DISKREETTI MATEMATIIKKA

Martti E. Pesonen

Versio 24. syyskuuta 2010

LUKIJALLE

Nimitys ”Diskreetti matematiikka” on merkitykseltään hyvin epämääräinen. Sillä ei ole mitään standardia, yleisesti sovittua sisältöä eikä selkeää ”ulkomuotoa”, eikä se ole matematiikan haara siinä mielessä kuin algebra, analyysi tai todennäköisyyslaskenta. Diskreetti matematiikka onkin yleisnimike äärellisten tai numeroituvien - tai niiksi yksinkertaistettujen, diskretoitujen - ilmiöiden käsittelyyn. Yleensä diskreetin matematiikan kurssi sisältää logiikan ja joukko-opin alkeiden ohella lukujoukkojen, relaatioiden ja funktioiden käsittelyä, kombinatoriikkaa ja muita lukumääräongelmia sekä joitain seuraavista: algebra, lukuteoria, hilateoria, automaattien teoria, verkko- eli graafiteoria, todennäköisyyslaskenta, generoivat funktiot, rekursiokaavat (tai differenssiyhtälöt). Tietotekniikan esiinmarssi on luonut tarpeen diskreetin matematiikan laajemmalle opiskelulle, tietokonehan toimii diskreetisti, mutta toisaalta se on myös mahdollistanut diskreettien systeemien helpomman käsittelyn myös opetuksessa.

Luentomoniste ”Diskreetti matematiikka” sisältää Joensuun yliopiston matematiikan laitoksen samannimisen kurssin ”teoreettisen” oppiaineksen. Sen lisäksi kurssilla on monisteen sisältöön perustuvia kotitehtäviä ja tietokoneharjoituksia.

Kurssiin liittyy jonkin verran yksinkertaista ohjelmointia, lähinnä Matlab- tai Maple-ympäristöissä. Tämän tarkoitus on antaa opiskelijalle, paitsi valmiuksia relaatioiden, verkkojen, lukumääräongelmien ja rekursiokaavojen käsittelyyn, myös harjaannusta tietotekniikan käyttöön äärellisen matematiikan ongelmien ratkaisemisessa.

Joensuussa 24. syyskuuta 2010

Martti E. Pesonen

Sisältö

1 JOHDANTO

Luomme kertauksenomaisen katsauksen joukko-oppiin ja palautamme mieliin induktiotodistusmenetelmän.

1.1 Pikakatsaus joukko-oppiin

Diskreetissä matematiikassa on aivan välttämätöntä käyttää työskentelyraamina joukko-oppia. Tässä oppimateriaalissa joukkokäsitettä ei pohdita kovin syvällisesti vaan tyydytään käytännölliseen, ns. intuitiiviseen (”naiiviin”) joukkokäsitteeseen ja tutustutaan joukkoalgebraan, jonka vastine löytyy lauselogiikasta (Luku 2). Joukon käsitettä sinänsä kuvataan hieman tarkemmin Luvussa 3.

Joukko

Otamme siis käyttöön käsitteet alkio ja joukko: *joukko* on kokoelma olioita, joita kutsumme *alkioiksi*. Samalla sovimme ristiriitojen välttämiseksi hierarkian; *joukko ei saa olla itsensä alkio.* Kuitenkin joukon alkioina saa olla muita joukkoja.

Tyhjää joukkoa eli joukkoa, jossa ei ole yhtään alkiota, merkitään symbolilla $\emptyset$.

Perusjoukko on, kustakin tilanteesta riippuen, laajin tarkasteltava alkiokokonaisuus. Perusjoukkoja voi olla yhtaikaa käytössä useita. Niitä merkitään tässä esityksessä lihavoiduilla symboleilla.

Olkoon $\mathbf{X}$ perusjoukko, A, B, A_i sen osajoukkoja, n positiivinen kokonaisluku ja I epätyhjä joukko, nk. *indeksijoukko*. Käytämme mm. seuraavia joukko-opin merkintöjä:

$x \in A$	joukon alkio
$x \notin A$	ei joukon alkio
$A = B$	joukoissa samat alkiot
$A \subseteq B$	osajoukko
$A \subset B$	aito osajoukko
$A \cup B$, $\cup_{i=1}^{n} A_i$, $\cup_{i=1}^{\infty} A_i$, $\cup_{i \in I} A_i$	joukkojen yhdisteitä
$A \cap B$, $\cap_{i=1}^{n} A_i$, $\cap_{i=1}^{\infty} A_i$, $\cap_{i \in I} A_i$	joukkojen leikkauksia
$\mathbf{X} \setminus A = \overline{A}$	komplementti
$A \setminus B = A \cap \overline{B}$	erotus

Tutuille lukujoukoille käytämme seuraavia merkintöjä:

$\mathbb{N} = \{1, 2, 3, \ldots\}$	luonnolliset luvut
$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$	perusluvut
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots\}$	kokonaisluvut
$\mathbb{Q} = \left\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\right\}$	rationaaliluvut
$\mathbb{R}$	reaaliluvut
$\mathbb{C}$	kompleksiluvut
A_+	joukon A (aidosti) positiivinen osa.

Äärellisen *lukumääräjoukon* määrittelemme seuraavasti:

$$[n] := \begin{cases} \emptyset, & \text{jos } n = 0, \\ \{1, 2, 3, \ldots, n\} & \text{muutoin} \end{cases}$$

Reaalilukujoukko ja sen osajoukot on järjestetty relaation '$\leq$' suhteen. Lisäksi joukot sisältyvät joukko-opillisesti toisiinsa seuraavalla tavalla:

$$\emptyset \subseteq [n] \subset \mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Joukkoalgebraa

Esitetään jo tässä vaiheessa kooste joukko-opin peruskaavoista, joista osa johdetaan tai muuten perustellaan Luvussa 3 tai harjoitustehtävissä. Symboli $\Leftrightarrow$ tarkoittaa "jos ja vain jos". eli "on yhtäpitävää, ekvivalenttia".

Lause 1.1.1 Olkoon $\mathbf{X}$ perusjoukko ja A, B, $C \subseteq \mathbf{X}$. Tällöin on

1)	$A \cap A = A \cup A = A$	idempotenttisuuslait
2)	$A \cap B = B \cap A$	vaihdannaisuus
3)	$A \cap (B \cap C) = (A \cap B) \cap C$	liitännäisyyslait
	$A \cup (B \cup C) = (A \cup B) \cup C$	
4)	$A \cap (A \cup B) = A \cup (A \cap B) = A$	absorptiolait
5)	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	osittelulait
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
6)	$A \cap \overline{A} = \emptyset$	komplementtilait
	$A \cup \overline{A} = \mathbf{X}$	
7)	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	de Morganin lait
	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	
8)	$A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A \subseteq B$	
9)	$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$.	

1.2 Täydellisen induktion periaate ja induktiotodistus

Diskreetin matematiikan keskeinen todistusmenetelmä, *induktiotodistus*, perustuu ns. *täydellisen induktion* eli *matemaattisen induktion periaatteeseen*, jonka taustalla on seuraava kokonaislukuja koskeva (ehkäpä algebrassa todistettava, mutta Peanon aksioomiinkin sisältyvä, ks. Matematiikan johdantokurssi) ominaisuus:

Jos joukko $S \subseteq \mathbb{N}$ toteuttaa ehdot:
1) S sisältää luvun 1,
2) jos $n \in S$, niin myös $n + 1 \in S$,
niin $S = \mathbb{N}$.

Myös seuraava – ilmeiseltä tuntuva – kokonaislukujen joukon ominaisuus kannattaa mainita eksplisiittisesti (vrt. minimaaliset alkiot Luvussa 8):

> Jokaisessa epätyhjässä alhaalta rajoitetussa kokonaislukujen joukon osajoukossa on pienin alkio. Erityisesti: jokaisessa epätyhjässä luonnollisten lukujen joukon osajoukossa on pienin alkio.

Lause 1.2.1 (induktioperiaate) Olkoon lausefunktio $P(n)$ luonnollisia lukuja n koskeva väite. Jos

1°) $P(1)$ on tosi, ja
2°) siitä, että $P(k)$ on tosi jollakin arvolla $k \geq 1$ seuraa, että $P(k+1)$ on tosi,

niin ominaisuus $P(n)$ on tosi kaikille luonnollisille luvuille $n \in \mathbb{N}$.

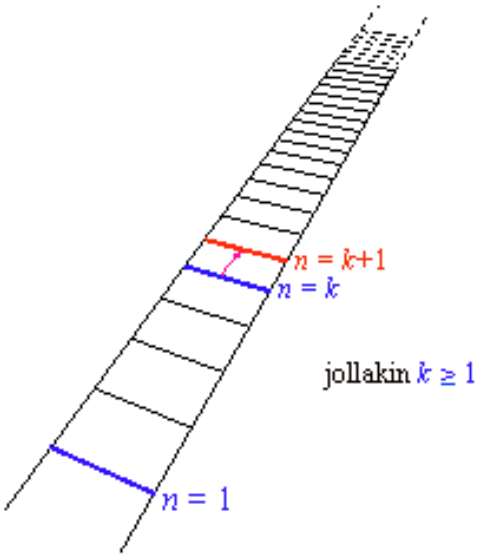
Kohta 2° jaetaan usein selvyyden vuoksi kahteen osaan I2) ja I3), jolloin **induktiotodistus koostuu kolmesta osasta**:

I1) $n = 1$: Osoitetaan $P(1)$ todeksi tavalla tai toisella.
I2) $n = k$: Tehdään *induktio-oletus*, jossa ilmaistaan, mitä "$P(k)$ on tosi jollakin arvolla $k \geq 1$" tarkoittaa ja oletetaan se todeksi.
I3) $n = k + 1$: *Induktioaskel* tai *induktioväite*, jossa todistetaan induktio-oletusta käyttäen "$P(k+1)$ on tosi".
Sanomme, että *väite on todistettu induktiolla lukujen $n \in \mathbb{N}$ suhteen*.

Induktiotodistus toimii seuraavasti (tietokoneohjelmasilmukan tapaan): Kohdassa I1) väite todistetaan suoraan pienimmällä väitetyllä arvolla $n = 1$. Induktio-oletus I2) on silloin laillinen, koska väite on tosi ainakin arvolla $k = 1$. Kohdassa I3) väite todistuu arvolle $n = 2$, joten se on voimassa arvoilla $n = 1$ ja $n = 2$.
Palataan kohtaan I2): edellisestä tiedetään väitteen olevan totta myös arvolla arvolla $k = 2$, joten I3) todistaa sen todeksi arvolla $k = 3$, jne, väite generoituu todeksi jokaiselle $n \in \mathbb{N}$, kunhan silmukka käydään läpi riittävän monta kertaa.

Induktiotodistuksen toimintaa voidaan havainnollistaa äärettömiin johtavilla tikapuilla (ks. Kuva 1): jotta voi kiivetä haluamalleen puolalle asti riittää:

1) että pääsee tavalla tai toisella ensimmäiselle puolalle ($n = 1$),
2) jos on päässyt jollekin puolalle, pystyy nousemaan yhtä ylemmäs ($P(k) =$ tosi $\Rightarrow P(k+1) =$ tosi).



Kuva 1: Induktioperiaatteen havainnollistus tikkaiden kiipeämisellä

Esimerkki 1.2.2 Palautetaan mieleen luvun n kertoma $n!$: aluksi sovitaan $0! := 1$ ja sitten $n! := 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n$.

Osoita, että $n^n \geq n!$ kaikilla $n \in \mathbb{N}$.

Todistus. I1) $n = 1$: $1^1 = 1 = 1!$ on tosi.

I2) $n = k$: Induktio-oletus: Oletetaan, että $k^k \geq k!$ jollakin $k \geq 1$.

I3) $n = k+1$: Induktioväite: $(k+1)^{k+1} \geq (k+1)!$.

Induktioväitteen todistus. Koska selvästikin $(k+1)^k \geq k^k$, saadaan

$$(k+1)^{k+1} = (k+1)(k+1)^k \geq (k+1)k^k.$$

Induktio-oletusta käyttäen edelleen $(k+1)k^k \geq (k+1)k! = (k+1)!$.

Siis induktioväite on tosi. Tällöin induktioperiaatteesta seuraa, että myös alkuperäinen väite on tosi kaikilla $n \in \mathbb{N}$. ■

Esimerkki 1.2.3 Osoita, että kaikilla $n \in \mathbb{N}$

$$2(1 + 2 + \cdots + n) = n(n + 1).$$

Todistus. I1) $n = 1$: Havaitaan heti, että kaava pitää paikkansa arvolla 1.
I2) $n = k$: Oletetaan, että kaava pitää paikkansa arvolla $k \geq 1$, ts.

$$2(1 + 2 + \cdots + k) = k(k + 1).$$

I3) $n = k+1$: Arvolla $k + 1$:

$$\begin{aligned} 2\big(1 + 2 + \cdots + k + (k + 1)\big) &= 2(1 + 2 + \cdots + k) + 2(k + 1) \\ &= k(k + 1) + 2(k + 1) \\ &= (k + 1)\big((k + 1) + 1\big). \end{aligned}$$

Kaava pitää siis paikkansa myös arvolla $k+1$, jos se pitää paikkansa arvolla $k \geq 1$. Täydellisen induktion periaatteen nojalla väite on tosi kaikilla $n \in \mathbb{N}$. ■

Esimerkki 1.2.4 Osoita, että kaikilla $n \in \mathbb{N}$

$$(1 + 2 + \cdots + n)^2 = 1^3 + 2^3 + \cdots + n^3.$$

Todistus. I1) $n = 1$: $1^2 = 1 = 1^3$, joten kaava pitää paikkansa arvolla 1.
I2) $n = k$: Oletetaan, että kaava pitää paikkansa arvolla $k \geq 1$, ts.

$$(1 + 2 + \cdots + k)^2 = 1^3 + 2^3 + \cdots + k^3.$$

I3) $n = k+1$: Arvolla $k + 1$ saadaan vasen puoli induktio-oletuksen ja Esimerkin 1.2.3 tuloksen nojalla muotoon

$$\begin{aligned} \big(1 + 2 + \cdots + k + (k + 1)\big)^2 &= \big((1 + 2 + \cdots + k) + (k + 1)\big)^2 \\ &= (1 + 2 + \cdots + k)^2 + 2(1 + 2 + \cdots + k)(k + 1) + (k + 1)^2 \\ &= (1^3 + 2^3 + \cdots + k^3) + k(k + 1)^2 + (k + 1)^2 \\ &= 1^3 + 2^3 + \cdots + k^3 + (k + 1)^3. \end{aligned}$$

Induktioaskel on todistettu, joten induktioperiaatteen ja kohtien I1-3) perusteella väite on tosi kaikilla $n \in \mathbb{N}$. ■

Tehtävä 1.2.5 Osoita, että kaikilla $n \in \mathbb{N}$ on luku $\frac{1}{6}(n^3 + 5n)$ kokonaisluku.
Vihje: esitys $n^3 + 5n = 6p$.

Tehtävä 1.2.6 Todista, että kaikilla $n \in \mathbb{N}$ on $2! \cdot 4! \cdot 6! \cdots (2n)! \geq \big((n + 1)!\big)^n$.

Esimerkki 1.2.7 Määritellään 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

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

Keksitään **väite**: $S_n = n^2$ kaikille $n \in \mathbb{N}$. Todistetaan tämä käyttäen matemaattista induktiota.

Todistus. I1) $n = 1$: Vasen puoli $S_1 = 1$, oikea puoli $1^2 = 1$. Siis väite on tosi arvolla $n = 1$.
I2) $n = k$: Induktio-oletus: $S_k = k^2$ jollakin $k \geq 1$.
I3) $n = k+1$: Induktioväite: $S_{k+1} = (k+1)^2$.

Induktioväitteen todistus käyttäen induktio-oletusta

$$S_{k+1} = \sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1)+(2(k+1)-1) = S_k+2k+1 = k^2+2k+1 = (k+1)^2.$$ ■

Siis induktioväite on tosi. Tällöin induktioperiaatteesta seuraa, että myös alkuperäinen väite $S_n = n^2$ kaikille $n \in \mathbb{N}$ on todistettu. ■

Edellä pienin arvo, jolla väitettä todistetaan, oli $n = 1$. Todistusperiaate kelpaa kuitenkin mille tahansa alhaalta rajoitetulle peräkkäisten kokonaislukujen joukolle $\{p, p+1, p+2, p+3, \ldots\}$, kunhan väite todistetaan erikseen sen pienimmällä arvolla $n = p$ ja induktio-oletus siirretään muotoon "$P(k)$ on tosi jollakin arvolla $k \geq p$". Tämän jälkeen todistetaan tätä induktio-oletusta käyttäen, että "$P(k+1)$ on tosi". Tämä muunnosmahdollisuus johtuu tietysti siitä, kokonaislukuja $m \geq p$ koskeva väite voitaisiin helposti muuntaa koskemaan lukuja $n \geq 1$ muunnoksella $n = m - p + 1$.

Tehtävä 1.2.8 Osoita, että kaikilla $n \in \mathbb{Z}$ on luku $\frac{1}{6}(n^3+5n)$ kokonaisluku.

Vihje: Tehtävässä 1.2.5 lienee osoitettu jo, että väite pätee luonnollisilla luvuilla $n \in \mathbb{N}$. Nolla ja negatiiviset luvut saadaan käsitellyiksi muuttujanvaihdolla $n \mapsto -n$, siis: Osoita, että kaikilla $n \geq 0$ on $\frac{1}{6}((-n)^3+5(-n))$ kokonaisluku.

Esimerkki 1.2.9 Varmistu, että on olemassa $n_0 \in \mathbb{N}$ niin, että $2^n < n!$ kaikilla $n \geq n_0$. Etsi mahdollisimman pieni n_0 ja todista väite sille induktiolla.

Todistus. Tutkitaan arvoja alusta lähtien:

$n = 1$: onko $2^1 < 1!$? Ei ole tosi, onhan $2 > 1$.

$n = 2$: onko $2^2 < 2!$? Ei ole tosi, sillä $4 > 2$.

$n = 3$: onko $2^3 < 3!$? Ei ole tosi, sillä $8 > 6$.

$n = 4$: onko $2^4 < 4!$? On tosi, sillä $16 < 24$. Ja tästähän repeää, ehkä: valitaan $n_0 := 4$.

Induktiotodistus. I1) Perusaskelma $n = 4$: Jo edellä, totta.
I2) $n = k$ (induktio-oletus): Oletetaan, että $2^k < k!$ jollakin kokonaisluvulla $k \geq 4$.
I3) $n = k+1$ (induktioaskel): Todistetaan väitteen pitävän paikkansa arvolla $k+1$. Mutta induktio-oletuksen mukaan saadaan heti $2^{k+1} = 2 \cdot 2^k < 2 \cdot k!$.

Koska $k \geq 4$, on $2 < k + 1$ ja siten $2^{k+1} < 2 \cdot k! < (k + 1)k! = (k + 1)!$.

Kohtien I1-3) myötä induktiotodistus on valmis; induktioperiaatteen nojalla $2^n < n!$ kaikilla $n \geq 4$, ja 4 on pienin kelvollinen alaraja. ■

Induktiotodistusta voidaan käyttää myös seuraavana variaationa: Olkoon $q \in \mathbb{Z}$ jokin luku ja $P(n)$ lukuja $n \geq q$ koskeva väite.
I1) $n = q$: Osoitetaan $P(q)$ todeksi tavalla tai toisella.
I2') $n = k$: Tehdään induktio-oletus muodossa: "jollakin $k \geq q$ on $P(m)$ tosi kaikilla arvoilla $q \leq m \leq k$".
I3) $n = k+1$: Induktioaskel: Todistetaan induktio-oletusta käyttäen "$P(k+1)$ on tosi". Tällöin väite on tosi kaikilla $n \in \mathbb{N}$, $n \geq q$.

Tätä versiota käytetään mm. lukuteoriassa ja verkkoteoriassa. Joskus tulee tilanteita, joissa induktio-oletus arvolla k sallii tilanteen palauttamisen arvosta $k + 1$ alemmalle tasolle, mutta ei tarkalleen tasolle k vaan esimerkiksi sitä pienempiin lukuihin tai joukkoihin, ks. esimerkiksi Lause 12.8.4.

Esimerkki 1.2.10 Luonnollinen luku $p \geq 2$ on *alkuluku*, jos se ei ole jaollinen muilla luonnollisilla luvuilla kuin ykkösellä ja itsellään, ts. jos luvulla on esitys luonnollisten lukujen tulona $p = ab$, niin $\{a, b\} = \{1, p\}$. Pienimpiä alkulukuja ovat 2, 3, 5, 7, 11, 13, 17, jne. Muut luonnolliset luvut ovat *yhdistettyjä lukuja*.

Todista, että jokainen luonnollinen luku $n \geq 2$ on itse alkuluku tai ainakin alkulukujen tulo.

Todistus. I1) $n = 2$: Määritelmän mukaan 2 on alkuluku.
I2) $n = k$ (induktio-oletus): Oletetaan, että on olemassa sellainen $k \geq 2$, että kukin luonnollinen luku m väliltä $2 \leq m \leq k$ on joko alkuluku tai alkulukujen

tulo.
I3) $n = k+1$ (induktioaskel): Todistetaan väitteen pitävän paikkansa luvulle $k+1$. Kannattaa huomata, että induktio-oletus on nytkin laillinen, koska ainakin arvolle $k = 2$ se on totta.
On siis osoitettava, että $k+1$ on alkuluku tai alkulukujen tulo. Jos se on alkuluku, on asia selvä. Muutoin $k+1$ on yhdistetty luku $k+1 = ab$, missä $a \geq 2$, $b \geq 2$ ja molemmat ovat enintään $\frac{1}{2}(k+1) \leq \frac{1}{2}(k+k) = k$. Induktio-oletuksen mukaan a on alkuluku tai alkulukujen tulo, samoin b. Täten myös $k+1 = ab$ on alkulukujen tulo.

Kohtien I1-3) myötä induktiotodistus on valmis; induktioperiaatteen nojalla jokainen luonnollinen luku $n \geq 2$ on alkuluku tai alkulukujen tulo. ■

2 LOGIIKKAA JA LOOGISTA PÄÄTTELYÄ

Logiikka on matematiikan ja filosofian välimaastoon luettava itsenäinen tiede, jonka tehtävänä on koota inhimillisessä ajattelussa esiintyvät lait ja rakentaa niistä ristiriidaton, yksinkertainen, mutta mahdollisimman täydellinen järjestelmä.

Logiikan perusobjekteja ovat *tosiksi* tai *epätosiksi* sovittavat ilmaukset tai väittämät, *lauseet*. Esimerkiksi ilmaus

> ”Maa on hieman navoiltaan litistynyt pallo.”

voitaneen nykyään helposti sopia todeksi lauseeksi, vaikkakaan näin ei ole aina ollut.

Logiikka ei puutu siihen, onko jokin perusväite sellaisenaan tosi vai ei, vaan se pyrkii tilanteessa, jossa tietyt väitteet on hyväksytty tosiksi, ratkaisemaan, mitä muita näistä väitteistä johdettuja väitteitä on pidettävä tosina.

Lauselogiikaksi eli *propositiologiikaksi* sanotaan totuusarvoiltaan yksiselitteisten *suljettujen lauseiden* ja niistä logiikan operaatioiden avulla *johdettujen* lauseiden totuusarvojen tarkastelua, ks. Luku 2.1.

Lausefunktiologiikan eli *predikaattilogiikan* avulla puolestaan tutkitaan – enimmäkseen lauselogiikasta saaduin menetelmin – *avointen lauseiden* loogisia arvoja. Avoimen lauseen totuusarvo voi riippua joistakin muuttujista, ja ennen totuusarvon määrittämistä täytyy lauseesta muodostaa suljettu lause sijoittamalla muuttujille arvot tai käyttämällä *kvantifiointioperaattoreita* eli *kvanttoreita*, ks. Luku 2.2.

Luvussa 2.3 luomme katsauksen matemaattisen todistamisen loogiseen perustaan.

2.1 Lauselogiikkaa

Lause ja totuusarvot

Määritelmä 2.1.1 Logiikassa *lause* (*statement*, *proposition*) tarkoittaa ilmausta tai väitettä, jolla on jompikumpi totuusarvoista *tosi* T (*true*) tai *epätosi* E (*false*). Todelle käytetään myös symbolia 1 ja epätodelle 0.

Tarkasti ottaen jokaisesta ilmauksesta saadaan lause liittämällä siihen jompikumpi totuusarvo, mutta *yleensä on järkevää liittää reaalimaailman ilmauksiin niiden havainnolliset totuusarvot.*

Reaalimaailman ilmauksen paikkansapitävyys, sen *havainnollinen* totuusarvo, voi eri yhteyksissä, eri ajanhetkinä ja eri ihmisten mielessä vaihdella. Logiikan kan-

nalta lauseen totuusarvon tulee kuitenkin olla yksiselitteinen; kussakin tilanteessa käytettävien lauseiden totuusarvot tulee tarkastelijoiden määrittää tai vaikkapa sopia keskenään.

Esimerkki 2.1.2 Mitkä seuraavista reaalimaailman ilmauksista

P: "Sataa vettä."

Q: "Sataa vanhoja ukkoja."

R: "Tuhatta ja sataa."

voidaan todeta lauseiksi liittämällä niihin niiden havainnolliset totuusarvot?

Ratkaisu. Ilmausta Q pidettäneen yleisesti epätotena lauseena. Ilmaukselle P saadaan totuusarvo vaikkapa vilkaisemalla ulos ikkunasta (kyseessähän on itse asiassa ajasta ja paikasta riippuva avoin lause). Sen sijaan R:lle ei voitane totuusarvoa määrätä, joten se ei ole logiikan mielessä lause (ellei sille totuusarvoa erikseen sovita).

Tehtävä 2.1.3 Mitkä seuraavista ovat mielestäsi logiikan lauseita ja mitkä totuusarvot niille asettaisit:

P: "Avaa ikkuna." _____

Q: "Rooma on Ranskassa." _____

R: "$3 < 2$." _____

S: "Arvoilla $x \neq 0$ on $x^2 + 1 > 0$." _____

Tehtävä 2.1.4 Edustakoot k, l ja m mitä tahansa kokonaislukuja. Mitkä seuraavista lauseista ovat tosia:

P: "$k(l + n) = kl + kn$." _____

Q: "$(m+1)^2 + n^2 + 2m^2 > 0$." _____

R: "$2k$ on parillinen luku." _____

S: "Jos m on parillinen, on olemassa kokonaisluku n, jolle $m = 2n$." _____

Konnektiivit

Logiikassa lauseita yhdistellään loogisilla operaattoreilla, nk. *konnektiiveillä*, joilla on ilmeiset vastineet reaalimaailman lauseiden yhdistelyssä:

$\neg$	negaatio	eli	”ei”	vaihtaa totuusarvon
$\vee$	disjunktio	eli	”tai”	edes yksi tosi
$\wedge$	konjunktio	eli	”ja”	kaikki tosia
$\Rightarrow$	implikaatio	eli	”seuraa”	”jos . . . niin”
$\Leftrightarrow$	ekvivalenssi	eli	”yhtäpitävää”	samat totuusarvot

Määritelmä 2.1.5 Olkoot P ja Q logiikan lauseita.

a) Lauseen P *negaatio* $\neg P$ on lause, jolla on päinvastainen totuusarvo kuin lauseella P.

b) Lauseiden P ja Q *disjunktio* $P \vee Q$ on lause, jonka totuusarvo on tosi, jos P on tosi tai Q on tosi, ja epätosi, jos P ja Q ovat epätosia.

c) Lauseiden P ja Q *konjunktio* $P \wedge Q$ on lause, jonka totuusarvo on tosi, jos P ja Q ovat tosia, muutoin epätosi.

d) Lauseiden P ja Q *implikaatio* $P \Rightarrow Q$ on lause, jonka totuusarvo on epätosi, jos P on tosi ja Q epätosi, muulloin tosi.

e) Lauseiden P ja Q *ekvivalenssi* $P \Leftrightarrow Q$ on lause, jonka totuusarvo on tosi, jos lauseilla P ja Q on sama totuusarvo, muulloin epätosi.

Johdettuja lauseita ovat kaikki ne lauseet, jotka saadaan äärellisen monella logiikan operaatioilla joistakin peruslauseista.

Huomautus 2.1.6 Negaatio kohdistuu yhteen, sitä seuraavaan lauseeseen, muut yhdistävät kahta lausetta, jotka voivat kaikki olla itsekin konnektiiveilla johdettuja; vrt. lukujen laskutoimitukset!

Esimerkki 2.1.7 Oletetaan, että lauseet P, Q ja R ovat tosia. Mitkä ovat seuraavien johdettujen lauseiden totuusarvot:

a) $P \wedge (Q \wedge R)$

b) $P \Rightarrow (\neg Q)$

c) $\big(\neg(P \Rightarrow R)\big) \Leftrightarrow Q$

Ratkaisu. a) P ja $Q \wedge R$ ovat tosia, joten lause on tosi.

b) P on tosi ja $\neg Q$ epätosi, joten implikaatio on epätosi.

c) Koska Q on tosi, on ekvivalenssi tosi täsmälleen silloin kun vasen puoli on tosi. Implikaatio $P \Rightarrow R$ on tosi, joten sen negaationa vasen puoli on epätosi, joten lause on epätosi.

Tehtävä 2.1.8 Oletetaan lauseista P, Q ja R, että P on epätosi, mutta muut tosia. Mitkä ovat seuraavien johdettujen lauseiden totuusarvot:

a) $P \wedge (Q \vee R)$ _____

b) $(P \wedge Q) \vee R$ _____

c) $\big(\neg(P \Rightarrow R)\big) \Leftrightarrow Q$ _____

Monimutkaisten johdettujen lauseiden totuusarvot (usein vielä peruslauseiden eri totuusarvoilla) määritetään nk. totuusarvotaulukoilla. Harjoitellaan kuitenkin vielä kielellisten ilmausten kääntämistä logiikan kielelle.

Esimerkki 2.1.9 Olkoot

P: ”Neljältä sataa.”

Q: ”Haen tyttären pyörällä.”

R: ”En hae tytärtä autolla.”

Silloin esimerkiksi

$\neg P$ tarkoittaa ”Neljältä ei sada.”

$Q \vee (\neg R)$ tarkoittaa ”Haen tyttären pyörällä tai autolla.”

$(\neg Q) \Leftrightarrow P$ tarkoittaa ”En hae tytärtä pyörällä jos ja vain jos neljältä sataa.”

Tehtävä 2.1.10 Mitä tarkoittavat Esimerkin 2.1.9 tapauksessa lauseet

a) $(\neg P) \Rightarrow Q$ _____

b) $Q \wedge (P \vee \neg P)$ _____

c) $(P \wedge \neg Q) \vee (Q \wedge \neg P)$ _____

d) $P \Rightarrow \neg R$ _____

Totuusarvotaulukko

Annetuista peruslauseista konnektiiveilla johdetun lauseen totuusarvot saadaan selville mekaanisilla laskuilla, jotka kannattaa formuloida *totuusarvotaulukoksi* (*truth table*). Totuusarvotaulukon vasempaan laitaan asetetaan alekkain peruslauseiden P_1, P_2, ..., P_n kaikki 2^n totuusarvoyhdistelmää. Näiden oikealle puolelle lasketaan haluttujen johdannaisten totuusarvot kullakin yhdistelmällä.

Esimerkki 2.1.11 Tai-konnektiivin taulukoksi saadaan:

P	Q	$P \vee Q$
T	T	T
T	E	T
E	T	T
E	E	E

Tehtävä 2.1.12 Muodosta implikaation taulukko (ks. Määritelmä 2.1.5):

P	Q	$Q \Rightarrow P$
T	T	T
T	E	
E	T	
E	E	

Taulukossa 1 ovat yhdellä operaatiolla saatujen johdettujen lauseiden totuusarvot taulukkona (ks. Määritelmä 2.1.5).

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
T	T	E	T	T	T	T
T	E	E	T	E	E	E
E	T	T	T	E	T	E
E	E	T	E	E	T	T

Taulukko 1: Logiikan peruslaskutaulukko

Yleisessä tapauksessa johdettu lause pilkotaan sellaisiksi välituloksiksi, joiden totuusarvot saadaan peruslaskutaulukosta 1. Äärimmäiseksi oikealle asetetaan kysytty lause tai lauseet ja menetellään kuten yllä (tai alla).

Esimerkki 2.1.13 Muodostetaan Tehtävän 2.1.10 kohdan c) lauseen

$$S : (P \wedge \neg Q) \vee (Q \wedge \neg P)$$

totuusarvotaulukko:

P	Q	$\neg P$	$\neg Q$	$P \wedge \neg Q$	$Q \wedge \neg P$	S
T	T	E	E	E	E	E
T	E	E	T	T	E	T
E	T	T	E	E	T	T
E	E	T	T	E	E	E

Tehtävä 2.1.14 Millä seuraavista lauseista $\neg P$, $Q \vee (\neg P)$, $(\neg Q) \Leftrightarrow P$ on samat totuusarvot kuin Esimerkin 2.1.13 lauseella

$$S : (P \wedge \neg Q) \vee (Q \wedge \neg P)?$$

P	Q	$\neg P$	$\neg Q$	$Q \vee (\neg P)$	$(\neg Q) \Leftrightarrow P$	S
T	T	E		T		
T	E					
E			E			
E						

Esimerkki 2.1.15 Pilkotaan Esimerkin 2.1.7 kohdan c) lause

$$L : \big(\neg(P \Rightarrow R)\big) \Leftrightarrow Q$$

osiin, joiden osatulokset saadaan suoraan peruslaskutaulukosta 1.

Ratkaisu. Lause on kahden lauseen $\neg(P \Rightarrow R)$ ja Q ekvivalenssi. Näistä ensimmäinen on lauseen $P \Rightarrow R$ negaatio. Taulukon otsikkoriville kirjoitetaan esimerkiksi

$$P \quad Q \quad R \quad P \Rightarrow R \quad \neg(P \Rightarrow R) \quad Q \quad \big(\neg(P \Rightarrow R)\big) \Leftrightarrow Q$$

Tehtävä 2.1.16 Laadi loppuun Esimerkin 2.1.15 lauseen

$$L : \big(\neg(P \Rightarrow R)\big) \Leftrightarrow Q$$

totuusarvotaulukko:

P	Q	R	$P \Rightarrow R$	$\neg(P \Rightarrow R)$	Q	L
T	T	T	T			
T	T	E	E			
T	E	T	T			
T	E					
E						
E						
E						
E						

Looginen ekvivalenssi ja tautologia

Määritelmä 2.1.17 Kaksi samoista peruslauseista johdettua lausetta L ja M ovat *loogisesti ekvivalentit* (merkitään $L \equiv M$), jos niillä on samat totuusarvot jokaisella peruslauseiden totuusarvoyhdistelmällä. Käytännössä tämä tarkoittaa, että kun lauseiden L ja M totuusarvot on laskettu samaan taulukkoon kaikilla peruslauseiden totuusarvoyhdistelmillä, niin lauseiden L ja M totuusarvosarakkeet ovat identtiset.

Esimerkki 2.1.18 Tehtävässä 2.1.14 havaittiin lauseilla

$$\begin{aligned} L &: (P \wedge \neg Q) \vee (Q \wedge \neg P) \\ M &: (\neg Q) \Leftrightarrow P \end{aligned}$$

olevan samat totuusarvot kaikilla peruslauseiden P ja Q yhdistelmillä. Ne ovat siis loogisesti ekvivalentteja:

$$(P \wedge \neg Q) \vee (Q \wedge \neg P) \equiv (\neg Q) \Leftrightarrow P.$$

Tehtävä 2.1.19 Osoita totuusarvotaulukon avulla, että

$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q).$$

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

Määritelmä 2.1.20 Johdettu lause on *tautologia*, jos se on tosi kaikilla peruslauseiden totuusarvoyhdistelmillä, ts. jos totuusarvosarake sisältää vain arvoja T.

Esimerkki 2.1.21 Osoitetaan tautologiaksi lause

$$\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q :$$

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$
T	T	T	T	T
T	E	E	E	T
E	T	T	E	T
E	E	T	E	T

Tehtävä 2.1.22 Osoita tautologioiksi lauseet

a) $P \Rightarrow (P \vee Q)$

b) $(P \Rightarrow Q) \Leftrightarrow \big((\neg Q) \Rightarrow (\neg P)\big)$.

P	Q	$P \Rightarrow Q$	$(\neg Q) \Rightarrow (\neg P)$	$(P \Rightarrow Q) \Leftrightarrow \big((\neg Q) \Rightarrow (\neg P)\big)$

Looginen ekvivalenssi ja tautologia käyvät yksiin seuraavalla tavalla:

Lause 2.1.23 Kaksi lausetta P ja Q ovat loogisesti ekvivalentit, jos ja vain jos $P \Leftrightarrow Q$ on tautologia.

Laskusääntöjä

Sulkujen käyttö. Johdetuissa lauseissa joudutaan käyttämään paljon sulkuja, jotta laskujärjestys tulee yksikäsitteisesti ilmi. Sulkuja voidaan kuitenkin vähentää – kuten luvuillakin laskettaessa – sopimalla operointijärjestys.

Sovitaan konnektiiveille hierarkia, jota noudatetaan mikäli sulkein ei ole muuta ilmoitettu:

1. $\neg$ operoi ensin (vrt. luvun etumerkki)
2. $\vee$ ja $\wedge$ operoivat tasavertaisina seuraavaksi (sulut!)
3. $\Rightarrow$ operoi sitten
4. $\Leftrightarrow$ operoi viimeisenä.

Tehtävä 2.1.24 Poista turhat sulut seuraavista:

a) $\big(P \wedge (\neg Q)\big) \vee (\neg R)$

b) $\big(P \wedge (\neg R)\big) \Leftrightarrow \big((\neg Q) \Rightarrow (P \vee Q)\big)$

Totuusarvotaulukoiden avulla voidaan todistaa seuraavat loogiset ekvivalenttiudet, joita käyttäen logiikan lauseita voidaan muunnella tarpeen mukaan, esimerkiksi sieventää yksinkertaisempaan muotoon. Sovitaan vielä, että $\mathbf{T}$ tarkoittaa lausetta, jolla on aina arvona tosi.

Laskusääntöjä 2.1.25 Kaikille lauseille P, Q ja R pätee:

$P \equiv P$	identiteetti
$P \wedge P \equiv P \vee P \equiv P$	idempotenssilait
$\neg\neg P \equiv P$	kaksoisnegaatio
$\neg(P \wedge \neg P) \equiv \mathbf{T}$	poissuljettu ristiriita
$P \vee \neg P \equiv \mathbf{T}$	poissuljettu kolmas
$P \vee Q \equiv Q \vee P$ $P \wedge Q \equiv Q \wedge P$	vaihdannaisuus
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	liitännäisyys
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	osittelulait
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	de Morganin lait
$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$	kontrapositio
$P \Rightarrow Q \equiv \neg P \vee Q$	implikaatio disjunktioksi

Todistus. Osittain jo perusteltukin: ensimmäinen de Morganin laki Tehtävänä 2.1.19 ■ ja kontrapositio Tehtävänä 2.1.22. Muut jätetään harjoitustehtäviksi. ■

Tehtävä 2.1.26 Sievennä lauseet

a) $\neg(P \wedge \neg Q)$ _____

b) $P \wedge \big((\neg P \vee Q) \vee \neg P\big)$ _____

2.2 Lausefunktiologiikkaa

Usein tarvitaan nk. *avoimia* lauseita, joiden totuusarvo *riippuu tilanteesta*, esimerkiksi jonkin muuttujan arvosta.

Esimerkki 2.2.1 Olkoot P_1 : "1 on parillinen" ja P_2 : "2 on parillinen". Silloin P_1 on epätosi, kun taas P_2 on tosi.

Yksittäisten lauseiden sijasta voimme rakentaa "parillisuudentestauskoneen" seuraavasti: Merkitään symbolilla

$P(n)$: "n on parillinen luku"

Nyt esimerkiksi $P(1)$, $P(3)$ ja $P(13)$ ovat epätosia, mutta $P(2)$, $P(6)$ ja $P(14)$ tosia.

Määritelmä 2.2.2 Väite P on (yksipaikkainen) *lausefunktio*, jos $P(x)$ on lause jokaisella tarkasteltavalla arvolla x.

Vastaavasti voidaan määritellä kaksi-, tai kolmepaikkaisia lausefunktioita $P(x, y)$, $P(x, y, z)$ jne ...

Esimerkki 2.2.3 Muodostetaan lausefunktio Q, jolla voi testata, onko $x - 1 > 0$:

$Q(x) : x - 1 > 0$

Ratkaisemalla epäyhtälö muotoon $x > 1$ näemme, että $Q(x)$ on tosi (esimerkiksi reaali)arvoilla $x > 1$.

Esimerkki 2.2.4 Olkoot muuttujien v, k ja p mahdolliset arvot

v on jokin viikonpäivä

k on jokin kalenterikuukausi

p on jokin luvuista 1, 2, 3, ..., 31.

Silloin lausefunktiolle

$P(v, k, p)$: "tänään on v, k:n p. päivä".

voidaan aina määrittää totuusarvo, kylläkin tarkasteluajankohdasta riippuen.

Esimerkiksi $P(\text{perjantai}, \text{joulukuu}, 24)$ on tosi vuonna 2004, muttei useimpina muina vuosina.

Tehtävä 2.2.5 Mitkä kaikista lauseista $P(v, k, p)$ ovat tänään tosia?

Entä mitkä eivät ole koskaan tosia?

Kvanttorit

Lausefunktioista saadaan mielenkiintoisia lauseita käyttäen nk. *kvanttoreita kaikilla* $\forall$ ja *on olemassa* $\exists$. Kvanttorien esiintymisjärjestys on näissä oleellista!

Kvanttorien avulla saadaan yhden muuttujan lausefunktioista kaksi eri lausetta:

$$\begin{array}{lll} \forall\, x: & p(x) & (\text{ kaikilla } x : p(x)) \\ \exists\, x: & p(x) & (\text{ ainakin yhdellä } x : p(x)) \end{array}$$

Esimerkki 2.2.6 Reaalilukuja koskevista lauseista a) $P : \forall\, x : x^2 = 4$

b) $Q : \exists\, x : x^2 = 4$ P on selvästi epätosi, mutta Q on tosi, sillä toisaalta esimerkiksi $3^2 \neq 4$, mutta kuitenkin $2^2 = 4$.

Tehtävä 2.2.7 Mitkä seuraavista kokonaislukuja koskevista lauseista ovat tosia? Perustele tarkoin!

a) $P : \forall\, n : n^2 > n$ _____

b) $Q : \exists\, n : n^2 < n$ _____

c) $R : \exists\, n : n^2 = 144$ _____

d) $R : \forall\, n : n^2 - n$ on parillinen _____

Kahden muuttujan lausefunktion avulla saadaan (periaatteessa) jo kahdeksan erilaista variaatiota:

$$\begin{array}{lll} \forall\, x, \forall\, y: & p(x,y) & (\text{ kaikilla } x \text{ ja kaikilla } y : p(x,y)) \quad (1) \\ \forall\, x, \exists\, y: & p(x,y) & (\text{ kaikilla } x \text{ on olemassa } y : p(x,y)) \quad (2) \\ \exists\, x, \forall\, y: & p(x,y) & (\text{ on olemassa sellainen } x \text{ että kaikilla } y : p(x,y)) \quad (3) \\ \exists\, x, \exists\, y: & p(x,y) & (\text{ on olemassa } x \text{ ja on olemassa } y : p(x,y)) \quad (4) \\ \forall\, y, \forall\, x: & p(x,y) & (\text{ kaikilla } y \text{ ja kaikilla } x : p(x,y)) \quad (5) \\ \forall\, y, \exists\, x: & p(x,y) & (\text{ kaikilla } y \text{ on olemassa } x : p(x,y)) \quad (6) \\ \exists\, y, \forall\, x: & p(x,y) & (\text{ on olemassa sellainen } y \text{ että kaikilla } x : p(x,y)) \quad (7) \\ \exists\, y, \exists\, x: & p(x,y) & (\text{ on olemassa } y \text{ ja on olemassa } x : p(x,y)) \quad (8) \end{array}$$

Tehtävä 2.2.8 Edellisistä kahdeksasta loogisesti erilaisia on vain kuusi, mitkä parit ovat samoja? _____

Tehtävä 2.2.9 Keksi esimerkki kahden muuttujan lausefunktiosta, jolle

a) kaavoilla (2) ja (3) on eri totuusarvo.

b) kaavoilla (2) ja (7) on eri totuusarvo.

Lausefunktion negaatio

Kvanttoreilla suljetun lausefunktion negaatio saadaan vaihtamalla olemassaolokvanttori $\exists$ kaikkikvanttoriksi $\forall$ ja päinvastoin sekä ottamalla lausefunktion negaatio. Esimerkiksi:

$\neg\,(\exists\, x \in A:\ P(x)) \quad \equiv \quad \forall\, x \in A:\ \neg P(x)$
"Ei pidä paikkaansa, että on olemassa $x \in A$, jolle $P(x)$ pätee."
"Ei ole olemassa alkiota $x \in A$, jolle $P(x)$ pätee."
"jokaiselle $x \in A$ on $P(x)$ epätotta."

$\neg\,(\forall\, x \in A:\ P(x)) \quad \equiv \quad \exists\, x \in A:\ \neg P(x)$
"Ei pidä paikkaansa, että kaikilla $x \in A$ pätee $P(x)$."
"On olemassa ainakin yksi alkio $x \in A$, jolle $P(x)$ ei päde."

$\neg\,(\exists\, x \in A,\ \forall\, y \in B:\ P(x,y)) \quad \equiv \quad \forall\, x \in A,\ \exists\, y \in B:\ \neg P(x,y)$

Jne.

Lause on epätosi, jos sen negaatio on tosi. Se, että jokin lause on epätosi perustellaan sen negaation avulla, näyttämällä negaatio todeksi.

Tehtävä 2.2.10 Mitkä seuraavista kolmen muuttujan lausefunktion avulla muodostetusta lauseista ovat tosia:

a) $\exists\, x, \forall\, y, \forall\, z : x(y+z^2) = 0$ _____

b) $\forall\, x, \forall\, y, \exists\, z : x(y+z^2) = 0$ _____

c) $\forall\, x, \exists\, z, \forall\, y : x(y+z^2) = 0$ _____

d) $\forall\, x, \forall\, z, \exists\, y : x(y+z^2) = 0$ _____

e) $\forall\, x, \exists\, y, \forall\, z : x(y+z^2) = 0$ _____

f) $\exists\, z, \forall\, y, \forall\, x : x(y+z^2) = 0$ _____

g) $\exists\, y, \exists\, x, \forall\, z : x(y+z^2) > 0$ _____

2.3 Matemaattinen todistaminen ja päättelyprosessit

Tieteissä pyritään joistakin tosiksi hyväksytyistä peruslauseista, esimerkiksi *aksioomista*, lähtien johtamaan logiikan lakien avulla uusia lauseita. Yleensä tämä tapahtuu niin, että esitetään hypoteesi, otaksuma, ja pyritään *todistamaan* se.

Suora todistus tarkoittaa menettelyä, jokin haluttu tulos johdetaan loogisella päättelyllä tosista tai tosiksi oletetuista ominaisuuksista (aksiooma, ulkoinen totuus).

Epäsuorassa todistuksessa taas lähdetään olettamuksesta, että haluttu väite ei olisikaan tosi (*vastaoletus* eli *antiteesi*), ja johdetaan ristiriita alkuperäisten oletusten kanssa, tai koetetaan johtaa jokin muu tunnetusti epätosi tulos (esimerkiksi $1 = 0$ tai että toisen asteen polynomilla on tasan kolme nollakohtaa).

Suora todistus

Olkoon P tosi lause ja Q todeksi osoitettava lause.
Suora todistus perustuu Esimerkin 2.1.21 tautologiaan

$$\big(P \wedge (P \Rightarrow Q)\big) \;\Rightarrow\; Q :$$

Kun osoitetaan, että $P \Rightarrow Q$ on tosi, on $P \wedge (P \Rightarrow Q)$ tosi. Koska koko lause on tautologia, on Q välttämättä tosi.

Käytännön todistuksissa ei oletus P yleensä yksin riitä, vaan apuna joudutaan käyttämään sopivia *ulkoisia totuuksia* U, esimerkiksi tunnettuja laskusääntöjä ja aikaisemmin todistettuja tuloksia. Nämä ulkoiset totuudet voidaan haluttaessa sisällyttää oletukseen kirjoittamalla oletus muotoon $P' \equiv P \wedge U$.

Esimerkki 2.3.1 Todistetaan suorasti:

Jos n on pariton kokonaisluku, niin n^2 on pariton kokonaisluku.

Ratkaisu. *Oletus-väitös-todistus-muodossa*:

Oletus. P: "n pariton kokonaisluku" tosi.

Väitös. Q: "n^2 pariton kokonaisluku" tosi.

Todistus. Käytetään ulkoista totuutta: pariton $n = 2k+1$ jollekin kokonaisluvulle k. Mutta lukujen laskusäännöistä seuraa

$$n^2 = (2k+1)^2 = 2(2k^2+2k) + 1,$$

joka on pariton luku (myös ulkoinen totuus!). Siis Q on tosi. ■

Epäsuora todistus

Puhdas epäsuora todistus perustuu kontraposition $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ ja suoran todistuksen yhdistämiseen; nimittäin myös

$$P \wedge \big(\neg Q \Rightarrow \neg P\big) \;\Rightarrow\; Q$$

on tautologia. Oletetaan, että $\neg Q$ on tosi, so. tehdään *vastaoletus* eli *antiteesi*. Tämän avulla osoitetaan, että $\neg P$ on tosi. Koska tämä on vastoin oletuksia, ei Q voi olla epätosi ja on siten tosi.

Esimerkki 2.3.2 Todista uudelleen, nyt epäsuorasti:

Jos n on pariton kokonaisluku, niin n^2 on pariton kokonaisluku.

Oletus. P: "n pariton kokonaisluku" tosi.

Väitös. Q: "n^2 pariton kokonaisluku" tosi.

Todistus. $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$, joten tehdään

Antiteesi: $\neg Q$ tosi eli n^2 on parillinen. Ulkoinen totuus: $n^2 = 2m$ jollekin kokonaisluvulle m. Harjoitustehtävänä todistetaan ulkoinen totuus:

Jos kokonaislukujen tulo ab on jaollinen alkuluvulla p, niin a tai b on jaollinen luvulla p.

Luku $n^2 = n \cdot n$ on siis jaollinen alkuluvulla 2, joten n on jaollinen luvulla 2. Siis n on parillinen eli $\neg P$ on tosi.

Tämä on ristiriita oletuksen kanssa, joten antiteesi on väärä ja väitös totta. ■

Esimerkki 2.3.3 Todistetaan käänteinen tulos:

Jos n^2 on pariton, niin n on pariton.

Oletus. Q tosi eli n^2 pariton.

Väitös. P tosi eli n pariton.

Todistus. Antiteesi: $\neg P$ tosi eli n parillinen. Silloin $n = 2k$ ja $n^2 = 2(2k^2)$, joka on parillinen. Siis $\neg Q$ on tosi. Tämä on vastoin oletusta, joten P on tosi. ■

On siis todistettu kokonaan

Lause 2.3.4 Kokonaisluku n on pariton jos ja vain jos n^2 on pariton.

Epäsuora todistus voi olla myös ”kiero”, joskus voi olla edullisempaa johtaan antiteesista jokin muu epätosi tulos kuin $\neg P$, esimerkiksi $1 < 0$.

Yleinen epäsuora todistustapa perustuu tautologiaan

$$\big[P \wedge \big((P \wedge \neg Q) \Rightarrow \mathbf{E}\big)\big] \;\Rightarrow\; Q,$$

Oletetaan, että $\neg Q$ on tosi, so. tehdään *vastaoletus* eli *antiteesi*. Tämän ja oletuksen ”P on tosi” avulla osoitetaan jokin järjettömyys.

Tehtävä 2.3.5 Todista: ”Jos $x > 5$, niin $x > 4$.” niin, että saat oletuksen vastaoletuksen avulla tuloksen $0 > 1$.

Päättelyn johdonmukaisuus

Matemaattinen todistus sisältää yleensä loogisia päättelyitä. Päättelyn johdonmukaisuuden selvittämisessä voidaan käyttää totuusarvotaulukoita. Tämä tarkoittaa, että loogisen pätevyyden tarkastaminen voidaan *mekanisoida*.

Määritelmä 2.3.6 *Päättely* (*argument*) on logiikan lause

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \;\Rightarrow\; B,$$

joka muodostuu kokoelmasta (mahdollisesti johdettuja) logiikan lauseita, *premissejä* $A_1, A_2, \ldots, A_n$ ja *johtopäätöksestä* B (*conclusion*).
Päättelyä sanotaan *johdonmukaiseksi* (*valid argument*), jos kyseinen päättelylause $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \;\Rightarrow\; B$ on tautologia.

Esimerkki 2.3.7 Onko seuraava päättely johdonmukainen?

Jos on eläkkeellä, saa alennuksen rautateillä. En ole eläkkeellä. Siis en saa alennusta rautateillä.

Ratkaisu. Valitaan P: ”Olen eläkkeellä.” ja Q: ”Saan alennuksen rautateillä.”

Päättely koostuu nyt premisseistä A_1: $P \Rightarrow Q$ ja A_2: $\neg P$ ja johtopäätöksestä B: $\neg Q$:

$P \Rightarrow Q$	:	Jos on eläkkeellä, saa alennuksen rautateillä.
$\neg P$	:	En ole eläkkeellä.
$\neg Q$	:	En saa alennusta rautateillä

Muodostamme päättelylauseen $\big((P \Rightarrow Q) \wedge \neg P\big) \Rightarrow \neg Q$ totuusarvotaulukon. Sen kolmannella rivillä on arvo epätosi, joten päättely ei ole johdonmukainen.

		A_1	A_2	$A_1 \wedge A_2$	B	$(A_1 \wedge A_2) \Rightarrow B$
P	Q	$P \Rightarrow Q$	$\neg P$		$\neg Q$	
T	T	T	E	E	E	T
T	E	E	E	E	T	T
E	T	T	T	T	E	$\boxed{E}$
E	E	T	T	T	T	T

Käytännön oikotie. Implikaatiolauseen totuusarvoista seuraa:
Päättelylause $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Rightarrow B$ on tautologia jos, ja vain jos, aina kun kaikki premissit A_i ovat tosia, myös johtopäätös B on tosi. Niinpä totuusarvotaulukosta voidaan jättää pari saraketta pois, kun tarkastellaan ne rivit, joilla premissit ovat tosia ja varmistetaan, että niillä riveillä johtopäätös on myös tosi. Johtopäätös *saa* tietenkin olla tosi muillakin riveillä.

Esimerkki 2.3.8 Onko seuraava päättely johdonmukainen:

Jos elintasoa jatkuvasti nostetaan, luonnonvarojen väheneminen ja luonnon saastuttaminen jatkuu. Jos luonnonvarojen väheneminen ja luonnon saastuttaminen jatkuu, ihmiskunta tuhoutuu taistelussa ehtyvistä luonnonvaroista tai menehtyy saasteisiin. Elintasoa nostetaan. Siis ihmiskunta tuhoutuu taisteluun ehtyvistä luonnonvaroista tai menehtyy saasteisiin.

Ratkaisu. Olkoot

P: ”Elintasoa nostetaan.”
Q: ”Luonnonvarojen väheneminen ja luonnon saastuttaminen jatkuu.”
R: ”Ihmiskunta tuhoutuu taistelussa ehtyvistä luonnonvaroista tai menehtyy saasteisiin.”

Päättelyn $\big((P \Rightarrow Q) \wedge (Q \Rightarrow R) \wedge P\big) \Rightarrow R$ totuusarvotaulukossa (täydennä!)

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	P	R
T	T	T	T	T	T	T
T	T	E	E			
T	E	T	T			
T	E					
E						
E						
E						
E						

vain ensimmäisellä rivillä ovat premissit tosia. Koska tällöin johtopäätös on tosi, on päättely johdonmukainen.

3 ALKEISJOUKKO-OPPIA

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.

3.1 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:

$$\{\, n \in \mathbb{N} \mid n = 2k < 10 \text{ jollekin } k \in \mathbb{N} \,\}. \tag{9}$$

- muodostetaan joukko-operaatioilla muista joukoista (ks. Luku 3.2).

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 (lausefunktio, ks. Luku 2.2) pätee eli ehto $P(x)$ on tosi.

Esimerkki 3.1.1 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 3.1.2 Esitä esimerkkijoukon (9) 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. Joukkoon kuulumattomuutta merkitään $x \notin A$.

Määritelmä 3.1.3 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 3.1.4 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 3.1.5 Jos P on sellainen ominaisuus, että $P(x)$ ei päde millään alkiolla $x \in \mathbf{X}$, ei joukolla $\{x \in \mathbf{X} \mid P(x)\}$ ole yhtään alkiota. Tällöin joukko on *tyhjä*, merkitään $\emptyset$ (*void*, *empty set*). Tyhjä joukko sisältyy jokaiseen joukkoon, ts. $\emptyset \subseteq A$ olipa A mikä tahansa joukko.

Esimerkki 3.1.6 (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.

3.2 Operoiminen joukoilla

Määritelmä 3.2.1 Olkoot A ja B perusjoukon $\mathbf{X}$ osajoukkoja. Joukkojen A ja B

(a) *yhdiste* eli *unioni* (*union*) on perusjoukon $\mathbf{X}$ osajoukko

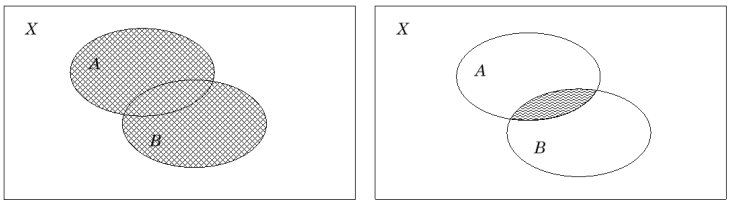
$$A \cup B := \{x \in \mathbf{X} \mid x \in A \text{ tai } x \in B\};$$

(b) *leikkaus* (*intersection*) on perusjoukon $\mathbf{X}$ osajoukko

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

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

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



Kuva 2: Joukkojen A ja B yhdiste ja leikkaus

Lause 3.2.2 Yhdisteellä ja leikkauksella on seuraavat ominaisuudet:

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

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

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

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

$(A \cap B) \cap C = A \cap (B \cap C)$ (liitännäisyys 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 $A \cap B \subseteq A$

(kommutatiivisuus = vaihdannaisuus, assosiatiivisuus = liitännäisyys)

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

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

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

Todistus. Esimerkiksi osittelulaki 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 3.2.3 Osittelulait 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 3.2.4 Perusjoukon $\mathbf{X}$ osajoukon A *komplementti* $\overline{A}$ on joukko

$$\overline{A} := \{\, x \in \mathbf{X} \mid x \notin A \,\}.$$

Lause 3.2.5 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) $A \subseteq B$ jos ja vain jos $\overline{B} \subseteq \overline{A}$

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

Todistus. Sopivia harjoitustehtäviä. ■

Määritelmä 3.2.6 Perusjoukon $\mathbf{X}$ osajoukkojen A ja B *erotus* $A \setminus B$ on joukko

$$A \setminus B := \{\, x \in \mathbf{X} \mid x \in A \text{ ja } x \notin B \,\}$$

Lause 3.2.7 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 3.2.8 Joukkojen A, $B \subseteq \mathbf{X}$ *symmetrinen erotus* $A \triangle B$ on joukko

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

Lause 3.2.9 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 yhdiste, leikkaus, komplementti, erotus ja symmetrinen erotus ovat edelleen perusjoukon $\mathbf{X}$ osajoukkoja. Näiden operaatioiden välillä löytyy riippuvuuksia. Voimme valita ns. perusoperaatioiksi esimerkiksi yhdisteen, leikkauksen ja komplementin, kuten yleensä tehdäänkin. Muut joukko-operaatiot voidaan esittää näiden perusoperaatioiden avulla. Kuten edellä nähtiin, riippuu symmetrinen erotus yhdisteestä 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 yhdiste, leikkaus ja komplementin muodostus ovat joukkoalgebrassa nk. *hilaoperaatiot*.

Seuraus 3.2.10 DeMorganin laeilla (C2) ja (C3) on voimassa luonnolliset yleistykset:

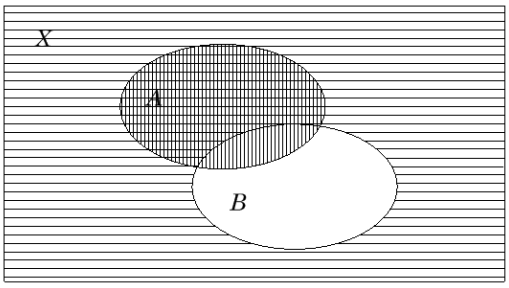
(C2') $\overline{A_1 \cup A_2 \cup \ldots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_n}$

(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. ■

Esimerkki 3.2.11 *Väite*: $A \subseteq B$ jos ja vain jos $A \cap \overline{B} = \emptyset$.

Kuvassa 3 ristikoitu alue edustaa joukkoa $A \cap \overline{B}$.



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

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 yhdisteen 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

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

3.3 Karteesinen tulo eli tulojoukko

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

Määritelmä 3.3.1 Kahden joukon $\mathbf{X}$ ja $\mathbf{Y}$ *karteesinen tulo* eli *tulojoukko* $\mathbf{X}\times\mathbf{Y}$ on järjestettyjen parien (x, y) joukko, missä $x \in \mathbf{X}$ ja $y \in \mathbf{Y}$; siis

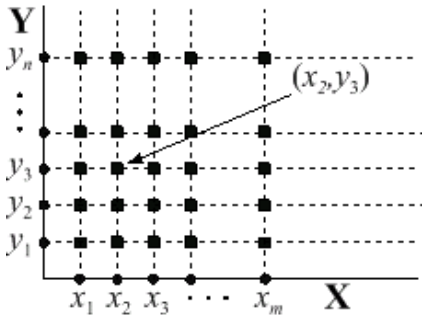
$$\mathbf{X}\times\mathbf{Y} := \{\, (x, y) \mid x \in \mathbf{X}, y \in \mathbf{Y} \,\}.$$

Esimerkki 3.3.2 Joukkojen $\mathbf{X} := \{x_1, x_2, x_3\}$ ja $\mathbf{Y} := \{y_1, y_2\}$ tulojoukossa on $3 \cdot 2 = 6$ alkiota

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

Tuttuja tulojoukkoja ovat xy-taso $\mathbb{R}^2$ ja vaikkapa $[0, 1] \times [1, 2]$, tason suorakulmio; piirrä se!

