4.5. $\vdash \neg P \to (P \to Q)$.

Todistus.

1. $(\neg Q \to \neg P) \to (P \to Q)$ $A3$
2. $((\neg Q \to \neg P) \to (P \to Q)) \to (\neg P \to ((\neg Q \to \neg P) \to (P \to Q)))$ $A1$
3. $\neg P \to ((\neg Q \to \neg P) \to (P \to Q))$ $MP, 1, 2$
4. $(\neg P \to ((\neg Q \to \neg P) \to (P \to Q))) \to ((\neg P \to (\neg Q \to \neg P)) \to (\neg P \to (P \to Q)))$ $A2$
5. $(\neg P \to (\neg Q \to \neg P)) \to (\neg P \to (P \to Q))$ $MP, 3, 4$
6. $\neg P \to (\neg Q \to \neg P)$ $A1$
7. $\neg P \to (P \to Q)$ $MP, 6, 5$

■

Lause 5.4.6. $\neg P, P \vdash Q$.

Todistus.

1. $\neg P$ pr.
2. $\neg P \to (\neg Q \to \neg P)$ A1
3. $\neg Q \to \neg P$ MP,1,2
4. $(\neg Q \to \neg P) \to (P \to Q)$ A3
5. $P \to Q$ MP,3,4
6. P pr.
7. Q MP,6,5

■

Lause 5.4.7. $\neg\neg P \vdash P$.

Todistus.

1.	$\neg\neg P$	$pr.$
2.	$\neg\neg P \to (\neg P \to \neg\neg\neg P)$	$Metat.2.3$
3.	$\neg P \to \neg\neg\neg P$	$MP, 1, 2$
4.	$(\neg P \to \neg\neg\neg P) \to (\neg\neg P \to P)$	$A3$
5.	$\neg\neg P \to P$	$MP, 3, 4$
6.	P	$MP, 1, 5$

■

Lauseessa (5.4.7) on käytetty hyväksi lausetta (?). Tämä on luvallista, sillä rivin 2 tilalle voidaan kirjoittaa lauseen (?) todistus.
Halutaan johtaa $\Delta \vdash P$. Jos on jo johdettu $\mathcal{P} \vdash Q$, missä $\mathcal{P} \in \Delta$, niin P:n Δ-päättelyssä voidaan kirjoittaa suoraan Q, kuten aksiooman tai premissin ollessa kyseessä. Kirjoittamalla Q:n tilalle Q:n Δ-päättely saadaan P:lle määritelmän (5.4.2) mukainen Δ-päättely.

Lause 5.4.8. $\vdash A$ *joss* $\emptyset \vdash A$.

Todistus. (1°) Olkoon $\vdash A$. Tällöin on olemassa A:n todistus $B_1, \ldots, B_n$, joka ei sisällä yhtään premissiä määritelmän (5.4.3) nojalla. Saman määritelmän nojalla tällainen jono on johto tyhjästä joukosta. Siis on olemassa tällainen johto eli $\emptyset \vdash A$.
(2°) Olkoon $\emptyset \vdash A$ eli on olemassa A:n johto $B_1, \ldots, B_n$ tyhjästä joukosta $\emptyset$. Koska $\emptyset$ on tyhjä, johto ei sisällä premissejä, ja se siis on määritelmän (5.4.3) nojalla A:n todistus. Siis $\vdash A$. ■
Seuraava lause on mielenkiintoinen, jos $\emptyset$ on ääretön. Jos silloin $\emptyset \vdash A$, niin tämä lause takaa, että on olemassa äärellinen joukko, mistä A on johdettavissa ja kääntäen.

Lause 5.4.9. $\Delta \vdash A$ *joss* Δ*:n jostakin äärellisestä osajoukosta* $\mathcal{P}$ *pätee* $\mathcal{P} \vdash A$.

Todistus. (1°) Olkoon $\Delta \vdash A$. Tällöin A:lla on johto Δ:sta, jota merkitsemme $B_1, \ldots, B_n$. Koska tämä jono on äärellinen (määr. (5.4.2)), se voi sisältää vain äärellisen määrän joukon Δ lauseita. Olkoon $\Delta^\circ = \Delta \cap \{B_1, \ldots, B_n\}$. Tällöin Δ°:n alkiot muodostavat A:n johdon Δ°:sta, koska $B_1, \ldots, B_n \vdash A$ eli $\Delta^\circ \vdash A$. Δ° on äärellinen, koska se koostuu alkioista $B_1, \ldots, B_n$, joita on äärellinen määrä, koska nämä muodostavat A:n deduktion Δ:sta. Siis, jos $\Delta \vdash A$, niin on olemassa Δ:n äärellinen osajoukko $\mathcal{P}$, josta pätee $\mathcal{P} \vdash A$.
(2°) Olkoon $\mathcal{P}$ äärellinen ja $\mathcal{P} \vdash A$. Olkoon lisäksi Δ sellainen, että se sisältää $\mathcal{P}$:n. Tällöin on olemassa A:n johto $B_1, \ldots, B_n$ $\mathcal{P}$:stä. Koska $\mathcal{P}$:n jokainen alkio on myös Δ:n alkio, niin määritelmän (5.4.2) nojalla $B_1 \ldots B_n$ on myös A:n johto Δ:sta, ts. $\Delta \vdash A$. ■
Tarkastellaan lauseita (5.3.11) ja (5.3.12). Edellinen saadaan jälkimäisestä siirtämällä ensin P ja sitten $\neg P$ symbolin $\vdash$ oikealle puolelle seuraavasti:

$$\begin{aligned} \neg P, P &\vdash Q \\ \neg P &\vdash P \to Q \\ &\vdash \neg P \to (P \to Q) \end{aligned}$$

Deduktiolause sanoo, että näin voidaan aina tehdä. Lauseen (5.3.12) todistus on lauseen (5.3.11) todistusta huomattavasti helpompi. Deduktioteoreema on hyvin hyödyllinen siksi, että sen avulla voidaan teoreeman todistus korvata premisseistä lähtevällä todistuksella eli johdolla. ■

Lause 5.4.10. ***(Deduktiolause)***. *Jos* $\Delta, P \vdash Q$*, niin* $\Delta \vdash P \to Q$.

Todistus. Todistus sivuutetaan. Mainittakoon kuitenkin, että deduktiolauseen todistuksessa tarvitaan vain aksioomia $A1$ ja $A2$ sekä päättelysääntöä MP. Deduktiolause on siis voimassa, vaikka kolmatta aksioomaa muutettaisiinkin. ■

Lause 5.4.11 (DT:n käänteisteoreema). *Jos* $\Delta \vdash P \to Q$*, niin* $\Delta, P \vdash Q$.

Todistus.

1.	P	$pr.$
	$\vdots$	
	Δ	$(P \to Q)$:n Δ-päättely
	$\vdots$	
2.	$P \to Q$	
3.	Q	$MP, 1, 2$

■

Esitämme vielä seuraavat lauseet.

Lause 5.4.12. *Jos* $A \in \Delta$*, niin* $\Delta \vdash A$.

Lause 5.4.13. *Jos* $\Delta \vdash A$*, niin* $\Delta \cup \mathcal{P} \vdash A$.

Lause 5.4.14. *Jos* $\Delta \vdash A$ *ja* $\mathcal{P}, A \vdash B$*, niin* $\Delta \cup \mathcal{P} \vdash B$.

Todistus. Todistukset harjoitustehtävinä. ■

Lause 5.4.15.

(a) $\vdash P \to P$,
(b) $\vdash \neg P \to (P \to Q)$,
(c) $\vdash \neg\neg P \to P$,
(d) $\vdash P \to \neg\neg P$,
(e) $\vdash (P \to Q) \to ((Q \to R) \to (P \to R))$,
(f) $\vdash (P \to Q) \to (\neg Q \to \neg P)$,
(g) $\vdash Q \to (\neg R \to \neg(Q \to R))$,
(h) $\vdash (R \to P) \to ((\neg R \to P) \to P)$.

Todistus. Kohdat (a) ja (b) on todistettu jo lauseissa (5.3.4) ja (5.3.11). Kohta (c) saadaan lauseesta (5.3.13) DT:llä. (d):n todistus on seuraava:

1.	$\neg\neg\neg P \to \neg P$	lause 5.4.15(c)
2.	$(\neg\neg\neg P \to \neg P) \to (P \to \neg\neg P)$	$A3$
3.	$P \to \neg\neg P$	$MP, 1, 2$

(e) DT:n nojalla riittää osoittaa, että $P \to Q$, $Q \to R$, $P \vdash R$.

1.	P	$pr.$
2.	$P \to Q$	$pr.$
3.	Q	$MP, 1, 2$
4.	$Q \to R$	$pr.$
5.	R	$MP, 3, 4$

(f) DT:n nojalla riittää osoittaa, että $P \to Q \vdash \neg Q \to \neg P$.

1.	$\neg\neg P \to P$	lause 5.4.15(c)
2.	$(\neg\neg P \to P) \to ((P \to Q) \to (\neg\neg P \to Q))$	lause 5.4.15(e)
3.	$(P \to Q) \to (\neg\neg P \to Q)$	$MP, 1, 2$
4.	$P \to Q$	$pr.$
5.	$\neg\neg P \to Q$	$MP, 3, 4$
6.	$(\neg\neg P \to Q) \to ((Q \to \neg\neg Q) \to (\neg\neg P \to \neg\neg Q))$	lause 5.4.15(e)
7.	$(Q \to \neg\neg Q) \to (\neg\neg P \to \neg\neg Q$	$MP, 5, 6$
8.	$Q \to \neg\neg Q$	lause 5.4.15(d)
9.	$\neg\neg P \to \neg\neg Q$	$MP, 8, 7$
10.	$(\neg\neg P \to \neg\neg Q) \to (\neg Q \to \neg P)$	$A3$
11.	$\neg Q \to \neg P$	$MP, 9, 10$

■

(g) DT:n nojalla riittää osoittaa, että $Q \vdash \neg R \to \neg(Q \to R)$.

1.	Q	$pr.$
2.	$Q \to R$	$pr.$
3.	R	$MP, 1, 2$
4.	$(Q \to R) \to R$	$DT, 2, 3$
5.	$(Q \to R) \to R) \to (\neg R \to \neg(Q \to R))$	lause 5.4.15(f)
6.	$\neg R \to \neg(Q \to R)$	$MP, 4, 5$

Todistuksen askeleessa 2 tehtiin lisäoletus $Q \to R$, josta päästiin askeleessa 4 eroon DT:n avulla. Ne lauseet, joissa lisäoletusta tarvitaan, on siirretty seuraavassa hiukan oikealle muista.
(h) Osoitetaan, että $R \to P \vdash (\neg R \to P) \to P$.

1.	$R \to P$	$pr.$
2.	$\quad \neg P$	$pr.$
3.	$\quad (R \to P) \to (\neg P \to \neg R)$	lause 5.4.15(f)
4.	$\quad \neg P \to \neg R$	$MP, 1, 3$
5.	$\quad \neg R$	$MP, 2, 4$
6.	$\quad \neg R \to (\neg P \to \neg(\neg R \to P))$	lause 5.4.15(g)
7.	$\quad \neg P \to \neg(\neg R \to P)$	$MP, 5, 6$
8.	$\quad \neg(\neg R \to P)$	$MP, 2, 7$
9.	$\neg P \to \neg(\neg R \to P)$	$DT, 2, 8$
10.	$(\neg P \to \neg(\neg R \to P)) \to ((\neg R \to P) \to P)$	$A3$
11.	$(\neg R \to P) \to P$	$MP, 9, 10$

Edellä mainitsimme *induktion lauseen pituuden suhteen.* Selvitimme siellä, kuinka osoitetaan se seikka, että $\mathcal{L}$:n kaikilla lauseilla on tietty ominaisuus. Tarkastelemme tässä erityisesti tapausta, jossa halutaan todistaa, että $\mathcal{L}$:n *teoreemoilla* on tietty ominaisuus φ. Tällöin riittää osoittaa, että

(1) $\varphi(A)$, jos A on aksiooma,
(2) jos A on päätelty MP:llä lauseista B ja C, ja jos $\varphi(B)$ ja $\varphi(C)$, niin myös $\varphi(A)$.

Tarkastelemme erästä lausejoukkoa, joka muodostaa ns. ***Suppesin-Genzenin päättelysääntöjärjestelmän***. Siihen luonnollisesti kuuluu myös Modus Ponens. Annamme nämä lauseet päättelykaavion muodossa ilman todistuksia. MP ei siis ole lause. Suppesin päättelysääntöjärjestelmä on joustavakäyttöinen, koska siinä esiintyvät myös muutkin kuin primitiiviset konnektiivit.

1. Modus (ponendo) ponens (MP)

$$\frac{P \to Q \quad P}{Q}$$

2. Modus (tollendo) tollens (TT)

$$\frac{P \to Q \quad \neg Q}{\neg P}$$

3. Modus (tollendo) ponens (TP)

$$\frac{P \vee Q \quad \neg P}{Q}$$

4. Vaihdantalait (KV)

$$\frac{P \wedge Q}{Q \wedge P}$$

5. (DV)

$$\frac{P \vee Q}{Q \vee P}$$

Tuonti- ja eliminointisäännöt:

6. KNT

$$\frac{P}{\neg\neg P}$$

7. KNE

$$\frac{\neg\neg P}{P}$$

8. KT

$$\frac{P \quad Q}{P \wedge Q}$$

9. KE

$$\frac{P \wedge Q}{P}$$

10. DT

$$\frac{P}{P \vee Q \quad Q \vee P}$$

11. DE

$$\frac{P \vee P}{P}$$

12. ET

$$\frac{P \to Q \quad Q \to P}{P \leftrightarrow Q}$$

13. EE

$$\frac{P \leftrightarrow Q}{P \to Q \quad Q \to P}$$

DeMorganin lait:

14. $DL1$
$$\frac{\neg P \wedge \neg Q}{\neg(P \vee Q)}$$

15. $DL2$
$$\frac{\neg(P \vee Q)}{\neg P \wedge \neg Q}$$

16. $DL3$
$$\frac{\neg P \vee \neg Q}{\neg(P \wedge Q)}$$

17. $DL4$
$$\frac{\neg(P \wedge Q)}{\neg P \vee \neg Q}$$

18. Hypoteettinen syllogismi (HS)
$$\frac{\begin{array}{l}P \to Q\\ Q \to R\end{array}}{P \to R}$$

19. Disjunktiivinen syllogismi (DS)
$$\frac{\begin{array}{l}P \vee Q\\ P \to R\\ Q \to S\end{array}}{R \vee S}$$

20. Ehdollisen todistuksen sääntö (DL)
$$\frac{\begin{array}{c}[P]\\ Q\end{array}}{P \to Q}$$

21. Epäsuoran todistuksen sääntö (ES)
$$\frac{\begin{array}{c}[\neg Q]\\ P \wedge \neg P\end{array}}{Q}$$

20. *Ehdollisen todistuksen sääntö* (DL): Jos lause Q voidaan johtaa lauseesta P ja joukosta premissejä, voidaan lause $P \Rightarrow Q$ johtaa pelkästään ko. premisseistä.
21. *Epäsuoran todistuksen sääntö* (ES): Jos premisseistä ja lauseesta $\neg Q$ voidaan johtaa looginen ristiriita, niin lause Q voidaan johtaa pelkästään ko. premisseistä.

Joitakin vihjeitä deduktion löytämiseksi

1. Jos deduktion konstruoinnissa on vaikeaa päästä alkuun tai se juuttuu paikalleen, yritetään epäsuoraa todistusta; Otetaan johdettavan lauseen negaatio apupremissiksi ja pyritään johtamaan ristiriita eli muotoa $P \wedge \neg P$ oleva lause. Jos tämä onnistuu, voidaan (ES):llä päätellä väite.

2. Jos väite on (moninkertainen) implikaatio, niin otetaan ko. implikaation etujäsen (etujäsenet) apupremisseiksi ja yritetään päätellä (sisimmän) implikaation takajäsen. Soveltamalla (DL):ää saadaan haluttu implikaatio (kun väite on moninkertainen implikaatio,

sovelletaan (DL):ää sopivassa järjestyksessä yhtä monta kertaa kuin implikaatiossa on nuolia).

Seuraavassa tarkastelemme formaalisten teorioiden eräitä keskeisiä käsitteitä sovittaen ne tässä $\mathcal{L}$:ään.

Konsistenssi (ristiriidattomuus)

Johdettavuuden käsitteen avulla voidaan käsitellä syntaktisesti lauseiden ja lausejoukkojen ristiriidattomuutta. Esimerkkejä inkonsistenteistä eli ristiriitaisista lausejoukoista ovat mm. $\Delta_1 = \{P, \neg P\}$ ja $\Delta_2 = \{P \to Q,\ P,\ \neg Q\}$. Näistä lausejoukoista voidaan johtaa ristiriita.

Lausejoukko Δ on ristiriitainen, joss $\Delta \vdash A$ ja $\Delta \vdash \neg A$. Lausejoukosta voidaan johtaa ristiriita, joss siitä voidaan johtaa *kaikki* lauseet. Täten siis lausejoukko Δ on konsistentti, jos jotakin lausetta ei voida siitä johtaa.

Määritelmä 5.4.16. *$\mathcal{L}$:n lausejoukko Δ on* konsistentti *$\mathcal{L}$:ssä, jos siinä on sellainen lause A, ettei $\Delta \vdash A$ päde. Lausejoukko on* inkonsistentti, *jos se ei ole konsistentti.*

Lause 5.4.17. *$\mathcal{L}$:n lausejoukko $\emptyset$ on inkonsistentti, joss on olemassa sellainen $\mathcal{L}$:n lause A, että $\Delta \vdash A$ja $\Delta \vdash \neg A$.*

Todistus. (i) Jos $\emptyset$ on inkonsistentti, niin määritelmän (5.4.16) nojalla ei ole olemassa yhtään lausetta, jota siitä ei voida johtaa. Tällöin on olemassa mm. sellainen A, että $\Delta \vdash A$ ja $\Delta \vdash \neg A$.
(ii) Olkoon A sellainen $\mathcal{L}$:n lause, että $\Delta \vdash A$ ja $\Delta \vdash \neg A$. Tällöin lauseen (5.3.12) nojalla $A, \neg A \vdash B$, jolloin B on mikä tahansa $\mathcal{L}$:n lause.
Koska $\Delta \vdash A$ ja $\Delta \vdash \neg A$ sekä $A, \neg A \vdash B$, niin lauseen (5.3.28) nojalla $\Delta \vdash B$. Tällöin määritelmän (5.4.16) nojalla Δ on inkonsistentti. ■

Esitämme joitakin konsistenssia koskevia tuloksia.

Lause 5.4.18. *$\mathcal{L}$:n lausejoukko Δ on konsistentti, joss jokainen $\mathcal{L}$:n äärellinen osajoukko on konsistentti.*

Lause 5.4.19. *$\Delta \vdash A$, joss $\Delta \cup \{\neg A\}$ on inkonsistentti.*

Lause (5.4.6) on Suppesin päättelysäännön RAA perustana.

Lause 5.4.20. *Jos Δ on konsistentti, niin kaikista $\mathcal{L}$:n lauseista A pätee, että joko $\Delta \cup \{A\}$ tai $\Delta \cup \{\neg A\}$ on konsistentti.*

Määritelmä 5.4.21. *$\mathcal{L}$:n lause Aon inkonsistentti, jos joukko $\{A\}$ on inkonsistentti.*

Lause 5.4.22. *$\mathcal{L}$:n lause A on inkonsistentti, joss $\vdash \neg A$.*

$\mathcal{L}$:n ristiriidattomuus, täydellisyys ja riippumattomuus

Ristiriidattomuudesta voidaan puhua monessa merkityksessä. Seuraavassa annamme neljä ristiriidattomuuden määritelmää.

Määritelmä 5.4.23. *1. Formaalinen kieli on* absoluuttisesti ristiriidaton, *jos sen jokainen lause ei ole teoreema.*

2. *Formaalinen kieli on* ristiriidaton tulkintaan nähden (sound, terve), *jos kielen jokainen teoreema on tautologia.*

3. *Formaalinen kieli on* kanonisesti ristiriidaton, *jos lauseen P ollessa tietty teoreema $\neg P$ ei ole teoreema.*

4. *Formaalinen kieli on* ristiriidaton negaatioon nähden, *jos kielessä ei ole sellaista lausetta Q, että $\vdash Q$ ja $\vdash \neg Q$.*

Seuraus 5.4.24. *Jos formaalinen kieli on ristiriidaton negaatioon nähden, niin se on kanonisesti ristiriidaton.*

Lause 5.4.25. *Edellä esitetty $\mathcal{L}$:n aksiomatisointi on ristiriidaton kaikissa määritelmän (5.4.23) merkityksissä (1)-(4).* ■

Todistus.

1. Osoitetaan ensin, että jokainen teoreema on tautologia, ts $\mathcal{L}$:n ristiriidattomuus tulkintaan nähden. Jokainen aksiooma $A1$, $A2$ ja $A3$ on tautologia (totea!). Päättelysääntö MP säilyttää tautologian, ts. jos $\models P$ ja $\models P \to Q$, niin $\models Q$. Todetaan tämä epäsuorasti. Jos Q ei olisi tautologia, niin Q saisi jollakin totuusarvojakelulla arvon E. Koska $P \to Q$ on tautologia, niin P saa tällä totuusarvojakelulla arvon E. Tällöin P ei olisi tautologia, mikä on vastoin oletusta. Koska siis MP säilyttää tautologian, niin jokainen teoreema on täten tautologia.

2. Jokainen lause ei ole tautologia, esim. atomilause p. Se ei voi olla teoreema, koska muuten se olisi määritelmän 5.4.23 kohdan (2) nojalla tautologia.

3. Oletetaan, että määritelmän 5.4.23 kohta (4) ei olisi voimassa, ts. olisi olemassa sellainen lause P, että $\vdash P$ ja $\vdash \neg P$. Lauseen (5.4.5) nojalla on $\vdash \neg P \to (P \to Q)$ olipa Q mikä lause tahansa. Siis saamme oletuksemme avulla deduktion

1.	$\neg P \to (P \to Q)$	lause 5.4.15(b)
2.	P	$ol.$
3.	$\neg P$	$ol.$
4.	$P \to Q$	$MP, 3, 1$
5.	Q	$MP, 2, 4$

   Siis $\vdash Q$, jolloin jokainen lause olisi teoreema. Tämä on vastoin määritelmän 5.4.23 kohtaa (1).

4. Määritelmän 5.4.23 kohta (3) seuraa kohdasta (4).

■

Täydellisyydestä puhutaan myös monessa mielessä. Tässä annamme kolme määritelmää täydellisyydelle.

Määritelmä 5.4.26.

1. Formaalinen kieli on *absoluuttisesti täydellinen*, jos kielen jokainen lause P on joko teoreema tai sen lisääminen aksioomaksi aiheuttaa sen, että kielen jokainen lause on teoreema.

2. Formaalinen kieli on *täydellinen tulkintaan nähden*, jos kielen jokainen tautologia on teoreema.

3. Formaalinen kieli on *täydellinen negaatioon nähden*, jos kielen jokaiselle lauseelle pätee, että se on teoreema tai sen negaatio on teoreema.

Lause 5.4.27. $\mathcal{L}$:n edellä esitetty aksiomatisointi ei ole absoluuttisesti täydellinen.

Todistus. Tarkastellaan $\mathcal{L}$:n atomilausetta p. Se ei ole teoreema, koska muuten se olisi metateoreeman (5.4.25) todistuksen mukaan tautologia. Lisätään p aksioomaksi. Jos $\mathcal{L}$ olisi absoluuttisesti täydellinen, niin p :stä voitaisiin johtaa mm. seuraava lause $\neg p$ eli $p \vdash \neg p$. Deduktioteoreeman nojalla on tällöin $\vdash p \rightarrow \neg p$. Koska metateoreeman (5.4.25) todistuksen mukaan jokainen teoreema on tautologia, niin $p \rightarrow \neg p$ on tautologia. Tämä on kuitenkin mahdotonta, sillä antamalla p :lle totuusarvo T saa lause $p \rightarrow \neg p$ totuusarvon E. ■
$\mathcal{L}$ on täydellinen tulkintaan nähden.

Lause 5.4.28. ($\mathcal{L}$:n täydellisyys tulkintaan nähden.) Jokainen tautologia on $\mathcal{L}$:n teoreema, ts. jos $\models P$, niin $\vdash P$.

Todistus. Lauseella on käänteinen teoreema. ■

Lause 5.4.29. (Terveys) Jokainen $\mathcal{L}$:n teoreema on tautologia, ts. jos $\vdash P$, niin $\models P$.

Lauseista (5.4.28) ja (5.4.29) saadaan *propositiologiikan päätulos*

$$\vdash P \Leftrightarrow \models P.$$

Lause 5.4.30. (Laajennettu täydellisyyslause). $\Delta \vdash P \leftrightarrow \Delta \models P$, missä Δ on lausejoukko.

5.5 Eräitä usein esiintyviä tehtävätyyppejä

1. Osoitettava lause P validiksi (invalidiksi).

   Tehtävä voidaan aina ratkaista totuustaulumenetelmällä. Se voidaan myös ratkaista todistamalla P $(\neg P)$ ja nojautumalla täydellisyystulokseen. Tehtävä voidaan johtaa myös distproof -menetelmällä.

2. Osoitettava, että $\Delta \models P$.

   Jos Δ on äärellinen, niin tehtävä ratkeaa totuustaulukkomenetelmällä. Myös muita edellisessä kohdassa esitettyjä menetelmiä voidaan soveltaa.

3. Osoitettava, että $\Delta \vdash P$.

   Tehtävä voidaan ratkaista deduktiivisesti tai käyttämälä em. semanttisia menetelmiä ja nojautumalla $\mathcal{L}$:n täydellisyyteen.

4. Osoitettava lausejoukko $\sum$ ristiriitaiseksi (ristiriidattomaksi).

   Tehtävä ratkaistaan joko johtamalla lausejoukosta $\sum$ muotoa $P \wedge \neg P$ oleva lause tai osoittamalla, ettei mikään totuusarvojakelu tee kaikkia $\sum$:n lauseita tosiksi, ja vetoamalla tämän jälkeen laajennettuun täydellisyyslauseeseen. Jos $\sum$ on äärellinen, voidaan $\sum$:n looginen luonne määrätä totuustaulumenetelmällä tutkimalla $\sum$:n lauseiden konjunktiota.

   $\sum$ osoitetaan ristiriidattomaksi etsimällä touusarvojakelu, joka toteuttaa $\sum$:n kaikki lauseet ja vetoamalla laajennettuun täydellisyyslauseeseen. *Lausejoukkoa ei voida osoittaa ristiriidattomaksi deduktion avulla.*

5. Osoitettava lause(joukko) $\sum$ toteutuvaksi (kumoutuvaksi).

   $\sum$ osoitetaan toteutuvaksi antamalla sellainen totuusarvojakelu, joka toteuttaa $\sum$:n kaikki lauseet. $\sum$ osoitetaan kumoutuvaksi antamalla sellainen totuusarvojakelu, joka tekee vähintään yhden $\sum$:n lauseista epätodeksi.

Esimerkki 5.5.1. Osoitettava lausejoukko
$\sum = \{\neg(C \vee D),\ B \rightarrow C,\ C \rightarrow D,\ \neg B\}$ ristiriidattomaksi.

1. $\neg B$ on tosi joss B on epätosi.
2. $B \rightarrow C$ on tosi B:n ollessa epätosi joss joko C on epätosi tai tosi. Valitaan C epätodeksi ja katsotaan mitä siitä seuraa.
3. $C \rightarrow D$ on tosi C:n ollessa epätosi joss joko D on epätosi tai tosi. Valitaan D epätodeksi.
4. Tällöin myös $\neg(C \vee D)$ on tosi.

Siis mm. malli $\mathcal{M} = \{A\}$ on $\sum$:n malli, joten laajennetun täydellisyyslauseen nojalla $\sum$ on ristiriidaton. Mallia $\mathcal{M} = \{A\}$ vastaa totuusarvojakelu, jossa A on tosi ja muut $\mathcal{L}$:n atomit epätosia.

5.6 Resoluutiomenetelmä

Havainnollistamme tässä yhteydessä *resoluutiomenetelmää* esimerkin avulla.

Resoluutiomenetelmää käytetään formaalisen logiikan soveltamisessa logiikkaohjelmaan.

Logiikkaohjelmointi liittyy mm. *automaattiseen teoreemojen todistamiseen*.

Logiikkaohjelmoinnin perusta:

- samaistus
- haku
- takaisinjäljitys

"Yhteinen nimittäjä": TEKOÄLY

Sovellusalue: ASIANTUNTIJAJÄRJESTELMÄT

Resoluutiomenetelmä on idealtaan yksinkertainen ja sen "mekanisoitavuusaste"on niin suuri, että menetelmä voidaan toteuttaa tehokkaasti tietokoneella.

Esimerkki 5.6.1. *Toteamus:* palkat eivät nouse.

Tutkitaan taloudellispoliittista tilannetta mahdollisen syyn selvittämiseksi. Havaitaan seuraavia seikkoja:

- *Jos palkat tai hinnat nousevat, tulee inflaatio.*
- *Jos inflaatio tulee, niin hallituksen on hillittävä sitä, tai kansa saa kärsiä.*
- *Jos kansa saa kärsiä, ministerit joutuvat epäsuosioon.*
- *Hallitus ei hillitse inflaatiota eivätkä ministerit joudu epäsuosioon.*

Voidaanko tästä vetää johtopäätös: PALKAT EIVÄT NOUSE.

Tutkimme probleemaa ensin klassisen logiikan keinoin "perinteellisellä"tavalla ja sen jälkeen katsomme, löytyisikö tapauksen selvittämiseen "mekaanisempi"keino, jota voitaisiin periaatteessa samalla tavalla soveltaa yleisesti mihin tahansa vastaavanlaisiin loogisiin tilannekuvauksiin.

Formalisoidaan luonnollisella kielellä esitetty tilannekuvaus:

P = palkat nousevat

H = hinnat nousevat

F = inflaatio tulee

L = hallituksen on hillittävä inflaatiota

K = kansa saa kärsiä

M = ministerit joutuvat epäsuosioon

Tilannekuvaus formaalisesti:

$$\text{Premissit} : \begin{cases} 1. P \vee H \rightarrow T \\ 2. F \rightarrow L \vee K \\ 3. K \rightarrow M \\ 4. \neg L \wedge \neg M \end{cases}$$

$$\text{Johto}: \begin{cases} 5. & \neg M & \text{KE, 4} \\ 6. & \neg L & \text{KE, 4} \\ 7. & \neg K & \text{TT, 3,5} \\ 8. & \neg L \wedge \neg K & \text{KT, 6,7} \\ 9. & \neg(L \vee K) & \text{DM, 8} \\ 10. & \neg F & \text{TT, 2,9} \\ 11. & \neg(P \vee H) & \text{TT, 1, 10} \\ 12. & \neg P \wedge \neg H & \text{DM, 11} \\ 13. & \neg P & \text{KE, 12} \end{cases}$$

Siis *tavoitelause* $\neg P$ seuraa loogisesti premisseistä.

Ohjelmoinnillisia hankaluuksia:

- Kaavoilta puuttuu tietty yhtenäinen esitysmuoto.
- Päättelysäännöillä on suuri lukumäärästä ja muodosta johtuva kirjavuus.

Pulman ratkaisu:

- Muutetaan tilannekuvauksen lauseet ns. *disjunktiomuotoon*, jolloin koko tilannekuvaus voidaan esittää *konjunktiivisessa normaalimuodossa*.
- Tällöin kukin lause voidaan esittää ns. *Hornin klausuulina* tai ns. *Kowalski-muodossa*:

propositio	Hornin klausuuli	Kowalski-muoto	
$K \vee \neg L_1 \vee \ldots \vee \neg L_n$	$K_1, \neg L_1, \ldots, L_n$	$K \leftarrow L_1 \vee \ldots \vee L_n$	ohjelmalause
K ($\Leftrightarrow$ tosi $\rightarrow K$)	K	$K \leftarrow$	fakta
$\neg L_1 \vee \ldots \vee \neg L_n$	$\neg L_1, \ldots, \neg L_n$	$\leftarrow L_1, \ldots, L_n$	tavoitelause

- Hyödynnetään *epäsuoran todistuksen*mkaavamaista periaatetta.

Tuloksena on ns. **resoluutiomenetelmä**. Epäsuoran todistuksen periaatteen mukaiseswti lisätään tilannekuvaukseen alkuperäisen tavoitelauseen negaatio ja tutkitaan, onko näin muodostettu lausejoukko loogisesti ristiriitainen. Jos näin on, menetelmä tuottaa tyhjän lauseen (= ristiriidan, loogisen epätoden), merk. $\square$.

Esimerkkitehtävän logiikkaohjelma:

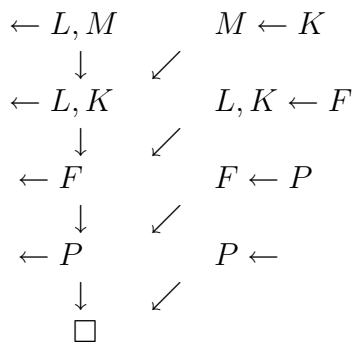
Hornin klausuuleina:

$$\mathbf{P} = \{\{\neg P, F\}, \{\neg H, F\}, \{\neg F, L, K\}, \{\neg K, M\}, \{\neg L\}, \{\neg M\}, \{P\}\},$$

Kowalski-muodossa:

$$\mathbf{P} = \{F \leftarrow P; F \leftarrow H; L, K \leftarrow F; M \leftarrow K; \leftarrow L; \leftarrow M; P \leftarrow\}.$$

Logiikkaohjelma **P** tuottaa seuraavan *resoluutiorefutaation*:



Tuloksena os siis tyhjä lause $\square$, joten $\neg P$ on tilannekuvauksen premissien looginen seuraus.

6 PREDIKAATTILOGIIKKA

6.1 Syntaksi

Motivoiva esimerkki, joka osoittaa predikaattilogiikan tarpeellisuuden:

Esimerkki 6.1.1.

Kaikki linnut ovat eläimiä.
Jokin varis on lintu.
Jokin varis on eläin.

Päättelyn formalisointi $\mathcal{L}$:ssä on muotoa

A
B
C

Määritelmä 6.1.2. *Predikaattilogiikan P aakkosto on seuraava:*

$v_1, v_2, \ldots, v_n, \ldots$	*muuttujat*
$c_1, c_2, \ldots, c_n, \ldots$	*(nimi)vakiot*
$P^i_j, \ \ i, j = 1, 2, \ldots, n, \ldots$	*predikaattisymbolit (i= paikkaluku, j=järj.nro)*
$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$	*konnektiivit*
$=$	*identiteettisymboli*
$\exists$	*eksistenssikvanttori*
$\forall$	*universaalikvanttori*
$(,)$	*sulut ja pilkku*

SOPIMUS: Otamme käyttöön seuraavat metamuuttujat:

$x, y, z, \ldots$	viittaavat muuttujiin,
$a, b, c, \ldots$	viittaavat vakioihin,
$A, B, C, \ldots, P, Q, R$	viittaavat predikaattisymboleihin,
$t, t_i, \ldots, t_j, \ldots$	viittaavat yleisesti termeihin.

LUONNEHDINTA:

Muuttujat: Luonnollisessa kielessä muuttujia vastaavat pronominit ja niiden kaltaiset ilmaisut.
Kun muuttujien paikalle sijoitetaan ilmauksia, jotka nimeävät yksilöitä, saadaan joko tosi tai epätosi lause.

Vakiosymbolit: Vakiosymboleja käytetään vastaamaan ilmauksia, jotka nimeävät jonkun tunnetun yksilön.

$t_i = t_j$, $(1 \leq i \leq n, 1 \leq j \leq n)$ ja $P(t_1, \ldots, t_n)$, ovat atomeja (eli atomikaavoja). Muita atomeja ei ole.

SOPIMUS: Kaavoihin viittaavina metamuuttujina käytetään pieniä kreikkalaisia kirjaimia α, β, ..., φ, ψ, ... ja kaavajoukkoihin viitataan isoilla kreikkalaisilla kirjaimilla $\Phi, \Psi, \ldots$. Merkintä

$$\varphi(v_i, \ldots, v_n)$$

tarkoittaa kaavaa,jossa muuttujat $v_1, \ldots, v_n$ esiintyvät *vapaina* (ks. määritelmä 6.1.7), jossa määritellään *vapaa muuttuja*).

Määritelmä 6.1.3. *Atomit ovat kaavoja. Jos φ ja ψ ovat kaavoja, niin myös $\varphi, (\varphi \wedge \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi), \exists x\varphi$ ja $\forall x\psi$ ovat kaavoja. Muunlaisia kaavoja ei ole.*
Kukin kaava voidaan esittää yksikäsitteisen rakennepuun avulla.

Esimerkki 6.1.4. *Atomikaavoja*
KUVA

Määritelmä 6.1.5. *Kun kaava $\exists x\varphi$ tai $\forall x\varphi$ on muodostettu määritelmän 7.5.1 avulla φ:stä, sanotaan kaavaa φ kvanttorin $\exists x$ tai $\forall x$* laajuudeksi *eli* vaikutusalueeksi *(scope) esiintyipä $\exists x\varphi$ tai $\forall x\varphi$ osana pidempää kaavaa tai ei.*

Esimerkki 6.1.6. *Nuolet liittävät kunkin kvanttorin kuhunkin esiintymään sen laajuuden: KUVA*

Määritelmä 6.1.7. *Muuttuja x esiintyy kaavassa ψ sidottuna, joss x esiintyy ψ:ssä kvanttorin $\exists x$ tai $\forall x$ laajuudessa. Myös ilmauksissa $\exists x$ ja $\forall x$ esiintyvää muuttujaa x sanotaan sidotuksi. Jos kaavassa ψ esiintyvä muuttuja x ei ole sidottu, se on vapaa.*

Määritelmä 6.1.8. *Kaava, jossa ei esiinny vapaita muuttujia, on suljettu kaava eli lause.*

Esimerkki 6.1.9. *Mitkään pommit eivät ole vaarallisia.*
$P(x) \rightarrow x$ *on pommi.*
$V(x) \rightarrow x$ *on vaarallinen.*

$\forall x(P(x) \rightarrow \neg V(x))$ *tai* $\neg\exists x(P(x) \wedge V(x))$
Nämä kaavat voidaan lukea: "Kaikista olioista x pätee, että jos x on pommi, niin x ei ole vaarallinen", *ja* "Ei ole niin, että on olemassa vaarallisia pommeja". *Nämä lauseet kuvaavat selvästi sammaa asiaintilaa, joten ne molemmat ovat lauseen* "Mitkään pommit eivät ole vaarallisia" *formalisointeja. Saadut perdikaattilogiikan ilmaisut voidaan osoittaa olevan loogisesti ekvivalentteja.*

Esimerkki 6.1.10. *Kaikki sitruunat eivät ole happamia.*

Tulkinta:	$S(x) \rightarrow x$ *on sitruuna.*
	$H(x) \rightarrow x$ *on hapan.*
Formalisointi:	$\neg\forall x(S(x) \rightarrow H(x))$,
tai yhtäpitävästi	$\exists x(S(x) \wedge \neg(H(x))$.

Esimerkki 6.1.11. *Kukaan Marxin kannattaja ei pidä kenestäkään positivistista.*

Tulkinta:	$M(x) \rightarrow x$ *on Marxin kannattaja.*
	$P(x) \rightarrow x$ *on positivisti.*
	$R(x, y) \rightarrow x$ *pitää y:stä.*
Formalisointi:	$\forall(M(x) \rightarrow \forall yP(y) \rightarrow \neg R(x, y)))$,
tai yhtäpitävästi	$\forall x\forall y(M(x) \wedge P(y) \rightarrow \neg(R(x, y))$.

Lause ”Kaikki oliot ovat hyviä” on formalisoituna $\forall x H(x)$. Tämä tarkoittaa samaa kuin ”Ei ole olemassa ei-hyviä olioita”, mikä on formalisoituna $\neg\exists x \neg H(x)$.
Kvanttoreilla on seuraava yhteys:

$$\forall x\varphi \Leftrightarrow_{df} \neg\exists x\neg\varphi.$$

Kaksoisnegaation eliminointisääntö $\Rightarrow$

$$\begin{aligned}\neg\forall x\varphi &\Leftrightarrow \exists x\neg\varphi\\ \neg\forall x\neg\varphi &\Leftrightarrow \exists x\varphi\\ \forall x\neg\varphi &\Leftrightarrow \exists x\varphi\end{aligned}$$

Esimerkki 6.1.12.

$$\begin{aligned}\neg\forall x S(x) \rightarrow H(x))\\ \exists x\neg(S(x) \rightarrow H(x))\\ \exists x\neg\neg(S(x) \wedge \neg H(x))\\ \exists x(S(x) \wedge \neg H(x))\end{aligned}$$

Rajoitetut kvanttorit $\forall_H$ ja $\exists_H$

Määritelmä 6.1.13.

$$\begin{aligned}\exists_H x\varphi(x) &\Leftrightarrow_{df} \exists x(H(x) \wedge \varphi(x))\\ \forall_H x\varphi(x) &\Leftrightarrow_{df} \forall x(H(x) \rightarrow \varphi(x))\end{aligned}$$

Rajoitettuja kvanttoreita käytetään usein muodossa

$$\begin{aligned}\exists x \in H : \varphi(x)\\ \forall x \in H : \varphi(x)\end{aligned}$$

Esimerkki 6.1.14.

$$\begin{aligned}\forall_V\ x\ E(x)\\ \forall\ x \in V : E(x)\end{aligned}$$

Formalisoinnin kulmakiviä:

$$\forall x(I(x) \rightarrow P(x)) \tag{6.1}$$
$$\forall x(I(x) \wedge P(x)) \tag{6.2}$$
$$\exists x(I(x) \wedge P(x)) \tag{6.3}$$
$$\exists x(I(x) \rightarrow P(x)) \tag{6.4}$$

$$\begin{aligned}\forall x(I(x) \rightarrow P(x)) &\equiv \neg\exists x\neg(I(x) \rightarrow P(x)) \equiv \neg\exists x\neg(\neg I(x) \vee P(x)\\ &\equiv \neg\exists x(I(x) \vee \neg P(x))\end{aligned}$$

Määritelmä 6.1.15. $\exists!$ *On olemassa täsmälleen yksi.*

$$\exists! x\varphi(X) \Leftrightarrow_{df} \exists x\varphi(x) \wedge \forall x\forall y(\varphi(x) \wedge \varphi(y) \rightarrow x = y(x \equiv y))$$

7 BOOLEN ALGEBROISTA

7.1 Yleistä taustaa

Boolen algebrat ovat hyödyllinen apuväline mm. tietotekniikassa, mutta ne tarjoavat myös hyvän esimerkin algebrallisista struktuureista, joilla on keskeinen merkitys matematiikassa.
Tämän logiikan algebralisoinnin tutkimuksen pani alulle ja kehitti edelleen *George Boole* (1815–1864), englantilainen loogikka ja matemaatikko. Teoksessaan ”The Mathematical Analysis of Logic” (1847) Boole ensimmäisenä sovelsi matemaattisia menetelmiä logiikkaan, minkä nojalla häntä pidetään yhtenä nykyaikaisen logiikan perustajista. Pääteoksessaan ”The Laws of Thought” (1854) Boole kehitti ajatuksiaan edelleen. Syntyi joukkoja käsittelevä matemaattinen teoria. Tätä joukkoja käsittelevää logiikan osaa, luokkakalkyylia, nimitetään kehittäjänsä mukaan *Boolen algebraksi*.

7.2 Operaatioista

Operaatioita on matematiikassa monenlaisia. Niiden eräs luokitteluperusta on se, kuinka monipaikkainen operaatio on. Vastaavasti, kuten esim. relaatioillakin, on olemassa mm. 1-paikkaisia, 2-paikkaisia, . . ., n-paikkaisia operaatioita. Määrittelemme operaation yleisesti seuraavalla tavalla.

Määritelmä 7.2.1. *n-paikkainen operaatio $\mathcal{O}(n = 0, 1, 2, \ldots)$ joukossa $S \neq \emptyset$ on kuvaus, joka liittää jokaiseen järjestettyyn n-jonoon $(a_1, \ldots, a_n)$, $a_i \in S$, $i = 1, 2, \ldots, n$, yksikäsitteisen S:n alkion, ts.*

$$\mathcal{O} : S^n \to S$$

Huom. Kun $n = 1$, on järjestetty n-jono S:n yksittäinen alkio. Kun $n = 0$, sovimme, että järjestetty n-jono on tyhjä.
Määritelmän mukaan *nollapaikkainen operaatio* joukossa $S \neq \emptyset$ on kuvaus

$$S^0 : \{\emptyset\} \to S$$

Tämä operaatio kiinnittää vakion joukossa S (se on operaation arvo $\emptyset$:lle).
Yksipaikkainen (eli *unaarinen*) *operaatio* joukossa $S \neq \emptyset$ on kuvaus

$$S^1 : S \to S$$

Esimerkki 7.2.2. *Itseisarvo $\| : \mathbb{R} \to \mathbb{R}$ on yksipaikkainen operaatio. Yleensä merkitään $\|(x) = |x|$.* Kaksipaikkainen *(eli* binäärinen*)* operaatio *joukossa $S \neq \emptyset$ on kuvaus*

$$S^2 : S \times S \to S$$

Esimerkki 7.2.3. *Operaatio $+$ on $\mathbb{Z}$:n binäärinen operaatio. Mm. $2, 3 \in \mathbb{Z}$, $+(2, 3) = 2 + 3 = 5 \in \mathbb{Z}$. Operaatio $+$ ei ole joukon $S = \{0, 1, 2\}$ binäärinen operaatio, sillä $2 + 2 = 4 \notin S$.*

Binääristä operaatiota havainnollistetaan joskus *operaatiotaulun* avulla, mikäli joukko, missä operaatio on määritelty, on äärellinen.

Esimerkki 7.2.4. *Modulaarinen yhteenlasku* $+(\mathrm{mod}\,3)$ *on binäärinen operaatio joukossa* $S = \{0, 1, 2\}$.

$+(\mathrm{mod}\,3)$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Huom. Jos $\mathcal{O}$ on joukon $S \neq \emptyset$ operaatio (eli operaatio joukossa S), sanotaan, että S on *suljettu* operaation $\mathcal{O}$ suhteen.
Joukon $S \neq \emptyset$ binäärinen operaatio $\circ$ (ts. $\forall a, b \in S \Rightarrow a \circ b \in S$) on

(a) *kommutatiivinen,* joss

$$\forall x\, \forall y \quad (x, y \in S \rightarrow x \circ y = y \circ x)$$

eli

$$x \circ y = y \circ x,\ \forall x, y \in S$$

(b) *assosiatiivinen,* joss

$$\forall x\, \forall y\, \forall z \quad (x, y, z \in S \rightarrow (x \circ y) \circ z = x \circ (y \circ z))$$

eli

$$(x \circ y) \circ z = x \circ (y \circ z),\ \forall x, y, z \in S$$

Joukon S alkio u on *identiteettialkio* (eli *ykkösalkio*) S:n binäärisen operaation $\circ$ suhteen, jos

$$\forall x \quad (x \in S \rightarrow u \circ x = x \circ u = x)$$

eli

$$u \circ x = x \circ u = x,\ \forall x \in S.$$

Esimerkki 7.2.5. *(a) Yhteenlasku ja kertolasku ovat kommutatiivisia binäärisiä operaatioita* $\mathbb{R}$*:ssä.*

(b) Yhteenlasku ja kertolasku ovat myös assosiatiivisia binäärisiä operaatioita $\mathbb{R}$*:ssä.*

Esimerkki 7.2.6. *Olkoon* $A = \{a, b, c, d, e\}$ *ja* $\circ$ *oheisen operaatiotaulun mukainen binäärinen operaatio* A*:ssa.*

$\circ$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

Operaatio $\circ$ on kommutatiivinen A:ssa. Helposti todetaan, että $\circ$ on myös assosiatiivinen A:ssa. Taulusta havaitsemme, että

$$(b \circ c) \circ d = d \circ d = b \quad \textit{ja} \quad b \circ (c \circ d) = b \circ a = b$$
$$(d \circ e) \circ d = c \circ d = a \quad \textit{ja} \quad d \circ (e \circ d) = d \circ c = a$$

jne. A:n identiteettialkio operaation $\circ$ suhteen on a. Voimme todeta, että a on ainoa identiteettialkio.

Esimerkki 7.2.7. *Rationaalilukujen joukon $\mathbb{Q}$ identiteettialkio yhteenlaskun suhteen on 0, koska $0 + x = x + 0 = x, \forall x \in \mathbb{Q}$. Joukolla $\mathbb{Q}$ ei ole muita identiteettialkioita ko. operaatioiden suhteen.*

Voidaan todistaa, että yleisesti pätee seuraava

Lause 7.2.8. *Jos joukolla on identiteettialkio annetun operaation suhteen, se on yksikäsitteinen.*

7.3 Boolen algebran määrittely ja perusominaisuudet

Boolen algebran, lyh. BA, muodostaa joukko alkioita $a, b, c, \ldots$, jotka toteuttavat tietyt aksioomat. BA:n spesifioi yleensä sen muodostavien alkioiden joukko, sekä tässä joukossa määritellyt operaatiot, joista kaksi on binäärisiä operaatioita ja yksi yksipaikkainen operaatio. Lisäksi BA:ta symbolisoivaan merkkijonoon otetaan usein mukaan myös binääristen operaatioiden identiteettialkiot. BA:n muodostavalla joukolla on tiettyjä vaatimuksia. Erityisesti ko. joukon on oltava suljettu BA:n muodostavien operaatioiden suhteen. Seuraava määritelmä aksiomatisoi yleisesti BA:n.

Määritelmä 7.3.1. *Olkoot $\wedge$ (*kohtaus*) ja $\vee$ (*yhdiste*) sellaisia binäärisiä operaatioita ja $'$ (*komplementti*) sellainen yksipaikkainen operaatio joukossa $B(\neq \emptyset)$ ja olkoot alkiot $\mathbf{0}$ ja $\mathbf{1}$ joukon B sellaisia alkioita, että seuraavat aksioomat ovat voimassa:*

- *(BA1) $\wedge$ ja $\vee$ ovat kommutatiivisia, ts, $\forall x, y \in B, x \vee y = y \vee x$ ja $x \wedge y = y \wedge x$*
- *(BA2) $\forall x \in B, x \vee \mathbf{0} = x$ ja $x \wedge \mathbf{1} = x$ eli $\mathbf{0}$ ja $\mathbf{1}$ ovat vastaavasti identiteettialkioita operaatioiden $\vee$ ja $\wedge$ suhteen.*
- *(BA3) Operaatiot $\wedge$ ja $\vee$ ovat distributiivisia, ts.*

$$\forall x, y, z \in B,\ x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

- *(BA4) Jokaista alkiota $x \in B$ kohti on olemassa sellainen alkio $x' \in B$, että $x \vee x' = 1$ ja $x \wedge x' = 0$.*
- *(BA5) B:n alkioille $\mathbf{0}$ ja $\mathbf{1}$ pätee $\mathbf{0} \neq \mathbf{1}$.*

Tällöin joukko B yhdessä mainittujen operaatioiden kanssa muodostaa Boolen algebran $\mathcal{B} = (B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$.

Esimerkki 7.3.2. *$\mathcal{B}_0 = (\{\emptyset, \{\emptyset\}\}, \cap, \cup, {}^c, \emptyset, \{\emptyset\})$ on kahden alkion $\emptyset$ ja $\{\emptyset\}$ muodostama BA, missä $B = \{\emptyset, \{\emptyset\}\}$, $\wedge = \cap$, $\vee = \cup$, $' = {}^c$, $\mathbf{0} = \emptyset$ ja $\mathbf{1} = \{\emptyset\}$. $\mathcal{B}_0$:n osoittamiseksi BA:ksi on ensin todettava, että $\cap$, $\cup$ ja ^{c} ovat operaatioita joukossa $\{\emptyset, \{\emptyset\}\}$.*

(1°) $\emptyset \cap \{\emptyset\} = \emptyset \in B$,

(2°) $\emptyset \cup \{\emptyset\} = \{\emptyset\} \in B$

(3°) $\emptyset^c = \{\emptyset\} \in B$ *ja* $\{\emptyset\}^c = \emptyset \in B$.

Siis ko. operaatiot ovat B:n operaatioita. Tämän jälkeen on osoitettava, että $\mathcal{B}_0$ toteuttaa BA:n määritelmän aksioomat. Kuten joukko-opista tiedetään, ovat operaatiot $\cap$ ja $\cup$ kommutatiivisia. Siis (BA1) on voimassa. Kohtien (1°) ja (2°) nojalla (BA2) on voimassa, ja kohdan (3°) nojalla (BA4) on voimassa. Joukko-opista on tuttua, että $\cap$ ja $\cup$ ovat distributiivisia. Siis (BA3) on voimassa. Selvästi $\emptyset \neq \{\emptyset\}$ on joukko-opin nojalla voimassa. Siis $\mathcal{B}$ on BA.

Esimerkki 7.3.3. *$\mathcal{B}_A(\mathcal{P}(A), \cap, \cup, {}^c, \emptyset, A), A \neq \emptyset$, on BA. Operaatiot $\cap$, $\cup$ ja ^{c} ovat joukko-opillisina operaatioina A:n osajoukkojen joukon $\mathcal{P}(A)$ operaatioita. $\mathcal{B}_A$:n osoittamiseksi BA:ksi on todettava, että se toteuttaa BA:n aksioomat. (BA1) ja (BA3) ovat joukko-opin nojalla voimassa. $C \cup \emptyset = C$ ja $C \cap \emptyset = C$ kaikille $C \subset A$ eli $C \in \mathcal{P}(A)$, joten (BA4) on voimassa. $\mathcal{B}_A$:n konstruktiossa oletettiin, että $A \neq \emptyset$, joten (BA5) on voimassa. Esimerkin 7.3.2 tapaus on erikoistapaus $\mathcal{B}_A$:sta. Siinä valittiin $A = \{\emptyset\}$. Jos sallimme tapauksen $A = \emptyset$, olisi $= = \emptyset = A\mathbf{1}$, joten (BA5) ei olisi voimassa.*

Esimerkki 7.3.4. *Olkoon B niiden positiivisten kokonaislukujen joukko, jotka sisältyvät tasan lukuun 70, ts. ovat luvun 70 tekijöitä. Tällöin b on joukko*

$$B = \{1, 2, 5, 7, 10, 14, 35, 70\}$$

Tällöin $(B, \text{ syt}, \text{pyj}, \ 70/\cdot, 1, 70)$ on BA. Esim. $\text{syt}(5, 14) = 70$, $5' = 70/5 = 14$ jne. Selvästi syt, pyj ja $70/\cdot$ ovat B:n operaatioita. Myös BA:n aksioomien voimassaolo voidaan todeta ko. systeemille. Tässä tarvitaan syt:n ja pyj:n ominaisuuksia.

Esimerkki 7.3.5. *Kun BA:n aksioomissa identiteetti '=' korvataan loogisella ekvivalenssilla '$\Leftrightarrow$', niin $\mathcal{B}_L = (B, \wedge, \vee, \neg, e, t)$, missä $B = \{e, t\}$, on BA. Siis propositiologiikka $\mathbb{L}$ muodostaa BA:n konjuktion, disjunktion ja negaation suhteen. $\mathbb{L}$:n totuusmääritelmien nojalla $\wedge, \vee$ ja $\neg$ ovat totuusarvojen joukon B operaatioita. $\wedge, \vee, \neg$:n ominaisuuksien nojalla $\vee$ ja $\wedge$ ovat sekä kommutatiivisia että distributiivisia, joten (BA1) ja (BA3) ovat voimassa. Konjuktion ja disjunktion totuusmääritelmien nojalla (BA2) on voimassa, samoin (BA4). Koska $e \neq t$, on (BA5) voimassa.*
Koska tarkkaanottaen esim. $\mathbb{L}$:n lauseet $\alpha \wedge \beta$ ja $\beta \wedge \alpha$ eivät ole identtiset vaan loogisesti ekvivalentit, on em. vaihto aksioomissa suoritettava. Lisäksi nolla-alkioksi e voidaan valita mikä tahansa muotoa $\alpha \wedge \neg\alpha$ oleva $\mathbb{L}$:n lause ja ykkösalkioksi t mikä tahansa muotoa $\alpha \vee \neg\alpha$ oleva $\mathbb{L}$:n lause. Jos haluamme säilyttää identiteettisymbolin tavallisen merkityksen, meidän on meneteltävä seuraavasti. Merkitään $[\alpha]$:lla kaikkia niitä $\mathbb{L}$:n lauseita, jotka ovat loogisesti ekvivalentteja lauseen α kanssa, ts. o$[\alpha]$ on α:n määräämä ekvivalenssiluokka loogisen ekvivalenssin suhteen. Täten on selvää, että

(i) $[\alpha] = [\beta]$, *joss* $\alpha \Leftrightarrow \beta$*;*

(ii) $[\alpha] \neq [\beta] \Rightarrow [\alpha] \cap [\beta] = \emptyset$*.*

Jos K_1 *ja* K_2 *ovat* $\mathbb{L}$*:n lauseiden eo:n kaltaisia ekvivalenssiluokkia, niin jos* $\alpha_1, \beta_1 \in K_1$ *ja* $\alpha_2, \beta_2 \in K_2$*, niin* $\alpha_1 \wedge \alpha_2$ *on loogisesti ekvivalentti lauseen* $\beta_1 \wedge \beta_2$ *kanssa.* $\alpha_1 \vee \alpha_2$ *on loogisesti ekvivalentti lauseen* $\beta_1 \vee \beta_2$ *kanssa, ja* $\neg\alpha_1$ *on loogisesti ekvivalentti lauseen* $\neg\beta_1$ *kanssa. Siis, kun otamme mielivaltaisen lauseen* $\xi_1 \in K_1$ *ja mielivaltaisen lauseen* $\xi_2 \in K_2$*, voimme määritellä identiteetit* $K_1 \wedge K_2 = [\xi_1 \wedge \xi_2]$, $K_1 \vee K_2 = [\xi_1 \vee \xi_2]$ *ja* $K_1' = [\neg\xi_1]$*. Jos* B *on eo:n kaltaisten ekvivalenssiluokkien joukko,* $e = [\alpha \wedge \neg\alpha]$ *ja* $t = [\alpha \vee \neg\alpha]$*, niin* $(B, \wedge, \vee, \neg, e, t)$ *on BA. Aksioomien (BA1)–(BA5) voimassaolon toteaminen johtaa* $\mathbb{L}$*:n tunnettuihin ominaisuuksiin. Esim. (BA1):n voimassaolon toteamiseksi tarkastelemme ekvivalenssiluokkia* K_1 *ja* K_2*, jolloin valitsemme mielivaltaiset lauseet* $\xi_1 \in K_1$ *ja* $\xi_2 \in K_2$*. Tällöin* $K_1 \vee K_2 = [\xi_1 \vee \xi_2]$*. Koska* $[\xi_1 \vee \xi_2] \Leftrightarrow [\xi_2 \vee \xi_1]$*, on* $[\xi_1 \vee \xi_2] = [\xi_2 \vee \xi_1] = K_2 \vee K_1$*, jolloin* $K_1 \vee K_2 = K_2 \vee K_1$*. Siis jos tarkastelemme* $\mathbb{L}$*:n lauseiden sijasta ko. lauseiden määräämiä ekvivalenssiluokkia, voidaan BA:n aksioomissa säilyttää identiteetti '=' sen normaalissa merkityksessä.*

Operaatioita $\wedge$ ja $\vee$ kutsutaan vastaavasti *suurimmaksi alarajaksi* ja *pienimmäksi ylärajaksi* (ks. lähemmin kappale 7.4), jolloin myös usein merkitään

$$x \wedge y = \inf\{c, y\} \quad \text{(infimum)}$$

ja

$$x \vee y = \sup\{x, y\} \quad \text{(supremum)}$$

Vastaavasti voidaan merkitä

$$\bigwedge_{i=1}^{n} x_i = \inf\{x_1, x_2, \ldots, x_n\}$$

ja

$$\bigvee_{i=1}^{n} x_i = \sup\{x_1, x_2, \ldots, x_n\}.$$

Voi olla myös $n = \infty$.
Operaatioita $\wedge$ ja $\vee$ kutsutaan lyhemmillä nimillä *kohtaus* (engl. *meet*) ja *yhdiste* (engl. *join*), kuten määritelmässä 7.3.1 tehtiin. Operaatiota $'$ kutsutaan *komplementiksi*, ts. x' on x:n komplementti. Identiteettialkioita $\mathbf{0}$ ja $\mathbf{1}$ kutsutaan vastaavasti *nolla-alkioksi* ja *ykkösalkioksi*. Näitä ei kuitenkaan pidä sekoittaa lukuihin 0 ja 1.
Yhdistämällä joukon B alkioita operaatioilla $\wedge, \vee$ ja $'$ saadaan Boolen algebran $\mathcal{B} = (B, \wedge, \vee, ', 0, 1)$ *ilmaisuja* (ns. *Boolen ilmaisuja*). ■

Lause 7.3.6. *(Komplementin yksikäsitteisyys). Olkoon* $(B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$ *BA ja* $x, y \in B$*. Jos* $x \vee y = \mathbf{1}$ *ja* $x \wedge y = \mathbf{0}$*, niin* $y = x'$*.*

Todistus. (1°)

$$\begin{array}{rcll} y & = & y \vee \mathbf{0} & BA2 \\ & = & y \vee (x \wedge x') & BA4 \\ & = & (y \vee x) \wedge (y \vee x') & BA3 \\ & = & (x \vee y) \wedge (y \vee x') & BA1 \\ & = & \mathbf{1} \wedge (y \vee x') & \text{oletus} \\ & = & (y \vee x') \wedge \mathbf{1} & BA1 \\ & = & y \vee x' & BA2 \end{array}$$

(2°)

$$\begin{array}{rcll} x' & = & x' \vee \mathbf{0} & BA2 \\ & = & x' \vee (x \wedge y) & \text{oletus} \\ & = & (x' \vee x) \wedge (x' \vee y) & BA3 \\ & = & (x \vee x') \wedge (x' \vee y) & BA1 \\ & = & \mathbf{1} \wedge (x' \vee y) & BA4 \\ & = & (x' \vee y) \wedge \mathbf{1} & BA1 \\ & = & x' \vee y & BA2 \\ & = & y \vee x' & BA1 \end{array}$$

Siis (1°):n ja (2°):n nojalla $y = x'$. ■

Seuraus 7.3.7. *BA:ssa* $(B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$ *pätee* $x'' = x$ *kaikille* $x \in B$.

Todistus. Väite seuraa suoraan lauseesta 7.2.8 (BA1):n ja (BA2):n nojalla. ■

Määritelmä 7.3.8. *BA:n ilmaisun* duaali *saadaan korvaamalla operaatiot* $\vee$ *ja* $\wedge$ *vastaavasti operaatioilla* $\wedge$ *ja* $\vee$ *sekä alkiot* $\mathbf{0}$ *ja* $\mathbf{1}$ *vastaavasti alkioilla* $\mathbf{1}$ *ja* $\mathbf{0}$.

Esimerkki 7.3.9. *Distributiivilain* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *duaali on toinen distributiivilaki* $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ *ja kääntäen. Yleisesti BA:n aksioomissa (BA1)–(BA4) olevat lausekkeet ovat toistensa duaaleja.*

On selvää, että jos ilmaisu β on ilmaisun α duaali, niin α on β:n duaali.

Lause 7.3.10. *(Dualiteettiperiaate). Jos BA:n ilmaisu* α *on johdettavissa aksioomista (BA1)–(BA5), niin myös* α*:n duaali on johdettavissa ko. aksioomista.*

Todistus. Aksiooman (BAi), $i = 1, 2, 3, 4$, lausekkeet ovat toistensa duaaleja. (BA5) on itsensä duaali. Täten, kun ilmaisun α todistuksessa jokainen ilmaus korvataan duaalillaan, saadaan α:n duaalin todistus, koska tällöin käytettyjen aksioomien duaalit ovat aksioomia. ■

Lause 7.3.11. *(Idempotenssi). Olkoon* $(B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$ *BA.* $x \wedge x = x$ *ja* $x \vee x = x, \forall x \in B$.

Todistus.

$$\begin{array}{rcll} x & = & x \wedge \mathbf{1} & BA2 \\ & = & x \wedge (x \vee x') & BA4 \\ & = & (x \wedge x) \vee (x \wedge x') & BA3 \\ & = & (x \wedge x) \vee \mathbf{0} & BA4 \\ & = & x \vee x & BA2 \end{array}$$

Dualiteettiperiaatteesta seuraa $x \vee x = x$. ■

Lause 7.3.12. *Olkoon* $(B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$ *BA. Kaikille alkioille* $x, y, z \in B$ *pätee*

(i) $x \wedge \mathbf{0} = \mathbf{0}$

(ii) $x \vee \mathbf{1} = \mathbf{1}$

(iii) $x \wedge (x \vee y) = x$

(iv) $x \vee (x \wedge y) = x$ ***(absorbtiolait)***

(v) $y \wedge x = z \wedge x, y \wedge x' = z \wedge x' \Rightarrow y = z$

(vi) $x \vee (y \vee z) = (x \vee y) \vee z$

(vii) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ ***(assosiatiivilait)***

(viii) $(x \vee y)' = x' \wedge y'$

(ix) $(x \wedge y)' = x' \vee y'$ ***(DeMorganin lait)***

(x) $x \vee y = (x' \wedge y')'$

(xi) $x \wedge y = (x' \vee y')'$

(xii) $x \wedge y' = \mathbf{0} \Leftrightarrow x \wedge y = x$

(xiii) $\mathbf{0}' = \mathbf{1}$

(xiv) $\mathbf{1}' = \mathbf{0}$

(xv) $x \wedge (x' \vee y) = x \wedge y$

(xvi) $x \vee (x' \wedge y) = x \vee y$

Todistus. (i) $x \wedge 0 = (x \wedge 0) \vee \mathbf{0} = (x \wedge \mathbf{0}) \vee (x \wedge x') = (x \wedge x') \vee (x \wedge \mathbf{0}) = x \wedge (x' \vee \mathbf{0}) = x \wedge x' = \mathbf{0}$.
(ii) on tosi (i):n duaalina.
(iii) $x \wedge (x \vee y) = (x \vee \mathbf{0}) \wedge (x \vee y) = x \vee (\mathbf{0} \wedge y) = x \vee \mathbf{0} = x$.
(iv) on tosi (iii):n duaalina.
(v) Oletetaan, että $y \wedge x = z \wedge x, y \wedge x' = z \wedge x'$. Tällöin on $y = y \wedge \mathbf{1} = y \wedge (x \vee x') = (y \wedge x) \vee (y \vee x') = (z \wedge x) \vee (z \vee x') = z \wedge (x \vee x') = z \wedge \mathbf{1} = z$.
(vi) Käytämme (v):ttä korvaamalla y lausekkeella $x \vee (y \vee z)$ ja z lausekkeella $(x \vee y) \vee z$. Täten on osoitettava (a) $(x \vee (y \vee z)) \wedge x = ((x \vee y) \vee z) \wedge x$ ja (b) $(x \vee (y \vee z)) \wedge x' ((x \vee y) \vee z) \wedge x'$.
Todistetaan (a): $(x \vee (y \vee z)) \wedge x = x \wedge (x \vee (y \vee z)) = x$ (iii):n nojalla. Myös $((x \vee y) \vee z) \wedge x = x \wedge ((x \vee y) \vee z) = [x \wedge (x \vee y)] \vee [x \wedge z] = x \vee (x \wedge z) = x$ (iii):n ja (iv):n nojalla. Täten on $(x \vee (y \vee z)) \wedge x = x = ((x \vee y) \vee z) \wedge x$.
Todistetaan (b): $(x \vee (y \vee z)) \wedge x' = x' \wedge (x \vee (y \vee z)) = (x' \wedge x) \vee (x' \wedge (y \vee z)) = 0 \vee (x' \wedge (y \vee z)) = x' \wedge (y \vee z)$. Myös $((x \vee y) \vee z) \wedge x' = x' \wedge [(x \vee y) \vee z] = (x' \wedge y) \vee (x' \wedge z) = x' \wedge (y \vee z)$. Täten on $(x \vee (y \vee z)) \wedge x' = x' \wedge (y \vee z) = ((x \vee y) \vee z) \wedge x'$.
(vii) on tosi (vi):n duaalina.

(viii) Todistaaksemme, että $(x \vee y)' = x' \wedge y'$ käytämme komplementin yksikäsitteisyyttä (Lause 7.2.8). On osoitettava, että (c) $(x \vee y) \wedge (x' \wedge y') = \mathbf{0}$ ja (d) $(x \vee y) \vee (x' \wedge y') = \mathbf{1}$.
Todistetaan (c): $(x \vee y) \wedge (x' \wedge y') = (x' \wedge y') \wedge (x \vee y) = [(x' \wedge y') \wedge x] \vee [(x' \wedge y') \wedge y] = [x \wedge (x' \wedge y')] \vee [x' \wedge (y' \wedge y)] = [\mathbf{0} \wedge y'] \vee [x' \wedge \mathbf{0}] = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$.
Todistetaan (d): $(x \vee y) \vee (x' \wedge y') = [(x \vee y) \vee x'] \wedge [(x \vee y) \vee y'] = [x' \vee (\vee y)] \wedge [x \vee (y \vee y')] = [(x' \vee x) \vee y] \wedge [x \vee \mathbf{1}] = [(x' \vee x) \vee y] \wedge \mathbf{1} = (x' \vee x) \vee y = \mathbf{1} \vee y = y \vee \mathbf{1} = \mathbf{1}$.
(ix) on tosi (viii):n duaalina.
(x) (viii):n nojalla on $(x \vee y)' = x' \wedge y'$. Täten $(x \vee y)'' = (x' \wedge y')'$. Toisaalta lauseen 7.2.8 seurauksen nojalla on $(x \vee y)'' = x \vee y$.
(xi) on tosi (x):n duaalina.
(xii) $x = x \wedge \mathbf{1} = x \wedge (y \vee y') = (x \wedge y) \vee (x \wedge y')$. Täten $x \wedge y' = \mathbf{0} \Rightarrow x = x \wedge y$. Kääntäen, olkoon $x = x \wedge y$. Tällöin on $x \wedge y' = \mathbf{0} \vee (x \wedge y') = (x \wedge x') \vee (x \wedge y') = x \wedge (x' \vee y') = x \wedge (x \wedge y)' = x \wedge x' = \mathbf{0}$.
(xiii) Koska $\mathbf{0} \vee \mathbf{1} = \mathbf{1}$ ja $\mathbf{0} \wedge \mathbf{1} = \mathbf{0}$, niin lauseen 7.2.8 nojalla on $\mathbf{0}' = \mathbf{1}$.
(xiv) on tosi (xiii):n duaalina.
(xv) $x \wedge (x' \vee y) = (x \wedge x') \vee (x \wedge y) = \mathbf{0} \vee (x \wedge y) = x \wedge y$.
(xvi) on tosi (xv):n duaalina. ■

7.4 Osittainen järjestys Boolen algebrassa

BA:ssa $\mathcal{B}$ määritellään sen perusjoukossa B binäärinen relaatio '$\leq$' ehdolla

$$x \leq y, \text{ joss } x \wedge y = x. \tag{7.1}$$

Symbolia '$\leq$' ei saa sekoittaa erityisesti lukujoukkojen tavalliseen järjestysrelaatioon *pienempi tai yhtäsuuri kuin*. Jos sekaannuksen vaaraa ilmenee, voidaan käyttää alaindeksointia $\leq_{\mathcal{B}}$.

Lause 7.4.1. *BA:ssa $\mathcal{B}$ on voimassa kaikille $x, y \in B$*

$$x \leq y, \textit{ joss } x \vee y = y.$$

Todistus. Olkoon $x, y \in B$ ja $x \leq y$. Tällöin

$$x \vee y = (x \wedge y) \vee y = y$$

(7.1):n ja lauseen 7.3.12 kohdan (iv) nojalla. Kääntäen, jos $x \vee y = y$, niin

$$x \wedge y = x \wedge (x \vee y) = x$$

lauseen 7.3.12 kohdan (iii) nojalla. ■

Esimerkki 7.4.2. *BA:ssa $(\mathcal{P}(A), \cap, \cup, ^c, \emptyset, A)$ relaatio $x \leq y$ on yhtäpitävä relaation $x \subset y$ kanssa, kun x ja y ovat mitä tahansa A:n osajoukkoja.*

Esimerkki 7.4.3. *Esimerkin 7.3.5 tapauksessa, kun A ja B ovat $\mathbb{L}$:n lauseita, on*

$$[A] \leq [B], \textit{joss } [A] \wedge [B] = [A].$$

Koska $[A] \wedge [B] = [A \wedge B]$*, niin*

$$[A] \leq [B], \textit{joss } [A \wedge B] = [A],$$

ts. jos $A \wedge B$ *ja* A *ovat loogisesti ekvivalentteja. Selvästi* $A \wedge B$ *ja* A *ovat loogisesti ekvivalentteja, joss* $A \vdash B$*. Täten* $[A] \leq [B]$*, joss* $A \vdash B$ *eli* $A \to B$ *on todistuva.*

Lause 7.4.4. *Olkoon* B *BA:n* $\mathcal{B}$ *perusjoukko, ja* $x, y, z \in B$*. Tällöin*

(i) $\leq$ *on refleksiivinen* B*:ssä, ts.* $x \leq x$*;*

(ii) $\leq$ *on transitiivinen* B*:ssä, ts.* $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$*;*

(iii) $\leq$ *on antisymmetrinen* B*:ssä, ts.* $(x \leq y \wedge y \leq x) \Rightarrow x = y$*.*

Todistus. (i) $x \wedge x = x$, joten väite seuraa (7.1):stä.
(ii) Oletetaan, että $x \wedge y = x$ ja $y \wedge z = y$. Silloin on

$$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$$

(7.1):n nojalla.
Oletetaan, että $x \wedge y = x$ ja $y \wedge x = y$. Silloin on (7.1):n nojalla

$$x = x \wedge y = y \wedge x = y.$$

Täten lause on tullut todistetuksi. ■
Kuten tiedetään, binäärinen relaatio R joukossa A on osittainen järjestys joukossa A, joss se on refleksiivinen, transitiivinen ja antisymmetrinen joukossa A. Osittainen järjestys väljemmässä mielessä voidaan määritellä siten, että otetaan huomioon vain transitiivisuus ja antisymmetrisyys. Jos '$\leq$' on (refleksiivinen) osittainen järjestys joukossa A, voidaan relaatio $x < y$ määritellä ehdolla $x \leq y \wedge x \neq y$. Täten on voimassa

Lause 7.4.5. *(i)* $\neg(x < x)$

(ii) $(x < y \wedge y \leq z) \Rightarrow x < z$

(iii) $(x \leq y \wedge y < z \Rightarrow x < z$

(iv) $(x < y \wedge y < z) \Rightarrow x < z$

(v) $\neg(x < y \wedge y < x)$

(vi) '$<$' *on irrefleksiivinen osittainen järjestys* A*:ssa.*

A:ssa vallitseva irrefleksiivinen osittainen järjestys $<$ voidaan laajentaa refleksiiviseksi osittaiseksi järjestykseksi A:ssa määrittelemällä $x \leq y \Leftrightarrow (x < y \vee x = y)$. Olkoon $\leq$ osittainen järjestys joukossa A. Alkiota $z \in A$ sanotaan osajoukon $Y \subset A$ *ylärajaksi*, jos $y \leq z$ kaikille $y \in Y$. Alkio $z \in A$ on osajoukon $Y \subset A$ *pienin yläraja*, joss

(1) z on Y:n yläraja;

(2) $z \leq w$ kaikille Y:n ylärajoille w.