Yleisemminkin tulojoukkoa voidaan havainnollistaa koordinaatiston tapaan kaksiulotteisilla kuvioilla, ks. Kuva 4.



Kuva 4: Tulojoukon koordinaatistoesitys

Tulojoukko voidaan muodostaa useammallekin joukolle. Tulojoukko toimii mm. relaation ja matriisien perusjoukkona, ks. Luvut 4 ja 5.

Samoin (yksinkertaisessa) suunnatussa verkossa (Luku 13) käytetään järjestettyjä pareja, mutta suuntaamattoman verkon yhteydessä käytetään nk. *ei-järjestettyä tuloa*, ks. Luku 12.

3.4 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 3.4.1 Joukolla $\mathbf{X} := \{1, 2, 3\}$ on yhteensä 8 osajoukkoa ja

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

Määritelmä 3.4.2 Joukkojen *kunnalla* $\mathcal{F}$ joukossa $\mathbf{X}$ tarkoitetaan sellaista $\mathbf{X}$:n osajoukkojen kokoelmaa, että aina 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 yhdisteen että komplementin ja leikkauksen suhteen.

Esimerkki 3.4.3 Joukkokuntia ovat esimerkiksi

(a) Joukon $\mathbf{X}$ potenssijoukko $\mathcal{P}(\mathbf{X})$,

(b) Joukon $\mathbf{X}$ kaikkien äärellisten osajoukkojen ja niiden komplementtien joukko,

(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 myös $\mathbf{X} = \overline{\emptyset} \in \mathcal{F}$.

3.5 Äärellisistä ja äärettömistä joukoista

Alkeisjoukko-opin lopuksi luomme pinnallisen katsauksen joukkojen kokovertailuun. Tarkemmin asiaa käsitellään Luvussa 10.

Määritelmä 3.5.1 Joukko $\mathbf{X}$ on *äärellinen*, jos se on joko tyhjä tai sen alkiot voidaan numeroida luonnollisilla luvuilla 1, 2, …, n jollakin $n \in \mathbb{N}$, ts. lukumääräjoukon $[n]$ alkioilla. Täsmällisemmin tämä voidaan ilmaista siten, että on olemassa bijektio (ks. Luku 5.7) joukkojen $\mathbf{X}$ ja $[n]$ välillä. Muut kuin äärelliset joukot ovat *äärettömiä*, ks. Luku 10.5.

4 MATRIISILASKENNAN ALKEITA

Yleistämme Luvussa 3.3 määritellyn tulojoukon useammille joukoille ja tutustumme laskemiseen luku- ja totuusarvovektoreilla ja matriiseilla.

4.1 Karteesinen tulo ja matriisi

Määritelmä 4.1.1 Äärellisen monen epätyhjän joukon $\mathbf{X}_1$, $\mathbf{X}_2$, $\mathbf{X}_3$, …, $\mathbf{X}_n$ *n-ulotteinen karteesinen tulo* eli *tulojoukko* on järjestettyjen jonojen joukko

$$\prod_{i=1}^{n} \mathbf{X}_i = \mathbf{X}_1 \times \mathbf{X}_2 \times \cdots \times \mathbf{X}_n := \{\, (x_1, x_2, \ldots, x_n) \mid x_i \in \mathbf{X}_i \,\}$$

ja sen alkioita $(x_1, x_2, \ldots, x_n)$ sanotaan *vektoreiksi*. Erityisesti merkitään

$$\mathbf{X}^n := \underbrace{\mathbf{X} \times \cdots \times \mathbf{X}}_{n \text{ kpl}}.$$

Joukkoa $\mathbb{R}^n$ varustettuna vektorien alkioittaisella yhteenlaskulla ja reaalivakiolla kertomisella

$$\begin{aligned} (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &:= (x_1{+}y_1, x_2{+}y_2, \ldots, x_n{+}y_n) \\ c \cdot (x_1, x_2, \ldots, x_n) &:= (cx_1, cx_2, \ldots, cx_n) \end{aligned}$$

sanotaan *n-ulotteiseksi euklidiseksi avaruudeksi*.

Vektoreiden $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ ja $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$ *skalaari-* eli *pistetulo* on luku

$$\mathbf{x} \cdot \mathbf{y} := \sum_{i=1}^{n} x_i y_i = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Vektorin $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ *pituus* eli *normi* on

$$\|\mathbf{x}\| = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \left(x_1^2 + x_2^2 + \cdots + x_n^2\right)^{1/2}.$$

Esimerkki 4.1.2 Avaruuden $\mathbb{R}^5$ vektoreille

$$\mathbf{x} = (2, -3, 0, 2, -2) \text{ ja } \mathbf{y} = (4, 2, 3, -1, 6)$$

ja reaaliluvulle $c = 4$ saadaan operaatioiden tuloksina

$$\begin{aligned}
(2, -3, 0, 2, -2) + (4, 2, 3, -1, 6) &= (2{+}4, -3{+}2, 0{+}3, 2{-}1, -2{+}6) \\
&= (6, -1, 3, 1, 4), \\
4 \cdot (2, -3, 0, 2, -2) &= (4{\cdot}2, 4{\cdot}(-3), 4{\cdot}0, 4{\cdot}2, 4{\cdot}(-2)) \\
&= (8, -12, 0, 8, -8), \\
(2, -3, 0, 2, -2) \cdot (4, 2, 3, -1, 6) &= 2{\cdot}4 + (-3){\cdot}2 + 0{\cdot}3 + 2{\cdot}(-1) + (-2){\cdot}6 \\
&= -12.
\end{aligned}$$

Jos tulojoukon tekijöitä $\mathbf{X}_i$ on mn kappaletta, $m, n \in \mathbb{N}$, ne voidaan indeksoida uudelleen ja kirjoittaa $m{\times}n$-suorakulmioksi muotoon

$$\mathcal{X} = \prod_{i,j}^{m,n} \mathbf{X}_{ij} := \begin{pmatrix}
\mathbf{X}_{11} & \times & \mathbf{X}_{12} & \times & \cdots & \times & \mathbf{X}_{1n} \\
\times & & \times & & & & \times \\
\mathbf{X}_{21} & \times & \mathbf{X}_{22} & \times & \cdots & \times & \mathbf{X}_{2n} \\
\times & & \times & & & & \times \\
\vdots & & \vdots & & \ddots & & \vdots \\
\times & & \times & & & & \times \\
\mathbf{X}_{m1} & \times & \mathbf{X}_{m2} & \times & \cdots & \times & \mathbf{X}_{mn}
\end{pmatrix}$$

Joukon $\mathcal{X}$ alkiota M sanotaan $m{\times}n$-*matriisiksi* ja merkitään

$$X = (x_{ij})_{m\times n} = \begin{pmatrix}
x_{11} & x_{12} & \cdots & x_{1n} \\
x_{21} & x_{22} & \cdots & x_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
x_{m1} & x_{m2} & \cdots & x_{mn}
\end{pmatrix}, \quad x_{ij} \in \mathbf{X}_{ij}.$$

Tällaisia tulojoukkoja ja matriiseja, jotka voivat koostua erilaisia tietotyyppejä edustavista perusjoukoista $\mathbf{X}_{ij}$, käytetään mm. taulukkolaskentaohjelmissa. Yksirivistä matriisia sanotaan myös *vaakavektoriksi* ja yksisarakkeista *pystyvektoriksi*. Matriisilaskennan yhteydessä vektorin alkioiden väliset pilkut korvataan usein tyhjeellä.

4.2 Matriisien laskutoimitukset

Matriisin $A = (a_{ij}) \in \mathbb{R}^{m\times n}$ *transpoosi* on matriisi $A^T = (b_{kl}) \in \mathbb{R}^{n\times m}$, missä $b_{kl} := a_{lk}$, ts. rivit on vaihdettu järjestyksessä sarakkeiksi. Avaruuden $\mathbb{R}^{m\times n}$ matriiseja voidaan laskea yhteen, kertoa vakiolla ja kertoa keskenään *alkioittain* kuten vektoreitakin.

Esimerkki 4.2.1 Olkoot

$$A := \begin{pmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad B := \begin{pmatrix} 2 & -1 & -2 \\ 1 & 3 & 1 \end{pmatrix}$$

Transpoosit ovat silloin

$$A^T = \begin{pmatrix} 1 & 3 \\ 2 & 0 \\ -2 & 1 \end{pmatrix} \quad \text{ja} \quad B^T = \begin{pmatrix} 2 & 1 \\ -1 & 3 \\ -2 & 1 \end{pmatrix}$$

Matriisien *yhteenlaskun* tulos on *summa*

$$A + B = \begin{pmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & -1 & -2 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & -4 \\ 4 & 3 & 2 \end{pmatrix}$$

Matriisin *kertominen skalaarilla* tarkoittaa *skaalausta*:

$$(-2)A = -2A = -\begin{pmatrix} 2 & 4 & -4 \\ 6 & 0 & 2 \end{pmatrix} = \begin{pmatrix} -2 & -4 & 4 \\ -6 & 0 & -2 \end{pmatrix}$$

Matriisien *alkioittainen tulo*:

$$A .* B = \begin{pmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{pmatrix} .* \begin{pmatrix} 2 & -1 & -2 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -2 & 4 \\ 3 & 0 & 1 \end{pmatrix}$$

Alkioittaisella tulolle ei juuri ole käyttöä esimerkiksi lineaarialgebrassa, mutta ainakin Matlab-ohjelmassa se on varsin hyödyllinen, mm. muodostettaessa piirrettäviksi tarkoitettujen objektien matriisiesityksiä.

Varsinainen *matriisien kertolasku* määritellään seuraavasti:

Määritelmä 4.2.2 Matriisien $A = (a_{ij}) \in \mathbb{R}^{m\times n}$ ja $B = (b_{jk}) \in \mathbb{R}^{n\times r}$ *(matriisi)tulo* on matriisi

$$AB = C = (c_{ik}) \in \mathbb{R}^{m\times r},$$

missä $c_{ik} := \sum_{j=1}^{n} a_{ij}b_{jk}$.

Tulomatriisin alkio c_{ik} on siis matriisin A rivin i ja matriisin B sarakkeen k pistetulo. Pystyvektorien $\mathbf{x}$ ja $\mathbf{y} \in \mathbb{R}^n$ pistetulo voidaan kirjoittaa matriisitulona

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x}^T\mathbf{y} = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^{n} x_i y_i.$$

Pystyvektorin $\mathbf{x}$ *normille* $\|\mathbf{x}\|$ pätee

$$\|\mathbf{x}\|^2 = \sum_{i=1}^{n} x_i^2 = \mathbf{x}^T\mathbf{x}.$$

Esimerkki 4.2.3 Esimerkin 4.2.1 matriiseille tuloja AB ja BA ei ole määritelty, koska molemmat ovat 2×3-matriiseja; sen sijaan

$$\begin{aligned} AB^T &= \begin{pmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 3 \\ -2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1\cdot2 + 2\cdot(-1) + (-2)\cdot(-2) & 1\cdot1 + 2\cdot3 + (-2)\cdot1 \\ 3\cdot2 + 0\cdot(-1) + 1\cdot(-2) & 3\cdot1 + 0\cdot3 + 1\cdot1 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 4 & 4 \end{pmatrix} \\ A^TB &= \begin{pmatrix} 1 & 3 \\ 2 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & -2 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 8 & 1 \\ 4 & -2 & -4 \\ -3 & 5 & 5 \end{pmatrix} \end{aligned}$$

Tehtävä 4.2.4 Osoita, että matriisien kertolasku *ei ole* vaihdannainen; yleensä $AB \neq BA$.

4.3 Nimityksiä ja laskusääntöjä

Avaruuden $\mathbb{R}^{n\times n}$ alkioita sanotaan *neliömatriiseiksi*. Avaruus $\mathbb{R}^{n\times n}$ on *suljettu* matriisien kertolaskun suhteen, sillä tulokin on $n\times n$-matriisi. Matriisin $(a_{ij})_{n\times n}$ *diagonaaliksi* sanotaan vektoria $(a_{11}, a_{22}, \ldots, a_{nn})$. Matriisia sanotaan *diagonaalimatriisiksi*, jos sen diagonaalin ulkopuolella olevat alkiot ovat nollia.

Matriisia O, jonka kaikki alkiot ovat nollia, kutsutaan *nollamatriisiksi*. Nollamatriisi on matriisien yhteenlaskun neutraalialkio.

Yksikkömatriisi on diagonaalimatriisi I, jonka diagonaalialkiot ovat ykkösiä. Yksikkömatriisi on matriisien kertolaskun neutraalialkio: jos $A \in \mathbb{R}^{n\times n}$, niin $AI = IA = A$. Matriisi $(a_{ij})_{n\times n}$ on *symmetrinen*, jos $a_{ij} = a_{ji}$ kaikilla $i, j \in [n]$, ts. jos matriisi on diagonaalin suhteen symmetrinen. Matriisi on *yläkolmiomatriisi*, jos sen diagonaalin alapuolella on vain nollia; vastaavasti määritellään *alakolmiomatriisi*.

Lause 4.3.1 Olkoon α skalaari ja matriisit A, B ja C sellaisia, että seuraavassa esiintyvät laskutoimitukset ovat järjellisiä. Silloin

(M1) $(A^T)^T = A$

(M2) $(\alpha A)^T = \alpha A^T$

(M3) $(A + B)^T = A^T + B^T$

(M4) $(AB)^T = B^T A^T$

(M5) $A + B = B + A$

(M6) $(A + B) + C = A + (B + C)$

(M7) $(AB)C = A(BC)$

(M8) $A(B + C) = AB + AC$

(M9) $(A + B)C = AC + BC$

(M20) $(\alpha\beta)A = \alpha(\beta A)$

(M11) $\alpha(AB) = (\alpha A)B = A(\alpha B)$

(M12) $(\alpha + \beta)A = \alpha A + \beta A$

(M13) $\alpha(A + B) = \alpha A + \alpha B$

4.4 Totuusarvo- ja kokonaislukumatriisit

Esimerkiksi relaatioiden yhteydessä (ks. Luku 5) on luonnollista käyttää totuusarvoista 1 ja 0 (tai *TOSI* $=$ *TRUE* ja *EPÄTOSI* $=$ *FALSE*) koostuvia matriiseja ja verkkojen yhteydessä totuus- tai kokonaislukumatriiseja. Nämä saadaan valitsemalla $\mathbf{X} := \{0, 1\}$ (tai $\mathbf{X} := \{T, E\}$) ja $\mathbf{X} := \mathbb{N}_0$.

Totuusarvojen tapauksessa lasketaan Boolen aritmetiikalla, jossa $+$ vastaa logiikan $\vee$-operaatiota ja $\cdot$ logiikan $\wedge$-operaatiota:

$$0+0=0,\ 0+1=1+0=1,\ 1+1=1,\ 0\cdot 0=0\cdot 1=1\cdot 0=0,\ 1\cdot 1=1,$$

eli taulukkoina

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Totuusarvomatriiseilla voidaan laskea muodollisesti samalla tavalla kuin on esitetty Luvussa 4.2, kuitenkin käyttäen nyt Boolen operaatioita.

Esimerkki 4.4.1 Totuusarvomatriisien alkioittainen Boolen summa ja tulo:

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

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

Esimerkki 4.4.2 Totuusarvomatriisien Boolen matriisitulo:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1{\cdot}0+0{\cdot}1+1{\cdot}1+0{\cdot}1 & 1{\cdot}0+0{\cdot}1+1{\cdot}0+0{\cdot}1 \\ 0{\cdot}0+1{\cdot}1+1{\cdot}1+0{\cdot}1 & 0{\cdot}0+1{\cdot}1+1{\cdot}0+0{\cdot}1 \end{pmatrix}$$

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

Verkkojen tapauksessa lasketaan normaalisti kokonaisluvuilla. Jos myös totuusarvotapauksessa $\mathbf{X} = \{0, 1\}$ käytetään kokonaislukujen laskutoimituksia, on matriisien laskutoimitusten tulokset redusoitava nk. *etumerkkifunktioilla* (funktion käsite: Määritelmä 5.7.1). Määritellään reaalifunktio $\mathrm{sign} : \mathbb{R} \to \{-1, 0, 1\}$,

$$\mathrm{sign}(x) := \begin{cases} +1, & \text{kun } x > 0 \\ 0, & \text{kun } x = 0 \\ -1, & \text{kun } x < 0 \end{cases}$$

ja matriisifunktio $\mathrm{SIGN} : \mathbb{R}^{m\times n} \to \{-1, 0, 1\}^{m\times n}$,

$$\mathrm{SIGN}\Big((a_{ij})_{m\times n}\Big) := \Big(\mathrm{sign}(a_{ij})\Big)_{m\times n}$$

Esimerkki 4.4.3 Funktio SIGN toimii seuraavaan tapaan:

$$\mathrm{SIGN}\begin{pmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$$

Esimerkki 4.4.4 Esimerkissä 4.4.2 saataisiin kokonaislukuaritmetiikalla

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Oikea tulos saadaan tästä ottamalla SIGN.

5 RELAATIOT JA FUNKTIOT

Tässä luvussa tarkastellaan tulojoukkojen osajoukkoja, nk. relaatioita, mm. relaatioiden yhdistämistä ja erilaisia relaatiotyyppejä.

5.1 Yleinen tulojoukko

Määrittelemme *järjestetyn parin* sulkeissa olevana jonona (x, y), jolle

$$[(x, y) = (u, v)] \Leftrightarrow [x = u \text{ ja } y = v]$$

Järjestetyn parin alkiot ovat siis määrätyssä järjestyksessä. Jos järjestetyn parin alkiot vaihtavat paikkaa keskenään, ei järjestetty pari välttämättä ole enää sama kuin alkuperäinen pari.

Poimitaan tähän tulojoukon eli karteesisen tulon määritelmät Luvuista 3.3 ja 4.1:

Joukkojen $\mathbf{X}$ ja $\mathbf{Y}$ *karteesinen tulo* eli *tulojoukko* on kaikkien järjestettyjen parien joukko

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

Yleisemmin, äärellisen monen epätyhjän joukon $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \ldots, \mathbf{X}_n$ *n-ulotteinen karteesinen tulo* on järjestettyjen jonojen joukko

$$\prod_{i=1}^{n} \mathbf{X}_i = \mathbf{X}_1\times\mathbf{X}_2\times\cdots\times\mathbf{X}_n := \{\, (x_1, x_2, \ldots, x_n) \mid x_i \in \mathbf{X}_i \,\}$$

Erityisesti merkitään $\mathbf{X}^1 = \mathbf{X}$ ja arvoilla $n > 1$ $\mathbf{X}^n := \underbrace{\mathbf{X}\times\cdots\times\mathbf{X}}_{n \text{ kpl}}$.

Esimerkki 5.1.1 Tyypillisiä tulojoukkoja:

a) Euklidinen taso $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$, jota käytetään perusjoukkona esimerkiksi reaalimuuttujan reaaliarvoisten funktioiden kuvaamisessa graafisesti.

b) Kolmiulotteinen avaruus $\mathbb{R}^3 = \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ soveltuu kahden muuttujan funktioiden esittämiseen; tällöin on oikeastaan kysymys pareista $((x, y), z)$, missä pari $(x, y) \mapsto z$.

c) Kokonaisluvun kymmenjärjestelmäesitys $n_k n_{k-1} \ldots n_2 n_1$ perustuu paikkamerkityksiin, joten esimerkiksi lukua 3527 voitaisiin merkitä myös järjestettynä nelikkona $(3, 5, 2, 7)$.

Tehtävä 5.1.2 Ovatko seuraavat oliot tulojoukon $\mathbb{N}\times\mathbb{Q}\times\mathbb{R}$ alkioita:

a) $(2, 3/5, 0.6)$ b) $(2.2, 3/5, 0.6)$ c) $(0, 3/5, 0.6)$
d) $(2, 3/5, 3/5)$ e) $(3/5, 2/5, 3)$ f) $\{2, 2/5, 3\}$

5.2 Relaation määritelmä

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. Esimerkiksi viinipullon oleminen pöydällä on viinipullon ja pöydän välinen relaatio, ja viinin kaataminen lasiin on pullon, viinin, lasin ja kaatajan välinen relaatio. Tietotekniikka on pullollaan relaatioiden käsittelyä, mm. tietokannoissa ja niiden välillä. Myös sukulaisuussuhteet ovat hyviä esimerkkejä relaatioista.

Määritelmä 5.2.1 Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ epätyhjiä joukkoja. Osajoukkoa $R \subseteq \mathbf{X}\times\mathbf{Y}$ sanotaan joukkojen $\mathbf{X}$ ja $\mathbf{Y}$ väliseksi *relaatioksi*, relaatioksi joukosta $\mathbf{X}$ joukkoon $\mathbf{Y}$ tai lyhyesti relaatioksi joukossa $\mathbf{X}\times\mathbf{Y}$.

Jos $(x, y) \in R$, sanotaan, että x ja y *ovat relaatiossa* R. Merkintä $(x, y) \in R$ korvataan usein merkinnällä xRy tai Rxy. Jos $(x, y) \notin R$, tätä merkitään joskus myös $x \not R\, y$.

Jos $R \subseteq \mathbf{X}\times\mathbf{X}$, sanotaan lyhyesti, että R on relaatio joukossa $\mathbf{X}$.

Vastaavaan tapaan määritellään *n-paikkainen relaatio* $R \subseteq \mathbf{X}_1\times\mathbf{X}_2\times\cdots\times\mathbf{X}_n$.

Karteesisen tulon alkion kuuluminen relaatioon R ilmaistaan merkinnöillä

kaksipaikkaisessa:	$xRy, Rxy, R(x, y), (x, y) \in R, \ldots$
kolmipaikkaisessa:	$Rxyz, R(x, y, z), (x, y, z) \in R, \ldots$
$\vdots$	
n-paikkaisessa:	$Rx_1x_2\ldots x_n, R(x_1, x_2, \ldots, x_n), (x_1, x_2, \ldots, x_n) \in R$

Kaksipaikkainen eli *binäärinen relaatio* R joukossa $\mathbf{X}\times\mathbf{Y}$ on Määritelmän 5.2.1 mukaan niiden järjestettyjen parien $(x, y) \in \mathbf{X}\times\mathbf{Y}$ joukko, joita liittää yhteen sääntö R, ts.

$$R = \{\, (x, y) \in \mathbf{X}\times\mathbf{Y} \mid x \text{ ja } y \text{ liittyvät toisiinsa } R\text{:n ilmaisemalla tavalla} \,\}$$

Tarkastelemme tässä pääasiassa kaksipaikkaisia relaatioita. Tietyt tarkastelut voidaan helposti laajentaa koskemaan myös useampipaikkaisia relaatioita.

Esimerkki 5.2.2 Jokaisessa tulojoukossa $\mathbf{X}\times\mathbf{Y}$ on ainakin triviaalit relaatiot

a) *universaalirelaatio* $\mathbb{V} := \mathbf{X}\times\mathbf{Y}$.

b) *tyhjä relaatio* $\Lambda := \emptyset$, jossa ei ole yhtään alkiota.

Universaalirelaatio joukossa $\mathbf{X}\times\mathbf{Y}$ vallitsee kaikkien parien $(x, y) \in \mathbf{X}\times\mathbf{Y}$ välillä. Joukko-opillisesti $\Lambda = \overline{\mathbb{V}}$ ja $\mathbb{V} = \overline{\Lambda}$.

Esimerkki 5.2.3 Valitaan $\mathbf{X} = \mathbf{Y} := \mathbb{R}$. Relaatio $P =$ ”olla aidosti pienempi kuin” joukossa $\mathbb{R}$ merkitään täsmällisesti seuraavalla tavalla:

$$\begin{aligned} P &= \{\,(a,b) \in \mathbb{R}^2 \mid a \text{ on aidosti pienempi kuin } b\,\} \\ &= \{\,(a,b) \in \mathbb{R}^2 \mid a < b\,\}. \end{aligned}$$

Kun nyt halutaan esimerkiksi ilmoittaa, että z on pienempi kuin Z, voidaan tämä tehdä merkitsemällä $(z, Z) \in P$, tai zPZ, tai $P(z, Z)$, tai PzZ. Koska kyseessä oli tuttu relaatio ’$<$’, voidaan käyttää myös suoraa merkintää

$$< = \{\,(a,b) \in \mathbb{R}^2 \mid a \text{ on aidosti pienempi kuin } b\,\}.$$

Relaatioon $<$ kuuluvat esimerkiksi alkiot $(2, 5)$ ja $(-2.3, 5)$, mutta siihen eivät kuulu esimerkiksi alkiot $(-2.3, -5.1)$ ja $(2, 2)$.

Esimerkki 5.2.4 Valitaan $\mathbf{X} = \mathbf{Y} := \mathbb{N}$ ja asetetaan

$$\leq := \{\,(m,n) \in \mathbb{N}^2 \mid m \text{ on pienempi tai yhtä suuri kuin } n\,\}.$$

Silloin $\leq$ on relaatio luonnollisten lukujen joukossa $\mathbb{N}$, nk. *järjestysrelaatio* (ks. Määritelmä 5.9.3). Relaatioon $\leq$ kuuluvat esimerkiksi alkiot $(2, 5)$ ja $(3, 3)$, mutta eivät $(-2.3, -2.3)$ ja $(5, 2)$.

Esimerkki 5.2.5 Tarkastellaan relaatiota R, jonka määrittelee

$$[\,xRy\,] \;\Leftrightarrow\; [\text{”}x \text{ on luvun } y \text{ tekijä”}\,]$$

joukossa $\mathbf{X} = \{2, 3, 5, 6\}$. Tällöin $2R2$, $2R6$, $3R3$, $3R6$, $5R5$ ja $6R6$, ja relaatio R on joukko

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

R on siis joukon $\mathbf{X}\times\mathbf{X}$ aito osajoukko.

Esimerkki 5.2.6 Valitaan $\mathbf{X} := \{\text{naiset}\}$ ja $\mathbf{Y} := \{\text{miehet}\}$. Silloin joukko

$$R := \{\,(N, M) \in \mathbf{X}\times\mathbf{Y} \mid N \text{ ja } M \text{ olleet joskus aviossa}\,\}$$

on relaatio joukossa $\mathbf{X}\times\mathbf{Y}$.

Esimerkki 5.2.7 Tasossa yksikköympyrän sisäosan muodostava joukko

$$D := \{\,(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\,\}$$

on relaatio joukossa $\mathbb{R}^2$, samoin ympyrän kehä $\{\,(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\,\}$.

Tehtävä 5.2.8 Keksi ehtomuotoinen esitys (ks. Luku 3.1) joukkojen

$$\mathbf{X} := \{1, 2, 3\} \quad \text{ja} \quad \mathbf{Y} := \{4, 5, 6\}$$

väliselle relaatiolle $R := \{(1, 5), (2, 6)\}$.

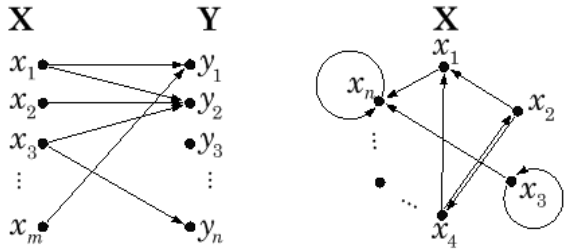
Relaation esitystapoja

Alkeellisin tapa esittää relaatio on luetella sen alkiot tai esittää riippuvuus jollakin kaavalla tai muulla sitovalla ehdolla. On olemassa lukuisia muitakin tapoja esittää relaatioita. Jotkut esitystavat on tarkoitettu havainnollistamaan itse relaatiota, jotkut taas helpottamaan tai mekanisoimaan niiden käsittelyä. Olkoot

$$\mathbf{X} = \{x_1, x_2, \ldots, x_n\}, \quad \mathbf{Y} = \{y_1, y_2, \ldots, y_m\}$$

ja $R \subseteq \mathbf{X} \times \mathbf{Y}$ relaatio. Seuraavassa esitellään relaation esittämiseen sopivia havainnollisia ja laskennallisia tapoja.

1. *Nuolikaaviona*, missä nuoli $x_i \longrightarrow y_j$ tarkoittaa, että $x_i R y_j$. Jos $\mathbf{X} = \mathbf{Y}$, voidaan relaatio esittää myös suunnattuna verkkona (ks. Luku 13). Kuvassa 5 näet nämä kahdentyyppiset esitystavat.



Kuva 5: Nuolikaavioesityksiä relaatioille joukoissa $\mathbf{X} \times \mathbf{Y}$ ja $\mathbf{X} \times \mathbf{X}$

2. *Taulukkona* (ks. Kuva 6), jonka kohdassa (x_i, y_j) on luku 1, jos $x_i R y_j$, muutoin luku 0.

R	y_1	y_2	$\cdots$	y_n
x_1	1	1	$\cdots$	0
x_2	0	1	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_m	0	0	$\cdots$	0

Kuva 6: Relaation ilmaiseminen taulukon avulla

3. *Matriisina*

$$M_R = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = \begin{array}{c} \mathbf{X}\backslash\mathbf{Y} \\ x_1 \\ x_2 \\ \vdots \\ x_m \end{array} \begin{array}{c} \begin{array}{cccc} y_1 & y_2 & \cdots & y_n \end{array} \\ \begin{pmatrix} 1 & 1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \end{array},$$

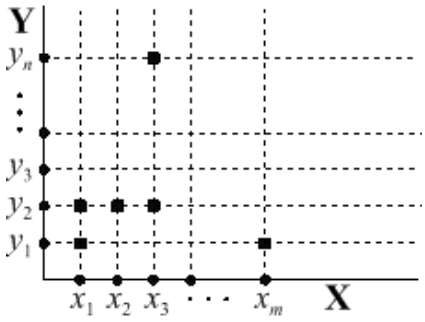
missä $a_{ij} = \chi_R(x_i, y_j)$.

4. Käyttäen *karakteristista funktiota* $\chi_R : \mathbf{X}\times\mathbf{Y} \to \{0, 1\}$,

$$\chi_R(x, y) := \begin{cases} 1, & \text{jos } xRy \\ 0, & \text{jos } x\not{R}\, y \end{cases}$$

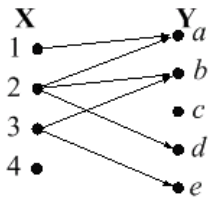
vrt. Luku 9.

5. *Koordinaatistokaaviona* samaan tapaan kuin yhden muuttujan reaalifunktioiden esittäminen tasossa. Muodostetaan perusjoukkoja $\mathbf{X}$ ja $\mathbf{Y}$ kannatteleva koordinaatisto, jonka akseleille joukkojen alkiot asetellaan sopiviin paikkoihin (vaikka niiden ei tarvitsekaan olla lukuja). Jotta tämä olisi yhteensopiva tutun reaalifunktioiden esittämisen kanssa, kannattaa asettaa ensimmäisen joukon $\mathbf{X}$ alkiot vaaka-akselille ja joukon $\mathbf{Y}$ alkiot pystyakselille. Kuvassa 7 relaation alkioita on kuvattu mustilla neliöillä.



Kuva 7: Relaation koordinaatistoesitys

Esimerkki 5.2.9 Kuvassa 8 on esitetty eräs joukkojen $\mathbf{X} := \{1, 2, 3, 4\}$ ja $\mathbf{Y} := \{a, b, c, d, e\}$ välinen relaatio R nuolikaaviona.



Kuva 8: Esimerkin 5.2.9 nuolikaavio

Muodostetaan sille muut esitysmuodot 2-5.

Taulukkoesitys

R	a	b	c	d	e
1	1	0	0	0	0
2	1	1	0	1	0
3	0	1	0	0	1
4	0	0	0	0	0

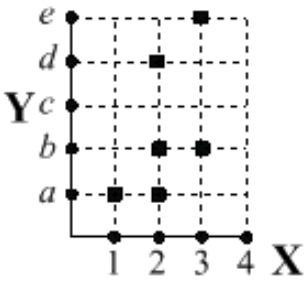
Matriisiesitys

$$R \quad \begin{matrix} a & b & c & d & e \end{matrix}$$
$$\begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Karakteristisen funktion avulla

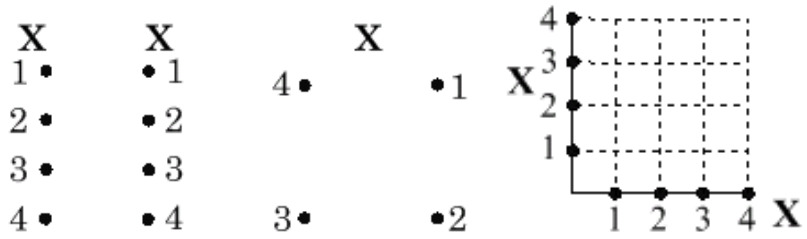
$$\begin{array}{llll} \chi_R(1,a) = 1 & \chi_R(2,a) = 1 & \chi_R(3,a) = 0 & \chi_R(4,a) = 0 \\ \chi_R(1,b) = 0 & \chi_R(2,b) = 1 & \chi_R(3,b) = 1 & \chi_R(4,b) = 0 \\ \chi_R(1,c) = 0 & \chi_R(2,c) = 0 & \chi_R(3,c) = 0 & \chi_R(4,c) = 0 \\ \chi_R(1,d) = 0 & \chi_R(2,d) = 1 & \chi_R(3,d) = 0 & \chi_R(4,d) = 0 \\ \chi_R(1,e) = 0 & \chi_R(2,e) = 0 & \chi_R(3,e) = 1 & \chi_R(4,e) = 0 \end{array}$$

Koordinaatistoesityksenä



Kuva 9: Esimerkin 5.2.9 koordinaatistoesitys

Tehtävä 5.2.10 Olkoon $\mathbf{X} := \mathbf{Y} = \{1, 2, 3, 4\}$ ja $\leq$ kokonaislukujen tavallinen suuruusjärjestys. Piirrä relaatiolle $\leq$ nuolikaavio-, verkko- ja koordinaatistoesitys Kuvaan 10.



Kuva 10: Tehtävän 5.2.10 kuvio

Määritä myös karakteristisen funktion arvot

$\chi_R(1,1) =$	$\chi_R(2,1) =$	$\chi_R(3,1) =$	$\chi_R(4,1) =$
$\chi_R(1,2) =$	$\chi_R(2,2) =$	$\chi_R(3,2) =$	$\chi_R(4,2) =$
$\chi_R(1,3) =$	$\chi_R(2,3) =$	$\chi_R(3,3) =$	$\chi_R(4,3) =$
$\chi_R(1,4) =$	$\chi_R(2,4) =$	$\chi_R(3,4) =$	$\chi_R(4,4) =$

5.3 Relaatioiden joukko-opilliset operaatiot

Koska relaatiot ovat joukkoja, niitä voidaan vertailla ja yhdistellä normaaliin tapaan joukko-opillisin operaatioin. Karakterisoidaan ne tässä relaatio-opillisin keinoin ja samlla esitellään niille logiikan mukaiset nimitykset.

Lause 5.3.1 Olkoot R ja $S \subseteq \mathbf{X}\times\mathbf{Y}$ relaatioita.

a) Relaatio R on relaation S osajoukko, siis $R \subseteq S$, jos ja vain jos on voimassa ehto

$$[\, xRy \,] \;\Rightarrow\; [\, xSy \,].$$

b) Relaatiot ovat joukkoina *samat* eli *identtiset* (merkitään $R = S$) jos ja vain jos $R \subseteq S$ ja $S \subseteq R$.

Lause 5.3.2 Olkoot R ja $S \subseteq \mathbf{X}\times\mathbf{Y}$ relaatioita.

a) Relaation R komplementti $\overline{R}$ karakterisoituu ehdolla

$$[\, x\overline{R}y \,] \;\Leftrightarrow\; [\, xRy \text{ ei päde} \,].$$

b) Relaatioiden R ja S *tulo* $R \cdot S$ on

$$R \cdot S = \{\, (x,y) \in \mathbf{X}\times\mathbf{Y} \mid xRy \text{ ja } xSy \},$$

ja se on sama kuin joukko-opillinen leikkaus $R \cap S$.

b) Relaatioiden R ja S *summa* $R + S$ on

$$R + S = \{\, (x,y) \in \mathbf{X}\times\mathbf{Y} \mid xRy \text{ tai } xSy \},$$

ja se on sama kuin joukko-opillinen yhdiste $R \cup S$.

Universaalirelaatio ja tyhjä relaatio ovat relaatio- ja joukko-opillisesti toistensa komplementteja, $\mathbb{V} = \overline{\Lambda}$ ja $\Lambda = \overline{\mathbb{V}}$.

Tehtävä 5.3.3 Karakterisoi kahden relaation joukko-opillinen erotus relaatiokielellä Lauseen 5.3.2 tapaan.

5.4 Relaation osapuolet, kuvat ja alkukuvat

Nimetään aluksi relaation osapuolet ja joukot, joiden kanssa tietty alkio tai joukko on relaatiossa.

Määritelmä 5.4.1 Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ epätyhjiä joukkoja. Relaatiossa $R \subseteq \mathbf{X}\times\mathbf{Y}$ ensimmäistä joukkoa $\mathbf{X}$ sanotaan relaation *lähtöjoukoksi* ja sen alkioita *riippumattomiksi muuttujiksi*. Vastaavasti jälkimmäistä joukkoa $\mathbf{Y}$ sanotaan relaation *maalijoukoksi* ja sen alkioita *riippuviksi muuttujiksi*. Sanomme myös, että relaation *suunta* on joukosta $\mathbf{X}$ joukkoon $\mathbf{Y}$.

Näitä nimityksiä on totuttu käyttämään erityisesti funktioiden yhteydessä. On syytä korostaa heti, että relaatiolla *määrittelyjoukko* ja *lähtöjoukko* eivät suinkaan ole sama asia (ks. Luku 5.7).

Esimerkki 5.4.2 Joukosta

$$R := \{\, (2,2), (2,4), (2,6), (3,6) \,\}$$

tulee relaatio ainakin seuraavilla valinnoilla:

a) Lähtöjoukko ja maalijoukko ovat $\mathbf{X} := \{1,2,3,4,5,6\}$; silloin $R \subseteq \mathbf{X}\times\mathbf{X}$. Myöskin tätä laajemmat joukot kelpaavat.

b) Lähtöjoukko on $\mathbf{X} := \{2,3\}$ ja maalijoukko $\mathbf{Y} := \{2,4,6\}$. Nämä ovat suppeimmat kelvolliset joukot, joille $R \subseteq \mathbf{X}\times\mathbf{Y}$, ja siis on relaatio.

Tehtävä 5.4.3 Mitkä seuraavista joukoista sopivat joukon R,

$$R := \{\, (2,2), (2,4), (2,6), (3,6) \,\}$$

lähtö- ja maalijoukoiksi $\mathbf{X}$ ja $\mathbf{Y}$ (ks. myös Esimerkki 5.4.2):

1) $\mathbf{X} := \{1,2,3\}$ ja $\mathbf{Y} := \{1,2,4,6\}$.

2) $\mathbf{X} := \{2,3,4\}$ ja $\mathbf{Y} := \{3,4,5,6\}$.

3) $\mathbf{X} := \{-1,2,3\}$ ja $\mathbf{Y} := \mathbb{R}$.

4) $\mathbf{X} := \mathbb{N}$ ja $\mathbf{Y} := \mathbb{Q}$.

Monesti relaation lähtöjoukossa ja maalijoukossa on alkioita, jotka eivät lainkaan esiinny itse relaation alkiopareissa. Joskus nämä voidaan jättää kokonaan huomiotta (esimerkiksi poistamalla lähtö- tai maalijoukosta), mutta toisinaan ne vaikuttavat olennaisesti relaation ominaisuuksiin (esimerkiksi refleksiivisyys ja funktio-ominaisuus).

Usein tarvitaan poimia relaatiosta osia tai selvittää alkioihin tai osajoukkoihin liittyvät jäsenet.

Määritelmä 5.4.4 Olkoon $R \subseteq \mathbf{X}\times\mathbf{Y}$ relaatio. Lähtöjoukon osajoukon $A \subseteq \mathbf{X}$ *kuvajoukko* relaatiossa R on maalijoukon osajoukko

$$R(A) := \{\, y \in \mathbf{Y} \mid (x, y) \in R \text{ jollakin } x \in A \,\}.$$

Vastaavasti maalijoukon osajoukon $B \subseteq \mathbf{Y}$ *alkukuvajoukko* on lähtöjoukon osajoukko

$$R^{-1}(B) := \{\, x \in \mathbf{X} \mid (x, y) \in R \text{ jollakin } y \in B \,\}.$$

Erityisesti lähtöjoukon alkion $x \in \mathbf{X}$ kuvajoukko on

$$R(x) := R(\{x\}) = \{\, y \in \mathbf{Y} \mid (x, y) \in R \,\}$$

ja maalijoukon alkion $y \in \mathbf{Y}$ alkukuvajoukko

$$R^{-1}(y) := R^{-1}(\{y\}) = \{\, x \in \mathbf{X} \mid (x, y) \in R \,\}.$$

Koko lähtöjoukon kuvajoukko $R(\mathbf{X})$ on relaation *arvojoukko* ja koko maalijoukon alkukuvajoukko $R^{-1}(\mathbf{Y})$ on relaation *määrittelyjoukko*.

Esimerkki 5.4.5 Joukon $\mathbf{X} := \{1, 2, 3, 4, 5, 6\}$ relaatiossa (ks. myös Esimerkki 5.4.2 ja Tehtävä 5.4.3)

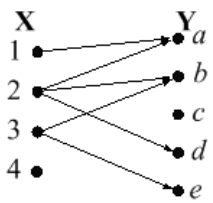
$$R = \{(2, 2), (2, 4), (2, 6), (3, 6)\}$$

alkion 2 kuvajoukko $R(2) = \{2, 4, 6\}$ ja alkion 2 alkukuvajoukko $R^{-1}(2) = \{2\}$.

Joukon $\{1, 2\}$ kuvajoukko on $\{2, 4, 6\}$ ja joukon $\{3, 4, 5\}$ kuvajoukko on $\{6\}$.

Joukon $\{1, 2, 3\}$ alkukuvajoukko on $\{2\}$ ja joukon $\{5, 6\}$ alkukuvajoukko $\{2, 3\}$. Joukon $\{1, 3, 5\}$ alkukuvajoukko on $\emptyset$.

Esimerkki 5.4.6 Kuvassa 11 on esitetty eräs joukkojen $\mathbf{X} := \{1, 2, 3, 4\}$ ja $\mathbf{Y} := \{a, b, c, d, e\}$ välinen relaatio R (ks. myös Esimerkki 5.2.9).



Kuva 11: Esimerkin 5.4.6 kaavio

Lähtöjoukon $\mathbf{X}$ alkioiden kuvajoukot ovat:

$R(1) = \{a\}$, $R(2) = \{a, b, d\}$, $R(3) = \{b, e\}$, $R(4) = \emptyset$.

Maalijoukon $\mathbf{Y}$ alkioiden alkukuvajoukot ovat:

$R^{-1}(a) = \{1, 2\}$, $R^{-1}(b) = \{2, 3\}$, $R^{-1}(c) = \emptyset$, $R^{-1}(d) = \{2\}$, $R^{-1}(e) = \{3\}$.

Edelleen esimerkiksi

$$\begin{aligned}
R(\{2,3\}) &= R(\{1,2,3\}) = R(\mathbf{X}) = \{a,b,d,e\} \\
R(\{1,4\}) &= R(1) = \{a\} \\
R(\{1,2\}) &= R(\{1,2,4\}) = \{a,b,d\} \\
R^{-1}(\{a,b\}) &= R^{-1}(\{a,b,c\}) = R^{-1}(\{a,b,c,d\}) = R^{-1}(\mathbf{Y}) = \{1,2,3\} \\
R^{-1}(\{b,c\}) &= R^{-1}(\{b,c,d\}) = R^{-1}(\{b,c,d,e\}) = R^{-1}(\{d,e\}) = \{2,3\}.
\end{aligned}$$

Tehtävä 5.4.7 Relaation

$$C := \{\, (x, y) \in \mathbb{R}^2 \mid x \geq 0,\ x^2 + y^2 = 1 \,\}$$

lähtö- ja maalijoukot ovat $\mathbb{R}$.

a) Määritä alkioiden 0, $1/2$, 1 ja 2 kuvajoukot.

b) Määritä alkioiden 0, $1/2$, 1 ja 2 alkukuvajoukot.

c) Mitkä olisivat suppeimmat mahdolliset lähtö- ja maalijoukot, joilla $\mathbb{R}$ voitaisiin korvata niin, että C pysyisi samana joukkona?

Tehtävä 5.4.8 Määritä Esimerkin 5.4.6 (Kuva 11) tapauksessa

a) joukon $\{a, d\}$ alkukuvan kuvajoukko.

b) alkion 2 kuvajoukon alkukuvajoukko.

5.5 Käänteisrelaatio ja relaatioiden yhdistäminen

Tutustutaan seuraavaksi relaatioiden kääntämiseen ja yhdistämiseen sekä todistetaan pari näitä koskevaa perustulosta.

Määritelmä 5.5.1 Relaation $R \subseteq \mathbf{X}\times\mathbf{Y}$ *käänteisrelaatio* on joukko

$$R^{-1} := \{\, (y,x) \in \mathbf{Y}\times\mathbf{X} \mid (x,y) \in R \,\}.$$

Relaatio ja käänteisrelaatio toteuttavat ehdon

$$xRy \;\Leftrightarrow\; yR^{-1}x,$$

ts. relaatioissa on samat parit mutta käänteisessä järjestyksessä; relaation suunta on vaihtunut.

Esimerkki 5.5.2 a) Relaatiosta $\leq$ saadaan kääntämällä relaatio $\geq = \leq^{-1}$. Siis $x \leq y \equiv y \leq^{-1} x \equiv y \geq x$.

b) Olkoon A kaikkien suomalaisten kirjainten aakkosjärjestystä kuvaava relaatio, siis

$$\alpha A \beta \;\Leftrightarrow\; \text{"}\alpha \text{ on ennen kirjainta } \beta\text{"}.$$

Tällöin A^{-1} tarkoittaa käänteistä aakkosjärjestystä, ts. $\alpha A^{-1}\beta$ tarkoittaa "α on kirjaimen β jälkeen".

Esimerkki 5.5.3 Edellä oli jo merkitty alkion kuvajoukkoa $R(x)$ ja alkukuvajoukkoa $R^{-1}(y)$. Koska

$$R(x) = \{\, y \in \mathbf{Y} \mid (x,y) \in R \,\} = \{\, y \in \mathbf{Y} \mid (y,x) \in R^{-1} \,\} = (R^{-1})^{-1}(x),$$

voidaan aavistella, että $R = (R^{-1})^{-1}$.

Lause 5.5.4 Jokaiselle relaatiolle R on $R = (R^{-1})^{-1}$.

Todistus. Olkoon $R \subseteq \mathbf{X}\times\mathbf{Y}$ mielivaltainen relaatio. Sen käänteisrelaatio $R^{-1} \subseteq \mathbf{Y}\times\mathbf{X}$, ja edelleen sen käänteisrelaatio $(R^{-1})^{-1} \subseteq \mathbf{X}\times\mathbf{Y}$. Siis R ja $(R^{-1})^{-1}$ ovat saman perusjoukon $\mathbf{X}\times\mathbf{Y}$ osajoukkoja. Sen, että joukot ovat samat, osoittaa lasku

$$(x,y) \in R \;\Leftrightarrow\; xRy \;\Leftrightarrow\; yR^{-1}x \;\Leftrightarrow\; x(R^{-1})^{-1}y \;\Leftrightarrow\; (x,y) \in (R^{-1})^{-1}.$$

■

Määritelmä 5.5.5 Joukon $\mathbf{X}\times\mathbf{X}$ *yksikkö-* eli *identtisyysrelaatio* on diagonaali

$$\Delta_{\mathbf{X}} := \{\, (x,x) \mid x \in \mathbf{X} \,\}.$$

Määritelmä 5.5.6 Relaatioiden $R \subseteq \mathbf{X}\times\mathbf{Y}$ ja $S \subseteq \mathbf{Y}\times\mathbf{Z}$ *yhdistetty relaatio* eli *kompositio* tai *suhteellinen tulo* on relaatio

$$S \circ R := \{\, (x,z) \in \mathbf{X}\times\mathbf{Z} \mid \text{ jollekin } y \in \mathbf{Y} :\ xRy \text{ ja } ySz \,\}.$$

Huomautus 5.5.7 a) Joukkojen $\mathbf{X}$ ja $\mathbf{Z}$ välille voi siis syntyä relaatio välittävien alkioiden $y \in \mathbf{Y}$ avulla.

b) Jos $R \subseteq \mathbf{X}\times\mathbf{Y}$, niin $R^{-1} \circ R \subseteq \mathbf{X}\times\mathbf{X}$ ja $R \circ R^{-1} \subseteq \mathbf{Y}\times\mathbf{Y}$.

c) Yksikkörelaatio $\Delta_{\mathbf{X}}$ vastaa matriisien avaruuden kertolaskun neutraalialkiota I ja kuvausten avaruuden identtistä kuvausta $\mathrm{Id}(x) := x$ (ks. Luku 5.7).

Nimittäin, jokaiselle $R \subseteq \mathbf{X}\times\mathbf{X}$ on (harjoitustehtävä)

$$\Delta_{\mathbf{X}} \circ R = R \circ \Delta_{\mathbf{X}} = R.$$

Esimerkki 5.5.8 Ihmisten joukossa relaatio

”henkilö x on henkilön z setä”

on relaatioiden ”henkilö x on henkilön y veli” ja ”henkilö y on henkilön z isä” suhteellinen tulo, sillä x on henkilön z setä, jos ja vain jos on (tai on ollut) olemassa sellainen henkilö y, että henkilö x on y:n veli ja y on henkilön z isä.

Tehtävä 5.5.9 Olkoot $\mathbf{X} := \{1,2,3\}$, $\mathbf{Y} := \{a,b,c\}$ ja $\mathbf{Z} := \{\alpha,\beta\}$. Piirrä seuraavaan kuvioon nuolet, jotka kuvaavat relaatioita

$$R := \{(1,a),(1,b),(2,b),(2,c),(3,a)\}, \quad S := \{(b,\alpha),(c,\alpha),(c,\beta)\}$$

ja relaatioita $S \circ R$ sekä R^{-1}:

$\mathbf{X}$	R	$\mathbf{Y}$	S	$\mathbf{Z}$	$\mathbf{X}$	$S \circ R$	$\mathbf{Z}$	$\mathbf{Y}$	R^{-1}	$\mathbf{X}$
1		a			1			a		1
				α			α			
2		b			2			b		2
				β			β			
3		c			3			c		3

Muodosta vielä kyseisten relaatioiden matriisit

$$M_R = \begin{pmatrix} & & \\ & & \end{pmatrix} \qquad M_S = \begin{pmatrix} & \\ & \\ & \end{pmatrix}$$

$$M_{S\circ R} = \begin{pmatrix} & \\ & \end{pmatrix} \qquad M_{R^{-1}} = \begin{pmatrix} & \\ & \end{pmatrix}$$

Lause 5.5.10 Relaatioille $R \subseteq \mathbf{X}\times\mathbf{Y}$ ja $S \subseteq \mathbf{Y}\times\mathbf{Z}$ pätee laskusääntö

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Todistus. $(S \circ R)^{-1}$ ja $R^{-1} \circ S^{-1}$ ovat selvästikin relaatioita joukosta $\mathbf{Z}$ joukkoon $\mathbf{X}$. Seuraava ekvivalenssiketju osoittaa, että relaatiot ovat samat:

$$\begin{aligned}
[\,(z,x) \in (S \circ R)^{-1}\,] &\Leftrightarrow [\,z(S \circ R)^{-1}x\,] \\
&\Leftrightarrow [\,x(S \circ R)z\,] \\
&\Leftrightarrow [\text{jollekin } y \in \mathbf{Y}:\ xRy \text{ ja } ySz\,] \\
&\Leftrightarrow [\text{jollekin } y \in \mathbf{Y}:\ yR^{-1}x \text{ ja } zS^{-1}y\,] \\
&\Leftrightarrow [\text{jollekin } y \in \mathbf{Y}:\ zS^{-1}y \text{ ja } yR^{-1}x\,] \\
&\Leftrightarrow [\,z(R^{-1} \circ S^{-1})x\,] \\
&\Leftrightarrow [\,(z,x) \in (R^{-1} \circ S^{-1})\,].
\end{aligned}$$

□

Lause 5.5.11 Relaatioille $R \subseteq \mathbf{X}\times\mathbf{Y}$, $S \subseteq \mathbf{Y}\times\mathbf{Z}$, $T \subseteq \mathbf{Z}\times\mathbf{V}$ pätee

$$(T \circ S) \circ R = T \circ (S \circ R).$$

Todistus. Koska $T \circ S \subseteq \mathbf{Y}\times\mathbf{V}$ ja $R \subseteq \mathbf{X}\times\mathbf{Y}$, on $(T \circ S) \circ R$ relaatio joukosta $\mathbf{X}$ joukkoon $\mathbf{V}$. Koska $T \subseteq \mathbf{Z}\times\mathbf{V}$ ja $S \circ R \subseteq \mathbf{X}\times\mathbf{Z}$, on myös $T \circ (S \circ R)$ relaatio joukosta $\mathbf{X}$ joukkoon $\mathbf{V}$. Väitteen osoittaa oikeaksi ekvivalenssiketju:

$$\begin{aligned}
[\,x\big((T \circ S) \circ R\big)v\,] &\Leftrightarrow [\text{jollekin } y \in \mathbf{Y}:\ xRy \text{ ja } y(T \circ S)v\,] \\
&\Leftrightarrow [\text{joillekin } y \in \mathbf{Y}, z \in \mathbf{Z}:\ xRy, ySz \text{ ja } zTv\,] \\
&\Leftrightarrow [\text{jollekin } z \in \mathbf{Z}:\ x(S \circ R)z \text{ ja } zTv\,] \\
&\Leftrightarrow [\,x\big(T \circ (S \circ R)\big)v\,].
\end{aligned}$$

□

Huomautus 5.5.12 a) Relaatioiden yhdistäminen ei ole vaihdannainen operaatio. Lauseen 5.5.11 mukaan tulo on kuitenkin liitännäinen, joten voidaan merkitä

$$T \circ S \circ R := (T \circ S) \circ R = T \circ (S \circ R).$$

b) Joukon $\mathbf{X}\times\mathbf{X}$ relaatioiden joukko varustettuna tulolla $\circ$ on algebralliselta rakenteeltaan *puoliryhmä*, jonka neutraalialkio on diagonaali $\Delta_{\mathbf{X}}$. Käänteisrelaatio ei yleensä toteuta *ryhmän käänteisalkiolta* vaadittavia ehtoja

$$R \circ R^{-1} = R^{-1} \circ R = \Delta_{\mathbf{X}},$$

joten kyseessä ei ole ryhmä (vasta bijektiivisten kuvausten joukko on ryhmä).

c) Lauseiden 5.5.10 ja 5.5.11 tuloksia käyttäen voidaan laskea esimerkiksi

$$(T \circ S \circ R)^{-1} = R^{-1} \circ S^{-1} \circ T^{-1}.$$

Joukon sisäiselle relaatiolle voidaan määritellä *potenssit* yhdistämällä sitä itsensä kanssa toistuvasti:

Määritelmä 5.5.13 Relaation $R \subseteq \mathbf{X} \times \mathbf{X}$ n. *potenssi* R^n määritellään luvuille $n \in \mathbb{N}_0$ seuraavasti:

1. $R^0 := \Delta_{\mathbf{X}}$,
2. $R^{n+1} := R^n \circ R$, $n \in \mathbb{N}_0$.

Nyt esimerkiksi $R^3 = (R \circ R) \circ R = R \circ R \circ R$.

Esimerkki 5.5.14 Relaatio ”olla isoisä” on relaation ”olla isä” toinen potenssi, ”olla isoisän isä” kolmas potenssi jne.

Määritelmä 5.5.15 Sanomme, että R-*ketju* vallitsee alkioiden x ja y välillä, jos niiden välillä vallitsee jokin relaation R potenssi.

Esimerkki 5.5.16 Relaatio ”isänpuoleinen esi-isä” on yleisessä muodossa esitetty R-ketju, kun $R =$ ”isä”.

Tehtävä 5.5.17 Formuloi ”isä”-relaatio tarkemmin, ja kirjoita potenssimuodossa ”isänisänisänisänisänisä”.

5.6 Käänteis- ja tulorelaation matriisit

Tarkastellaan relaatioiden matriisiesityksiä käytettäessä kokonaislukujen laskutoimituksia. Osoitetaan, että relaatioiden kääntäminen ja yhdistäminen voidaan mekanisoida matriisilaskennaksi. Luvussa 4.4 on jo määritelty etumerkkifunktiot $\mathrm{sign} : \mathbb{R} \to \{-1, 0, 1\}$ ja $\mathrm{SIGN} : \mathbb{R}^{m\times n} \to \{-1, 0, 1\}^{m\times n}$.

Lause 5.6.1 Olkoot $R \subseteq \mathbf{X}\times\mathbf{Y}$ ja $S \subseteq \mathbf{Y}\times\mathbf{Z}$ relaatioita. Silloin

a) $M_{R^{-1}} = M_R^T$,

b) $M_{S\circ R} = \mathrm{SIGN}(M_R M_S)$.

Todistus. a) Merkitään $M_R = (a_{ij})$, $M_R^T = (b_{ji})$ ja $M_{R^{-1}} = (b'_{ji})$, jolloin $b_{kl} = a_{lk}$. Koska relaation matriisin alkiot ovat lukuja 1 tai 0, seuraava ekvivalenssiketju todistaa väitteen:

$$[\, b'_{ji} = 1\,] \Leftrightarrow [\, y_j R^{-1} x_i\,] \Leftrightarrow [\, x_i R y_j\,] \Leftrightarrow [\, a_{ij} = 1\,] \Leftrightarrow [\, b_{ji} = 1\,].$$

b) Olkoot

$$\begin{array}{rclcrcl} M_R &=& (a_{ij})_{m\times n}, & & M_S &=& (b_{jk})_{n\times r}, \\ M_{S\circ R} &=& (c_{ik})_{m\times r}, & & M_R M_S &=& (c'_{ik})_{m\times r}, \end{array}$$

missä $c'_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$. Koska $c_{ik} = 0$ tai 1 ja $c'_{ik} \geq 0$, väitteen todistaa päättely

$$\begin{array}{rcl} [\, c_{ik} = 1\,] & \Leftrightarrow & [\, x_i (S \circ R) z_k\,] \\ & \Leftrightarrow & [\,\text{jollakin } y_j \in \mathbf{Y}:\ x_i R y_j, y_j S z_k\,] \\ & \Leftrightarrow & [\,\text{jollakin } j:\ a_{ij} = 1 \text{ ja } b_{jk} = 1\,] \\ & \Leftrightarrow & [\, c'_{ik} > 0\,] \\ & \Leftrightarrow & [\,\mathrm{sign}(c'_{ik}) = 1\,]. \end{array}$$

□

Esimerkki 5.6.2 Tehtävän 5.5.9 relaatioiden matriisit olivat

$$M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad M_S = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$M_{S\circ R} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad M_{R^{-1}} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} = M_R^T.$$

Silloin

$$M_R M_S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 0 \end{pmatrix}.$$

Edelleen voidaan helposti johtaa mm. komplementin, yhdisteen, leikkauksen ja erotuksen matriisien laskukaavat (harjoitustehtävä).

5.7 Kuvaukset eli funktiot

Edellä on jo käytetty funktion käsitettä tutussa muodossaan (etumerkkifunktiot ja karakteristinen funktio). Täsmällinen määrittely ja perusominaisuuksien esittely suoritetaan relaatiotulkinnan avulla.

Määritelmä 5.7.1 Relaatio $F \subseteq \mathbf{X}\times\mathbf{Y}$ on *kuvaus* eli *funktio*, jos seuraavat kaksi ehtoa ovat täytetyt:

1) Jokaista $x \in \mathbf{X}$ kohti on olemassa $y \in \mathbf{Y}$ siten, että xFy.

2) Jos xFy ja xFz, niin $y = z$.

Funktioiden yhteydessä käytetään joitakin erikoismerkintöjä: Jos relaatio F on kuvaus, niin

$F : \mathbf{X} \to \mathbf{Y}$	tarkoittaa	$F \subseteq \mathbf{X}\times\mathbf{Y}$
$F(x) = y$	tarkoittaa	xFy
$x \mapsto F(x)$	tarkoittaa	kuvauksen *sääntöä*

Merkintää $x \mapsto F(x)$ käytetään usein ilmaisemaan pelkkää funktion sisältämää sääntöä, kun määrittelyjoukkoa tai arvojoukkoa ei haluta tai tarvitse ilmaista, tai esimerkiksi muodossa $x \mapsto 2x - 1$, kun itse funktiota ei katsota tarpeelliseksi nimetä.

Jos F on kuvaus $\mathbf{X} \to \mathbf{Y}$ ja $F(x) = y$, sanotaan (kuten osittain jo relaatioiden yhteydessä Luvussa 5.4), että

- y on pisteen x *kuvapiste* eli *arvo* kuvauksessa F
- $\mathbf{X}$ on *lähtöjoukko* ja samalla *määrittelyjoukko*, $\mathbf{Y}$ *maalijoukko*
- $F(A) := \{\, F(x) \mid x \in A \,\}$ on joukon $A \subseteq \mathbf{X}$ *kuvajoukko*

- $F^{-1}(B) := \{\, x \in \mathbf{X} \mid F(x) \in B \,\}$ on joukon $B \subseteq \mathbf{Y}$ *alkukuvajoukko*
- $F(\mathbf{X}) := \{\, F(x) \mid x \in \mathbf{X} \,\}$ on funktion *arvojoukko*
- epätyhjään joukkoon $A \subseteq \mathbf{X}$ liittyvä kuvaus $F|A : A \to \mathbf{Y}$,

  $$(F|A)(x) := F(x), \quad x \in A,$$

  on kuvauksen F *rajoittuma(kuvaus) joukkoon* A
- F on *injektio*, jos se toteuttaa vaatimuksen

  $$F(x_1) = F(x_2) \quad \Rightarrow \quad x_1 = x_2$$

- F on *surjektio*, jos $F(\mathbf{X}) = \mathbf{Y}$
- F on *bijektio*, jos se on injektio ja surjektio
- käänteisrelaatio F^{-1} on *käänteiskuvaus*, mikäli se on kuvaus.

On helppo osoittaa, että kuvauksella $F : \mathbf{X} \to \mathbf{Y}$ on käänteiskuvaus jos ja vain jos F on bijektio. Käänteiskuvaus on myös bijektio.

Jos $F : \mathbf{X} \to \mathbf{Y}$ on injektio, kuvaus $F' : \mathbf{X} \to F(\mathbf{X})$,

$$F'(x) := F(x),$$

– jossa siis on vain rajattu funktion F maalijoukko arvojoukoksi – on bijektio; merkitään edelleen $F = F'$.

Esimerkki 5.7.2 Yksinkertaisuudestaan huolimatta tärkeä työkalu on *identtinen kuvaus* eli *identiteettifunktio* $\mathrm{Id}_{\mathbf{X}} : \mathbf{X} \to \mathbf{X}$,

$$\mathrm{Id}_{\mathbf{X}}(x) := x.$$

Jos $F : \mathbf{X} \to \mathbf{Y}$ on bijektio, niin yhdistetyt kuvaukset ovat identtisiä kuvauksia $F \circ F^{-1} = \mathrm{Id}_{\mathbf{Y}}$ ja $F^{-1} \circ F = \mathrm{Id}_{\mathbf{X}}$.

Esimerkki 5.7.3 Olkoon $f : \mathbb{R} \to \mathbb{R}$ funktio $f(x) := x^2$.

Tällöin f ei ole surjektio, koska kuvien joukko $[0, +\infty[$ on maalijoukon $\mathbb{R}$ aito osajoukko.

Tämä f ei myöskään ole injektio, koska esimerkiksi $f(-1) = (-1)^2 = 1 = 1^2 = f(1)$.

Jos f olisi funktio $f : \mathbb{R}_+ \to \mathbb{R}_+$, olisi se injektio, koska yhtälöstä $u^2 = v^2$ seuraa $u = v$ kaikille positiivisille reaaliluvuille u ja v. Lisäksi f olisi tällöin surjektio, koska kuvajoukko olisi sama kuin arvojoukko $\mathbb{R}_+$.

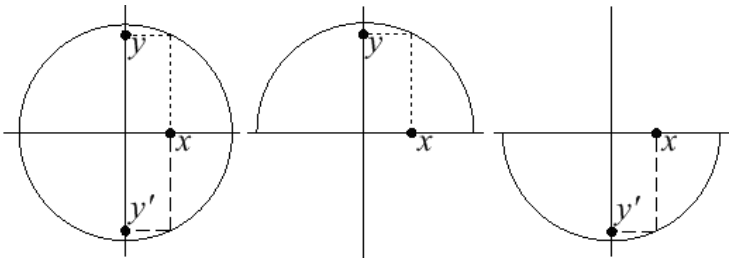
Esimerkki 5.7.4 Esimerkissä 5.2.7 todettiin relaatioksi ympyrän sisus ja kehä

$$D := \{\, (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1 \,\}, \quad C := \{\, (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \,\}.$$

Joukosta D on vaikea kehittää yhden reaalimuuttujan funktiota, mutta kehästä kylläkin. Siinäkin on selvitettävä tarkkaan sopivat lähtö- ja maalijoukot, jotta Määritelmän 5.7.1 määrittely- ja yksikäsitteisyysvaatimukset 1) ja 2) toteutuvat.

Otetaan tarkasteluun ympyrän ylempi puolisko ja rajataan lähtöjoukko reaalivälikSi $I := [-1, 1]$. Koko ympyrän kehä piirtyy ottamalla kaksikäsitteinen sääntö $x \mapsto \pm\sqrt{1 - x^2}$, joka tuottaa kuvapisteet y ja y'.

Valitsemalla vain $x \mapsto +\sqrt{1 - x^2} =: y$ saadaan ylempi puoliympyrä, ja valitsemalla $x \mapsto -\sqrt{1 - x^2} =: y'$ saadaan alempi, ks. Kuva 12.

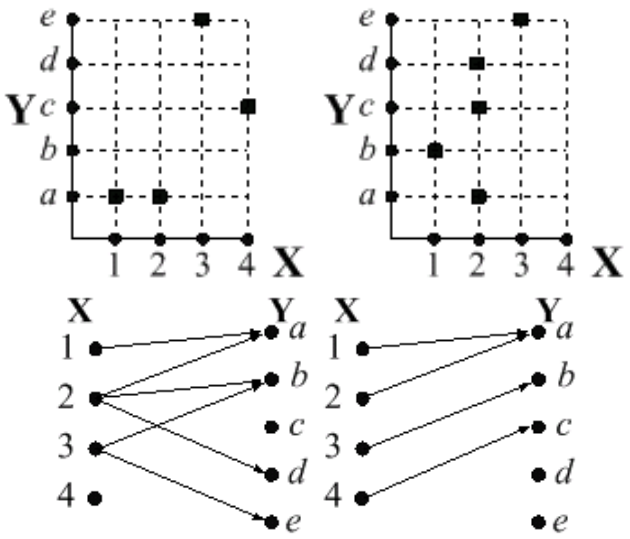


Kuva 12: Ympyrä ja tulkinta reaalifunktioksi

Tehtävä 5.7.5 Mitä tapahtuukaan, jos laajennamme Esimerkissä 5.7.4 määrittelyjoukon vaikkapa väliksi $J := [-2, 2]$ tai jopa koko joukoksi $\mathbb{R}$?

Koska yhden muuttujan funktiot ovat relaatioita, niitä voidaan esittää samoilla keinoin kuin relaatioita, ks. Luku 5.2.

Tehtävä 5.7.6 Missä Kuvan 13 esityksistä on kyseessä funktio?



Kuva 13: Mitkä relaatiot ovat funktioita?

5.8 Laatikko- eli kyyhkyslakkaperiaate

Seuraava tuttu ilmiö, nk. laatikko- eli kyyhkyslakkaperiaate (*the pigeon hole principle*)

> *On käytettävissä m laatikkoa. Jos $n > m$ kappaletta palloja asetetaan noihin laatikoihin, on ainakin yhdessä vähintään 2 palloa.*

voidaan esittää matematiikan kielellä funktion avulla:

Lause 5.8.1 (laatikkoperiaate) Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ äärellisiä joukkoja, joille $\#\mathbf{X} > \#\mathbf{Y}$. Jos $f : \mathbf{X} \to \mathbf{Y}$ on kuvaus, on joukossa $\mathbf{X}$ pistepari $x_1 \neq x_2$, jolle $f(x_1) = f(x_2)$.

Todistus. Määritelmän 10.1.1 mukaan funktio f ei voi olla injektio, joten on olemassa $x_1 \neq x_2$, joille $f(x_1) = f(x_2)$. □

Lauseen 5.8.1 vahvennus, nk. *yleistetty laatikkoperiaate* todistetaan alkukuvan ja summaperiaatteen avulla.

Lause 5.8.2 (yleistetty laatikkoperiaate) Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ äärellisiä joukkoja ja $f : \mathbf{X} \to \mathbf{Y}$ kuvaus. Jos $\#\mathbf{X} > n \cdot \#\mathbf{Y}$, niin $\#(f^{-1}(y)) > n$ jollakin $y \in \mathbf{Y}$.

Todistus. Olkoon $\mathbf{Y} = \{y_1, y_2, \ldots, y_m\}$, $m := \#\mathbf{Y}$ ja $\mathbf{X}_j := f^{-1}(y_j)$ kaikilla $j \in [m]$.

Vastaoletus: $\#\mathbf{X}_j \leq n$ kaikilla $j \in [m]$. Koska f on kuvaus, on

$$\mathbf{X} = \bigcup_{j=1}^{m} \mathbf{X}_j \quad \text{ja} \quad \mathbf{X}_i \cap \mathbf{X}_j = \emptyset$$

kaikilla $i \neq j$, joten summaperiaatteen (Lause 10.2.1) ja vastaoletuksen nojalla

$$\#\mathbf{X} = \#\mathbf{X}_1 + \#\mathbf{X}_2 + \cdots + \#\mathbf{X}_m \leq n \cdot m.$$

Toisaalta oletuksen mukaan $\#\mathbf{X} > n \cdot \#\mathbf{Y}$, mikä johtaa edellisen nojalla ristiriitaan

$$n \cdot m = n \cdot \#\mathbf{Y} < \#\mathbf{X} \leq n \cdot m.$$

□

Esimerkki 5.8.3 Aritmeettinen muotoilu yleistetylle laatikkoperiaatteelle:

Olkoot $n_1, n_2, \ldots, n_k \in \mathbf{N}_0$ lukuja ja

$$\frac{n_1 + n_2 + \cdots + n_k}{k} > n.$$

Silloin ainakin yksi luvuista $n_j > n$, ts. kaikki luvut eivät voi olla aidosti pienempiä kuin niiden keskiarvo.

Esimerkki 5.8.4 Oletetaan, että maapallon valtioiden pääkaupunkien joukon $\mathbf{X}$ kardinaliteetti on 200. Olkoon näissä mahdollisten lämpötilojen joukko eräällä hetkellä $\mathbf{Y} = \{-40°, -39°, \ldots, +39°, +40°\}$. Tavallisen laatikkoperiaatteen (Lause 5.8.1) mukaan kuvaus $f : \mathbf{X} \to \mathbf{Y}$,

$$f : \text{pääkaupunki} \mapsto \text{lämpötila kyseisessä kaupungissa}$$

saa (asteen tarkkuudella) saman arvon ainakin kahdessa kaupungissa. Yleistetyn laatikkoperiaatteen (Lause 5.8.2) nojalla ainakin 3 kaupungissa on sama lämpötila, sillä $n = 2$ on suurin luku, jolle $\#\mathbf{X} = 200 > n \cdot 81 = n \cdot \#\mathbf{Y}$.

5.9 Ekvivalenssi ja järjestys

Kuvaus oli kahden joukon välinen relaatio. Tarkastellaan yhden joukon sisäisiä relaatioita. Nimetään aluksi relaatioiden tärkeimpiä ominaisuuksia (ks. myös Luku 5.10).

Määritelmä 5.9.1 Relaation $R \subseteq \mathbf{X}\times\mathbf{X}$ sanotaan olevan

a) *refleksiivinen*, jos jokaiselle $x \in \mathbf{X}$ on xRx,

b) *symmetrinen*, jos kaikilla $x, y \in \mathbf{X}$ pätee

$$[\, xRy \,] \quad \Rightarrow \quad [\, yRx \,],$$

c) *antisymmetrinen*, jos kaikilla $x, y \in \mathbf{X}$ pätee

$$[\, xRy \ \& \ yRx \,] \quad \Rightarrow \quad [\, x = y \,],$$

d) *transitiivinen*, jos kaikilla $x, y, z \in \mathbf{X}$ pätee

$$[\, xRy \ \& \ yRz \,] \quad \Rightarrow \quad [\, xRz \,],$$

e) *täysi*, jos kaikilla x, $y \in \mathbf{X}$ pätee xRy tai yRx.

Lause 5.9.2 Relaatio $R \subseteq \mathbf{X}\times\mathbf{X}$ on

α) refleksiivinen jos ja vain jos $\Delta_{\mathbf{X}} \subseteq R$,

β) symmetrinen jos ja vain jos $R = R^{-1}$,

γ) antisymmetrinen jos ja vain jos $R \cap R^{-1} \subseteq \Delta_{\mathbf{X}}$,

δ) transitiivinen jos ja vain jos $R \circ R \subseteq R$,

ϵ) täysi jos ja vain jos $R \cup R^{-1} = \mathbf{X}\times\mathbf{X}$.

Todistus. Kohdat α), β) ja ϵ) ovat ilmeisiä. Kohta δ) on harjoitustehtävä. Todistetaan näytteeksi kohta γ).

Olkoon R antisymmetrinen ja $(x, y) \in R \cap R^{-1}$. Silloin on xRy ja yRx, joten antisymmetrisyyden perusteella $x = y$ ja siten $(x, y) \in \Delta_{\mathbf{X}}$.

Olkoon toiseksi $R \cap R^{-1} \subseteq \Delta_{\mathbf{X}}$ ja xRy ja yRx. Silloin $(x, y) \in R \cap R^{-1} \subseteq \Delta_{\mathbf{X}}$, joten $x = y$. Siis R on antisymmetrinen. □

Määritelmä 5.9.3 Relaatio $R \subseteq \mathbf{X}\times\mathbf{X}$ on

a) *ekvivalenssirelaatio*, jos se on refleksiivinen, symmetrinen ja transitiivinen,

b) *kvasijärjestys*, jos se on refleksiivinen ja transitiivinen,

c) *osittainen järjestys*, jos se on refleksiivinen, antisymmetrinen ja transitiivinen,

d) *täydellinen järjestys* eli *totaali järjestys* (tai lyhyesti *järjestys*), jos se on täysi osittainen järjestys.

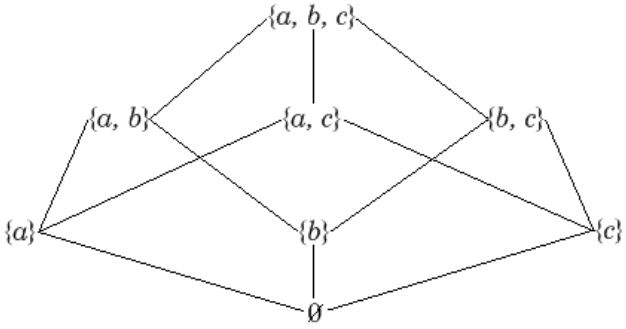
Esimerkki 5.9.4 Yhtäsuuruusrelaatio '$=$' on ekvivalenssi vaikkapa reaalilukujen joukossa.

Esimerkki 5.9.5 Tarkastellaan sukunimellisten ihmisten joukossa relaatiota

$$[\, xSy \,] \;\Leftrightarrow\; [\ \text{"henkilöllä } x \text{ on sama sukunimi kuin henkilöllä } y\text{"}\,].$$

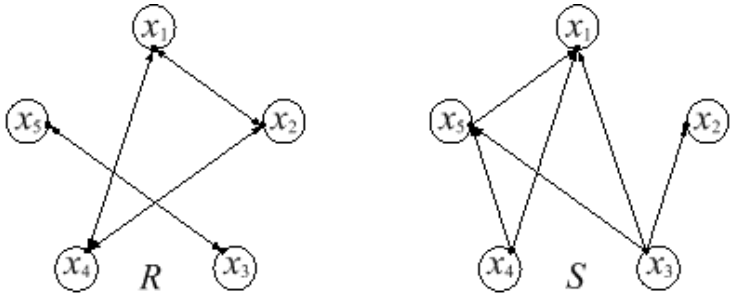
Määritelmän 5.9.3 refleksiivisyysvaatimus on tässä triviaali. Lukija toteaa helposti, että myös symmetrisyys ja transitiivisuus ovat voimassa. Siis S on ekvivalenssirelaatio.

Esimerkki 5.9.6 Inkluusiorelaatio '$\subseteq$' on kvasi- ja osittainen järjestys minkä tahansa joukon $\mathbf{X}$ potenssijoukossa $\mathcal{P}(\mathbf{X})$. Se ei ole totaali, mikäli joukossa on $\mathbf{X}$ on enemmän kuin yksi alkio. Kolmen alkion joukon järjestysrakenne käy ilmi Kuvasta 14.



Kuva 14: Esimerkin 5.9.6 inkluusiorelaatio Hassen kaaviona

Tehtävä 5.9.7 Olkoon $\mathbf{X} := \{x_1, x_2, x_3, x_4, x_5\}$. Mitkä Määritelmien 5.9.1 ja 5.9.3 ominaisuuksista ovat voimassa Kuvan 15 relaatioille R, $S \subseteq \mathbf{X}\times\mathbf{X}$?



Kuva 15: Tehtävän 5.9.7 relaatiot kaavioina

Ratkaisu. R on refleksiivinen, symmetrinen ja transitiivinen, ja siis ekvivalenssi. Se ei ole antisymmetrinen eikä täysi.

S on refleksiivinen, antisymmetrinen ja transitiivinen, ja siis osittainen järjestys. Se ei ole symmetrinen eikä täysi.

Tehtävä 5.9.8 Olkoon $\mathbf{X} := \{x_1, x_2, x_3, x_4, x_5\}$. Mitkä Määritelmien 5.9.1 ja 5.9.3 ominaisuuksista ovat voimassa relaatioille R, $S \subseteq \mathbf{X}\times\mathbf{X}$, joiden matriisit ovat

$$M_R := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad M_S := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Ratkaisu. S on refleksiivinen, symmetrinen ja transitiivinen, ja siis ekvivalenssi. Se ei ole antisymmetrinen eikä täysi.

R on refleksiivinen, antisymmetrinen ja transitiivinen, ja siis osittainen järjestys. Se ei ole symmetrinen eikä täysi.

Huomaa, että Tehtävän 5.9.7 R on sama kuin Tehtävän 5.9.8 S, ja kääntäen.

Perusteellisempi ekvivalenssien tarkastelu on Luvussa 7. Järjestyksiä käsitellään tarkemmin Luvussa 8.

5.10 Muita relaatiotyyppejä

Esitellään Luvussa 5.9 määriteltyjen relaatio-ominaisuuksien lisäksi vielä eräitä muita erityispiirteitä; mukana ovat myös em. ominaisuudet.

Määritelmä 5.10.1 Olkoon $R \subseteq \mathbf{X}\times\mathbf{X}$. Sanotaan, että

(1) R on *refleksiivinen* joukossa $\mathbf{X}$, jos jokaiselle $x \in \mathbf{X}$ on xRx.

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

(3) R on *non-refleksiivinen* joukossa $\mathbf{X}$, jos on olemassa alkio $x \in \mathbf{X}$, jolle xRx, ja on olemassa alkio $y \in \mathbf{X}$, jolle $y\overline{R}y$.

(4) R on *symmetrinen* joukossa $\mathbf{X}$, jos kaikilla $x, y \in \mathbf{X}$ pätee

$$[\,xRy\,] \quad \Rightarrow \quad [\,yRx\,].$$

(5) R on *asymmetrinen* joukossa $\mathbf{X}$, jos jokaiselle alkioparille $x, y \in \mathbf{X}$ pätee

$$[\,xRy\,] \quad \Rightarrow \quad [\,y\overline{R}x\,].$$

(6) R on *non-symmetrinen* joukossa $\mathbf{X}$, jos on olemassa alkiot x, $y \in \mathbf{X}$, joille sekä xRy että yRx, ja on olemassa alkiot $r, s \in \mathbf{X}$, joille rRs mutta $s \not R r$.

(7) R on *antisymmetrinen* joukossa $\mathbf{X}$, jos kaikilla $x, y \in \mathbf{X}$ pätee

$$[\,xRy \;\&\; yRx\,] \quad \Rightarrow \quad [\,x = y\,],$$

(8) R on *transitiivinen* joukossa $\mathbf{X}$, jos kaikilla $x, y, z \in \mathbf{X}$ pätee

$$[\,xRy \;\&\; yRz\,] \quad \Rightarrow \quad [\,xRz\,],$$

(9) R on *intransitiivinen* joukossa $\mathbf{X}$, jos kaikilla $x, y, z \in \mathbf{X}$ pätee

$$[\,xRy \;\&\; yRz\,] \quad \Rightarrow \quad [\,\text{ei ole } xRz\,],$$

(10) R on *non-transitiivinen* joukossa $\mathbf{X}$, jos on olemassa $x, y, z \in \mathbf{X}$, joille xRy, yRz ja xRz, ja on olemassa $r, s, t \in \mathbf{X}$, joille rRs ja sRt mutta $r \not R t$.

(11) R on *yhtenäinen* joukossa $\mathbf{X}$, jos kaikilla x, $y \in \mathbf{X}$, $x \neq y$, pätee xRy tai yRx.

(12) R on *täysi* joukossa $\mathbf{X}$, jos kaikilla x, $y \in \mathbf{X}$ pätee xRy tai yRx.

Tehtävä 5.10.2 Osoita, että jos joukon $\mathbf{X}$ relaatio on non-refleksiivinen, niin joukolla $\mathbf{X}$ on sellainen osajoukko, jossa R on refleksiivinen, sekä sellainen osajoukko, jossa R on irrefleksiivinen.

Esimerkki 5.10.3 Seuraavassa esimerkkejä Määritelmässä 5.10.1 nimetyistä ominaisuuksista. ■

(1) Relaatio $xSy = x \geq y$ on refleksiivinen kokonaislukujen joukossa $\mathbb{Z}$, koska $x \geq x$ kaikilla alkioilla $x \in \mathbb{Z}$.

(2) Relaatio $x\ddot{A}y =$ "x on henkilön y äiti" on irrefleksiivinen ihmisten joukossa, koska kukaan ei ole itsensä äiti.

(3) Relaatio $xNy =$ "x on luvun y neliö" on non-refleksiivinen reaalilukujen joukossa $\mathbb{R}$, koska esimerkiksi $1 = 1^2$, mutta $2 \neq 2^2$.

(4) Relaatio $xPy =$ "x on henkilön y puoliso" on symmetrinen yksiavioisten avioliitossa elävien ihmisten joukossa; nimittäin jos x ja y ovat naimisissa, niin y ja x ovat naimisissa.

(5) Relaatio $x\ddot{A}y =$ "x on henkilön y äiti" on asymmetrinen ihmisten joukossa; nimittäin jos x on henkilön y äiti, ei y voi olla henkilön x äiti, ts. $y\overline{\ddot{A}}x$.

(6) Relaatio $xVy =$ "x on henkilön y veli" on non-symmetrinen ihmisten joukossa. Jotkut ovat veljeksiä, mutta monilla miehillä on myös siskoja.

(7) Relaatio $xRy = x \leq y$ on antisymmetrinen joukossa $\mathbb{Z}$, sillä jos $x \leq y$ ja $y \leq x$, niin välttämättä $x = y$.

(8) Relaatio $xEy =$ "x on henkilön y esimies" on transitiivinen sotilaiden joukossa; nimittäin jos x, y ja z ovat keitä tahansa sellaisia sotilashenkilöitä, että xEy ja yEz, niin myös xEz.

(9) Relaatio $xTy =$ "x on henkilön y tytär" on intransitiivinen ihmisten joukossa; jos nimittäin x, y ja z ovat keitä tahansa sellaisia henkilöitä, että xTy ja yTz, niin xTz ei voi olla voimassa.

(10) Relaatio $xYy =$ "x on henkilön y ystävä" on non-transitiivinen ihmisten joukossa; nmittäin jos xYy ja yYz, niin voi olla myös xYz, mutta ei välttämättä.

(11) Relaatio $xRy = x > y$ on yhtenäinen joukossa $\mathbb{Z}$, sillä jos x ja y ovat mitä tahansa erisuuria kokonaislukuja, niin $x > y$ tai $y > x$.

(12) Relaatio $xRy = x \leq y$ on täysi joukossa $\mathbb{R}$, sillä kaikille luvuille x, $y \in \mathbb{R}$ pätee xRy tai yRx.

6 RELAATION SULKEUMA

Tarkastelemme tässä erilaisten relaatioiden sulkeumia, ts. suppeimpia tietyt ehdot täyttävistä relaatioista. Kaikkien ominaisuuksien suhteen ei sulkeumaa tietenkään ole olemassa (esimerkiksi järjestysominaisuus).

6.1 Relaation sulkeuman määrittely

Tarkastellaan relaatiota $R \subseteq \mathbf{X}\times\mathbf{X}$.

Ongelma. On löydettävä relaation R sisältävistä tietyn ehdon $\mathcal{E}$ täyttävistä relaatioista *suppein*, ts. relaatio $\overline{R} \subseteq \mathbf{X}\times\mathbf{X}$, jolle

a) $R \subseteq \overline{R}$,

b) $\overline{R}$ toteuttaa ehdon $\mathcal{E}$,

c) jos $S \supseteq R$ toteuttaa ehdon $\mathcal{E}$, niin $\overline{R} \subseteq S$.

Ongelmalla ei aina ole ratkaisua. Ratkaisu on olemassa (ja se on samalla yksikäsitteinen) jos ja vain jos joukko

$$\tilde{R} := \bigcap \{\, T \subseteq \mathbf{X}\times\mathbf{X} \mid R \subseteq T,\ T \text{ toteuttaa ehdon } \mathcal{E} \,\}$$

on epätyhjä ja toteuttaa ehdon $\mathcal{E}$.

Annettuun relaatioon R (mahdollisesti) liittyvää suppeinta sen sisältävää refleksiivistä (vast. symmetristä, transitiivista) relaatiota sanotaan relaation R refleksiiviseksi (vast. symmetriseksi, transitiiviseksi) *sulkeumaksi* ja sitä merkitään symbolilla $\overline{R}$. Osoitetaan, että nämä sulkeumat ovat aina olemassa. Refleksiivisyyden ja symmetrisyyden osalta asia on helpohko, transitiivisuustapaus on mielenkiintoisempi.

Lause 6.1.1 Relaation $R \subseteq \mathbf{X}\times\mathbf{X}$

a) refleksiivinen sulkeuma on $\overline{R}^r = \Delta_{\mathbf{X}} \cup R$,

b) symmetrinen sulkeuma on $\overline{R}^s = R^{-1} \cup R$.

Todistus. Harjoitustehtävä. □

Esimerkki 6.1.2 Olkoon $\mathbf{X} := \{x_1, x_2, x_3, x_4, x_5\}$, kaikki eri alkioita. Määritä relaation $R \subseteq \mathbf{X}\times\mathbf{X}$,

$$R := \{(x_1, x_1), (x_1, x_3), (x_3, x_1), (x_3, x_5), (x_4, x_4), (x_5, x_1), (x_5, x_2)\},$$

refleksiivinen ja symmetrinen sulkeuma.

Ratkaisu. Lisätään tarvittavat parit:
$\overline{R}^r = R \cup \{(x_2, x_2), (x_3, x_3), (x_5, x_5)\}$
$\overline{R}^s = R \cup \{(x_1, x_5), (x_2, x_5), (x_5, x_3)\}$

6.2 Relaation transitiivinen sulkeuma

Lause 6.2.1 a) Jos relaatiot $R_i \subseteq \mathbf{X}\times\mathbf{X}$, $i \in I$, ovat transitiivisia, niiden leikkaus $\bigcap_{i\in I} R_i$ on transitiivinen.

b) Olkoon $R \subseteq \mathbf{X}\times\mathbf{X}$ relaatio. Relaatiolla R on transitiivinen sulkeuma $\overline{R}^t$ ja se saadaan kaikkien relaation R sisältävien transitiivisten relaatioiden leikkauksena.

Todistus. a) Merkitään $R' := \bigcap_{i\in I} R_i$. Jos $xR'y$ ja $yR'z$, jokaisella $i \in I$ on xR_iy ja yR_iz. Koska relaatiot R_i ovat transitiivisia, seuraa xR_iz kaikilla $i \in I$, joten $xR'z$. Relaatio R' on siis transitiivinen.

b) Olkoon R annettu relaatio joukossa $\mathbf{X}$. Koska relaatio $\mathbf{X}\times\mathbf{X}$ on triviaalisti transitiivinen, on joukko

$$\mathcal{T} := \{\, T \subseteq \mathbf{X}\times\mathbf{X} \mid R \subseteq T,\ T \circ T \subseteq T \,\}$$

epätyhjä ja koostuu Lauseen 5.9.2 mukaan kaikista relaation R sisältävistä transitiivisista relaatioista. Kohdan a) nojalla $\cap\mathcal{T}$ on relaation R sisältävä transitiivinen relaatio. Määrittelynsä perusteella se on sellaisista suppein, joten transitiivinen sulkeuma on olemassa ja on

$$\overline{R}^t = \bigcap\{\, T \subseteq \mathbf{X}\times\mathbf{X} \mid R \subseteq T,\ T \circ T \subseteq T \,\}.$$

□

Pienehköjen relaatioiden transitiivinen sulkeuma voidaan muodostaa lisäämällä transitiivisuudelle välttämättömät parit. Tämä voidaan joutua tekemään useammalla ”kierroksella”; kun ilmiselvät puutteet on korjattu, voidaan lisäysprosessi joutua uusimaan edellisten lisäysten takia.

Esimerkki 6.2.2 Olkoon $\mathbf{X} := \{x_1, x_2, x_3, x_4, x_5\}$, kaikki eri alkioita. Määritetään relaation $R \subseteq \mathbf{X}\times\mathbf{X}$,

$$R := \{(x_2, x_3), (x_2, x_5), (x_3, x_1), (x_5, x_2)\}$$

transitiivinen sulkeuma.

Koska R ei ole tansitiivinen, siihen pitää lisätä ainakin parit (x_2, x_1), (x_2, x_2), (x_5, x_3) ja (x_5, x_5). Onko saatu relaatio

$$R' := \{(x_2, x_3), (x_2, x_5), (x_3, x_1), (x_5, x_2), (x_2, x_1), (x_2, x_2), (x_5, x_3), (x_5, x_5)\}$$

transitiivinen? Ei, sillä nyt siitä puuttuu ainakin (x_5, x_1). Mutta ei muuta puutukaan ja

$$\overline{R}^t := R \cup \{(x_2, x_1), (x_2, x_2), (x_5, x_3), (x_5, x_5), (x_5, x_1)\}.$$

Sulkeuman muodostamisessa voidaan tarvita useitakin täydennyskierroksia. Tämä voidaan mekanisoida relaatioiden yhdistämiseksi, ts. *potenssien* avulla (tarkastellaan myös Luvussa 5.5).

Määritelmä 6.2.3 Relaation $R \subseteq \mathbf{X}\times\mathbf{X}$ n. *potenssi* R^n määritellään luvuille $n \in \mathbb{N}_0$ seuraavasti:

1. $R^0 := \Delta_{\mathbf{X}}$,
2. $R^{n+1} := R^n \circ R$, $n \in \mathbb{N}_0$.

Lemma 6.2.4 a) Jos $R' \subseteq R \subseteq \mathbf{X}\times\mathbf{Y}$ ja $S' \subseteq S \subseteq \mathbf{Y}\times\mathbf{Z}$, niin

$$S' \circ R' \subseteq \left\{ \begin{array}{c} S' \circ R \\ S \circ R' \end{array} \right\} \subseteq S \circ R.$$

b) Jos $R \subseteq S \subseteq \mathbf{X}\times\mathbf{X}$, niin $R^k \subseteq S^k$ kaikilla $k \in \mathbb{N}$.

c) Jos $S \subseteq \mathbf{X}\times\mathbf{X}$ on transitiivinen, niin $S^k \subseteq S$ kaikilla $k \in \mathbb{N}$.

Todistus. Harjoitustehtäviä. □

Lause 6.2.5 Mielivaltaisen relaation $R \subseteq \mathbf{X}\times\mathbf{X}$ transitiivinen sulkeuma voidaan muodostaa suoralla kaavalla

$$\overline{R}^t = \bigcup_{k=1}^{\infty} R^k.$$

Jos erikoisesti $\mathbf{X}$ on äärellinen n-alkioinen joukko, niin

$$\overline{R}^t = \bigcup_{k=1}^{n} R^k. \tag{10}$$

Todistus. Osoitetaan, että myös joukko

$$R^+ := \bigcup_{k=1}^{\infty} R^k$$

on suppein relaation R sisältävistä transitiivisista relaatioista. Sen jälkeen väite seuraa suppeimman yksikäsitteisyydestä.

Triviaalisti $R = R^1 \subseteq R^+$.

Olkoot xR^+y ja yR^+z. Silloin $(x, y) \in R^q$ ja $(y, z) \in R^p$ joillekin $q, p \in \mathbb{N}$, joten $(x, z) \in R^p \circ R^q = R^{p+q} \subseteq R^+$. Siis R^+ on transitiivinen.

Olkoon lopuksi $S \subseteq \mathbf{X}\times\mathbf{X}$ transitiivinen relaation R sisältävä relaatio. Olkoon niinikään $S^+ := \bigcup_{k=1}^{\infty} S^k$. Koska S on transitiivinen, on Lemman 6.2.4 c)-kohdan nojalla $S^+ \subseteq S$. Koska $R \subseteq S$, on Lemman b)-kohdan mukaan $R^k \subseteq S^k$ kaikilla $k \in \mathbb{N}$. Siis

$$R^+ = \bigcup_{k=1}^{\infty} R^k \subseteq \bigcup_{k=1}^{\infty} S^k = S^+ \subseteq S,$$

joten R^+ on suppein relaation R sisältävistä transitiivisista relaatioista. Väitteen toinen osa on harjoitustehtävä. □

Tehtävä 6.2.6 Keksi esimerkki relaatiosta, jossa on jokin n kappaletta alkioita, ja jonka transitiivisen sulkeuman laskemiseksi kaavalla (10) todella tarvitaan kaikki potenssit R^k, $k \in [n]$.

Ratkaisu. Olkoonpa vaikka $\mathbf{X} := \{1, 2, 3\}$ ja $R := \{(1, 2), (2, 3), (3, 1)\}$. Silloin $R^2 := \{(1, 3), (2, 1), (3, 2)\}$ ja $R^3 := \{(1, 1), (2, 2), (3, 3)\}$.

Huomautus 6.2.7 Äärellisessä n-alkioisessa joukossa määritellyn relaation R matriisin $M = M_R$ avulla

$$\begin{aligned} M_{\overline{R}^t} &= \mathrm{SIGN}\left(\sum_{k=1}^{n} M^k\right) \\ &= \mathrm{SIGN}\left(M(I + M(I + \ldots M(I + M)\ldots))\right). \end{aligned}$$

Käytännön laskuissa jälkimmäinen esitysmuoto on edullisempi, miksi? Suurten matriisien käsittelyssä tämäkin menetelmä on hidas, parempaan tulokseen päästään soveltamalla verkkoteorian yksinkertaista *Floydin* menetelmää, ks. Luku 14 (harjoitustehtävä).

7 EKVIVALENSSIRELAATIO

Tarkastellaan lähemmin Määritelmässä 5.9.3 esiteltyä ekvivalenssirelaatiota, ts. relaatiota $R \subseteq \mathbf{X}\times\mathbf{X}$, joka on

(R) *refleksiivinen*: jokaiselle $x \in \mathbf{X}$ on xRx,

(S) *symmetrinen*: kaikilla $x, y \in \mathbf{X}$ pätee: $xRy \;\Rightarrow\; yRx$,

(T) *transitiivinen*: kaikilla $x, y, z \in \mathbf{X}$ pätee: $xRy \;\&\; yRz \;\Rightarrow\; xRz$.

7.1 Ekvivalenssirelaation määritelmä

Määritelmä 7.1.1 Relaatio $R \subseteq \mathbf{X}\times\mathbf{X}$ on *ekvivalenssirelaatio*, jos se on refleksiivinen, symmetrinen ja transitiivinen.

Sana ekvivalenssi tarkoittaa samuutta tai samanarvoisuutta. Samassa joukossa voi olla erilaisia ekvivalenssirelaatioita; esimerkiksi atomin ytimet ovat *kemiallisesti* ekvivalentit, jos niiden ytimillä on sama varaus, ja *fysikaalisesti* ekvivalentit, jos niillä on sama varaus ja massaluku.

Esimerkki 7.1.2 Olkoon $\mathbf{X}$ epätyhjä joukko. Silloin siellä on aina ekvivalensseja, ainakin diagonaali $\Delta_{\mathbf{X}}$ ja koko tulo $\mathbf{X}\times\mathbf{X}$.

Esimerkki 7.1.3 Tarkastelemme opiskelijoiden joukossa $\mathbf{X}$ relaatiota

$$[\, x\mathcal{O}y \,] \;\Leftrightarrow\; [\; \text{'}x \text{ opiskelee samaa pääainetta kuin } y\text{'} \,]. \tag{11}$$

On helposti todettavissa, että $\mathcal{O}$ on ekvivalenssirelaatio $\mathbf{X}$.

Esimerkki 7.1.4 Kokonaislukujen joukossa on seuraava relaatio R ekvivalenssi:

$$[\, xRy \,] \;\Leftrightarrow\; [\, x - y \text{ jaollinen luvulla } 6 \,]$$

Esimerkki 7.1.5 Onko seuraava kokonaislukujen joukossa määritelty relaatio ekvivalenssi:

$$[\, xRy \,] \;\Leftrightarrow\; [\, |x - y| = 3 \,]?$$

Ratkaisu. Ei tietenkään. Esimerkiksi se ei ole refleksiivinen, koska $|x - x| = 0 \neq 3$. Ei se ole transitiivinenkaan, nimittäin $(9, 6) \in R$ ja $(6, 3) \in R$, mutta $(9, 3) \notin R$. Symmetrinen se ilmeisesti on.

Tehtävä 7.1.6 Määritellään tasossa $\mathbb{R}^2$ relaatio R,

$$[\, (x, y)\, R\, (x', y') \,] \quad\Leftrightarrow\quad [\, x - x' = y - y' \,].$$

Mitkä ekvivalenssin vaatimukset ovat tälle relaatiolle voimassa?

7.2 Ekvivalenssiluokat ja ositukset

Tietty ekvivalenssirelaation määräämä ominaisuus yhdistää perusjoukon alkioita.

Esimerkki 7.2.1 Tarkastellaan Esimerkin 7.1.3 ekvivalenssirelaatiota (11) opiskelijoiden joukossa $\mathbf{X}$. Relaatio $\mathcal{O}$ jakaa joukon $\mathbf{X}$ erillisiin osiin, nk. *ekvivalenssiluokkiin* seuraavasti:

$$\begin{aligned} A_1 &= \text{kansantaloustiedettä pääaineenaan opiskelevat} \\ A_2 &= \text{markkinointia pääaineenaan opiskelevat} \\ &\vdots \\ A_\mu &= \text{matematiikkaa pääaineenaan opiskelevat} \end{aligned}$$

Määritelmä 7.2.2 Olkoon relaatio $R \subseteq \mathbf{X}\times\mathbf{X}$ ekvivalenssi. Alkion $x \in \mathbf{X}$ määräämä *ekvivalenssiluokka* relaatiossa R on joukko

$$R(x) := \{\, y \in \mathbf{X} \mid xRy \,\},$$

jota sanotaan myös *R-ekvivalenssiluokaksi* tai ekvivalenssiluokaksi *modulo* R. Kaikkien ekvivalenssiluokkien (modulo R) joukko on joukon $\mathbf{X}$ *tekijäjoukko* (*quotient*) modulo R, ja sitä merkitään

$$\mathbf{X}/R := \{\, R(x) \mid x \in \mathbf{X} \,\}.$$

Esimerkki 7.2.3 Esimerkin 7.1.4 kokonaislukujen joukon ekvivalenssissa R

$$[xRy] \quad \Leftrightarrow \quad [x - y \text{ jaollinen luvulla } 6]$$

on ekvivalenssiluokat $R(x) = \{\, y \in \mathbf{X} \mid x - y \text{ jaollinen luvulla } 6 \,\}$, eli

$$\begin{aligned} R(0) &= \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\} = \{\, 6k \mid k \in \mathbb{Z} \,\} \\ R(1) &= \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\} = \{\, 6k+1 \mid k \in \mathbb{Z} \,\} \\ R(2) &= \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\} = \{\, 6k+2 \mid k \in \mathbb{Z} \,\} \\ &\vdots \\ R(5) &= \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\} = \{\, 6k+5 \mid k \in \mathbb{Z} \,\} \end{aligned}$$

Muiden kokonaislukujen määräämät ekvivalenssiluokat ovat näitä samoja:
$R(0) = R(-6) = R(6) = \ldots$, $R(1) = R(-5) = R(7) = \ldots$,
$R(2) = R(-4) = R(8) = \ldots, \ldots$, $R(5) = R(-1) = R(11) = \ldots$

Esimerkki 7.2.4 Tarkastellaan edelleen Esimerkin 7.2.1 opiskelijoiden pääaine-ekvivalenssia $\mathcal{O}$ (kaava (11)). Olkoon opiskelijan μ pääaine matematiikka. Tällöin relaatio $x\mathcal{O}\mu$ ilmaisee sen, että x opiskelee samaa pääainetta kuin μ. Kaikkien opiskelijoiden joukko, jotka opiskelevat samaa pääainetta kuin μ, voidaan ilmaista joukkona

$$\mathcal{O}(\mu) = \{\, x \in \mathbf{X} \mid x\mathcal{O}\mu \,\} = A_\mu.$$

Olettaen, että jokaikisellä opiskelijalla on yksi ja vain yksi pääaine tietyllä tarkasteluhetkellä, joukoilla A_i on mm. seuraavat ominaisuudet: kukin $A_i \subseteq \mathbf{X}$, $A_i \cap A_j = \emptyset$ kaikilla $i \neq j$ ja $A_1 \cup A_2 \cup \ldots \cup A_\mu = \mathbf{X}$.

Kaikki pääaineopiskelijajoukot ovat tekijäjoukko

$$\mathbf{X}/\mathcal{O} = \{\, \mathcal{O}(x) \mid x \in \mathbf{X} \,\}.$$

Esimerkeissä 7.2.3 ja 7.2.4 esiintyneet ekvivalenssiluokkien ominaisuudet ovat yleisestikin voimassa:

Lause 7.2.5 Olkoon $R \subseteq \mathbf{X}\times\mathbf{X}$ ekvivalenssirelaatio ja x, $y \in \mathbf{X}$. Tällöin

a) $x \in R(x)$,

b) $[\, R(x) \cap R(y) \neq \emptyset \,] \Leftrightarrow [\, xRy \,]$,

c) $[\, R(x) = R(y) \,] \Leftrightarrow [\, xRy \,]$.

Todistus. Harjoitustehtävä. □

Esimerkki 7.2.6 a) Tarkastellaan kompleksitasoa $\mathbb{C} \simeq \mathbb{R}^2$, jonka alkiota merkitään

$$z = re^{i\varphi}, \quad r \geq 0, \quad 0 \leq \varphi < 2\pi.$$

Relaatio $\bigcirc \subseteq \mathbb{C}\times\mathbb{C}$,

$$[\, r_1 e^{i\varphi_1} \bigcirc r_2 e^{i\varphi_2} \,] \;\Leftrightarrow\; [\, r_1 = r_2 \,],$$

on ekvivalenssi. Se jakaa tason ekvivalenssiluokkiin, jotka ovat origokeskisiä ympyröitä

$$D_\rho := \{\, z \in \mathbb{C} \mid z = \rho e^{i\varphi},\ 0 \leq \varphi < 2\pi \,\}, \quad \rho \geq 0.$$

b) Merkitään $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ ja määritellään relaatio $R \subseteq (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*)$,

$$[\, (m_1, n_1) R (m_2, n_2) \,] \;\Leftrightarrow\; [\, m_1 n_2 = n_1 m_2 \,].$$

Suoralla laskulla voidaan todeta, että R on ekvivalenssirelaatio. Olkoot vastaavat joukon $\mathbb{Z}\times\mathbb{Z}^*$ ekvivalenssiluokat $R(m,n)$. Näitä luokkia kutsutaan *rationaaliluvuiksi* ja niiden muodostamaa joukkoa, ts. joukon $\mathbb{Z}\times\mathbb{Z}^*$ tekijäjoukkoa modulo R merkitään symbolilla $\mathbb{Q}$. Alkion $(m,n) \in \mathbb{Z}\times\mathbb{Z}^*$ määräämälle ekvivalenssiluokalle voidaan käyttää tuttua merkintää $R(m,n) = m/n$. Lauseen 7.2.5 mukaan

$$\begin{aligned}\left[\, \frac{m_1}{n_1} = \frac{m_2}{n_2} \,\right] \quad &\Leftrightarrow \quad [\, R(m_1,n_1) = R(m_2,n_2)\,] \\ &\Leftrightarrow \quad [\, (m_1,n_1) R (m_2,n_2)\,] \\ &\Leftrightarrow \quad [\, m_1 n_2 = n_1 m_2\,].\end{aligned}$$

Tehtävä 7.2.7 Määritä Tehtävän 7.1.6 relaation ekvivalenssiluokat.

Ositukset

Olkoon annettu ekvivalenssirelaatio $R \subseteq \mathbf{X}\times\mathbf{X}$. Koska R on refleksiivinen, on jokainen alkio $x \in \mathbf{X}$ relaatiossa ainakin itsensä kanssa. Jokainen alkio on siis jossakin ekvivalenssiluokassa. Toisaalta mikään alkio ei voi kuulua Lauseen 7.2.5 nojalla useampaan kuin yhteen ekvivalenssiluokkaan. Täten ekvivalenssirelaatio jakaa perusjoukon $\mathbf{X}$ pistevieraisiin osiin, ts. määrää seuraavan määritelmän mukaisen osituksen.

Määritelmä 7.2.8 Perhe $\mathcal{A} = \{\, \mathbf{X}_i \subseteq \mathbf{X} \mid i \in I \,\}$ on joukon $\mathbf{X}$ *ositus*, jos

a) jokainen $\mathbf{X}_i$ on epätyhjä,

b) $\bigcup_{i\in I} \mathbf{X}_i = \mathbf{X}$,

c) $\mathbf{X}_i \cap \mathbf{X}_j$ on tyhjä aina, kun $i \neq j$.

Lause 7.2.9 a) Ekvivalenssirelaation $R \subseteq \mathbf{X}\times\mathbf{X}$ määräämät ekvivalenssiluokat $\{\, R(x) \mid x \in \mathbf{X} \,\}$ muodostavat joukon $\mathbf{X}$ osituksen.

b) Jos $\mathcal{A} = \{\, \mathbf{X}_i \mid i \in I \,\}$ on joukon $\mathbf{X}$ ositus, on olemassa täsmälleen yksi ekvivalenssirelaatio $R \subseteq \mathbf{X}\times\mathbf{X}$, joka muodostaa osituksen $\mathcal{A}$, nimittäin

$$R := \{\, (x,y) \in \mathbf{X}\times\mathbf{X} \mid x,y \in \mathbf{X}_i \text{ jollekin } i \,\}.$$

Todistus. Kohta a) on todettu edellä.

b) Selvästi R on relaatio joukossa $\mathbf{X}$. Osoitetaan, että R on refleksiivinen, symmetrinen ja transitiivinen.

1) Olkoon $x \in \mathbf{X}$ mielivaltainen. Koska $\mathcal{A}$ on ositus, on olemassa indeksi $i \in I$, jolle $x \in \mathbf{X}_i$. Mutta silloin $(x,x) \in R$ eli xRx. Täten R on refleksiivinen.

2) Olkoot xRy. Silloin x ja y ovat samassa joukossa $\mathbf{X}_j$, joten myös yRx, mikä osoittaa symmetrisyyden.

3) Olkoot xRy ja yRz. On olemassa i_1, $i_2 \in I$, joille x, $y \in \mathbf{X}_{i_1}$ ja y, $z \in \mathbf{X}_{i_2}$. Koska y kuuluu molempiin ja $\mathcal{A}$ on ositus, on $\mathbf{X}_{i_1} = \mathbf{X}_{i_2}$. Siis x, $z \in \mathbf{X}_{i_1}$ eli xRz. Relaatio R on siis myös transitiivinen.

Tuli siis osoitetuksi, että R on ekvivalenssi. Jos $S \subseteq \mathbf{X}\times\mathbf{X}$ on jokin ekvivalenssi, joka määrää osituksen $\mathcal{A}$, niin

$$[\, xSy \,] \;\Leftrightarrow\; [\, x, y \in \mathbf{X}_i \,] \;\Leftrightarrow\; [\, xRy \,]$$

eli $S = R$. □

Huomautus 7.2.10 a) Lause 7.2.9 osoittaa, että ekvivalenssirelaatio voidaan ilmaista antamalla siihen liittyvä ositus.

b) On helposti osoitettavissa, että ekvivalenssien leikkaus on ekvivalenssi. Jokainen relaatio voidaan täydentää ekvivalenssiksi Lauseiden 6.1.1 ja 6.2.5 tarjoamin keinoin. On siis olemassa *ekvivalenssisulkeuma* (harjoitustehtävä).

Tehtävä 7.2.11 Ilmoita se ositus, jonka määrää Esimerkeissä 7.1.4 ja 7.2.3 käsitelty kokonaislukujen joukon ekvivalenssi R

$$[xRy] \quad \Leftrightarrow \quad [x - y \text{ jaollinen luvulla } 6].$$

Ratkaisu. Ositus on joukko

$$\mathbb{Z}/R = \{\, R(x) \mid x \in \mathbb{Z} \,\} = \{R(0), R(1), R(2), R(3), R(4), R(5)\},$$

ks. Esimerkki 7.2.3.

8 JÄRJESTYSRELAATIO

Tarkastellaan lähemmin Määritelmässä 5.9.3 esiteltyä järjestysrelaatiota, ts. relaatiota $R \subseteq \mathbf{E}\times\mathbf{E}$, joka on

(R) *refleksiivinen*: jokaiselle $x \in \mathbf{E}$ on xRx,

(A) *antisymmetrinen*: kaikilla $x, y \in \mathbf{E}$ pätee

$$[\, xRy \ \&\ yRx \,] \quad \Rightarrow \quad [\, x = y \,],$$

(T) *transitiivinen*: kaikilla $x, y, z \in \mathbf{X}$ pätee

$$[\, xRy \ \&\ yRz \,] \quad \Rightarrow \quad [\, xRz \,],$$

Tutkitaan järjestettyjen joukkojen rakennetta ja esittämistä, järjestetyn joukon äärimmäisiä alkioita ja täysin järjestettyjä joukkoja.

8.1 Järjestys ja duaaliperiaate

Olkoon $\mathbf{E}$ tässä luvussa epätyhjä joukko. Palautetaan mieleen osittaisen järjestyksen määritelmä.

Määritelmä 8.1.1 Relaatio $R \subseteq \mathbf{E}\times\mathbf{E}$ on *osittainen järjestysrelaatio*, jos se on refleksiivinen, antisymmetrinen ja transitiivinen.

Jos lisäksi R on täysi, ts. jokaiselle parille $x, y \in \mathbf{E}$ pätee xRy tai yRx, niin R on *täydellinen* eli *totaali järjestys*.

Määritelmä 8.1.2 Pari $(\mathbf{E}, \leq)$ on *osittain järjestetty joukko*, jos $\leq$ on osittainen järjestys epätyhjässä joukossa $\mathbf{E}$. Vastaavasti määritellään *täydellisesti* eli *totaalisti järjestetty joukko*.

Seuraavassa ”järjestys” on aina osittainen järjestys, ellei toisin erikseen mainita. Järjestykselle käytetään merkintää $\leq$, joka luetaan ”pienempi tai yhtä kuin”. Sovitaan lisäksi merkinnästä *aito pienemmyys* $<$:

$$[\, x < y \,] \ \Leftrightarrow\ [\, x \leq y \text{ ja } x \neq y \,],$$

joka relaationa on transitiivinen. Jos $(\mathbf{E}, \leq)$ on järjestetty joukko ja $F \subseteq \mathbf{E}$, niin pari $(F, \leq)$ on myös järjestetty joukko. Laajemmasta joukosta $\mathbf{E}$ periytyvää järjestystä $\leq$ sanotaan parin $(\mathbf{E}, \leq)$ joukkoon F *indusoimaksi*.

Esimerkki 8.1.3 Olkoon X joukko ja $\mathbf{E} := \mathcal{P}(X)$. Silloin ”olla osajoukko” eli inkluusio $\subseteq$ on osittainen järjestys joukossa $\mathcal{P}(X)$. Tämä ei ole täydellinen järjestys, jos $\#X \geq 2$ (ks. Esimerkki 5.9.6).

Esimerkki 8.1.4 Jos $(\mathbf{E}, \leq)$ on järjestetty joukko, niin joukko $\mathbf{E}$ varustettuna käänteisrelaatiolla $\geq := (\leq)^{-1}$ on myös järjestetty joukko.

Dualiteettiperiaate. Kaikista järjestetyille joukoille pätevistä lauseista saadaan ”uusia” kääntämällä järjestys.

8.2 Äärimmäiset alkiot sekä infimum ja supremum

Tarkastellaan järjestetyn joukon äärimmäisiä alkioita.

Määritelmä 8.2.1 Olkoon $(\mathbf{E}, \leq)$ järjestetty joukko ja $F \subseteq \mathbf{E}$.
Alkio $a \in \mathbf{E}$ on *minimaalinen*, jos $x = a$ aina, kun $x \leq a$.
Alkio $a \in \mathbf{E}$ on *maksimaalinen*, jos $x = a$ aina, kun $a \leq x$.
Alkio $a \in \mathbf{E}$ on *äärimmäinen*, jos a on minimaalinen tai maksimaalinen.
Alkio $a \in \mathbf{E}$ on joukon $\mathbf{E}$ *pienin alkio*, jos $a \leq x$ kaikilla $x \in \mathbf{E}$.
Alkio $a \in \mathbf{E}$ on joukon $\mathbf{E}$ *suurin alkio*, jos $x \leq a$ kaikilla $x \in \mathbf{E}$.
Alkio $a \in \mathbf{E}$ on joukon F *alaraja*, jos $a \leq x$ kaikilla $x \in F$.
Alkio $a \in \mathbf{E}$ on joukon F *yläraja*, jos $x \leq a$ kaikilla $x \in F$.
Alkio $a \in \mathbf{E}$ on joukon F *suurin alaraja* eli *infimum*, jos se on joukon F alarajojen joukon suurin alkio.
Alkio $a \in \mathbf{E}$ on joukon F *pienin yläraja* eli *supremum*, jos se on joukon F ylärajojen joukon pienin alkio.
Joukko F on *alhaalta* (vast. *ylhäältä*) *rajoitettu*, jos sillä on alaraja (vast. yläraja) joukossa $\mathbf{E}$. Joukko F on *rajoitettu*, jos se on alhaalta ja ylhäältä rajoitettu.

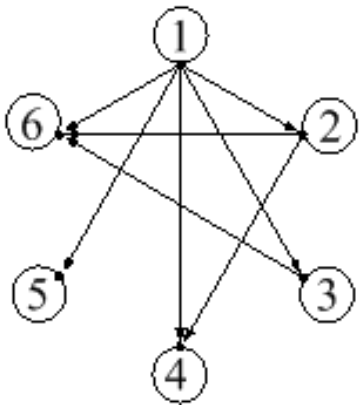
Esimerkki 8.2.2 Tarkastellaan joukkoa $\mathbf{E} := \{1, 2, 3, 4, 5, 6\}$. Määritellään joukossa $\mathbf{E}$ relaatio

$$[\, x \lhd y \,] \;\Leftrightarrow\; [\, y \text{ on jaollinen luvulla } x \,].$$

Relaatio on esitetty nuolikaaviona Kuvassa 16, josta on helppo tarkastaa osittaisen järjestyksen vaatimukset.

Järjestetyllä joukolla $(\mathbf{E}, \lhd)$ on ominaisuudet:

- äärimmäisiä alkioita ovat 1, 4, 5 ja 6, joista 1 on minimaalinen ja pienin alkio
- suurinta alkiota ei ole, mutta 4, 5 ja 6 ovat maksimaalisia
- luku 6 on joukon $\{1, 2, 3, 6\}$ yläraja ja supremum



Kuva 16: Jaollisuusesimerkin 8.2.2 nuolikaavio

• joukolla $\{1, 2, 3, 5, 6\}$ ei ole ylärajaa

Lause 8.2.3 Olkoon $(\mathbf{E}, \leq)$ järjestetty joukko.

a) Joukossa $\mathbf{E}$ on korkeintaan yksi pienin ja yksi suurin alkio.
b) Osajoukolla $F \subseteq \mathbf{E}$ on korkeintaan yksi infimum ja supremum.
c) Joukossa $\mathbf{E}$ on pienin alkio jos ja vain jos $\mathbf{E}$ on alhaalta rajoitettu. Vastaava pätee suurimmalle alkiolle.

Todistus. Kohdat a) ja b) ovat harjoitustehtäviä. Kohta c) on ilmeinen. □

Merkintöjä. Joukon $\mathbf{E}$ pienintä alkiota merkitään $\min \mathbf{E}$ ja suurinta $\max \mathbf{E}$. Luonnollisesti voidaan puhua myös osajoukon $F \subseteq \mathbf{E}$ pienimmästä ja suurimmasta alkiosta, kun paria $(F, \leq)$ tarkastellaan järjestettynä joukkona. Joukon $F \subseteq \mathbf{E}$ suurinta alarajaa merkitään $\inf F$, pienintä ylärajaa $\sup F$.

Huomautus 8.2.4 Määritelmässä 8.2.1 esitellyt käsitteet muodostavat *duaaleja pareja*: siirryttäessä järjestyksestä $\leq$ sen duaaliin relaatioon $\geq$ muuttuu kukin käsite sen duaaliksi pariksi. Esimerkiksi parin $(\mathbf{E}, \leq)$ pienin alkio – mikäli se on olemassa – on parin $(\mathbf{E}, \geq)$ suurin alkio.

8.3 *Pienimmän ylärajan ominaisuus

Olkoon $(\mathbf{E}, \leq)$ järjestetty joukko ja $F \subseteq \mathbf{E}$. Vaikka joukko F olisikin ylhäältä rajoitettu joukossa $\mathbf{E}$, ei pienintä ylärajaa – puhumattakaan joukon F suurimmasta alkiosta – tarvitse olla olemassa (vrt. Lause 8.2.3).

Määritelmä 8.3.1 Järjestetyllä joukolla $(\mathbf{E}, \leq)$ on *pienimmän ylärajan ominaisuus* (P.Y.O.), jos jokaisella ylhäältä rajoitetulla joukolla $F \subseteq \mathbf{E}$ on pienin yläraja joukossa $\mathbf{E}$, ts. on olemassa $\sup F$ ja $\sup F \in \mathbf{E}$.

Järjestetyllä joukolla $(\mathbf{E}, \leq)$ on *suurimman alarajan ominaisuus* (S.A.O.), jos duaalisella järjestetyllä joukolla $(\mathbf{E}, \geq)$ on P.Y.O.

Voidaan osoittaa, että joukolla on P.Y.O. aina ja vain, kun sillä on S.A.O.

Esimerkki 8.3.2 a) Järjestetyllä joukolla $(\mathbb{R}, \leq)$ ei ole äärimmäisiä alkioita, ylä- tai alarajoja eikä suurinta tai pienintä alkiota. On mahdollista osoittaa, että sillä on kuitenkin P.Y.O.

b) Joukolla $(\mathbb{Q}, \leq)$ ei ole pienimmän ylärajan ominaisuutta. Esimerkiksi ylhäältä rajoitetulla osajoukolla $F := \{\, q \in \mathbb{Q} \mid q^2 < 2 \,\}$ ei ole pienintä ylärajaa (*Analyysi*).

c) Joukolla $(\mathbb{Z}, \leq)$ on P.Y.O; itse asiassa ylhäältä rajoitetussa joukossa $F \subseteq \mathbb{Z}$ on jopa suurin alkio.

8.4 Järjestetty joukko Hassen kaaviona

Äärellinen järjestetty joukko $(\mathbf{E}, \leq)$ voidaan – ainakin periaatteessa – aina esittää havainnollisena nuolikaaviona, nk. *Hassen kaaviota*, ks. Kuva 17. Kyseessä on erikoistapaus suunnatusta verkosta (ks. Luku 13).

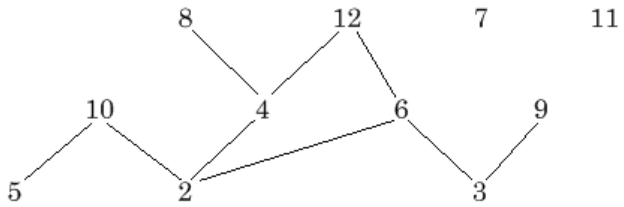
Määritelmä 8.4.1 Olkoon $(\mathbf{E}, \leq)$ järjestetty joukko ja $x, y \in \mathbf{E}$, $x \neq y$. Alkio x on alkion y *välitön edeltäjä* ja y alkion x *välitön seuraaja*, jos (vrt. verkoilla Määritelmä 13.8.3)

$$[\, x < y \text{ ja } x \leq z \leq y \,] \quad \Rightarrow \quad [\, z = x \text{ tai } z = y \,].$$

Piirretään kuvioon joukon $\mathbf{E}$ alkiot ja nuolet kustakin alkiosta sen välittömiin seuraajiin. Tavallisesti tämä koetetaan tehdään sillä tavoin, että nuolet osoittavat aina ylöspäin tai yläviistoon. Minimaaliset alkiot tulevat siis alimmaisiksi ja maksimaaliset ylimmiksi. Näin piirrettyä kaaviota sanotaan järjestetyn joukon $(\mathbf{E}, \leq)$ *Hassen kaavioksi* eli *Hassen diagrammiksi*. Hassen kaaviota luetaan "transitiivisesti": jos kaaviossa $x < y$ ja $y < z$, niin "kuvitellaan" myös $x < z$. Lisäksi refleksiivisyyttä – siis pareja (x, x) – ei merkitä, vaikka se tietysti oletetaankin.

Esimerkki 8.4.2 Olkoon $\mathbf{E} = \{2, 3, \ldots, 12\}$ ja

$$\leq := \{\, (x, y) \in \mathbf{E} \times \mathbf{E} \mid y = xz \text{ jollekin } z \in \mathbb{Z} \,\}.$$



Kuva 17: Esimerkin 8.4.2 relaatio Hassen kaaviona

Parin $(\mathbf{E}, \leq)$ Hassen kaavio on Kuvassa 17.

Kun kaaviota luetaan transitiivisesti, saadaan esimerkiksi $2 \leq (4 \leq) 8$. Kaavion mukaan

• minimaalisia alkioita ovat 5, 2, 3, 7 ja 11

• maksimaalisia alkioita ovat 10, 8, 12, 9, 7 ja 11

• pienintä tai suurinta alkiota ei ole

• 3 on joukkojen $\{3, 9\}$ ja $\{6, 9\}$ alaraja ja infimum

• joukon $\{2, 3\}$ ylärajoja ovat 6 ja 12, supremum on 6

• joukolla $\{8, 9, 12\}$ ei ole ala- eikä ylärajoja.