Relaation $\leq$ antisymmetrisyyden nojalla A:n osajoukolla Y on enintään yksi pienin yläraja. Alkiota $z \in A$ sanotaan osajoukon $Y \subset A$ *alarajaksi*, jos $z \leq y$ kaikille $y \in Y$. Alkio $z \in A$ on osajoukon $Y \subset A$ *suurin alaraja*, joss

(3) z on Y:n alaraja;

(4) $w \leq z$ kaikille Y:n alarajoille w.

Relaation $\leq$ antisymmetrisyyden nojalla A:n osajoukolla Y on enintään yksi suurin alaraja.

Esimerkki 7.4.6. *Tavallinen järjestysrelaatio $\leq$ on osittainen järjestys kokonaislukujen joukossa $\mathbb{Z}$. Millä tahansa $\mathbb{Z}$:n osajoukolla, jolla on yläraja (vastaavasti alaraja) on pienin yläraja (suurin alaraja), joka on ko. osajoukon suurin (pienin) alkio. Kuitenkin $\mathbb{Z}$:lla on ei-tyhjiä osajoukkoja, joilla ei ole pienintä ylärajaa (suurinta alarajaa), esim. $\mathbb{Z}$ itse ja vaikkapa parillisten kokonaislukujen joukko, jolla ei ole pienintä ylärajaa eikä suurinta alarajaa.*

Esimerkki 7.4.7. *Tavallinen järjestysrelaatio $\leq$ on osittainen järjestys kokonaislukujen joukossa $\mathbb{R}$. Jokaisella $\mathbb{R}$:n ei-tyhjällä osajoukolla, jolla on yläraja (vastaavasti alaraja), on pienin yläraja (suurin alaraja).*

Esimerkki 7.4.8. *Tavallinen järjestysrelaatio $\leq$ on osittainen järjestys rationaalilukujen joukossa $\mathbb{Q}$. On olemassa sellaisia $\mathbb{Q}$:n ei-tyhjiä osajoukkoja, jotka ovat ylhäältä rajoitettuja, mutta niillä ei ole pienintä ylärajaa. Esimerkkeinä mainittakoon positiivisten rationaalilukujen x joukko, jossa $x^2 < 2$. Luku $\sqrt{2}$ rajoittaa tätä joukkoa ylhäältä, mutta irrationaalilukuna se ei kuulu siihen. Toisaalta, jos valitaan $\sqrt{2}$:sta pienempi rationaaliluku q, joka on kuinka lähellä hyvänsä lukua $\sqrt{2}$, löydetään aina sellainen rationaaliluku r, että $q < r < \sqrt{2}$. Siis ko. joukolla ei ole pienintä ylärajaa.*

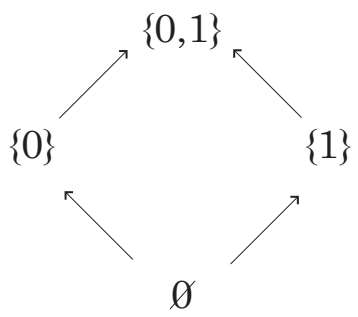
Osittainen järjestys, joka on yhtenäinen, on kokonaisjärjestys. Siis binäärinen relaatio R joukossa A on kokonaisjärjestys, jos se on refleksiivinen, transitiivinen, antisymmetrinen ja yhtenäinen joukossa A.

Esimerkki 7.4.9. *Tavallinen järjestysrelaatio $\leq$ on kokonaisjärjestys joukossa $\mathbb{Z}$, koska se on $\mathbb{Z}$:n osittainen järjestys (ks. Esim. 7.4.6) ja lisäksi*

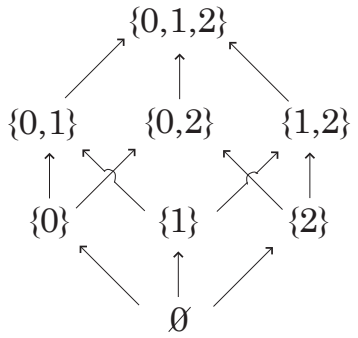
$$\forall x, y \in \mathbb{Z}, x < y \text{ tai } y < x.$$

Esimerkki 7.4.10. *BA:ssa $(\mathcal{P}(\{0,1\}), \cap, \cup, {}^c, \emptyset, \{0,1\})$ määritelty osittainen järjestys '$\subset$' ei ole yhtenäinen eikä täten kokonaisjärjestys $\mathcal{P}(\{0,1\})$:ssä, koska esim. $\{0\} \not\subset \{1\}$ ja $\{1\} \not\subset \{0\}$.*

Äärellisen joukon A osittainen järjestys voidaan esittää diagrammana, jossa A:n alkiot kuvataan pisteinä, ja piste x on osittaisessa järjestysrelaatiossa y:n kanssa, joss x:stä päästään y:hyn nuolien muodostamaa polkua pitkin nuolien suunnassa, joita voi olla $0, 1, 2, \ldots, n$ kpl.
BA:ssa määritellyllä osittaisella järjestyksellä on tietty ominaisuus, jota ei kaikilla osittaisilla järjestyksillä ole.



Kuva 4: Relaatio $\subset$ esimerkin 7.4.10 BA:ssa



Kuva 5: Relaatio $\subset$ joukossa $\mathcal{P}(\{0,1,2\})$

Lause 7.4.11. *Olkoon B BA:n $\mathcal{B}$ perusjoukko. Tällöin kaikille alkioille $x, y \in B$ on voimassa ehto*

$$\textit{joukolla } \{x,y\} \subset B \textit{ on pienin yläraja } x \vee y \textit{ ja suurin alaraja } x \wedge y. \tag{7.2}$$

Todistus. 1°) $x \leq x \vee y$, koska $x \wedge (x \vee y) = x$. Samoin on $y \leq x \vee y$. Täten $x \vee y$ on joukon $\{x, y\}$ yläraja. Olkoon w joukon $\{x, y\}$ mikä tahansa yläraja. Tällöin on $x \leq w$ ja $y \leq w$, ts. $x \wedge w = x$ ja $y \wedge w = y$. Täten $(x \vee y) \wedge w = (x \wedge w) \vee (y \wedge w) = x \vee y$, ts. $x \vee y \leq w$. Täten $x \vee y$ on joukon $\{x, y\}$ pienin yläraja.
2°) $x \wedge y \leq x$, koska $(x \wedge y) \wedge x = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y$. Samoin $x \wedge y \leq y$, koska $(x \wedge y) \wedge y = x \wedge (y \wedge y) = x \wedge y$. Siis $x \wedge y$ on joukon $\{x, y\}$ alaraja. Olkoon w joukon $\{x, y\}$ mikä tahansa alaraja. Tällöin $w \leq x$ ja $w \leq y$, ts. $w \wedge x = w$ ja $w \wedge y = w$. Täten $w \wedge (x \wedge y) = (w \wedge x) \wedge y = w \wedge y = w$, ts. $w \leq (x \wedge y)$. Täten $x \wedge y$ on joukon $\{x, y\}$ suurin alaraja. ■

7.5 Boolen kaavat ja funktiot

Määritelmä 7.5.1. *Olkoot $x_1, x_2, \ldots$ numeroituva joukko muuttujia, jotka kukin saavat arvoikseen jonkin BA:n alkion. Tällöin symboleista*

$$x_1, x_2, \ldots, \mathbf{0}, \mathbf{1}, \vee, \wedge, \ ',' \, (\textit{ ja } ')'$$

muodostettu äärellinen jono on Boolen kaava*, merk. BK, joss*

1° *se on joko muuttuja* x_i, **0** *tai* **1**,

2° *se on muotoa* $(\alpha \vee \beta), (\alpha \wedge \beta)$ *tai* α', *missä* α *ja* β *ovat Boolen kaavoja.*

Määritelmä 7.5.2. *Olkoon* $\mathcal{B} = (B, \vee, \wedge, ', \mathbf{0}, \mathbf{1})$ *jokin BA sekä* $f : B \to B$ *kuvaus. Tällaista* f*:ää kutsutaan* n*:n muuttujan* Boolen fuktioksi *(BF)* $\mathcal{B}$*:ssä.*

Yleensä BF:t esitetään taulukon muodossa, jossa kullakin vaakarivillä on tietyt muuttujien arvot ja vastaava funktion arvo. Taulukko on täten analoginen totuustaulujen kanssa. Jokainen BK määrittelee yksikäsitteisen BF:n jokaisessa BA:ssa. Toisaalta kaksi eri kaavaa voi määritellä saman funktion. Tämä voidaan todeta siten, että tarkasteltaessa jonkin BK:n taulua kukin muuttujien arvokombinaatio on järjestetty n-jono, missä n on muuttujien lukumäärä, jolloin ko. jono on joukon B^n alkio, joka kuvautuu tietylle B:n alkiolle taulun osoittamalla tavalla.
Annamme vielä seuraavan

Määritelmä 7.5.3. *Alkio* x *on BA:n* atomi, *jos ehdosta* $0 \leq z \leq x$ *seuraa, että* $z = 0$ *tai* $z = x$.

Atomeja ovat siis ne alkiot, jotka ovat lähinnä 0-alkion ”yläpuolella”.

7.6 Normaalimuodot

Literaaleilla tarkoitetaan muuttujia $x, y, z, \ldots$ tai niiden komplementteja
$x', y', z', \ldots$. *Peruskonjunktiolla* tarkoitetaan (i) literaalia tai (ii) kahden tai useamman eri literaalin konjunktiota. Esim. x_2, u', $x \wedge y$ ja $x_1' \wedge u \wedge r$ ovat peruskonjunktioita, kun taas x'', $x \wedge y \wedge x$ ja $y \wedge x \wedge z \wedge y'$ eivät ole. Tässä ”kaksi eri literaalia” tulkitaan niin vahvasti, että literaalien x ja x' ei katsota olevan eri literaaleja. Vastaavat määrittelyt tehdään operaation $\vee$ suhteen, jolloin saadaan *perusdisjunktio*.
BK:t voidaan esittää muodossa, jossa esiintyy vain peruskonjunktioiden disjunktioita tai perusdisjunktioiden konjunktioita. Esim. kaava $(x' \wedge y) \vee (x \wedge y') \vee (x \wedge y)$ on muodossa, jossa esiintyy peruskonjunktioiden disjunktioita. Vastaavasti kaava $(x \vee y') \wedge (x' \vee y) \wedge (x' \vee y')$ on muodossa, jossa esiintyy perusdisjunktioiden konjunktioita.

Määritelmä 7.6.1. *Olkoon* $n \geq 1$ *ja* x_i^* $(i = 1, \ldots, n)$ *literaali. Tällöin* n*:n muuttujan BK on* disjunktiivisessa normaalimuodossa *(merk.* dnf*), jos se on sellaisessa muodossa*

$$(x_1^* \wedge x_2^* \wedge \ldots \wedge x_n^*) \vee (x_1^* \wedge x_2^* \wedge \ldots \wedge x_n^*) \vee \ldots \vee (x_1^* \wedge x_2^* \wedge \ldots \wedge x_n^*), \tag{7.3}$$

missä mitkään kaksi peruskonjunktiota eivät ole identtisiä.

Määritelmä 7.6.2. *Olkoon* $n \geq 1$ *ja* x_i^* $(i = 1, \ldots, n)$ *literaali. Tällöin* n*:n muuttujan BK on* konjunktiivisessa normaalimuodossa *(merk.* knf*), jos se on sellaisessa muodossa*

$$(x_1^* \vee x_2^* \vee \ldots \vee x_n^*) \wedge (x_1^* \vee x_2^* \vee \ldots \vee x_n^*) \wedge \ldots \wedge (x_1^* \vee x_2^* \vee \ldots \vee x_n^*), \tag{7.4}$$

missä mitkään kaksi perusdisjunktiota eivät ole identtisiä.

Määritelmä 7.6.3. *Sellainen* n*:n muuttujan disjunktiivinen normaalimuoto, missä on* 2^n *erilaista peruskonjunktioiden disjunktiota, on* n*:n muuttujan* täysi disjunktiivinen normaalimuoto.

Määritelmä 7.6.4. *Sellainen n:n muuttujan konjunktiivinen normaalimuoto, missä on 2^n erilaista perusdisjunktioiden konjunktiota, on n:n muuttujan* täysi konjunktiivinen normaalimuoto.

Lause 7.6.5. *Olkoon $n \geq 1$. Jos n:n muuttujan BK:n täydessä dnf:ssä muuttujat saavat satunnaisesti arvoja 0 tai 1, niin minkä tahansa tällaisen muuttujien kiinnityksen jälkeen ko. BK:ssa täsmälleen yhdellä peruskonjunktiolla on arvo 1 ja kaikilla muilla 0.*

Todistus. Olkoot $a_1, a_2, \ldots, a_n$ vastaavasti muuttujien $x_1, x_2, \ldots, x_n$ arvot, jolloin kukin a_i on **0** tai **1** ($i = 1, \ldots, n$). Valitaan ko. BK:n dnf:stä peruskonjunktio seuraavasti: kutakin muuttujaa x_i kohti ko. termissä esiintyy x_i, jos $a_i = 1$, $i = 1, \ldots, n$. Täyden dnf:n määritelmän perusteella tällainen tulotermi on aina olemassa ja sen valintaperusteista johtuen se saa arvon 1. Edelleen täyden dnf:n määritelmän perusteella ko. BK:n muut peruskonjunktiot saavat arvoikseen nollan, koska täten niissä vähintään yksi literaali saa arvon 0, jolloin koko termi saa arvon 0. ■

Seuraus 7.6.6. *Olkoon $n \geq 1$. Tällöin muuttujan täydessä dnf:ssä oleva BK saa aina arvon 1.*

Todistus. Seurauksen paikkansapitävyys seuraa suoraan määritelmästä 9?? ja lauseesta 10??. ■

Lause 7.6.7. *Olkoon $n \geq 1$. Jos n:n muuttujan BK:n täydessä knf:ssä muuttujat saavat satunnaisesti arvoja **0** tai **1**, niin minkä tahansa tällaisen muuttujien kiinnityksen jälkeen ko. BK:ssa täsmälleen yhdellä peruskonjunktiolla on arvo 0 ja kaikilla muilla 1.*

Todistus. Lauseen paikkansapitävyys seuraa dualiteetin periaatteen nojalla lauseesta 7.6.5. ■

Seuraus 7.6.8. *Olkoon $n \geq 1$. Tällöin n:n muuttujan täydessä knf:ssä oleva BK saa aina arvon 0.*

Todistus. Seurauksen paikkansapitävyys seuraa suoraan määritelmästä 10?? ja lauseesta 11??. ■

Huom. Täydet dnf:t saavat lauseen 10?? nojalla *identtisesti* arvon 0. Tällöin siis muuttujien saamat arvot eivät vaikuta ko. täyden normaalimuodon saamaan arvoon. Sensijaan, kun normaalimuodot eivät ole täysiä, muuttujien saamat arvot vaikuttavat ko. kaavan saamaan arvoon.

7.7 Isomorfismit

Funktiota φ sanotaan isomorfismiksi BA:sta

$$\mathcal{B} = (B, \wedge, \vee, ', \mathbf{0}, \mathbf{1})$$

BA:han

$$\mathcal{C} = (C, \wedge^*, \vee^*, '^*, \mathbf{0}^*, \mathbf{1}^*),$$

joss (a) φ on bijektio B:stä C:hen. (b) $\forall x, y \in B, \varphi(x \wedge y) = \varphi(x) \wedge^* \varphi(y), \varphi(x \vee y) = \varphi(x) \vee^* \varphi(y)$ ja $\varphi(x') = [\varphi(x)]'^*$.

Lause 7.7.1. *Olkoon φ isomorfismi BA:sta $\mathcal{B}$ BA:han $\mathcal{C}$. Silloin*

(a) $\varphi(\mathbf{0}) = \mathbf{0}^*$ *ja* $\varphi(\mathbf{1}) = \mathbf{1}^*$

(b) φ*:lle pätee:* $\forall x, y \in B, \varphi(x \wedge y) = \varphi(x) \wedge^* \varphi(y) \Leftrightarrow \varphi/x \vee y) = \varphi(x) \vee^* \varphi(y)$

(c) Jos θ on isomorfismi BA:sta $\mathcal{B}$ BA:han $\mathcal{D} = (D, \wedge^{**}, \vee^{**}, {}'^{**}, \mathbf{0}^{**}, \mathbf{1}^{**})$, niin yhdistetty kuvaus on isomorfismi BA:sta $\mathcal{B}$ BA:han $\mathcal{D}$.

(d) Käänteiskuvaus φ^1 on isomorfismi $\varphi(B)$:n määräämästä $\mathcal{C}$:n alialgebrasta $\mathcal{B}$:lle. Erityisesti, jos φ on bijektio, on φ^1 isomorfismi $\mathcal{C}$:tä $\mathcal{D}$:hen.

Todistus sivuutetaan.
Sanomme, että $\mathcal{B}$ ja $\mathcal{C}$ ovat isomorfiset, joss on olemassa isomorfismi $\mathcal{B}$:stä $\mathcal{C}$:hen. Keskenään isomorfisilla BA:illa on tietyssä mielessä sama Boolen struktuuri, ts. ominaisuus, joka on yhdessä BA:ssa, on myös missä tahansa ko. BA:n kanssa isomorfisessa BA:ssa.

Esimerkki 7.7.2. *Olkoon $\mathcal{C} = (\{\mathbf{0}_B, \mathbf{1}_B\}, \wedge_B, \vee_B, {}'_B, \mathbf{0}_B, \mathbf{1}_B)$ jonkin BA:n $\mathcal{B}$ alialgebra ja $\mathcal{D} = (\{0, 1\}, \cdot, +, 1 - ., 0, 1)$. Tällöin funktio φ, jolle $\varphi(\mathbf{0}_B) = 0$ ja $\varphi(\mathbf{1_B}) = 1$ on isomorfismi $\mathcal{C}$:stä $\mathcal{D}$:hen.*

7.8 Boolen algebrat ja propositiologiikka

Edellä esitetyt esimerkit 7.3.5 ja 7.4.3 liittyvät propositiologiikan ja BA:n välisiin suhteisiin. Niissä tarkastellaan lähinnä propositiologiikan muodostamaa Boolen algebraa. Tässä tarkastellaan lähinnä propositiologiikan ja BA:n struktuurillisia samankaltaisuuksia.
$\mathbb{L}$:n lause A vastaa Boolen kaavaa τ, jos τ saadaan A:sta korvaamalla τ:ssa BA:n operaatiot vastaavilla $\mathbb{L}$:n konnektiiveilla ja sijoittamalla BA:n muuttujien $x, y, z, \ldots$ paikalle vastaavasti $\mathbb{L}$:n lausemuuttujat $A, B, C, \ldots$.

Esimerkki 7.8.1. *Boolen kaavaa $x \vee (y \wedge z')$ vastaa $\mathbb{L}$:n lause $A \vee (B \wedge \neg C)$. Samoin $\mathbb{L}$:n lausetta $\neg(\neg A \wedge (B_1 \vee A))$ vastaa Boolen kaava $(x' \wedge (y_1 \vee x))'$.*

$\mathbb{L}$:n lausetta, joka vastaa Boolen kaavaa τ, merkitään $SF(\tau)$.

Lause 7.8.2. *Yhtälö $\tau = \sigma$ on voimassa kaikissa BA:issa, joss $SF(\tau)$ on loogisesti ekvivalentti $SF(\sigma)$:n kanssa.*

Todistus. Eo. seurauksen nojalla $\tau = \sigma$ on voimassa kaikissa BA:issa, joss $\tau = \sigma$ on voimassa 2-arvoisessa BA:ssa $\mathcal{C} = (\{E, T\}, \wedge_C, \vee_C, {}'_C, E, T)$, missä operaatioilla on $\mathbb{L}$:n konnektiivien merkitys. On selvää, että $\tau = \sigma$ on voimassa $\mathcal{C}$:ssä, joss $SF(\tau)$ ja $SF(\sigma)$ aina saavat samat totuusarvot, jolloin ne myös ovat loogisesti ekvivalentit. ■

Esimerkki 7.8.3. *Tarkastellaan yhtälöä*

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Vastaavat $\mathbb{L}$:n lauseet ovat $A \wedge (B \vee C)$ ja $(A \wedge B) \vee (A \wedge C)$. Näiden loogisen ekvivalenssin toteamiseksi voidaan esim. muodosta kummankin lauseen totuustaulu. Lauseiden ekvivalenssista seuraa, että alkuperäinen yhtälö on voimassa missä tahansa BA:ssa.

7.9 Lisää Boolen funktioista

Oletetaan, että f ja g ovat n:n muuttujan funktioita Boolen algebrassa $\mathcal{B}$ eli kuvauksia $B^n \to B$. Luonnollisella tavalla voidaan määritellä uudet funktiot $f', f \wedge g$ ja $f \vee g \ : \ B^n \to B$. Funktioiden joukossa määriteltyinä operaaitoina $\vee, \wedge$ ja $'$ toteuttavat BA:n aksioomat, kun **0**- ja **1**-alkioiksi otetaan vakiofunktiot **0** ja **1**. Näinollen funktiot $B^n \to B$ muodostavat uuden BA:n ja niille pätee siis kaikki, mitä edellä on todettu yleisesti.
Jatkossa rajoitutaan pelkästään BA:ssa $\mathcal{B} = (\{0,1\}, \wedge, \vee, ', 0, 1)$ määriteltyihin funktioihin. Ne voidaan määritellä totuustaulujen avulla, joillaoin n:n muuttujan funktiolle $f(x_1, x_2, \ldots, x_n)$ tarvitaan 2^n-rivinen taulu. Sovitaan, että tauluissa annetaan muuttujille $x_1, x_2, \ldots, x_n$ arvoja siten, että i:nnellä rivillä jono x_1, x_2, x_n on luvun i esitys binäärilukuna $i = 0, 1, 2, \ldots, 2^n - 1$. Tällöin riittää tuntea vain funktion arvojen muodostama sarake, joka voidaan esittää (ylhäältä alkaen) vektorina $(b_0, b_1, \ldots, b_{m-1})$, missä $m = 2^n$.
Funktiot $B^n \to B$ voidaan siis samaistaa BA:n $\mathcal{B}^m$=$(B^m, \wedge, \vee, ', (0,0,\ldots,0),$
$(1,1,\ldots,1))$ kanssa ($m = 2^n$) ja funktioiden väliset operaatiot voidaan suorittaa komponenteittain: Jos $f = (a_0, a_1, \ldots, a_{m-1})$ ja $g = (b_0, b_1, \ldots, b_{m-1})$, niin esimerkiksi

$$f' \vee g = (a'_0 \vee b_0, a'_1 \vee b_1, \ldots, a'_{m-1} \vee b_{m-1}).$$

Samoin totuusfunktioiden osittainen järjestys määräytyy komponenteittain seuraavasti:

$$f \leq g \Leftrightarrow a_0 \leq b_0, a_1 \leq b_1, \ldots, a_{m-1} \leq b_{m-1}.$$

Kuten reaalifunktioidenkin kohdalla myös Boolen funktioille on $f \leq g$, joss f saa aina pienemmän tai yhtä suuren arvon kuin g.
BA:n $\mathcal{B}^m$ atomit ovat vektoreita, joissa yksi komponentti on 1 ja muut nollia. Katsotaan, mitä tämä merkitsee, kun $\mathcal{B}^m$ tulkitaan funktioalgebraksi (kun $m = 2^n$).
Olkoon $f(x_1, x_2, \ldots, x_n)$ funktio, jonka totuustaulussa on tasan yksi ykkönen. Olkoon

$$f(v_1, v_2, \ldots, v_n) = 1$$

ja muilla x_i:den arvoilla $f = 0$. Tällöin funktiota f esittää Boolen kaava

$$\alpha_1 \wedge \alpha_2 \wedge \ldots \alpha_n, \text{ missä } \alpha_i = \begin{cases} x_i, & \text{jos } v_i = 1 \\ x'_i, & \text{jos } v_i = 0 \end{cases}$$

Kaavaa $\alpha_1 \wedge \alpha_2 \wedge \ldots \alpha_n$ (ja vastaavaa funktiota) kutsutaan *mintermiksi*. Mintermistä käytetään merkintää m_j, missä j on binääriluvun $v_1 v_2 \ldots v_n$ arvo 10-järjestelmässä (j on siis totuustaulun sen rivin numero, jolla f:n ainoa 1 esiintyy). Yleisesti *termeiksi* nimitetään kaikkia niitä peruskonjunktioita eli literaalien konjunktioita, joissa sama muuttuja esiintyy korkeintaan kerran.
Koska mintermit ovat n:n muuttujan funktioalgebran atomeja, voidaan kaikki totuusfunktiot esittää mintermien disjunktiona eli täydessä disjunktiivisessa normaalimuodossa: Jos

$$f = (b_0, b_1, \ldots, b_{m-1}) \text{ ja } b_j = \begin{cases} 1, & \text{kun } j = j_1, j_2, \ldots, j_k \\ 0, & \text{muulloin,} \end{cases}$$

niin

$$f = m_{j_1} \vee m_{j_2} \vee \ldots \vee m_{j_k} = \bigvee_{r=1}^{k} m_{j_r}.$$

Tässä dnf on sama kuin funktion esitys termien yhdisteenä.
Funktion täysi dnf on helppo muodostaa, jos on käytettävissä funktion totuustaulu. Sen jokaista arvosarakkeessa esiintyvää ykköstä kohti tulee disjunktioon yksi mintermi, jonka i:s literaali on x_1 tai x_i' sen mukaan, onko kyseisellä vaakarivillä i:s muuttuja 1 vai 0. Kirjoittamista voidaan yksinkertaistaa jättämällä kohtausoperaatiot $\wedge$ merkitsemättä, siis $x \wedge y = xy$.

Esimerkki 7.9.1. *Kolmen muuttujan funktio f:*

$$f(x,y,z) = (1,0,0,1,1,0,1,0) = m_0 \vee m_3 \vee m_4 \vee m_6 = x'y'z' \vee x'yz \vee xy'z' \vee xyz'.$$

f:n totuustaulu on seuraava:

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Funktiolle f' saadaan esitys DeMorganin säännöllä

$$\begin{aligned} f' &= (x'y'z' \vee x'yz \vee xy'z' \vee xyz')' = (x'y'z')'(x'yz)'(xy'z')'(xyz')' \\ &= (x \vee y \vee z)(x \vee y' \vee z')(x' \vee y \vee z)(x' \vee y' \vee z) \end{aligned}$$

eli dnf:stä päästään knf:ään muodostettaessa DeMorganin lain avulla f:stä f'. Funktiolle f saataisiin täysi knf muodostamalla dnf f':lle ja muodostamalla sen komplementti, mutta se voidaan myös lukea suoraan totuustaulusta: Jokaista arvosarakkeessa esiintyvä nollaa kohti tulee kohtaukseen yksi makstermi (merk. M_j, kun ollaan j:nnellä rivillä), jonka i:s literaali on x_i tai x_1' sen mukaan, onko kyseisellä vaakarivillä i:s muuttuja 0 vai 1. Siis

$$f(x,y,z) = (x \vee y \vee z')(x \vee y' \vee z)(x' \vee y \vee z')(x' \vee y' \vee z').$$

Edellä on tullut todistetuksi, että jokainen totuusfunktio voidaan esittää (täydessä) dnf:ssä ja knf:ssä. Tästä näkyy erityisesti, että jokainen Boolen funktio voidaan esittää jollakin Boolen kaavalla (eli operaatioilla $\wedge$, $\vee$ ja $'$). Tämä koskee kaikkien Boolen algebrojen funktioita (eikä vain algebraa $\mathcal{B} = (\{0,1\}, \vee, \wedge, ', 0, 1)$).
Funktion täysi dnf tai knf saattaa olla yksinkertainen muodostaa, mutta se ei yleensä ole yksinkertaisin kaava, jolla funktio voidaan esittää.

Esimerkki 7.9.2. *Funktion $f(x,y,z) = x \vee y \vee z'$ täysi dnf on*

$$xyz \vee xyz' \vee xy'z \vee xy'z' \vee x'yz'$$

sillä tämä on mintermien yhdiste ja $x(yz \vee yz' \vee y'z \vee y'z') \vee (x \vee x')yz' = x1 \vee 1yz' = x \vee yz'$. Neljä ensimmäista mintermiä tuottivat siis yhdisteenään x:n, erityisesti kukin niistä oli $< x$. Samoin jokainen termi $x\alpha$, missä $\alpha \in \{y, y', z, z'\}$, on pienempi kuin x, sillä $x \wedge x\alpha = x\alpha$ ja $x \neq x\alpha$.

Määritelmä 7.9.3. *Termi t on funktion f* implikantti, *jos $t \leq f$.*

Nimitys johtuu siitä, että tilanteessa $t \leq f$ funktion $t' \leq f$ eli $t \to f$ arvo on identtisesti 1. Termi t siis implikoi funktion f, jos t on f:n alapuolella funktioalgebran hilassa. Jos funktio f on esitetty joidenkin termien yhdisteenä $f = t_1 \vee t_2 \vee \ldots \vee t_k$ (siis dnf:ssä), niin jokainen t_j on f:n implikantti, koska f on niiden yläraja. Koska kohtauksen muodostaminen merkitsee alarajan etsimistä, näemme, että termi $t = \alpha_1\alpha_2 \ldots \alpha_t$ on sellaisten termien implikantti, jotka saadaan t:stä poistamalla yksi tai useampi literaali α_i, eikä minkään muun (näemme suoraan myös idempotenttisuuden nojalla kuten esimerkissä 7.9.2). Poistamalla siis termistä t literaaleja saadaan yhä suurempia termejä.

Määritelmä 7.9.4. *Sellainen termi, joka on funktion implikantti, mutta jota suuremmat eivät enää ole, on f:n* alkuimplikantti.

Esimerkki 7.9.5. *Funktion $f(x,y,z) = x \vee yz'$ implikantteja ovat kaikki sen mintermit (ks. esim. 7.9.2) ja termit xy, xy', xz ja xz'. Alkuimplikantteja ovat x ja yz'. Muita implikantteja ei ole.*
Funktion $g(x,y,z) = xy \vee xy'z \vee x'yz'$ kaikki alkuimplikantit ovat xy, xz, yz'. Funktio g voidaan sieventää muotoon $g = xz \vee yz'$, josta ei heti näy, että myös xy on sen implikantti. Alkuimplikanttien ominaisuuksia käytetään mm. loogisten piirien minimoinnissa.

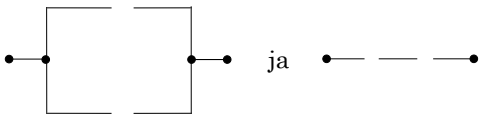
7.10 Kytkinpiirit

Kytkin (tunnuksena literaali α) on sähköjohdossa oleva laite, joka ei vaikuta virran kulkuun ollessaan kiinni ($\alpha = 1$) ja joka estää virran kulun ollessaan auki ($\alpha = 0$). Kytkintä merkitään '$\cdots - \alpha - \cdots$', missä α voi olla esim. x tai x'.
Kytkinpiiri muodostuu, kun kaksi pistettä A ja B yhdistetään kytkimiä sisältävillä johtimilla. Kytkinpiiri, jonka literaaleissa esiintyvät muuttujat $x_1, x_2, \ldots, x_n$, esittää Boolen funktiota $f(x_1, x_2, \ldots, x_n)$, joka saa arvon 1, kun virta voi kulkea A:ta B:hen, ja arvon 0, kun virta ei voi kulkea ko. pisteiden välillä. Piirin esittämä funktio löydetään käymällä läpi kaikki silmukattomat polut A:sta B:hen muodostaen niissä esiintyvien literaalien kohtaus ja lopuksi näiden kohtausten yhdiste.

Esimerkki 7.10.1. *Kytkinpiiri*

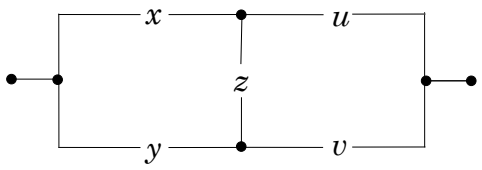
esittää funktiota $f(x,y,z) = y \vee x'y' \vee x'z$.

Tämä on esimerkki *rinnakkais-sarjapiireistä,* jotka voidaan muodostaa lähtien piireistä



siten, että kahdesta jo olemassaolevasta piiristä saadaan uusi piiri sijoittamalla toinen piiri toisen jonkin kytkimen paikalle. Lopuksi määrätään kytkimien toiminta nimeämällä ne literaaleilla.

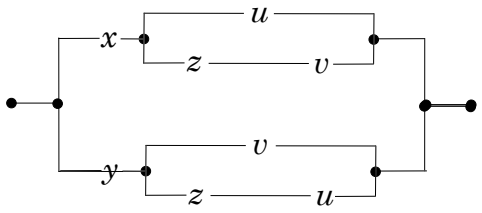
Esimerkki 7.10.2. *Piiriä*



ei voida muodostaa edellä kuvatulla tavalla. Kyseessä on ns. siltapiiri. *Se esittää funktiota*

$$f(x, y, z, u, v) = xu\vee, xzv \vee yzu \vee vy.$$

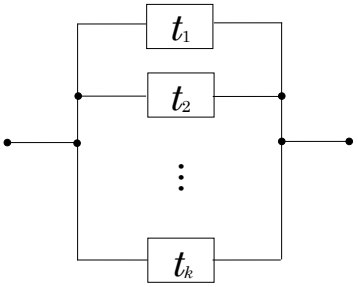
Saman funktion toteuttaminen rinnakkais-sarjamuotoisella piirillä on huomattavasti mutkikkaampaa:



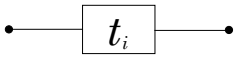
Jokainen Boolen funktio voidaan esittää kytkinpiirinä: Olkoon funktion $f(x_1, x_2, \ldots, x_n)$ *esitys dnf:ssä*

$$f = t_1 \vee t_2 \vee \ldots \vee t_k.$$

Muodostetaan piiri



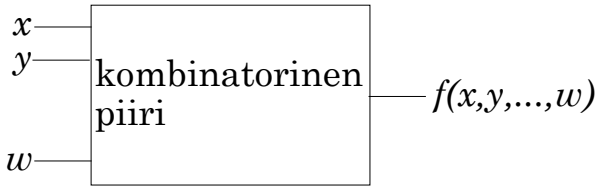
missä kukin laatikko



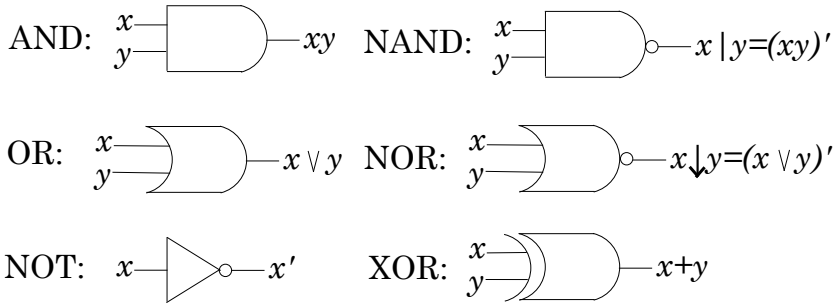
tarkoittaa piiriä $--\alpha_1--\alpha_2--\cdots--\alpha_k--$*, jossa* $\alpha_1\alpha_2\cdots\alpha_k = t_i$*. Tämä on rinnakkais-sarjapiiri, joka esittää funktiota* f*.*

7.11 Kombinatoriset piirit

Kombinatoriset eli *loogiset piirit* ovat elektronisia systeemejä, joilla toteutetaan totuusfunktioita syöttämällä piiriin muuttujien arvot jännitetasoina (esim. $1 = 5V$ ja $0 = 0V$) ja tuloksena saadaan funktion arvoa vastaava jännite (joka voidaan edelleen syöttää muille piireille). Siis

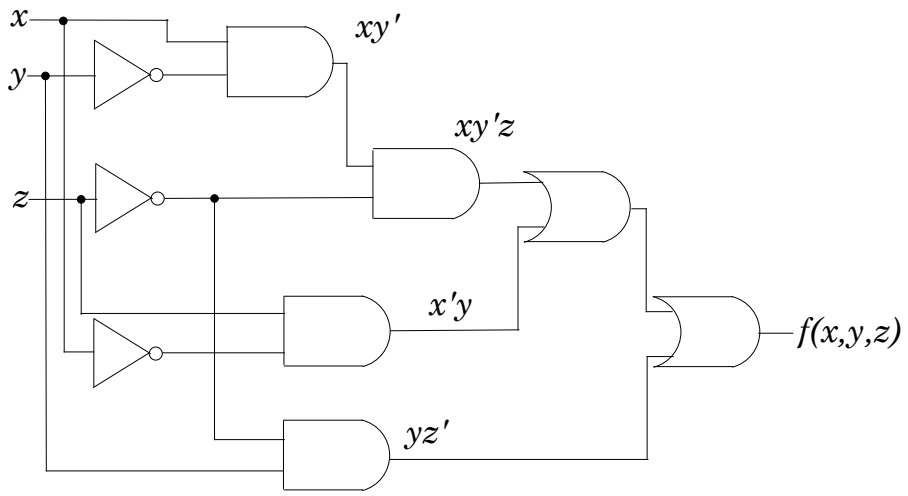


Loogiset piirit rakennetaan *porteista*, jotka toteuttavat loogiset perusoperaatiot $\wedge, \vee$ ja $'$ eli AND, OR ja NOT. Lisäksi on portit operaatioille $|$, $\downarrow$ ja $+$ eli NANS, NOR ja XOR. Porttien piirrosmerkit ovat

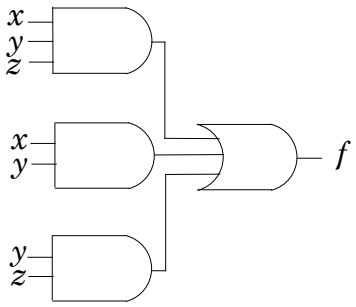


On selvää, että AND-, OR- ja NOT-porteilla voidaan toteuttaa kaikki Boolen funktiot.