Tehtävä 8.4.3 Tarkastellaan joukkoa $\mathbf{E} := \{1, 2, 3, 4, 5, 6\}$ ja Esimerkin 8.2.2 järjestysrelaatiota

$$[\, x \lhd y \,] \;\Leftrightarrow\; [\, y \text{ on jaollinen luvulla } x \,].$$

Esitä relaatio Hassen kaaviona.

8.5 Maksimaalisen alkion olemassaolo

Lauseessa 8.2.3 todettiin pienimmän ja suurimman alkion sekä infimumin ja supremumin yksikäsitteisyys. Todistetaan joitakin äärimmäisten alkioiden olemassaolo- ja yksikäsitteisyystuloksia.

Lause 8.5.1 Olkoon $(\mathbf{E}, \leq)$ äärellinen järjestetty joukko.

a) Joukossa $\mathbf{E}$ on ainakin yksi maksimaalinen ja yksi minimaalinen alkio.

b) Jos $a \in \mathbf{E}$ on ainoa minimaalinen alkio, on a pienin alkio. Vastaava pätee suurimmalle alkiolle.

Todistus. a) Duaalisuuden nojalla riittää näyttää esimerkiksi minimaalisen alkion olemassaolo. Todistetaan väite induktiolla alkiomäärän $n = \#\mathbf{E}$ suhteen.

Jos $n = 1$, on asia selvä. Oletetaan, että väite pitää paikkansa joukoille, joissa on korkeintaan n alkiota, $n \geq 1$. Olkoon $\mathbf{E}$ joukko, jossa on $n+1$ alkiota. Olkoon $a \in \mathbf{E}$. Merkitään

$$V := \{\, x \in \mathbf{E} \mid x < a \,\}.$$

Jos $V = \emptyset$, on a minimaalinen alkio. Olkoon $V \neq \emptyset$. Silloin pari $(V, \leq)$ on järjestetty joukko ja $\#V \leq n$. Induktio-oletuksen nojalla joukossa V on minimaalinen alkio, olkoon eräs niistä b. Osoitetaan, että b on koko joukon $\mathbf{E}$ minimaalinen alkio.

Olkoon $x \in \mathbf{E}$, $x \leq b$, mielivaltainen. Koska $x \leq b < a$, on $x \in V$. Koska b on joukon V minimaalinen alkio, on $x = b$. Siis b on minimaalinen myös joukossa $\mathbf{E}$.

b) Olkoon $a \in \mathbf{E}$ ainoa minimaalinen alkio. Merkitään

$$F := \{\, x \in \mathbf{E} \mid a \leq x \,\}$$

ja $G := \mathbf{E} \setminus F$. Riittää osoittaa, että G on tyhjä joukko.

Antiteesi: On olemassa $y \in G$. Koska joukko $(G, \leq)$ on äärellinen, on siinä a)-kohdan nojalla minimaalinen alkio $b \in G$. Alkio b on minimaalinen myös joukossa $\mathbf{E}$. Nimittäin, jos olisi olemassa $u \in \mathbf{E}$, jolle $u < b$, niin $u \in F$, $a \leq u < b$ ja siten $b \in F$, mikä on ristiriita. Joukossa $\mathbf{E}$ on täten minimaaliset alkiot $a \neq b$, mikä on vastoin oletusta. Siis $G = \emptyset$ ja $F = \mathbf{E}$, joten a on pienin alkio. □

8.6 Järjestysisomorfia

Tarkastellaan järjestyksen säilymistä järjestettyjen joukkojen välisessä kuvauksessa.

Määritelmä 8.6.1 Olkoot $(\mathbf{E}, \leq)$ ja $(\mathbf{E}', \leq')$ järjestettyjä joukkoja.

a) Kuvaus $f : \mathbf{E} \to \mathbf{E}'$ on *järjestyksen säilyttävä* tai *järjestyshomomorfismi*, jos kaikilla $x, y \in \mathbf{E}$ pätee

$$[\, x \leq y \,] \;\Rightarrow\; [\, f(x) \leq' f(y) \,].$$

b) Joukot $(\mathbf{E}, \leq)$ ja $(\mathbf{E}', \leq')$ ovat järjestystensä suhteen *isomorfiset*, jos on olemassa bijektio $f : \mathbf{E} \to \mathbf{E}'$, jolle f ja f^{-1} ovat järjestyksen säilyttäviä. Tällainen kuvaus f on *kasvava isomorfismi*. Isomorfisuutta järjestettyjen joukkojen välillä merkitään $(\mathbf{E}, \leq) \approx (\mathbf{E}', \leq')$.

Huomautus 8.6.2 Isomorfia voitaisiin määritellä myös Hassen kaavioiden verkkoisomorfian avulla.

8.7 Täydellisesti järjestetty joukko

Lauseet 8.7.1 ja 8.7.2 osoittavat, että täydellisesti järjestetty joukko on teorialtaan sangen yksioikoinen ja siten mielenkiinnoton.

Lause 8.7.1 Jos täydellisesti järjestetyssä joukossa on minimaalinen (vast. maksimaalinen) alkio, niin se on pienin (vast. suurin) alkio; erikoisesti se on yksikäsitteinen.

Todistus. Olkoon $a \in \mathbf{E}$ minimaalinen. Täydellisessä järjestyksessä pätee jokaiselle $x \in \mathbf{E}$ epäyhtälö $x \leq a$ tai $a \leq x$. Jos $x \leq a$, niin minimaalisuuden nojalla $x = a$. Siis $a \leq x$ kaikilla $x \in \mathbf{E}$, joten a on pienin alkio. □

Lause 8.7.2 Äärellinen täydellisesti järjestetty joukko $(\mathbf{E}, \preceq)$ on isomorfinen sen alkiomäärän lukumääräjoukon kanssa, ts.

$$(\mathbf{E}, \preceq) \;\approx\; \big([\#\mathbf{E}], \leq\big).$$

Todistus. Induktiotodistus luvun $n = \#\mathbf{E}$ suhteen. Tapaus $n = 1$ on selvä. Oletetaan, että väite pätee kaikille täydellisesti järjestetyille joukoille, joissa on korkeintaan $n{-}1$ alkiota. Olkoon $\#\mathbf{E} = n$. Lauseiden 8.5.1 ja 8.7.1 nojalla on olemassa suurin alkio $a \in \mathbf{E}$. Silloin järjestetyssä joukossa $\mathbf{E}\backslash\{a\}$ on $n{-}1$ alkiota, joten

$$\big(\mathbf{E}\backslash\{a\}, \preceq\big) \;\approx\; \big([n{-}1], \leq\big).$$

On siis olemassa järjestyksen säilyttävä bijektio $f : \mathbf{E}\backslash\{a\} \to [n{-}1]$. Kuvaus $g : \mathbf{E} \to [n]$,

$$g(x) := \begin{cases} f(x), & \text{kun } x \neq a, \\ n, & \text{kun } x = a, \end{cases}$$

on bijektio ja säilyttää järjestyksen. □

9 JOUKON KARAKTERISTINEN FUNKTIO

Tarkastelemme joukon esittämistä ns. *karakteristisella funktiolla*. Tämä vastaa sitä tapaa, jolla sumeita joukkoja esitetään, ts. käytetään jäsenyysfunktiota. Funktiota käytetään myös todennäköisyyslaskennassa, usein nimellä *indikaattori*.

9.1 Karakteristinen funktio ja potenssijoukko

Funktion käsite sinällään on esitelty Luvussa 5.7, potenssijoukko Luvussa 3.4.

Määritelmä 9.1.1 Joukon $A \subseteq \mathbf{X}$ *karakteristinen funktio* on kuvaus $\chi_A : \mathbf{X} \to \{0, 1\}$,

$$\chi_A(x) := \begin{cases} 1, & \text{jos } x \in A, \\ 0, & \text{jos } x \in \mathbf{X} \backslash A. \end{cases}$$

Karakteristinen funktio χ_A siis lajittelee saamansa arvon avulla perusjoukon $\mathbf{X}$ alkiot niihin, jotka kuuluvat joukkoon A (arvo $= 1$), ja niihin jotka eivät kuulu (arvo $= 0$).

Jos $\mathbf{X}$ on tavallinen äärellinen joukko ja $\#\mathbf{X} = n$, on sen potenssijoukko (sen kaikkien osajoukkojen joukko) $\mathcal{P}(\mathbf{X})$ äärellinen ja siinä on 2^n alkiota (ks. Lause 10.2.5).

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

$$\mathrm{Ch}(\mathbf{X}) := \{\, \chi \mid \chi : \mathbf{X} \to \{0, 1\} \text{ funktio} \,\}$$

ovat *yhtä mahtavia*, ks. Luku 10.1.1.

Niitä voidaan sanoa jopa joukko-opillisesti *isomorfisiksi*, sillä $\mathcal{P}(\mathbf{X})$ ja $\mathrm{Ch}(\mathbf{X})$ vastaavat struktuuriltaan täysin toisiaan. Bijektiiviset kuvaukset $\varphi : \mathcal{P}(\mathbf{X}) \to \mathrm{Ch}(\mathbf{X})$ ja $\psi : \mathrm{Ch}(\mathbf{X}) \to \mathcal{P}(\mathbf{X})$,

$$\varphi(A) := \chi_A \quad \text{ja} \quad \psi(\chi) := \{\, x \in \mathbf{X} \mid \chi(x) = 1 \,\} \tag{12}$$

nimittäin muuntavat joukko-opin funktioiden tarkasteluksi; tässä joukko ja sen karakteristinen funktio samaistetaan.

On helppo osoittaa φ ja ψ toistensa käänteisfunktioiksi. Niiden yhdistetyt kuvaukset ovat identiteettikuvauksia, ts.

$$\varphi \circ \psi = \mathrm{Id}_{\mathrm{Ch}(\mathbf{X})} \quad \text{ja} \quad \psi \circ \varphi = \mathrm{Id}_{\mathcal{P}(\mathbf{X})}.$$

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

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

että intuitiivinen malli $\mathcal{P}(\mathbf{X})$ korvataan matemaattisella mallilla $\mathrm{Ch}(\mathbf{X})$. Käyttämällä joukkoa $\mathrm{Ch}(\mathbf{X})$ 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.

9.2 Karakteristinen funktio ja joukko-operaatiot

Joukkoon $\mathrm{Ch}(\mathbf{X})$ kuuluvien funktioiden arvojen joukko on siis $\{0, 1\}$. Tarkastelemme joukon $\mathbf{X}$ osajoukoille määriteltyjen joukko-operaatioiden yhdiste, leikkaus ja komplementti vastineita karakteristisen funktioiden joukossa $\mathrm{Ch}(\mathbf{X})$ ja niiden arvojoukossa $\{0, 1\}$.

Olkoot $A, B \subseteq \mathbf{X}$. Tällöin myös $A \cup B \subseteq \mathbf{X}$. Tutkimme, miten voimme yhdistää funktiot χ_A ja χ_B siten, että tulos kuuluu joukkoon $\mathrm{Ch}(\mathbf{X})$ eli on yhdisteen $A \cup B$ 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 yhdistettä vastaa siis ns. 'mukaanlukeva tai', eli sovimme, että ei ole välttämätöntä merkitä näkyviin erityisesti sitä seikkaa, että tapaus '$x \in A$ ja $x \in B$' on myös mahdollinen. Sovimme siis, että 'tai' ilman "lisukkeita" on mukaanlukeva tai. Jos meillä 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 yhdiste vaan symmetrinen erotus. Siis yhdisteen 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

$$\chi_A(x) = 1 \text{ tai } \chi_B(x) = 1.$$

Merkitsemme tätä symbolisesti ilmaisulla

$$\chi_A(x) \vee \chi_B(x) = 1. \tag{13}$$

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

$$\chi_A(x) \vee \chi_B(x) = 0. \tag{14}$$

Voimmekin määritellä joukon $A \cup B$ karakteristisen funktion muodossa 'χ_A tai χ_B' eli muodossa

$$\chi_{A\cup B} = \chi_A \vee \chi_B$$

kaikille joukoille $A, B \subseteq \mathbf{X}$, jolloin $\chi_A, \chi_B \in \mathrm{Ch}(\mathbf{X})$.

Koska $A \cup B \subseteq \mathbf{X}$ eli $A \cup B \in \mathcal{P}(\mathbf{X})$, niin myös $\chi_A \vee \chi_B \in \mathrm{Ch}(\mathbf{X})$. Yhtälön (14) perusteella siis sekä $\chi_A(x) = 0$ että $\chi_B(x) = 0$ tarkalleen silloin, kun $x \notin A \cup B$. Jos olisi joko $\chi_A(x) = 1$ ja $\chi_B(x) = 0$ tai $\chi_A(x) = 0$ ja $\chi_B(x) = 1$, olisi tilanne yhtälön (13) mukainen, eli $\chi_{A\cup B}(x) = 1$.

Kokoamme yhteen funktion $\chi_A \vee \chi_B$ arvot esitettynä χ_A:n ja χ_B:n arvojen avulla Taulukon 9.2.1 mukaisesti.

Taulukko 9.2.1 Yhdisteen $A \cup B$ karakteristinen funktio.

χ_A	χ_B	$\chi_A \vee \chi_B$
0	0	0
0	1	1
1	0	1
1	1	1

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 $\chi_A(x) = 1$ ja $\chi_B(x) = 1$. Jos $x \notin A$ tai $x \notin B$, niin $x \notin A \cap B$, ts. jos $\chi_A(x) = 0$ tai $\chi_B(x) = 0$, niin $\chi_{A\cap B}(x) = 0$. Voimme siis ilmaista leikkauksen $A \cap B$ karakteristisen funktion muodossa 'χ_A ja χ_B', jota symbolisesti merkitsemme ehdolla

$$\chi_{A\cap B} = \chi_A \wedge \chi_B.$$

Funktion $\chi_{A\cap B}$ arvot riippuvat funktioiden χ_A ja χ_B arvoista Taulukon 9.2.2 osoittamalla tavalla.

Taulukko 9.2.2 Leikkauksen $A \cap B$ karakteristinen funktio.

χ_A	χ_B	$\chi_A \wedge \chi_B$
0	0	0
0	1	0
1	0	0
1	1	1

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 $x \in \mathbf{X}\backslash A$ eli

$x \notin A$. Tämä on yhtäpitävä sen kanssa, että $\chi_{\overline{A}}(x) = 1$. Jos taas $x \in A$, niin $x \notin \overline{A}$, jolloin $\chi_{\overline{A}}(x) = 0$. Määrittelemme siis komplementin $\overline{A}$ karakteristisen funktion muodossa 'ei χ_A', jota merkitsemme symbolisesti ehdolla

$$\chi_{\overline{A}}(x) = \neg\chi_A.$$

Taulukko 9.2.3 antaa funktion $\chi_{\overline{A}}(x)$ arvon, kun funktion χ_A arvo tiedetään.

Taulukko 9.2.3 Komplementin $\overline{A}$ karakteristinen funktio.

χ_A	$\neg\chi_A$
0	1
1	0

Edellä olevia taulukoita vastaavat seuraavat laskennalliset kaavat, joiden avulla joukkojen yhdisteen, leikkauksen ja komplementin karakteristisen funktioiden arvot voidaan laskea, kun kyseessä olevien joukkojen karakteristisen funktioiden arvot tiedetään.

Lause 9.2.4 Joukon $\mathbf{X}$ osajoukkojen karakteristisille funktioille on voimassa

$$\begin{aligned} \chi_A \vee \chi_B &= \max(\chi_A, \chi_B) \\ \chi_A \wedge \chi_B &= \min(\chi_a, \chi_B) \\ \neg\chi_A &= 1 - \chi_A \end{aligned}$$

Jos $A \subseteq \mathbf{X}$ on äärellinen, sen alkiomäärä voidaan esittää laskemalla yhteen ykkösiä niin monta kuin alkioita on, siis muodossa

$$\#A = \sum_{x\in A} 1 = \sum_{x\in A} \chi_A(x) = \sum_{x\in A} \chi_A(x) + \sum_{x\in \mathbf{X}\setminus A} \chi_A(x) = \sum_{x\in \mathbf{X}} \chi_A(x).$$

Lauseen 9.2.4 laskukaavat voidaan voidaan ilmaista myös artimeettisissa muodoissa (yhteen- ja kertolaskujen avulla):

Lause 9.2.5 Olkoot A, B ja A_1, A_2, ..., $A_n \subseteq \mathbf{X}$. Silloin

a) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}$

b) $\chi_{A_1\cap A_2\cap\cdots\cap A_n} = \chi_{A_1}\chi_{A_2}\cdots\chi_{A_n}$

c) $\chi_{\mathbf{X}\setminus A} = 1 - \chi_A$

Todistus. c) Jos $x \in A$, on $\chi_{\mathbf{X}\setminus A}(x) = 0 = 1 - 1 = 1 - \chi_A(x)$. Jos taas $x \in (\mathbf{X}\setminus A)$, niin $\chi_{\mathbf{X}\setminus A}(x) = 1 = 1 - 0 = 1 - \chi_A(x)$.

b) Väite seuraa ekvivalenssiketjusta

$$\begin{aligned}
[\,\chi_{A_1\cap A_2\cap\cdots\cap A_n}(x) = 1\,] &\Leftrightarrow [\,x \in (A_1 \cap \cdots \cap A_n)\,] \\
&\Leftrightarrow [\,\chi_{A_1}(x) = \cdots = \chi_{A_n}(x) = 1\,] \\
&\Leftrightarrow [\,\chi_{A_1}(x)\cdots\chi_{A_n}(x) = 1\,].
\end{aligned}$$

a) Todistetaan tarkastelemalla funktioiden $\chi_{A\cup B}$ ja $\chi_A+\chi_B-\chi_{A\cap B}$ arvoja erikseen kussakin tapauksessa $x \in A$ ja $x \in B$, $x \in A$ ja $x \notin B$, $x \notin A$ ja $x \in B$ sekä viimein $x \notin A$ ja $x \notin B$. □

Kun vertaamme Lauseen 9.2.4 kaavoja edellä olleisiin vastaaviin taulukoihin, havaitsemme, että ne ovat täysin yhteensopivat. Lauseen 9.2.4 kaavojen 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 esimerkiksi mainittujen lukujen väliltä, olemme karakteristisiten funktioidemme kanssa jossakin ei-klassisessa logiikassa, joka tällöin on jokin moniarvologiikka.

Jos määrittelemme konnektiivit Lauseen 9.2.4 kaavojen 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.

9.3 Johdatusta Boolen algebroihin

$\mathcal{P}(\mathbf{X})$ yhdessä perusoperaatioiden yhdiste, leikkaus ja komplementti muodostaa algebrallisen struktuurin, jota merkitsemme symbolijonolla $\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{\neg}, \emptyset, \mathbf{X}\rangle$. Tällaista struktuuria kutsutaan *Boolen algebraksi.*

Vastaava algebrallinen struktuuri karakteristisiten funktioiden joukolle on $\mathrm{Ch}(\mathbf{X})$ on $\langle \mathrm{Ch}(\mathbf{X}), \vee, \wedge, \neg, 0, 1\rangle$.

Palautamme vielä mieleen edellä määritellyt samaistusfunktiot (12):

$$\varphi(A) := \chi_A \quad \text{ja} \quad \psi(\chi) := \{\, x \in \mathbf{X} \mid \chi(x) = 1 \,\}$$

Yhdistämällä nämä edellä oleviin tarkasteluihin saamme laskukaavat muotoihin:

Seuraus 9.3.1 Samaistuskuvaus 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) $\varphi(\emptyset) = 0, \;\; \varphi(\mathbf{X}) = 1$

Struktuurit $\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{-}, \emptyset, \mathbf{X}\rangle$ ja $\langle \mathrm{Ch}(\mathbf{X}), \vee, \wedge, \neg, 0, 1\rangle$ ovat tässä mielessä isomorfiset, mikä perustelee algebrallisesti sen, 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 epätyhjässä joukossa $\mathbf{B}$ ja olkoot alkiot $\mathbf{0}$ ja $\mathbf{1}$ joukon $\mathbf{B}$ sellaisia alkioita, että seuraavat aksioomat ovat voimassa:

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

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

(BA2) Jokaiselle alkiolla $x \in \mathbf{B}$ 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 $x, y, z \in \mathbf{B}$ 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 $x \in \mathbf{B}$ kohti on olemassa sellainen alkio $x' \in \mathbf{B}$, että

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

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

Tällöin joukko $\mathbf{B}$ yhdessä mainittujen operaatioiden kanssa muodostaa Boolen algebran

$$\mathcal{B} = (\mathbf{B}, \wedge, \vee, ', \mathbf{0}, \mathbf{1}).$$

On helppoa todeta tämän määritelmän perusteella, että $\langle \mathcal{P}(\mathbf{X}), \cup, \cap, ^{-}, \emptyset, \mathbf{X}\rangle$ ja $\langle \mathrm{Ch}(\mathbf{X}), \vee, \wedge, \neg, 0, 1\rangle$ ovat todella Boolen algebroja.

10 JOUKKOJEN ALKIOMÄÄRISTÄ

Äärellisiä ja äärettömiä joukkoja on alustavasti käsitelty jo Luvussa 3.5. Tarkastellaan nyt keinoja vertailla joukkojen ”suuruuksia”. Jos joukko $\mathbf{X}$ on äärellinen, sen koon mitaksi voidaan luonnollisesti ottaa alkioiden lukumäärä $\#\mathbf{X}$. Jotta myös äärettömien joukkojen kokoja päästään vertailemaan, määritellään joukkojen välisten funktioiden avulla abstraktimpi käsite kardinaaliluku eli kardinaliteetti. Joukon kardinaaliluku on alkiomäärän käsitteen *yleistys* siinä mielessä, että sen rajoittuma äärellisten joukkojen luokkaan voidaan *samaistaa* joukkojen alkioiden lukumäärien kanssa. Määrittelyn yhteydessä joukon $\mathbf{X}$ kardinaalilukua merkitään $\mathrm{card}\,\mathbf{X}$, mutta kun samaistus on suoritettu, siirrytään käyttämään alkiomäärämerkintää $\#\mathbf{X}$, joka äärellisen joukon yhteydessä tulkitaan kardinaaliluvun yksikäsitteisesti määräämäksi perusluvuksi $n = \#\mathbf{X} \in \mathbf{N}_0$.

10.1 Mahtavuuksien vertailu

Lähdetään liikkeelle joukkojen suhteellisesta suuruudesta.

Määritelmä 10.1.1 Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ joukkoja. Sanotaan, että

1) joukot $\mathbf{X}$ ja $\mathbf{Y}$ ovat *yhtä mahtavat*, jos joko $\mathbf{X} = \mathbf{Y} = \emptyset$ tai on olemassa bijektio $\mathbf{X} \to \mathbf{Y}$; merkitään $\mathbf{X} \simeq \mathbf{Y}$.

2) joukko $\mathbf{X}$ on *korkeintaan yhtä mahtava* kuin $\mathbf{Y}$ (tai joukko $\mathbf{Y}$ on *vähintäin yhtä mahtava* kuin $\mathbf{X}$), jos joko $\mathbf{X} = \emptyset$ tai on olemassa injektio $\mathbf{X} \to \mathbf{Y}$; merkitään $\mathbf{X} \preceq \mathbf{Y}$.

3) joukko $\mathbf{Y}$ on *(aidosti) mahtavampi* kuin $\mathbf{X}$, jos joko $\mathbf{X} = \emptyset$ ja $\mathbf{Y} \neq \emptyset$, tai on olemassa injektio, mutta ei bijektiota $\mathbf{X} \to \mathbf{Y}$; merkitään $\mathbf{X} \prec \mathbf{Y}$.

Esimerkki 10.1.2 Tarkastellaan reaalista eksponenttifunktiota $\exp : \mathbb{R} \to \mathbb{R}$ ja muodostetaan funktio $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) := \frac{e^x}{e^x + 1}.$$

Analyysin keinoin nähdään helposti, että f on jatkuva, aidosti kasvava ja

$$\lim_{x \to -\infty} f(x) = 0, \quad \lim_{x \to \infty} f(x) = 1.$$

Funktio f on siis bijektio $\mathbb{R} \to]0, 1[$, ja siten $\mathbb{R} \simeq]0, 1[$.

Lause 10.1.3 ”Yhtämahtavuus” $\simeq$ on ekvivalenssirelaatio kaikkien joukkojen luokassa.

Todistus. Harjoitustehtävä. □

Puetaan lauseiksi intuitiivisesti ilmeiset äärellisten joukkojen yhdisteiden ja tulojen alkiomääriä koskevat tulokset. Merkintä $\#\mathbf{X}$ tarkoittaa edelleenkin äärellisen joukon $\mathbf{X}$ alkioiden lukumäärää.

Lause 10.1.4 Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ äärellisiä joukkoja.

a) Jos $\mathbf{X} \subseteq \mathbf{Y}$, niin $\#\mathbf{X} \leq \#\mathbf{Y}$.

b) Jos $\mathbf{X} \subset \mathbf{Y}$, niin $\#\mathbf{X} < \#\mathbf{Y}$.

Todistus. a) Jos $\mathbf{X} = \mathbf{Y}$, on asia selvä; muussa tapauksessa riittää todistaa vahvempi väite b). Todistetaan väite b) induktiolla luvun $m = \#\mathbf{Y} \in \mathbf{N}$ suhteen.

1) Olkoon $\#\mathbf{Y} = 1$. Koska tällöin $\mathbf{X} = \emptyset$, on $\#\mathbf{X} = 0 < 1 = \#\mathbf{Y}$.

2) Oletetaan, että väite on tosi joukoille, joiden kardinaaliluku $= m \in \mathbf{N}$. Olkoon $\mathbf{Y} = \{y_1, y_2, \ldots, y_m, y_{m+1}\}$ ja $\mathbf{X} \subset \mathbf{Y}$. Tällöin on olemassa $y_k \in \mathbf{Y}\backslash\mathbf{X}$. Kuvaus $f : \mathbf{Y}\backslash\{y_k\} \to [m]$,

$$f(y_i) := \begin{cases} i, & \text{kun } i < k, \\ i{-}1, & \text{kun } i > k, \end{cases}$$

on selvästi bijektio, joten $\#(\mathbf{Y}\backslash\{y_k\}) = m$. Koska $\mathbf{X} \subseteq \mathbf{Y}\backslash\{y_k\}$, on induktio-oletuksen mukaan

$$\#\mathbf{X} \leq m < m + 1 = \#\mathbf{Y}.$$

Siis väite on tosi arvolla $m{+}1$. Induktioperiaatteen mukaan väite b) on tosi kaikilla $\mathbf{Y}$, joille $\#\mathbf{Y} = m \in \mathbf{N}$. □

10.2 Joukkojen alkiomääriä

Lause 10.2.1 (summaperiaate) Jos $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_p$, $p \in \mathbf{N}$, on kokoelma äärellisiä joukkoja, jotka ovat pareittain erillisiä, ts. $\mathbf{X}_i \cap \mathbf{X}_j = \emptyset$ kaikilla $i \neq j$, niin niiden yhdiste on äärellinen ja

$$\#\left(\bigcup_{j=1}^{p} \mathbf{X}_j\right) = \sum_{j=1}^{p} \#\mathbf{X}_j.$$

Todistus. Todistetaan väite tapauksessa $p = 2$. Yleinen tapaus on helppo todistaa tätä käyttäen induktiolla (harjoitustehtävä). Olkoot $\mathbf{X}$ ja $\mathbf{Y}$ äärellisiä joukkoja,

joille $\mathbf{X} \cap \mathbf{Y} = \emptyset$. Olkoot $n = \#\mathbf{X}$, $m = \#\mathbf{Y}$ ja kuvaukset $f : \mathbf{X} \to [n]$, $g : \mathbf{Y} \to [m]$ bijektioita. Tällöin kuvaus $h : \mathbf{X} \cup \mathbf{Y} \to [n+m]$,

$$h(z) := \begin{cases} f(z), & \text{kun } z \in \mathbf{X}, \\ g(z) + n, & \text{kun } z \in \mathbf{Y}, \end{cases}$$

on bijektio. Täten $\#(\mathbf{X} \cup \mathbf{Y}) = n + m = \#\mathbf{X} + \#\mathbf{Y}$. □

Lause 10.2.2 Kahden äärellisen joukon A ja B alkiomäärille on voimassa

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

Kolmen äärellisen joukon A, B ja C pätee kaava

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

Lauseiden 10.2.1 ja 10.2.2 yleistys *joukkojen yleinen yhteenlaskukaava* eli *summa- ja erotusperiaate*: ■

Lause 10.2.3 (summa- ja erotusperiaate) Jos $A_1, \ldots, A_n$ ovat äärellisiä joukkoja, niin

$$\begin{aligned} \#(A_1 \cup \ldots \cup A_n) = \sum_{i=1}^{n} \#A_i &- \sum_{1 \le i < j \le n} \#(A_i \cap A_j) \\ &+ \sum_{1 \le i < j < k \le n} \#(A_i \cap A_j \cap A_k) \\ &- \cdots + (-1)^{n-1} \#(A_1 \cap \ldots \cap A_n). \end{aligned}$$

Todistus. Merkitään $\mathbf{X} = A_1 \cup \ldots \cup A_n$. Jos $x \in \mathbf{X}$, on $x \in A_i$ jollekin $i \in [n]$, joten

$$\begin{aligned} 1 &= \chi_{\mathbf{X}} \\ &= 1 - (1 - \chi_{A_1})(1 - \chi_{A_2}) \cdots (1 - \chi_{A_n}) \\ &= 1 - \Bigg(1 - \sum_{i=1}^{n} \chi_{A_i} + \sum_{1 \le i < j \le n} \chi_{A_i} \chi_{A_j} \\ &\qquad - \sum_{1 \le i < j < k \le n} \chi_{A_i} \chi_{A_j} \chi_{A_k} + \cdots + (-1)^n \chi_{A_1} \cdots \chi_{A_n} \Bigg) \\ &= \sum_{i=1}^{n} \chi_{A_i} - \sum_{1 \le i < j \le n} \chi_{A_i} \chi_{A_j} + \sum_{1 \le i < j < k \le n} \chi_{A_i} \chi_{A_j} \chi_{A_k} \\ &\qquad - \cdots + (-1)^{n-1} \chi_{A_1} \cdots \chi_{A_n}. \end{aligned}$$

Lauseen 9.2.5 kohdan b) nojalla saadaan edellisestä

$$\begin{aligned}\#(A_1 \cup \ldots \cup A_n) = \#\mathbf{X} &= \sum_{x\in\mathbf{X}} \chi_{\mathbf{X}}(x) \\ &= \sum_{x\in\mathbf{X}} \sum_{i=1}^{n} \chi_{A_i}(x) - \sum_{x\in\mathbf{X}} \sum_{1\le i<j\le n} \chi_{A_i\cap A_j}(x) \\ &\quad + \sum_{x\in\mathbf{X}} \sum_{1\le i<j<k\le n} \chi_{A_i\cap A_j\cap A_k}(x) \\ &\quad - \cdots + (-1)^{n-1} \sum_{x\in\mathbf{X}} \chi_{A_1\cap\ldots\cap A_n}(x).\end{aligned}$$

Vaihtamalla summausjärjestys ja ottamalla huomioon, että

$$\#A = \sum_{x\in\mathbf{X}} \chi_A(x)$$

kaikilla $A \subseteq \mathbf{X}$, saadaan

$$\begin{aligned}\#(A_1 \cup \ldots \cup A_n) &= \sum_{i=1}^{n} \sum_{x\in\mathbf{X}} \chi_{A_i}(x) - \sum_{1\le i<j\le n} \sum_{x\in\mathbf{X}} \chi_{A_i\cap A_j}(x) \\ &\quad + \sum_{1\le i<j<k\le n} \sum_{x\in\mathbf{X}} \chi_{A_i\cap A_j\cap A_k}(x) \\ &\quad - \cdots + (-1)^{n-1} \sum_{x\in\mathbf{X}} \chi_{A_1\cap\ldots\cap A_n}(x) \\ &= \sum_{i=1}^{n} \#A_i - \sum_{1\le i<j\le n} \#(A_i \cap A_j) \\ &\quad + \sum_{1\le i<j<k\le n} \#(A_i \cap A_j \cap A_k) \\ &\quad - \cdots + (-1)^{n-1} \#(A_1 \cap \ldots \cap A_n).\end{aligned}$$

□

Lause 10.2.4 Äärellisten joukkojen $\mathbf{X}$ ja $\mathbf{Y}$ tulojoukon alkiomäärille on

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

Esimerkkien 3.1.6 ja 3.4.1 perusteella voitaneen arvata seuraava potenssijoukkojen alkiomääriä koskeva tulos, joka todistetaan induktiotodistusharjoitukseksi.

Lause 10.2.5 Jos joukossa A on $n \in \mathbb{N}_0$ alkiota, niin sen potenssijoukossa $\mathcal{P}(A)$ on 2^n alkiota.

Todistus. Perustellaan väite matemaattisella induktiolla joukon alkiomäärän $n = 0, 1, 2, 3, \ldots$ suhteen.

(1) Kun $n = 0$, on asia selvä Esimerkin 3.1.6 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. ■

10.3 Äärellisen joukon ositukset

Olkoon $\mathbf{X}$ epätyhjä äärellinen joukko, jossa on $\#\mathbf{X} = n$ alkiota. Voidaan selvästikin olettaa, että $\mathbf{X} = [n]$.

Ongelma. Kuinka monta erilaista ositusta on joukossa $[n]$?

Ratkaisu saadaan seuraavalla tarkastelulla. Sanotaan, että joukon $[n]$ ositus on *k-osainen*, jos osituksessa on k kappaletta joukon $[n]$ osajoukkoja. Merkitään

$p(n) =$ joukon $[n]$ kaikkien ositusten lukumäärä,

$p(n, k) =$ joukon $[n]$ k-osaisten ositusten lukumäärä.

Selvästi $p(n, n) = 1$ ja $p(n, 1) = 1$ kaikilla $n \in \mathbf{N}$ ja $p(n) = \sum_{k=1}^{n} p(n, k)$.

Lause 10.3.1 (palautuskaava) Jos joukossa $\mathbf{X}$ on $n \in \mathbf{N}$ alkiota, niin kaikilla $n > k > 1$ on

$$p(n, k) = k\,p(n-1, k) + p(n-1, k-1).$$

Todistus. Joukon $[n]$ k-osaisia osituksia saadaan joukon $[n-1]$ osituksista seuraavilla tavoilla:

1) Joukon $[n-1]$ k-osaisen osituksen yhteen joukkoon lisätään n.

2) Joukon $[n-1]$ $(k-1)$-osainen ositus täydennetään joukolla $\{n\}$.

Lasketaan montako näitä saadaan yhteensä.

Tapa 1. Olkoon $\{A_1, \ldots, A_k\}$ joukon $[n-1]$ k-osainen ositus. Sitä vastaavat seuraavat k kappaletta joukon $[n]$ osituksia:

$$\begin{gathered}\{A_1 \cup \{n\}, A_2, \ldots, A_k\} \\ \{A_1, A_2 \cup \{n\}, \ldots, A_k\} \\ \vdots \\ \{A_1, A_2, \ldots, A_k \cup \{n\}\} \quad .\end{gathered}$$

Näin saadaan $k\,p(n-1,k)$ joukon $[n]$ k-osaista ositusta.

Tapa 2. Jokaista joukon $[n-1]$ $(k-1)$-osaista ositusta $\{B_1, \ldots, B_{k-1}\}$ vastaa joukon $[n]$ k-osainen ositus $\{B_1, \ldots, B_{k-1}, \{n\}\}$; yhteensä $p(n-1,k-1)$ ositusta.

Tavoilla 1 ja 2 saadut ositukset ovat aivan ilmeisesti erilaisia, joten

$$p(n,k) \geq k\,p(n-1,k) + p(n-1,k-1).$$

Yhtäsuuruuden osoittamiseksi riittää näyttää, että jokainen joukon $[n]$ k-osainen ositus saadaan tavalla 1 tai 2. Olkoon $\mathcal{A} := \{A_1, \ldots, A_k\}$ mielivaltainen joukon $[n]$ k-osainen ositus ja olkoon A_i alkion n sisältävä joukko. Silloin:

a) Jos $A_i \backslash \{n\} = \emptyset$, on $A_i = \{n\}$, joten ositus $\mathcal{A}$ on tyyppiä 2.

b) Jos $A_i \backslash \{n\} \neq \emptyset$, on kokoelma $\{A_1, \ldots, A_i \backslash \{n\}, \ldots, A_k\}$ eräs joukon $[n-1]$ k-osainen ositus; täten $\mathcal{A}$ on tyyppiä 1.

On osoitettu, että myös $p(n,k) \leq k\,p(n-1,k) + p(n-1,k-1)$. □

Esimerkki 10.3.2 Lasketaan ilman palautuskaavaa joukon $[6]$ kolmiosaisten ositusten määrä. Niitä on kolmea tyyppiä:

$$\begin{gathered}\big\{\{a\}, \{b\}, \{c,d,e,f\}\big\}, \\ \big\{\{a\}, \{b,c\}, \{d,e,f\}\big\}, \\ \big\{\{a,b\}, \{c,d\}, \{e,f\}\big\}.\end{gathered}$$

Ensimmäistä tyyppiä on 15, toista 60 ja kolmatta 15 erilaista, yhteensä 90 (ks. Esimerkki 10.4.1).

10.4 Stirlingin kolmio

Palautuskaavan avulla luvut $p(n,k)$ voidaan helposti laskea. Luvut voi näppärästi ilmaista nk. *Stirlingin kolmion* avulla (Taulukko 2).

$p(n,k)$	$k=1$	2	3	4	$5\ldots$	$p(n)=\sum p(n,k)$
$n=1$	1					1
2	1	1				2
3	1	3	1			5
4	1	7	6	1		15
5	1	15	25	10	1	52
6	1	31	90	65	$15\ldots$	203
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Taulukko 2: Stirlingin kolmio

Palautuskaavat (Lause 10.3.1)

$$\begin{aligned} p(n,1) &= p(n,n)=1, \\ p(n,k) &= k\,p(n{-}1,k)+p(n{-}1,k{-}1) \end{aligned}$$

ovat esimerkki kaksiulotteisesta rekursiokaavasta, ks. Luku 17.

Esimerkki 10.4.1 Palautuskaava antaa

$$p(6,3)=3\,p(5,3)+p(5,2)=3\cdot 25+15=90.$$

Selvitä, miten tämä saadaan taulukosta palautuskaavaa käyttäen ja laske vastaavaan tapaan $p(7,4)$. (Vastaus: $p(7,4)=350$.)

Huomautus 10.4.2 Ositus-ongelmassa joukon alkiot ovat nimettyjä, joten on merkittävää, *mitkä alkiot* osajoukkoon kuuluvat.

10.5 Äärettömistä joukoista - numeroituvuus

Määritelmä 10.5.1 Joukko $\mathbf{X}$ on *ääretön*, jos se ei ole äärellinen. Joukko $\mathbf{X}$ on *numeroituva*, jos sen alkiot voidaan numeroida kaikilla positiivisilla kokonaisluvuilla, ts. on olemassa bijektio joukkojen $\mathbf{X}$ ja $\mathbb{N}$ välillä. Ääretön ei-numeroituva joukko on *ylinumeroituva*.

Joukon alkioiden määrä ilmaisee joukon *mahtavuuden* eli *kardinaalisuuden*. Joukon $\mathbf{X}$ mahtavuutta esittää ns. *kardinaaliluku*, jota merkitään symbolilla $\mathrm{card}\,\mathbf{X}$, tai myös $\#\mathbf{X}$.

Joskus sanotaan korostaen, että joukko on *numeroituvasti ääretön*, mutta tällöin yleensä numeroituviksi luetaan myös äärelliset joukot.

On selvää, että äärellisen joukon osajoukko on äärellinen. Myös minkä tahansa joukon äärellisen joukon leikkaus on äärellinen. Ilmeistä on myös, että kahden äärellisen joukon yhdiste 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.

Esimerkki 10.5.2 a) Positiivisten parillisten kokonaislukujen joukko on numeroituva. Bijektio on tällöin muotoa $f(n) := 2n$.

b) Kokonaislukujen joukko on numeroituva. Numeroiminen voidaan tehdä esimerkiksi seuraavasti:

$1 \mapsto 0, 2 \mapsto 1, 3 \mapsto -1, 4 \mapsto 2, 5 \mapsto -2, 6 \mapsto 3, 7 \mapsto -3, \ldots$

Tällainen bijektio on muotoa $g : \mathbb{N} \to \mathbb{Z}$,

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

c) $\mathbb{R}$ voidaan osoittaa ylinumeroituvaksi, samoin $\mathbb{R} \setminus \mathbb{Q}$, mutta $\mathbb{Q}$ on numeroituva.

Selvästi äärellisen joukon ja numeroituvan joukon yhdiste on numeroituva ja kahden numeroituvan joukon yhdiste on numeroituva.

Jos numeroituvasta joukosta vähennetään äärellinen joukko, on erotus numeroituva.

11 LUKUTEORIAN ALKEITA

Lukuteoriassa käsitellään kokonaislukujen tiettyjä ominaisuuksia tai sellaisia reaali- ja kompleksilukujen ominaisuuksia, jotka ovat läheisessä yhteydessä kokonaislukuihin. Aluksi esitellään joitakin tunnettuja lukuteorian ongelmia, joista vain osaa on tässä esityksessä mahdollista käsitellä tarkemmin.

Lukuteoreettisia probleemoja

Alkuluku on sellainen kokonaisluku $p > 1$, jolla ei ole muita positiivisia tekijöitä kuin luku 1 ja p itse.

I Multiplikatiiviset probleemat

Ongelmia, jotka käsittelevät lukujen jaollisuutta, sanotaan *multiplikatiivisiksi*.

(1) Lukuteorian peruslause eli **Aritmetiikan peruslause**

Jokainen kokonaisluku $n \geq 2$ voidaan esittää yksikäsitteisesti (tekijöiden järjestystä lukuunottamatta) alkulukujen tulona

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

missä p_1, p_2, …, p_r ovat alkulukuja ja a_1, a_2, …, $a_r \in \mathbb{N}$.

(2) Kokonaisluvun kanssa jaottomien lukujen määrä

Olkoon $\phi(n)$ kokonaisluvun n kanssa jaottomien positiivisten kokonaislukujen määrä, ts. luvun n kanssa suhteellisten alkulukujen määrä

$$\phi(n) := \#\{k \in \mathbb{N} \mid k \leq n,\ \text{syt}(k, n) = 1\}.$$

Funktiota $\phi : \mathbb{N} \to \mathbb{N}$ sanotaan *Eulerin funktioksi* (*Euler totient function*, *Euler's phi*).

Esimerkiksi $\phi(5) = 4$, sillä $\text{syt}(5, k) = 1$ kaikilla $k = 1, 2, 3, 4$, mutta $\phi(6) = 2$, sillä vain $\text{syt}(6, 1) = 1$ ja $\text{syt}(6, 5) = 1$.

Jos $m \in \mathbb{N}$, niin $\phi(m) = m-1$ jos ja vain jos m on alkuluku.

Eulerin funktiolla on seuraavat ominaisuudet:

1. Jos p ja q ovat keskenään jaottomia, niin $\phi(pq) = \phi(p)\phi(q)$.
2. Jos erityisesti p_1, p_2, …, p_n ovat eri alkulukuja, niin

$$\phi(p_1 p_2 \cdots p_n) = \phi(p_1)\phi(p_2) \ldots \phi(p_n).$$

3. Jos p on alkuluku ja $a \in \mathbb{N}$, niin $\phi(p^a) = p^a(1 - \frac{1}{p})$.

4. Jos $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ on luvun n kanoninen esitys alkulukujen tulona (ks. Aritmetiikan peruslause), niin

$$\phi(n) = n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_r})$$

(3) Kokonaisluvun positiivisten tekijöiden lukumäärä

Olkoon $\tau(n)$ kokonaisluvun n positiivisten tekijöiden lukumäärä.

Esimerkki. a) $\tau(12) = 6$, koska luvun 12 positiiviset tekijät ovat 1, 2, 3, 4, 6 ja 12, ja niitä siis on 6 kappaletta.

b) $\tau(p) = 2$ jos ja vain jos p on alkuluku, ovathan ainoat positiiviset tekijät 1 ja$p$.

c) $\tau(2^m) = m + 1$, sillä luvun 2^m positiiviset tekijät ovat

$$1, 2, 2^2, 2^3, \ldots, 2^m.$$

Täten arvoilla $n = 2^m$ on $\tau(n) = \frac{\log n}{\log 2} + 1$.

Koska alkulukuja on äärettömän paljon, on funktiolla $\tau(n)$ arvo 2 äärettömän monella arvolla n. Toisaalta $\tau(n)$ voi saada kuinka suuria arvoja tahansa, koska $\tau(2^m) = m + 1$.

Lukuun $\tau(n)$ liittyviä kysymyksiä:

1) Mikä on lukumäärän $\tau(n)$ arvo keskimäärin, ts. mitä voidaan sanoa lausekkeen

$$\frac{1}{N} \sum_{n=1}^{N} \tau(n)$$

arvosta, kun $N \to \infty$?

2) Onko $\tau(n)\tau(m) = \tau(mn)$ aina, kun luvuilla m ja n ei ole yhteisiä tekijöitä (multiplikatiivisuus)?

3) Onko aina $\tau(n) \leq \frac{\log n}{\log 2} + 1$, ts. antavatko muotoa 2^m olevat luvut suhteellisesti suurimman τ-funktion arvon?

4) Kuinka monta ratkaisua on yhtälöllä $\tau(n) = 2$ arvoilla $n \leq N$, kun N on annettu positiivinen kokonaisluku, ts. kuinka moni luvuista 1, 2, ..., N on alkuluku?

(4) Alkulukujen jakautuminen

Olkoon $\pi(N)$ alkulukujen $p \leq N$ lukumäärä, eli

$$\pi(N) := \#\{p \in \mathbb{N} \mid p \leq N \text{ on alkuluku}\}.$$

Esimerkki. $\pi(10) = 4$, koska lukua 10 pienemmät alkuluvut ovat $2, 3, 5$ ja 7, siis 4 kappaletta.

Alkulukulause (Gauss, Legendre, Hadamard, todistettu 1896).

$$\lim_{N\to\infty} \frac{\pi(N)}{\frac{N}{\ln N}} = 1.$$

Bertrandin lause. Jos $n > 1$, niin lukujen n ja $2n$ välissä on ainakin yksi alkuluku.

Dirichlet'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 probleemoista

1) Mitkä luvut voidaan esittää kahden kokonaisluvun neliöiden summana ja montako tällaista esitystä kullakin kokonaisluvulla on?

   Esimerkiksi $5 = 1^2 + 2^2$ ja $13 = 2^2 + 3^2$, mutta luvulla 12 ei tällaista esitystä ole.

2) Mitkä luvut voidaan esittää neliömuotojen avulla?

   Esimerkiksi semidefiniitti kahden muuttujan neliömuoto

   $$x^2 + 2xy + 2y^2$$

   esittää luvun 10, sillä yhtälöllä

   $$x^2 + 2xy + 2y^2 = 10$$

   on kokonaislukuratkaisu $x = 2$, $y = 1$.

   Geometrisesti tämä tarkoittaa, että kokonaislukupiste $(2, 1)$ on ellipsin $x^2 + 2xy + 2y^2 = 10$ kehällä, ks. Kuva 18).

Kuva 18: Piste $(2, 1)$ ellipsillä $x^2 + 2xy + 2y^2 = 10$

3) **Goldbachin konjektuuri (1742):** Jokainen lukua 2 suurempi kokonaisluku voidaan esittää kolmen alkuluvun summana (hän piti muuten lukua 1 alkulukuna).

   Myöhempi versio Eulerilta sanoo: Jokainen lukua 4 suurempi parillinen kokonaisluku voidaan esittää kahden parittoman alkuluvun summana.

   Esimerkiksi $16 = 2 + 7 + 7$ ja $12 = 5 + 7$.

III Diofantoksen yhtälöt

Diofantoksen yhtälöt ovat yhden tai useamman muuttujan yhtälöitä, joilla etsitään kokonaislukuratkaisuja (tai ainakin rationaalisia ratkaisuja). Seuraavassa esimerkkejä ongelmista:

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

$$ax + by = c,$$

missä a, b ja c ovat kokonaislukuja.

Esimerkki. Etsi kokonaislukuratkaisut yhtälölle $5x + 22y = 18$.

Koska luvun $x = \frac{1}{5}(18 - 22y)$ pitää olla kokonaisluku, on $x = \frac{1}{5}(15 + 3 - 20y - 2y) = (3 - 4y) + \frac{1}{5}(3 - 2y) = 3 - 4y + z$, missä $z = \frac{1}{5}(3 - 2y)$. Edelleen ratkaistaan tästä y: $y = \frac{1}{2}(3-5z) = 1-2z+\frac{1}{2}(1-z) = 1-2z+t$, missä $t = \frac{1}{2}(1 - z)$. Parametrista t riippuvat ratkaisut saadaan sijoittamalla $z = 1 - 2t$

$$\begin{aligned} y &= \tfrac{1}{2}(3 - 5z) = -1 + 5t \\ x &= \tfrac{1}{2}(3 - 5z) = 8 - 22t, \quad t \in \mathbb{Z}. \end{aligned}$$

IV Diofantoksen 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 kokonaislukukertoimisen polynomiyhtälön

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

ratkaisu.

11.1 Jaollisuus ja tekijät

Kokonaislukuja koskevia väitteitä todistettaessa on usein edullista käyttää algebrassa todistettavaa ns. *jakoyhtälöä* (*division algorithm*).

Lause 11.1.1 (kokonaislukujen jakoyhtälö) Jos $m \in \mathbb{Z}$ ja $n \in \mathbb{N}$, on olemassa yksikäsitteisesti määrätyt luvut q, $r \in \mathbb{Z}$, joille

$$m = qn + r \text{ ja } 0 \leq r < n. \tag{15}$$

Jakoyhtälöesityksessä (15) luku q on *osamäärä* (*quotient*) ja luku r *jakojäännös* (*remainder*). On huomattava, että vaikka käsittelyssä olisi negatiivisiakin lukuja, jakojäännöksen pitää olla ei-negatiivinen; sitä sanotaankin usein *pienimmäksi ei-negatiiviseksi jäännökseksi*.

Määritelmä 11.1.2 Olkoot a, $b \in \mathbb{Z}$. Tällöin a on luvun b *tekijä* (*factor*), jos $b = ka$ jollekin $k \in \mathbb{Z}$.

Jos a on luvun b tekijä, sanotaan myös, että "a *jakaa* luvun b" tai "b on jaollinen luvulla a".

Merkintä tälle on $a \mid b$. Vastaavasti merkitään $a \nmid b$, jos a ei ole luvun b tekijä.

Luku 0 jakaa (vain) itsensä, onhan $0 = k \cdot 0$. Muutoin k on yksikäsitteinen.

Esimerkki 11.1.3 $5 \mid 10$, koska $10 = 2 \cdot 5$. Luku 3 ei jaa lukua 10, eli $3 \nmid 10$, koska ei ole sellaista kokonaislukua k, että $10 = k \cdot 3$.

Esimerkki 11.1.4 a) Jaa jakoyhtälöllä luku -243 luvulla 7.

b) Mille luvuille $n \in \mathbb{N}$ on $n \mid 24$?

Ratkaisu. a) Normaali jako antaa $-243/7 = -34 - 5/7$, joten positiivisuusvaatimuksen mukaan $-243 = (-35) \cdot 7 + 2$.

b) Ainakin $n = 1$ ja 24. Muista riittää tarkastaa luvut välillä $2 \leq n \leq 24/2 = 12$. Siis luvut ovat $n = 1, 2, 3, 4, 6, 8, 12, 24$.

Tehtävä 11.1.5 Todista, että minkään kokonaisluvun kuutio ei ole muotoa $4k+2$ millään $k \in \mathbb{Z}$.

Tekijärelaatiolla on seuraavanlaisia ominaisuuksia:

Lause 11.1.6 Olkoot a, b, c, $d \in \mathbb{Z}$. Tällöin:

1. $a \mid 0$, $1 \mid a$, $-1 \mid a$, $a \mid a$, $-a \mid a$.
2. Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
3. Jos $a \mid b$ ja $c \mid d$, niin $ac \mid bd$.
4. $a \mid 1 \quad \Leftrightarrow \quad a = 1$ tai $a = -1$.
5. $a \mid b$ ja $b \mid a \quad \Leftrightarrow \quad a = b$ tai $a = -b$.
6. Jos $a \mid b$ ja $b \neq 0$, niin $|a| \leq |b|$.
7. Jos $a \mid b_i$ kaikilla $i = 1, \ldots, n$, niin $a \mid b_1c_1 + \ldots + b_nc_n$ kaikilla $c_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$.
8. Jos $a \mid b_i$ kaikilla $i = 1, 2, \ldots, n-1$, mutta $a \nmid b_n$, niin $a \nmid b_1 + \ldots + b_n$.

Todistus. 1-7 pääosin algebrassa. Kohta 8 seuraa kohdasta 7 (harjoitustehtävä). ■

11.2 Kokonaislukujen kantaesitys

Roomalaisessa lukujärjestelmässä I, II, III, IV, ..., IX, X, ... tarvitaan kokonaislukujen esittämiseen äärettömän monta erilaista numeromerkkiä.

Positiojärjestelmässä luvun suuruuden määräävät esiintyvien numeromerkkien paikat siten, että jos kantaluku on k, niin esitys

$$a_n a_{n-1} \ldots a_1 a_0$$

tarkoittaa lukua

$$a_n k^n + a_{n-1} k^{n-1} + \ldots + a_1 k + a_0.$$

Tarvitaan siis vain $k - 1$ numeromerkkiä ja nolla.

Esimerkki 11.2.1 10-järjestelmässä

$$2056 = 2 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10 + 6.$$

Binäärijärjestelmässä (kantalukuna 2)

$$1101 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1,$$

mikä vastaa kymmenjärjestelmän lukua 13.

Kokonaislukujen jakoyhtälöstä seuraa:

Lause 11.2.2 Olkoon kantaluku $k \geq 2$. Silloin jokainen luonnollinen luku a voidaan esittää yksikäsitteisesti muodossa

$$a_n k^n + a_{n-1} k^{n-1} + \ldots + a_1 k + a_0,$$

missä $n \in \mathbb{N}_0$, $0 \leq a_i < k$ kaikilla $i = 1, 2, 3, \ldots, n$ ja $a_0 > 0$.

Merkitsemme jatkossa k-järjestelmän lukuja

$$(a_n a_{n-1} \ldots a_1, a_0)_k.$$

Jos lukua k ei merkitä näkyviin, on kyseessä 10-järjestelmän luku.

Esimerkki 11.2.3 6-järjestelmän luku $(1234)_6$ tarkoittaa esitystä

$$1 \cdot 6^3 + 2 \cdot 6^2 + 3 \cdot 6^1 + 4 \cdot 6^0.$$

Esimerkki 11.2.4 Kymmenjärjestelmän luku 4457 saadaan 11-järjestelmään vaikkapa jakoyhtälön (Lause 11.1.1) avulla: ■

$$\begin{aligned} 4457 &= 405 \cdot 11 + 2 = (36 \cdot 11 + 9) \cdot 11 + 2 \\ &= ((3 \cdot 11 + 3) \cdot 11 + 9) \cdot 11 + 2 = 3 \cdot 11^3 + 3 \cdot 11^2 + 9 \cdot 11 + 2 \\ &= (3392)_{11}. \end{aligned}$$

Esimerkki 11.2.5 Harjoitellaan yhteen- ja kertolaskua 4-järjestelmässä kymmenjärjestelmän kautta:

$$\begin{aligned} (23)_4 + (131)_4 &= (2 \cdot 4 + 3) + (1 \cdot 4^2 + 3 \cdot 4 + 1) = 11 + 29 = 40 \\ &= 2 \cdot 4^2 + 2 \cdot 4 + 0 = (220)_4 \\ (23)_4 \cdot (131)_4 &= 11 \cdot 29 = 319 = 1 \cdot 4^4 + 0 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 = (10333)_4. \end{aligned}$$

Voidaan myös laskea suoraan 4-järjestelmässä, vaikkapa katsoen yhteen- ja kertotaulukosta Taulukko 3. Silloin vanhalla tutulla "alekkainlaskulla":

$$\begin{array}{r} (23)_4 \\ (131)_4 \\ \hline (220)_4 \end{array} \qquad \begin{array}{r} (131)_4 \\ (23)_4 \\ \hline (1113)_4 \\ (322)_4 \\ \hline (10333)_4 \end{array}$$

$1+1=2$	$1\cdot 1=1$
$1+2=3$	$1\cdot 2=2$
$1+3=10$	$1\cdot 3=3$
$2+2=10$	$2\cdot 2=10$
$2+3=11$	$2\cdot 3=12$
$3+3=12$	$3\cdot 3=21$

Taulukko 3: 4-järjestelmän yhteen- ja kertolaskutaulu

11.3 Suurin yhteinen tekijä (syt) ja Eukleideen algoritmi

Määritelmä 11.3.1 Olkoot $a_1, \ldots, a_n \in \mathbb{Z}$ lukuja, joista ainakin yksi ei ole nolla. Lukujoukon $\{a_1, \ldots, a_n\}$ *suurin yhteinen tekijä* (*greatest common divisor, gcd*) $d = \text{syt}(a_1, \ldots, a_n)$ on suurin luku $d \in \mathbb{N}$, jolle $d \mid a_i$ kaikilla $i = 1, 2, \ldots, n$. Ehtomuotoisena ilmauksena tämä on

$$\text{syt}(a_1, \ldots, a_n) = \max\{\, k \in \mathbb{Z} : k \mid a_i \text{ kaikilla } i = 1, 2, 3, \ldots, n \,\}.$$

Mikäli $\text{syt}(a, b) = 1$, lukuja a ja b sanotaan *keskenään jaottomiksi* tai *suhteellisiksi alkuluvuiksi* (*relatively prime, coprime*).

On ilmeistä, että $\text{syt}(a, b)$ on lukujen a ja b sellainen yhteinen tekijä, joka on positiivinen ja jaollinen kaikilla näiden lukujen yhteisillä tekijöillä. Suurin yhteinen tekijä voidaan siis karakterisoita myös näin:

Lause 11.3.2 Olkoot a ja b kokonaislukuja, joista ainakin toinen on erisuuri kuin 0, ja olkoon d positiivinen kokonaisluku. Silloin d on lukujen a ja b suurin yhteinen tekijä, jos ja vain jos seuraavat kaksi ehtoa toteutuvat:

1. $d \mid a$ ja $d \mid b$, ja
2. jos $c \mid a$ ja $c \mid b$, niin $c \mid d$.

Huomautus 11.3.3 Käytännössä syt voidaan määrittää

(a) etsimällä lukujen a ja b yhteiset tekijät ja valitsemalla niistä suurin.

(b) jakamalla luvut alkutekijöihin, esimerkiksi

$$\left.\begin{array}{l} 4 = 2\cdot 2 \\ 12 = 2\cdot 2\cdot 3 \end{array}\right\} \Rightarrow \text{syt}(4, 12) = 2\cdot 2 = 4.$$

(c) jakoalgoritmilla, kuten Eukleideen algoritmilla.

Lause 11.3.4 (Eukleideen algoritmi) Olkoot a ja b positiivisia kokonaislukuja ja olkoon $a \geq b$. Jos $b \mid a$, niin $\text{syt}(a,b) = b$. Jos $b \nmid a$, sovella toistuvasti jakoyhtälöä:

$$\begin{aligned} a &= bq_0 + r_0,\ 0 < r_0 < b \\ b &= r_0q_1 + r_1,\ 0 \leq r_1 < r_0 \\ r_0 &= r_1q_2 + r_2,\ 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3,\ 0 \leq r_3 < r_2, \\ &\vdots \end{aligned}$$

Prosessi päättyy, kun saadaan jakojäännös $r_{n+1} = 0$. Tämän täytyy tapahtua äärellisellä määrällä askelia, ts. jollekin kokonaisluvulle n on

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n,\ 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

Viimeistä edellinen jakojäännös $r_n = \text{syt}(a,b)$.

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:

$$b > r_0 > r_1 > r_2 > \ldots > r_n > r_{n+1} = 0.$$

Eukleideen algoritmista voidaan päätellä:

Lause 11.3.5 Jos a ja b eivät molemmat ole nollia, niin $\text{syt}(a,b)$ on aina olemassa ja on yksikäsitteinen.

Kirjataan vielä joitakin suurimman yhteisen tekijän perusominaisuuksia, mm. liitännäisyys ja lineaarikombinaatioesitys.

Lause 11.3.6 Lukujen suurimmalle yhteiselle tekijälle pätee aina, kun syt on määritelty:

1) $\text{syt}(a+bm,b) = \text{syt}(a,b)$ (käy Eukleideen algoritmin perusteluun)

2) $\text{syt}(ca_1, ca_2, \cdots, ca_n) = c\,\text{syt}(a_1, a_2, \cdots, a_n)$ kaikilla $c \in \mathbb{N}$.

3) $\text{syt}(a_1, \ldots, a_{n-1}, a_n) = \text{syt}(\text{syt}(a_1, \ldots, a_{n-1}), a_n)$.

4) Jos $\text{syt}(a_1, \ldots, a_n) = d$, on olemassa sellaiset luvut $x_1, \ldots, x_n$, että

$$x_1a_1 + \ldots + x_na_n = d.$$

5) Jos $a \mid bc$ ja $\text{syt}(a,b) = 1$, niin $a \mid c$.

Lause 11.3.7 Diofantoksen yhtälöllä

$$ax + by = c$$

on ratkaisu, jos ja vain jos $\text{syt}(a, b) \mid c$.

Geometrisesti lause voidaan tulkita siten, että suora $ax + by = c$ kulkee ainakin yhden xy-tason verkkopisteen (kokonaislukupisteen) kautta, mikäli $\text{syt}(a, b) \mid c$. Koska suoran kulmakerroin on rationaaliluku, suora kulkee itse asiassa äärettömän monen verkkopisteen kautta.

11.4 Alkuluvut ja tekijöihin jako

Määritelmä 11.4.1 Luonnollista lukua $p \geq 2$ sanotaan *alkuluvuksi* (*prime number*), jos se on jaollinen vain luvuilla ± 1 ja $\pm p$.