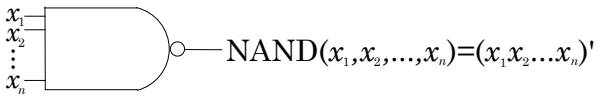
Esimerkki 7.11.1. $f(x,y,z) = xy'z' \vee x'z \vee yz' = ((xy')z' \vee x'z)yz'$



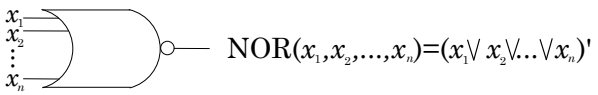
NOT-portit kuvion alusta jätetään yleensä merkitsemättä näkyviin eli syöttömuuttujien komplementointi ja jakelu porteille oletetaan etukäteen suoritetuksi.
Kaksisisäänmenoisten perusporttien lisäksi on portteja, joissa on enemmän kuin kaksi sisäänmenoa eli mahdollista syöttömuuttujaa. Täten esim. funktio $f = xy'z' \vee x'z \vee yz'$ voidaan toteuttaa tämän normaalimuotonsa perusteella, jolloin saadaan ns. *kaksitasoinen* piiri, tässä tapauksessa AND-OR-piiri.



Usean muuttuja AND- ja OR-porttien merkitys on selvä, koska termit eli peruskonjunktiot (esim. $xy'z'$) ja niiden duaalit eli perusdisjunktiot (esim. $x \vee y' \vee z'$) ovat hyvinmääriteltyjä operaatioiden $\wedge$ ja $\vee$ assosiatiivisuuden nojalla. Mutta operaatiot $|$ ja $\downarrow$ eivät ole assosiatiivisia, joten esim. kirjoitelma $x \downarrow y' \downarrow z'$ sellaisenaan on mieletön.
Sovitaan usean muuttujan NAND- ja NOR-porttien toiminta suorana yleistyksenä kahden muuttujan tilanteesta:



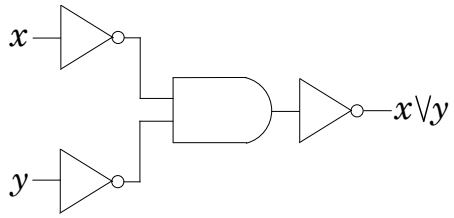
$$= \begin{cases} 0, & \text{jos } x_i = 1 \forall i, \\ 1, & \text{muulloin.} \end{cases}$$



$$= \begin{cases} 1, & \text{jos } x_i = 0 \forall i, \\ 0, & \text{muulloin.} \end{cases}$$

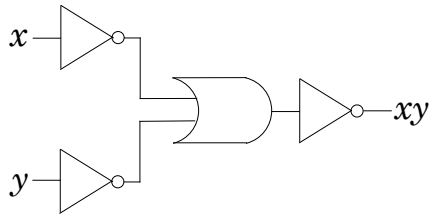
On huomattava, että piirtämistavasta huolimatta myös AND-OR- samoin kuin OR-AND-piirit (jotka vastaavat funktion knf:ää) sisältävät NOT-portteja. Pelkillä AND- ja OR-porteilla ei voida toteuttaa kaikkia funktioita (esim. komplementtia). Sensijaan porttisysteemit AND, NOT ja OR, NOT ovat (*funktionaalisesti*) *täydellisiä* eli kaikki funktiot voidaan esittää jommankumman systeemin porteilla. Tämän perustelemiseksi riittää todeta, että DeMorganin säännön nojalla

$x \vee y = (x'y')'$ eli



ja toisaalta (duaalisti)

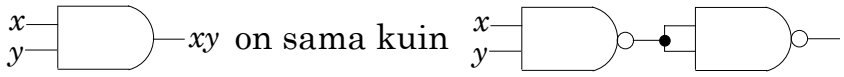
$xy = (x' \vee y')'$ eli



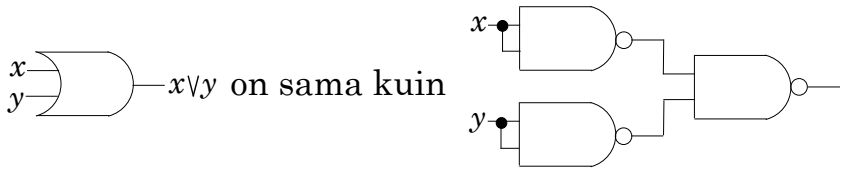
Kaikki totuusfunktiot on mahdollista toteuttaa myös käyttäen pelkästään yhdentyyppisiä portteja. Tällaisia systeemejä ovat NAND ja NOR, sillä

$$\begin{aligned} xy &= ((xy)'(xy)')' = ((x \vee x)' \vee (y \vee y)')' \\ x \vee y &= ((xx)'(yy)')' = ((x \vee y)' \vee (x \vee y)')' \\ x' &= (xx)' = (x \vee x)', \end{aligned}$$

missä keskimmäiset lausekkeet ovat pelkkiä NAND:ejä ja oikeanpuoleiset pelkkiä NOR:eja. Siis esim.



ja



NAND-porteilla toteutettuina. Käytännössä NAND- ja NOR-portit, joista AND- ja OR-portit muodostetaan komplementoinnilla, ovat integroiduissa piireissä tekniseltä kannalta perusteltuja. Ensinäkemältä vaikuttaisi siltä, että kaksitasoisen ANS-OR-piirin konstruoiminen pelkästään NAND-porteilla lisäisi tarvittavien porttien määrää huomattavasti ja lisäisi samalla porttitasojen määrää. Näin ei kuitenkaan ole, sillä jos korvataan AND-OR-piirin kukin AND- ja OR-portti NAND-portilla, jossa on vastaava määrä sisäänmenoja, saadaan saman funktion toteuttava NAND-NAND-piiri. Erityisesti siis NAND-NAND-piiri voidaan lukea suoraan funktion dnf:stä. Duaalinen tulos koskee luonnollisesti funktion esitystä OR-AND-piirillä ja NOR-NOR-piirillä funktion kmf:n perusteella.
Todistetaan yllä esitetty väite NAND:n tapauksessa. Olkoon f esitetty AND-OR-piirillä eli AND- ja OR-funktioilla:

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= OR[AND(\alpha_1, \alpha_2, \ldots, \alpha_n), AND(\beta_1, \beta_2, \ldots, \beta_n), \ldots, \\ &\quad AND(\gamma_1, \gamma_2, \ldots, \gamma_n)], \end{aligned}$$

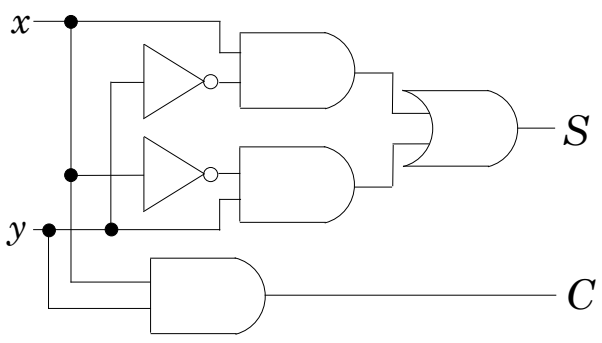
missä α_i:t, β_i:t ja γ_i:t ovat literaaleja. Korvataan AND- ja OR-funktiot (siis portit) NAND-funktioilla. Saadaan

$$\begin{aligned} & NAND[NAND(\alpha_1, \alpha_2, \ldots, \alpha_n), NAND(\beta_1, \beta_2, \ldots, \beta_n), \ldots, \\ & \quad NAND(\gamma_1, \gamma_2, \ldots, \gamma_n)] \\ = \; & [(\alpha_1, \alpha_2, \ldots, \alpha_n)'(\beta_1, \beta_2, \ldots, \beta_n)' \ldots (\gamma_1, \gamma_2, \ldots, \gamma_n)']' \\ = \; & (\alpha_1, \alpha_2, \ldots, \alpha_n)'' \vee (\beta_1, \beta_2, \ldots, \beta_n)'' \vee \ldots \vee \gamma_1, \gamma_2, \ldots, \gamma_n)'' = f \end{aligned}$$

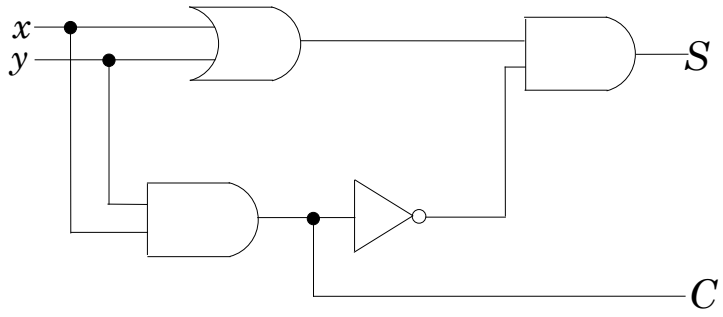
Esimerkki 7.11.2. *Konstruoidaan AND-, OR- ja NOT-porteista* puolisummain *eli piiri, jolla on kaksi sisäänmenoa x ja y sekä kaksi ulostuloa, nimittäin (1-bittisten) binäärilukujen x ja y summan oikeanpuoleinen bitti s ja sen vasen bitti c eli muistinumero (carry). Puolisummaimen totuustaulua on*

x	y	c	s
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

josta nähdään, että $s = x + y$ (eli XOR) ja $c = xy$ (eli AND). Koska $x + y = xy' \vee x'y$, on puolisummainen piiri seuraavanlainen:



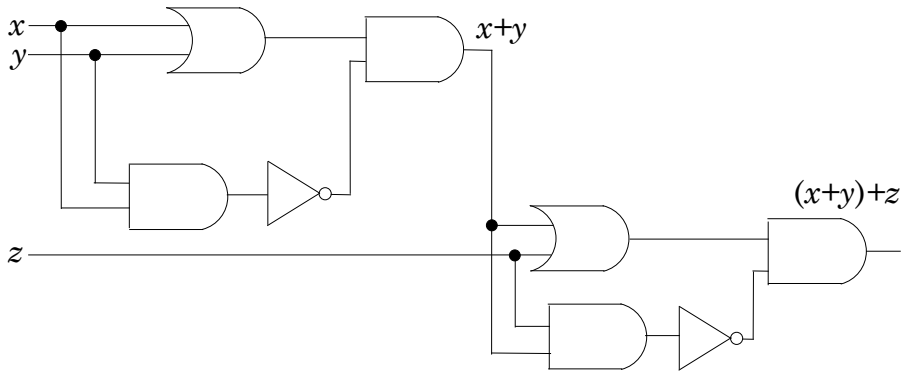
Tätä voidaan yksinkertaistaa huomaamalla, että $x + y = (x \vee y)(xy)'$, jolloin s:lle tarvitaan vain neljä porttia ja c voidaan ottaa välistä:



Esimerkki 7.11.3. *Kokosummain on piiri, jolla on kolme syöttömuuttujaa x, y ja z ja kaksi tulosmuuttujaa: $s = x + y + z$ eli binäärilukujen x, y ja z summan oikeanpuoleinen bitti ja c on tämän yhteenlaskun muistinumero (ideana on se, että z on muistinumero edellisestä yhteenlaskusta). Totuustaulu on*

x	y	z	c	s
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Koska $s = (x + y) + z$, voidaan käyttää kahta puolisummaimen "s-osaa" (eli XOR-piiriä) peräkkäin:



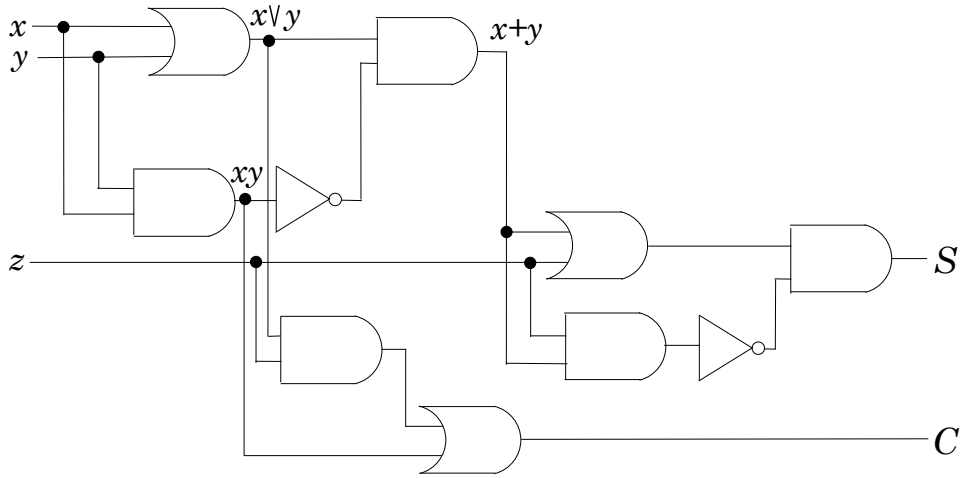
Tähän pitäisi liittää muistinumeropiiri. Sille saadaan totuustaulusta

$$\begin{aligned} c &= x'yz \vee xy'z \vee xyz' \vee xyz = x'yz \vee xy'z \vee xy \\ &= x'yz \vee x(y'z \vee y) = x'yz \vee x(z \vee y) \\ &= x'yz \vee xz \vee xy = (x'y \vee x)z \vee xy = xz \vee yz \vee xy \end{aligned}$$

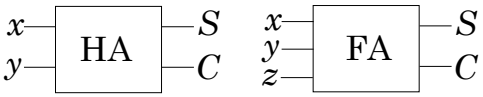
Edellä rakennetusta piiristä löytyisi valmiina jo xy ja $x \vee y$, joten muokataan c:tä vielä

$$c = xy \vee xz \vee yz = xy \vee z(x \vee y).$$

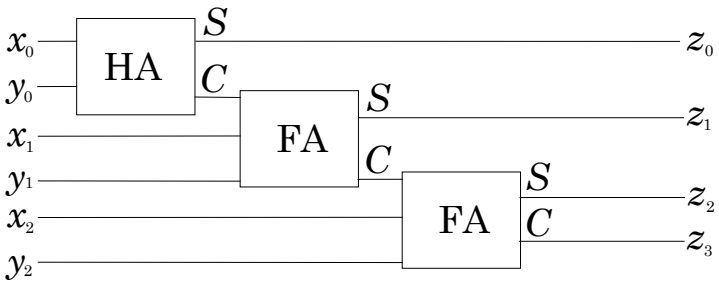
Lopputuloksena saadaan kokosummainpiiri



Merkitään puolisummainpiiriä (half-odder) laatikolla HA ja kokosummaipiiriä (full-odder) laatikolla FA.



Rakennetaan näistä piiri, joka laskee yhteen 3-bittisiä lukuja $x_2x_1x_0$ ja $y_2y_1y_0$ antaen tuloksena luvun $z_3z_2z_1z_0$.



Vastaavalla konstruktiolla voidaan periaatteessa toteuttaa yhteenlasku miten suurille binääriluvuille tahansa. Käytännössä voi esiintyä ongelmia ajoituksessa (z_n on jäljessä z_0:sta).
Suunniteltaessa kombinatorista piiriä on mahdollista, ettei kaikkia muuttujien arvojen yhdistelmiä voi esiintyä syöttönä tai piiriltä ei muuten edellytetä mitään tulosta joillakin bittikombinaatioilla. Tällaisia kombinaatioita sanotaan *don't care -ehdoiksi*. Koska piiri kuitenkin toteuttaa jonkin Boolen funktion, joka muodostaa tuloksen kaikille 2^n syöttökombinaatioille, täytyy don't care -tilanteillekin määritellä tulokset. Ne voidaan kuitenkin valita täysin vapaasti – vaikka siten, että funktion toteutus piirinä on edullisin mahdollinen.

Esimerkki 7.11.4. *Piirille syötetään binäärikoodattu desimaaliluku $xyzw$ (eli 4 bittiä). Piirin pitää tulostaa 1, jos luku on $0, 2, 3, 4, 7$ tai 8, ja 0, jos se on $1, 5, 6$ tai 9. Totuustaulussa olisi 16 riviä, joten säästetään tilaa ja kirjoitetaan toisenlainen taulukko:*

zw/xy	00	01	10	11
00	${}^{0}1$	${}^{4}1$	${}^{8}1$	d
01	${}^{1}0$	${}^{5}0$	${}^{9}0$	d
10	${}^{2}1$	${}^{6}0$	d	d
11	${}^{3}1$	${}^{7}1$	d	d

Ruutujen ylänurkkaan on merkitty, minkä luvun BCD-koodista on kyse. Esim. vaakarivin 01 ja pystyrivin 10 risteyskohdassa ruutu vastaa bittikombinaatiota $xyzw = 1001 (= 9_{10})$. Arvot 0 ja 1 on merkitty vaadittuihin paikkoihin ja d-kirjaimet osoittavat don't care -ehtoja. Arvon 0 tai 1 valinta niiden kohdalle kannattaa tehdä vasta piirin minimoinnin yhteydessä.

8 GRAAFITEORIAA

8.1 Verkkorakenteiden perusominaisuuksia

Määritelmä 8.1.1. Graafi *eli* verkko $G = (V, E)$ *koostuu äärellisistä joukoista* V *ja* E*, joista* V *on* kärkien *eli* solmujen*, ja* E sivujen *eli* särmien *eli* haarojen *joukko siten, että pätee:*

(1) Jos $e \in E$*, niin on olemassa pari* $(a, b) \in V \times V$ *siten, että* $a \in e$ *ja* $b \in e$*.*

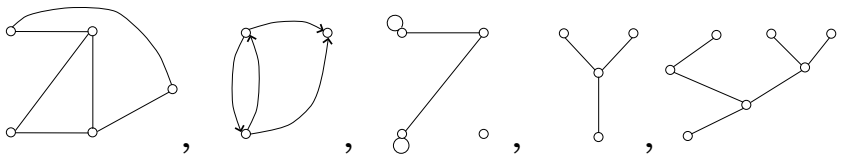
(2) Jos $e \in E$ *ja* (a, b) *on (1):ssä tarkoitettu pari, ja lisäksi*$(x, y) \in V \times V$*,* $x \in e$*,* $y \in e$*, niin on* $\{x, y\} = \{a, b\}$*.*

Määritelmä 8.1.2. *Graafin* $G = (V, E)$ *sivu* $e \in E$ *on* suunnistettu*, jos määritelmän 8.1.1 ehdossa (2) on oltava järjestetyille pareille* $(x, y) = (a, b)$*, ja* suunnistamaton*, jos molemmat parit* (a, b) *ja* (b, a) *liittyvät* e*:hen ehdon (1) tarkoittamalla tavalla. Graafi* G *on suunnistettu tai vastaavasti suunnistamaton, jos vastaava ominaisuus on sen kaikilla sivuilla.*

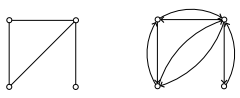
Määritelmä 8.1.3. *Graafi* $G = (V, E)$ *on* lineaarinen*, jos kullakin* $(a, b) \in V \times V$ *on korkeintaan yksi* $e \in E$ *eikä* G*:ssä ole ns.* silmukoita*, eli tyyppiä* (a, a) *olevia sivuja.* G *on* multigraafi*, jos se ei ole lineaarinen.*

Määritelmä 8.1.4. *Jos* $(a, b) \in V \times V$ *on* $e \in E$*:n määritelmän 8.1.1 mukaan määräämä kärkipari, merkitään* $e = (a, b)$*. Multigraafin tapauksessa indeksoidaan tämä tarvittaessa samaan kärkipariin liittyvien sivujen erottamiseksi. Mahdollista suunnistusta voidaan korostaa merkinnällä* $e = (\overrightarrow{a, b})$*. Suunnistetulle sivulle* $e = (\overrightarrow{a, b})$ *on* a *sivun* alku- *tai* lähtökärki *ja* b *sivun* loppu- *tai* tulokärki*.*

Huom. Graafeja voidaan esittää kuvioina:



Suunnistamaton graafi määrittelee aina erään suunnistetun graafin, kun sivut korvataan vastakkaisiin suuntiin osoittavien sivujen muodostamilla sivupareilla:

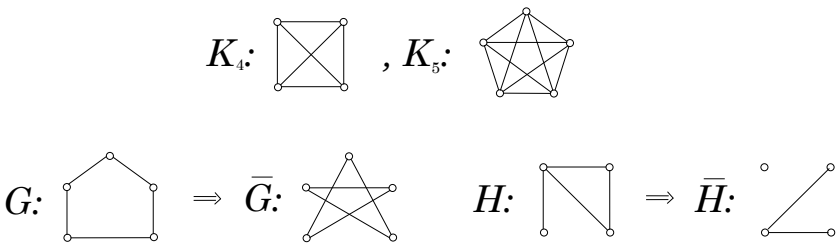


Määritelmä 8.1.5. *Graafin* $G = (V, E)$ *kärjen* $a \in V$ aste *on sivujen* $(a, b) \in E$ *tai* $(b, a) \in E$ *lukumäärä. Suunnistetun graafin kärjen* a tuloaste *on sivujen* $(\overrightarrow{b, a})$ *ja* lähtöaste *sivujen* $(\overrightarrow{a, b})$ *lukumäärä. Silmukka* $(\overrightarrow{a, a})$ *lasketaan mukaan* a*:n sekä tulo- että lähtöasteeseen, ja suunnistamaton* (a, a) *lisään astetta* 2*:lla.*

Määritelmä 8.1.6. $G_1 = (V_1, E_1)$ *on graafin* $G = (V, E)$ aligraafi*, jos* $V_1 \subseteq V$ *ja* $E_1 \subseteq E$*.*

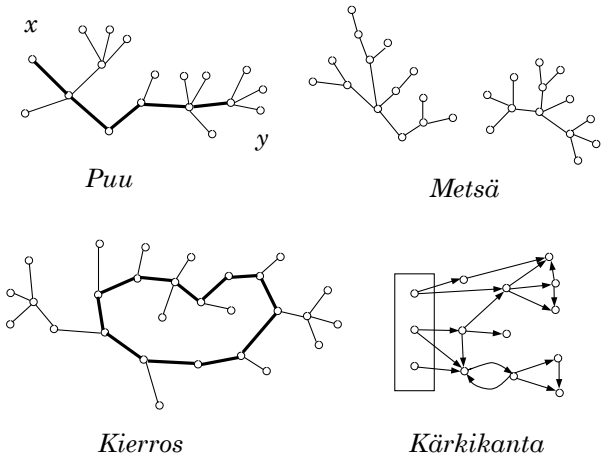
Määritelmä 8.1.7. *Lineaarinen graafi K_n on n:n pisteen* täydellinen graafi*, jos siinä on n kärkeä ja jokainen (a, b) on sivu, kun $a \neq b$. Lineaarisen graafin $G = (V, E)$* komplementti *on $\bar{G} = (V, \bar{E})$, jolla on samat kärjet kuin G:llä, mutta $(a, b) \in \bar{E} \Leftrightarrow (a, b) \notin E$, kun $a \neq b$.*

Esim.



Määritelmä 8.1.8. *Graafin $G = (V, E)$ kärjet $a, b \in V$ ovat* vierekkäiset*, jos on olemassa sivu $(a, b) \in E$ tai $(b, a) \in E$. Kärjet $x, y \in V$ ovat* yhdistetyt*, jos on olemassa ns.* tie *x:stä y:hyn. Tämä on jono sivuja $(a_0, a_1), (a_1, a_2), \ldots, (a_{k-1}, a_k)$, joiden on oltava suunnistettuja, jos G on suunnistettu graafi, ja $a_0 = x, a_k = y$. G on* yhtenäinen graafi*, jos kaikki $x, y \in G$ ovat yhdistettyjä. Polku $(a_0, a_1), (a_1, a_2), \ldots, (a_{k-1}, a_k)$, jolle $a_k = a_0$, on* kierros*. Suunnistamaton yhtenäinen lineaarinen graafi, jossa ei ole kierrosta, on* puu*. Suunnistamaton lineaarinen ei-yhtenäinen kierrokseton graafi on* metsä*.*
Suunnistetun graafin kärkikanta *on minimaalinen kärkijoukko V_1, josta lähtevillä suunnistuksen suuntaisilla poluilla voi saavuttaa kaikki kärjet $y \in V - V_1$.*

Esim.



Määritelmä 8.1.9. *Graafit $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ ovat* isomorfiset*, $G_1 \sim G_2$, jos on olemassa kääntäen yksikäsitteinen kuvaus $f : G_1 \to G_2$, jolle $f(V_1) = V_2, f(E_1) = E_2$ ja $(a, b) \in E_1 \Rightarrow f((a, b)) = (f(a), f(b)) \in E_2$.*

Lause 8.1.10. *Jos graafit $G_1 \sim G_2$, niin näiden vastakärkien $a, f(a)$ asteet ovat samat. Jos $H_1 \subset G_1$ on G_1:n aligraafi ja isomorfiassa $f : G_1 \to G_2$ on $f(H_1) = H_2 \subset G_2$, niin on $H_1 \sim H_2$.*

Lause 8.1.11. *Graafit $G_1 \sim G_2$, jos ja vain jos niiden komplementeille pätee $\bar{G}_1 \sim \bar{G}_2$.*

Todistus. Nämä seuraavat välittömästi esitetyistä määritelmistä. ■

Lause 8.1.12. *Jos $G = (V, E)$ ja $|V| = n$, $|E| = m$, ja kärkien asteet ovat $d(a_i), i = 1, 2, \ldots, n$, niin $\sum_{i=1}^{n} d(a_i = 2m$.*

Todistus. $\sum_{i=1}^{n} d(a_i =$ niiden tapausten lukumäärä, joissa jokin sivu osuu johonkin kärkeen. Toisaalta kukin sivu osuu kahteen kärkeen (silmukalla $(a, a) \in E$ osuma kahdesti samaan kärkeen), joten sivu-kärki -osumia on yhteensä $2m$. Nyt seuraa heti. ■

Lause 8.1.13. *Graafin G paritonta astetta olevien kärkien lukumäärä on parillinen.*

Määritelmä 8.1.14. *Graafin $G = (V, E)$* riippumaton joukko *on $V_1 \subseteq V$, jolle $a, b \in V_1 \Rightarrow (a, b) \notin E$. G:n* dominoiva joukko *on $D \subseteq V$, jolle $x \in V \Rightarrow \exists d \in D : (d, x) \in E$. Aligraafi $G_1 \subseteq G$ on* klikki, *jos G_1 on täydellinen, eikä ole olemassa täydellistä aligraafia $G_2 \neq G_1$, jolle $G_1 \subset G_2 \subseteq G$.*

Määritelmä 8.1.15. *Olkoon $G = (V, E)$ lineaarinen suunnistettu graafi, ja sen kärjet ja sivut luetteloitu järjestyksiin $x_1, x_2, \ldots, x_n$ ja $e_1, e_2, \ldots, e_m$. G:n* naapurimatriisi *on $n \times m$- matriisi $C = c_{ij}$, jolle $c_{ij} = 1$, jos $(\overrightarrow{x_i, x_j}) \in E$ ja $c_{ij} = 0$ muuten. G:n* insidenssimatriisi *on $n \times m$-matriisi $B = (b_{ij})$, ja $b_{ij} = -1$, jos e_n alkaa$= 1$, jos loppuu x_i:stä, ja $= 0$, muuten.*

Huom. Sekä C että B sisältävät yleensä paljon 0:ia alkioina. Tilaa säästävämpiä esitystapoja graafille olisivat:

(1) Muodostetaan ns. *naapuriluettelo*: Muistipaikoille $1, 2, \ldots, n, \ldots$ merkitään jonoon luettelo kärjistä, joihin kulloinkin vuorossa olevasta kärjestä lähtee sivu. Apuna on oltava ns. *indeksilista*, johon on merkitty kärjen numero i kohdalle sen muistipaikan osoite, josta x_i:n tiedot alkavat. Ellei x_i:stä lähde sivua, merkitään tähän 0 tai muu olematon osoite.

(2) Luetteloidaan sivut $m \times 2$-matriisin k:s vaakarivi koostuu sivun $e_k = (\overrightarrow{x_i, x_j})$ kärkien numeroista (i, j).

(3) *Ketjutettu lista:* Nytkin kärjen x_i tietojen *alkuosoite* on *indeksilistalla* kohdassa i. Alkuosoitteen osoittamalla paikalla *tietolistalla* on ensimmäinen tieto x_i:n naapureista. Tämän rinnalla on *osoitinlista*, josta luetaan *seuraavan* x_i-tiedon osoite jne., kunnes tiedot loppuvat ja osoitinlistalla on 0 (tms.). Jos on tarpeen siirtyä listalla molempiin suuntiin, olisi ylläpidettävä myös toista osoitinlistaa edellisiä osoitteita varten. Näiden rinnalla voi pitää erillistä *vapaiden osoitteiden listaa*, ja sen viimeistä alkiota osoittavaa osoitinta. Jos nyt sivu $(\overrightarrow{x, y})$ poistettaisiin graafista, poistetaan y:n osoite x:n tiedoista, ja korjataan seuraavaa osoitteen listalle y:n seuraava osoite, sekä täällä edelliseksi osoitteeksi x:n osoite. Samalla y:n osoite voidaan merkitä vapaiden osoitteiden listan viimeiseksi, ja kasvattaa vapaan osoitteen osoitinta 1:llä. Jos graafiin lisätään sivu $(\overrightarrow{x, z})$, sijoitetaan arvo z vapaiden osoitteiden listan viimeiseen osoitteeseen, vähennetään 1:llä vapaan osoitteen

osoitinta, ja muutetaan x:n listan osoittimia siten, että z:n osoite tulee mukaan. Suunnistamattomat sivut vastaavat tässä kahta sivua $(\overrightarrow{a,b})$ ja $(\overrightarrow{b,a})$. Jos jokin kärki poistetaan kokonaan, asetetaan tämän kohdalle indeksilistalle 0 ja poistetaan kaikki siihen liittyneet sivut. Vastaavasti voi lisätä kärkiä. Suunnistamattomassa graafissa ovat näillä listoilla aina molemmat sivut $(\overrightarrow{a,b})$ ja $(\overrightarrow{b,a})$, ja jos suunnistettua graafia tulisi varautua lukemaan myös "vastavirtaan", olisi joko ylläpidettävä toista tietolistaa tätä varten tai sisällytettävä nytkin listoihin molemmat parit ja merkittävä erikseen sivun suunta.

(4) Näitä esityksiä voisi soveltaa myös multigraafeille, jos esim. sivuja x:stä y:hyn olisi k kpl, voisi y olla k kertaa x:n naapuriluettelossa jne.

(5) Pienehköjä graafeja voi esittää havainnollisesti kuvioina: kärjet merkitään pisteinä tasoon (tms.) ja sivut näitä yhdistävinä kaarina.

8.2 Eulerin ja Hamiltonin kierrokset

Esim. (Königsbergin siltaprobleema) Königsbergissä Itä-Preussissa 1800-luvulla oli käytettävissä kuvion mukaiset sillat Pregel-joen saarien ja rantojen välillä. Kysymys: Onko mahdollista tehdä kävelyretki siten, että jokaisen sillan kautta kuljettaisiin tasan yhden kerran?

Todetaan: Tilannetta voi kuvata multigraafilla jossa on 4 kärkeä, joiden asteet ovat $d(a) = d(c) = d(d) = 3, d(b) = 5$. (Kärjet maa-alueita, sivut siltoja)

Määritelmä 8.2.1. *Graafin* $G = (V, E)$ Eulerin reitti *on reitti* $(a_0, a_1)_1, (a_1, a_2)_1, \ldots, (a_{n-1}, a_n)_k$, *missä jokainen sivu* $(a, b)_i \in E$ *on mukana, ja jokainen kärki on mukana vähintään kerran. Eulerin polku on* Eulerin kierros, *jos lisäksi on* $a_n = a_0$. ■

Lause 8.2.2. *Suunnistamattomalla graafilla G on Eulerin kierros, jos ja vain jos G on yhtenäinen ja sen kaikkien kärkien asteet ovat parillisia. G:llä on Eulerin reitti, joka ei ole Eulerin kierros, jos ja vain jos G on yhtenäinen ja sillä on tasan kaksi kärkeä, joiden aste on pariton.*

Todistus. (1) Eulerin kierros kulkee kaikkien kärkien kautta, mistä seuraa G:n yhtenäisyys. Jos b on kierroksen sisällä oleva kärki, lisääntyy $d(b)$ 2:lla, kun kierros kulkee b:n kautta, myös silmukan (b, b) tapauksessa (vrt. määritelmä 8.1.5). Alkukärjessä a ovat myös kierroksen ensimmäinen ja viimeinen sivu erillisiä, joten niistäkin tulee lisäys 2 asteeseen $d(a)$. Siis asteet ovat parillisia, jos G:ssä on Eulerin kierros.
(2) Olkoon G yhtenäinen ja kaikki kärjet parillista astetta. Muodostetaan polkuja lähtien eri kärjistä. Kärjestä a lähtevä polku ei pysähdy kärkeen $b \neq a$, koska $d(b)$ on parillinen: on olemassa sivu myös b:stä lähtöä varten, jos polku on sinne tullut. Jo käytetyt sivut jätetään aina pois, ja jatketaan polkujen muodostusta, kunnes kaikki sivut on käytetty. Näin syntyy joukko kierroksia G:hen. Jos näitä on enemmän kuin yksi, on niiden kuitenkin kohdattava toisiaan

joissakin kärjissä, koska G on yhtenäinen. Kaksi kierrosta C_1, C_2 voidaan nyt yhdistää sijoittamalla C_2 yhteisestä kärjestä c alkaen ja siihen loppuen C_1:n väliin. Näin jatkaen päädytään Eulerin kierrokseen G:ssä.
(3) Yhdistämällä lisäsivulle Eulerin polun alku- ja loppukärjet tai kaksi parittoman asteen kärkeä, saadaan loput väitteet palautetuiksi edelliseen. ■
Esim. (jatk.) Königsbergin siltagraafissa on 4 kärkeä, joiden aste on pariton, joten sillä ei ole Eulerin kierrosta eikä edes Eulerin polkua. Vaaditun kaltainen kävelyretki on siis mahdoton.

Määritelmä 8.2.3. *Graafin $G = (V, E)$* Hamiltonin polku *on G:n polku, jolla jokainen $a \in V$ esiintyy tasan yhden kerran. Hamiltonin polku on* Hamiltonin kierros, *jos G:ssä lisäksi on sivu Hamiltonin polun loppupisteestä sen alkupisteeseen.*

Huom. Hamiltonin kierrosta C muodostettaessa pätee:

(1) On oltava $d(a) \geq 2$ kaikille $a \in V$. Jos $d(a) = 2$, on molempien a:n kautta kulkevien sivujen oltava C:llä

(2) C:llä ei voi olla osana G:n aitoa osakierrosta, eli kierrosta, jolta puuttuu jokin $b \in V$.

(3) C käyttää tasan kahta kärjen $x \in V$ kautta kulkevaa sivua. C:tä muodostettaessa voi siis x:n ohittamisen jälkeen rajoittaa aligraafin, josta on poistettu muut sivut, joilla x on.

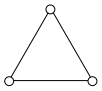
Lause 8.2.4. *Olkoon $G = (V, E)$, $|V| = n$, suunnistamaton ja G:ssä ei ole silmukoita. G:ssä on Hamiltonin polku, jos $d(x) + d(y) \geq n - 1$ kaikille $x, y \in V, x \neq y$.*

8.3 Tasograafeista

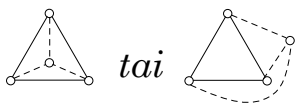
Esimerkki 8.3.1. *Täydellinen suunnistamaton graafi K_4*

K_4: 

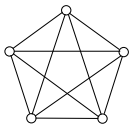
voidaan piirtää tasoon lähtemällä kolmiosta K_3

K_3: 

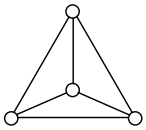
ja lisäämällä siihen 4. kärki ja siihen liittyvät sivut. Tämän voi tehdä niin, että ei synny toisiaan leikkaavia sivuja piirrettävään kuvioon:



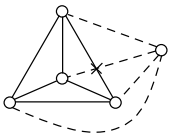
Jos edelleen graafi K_5

K_5: 

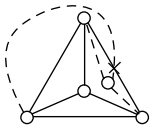
yritettäisiin piirtää niin, että leikkauksia ei olisi (paitsi tietenkin kärjissä), olisi siis kuvioon



lisättävä yksi kärki ja siitä lähtevät 4 sivua. Jos lisäys tapahtuu kuvion ulkopuolella, voi sisällä olevan kärjen tavoittaa vain leikkaamalla vanhaa sivua:

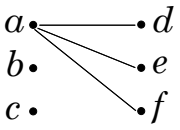


Jos taas lisäys suoritetaan jonkin pikkukolmion sisään on 4. vanhan kärjen saavuttamisesksi leikattava ko. pikkukolmion sivua:

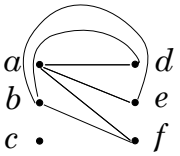


Edelleen: Jotta eri kärkien asteet tulisivat kuviosta oikein esille, ei uutta kärkeä voi sijoittaa vanhalle sivulle tai uutta sivua piirtää vanhan kärjen kautta. Siis: Graafia K_5 ei voi piirtää tasoon ilman, että jotkin sivut leikkaavat muualla kuin kärjessä.