Jos alkuluku p on luvun a tekijä, sitä sanotaan luvun a *alkutekijäksi*. Jos luku a ei ole alkuluku, niin a on *yhdistetty luku* (*composed*).

Esimerkki 11.4.2 Alkulukuja ovat mm. $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Luku 1 ei ole alkuluku eikä yhdistetty luku. Luku 2 on ainoa parillinen alkuluku.

Kokonaislukujen joukossa alkuluvuilla on keskeinen asema. Ne ovat yksinkertaisimpia lukuja, joiden avulla kaikki kokonaisluvut voidaan muodostaa käyttäen pelkästään kertolaskua. Tämän kokonaisluvun alkutekijöihin jaon takaa algebrassa todistettava *Aritmetiikan peruslause*.

Lause 11.4.3 (Aritmetiikan peruslause) Jokainen luonnollinen luku $n \geq 2$ on esitettävissä (järjestystä vaille) yksikäsitteisellä tavalla tulona

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

missä $p_1, p_2, \ldots, p_r$ ovat alkulukuja ja $a_1, a_2, \ldots, a_r \in \mathbb{N}$.

Tätä esitystä kutsutaan luvun n *kanoniseksi esitykseksi* tai *alkutekijäesitykseksi*.

Lause 11.4.4 (Eukleideen lause) Alkulukuja äärettömän monta.

Lause 11.4.5 (Dirichlet'n lause arvoilla $a = 3$ ja $b = 2$) Muotoa $3n + 2$ olevia alkulukuja on äärettömän monta.

Alkulukuja on siis äärettömän paljon, mutta suurten lukujen joukossa niitä on yhä harvemmassa. Jokainen alkuluku (paitsi 2 ja 3) on muotoa $6n \pm 1$, mutta kaikki

nämä eivät ole alkulukuja. Vuonna 1960 suurin tunnettu alkuluku oli $2^{3217}-1$, v. 1989 jo $391581 \cdot 2^{216193}-1$ ja v. 2001 jo $2^{13466917}-1$. Nykyisen tilanteen ja paljon muuta infoa saa osoitteesta

`http://www.utm.edu/research/primes/largest.html`

Tehtävä 11.4.6 Selvitä kuinka monta numeroa on luvun $2^{13466917}-1$ normaalissa kymmenjärjestelmäesityksessä.

Alkuluvut ovat nykyäänkin intensiivisen tutkimuksen kohteena. Monet koodaus-, salakirjoitus- ja tietosuojausmenetelmät perustuvat siihen, että annetun kokonaisluvun alkutekijöihin jako on hidas prosessi. Esimerkiksi satanumeroisen kokonaisluvun jako kestää nykyään noin kuukauden parhaalla tunnetulla ohjelmalla, joka toimii hajautetun laskennan periaatteella käyttäen hyväksi satojen tietokoneiden joutoaikaa. Kun käytetään 155-numeroisia (512 bittiä) lukuja, on jakoaika n. 40 000-kertainen.

Esitetään lopuksi antiikin kreikkalaisen matemaatikon Eratostheneen kehittämä menetelmä *Eratostheneen seula* joukon $[N]$ alkulukujen etsimiseksi.

Olkoon $a \leq N$ mielivaltainen luonnollinen luku. Jos a on yhdistetty luku, sillä on alkutekijöinä vain lukuja p, $p \leq \sqrt{a} \leq \sqrt{N}$.

> *Kirjoitetaan luvut* $1, 2, 3, \ldots, N$ *jonoon. Poistetaan ensin joukosta* $[N]$ *luku* 1. *Sitten poistetaan kaikki luvulla* 2 *jaolliset paitsi* 2, *luvulla* 3 *jaolliset paitsi* 3, *luvulla* 4 *jaolliset (turhaa!), luvulla* 5 *jaolliset paitsi itse* 5, *jne.*

Lopuksi jäävät jäljelle alkuluvut $2 \leq p \leq N$, ks. Kuvan 19 algoritmi.

Aseta $I = [N]$; $I_0 = I \setminus \{1\}$; alkuluvut $= \emptyset$;
while $(I_0 \neq \emptyset)$
luku $= \min I_0$;
$I_0 = I_0 \setminus (\text{luku} * I)$;
alkuluvut $=$ alkuluvut $\cup \{\text{luku}\}$;
end

Kuva 19: Eratostheneen seula algoritmina

Alkuehtoista **while**-silmukkaa toistetaan, kunnes joukko I_0 on tyhjä. Muuttuja ”luku” saa vuorollaan alkulukuarvot $2, 3, \ldots$, jotka kerätään joukkoon ”alkuluvut”. Algoritmi on suoraviivainen, mutta käytännössä raskas toteuttaa.

Esimerkki 11.4.7 Yhdistetylle luvulle $N = 48$ on $\sqrt{N} < 7$, joten alkutekijöitä ovat vain luvut 2, 3 ja $5 < 7$. Seuraavassa on alleviivattu kaikki lukua $N = 48$ pienemmät alkuluvut:

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

11.5 Kongruenssi

Määritelmä 11.5.1 Olkoot $m \in \mathbb{N}$ ja $a, b \in \mathbb{Z}$. Tällöin a *on kongruentti luvun* b *kanssa modulo* m, jos

$$m \mid (a - b).$$

Kongruenttisuutta merkitään $a \equiv b \pmod{m}$. Jos taas $m \nmid (a-b)$, sanomme, että a *on epäkongruentti luvun* b *kanssa modulo* m, ja tätä merkitään $a \not\equiv b \pmod{m}$. Luku m on *moduli*.

Esimerkki 11.5.2 Jakoyhtälön ja kongruenssin yhteys: Jos $n = qm + r$, niin $m \mid n - r$ eli $n \equiv r \pmod{m}$. Jos $m \mid n$, niin $n \equiv 0 \pmod{m}$ ja kääntäen.

Esimerkki 11.5.3 1) $627 \equiv 427 \pmod{10}$, koska $10 \mid 627 - 427$.

2) $31 \equiv -9 \pmod{10}$, koska $10 \mid 31 + 9$.

3) $7 \not\equiv 5 \pmod{10}$, koska 10 ei jaa lukua $7 - 5$.

4) $7 \equiv 5 \pmod{2}$. Yleensäkin parittomat luvut ovat keskenään kongruentteja $\bmod 2$.

5) $a \equiv b \pmod{1}$ on voimassa jokaisella $a, b \in \mathbb{Z}$.

Kongruenssi merkittävä paitsi algebrallisesti, myös relaatio-opillisesti, sillä se on ekvivalenssi, ks. tarkemmin Luvut 5 ja 7.

Lause 11.5.4 (Kongruenssi on ekvivalenssirelaatio) Olkoon $m \in \mathbb{N}$ ja olkoot $a, b, c \in \mathbb{Z}$. Tällöin ”olla kongruentti” on ekvivalenssirelaatio joukossa $\mathbb{Z}$:

1. $a \equiv a \pmod{m}$ kaikilla $a \in \mathbb{Z}$. (refleksiivisyys)
2. Jos $a \equiv b \pmod{m}$, niin $b \equiv a \pmod{m}$. (symmetrisyys)
3. Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $a \equiv c \pmod{m}$ (transitiivisuus)

Lause 11.5.5 Kongruenssille on voimassa:

1. Jos $a \equiv b \pmod m$ ja $c \equiv d \pmod m$, niin $a+c \equiv b+d \pmod m$.
2. Jos $a_i \equiv b_i \pmod m$ kaikilla $i = 1, \ldots, n$, niin $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m$.
3. Jos $a \equiv b \pmod m$, niin $a+c \equiv b+c \pmod m$ ja ja $ac \equiv bc \pmod m$.
4. Jos $a \equiv b \pmod m$ ja $c \equiv d \pmod m$, niin $ac \equiv bd \pmod m$.
5. Jos $a_i \equiv b_i \pmod m$ kaikilla $i = 1, \ldots, n$, niin $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod m$.
6. Jos $a \equiv b \pmod m$ ja $n \in \mathbb{N}$, niin $a^n \equiv b^n \pmod m$.
7. Jos $a \equiv b \pmod m$ ja polynomi $P(x) = a_n x^n + \ldots + a_1 x + a_0$ on kokonaislukukertoiminen, niin $P(a) \equiv P(b) \pmod m$.

Transitiivisuuden

Jos $a \equiv b \pmod m$ ja $b \equiv c \pmod m$, niin $a \equiv c \pmod m$

nojalla voidaan kirjoittaa kongruensseja yhteen: $a \equiv b \equiv c \pmod m$, mikäli kaikki luvut a, b, c ovat kongruentteja saman luvun kanssa modulo m.

Esimerkki 11.5.6 Mikä on jäännös, kun luku

$$N := 18^2 \cdot 13^6 + 20^4 \cdot 10^7$$

jaetaan luvulla 11, ts. mikä on pienin $x \geq 0$, jolle $N \equiv x \pmod{11}$?

Ratkaisu. Perustele itse seuraava laskeskelu:

Koska $18 \equiv -4 \pmod{11}$, on $18^2 \equiv (-4)^2 \equiv 16 \equiv 5 \pmod{11}$.

Koska $13 \equiv 2 \pmod{11}$, on $13^3 \equiv 8 \equiv -3 \pmod{11}$, ja siten $13^6 \equiv (-3)^2 = 9 \equiv -2 \pmod{11}$.

Koska $20 \equiv -2 \pmod{11}$, on $20^4 \equiv (-2)^4 \equiv 5 \pmod{11}$.

Koska $10 \equiv -1 \pmod{11}$, on $10^7 \equiv (-1)^7 \equiv -1 \pmod{11}$.

Siis $N \equiv 5 \cdot (-2) + 5 \cdot (-1) \equiv -4 \equiv 7 \pmod{11}$. Jäännös on siis 7.

Kongruenssin jakaminen luvulla onnistuu suoraan vain erikoistapauksessa:

Lause 11.5.7 Kun $a, b, c \in \mathbb{Z}$, niin

$$[\, ac \equiv bc \,(\bmod m) \wedge \text{syt}(c, m) = 1\,] \;\Rightarrow\; [\, a \equiv b \,(\bmod m)\,]. \tag{16}$$

Todistus. Koska $m \mid ac - bc$, on $m \mid c(a-b)$. Koska $\text{syt}(m, c) = 1$, on välttämättä $m \mid a - b$ eli $a \equiv b \,(\bmod m)$. ■

Huomautus 11.5.8 Lauseen 11.5.7 ehto $\text{syt}(c, m) = 1$ on välttämätön, sillä esimerkiksi $22 \equiv 16 \,(\bmod 6)$, mutta $11 \not\equiv 8 \,(\bmod 6)$.

Supistussäännön yleisempi muoto on:

Lause 11.5.9 Jos $a, b, c \in \mathbb{Z}$, niin

$$[\, ac \equiv bc \,(\bmod m)\,] \;\Rightarrow\; \left[\, a \equiv b \,\left(\bmod \frac{m}{\text{syt}(c, m)}\right)\right]. \tag{17}$$

Todistus. Koska $m \mid ac - bc$, on $m \mid c(a-b)$. Merkitään $d := \text{syt}(c, m)$, $m = k_1 d$, $c = k_2 d$. Tällöin on $\text{syt}(k_1, k_2) = 1$. Edelleen, koska $k_1 d \mid k_2 d(a-b)$, myös $k_1 \mid k_2(a-b)$. Koska $\text{syt}(k_1, k_2) = 1$, on $k_1 \mid (a-b)$ ja siis $a \equiv b \,(\bmod k_1)$. Mutta $k_1 = \frac{m}{d}$, missä $d := \text{syt}(c, m)$, joten väite tulee todistetuksi. ■

Lukujen kongruenssiin liittyvät jäännösluokat ekvivalenssiluokkien kautta. Muistamme, että jokainen luku $a \in \mathbb{Z}$ voidaan esittää muodossa

$$a = qm + r,$$

missä r on jokin luvuista $0, 1, 2, \ldots, m-1$. Luku r oli *luvun a pienin ei-negatiivinen jäännös modulo m.*

Kaikki kokonaisluvut jakautuvat ekvivalenssiluokkiin sen mukaan, kuinka suuri tämä jäännös on. Koska kyseessä on ekvivalenssin lisäksi kongruenssi, puhumme *kongruenssiluokista* $\bmod m$.

Merkitään esimerkiksi $\langle 0 \rangle_m$ lukujoukkoa, joiden jäännös modulo m on 0, $\langle 1 \rangle_m$ joukkoa, joiden jäännös on 1, …, $\langle m-1 \rangle_m$ niitä, joiden jäännös on $m-1$.

Esimerkki 11.5.10 Kun $m = 4$, saadaan jäännösluokat

$$\begin{aligned}
\langle 0 \rangle_4 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
\langle 1 \rangle_4 &= \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
\langle 2 \rangle_4 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
\langle 3 \rangle_4 &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

Yleisesti on

$$\langle r \rangle_m = \{a \in \mathbb{Z} \mid a \equiv r \,(\bmod m)\}.$$

11.6 Lineaarinen kongruenssiyhtälö

Tarkastellaan yhden muuttujan lineaarista kongruenssiyhtälöä

$$ax \equiv b \ (\mathrm{mod}\, m).$$

Tällä yhtälöllä voi olla ratkaisuja, jopa äärettömästi, tai ei ollenkaan, riippuen siinä esiintyvien lukujen keskinäisistä suhteista.

Esimerkki 11.6.1 a) Esimerkiksi yhtälön

$$2x \equiv 5 \ (\mathrm{mod}\, 3)$$

ratkaisuina ovat ainakin luvut 1, 4, 7 ja 10. Itse asiassa, jos $x \equiv 1 \ (\mathrm{mod}\, 3)$, niin silloin $2x \equiv 2 \equiv 5 \ (\mathrm{mod}\, 3)$ eli kaikki sellaiset luvut x ovat ratkaisuja. Näin kaikki kongruenssiluokan $\langle 1 \rangle_3$ (ykkösen määräämä kongruenssiluokka modulo 3) alkiot ovat ratkaisuja yhtälölle $2x \equiv 5 \ (\mathrm{mod}\, 3)$.

b) Toisaalta yhtälöllä

$$2x \equiv 5 \ (\mathrm{mod}\, 4)$$

ei ole yhtään ratkaisua, sillä pariton luku $2x-5$ ei ole jaollinen neljällä.

c) Yhtälöllä

$$2x \equiv 4 \ (\mathrm{mod}\, 6)$$

on ratkaisuina ainakin luvut 2, 8, 14, 20 ja -1, 5, 11, 17. Itse asiassa kongruenssiluokat $\langle 2 \rangle_6$ ja $\langle 5 \rangle_6$ ovat ratkaisuja.

Todistamatta esitetään ratkeavuudelle aluksi yksinkertainen erikoistapaus:

Lause 11.6.2 Olkoon $m \in \mathbb{N}$ ja olkoot a, $b \in \mathbb{Z}$ sellaisia, että $\mathrm{syt}(a, m) = 1$. Tällöin kongruenssin

$$ax \equiv b \ (\mathrm{mod}\, m)$$

ratkaisujoukko $\{ x \in \mathbb{Z} \mid ax \equiv b \ (\mathrm{mod}\, m) \}$ koostuu tasan yhdestä kongruenssiluokasta $(\mathrm{mod}\, m)$, ts. on olemassa $x_0 \in \{ 0, 1, 2, \ldots, m-1 \}$ jonka avulla saadaan koko ratkaisujoukko

$$\langle x_0 \rangle_m = \{ x_0 + km \mid k \in \mathbb{Z} \}.$$

Esimerkki 11.6.3 Ratkaistaan kongruenssiyhtälö $26x \equiv 2 \ (\mathrm{mod}\, 15)$.

Ratkaisu. Koska $\mathrm{syt}(26, 15) = 1$, on kongruenssiyhtälöllä Lauseen 11.6.2 mukaan yksikäsitteinen ratkaisu, ja se on eräs kongruenssiluokka $\langle x_0 \rangle_{15}$ (siis modulo 15). Yksi ratkaisu x_0 voidaan etsiä kokeilemalla lukuja 0, 1, …, 5, 7 $=: x_0$. Siis ratkaisujoukko on kongruenssiluokka $\langle 7 \rangle_{15} = \{ 7 + 15k \mid k \in \mathbb{Z} \}$.

Tehtävä 11.6.4 Ratkaise kongruenssiyhtälö $58x \equiv 2 \pmod{33}$.

Esimerkki 11.6.5 Ratkaise kongruenssiyhtälö $58x \equiv 2 \pmod{32}$.

Ratkaisu. Nyt ei voida suoraan käyttää Lausetta 11.6.2. Mutta voidaan muokata yhtälöä: eräällä $k \in \mathbb{Z}$ on:

$$\begin{aligned} 58x \equiv 2 \pmod{32} &\Leftrightarrow 58x - 2 = 32k \Leftrightarrow 29x - 1 = 16k \\ &\Leftrightarrow 29x \equiv 1 \pmod{16}. \end{aligned}$$

Mutta tälle yhtäpitävälle kongruenssille on $\text{syt}(29, 16) = 1$, joten Lauseen 11.6.2 mukaan ratkaisuna on tasan yksi kongruenssiluokka $\langle x_0 \rangle_{16}$. Esimerkiksi kokeilemalla nähdään luku $x_0 = 5$ ratkaisuksi. Siis myös alkuperäisellä yhtälöllä on ratkaisuna

$$\langle 5 \rangle_{16} = \{\, 5 + 16k \mid k \in \mathbb{Z} \,\}.$$

Yleinen tulos perustuu syt:n ja yhtälön oikean puolen vakion keskinäiseen jaollisuuteen.

Lause 11.6.6 Olkoon $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ ja $d := \text{syt}(a, m)$.

a) Kongruenssiyhtälöllä

$$ax \equiv b \pmod{m}$$

on ratkaisuja jos ja vain jos $d \mid b$.

b) Jos x_0 on yhtälön eräs ratkaisu, niin täydellinen ratkaisujoukko on

$$\{\, x_0 + k \tfrac{m}{d} \mid k \in \mathbb{Z} \,\} = \langle x_0 \rangle_{\frac{m}{d}}\,.$$

Tehtävä 11.6.7 Ratkaise

a) $60x \equiv 20 \pmod{45}$.

b) $60x \equiv 30 \pmod{45}$.

12 SUUNTAAMATTOMAT VERKOT

Perinteistä *verkkojen* sovellusaluetta ovat olleet maantieteellisiin verkkoihin kuten tiestö ja vesistö, sähköisiin verkkoihin kuten puhelinverkko ja sähkönsiirtoverkko sekä materian virtaukseen putkistossa liittyvät ongelmat. Uudempia verkkoina esitettävissä olevia struktuureja ovat mm. integroidut piirit ja mikroprosessorit, tietokoneohjelman vuokaaviot, yrityksen henkilöstöstruktuurit, tietopankit ja vaikkapa kansallisen tai koko maailman talouselämän rakenne. Modernin teknologian ripeä kehitys on, paitsi tuonut lisää verkkojen avulla ratkaistavia ongelmia, myös mahdollistanut yhä laajempien perinteistenkin ongelmakokonaisuuksien käsittelyn nopeasti, tehokkaasti ja halvalla.

Tässä luvussa tarkastellaan suuntaamattomia verkkoja, Luvussa 13 suunnattuja verkkoja ja Luvussa 14 yhteisesti verkkojen isomorfisuutta ja tasoverkko-ominaisuutta sekä lyhyesti esimerkkien valossa painotettujen verkkojen ongelmia.

12.1 Suuntaamattoman verkon määrittely

Suuntaamaton verkko soveltuu sellaisten struktuurien malliksi, joissa materia tai informaatio voi liikkua kahta kohdetta yhdistävässä välineessä kumpaan suuntaan tahansa. Tätä varten käytämme karteesisen tulon asemasta *järjestämättömiä pareja*.

Määritelmä 12.1.1 Joukon $\mathbf{X}$ *ei-järjestetty tulo* itsensä kanssa on sen järjestämättömien parien $\{a_1, a_2\}$ joukko

$$\mathbf{X} \,\&\, \mathbf{X} := \big\{\, \{a_1, a_2\} \mid a_1, a_2 \in \mathbf{X} \,\big\}.$$

Huomautus 12.1.2 Järjestämätön pari $\{a_1, a_2\} \in \mathbf{X} \,\&\, \mathbf{X}$ ei tarkasti ottaen ole *joukko*, sillä kukin $\{a_i, a_i\}$ on järjestämätön pari, mutta joukkonahan siinä olisi vain yksi alkio.

Karteesisen tulon ja järjestämättömän tulon ero voidaan ilmaista seuraavasti: joukossa $\mathbf{X} \times \mathbf{Y}$

$$[\,(a_1, b_1) = (a_2, b_2)\,] \;\Leftrightarrow\; [\,a_1 = a_2 \text{ ja } b_1 = b_2\,],$$

mutta joukossa $\mathbf{X} \,\&\, \mathbf{X}$

$$[\,\{a_1, a_2\} = \{a_3, a_4\}\,] \;\Leftrightarrow\; [\,(a_1 = a_3 \text{ ja } a_2 = a_4) \text{ tai } (a_1 = a_4 \text{ ja } a_2 = a_3)\,].$$

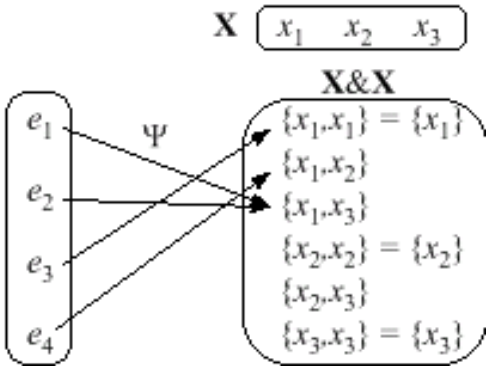
Määritelmä 12.1.3 Kolmikko $(\mathbf{X}, E, \Psi)$ on *suuntaamaton verkko* eli *graafi* (*(undirected) graph, multigraph*), jos $\mathbf{X} \neq \emptyset$ ja E ovat joukkoja ja $\Psi : E \to \mathbf{X} \,\&\, \mathbf{X}$ on kuvaus. Suuntaamattoman verkon yhteydessä käytetään nimityksiä

solmu (*vertex, node*)	=	joukon $\mathbf{X}$ alkio
kaari tai väli (*edge, link, arc*)	=	joukon E alkio
vastaavuuskuvaus (*incidence mapping*)	=	funktio Ψ

Esimerkki 12.1.4 Olkoot $\mathbf{X} = \{x_1, x_2, x_3\}$, $E = \{e_1, e_2, e_3, e_4\}$ ja

$$\Psi(e_1) = \Psi(e_2) = \{x_1, x_3\},\ \Psi(e_3) = \{x_1\},\ \Psi(e_4) = \{x_1, x_2\}.$$

Silloin kolmikko $G := (\mathbf{X}, E, \Psi)$ on suuntaamaton verkko, jossa on solmut x_1, x_2 ja x_3, kaaret e_1, e_2, e_3 sekä e_1 sekä vastaavuuskuvauksena Ψ, ks. Kuva 20.



Kuva 20: Esimerkin 12.1.4 verkko osina

Määritelmä 12.1.5 Jos $\Psi(e) = \{x, y\}$, solmut x ja y ovat kaaren e *päitä* tai *päätesolmuja* ja kaari e *yhdistää* solmut x ja y. Sanotaan myös, että kaari e *liittyy* solmuihin x ja y ja vastaavasti solmut x ja y liittyvät kaareen e. Kaksi solmua ovat *vierekkäisiä* (*adjacent*), jos ne ovat saman kaaren päitä. Kaksi kaarta ovat *rinnakkaisia*, jos niillä on yhteiset päätesolmut, ja *vierekkäisiä*, jos niillä on ainakin yksi yhteinen pää. Jos $\Psi(e) = \{x, x\}$, on e *silmukka* tai *luuppi*. Tällöin merkitään lyhyesti $\Psi(e) = \{x\}$. Solmun $x \in \mathbf{X}$ *asteluku* (*degree*) on

$$d_G(x) := \#\big\{\, e \in E \mid \Psi(e) = \{x, y\}, y \neq x \,\big\} + 2 \cdot \#\big\{\, e \in E \mid \Psi(e) = \{x\} \,\big\},$$

ts. niiden kaarien lukumäärä, joilla on päänä x, kun silmukat lasketaan kahdesti. Solmu $x \in \mathbf{X}$ on *erillinen* tai *eristetty* (*isolated*), jos $d_G(x) = 0$, ts. jos se ei ole minkään kaaren pää.

Tehtävä 12.1.6 Selvitä yllä kuvattuja asioita Esimerkin 12.1.4 verkosta.

Havainnollisempia verkon esitystapoja löytyy Luvusta 12.4.

12.2 Suuntaamattoman verkon ominaisuuksia

Määritelmä 12.2.1 Suuntaamaton verkko $(\mathbf{X}, E, \Psi)$ on

- *surkastunut* eli *degeneroitunut*, jos $E = \emptyset$.
- *äärellinen*, jos joukot $\mathbf{X}$ ja E ovat äärellisiä, muutoin *ääretön*.
- *täydellinen*, jos jokaisen solmuparin $x \neq y$ välillä on ainakin yksi kaari.
- *yksinkertainen*, jos siinä ei ole silmukoita eikä rinnakkaisia kaaria.

Huomautus 12.2.2 a) Jokaisesta verkosta saadaan täydellinen lisäämällä puuttuvat kaaret, samoin verkosta saadaan yksinkertainen poistamalla silmukat ja liiat rinnakkaiset kaaret.

b) Yksinkertaisessa verkossa solmupari $\{x, y\}$ ja niitä yhdistävä kaari $e = \Psi^{-1}(\{x, y\})$ usein samaistetaan ja puhutaan lyhyesti kaaresta $e \sim \{x, y\}$.

Lause 12.2.3 Jos $G = (\mathbf{X}, E, \Psi)$ on äärellinen suuntaamaton verkko, niin

a) $\sum_{x \in \mathbf{X}} d_G(x) = 2 \cdot \#E$,

b) asteluvultaan parittomien solmujen lukumäärä on parillinen.

Todistus. a) Jos kaaria on yksi, on kahden solmun asteluku 1 tai yhden asteluku 2. Jos kaaria on n kappaletta, yhden lisääminen nostaa astelukujen summaa kahdella.

b) Kohdan a) mukaan

$$2 \cdot \#E = \sum_{x \in \mathbf{X}} d_G(x) = \sum_{d_G(x) \text{ parillinen}} d_G(x) + \sum_{d_G(x) \text{ pariton}} d_G(x),$$

joka on parillinen luku. Parillisasteisten solmujen astelukujen summa on parillinen, joten parittomia termejä on oltava parillinen määrä. □

Esimerkki 12.2.4 Esimerkin 12.1.4 verkossa $G = (\mathbf{X}, E, \Psi)$ oli $\mathbf{X} = \{x_1, x_2, x_3\}$, $E = \{e_1, e_2, e_3, e_4\}$ ja

$$\Psi(e_1) = \Psi(e_2) = \{x_1, x_3\},\ \Psi(e_3) = \{x_1\},\ \Psi(e_4) = \{x_1, x_2\}.$$

Verkko G ei ole yksinkertainen, sillä siinä on silmukka, tai siksi, että solmuja x_1 ja x_3 yhdistää kaksi kaarta. Verkko G ei ole täydellinen, sillä solmuja x_2 ja x_3 ei yhdistä mikään kaari. Solmu x_1 on astetta 5 ja $d_G(x_3) = 2$.

12.3 Suuntaamattoman verkon aliverkko

Määritelmä 12.3.1 a) Verkko $G' = (\mathbf{X}', E', \Psi')$ on verkon $G = (\mathbf{X}, E, \Psi)$ *aliverkko* (merkitään $G' \subseteq G$), jos seuraavat ehdot ovat voimassa:

1) $\emptyset \neq \mathbf{X}' \subseteq \mathbf{X}$,

2) $E' \subseteq E$,

3) $\Psi(E') \subseteq \mathbf{X}' \,\&\, \mathbf{X}'$ ja $\Psi' = \Psi|E'$.

Jos $G' \subseteq G$ on aliverkko ja lisäksi $E' = \Psi^{-1}(\mathbf{X}' \,\&\, \mathbf{X}')$, niin G' on solmujoukon $\mathbf{X}'$ *virittämä* aliverkko.

b) Verkon $G = (\mathbf{X}, E, \Psi)$ *diagonaali* on joukko $\Delta_{\mathbf{X}} := \big\{\, \{x, x\} \mid x \in \mathbf{X} \,\big\}$. Verkon G *komplementti* on verkko $\overline{G} := (\mathbf{X}, F, \Gamma)$, missä

$$F := (\mathbf{X} \,\&\, \mathbf{X}) \setminus (\Psi(E) \cup \Delta_{\mathbf{X}})$$

ja $\Gamma : F \to \mathbf{X} \,\&\, \mathbf{X}$ on identtinen kuvaus.

Huomautus 12.3.2 a) Aliverkko $G' \subseteq G$ on solmujoukon $\mathbf{X}'$ virittämä jos ja vain jos E' sisältää täsmälleen solmujoukkoon $\mathbf{X}'$ liittyvät verkon G kaaret.

b) Verkon komplementti on yksinkertainen verkko. Täydellisen verkon komplementti on surkastunut verkko. Verkosta saadaan yksinkertainen ottamalla sen komplementin komplementti.

Esimerkki 12.3.3 Esimerkin 12.1.4 verkossa $G = (\mathbf{X}, E, \Psi)$ oli $\mathbf{X} = \{x_1, x_2, x_3\}$, $E = \{e_1, e_2, e_3, e_4\}$ ja

$$\Psi(e_1) = \Psi(e_2) = \{x_1, x_3\},\ \Psi(e_3) = \{x_1\},\ \Psi(e_4) = \{x_1, x_2\}.$$

Sen aliverkkoja ovat esimerkiksi $G' = (\mathbf{X}', E', \Psi')$, kun

a) $\mathbf{X}' = \{x_1, x_2, x_3\}$, $E' = \{e_4\}$ ja $\Psi'(e_4) = \{x_1, x_2\}$.

b) $\mathbf{X}' = \{x_1, x_3\}$, $E' = \{e_2, e_3\}$, $\Psi'(e_2) = \{x_1, x_3\}$ ja $\Psi'(e_3) = \{x_1\}$.

Solmujoukon $\mathbf{X}' := \{x_1, x_3\}$ virittämään aliverkkoon on otettava kaikki näihin liittyvät kaaret, joten on oltava $E' = \{e_1, e_2, e_3\}$, $\Psi'(e_1) = \Psi'(e_2) = \{x_1, x_3\}$, $\Psi'(e_3) = \{x_1\}$ ja $\Psi'(e_4) = \{x_1, x_2\}$

Verkon G komplementin kaaret ovat

$$F = (\mathbf{X} \,\&\, \mathbf{X}) \setminus (\Psi(E) \cup \Delta_{\mathbf{X}}) = \big\{\{x_2, x_3\}\big\}.$$

12.4 Suuntaamattomien verkkojen esitystapoja

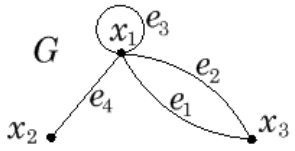
Tilanteesta riippuen on hyödyllistä kyetä kuvaamaan verkkoja toisaalta jollakin havainnollisella, toisaalta jollakin matemaattiseen manipulointiin ja mekaaniseen käsittelyyn sopivalla tavalla. Äärellinen suuntaamaton verkko $G = (\mathbf{X}, E, \Psi)$ voidaan esittää mm. luettelona, kaaviona tai matriiseina.

1. Luettelo sisältää solmujen ja kaarten joukot sekä vastaavuuskuvauksen:

$$\begin{array}{ll} \text{solmut} & \mathbf{X} = \{x_1, x_2, \ldots, x_n\} \\ \text{kaaret} & E = \{e_1, e_2, \ldots, e_m\} \\ \text{vastaavuus} & \Psi(e_1) = \{x_{k_1}, x_{l_1}\}, \ldots, \Psi(e_m) = \{x_{k_m}, x_{l_m}\} \end{array}$$

vrt. Esimerkki 12.1.4.

2. Kaavioesitys on geometrinen kuvio, jossa solmuja vastaavat 2- tai 3-ulotteisen avaruuden pisteet ja kaaria geometriset kaaret, jotka eivät kosketa toisiaan (muualla kuin yhteisessä päätesolmussa). Solmupari x, y yhdistetään piirtämällä kaikki niitä yhdistävät kaaret e_i, joille $\Psi(e_i) = \{x, y\}$. Tällöin pisteiden lukumäärä $= \#\mathbf{X}$ ja kaarien lukumäärä $= \#E$. Jos verkko on mahdollista esittää tasossa niin, etteivät kaaret leikkaa toisiaan, on kyseessä *tasoverkko*, muutoin *avaruusverkko*. Jokainen äärellinen verkko voidaan esittää kaaviona avaruudessa $\mathbb{R}^3$ (ks. Luku 14.2). Kuva 21 esittää Esimerkin 12.1.4 verkkoa tasoverkkomuodossa.



Kuva 21: Esimerkin 12.1.4 verkko tasokaaviona

3. Yhteysmatriisi (*adjacency matrix*) $M_G = (a_{ij})_{n\times n}$ muodostetaan asettamalla

$$a_{ij} := \#(\Psi^{-1}(\{x_i, x_j\})), \quad i, j \in [n].$$

Luku a_{ij} on solmuja x_i ja x_j yhdistävien kaarten lukumäärä. Suuntaamattoman verkon yhteysmatriisi on symmetrinen. Esimerkin 12.1.4 verkon yhteysmatriisi on

$$M_G = (a_{ij})_{3\times 3} = \begin{array}{c} G \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix} \end{array}$$

4. Vastaavuusmatriisi (*incidence matrix*) $V_G = (b_{ij})_{m\times n}$ muodostetaan asettamalla

$$b_{ij} := \begin{cases} 1, & \text{jos } e_j \text{ liittyy solmuun } x_i, \\ 0, & \text{muutoin.} \end{cases}$$

Esimerkin 12.1.4 verkon esitys on

$$V_G = (b_{ij})_{3\times 4} = \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cccc} G & e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{array}.$$

Yhteysmatriisi on matriisiesityksistä yleisimmin käytetty. Se vie yleensä vähemmän tilaa kuin vastaavuusmatriisi, ainakin jos kaaria on paljon. Toisaalta vastaavuusmatriisi mahdollistaa rinnakkaisten kaarten erottelemisen. Yhteysmatriisi ei yksin sovellu *painotettujen verkkojen* käsittelyyn kuin solmupainojen osalta, kun taas vastaavuusmatriisiin voidaan lisätä yksi rivi ilmoittamaan kaaripainot ja sarake ilmoittamaan solmupainot, ks. Luku 15.

12.5 Ketjut ja yhtenäisyys

Tarkastellaan liikkumista verkossa solmusta toiseen pitkin peräkkäisten kaarten muodostamia jonoja.

Määritelmä 12.5.1 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko. Kaarivektori $c = (e_1, e_2, \ldots, e_n) \in E^n$ on verkon G *ketju*, jos

1) $e_i \neq e_j$ kaikilla $i \neq j$,

2) on olemassa solmuvektori (*solmujono*) $(x_0, x_1, \ldots, x_n) \in \mathbf{X}^{n+1}$, jolle

$$\Psi(e_i) = \{x_{i-1}, x_i\}, \quad i \in [n].$$

Jos kaarivektori c toteuttaa ehdon 2), sitä sanotaan *kaarijonoksi*. Jos c on ketju verkossa G, sanotaan, että c *kulkee* solmujen x_i *kautta*; tällöin käytetään merkintää

$$(e_1, e_2, \ldots, e_n) \sim (x_0, x_1, x_2, \ldots, x_n).$$

Solmu x_0 on ketjun *alkupää* ja x_n sen *loppupää*; tätä merkitään $x_0 \to x_n$. Jos $x_0 = x_n$, on ketju *suljettu*, muutoin *avoin*. Jos $x_i \neq x_j$ muilla indekseillä paitsi mahdollisesti $x_0 = x_n$, on ketju *yksinkertainen*. Ketjun c *pituus* on luku $|c| :=$ kaarien lukumäärä n. Ketjun kaarten joukkoa merkitään

$$< c >:= \{e_1, e_2, \ldots, e_n\}.$$

Ketju $c' = (f_1, f_2, \ldots, f_m)$ on ketjun $c = (e_1, e_2, \ldots, e_n)$ *aliketju* (merkitään $c' \subseteq c$), jos jollekin $i \in [n - m + 1]$

$$c' = (e_i, e_{i+1}, \ldots, e_{i+m-1}).$$

Aliketju c' on *aito* aliketju, jos $c' \neq c$. Kaarijonolle käytetään vastaavia nimityksiä ja merkintöjä.

Huomautus 12.5.2 a) Jokainen ketju on määritelmän mukaan kaarijono. Kaarijono voi sisältää saman kaaren useammin kuin kerran, jolloin se ei ole ketju. Kaarijonolle voi olla

$$|c| > \# < c > .$$

b) Kun on annettu ketjun alku- ja loppupäät x_0 ja x_n, ketju määrää solmujonon $(x_0, x_1, \ldots, x_n)$ yksikäsitteisesti. Jos on annettu vain kaaret, esimerkiksi

$$\Psi(e_1) = \Psi(e_2) = \ldots = \Psi(e_n) = \{x, y\},$$

on ketjun aikaansaamiseksi kiinnitettävä jonon alku- tai loppupää.

Esimerkki 12.5.3 Olkoot

$$\begin{aligned} \mathbf{X} &= \{x_0, x_1, x_2, x_3, x_4\}, \\ E &= \{e_1, e_2, e_3, e_4\}, \\ \Psi &: \{x_0, x_1\}, \{x_1, x_3\}, \{x_3, x_4\}, \{x_4, x_1\}. \end{aligned}$$

Kaarijono $c := (e_1, e_2, e_3, e_4)$ on ketju alkupäänä x_0 ja loppupäänä x_1. Ketju kulkee solmujen x_0, x_1, x_3, x_4 ja x_1 kautta ja sen pituus $|c| = 4$. Ketju ei ole suljettu eikä yksinkertainen. Kaarijono (e_2, e_3, e_4) on yksinkertainen suljettu ketju alku- ja loppupäänä solmu x_1. Kaarijono (e_1, e_2, e_3) on avoin yksinkertainen ketju $x_0 \rightarrow x_4$. Lisäksi se on ketjun c aito aliketju. Kaarijonot (e_1, e_2, e_2) ja (e_2, e_3, e_4, e_2) eivät ole ketjuja; (e_1, e_3) ei ole edes kaarijono. Mikään kaarijono ei kulje solmun x_2 kautta.

Joskus on tarpeen pelkistää ketjuja:

Lause 12.5.4 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko, $x, y \in \mathbf{X}$ ja c ketju $x \rightarrow y$. Silloin on olemassa yksinkertainen ketju $x \rightarrow y$, joka voidaan valita niin, että se sisältää vain ketjun c kaaria.

Todistus. Harjoitustehtävä.
Vihje: lyhin ketjun c kaarista koostuva ketju on yksinkertainen. □

Lause 12.5.5 Jos $G = (\mathbf{X}, E, \Psi)$ on äärellinen suuntaamaton verkko, joukko

$$S := \{\, (x, y) \in \mathbf{X}\times\mathbf{X} \mid x = y \text{ tai on olemassa ketju } x \to y \,\}$$

on ekvivalenssirelaatio.

Todistus. Selvästikin S on relaatio joukossa $\mathbf{X}$.

1) (refleksiivisyys) Joukon S määrittelyn perusteella xSx kaikilla $x \in \mathbf{X}$.

2) (symmetrisyys) Olkoon xSy. Tällöin joko

   a) $x = y$, jolloin $y = x$ ja ySx, tai

   b) $x \neq y$, jolloin on olemassa ketju $(e_1, \ldots, e_n)$ alkupäänä x ja loppupäänä y. Kaarijono $(e_n, \ldots, e_1)$ on silloin ketju $y \to x$.

   Siis joka tapauksessa ySx.

3) (transitiivisuus) Olkoot xSy ja ySz. Jos x, y, z eivät ole kaikki eri solmuja, on asia selvä. Oletetaan, että $x \neq y \neq z \neq x$. On siis olemassa ketjut

$$c = (e_1, e_2, \ldots, e_n) \sim (x = x_0, x_1, \ldots, x_n = y),$$

$$d = (f_1, f_2, \ldots, f_m) \sim (y = y_0, y_1, \ldots, y_m = z).$$

   Tarkastellaan kaarijoukkoja $< c >$ ja $< d >$.

   α) Jos $< c > \cap < d >= \emptyset$, kaarijono $(e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_m)$ on ketju päinään solmut x ja z, ja siten xSz.

   β) Jos taas $< c > \cap < d >\neq \emptyset$, olkoon e_k ensimmäinen ketjun c kaari, joka on myös ketjussa d. Olkoon $j \in [m]$ indeksi, jolle $e_k = f_j$. On kaksi mahdollisuutta: $x_{k-1} = y_{j-1}$ tai $x_{k-1} = y_j$. Jos $x_{k-1} = y_{j-1}$, kaarijono

$$(e_1, e_2, \ldots, e_{k-1}, f_j, f_{j+1}, \ldots, f_m)$$

   on ketju $x \to z$. Jos taas $x_{k-1} = y_j$, niin jättämällä edellisestä pois kaari f_j saadaan ketju

$$(e_1, e_2, \ldots, e_{k-1}, f_{j+1}, \ldots, f_m),$$

   jonka päät ovat x ja z.

   Siis joka tapauksessa xSz.

□

Määritelmä 12.5.6 Äärellisen suuntaamattoman verkon $G = (\mathbf{X}, E, \Psi)$ *yhtenäiset komponentit* ovat ekvivalenssiluokkien $S(x)$, $x \in \mathbf{X}$, virittämät aliverkot. Verkko on *yhtenäinen*, jos sillä on vain yksi yhtenäinen komponentti.

Huomautus 12.5.7 a) Lauseiden 12.5.5 ja 7.2.9 mukaan verkon $G = (\mathbf{X}, E, \Psi)$ solmujen ekvivalenssiluokat $S(x)$ muodostavat joukon $\mathbf{X}$ osituksen. Kukin osituksen alkio virittää aliverkon, yhtenäisen komponentin, joka on itse yhtenäinen verkko (harjoitustehtävä). Yhtenäiset komponentit ovat siinä mielessä erillisiä, että komponentista toiseen ei ole kaarijonoja.

b) Verkko $G = (\mathbf{X}, E, \Psi)$ on yhtenäinen jos ja vain jos $S(x) = \mathbf{X}$ kaikilla $x \in \mathbf{X}$, eli täsmälleen silloin, kun jokaista solmuparia $x \neq y$ kohti on olemassa ketju päinä x ja y.

Yhtenäisyyden testaus. Verkon yhtenäisyyttä voidaan tietenkin testata samaan tapaan kuin lasketaan relaation transitiivinen sulkeuma. Monissa verkkoalgoritmeissa on osana verkon (tai sen aliverkkojen) yhtenäisyyden testauksia, joten siihen on syytä olla käytettävissä nopea menetelmä. Hyviä menetelmiä ovat nk. *depth-first-* ja *breadth-first-menetelmät*, joiden etuna on se, että niitä voidaan sopivasti modifioituina käyttää moniin muihinkin ongelmiin. Edellisessä lähdetään yhdestä solmusta muodostamaan ketjua niin, ettei vierailla missään solmussa kuin kerran; kun joudutaan umpikujaan, palataan edelliseen risteykseen ja tutkitaan seuraava reitti jne. Jälkimmäisessä taas lähdetään yhdestä solmusta ja edetään kaikkia siitä lähteviä ketjuja, seuraavista solmuista taas kaikkia jne. Verkko on yhtenäinen, jos näin tullaan vierailleeksi kaikissa solmuissa (harjoitustehtäviä).

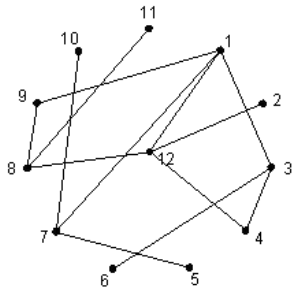
Syvyys- ja leveysalgoritmit. Tarkastellaan depth-first ja breadth-first algoritmeja esimerkin kautta. Tässä tarkoitus on selvittää niiden avulla onko verkko yhtenäinen.

Esimerkki 12.5.8 Olkoon $G = (\mathbf{X}, E, \Psi)$ verkko annettuna Kuvion 22 avulla. Kun on selvitettävänä verkon yhtenäisyys, riittää valita mikä tahansa lähtösolmuksi. Siispä lähdetään liikkeelle solmusta 1 ja vielä sovitaan valintatilanteissa valittavaksi aina numeroltaan pienin solmu. Nyt depth-first algoritmilla vierailaan solmuissa seuraavasti:

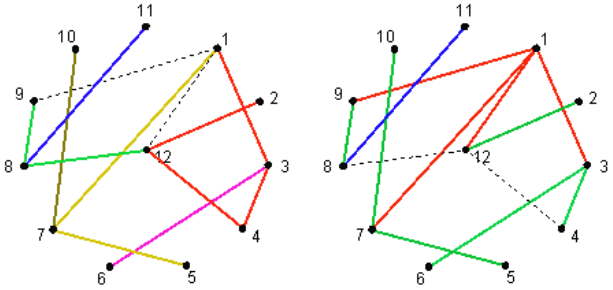
1 3 4 12 2 [12] 8 9 [8] 11 [8 12 4 3] 6 [3 1] 7 5 [7] 10 [7 1]

Breadth-first taas toimii seuraavasti (vrt. Kuviot 23):

1: [3 [4 6]], [7 [5 10]], [9 [8 [11]]], [12 [2]]

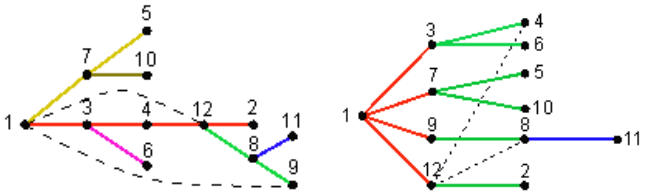


Kuva 22: Esimerkin 12.5.8 verkko



Kuva 23: Depth- ja breadth-menetelmät Esimerkin 12.5.8 verkossa

Verkko on siis yhtenäinen. Kun jätetään käyttämättömiksi jääneet kaaret pois, saadaan verkolle virittävät puut (ks. Luku 12.9); itse asiassa solmun 1 virittämän yhtenäisen komponentin virittävät puut haettuina näillä menetelmillä. Näin saadaan selkeämmät Kuviot 24.



Kuva 24: Menetelmät tuottavat Esimerkin 12.5.8 verkolle virittävät puut

Kaksiyhtenäisyys ja jakavat solmut. Joskus tarvitaan tavallista yhtenäisyyttä vahvempia ominaisuuksia. Jos esimerkiksi tietoverkko rakennetaan vain yhtenäiseksi, voi yhden solmun poistuminen käytöstä kaataa systeemin.

Määritelmä 12.5.9 Verkon solmua, jonka poisto epäyhtenäistää alunperin yhtenäisen verkon, sanotaan *jakavaksi* tai *leikkaussolmuksi* (*articulation node, cut-vertex*).

Määritelmä 12.5.10 Yhtenäinen verkko on *kaksiyhtenäinen* (*biconnected*), jos
a) siinä on yksi tai kaksi solmua, tai
b) siinä on vähintäin kolme solmua ja jokaista kolmea eri solmua x, y, z kohti löytyy ainakin yksi ketju $x \rightarrow z$, joka ei kulje solmun y kautta.

Lause 12.5.11 Yhtenäinen suuntaamaton verkko on kaksiyhtenäinen jos ja vain jos siinä ei ole jakavia solmuja.

Todistus. Harjoitustehtävä. □

12.6 Hamiltonin ketjut

Olkoon $G = (\mathbf{X}, E, \Psi)$ tässä pykälässä suuntaamaton, äärellinen, yhtenäinen ja yksinkertainen verkko. Jos annettu verkko ei ole yksinkertainen, yksinkertaistetaan se poistamalla ylimääräiset rinnakkaiset kaaret. Tarkastellaan yksinkertaisia ketjuja, jotka ”täyttävät” verkon niin, että niitä pitkin voi kulkea verkon jokaisen solmun kautta täsmälleen kerran. Tällainen ketju voi olla avoin tai suljettu. Jos verkossa on suljettu Hamiltonin ketju, on siinä myös avoin. Tässä tarkastellaan lähinnä suljettujen ketjujen olemassaoloa, sillä se liittyy olennaisesti mm. *kauppamatkustajan ongelmaan.*

Määritelmä 12.6.1 Yksinkertaista ketjua, joka kulkee verkon jokaisen solmun kautta, sanotaan *Hamiltonin ketjuksi*. Verkko on *Hamiltonin verkko*, jos siinä on yksikin suljettu Hamiltonin ketju.

Heti voidaan todeta, että ainakin täydellisessä verkossa on suljettuja Hamiltonin ketjuja.

Kauppamatkustajan ongelma (*travelling salesperson problem*). Kauppamatkustajan täytyy käydä kiertomatkallaan täsmälleen kerran kussakin Suomen kaupungissa. Onko tämä ylipäätään mahdollista? Jos on, mikä on lyhin reitti?

Probleema voidaan pukea matemaattiseen muotoon äärellisen suuntaamattoman verkon avulla: kaupungit ovat verkon solmuja, tiet kaaria ja kuhunkin kaareen lii-

tetään välimatkan pituutta kuvaava painokerroin. Onko näin muodostuvassa verkossa suljettuja Hamiltonin ketjuja? Mikä niistä on lyhin?

Vaatimuksia joudutaan usein käytännössä väljentämään sallimalla useampi vierailu samassa kaupungissa tai jättämällä jokin kaupunki pois. Suurten verkkojen kyseessä ollen on usein ainoa keino turvautua approksimatiivisiin ratkaisuihin. Näitä on nykyään kehitteillä runsaasti ja parhaimmillaan päästään ratkaisuihin, jotka poikkeavat oikeasta vain muutaman prosentin verran (ks. Luku 14, s. 181).

Triviaali menetelmä. Yleisesti on hankalaa selvittää, onko verkossa Hamiltonin ketjuja. Ainoa yleinen menetelmä on triviaali menetelmä tutkia kaikki mahdolliset ketjut. Tämä voidaan tehdä alkaen samaan tapaan kuin depth-first-menetelmässä, eli kulkien ensin niin kauas lähtösolmusta kuin päästään vierailematta edellisissä solmuissa uudestaan. Jos näin saadussa ketjussa on kaikki solmut, on saatu avoin Hamiltonin ketju ja voidaan tarkastaa, voidaanko ketju sulkea. Tarvittaessa palataan edelliseen solmuun ja valitaan toinen reitti jne. Solmuissa vierailuista pidetään kirjaa niin, että tiedetään, onko kunkin solmun kaikki lähtösuunnat jo tarkastettu (harjoitustehtävä).

Välttämättömiä ehtoja. Osoitettaessa, että verkossa *ei voi olla* suljettua Hamiltonin ketjua, voidaan käyttää seuraavia konkreettisia sääntöjä, jotka ovat ketjun olemassaololle *välttämättömiä*, tai joita tulee noudattaa ketjua muodostettaessa:

1) Jos verkossa on $n \geq 2$ solmua, avoimessa Hamiltonin ketjussa on aina $n-1$ kaarta, suljetussa n kaarta.

2) Jos solmun x asteluku on 2, niin molemmat kaaret, joiden päänä on x, kuuluvat jokaiseen suljettuun Hamiltonin ketjuun.

3) Hamiltonin ketjun mikään aito aliketju ei ole suljettu.

4) Kun muodostettavana oleva Hamiltonin ketju on kulkenut solmun x kautta, kaikki muut solmuun x liittyvät kaaret voidaan poistaa; niitä ei nimittäin enää voi käyttää. Tämä ei tietenkään koske avoimen ketjun päitä.

5) Hamiltonin verkot ovat kaksiyhtenäisiä (harjoitustehtävä).

Yleisemmin: Verkossa G ei ole suljettua Hamiltonin ketjua, jos poistamalla $k \in \mathbb{N}$ kappaletta solmuja ja niihin liittyvät kaaret jää jäljelle verkko, jossa on $p > k$ yhtenäistä komponenttia.

Esimerkki 12.6.2 Olkoot $\mathbf{X} = \{a, b, c, d, e\}$ ja

$$E = \big\{\{a, c\}, \{a, d\}, \{d, c\}, \{c, b\}, \{b, e\}, \{e, c\}\big\}.$$

Osoita, että verkossa ei ole suljettua Hamiltonin ketjua, mutta on avoin.

Ratkaisu. Ketju, joka kulkee solmujonon (a, d, c, b, e), on eräs avoin Hamiltonin ketju. On ainakin neljä tapaa todistaa, ettei suljettua Hamiltonin ketjua ole. Ensiksikin, kohdan 2 mukaan siihen kuuluisivat kaikki kaaret.

a) Ketjussa on kuusi kaarta, mikä on vastoin kohtaa 1.

b) Aliketju $(\{c, a\}, \{a, d\}, \{d, c\})$ on suljettu ja aito, mikä on vastoin ehtoa 3.

c) Solmuun c liittyy neljä kaarta, joista kaksi ei ehdon 4 mukaan voi kuulua Hamiltonin ketjuun.

d) Solmu c on jakava, joten verkko ei ole kaksiyhtenäinen.

*__Riittäviä ehtoja.__ Esitetään joitakin Hamiltonin ketjun olemassaolon takaavia tuloksia.

Lause 12.6.3 Olkoon $G = (\mathbf{X}, E, \Psi)$ suuntaamaton äärellinen, yhtenäinen ja yksinkertainen verkko, jossa on n solmua, $n \geq 3$.

a) (*Diracin lause*) Jos $d_G(x) \geq n/2$ kaikilla $x \in \mathbf{X}$, on verkossa suljettu Hamiltonin ketju.

b) Olkoon $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$. Oletetaan, että solmut on järjestetty niin, että kaikilla $i \in [n-1]$ on
$$d_G(x_i) \leq d_G(x_{i+1}).$$
Jos jokaiselle $k \leq n/2$ on voimassa joko $d_G(x_k) > k$ tai $d_G(x_{n-k}) \geq n-k$, on verkossa suljettu Hamiltonin ketju.

Todistus. Todistetaan näytteeksi Diracin lause vuodelta 1952. On helppo osoittaa, että mikä tahansa verkko voidaan täydentää Hamiltonin verkoksi lisäämällä siihen solmuja ja niistä kustakin kaaret alkuperäisen verkon jokaiseen solmuun. Näitä lisäsolmuja tarvitaan korkeintaan n kappaletta. Olkoon $m \in \mathbb{N}_0$ pienin määrä solmuja, joiden lisääminen verkkoon G antaa tulokseksi Hamiltonin verkon $G' = (\mathbf{X}', E', \Psi')$.

Osoitetaan, että $m = 0$. *Vastaoletus*: $m > 0$. Jokaiseen solmuun $x \in \mathbf{X}$ liittyy oletuksen mukaan vähintäin $n/2 + m$ kaarta, joten sillä on ainakin näin monta viereistä solmua. Olkoon c verkon G' suljettu Hamiltonin ketju $x_1 \to x' \to x_2 \to \ldots \to x_1$, missä $x_1, x_2 \in \mathbf{X}$ ja $x' \in \mathbf{X}' \setminus \mathbf{X}$ (tarvittaessa uudelleen indeksointi). Solmut x_1 ja x_2 eivät voi olla vierekkäisiä verkossa G, sillä muutoin solmua x' ei

olisi tarvittu. Jos x_p on solmun x_1 viereinen, ei x_{p+1} voi olla solmun x_2 vieressä, sillä silloin voitaisiin x' kiertää muuntamalle ketjua seuraavasti

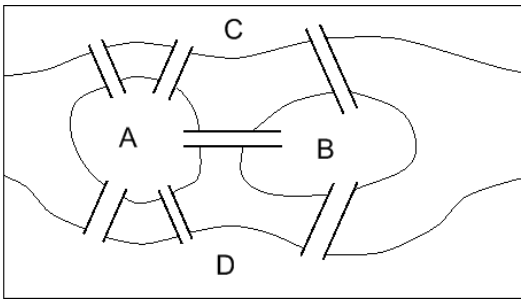
$$x_1 \to x_p \to x_{p-1} \to \ldots \to x_2 \to x_{p+1} \to \ldots \to x_1.$$

Täten solmuja, jotka eivät ole vierekkäisiä solmulle x_2, on vähintäin $n/2 + m$ kappaletta. Koska myös vierekkäisiä on ainakin näin paljon, olisi solmuja ainakin $n + 2m$. Toisaalta solmuja on kaikkiaan $n + m$. Siis $m = 0$, joten verkko G on Hamiltonin verkko. □

12.7 Eulerin ketjut

Toinen esimerkki ketjuista, nk. Eulerin ketju, on peräisin kuuluisasta esimerkistä *Königsbergin sillat*, jota voidaan pitää verkkoteorian alkuna. Olkoon tässä pykälässä $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko.

Königsbergin sillat. Preussilaisen kaupungin Königsbergin (nyk. Venäjän *Kaliningrad*) läpi virtaa Pregel-joki, jossa on peräkkäin kaksi saarta (ks. Kuva 25).



Kuva 25: Königsbergin sillat 1700-luvulla

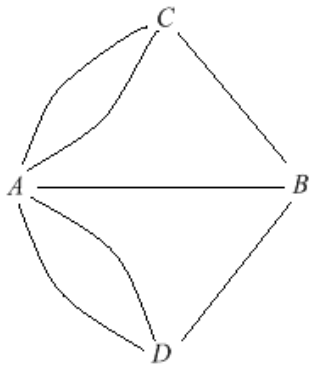
Isomman saaren A kautta kulkee joen yli kaksi siltaa, pienemmän saaren B kautta yksi. Lisäksi saaria yhdistää toisiinsa yksi silta, yhteensä siis 7 siltaa. Kaupunkilaiset yrittivät kauan saada selville, miten tehdä sellainen kävelyretki, jonka aikana kukin silta ylitetään tasan kerran. Lopulta asiaa kysyttiin sveitsiläiseltä Leonhard Eulerilta, joka pian todisti, ettei ratkaisua ole. Eulerin alkuperäinen päättely oli seuraava: *Jos kyseinen retki on mahdollinen, kuinka monta kertaa kävelijä käy retken aikana saarella A? Jos hän käy kerran, kahdesti tai kolmesti, hän käyttää vastaavasti 2, 4 tai 6 siltaa, joiden toinen pää on kyseisellä saarella. Mutta siltoja onkin 5!* Ongelmaa tutkiessaan Euler tuli samalla keksineeksi verkon käsitteen ja huomasi, että se kelpasi malliksi moneen muuhunkin käytännön ongelmaan.

Määritelmä 12.7.1 Ketju $c = (e_1, e_2, \ldots, e_n)$ verkossa $G = (\mathbf{X}, E, \Psi)$ on *Eulerin ketju*, jos $\{e_1, e_2, \ldots, e_n\} = E$, ts. jos jokainen kaari esiintyy ketjussa tasan kerran. Jos verkossa G on suljettu Eulerin ketju, on G *Eulerin verkko*.

Königsbergin sillat-ongelma voidaan pukea verkkoteorian kielelle seuraavasti: Olkoot C ja D joen rannat (ks. Kuva 26).

Muodostetaan verkko G, jossa sillat ovat kaaria solmujen A, B, C ja D välillä. Kyseinen kävelyreitti vastaisi jotakin Eulerin ketjua $(e_1, e_2, \ldots, e_7)$.

Toisin kuin Hamiltonin ketjulle, Eulerin ketjun olemassaololle voidaan antaa täsmällinen ja konkreettinen karakterisointi.



Kuva 26: Königsbergin sillat verkkokaaviona

Lause 12.7.2 Olkoon G äärellinen suuntaamaton verkko, jossa ei ole erillisiä solmuja.

a) Verkossa G on suljettu Eulerin ketju jos ja vain jos G on yhtenäinen ja siinä ei ole paritonasteisia solmuja. Eulerin verkon jokainen Eulerin ketju on suljettu.

b) Verkossa G on avoin Eulerin ketju jos ja vain jos G on yhtenäinen ja siinä on täsmälleen kaksi paritonasteista solmua. Jos verkossa G on yksikin avoin Eulerin ketju, sen jokainen Eulerin ketju on avoin päinään kyseiset paritonasteiset solmut.

Todistus. Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko, jossa ei ole erillisiä solmuja.

$\boxed{\Rightarrow}$ Olkoon $c = (e_1, e_2, \ldots, e_n)$ verkon G (avoin tai suljettu) Eulerin ketju ja $(x_0, x_1, x_2, \ldots, x_n)$ vastaava solmujono. Koska verkossa ei ole erillisiä solmuja ja $\{e_1, e_2, \ldots, e_n\} = E$, ketju c kulkee kaikkien solmujen kautta. Täten G on yhtenäinen.

Osoitetaan, että paritonasteisia ovat vain x_0 ja x_n tai ei kumpikaan. Jos $n = 1$, on asia selvä: on kaksi yksiasteista solmua, joita yhdistää kaari e_1. Olkoon $n \geq 2$. Tarkastellaan mielivaltaista solmua $x_i \in \{x_1, x_2, \ldots, x_{n-1}\}$, $x_i \neq x_0$, $x_i \neq x_n$. Silloin x_i ei ole ketjun pää. Koska

$$\Psi(e_i) = \{x_{i-1}, x_i\} \quad \text{ja} \quad \Psi(e_{i+1}) = \{x_i, x_{i+1}\},$$

eli solmua x_i vastaa pareittain kaksi kaarta e_i ja e_{i+1}, ja koska $\{e_1, e_2, \ldots, e_n\} = E$, on $d_G(x_i)$ parillinen. Paritonasteisia voivat olla siis vain x_0 tai x_n; Lauseen 12.2.3 kohdan b) nojalla molemmat tai ei kumpikaan. ∎

a) Jos paritonasteisia ei ole, ovat $d_G(x_0)$ ja $d_G(x_n)$ parillisia lukuja ja siten $x_0 = x_n$, eli ketju on suljettu.

b) Jos x_0 ja x_n ovat paritonta astetta, ne ovat eri solmuja ja ketjun c päitä.