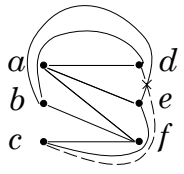
Esimerkki 8.3.2. *Pyritään yhdistämään 3 pistettä a, b, c parittain toisiin 3 pisteeseen d, e, f siten, että tasokuviossa ei olisi leikkaavia yhdistyskaaria. Aluksi yhdistetään a pisteisiin d, e, f:*



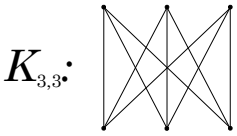
Sitten yhdistetään b:



(Muut mahdolliset kuviot olisivat tämän kanssa topologisesti ekvivalentteja: tarvittaessa suoritetaan kuvaus, jolla se alue, jolla c on, viedään sivujen rajoittaman alueen ulkopuoliseksi alueeksi)
Pistettä c ei nyt voi yhdistää kaikkiin pisteisiin d, e, f leikkaamatta jotakin sivua (tai kulkematta jonkin ylimääräisen kärjen kautta):



Saatua graafia $K_{3,3}$



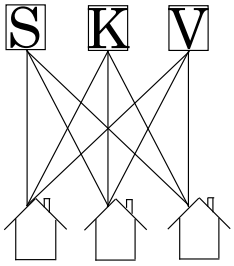
ei siis myöskään voi piirtää tasoon ilman em. tavalla leikkaavia sivuja.

Määritelmä 8.3.3. *Graafi $G = (V, E)$ on* tasoittuva graafi*, jos sillä on olemassa* tasoesitys*, jossa kärjet vastaavat eräitä tason pisteitä, ja sivut kärkiä tasossa yhdistäviä kaaria,joilla ei ole muita yhteisiä pisteitä kuin sivujen yhteisiä kärkiä vastaavat pisteet päätepisteinään.*

Määritelmä 8.3.4. *Graafit $G_1 = (V_1, E_1)$ ja $G_2 = (V_2, E_2)$ esittävät samaa* konfiguraatiota*, jos graafit, jotka saadaan näistä linearisoimalla, ja jättämällä pois suunnistukset ja astetta 2 olevat kärjet, jolloin poistettaessa polulta $(a, b), (b, c)$ kärki b, on tarvittaessa lisättävä sivu (a, c), ovat isomorfiset.*

Lause 8.3.5. *Graafi $G = (V, E)$ on tasoittuva graafi, jos ja vain jos se ei sisällä aligraafinaan konfiguraatiota K_5 tai $K_{3,3}$.*

Todistus. Jos K_5 tai $K_{3,3}$ on G:ssä, ei G esimerkkien 8.3.1 ja 8.3.2 mukaan ole tasograafi. Todistus käänteiseen suuntaan sivuutetaan. ■
Huom. K_5:ttä sanotaan *tähtigraafiksi*, ja $K_{3,3}$:a *laitosgraafiksi*:
”Yhdistettävä sähkö-, kaasu- ja vesilaitokset kolmeen taloon niin, että ko. johdot eivät mene ristikkäin”, siis:



Lause 8.3.6. *Olkoon $G = (V, E)$ on yhtenäinen tasoittuva graafi, $|V| = v$, $|E| = e$, niin sen jokaisessa tasoesityksessä on tasoalueiden lukumäärä $r = e - v + 2$.*

Todistus. (1) Jos $e = |E| = 0$, on yhtenäisyyden vuoksi oltava $v = |V| = 1$, ja tasoalueita on yksi: koko taso, josta on poistettu ainoata kärkeä esittävä piste. Näille pätee $1 = 0 - 1 + 2$.
(2) Induktio-oletus: $r = e - v + 2$, jos $e < n$. Olkoon sitten $e = n$. Erotetaan tapaukset:
(a) G:ssä on astetta 1 oleva kärki y: tätä esittää jonkin osa-alueen sisään päättyvä kaari (x, y). Jos y ja sivu (x, y) jätetään pois, on uudessa graafissa G' : $|E'| = n - 1$ ja $|V'| = v - 1$, eikä sivun (x, y) poisto muuta alueiden lukumäärää r. Nyt on siis: $r = |E'| - |V'| + 2 = (n - 1) - (v - 1) + 2 = e - v + 2$.
(b) G:n kaikkien kärkien aste ≥ 2. Olkoon (x, y) eräs sivu, joka on osa-alueiden A_0, A_1 rajalla, ja A_0 ääretön osa-alue. Jos $x \neq y$, sivun (x, y) poisto ei poista kärkiä x, y, ja jos $x = y$, on tämä joko graafin ainoa kärki, joka jätetään jäljelle, tai vielä yhdistetty muuhun graafiin yhtenäisyyden perusteella. Kaikissa näissä tapauksissa alueet A_0, A_1 yhdistyvät, ja uudelle graafille G' on $|E'| = n-1, |V'| = |V| = v$ ja $r' = r-1$. Siis: $r' = |E'|-|V'|+2$, joten $r-1 = n-1-v+2$ eli $r = e - v + 2$. ■

Lause 8.3.7. *Olkoon $G = (V, E)$ yhtenäinen lineaarinen tasoittuva graafi, $|V| = v$, $|E| = e$, $e > 1$ ja $r =$ alueiden lukumäärä tasoesityksessä. Tällöin on $3r \leq 2e$ ja $e \leq 3v - 6$.*

Todistus. Pareja (alue, reunasivu) on $\leq 2e$, koska kukin sivu on kahden osa-alueen reunan osana (ääretön alue mukaanlukien), tai jotkin sivut päättyvät astetta 1 olevaan kärkeen, jääden pois em. parien luettelosta. Toisaalta kullakin alueella on vähintään 3 reunasivua, koska G on lineaarinen. Siis em. pareja on $\geq 3r$ kpl, joten $3r \leq 2e$. Nyt on edelleen lauseen 8.3.6 mukaan: $0 = v - e + r - 2 \leq v - e + \frac{2}{3}e - 2 = v - \frac{1}{3}e - 2$, joten $e \leq 3v - 6$. ■
Esim. Tähtigraafille K_5 on $v = 5$, $e = \binom{5}{2} = 10$, joten $3v - 6 = 9 < 10 = e \Rightarrow K_5$ ei ole tasograafi. Toisaalta laitosgraafille $K_{3,3}$ on $v = 6$, $e = 9$, joten $3v-6 = 12 > 9 = e$, vaikka $K_{3,3}$ ei olekaan tasograafi. Todetaan: $K_{3,3}$:ssa ei ole kolmioita, vaan mahdollisten alueiden reunoilla olisi vähintään 4 sivua. Jos $K_{3,3}$ olisi tasograafi, olisi siis $4r \leq 2e = 18$, mutta toisaalta olisi $4r = 4(e - v + 2) = 4 \cdot (9 - 6 + 2) = 20$.

Määritelmä 8.3.8. *Olkoot $A_1, \ldots, A_r$ osa-alueet tasograafin $G = (V, E)$ tasoesityksessä. G:n eräs* duaaligraafi *G^d muodostuu kärjistä $x_j \in A_j, j = 1, \ldots, r$ ja sivuista $s_k, k = 1, \ldots, e$, siten, että s_k yhdistää ne tai sen x_i, x_j, jotka ovat sivun $e_k \in E$ eripuolisissa alueissa.*

Huom. Myös G^d on eräs tasograafi.

8.4 Graafien värityksistä

Esim. Väritettävä oheinen kartta siten, että naapurimaat ovat erivärisiä:

Ilmeisesti kolme väriä riittää, ja on myös tarpeen. Jos tason ääretön alue (U) olisi viiden ”maa”, tarvittaisiin vielä 4. väri tätä varten. Kartan duaaligraafi olisi nyt

Kartan värittäminen olisi nyt ekvivalenttia duaalin väritykselle seuraavasti:

Määritelmä 8.4.1. *Graafin $G = (V, E)$* väritys *on kuvaus $\varphi : V \to C$, missä C on äärellinen, ns. värien, joukko, ja jolle pätee: jos $a \neq b$, ja on olemassa sivu $(a, b) \in E$ tai $(b, a) \in E$, niin $\varphi(a) \neq \varphi(b)$. Jos on olemassa G:n väritys, kun $|C| = k$, on G k-väritettävissä. G:n* kromaattinen luku *$\gamma(G)$ on pienin k, jolla G on k-väritettävissä. G on* värikriittinen, *jos G:n kromaattinen luku alenee, kun G:stä poistetaan jokin kärki siihen kuuluvine sivuineen.*

Lause 8.4.2. *Jos G:n suurin klikki on k-kärkinen, niin $\gamma(G) \geq k$.*

Lause 8.4.3. *Jos G on lineaarinen, ei täydellinen, ja kärkien maksimiaste $d \geq 3$, niin $\gamma(G) \leq d$.*

Lause 8.4.4. *Olkoon $k \in \mathbb{N}$. On olemassa graafi $G = (V, E)$, jolle $\gamma(G) = k$, vaikka G:ssä ei ole aligraafina kolmiota K_3.*

Lause 8.4.5. *Olkoon $G = (V, E)$:ssä $E \neq \emptyset$. $\gamma(G) = 2$, jos ja vain jos G:ssä ei ole yhtään parittoman monta sivua sisältävää kierrosta.*

Määritelmä 8.4.6. *Yhtenäinen graafi G, jolle $\gamma(G) = 2$ on* kaksijakoinen.

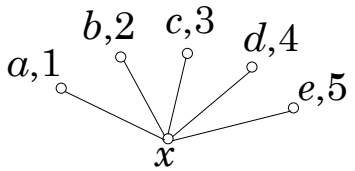
Esim. Laitosgraafi $K_{3,3}$ on 2-jakoinen. Tähtigraafille K_5 on ilmeisesti $\gamma(K_5) = 5$.

Lause 8.4.7. *Tasograafille on $\gamma(G) \leq 4$.*

Huom. Tämä on ns. *neliväriprobleema*, joka on todistettu muodostamalla 4-väritykset joukkoon konfiguraatioita, joka puolestaan on osoitettu kattavaksi, eli että kaikki tasograafien väritystehtävät palautuvat näihin. Tarpeellisten alatapausten määrä oli lähes 2000. Työ on tehty tietokoneella v. 1976.

Lause 8.4.8. *Tasograafille on $\gamma(G) \leq 5$.*

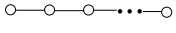
Todistus. (1) Jos olisi $d(a) \geq 6$ kaikilla $a \in V$, niin $2e = \sum_k d(a_k) \geq 6v$. Toisaalta on $e \leq 3v - 6$, joten on olemassa kärki, jolle $d(a) \leq 5$.
(2) Jos $v = 1$, on $\gamma(G) = 1 \leq 5$. Induktio-oletus: Jos $v' = |V'| \leq n - 1, n \geq 2$, on $G' = (V', E')$ 5-väritettävissä. Olkoon $G = (V, E)$, ja $|V| = n, n \geq 2$, ja olkoon $x \in V$:lle $d(x) \leq 5$. Nyt on $G' = G - \{x\}$ induktio-oletuksen mukaan 5-väritettävissä. Jos $d(x) \leq 4$, on eräs 5:stä väristä käytettävissä heti x:n väriksi, samoin jos $d(x) = 5$ ja joillakin x:n naapureista on sama väri, jää eräs väri vapaaksi. Olkoot siis x:n naapurit a, b, c, d, e ja niillä värit $1, 2, 3, 4, 5$:



Tarkastellaan aluksi kaikkia a:sta lähteviä polkuja, joilla on vain värejä 1 ja 3 (vuorotellen!). Jos näistä mikään ei johda c:hen, voi värit 1 ja 3 vaihtaa näillä poluilla, jolloin a:n väriksi tulee 3 ja 1 vapautuu x:lle. Jos taas jokin $1-3$-polku johtaa a:sta c:hen, tämä yhdessä sivujen (c, x) ja (x, a) kanssa muodostaa kierroksen. Koska G on tasograafi, jonka tasoesityksessä kärjet ovat kuvatussa järjestyksessä, ei ole vastaavaa $2-4$-polkua b:stä d:hen. Nyt voi b:stä alkavilla $2-4$-poluilla vaihtaa värit, jolloin b:n väriksi tulee 4, ja x:lle jää väri numero 2.
Siis: $\gamma(G) \leq 5$, kun $G = (V, E)$ on tasograafi. ■

Määritelmä 8.4.9. *Olkoon $G = (V, E)$ suunnistamaton lineaarinen graafi. G:n* kromaattinen polynomi $P_G(\lambda)$ *on polynomi, jolle $P_G(k)$ on G:n eri k-väritysten lukumäärä.*

Esim.(1) $|V| = n, E = \emptyset \Rightarrow P_G(\lambda) = \lambda^n$
(2) $G = K_n \Rightarrow P_G(\lambda) = \lambda(\lambda-1)\cdot\ldots\cdot(\lambda-n+1)$, tulosäännöllä
(3) Olkoon G yksinkertainen n-kärkinen polku, ei kierros $\Rightarrow P_G(\lambda) = \lambda(\lambda-1)^{n-1}$:



(4) $G = C_1 \cup \ldots \cup C_k$, missä $(i \neq j, a_i \in C_i, b_j \in C_j \Rightarrow (a_i, b_j) \notin E) \Rightarrow P_G(\lambda) = P_{C_1}(\lambda)\cdot\ldots\cdot P_{C_k}(\lambda)$.

Lause 8.4.10. *Olkoon $G = (V, E)$ suunnistamaton, lineaarinen ja yhtenäinen graafi. Merkitään sivulle $e \in E$: $G_e =$ aligraafi, jossa sivu $e = (A, b)$ on poistettu G:stä, mutta ei kärkiä a, b, ja G'_e muodostettu G_e:stä samaistamalla kärjet a, b ja linearisoimalla. Tällöin on*

$$P_{G_e}(\lambda) = P_G(\lambda) + P_{G'_e}(\lambda)$$

Todistus. G_e:n värityksissä ne, joille $\varphi(a) \neq \varphi(b)$, ovat myös G:n värityksiä, ja jos $\varphi(a) = \varphi(b)$, ei saada G:n, vaan G'_e:n aidot väritykset. ■
Huom. Tätä voi käyttää ”hajoittamalla” graafi osiin, joiden polynomit voidaan muodostaa, tai myös lisäämällä sivuja, kunnes saadaan täydellinen graafi: G_e^+ : uusi sivu $e = (a, b)$, ja G_e^{++} : kärjet a, b samoiksi $\Rightarrow P_G(\lambda) = P_{G_e^+}(\lambda) + P_{G_e^{++}}(\lambda)$.

Lause 8.4.11. *Olkoon G suunnistamaton graafi, jolla on aligraafit G_1, G_2 siten, että $G = G_1 \cup G_2$ ja $G_1 \cap G_2 = K_n$. Tällöin on $P_G(\lambda) = \frac{P_{G_1}(\lambda)\cdot P_{G_2}(\lambda)}{\lambda(\lambda-1)\cdot\ldots\cdot(\lambda-n+1)}$.*

Todistus. Koska $G_1 \cap G_2 = K_n$, on K_n:n aligraafina G_1:ssä ja G_2:ssä, jolloin $\gamma(G_1), \gamma(G_2) \leq n$. K_n:llä on $\lambda(\lambda-1)\cdot\ldots\cdot(\lambda-n+1)$ väritystä. Kutakin näistä vastaa $\frac{P_{G_i}(\lambda)}{\lambda(\lambda-1)\cdot\ldots\cdot(\lambda-n+1)}$ tapaa värittää G_i:n loput kärjet, $i = 1, 2$. Näistä seuraa väite tulosäännöllä (K.1.4).?? ■

Määritelmä 8.4.12. *Graafin $G = (V, E)$* sivuväritys *on kuvaus φ, joka kuvaa E:n värijoukkoon siten, että $\varphi(e_1) \neq \varphi(e_2)$, jos $e_1 \neq e_2$ ja niillä on yhteinen kärki.*

Huom. Seuraava palauttaa tämän kärkivärityksen:

Määritelmä 8.4.13. *Graafin $G = (V, E)$* viivagraafi $L(G)$ *on suunnistamaton graafi, jonka kärkinä ovat sivut $e \in E$ ja $L(G)$:ssä on $e_1, e_2 \in E$:n välillä sivu, jos ja vain jos e_1:llä ja e_2:lla on G:ssä yhteinen kärki.*

Lause 8.4.14. *Jos d on G:n kärkien maksimiaste, tarvitaan G:n sivuväritykseen vähintään joko d tai $d+1$ väriä.*

8.5 Puista

Määritelmä 8.5.1. *Aligraafi $T \subseteq G$ on G:n* virittäjäpuu, *T on puu, ja kaikki G:n kärjet ovat kärkinä T:ssä.*

Lause 8.5.2. *Suunnistamattoman puun $T = (V, E)$ kärkien $a, b \in V$ välillä on 1-käsitteinen polku. Suunnistamaton graafi G on yhtenäinen, jos ja vain jos sillä on olemassa virittäjäpuu.*

Lause 8.5.3. *Puulle $T = (V, E)$ pätee: $|V| = |E| + 1$ ja jos $|V| \geq 2$, on T:ssä ainakin kaksi kärkeä, joiden aste on 1.*

Todistus. $|V| = |E| + 1$ voidaan todistaa induktiolla. Jos $|V| = n \geq 2$, on siis $|E| = n - 1$, ja edelleen $2(n-1) = 2|E| = \sum_{a \in V} d(a)$. Jos nyt $d(a) \geq 2$, olisi $\sum_{a \in V} d(a) \geq 2|V| = 2n$. Tämä on ristiriita, jonka poistaminen vaatii 2 astetta 1 olevaa kärjen olemassaoloa, kun toisaalta eristettyjä kärkiä ei ole. ■
Huom. Jos G on *epäyhtenäinen*, voisi puhua vastaavasti sen *virittäjämetsästä*.

Määritelmä 8.5.4. *Suunnistettu graafi $G = (V, E)$ on* suunnistettu puu, *jos siitä tulee puu, kun suunnistus poistetaan ja se linearisoidaan. Suunnistettu puu on* juurrutettu, *jos on olemassa tasan yksi kärki $r \in V$, ns.* juuri, *jonka tuloaste $d^+(r) = 0$, ja kaikille muille kärjille on $d^+(x) = 1$. Kärjet, joiden lähtöaste $d^-(x) = 0$, ovat puun* lehtiä, *muut kärjet* sisäkärkiä.
Jos kaikkien sisäkärkien lähtöaste on $d^-(x) = m$, on G m-puu. Kärjen $x \in G$ taso *on polulla r:stä x:ään olevien sivujen lukumäärä, eli ko. polun pituus. G:n* korkeus *h on sen kärkien maksimitaso. G on* balansoitu, *jos kaikki lehdet ovat tasoilla h tai $h-1$. Kärjen $x \neq r$* isä *on y, jolle $(\overrightarrow{y,x} \in E$, ja tällöin x on y:n* poika. *Jos myös $(\overrightarrow{y,z} \in E$, ovat x ja z* veljeksiä. *Kärjet, joista on suunnistettu polku x:ään ovat x:n (esi)*vanhempia *ja kärjet, joihin x:stä on suunnistettu polku, ovat x:n* jälkeläisiä. *G:n x-*alipuu *on aligraafi, jossa on x ja sen kaikki jälkeläiset vastaavine sivuineen.*

Huom. m-puuta, jolle $m = 2$, sanotaan usein *binääripuuksi*, ja puuta, jolle $m = 3$, *ternääripuuksi* jne.

Lause 8.5.5. *Onkoon m-puussa $G = (V, E)$ $|V| = n$ ja k lehteä sekä s sisäkärkeä. Tällöin on $n = ms + 1$, $k = (m-1)s + 1$, $s = \frac{k-1}{m-1} = \frac{n-1}{m}$.*

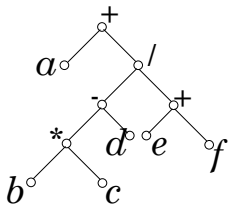
Määritelmä 8.5.6. *Juurrutetun puun kärkien* universaaliosoitteet *muodostetaan seuraavasti:*
(1) Juuren osoite $= 0$.
(2) Tason 1 kärjille merkitään osoitteen $1, 2, \ldots$. Jos kuviossa juuri on ylinnä, tehdään tämä vasemmalta oikealle.
(3) Olkoon $v \in V$ sisäkärki tasolla $n \geq 1$, ja $v_1, \ldots, v_k$ sen pojat. Jos v:n osoitemerkki on a, merkitään $v_1, \ldots, v_k$ (vasemmalta oikealle): $a.1, \ldots, a.k$. Osoitteille b, c on $b < c$ sanakirjajärjestyksessä, *jos on (1) $b = a_1 \cdot \ldots \cdot a_m, c = a_1 \cdot \ldots, a_m \cdot a_{m+1} \cdot \ldots \cdot a_n$, missä $m < n$, tai (2) $b = a_{1.m} \cdot a_m \cdot x_1 \cdot \ldots \cdot y, c = a_{1.m} \cdot a_m \cdot x_2 \cdot \ldots z$, ja $x_1 < x_2$.*

Määritelmä 8.5.7. Palautuva haku *(backtracking, depth-first-search) juurrutetussa puussa kulkee juuresta lähteviä polkuja pitkin lehtiin asti palaten aina tasolle n olevan kärjen x kautta*

niihin x:n alipuihin, joita ei vielä ole kierretty. Kun kaikki x:stä lähtevät alipuut on kierretty, palataan x:n isään tasolle $n-1$ ja jatketaan tästä tämän muihin poikiin. Laajeneva haku *(breadth-first-search) lähtee puun juuresta, kulkee sitten kaikki tason 1 kärjet, ja aina tason n kärkien jälkeen kaikki tason $n+1$ kärjet.*

Määritelmä 8.5.8. *Palautuvaan hakuun liittyen voidaan puun $T=(V,E)$ kärjille antaa järjestyksiä seuraavin tavoin: Kun kärjelle x on kerran annettu numero, ei sitä prosessin kuluessa enää muuteta, ja saavuttaessa kärkeen x, josta lähtee alipuut $T_1, T_2, \ldots, T_k$, numeroidaan näiden kärjet*
(a) esijärjestystä *noudatettaessa ensin x ja sitten T_1:n, T_2:n, …, T_k:n kärjet,*
(b) jälkijärjestyksessä T_1*:n, T_2:n, …, T_k:n kärjet ja näiden jälkeen x,*
(c) välijärjestyksessä *ensin T_1:n kärjet, sitten x, ja sitten T_2:n, …, T_k:n kärjet.*

Esim. Merkitään laskulausekkeen $a+\frac{bc-d}{e+f}$ operandit binääripuun lehdiksi ja laskutoimitusmerkit sisäkärkiin:



Tämän kierto *välijärjestyksessä*vastaa nyt laskujärjestystä $a+((b*c)-d)/(e+f)$. Sulkumerkkivapaaseen esitykseen (joka on tarpeen esim. generoitaessa konekielistä ohjelmaa, joka tietokoneessa todella laskisi ko. lausekkeen arvon!) päästään esim. ns. *puolalaista merkintätapaa käyttäen*:
Laskutoimitusta $x \odot y$ merkitään $\odot xy$:llä, jolloin yo. puun *esijärjestys* olisi: $+a/-*bcd+ef$. Tämä lasketaan oikealta vasemmalle: Uudet operandit sijoitetaan *pinomuistiin* alimmaksi, laskutoimitus operoi kahteen pinon alimpaan lukuun ja jättää tuloksen näiden sijasta pinoon alimmaksi (jotkin operaatiot voivat näin vaikuttaa vain yhteen operandiin, esim. $|x|$ jne.).

Algoritmi 8.5.9. *Olkoon $G=(V,E)$ yhtenäinen ja suunnistamaton. G:n* virittäjäpuun $T=(V,E')$ *muodostamiseksi valitaan $r \in V$ juureksi, ja sivuiksi r:stä alkavilla, joko palautuvaa tai laajenevaa hakua soveltaen muodostetuilla poluilla olevat sivut, kun ohitetut kärjet merkitään, eikä polku saa tulla jo merkittyyn kärkeen.*

Määritelmä 8.5.10. *Olkoon $G=(V,E)$ yhtenäinen ja suunnistamaton. $x \in V$ on* artikulointipiste *G:ssä, jos $G-\{x\}$ ei ole yhtenäinen. Jos G:ssä ei ole artikulointipisteitä, on G* kahdesti yhtenäinen. *Jos G:n artikulointipisteet ensin poistetaan ja sitten palautetaan erikseen jäljelle jääneisiin aligraafeihin, saadaan G:n* kahdesti yhtenäiset komponentit.

Algoritmi 8.5.11. *Olkoon $G=(V,E)$:n palautuvalla haulla muodostettu virittäjäpuu T, ja kärjet T:n esijärjestyksessä $x_1, x_2, \ldots, x_n$, ja $i(y)=i$, jos $y=x_i$. Suoritetaan kullekin x_j, $j=n, n-1, \ldots, 3$, tässä järjestyksessä, seuraavat askeleet:*
(1) $back^*(x_j)=\min\{i(z) \mid z$ *ja* x_j *naapureita*$\}$

(2) $back(x_j) = \min\{back^*(x_j), \{back(y) \mid y$ *on* x_j*:n poika*$\}\}$
(3) Jos $back(x_j) = i(w)$*, missä* w *on* x_j*:n isä, on* w *artikulointipiste, ja* x_j*-alipuun yhdessä* w*:n kanssa virittämä aligraafi on* G*:n kahdesti yhtenäinen komponentti*
(4) Poistetaan G*:stä* x_j*-alipuu ja jatketaan prosessia jäljelle jääneessä graafissa.*

Huom. x_j:n isä w on mukana $back(x_j)$:tä etsittäessä ja jos x_j:llä on *paluusivu* tätä aiempaan kärkeen, ei ”katkaisua” tehdä w:ssä. Kohdassa (2) tutkitaan rekursiivisesti mahdolliset paluureitit x_j:n jälkeläisten kautta.

8.6 Optimointi- ja sovitustehtäviä

Määritelmä 8.6.1. *Graafi* $G = (V, E)$ *on* mitoitettu verkko*, jos kaikilla* $e \in E$ *on olemassa reaalinen* e*:n* pituus $k(e) \geq 0$*. Kärkien* $a, z \in V$ *välisen* polun pituus *on ko. polulle kuuluvien sivujen pituuksien summa. Jos* G *on yhtenäinen, on* G*:n* virittäjäpuu T minimaalinen*, jos* T*:ssä olevien sivujen pituuksien summa* $\leq$ *mielivaltaisen virittäjäpuun* T' *sivujen pituuksien summa.*

Algoritmi 8.6.2. (Kruskalin algoritmi) *Aloittaen tyhjästä aligraafista* $T_1 = \emptyset$*, muodostetaan aligraafit* $T_1, T_2, \ldots, T_n$*,* $n = |V|$*, seuraavasti: Jos* T_{i-1}*:n sivut ovat* $e_1, \ldots, e_{i-1} \in E$*, valitaan* T_i*:hin näiden lisäksi sellainen sivu* $e_i \in E - \{e_1, \ldots, e_{i-1}\}$*, ja tämän kärjet, jolle* $k(e_i) = \min\limits_{e \in E - \{e_1, \ldots, e_{i-1}\}} \{k(e)\}$*, ja joka ei muodosta kierrosta yhdessä* $e_1, \ldots, e_{i-1}$*:n kanssa.*

Algoritmi 8.6.3. (Primin algoritmi) *Aloittaen graafista* $T_1 = \{v_1\}$*, jossa on* 1 *kärki* $v_1 \in V$*, eikä sivuja, muodostetaan puut* $T_1, T_2, \ldots, T_n$*, lisäämällä* T_{i-1}*:een kärkiin* $v_1, \ldots, v_{i-1}$ *kärki* v_i *ja sivu* $e_i = (v_j, v_i)$*, jolle* $k(e_i)$ *minimoituu, kun lisäys ei synnytä kierrosta, ja* $j = 1, 2, \ldots, i-1$*.*

Lause 8.6.4. *Jos* $G = (V, E)$ *on yhtenäinen suunnistamaton mitoitettu verkko, ovat Kruskalin ja Primin algoritmeilla muodostetut* G*:n virittäjäpuut minimaalisia.*

Algoritmi 8.6.5. (Minimipolkujen etsintä) *Olkoon* $G = (V, E)$ *yhtenäinen, suunnistamaton ja mitoitettu verkko, jossa tarkastellaan eräästä* $a \in V$ *alkavia polkuja. Annetaan* G*:n kärjille tunnukset seuraavasti:*
(1) a*:lle tunnus* $(-, 0)$*,*
(2) Sivuille $e = (p, q)$*, joille* p*:llä on tunnus* $(r, d(p))$*, ja* q*:lla ei ole tunnusta, muodostetaan lauseke* $d(p) + k(e) = d(q)$*. Sellainen* q*, jolle tämä minimoituu, saa tunnukset* $(p, d(q))$*.*
(3) Prosessia toistetaan, kunnes kaikilla kärjillä on tunnukset, tai on saatu tunnus halutulle loppupisteelle z*. Lyhin etäisyys* a*:sta* z*:aan on* z*:n tunnuksen* $(y, d(z))$ *jälkiosa* $d(z)$*, ja minimipolku kulkee palautuvaan suuntaan* z*:sta tunnusten alkuosien osoittamien kärkien kautta* a*:han.*

Huom. Minimipolkujen tai -puiden ei tarvitse olla yksikäsitteisesti määrättyjä.

Määritelmä 8.6.6. *Olkoon* $G = (V, E)$ *suunnistettu mitoitettu lineaarinen täydellinen graafi. Ns.* kauppamatkustajaprobleeman *ratkaisu* G*:ssä on* G*:n pituudeltaan minimaalinen Hamiltonin kierros.*

Huom. 1 Kauppamatkustajan kiertäessä n kaupunkia voisivat sivujen pituudet vastata matkakuluja tms. Jos G ei ole täydellinen, mutta siinä on olemassa Hamiltonin kierros, voisi asettaa $k(e) = \infty$ niille täydellisen graafin sivuille, joille $e \notin E$.
Huom 2 Täydellisellä n-kärkisellä graafilla on $(n-1)!$ Hamiltonin kierrosta, joten kaikkien mahdollisten Hamiltonin kierrosten tutkiminen ei ole käytännössä kelvollinen tapa etsiä ratkaisua kauppamatkustajaprobleemalle. Seuraavan esimerkin mukaista *haaraudu - ja - arvioi -menettelyä* voisi yrittää, mutta on huomattava, että tämäkään ei välttämättä ole laskutyön kannalta taloudellinen.
Esim. Olkoon kauppamatkustajan suoritettava kierros neljän kaupungin x_1, x_2, x_3, x_4 kautta, ja matkakustannus $x_i \to x_j$ olkoon $c_{ij} = k(\overrightarrow{x_i, x_j})$. Olkoot em. kustannukset koottu oheiseen matriisiin, jossa $c_{ii} = \infty$ on osoittamassa, että huomioidaan vain eri kaupunkien väliset matkat.

$$C = \begin{pmatrix} \infty & 3 & 9 & 7 \\ 3 & \infty & 6 & 5 \\ 5 & 6 & \infty & 6 \\ 9 & 7 & 4 & \infty \end{pmatrix}$$

Nyt voi arvioida, että matkan hinta on vähintään $3+3+5+4 = 15$, koska Hamiltonin kierros sisältää sivun joka vaakariviltä. Vähennetään eri vaakariveiltä ko. minimiarvot, jolloin tähän ehkä tulevat lisät voi esittää uutena matriisina:

$$C = \begin{pmatrix} \infty & 0 & 6 & 4 \\ 0 & \infty & 3 & 2 \\ 0 & 1 & \infty & 1 \\ 5 & 3 & 0 & \infty \end{pmatrix}.$$

Mukaan on tultava myös sivu joka pystyriviltä, joten hintaan tulee lisää vähintään $0+0+0+1 = 1$. Matkan hinta tulee siis olemaan ainakin $15+1 = 16$, ja siihen ehkä tulevia lisiä esittää:

$$C = \begin{pmatrix} \infty & 0 & 6 & 3 \\ 0 & \infty & 3 & 1 \\ 0 & 1 & \infty & 0 \\ 5 & 3 & 0 & \infty \end{pmatrix}.$$

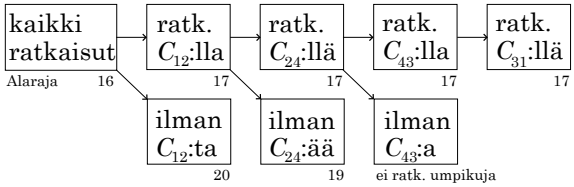
Jos ratkaisu nyt ei kulkisi esim. sivun $(1,2)$ kautta ($c_{12} = 0$), esitetään tätä asettamalla $c_{12} = \infty$

$$C = \begin{pmatrix} \infty & \infty & 3 & 0 \\ 0 & \infty & 3 & 1 \\ 0 & 0 & \infty & 0 \\ 5 & 2 & 0 & \infty \end{pmatrix},$$

jonka jälkeen ensimmäiseltä vaaka- ja toiselta pystyriviltä saadaan arvio tällaisen reitin hinnalle: $16+3+1 = 20$ vähintään. Jos taas c_{12} on mukana, loppumatkalla ei enää ole 1. vaaka- eikä 2. pystyrivin sivua, eikä c_{21}:ä. Loppumatkan kuluihin tulee nyt vähintään 1. vaakariviltä numero 2, siis hinta yhteensä vähintään $16+1 = 17$, ja tähän mahdolliset lisät:

$$C = \begin{pmatrix} \infty & \infty & \infty & \infty \\ \infty & \infty & 2 & 0 \\ 0 & \infty & \infty & 0 \\ 5 & \infty & 0 & \infty \end{pmatrix}.$$

Nyt voi jälleen haarautua esim. c_{24}:stä. Jos c_{24} ei ole mukana, on hinta vähintään $17 + 2 = 19$, tutkimalla 2. vaakariviä. Jos c_{24} on mukana, on asetettava myös $c_{42} = \infty$ ja $c_{41} = \infty$ (koska osapolku toistaiseksi on $x_1 \to x_2 \to x_4$, eikä Hamiltonin kierros voisi vielä palata x_1:een). Nyt olisi jäljellä enää matkan täydennys kierrokseksi x_3:n kautta: $x_4 \to x_3 \to x_2$, ja koska $c_{43} = c_{31} = 0$, ei tämä enää lisää hintaa. Siis: reitillä $x_1 \to x_2 \to x_4 \to x_3 \to x_1$ saavutetaan hinta 17, joka on minimihinta läpikäydyn päättelyn mukaan.
Ratkaisun etsiminen eteni seuraavassa puussa:



Huom. Haarautumista varten olisi usein edullista valita se 0-elementti, jonka poisjättäminen maksimoisi alarajahinnan lisäyksen.

Määritelmä 8.6.7. *Olkoon $G = (V, E)$ mitoitettu suunnistettu verkko, jossa sivujen pituuksia $k(e)$, $e \in E$, sanottakoon niiden* kapasiteeteiksi. *Olkoon $In(x) = \{e \in E \mid \exists y : e = (\overrightarrow{y, x})\}$ ja $Out(x) = \{e \in E \mid \exists y : e = (\overrightarrow{x, y})\}$. G:n sivuille määritelty funktio $\varphi : E \to \mathbb{R}$ on* virtaus lähteestä a nieluun z, *jos*

(1) $0 \leq \varphi(e) \leq k(e)$, *kaikilla* $e \in E$,

(2) $e \in In(a)$ *tai* $e \in Out(z) \Rightarrow \varphi(e) = 0$,

(3) $x \neq a$ *ja* $x \in z \Rightarrow \sum_{e \in In(x)} \varphi(e) = \sum_{e \in Out(x)} \varphi(e)$.

Huom. Voisi tarkastella myös verkkoja, joissa olisi useita lähteitä tai nieluja mutta nämä voidaan palauttaa määritelmän 8.6.7 tapaukseen lisäämällä graafiin ”superlähde” a ja ”supernielu” z sekä sivut a:sta alkuperäisiin lähteisiin ja z:aan alkuperäisistä nieluista. Näille on annettava riittävät kapasiteetit alkuperäisten lähteiden ja nielujen kokonaiskapasiteettien tyydyttämiseksi.

Määritelmä 8.6.8. *Olkoon $P \subset V$ virtausverkossa $G = (V, E)$, ja $\overline{P} = V - P$. Sivujoukko $(P, \overline{P}) = \{(\overrightarrow{x, y}) \mid x \in P$ ja $y \in \overline{P}\} \subset E$ on* katkos, *ja jos $a \in P, z \in \overline{P}$, se on a-z -*katkos.

Määritelmä 8.6.9. *Olkoon $G = (V, E)$ virtausverkko. Virtaukselle $\varphi : E \to \mathbb{R}$ on*

(1) sivu $e \in E$ kyllästetty, *jos* $\varphi(e) = k(e)$,

(2) φ*:n* arvo $|\varphi| = \sum_{v \in V} \varphi(\overrightarrow{a, v})$, *kun* $a =$ *lähde*,

(3) katkoksen $(P, \overline{P})$ kapasiteetti $k(P, \overline{P}) = \sum_{x \in P, y \in \overline{P}} k(\overrightarrow{x, y})$.