$\boxed{\Leftarrow}$ Oletetaan, että verkko G on yhtenäinen ja sen paritonasteisten solmujen lukumäärä on 0 tai 2.

a') Olkoot kaikki solmut parillista astetta. Olkoon $a \in \mathbf{X}$ mielivaltainen. Koska a ei ole erillinen solmu ja G on yhtenäinen, on olemassa ketjuja, joiden alkupää on a. Tällaisten ketjujen pituudet ovat $\leq \#E$, joten on olemassa sellainen, jonka pituus $n \leq \#E$ on suurin, olkoon eräs niistä

$$c = (e_1, e_2, \ldots, e_n) \sim (a, x_1, \ldots, x_n).$$

Osoitetaan, että c on Eulerin ketju verkossa G. Määritellään verkolle G aliverkot

$$G' = (\mathbf{X}, E', \Psi|E') \quad \text{ja} \quad G'' = (\mathbf{X}, E'', \Psi|E''),$$

missä $E' := \{e_1, e_2, \ldots, e_n\}$ ja $E'' := E \setminus E'$. Silloin c on Eulerin ketju verkossa G'.

Väite 1. Ketju c on suljettu, ts. $a = x_n$.

Todistus. Tehdään vastaoletus: $x_n \neq a$. Silloin $d_{G'}(x_n)$ on pariton ja siten aidosti pienempi kuin $d_G(x_n)$, joka oli parillinen. Tästä seuraa, että on olemassa $e \in E''$, jonka päänä on x_n. Mutta silloin ketju $c' := (e_1, e_2, \ldots, e_n, e)$ on verkon G ketju alkupäänä a ja $|c'| > |c|$, mikä on vastoin ketjun c valintaa. Siis c on suljettu. $\triangle$

Merkitään

$$\mathbf{Y} = \{x_0 := a, x_1, \ldots, x_n\}.$$

Osoitetaan, että $\mathbf{Y} = \mathbf{X}$, ja tämän avulla, että c on Eulerin ketju verkossa G.

Väite 2. Jos $e \in E$ ja $\Psi(e) \cap \mathbf{Y} \neq \emptyset$, on $e \in E'$.

Todistus. Vastaoletus: On olemassa kaari $e \in E''$ päänään solmu $x_i \in \mathbf{Y}$. Olkoon $G_i'' = (\mathbf{X}_i'', E_i'', \Psi_i'')$ se verkon G'' yhtenäinen komponentti, jolle $x_i \in \mathbf{X}_i''$. Osoitetaan, että verkossa G_i'' ei ole paritonasteisia solmuja. Olkoon $x \in \mathbf{X}_i''$ mielivaltainen. Koska G_i'' on verkon G'' yhtenäinen komponentti, on

$$d_{G_i''}(x) = d_{G''}(x).$$

Luku

$$d_G(x) = d_{G'}(x) + d_{G''}(x)$$

on oletuksen mukaan parillinen. Luku $d_{G'}(x)$ on parillinen, koska c on suljettu Eulerin ketju verkossa G'. Täten on myös $d_{G_i''}(x) = d_{G''}(x)$ parillinen. Verkko G_i'' on siis yhtenäinen ja sen solmut ovat parillista astetta, joten se toteuttaa samat

oletukset kuin G tapauksen a') alussa. Tämän nojalla on olemassa suljettu joukon E'' alkioista muodostuva ketju $c'' = (e''_1, e''_2, \ldots, e''_m)$ verkossa G''_i päinä x_i. Tällöin ketju

$$(e_1, e_2, \ldots, e_i,\ e''_1, e''_2, \ldots, e''_m,\ e_{i+1}, \ldots, e_n)$$

on verkon G ketju alkupäänä a. Tämä on mahdotonta, sillä sen pituus olisi $|c''| = m + n > n = |c|$. △

Väite 3. $\mathbf{Y} = \mathbf{X}$.

Todistus. Triviaalisti $\mathbf{Y} \subseteq \mathbf{X}$. Vastaoletus: On olemassa solmu $x \in (\mathbf{X} \setminus \mathbf{Y})$. Koska G on yhtenäinen, on olemassa ketju $x \to a$,

$$d = (f_1, f_2, \ldots, f_m) \sim (z_0 := x, z_1, \ldots, z_m := a).$$

Joukko $\{\, k \in [m] \mid z_k \in \mathbf{Y}\}$ on äärellinen ja epätyhjä, sillä $z_m = a \in \mathbf{Y}$. Olkoon $j \in [m]$ sen pienin alkio. Koska $\Psi(f_j) = \{z_{j-1}, z_j\}$ ja $z_j \in \mathbf{Y}$, on $z_j \in \Psi(f_j) \cap \mathbf{Y}$. Väitteen 2 nojalla $f_j \in E'$ ja siten $z_{j-1} \in \mathbf{Y}$. Tämä on vastoin indeksin j määrittelyä, joten vastaoletus on väärä. Siis $\mathbf{Y} = \mathbf{X}$. △

Olkoon lopuksi $e \in E$ mielivaltainen. Väitteen 3 nojalla $\Psi(e) \cap \mathbf{X} = \Psi(e) \cap \mathbf{Y} \neq \emptyset$, joten väitteen 2 nojalla $e \in E'$. Täten $E = E'$ ja c on suljettu Eulerin ketju verkossa G. Kohta a') on siis todistettu.

b') Olkoon verkossa täsmälleen kaksi paritonasteista solmua $a, b \in \mathbf{X}$. Täydennetään G verkoksi G^*, joka toteuttaa kohdan a') oletukset. Olkoon $\alpha \notin E$ jokin alkio. Määritellään $E^* := E \cup \{\alpha\}$ ja kuvaus $\Psi^* : E^* \to \mathbf{X}\,\&\,\mathbf{X}$,

$$\Psi^*(e) := \begin{cases} \Psi(e), & \text{kun } e \in E \\ \{a, b\}, & \text{kun } e = \alpha. \end{cases}$$

Silloin $G^* := (\mathbf{X}, E^*, \Psi^*)$ on verkko, joka toteuttaa kohdan a') oletukset: G^* on yhtenäinen ja solmujen asteet parillisia. Siis verkossa G^* on suljettu Eulerin ketju

$$c^* = (g_1, g_2, \ldots, g_{p-1},\ g_p = \alpha,\ g_{p+1}, \ldots, g_k).$$

Näin saadaan verkkoon G avoin Eulerin ketju

$$(g_{p+1}, g_{p+2}, \ldots, g_k,\ g_1, g_2, \ldots, g_{p-1}),$$

jonka päät ovat $a \neq b$. Siis kohta b') ja siten koko lause on todistettu. □

Huomautus 12.7.3 a) Lause antaa tyhjentävän ratkaisun Königsbergin silta-probleemalle; sitä vastaavassa verkossa ovat kaikki neljä solmua paritonta astetta.

b) Lause ei kerro miten verkkoon konstruoidaan Eulerin ketju. Eräs menetelmä on *Fleuryn algoritmi*, joka on havainnollinen, muttei kovin tehokas.

Algoritmi Eulerin ketjun löytämiseksi. Oletetaan, että $G = (\mathbf{X}, E, \Psi)$ on äärellinen suuntaamaton verkko, joka on yhtenäinen ja jonka solmujen asteet ovat parillisia. Valitaan jokin solmu $x_0 \in \mathbf{X}$. Poistetaan jokin siihen liittyvä kaari. Jos jäljelle jäävä aliverkko on yhtenäinen, otetaan kaari ketjuun, muutoin kaari palautetaan verkkoon ja valitaan uusi. Näin saadaan alulle ketju $c_1 = (e_1)$. Siirrytään valitun kaaren toiseen päähän, olkoon se x_1. Menetellen kuten solmun x_0 tapauksessa saadaan $c_2 = (e_1, e_2)$. Kun jonkin solmun aste putoaa nollaksi, solmu poistetaan. Verkossa kuljetaan näin, kunnes kaikki kaaret on poistettu. Poistettujen kaarien muodostama kaarijono $c_{\#E} = (e_1, e_2, \ldots, e_{\#E})$ on eräs suljettu Eulerin ketju alkuperäisessä verkossa G. Algoritmin eräs formaali muotoilu Kuvassa 27.

Aseta $i = 0$; $m = \#E$; $G_0 = (\mathbf{X}_0, E_0, \Psi_0) = (\mathbf{X}, E, \Psi)$;
valitse lähtösolmu $x_0 \in \mathbf{X}_0$;
while $(i < m)$
aseta $i = i + 1$; $yhtenainen = 0$;
while $(yhtenainen == 0)$
valitse kaari $e_i \in E_{i-1}$, jolle $\Psi(e_i) = \{x_{i-1}, x_i\}$;
aseta $E_i = E_{i-1} \setminus \{e_i\}$; $\Psi_i = \Psi_{i-1}|E_i$;
if $(d_{G_{i-1}}(x_{i-1}) == 1)$ $\mathbf{X}_i = \mathbf{X}_{i-1} \setminus \{x_{i-1}\}$; **else**, $\mathbf{X}_i = \mathbf{X}_{i-1}$; **end if**
aseta $G_i = (\mathbf{X}_i, E_i, \Psi_i)$;
if (G_i on yhtenäinen) $yhtenainen = 1$; **end if**
end while
aseta $c_i = (e_1, e_2, \ldots, e_i)$;
end while

Kuva 27: Fleuryn algoritmi Eulerin ketjun löytämiseksi

Annetusta suuntaamattomasta verkosta on ennen algoritmin käyttöä testattava solmujen astelukujen kelvollisuus. Menetelmässä on useita aliverkkojen yhtenäisyyden testauksia, mihin soveltuvat esimerkiksi etsintämenetelmät breadth-first ja depth-first. Algoritmia voi soveltaa pienin muutoksin myös avoimen Eulerin ketjun etsimiseen (harjoitustehtäviä).

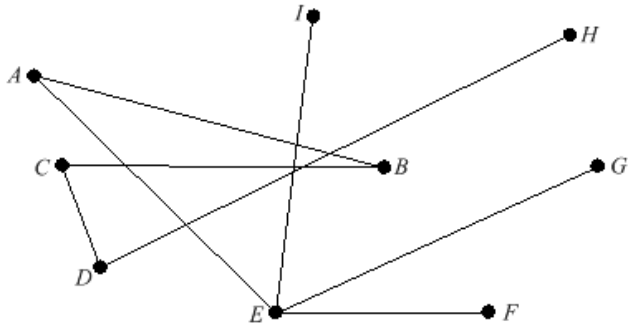
12.8 Suuntaamattomat puut

Tarkastellaan erikoistapauksena verkkoja, jotka ovat siinä mielessä optimaalisia, että niissä ei ole suljettuja ketjuja, mutta jotka silti ovat yhtenäisiä.

Määritelmä 12.8.1 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko. Joukko $S \subseteq E$ on verkon G *sykli*, jos S on jonkin suljetun ketjun $c = (e_1, e_2, \ldots, e_n)$ kaarien joukko eli $S =< c >$. Verkko G on *syklitön* eli *metsä*, jos siinä ei ole yhtään sykliä (eli ei yhtään suljettua ketjua). Jos G on yhtenäinen metsä, sitä sanotaan *puuksi*.

On selvää, että metsän yhtenäiset komponentit ovat puita. Seuraava lause kertoo puun erikoiset ominaisuudet: kaaren lisääminen tuo syklin ja kaaren poistaminen tekee epäyhtenäiseksi. Puu on tässä mielessä optimaalinen yhtenäinen verkko.

Esimerkki 12.8.2 Kuva 28 esittää puuta, vaikkakaan se ei ole piirretty ihan standardiin muotoon.



Kuva 28: Eräs 9-solmuinen puu

Lause 12.8.3 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko. Seuraavat ominaisuudet ovat yhtäpitäviä:

a) Verkko G on puu.

b) Verkko G on syklitön, mutta jokaisessa aidosti laajemmassa verkossa $G' = (\mathbf{X}, E', \Psi')$, missä $E \subset E'$ ja $\Psi = \Psi'|E$, on sykli.

c) Verkko G on yhtenäinen, mutta jokainen aidosti suppeampi verkko $G'' = (\mathbf{X}, E'', \Psi'')$, missä $E'' \subset E$ ja $\Psi'' = \Psi|E''$, on epäyhtenäinen.

Todistus. Todistetaan seuraavasti: a) $\Leftrightarrow$ b) ja a) $\Leftrightarrow$ c).

a) $\Rightarrow$ b) Olkoon G puu ja G' kohdassa b) kuvattu laajempi verkko. Olkoon $e \in E' \setminus E$ ja $\Psi'(e) = \{x, y\}$. Jos $x = y$, on verkossa G' sykli $\{e\}$. Oletetaan, että $x \neq y$. Koska G on yhtenäinen, on siinä ketju $x \to y$. Lisäämällä tähän ketjuun kaari e saadaan verkkoon G' suljettu ketju, jonka kaaret muodostavat syklin.

b) $\Rightarrow$ a) Olkoon b) voimassa verkolle G. Koska G on syklitön, riittää osoittaa, että se on yhtenäinen. Olkoot $x, y \in \mathbf{X}$, $x \neq y$. Näytetään, että on olemassa ketju $x \to y$. Olkoon $\alpha \notin E$ ja $E' := E \cup \{\alpha\}$. Määritellään kuvaus $\Psi' : E' \to \mathbf{X} \,\&\, \mathbf{X}$,

$$\Psi'|E := \Psi, \quad \Psi'(\alpha) := \{x, y\}.$$

Ehdon b) oletusten mukaan verkossa G' on eräs sykli $S =< c >$, missä c on suljettu ketju. Koska G on syklitön, on $\alpha \in < c >$. Ketjun c muut kaaret muodostavat ketjun $x \to y$ verkossa G, joten G on yhtenäinen.

a) $\Rightarrow$ c) Olkoon G puu ja G'' kohdassa c) kuvattu suppeampi verkko. On osoitettava, että G'' ei ole yhtenäinen. Vastaoletus: G'' on yhtenäinen. Valitaan jokin $e \in E \setminus E''$. Olkoon $\Psi(e) = \{x, y\}$. Koska G on puu, on $x \neq y$. Vastaoletuksen mukaan on olemassa verkon G'' ketju $x \to y$. Kun lisätään ketjuun kaari e, saadaan verkkoon G suljettu ketju ja siten sykli. Tämä on ristiriita oletuksen kanssa, joten G'' on epäyhtenäinen.

c) $\Rightarrow$ a) Oletetaan, että c) on voimassa verkolle G. Osoitetaan epäsuorasti, että G on syklitön. Oletetaan, että S on verkon G sykli. Olkoon $e \in S$ kaari. Silloin aidosti suppeampi verkko $G'' := (\mathbf{X}, E \setminus \{e\}, \Psi|E \setminus \{e\})$ on edelleen yhtenäinen, mikä on ristiriita kohdan c) oletuksen kanssa. □

Lause 12.8.4 Jos $G = (\mathbf{X}, E, \Psi)$ on äärellinen suuntaamaton metsä, jossa on p komponenttia, on voimassa

$$\#\mathbf{X} = \#E + p.$$

Erikoisesti, jos G on puu, on $\#\mathbf{X} = \#E + 1$.

Todistus. Todistetaan ensin jälkimmäinen väite induktiolla kaarien lukumäärän $\#E$ suhteen. Jos $\#E = 0$, niin solmuja ei voi olla kuin yksi, eli $\#\mathbf{X} = 1$. Oletetaan, että väite pätee puille, joissa on kaaria korkeintaan m kappaletta. Olkoon G puu, jossa $\#E = m + 1$. Olkoon e sen eräs kaari. Verkko

$$G - e := (\mathbf{X}, E \setminus \{e\}, \Psi|E \setminus \{e\})$$

on Lauseen 12.8.3 kohdan c) nojalla epäyhtenäinen, mutta sen yhtenäiset komponentit

$$G_i = (\mathbf{X}_i, E_i, \Psi_i), \quad i \in [k]$$

ovat puita ja $\#E_i \leq m$ kaikilla $i \in [k]$. Osoitetaan, että $k = 2$, ts. että $\mathbf{X} = \mathbf{X}_1 \cup \mathbf{X}_2$. Olkoon $\Psi(e) = \{x_1, x_2\}$. Nämä ovat eri solmuja ja sijaitsevat eri komponenteissa $\mathbf{X}_i$ ja $\mathbf{X}_j$. Indeksoidaan joukot uudelleen niin, että $x_1 \in \mathbf{X}_1$ ja $x_2 \in \mathbf{X}_2$. Olkoon $x \in \mathbf{X}\backslash\{x_1, x_2\}$ mielivaltainen. Koska G on yhtenäinen, on olemassa ketju $c = (e_1, e_2, \ldots, e_n)$ päinä x ja x_1. On kaksi mahdollisuutta:

1) Jos c on verkon $G - e$ ketju, niin x ja x_1 ovat verkon $G - e$ samassa komponentissa ja siten $x \in \mathbf{X}_1$.

2) Jos taas $e \in \{e_1, e_2, \ldots, e_n\}$, on olemassa ketju päinä x ja x_2, joten $x \in \mathbf{X}_2$.

Kohtien 1) ja 2) nojalla $x \in \mathbf{X}_1 \cup \mathbf{X}_2$. On siis osoitettu, että $\mathbf{X} = \mathbf{X}_1 \cup \mathbf{X}_2$, joten $k = 2$. Koska $\#E_i \leq m$, seuraa induktio-oletuksesta

$$\#\mathbf{X}_i = \#E_i + 1, \quad i = 1, 2.$$

Koska $\mathbf{X}_1 \cap \mathbf{X}_2 = \emptyset$ ja $E_1 \cap E_2 = \emptyset$, on summaperiaatteen nojalla

$$\begin{aligned} \#\mathbf{X} = \#\mathbf{X}_1 + \#\mathbf{X}_2 &= \#E_1 + \#E_2 + 2 = \#(E_1 \cup E_2) + 2 \\ &= \#(E \setminus \{e\}) + 2 = \#E - 1 + 2 = \#E + 1. \end{aligned}$$

Jos G on metsä, jossa on p yhtenäistä komponenttia, on kukin komponentti puu, jossa on solmuja yksi enemmän kuin kaaria, yhteensä p kappaletta. □

12.9 Virittävät puut

Jos halutaan tutkia verkkoa lähinnä sen solmujen osalta, ei ole tarpeen käyttää sen kaikkia kaaria. Verkossa liikkuminen helpottuu, jos sille löydetään aliverkko, joka sisältää samat solmut, mutta on puu.

Määritelmä 12.9.1 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko. Jos sen aliverkko $H = (\mathbf{X}, E', \Psi|E')$ on puu, sanotaan, että H *virittää* verkon G, tai että H on verkon G *virittävä* puu.

Lause 12.9.2 Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton verkko, joka on yhtenäinen. Jos $G' = (\mathbf{X}, E', \Psi|E')$ on sen syklitön aliverkko, on olemassa sellainen puu $H = (\mathbf{X}, F, \Psi|F)$, että $E' \subseteq F \subseteq E$.

Todistus. Induktiolla luvun $d := \#E - \#E'$ suhteen.

1) Arvolla $d = 0$ on $E = E'$, jolloin G oletusten mukaan on itse puu.

2) Oletetaan, että väite on tosi sellaisille äärellisille yhtenäisille verkoille ja niiden syklittömille aliverkoille, joille $d \leq n$. Olkoon $d = n+1$ ja G, G' lauseen oletukset

toteuttavia verkkoja. Jos itse G on syklitön, on $H := G$ vaatimukset täyttävä puu. Olkoon siis S verkon G sykli. Koska G' on syklitön, on olemassa kaari $e \in (E\backslash E') \cap S$. Tällöin verkko

$$G - e := (\mathbf{X}, E\backslash\{e\}, \Psi|E\backslash\{e\})$$

on yhtenäinen, $E' \subseteq E\backslash\{e\}$ ja $\#(E\backslash\{e\}) - \#E' = n$. Induktio-oletuksen mukaan on olemassa sellainen puu $H = (\mathbf{X}, F, \Psi|F)$, että $E' \subseteq F \subseteq E\backslash\{e\} \subseteq E$. □

Seuraus 12.9.3 Äärellinen suuntaamaton verkko on puun virittämä jos ja vain jos se on yhtenäinen.

Todistus. Jos verkon G virittää puu, on G tällöin triviaalisti yhtenäinen. Oletetaan, että verkko G on yhtenäinen. Valitaan jokin kaari $e \in E$ ja sovelletaan Lausetta 12.9.2 joukkoon $E' := \{e\}$. Vastaava verkko $G' := (\mathbf{X}, E', \Psi|E')$ on syklitön, joten on olemassa verkon G virittävä puu. □

Huomautus 12.9.4 Lauseesta 12.9.2 voidaan kehittää algoritmi yhtenäisen verkon virittävän puun löytämiseksi. On kaksi tapaa toimia:

1) Vähennetään verkosta kaaria niin, että verkko säilyy yhtenäisenä.

2) Otetaan verkon syklitön aliverkko, esimerkiksi yksi kaari, ja lisätään kaaria niin, että verkko pysyy syklittömänä.

***Virittävien puiden lukumäärä.** Esitetään todistamatta kaksi tunnettua suuntaamattoman verkon virittävien puiden lukumäärää koskevaa tulosta.

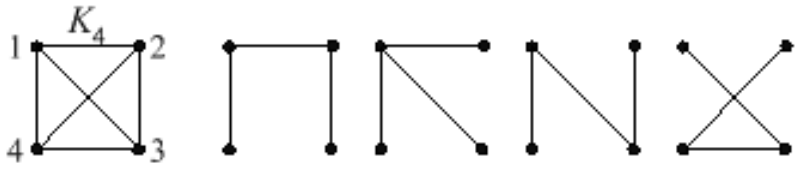
Lause 12.9.5 (Cayleyn lause) Olkoon $K_n = (\mathbf{X}, E, \Psi)$ äärellinen, täydellinen yksinkertainen suuntaamaton verkko, jossa on $n \geq 2$ solmua. Verkolla K_n on n^{n-2} erilaista virittävää puuta.

Esimerkki 12.9.6 Verkon K_4 virittäviä puita ovat Kuvassa 29 esiintyvät tyypit eri asennoissa, ja kussakin luokassa on 4 erilaista puuta.

Yhteensä näitä on siis $4 \cdot 4 = 4^{4-2} = 16$.

Lause 12.9.7 (Kirchhoffin lause) Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen yhtenäinen silmukaton verkko matriisina $A_G = (a_{ij})_{n\times n}$. Olkoon D_G se diagonaalimatriisi, jonka diagonaalin muodostavat solmujen asteluvut $d_G(x_i)$, $i \in [n]$, ja

$$C_G := -A_G + D_G.$$



Kuva 29: Verkon K_4 virittävien puiden tyypit

Verkon G virittävien puiden määrä on

$$N = |\det(C_G(1,1))|,$$

missä determinantti on alkiota c_{11} vastaava matriisin C_G alideterminantti (ks. *Lineaarialgebra*). Itse asiassa voitaisiin ottaa mikä tahansa alideterminantti.

Esimerkki 12.9.8 Olkoon G verkko, jonka matriisi on

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad \text{jolloin} \quad C_G = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 2 & -1 & 0 \\ -1 & -1 & 3 & -1 \\ -1 & 0 & -1 & 2 \end{pmatrix}.$$

Verkon G virittävien puiden lukumäärä on täten

$$N = |\det(C_G(1,1))| = \left| \det \begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{pmatrix} \right| = 8.$$

13 SUUNNATUT VERKOT

Jos verkon solmujen välisiin kaariin liitetään suunta, syntyy ns. suunnattu verkko. Suuntaaminen saadaan aikaan yksinkertaisesti korvaamalla suuntaamattoman verkon tapauksessa käytetty ei-järjestetty tulo $\mathbf{X} \,\&\, \mathbf{X}$ tulolla $\mathbf{X}\times\mathbf{X}$. (ks. Määritelmät 12.1.1 ja 12.1.3). Suunnattua verkkoa käytetään mallina struktuureissa, joissa liikenne kutakin kahden vierekkäisen solmun välistä kaarta pitkin on sidottu yhteen suuntaan.

13.1 Suunnatun verkon määrittely

Määritelmä 13.1.1 Kolmikko $G = (\mathbf{X}, U, \Psi)$ on *suunnattu verkko* eli *digraafi* (*directed graph, digraph*), jos $\mathbf{X} \neq \emptyset$ ja U ovat joukkoja ja $\Psi : U \to \mathbf{X}\times\mathbf{X}$ on kuvaus. Joukon $\mathbf{X}$ alkiot ovat verkon G *solmuja* (*vertex, node*), joukon U alkiot *nuolia* tai *suunnattuja välejä* (arc, arrow) ja kuvaus Ψ *vastaavuuskuvaus*.

Jos $\Psi(u) = (x, y)$, solmu x on nuolen u *lähtö-* tai *alkusolmu* ja y *maali-* tai *loppusolmu*, yhteiseltä nimeltään *päätesolmut*. Sanotaan, että nuoli u *yhdistää* solmun x solmuun y; merkitään $x \to y$. Suunnatun verkon olioille käytetään suuntaamattomien verkkojen yhteydessä esitettyjä nimityksiä *liittyy, vierekkäinen, rinnakkainen, silmukka eli luuppi, erillinen, surkastunut, äärellinen*, jos näitä voidaan käyttää tilanteessa, jossa nuolet tulkitaan kaariksi. Lisäksi sanotaan, että nuolet $u \neq v$ ovat *vahvasti rinnakkaiset*, jos $\Psi(u) = \Psi(v)$, ja *vastakkaiset*, jos $\Psi(u) = (x, y)$ ja $\Psi(v) = (y, x)$. Solmun x *lähtöaste* eli *positiivinen asteluku* on luku

$$d_G^+(x) := \#\big\{\, u \in U \mid \Psi(u) = (x, y),\ y \in \mathbf{X} \,\big\}$$

ja *maaliaste* eli *negatiivinen asteluku*

$$d_G^-(x) := \#\big\{\, u \in U \mid \Psi(u) = (y, x),\ y \in \mathbf{X} \,\big\}.$$

Jos $\Psi(u) = (x, y)$, sanotaan, että u *liittyy positiivisesti* solmuun x ja *negatiivisesti* solmuun y.

Verkko on *täydellinen*, jos jokaista solmuparia $x \neq y$ yhdistää nuoli ainakin toiseen suuntaan. Verkko on *yksinkertainen*, jos se ei sisällä silmukoita eikä vahvasti rinnakkaisia nuolia. Yksinkertaisessa verkossa nuoli u samaistetaan kuvaansa $u \sim \Psi(u) = (x, y)$.

Esimerkki 13.1.2 Olkoot $\mathbf{X} = \{x_1, x_2, x_3\}$, $U = \{u_1, u_2, u_3, u_4\}$ ja

$$\begin{array}{lcllcl} \Psi(u_1) & = & (x_3, x_1), & \Psi(u_2) & = & (x_1, x_3), \\ \Psi(u_3) & = & (x_1, x_1), & \Psi(u_4) & = & (x_1, x_2). \end{array}$$

Verkko $G := (\mathbf{X}, U, \Psi)$ ei ole yksinkertainen eikä täydellinen. Solmun x_1 asteet ovat $d_G^+(x_1) = 3$, $d_G^-(x_1) = 2$, entä muiden?

Tehtävä 13.1.3 Piirrä Esimerkin 13.1.2 tilanteesta Esimerkin 12.1.4 kuviota vastaava joukko-opillinen kaavio.

13.2 Suunnatun verkon aliverkko

Määritelmä 13.2.1 a) Suunnattu verkko $G' = (\mathbf{X}', U', \Psi')$ on suunnatun verkon $G = (\mathbf{X}, U, \Psi)$ *aliverkko* (merkitään $G' \subseteq G$), jos seuraavat ehdot ovat voimassa:

1) $\emptyset \neq \mathbf{X}' \subseteq \mathbf{X}$,

2) $U' \subseteq U$,

3) $\Psi(U') \subseteq \mathbf{X}' \times \mathbf{X}'$ ja $\Psi' = \Psi | U'$.

Jos erikoisesti $U' = \Psi^{-1}(\mathbf{X}' \times \mathbf{X}')$, on G' solmujoukon $\mathbf{X}'$ *virittämä* aliverkko.

b) Verkon $G = (\mathbf{X}, U, \Psi)$ *diagonaali* on joukko $\Delta_{\mathbf{X}} := \{\, (x, x) \mid x \in \mathbf{X} \,\}$. Verkon G *komplementti* on suunnattu verkko $\overline{G} = (\mathbf{X}, V, \Gamma)$, missä

$$V := \mathbf{X} \times \mathbf{X} \setminus (\Psi(U) \cup \Delta_{\mathbf{X}})$$

ja $\Gamma : V \to \mathbf{X} \times \mathbf{X}$ on identtinen kuvaus.

Huomautus 13.2.2 a) Jokaiseen suunnattuun verkkoon $\vec{G} = (\mathbf{X}, U, \Psi)$ liittyy suuntaamaton verkko $G = (\mathbf{X}, E, \Phi)$, missä

$$[\, \Phi(u) = \{x, y\} \,] \;\Leftrightarrow\; [\, \Psi(u) = (x, y) \,],$$

ts. nuolet on korvattu kaarilla. Tätä sanotaan suunnattua verkkoa *vastaavaksi suuntaamattomaksi verkoksi*.

b) Suuntaamattomasta verkosta päästään suunnattuun, kun jokainen kaari $\{x, y\}$ korvataan nuolilla (x, y) ja (y, x). Näin saatua verkkoa sanotaan suuntaamatonta verkkoa *vastaavaksi suunnatuksi verkoksi*. Lauseessa 13.5.2 tarkastellaan vielä erästä yhtenäisen verkon suuntaamistapaa.

c) Yksinkertaisen, täydellisen n-solmuisen suunnatun verkon solmun lähtö- ja tuloasteiden summa on *vähintäin* $n-1$, kun taas suuntaamattoman verkon asteet ovat tasan $n-1$.

Esimerkki 13.2.3 Esimerkissä 13.1.2 oli suunnattu verkko $G = (\mathbf{X}, U, \Psi)$, missä $\mathbf{X} = \{x_1, x_2, x_3\}$, $U = \{u_1, u_2, u_3, u_4\}$ ja

$$\begin{array}{lcllcl} \Psi(u_1) & = & (x_3, x_1), & \Psi(u_2) & = & (x_1, x_3), \\ \Psi(u_3) & = & (x_1, x_1), & \Psi(u_4) & = & (x_1, x_2). \end{array}$$

Sen aliverkkoja ovat mm. $G' = (\mathbf{X}', U', \Psi')$, kun

a) $\mathbf{X}' = \{x_1, x_2\}$, $U' = \{u_3\}$ ja $\Psi'(u_3) = (x_1, x_1)$.

b) $\mathbf{X}' = \{x_1, x_3\}$, $U' = \{u_1\}$ ja $\Psi'(u_1) = (x_3, x_1)$.

Onko kohdan b) aliverkko solmujoukon $\{x_1, x_3\}$ virittämä aliverkko?

Muodostetaan vielä verkon G komplementti puuttuvien nuolien

$$V := (\mathbf{X}\times\mathbf{X}) \setminus (\Psi(U) \cup \Delta_{\mathbf{X}}) = \{(x_2, x_1), (x_2, x_3), (x_3, x_2)\}$$

avulla; $\overline{G} := (\mathbf{X}, V, \mathrm{Id}_V)$.

Lause 13.2.4 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko. Silloin

$$\sum_{x\in\mathbf{X}} d_G^+(x) + \sum_{x\in\mathbf{X}} d_G^-(x) = 2 \cdot \#U.$$

Todistus. Jokaisella nuolella on täsmälleen yksi lähtö ja maali. □

13.3 Suunnattujen verkkojen esitystapoja

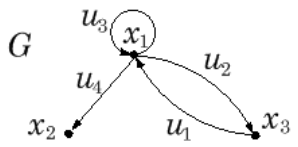
Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko. Verkkoa voidaan kuvata havainnollisesti luettelona tai kaaviona ja matemaattiseen käsittelyyn sopivalla yhteysmatriisilla.

1. Luettelo antaa solmujen ja nuolien joukot sekä vastaavuuskuvauksen:

$$\begin{array}{ll} \text{solmut} & \mathbf{X} = \{x_1, x_2, \ldots, x_n\}, \\ \text{nuolet} & U = \{u_1, u_2, \ldots, u_m\}, \\ \text{vastaavuus} & \Psi : (x_{k_1}, x_{l_1}), (x_{k_2}, x_{l_2}), \ldots, (x_{k_m}, x_{l_m}), \end{array}$$

missä $\Psi(u_i) = (x_{k_i}, x_{l_i})$, $i \in [m]$ (vrt. Esimerkki 13.1.2).

2. Nuolikaavio on geometrinen kuvio, jossa solmuja vastaavat pisteet ja nuolia geometriset suunnistetut kaaret tasossa (*tasoverkko*) tai muussa avaruudessa (*avaruusverkko*), ks. Luku 12 *Kaavioesitys* ja Luku 14 *Taso- vai avaruusverkko?* Kuvassa 30 Esimerkin 13.1.2 verkko tasokaaviona.



Kuva 30: Esimerkin 13.1.2 verkko nuolikaaviona

3. Yhteysmatriisi (*adjacency matrix*) $M_G = (a_{ij})_{n\times n}$ muodostuu vahvasti rinnakkaisten nuolten lukumääristä

$$a_{ij} := \#(\Psi^{-1}((x_i, x_j))), \quad i, j \in [n].$$

Toisin kuin suuntaamattoman verkon tapauksessa M_G ei ole yleensä symmetrinen, joten suunnatun verkon koko matriisi sisältää informaatiota. Esimerkin 13.1.2 tapauksessa yhteysmatriisi on

$$M_G = (a_{ij})_{3\times 3} = \begin{array}{c} G \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$$

Huomautus 13.3.1 Suunnattuun verkkoon $G = (\mathbf{X}, U, \Psi)$ liittyy yksinkertainen suunnattu verkko $G_0 := \big(\mathbf{X}, \Psi(U)\backslash\Delta_{\mathbf{X}}, \mathrm{Id}\big)$, josta siis on poistettu ylimääräiset rinnakkaiset nuolet ja kaikki luupit.

Nuolten kuvajoukkoa $\Psi(U) \subseteq \mathbf{X}\times\mathbf{X}$ (luupitkin yksinkertaisina mukaan lukien) sanotaan verkon G *seuraajarelaatioksi*, sitä merkitään $R_G := \Psi(U)$ ja

$$[\, xR_Gy \,] \;\Leftrightarrow\; [\, \Psi(u) = (x, y) \text{ jollekin } u \in U \,].$$

Yksinkertainen suunnattu verkko on siis tulkittavissa relaatioksi. Useissa yhteyksissä riittää tarkastella ei-yksinkertaistakin verkkoa sen seuraajarelaation avulla. Matriiseille pätee joka tapauksessa

$$M_{R_G} = \mathrm{SIGN}(M_G).$$

Esimerkki 13.3.2 Olkoot $\mathbf{X} = \{x_1, x_2, x_3\}$, $U = \{u_1, u_2, u_3\}$ ja

$$\Psi(u_1) = \Psi(u_2) = (x_1, x_2), \quad \Psi(u_3) = (x_1, x_3).$$

Tällöin $R_G = \{(x_1, x_2), (x_1, x_3)\}$.

13.4 Polut ja yhtenäisyys

Ketjua vastaa suunnatussa verkossa polku, jolla on selkeästi määräytyvä suunta. Olkoon $G = (\mathbf{X}, U, \Psi)$ tässä pykälässä äärellinen suunnattu verkko.

Määritelmä 13.4.1 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko. Nuolivektori $p = (u_1, u_2, \ldots, u_n) \in U^n$ on *polku* verkossa G, jos

1) $u_i \neq u_j$ kaikilla $i \neq j$,

2) on olemassa solmujono $(x_0, x_1, \ldots, x_n) \in \mathbf{X}^{n+1}$, jolle

$$\Psi(u_i) = (x_{i-1}, x_i)$$

kaikilla $i \in [n]$.

Jos p toteuttaa ehdon 2), sitä sanotaan *nuolijonoksi*. Solmu x_0 on polun *lähtö* ja x_n *maali*; merkitään $x_0 \to x_n$. Sanotaan, että polku p *kulkee* solmujen x_0, x_1, …, x_n kautta; merkitään $p = (u_1, u_2, \ldots, u_n) \sim (x_0, x_1, \ldots, x_n)$. Jos $x_0 = x_n$, on polku *suljettu*, muutoin *avoin*. Jos kaikille muille indekseille on $x_i \neq x_j$, on polku *yksinkertainen*. Merkitään polkuun kuuluvien nuolten joukkoa $< p >:= \{u_1, u_2, \ldots, u_n\}$ ja polun *pituutta* eli sen nuolten määrää $|p| := \# < p >$.

Polku $p' = (v_1, v_2, \ldots, v_m)$ on polun p *alipolku*, (merkitään $p' \subseteq p$), jos jollekin $i \in [n-m+1]$

$$p' = (u_i, u_{i+1}, \ldots, u_{i+m-1}).$$

Alipolku $p' \subseteq p$ on *aito*, jos $p' \neq p$. Nuolijonolle käytetään vastaavia nimityksiä ja merkintöjä.

Huomautus 13.4.2 a) Polku määrää solmujonon yksikäsitteisesti: jos

$$p = (u_1, \ldots, u_n) \sim (x_0, \ldots, x_n) \text{ ja } p = (u_1, \ldots, u_n) \sim (y_0, \ldots, y_n),$$

on $x_i = y_i$ kaikilla $i \in [n] \cup \{0\}$. Sen sijaan annettua solmujonoa voi vastata useita polkuja. Jos verkko on yksinkertainen, myös solmujono määrää polun yksikäsitteisesti (vrt. Huomautus 12.5.2 b).

b) Jokaista polkua $x \to y$ kohti on olemassa yksinkertainen polku $x \to y$ (harjoitustehtävä, vrt. Lause 12.5.4).

Esimerkki 13.4.3 Olkoot $\mathbf{X} = \{x_1, x_2, x_3\}$ ja $U = \{u_1, u_2, u_3\}$ sekä

$$u_1 = (x_1, x_2), \quad u_2 = (x_2, x_3), \quad u_3 = (x_3, x_2).$$

Polku (u_1, u_2, u_3) ei ole suljettu eikä yksinkertainen, sillä vastaava solmujono on (x_1, x_2, x_3, x_2). Sen aito alipolku (u_2, u_3) on suljettu ja yksinkertainen. Nuolijono (u_1, u_2, u_3, u_2) ei ole polku.

Määritellään kaksi eriasteista yhtenäisyyden käsitettä. Siihen tarvitaan ekvivalenssirelaation määräämää ositusta.

Lause 13.4.4 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko. Joukko

$$S := \{\, (x, y) \in \mathbf{X}\times\mathbf{X} \mid x = y \text{ tai on olemassa polut } x \to y \text{ ja } y \to x \,\}$$

on ekvivalenssirelaatio joukossa $\mathbf{X}$.

Todistus. Kuten suuntaamattoman verkon tapauksessa, ks. Lause 12.5.5. □

Määritelmä 13.4.5 Suunnatun verkon $G = (\mathbf{X}, U, \Psi)$ *vahvasti yhtenäiset komponentit* ovat solmujoukkojen $S(x)$, $x \in \mathbf{X}$, virittämät aliverkot. Verkko G on *vahvasti yhtenäinen*, jos sillä on vain yksi vahvasti yhtenäinen komponentti.

Määritelmä 13.4.6 Äärellinen suunnattu verkko on *yhtenäinen*, jos sitä vastaava suuntaamaton verkko on yhtenäinen (nuolet on korvattu kaarilla).

Huomautus 13.4.7 a) Suunnatun verkon G vahvasti yhtenäisen komponentin G_i jokaista solmuparia (x, y), $x \neq y$, kohti on olemassa polut $x \to y$ ja $y \to x$ verkossa G_i.

b) Suunnattu verkko G on vahvasti yhtenäinen jos ja vain jos jokaista solmuparia (x, y), $x \neq y$, kohti on olemassa polut $x \to y$ ja $y \to x$ verkossa G. Verkko itse on nimittäin sen ainoa vahvasti yhtenäinen komponentti.

c) Vahvasti yhtenäinen suunnattu verkko on aina yhtenäinen. Esimerkin 13.4.3 verkko on yhtenäinen, mutta ei vahvasti yhtenäinen.

d) Vahvasti yhtenäiset komponentit löytyvät esimerkiksi depth-first-etsinnän avulla (harjoitustehtävä).

13.5 *Suuntaamattoman verkon suunnistaminen

Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen yhtenäinen suuntaamaton verkko.

Määritelmä 13.5.1 Äärellinen yhtenäinen suuntaamaton verkko on *suunnistuva* (*orientable*), jos sen kaaret voidaan muuttaa nuoliksi niin, että saadaan vahvasti yhtenäinen suunnattu verkko.

Ongelma. Millaisen verkon kaarille voidaan kiinnittää suunta niin, että saadaan vahvasti yhtenäinen suunnattu verkko?

Lause 13.5.2 Äärellinen yhtenäinen suuntaamaton verkko on suunnistuva jos ja vain jos sen jokainen kaari kuuluu johonkin suljettuun ketjuun. Erikoisesti yhtenäinen Eulerin verkko on suunnistuva.

Todistus. a) Jos verkko G on suunnistuva, suunnistetaan se vahvasti yhtenäiseksi suunnatuksi verkoksi $\overline{G}$. Olkoon e jokin verkon G kaari. Jos e on silmukka, on se suljetussa ketjussa (e). Olkoot kaaren e päät $x \neq y$. Olkoon $\overline{e}$ kaarta e vastaava verkon $\overline{G}$ nuoli, esimerkiksi $x \to y$. Verkossa $\overline{G}$ on polku $p : y \to x$. Yhdistämällä p ja $(\overline{e})$ saadaan suljettu polku, johon $\overline{e}$ kuuluu. Tällöin vastaava verkon G ketju sisältää kaaren e.

b) Olkoon G sellainen, että sen jokainen kaari kuuluu suljettuun ketjuun. Suunnistetaan yksi tällainen ketju c_0 poluksi p_0 kulkemalla se yhteen suuntaan ja antamalla kullekin kaarelle menosuunta. Syntynyt suunnattu aliverkko G_0 on vahvasti yhtenäinen. Toistetaan seuraavaa arvoilla $i = 1, 2, \ldots$, kunnes kaikki kaaret on suunnistettu:

Jos verkossa G on kaaria, joille ei vielä suuntaa ole annettu, valitaan sellainen kaari $e_i \notin G_{i-1}$, jolla on yhteinen pää $x_i \in G_{i-1}$ jonkin jo suunnistetun ketjun c_m, $m \leq i-1$, kaaren kanssa. Olkoon $y_i \notin G_{i-1}$ kaaren e_i toinen pää. Valitaan suljettu ketju c_i', johon e_i kuuluu. Lähdetään etenemään ketjussa c_i' seuraavasti:

$$x_i \to y_i \to \ldots \to z_i,$$

missä z_i on ensimmäinen vastaan tuleva jo suunnistettuun aliverkkoon G_{i-1} kuuluva solmu.
α) Jos $x_i = z_i$, suunnistetaan ketju $c_i := c_i'$ äskeisen kulkusuunnan mukaan poluksi p_i.
β) Oletetaan, että $x_i \neq z_i$. Koska aliverkko G_{i-1} on vahvasti yhtenäinen, on siellä polku $p_i' : z_i \to x_i$. Suunnistetaan kuljettu ketjun c_i' aliketju polun p_i' suunnan mukaan poluksi p_i.

Näin saatu aidosti laajempi aliverkko on vahvasti yhtenäinen. □

13.6 Hamiltonin polut

Jos kauppamatkustajan ongelmaa tutkitaan suunnatussa verkossa, on Hamiltonin polun olemassaolo-ongelma vielä hankalampi kuin suuntaamattomassa verkossa. Olkoon $G = (\mathbf{X}, U, \Psi)$ tässä pykälässä äärellinen suunnattu verkko.

Määritelmä 13.6.1 Äärellisen suunnatun verkon yksinkertainen polku, joka kulkee kaikkien solmujen kautta, on *Hamiltonin polku*. Verkko on *Hamiltonin verkko*, jos siinä on suljettu Hamiltonin polku.

Probleema. Millaisissa verkoissa on Hamiltonin polkuja?

Osoitetaan, että äärellisessä täydellisessä suunnatussa verkossa on avoin Hamiltonin polku. Jos verkko lisäksi on vahvasti yhtenäinen, se on Hamiltonin verkko. Esimerkki 13.6.7 osoittaa, että verkon äärellisyys on välttämätön ominaisuus. Täydellisyys ei tietenkään ole välttämätöntä.

Huomautus 13.6.2 a) Suunnatussa verkossa on Hamiltonin polku jos ja vain jos vastaavassa yksinkertaisessa verkossa on Hamiltonin polku. Riittää siis tarkastella yksinkertaisia verkkoja.

b) Jos suunnatussa verkossa on (suljettu) Hamiltonin polku, niin vastaavassa suuntaamattomassa verkossa on (suljettu) Hamiltonin ketju.

c) Jos verkossa on suljettu Hamiltonin polku, on siinä myös avoin Hamiltonin polku. Jos suunnatussa verkossa on avoin Hamiltonin polku, jota ei voi sulkea, voi siinä silti olla suljettujakin Hamiltonin polkuja.

d) Olkoon $p = (u_1, u_2, \ldots, u_n) \sim (x_0, x_1, \ldots, x_n)$ Hamiltonin polku suunnatussa verkossa G. Kun määritellään alipolut

$$p_i := (u_1, u_2, \ldots, u_i), \quad i \in [n],$$

niin jokaista $y \neq x_0$ kohti on olemassa indeksi $i \in \mathbb{N}$, jolle p_i on polku $x_0 \to y$.

Määritelmä 13.6.3 Suunnatun verkon $G = (\mathbf{X}, U, \Psi)$ solmu x on *juuri*, jos jokaista $y \in \mathbf{X}$, $y \neq x$, kohti on olemassa polku $x \to y$.

Lause 13.6.4 Jos suunnatussa verkossa on Hamiltonin polku, on siinä ainakin yksi juuri.

Todistus. Jos Hamiltonin polku on avoin, on sen lähtösolmu juuri. Jos polku on suljettu, jokainen solmu on juuri. □

Lause 13.6.5 Äärellisessä täydellisessä suunnatussa verkossa on juuri.

Todistus. Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen täydellinen suunnattu verkko. Todistetaan väite induktiolla solmuluvun $\#\mathbf{X}$ suhteen.

1) Tapaukset $\#\mathbf{X} = 1, 2$ ovat selviä.

2) Olkoon väite tosi verkoille, joissa on $k \geq 2$ solmua. Olkoon G verkko, jossa on $k + 1$ solmua. Valitaan $x \in \mathbf{X}$. Olkoon G' solmujoukon $\mathbf{X} \setminus \{x\}$ virittämä aliverkko. Koska G on täydellinen, on myös G' täydellinen. Verkossa G' on k solmua, joten induktio-oletuksen nojalla siinä on juuri, olkoon eräs niistä y. Olkoon $z \in \mathbf{X} \setminus \{x\}$ mielivaltainen. Silloin verkossa G' on polku $y \to z$. Koska G on täydellinen, on olemassa $u \in U$, jolle $\Psi(u) = (x, y)$ tai $\Psi(u) = (y, x)$. Edellisessä tapauksessa on olemassa polku $x \to z$, ja siten x on juuri verkossa G. Jälkimmäisessä taas y on juuri. □

Seuraus 13.6.6 Oletetaan, että $G = (\mathbf{X}, U, \Psi)$ on äärellinen täydellinen suunnattu verkko, jossa on $n \geq 2$ solmua. Jos $x \in \mathbf{X}$ on verkon G juuri, on olemassa solmujoukon $\mathbf{X}' := \mathbf{X} \setminus \{x\}$ virittämän aliverkon juuri x' ja nuoli $u \in U$, joille $\Psi(u) = (x, x')$.

Todistus. Harjoitustehtävä. □

Esimerkki 13.6.7 Kokonaislukujen joukossa $\mathbb{Z}$ relaatio

$$R := \{\, (x, y) \in \mathbb{Z}\times\mathbb{Z} \mid x \leq y \,\}$$

voidaan tulkita suunnatuksi verkoksi, jonka solmujoukko on $\mathbb{Z}$, nuolet

$$U := \{\, u_{x,y} = (x, y) \mid x \leq y \,\}$$

ja $\Psi : U \to \mathbb{Z}\times\mathbb{Z}$ identtinen kuvaus. Verkko $G := (\mathbb{Z}, U, \Psi)$ on ääretön täydellinen suunnattu verkko, jossa ei ole juurta. Jos $\mathbb{Z}$ korvataan luonnollisten lukujen joukolla, on alkio 1 juuri ja verkossa on avoin Hamiltonin polku, mutta ei suljettua.

Lause 13.6.8 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen täydellinen suunnattu verkko, jossa on vähintäin kaksi solmua.

a) Verkon G jokaisesta juuresta lähtee Hamiltonin polku.

b) Verkossa G on Hamiltonin polku.

c) Jos verkko G on vahvasti yhtenäinen, se on Hamiltonin verkko.

Todistus. a) Induktiolla solmuluvun $\#\mathbf{X}$ suhteen.

1) Tapaus $\#\mathbf{X} = 2$ on selvä.

2) Olkoon väite tosi arvolla $k = \#\mathbf{X} \geq 2$. Olkoon verkossa G solmuja $k+1$ kappaletta. Olkoon $x \in \mathbf{X}$ verkon G juuri. Olkoon G' solmujoukon $\mathbf{X}' := \mathbf{X} \setminus \{x\}$ virittämä aliverkko. Verkko G' on täydellinen ja $\#\mathbf{X}' = k$. Etsitään verkosta G Hamiltonin polku, jonka lähtösolmu on x.

Induktio-oletuksen mukaan verkon G' juurista lähtee Hamiltonin polkuja. Koska x on verkon G juuri, on Seurauksen 13.6.6 nojalla olemassa verkon G' juuri x' ja $u \in U$, joille $\Psi(u) = (x, x')$. Olkoon

$$(v_1, v_2, \ldots, v_m) \sim (x', x'_1, \ldots, x'_m)$$

juuresta x' lähtevä Hamiltonin polku verkossa G'. Polku

$$(u, v_1, v_2, \ldots, v_m) \sim (x, x', x'_1, \ldots, x'_m)$$

on verkon G Hamiltonin polku, joka lähtee juuresta x.

b) Lause 13.6.5 ja kohta a).

c) Sivuutetaan. □

Lause 13.6.9 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen vahvasti yhtenäinen suunnattu verkko, jossa on $n \geq 2$ solmua. Jos jokaiselle solmulle $x \in \mathbf{X}$ pätee

$$d^+_G(x) \geq \frac{n}{2} \quad \text{ja} \quad d^-_G(x) \geq \frac{n}{2},$$

on G Hamiltonin verkko.

Todistus. Sivuutetaan. Lause on Diracin Lauseen 12.6.3 muunnelma. □

Esimerkki 13.6.10 Äärellistä täydellistä yksinkertaista suunnattua verkkoa, jossa jokaista solmuparia yhdistää täsmälleen yksi nuoli, sanotaan *turnaukseksi* (*tournament*). Nimi johtuu siitä, että verkko kuvaa kilpailua, jossa jokainen pelaa jokaista vastaan eikä tasapeleja hyväksytä. Jos turnaus on relaationa transitiivinen, se ei ole vahvasti yhtenäinen ja sen pelaajat muodostavat yksikäsitteisen avoimen Hamiltonin polun.

Algoritmeja Hamiltonin polun löytämiseksi

Triviaalialgoritmi toimii kuten suuntaamattomankin verkon tapauksessa, mutta on tietenkin suoritusajaltaan ei-polynomiaalinen.

Äärellisen täydellisen suunnatun verkon avoimen Hamiltonin polun etsiminen käy myös Lauseen 13.6.8 a) todistuksesta poimitulla verkon tyhjentämiseen perustuvalla algoritmilla, jossa käytetään edellä todistettuja tuloksia. Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen täydellinen suunnattu verkko, jossa on $n \geq 2$ solmua. Olkoon $G_0 := G$. Lauseen 13.6.5 nojalla verkossa G_0 on juuri ja Lauseen 13.6.8 a) mukaan juuresta lähtee Hamiltonin polku.

> *Valitaan verkon G_0 juuri x_0.* Toistetaan arvoilla $i = 1, 2, \ldots, n-1$:
>
> *Olkoon G_i se verkon G_{i-1} aliverkko, joka saadaan poistamalla solmu x_{i-1} ja siihen liittyvät nuolet. Verkko G_i on täydellinen, joten siinä on juuria. Valitaan sellainen solmusta x_{i-1} lähtevä nuoli u_i, jonka maali on verkon G_i juuri x_i (Seuraus 13.6.6), ja lisätään polkuun $p_i := (u_1, u_2, \ldots, u_i)$.*

Polku $p_{n-1} = (u_1, u_2, \ldots, u_{n-1})$ on eräs avoin Hamiltonin polku alkuperäisessä verkossa G. Lisäksi voidaan tarkastaa, voidaanko polku vielä täydentää suljetuksi. Menetelmä on esitetty pseudo-ohjelmana Kuvassa 31.

Aseta $i = 0$; $n = \#\mathbf{X}$; $G_0 = (\mathbf{X}_0, U_0, \Psi_0) = (\mathbf{X}, U, \Psi)$;
etsi verkosta G_0 juuri $x_0 \in \mathbf{X}_0$;
while $(i < n - 1)$ aseta $i = i + 1$;
$\mathbf{X}_i = \mathbf{X}_{i-1} \setminus \{x_{i-1}\}$;
$U_i = U_{i-1} \setminus \{$ nuolet päänä $x_{i-1}\}$;
$\Psi_i = \Psi_{i-1}|U_i$;
$G_i = (\mathbf{X}_i, U_i, \Psi_i)$;
etsi juuri $x_i \in G_i$, jolle $\Psi(u_i) = (x_{i-1}, x_i)$;
aseta $p_i = (u_1, u_2, \ldots, u_i)$;
end while
(**if** on olemassa u_n, jolle $\Psi(u_n) = (x_{n-1}, x_0)$
aseta $p_n = (u_1, u_2, \ldots, u_{n-1}, u_n)$ **end if**)

Kuva 31: Tyhjennysalgoritmi

Annetusta suunnatusta verkosta on ennen algoritmin käyttöä testattava täydellisyys. Samoin on muodostettava algoritmi verkon juuren etsimiseksi tai tutkimiseksi, onko tietty solmu verkon juuri. Tyhjennysmenetelmä ei ole tehokas, mut-

ta se on havainnollinen ja käyttää hyväkseen edellä todistettuja tuloksia. Menetelmällä ei välttämättä löydetä sellaista avointa Hamiltonin polkua, joka voidaan täydentää suljetuksi, vaikka sellaisia olisikin (harjoitustehtäviä).

Esimerkki 13.6.11 Olkoon G suunnattu verkko solmuina 1, 2, 3, 4, 5. Olkoot verkon nuolet $(1,3)$, $(2,1)$, $(2,3)$, $(2,4)$, $(2,5)$, $(3,5)$, $(4,1)$, $(4,3)$, $(5,1)$, $(5,4)$. Etsi verkon G Hamiltonin polut.

Ratkaisu. Heti nähdään, että verkko on täydellinen, joten Hamiltonin polkuja on olemassa. Solmu 2 on ainoa juuri, sillä siihen ei päästä mistään muusta solmusta. Täten mikään Hamiltonin polku ei voi olla suljettu ja avoimet Hamiltonin polut lähtevät solmusta 2. Ne ovat solmujonoin lueteltuina 21354, 23541, 24135, 24351 ja 25413. Jos verkosta poistetaan esimerkiksi nuoli $(2,4)$, ei verkko ole täydellinen, mutta siinä on vielä 3 Hamiltonin polkua.

13.7 Eulerin polut ja de Bruijnin jonot

Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko. Eulerin polun olemassaolo karakterisoidaan vastaavaan tapaan kuin suuntaamattoman verkon tapauksessa.

Määritelmä 13.7.1 Suunnatun verkon polku on *Eulerin polku*, jos jokainen verkon nuoli esiintyy polussa täsmälleen kerran. Suunnattu verkko on *Eulerin verkko*, jos siinä on suljettu Eulerin polku.

Lause 13.7.2 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen suunnattu verkko, jossa ei ole erillisiä solmuja. Tällöin verkossa G on Eulerin polku jos ja vain jos G on yhtenäinen ja jompikumpi seuraavista ehdoista on täytetty:

1) $d_G^+(x) = d_G^-(x)$ kaikilla $x \in \mathbf{X}$,

2) on olemassa sellaiset solmut x_1, $x_2 \in \mathbf{X}$, että

$$\begin{aligned} d_G^+(x_1) &= d_G^-(x_1) + 1, \\ d_G^-(x_2) &= d_G^+(x_2) + 1, \end{aligned}$$

ja $d_G^+(x) = d_G^-(x)$ kaikilla $x \in \mathbf{X} \backslash \{x_1, x_2\}$.

Kohdan 1) tapauksessa jokainen Eulerin polku on suljettu ja kohdan 2) tapauksessa jokainen Eulerin polku on avoin polku $x_1 \to x_2$.

Todistus. Samaan tapaan kuin suuntaamattomalle verkolle. □

Eulerin verkon sovelluksena tarkastellaan aakkoston de Bruijnin jonoja, joiden avulla kaikki tietynpituiset sanat voidaan ilmaista kompaktissa muodossa. Tässä pykälässä käytetään seuraavaa erikoistermistöä:

Määritelmä 13.7.3 Olkoon S äärellinen epätyhjä joukko. Joukko S on *aakkosto* ja sen alkiot *kirjaimia*. Olkoon $n \in \mathbb{N}$. Vektori $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in S^n$ on aakkoston S n-kirjaiminen *sana* ja sanan $\mathbf{w}$ *pituus* on n. Sanalle käytetään lyhennysmerkintää

$$w_1 w_2 \ldots w_n := (w_1, w_2, \ldots, w_n).$$

Jos $k = \#S$, on erilaisia n-kirjaimisia sanoja $N := k^n$ kappaletta. Aakkoston S sana

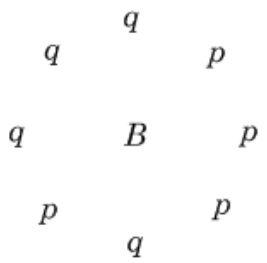
$$B = b_0 b_1 \ldots b_{N-1}$$

on *de Bruijnin jono* sanapituudelle n, jos jokaista n-kirjaimista sanaa $\mathbf{w} \in S^n$ kohti on olemassa yksikäsitteisesti määrätty indeksi i, $i{+}1 \in [N]$, jolle

$$\mathbf{w} = b_i b_{i+1} \ldots b_{i+n-1},$$

kun indeksit otetaan modulo N, ts. indeksin $N{-}1$ jälkeen jatketaan nollasta eteenpäin. Tilannetta voi havainnollistaa kirjoittamalla jono B ympyrän kehälle tasavälein kellotaulun tapaan ja lukemalla siitä n-kirjaimisia sanoja myötäpäivään, lähtien kustakin kirjaimesta vuorollaan.

Esimerkki 13.7.4 Aakkostossa $S = \{p, q\}$ on kolmikirjaimisia sanoja $2^3 = 8$ kappaletta. Eräs kolmikirjaimisten sanojen de Bruijnin jono on $B := pppqpqqq$, ks. Kuva 32, sillä siitä löytyvät kaikki sanat ppp, ppq, pqp, qpq, pqq, qqq, qqp ja qpp.



Kuva 32: Esimerkin 13.7.4 de Bruijnin jono

Lause 13.7.5 Jokaisessa aakkostossa on de Bruijnin jono jokaiselle sanapituudelle.

Todistus. Olkoon S aakkosto, $k := \#S$, $n \in \mathbb{N}$ mielivaltainen sanapituus ja $N := k^n$. Jos $n = 1$, on väite triviaalisti tosi. Olkoon $n \geq 2$. Asetetaan solmujoukoksi $\mathbf{X} := S^{n-1}$, nuoliksi $U := S^n$ ja vastaavuuskuvaukseksi siirto $\Psi : U \to S^{n-1} \times S^{n-1}$,

$$\Psi(x_1 \dots x_n) := (x_1 \dots x_{n-1}, x_2 \dots x_n).$$

Silloin $G := (\mathbf{X}, U, \Psi)$ on äärellinen suunnattu verkko, jossa ei ole erillisiä solmuja. Kukin yksittäinen sana $\mathbf{x} = x_1 \dots x_{n-1}$ voi saada "kaverikseen" k erilaista sanaa $x_2 \dots x_n$, sillä kirjain x_n voidaan valita aakkostosta miten vain, muut on kiinnitetty. Tämän ja symmetrian perusteella

$$d_G^+(\mathbf{x}) = d_G^-(\mathbf{x}) = k$$

kaikilla $\mathbf{x} \in \mathbf{X}$. Todetaan vielä, että G on yhtenäinen osoittamalla se jopa vahvasti yhtenäiseksi. Olkoot $\mathbf{x} = x_1 \dots x_{n-1}$, $\mathbf{y} = y_1 \dots y_{n-1} \in \mathbf{X}$ mielivaltaisia. Silloin

$$p := (\underbrace{x_1 \dots x_{n-1}}_{\mathbf{x}} y_1, x_2 \dots x_{n-1} y_1 y_2, \dots, x_{n-1} \underbrace{y_1 \dots y_{n-1}}_{\mathbf{y}})$$

on polku $\mathbf{x} \to \mathbf{y}$. Vastaavasti löytyy polku $\mathbf{y} \to \mathbf{x}$. Siis G on vahvasti yhtenäinen ja siten yhtenäinen. Lauseen 13.7.2 nojalla on verkossa G suljettu Eulerin polku. Tässä tapauksessa polku koostuu kaikista n-kirjaimisista sanoista ja kukin niistä esiintyy kerran. Polun sanasta saadaan seuraava sana jättämällä ensimmäinen kirjain pois ja lisäämällä loppuun yksi kirjain. Jos Eulerin polku on

$$\begin{aligned}&(b_0 \dots b_{n-1}, b_1 \dots b_n, \dots, b_{N-n} \dots b_{N-1},\\ &b_{N-n+1} \dots b_{N-1} b_0, \dots, b_{N-1} b_0 \dots b_{n-2}),\end{aligned}$$

on sana $b_0 b_1 \dots b_{N-1}$ eräs de Bruijnin jono sanapituudelle $n \geq 2$ aakkostossa S. □

13.8 Suunnatut puut

Olkoon $G = (\mathbf{X}, U, \Psi)$ tässä pykälässä äärellinen suunnattu verkko. Tarkastellaan suunnattujen puiden rakennetta.

Määritelmä 13.8.1 Äärellinen suunnattu verkko $G = (\mathbf{X}, U, \Psi)$ on *suunnattu metsä*, jos verkkoa G vastaava suuntaamaton verkko on metsä, ts. syklitön. Verkko G on *suunnattu puu*, jos vastaava suuntaamaton verkko on puu, ts. yhtenäinen ja syklitön. Suunnattu puu on *juurellinen*, jos siinä on juuri.

Lause 13.8.2 Jos $G = (\mathbf{X}, U, \Psi)$ on äärellinen suunnattu puu, niin

a) jokainen sen polku on yksinkertainen ja lähtö ja maali ovat eri solmuja, ts. polku on yksinkertainen ja avoin.

b) jokaista sen solmuparia yhdistää korkeintaan yksi polku.

c) siinä on korkeintaan yksi juuri.

Todistus. a) Olkoot $x, y \in \mathbf{X}$ solmuja ja

$$p = (u_1, u_2, \ldots, u_n) \sim (x = x_0, x_1, \ldots, x_n = y)$$

polku. Jos olisi $x_i = x_j$ joillekin $0 \leq i < j \leq n$, polkua p vastaava ketju sisältäisi syklin $\{u_{i+1}, \ldots, u_j\}$. Tämä on ristiriita oletuksen kanssa. Siis polku on yksinkertainen. Erikoisesti $x \neq y$.

b) Olkoot p, q kaksi eri polkua $x \to y$, missä $x \neq y$. Unohtaen nuolten suunnat saisimme vastaavat ketjut $c_p\ x \to y$ ja $c_q\ y \to x$. Kuten Lauseen 12.5.5 transitiivisuusosan todistuksessa, voitaisiin löytää ketju $x \to x$, joka siis olisi suljettu. Vastaava kaarijoukko olisi sykli vastaavassa suuntaamattomassa puussa, mikä on vastoin oletuksia.

c) Jos $x \neq y$ ovat juuria, niin on olemassa polut $p_1 : x \to y$ ja $p_2 : y \to x$. Mutta silloin $p_1 p_2$ on polku $x \to x$. Tämä on ristiriita kohdan a) kanssa. □

Määritelmä 13.8.3 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen juurellinen suunnattu puu.

a) Jos on olemassa polku $x \to y$, sanotaan solmua x solmun y *edeltäjäksi* ja solmua y solmun x *seuraajaksi*.

b) Solmuparissa $\Psi(u) = (x, y)$ solmu x on solmun y *välitön* edeltäjä ja solmu y solmun x *välitön* seuraaja.

c) Solmu, jolla ei ole seuraajia, on *lehti* tai *päätesolmu*. Muut solmut ovat *haaroja* tai *haarasolmuja*.

Huomautus 13.8.4 Lauseesta 13.8.2 seuraa, että äärellisessä juurellisessa puussa

1) juurella ei ole edeltäjiä, muilla solmuilla on täsmälleen yksi välitön edeltäjä,

2) jokainen solmu on joko haara tai lehti, ei molempia. Haarasolmulla voi olla useita välittömiä seuraajia,

3) jokaisesta solmusta on sen jokaiseen seuraajaan täsmälleen yksi polku. Jokainen solmusta lähtevä polku päättyy seuraajaan eikä mikään polku kulje edeltäjän kautta.

Lause 13.8.5 Olkoon $G = (\mathbf{X}, U, \Psi)$ äärellinen juurellinen suunnattu puu ja $x \in \mathbf{X}$ mielivaltainen. Jos $\mathbf{X}_x$ on joukko, jonka muodostavat x ja sen kaikki seuraajat, solmujoukon $\mathbf{X}_x$ virittämä verkon G aliverkko G_x on juurellinen suunnattu puu, jonka juuri on solmu x.

Todistus. Olkoon $y \in \mathbf{X}_x \setminus \{x\}$ mielivaltainen. Koska y on solmun x seuraaja puussa G, on siinä täsmälleen yksi polku $p : x \to y$. Polun p nuolet ovat joukon $\mathbf{X}_x$ solmujen välisiä, joten p on polku $x \to y$ myös aliverkossa G_x. Täten x on verkon G_x juuri.

Olkoot H ja H_x verkkoja G ja G_x vastaavat suuntaamattomat verkot. Edellä tuli jo osoitetuksi, että H_x on yhtenäinen. Verkossa H ei ole syklejä, joten niitä ei voi olla myöskään sen aliverkossa H_x. Täten H_x on suuntaamaton puu. Määritelmän 13.8.1 mukaan suunnattu verkko G_x on juurellinen puu. □

Lause 13.8.6 Jokainen äärellinen suuntaamaton puu voidaan suunnata juurelliseksi suunnatuksi puuksi.

Todistus. Olkoon $G = (\mathbf{X}, E, \Psi)$ äärellinen suuntaamaton puu. Valitaan yksi solmu $x \in \mathbf{X}$ ja muutetaan siitä lähtevät kaaret nuoliksi. Siirrytään näiden nuolten maaleihin ja toistetaan suuntaaminen. Näin saadaan kaikki kaaret suunnatuiksi niin, että mielivaltaiseen solmuun y päättyvä ketju $x \to y$ muuttuu poluksi. □

Olkoon G äärellinen yhtenäinen suunnattu verkko. Koska sitä vastaava suuntaamaton verkko H on yhtenäinen, se on Seurauksen 12.9.3 mukaan erään puun P virittämä. Antamalla puun P kaarille niiden alkuperäiset suunnat saadaan suunnatun verkon G virittävä suunnattu puu. Tämä ei kuitenkaan ole yleensä juurellinen puu. (harjoitustehtävä). Voidaan kuitenkin osoittaa, että löytyy virittävä suunnattu metsä, jonka puut ovat juurellisia. Jos verkko G on vahvasti yhtenäinen, on virittävä suunnattu juurellinen puu olemassa.

13.9 Binääripuut

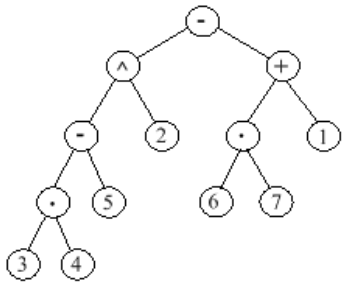
Suunnattujen juurellisten puiden erikoistapauksia, nk. *binääripuita*, käytetään erityisesti tietotekniikassa, mutta myös monissa muissa yhteyksissä.

Määritelmä 13.9.1 Suunnattu juurellinen puu on *binääripuu* (*binary tree*), jos jokaisella solmulla on (enintään) kaksi lasta. Näitä kutsutaan *vasemmaksi* ja *oikeaksi*.

Esimerkki 13.9.2 Aritmeettisen lausekkeen laskujärjestys voidaan esittää binääripuuna. Esimerkiksi lauseke

$$(3{\cdot}4-5)^2-(6{\cdot}7+1)$$

binääripuuna Kuvassa 33.



Kuva 33: Esimerkin 13.9.2 laskutoimitus binääripuuna

Tehtävä 13.9.3 Esitä ainakin kahdella eri tavalla binääripuuna lauseke

$$(a-b)(a+b),$$

missä a ja b ovat reaalilukuja.

Tehtävä 13.9.4 Esittele jokin omaan alaasi kuuluva ongelma, jossa käytetään apuna binääripuita.

14 VERKKOTEORIAN ONGELMIA

Luvuissa 12 ja 13 on tarkasteltu Eulerin ja Hamiltonin ketjujen ja polkujen sekä virittävien puiden olemassaoloa painottamattomassa verkossa. Esitettiin myös joitakin teorian pohjalta kehiteltyjä menetelmiä näiden etsimiseksi. Tässä täydentävässä luvussa tarkastellaan mm. verkkojen isomorfisuutta, planaarisuutta eli tasoverkko-ominaisuutta ja tunnetuimpia verkko-ongelmia painotetuissa verkoissa.

14.1 Verkkojen isomorfisuudesta

Verkkojen isomorfisuusongelmia esiintyy käytännön tasolla mm. kemiassa, tiedonhakujärjestelmissä ja lingvistiikassa. Jos esimerkiksi on saatu selvitetyksi kahden monimutkaisen yhdisteen rakennetta kuvaavat verkot, jotka saattavat olla hyvinkin eri näköisiä, miten saadaan selville, ovatko yhdisteet samat? Vastaus on: täsmälleen silloin, kun vastaavat verkot ovat isomorfiset. Isomorfisuuden määrittely on oleellisesti sama suuntaamattomalle ja suunnatulle verkolle.

Määritelmä 14.1.1 a) Suuntaamattomat Verkot $G = (\mathbf{X}, E, \Psi)$ ja $G' = (\mathbf{X}', E', \Psi')$ ovat *isomorfiset* (merkitään $G \cong G'$), jos on olemassa sellaiset bijektiot $f : \mathbf{X} \to \mathbf{X}'$ ja $g : E \to E'$, että kaikilla $e \in E$ ja $x, y \in \mathbf{X}$

$$[\,\Psi(e) = \{x, y\}\,] \;\Leftrightarrow\; [\,\Psi'(g(e)) = \{f(x), f(y)\}\,].$$

b) Suunnatut verkot $G = (\mathbf{X}, U, \Psi)$ ja $G' = (\mathbf{X}', U', \Psi')$ ovat *isomorfiset* (merkitään $G \cong G'$), jos on olemassa sellaiset bijektiot $f : \mathbf{X} \to \mathbf{X}'$ ja $g : U \to U'$, että

$$[\,\Psi(u) = (x, y)\,] \;\Leftrightarrow\; [\,\Psi'\big(g(u)\big) = \big(f(x), f(y)\big)\,].$$

Lause 14.1.2 Verkkojen välinen isomorfia on ekvivalenssirelaatio (harjoitustehtävä). Yleisesti kahden verkon isomorfisuuden toteaminen on hyvin hankala ja työläs tehtävä.

Olkoot $G = (\mathbf{X}, A, \Psi)$ ja $H = (\mathbf{Y}, B, \Gamma)$ kaksi äärellistä verkkoa, molemmat joko suuntaamattomia tai suunnattuja. Seuraavat ehdot ovat isomorfisuudelle *välttämättömiä*: Jos $G \cong H$, verkoissa on

a) sama määrä solmuja, $\#\mathbf{X} = \#\mathbf{Y}$,
b) sama määrä kaaria tai nuolia, $\#A = \#B$,
c) sama määrä kunkin asteluvun omaavia solmuja,
d) samat määrät tietynpituisia (suljettuja) ketjuja tai polkuja,

e) sama määrä yhtenäisiä ja vahvasti yhtenäisiä komponentteja, ja jokaista verkon G komponenttia vastaa sen kanssa verkkona isomorfinen verkon H komponentti, joille pätevät kohdat a) – d).

Nämä ominaisuudet eivät suinkaan riitä isomorfisuuden osoittamiseen, mutta niitä voidaan käyttää osoitettaessa, että kaksi verkkoa *eivät ole* isomorfisia.

Pienehköjen yksinkertaisten verkkojen isomorfisuus saattaa ratketa komplementteja tutkimalla.

Lause 14.1.3 Jos G ja H ovat kaksi yksinkertaista verkkoa, ne ovat isomorfiset jos ja vain jos niiden komplementit ovat isomorfiset.

Todistus. Harjoitustehtävä. □

Yleisesti kahden äärellisen verkon isomorfisuuden toteaminen on periaatteessa aina ratkaistavissa suoralla laskulla. Jos verkot ovat suuria, menetelmä on kuitenkin erittäin hidas, sillä laskenta-aika on verrannollinen solmujen määrän kertomaan. Yleistä algoritmia, jonka laskenta-aika olisi verrannollinen solmujen määrään polynomiaalisesti, ei ole onnistuttu kehittämään.

Lause 14.1.4 Jos G ja H ovat kaksi äärellistä verkkoa, ne ovat isomorfiset jos ja vain jos verkon H solmut voidaan järjestää niin, että verkkojen yhteysmatriisit ovat samat.

Todistus. Yhteysmatriisi määrää verkon yksikäsitteisesti, ja kääntäen. □

Jos verkoissa on n solmua, on muodostettava joukon $[n]$ kaikki eri järjestykset (*permutaatiot*, Määritelmä 16.2.1), joita on $n!$ kappaletta, ja verrattava matriisia M_G kuhunkin matriisista M_H järjestämällä saatavaan matriisiin. Erikoista tyyppiä oleville verkoille, kuten puille ja tasoverkoille, on kehitetty nopeitakin menetelmiä.

Esimerkki 14.1.5 Ovatko Kuvan 34 verkot isomorfisia?

Kuva 34: Esimerkin 14.1.5 verkot

Ratkaisu. Vasemmassa verkossa on kaksi, oikeassa kolme erilaista 4-pituista suljettua ketjua, joten kohdan d) nojalla verkot eivät ole isomorfiset.

Esimerkki 14.1.6 Olkoot G ja H verkkoja matriiseina

$$M_G = \begin{pmatrix} 1 & 1 & 3 & 0 & 1 \\ 1 & 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad M_H = \begin{pmatrix} 2 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Osoita, että verkot ovat isomorfiset.

Ratkaisu. Verkot ovat suunnattuja, sillä matriisit eivät ole symmetrisiä. Olkoot

$$\begin{array}{rclcrcl} \mathbf{X} & := & \{x_1, x_2, x_3, x_4, x_5\}, & & G & := & (\mathbf{X}, U, \Psi), \\ \mathbf{Y} & := & \{y_1, y_2, y_3, y_4, y_5\}, & & H & := & (\mathbf{Y}, V, \Gamma). \end{array}$$

Olkoot $M_G = (a_{ij})_{5\times 5}$ ja $M_H = (b_{ij})_{5\times 5}$. Yritetään muodostaa bijektio $f : \mathbf{X} \to \mathbf{Y}$ käyttäen isomorfisuudelle välttämättömiä ehtoja. Koska $a_{13} = b_{24} = 3$, on valittava $f(x_1) := y_2$ ja $f(x_3) := y_4$. Koska solmut x_4 ja y_5 ovat ainoita, joiden lähtöaste on 1, täytyy olla $f(x_4) := y_5$. Koska $(x_4, x_5) \in U$, on oltava

$$(f(x_4), f(x_5)) = (y_5, f(x_5)) \in V,$$

joten pitää valita $f(x_5) := y_3$. Lopuksi olkoon $f(x_2) := y_1$. Järjestämällä funktion f mukaan saadaan

$$M_H = \begin{array}{c} H \\ y_2 \\ y_1 \\ y_4 \\ y_5 \\ y_3 \end{array} \begin{array}{c} \begin{array}{ccccc} y_2 & y_1 & y_4 & y_5 & y_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 3 & 0 & 1 \\ 1 & 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array},$$

mistä nähdään, että verkot ovat isomorfiset.

14.2 Taso- vai avaruusverkko?

Joskus on tärkeätä tietää, voidaanko annettu verkko esittää tasokaaviona niin, etteivät kaaret tai nuolet leikkaa toisiaan. Tällainen tilanne on tuttu mm. elektroniikassa suunniteltaessa integroituja tai painettuja virtapiirejä. Tehtävä on yksinkertainen asettaa ja periaatteessa myös suorittaa, mutta – kuten monet muutkin verkko-ongelmat – käytännössä hidas toteuttaa. Vaikka verkko onnistuttaisiinkin todistamaan tasoverkoksi, jää yleensä vielä selvitettäväksi, miten se on tasoon piirrettävä. Seuraavassa käsiteltävä tasoverkko-ominaisuuden tarkastelu on esitetty suuntaamattoman verkon terminologialla, mutta se soveltuu ymmärrettävästi yhtä hyvin suunnatulle verkolle.

Geometrisista käyristä

Tarkastellaan aluksi euklidisen avaruuden $\mathbb{R}^n$ käyriä. Esimerkiksi integraalilaskennan yhteydessä käyrällä tarkoitetaan jatkuvaa kuvausta $\gamma : [a, b] \to \mathbb{R}^n$. Monissa muissa tilanteissa – kuten suuntaamattoman geometrisen verkon yhteydessä – riittää tarkastella tällaisten käyrien *kuvajoukkoja* eli *jälkiä* $C_\gamma := \gamma([a, b])$.

Määritelmä 14.2.1 a) Avaruuden $\mathbb{R}^n$ osajoukko C on *käyrä*, jos on olemassa suljettu väli $[a, b]$, $a < b$, ja jatkuva kuvaus $\gamma : [a, b] \to \mathbb{R}^n$, joille $C = \gamma([a, b])$. Kuvaus γ on käyrän (eräs) *parametriesitys*.

b) Käyrä on *Jordanin kaari*, jos sillä on parametriesitys, joka on injektio. Käyrä on *yksinkertainen*, jos sillä on parametriesitys γ, jolle $\gamma|[a, b[$ on injektio. Käyrä C on *suljettu* tai *umpinainen*, jos $\gamma(a) = \gamma(b)$. Käyrä on *Jordanin käyrä*, jos se on yksinkertainen ja suljettu.

c) Jos $\{\mathbf{x}, \mathbf{y}\} = \{\gamma(a), \gamma(b)\}$, sanotaan, että käyrä *yhdistää* pisteet $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ ja että pisteet $\mathbf{x}$ ja $\mathbf{y}$ ovat käyrän *päät*.

d) Käyrä C *leikkaa itseään* pisteessä $\mathbf{x} \in \mathbb{R}^n$, jos jokaista sen parametriesitystä γ vastaa lukupari $s, t \in [a, b]$, $s < t$, jolle $\gamma(s) = \gamma(t) = \mathbf{x}$. Kaksi käyrää C ja D *leikkaavat toisensa* pisteessä $\mathbf{x} \in \mathbb{R}^n$, jos $\mathbf{x} \in C \cap D$.

e) Olkoot C ja D kaksi käyrää, joilla on ainakin yksi yhteinen pää. Käyrien *yhdiste* on joukko $CD := C \cup D$.

Lause 14.2.2 (Jordanin käyrälause) Jordanin käyrä C tasossa $\mathbb{R}^2$ jakaa tason kahteen pistevieraaseen alueeseen, joiden molempien reuna on C.

Todistus. Syvällinen topologinen tulos. □

Huomautus 14.2.3 1) Käyrällä on aina useita parametriesityksiä. Jordanin kaari ei leikkaa itseään ja Jordanin käyrä leikkaa itseään ainoastaan päissään.

2) Jos käyrä C yhdistää pisteet $\mathbf{x}$, $\mathbf{y}$ ja käyrä D yhdistää pisteet $\mathbf{y}$, $\mathbf{z}$, niiden yhdiste CD on käyrä, joka yhdistää pisteet $\mathbf{x}$ ja $\mathbf{z}$.

3) Jos Jordanin käyrä C jakaa tason alueisiin A_1, A_2 ja $\mathbf{x}_1 \in A_1$, $\mathbf{x}_2 \in A_2$, niin jokainen näitä pisteitä yhdistävä käyrä leikkaa käyrää C.

Geometrinen verkko ja abstrakti verkko

Määritellään aluksi verkon erikoistapaus, geometrinen verkko. Sitten käsitellään abstraktin verkon esittämistä geometrisena verkkona euklidisessa avaruudessa.

Määritelmä 14.2.4 Kolmikko $\mathcal{G} = (\mathcal{X}, \mathcal{E}, \Psi)$ on *geometrinen verkko* avaruudessa $\mathbb{R}^n$, jos

a) $\mathcal{X} \subseteq \mathbb{R}^n$ on epätyhjä pistejoukko,

b) $\mathcal{E}$ on joukko näitä pisteitä yhdistäviä yksinkertaisia käyriä, jotka eivät leikkaa toisiaan ja sisältävät pisteitä $\mathbf{x} \in \mathcal{X}$ korkeintaan päinään,

c) $\Psi : \mathcal{E} \to \mathcal{X} \,\&\, \mathcal{X}$ on kuvaus, joka liittää käyrään sen päät.

Huomautus 14.2.5 Olkoon $\mathcal{G} = (\mathcal{X}, \mathcal{E}, \Psi)$ avaruuden $\mathbb{R}^n$ geometrinen verkko.

a) On ilmeistä, että geometrinen verkko on suuntaamaton verkko, kun $\mathcal{X}$ tulkitaan solmujen joukoksi, $\mathcal{E}$ kaarten joukoksi, jossa silmukat ovat Jordanin käyriä, muut kaaret Jordanin kaaria ja Ψ on vastaavuuskuvaus.

b) Kaarijono on sen sisältämien kaarien yhdiste. Jos $c = C_1C_2 \dots C_n$, missä kukin C_i on geometrisen verkon kaari, on ketju, se voi käyränä leikata itseään vain solmuissa. Yksinkertainen suljettu ketju on Jordanin käyrä.

c) Tason ($n = 2$) geometrisessa verkossa yksinkertainen suljettu ketju jakaa tason Jordanin käyrälauseen mukaan kahteen erilliseen alueeseen, joista toinen on rajoitettu ja toinen ei. Näin äärellinen verkko jakaa tason äärellisen moneen alueeseen.

Lause 14.2.6 Jokainen äärellinen suuntaamaton verkko on isomorfinen avaruuden $\mathbb{R}^3$ jonkin geometrisen verkon kanssa. Yleisemmin, väite pätee jopa verkolle, jossa on numeroituva määrä solmuja ja kaaria.

Todistus. Asetetaan solmut kolmiulotteisen xyz-koordinaatiston positiiviselle x-akselille pisteisiin $1, 2, 3, \dots$. Koska kaaria on numeroituva määrä, voidaan kutakin kaarta e_i varten ottaa eri taso T_i, joka sisältää x-akselin. Kaari e_i voidaan nyt piirtää omaan tasoonsa T_i. □

Verkon planaarisuus

Tarkastellaan tasoverkon ominaisuuksia, mm. Eulerin kaavoja sekä esitetaan tunnettu Kuratowskin lause, joka karakterisoi tasoverkko-ominaisuuden.

Määritelmä 14.2.7 Suuntaamaton verkko G on *tasoverkko* eli *planaarinen*, jos se on isomorfinen tason jonkin geometrisen verkon kanssa, muutoin *avaruusverkko*.

Seuraavaa lausetta käytetään usein osoitettaessa verkkoa avaruusverkoksi.

Lause 14.2.8 (Eulerin kaava verkoille) Olkoon $\mathcal{G} = (\mathcal{X}, \mathcal{E}, \Psi)$ tason äärellinen geometrinen verkko, jossa on n solmua ja m kaarta. Oletetaan, että $\mathcal{G}$ jakaa tason tason r alueeseen.

a) Jos verkko $\mathcal{G}$ on yhtenäinen, on

$$n - m + r = 2. \tag{18}$$

b) Jos verkossa on p yhtenäistä komponenttia, on

$$n - m + r = p + 1.$$

Todistus. a) Väite voidaan todistaa induktiolla (harjoitustehtävä) tai käyttää Huomautuksen 14.2.9 menetelmää, jonka avulla mikä tahansa tason äärellinen yhtenäinen geometrinen verkko voidaan tyhjentää yhdeksi solmuksi, jolle kaava selvästikin pitää paikkansa.

b) Kullekin yhtenäiselle komponentille $\mathcal{G}_i$ erikseen pätee (18):

$$n_i - m_i + r_i = 2, \quad i \in [p]. \tag{19}$$

Kun lasketaan koko verkon jakamia alueita, otetaan rajoittamaton alue vain kerran, joten alueita on yhteensä $r = \sum_{i=1}^{p} r_i - (p-1)$. Kun lasketaan yhtälöt (19) puolittain yhteen saadaan $n - m + r + p - 1 = 2p$ eli $n - m + r = p + 1$. □

Huomautus 14.2.9 Tason yhtenäiselle geometriselle verkolle pysyy luku $n-m+r$ muuttumattomana, jos verkkoa muunnetaan niin, että se pysyy yhtenäisenä geometrisena verkkona ja

a) poistetaan (tai lisätään) yksi kaari.

b) poistetaan (tai lisätään) yksi kaari ja siihen liittyvä yksiasteinen solmu.

Seuraus 14.2.10 Jos $\mathcal{G} = (\mathcal{X}, \mathcal{E}, \Psi)$ on äärellinen yhtenäinen yksinkertainen geometrinen tasoverkko, jossa on $n \geq 3$ solmua ja m kaarta, niin

$$m \leq 3n - 6.$$

Todistus. Jokaista aluetta rajoittaa ainakin 3 kaarta ja jokainen kaari rajoittaa korkeintaan kahta aluetta, joten $3r \leq 2m$. Eulerin kaavan 18 mukaan

$$m = n + r - 2 \leq n + \frac{2}{3}m - 2,$$

josta $m/3 \leq n - 2$. □

Huomautus 14.2.11 a) Jos verkko on tasoverkko, sitä voidaan muuntaa planaarisuuden kärsimättä seuraavasti:

1. Poistetaan silmukat ja rinnakkaiset kaaret.

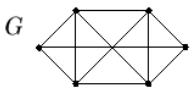
2. Poistetaan 2-asteinen solmu ja yhdistetään siihen liittyneet kaaret.

3. Kaari ”kutistetaan” pisteeksi, jolloin kaaren päät yhtyvät yhdeksi solmuksi.

Verkon yksinkertaisuus saatetaan tapauksissa 2 tai 3 menettää.

b) Avaruusverkko puolestaan pysyy avaruusverkkona, jos sitä muunnetaan kohtien 1 ja 2 menetelmillä; sen sijaan ”kutistaminen” voi muuttaa verkon tasoverkoksi.

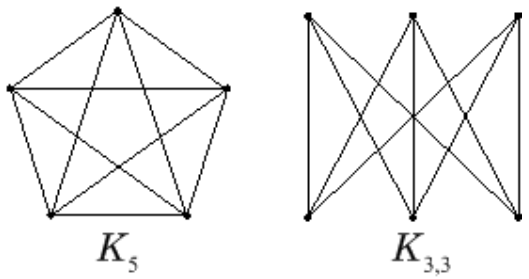
Esimerkki 14.2.12 Onko Kuvan 35 verkko G tasoverkko?



Kuva 35: Esimerkin 14.2.12 verkko

Ratkaisu. Verkko on yksinkertainen ja siinä on 6 solmua ja 11 kaarta, joten pätee $11 < 3 \cdot 6 - 6 = 12$, mikä ei ole planaarisuuden kanssa ristiriidassa. Kutistetaan pisin vaakasuora kaari. Muunnettu verkko G' on yksinkertainen ja siinä on 5 solmua ja 10 kaarta, joten $10 > 3 \cdot 5 - 6 = 9$. Seurauksen 14.2.10 nojalla verkko G' ei ole tasoverkko, joten myöskään G ei ole.

Esimerkki 14.2.13 Äärellisiä avaruusverkkoja on olemassa ainakin kaksi, nk. *Kuratowskin verkot* K_5 ja $K_{3,3}$, ks. Kuva 36.



Kuva 36: Kuratowskin avaruusverkot K_5 ja $K_{3,3}$

K_5 on yksinkertainen täydellinen 5-solmuinen verkko ja $K_{3,3}$ nk. *täydellinen kaksijakoinen* (*complete bipartite*) 3+3-solmuinen verkko. Verkon $K_{3,3}$ solmut voidaan jakaa kahteen ryhmään $L = \{1, 2, 3\}$ ja $A = \{a, b, c\}$ niin, että

a) jokaisesta $x \in L$ on yksi kaari jokaiseen $y \in A$,

b) kummankaan ryhmän solmujen välillä ei ole kaaria.

Verkot todistetaan avaruusverkoiksi Jordanin käyrälauseen tai Seurauksen 14.2.10 avulla (harjoitustehtävä).

Seuraava lause karakterisoi äärellisten verkkojen planaarisuuden.

Lause 14.2.14 (Kuratowskin lause) Äärellinen verkko on tasoverkko jos ja vain jos se ei sisällä yhtään sellaista aliverkkoa, joka voidaan muuntaa Huomautuksen 14.2.11 keinoin 1 ja 2 (ei 3) verkoksi, joka on isomorfinen Kuratowskin verkon K_5 tai $K_{3,3}$ kanssa (ks. Esimerkki 14.2.13).

14.3 Kartan väritys

Tasokartan värittämisongelma (*graph coloring*) askarrutti tutkijoita ja maallikkojakin viime vuosisadan puolivälistä lähtien. Oletetaan, että $\mathcal{G}$ on eräs valtioiden rajoja kuvaava tasokartta. Valtiot oletetaan yhtenäisiksi alueiksi ja rajanaapuruus tarkoittaa, että valtioilla on yhteistä rajaa enemmän kuin yksittäisten pisteiden verran. Kuinka monta eri väriä tarvitaan kartan värittämisessä, kun rajanaapureilla on oltava eri värit?

Ongelmana on löytää kartan $\mathcal{G}$ *kromaattinen luku* $\gamma_{\mathcal{G}} \in \mathbb{N}$, so. pienin määrä värejä, jolla kartta voidaan värittää. Probleema voidaan muotoilla verkkoteorian kielelle seuraavasti: Olkoon $G = (\mathbf{X}, E, \Psi)$ suuntaamaton verkko, jossa

1) valtiot = solmut $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$,

2) ”olla rajanaapureita” merkitsee kaarta $\{x_1, x_2\} \in E$,

3) vastaavuuskuvaus Ψ on joukon E identtinen kuvaus.

Ongelma. *Mikä on pienin joukko* $[\gamma_G] \subseteq \mathbb{N}$, *jonka alkioilla verkon* G *solmut voidaan numeroida niin, että minkään kaaren päillä ei ole sama numero?*

Aikojen myötä on esitetty lukuisa joukko osatuloksia tietyn tyyppisille verkoille sekä yleisiä tuloksia $\gamma \leq 6$, $\gamma \leq 5$, joiden todistaminen ei ole edes kovin työlästä. On myös ollut kauan selvää, että on tasoverkkoja, joille $\gamma = 4$.

Esimerkki 14.3.1 Montako väriä tarvitaan Kuvan 37 kartan värittämiseen?

Kuva 37: Esimerkin 14.3.1 verkko

Ratkaisu. Selvästi 3 väriä ei riitä, sillä jo sisemmän täydellisen nelisolmuisen aliverkon värittämiseen tarvitaan vähintäin 4. Toisaalta, jos käytettävissä on 4 väriä, väritys onnistuu helposti. Siis verkon kromaattinen luku $\gamma = 4$.

Vuonna 1976 K. Appel ja W. Haken ([11]) esittivät kuuluisalle *neliväriväittämälle* todistuksen, joka perustuu oleellisesti tietokoneen käyttöön. Työhön kului aikaa 4 vuotta ja yli 1200 tietokonetuntia.

Lause 14.3.2 (Appel ja Haken) Tasoverkon kromaattinen luku $\gamma \leq 4$.

Lause 14.3.3 (Brooks, 1941) Olkoon G äärellinen suuntaamaton verkko, jonka solmujen asteilla on yläraja $d \in \mathbb{N}$. Silloin

a) $\gamma_G \leq d + 1$,

b) $\gamma_G \leq d$, paitsi jos
1. verkolla G on komponenttina K_{d+1} tai
2. $d = 2$ ja verkolla G on komponenttina paritonta pituutta oleva suljettu ketju.

15 PAINOTETUT VERKOT

Verkon avulla muotoillulla ongelmalla saattaa olla useita ratkaisuja, jotka kaikki eivät kuitenkaan ole yhtä toivottuja. Jos esimerkiksi kauppamatkustajan ongelmalla (ks. Luku 12.6) on ratkaisuja, on jokin reiteistä lyhin (lyhimpiä voi olla useita erilaisia). Jos ongelmaa väljennetään luopumalla osasta kaupunkeja, on hylättävät kaupungit valittava jollakin kriteerillä, esimerkiksi pienuuden perusteella. Tällaisissa tapauksissa on järkevää määritellä kaarille ja/tai solmuille painokertoimet ja pyrkiä löytämään ratkaisu, jossa painokerrointen summa tms. on – tilanteesta riippuen – edullisin. Kauppamatkustajan ongelman tapauksessa solmupainot voisivat olla kaupungin kokoon liittyviä ja kaaripainot välimatkoja tai matka-aikoja.

15.1 Painotettu verkko

Määritelmä 15.1.1 Olkoon $G = (\mathbf{X}, A, \Psi)$ verkko. Viisikkoa

$$G_W = (\mathbf{X}, A, \Psi, g_{\mathbf{X}}, g_A),$$

missä $g_{\mathbf{X}} : \mathbf{X} \to \mathbb{R}$ ja $g_A : A \to \mathbb{R}$ ovat kuvauksia, nk. *painofunktioita* (*weight function*), sanotaan *painotetuksi verkoksi* (*weighted graph, network*).

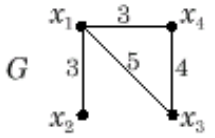
Usein verkossa on vain solmu- tai kaaripainot. Jos esimerkiksi solmupainoja ei ole annettu, asetetaan solmupainoiksi vakiofunktio $g_{\mathbf{X}} = 1$ tai jätetään se kokonaan pois. Tässä esityksessä rajoitutaan äärellisiin suuntaamattomiin verkkoihin, joissa on vain kaaripainoja. Lisäksi verkot ovat yksinkertaisia tai ne yksinkertaistetaan jättämällä pois ”turhat” rinnakkaiset kaaret. Esitettävistä menetelmistä ne, joissa käytetään etäisyysmatriisia, soveltuvat myös suunnatuille verkoille.

Määritelmä 15.1.2 Olkoon $G = (\mathbf{X}, E, \Psi, g_E)$ yksinkertainen painotettu verkko yhteysmatriisina $M_G = (a_{ij})_{n\times n}$. Matriisi $M_{G,W} = (w_{ij})_{n\times n}$, missä

$$w_{ij} := \begin{cases} g_E(\{x_i, x_j\}), & \text{jos } a_{ij} > 0, \\ \infty, & \text{jos } a_{ij} = 0, i \neq j, \\ 0, & \text{jos } i = j, \end{cases}$$

on verkon G *painomatriisi* eli *etäisyysmatriisi*.

Esimerkki 15.1.3 Kuvassa 38 on eräs suuntaamaton painotettu verkko ja sen etäisyysmatriisi:



$$M_{G,W} = \begin{pmatrix} 0 & 3 & 5 & 3 \\ 3 & 0 & \infty & \infty \\ 5 & \infty & 0 & 4 \\ 3 & \infty & 4 & 0 \end{pmatrix}$$

Kuva 38: Esimerkin 15.1.3 verkko ja painomatriisi

15.2 Lyhin ketju

Olkoon $G = (\mathbf{X}, E, \Psi, g_E)$ yksinkertainen painotettu verkko.

Ongelma Etsi verkon kahta solmua x ja y yhdistävistä ketjuista lyhin.

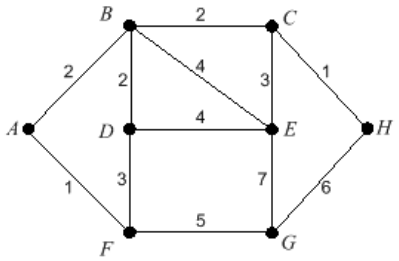
Alkeellisin ja samalla tehottomin menetelmä on etsiä kaikki ketjut $x \to y$ ja valita näistä lyhin.

Huomattavasti parempi, mutta myös hieman hankalammin käsiteltävä menetelmä on *E. Dijkstran* vuonna 1959 esittämä algoritmi, jolla haluttaessa saadaan myös lyhimmät ketjut solmusta x kaikkiin muihin solmuihin *virittävän puun* muodossa (ks. Määritelmä 12.9.1):

> *Olkoon H aluksi verkko, jossa on vain lähtösolmu x. Lähdetään kasvattamaan verkkoa H yksi solmu kerrallaan toistamalla seuraavaa prosessia, kunnes solmu y (tai kaikki solmut) ovat verkossa H:*
>
> **Toista** Etsitään sellainen verkkoon H kuulumaton solmu, johon on lyhin matka lähtösolmusta x verkossa H. Lisätään tämä solmu ja kaari verkkoon H.

On selvää, että näin syntyneessä verkossa H jokaista solmuparia $x \neq z$ yhdistää täsmälleen yksi ketju. On myös melko ilmeistä, että kaikki muut ketjut verkossa G ovat ainakin yhtä pitkiä.

Tehtävä 15.2.1 Etsi lyhimmät ketjut Kuvan 39 verkon solmusta A muihin solmuihin.



Kuva 39: Tehtävän 15.2.1 painotettu verkko

Jos halutaan tietää ainoastaan kaikkien solmuparien välisten lyhimpien ketjujen *pituudet*, voidaan käyttää mekaanista *Floydin* algoritmia. Olkoon $D = (d_{ij})_{n\times n}$ verkon G etäisyysmatriisi. Kuvan 40 funktio palauttaa lyhimpien ketjujen pituudet sisältävän matriisin L_G.

function $L =$ lyhimmat(D);
$L = D$;
for $k = 1 : n$
for $i = 1 : n$
for $j = 1 : n$ aseta $L(i,j) = \min\big(L(i,j), L(i,k) + L(k,j)\big)$; **end**
end
end

Kuva 40: Floydin algoritmilla lyhimpien ketjujen pituudet

Esimerkki 15.2.2 Esimerkin 15.1.3 tapauksessa etäisyysmatriisista saadaan Floydin menetelmällä lyhimpien ketjujen pituudet

$$L_G = \begin{pmatrix} 0 & 3 & 5 & 3 \\ 3 & 0 & 8 & 6 \\ 5 & 8 & 0 & 4 \\ 3 & 6 & 4 & 0 \end{pmatrix}$$

Tehtävä 15.2.3 Laske Tehtävän 15.2.1 lyhimpien ketjujen pituudet.

15.3 Minimaalinen virittävä puu

Olkoon $G = (\mathbf{X}, E, \Psi, g_E)$ yksinkertainen yhtenäinen painotettu verkko, jossa on n solmua. Olkoon ongelmana löytää verkolle *minimaalinen* virittävä puu (*minimal (spanning), economy tree*), ts. virittävä puu, jonka kaarten painokerrointen summa on mahdollisimman pieni.

Jos verkossa on vähänlaisesti kaaria, minimaalisen virittävä puu $(\mathbf{X}, T, \Psi)$ löytyy nopeimmin *Kruskalin algoritmilla*, joka on Kuvassa 41.

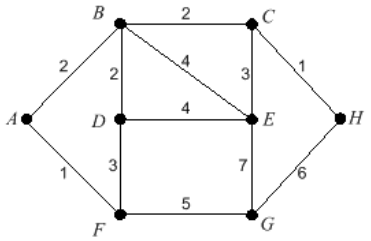
Aseta $i = 0, T = \emptyset$;
while $(i < n - 1)$
valitse sellainen kaari $e \in E \setminus T$, jolle
1) $(\mathbf{X}, T \cup \{e\}, \Psi)$ on syklitön
2) $g_E(e)$ on mahdollisimman pieni
aseta $T = T \cup \{e\}$; $i = i + 1$;
end

Kuva 41: Mimimaalinen virittävä puu Kruskalin algoritmilla

Primin algoritmi tuottaa niinikään minimaalisen virittävän puun:

> *Otetaan puuksi P_1 lyhin kaari ja sen päätesolmut.*
> **Toistetaan** arvoilla $k = 2, 3, \ldots, n - 1$: Muodostetaan verkon G aliverkko P_k lisäämällä puuhun P_{k-1} päätesolmuineen lyhin niistä kaarista, joiden toinen pää on puussa P_{k-1}, mutta toinen ei. Silloin P_k on puu.

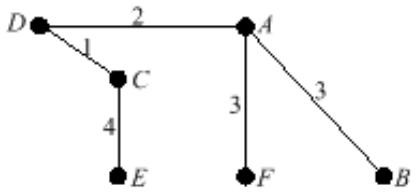
Tehtävä 15.3.1 Etsi Primin algoritmilla halvin virittävä puu Kuvan 42 verkosta.



Kuva 42: Tehtävän 15.3.1 painotettu verkko

Tehtävä 15.3.2 Etsi Kruskalin algoritmilla halvin virittävä puu Tehtävän 15.3.1 verkosta.

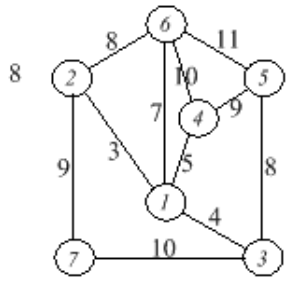
Esimerkki 15.3.3 Esimerkille 15.4.1 saadaan Primin menetelmällä virittävä puu (Kuva 43), jonka kaarten painojen summa on 13 yksikköä.



Kuva 43: Virittävä puu Esimerkkiin 15.3.3

Onko muitakin yhtä halpoja?

Tehtävä 15.3.4 Rakenna Kuvan 44 painotetulle verkolle



Kuva 44: Tehtävän 15.3.4 painotettu verkko

a) halvin virittävä puu Primin algoritmilla.

b) virittävä puu Dijkstran algoritmilla alkaen solmusta 4.

15.4 Kauppamatkustajan ongelma

Olkoon $G = (\mathbf{X}, E, \Psi, g_E)$ yksinkertainen täydellinen painotettu verkko, jossa on n solmua. Periaatteessa minimaalisen suljetun Hamiltonin ketjun voi verkosta löytää tutkimalla kaikkia mahdollisia suljettuja Hamiltonin ketjuja. Koska täydellisessä n-solmuisessa verkossa on $(n-1)!$ kappaletta erilaisia suljettuja Hamiltonin ketjuja, on menetelmä äärimmäisen työläs. Itse asiassa kelvollista nopeata yleistä menetelmää ei ole onnistuttu kehittämään.

Esitetään lopuksi eräs nopea menetelmä, joka antaa kohtuullisen *approksimatiivisen* ratkaisun (ks. algoritmi Kuvassa 45). Voidaan osoittaa, että menetelmän antama ratkaisu on huonoimmassakin tilanteessa pituudeltaan korkeintaan kaksinkertainen verrattuna oikeaan ratkaisuun, mutta usein huomattavasti tarkempi. Oletetaan, että verkon painot toteuttavat kolmioepäyhtälön $w_{ik} \leq w_{ij} + w_{jk}$, minkä useimmat käytännön ongelmat toteuttavat.

Valitse solmu x_1, sitä lähinnä oleva solmu x_2 ja aseta $h_2 = (x_1, x_2, x_1)$;
for $k = 2 : (n-1)$
valitse solmu $z_k \in \mathbf{X}$, joka
1) ei ole ketjussa h_k,
2) on lähinnä ketjua h_k;
olkoon $x_p \in < h_k >$ lähinnä solmua z_k;
lisää z_k jonoon h_k solmun x_p edelle ja indeksoi uudelleen;
aseta $h_{k+1} = (x_1, x_2, \ldots, x_{k+1}, x_1)$;
end

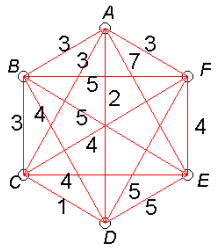
Kuva 45: Quick travelling salesperson-algoritmi

Kauppamatkustajan ongelman yhteydessä on edullista muuntaa etäisyysmatriisia niin, että diagonaali asetetaan äärettömäksi.

Esimerkki 15.4.1 Olkoon G painotettu verkko, jonka etäisyysmatriisi on (ks. myös Kuva 46)

$$M_{G,W} = \begin{pmatrix} \infty & 3 & 3 & 2 & 7 & 3 \\ 3 & \infty & 3 & 4 & 5 & 5 \\ 3 & 3 & \infty & 1 & 4 & 4 \\ 2 & 4 & 1 & \infty & 5 & 5 \\ 7 & 5 & 4 & 5 & \infty & 4 \\ 3 & 5 & 4 & 5 & 4 & \infty \end{pmatrix}.$$

Olkoot solmut vastaavassa järjestyksessä A, B, C, D, E ja F. Lähdetään solmusta A ja valitaan matriisin perusteella $h_2 = (A, D, A)$. Näitä solmuja lähinnä on



Kuva 46: Esimerkin 15.4.1 verkon eräs esitysmuoto

solmu C, jota lähinnä on D. Asetetaan siis $h_3 = (A, C, D, A)$. Jatkossa on hieman valinnan varaa: Edellisiä lähinnä on kaksi solmua, B ja F. Valitaan näistä B, joka on lähimpänä ketjun solmua C ja asetetaan $h_4 = (A, B, C, D, A)$. Solmu F on edelleen lähimpänä ketjua h_4, joten asetetaan $h_5 = (A, B, C, D, F, A)$. Solmu E on lähinnä solmua F, joten asetetaan $h_6 = (A, B, C, D, E, F, A)$. Näin saadun suljetun Hamiltonin ketjun pituus on 19, kun lyhin olisi 18. Aloittamalla jostain muusta solmusta tai tekemällä äskeiset valinnat toisin saataisiin erilaisia arvioita.

16 KOMBINATORIIKKAA

Joukon mahtavuutta ja kardinaliteettia tarkasteltiin Luvussa 10. Samoin todistettiin äärellisten joukkojen summa- ja erotusperiaate eli joukkojen yleinen yhteenlaskukaava (Lause 10.2.3) sekä palautuskaava joukon ositusten lukumäärien laskemiseksi (Lause 10.3.1). Tässä luvussa tarkastellaan kombinatoriikan alkeita.

Kombinatoriikassa tarkastellaan äärellisen joukon $A = \{a_1, a_2, \ldots, a_n\}$ osajoukkojen valintaan liittyviä kysymyksiä. Osajoukot voivat myös olla järjestettyjä osajoukkoja. Osajoukot, olivatpa ne järjestettyjä tai eivät, voidaan valita siten, että kukin alkio voi esiintyä vain kerran tai siten, että tietty alkio voi esiintyä useamman kerran. Kun esimerkiksi n alkiota a_1, a_2, ..., a_n on annettu, voidaan ne ilmeisesti aina esittää järjestysluvuin $1, 2, \ldots, n$. Näin ajattelemme alkioita esitettävän jatkossa.

Konbinatoriikan perustyökaluja ovat mm. summa- ja tuloperiaatteet, variaatiot, kombinaatiot sekä binomi- ja multinomikertoimet. Sovellutuksena tarkastellaan joukon alkioluokkiin jakoja eli ositteluja multinomikerrointen avulla.

16.1 Tulo- ja summaperiaate

Monissa yhteyksissä, esimerkiksi todennäköisyyslaskennassa, tulee toistuvasti vastaan seuraava perusongelma: *Kuinka monta alkiota on joukossa, joka on muodostettu tunnetuista joukoista tiettyjen alkeisoperaatioiden avulla?*

Esimerkki 16.1.1 Laatikko sisältää viisi tuotetta a_1, a_2, a_3, a_4 ja a_5. Valitaan laatikosta umpimähkään kolme tuotetta, jotka asetetaan näytteille vierekkäin. Montako keskenään erilaista järjestettyä joukkoa saadaan?

Ratkaisu. Tässä tapauksessa kukin tuote voi esiintyä vain kerran kussakin osajoukossa. Ensimmäinen tuote voidaan valita viidellä eri tavalla. Tämän jälkeen voidaan seuraava tuote valita neljällä eri tavalla (edellisen valinnan jälkeen jäljelläolevista) ja viimeinen tuote kolmella eri tavalla. Keskenään erilaisia järjestettyjä kolmen tuotteen joukkoja saadaan kaikkiaan $5 \cdot 4 \cdot 3 = 60$ kappaletta.

Esimerkki 16.1.2 Kuinka monella eri tavalla voidaan muodostaa kolminumeroinen luku, kun ensimmäinen numero ei saa olla nolla?

Ratkaisu. Ensimmäinen numero voidaan valita yhdeksällä eri tavalla, toinen ja kolmas numero kumpikin voidaan valita kymmenellä eri tavalla. Keskenään erilaisia kolminumeroisia lukuja saadaan näin ollen $9 \cdot 10 \cdot 10 = 900$ kappaletta.

Lause 16.1.3 (tuloperiaate valinnoissa) Jos

operaatio N_1 voidaan suorittaa n_1:llä eri tavalla
operaatio N_2 voidaan suorittaa n_2:lla eri tavalla
$\vdots$
operaatio N_k voidaan suorittaa n_k:lla eri tavalla

niin, operaatiojono $N_1 N_2 \ldots N_k$ voidaan suorittaa tulon $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ ilmoittamalla eri tavalla.

Matematiikan kielellä tämä tarkoittaa:

Lause 16.1.4 (tuloperiaate joukoille) Jos A_1, A_2, ..., A_k ovat äärellisiä joukkoja, 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.

Esimerkki 16.1.5 Monellako eri tavalla voidaan Esimerkissä 16.1.1 mainitusta laatikosta valita enintään kolme tuotetta käsittävä järjestetty joukko?

Ratkaisu. Valittu joukko voi sisältää yhden, kaksi tai kolme tuotetta. Yhden tuotteen joukko voidaan valita viidellä eri tavalla. Kahden tuotteen joukko voidaan valita $5 \cdot 4 = 20$ eri tavalla, kolmen tuotteen joukko $5 \cdot 4 \cdot 3 = 60$ eri tavalla. Näin ollen voidaan enintään kolmen tuotteen järjestetty joukko valita $5 + 20 + 60 = 85$ eri tavalla.

Lause 16.1.6 (summaperiaate valinnoissa) Oletetaan, että

operaatio M_1 voidaan suorittaa m_1:llä eri tavalla
operaatio M_2 voidaan suorittaa m_2:lla eri tavalla
$\vdots$
operaatio M_k voidaan suorittaa m_k:lla eri tavalla

ja lisäksi, että operaatiot ovat kaikki toisensa poissulkevia. Tällöin voidaan operaatio "M_1 tai M_2 tai ... tai M_k" toteuttaa $m_1 + m_2 + \ldots + m_k$ eri tavalla.

Matematiikan kielellä tämä tarkoittaa:

Lause 16.1.7 (summaperiaate joukoille) 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 10.2.1.

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 $E_1, E_2, \ldots, E_k$. Tämän 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.

Alkeistapausten lukumäärien käsittely helpottuu, kun otetaan käyttöön käsitteet kombinaatio ja variaatio sekä sen erikoistapaus permutaatio.

16.2 Variaatiot ja permutaatiot

Olkoon meillä n alkiota, jotka järjestämme peräkkäin kaikilla mahdollisilla tavoilla. Jokaista tällaista järjestystä kutsutaan n:n alkion permutaatioksi. Yleisemmin, joukosta $A = \{a_1, a_2, \ldots, a_n\}$ otettuja k alkion järjestettyjä jonoja sanotaan k-variaatioiksi.

Määritelmä 16.2.1 Olkoon A epätyhjä joukko, $n := \#A$ ja $k \in [n]$. 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*.

Kahden alkion joukolla on kaksi permutaatiota, esimerkiksi joukolla $\{1, 2\}$ jonot $(1, 2)$ ja $(2, 1)$. Kun $n = 3$, on permutaatioita kuusi kappaletta:

$$(1,2,3),\ (1,3,2),\ (2,1,3),\ (2,3,1),\ (3,1,2),\ (3,2,1)$$

Huomautus 16.2.2 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 $i \in [k]$.

Lause 16.2.3 Äärellisen n-alkioisen joukon k-variaatioiden lukumäärä on

$$V(n,k) := n(n-1)\cdots\big(n-(k-1)\big) = \frac{n!}{(n-k)!} \tag{20}$$

Erikoisesti n-alkioisen joukon kaikkien permutaatioiden lukumäärä on

$$V(n,n) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n = n!$$

Symboli $n!$ on luvun n *kertoma*, jolle asetetaan $0! := 1$.

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 $n(n-1)\cdots\big(n-(k-1)\big)$ kappaletta. Siis kaava (20) on todistettu:

$$V(n,k) = n(n-1)\cdots\big(n-(k-1)\big) = \frac{n!}{(n-k)!}$$

Toinen väite on vain tämän erikoistapaus. □

Esimerkki 16.2.4 Kilpailussa jaetaan 1., 2., 3. ja 4. palkinto. Kilpailijoita on 16. Montako erilaista palkintojenjakomahdollisuutta on olemassa?

Ratkaisu. Mahdollisuuksia on $V(16,4) = 16 \cdot 15 \cdot 14 \cdot 13 = 43680$ kappaletta.

Permutaatioiden luokittelu

Määritelmä 16.2.5 Olkoot n-alkioisen joukon alkioiden järjestysluvut 1, 2, 3, …, n. Permutaatiota $(1,2,3,\ldots,n)$, jossa kaikki järjestysluvut ovat suuruusjärjestyksessä, sanotaan *peruspermutaatioksi*. Näiden alkioiden kaikissa muissa permutaatioissa on joitakin lukuja, jotka eivät esiinny niiden suuruusjärjestyksessä. Jokaisen tällaisen lukuparin sanotaan muodostavan *käänteisen järjestyksen* eli *inversion*.

Esimerkki 16.2.6 Joukon $\{1,2,3,4,5,6,7\}$ permutaatiossa

$$(3,5,1,7,4,2,6)$$

on yhdeksän inversiota, nimittäin ne, jotka muodostuvat lukupareista

$$(3,1),(3,2),(4,2),(5,1),(5,2),(5,4),(7,2),(7,4),(7,6).$$

Määritelmä 16.2.7 Permutaation sanotaan olevan *parillinen* tai *pariton* sen mukaan, onko sen inversioiden lukumäärä parillinen (mukaanlukien 0) vai pariton. Permutaatiot jaetaan täten kahteen luokkaan, joita voidaan kutsua *parilliseksi luokaksi* ja *parittomaksi luokaksi*. Kahden alkion keskinäistä paikanvaihtoa kutsutaan *transpositioksi*.

Permutaatioluokille on voimassa seuraava lause.

Lause 16.2.8 Jos permutaatiossa kaksi alkiota vaihtaa paikkaa keskenään, permutaation luokka muuttuu. Jos permutaatiossa tehdään k tällaista paikanvaihtoa, permutaation luokka säilyy tai vaihtuu sen mukaan, onko k parillinen vai pariton.

Todistus. Riittänee todistaa lauseen ensimmäinen osa, joka vastaa toisen osan tapausta $k = 1$. Oletetaan alkiot merkityiksi järjestysluvuilla 1, 2, 3, . . ., n. Valitsemme näistä järjestysluvuista mielivaltaisesti kaksi ja merkitsemme niitä symboleilla a ja b, ja vaihdamme niitä vastaavien alkioiden paikat keskenään. Jos a ja b ovat vierekkäisiä alkioita, lisääntyy tai vähenee inversioiden määrä yhdellä, sillä jos a on ennen lukua b, laskee inversioiden määrä yhdellä, jos $a > b$, ja kasvaa yhdellä, jos $a < b$. Lause siis pätee tältä osin. Oletetaan nyt, että a on ennen lukua b, ja niiden välissä on m muuta alkiota, joiden järjestyslukuja merkitsemme symbolein $c_1, c_2, \ldots, c_m$. Lukujen a ja b transpositio voidaan tällöin ajatella tapahtuvan seuraavalla tavalla: a vaihtaa paikkaa ensin luvun c_1 kanssa, sitten luvun c_2 kanssa jne., ja lopuksi luvun b kanssa. Näiden $(m + 1)$:n vierekkäisten alkioiden transpositioiden jälkeen a on alkioiden $c_1, c_2, \ldots, c_m$ ja b oikealla puolella luvun b ollessa välittömästi a:n vasemmalla puolella. Sitten b vaihtaa paikka ensin luvun c_m kanssa, sitten luvun c_{m-1} kanssa jne., ja lopuksi luvun c_1 kanssa. Täten olemme saaneet halutun permutaation, jossa a ja b ovat vaihtaneet paikka vierekkäisten alkioiden kanssa $(m + 1) + m = 2m + 1$ kertaa. Koska luku $2m + 1$ on pariton kaikilla arvoilla $m = 1, 2, \ldots$, on permutaatio vaihtanut luokkaa. ■

Tämän tapauksen perusteella saamme seuraavan tuloksen:

Lause 16.2.9 Olkoon joukossa n alkiota. Silloin parillisia ja parittomia permutaatioita on yhtä paljon, nimittäin $\frac{1}{2}n!$ kappaletta.

Todistus. Kirjoitamme näkyviin kaikki parilliset permutaatiot, joissa jokaisessa annamme sitten kahden ensimmäisenä olevan alkion vaihtaa paikkaa keskenään. Saamme täten pelkästään erilaisia permutaatioita, jotka ovat kaikki parittomia. Tällä tavalla olemme saaneet myös *kaikki* parittomat permutaatiot, sillä jos vielä löytyisi pariton permutaatio, siitä tulisi kahden ensimmäisen alkion transpositiolla parillinen, ja tämän täytyy löytyä aikaisemmasta parillisten permutaatioiden luettelosta. ■

Esimerkki 16.2.10 Kolmialkioisen joukon $\{1, 2, 3\}$ parilliset permutaatiot ovat

$$(1, 2, 3),\ (2, 3, 1),\ (3, 1, 2),$$

ja parittomat

$$(1, 3, 2),\ (2, 1, 3),\ (3, 2, 1).$$

Permutaatiot, joissa on osittain samoja alkioita

Tähän mennessä olemme tarkastelleet n-alkioisen joukon permutaatioita. Jos nyt jotkin n-jäsenisen jonon alkioista ovat samoja, on selvää, että erilaisten permutaatioiden lukumäärä on pienempi kuin $n!$. Jos meillä on esimerkiksi $n = 4$ ja alkiot listana $[1, 1, 2, 2]$, saamme vain seuraavat toisistaan eriävät permutaatiot:

$$(1,1,2,2),\ (1,2,1,2),\ (1,2,2,1),\ (2,1,1,2),\ (2,1,2,1),\ (2,2,1,1).$$

Näiden eri permutaatioiden lukumäärä on kuusi, kun nelialkioisen joukon permutaatioita olisi $4! = 24$.

Laskettaessa tämänkaltaisissa tapauksissa permutaatioiden lukumääriä kirjoitetaan ensin ylös n-alkioisen joukon $\{c_1, c_2, \ldots, c_n\}$ kaikki $n!$ permutaatiota P_i, $i = 1, 2, \ldots, n!$. Asetamme niiden alkioista m_1 kappaletta keskenään samoiksi, esimerkiksi $c_1 = c_2 = \ldots = c_{m_1} = a_1$. Edellisissä permutaatioissa P_i tulevat kaikki ne permutaatiot P_j keskenään samoiksi, jotka P_i:ssä on permutoitu vain näiden m_1 alkion $c_1, c_2, \ldots, c_{m_1}$ suhteen. Erilaisten permutaatioiden lukumäärä on täten

$$\frac{n!}{m_1!}.$$

Samaistetaan nyt loput $n - m_1 = m_2$ alkiota, esimerkiksi

$$c_{m_1+1} = c_{m_1+2} = c_{m_1+m_2} = \ldots = a_2,$$

missä $a_1 \neq a_2$. Saamme analogisesti edellisen tarkastelun perusteella näiden alkioiden permutaatioiden lukumääräksi

$$\frac{n!}{m_1!\, m_2!}.$$

Kun tämä menettely yleistetään, saadaan seuraava tulos:

Lause 16.2.11 Jos n-jonon jäsenistä vain ν kappaletta on erilaisia, esimerkiksi $a_1, a_2, \ldots, a_\nu$, jolloin

m_1 kappaletta on samoja kuin a_1
m_2 kappaletta on samoja kuin a_2
$\vdots$
m_ν kappaletta on samoja kuin a_ν

ja $m_1 + m_2 + \ldots + m_\nu = n$, on näiden alkioiden erilaisten permutaatioiden lukumäärä

$$\frac{n!}{m_1!\, m_2! \cdots m_\nu!}.$$

Lauseessa 16.2.11 saatua permutaatioiden lukumäärää kutsutaan myös *multinomikertoimeksi*. Se on binomikertoimen yleistys. Tämä kerroin esiintyy tuonnempana ns. *polynomilauseen* 16.6.1 ja osittelujen yhteydessä (Luku 16.7). Binomikertoimen $\binom{n}{k}$ merkintätavan yleistyksenä merkitään multinomikertoimia

$$\binom{n}{m_1, m_2, \ldots, m_\nu} := \frac{n!}{m_1!\, m_2! \cdots m_\nu!},$$

mistä käytetään myös merkintää $M(n; m_1, m_2, m_3, \ldots, m_\nu)$.

16.3 Kombinaatiot

Jos valitsemme n:stä annetusta alkiosta k alkiota, kutsutaan näitä valittuja alkioita k:n alkion kombinaatioksi annetusta n:stä alkiosta. Tällöin jätetään ottamatta huomioon valittujen alkioiden järjestys.

Määritelmä 16.3.1 Olkoon A epätyhjä joukko, $n := \#A$ ja $k \in [n]$. Joukon A *k-kombinaatioita* ovat kaikki sen k-alkioiset osajoukot $\{a_1, a_2, \ldots, a_k\} \subseteq A$.

Esimerkki 16.3.2 Olkoon $n = 4$ ja $k = 2$, sekä alkioiden järjestysluvut $1, 2, 3$ ja 4. Tällöin näistä alkioista voidaan valita kaksi seuraavasti:

$$\{1,2\},\ \{1,3\},\ \{1,4\},\ \{2,3\},\ \{2,4\},\ \{3,4\}$$

eli niitä on kaikkiaan kuusi erilaista.

Lause 16.3.3 Äärellisen n-alkioisen joukon k-kombinaatioiden lukumäärä on

$$K(n,k) := \frac{n!}{k!\,(n-k)!} \tag{21}$$

Näitä lukumääriä, *binomikertoimia*, merkitään

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!}$$

ja luetaan "n k:n yli".