Lause 8.6.10. *Olkoon φ G:n a-z -virtaus. Tällöin a:sta lähtevä virtaus ja z:aan saapuva virtaus ovat yhtä suuret.*

Todistus. Määritelmän 8.6.7 kohdan (3) mukaan on joukolle $P \subset V$, jolle $a \notin P$ ja $z \notin P$:

$$\sum_{x \in P} \sum_{e \in In(x)} \varphi(e) = \sum_{x \in P} \sum_{e \in Out(x)} \varphi(e).$$

Jos tässä on $e = (s,t)$, missä $s,t \in P$, on $\varphi(e)$ yhtälön molemmilla puolilla, ja se voidaan eliminoida, jolloin jää jäljelle:

$$\sum_{e \in (\overline{P},P)} \varphi(e) = \sum_{e \in (P,\overline{P})} \varphi(e), \text{ kun } a \notin P, z \notin P.$$

Jos nyt G:ssä ei ole sivua $(\overrightarrow{a,z})$, valitaan $P = V - \{a,z\}$, jolloin $\overline{P} = \{a,z\}$. Määritelmän 8.6.7 kohdan (2) mukaan kaikki virtaus $\overline{P}$:sta lähtee a:sta ja kaikki virtaus $\overline{P}$:aan saapuu z:aan. Nyt on siis virtaus a:sta $= \sum_{e \in (\overline{P},P)} \varphi(e) = \sum_{e \in (P,\overline{P})} \varphi(e) =$ virtaus z:aan.
Jos G:ssä on sivu $(\overrightarrow{a,z})$, lähtee a:sta ja tulee z:aan tätä pitkin virtaus $\varphi(\overrightarrow{a,z})$ ja edellinen päättely pätee muille sivuille. ■

Lause 8.6.11. (Maksimivirtaus-minimikatkos-teoreema) *Virtausverkon $G = (V,E)$ a-z-virtaukselle φ ja a-z-katkokselle $(P,\overline{P})$ on: $|\varphi| \leq k(P,\overline{P})$. Tässä on $|\varphi| = k(P,\overline{P})$, jos ja vain jos kaikilla $e \in (\overline{P},P)$ on $\varphi(e) = 0$ ja kaikilla $e \in (P,\overline{P})$ on $\varphi(e) = k(e)$. Jos on $|\varphi| = k(P,\overline{P})$, niin φ on maksimaalinen virtaus ja $k(P,\overline{P})$ on minimaalinen a-z-katkoksen kapasiteetti.*

Todistus. Lisätään G:hen kärki $a' \notin P$, ja sivu $(\overrightarrow{a',a})$, jolle annetaan kapasiteetti, joka on riittävän suuri, ja virtaus $|\varphi|$. Nyt φ on a'-z-virtaus, jolle

$$|\varphi| \leq \sum_{e \in (\overline{P},P)} \varphi(e) = \sum_{e \in (P,\overline{P})} \varphi(e) \leq \sum_{e \in (P,\overline{P})} k(e) = k(P,\overline{P}),$$

kuten lausetta 8.6.10 todistettaessa. Muut väitteet seuraavat nyt tästä. ■

Algoritmi 8.6.12. (Virtauksen kasvatus) *Olkoon $G = (V,E)$ virtausverkko, ja φ eräs sen a'-z-virtaus. Tämän lisäämiseksi suoritetaan:*

(1) Lähteelle a annetaan tunnus $(-,\infty)$.

(2) a:sta aloittaen selataan kärkiä, jolloin selattavan kärjen p tunnuksen jälkiosa on merkitty Δ:llä, ja tutkitaan p:n kautta kulkevat sivut seuraavasti:
(a) Jos $e = (\overrightarrow{q,p})$, ja $\varphi(e) > 0$, ja q:lla ei vielä ole tunnusta, asetetaan q:lle tunnus $(p^-, \Delta q)$, missä $\Delta q = \min(\Delta p, \varphi(e))$
(b) Jos $e = (\overrightarrow{p,q})$, q:lla ei tunnusta, ja $s(e) = k(e) - \varphi(e) > 0$, asetetaan q:n tunnukseksi $(p^+, \Delta q)$, missä $\Delta q = \min(\Delta p, s(e))$.

(3) Jos nielulle z saadaan tunnus, jonka jälkiosa on $\Delta z > 0$, muodostetaan polku a:sta z:aan siten, että z:sta palataan tunnusten alkuosien osoittamaa reittiä a:han. Tällä polulla kasvatetaan virtausta Δz:n verran.

(4) Jos z ei saanut tunnusta, jatkuu kärkien selaus jossakin muussa tunnistetussa kärjessä. Jos selausta ei voi enää jatkaa, merkitään $P = \{v \in V \mid v$:llä on tunnus$\}$. Tällöin on $(P, \overline{P})$ kyllästetty a-z-katkos, $|\varphi| = k(P, \overline{P})$ ja φ maksimivirtaus.

Määritelmä 8.6.13. *Olkoon $G = (V, E)$ suunnistamaton ja kaksijakoinen: $V = X \cup Y$, ja $X \cap Y = \emptyset$, $(x, y) \in E \Rightarrow x \in X$ ja $y \in Y$.* Sovitus *G:ssä on joukko $F \subseteq E$, jolle $(a, b), (c, d) \in F \Rightarrow a \neq c, d$ ja $b \neq c, d$. X:n* täydellinen sovitus *Y:hyn on sovitus, jolle $x \in X \Rightarrow \exists y \in Y : (x, y) \in F$.*

Lause 8.6.14. *Kaksijakoisessa graafissa $G = (V, E)$ on olemassa X:n täydellinen sovitus Y:hyn, jos ja vain jos kaikille $A \subseteq X$, $R(A) = \{y \in Y \mid \exists (x, y) \in E\}$ on $|A| \leq |R(A)|$.*

Lause 8.6.15. *Edellisin merkinnöin on olemassa X:n täydellinen sovitus Y:hyn, jos jollekin $k \in \mathbb{N}$ pätee: $d(x) \geq k \geq d(y)$, kaikilla $x \in X, y \in Y$.*

Määritelmä 8.6.16. *Kaksijakoisessa graafissa $G = (V, E)$ muodostettu sovitus $F \subseteq E$ on* maksimaalinen, *jos mahdollisimman monella $x \in X$ on olemassa $y \in Y$ siten, että $(x, y) \in F$. Jos $A \subseteq X$, on $\delta(A) = |A| - |R(A)|$ joukon A* vaje. Graafin G vaje *on $\delta(G) = \max\{\delta(A) \mid A \subseteq X\}$.*

Lause 8.6.17. *Kaksijakoisessa graafissa $G = (V, E)$, $V = X \cup Y$, on olemassa maksimaalinen X:n sovitus Y:hyn, ja tässä on mukana $|X| - \delta(G)$ kärkeä joukosta X.*

Määritelmä 8.6.18. *G:n kärkijoukko $S \subseteq V$ on* sivupeite, *jos $(a, b) \in E \Rightarrow a \in S$ tai $b \in S$.*

Lause 8.6.19. *Kaksijakoisen graafin maksimaalinen sovitus ja minimaalinen sivupeite ovat yhtä suuret.*

Huom. Sovitettaessa X Y:hyn olisi G:n naapurimatsiisista löydettävä *riippumaton* joukko alkioita 1 (ei kahta samalla vaaka- tai pystyrivillä). Edelleen: *Sovitus vastaa kokonaislukuarvoista a-z-virtausta* kärkien $x \in X$ eteen sijoitetusta superlähteestä a kärkien $y \in Y$ jälkeen sijoitettuun supernieluun z, kun kaikkien sivujen kapasiteetti on $k(x, y) = 1$, ja siis vain arvot $\varphi(x, y) = 0$ tai 1 sallitaan.

Algoritmi 8.6.20. (Sovituksen kasvatusalgoritmi) *Olkoon $n \times m$-matriisin A alkiot $a_{ij} = 0$ tai 1 ja I riippumaton joukko alkioita 1.*

(1) Annetaan A:ssa tunnus _ I:hin kuuluville 1:lle, ja tunnus $*$ vaakariveille, joilla ei ole merkittyä 1:tä.

(2) Viimeksi merkittyjen vaakarivien selaus: Tunnus i niille vapaille pystyriveille, joilla on vapaa 1 vaakarivillä i.

(3) Viimeksi merkittyjen pystyrivien selaus: Tunnus j sille vaakariville, jolla on merkitty 1 pystyrivillä j. Jos vaakarivejä merkittiin, palataan (2):een, muuten:

(4) Jos viimeksi selattu pystyrivi oli j_0, merkitän sen tunnuksen i_1 osoittama alkio 1, poistetaan merkki vaakarivilta i_1 sen tunnuksen j_1 osoittamalla pystyrivillä olevasta 1:stä, merkitään pystyriviltä j_1 sen tunnuksen i_2 osoittama 1 jne., kunnes tullaan $*$:llä merkitylle riville ja palataan (1):een.

9 KOMBINATORIIKKAA

Joukon mahtavuutta ja kardinaliteettia tarkasteltiin Luvussa **??**. Samoin todistettiin äärellisten joukkojen summa- ja erotusperiaate eli joukkojen yleinen yhteenlaskukaava (Lause **??**) sekä palautuskaava joukon ositusten lukumäärien laskemiseksi (Lause **??**). Tässä luvussa palautetaan aluksi mieleen variaatioit ja kombinaatiot sekä binomi- ja multinomikertoimet ja niiden sovellutuksena tarkastellaan joukon alkioluokkiin jakoja eli ositteluja multinomikerrointen avulla.

9.1 Summa- ja tuloperiaate

Monissa yhteyksissä, esimerkiksi todennäköisyyslaskennassa, tulee toistuvasti vastaan seuraava perusongelma: *Kuinka monta alkiota on joukossa, joka on muodostettu tunnetuista joukoista tiettyjen alkeisoperaatioiden avulla?*

Summaperiaate. Jos $A_1, A_2, \ldots, A_k \subseteq E$ ovat erillisiä, ts. pareittaiset leikkaukset ovat tyhjiä, on voimassa summaperiaate

$$\#(A_1 \cup A_2 \cup \cdots \cup A_k) = \#A_1 + \#A_2 + \cdots + \#A_k,$$

ks. Lause **??**.

Tuloperiaate. Jos $A_1 \times A_2 \times \cdots \times A_k \subseteq E$, on voimassa tuloperiaate

$$\#(A_1 \times A_2 \times \cdots \times A_k) = \#A_1 \cdot \#A_2 \cdots \#A_k.$$

Tuloperiaatetta voidaan havainnollistaa juurellisena puuna, jossa solmun välittömien seuraajien määrä kuvaa kunkin vaiheen tulosmahdollisuuksia.

Summa- ja tuloperiaatteen probabilistinen tulkinta. Olkoon koetta tehtäessä n tulosmahdollisuutta eli *alkeistapausta* $E = \{e_1, e_2, \ldots, e_n\}$. *Pistetodennäköisyysfunktio* $p_E : E \to [0, 1]$ on kuvaus, jolle

$$\sum_{i=1}^{n} p_E(e_i) = 1.$$

Alkeistapauksen e_i *todennäköisyys* on luku $p_E(e_i)$. *Tapahtuman* $A \subseteq E$ todennäköisyys on luku

$$P(A) := \sum_{e_i \in A} p_E(e_i).$$

Jos tapahtumat $A_1, A_2, \ldots, A_k \subseteq E$ ovat toisensa poissulkevia, niin summaperiaatteen mukaan

$$P\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} P(A_i).$$

Olkoon sitten kyseessä koe, joka voidaan ajatella suoritetuksi useassa toisistaan riippumattomassa vaiheessa $i = 1, 2, \ldots, k$, joissa kaikkien alkeistapausten joukot ovat $E_1, E_2, \ldots, E_k$. Tällöin ilmiön malliksi käy *tulokenttä* $E := E_1 \times E_2 \times \cdots \times E_k$. Jos $A_1 \times A_2 \times \cdots \times A_k \subseteq E$ on tulokentän tapahtuma, saadaan tuloperiaatteen mukaan

$$P\left(\prod_{i=1}^{k} A_i\right) = \prod_{i=1}^{k} P_i(A_i),$$

missä P_i on todennäköisyys vastaavassa projektiokentässä E_i.

9.2 Variaatiot ja kombinaatiot

Alkeistapausten lukumäärien käsittely helpottuu, kun otetaan käyttöön variaatio ja kombinaatio.

Määritelmä 9.2.1. Olkoon A epätyhjä joukko, $n := \#A$ ja $k \in [n]$.

a) Joukon A k-*variaatioita* ovat kaikki eri alkioista muodostetut vektorit

$$(a_1, a_2, \ldots, a_k) \in A^k, \quad a_i \neq a_j, \text{ kun } i \neq j.$$

Joukon A n-variaatioita sanotaan *permutaatioiksi*.

b) Joukon A k-alkioiset osajoukot $\{a_1, a_2, \ldots, a_k\} \subseteq A$ ovat sen k-*kombinaatioita*.

Huomautus 9.2.2. a) Joukon A k-variaatio voitaisiin yhtä hyvin määritellä injektiona $f : [k] \to A$. Nimittäin, jokainen injektio f määrää k-variaation $\big(f(1), \ldots, f(k)\big)$ ja kääntäen, jokainen variaatio $(a_1, a_2, \ldots, a_k)$ määrää injektion, kun määritellään $f(i) := a_i$ kullekin $i \in [k]$.
b) Joukon k-variaatiot saadaan muodostamalla kaikkien k-kombinaatioiden permutaatiot.

Lause 9.2.3. Äärellisen n-alkioisen joukon k-variaatioiden lukumäärä on

$$V(n,k) := n(n-1)\cdots\big(n-(k-1)\big) = \frac{n!}{(n-k)!} \tag{9.1}$$

ja k-kombinaatioiden lukumäärä on

$$K(n,k) := \binom{n}{k} := \frac{n!}{k!\,(n-k)!}, \tag{9.2}$$

missä merkintä $\binom{n}{k}$ on *binomikerroin*, joka luetaan "n k:n yli".

Todistus. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$. Muodostettaessa k-variaatiota sen

1. alkio voidaan valita n *tavalla,*

2. alkio voidaan valita $n-1$ *tavalla,*

$\vdots$

k*. alkio voidaan valita* $n-(k-1)$ *tavalla.*

Tuloperiaatteen nojalla erilaisia k-variaatioita on $n(n-1)\cdots\big(n-(k-1)\big)$, joten kaava (9.1) on todistettu.
Jokainen k-kombinaatio $\{a_{i_1}, \ldots, a_{i_k}\}$ voidaan järjestää k-variaatioksi alkuosan nojalla

$$\frac{k!}{(k-k)!} = \frac{k!}{0!} = k!$$

eri tavalla. Jokaista k-kombinaatiota vastaa siis $k!$ kappaletta k-variaatioita, joten k-kombinaatioiden lukumäärä on

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Siis kaava (9.2) on todistettu. □

Lause 9.2.4. Olkoot $0 \leq k \leq n \in \mathbb{N}$. Binomikertoimille pätee

$$\begin{aligned}
&1) && \binom{n}{k} &&= && \tbinom{n}{n-k} \\
&2) && \binom{n}{1} &&= && \binom{n}{n-1} = n \\
&3) && \binom{n+1}{k} &&= && \binom{n}{k-1} + \binom{n}{k} \\
&4) && (a+b)^n &&= && \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&5) && \sum_{k=0}^{n} \binom{n}{k} &&= && 2^n.
\end{aligned}$$

Todistus. Kaavat 1) ja 2) ovat ilmeisiä. Kaava 3) lasketaan laventamalla yhtälön oikean puolen yhteenlaskettavat samannimisiksi ja sieventelemällä. Kaava 4) on muualtakin tuttu binomikaava ja 5) on binomikaavan sovellutus arvoilla $a = b = 1$. □

9.3 Osittelut ja multinomikertoimet

Tarkastellaan äärellisen joukon nimettyihin alkioluokkiin jakojen määriä. Eri tapoja jakaa äärellinen n-alkioinen joukko kahteen nimettyyn luokkaan niin, että luokassa 1 on n_1 ja luokassa 2 on $n_2 = n - n_1$ alkiota, on niin monta kuin on n-alkioisen joukon n_1-kombinaatioita, ts.

$$\binom{n}{n_1} = \frac{n!}{n_1!\,n_2!}.$$

Yleistetään tämä tulos useammalle luokkamäärälle.

Lause 9.3.1. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$. Eri tapoja jakaa joukko A nimettyihin luokkiin $1, 2, 3, \ldots, k \in \mathbb{N}$ niin, että luokassa i on n_i alkiota ja $\sum_{i=1}^{k} n_i = n$, on *multinomikertoimen*

$$M(n; n_1, n_2, n_3, \ldots, n_k) := \frac{n!}{n_1!\,n_2!\,n_3!\,\cdots\,n_k!}$$

ilmoittama määrä.

Todistus. Induktiolla luvun k suhteen:
1) Jos $k = 1$, on $n_1 = n$ ja $\frac{n!}{n!} = 1$.
2) Tapaus $k = 2$ johdettiin edellä.
3) Oletetaan, että väite on tosi arvoilla $2 \leq k \leq m$. Olkoon luokkia $m+1$ kappaletta ja luokassa $m+1$ alkioita n_{m+1}. Ajatellaan sijoittelu suoritetuksi kahdessa vaiheessa

a) n_{m+1} alkiota n:stä luokkaan $m+1$,

b) $n-n_{m+1}$ alkiota luokkiin $1, 2, 3, \ldots, m$.

Tuloperiaatteen ja induktio-oletuksen mukaan tapoja on yhteensä

$$\binom{n}{n_{m+1}} \times \frac{(n-n_{m+1})!}{n_1!\, n_2!\, n_3! \cdots n_m!} = \frac{n!}{n_1!\, n_2!\, n_3! \cdots n_m!\, n_{m+1}!}.$$

Induktioperiaatteen nojalla lause on todistettu. □

Huomautus 9.3.2. Osa luokista voi olla tyhjiä, jolloin $n_i! = 0! = 1$. Toinen ero Luvussa **??** esillä olleeseen *osituksen* käsitteeseen on se, että osittelussa luokat ovat nimettyjä; ne voidaan erottaa toisistaan.

Esimerkki 9.3.3. Tarkastellaan 5 henkilön H_i, $i = 1, 2, 3, 4, 5$, jakamista 3 ryhmään.
a) Kuinka monella tavalla henkilöt on mahdollista jakaa nimettyihin ryhmiin A, B ja C niin, että ryhmissä B ja C on molemmissa kaksi henkilöä?
Ratkaisu. *Tapa 1.* Multinomikertoimien avulla

$$M(5; 1, 2, 2) = \frac{5!}{1!\, 2!\, 2!} = 30.$$

Tapa 2. Tuloperiaatetta käyttäen: on

5 tapaa asettaa yksi henkilö H_i ryhmään A,

$\binom{4}{2}$ tapaa valita neljästä kaksi ryhmään B,

1 tapa täyttää ryhmä C.

Täten tapoja on yhteensä $5 \cdot \binom{4}{2} \cdot 1 = 30$.
b) Kuinka monella tavalla henkilöt voidaan jakaa kolmeen epätyhjään nimettömään ryhmään niin, että yhdessä ryhmässä on yksi ja molemmissa muissa kaksi henkilöä?
Ratkaisu. *Tapa 1.* On kyse viiden alkion joukon 3-osaisista osituksista. Kaikki ositukset eivät kelpaa, nimittäin ne, joissa yhteen ryhmään otetaan kolme henkilöä. Koska näitä on $\binom{5}{3}$, on kelvollisia osituksia palautuskaavan (Lause **??**) tai Stirlingin kolmion (Taulukko **??**) mukaan $p(5, 3) - \binom{5}{3} = 25 - 10 = 15$.
Tapa 2. Tehtävä ratkeaa myös tuloperiaatetta käyttäen:

1-henkilöisen ryhmän jäsen voidaan valita 5 tavalla,

4 henkilöä voidaan jakaa kahden henkilön ryhmiin 3 eri tavalla,

joten hyväksyttäviä tapoja on tuloperiaatteen mukaan $5 \cdot 3 = 15$.

10 AUTOMAATTIEN TEORIA

10.1 Äärelliset automaatit

10.1.1 Peruskäsitteitä

Olkoon Σ joukko. *Merkkijono* eli *sana* yli Σ:n on Σ^n:n alkio jollakin $n \in \mathbb{N}_0$. Sanaa

$$\alpha = (\alpha_1, \ldots, \alpha_n)$$

merkitään jatkossa lyhyesti $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$. α:n *pituus* $l(\alpha)) = n$. Sana, jonka pituus $= 0$, on *tyhjä sana*, merk. λ. Σ:n kaikkien sanojen joukkoa merkitään Σ^*:llä, ts.

$$\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n.$$

Ei-tyhjien sanojen joukkoa merkitään Σ^+:lla, ts.

$$\Sigma^+ = \bigcup_{n=1}^{\infty} \Sigma^n.$$

Joukkoa $\{a\}^*$ merkitään a^*:llä ja vastaavasti joukkoa $\{a\}^+$ a^+:lla. Sanaa $aa \ldots a$ (n kpl a:ta) merkitään a^n:llä.
Sanojen $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$ ja $\beta = \beta_1\beta_2 \ldots \beta_m$ *katenaatio* on

$$\alpha\beta = \alpha_1\alpha_2 \ldots \alpha_n\beta_1\beta_2 \ldots \beta_m.$$

Joukkojen $L_1 \subseteq \Sigma$ ja $L_2 \subseteq \Sigma$ katenaatio L_1L_2 on

$$L_1L_2 = \{\alpha\beta | \alpha \in L_1, \beta \in L_2\}.$$

(L_1L_2 on siis karteesinen tulo $L_1 \times L_2$).
Sana β on sananα *osasana*, jos $\alpha = \mu\beta\eta$, missä μ ja η ovat sanoja.

10.1.2 Äärellinen puoliautomaatti

(*Deterministinen*) *äärellinen puoliautomaatti* on viisikko

$$\mathcal{A} = (S, I, f, s_0, A),$$

missä S on äärellinen joukko (*tilajoukko*), I on äärellinen joukko (*syöttöaakkosto*), f on kuvaus $S \times I \to S$ (*tilansiirtofunktio*), $s_0 \in S$ (*alkutila*) ja $A \subseteq S$ (*hyväksyvien tilojen joukko*).
Äärellinen puoliautomaatti voidaan antaa myös matriisina (*tilataulu, siirtymätaulu*)

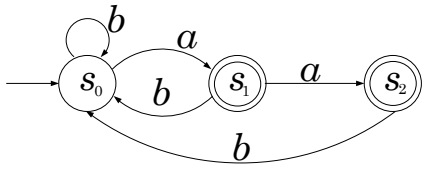
$S \backslash I$	a_1	a_2	$\ldots$	a_m
s_0	$f(s_0, a_1)$	$f(s_0, a_2)$	$\ldots$	$f(s_0, a_m)$
s_1	$f(s_1, a_1)$	$f(s_1, a_2)$	$\ldots$	$f(s_1, a_m)$
$\vdots$	$\vdots$			$\vdots$
s_k	$f(s_k, a_1)$	$f(s_k, a_2)$	$\ldots$	$f(s_k, a_m)$

(jonka lisäksi on annettava s_0 ja A) tai suunnattuna graafina (*tiladiagrammi, siirtymädiagrammi*), jonka pisteinä (kärkinä, solmuina) ovat tilat ja jossa on kaari $s \to t$, jos ja vain jos $f(s,a) = t$ jollekin $a \in I$. Tällöin ko. kaari merkataan a:lla. Alkutila ilmoitetaan (ylimääräisellä) kaarella, jolla ei ole lähtökärkeä, ja hyväksyvät tilat merkitään kaksinkertaisella rengastuksella.
Puoliautomaatin syötöt ovat I^*:n sanoja. Sanan ensimmäisen kirjaimen syötön alkaessa automaatti on alkutilassaan. Kirjaimen a syöttö automaatin ollessa tilassa s aiheuttaa tilan muuttumisen s:stä tilaksi $f(s,a)$. Jos tila viimeisen kirjaimen syötön jälkeen on hyväksyvä (eli $\in A$), automaatti *hyväksyy* ko. sanan, muuten *hylkää*. Puoliautomaatin $\mathcal{A}$ hyväksymien sanojen joukkoa merkitään $A(\mathcal{A})$:lla.
Olkoon $\alpha = a_1, \ldots, a_n \in I^*$, ja olkoot $\delta_0 = s_0, \delta_1, \delta_2, \ldots, \delta_n$ tilat,joille

$$f(\delta_{i-1}, a_i) = \delta_i, \;\; i = 1, 2, \ldots, n.$$

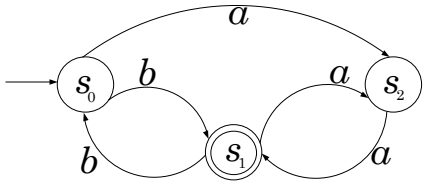
Tällöin polku $s_0 \to \delta_1 \to \delta_2 \to \ldots \to \delta_n$ *esittää* α:a. α siis hyväksytään, jos ja vain jos $\delta_n \in A$.

Esimerkki 10.1.1. *Hyväksyykö oheinen puoliautomaatti sanan α =abaa?*



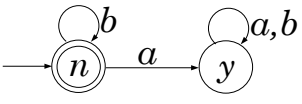
α:a esittää polku $s_0 \to s_1 \to s_0 \to s_1 \to s_2$. Koska s_2 on hyväksyvä tila, automaatti hyväksyy sanan α.

Esimerkki 10.1.2. *Hyväksyykö oheinen puoliautomaatti A sanan abbabba?*

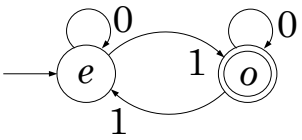


Sanaa abbabba esittää polku $s_0 \to s_2 \to s_2 \to s_2 \to s_1 \to s_0 \to s_1 \to s_2$. Koska s_2 ei ole hyväksyvä tila, A ei hyväksy sanaa abbabba.

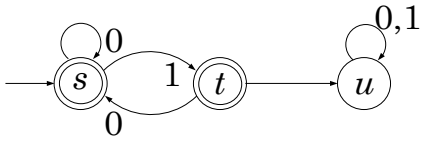
Esimerkki 10.1.3. *Suunnittele äärellinen puoliautomaatti, joka hyväksyy aakkoston $\{a, b\}$ täsmälleen ne sanat, joissa ei ole yhtään a-kirjainta.*
y - a löydetty
n - ei yhtään a:ta löydetty.



Esimerkki 10.1.4. *Suunnittele äärellinen puoliautomaatti, joka hyväksyy täsmälleen ne binäärijonot, joissa on pariton määrä ykkösiä.*
e - parillinen, o - pariton



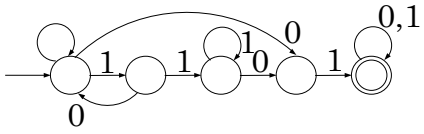
Esimerkki 10.1.5. *Määrää $Ac(\mathcal{A})$, kun $\mathcal{A}$ on:*



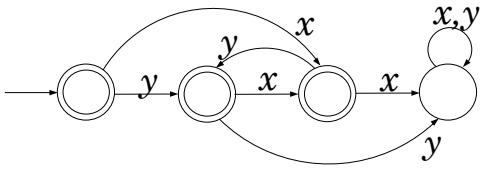
(Ainoaan) Hylkäävään tilaan voidaan päästä vain, jos on syötetty kaksi peräkkäistä ykköstä. Siis

$$\alpha \in Ac(\mathcal{A}) \Leftrightarrow \alpha\text{:ssa ei ole kahta peräkkäistä ykköstä.}$$

Esimerkki 10.1.6. *Suunnittele äärellinen puoliautomaatti, joka hyväksyy täsmälleen ne binäärijonot, joilla on osajonona 1101.*



Esimerkki 10.1.7. *Määrää $Ac(\mathcal{A})$, kun $\mathcal{A}$ on:*

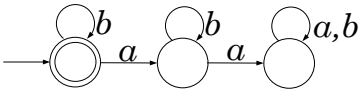


$\mathcal{A}$:n tilaksi tulee hylkäävä tila, joss sille syötetään kaksi peräkkäistä x:ää tai kaksi peräkkäistä y:tä. Siis

$$Ac(\mathcal{A}) = \{\alpha \mid \alpha = xyxyxy \ldots \text{ tai } yxyxyx \ldots\}$$

Äärelliset puoliautomaatit $\mathcal{A}_1$ ja $\mathcal{A}_2$ ovat ekvivalentteja, jos $Ac(\mathcal{A}_1) = Ac(\mathcal{A}_2)$.

Esimerkki 10.1.8.



ja esimerkin 10.1.3 puoliautomaatti ovat ekvivalentteja.

Epädeterministinen äärellinen puoliautomaatti on viisikko

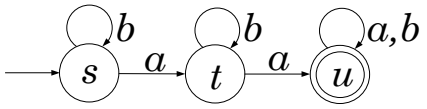
$$\mathcal{A} = (S, I, f, s_0, A),$$

missä S, I, s_0 ja A ovat kuten deterministisellä äärellisellä puoliautomaatilla ja f on kuvaus $S \times I \to P(s)$ (= S:n osajoukkojen joukko).
Epädeterministisen äärellisen puoliautomaatin tilansiirto voi siis olla monikäsitteinen tai määrittelemätön (kun se deterministisellä äärellisellä puoliautomaatilla on aina yksikäsitteisesti määritelty).

Esimerkki 10.1.9.

	a	b
$\to s$	$\{t\}$	$\{s\}$
t	0	$\{t, u\}$
u	0	0

eli

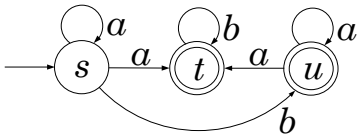


on epädeterminstinen äärellinen puoliautomaatti.

Esimerkki 10.1.10. *Samoin on*

	a	b
$\to s$	s, t	u
t	$-$	t
u	u, t	$-$

eli



missä joukot on kirjoitettu ilman sulkuja ja tyhjä joukko on merkitty viivalla.

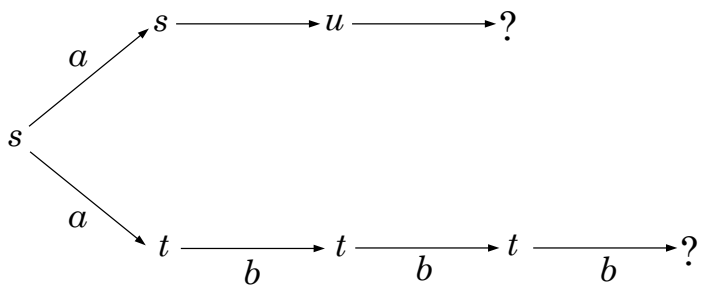
Olkoon $\mathcal{A} = (S, I, f, s_0, A)$ epädeterministinen äärellinen puoliautomaatti, ja olkoon $\alpha = a_1, \ldots, a_n \in I^*$. Jos on olemassa tilat $\delta = s_0, \delta_1, \ldots, \delta_n$

$$\delta_i \in f(\delta_{i-1}, a_i), i = 1, \ldots, n$$

sanotaan, että polku $s_0 \to \delta_1 \to \delta_2 \to \ldots \to \delta_n$ esittää sanaa α.
α:a esittäviä polkuja voi olla useita. Jos jokin α:a *esittävä* polku $s_0 \to \delta_1 \to \ldots \to \delta_n$ täyttää ehdon $\delta_n \in A$, sanotaan, että $\mathcal{A}$ *hyväksyy* α:n.

Esimerkki 10.1.11. *Olkoon $\mathcal{A}$ kuten esimerkissä 10.1.9. Sanaa $\alpha = bbabb$ esittävät polut $s \to s \to s \to t \to t \to u$ ja $s \to s \to s \to t \to t \to t$. Koska näistä ainakin yksi päättyy A:han, $\mathcal{A}$ hyväksyy α:n.*

Esimerkki 10.1.12. *Esimerkin 10.1.10 $\mathcal{A}$ ei hyväksy sanaa $abba$, koska ei ole A:han päättyvää α:a esittävä polkua*



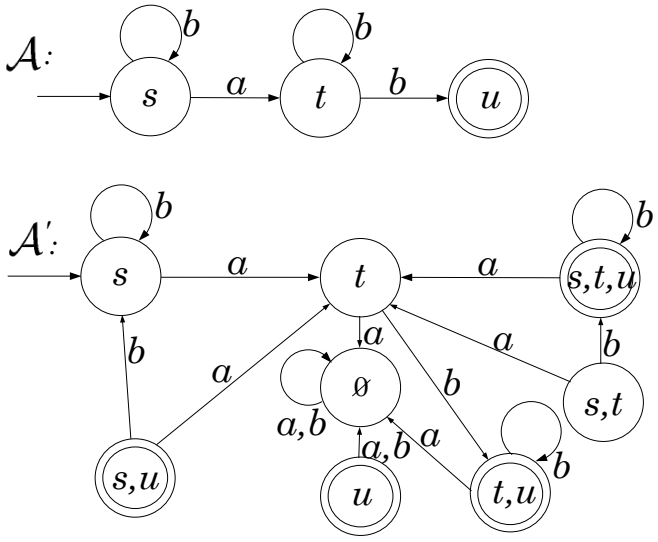
Määritelmistä nähdään suoraan, että deterministinen äärellinen puoliautomaatti on epädeterminististen äärellisten puoliautomaattien erikoistapaus. (Yksialkioinen joukko ja sen alkio samaistetaan : $\{s\} = s$). Näin ollen vastaus kysymykseen ”Onko mielivaltaista determinististä äärellistä puoliautomaattia kohti olemassa sen kanssa ekvivalentti epädeterministinen äärellinen puoliautomaatti” on selvä: on ; se itse täyttää vaaditun ehdon. Sen sijaan kysymys toiseen suuntaan on mielenkiintoinen ja tärkeä. Vastaus on (ehkä hieman yllättäen) myönteinen.

Lause 10.1.13. *Olkoon $\mathcal{A} = (S, I, f, s_0, A)$ epädeterministinen äärellinen puoliautomaatti. Olkoon*

$$\begin{aligned} S' &= P(S) \\ I' &= I \\ s'_0 &= \{s_0\} \quad = s_0 \text{ ; samaistus!)} \\ A' &= \{X \subseteq x \mid X \cap A \neq 0\} \\ f'(X,a) &= \begin{cases} 0, & \text{jos } X = \emptyset \\ \cup f(s,a), & \text{jos } X \neq \emptyset \\ s \in X & \end{cases} \end{aligned}$$

Silloin deterministinen äärellinen puoliautomaatti $\mathcal{A}' = (S', I', f', s'_0, A')$ on ekvivalentti $\mathcal{A}$:n kanssa

Esimerkki 10.1.14.



Lauseen todistus. Oletetaan, että $\alpha = a_1, \ldots, a_n \in Ac(\mathcal{A})$. Silloin $\exists s_0 = \delta_0, \delta_1, \ldots, \delta_n \in S$

$$\delta_i \in f(\delta_{i-1}, a_i), \quad i = 1, \ldots, n \text{ ja } \delta_n \in A.$$

Asetetaan

$$\begin{aligned} B_0 &= \{s_0\} \text{ ja} \\ B_i &= f'(B_{i-1}, a_i), \quad i = 1, \ldots, n. \end{aligned}$$

Koska

$$B_1 = f'(b_0, a_1) = f'(\{s_0\}, a_1) = f(s_0, a_1),$$

niin $\delta_1 \in B_1$. Nyt

$$\begin{aligned} &\delta_2 \in f(\delta_1, a_2) \subseteq \cup f(s, a_2) = f'(B_1, a_2) = B_2 \\ &s \in B_1. \end{aligned}$$

Samoin osoitetaan, että $\delta_3 \in B_3, \ldots, \delta_n \in B_n$. Koska $\delta_n \in A$, niin $B_n \in A'$. Saadaan siis

$$\begin{aligned} &f'(s_0, a_1) = f'(B_0, a_1) = B_1 \\ &f'(B_1, a_2) = B_2 \\ &f'(B_{n-1}, a_n) = B_n. \end{aligned}$$

Siten $\alpha = a_1, \ldots, a_n \in Ac(\mathcal{A}')$. Silloin $\exists \{s_0\} = s_0' = B_0, B_1, \ldots, B_n$

$$\begin{aligned} &f'(B_{i-1}, a_i) = B_i, \quad i = 1, \ldots, n \text{ ja} \\ &B_n \cap A \neq 0; \text{ olkoon } \delta_n \exists B_n \cap A. \end{aligned}$$

Koska $\delta_n \in B_n = f'(B_{n-1}, a_n) = \cup f(s, a_n)$,

$$s \in B_{n-1}.$$

On olemassa $\delta_{n-1} \in B_{n-1}$, jolle $\delta_n \in f(\delta_{n-1}, a_n)$.
Vastaavasti osoitetaan, että

$$\exists \delta_i \in B_i \quad \delta_{i+1} \in f(\delta_i, a_{i+1}), \quad i = n-1, n-1, \ldots, 0.$$

Erityisesti $\delta_0 \in B_0 = \{s_0\}$, joten $\delta_0 = s_0$. Koska $\delta_n \in A$, niin $\alpha \in Ac(\mathcal{A})$.
Seuraavaksi konstruoidaan äärellinen puoliautomaatti, jonka hyväksymien sanojen joukko on kahden annetun puoliautomaatin hyväksymien sanojen joukon unioni.

Lause 10.1.15. *Olkoon $\mathcal{A}_1 = (S_1, I, f_1, s_{01}, A_1)$ ja $\mathcal{A}_2 = (S_2, I, f_2, s_{02}, A_2)$ deterministisiä äärellisiä puoliautomaatteja, ja oletetaan, että $S_1 \cap S_2 = \emptyset$. Määritellään*

$$\mathcal{A} = (S, I, f, s_0, A),$$

missä

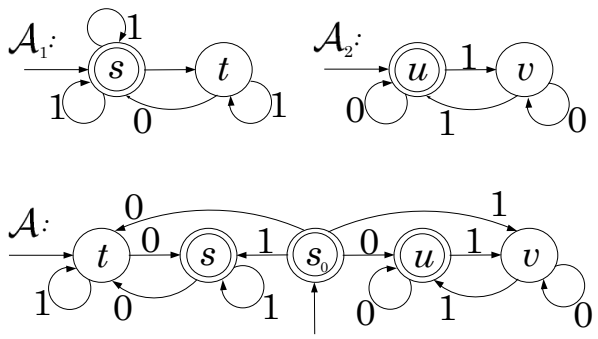
$$\begin{aligned} s_0 &\notin S_1 \cup S_2 \\ S &= \{s_0\} \cup S_1 \cup S_2 \\ f(s,a) &= \begin{cases} f_1(s,a), & \textit{jos } s \in S_1 \\ f_2(s,a), & \textit{jos } s \in S_2 \\ \{f_1(s_{01},a), f_2(s_{02}), a\}, & \textit{jos } s = s_0 \end{cases} \\ A &= \begin{cases} A_1 \cup A_2, & \textit{jos } s_{01} \notin A_1 \textit{ ja } s_{02} \notin A_2 \\ A_1 \cup A_2 \cup \{s_0\}, & \textit{muulloin.} \end{cases} \end{aligned}$$

Silloin

$$Ac(\mathcal{A}) = Ac(\mathcal{A}_1) \cup Ac(\mathcal{A}_2).$$

Todistus. Sivuutetaan.