Todistus. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$. Jokainen k-kombinaatio $\{a_{i_1}, \ldots, a_{i_k}\}$ voidaan järjestää k-variaatioksi Lauseen 16.2.3 nojalla

$$V(k,k) = \frac{k!}{(k-k)!} = \frac{k!}{0!} = k!$$

eri tavalla. Jokaista k-kombinaatiota vastaa siis $k!$ kappaletta k-variaatioita, joten k-kombinaatioiden lukumäärä on edellä määritelty binomikerroin

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Siis kaava (21) on todistettu. ■

Huomattakoon siis, että joukon k-variaatiot saadaan muodostamalla kaikkien k-kombinaatioiden permutaatiot.

Esimerkki 16.3.4 Kymmenestä henkilöstä voidaan muodostaa erilaisia seitsemän henkilön jonoja

$$V(10,7) = \frac{10!}{(10-7)!} = 604800 \text{ kappaletta.}$$

Jos jonot järjestetään aakkosjärjestykseen, on järjestys yksikäsitteinen ja mahdollisuuksia jää vain

$$K(10,7) = \frac{10!}{7! \cdot 3!} = 120 \text{ kappaletta.}$$

Esimerkki 16.3.5 Montako sanaa saadaan käyttämällä kirjainjonon MISSISSIPPI kirjaimet?

Ensin valitaan neljä paikka S-kirjaimille, sitten neljä paikkaa I-kirjaimille jne. Tulos on

$$\binom{11}{4} \cdot \binom{7}{4} \cdot \binom{3}{2} \cdot \binom{1}{1} = \frac{11!}{7! \cdot 4!} \cdot \frac{7!}{3! \cdot 4!} \cdot \frac{3!}{2! \cdot 1!} \cdot \frac{1!}{1! \cdot 0!} = 34650$$

16.4 Järjestämätön otanta takaisinpanolla

Binomikertoimet $K(n,k)$ määriteltiin järjestämättömien k kappaleen otantojen lukumääränä n-alkioisesta joukosta ilman takaisinpanoa (ks. Luku 16.3).

Lause 16.4.1 Järjestämättömien k:n kappaleen otantojen määrä n-alkioisesta joukosta takaisinpanolla on

$$\binom{n+k-1}{k} = K(n+k-1,k).$$

Tämä on sama luku, kuin on eri tapoja asettaa k identtistä palloa n:ään nimettyyn lokeroon, joiden vetoisuudet ovat rajattomat.

Todistus. Olkoon $A = \{a_1, a_2, \ldots, a_n\}$. Lauseen otantatulkinnassa joukon A alkioita otetaan toistuvasti yksi kerrallaan ja palautetaan otettu identifioinnin jälkeen takaisin. Pallot-ja-lokerot-tulkinnassa A on nimetyt lokerot, joihin identtisiä palloja asetellaan. Otannassa tietyn alkion a_i esiintymiskertojen määrä k_i vastaa lokeroon a_i laitettujen pallojen määrää ja $k = k_1 + k_2 + \ldots + k_n$.

Nyt kutakin otantaa (tai lokeroihin asettamista) vastaa k palloa (p) ja $n-1$ väliseinää ($|$) sisältävä "koodi", jonka pituus on $k+n-1$, esimerkiksi

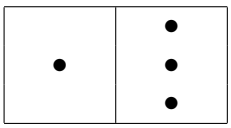
$$\underset{k_1 \text{ kpl}}{ppp} \;|\; ppppp \;|\; \ldots \;\; ppp \;|\; \underset{k_n \text{ kpl}}{ppppp}$$

Koska väliseinät $|$ voivat olla missä hyvänsä, eri mahdollisuuksia asettaa ne paikoilleen on (sama kuin asettaa k palloa noille paikoille)

$$\binom{n+k-1}{n-1} = \frac{(n+k-1)!}{(n-1)!\,k!} = \binom{n+k-1}{k}.$$

■

Esimerkki 16.4.2 Montako erilaista dominolaattaa on olemassa?



Ratkaisu. Dominolaatassa on kaksi paikkaa, $k = 2$, joissa voi olla $0-6$ täplää (nimetyt lokerot), siis $n = 7$. Eri tapoja asettaa 2 paikkaa 7 nimettyyn lokeroon, eli erilaisia laattoja, on

$$\binom{7+2-1}{2} = \binom{8}{2} = \frac{8!}{2!\cdot 6!} = 28.$$

16.5 Binomikertoimet ja binomilause

Luvussa 16.3 määritellyillä binomikertoimilla

$$K(n,k) = \binom{n}{k}$$

on tärkeitä ominaisuuksia.

Lause 16.5.1 (binomilause) Kaikilla $x, y \in \mathbb{R}$ ja kaikilla $n \in \mathbb{N}$ on voimassa

$$(x+y)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} x^{n-k} y^k$$

Todistus. Tämä jo koulumatematiikastakin tuttu binomikaava todistetaan usein induktiolla. Kombinatoriikka antaa kuitenkin yksinkertaisemman todistusmenetelmän.

On ilmeistä, että potenssiin korotus antaa lausekkeen, joka on muotoa

$$(x+y)^n = x^n + a_1 x^{n-1} y + \ldots + a_k x^{n-k} y^k + \ldots + a_{n-1} x y^{n-1} + y^n.$$

Riittää siis osoittaa, että

$$a_k = \frac{n!}{k!(n-k)!}$$

Suorittamalla potenssin $(x+y)^n$ kertolaskut saadaan muotoa $x^{n-k}y^k$ olevia potenssituloja valitsemalla y k:sta muusta tekijästä. Termi $x^{n-k}y^k$ esiintyy näin ollen yhtä monta kertaa, kuin on k:n alkion kombinaatioita n:stä alkiosta. Siis saamme

$$a_k = \binom{a}{k} = \frac{n!}{k!(n-k)!}$$

■

Kootaan binomikerrointen ominaisuuksia yhteen:

Lause 16.5.2 Olkoot $0 \leq k \leq n \in \mathbb{N}$. Binomikertoimille pätee

$$\begin{aligned}
&1) && \binom{n}{k} &&= && \binom{n}{n-k} \\
&2) && \binom{n}{1} &&= && \binom{n}{n-1} = n \\
&3) && \binom{n+1}{k} &&= && \binom{n}{k-1} + \binom{n}{k} \\
&4) && (x+y)^n &&= && \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\
&5) && \sum_{k=0}^{n} \binom{n}{k} &&= && 2^n.
\end{aligned}$$

Todistus. Kaavat 1) ja 2) ovat ilmeisiä. Kaava 3) lasketaan laventamalla yhtälön oikean puolen yhteenlaskettavat samannimisiksi ja sieventelemällä. Kaava 4) on edellä todistettu binomikaava (Lause 16.5.1), ja 5) on binomikaavan sovellutus arvoilla $a = b = 1$. ■

Tehtävä 16.5.3 Osoita, että binomikertoimille pätee yhtälö

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Voimme määritellä mielivaltaiselle reaalimuuttujalle x luvun $\binom{x}{k}$

$$\binom{x}{k} = \frac{x(x-1)(x-2)\dots(x-k+1)}{k!}.$$

Myös tällöin on voimassa

$$\binom{x}{k} + \binom{x}{k+1} = \binom{x+1}{k+1},$$

kun $k \geq 0$ on mielivaltainen kokonaisluku.

16.6 Polynomilause ja multinomikertoimet

Binomilauseen 16.5.1 yleistys on seuraava polynomilause.

Lause 16.6.1 (polynomilause) Kaikilla x_1, x_2, x_3, ..., $x_k \in \mathbb{R}$ ja kaikilla $n \in \mathbb{N}$ on voimassa

$$(x_1 + x_2 + \ldots + x_k)^n = \sum \frac{n!}{m_1! m_2! \ldots m_k!} x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k},$$

missä summa ulotetaan yli kaikkien lukujen $m_i = 0, 1, 2, \ldots, n$, kun $i = 1, 2, \ldots, k$ ja $m_1 + m_2 + \ldots + m_k = n$.

Todistus. Tarkastellaan n:n tekijän tuloa

$$(x_1 + x_2 + \ldots + x_k)(x_1 + x_2 + \ldots + x_k) \ldots (x_1 + x_2 + \ldots + x_k) \tag{22}$$

ja etsitään määrätty lukumäärä tapoja, joilla potenssitulot

$$x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k} \tag{23}$$

voivat muodostua, kun $m_1 + m_2 + \ldots + m_k = n$. Tulo (22) on sama kuin muotoa

$$x_{\nu_1} + x_{\nu_2} + \ldots + x_{\nu_n}$$

olevien termien summa. Jotta saataisiin tietää, kuinka monta tällaista termiä samaistuu termiin (22), havaitaan, että n:stä indeksistä $\nu_1, \nu_2, \ldots, \nu_n$ aina m_1 kpl saa arvon 1, m_2 kpl arvon 2 jne. ja lopulta m_k indeksiä arvon k. Tyyppiä (22) olevien termien lukumäärä saadaan täten permutoimalla n alkiota $\nu_1, \nu_2, \ldots, \nu_n$, kun m_1 alkiota on yhtäkuin 1, m_2 alkiota on yhtäkuin 2 jne. ja lopulta m_k alkiota yhtäkuin k. Lauseen 16.2.11 mukaan tämä lukumäärä on

$$M(n; m_1, m_2, m_3, \ldots, m_k) = \frac{n!}{m_1!\, m_2! \cdots m_k!},$$

joka on siis potenssitulon (23) kerroin. ■

16.7 Osittelut ja multinomikertoimet

Edellä johduttiin multinomikertoimiin permutaatioista päin. Päädymme multinomikertoimiin myös (ainakin näennäisesti) toiselta kautta.

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 16.7.1 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 16.7.2 Osa luokista voi olla tyhjiä, jolloin $n_i! = 0! = 1$. Toinen ero Luvussa 10.3 esillä olleeseen *osituksen* käsitteeseen on se, että osittelussa luokat ovat nimettyjä; ne voidaan erottaa toisistaan.

Esimerkki 16.7.3 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 10.3.1) tai Stirlingin kolmion (Taulukko 2) 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 $5 \cdot 3 = 15$.

17 REKURSIOKAAVA - DIFFERENSSIYHTÄLÖ

Monet matemaattiset tehtävät, mm. kombinatoriikan lukumääräongelmat (ks. Luku 16) ja numeerisen matematiikan approksimointimenetelmät johtavat lukujonon käsittelyyn. Lukumääräongelman yhteydessä jono ei yleensä ole analyysin mielessä suppeneva; tehtävänä voi olla löytää yksinkertainen menetelmä haluttujen jonon lukujen laskemiseksi tai arvio jonon käytöksestä suurilla indeksin arvoilla. Numeerisissa menetelmissä taas ollaan kiinnostuneita jonon suppenemisesta, erityisesti suppenemisvauhdista, jotta laskettavalle suureelle saadaan nopeasti hyvä approksimaatio.

Jos ongelman ratkaisemisessa tarkasteltava lukujono on saatu muodossa, jossa jonon luku riippuu jonkin säännön mukaan edeltävistä luvuista tai niiden erotuksista, on kyseessä rekursiokaava tai vastaavasti differenssiyhtälö. Nämä ovat saman asian eri tulkintoja. Joskus sanotaan myös, että jono on annettu induktiivisesti. Erityisesti numeerisessa matematiikassa rekursiokaavan käyttöä jonon jäsenten laskemiseen sanotaan *iteroinniksi.*

17.1 Rekursiokaavan ja differenssiyhtälön yhteys

Määritellään rekursiokaava ja differenssiyhtälö sekä tarkastellaan esimerkkejä näiden käyttötilanteista.

Rekursiokaava

Olkoon $(a_n)_{n\geq 0} = (a_0, a_1, a_2, \ldots)$ reaalilukujono tai yleisemmin alkiojono jossakin avaruudessa X.

Määritelmä 17.1.1 Avaruuden X jono $(a_n)_{n\geq 0}$ on määritelty *rekursiivisesti*, jos

$$a_n = f(n, a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \tag{24}$$

missä $f : \mathbb{N}\times X^k \to X$ on kuvaus. Yhtälö (24) on k. *kertaluvun rekursiokaava.* Jonon alkiot $a_0, a_1, \ldots, a_{k-1}$ ovat *alkuarvoja* tai *päätösarvoja*, riippuen tarkastelutavasta.

Yhtälö (24) on *normaalimuotoinen* rekursiokaava, yleisempi muoto on

$$g(n, a_n, a_{n-1}, a_{n-2}, \ldots, a_{n-k}) = 0. \tag{25}$$

Huomautus 17.1.2 a) Määritelmässä voitaisiin sallia, että a_n riippuu kaikista edeltävistä jonon alkioista. Yleensä tällainen tilanne kannattaa yrittää muuntaa muotoon (24).

b) Jotta jonon jäseniä voidaan laskea rekursiokaavasta, on tunnettava arvot a_0, a_1, a_2, ..., a_{k-1}. Jos rekursiokaavaa käytetään alkioiden a_n laskemiseen arvoilla $n = k, k+1, \ldots$ tässä järjestyksessä, on kyseessä *induktiivinen menetelmä*. Tällöin tunnettuja alkioita a_0, ..., a_{k-1} sanotaan *alkuarvoiksi*.

c) Jos lähdetään laskemaan alkiota a_n "takaperin" niin, että saadaan lopulta määritetyksi funktio F, jolle

$$a_n = F(a_{k-1}, \ldots, a_2, a_1, a_0),$$

voidaan alkioita a_0, a_1, a_2, ..., a_{k-1} sanoa *päätösarvoiksi*. Tällainen lähestymistapa on *rekursiivinen* menetelmä.

Differenssioperaattorit ja differenssiyhtälöt

Määritellään aluksi lukujonon differenssioperaattorit ja edelleen niiden avulla differenssiyhtälö. Lukujonon

$$(a_n)_{n\geq 0} = a_0, a_1, a_2, a_3, \ldots, a_{n-2}, a_{n-1}, a_n, a_{n+1}, a_{n+2}, \ldots$$

peräkkäisten termien erotukset, *differenssit* (*difference*) ovat

$\Delta a_n := a_{n+1} - a_n,\ n \geq 0$	erotus eteenpäin	"delta"
$\nabla a_n := a_n - a_{n-1},\ n \geq 1$	erotus taaksepäin	"nabla"

Näitä yhdistää yhtälö $\Delta a_{n-1} = \nabla a_n$.

Asetetaan yleinen lukujonon differenssien määritelmä:

Määritelmä 17.1.3 Olkoon $(a_n)_{n\geq 0}$ lukujono. Differenssioperaattorin Δ *potenssit* määritellään induktiivisesti

$$\begin{aligned}
\Delta^0 a_n &:= a_n, \\
\Delta^1 a_n &:= a_{n+1} - a_n = \Delta a_n, \\
\Delta^2 a_n &:= \Delta^1 a_{n+1} - \Delta^1 a_n = a_{n+2} - 2a_{n+1} + a_n, \\
&\vdots \\
\Delta^{k+1} a_n &:= \Delta^k a_{n+1} - \Delta^k a_n, \quad k \geq 1.
\end{aligned}$$

Operaattori Δ^k on k. kertaluvun *erotus eteenpäin* (*forward difference*). Vastaavas-

ti

$$\begin{aligned}
\nabla^0 a_n &:= a_n, \\
\nabla^1 a_n &:= a_n - a_{n-1} = \nabla a_n, \\
\nabla^2 a_n &:= \nabla^1 a_n - \nabla^1 a_{n-1} = a_n - 2a_{n-1} + a_{n-2}, \\
&\vdots \\
\nabla^{k+1} a_n &:= \nabla^k a_n - \nabla^k a_{n-1}, \quad n \geq k+1.
\end{aligned}$$

Operaattori ∇^k on k. kertaluvun *erotus taaksepäin* (*backward difference*). Taaksepäin-erotuksessa on huomioitava, että $\nabla^k a_n$ on määritelty vain arvoilla $n \geq k$.

Esimerkki 17.1.4 Lukujonolle $(a_n)_{n\geq 0}$ on arvoilla $n \geq 3$

$$\nabla^3 a_n = \nabla^2 a_n - \nabla^2 a_{n-1} = a_n - 3a_{n-1} + 3a_{n-2} - a_{n-3}$$

ja yleisesti

$$\nabla^k a_n = \sum_{i=0}^{k} (-1)^i \binom{k}{i} a_{n-i}.$$

Määritelmä 17.1.5 Olkoon $(a_n)_{n\geq 0}$ lukujono. Muotoa

$$g(n, a_n, \nabla a_n, \nabla^2 a_n, \ldots, \nabla^k a_n) = 0$$

olevaa yhtälöä sanotaan k. kertaluvun *differenssiyhtälöksi taaksepäin* ja sen erikoistapausta

$$a_n = f(n, a_{n-1}, \nabla a_{n-1}, \nabla^2 a_{n-1}, \ldots, \nabla^{k-1} a_{n-1})$$

normaalimuotoiseksi differenssiyhtälöksi taaksepäin.

Vastaavasti muotoa

$$g(n, a_{n-k}, \Delta a_{n-k}, \Delta^2 a_{n-k}, \ldots, \Delta^k a_{n-k}) = 0$$

olevaa yhtälöä sanotaan k. kertaluvun *differenssiyhtälöksi eteenpäin* ja sen erikoistapausta

$$a_n = f(n, a_{n-k}, \Delta a_{n-k}, \Delta^2 a_{n-k}, \ldots, \Delta^{k-1} a_{n-k})$$

normaalimuotoiseksi differenssiyhtälöksi taaksepäin.

On ilmeistä, että differenssiyhtälö voidaan aina muuntaa Määritelmän 17.1.1 mukaiseksi rekursiokaavaksi. Myös käänteinen onnistuu periaatteessa, mutta on vähemmän triviaalia toteuttaa.

Esimerkki 17.1.6 Differenssiyhtälö

$$\nabla^2 a_n - 3\nabla a_n = 6$$

muuntuu rekursiokaavaksi

$$a_n - 2a_{n-1} + a_{n-2} - 3a_n + 3a_{n-1} = -2a_n + a_{n-1} + a_{n-2} = 6.$$

Esimerkki 17.1.7 Olkoot p, q ja r vakioita. Rekursiokaava

$$a_n + pa_{n-1} + qa_{n-2} = r$$

muuntuu differenssiyhtälöksi vaikkapa seuraavasti: järjestetään vasempaan puoliskoon differenssit, lisäten tarvittavat korjaustermit:

$$\begin{aligned} a_n + pa_{n-1} + qa_{n-2} &= a_n + pa_{n-1} + q(a_n - 2a_{n-1} + a_{n-2}) - qa_n + 2qa_{n-1} \\ &= (1-q)a_n + (p+2q)a_{n-1} + q\nabla^2 a_n \\ &= (1+p+q)a_n - (p+2q)\nabla a_n + q\nabla^2 a_n. \end{aligned}$$

Täten saamme rekursiokaavan kanssa yhtäpitävän differenssiyhtälön

$$(1+p+q)a_n - (p+2q)\nabla a_n + q\nabla^2 a_n = r.$$

Esimerkki 17.1.8 Muunna differenssiyhtälö

$$a_n = 5\Delta a_{n-2} - a_{n-2}$$

rekursiokaavaksi.

Ratkaisu. Koska $\Delta a_{n-2} = a_{n-1} - a_{n-2}$, saa yhtälö normaalimuodon

$$a_n = 5a_{n-1} - 6a_{n-2}.$$

Esimerkki 17.1.9 Muunna rekursiokaava

$$a_{n+2} - a_{n+1} - 2a_n = 0.$$

differenssiyhtälöksi, jossa käytetään erotuksia eteenpäin.

Ratkaisu. $a_{n+2} = a_{n+1} + 2a_n = a_{n+1} - a_n + 3a_n = \Delta a_n + 3a_n$ ja siten

$$a_{n+2} = \Delta a_n + 3a_n \quad \text{tai} \quad a_n = \Delta a_{n-2} + 3a_{n-2}.$$

Tehtävä 17.1.10 Muunna rekursiokaava

$$a_{n+2} + 2a_{n+1} - 6a_n = 1$$

differenssiyhtälöksi, jossa käytetään erotuksia eteenpäin.

Vastaus: $\Delta^2 a_n + 4\Delta a_n - 3a_n = 1$ tai $\Delta^2 a_{n-2} + 4\Delta a_{n-2} - 3a_{n-2} = 1$.

Muun muassa differentiaaliyhtälöiden ja diskreettien stokastisten prosessien yhteydessä on luonnollista käyttää differenssiyhtälöä, kun taas lukumääräongelmissa käytetään useimmiten rekursiokaavoja.

Esimerkki 17.1.11 Differentiaaliyhtälön numeerinen ratkaiseminen voidaan usein aloittaa *diskretisoimalla* se. Kirjoitetaan differentiaaliyhtälöön $y' = f(x, y)$ liittyvä alkuarvotehtävä muotoon

$$dy = f(x, y)\, dx, \qquad y(x_0) = y_0.$$

Olkoot $x_0 < x_1 < x_2 < \ldots$ ja $y_0 < y_1 < y_2 < \ldots$ pistejonoja. Korvataan yhtälössä "äärettömän pieni" differentiaalinen poikkeama dv äärellisellä erotuksella ∇v_k ja siirrytään tarkastelemaan esimerkiksi yhtälöä

$$\nabla y_k = f\left(\frac{x_k + x_{k-1}}{2}, \frac{y_k + y_{k-1}}{2}\right) \cdot \nabla x_k.$$

Tämän avulla saadaan approksimaatioita alkuarvotehtävän ratkaisulle pisteissä y_1, y_2, ... ratkaisematta itse differentiaaliyhtälöä.

Esimerkki 17.1.12 Kuinka monella tavalla n erilaista esinettä voidaan laittaa riviin? Kuinka monta permutaatiota on joukolla $[n]$?

Ratkaisu. Tehtävä on ratkaistu aiemmin suoraan tuloperiaatteella. Toinen tapa on muodostaa rekursiokaava: Yhden alkion joukolla on 1 permutaatio. Olkoon a_n joukon $[n]$ permutaatioiden määrä, $n \in \mathbb{N}$. Alkio $n{+}1$ voidaan asettaa näiden alkuun, väliin tai loppuun yhteensä $n{+}1$ eri tavalla. Täten $a_{n+1} = (n+1)a_n$, eli

$$\begin{aligned} a_1 &:= 1, \\ a_{n+1} &:= (n{+}1)a_n, \quad n \in \mathbb{N}. \end{aligned}$$

Esimerkki 17.1.13 Lapsi hyppii n-askelmaisia portaita ylöspäin yksi tai kaksi askelta kerrallaan. Miten monella eri tavalla a_n hän voi portaat nousta ylös?

Ratkaisu. Alkuarvot ovat $a_0 = 1$, $a_1 = 1$. Tasolle n voidaan tulla joko tasolta $n-1$ tai tasolta $n-2$. Yhteenlaskuperiaatteen mukaan saadaan nk. Fibonaccin alkuarvotehtävä (ks. Luku 18.4)

$$a_n = a_{n-1} + a_{n-2},\ a_0 = 1,\ a_1 = 1.$$

17.2 Rekursiivisesta ohjelmoinnista

Useissa ohjelmointikielissä on mahdollista muodostaa rekursiivisia (ali)ohjelmia. Ne ovat yleensä tyypiltään *funktioita*, jotka annetuista lähtöarvoista laskevat tuloksen ja palauttavat sen kutsuvaan ohjelmaan. Rekursiivisuus tarkoittaa sitä, että funktio kutsuu itseään toistuvasti, kunnes jokin päätösehto toteutuu. Kutsujen yhteydessä informaatio kasaantuu Huomautuksen 17.1.2 c)-kohdassa kuvatulla tavalla.

Laskettaessa rekursiivisesti annetun alkiojonon alkiota a_K tietokoneohjelmalla olisi luonnollista käyttää rekursiivista funktiota, joka kutsuu itseään, kunnes alkuehdot (päätösehdot) tulevat vastaan. Tällainen ohjelma joutuu käyttämään tietokoneen muistia epätaloudellisesti ja siten ohjelma toimii hitaammin kuin vastaava suora toteutus. Jos muistia on käytettävissä huomattavan vähän, voi käydä jopa niin, että rekursiivinen ohjelma ei pysty tehtävästä suoriutumaan, vaikka induktiivinen ohjelma toimii hyvin (vrt. Esimerkki 18.4.5).

17.3 Rekursiokaavojen käyttötilanteita

A. Monet matematiikan erikoisfunktiot ja operaattorit (vrt. differenssioperaattorit edellä) määritellään rekursiokaavoilla.

Esimerkki 17.3.1 *Tšebyševin polynomit* $T : \mathbb{R} \to \mathbb{R}$ määritellään seuraavasti:

$$\begin{aligned} T_0 &:= 1, \\ T_1(t) &:= t, \\ T_{n+1}(t) &:= 2tT_n(t) - T_{n-1}(t). \end{aligned}$$

Kullakin kiinteällä $t \in \mathbf{R}$ on kyseessä reaalinen lukujono.

B. Jos rekursiivisesti annettu lukujono *suppenee*, raja-arvo voidaan joskus laskea suoraan rekursiokaavasta. Alkuarvojen valinta vaikuttaa yleensä oleellisesti jonon käytökseen. Rekursiokaavalla laskettu raja-arvoehdokas taas on usein alkuarvoista riippumaton. Tämä voi johtaa tilanteeseen, että ”raja-arvo” voidaan muodollisesti määrittää rekursiokaavasta, vaikka jono ei edes suppene! On siis erikseen todettava jonon suppenevuus; vasta sitten voidaan rekursiokaavaa käyttää luotettavasti itse raja-arvon laskemiseen.

Esimerkki 17.3.2 Olkoon arvoilla $n \in \mathbb{N}$

$$a_n := \frac{1}{2}\left(a_{n-1} + \frac{2}{a_{n-1}}\right).$$

Olkoon $a_0 \neq 0$. Voitaisiin osoittaa, että jono $(a_n)_{n\in\mathbb{N}}$ on monotoninen ja rajoitettu, joten sillä on raja-arvo $a \in \mathbb{R}$ (ks. Analyysin kurssit). Koska

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n-1} = a,$$

saadaan

$$a = \lim_{n\to\infty} a_n = \frac{1}{2}\left(a + \frac{2}{a}\right),$$

mistä $a = \pm\sqrt{2}$. Koska kaikki jonon luvut ovat samaa merkkiä kuin a_0, myös raja-arvon etumerkki on sama kuin alkuarvon $a_0 \neq 0$.

Esimerkki 17.3.3 b) Olkoot aluksi a_0, $a_1 \in \mathbb{R}$ ja

$$a_n := \frac{a_{n-1}}{2} + a_{n-2}^2, \qquad n \geq 2.$$

Oletetaan, että jono on suppeneva raja-arvona $a \in \mathbb{R}$. Ottamalla raja-arvo kaavan molemmista puolista ja käyttämällä raja-arvon laskusääntöjä saadaan yhtälö

$$a = \frac{a}{2} + a^2,$$

josta $a = 0$ tai $a = 1/2$. Jono ei kuitenkaan suppene millä tahansa alkuarvoilla! On ilmeistä, että raja-arvo on $1/2$ alkuarvoilla $a_0 = a_1 = 1/2$. Etsi muita alkuarvoja, joilla jono suppenee (esimerkiksi tietokoneella tai laskimella).

C. Useat numeerisen matematiikan algoritmit perustuvat rekursiokaavan määrittelemään iteraatioon.

Esimerkki 17.3.4 Tarkastellaan funktion f *kiintopisteiden* etsimistä eli yhtälön $f(x) = x$ ratkaisemista. Otetaan alkuarvoksi erään ratkaisun jokin approksimaatio a ja muodostetaan approksimoiva jono

$$\begin{aligned} x_0 &:= a, \\ x_n &:= f(x_{n-1}), \quad n \in \mathbb{N}. \end{aligned}$$

Jos f toteuttaa tietyt ehdot ratkaisun lähistöllä, saadaan kohti ratkaisua suppeneva jono (*Banachin kiintopistelause*).

Esimerkki 17.3.5 Yhtälön $g(x) = 0$ ratkaisemiseksi *Newtonin menetelmällä* muodostetaan vastaavasti jono

$$\begin{aligned} x_0 &:= a, \\ x_{n+1} &:= x_n - \frac{g(x_n)}{g'(x_n)}, \quad n \in \mathbb{N}_0. \end{aligned}$$

D. Tietokoneiden kehityksen myötä on tullut muotiin nk. *fraktaaligeometria*, jonka näkyvin muoto ovat kauniit monimutkaiset tietokonegrafiikalla muodostetut fraktaalikuviot. Näitä kuvioita muodostetaan useimmiten rekursiokaavojen avulla.

Esimerkki 17.3.6 Fraktaalikuvioista tunnetuin on *Benoit Mandelbrotin* nimeä kantava kompleksitason joukko M, joka määritellään seuraavasti: Kompleksiluku $c \in M$ jos ja vain jos rekursiokaavan

$$\begin{aligned} z_0 &:= 0, \\ z_n &:= z_{n-1}^2 + c, \quad n \in \mathbb{N} \end{aligned}$$

määrittelemä kompleksilukujono $(z_n)_{n\geq 0}$ on rajoitettu. Kuvio muodostetaan tason osasta niin, että joukon M alkiot värjätään eri värillä kuin muut. Voidaan vielä käyttää useita värejä lähellä reunaa sen mukaan, kuinka nopeasti jono havaitaan rajoittamattomaksi. Kuvio on kaunis ja monimuotoinen; suurentamalla sen yksityiskohtia saadaan näkyviin loputtomasti samankaltaisesti toistuvaa hienorakennetta.

E. Diskreetin matematiikan lukumäärä- yms. ongelmissa ollaan kiinnostuneita itse jonon luvuista.

Esimerkki 17.3.7 Olkoon $a_{n,k}$ luku, joka ilmoittaa, kuinka monella tavalla voidaan valita k alkion kokoelma n erilaisen esineen $\{e_1, e_2, \ldots, e_n\}$ joukosta. Määritä luvut $a_{n,k}$.

Ratkaisu. Jaetaan tehtävä kahteen osaan sen mukaan, käytetäänkö esinettä e_1. On olemassa $a_{n-1,k}$ k-alkioista joukkoa, joihin e_1 ei kuulu ja $a_{n-1,k-1}$ k-alkioista joukkoa, joihin se kuuluu. Näin saadaan *kaksimuuttujainen* rekursiokaava

$$\begin{aligned} a_{n,0} &:= a_{n,n} := 1, \quad n \in \mathbb{N}_0, \\ a_{n,k} &:= 0, \quad k > n, \\ a_{n,k} &:= a_{n-1,k} + a_{n-1,k-1}, \quad k < n, \end{aligned}$$

jonka ratkaisut voidaan kirjoittaa taulukon muotoon:

$a_{n,k}$	$k=0$	1	2	3	4	5	$\cdots$
$n=0$	1	0	0	0	0	0	$\cdots$
1	1	1	0	0	0	0	$\cdots$
2	1	2	1	0	0	0	$\cdots$
3	1	3	3	1	0	0	$\cdots$
4	1	4	6	4	1	0	$\cdots$
5	1	5	10	10	5	1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

17.4 Rekursiokaavan ratkaiseminen

Monesti konkreettisen ongelman matemaattinen mallitus johtaa rekursiokaavaan, josta haluttu tulos a_K voidaan periaatteessa laskea. Tämä voi kuitenkin olla käytännössä hidasta tai jopa mahdotonta, jos kaava on riittävän monimutkainen ja K suuri. Joskus on mahdollista *ratkaista* rekursiokaava, ts. määrittää funktio g, jolle

$$a_n = g(n, a_{k-1}, \ldots, a_0)$$

saadaan lasketuksi mille tahansa $n \geq k$ suoraan, laskematta ensin lukuja a_k, a_{k+1}, …, a_{n-1}. Jono $(a_n)_{n\geq 0}$ tai yhtä hyvin funktio g on rekursiokaavan *ratkaisu.*

Erikoista tyyppiä oleva – esimerkiksi lineaarinen – rekursiokaava voidaan ratkaista *ratkaisukaavalla* tai muulla eksplisiittisellä menetelmällä. Joskus ratkaisu keksitään jollakin epäeksaktilla keinolla, jopa arvaamalla, ja todistetaan oikeaksi vaikkapa induktioperiaatteella.

Esimerkki 17.4.1 Esimerkin 17.3.7 kaksiulotteisen rekursiokaavan

$$a_{n,k} := a_{n-1,k} + a_{n-1,k-1}$$

ja sen alkuehdot toteuttavaksi ratkaisuksi voidaan todentaa Lauseen 16.5.2 kohdan 3) avulla binomikertoimet

$$a_{n,k} = \binom{n}{k}.$$

Esimerkki 17.4.2 Permutaatioesimerkin 17.1.12 rekursiokaavan

$$\begin{aligned} a_0 &:= 1, \\ a_n &:= na_{n-1}, \quad n \in \mathbb{N} \end{aligned}$$

ratkaisuksi on jo Lauseessa 16.2.3 todettu kertoma $a_n = n!$. Eksakti ratkaisu ei kuitenkaan ole (ollut) käytännöllinen suurilla arvoilla n. Klassillisella *Stirlingin kaavalla*

$$n! \approx s_n := \sqrt{2\pi n}\,\left(\frac{n}{e}\right)^n$$

saadaan suurten lukujen kertomille hyviä arvioita. Absoluuttinen virhe $|n! - s_n|$ kylläkin kasvaa, kun n kasvaa, mutta suhteelliselle virheelle pätee

$$\lim_{n\to\infty} \left|\frac{n! - s_n}{s_n}\right| = 0.$$

Esimerkiksi $100! = 9.3326 \cdot 10^{157}$ ja $s_{100} = 9.3248 \cdot 10^{157}$, jolloin suhteellinen virhe on noin 0.00083.

18 LINEAARINEN REKURSIOKAAVA

Kuten differentiaaliyhtälöiden teoriassa, (ainakin vakiokertoimisille) lineaarisille rekursiokaavoille voidaan johtaa mekaaniset ratkaisumenetelmät.

18.1 Lineaarisen rekursiokaavan muoto

Määritelmä 18.1.1 Jos reaalilukujonolle $(a_n)_{n\geq 0}$ on voimassa

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = f(n), \tag{26}$$

missä luvut $c_i \in \mathbb{R}$ ovat *kertoimia*, c_0, $c_k \neq 0$, $n \geq k > 0$ ja f reaaliarvoinen funktio, yhtälö (26) on *lineaarinen vakiokertoiminen* rekursiokaava (LVRK), jonka *kertaluku* on k. Jos $f \equiv 0$, rekursiokaava on *homogeeninen* (LHVRK).

Huomautus 18.1.2 Lineaariseksi sanotaan myös rekursiokaavan (LVRK) yleisempää muotoa, jossa kertoimet c_i eivät välttämättä ole vakioita vaan funktioita $c_i : \mathbb{N}_0 \to \mathbb{R}$. Itse asiassa kertoimet ovat tällöin lukujonoja.

Esimerkki 18.1.3 Kaava

$$2na_n + 4a_{n-1} + \ln(n+1)a_{n-2} = e^n$$

on toisen kertaluvun lineaarinen epähomogeeninen ei-vakiokertoiminen rekursiokaava.

Esimerkki 18.1.4 Tarkastellaan lukujonoa $(a_n)_{n\geq 0} = 1, 1, -1, -1, 1, 1, -1, -1, \ldots$. Helposti nähdään, että se toteuttaa rekursiokaavan $a_n + an - 2 = 0$. Toisaalta tämän saman rekursiokaavan toteuttaa myös moni muu jono, esimerkiksi $(a_n)_{n\geq 0} = 2, 1, -2, -1, 2, 1, -2, -1, 2, 1, \ldots$ Yksinkertaisillekaan jonoille ei ole aina helppo keksiä suoraa esityskaavaa, sitä ratkaisua. ■

Seuraavissa luvuissa tarkastellaan lineaarisen vakiokertoimisen rekursiokaavan ja alkuarvotehtävän ratkaisemista.

Ratkaisumenetelmät perustuvat polynomiyhtälöiden ratkaisemiseen, ja tämä tuo mukanaan välttämättömyyden käyttää kompleksilukuja.

18.2 Kompleksiluvuista

Toisen asteen polynomiyhtälöllä $a\alpha^2 + b\alpha + c = 0$ ei ole reaalialueessa ratkaisua, jos sen *diskriminantti* $D := b^2 - 4ac$ on aidosti negatiivinen. Kunnan $\mathbb{R}$ laajennuksessa, *kompleksialueessa* eli *kompleksitasossa* $\mathbb{C}$ yhtälöllä on kuitenkin ratkaisut

$$\alpha_{1,2} = \frac{-b \pm i\sqrt{-D}}{2a},$$

missä $i := \sqrt{-1}$ on nk. *imaginaariyksikkö*, jolle siis $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i$, $i^6 = -1$ jne.

Lause 18.2.1 (algebran peruslause) Jokaisella kompleksimuuttujan k. asteen polynomiyhtälöllä $P_k(z) = 0$ on kompleksitasossa k kappaletta juuria, kun useampikertaiset juuret lasketaan kertalukunsa mukaan. ■

Kompleksiluku $z = x+iy$ voidaan samaistaa euklidisen xy-tason pisteen $(x, y) \in \mathbb{R}^2$ kanssa; $x + iy \simeq (x, y)$. Lineaariavaruudeksi tulkitun avaruuden $\mathbb{C}$ kannan muodostavat vektorit $1 \simeq (1, 0)$ ja $i \simeq (0, 1)$, jolloin

$$z = x \cdot 1 + y \cdot i \simeq x(1, 0) + y(0, 1) = (x, y).$$

Kompleksiluvun $z = x + iy$ *reaaliosa* on x, *imaginaariosa* on y ja *liittoluku*

$$\overline{z} := x - iy.$$

Kompleksiluku voidaan esittää napakoordinaateissa (r, φ) seuraavasti (ks. myös Kuva 47):

$$z = x + iy = r(\cos\varphi + i\sin\varphi) = re^{i\varphi} = |z|e^{i\arg z},$$

missä

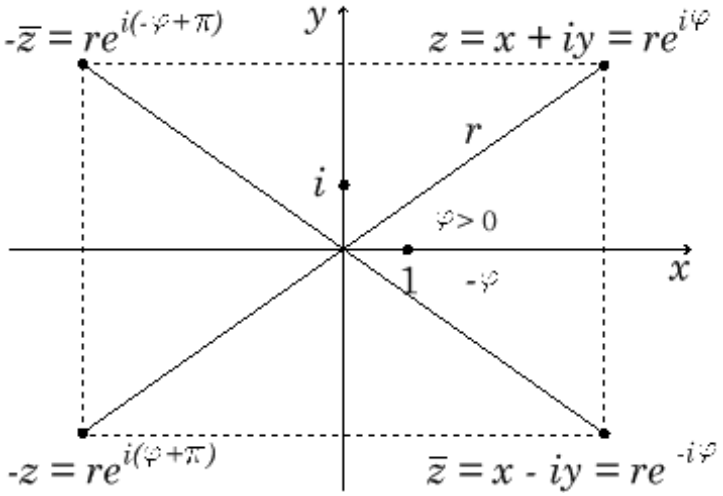
$$|z| = r := \sqrt{x^2 + y^2} = |\overline{z}| = \sqrt{z\overline{z}}$$

on luvun z *moduli* (eli *normi*, *pituus*) ja $\arg z = \varphi$ sen *argumentti*, so. kulma, jonka vektori z muodostaa positiivisen x-akselin kanssa. Kulma ei ole yksikäsitteisesti määrätty, mutta jos on valittu $\arg z = \varphi$, on kosinin ja sinin jaksollisuuden nojalla myös

$$z = re^{i\varphi} = re^{i(\varphi + n2\pi)} \text{ kaikilla } n \in \mathbb{Z}.$$

Jos $|z| > 0$, kulma voidaan valita esimerkiksi seuraavien sääntöjen mukaan:

$$\begin{aligned}
&\text{jos} \quad x > 0, \quad \varphi = \arg z = \overline{\arctan}\,\frac{y}{x} \\
&\text{jos} \quad x < 0, \quad \varphi = \arg z = \overline{\arctan}\,\frac{y}{x} + \pi \\
&\text{jos} \quad x = 0, \quad \varphi = \arg z = \frac{\pi}{2}\,\mathrm{sign}(y)
\end{aligned}$$



Kuva 47: Kompleksilukuja tasossa

Kompleksilukujen yhteen- ja kertolaskut: jos $z_k = x_k + iy_k = r_k e^{i\varphi_k}$, niin

$$\begin{aligned} z_1 + z_2 &= (x_1 + x_2) + i(y_1 + y_2), \\ z_1 z_2 &= (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \\ &= (r_1 e^{i\varphi_1})(r_2 e^{i\varphi_2}) = |z_1||z_2| e^{i(\varphi_1+\varphi_2)}. \end{aligned}$$

Potenssiin korotus saadaan *de Moivren* kaavalla

$$z^n = (re^{i\varphi})^n = r^n e^{i(n\varphi)} = |z|^n(\cos n\varphi + i \sin n\varphi).$$

Esimerkki 18.2.2 a) Muunnetaan $1 + i\sqrt{3}$ suorakulmaisista napakoordinaatteihin:

$$1 + i\sqrt{3} = \sqrt{1+3}\, e^{i \overline{\arctan}\sqrt{3}} = 2e^{i\frac{\pi}{3}} = 2e^{-i\frac{5\pi}{3}}.$$

Esimerkki 18.2.3 Jatkossa tarvitaan helposti edellisistä johdettavia kaavoja

$$\begin{aligned} z^n + (\overline{z})^n &= 2|z|^n \cos n\varphi \in \mathbb{R}, \\ z^n - (\overline{z})^n &= 2i|z|^n \sin n\varphi \in \mathbb{C}. \end{aligned}$$

Esimerkki 18.2.4 Jos luvut

$$w_n = Az^n + B(\overline{z})^n = |z|^n \left((A+B)\cos n\varphi + i(A-B)\sin n\varphi\right)$$

ovat *reaalisia*, on olemassa vakiot C, $D \in \mathbb{R}$, joille (harjoitustehtävä)

$$w_n = |z|^n(C \cos n\varphi + D \sin n\varphi).$$

18.3 Homogeeninen rekursiokaava

Yleinen ratkaisu. Lineaarinen homogeeninen vakiokertoiminen rekursiokaava (LHVRK)

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0, \tag{27}$$

missä luvut $c_i \in \mathbf{R}$ ovat vakioita, ratkaistaan samaan tapaan kuin lineaarinen homogeeninen vakiokertoiminen differentiaaliyhtälö. Kun sijoitetaan yrite

$$a_n := \alpha^n$$

yhtälöön LHVRK (27), saadaan yhtälö $c_0\alpha^n + c_1\alpha^{n-1} + \cdots + c_k\alpha^{n-k} = 0$, josta jakamalla luvulla α^{n-k}

$$c_0\alpha^k + c_1\alpha^{k-1} + \cdots + c_k = 0. \tag{28}$$

Yhtälöllä LHVRK (27) on ratkaisuna muotoa $a_n = \alpha^n$ oleva ratkaisujono $(a_n)_{n\geq 0}$ jos ja vain jos α on LHVRK:n *karakteristisen yhtälön* (28) ratkaisu. Algebran peruslauseen mukaan karakteristisella yhtälöllä on kompleksitasossa k kappaletta juuria, joista jotkut voivat olla useampikertaisia. Ratkaistaessa karakteristista yhtälöä on muistettava, että jos $\alpha := a + ib$ on juuri, myös $\overline{\alpha} = a - ib$ on juuri.

Lause 18.3.1 Olkoot $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{C}$ lineaarisen vakiokertoimisen rekursiokaavan LHVRK (27) karakteristisen polynomiyhtälön (28) juuret lueteltuina niin, että useampikertaiset juuret ovat peräkkäin. Yhtälön LHVRK *yleinen ratkaisu* on silloin

$$a_n = \mathbf{B}_1\alpha_1^n + \mathbf{B}_2\alpha_2^n + \cdots + \mathbf{B}_k\alpha_k^n,$$

missä kertoimet $\mathbf{B}_p$ määräytyvät juuren kertaluvun mukaan seuraavasti:

$p := 1$;
while $p \leq k$
  $m_p :=$ juuren α_p kertaluku;
  for $j = 0, 1, \ldots, m_p - 1$
    $\mathbf{B}_{p+j} = A_{p+j}n^j, \quad A_{p+j} \in \mathbb{C}$;
  end;
  $p := p + m_p$;
end

Todistus. Sivuutetaan (ei kovin vaikea, mutta työläs). □

Esimerkki 18.3.2 Ratkaise rekursiokaava

$$a_n - 2a_{n-1} = 0.$$

Ratkaisu. Sijoitus $a_n := \alpha^n$ antaa yhtälön $\alpha^n - 2\alpha^{n-1} = 0$, josta jakamalla luvulla α^{n-1} saadaan karakteristinen yhtälö

$$\alpha - 2 = 0.$$

Tällä on ratkaisu $\alpha = 2$, joten rekursiokaavan yleinen ratkaisu on

$$a_n := A2^n,\ A \in \mathbb{C}.$$

Esimerkki 18.3.3 Ratkaise rekursiokaava

$$a_n = 4a_{n-1} - 4a_{n-2}, \quad n \geq 2.$$

Ratkaisu. Karakteristinen yhtälö on $\alpha^n = 4\alpha^{n-1} - 4\alpha^{n-2}$, josta jakamalla luvulla α^{n-2} saadaan karakteristinen yhtälö

$$\alpha^2 - 4\alpha + 4 = 0.$$

Tällä on ratkaisut $\alpha_1 = \alpha_2 = 2$, joten rekursiokaavan yleinen ratkaisu on

$$a_n = A_1 2^n + A_2 n 2^n, \quad A_1, A_2 \in \mathbb{C}.$$

18.4 Alkuarvotehtävä

Kertalukua k olevan rekursiokaavan yleinen ratkaisu sisältää siis k vapaata parametria $A_p \in \mathbb{C}$. Jos rekursiokaavalle on annettu alkuarvot $a_0, a_1, \ldots, a_{k-1}$, voidaan yleisestä ratkaisusta poimia näitä vastaava yksittäisratkaisu. Tämä *alkuarvotehtävän* ratkaiseminen johtaa yhtälöryhmän ratkaisemiseen.

Esimerkki 18.4.1 Ratkaise rekursiokaava

$$\begin{aligned} a_0 &:= 1,\ a_1 := 0, \\ a_n &:= -a_{n-2}, \quad n \geq 2. \end{aligned}$$

Ratkaisu. Karakteristisen yhtälön $\alpha^2 + 1 = 0$ juuret ovat $\alpha_{1,2} = \pm i$. Yleinen ratkaisu on siten

$$a_n = A_1 i^n + A_2 (-i)^n.$$

Alkuehdoista saadaan yhtälöryhmä

$$\left\{ \begin{array}{rcrcrcl} A_1 & + & A_2 & = & a_0 & = & 1 \\ iA_1 & - & iA_2 & = & a_1 & = & 0, \end{array} \right.$$

jonka ratkaisut ovat $A_1 = A_2 = 1/2$. Siis haettu ratkaisu on

$$a_n = \frac{i^n + (-i)^n}{2} = (1, 0, -1, 0, 1, 0, -1, 0, \ldots).$$

Esimerkki 18.4.2 Ratkaise rekursiokaava

$$\begin{aligned} a_0 &:= 0,\ a_1 := 1,\ a_2 := 2, \\ a_n &:= 2a_{n-1} + 2a_{n-2} + 3a_{n-3}, \quad n \geq 3. \end{aligned}$$

Ratkaisu. a) *Homogeeniyhtälön yleinen ratkaisu:* Karakteristisen yhtälön

$$\alpha^3 - 2\alpha^2 - 2\alpha - 3 = 0$$

eräs juuri on $\alpha_1 = 3$. Jaetaan yhtälön vasen puoli tekijällä $\alpha - 3$, jolloin saadaan

$$(\alpha - 3)(\alpha^2 + \alpha + 1) = 0.$$

Muut juuret ovat siis $\alpha_{2,3} = (-1 \pm i\sqrt{3})/2$, joten yleinen ratkaisu on

$$a_n = A_1 3^n + A_2 \left(\frac{-1 + i\sqrt{3}}{2} \right)^n + A_3 \left(\frac{-1 - i\sqrt{3}}{2} \right)^n,\ A_k \in \mathbb{C}.$$

b) *Haluttu yksittäisratkaisu:* Muodostetaan kompleksinen yhtälöryhmä

$$\begin{cases} A_1 + A_2 + A_3 = 0 \\ \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3 A_3 = 1 \\ \alpha_1^2 A_1 + \alpha_2^2 A_2 + \alpha_3^2 A_3 = 2, \end{cases}$$

josta ratkaistaan vakiot A_k (harjoitustehtävä).

Esimerkki 18.4.3 (Fibonaccin luvut) Ensimmäinen matematiikassa käytetty rekursiokaava lienee ollut Leonardo di Pisan eli Fibonaccin rekursiokaava

$$\begin{aligned} a_0 &:= 1,\ a_1 := 1, \\ a_n &:= a_{n-1} + a_{n-2}, \quad n \geq 2, \end{aligned}$$

joka on peräisin 1200-luvun alkupuolelta. Tässä luku a_n ilmaisee kanipopulaation pariskuntien lukumäärän n kuukauden kuluttua alusta, jolloin pareja oli yksi vastasyntynyt, ja jokainen vähintäin kaksi kuukautta vanha pariskunta saa kuukauden vaihteessa tyttö- ja poikakanin. Jonon $(a_n)_{n\in\mathbb{N}}$ jäsenet ovat *Fibonaccin lukuja*.

Toinen sovellus Fibonaccin luvuille on seuraava: On kiivettävä n porrasta ylös. Jokaisella askeleella noustaan yksi tai kaksi porrasta. Kuinka monella tavalla kiipeäminen voidaan suorittaa (ks. Esimerkki 17.1.13) ?

Fibonaccin rekursiokaavan ratkaisi de Moivre 1700-luvun alkupuolella käyttäen jonon generoivaa funktiota (harjoitustehtävä).

Esimerkki 18.4.4 Fibonaccin kaava on kuitenkin 2. kertaluvun lineaarinen homogeeninen vakiokertoiminen rekursiokaava. Karakteristisen yhtälön

$$\alpha^2 = \alpha + 1$$

ratkaisut ovat $\alpha_{1,2} = 1/2\,(1 \pm \sqrt{5})$. Täten yhtälön yleinen ratkaisu on

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n, \quad A_1, A_2 \in \mathbb{C}.$$

Kun otetaan huomioon alkuarvot $a_0 = a_1 = 1$, saadaan

$$A_1 = \frac{1}{\sqrt{5}}\,\frac{1}{2}(1+\sqrt{5}), \quad A_2 = -\frac{1}{\sqrt{5}}\,\frac{1}{2}(1-\sqrt{5}),$$

mistä lopullinen kaava

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1}{2}(1+\sqrt{5})\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1}{2}(1-\sqrt{5})\right)^{n+1}.$$

```
function F = Fibonacci(N);
if N < 2
  F = 1;
  else
  a_{i-2} = 1; a_{i-1} = 1;
  for ind = 2 : N
    a_i = a_{i-1} + a_{i-2};
    a_{i-2} = a_{i-1}; a_{i-1} = a_i;
  end
  F = a_i;
end
```

```
function F = Fiborek(N);
if N < 2
  F = 1;
  else
  F = Fiborek(N−1) + Fiborek(N−2);
end
```

Kuva 48: Suora ja rekursiivinen ohjelma Fibonaccin luvuille

Esimerkki 18.4.5 Fibonaccin lukujen laskeminen rekursiokaavasta tietokoneohjelmalla on valaiseva esimerkki siitä, että rekursiivista ohjelmaa ei kannata käyttää tällaiseen tehtävään. Kuvassa 48 esimerkki induktiivisesta ja rekursiivisesta ohjelmasta. Esimerkiksi lukua $a_{15} = 987$ laskettaessa

a) suorassa ohjelmassa on yksi ohjelman kutsu, 14 yhteenlaskua (ja sijoituskäskyjä, joita kylläkin voisi vähentää kirjoittamalla ohjelma esimerkiksi käyttäen vektoria F),

b) rekursiivisessa on yhteenlaskujen lisäksi funktion kutsuja 1973 kappaletta.

Käytettäessä MATLAB-ohjelmaa eräällä tietokoneella meni suorituksiin aikaa 0.3 ja 63 sekuntia.

18.5 Lineaarinen vakiokertoiminen rekursiokaava

Luvussa 18.3 johdettiin lineaariselle homogeeniselle vakiokertoimiselle rekursiokaavalle ratkaisumenetelmä. Tässä Luvussa tarkastellaan yleisen lineaarisen vakiokertoimisen rekursiokaavan LVRK

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = f(n) \tag{29}$$

ratkaisemista vastaavan lineaarisen homogeeniyhtälön yleisen ratkaisun ja epähomogeenikaavan yksittäisratkaisun summana.

Lause 18.5.1 Olkoon lineaarisen vakiokertoimisen homogeeniyhtälön (30)

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0 \tag{30}$$

FUNKTIO $f(n)$	YRITE p_n
d	D
$d_1n + d_0$	$D_1n + D_0$
$\vdots$	$\vdots$
$d_rn^r + d_{r-1}n^{r-1} + \cdots + d_0$	$D_rn^r + D_{r-1}n^{r-1} + \cdots + D_0$
$d\lambda^n$	$D\lambda^n$
$(d_1n + d_0)\lambda^n$	$(D_1n + D_0)\lambda^n$
$\vdots$	$\vdots$
$(d_rn^r + \cdots + d_0)\lambda^n$	$(D_rn^r + \cdots + D_0)\lambda^n$

Taulukko 4: Yritetaulukko

yleinen ratkaisu $(h_n)_{n\geq 0}$ ja yksi epähomogeeniyhtälön (29) ratkaisu $(e_n)_{n\geq 0}$. Yhtälön LVRK (29) täydellisen ratkaisun muodostaa edellisten summajono $(a_n)_{n\geq 0}$, ts. jono

$$a_n := h_n + e_n.$$

Todistus. Samaan tapaan kuin differentiaaliyhtälöiden tapauksessa. □

Ongelmana on siis löytää epähomogeeniyhtälölle yksi ratkaisu. Yksinkertaisissa tapauksissa tämä onnistuu *yritteellä*.

Yritemenetelmä. Yhden ratkaisun löytämiseksi epähomogeeniyhtälölle LVRK

$$c_0a_n + c_1a_{n-1} + \cdots + c_ka_{n-k} = f(n) \tag{31}$$

muodostetaan *yritejono* $(p_n)_{n\geq 0}$, jonka muoto riippuu funktiosta f ja vastaavan homogeeniyhtälön ratkaisuista ja joka sisältää *määräämättömiä vakioita*. Yrite sijoitetaan epähomogeeniyhtälöön lukujen a_k paikalle ja vakioiden arvot lasketaan.

Eräissä yksinkertaisissa tapauksissa yrite voidaan valita Taulukon 4 avulla. Taulukossa luvut d_i, λ ja $r \in \mathbb{R}$ ovat funktion f määräämiä tunnettuja vakioita ja D_i yritteen määräämättömiä vakioita. Taulukon käyttöä koskevia ohjeita on koottu Huomautukseen 18.5.2

Huomautus 18.5.2 a) Jos funktio f on esimerkiksi astetta r oleva polynomi, jonka alempaa astetta olevia termejä puuttuu, on yrite silti otettava täydellisenä.

b) Jos f on eri tyyppisten funktioiden summa $f_1 + f_2 + \cdots + f_k$, missä kutakin funktiota f_i vastaa taulukossa jono $(p_{n,i})_{n\geq 0}$, yritteeksi otetaan summajono $(p_{n,1} + p_{n,2} + \cdots + p_{n,k})_{n\geq 0}$.

c) Jos homogeeniyhtälöllä on ratkaisuna jono $(b_n)_{n\geq 0}$, joka on samaa muotoa (esim. polynomi) kuin kokeiltava yrite $(p_n)_{n\geq 0}$, tulee yritteeksi ottaa jono $(np_n)_{n\geq 0}$. Mikäli tällainenkin on homogeeniyhtälön ratkaisu (tai vakioita ei voida saaduista yhtälöistä ratkaista), otetaan yritteeksi $(n^2p_n)_{n\geq 0}$, jne.

Esimerkki 18.5.3 Ratkaise rekursiokaava

$$a_{n+2} - 4a_{n+1} + 4a_n = 2^n, \quad n \geq 0.$$

Etsi se ratkaisu, jolle $a_0 = a_1 = 0$.

Ratkaisu. Vastaavan homogeeniyhtälön karakteristisella yhtälöllä

$$\alpha^2 - 4\alpha + 4 = (\alpha - 2)^2 = 0$$

on kaksoisjuuri $\alpha = 2$, joten yleinen ratkaisu on

$$h_n = A_1 2^n + A_2 n 2^n, \quad A_1, A_2 \in \mathbb{R}.$$

Epähomogeeniyhtälölle saataisiin taulukon perusteella yrite $p_n = D2^n$, mutta koska tämä – ja jopa $p_n = Dn2^n$ – on homogeeniyhtälön ratkaisu, tehdään yrite

$$p_n := Dn^2 2^n,$$

joka ei ole homogeeniyhtälön ratkaisu. Sijoitetaan yrite rekursiokaavaan

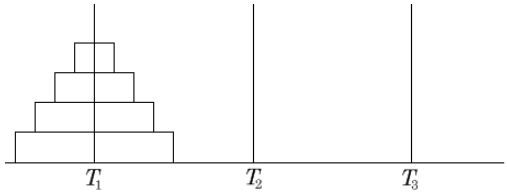
$$\begin{aligned}
p_{n+2} - 4p_{n+1} + 4p_n &= 2^n \\
D(n+2)^2 2^{n+2} - 4D(n+1)^2 2^{n+1} + 4Dn^2 2^n &= 2^n \\
D2^n \left(4(n+2)^2 - 8(n+1)^2 + 4n^2\right) &= 2^n \\
D2^n(4n^2 + 16n + 16 - 8n^2 - 16n - 8 + 4n^2) &= 2^n \\
8D2^n &= 2^n
\end{aligned}$$

Epähomogeeniyhtälön eräs ratkaisu on siis $e_n = 1/8\, n^2\, 2^n$. Tehtävän yleinen ratkaisu on siten $a_n = h_n + e_n$ eli

$$a_n = A_1 2^n + A_2 n 2^n + \frac{1}{8} n^2\, 2^n, \quad A_1, A_2 \in \mathbb{R}.$$

Alkuarvot $a_0 = a_1 = 0$ toteuttavaksi ratkaisuksi saadaan arvoilla $A_1 = 0$ ja $A_2 = -1/8$ jono

$$a_n = n(n-1)2^{n-3}.$$



Kuva 49: Hanoin kolme tornia

Esimerkki 18.5.4 (Hanoin tornit) On pystytetty kolme tankoa T_1, T_2 ja T_3. Tankoon T_1 on pinottu n kappaletta reiällisiä kiekkoja suuruusjärjestykseen suurin alimmaiseksi, ks. Kuva 49. Kiekkojen muodostama torni on siirrettävä tangosta T_1 tankoon T_2 niin, että suurempi kiekko ei ole koskaan pienemmän päällä. Apuna saa käyttää tankoa T_3.

Probleema. Kuinka pienellä siirtomäärällä a_n tehtävästä voidaan selviytyä?

Ratkaisu. Oletetaan, että tilanne on edennyt seuraavaan vaiheeseen: Tangossa T_1 on vain suurin kiekko n, tanko T_2 on tyhjä ja kaikki muut kiekot ovat suuruusjärjestyksessä tangossa T_3. Tähän on tarvittu a_{n-1} siirtoa. Nyt tarvitaan yksi siirto siirrettäessä suurin tankoon T_2 ja toiset a_{n-1} siirtoa, jotta $n-1$ kiekkoa saadaan tankoon T_2 suurimman päälle. Näin saadaan rekursiokaava

$$a_n = a_{n-1} + 1 + a_{n-1} = 2a_{n-1} + 1$$

alkuarvona $a_1 = 1$. Rekursiokaava on lineaarinen, vakiokertoiminen ja epähomogeeninen. Homogeeniyhtälön yleinen ratkaisu on

$$h_n = A2^n.$$

Vakiojono $p_n := D$ yritteenä saadaan yhtälö $p_n = D = 2D + 1$, josta $D = -1$. Epähomogeeniyhtälöllä on siis yhtenä ratkaisuna $e_n = -1$. Rekursiokaavan yleiseksi ratkaisuksi saadaan

$$a_n = A2^n - 1.$$

Vaaditun alkuehdon $a_1 = 1$ toteuttava ratkaisu on

$$a_n = 2^n - 1, \quad n \in \mathbb{N}.$$

Hanoin tornien ongelma voidaan siis ratkaista käyttäen enintään $2^n - 1$ siirtoa. Rekursiokaavan muodostamisesta selviää, että tämä on myös minimimäärä.

Viitteet

[1] Bavel, Z.: Math companion for computer science. – Reston Publishing Company, Reston, 1982.

[2] Levy, L.S.: Discrete structures of computer science. – John Wiley & Sons, New York, 1980.

[3] McEliece, R.J., Ash, R.B. ja C. Ash: Introduction to discrete mathematics. – McGraw-Hill, Singapore, 1989.

[4] Tucker, A.: Applied combinatorics. – John Wiley & Sons, New York, 1984.

[5] Wiitala, S.A.: Discrete mathematics - a unified approach. – McGraw-Hill, Singapore, 1987.

[6] Savolainen, V.: Verkkoteorian perusteet ja algoritmit. – Gaudeamus, Vaasa, 1978.

[7] Wilson, R.J.: Introduction to graph theory. – Longman, Whitstable, 1975.

[8] Harary, F. (toim.): New directions in the theory of graphs. – Academic Press, New York - London, 1973.

[9] Skiena, S.S: Implementing discrete mathematics: Combinatorics and graph theory with *Mathematica*. – Addison-Wesley, Redwood City, 1990.
Mathematica-ohjelmapaketti `Combinatorica.m`

[10] Savolainen, V.: Verkkoteoria. – Docendo Finland Oy, Jyväskylä, 2001.

[11] K. Appel ja W. Haken: The solution of the Four-Color-Map Problem. Scientific American, vol. 237, 1976.

Hakemisto