Esimerkki 10.1.16.



Ja sitten katenaation hyväksyvä puoliautomaatti.

Lause 10.1.17. *Olkoot $\mathcal{A}_1$ ja $\mathcal{A}_2$ kuten edellisessä lauseessa. Määritellään*

$$\mathcal{A} = (S, I, f, s_0, A),$$

missä

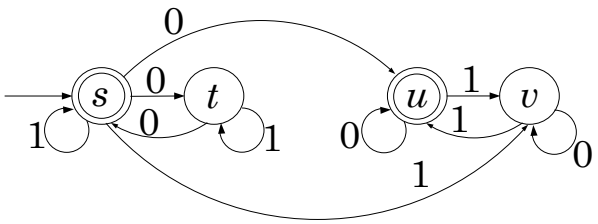
$$\begin{aligned} S &= S_1 \cup S_2 \\ \mathcal{A}(s,a) &= \begin{cases} f_2(s,a), & \textit{jos } s \in S_2 \\ f_1(s,a), & \textit{jos } s \in S_1 - A_1 \\ \{f_1(s,a), f_2(s_{02}), a\}, & \textit{jos } s \in A_1 \end{cases} \\ s_0 &= s_{01} \\ A &= \begin{cases} A_1 \cup A_2, & \textit{jos } s_{02} \in A_2 \\ A_2, & \textit{muulloin.} \end{cases} \end{aligned}$$

Silloin

$$Ac(\mathcal{A}) = Ac(\mathcal{A}_1)Ac(\mathcal{A}_2).$$

Todistus. Sivuutetaan. ■

Esimerkki 10.1.18. *$\mathcal{A}_1$ ja $\mathcal{A}_2$ kuten esimerkissä 10.1.16.*



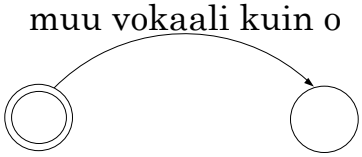
Esimerkki 10.1.19. *Ob on kieli, joka saadaan lisäämällä (esim.) englannin kielen sanoihin ob jokaisen vokaalin eteen.*

Esimerkki 10.1.20. *Hobby ei ole ob-kielen sana.*

Englanti	*Ob-kieli*
example	*obexobamplobe*
string	*strobing*
another	*obanobothober*
job	*jobob*

Esimerkki 10.1.21. *Suunnittele puoliautomaatti, jonka hyväksymä kieli on ob-kieli.*

[Jos yo. puoliautomaatin on oltava deterministinen, piirretään vielä]



Esimerkki 10.1.22. *Suunnittele äärellinen puoliautomaatti, joka hyväksyy sanat*

$$L = \{a^n b^n \mid n \in \mathbb{N}\}.$$

Vaadittua automaattia ei ole. Vastaoletus: A on äärellinen puoliautomaatti, jolle $A_c(\mathcal{A}) = L$. Olkoon $\mathcal{A}$:lle k tilaa. Sana $\alpha = a^k b^k \in A_c(\mathcal{A})$. α:a esittävän polun alusta se osa, joka esittää sanaa a^k kulkee $k+1$ kärjen eli tilan kautta. Koska tiloja on k kappaletta, jokin tila, sanokaamme s esiintyy ko. alkuosassa (ainakin) kahdesti. Siis tällä osalla on suljettu osapolku $s \to \ldots \to s$. Olkoon sen pituus j (jolloin $j \geq 1$). Lisäämällä tämä silmukka alkuperäiseen polkuun saadaan polku, joka esittää sanaa $\alpha' = a^{k+1}b^k$. Koska tämä polku päättyy samaan tilaan kuin alkuperäinenkin, α:a esittävä polku, niin, koska $\alpha \in A_c(\mathcal{A})$, myös $\alpha' \in A_c(\mathcal{A})$. Mutta $\alpha' = a^{k+j}b^k \notin L$.

10.1.3 Äärellinen automaatti

Äärellinen automaatti on kuusikko $\mathcal{M} = (\mathcal{I}, \mathcal{J}, \mathcal{O}, f, g, s_0)$, missä $\mathcal{I}, \mathcal{J}, f$ ja s_0 ovat kuten äärellisellä puoliautomaatilla. $\mathcal{O}$ on äärellinen joukko (tulostusaakkosto) ja g on kuvaus $\mathcal{I} \times \mathcal{J} \to \mathcal{O}$ (tulostusfunktio).
Äärellistä automaattia sanotaan myös *Mealyn automaatiksi*. Siinä erikoistapauksessa, että g riippuu vain s:stä, $\mathcal{M}$:ä sanotaan myös *Mooren automaatiksi*.
$\mathcal{M}$ voidaan antaa taulukkona:

$\mathcal{I} \setminus \mathcal{J}$	f			g		
	a_1	$\dots$	a_n	a_1	$\dots$	a_n
s_0	$f(s_0, a_1)$	$\dots$	$f(s_0, a_n)$	$g(s_0, a_1)$	$\dots$	$g(s_0, a_n)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
s_k	$f(s_k, a_1)$	$\dots$	$f(s_k, a_n)$	$g(s_k, a_1)$	$\dots$	$g(s_k, a_n)$

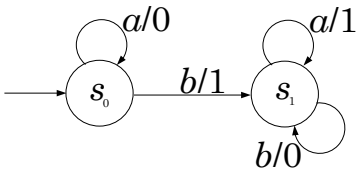
(jolloin lisäksi on mainittava alkutila) tai suunnattuna graafina, jossa on kaari $s \to t$, joka on merkattu a/o, joss $f(s, a) = t$ ja $g(s, a) = o$. Alkutila on merkitty tulevalla nuolella, jolla ei ole lähtökärkeä.
Automaatin syötöt ovat kuten puoliautomaatilla. Sana $b_1 \dots b_n \in \mathcal{O}^*$ on syöttöä $a_1 \dots a_n \in \mathcal{J}$ vastaava tulostus, jos $\exists s_0 = \delta_0, \delta_1, \dots, \delta_n \in \mathcal{I}$.

$$\begin{aligned} \delta_i &= f(\delta_{i-1}, a_i), \quad i = 1, \dots, n \\ b_i &= g(\delta_{i+1}, a_i), \quad i = 1, \dots, n \end{aligned}$$

Esimerkki 10.1.23.

$\mathcal{I} \setminus \mathcal{J}$	f		g	
	a	b	a	b
s_0	s_0	s_1	0	1
s_1	s_1	s_1	1	0

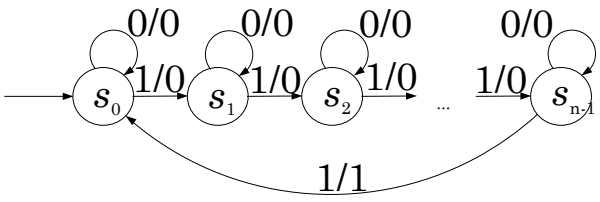
eli



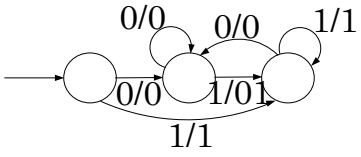
Syöttöä $aababba$ *vastaava tulostus on* 0011001.

Esimerkki 10.1.24. *(Sarjasummaaja). Suunnittele äärellinen automaatti, joka suorittaa kahden binääriluvun sarjayhteenlaskun, ts. joka saatuaan syöttönä binääriluvut* $x = x_n \dots x_1$ *ja* $y = y_n \dots y_1$ *muodossa* $x_1 y_1 x_2 y_2 \dots x_n y_n 00$ *tulostaa* $z_1 z_2 \dots z_n z_{n+1}$*, missä* $z_{n+1} z_n \dots z_1$ *on* $x + y$*.*
$J = \{0, 1\}^2, \mathcal{O} = \{0, 1\}$*, NC – ei muistinumeroa, C – muistinumero:*

Esimerkki 10.1.25. *Äärellinen automaatti, joka tulostaa ykkösen k:nnen syötetyn 1:n kohdalla, missä $k = 0 (\mathrm{mod}\, n)$ ja $k > 0$ ($n \in \mathbb{N}$ on annettu); muulloin tulostetaan 0. Syötöt binäärijonona.*

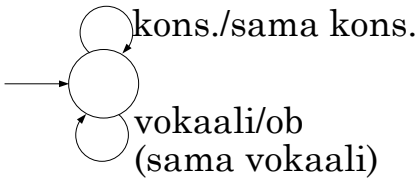


Esimerkki 10.1.26. *Automaatti*

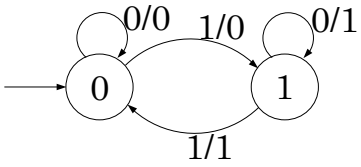


lisää syötetyn binäärijonon jokaiseen muotoa 0^+ olevan osajonon perään yhden nollan.

Esimerkki 10.1.27. *Automaatti kääntää englannista ob-kieleen.*



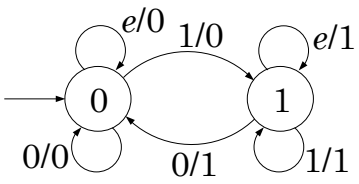
Esimerkki 10.1.28. *(trigger flip-flop)*



eli

		f		g	
$\mathcal{I}$	$\mathcal{J}$	0	1	0	1
0		0	1	0	0
1		1	0	1	1

Esimerkki 10.1.29. *(IR flip-flop)*



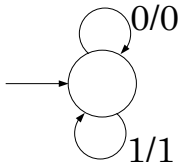
eli

$\mathcal{I}$ \ $\mathcal{J}$	f			g		
	e	0	1	e	0	1
0	0	0	1	0	0	0
1	1	0	1	1	1	1

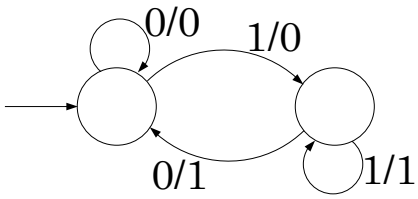
Havaitaan:

$$f(s,e) = s$$
$$f(s,0) = 0 \quad g(s,a) = s$$
$$f(s,1) = 1$$

Esimerkki 10.1.30. *Suunnittele automaatti, joka tulostaa binäärijonon k bitin viiveellä, ts. jos $y_1 \dots y_n$ on syöttöä $x_1 \dots x_n$ vastaava tulostus, niin $y_i = s_{i-k}, i = k+1, \dots, n$ (y_1:lle, …, y_k:lle ei ehtoa).*
Tehtävällä on ratkaisu $\forall k \in \mathbb{N}_0$. Tiloja tarvitaan 2^k. Ohessa ratkaisut tapauksissa $k = 0$ ja $k = 1$.
$k = 0$:

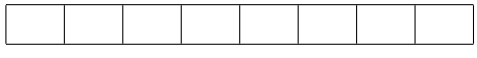


$k = 1$:



10.2 Turing-kone

Turingin kone on viisikko (S, Σ, fs_0, b), missä S on äärellinen joukko (tilajoukko), Σ on äärellinen joukko (*syöttö- ja tulostusaakkosto*), f on kuvaus $S \times \Sigma \to S \times \Sigma \times \{L, H, R\}$, $s_0 \in S$ (*alkutila*) ja $b \in \Sigma$ (*blanko, tyhjä*).
Turingin koneen syöttö- ja tulostusvälineenä on molempiin suuntiin ääretön nauha, jolla oleviin *ruutuihin* mahtuu tekstiä yksi merkki ruutua kohti. Tekstiä luetaan ja kirjoitetaan koneeseen kuuluvalla *luku/kirjoituspäällä*, merkki kerrallaan.



$\Uparrow$

Koneen syöttönä on jokin Σ^*:n sana, jonka kirjaimista vain äärellinen määrä saa olla blankosta poikkeavia. Kun ruudussa oleva merkki on luettu, sen päälle kirjoitetaan jokin merkki (mahdollisesti sama), tila (mahdollisesti) vaihdetaan ja luku/kirjoituspää siirretään yksi ruutu vasemmalle (L), oikealle (R) tai ei minnekään (H). H merkitsee koneen toiminnan pysäyttämistä. Syöttöä vastaava *tulostus* on se, mitä on nauhalla pysähtymishetkellä.
Luku/kirjoituspään sijainti (syöttösanaan nähden) alkutilanteessa on annettava.
Funktio f tarkoittaa seuraavaa: Esimerkiksi $f(s,a) = (t,b,R)$ merkitsee, että jos tila on s ja luettu kirjain a, vaihdetaan tilaksi t, kirjoitetaan a:n paikalle b ja siirrytään seuraavaan ruutuun oikealle.

Esimerkki 10.2.1. *Turingin kone, joka lisää annetun bittijonon loppuun* 0*:n tai* 1*:n niin, että bittien summa on* $= 0 (\mathrm{mod}\, 2)$.

b	b	$1\,1\,0\ldots\ldots\ldots 1\,1\,0$	b	b	b

$\Uparrow\ s_0$

s_0 – *parillinen määrä ykkösiä*
s_1 – *pariton määrä ykkösiä*

$S \backslash \Sigma$	f		
	0	1	b
s_0	$(s_0, 0, R)$	$(s_1, 1, R)$	$(s_0, 0, R)$
s_1	$(s_1, 0, R)$	$(s_0, 1, R)$	$(s_1, 1, H)$

Tulos:

b	b	$1\,1\,0\ldots\ldots\ldots 1\,1\,0$	0	b	b

$\Uparrow\ s_0$

tai

b	b	$1\,1\,0\ldots\ldots\ldots 1\,1\,0$	1	b	b

$\Uparrow\ s_1$

Esimerkki 10.2.2. *Turingin kone, joka poistaa bittijonon viimeisen bitin.*

b	b	$1\,0\,1\ldots\ldots\ldots 0\,1\,1\,0$	0	b	b

$\Uparrow\ s_0$

$f(s_0, 0) = (s_1, 0, R)$ *(s_0 tutkii, onko syöttöjono tyhjä)*
$f(s_0, 1) = (s_1, 1, R)$
$f(s_0, b) = (s_0, b, H)$

$f(s_1, 0) = (s_1, 0, R)$ *(s_1 etsii syöttöjonojen lopun)*
$f(s_1, 1) = (s_1, 1, R)$

$f(s_1, b) = (s_2, b, H)$

$f(s_2, 0) = (s_3, b, L)$ *(s_2 pyyhkii yli viimeisen bitin)*
$f(s_2, 1) = (s_3, b, L)$
$f(s_2, b) =$ *mv., (ei voi esiintyä)*

$f(s_3, 0) = (s_3, 0, L)$ *(s_3 etsii syötön ensimmäistä bittiä edeltävän blankon)*
$f(s_3, 1) = (s_3, 1, L)$
$f(s_3, b) = (s_4, b, R)$

$f(s_4, 0) = (s_0, 0, H)$ *(s_4 pyöräyttää koneen)*
$f(s_4, 1) = (s_0, 1, H)$
$f(s_4, b) = (s_0, b, H)$

b	b	$1\,0\,1\ldots\ldots\ldots 0\,1\,1$	b	b	b

$\Uparrow s_0$

Esimerkki 10.2.3. $S = \{s_0, s_1\}, \Sigma = \{a, b, b\}$

$$\begin{aligned} f(s_0, a) &= (s_1, a, R) \\ f(s_0, b) &= (s_0, b, H) \\ f(s_0, b) &= (s_0, b, H) \end{aligned}$$

$$\begin{aligned} f(s_1, a) &= (s_1, a, R) \\ f(s_1, b) &= (s_1, a, R) \\ f(s_1, a) &= (s_1, a, R) \end{aligned}$$

Ensimmäinen luettu kirjain tulostetaan sellaisenaan. Jos se oli b tai b, pysähdytään; jos a, tulostetaan äärettömän monta a:ta siitä oikealle.

Esimerkki 10.2.4. *Suunnittele Turingin kone, joka tutkii, onko sulkujoukko "oikein" muodostettu. Oikein muodostettujen sulkujonojen joukko P määritellään seuraavasti:*

(1) $(\ ) \leftarrow P$

(2) (2.1) $E \in P \Rightarrow (E) \in P$

(2.2) $E, F \in P \Rightarrow EF \in P$

Siis esimerkiksi $((\ )) \in P$, $(((\ )(\ ))) \in P$, $((\ ))(((\ ) \notin P$.

$$s = \{s_0, s_1, s_2\}, \Sigma = \{(,), X, b, 0, 1\}$$

b	b	$(\ (\ )\ \ldots\ldots\ldots\ (\ )\ )$	b	b	$\ldots$

$\Uparrow\ s_0$

$$
\begin{aligned}
f(s_0, () &= (s_0, (, R) \\
f(s_0,)) &= (s_1, X, L) \\
f(s_0, X) &= (s_0, X, R) \\
f(s_0, b) &= (s_2, b, L) \\
f(s_0, 0) &= \textit{mv. (ei voi esiintyä)} \\
f(s_0, 1) &= \textit{mv. (ei voi esiintyä)} \\
\\
f(s_1, () &= (s_0, X, R) \\
f(s_1,)) &= (s_1,), L) \\
f(s_1, X) &= (s_1, X, L) \\
f(s_1, b) &= (s_0, 0, H) \\
f(s_1, 0) &= \textit{mv. (ei voi esiintyä)} \\
f(s_1, 1) &= \textit{mv. (ei voi esiintyä)} \\
\\
f(s_2, () &= (s_0, 0, H) \\
f(s_2,)) &= \textit{mv. (ei voi esiintyä)} \\
f(s_2, X) &= (s_2, X, L) \\
f(s_2, b) &= (s_0, 1, H) \\
f(s_2, 0) &= \textit{mv. (ei voi esiintyä)} \\
f(s_2, 1) &= \textit{mv. (ei voi esiintyä)}
\end{aligned}
$$

Testataan jonolla (((( ) (*:*

$$
\begin{array}{cccccccccccccc}
\ldots & b & b & \underline{(} & (& (& (&) & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& \underline{(} & (& (&) & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& \underline{(} & (&) & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& \underline{(} &) & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& (& \underline{)} & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& \underline{(} & X & (& b & b & \ldots & / & s_1 \\
\ldots & b & b & (& (& (& X & \underline{X} & (& b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& X & X & \underline{(} & b & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& X & X & (& \underline{b} & b & \ldots & / & s_0 \\
\ldots & b & b & (& (& (& X & X & \underline{(} & b & b & \ldots & / & s_2 \\
\ldots & b & b & (& (& (& X & X & \underline{0} & b & b & \ldots & / & s_0
\end{array}
$$

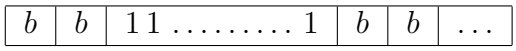
ja jonolla ( ) (( ) ( )) *:*

$$
\begin{array}{cccccccccccccccc}
\ldots & b & b & \underline{(} &) & (& (&) & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & \overline{(} &) & (& (&) & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & \underline{(} & \bar{X} & (& (&) & (&) &) & b & b & \ldots & / & s_1 \\
\ldots & b & b & \bar{X} & \underline{X} & (& (&) & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & \underline{(} & (&) & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & \overline{(} & \underline{(} &) & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& \overline{(} & \underline{)} & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& \underline{(} & \bar{X} & (&) &) & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & (& \bar{X} & \underline{X} & (&) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& X & X & \underline{(} &) &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& X & X & \overline{(} & \underline{)} &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& X & X & \underline{(} & \bar{X} &) & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & (& X & X & \bar{X} & \underline{X} &) & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& X & X & X & X & \underline{)} & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & (& X & X & X & \underline{X} & \bar{X} & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & (& X & X & \underline{X} & X & X & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & (& X & \underline{X} & X & X & X & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & (& \underline{X} & X & X & X & X & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & \underline{(} & X & X & X & X & X & b & b & \ldots & / & s_1 \\
\ldots & b & b & X & X & \bar{X} & \underline{X} & X & X & X & X & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & \bar{X} & \underline{X} & X & X & X & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & X & X & \underline{X} & X & X & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & X & X & X & \underline{X} & X & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & X & X & X & X & \underline{X} & b & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & X & X & X & X & X & \underline{b} & b & \ldots & / & s_0 \\
\ldots & b & b & X & X & X & X & X & X & X & \underline{X} & b & b & \ldots & / & s_2 \\
 & & & & & & & \vdots & & & & & & & & \\
\multicolumn{16}{c}{\textit{siirretään vasemmalle}} \\
 & & & & & & & \vdots & & & & & & & & \\
\ldots & b & b & \underline{X} & X & X & X & X & X & X & X & b & b & \ldots & / & s_2 \\
\ldots & b & \underline{b} & X & X & X & X & X & X & X & X & b & b & \ldots & / & s_2 \\
\ldots & \underline{1} & b & X & X & X & X & X & X & X & X & b & b & \ldots & / & s_0
\end{array}
$$

Esimerkki 10.2.5. *Suunnittele Turing-kone, joka muuntaa annetun luonnollisen luvun binäärijärjestelmään. Syöttö* n *annetaan muodossa*

$$n = 11 \ldots 1 (n \textit{ kpl})$$

$$S = \{s_0, s_1, s_2, s_3, s_4\}, \Sigma = \{b, 1, A, B, X\} \quad (A \textit{ vastaa } 0\textit{:a, } B \textit{ } 1\textit{:stä})$$



$$
\begin{aligned}
f(s_0, b) &= (s_2, b, L) \\
f(s_0, 1) &= (s_1, X, R) \\
f(s_0, A) &= (s_0, A, R) \\
f(s_0, B) &= (s_0, B, R) \\
f(s_0, X) &= (s_0, X, R)
\end{aligned}
$$

$$
\begin{aligned}
f(s_1, b) &= (s_3, b, L) \\
f(s_1, 1) &= (s_0, 1, R) \\
f(s_1, A) &= (s_1, A, R) \\
f(s_1, B) &= (s_1, B, R) \\
f(s_1, X) &= (s_1, X, R)
\end{aligned}
$$

$$
\begin{aligned}
f(s_2, b) &= (s_4, A, R) \\
f(s_2, 1) &= (s_2, 1, L) \\
f(s_2, A) &= (s_2, A, L) \\
f(s_2, B) &= (s_2, B, L) \\
f(s_2, X) &= (s_2, X, L)
\end{aligned}
$$

$$
\begin{aligned}
f(s_3, b) &= (s_4, B, R) \\
f(s_3, 1) &= (s_3, 1, L) \\
f(s_3, A) &= (s_3, A, L) \\
f(s_3, B) &= (s_3, B, L) \\
f(s_3, X) &= (s_3, X, L)
\end{aligned}
$$

$$
\begin{aligned}
f(s_4, b) &= (s_0, b, H) \\
f(s_4, 1) &= (s_1, X, R) \\
f(s_4, A) &= (s_4, A, R) \\
f(s_4, B) &= (s_4, B, R) \\
f(s_4, X) &= (s_4, X, R)
\end{aligned}
$$

Testataan luvulla 5*:*

$$
\begin{array}{cccccccccccccc}
\ldots & b & b & b & b & \underline{1} & 1 & 1 & 1 & 1 & b & b & \ldots & / \; s_0 \\
\ldots & b & b & b & b & X & \underline{1} & 1 & 1 & 1 & b & b & \ldots & / \; s_1 \\
\ldots & b & b & b & b & X & 1 & \underline{1} & 1 & 1 & b & b & \ldots & / \; s_0 \\
\ldots & b & b & b & b & X & 1 & X & \underline{1} & 1 & b & b & \ldots & / \; s_1 \\
\ldots & b & b & b & b & X & 1 & X & 1 & \underline{1} & b & b & \ldots & / \; s_0 \\
\ldots & b & b & b & b & X & 1 & X & 1 & X & \underline{b} & b & \ldots & / \; s_1 \\
\ldots & b & b & b & b & X & 1 & X & 1 & \underline{X} & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & b & X & 1 & X & \underline{1} & X & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & b & X & 1 & \underline{X} & 1 & X & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & b & X & \underline{1} & X & 1 & X & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & b & \underline{X} & 1 & X & 1 & X & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & \underline{b} & X & 1 & X & 1 & X & b & b & \ldots & / \; s_3 \\
\ldots & b & b & b & B & \underline{X} & 1 & X & 1 & X & b & b & \ldots & / \; s_4 \\
\ldots & b & b & b & B & X & \underline{1} & X & 1 & X & b & b & \ldots & / \; s_4 \\
\ldots & b & b & b & B & X & X & \underline{X} & 1 & X & b & b & \ldots & / \; s_1 \\
\ldots & b & b & b & B & X & X & X & \underline{1} & X & b & b & \ldots & / \; s_1 \\
\ldots & b & b & b & B & X & X & X & 1 & \underline{X} & b & b & \ldots & / \; s_0 \\
\ldots & b & b & b & B & X & X & X & 1 & X & \underline{b} & b & \ldots & / \; s_0 \\
\ldots & b & b & b & B & X & X & X & 1 & \underline{X} & b & b & \ldots & / \; s_2 \\
 & & & & & & & \vdots & & & & & &
\end{array}
$$

siirretään vasemmalle

$$
\begin{array}{cccccccccccccc}
 & & & & & & & \vdots & & & & & & \\
\ldots & b & b & \underline{b} & B & X & X & X & 1 & X & b & b & \ldots & / \; s_2 \\
\ldots & b & b & A & \underline{B} & X & X & X & 1 & X & b & b & \ldots & / \; s_4 \\
 & & & & & & & \vdots & & & & & &
\end{array}
$$

siirretään oikealle

$$
\begin{array}{cccccccccccccc}
 & & & & & & & \vdots & & & & & & \\
\ldots & b & b & A & B & X & X & X & \underline{1} & X & b & b & \ldots & / \; s_4 \\
\ldots & b & b & A & B & X & X & X & X & \underline{X} & b & b & \ldots & / \; s_1 \\
\ldots & b & b & A & B & X & X & X & X & X & \underline{b} & b & \ldots & / \; s_1 \\
\ldots & b & b & A & B & X & X & \underline{X} & X & \underline{X} & b & b & \ldots & / \; s_3 \\
 & & & & & & & \vdots & & & & & &
\end{array}
$$

siirretään vasemmalle

$$
\begin{array}{cccccccccccccc}
 & & & & & & & \vdots & & & & & & \\
\ldots & b & \underline{b} & A & B & X & X & X & X & X & b & b & \ldots & / \; s_3 \\
\ldots & b & B & \underline{A} & B & X & X & X & X & X & b & b & \ldots & / \; s_4 \\
 & & & & & & & \vdots & & & & & &
\end{array}
$$

siirretään oikealle

$$
\begin{array}{cccccccccccccc}
 & & & & & & & \vdots & & & & & & \\
\ldots & b & B & A & B & X & X & X & X & X & \underline{b} & b & \ldots & / \; s_4 \\
\ldots & b & B & A & B & X & X & X & X & X & \underline{b} & b & \ldots & / \; s_0
\end{array}
$$

Tulos on siis BAB *eli* 010*, niin kuin pitääkin.*

Turingin koneiden todellinen tärkeys johtuu *Turingin hypoteesista* eli *Churcin teesistä*: Jokainen funktio, joka voidaan laskea jollakin (ehkä hypoteettisella) digitaalisella tietokoneella, voidaan laskea jollakin Turingin koneella.
Churcin teesistä seuraa, että Turingin kone on digitaalisen tietokoneen oikea abstrakti malli. Churcin teesistä saadaan myös seuraava muodollinen määritelmä algoritmille: *Algoritmi* on Turingin kone, joka syötön saatuaan pysähtyy äärellisen ajan kuluessa.

11 FORMAALISET KIELET

11.1 Kielioppi ja kieli

Kielioppi on nelikko

$$G = (N, T, S, P),$$

missä N on äärellinen joukko (*välisymbolien* joukko); T on äärellinen joukko (*loppusymbolien* (*päätesymbolien*) joukko), missä $N \cap T = \emptyset$; $S \in N$ (*alkusymboli, lähtösymboli*) ja P on joukon

$$((N \cup T)^* \backslash T^*) \times (N \cup T)^*$$

äärellinen osajoukko (*produktioiden* joukko).

Esimerkki 11.1.1. *Olkoon*
$N = \{S, A\}$, $T = \{a, b\}$ *ja* $P = \{(S, bS), (S, aA), (A, bA), (A, b)\}$.
Silloin $G = (N, T, S, P)$ *on kielioppi.*

Produktioita merkitään usein $\alpha \to \beta$ merkinnän (α, β) asemesta.
Olkoon $G = (N, T, S, P)$ kielioppi. Jos $\mu\alpha\nu \in (N \cup T)^*$ ja $\alpha \to \beta$ on produktio, sanotaan, että $\mu\beta\nu$ on *suoraan johdettavissa* $\mu\alpha\nu$:sta, merkitään

$$\mu\alpha\nu \Rightarrow \mu\beta\nu.$$

Jos $\alpha_i \in (N \cup T)^*$, $i = 1, \ldots, n$ ja α_{i+1} on suoraan johdettavissa α_i:stä, $i = 1, \ldots, n-1$, sanotaan, että α_n on *johdettavissa* α_1:stä, merkitään

$$\alpha_1 \Rightarrow *\alpha_n.$$

$\alpha_1 \Rightarrow \alpha_2 \Rightarrow \ldots \Rightarrow \alpha_n$ on α_n:n *johto* α_1:stä, G:n *generoima*(*määräämä*) *kieli* on

$$L(G) = \{\alpha \in T^* \mid S \Rightarrow^* \alpha\}.$$

Esimerkki 11.1.2. *Tarkastellaan esimerkin 11.1.1 kielioppia. Käyttämällä produktiota* $A \to bA$ *todetaan, että*

$$aAbb \Rightarrow abAbb.$$

$bbab \in L(G)$, *koska* $S \Rightarrow^* bbab$*:*

$$S \Rightarrow bS \Rightarrow bbS \Rightarrow bbaA \Rightarrow bbab.$$

Ainoat johdot S*:stä ovat*

$$\begin{aligned}
S &\Rightarrow bS \\
&\vdots \\
&\Rightarrow b^n S \qquad (n \geq 0) \\
&\Rightarrow b^n aA \\
&\vdots \\
&\Rightarrow b^n ab^{m-1} A \\
&\Rightarrow b^n ab^m \qquad (m \geq 1)
\end{aligned}$$

Siis

$$\begin{aligned} L(G) &= \{b^n a b^m \mid n \in \mathbb{N}_0, m \in \mathbb{N}\} \\ &= \{\alpha \in \{a,b\}^* \mid \alpha\textit{:ssa on täsmälleen yksi } a \textit{ ja } \alpha \textit{ päättyy } b\textit{:hen}\}. \end{aligned}$$

Produktiot $\alpha \to \beta_1, \ldots, \alpha \to \beta_k$ kirjoitetaan usein lyhyesti

$$\alpha \to \beta_1 | \beta_2 | \ldots | \beta_k.$$

Esimerkki 11.1.3. $G = (N, T, S, P)$, *missä* $N = \{S, A, B, C\}$, $T = \{a, b\}$,

$$\begin{aligned} P \;:\; & S \to aA \\ & A \to bA|aB|C \\ & B \to aB|C \\ & C \to b. \end{aligned}$$

$aaaaab \in L(G)$, *sillä*

$$S \Rightarrow aA \Rightarrow a^2B \Rightarrow a^3b \Rightarrow a^4B \Rightarrow a^5B \Rightarrow a^5C \Rightarrow a^5b.$$

$ababbbb \notin L(G)$, *sillä ainoa yritys*

$$S \Rightarrow aA \Rightarrow abA \Rightarrow abaB \Rightarrow abaC \Rightarrow abab$$

ei tuota haluttua sanaa.

Esimerkki 11.1.4. $G = (N, T, S, P)$, *missä* $N = \{S, A, B\}$, $T = \{a, b\}$,

$$\begin{aligned} P \;:\; & S \to aA \\ & A \to aAB|a \\ & B \to b. \end{aligned}$$

Voidaan osoittaa, että $L(G) = \{a^{n+1}b^n \mid n \in \mathbb{N}_0\}$.

Backus-Naur -muodossa (BNF) välisymbolit merkitään kulmasuluilla, ja produktio $\alpha \to \beta$ merkitään $\alpha ::= \beta$.

Esimerkki 11.1.5. *Kielioppi* G*:*
<digit> $::= 0|1|2|3|4|5|6|7|8|9$
<integer> ::= <signed integer>|<unsigned integer>
<signed integer> ::= +<unsigned integer>|-<unsigned integer>
<unsigned integer> ::= <digit>|<digit><unsigned integer>
alkusymboli <integer>
on määritelmän mukaisessa muodossa

$$G = (N, T, S, P),$$

missä

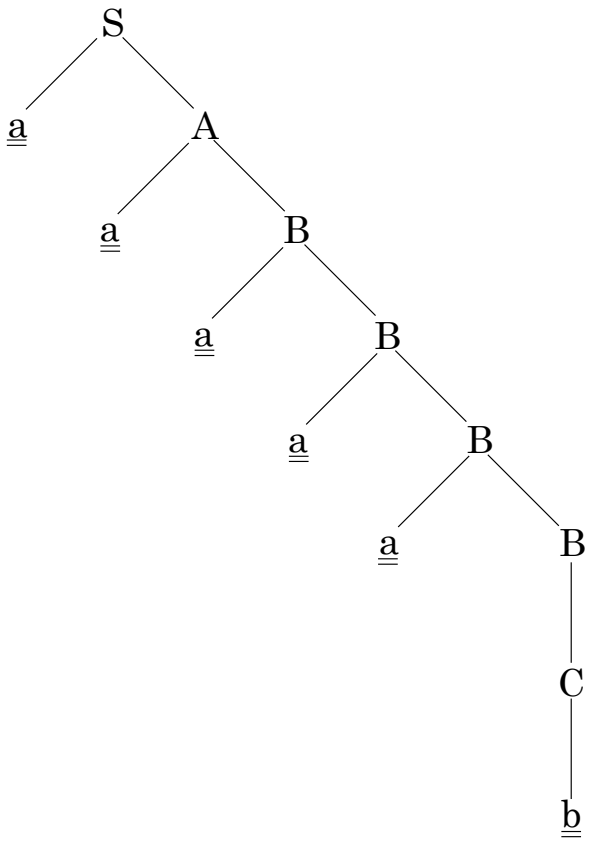
$$
\begin{aligned}
N &= \{\text{<digit>, <integer>, <signed integer>, <unsigned integer>}\},\\
T &= \{0,1,2,3,4,5,6,7,8,9,+,-\},\\
S &= \text{<integer>},\\
P &: \text{<digit>} \to 0|1|2|3|4|5|6|7|8|9\\
&\quad \text{<integer>} \to \text{<signed integer>}|\text{<unsigned integer>}\\
&\quad \text{<signed integer>} \to +\text{<unsigned integer>}|-\text{<unsigned integer>}\\
&\quad \text{<unsigned integer>} \to \text{<digit>}|\text{<digit><unsigned integer>}.
\end{aligned}
$$

G generoi kokonaisluvut. Esimerkkinä kokonaisluvun -901 johto:

$$
\begin{aligned}
\text{<integer>} &\Rightarrow \text{<signed integer>}\\
&\Rightarrow -\text{<unsigned integer>}\\
&\Rightarrow -\text{<digit><unsigned integer>}\\
&\Rightarrow -\text{<digit><digit><unsigned integer>}\\
&\Rightarrow -\text{<digit><digit><digit>}\\
&\Rightarrow -9\text{<digit><digit>}\\
&\Rightarrow -90\text{<digit>}\\
&\Rightarrow -901
\end{aligned}
$$

Sanan johto voidaan esittää tyyppiä context-free (määritellään myöhemmin) olevissa kielio-peissa myös *jäsennyspuun* avulla. Jäsennyspuun käsite selvinnee seuraavasta esimerkistä.

Esimerkki 11.1.6. *Olkoon G kuten esimerkissä 11.1.3. Sanan $aaaaab$ jäsennyspuu on*



Jos kielioppi ei ole context-free, sanan johtoa ei välttämättä voida esittää puuna, vaan suunnattuna graafina, jossa on silmukoita.
Seuraavaksi tarkastellaan kieliopin yksikäsitteisyyttä.
Sanan $\in L(G)$ johto ei välttämättä ole yksikäsitteinen. *Vasemmalta kanoninen johto* on sellainen, jossa produktioita sovelletaan kussakin vaiheessa vasemmalta oikealle - järjestyksessä, ts. vasemmalta oikealle katsottuna ensimmäisessä mahdollisessa kohdassa.

Esimerkki 11.1.7. *Produktiota $S \to AB$, $A \to a$ ja $B \to b$ käyttäen on sanalla ab johdot*

$$S \to AB \to aB \to ab \quad \textit{ja} \quad S \to AB \to Ab \to ab.$$

Näistä vain ensimmäinen on vasemmalta kanoninen johto.

Kielioppi on *yksikäsitteinen*, jos sen generoiman kielen jokaisen sanan vasemmalta kanoninen johto on yksikäsitteinen.

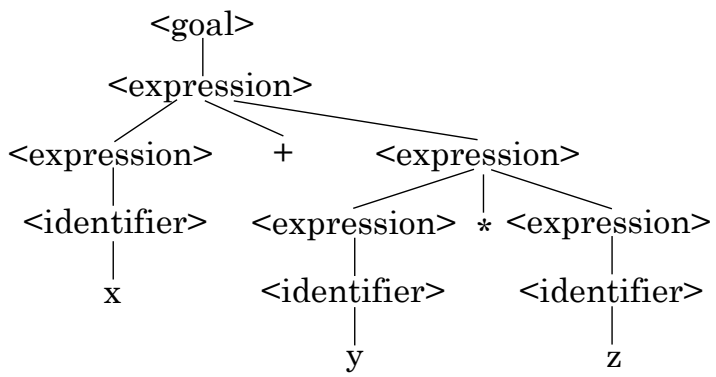
Esimerkki 11.1.8. *Kielioppi*

$$\begin{aligned} \textit{<goal>} &::= \textit{<expression>} \\ \textit{<expression>} &::= \textit{<expression>} + \textit{<expression>} \mid \textit{<expression>} * \textit{<expression>} \\ &\quad \mid \textit{<identifier>} \\ < identifier > &::= x \mid y \mid z \end{aligned}$$

ei ole yksikäsitteinen, sillä sanalla $x + y * z$ on vasemmalta kanoniset johdot.

$$
\begin{aligned}
\langle \textit{goal} \rangle &::= \langle \textit{expression} \rangle \\
&::= \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= \langle \textit{expression} \rangle + \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= x + \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= x + \langle \textit{identifier} \rangle * \langle \textit{expression} \rangle \\
&::= x + y * \langle \textit{expression} \rangle \\
&::= x + y * \langle \textit{identifier} \rangle \\
&::= x + y * z
\end{aligned}
$$

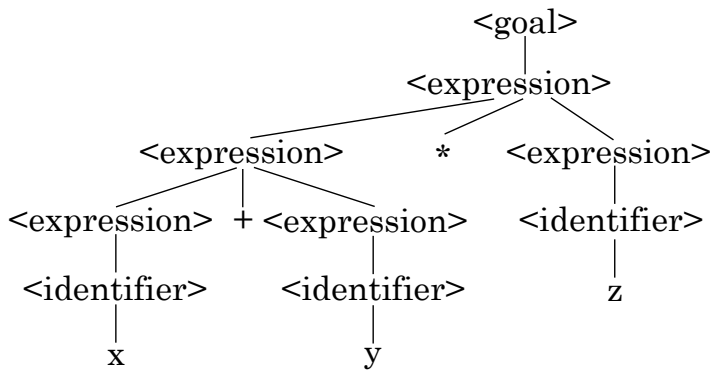
eli jäsennyspuuna



ja

$$
\begin{aligned}
\langle \textit{goal} \rangle &::= \langle \textit{expression} \rangle \\
&::= \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= \langle \textit{expression} \rangle + \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= \langle \textit{identifier} \rangle + \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= x + \langle \textit{expression} \rangle * \langle \textit{expression} \rangle \\
&::= x + \langle \textit{identifier} \rangle * \langle \textit{expression} \rangle \\
&::= x + y * \langle \textit{expression} \rangle \\
&::= x + y * \langle \textit{identifier} \rangle \\
&::= x + y * z
\end{aligned}
$$

eli jäsennyspuuna



Edellisen johdon 'merkitys' on $x + (y * z)$ *ja jälkimmäisen* $(x + y) * z$*.*

Esimerkki 11.1.9. *Kieliopissa*
<*goal*> ::= <*expression*>
<*expression*> ::= <*term*>|<*expression*>+<*term*>
<*term*> ::= <*factor*>|<*term*>∗<*factor*>
<*factor*> ::= $x \mid y \mid z$
sanalla $x + y * z$ *on vain yksi vasemmalta kanoninen johto, nimittäin*

$$\begin{aligned}
\text{<goal>} &::= \text{<expression>} \\
&::= \text{<expression>}*\text{<term>} \\
&::= \text{<term>}+\text{<term>} \\
&::= \text{<factor>}+\text{<term>} \\
&::= x + \text{<term>} \\
&::= x + \text{<term>}*\text{<factor>} \\
&::= x + \text{<factor>}*\text{<factor>} \\
&::= x + y * \text{<factor>} \\
&::= x + y * z
\end{aligned}$$

11.2 Kielioppien tyyppejä

Kielioppi on
tyyppiä 0, jos se on kielioppi;
tyyppiä 1, jos sen jokainen produktio $\alpha \to \beta$ täyttää ehdon

$$1(\alpha) \leq 1(\beta);$$

context-sensitive, jos sen jokainen produktio on muotoa

$\alpha A \beta \to \alpha \delta \beta$, missä $\alpha, \beta \in (N \cup T)^*$, $A \in N$ ja $\delta \in (N \cup T)^+$;

context-free eli *tyyppiä 2*, jos sen jokainen produktio on muotoa

$A \to \delta$, missä $A \in N$ ja $\delta \in (N \cup T)^+$;

oikealta lineaarinen, jos sen jokainen produktio on muotoa

$$A \to a \text{ tai } A \to aB, \text{ missä } A, B \in N, a \in T;$$

vasemmalta lineaarinen, jos sen jokainen produktio on muotoa

$$A \to a \text{ tai } A \to Ba, \text{ missä } A, B \in N, a \in T;$$

säännöllinen eli *tyyppiä 3*, jos se on vasemmalta tai oikealta lineaarinen.
Huom. Eo. käsitteiden määritelmät vaihtelevan jonkin verran kirjallisuudessa.

Esimerkki 11.2.1. *Esimerkin 11.1.1 kielioppi on oikealta lineaarinen, esimerkkien 11.1.3, 11.1.4, 11.1.5, 11.1.8 ja 11.1.9 kieliopit ovat context-free.*

Esimerkki 11.2.2. *Kielioppi $G = (N, T, S, P)$, missä $N = (S, A, B)$, $T(a, b)$, $P = \{S \to aAB, AB \to bB, B \to b, A \to aBA \,|\, aB\}$, on context-sensitive, mutta ei context-free.*

Kieli on tyyppiä 0 (tyyppiä 1, context-sensitive, tyyppiä 2, tyyppiä 3), jos on olemassa sen generoiva kielioppi, joka on tyyppiä 0 (tyyppiä 1, context-sensitive, tyyppiä 2, tyyppiä 3).

Esimerkki 11.2.3. *Esimerkin 11.1.5 kieli (kokonaisluvut) on context-free.*

Kieliopit G_1 ja G_2 ovat *ekvivalentit*, jos ne generoivat saman kielen:
$L(G_1) = L(G_2)$.
On mahdollista, että $L(G_1) = L(G_2)$, vaikka G_1 ja G_2 ovat eri tyyppiä.

Esimerkki 11.2.4. *Esimerkin 11.1.5 kielioppi, joka generoi kokonaisluvut, on context-free, mutta ei säännöllinen. Myös kielioppi*
<digit> ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<integer> ::= *<signed integer>*|*<unsigned integer>*
<signed integer> ::= +*<unsigned integer>*| −*<unsigned integer>*
<unsigned integer> ::= *<digit>*| 0 *<unsigned integer>*| 1 *<unsigned integer>* . . . | 9 *<unsigned integer>*
alkusymboli: <integer>
generoi kokonaisluvut, ja tämä kielioppi on säännöllinen.

11.3 kielioppien ja automaattien välinen yhteys

Tarkastelemme lopuksi hieman kielioppien ja automaattien välisiä yhteyksiä.

Lause 11.3.1. *Kieli L on säännöllinen, jos on olemassa äärellinen puoliautomaatti, jonka hyväksymien sanojen joukko on L.*

Todistuksen idea. "⇐", ts. oletetaan, että $\mathcal{A}$ on äärellinen puoliautomaatti, jolle $Ac(\mathcal{A}) = L$, ja väitetään, että L on säännöllinen, eli että on olemassa säännöllinen kielioppi G, jolle $L(G) = L$. Konstruoidaan G seuraavasti: Välisymboleiksi otetaan $\mathcal{A}$:n tilat, loppusymboleiksi $\mathcal{A}$:n syöttöaakkosto, alkusymboliksi $\mathcal{A}$:n alkutila, ja produktioihin otetaan

$$S \to S'$$

jos $\mathcal{A}$:n diagrammissa on nuoli $S \to S'$, joka on merkattu a:lla, ja

$$S \to a,$$

jos $\mathcal{A}$:n diagrammissa on a:lla merkattu nuoli S:stä hyväksyvään tilaan.
Selvästi G on säännöllinen (oikealta lineaarinen), ja on melko helppo osoittaa, että G täyttää vaaditun ehdon $L(G) = L$.

Esimerkki 11.3.2. *Olkoon $\mathcal{A}$ esimerkin 10.1.4 äärellinen puoliautomaatti. Yo. konstruktion mukainen G on*

$$G = (N, T, S, P),$$

missä

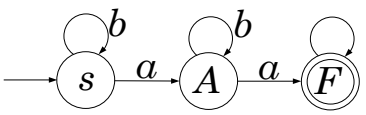
$$\begin{aligned} N &= \{e, o\}, \\ T &= \{0, 1\}, \\ S &= o \\ P &= \{e \to 0e, e \to 1o, o \to 1e, o \to 0o, e \to 1, o \to 0\} \end{aligned}$$

"$\Rightarrow$", ts. oletetaan, että L on säännöllinen kieli, ja väitetään, että on olemassa äärellinen puoliautomaatti $\mathcal{A}$, jolle $Ac(\mathcal{A}) = L$.
Koska L on säännöllinen, on olemassa säännöllinen kielioppi G, jolle $L(G) = L$. Tarkastellaan tässä vain tapausta G oikealta lineaarinen. (Toinen mahdollisuus eli G vasemmalta lineaarinen on jonkin verran mutkikkaampi käsitellä.)
Olkoon $G = (N, T, S, P)$. Määritellään $\mathcal{A} = (S, I, f, s_0, A)$ seuraavasti:

$$\begin{aligned} S &= N \cup \{F\}, \text{ missä } F \notin N \cup T, \\ I &= T, \\ f(s, a) &= \{t \mid s \to at \in P\} \cup \{F \mid s \to a \in P\}, \\ s_0 &= S, \\ A &= \{F\}. \end{aligned}$$

Selvästi $\mathcal{A}$ on äärellinen puoliautomaatti (ei välttämättä deterministinen), ja voidaan melko helposti osoittaa, että $Ac(\mathcal{A}) = L$.

Esimerkki 11.3.3. *Olkoon G esimerkin 11.1.1 (oikealta lineaarinen kielioppi. Yo. konstruktion mukainen $\mathcal{A}$ on*



12 LUKUTEORIAA

Lukuteoriassa käsitellään kokonaislukujen

$$\ldots, -2, -1, 0, 1, 2, \ldots$$

tiettyjä ominaisuuksia tai sellaisia reaali- ja kompleksilukujen ominaisuuksia, jotka ovat läheisessä yhteydessä kokonaislukuihin.

12.1 Lukuteoreettisia probleemeja

I Multiplikatiiviset probleemat käsittelevät lukujen jaollisuutta.

(1) **Lukuteorian peruslause.** Jokainen kokonaisluku $k > 1$ voidaan esittää yksikäsitteisesti (tekijöiden järjestystä lukuunottamatta) alkulukujen tulona.

Alkuluku on sellainen kokonaisluku $p > 1$, jolla ei ole muita tekijöitä (> 0) kuin luku 1 ja luku p itse.

(2) Merkitään kokonaisluvun n positiivisten tekijöiden lukumäärää $\tau(n)$:llä.

Esim. $\tau(12) = 6$, koska sen positiiviset tekijät ovat

$$1, 2, 3, 4, 6 \text{ ja } 12$$

Niitä on siis 6 kpl. $\tau(p) = 2 \Leftrightarrow p$ on alkuluku. p:n positiiviset tekijät ovat 1 ja$p$.
$\tau(2^m) = m + 1$, sillä 2^m:n positiiviset tekijät ovat

$$1, 2, 2^2, 2^3, \ldots, 2^m.$$

Siis $\tau(n) = \frac{\log n}{\log 2} + 1$, kun $n = 2^m$.

Koska alkulukuja on äärettömän paljon , niin $\tau(n)$:llä on arvo 2 äärettömän monella n:n arvolla

Toisaalta $\tau(n)$ voi saada kuinka suuria arvoja tahansa, koska $\tau(2^m) = m + 1$.

$\tau(n)$:ään liittyviä kysymyksiä:

(a) Mikä on $\tau(n)$:n arvo keskimäärin, ts. mitä voidaan sanoa lausekkeen

$$\frac{1}{N} \sum_{n=1}^{N} \tau(n)$$

arvosta, kun $N \to \infty$?

(b) Onko $\tau(n)\tau(m) = \tau(mn)$ aina, kun m:llä ja n:llä ei ole yhteisiä tekijöitä (multiplikatiivisuus)?

(c) Onko aina $\tau(n) \leq \frac{\log n}{\log 2} + 1$, ts. antavatko muotoa 2^m olevat luvut suhteellisesti suurimman τ-funktion arvon?

(d) Kuinka monta ratkaisua on yhtälöllä $\tau(n) = 2$, kun $n \leq N$ (N on annettu positiivinen kokonaisluku), ts. kuinka moni luvuista $1, 2, \ldots, N$ on alkuluku?

(3) **Alkulukujen jakautuminen**

Merkitään

$$\pi(N) = \#\{p \,|\, p \leq N \text{ on alkuluku}\}.$$

$\pi(N)$ on siis niiden alkulukujen p lukumäärä, jotka toteuttavat ehdon $p \, leN$.

Esim. $\pi(10) = 4$, koska 10:tä pienemmät alkuluvut ovat $2, 3, 5$ ja 7 (4 kpl).

Gauss, Legendre, Hadamard (tod. 1896):

Alkulukulause.

$$\lim_{N\to\infty} \frac{\pi(N)}{\frac{N}{\ln N}} = 1.$$

Bertrandin lause. Jos $n > 1$, niin lukujen n ja $2n$ välissä on ainakin yksi alkuluku.

Diricklet'n lause. Jos luvuilla a ja b ei ole yhteisiä tekijöitä, on lukujonossa

$$na + b \quad (n = 0, 1, 2, \ldots)$$

äärettömän monta alkulukua.

II Additiiviset probleemat

Additiiviset probleemat käsittelevät positiivisten kokonaislukujen esittämistä joidenkin erikoistyyppisten kokonaislukujen summana.

Esimerkkejä additiivisista probleemeista

(1) Mitkä luvut voidaan esittää kahden kokonaisluvun neliöiden summana ja montako tällaista esitystä kullakin kokonaisluvulla on?
$5 = 1^2 + 2^2$
$13 = 2^2 + 3^2$
12:lla ei tällaista esitystä ole.

(2) Definiittibinäärinen neliömuoto

$$x^2 + 2xy + 2y^2$$

esittää luvun 10, sillä yhtälöllä

$$x^2 + 2xy + 2y^2 = 10$$

on kokonaislukuratkaisu $x = 2$, $y = 1$.

Geometrisesti: Ellipsin $x^2 + 2xy + 2y^2 = 10$ kehällä on kokonaislukupiste $(2, 1)$

KUVA

(3) **Goldlandin väite:** Jokainen luku voidaan esittää kahden parittoman alkuluvun summana.

Esim. $12 = 5 + 7$

III Diofantoksen yhtälöt

Diofantoksen yhtälöt ovat yhden tai useamman muuttujan yhtälöitä, joilla etsitään kokonaislukuratkaisuja (tai ainakin rationaalisia ratkaisuja).

Esim.

(1) Mitkä ovat yhtälön

$$x^2 + y^2 = z^2$$

kaikki kokonaislukuratkaisut? Eräs ratkaisu on $x = 3$, $y = 4$, $z = 5$.

(2) Fermat'n yhtälö

$$x^n + y^n = z^n.$$

Fermat väitti, että tällä yhtälöllä ei ole kokonaislukuratkaisuja, kun $n \geq 3$ (paitsi triviaalit ratkaisut $x = 0$, $y = \pm z$). Yhtälön tutkiminen on vaikuttanut ratkaisevasti lukuteorian kehitykseen.

(3) Lineaarinen yhtälö

$$ax + by = c$$

(a, b ja c ovat kokonaislukuja).

Esim. $5x + 22y = 18$

$$\begin{aligned}
x &= \frac{18 - 22y}{5} \text{ pitää olla kokonaisluku } \Rightarrow \\
x &= 3 - 4y + \frac{3 - 2y}{5} = 3 - 4y + z \Rightarrow z = \frac{3 - 2y}{5} \Rightarrow \\
y &= \frac{3 - 5z}{2} = 1 - 2z + \frac{1 - z}{2} = 1 - 2z + t \Rightarrow t = \frac{1 - z}{2} \Rightarrow \\
z &= 1 - 2t \\
& t \in \mathbb{Z} \Rightarrow \left\{ \begin{array}{rcl} x &=& 8 - 22t \\ y &=& -1 + 5t \end{array} \right. \quad (t = 0, t = \pm 1, t = \pm 2, \ldots).
\end{aligned}$$

IV Diofantonksen approksimaatiot

(1) Jos α on annettu reaaliluku ja N luonnollinen luku, on määrättävä sellainen rationaaliluku $\frac{p}{q}$, missä $q \leq N$, että erotus

$$\left| \alpha - \frac{p}{q} \right|$$

on mahdollisimman pieni.

(2) Lukujen e ja π transkendenttisuustodistukset. Luku on transkendenttinen, jos se ei ole minkään yhtälön

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

($a_i \in \mathbb{Z} \forall i$) juuri.

12.2 Kokonaislukujen kantaesitys

Roomalainen järjestelmä: I, II, III, ...
Kokonaislukujen esittämiseen tarvitaan äärettömän monta numeromerkkiä.
Positiojärjestelmät: Luvun suuruuden määräävät esiintyvien numeromerkkien paikat siten, että jos kantaluku on k, niin

$$a_n a_{n-1} \dots a_1 a_0$$

tarkoittaa lukua

$$a_n k^n + a_{n-1} k^{n-1} + \dots + a_1 k + a_0.$$

Tarvitaan siis vain $k-1$ numeromerkkiä ja nolla.
Esim. 10-järjestelmässä

$$2056 = 2 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10 + 6.$$

Lause 12.2.1. *Jos a ja b ovat mielivaltaisia kokonaislukuja ($b \neq 0$), on olemassa sellaiset yksikäsitteisesti määrätyt kokonaisluvut q ja r, että on voimassa*

$$a = qb + r, \quad 0 \leq r \leq |b|. \tag{12.1}$$

Lause 12.2.2. *Olkoon $k > 1$. Silloin jokainen luonnollinen luku a voidaan esittää yksikäsitteisesti muodossa*

$$a = a_0 + a_1 k + \dots + a_n k^n,$$

missä $0 \leq a_i < k$ ($i = 1, \dots, n$) ja $a_0 > 0$.

k-järjestelmän lukua merkitään

$$(a_n a_{n-1} \dots a_1, a_0)_k,$$

esim. $(1234)_6$. Jos k:ta ei merkitä näkyviin, on kyseessä 10-järjestelmän luku.

Esimerkki 12.2.3. *Luku 4457 11-järjestelmässä:*
KUVA
Siis

$$\begin{aligned} 4457 &= 2 + 11 \cdot 405 = 2 + 11 \cdot (9 + 11 \cdot 36) \\ &= 2 + 9 \cdot 11 + 11^2(3 + 3 \cdot 11) = 2 + 9 \cdot 11 + 3 \cdot 11^2 + 3 \cdot 11^3 \\ &= (3392)_{11}. \end{aligned}$$

Esimerkki 12.2.4. *Yhteen- ja kertolasku:*

$$\begin{aligned} (23)_4 + (131)_4 &= (2 \cdot 4 + 3) + (1 \cdot 4^2 + 3 \cdot 4 + 1) = 11 + 29 = 40) \\ &= 2 \cdot 4^2 + 2 \cdot 4 + 0 \\ &= (220)_4; \end{aligned}$$

$$(23)_4 \cdot (131)_4 = 11 \cdot 29 = 319 = (10333)_4$$

Toisin: 4*-järjestelmässä on*

$1+1=2$	$1\cdot 1=1$
$1+2=3$	$1\cdot 2=2$
$1+3=10$	$1\cdot 3=3$
$2+2=10$	$2\cdot 2=10$
$2+3=11$	$2\cdot 3=12$
$3+3=12$	$3\cdot 3=21$

Täten

$$\begin{array}{r} (23)_4 \\ (131)_4 \\ \hline (220)_4 \end{array} \qquad \begin{array}{r} (131)_4 \\ (23)_4 \\ \hline 1113 \\ 322 \\ \hline (10333)_4 \end{array}$$

12.3 Jaollisuus ja Eukleideen algoritmi

Tarkastelemme ensin jaollisuuden määritelmää ja alkulukua.

Määritelmä 12.3.1. *Kokonaisluku* a sisältyy *kokonaislukuun* b *(merk.* $a|b$*) eli* b *on jaollinen* a*:lla, jos on olemassa sellainen kokonaisluku* k*, että* $b = k\cdot a$*. Muulloin* a *ei sisälly* b*:hen.*

Esim. $5|10$, koska $10 = 2\cdot 5$; 3 ei sisälly 10:een, koska ei ole sellaista kokonaislukua k, että $10 = k\cdot 3$.
Luku 0 sisältyy vain itseensä. Tällöin k:ksi kelpaa mikä kokonaisluku tahansa. Muulloin k on yksikäsitteisesti määrätty.

$\underline{a|b:}$ a jakaa b:n
a on b:n tekijä
b on a:n monikerta
b sisältää a:n tekijänä

Lause 12.3.2. *(1)* $a|0, \pm a|0, \pm 1|a$*;*

(2) $a|b, b|c \Rightarrow a|c$*;*

(3) $a|b \Rightarrow a|mb$*;*

(4) $a|b_1, \ldots, a|b_n \Rightarrow a|b_1 + \ldots b_n$*;*

(5) $a|b_1, \ldots, a|b_{n-1}$ *mutta ei* $a|b_n \Rightarrow$ *ei* $a|b_1 + \ldots b_n$*.*

Määritelmä 12.3.3. *Luonnollista lukua* $p > 1$ *sanotaan* alkuluvuksi*, jos se on jaollinen vain* ± 1*:llä ja* $\pm p$*:llä. Muussa tapauksessa* p *on* yhdistetty.

Huom. Luku 1 ei ole alkuluku eikä yhdistetty. Luku 2 on ainoa parillinen alkuluku. Jokainen yhdistetty luku (> 1) voidaan esittää alkulukujen tulona, sillä jos a on yhdistetty, niin $a = b\cdot c$, $1 < b < a$, $1 < c < a$. Jos b ja c ovat alkulukuja, on asia selvä. Muussa tapauksessa esim. $b = d\cdot e$, $1 < d < b$, $1 < e < b$. Menettely voidaan toistaa vain äärellisen monta kertaa, koska tekijät pienenevät, mutta ovat 1:tä suurempia.

Lause 12.3.4. *(Eukleideen lause). Alkulukuja äärettömän monta.*

Lause 12.3.5. *(Diricklet'n lause, kun $a = 3$ ja $b = 2$). Muotoa $3n + 2$ olevia alkulukuja on äärettömän monta.*

Eratostheneen seula on menettely, jolla voidaan määrittää annettua lukua N pienemmät alkuluvut.
Olkoon a mielivaltainen luonnollinen luku toteuttaen ehdon $a \leq N$. Jos a on yhdistetty, sillä on alkutekijä $\leq \sqrt{a} \leq \sqrt{N}$. Kirjoitetaan luvut $1, 2, 3, \ldots, N$ jonoon ja pyyhitään poi kaikkien $\sqrt{N}$:ää pienempien alkulukujen monikerrat.
Esim. $N = 48$, $\sqrt{N} < 7 \Rightarrow$ alkuluvut 2, 3 ja 5.

1	$\underline{2}$	$\underline{3}$	4	$\underline{5}$	6	$\underline{7}$	8	9	10	$\underline{11}$	12
$\underline{13}$	14	15	16	$\underline{17}$	18	$\underline{19}$	20	21	22	$\underline{23}$	24
25	26	27	28	$\underline{29}$	30	$\underline{31}$	32	33	34	35	36
$\underline{37}$	38	39	40	$\underline{41}$	42	$\underline{43}$	44	45	46	$\underline{47}$	48

Suurin yhteinen tekijä (syt)
Tarkastellaan lukuja a ja b, jotka molemmat eivät ole nollia.

Määritelmä 12.3.6. *Lukujen a ja b* suurin yhteinen tekijä $syt(a, b)$ *on a:n ja b:n sellainen yhteinen tekijä, joka on positiivinen ja jaollinen kaikilla näiden lukujen yhteisillä tekijöillä. Täten $d = syt(a, b)$, jos*

(1) $d > 0$,

(2) $d|a$ *ja* $d|b$,

(3) $k|a$ *ja* $k|b \Rightarrow k|d$.

Vastaavasti määritellään lukujen $a_1, \ldots, a_n$ suurin yhteinen tekijä $syt(a_1, \ldots, a_n)$.

Käytännössä syt voidaan määrittää (a) etsimällä lukujen a ja b yhteiset tekijät ja valitsemalla niistä suurin, (b) jakamalla luvut alkutekijöihin, esim.

$$\left.\begin{array}{l} 4 = 2 \cdot 2 \\ 12 = 2 \cdot 2 \cdot 3 \end{array}\right\} \Rightarrow syt(4, 12) = 2 \cdot 2 = 4$$

tai (c) jakoalgoritmilla, kuten Eukleideen algoritmilla.
Eukleideen algoritmi

Lause 12.3.7. *Kokonaislukujen a ja b ($b \neq 0$) syt voidaan määrittää seuraavalla* Eukleideen algoritmilla*:*

$$\begin{aligned}
a &= q_1 b + r_1, && 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Tällöin $syt(a, b) = r_n$.

Eukleideen algoritmin muodostaa ketju peräkkäisiä jakolaskuja, joissa jaettavana on edellinen jakaja ja jakajana edellinen jakojäännös. Ketju päättyy, koska jakojäännökset r_i muodostavat alenevan ei-negatiivisten kokonaislukujen jonon:

$$|b| > r_1 > r_2 > r_3 > \ldots > r_n > 0 > r_{n+1} = 0.$$

Lause 12.3.8. *Jos a ja b eivät molemmat ole nollia, niin $syt(a, b)$ on aina olemassa ja on yksikäsitteinen.*

Syt:n perusominaisuuksia
Syt:n määritelmä $\Rightarrow syt(a, b, c) = syt(syt(a, b), c)$. Yleisesti pätee

$$syt(a_1, \ldots, a_k, a_{k+1}) = syt(syt(a_1, \ldots, a_k), a_{k+1}). \tag{12.2}$$

Lause 12.3.9. *Jos $syt(x_1, \ldots, a_s) = d$, on olemassa sellaiset luvut $x_1, \ldots, x_s$, että*

$$x_1 x_1 + \ldots + x_s a_s = d.$$

Lause 12.3.10. *Diofantoksen yhtälöllä*

$$ax + by = c$$

on ratkaisu, joss $d|c$, missä $d = syt(a, b)$.

Geometrisesti lause voidaan tulkita siten, että suora $ax + by = c$ kulkee ainakin yhden xy-tason verkkopisteen (kokonaislukupisteen) kautta, mikäli $d|c$, $d = syt(a, b)$. Koska suoran kulmakerroin on rationaaliluku, kulkee suora itse asiassa äärettömän monen verkkopisteen kautta.

12.4 Kongruenssi

Ekvivalenssirelaatio
Jos a ja b ovat kokonaislukuja, niin joko $a = b$ tai $a \neq b$. Tämä relaatio '$\neq$' joko vallitsee tai ei vallitse esim. kahden mielivaltaisen kokonaisluvun välillä. Tällä relaatiolla on mm. seuraavat ominaisuudet:

(1) jokainen $a = a$;

(2) $a = b \Rightarrow b = a$;

(3) $a = b, b = c \Rightarrow a = c$.

Määritelmä 12.4.1. *Jos joukon A kahden mielivaltaisen alkion a ja b välillä joko vallitsee relaatio $\sim$ (ts. $a \sim b$) tai ei vallitse, ja jos tämä relaatio on*

(i) refleksiivinen A:ssa, ts. $\forall a \in A : a \sim a$,

(ii) symmetrinen A:ssa, ts. $\forall a, b \in A : a \sim b \Rightarrow b \sim a$,

(iii) transitiivinen A:ssa, ts. $\forall a, b, c \in A : a \sim b, b \sim c \Rightarrow a \sim c$,

niin $\sim$ on ekvivalenssirelaatio A:ssa.

Ekvivalenssirelaatioita: '$=$', kolmioiden yhdenmuotoisuus, suorien yhdensuuntaisuus, asuminen samassa talossa, opiskella samaa pääainetta jne.
Esim. kokonaislukujen jaollisuusrelaatio ei ole ekvivalenssirelaatio, koska se ei ole symmetrinen.

Kongruenssin määritelmä ja perusominaisuudet

Määritelmä 12.4.2. *Jos $m|a-b$, sanomme, että a* on kongruentti b:n kanssa modulo m, *ja merkitsemme*

$$a \equiv b (\mathrm{mod}\, m).$$

Jos taas m ei sisälly $(a-b)$:hen, sanomme, että a on epäkongruentti b:n kanssa modulo m, *merk.* $a \pm b (\mathrm{mod}\, m)$. *Luku m on* moduli.

Jos $N = qm + r$, niin $m|N-r$ eli $N \equiv r (\mathrm{mod}\, m)$. Jos $m|N$, niin $N \equiv 0 (\mathrm{mod}\, m)$ ja kääntäen.
Esim.

(1) $627 \equiv 427 (\mathrm{mod}\, 10)$, koska $10|627-427$.

(2) $31 \equiv -9 (\mathrm{mod}\, 10)$, koska $10|31+9$.

(3) $7 \pm 5 (\mathrm{mod}\, 10)$, koska 10 ei sisälly lukuun $7-5$.
$7 \equiv 5 (\mathrm{mod}\, 2)$. Yleensä parittomat luvut ovat keskenään kongruentteja $\mathrm{mod}\, 2$.

(4) $a \equiv b (\mathrm{mod}\, 1)$ on voimassa jokaisella a:lla ja b:llä.

Lause 12.4.3. *Kongruenssi on ekvivalenssirelaatio, ts, (i)* $a \equiv a (\mathrm{mod}\, m)$, *(ii)* $a \equiv b (\mathrm{mod}\, m) \Rightarrow$ $b \equiv a (\mathrm{mod}\, m)$ *ja (iii)* $a \equiv b (\mathrm{mod}\, m), b \equiv c (\mathrm{mod}\, m) \Rightarrow a \equiv c (\mathrm{mod}\, m)$.

Lause 12.4.4. *Kongruenssille on voimassa*

$$a \equiv b (\mathrm{mod}\, m), c \equiv d (\mathrm{mod}\, m) \Rightarrow a \pm c \equiv b \pm d (\mathrm{mod}\, m); \tag{12.3}$$

$$a_i \equiv b_i (\mathrm{mod}\, m), (i = 1, \ldots, n) \Rightarrow \sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i (\mathrm{mod}\, m); \tag{12.4}$$

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow ac \equiv bc (\mathrm{mod}\, m); \tag{12.5}$$

$$a \equiv b (\mathrm{mod}\, m), c \equiv d (\mathrm{mod}\, m) \Rightarrow ac \equiv bd (\mathrm{mod}\, m); \tag{12.6}$$

$$a_i \equiv b_i (\mathrm{mod}\, m), (i = 1, \ldots, n) \Rightarrow \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i (\mathrm{mod}\, m); \tag{12.7}$$

$$a \equiv b (\mathrm{mod}\, m), n \in \mathbb{N} \Rightarrow a^n \equiv b^n (\mathrm{mod}\, m); \tag{12.8}$$

$$a \equiv b (\mathrm{mod}\, m), P(x) = a_n x^n + \ldots + a_1 x + a_0 \text{ } (a_i\text{:t kokonaislukuja}) \tag{12.9}$$

$$\Rightarrow a \equiv P(b) (\mathrm{mod}\, m). \tag{12.10}$$

Esimerkki 12.4.5. *Mikä on jäännös, kun luku*

$$N = 18^2 \cdot 13^6 + 20^4 \cdot 10^7$$

jaetaan 11*:llä, ts. mikä on* x*, kun* $N \equiv x(\mathrm{mod}\, 11)$*?*
Ratkaisu: $18 \equiv -4(\mathrm{mod}\, 11) \Rightarrow 18^2 \equiv (-4)^2 = 16(\mathrm{mod}\, 11), 16 \equiv 5(\mathrm{mod}\, 11)$*;*
$13 \equiv 2(\mathrm{mod}\, 11) \Rightarrow 13^2 \equiv 8 \equiv -3(\mathrm{mod}\, 11), 13^6 \equiv (-4)^2 \equiv -2(\mathrm{mod}\, 11)$*;*
$20 \equiv -2(\mathrm{mod}\, 11) \Rightarrow 20^4 \equiv (-2)^4 \equiv 5(\mathrm{mod}\, 11)$*;*
$10 \equiv -1(\mathrm{mod}\, 11) \Rightarrow 10^7 \equiv (-1)^7(\mathrm{mod}\, 11)$.
Siis $N \equiv 5 \cdot (-2) + 5 \cdot (-1) \equiv -4(\mathrm{mod}\, 11)$*. Jäännös on siis* 7*.*

Kongruenssin jakaminen luvulla

Lause 12.4.6. *Kun* $a, b, c \in \mathbb{Z}$*, niin*

$$ac \equiv bc(\mathrm{mod}\, m), syt(c, m) = 1 \Rightarrow a \equiv b(\mathrm{mod}\, m). \tag{12.11}$$

Huom. Ehto $syt(c, m) = 1$ on välttämätön, sillä esim. $22 \equiv 16(\mathrm{mod}\, 6)$, mutta $11 \pm 8(\mathrm{mod}\, 6)$.
Todistus. $m|ac - bc \Rightarrow m|c(a - b) \Rightarrow^{syt(m,c)=1} m|a - b$ eli $a \equiv b(\mathrm{mod}\, m)$. ■

Lause 12.4.7. $a, b, c \in \mathbb{Z} \Rightarrow$

$$ac \equiv bc(\mathrm{mod}\, m) \Rightarrow a \equiv b \left(\mathrm{mod}\, \frac{m}{syt(c, m)}\right). \tag{12.12}$$

Todistus. $m|ac - bc \Rightarrow m|c(a - b)$. Merk. $syt(c, m) = d, m = k_1 d, c = k_2 d$. Tällöin on $syt(k_1, k_2) = 1$. Edelleen saadaan

$$k_1 d|k_2 d(a - b) \Rightarrow k_1|k_2(a - b) \Rightarrow^{syt(k_1,k_2)=1} k_1|(a - b) \Rightarrow a \equiv b(\mathrm{mod}\, k_1)$$
$$\Rightarrow a \equiv b \left(\mathrm{mod}\, \frac{m}{d}\right) \Rightarrow a \equiv b \left(\mathrm{mod}\, \frac{m}{syt(c, m)}\right).$$

■

Jäännösluokat
Jokainen luku a voidaan esittää muodossa

$$a = qm + r,$$

missä r on jokin luvuista $0, 1, 2, \ldots, m - 1$. Luku r on ns. *a:n pienin ei-negatiivinen jäännös (mod* m*).*
Kaikki kokonaisluvut jakautuvat luokkiin sen mukaan, kuinka suuri tämä jäännös on (⇒ jäännösluokat (mod m)).
Merkitään esim. <0> ⇔ jäännös 0, <1> ⇔ jäännös 1, ..., <$m-1$> ⇔ jäännös $m-1$. Erityisesti on <r> on a:n määräämä jäännösluokka (mod m).

Esimerkki 12.4.8. *Kun* $m = 4$*, saadaan jäännösluokat*

$$\begin{aligned} <0> &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\ <1> &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\ <2> &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\ <3> &= \{\ldots, -5, -1, 3, 7, 11, \ldots\} \end{aligned}$$

Yleisesti on

$$<r>\{a_i \,|\, a_i \equiv r(\mathrm{mod}\, m)\}.$$

Viitteet

[1] K. Appel ja W. Haken: The solution of the Four-Color-Map Problem. Scientific American, vol. 237, 1976)

[2] Bavel, Z.: Math companion for computer science. – Reston Publishing Company, Reston, 1982.

[3] R. Haggarty, *Discrete Mathematics for Computing*. – Addison-Wesley, Pearson Education Limited, 2002.

[4] Harary, F. (toim.): New directions in the theory of graphs. – Academic Press, New York - London, 1973.

[5] R. Johnsonbaugh, *Discrete Mathematics*. – Prentice Hall, 4. painos, 2001.

[6] Levy, L.S.: Discrete structures of computer science. – John Wiley & Sons, New York, 1980.

[7] J. K. Mattila, *Sumean logiikan oppikirja. Johdatus sumean matematiikkaan*. – Art House, 3. painos, 2002.

[8] McEliece, R.J., Ash, R.B. ja C. Ash: Introduction to discrete mathematics. – McGraw-Hill, Singapore, 1989.

[9] T. Metsänkylä, M. Näätänen, *Algebra*. – Limes ry., 2003.

[10] C. V. Negoita, D. A. Ralescu, *Applications of Fuzzy Sets to Systems Analysis*. – Birkhäuser, 1975.

[11] V. Rantala, A. Virtanen, *LOGIIKKAA. Teoriaa ja sovelluksia*. – Tampereen yliopisto, Matemaattisten tieteiden laitos, 1995.

[12] Savolainen, V.: Verkkoteorian perusteet ja algoritmit. – Gaudeamus, Vaasa, 1978.

[13] Savolainen, V.: Verkkoteoria. – Docendo Finland Oy, Jyväskylä, 2001.

[14] C. Schumacher, *Chapter Zero. Fundamental Notions of Abstract Mathematics*. – Addison-Wesley, 2. painos, 2001

[15] Skiena, S.S: Implementing discrete mathematics: Combinatorics and graph theory with *Mathematica.* – Addison-Wesley, Redwood City, 1990.
Mathematica-ohjelmapaketti `Combinatorica.m`

[16] Tucker, A.: Applied combinatorics. – John Wiley & Sons, New York, 1984.

[17] Wiitala, S.A.: Discrete mathematics - a unified approach. – McGraw-Hill, Singapore, 1987.

[18] Wilson, R.J.: Introduction to graph theory. – Longman, Whitstable, 1975.

[19] L. A. Zadeh, Fuzzy sets, *Information and Control*, 8, 1965.