

# Diskreetti matematiikka II

Vesa Halava

Luentomoniste

Turun yliopisto  
Matematiikan laitos  
20014 Turku

2010

# Sisältö

<b>1 Rakenteellinen induktio ja rekursio</b>	<b>1</b>
1.1 Induktioperiaate . . . . .	1
1.2 Induktiiviset määrittelyt . . . . .	4
1.3 Joukkojen induktiiviset määritelmät . . . . .	6
1.4 Funktioiden induktiiviset määritelmät . . . . .	8
1.5 Rakenteellinen induktio . . . . .	9
1.6 Sovellus: Ohjelmien oikeellisuus* . . . . .	11
<b>2 Rekursiiviset lukujonot</b>	<b>16</b>
2.1 Palautuskaava . . . . .	16
2.2 II kertaluvun homogeenisen lineaarinen palautuskaava . . . . .	17
2.3 Epähomogeenisen lineaarisen palautuskaavan ratkaisu . . . . .	20
2.4 Sovellus: Matriisit ja rekursiot* . . . . .	22
<b>3 Boolean algebrat ja matriisit</b>	<b>24</b>
3.1 Boolean algebra . . . . .	24
3.2 Totuusfunktiot ja propositiot . . . . .	26
3.3 Boolean algebra ja osittainen järjestys . . . . .	30
3.4 Esityslause . . . . .	33
3.5 Boolean matriisit . . . . .	35
3.6 Sovellus: Relaation esitys Boolean matriisin avulla* . . . . .	39
<b>4 Kielet ja äärelliset automaattit</b>	<b>43</b>
4.1 Aakkosto, sana ja kieli . . . . .	43
4.2 Kielten operaatioita . . . . .	44
4.3 Säännölliset ilmaisut . . . . .	46
4.4 Epädeterministinen äärellinen automaatti . . . . .	48
4.5 Deterministinen äärellinen automaatti . . . . .	51
4.6 Deterministisen ja epädeterministisen automaatin ekvivalenssi . . . . .	53
4.7 Tunnistuvien kielten sulkeumaominaisuuksia . . . . .	57
4.8 Äärelliset automaattit ja säännölliset ilmaisut . . . . .	58
4.9 Epäsäännöllinen kieli . . . . .	61
4.10 Automaatin minimointi . . . . .	61

## Alkusanat

Diskreettiä matematiikkaa on vaikea määritellä. Siihen kuuluu osia monilta matematiikan eri aloilta kuten algebrasta, lukuteoriasta, kombinatoriikasta, logiikasta jne. Yleensä diskreettinä matematiikkana pidetään kaikkea matematiikkaa, joka käsittelee "epäjatkuvia" objekteja.

Tämä kurssi on tarkoitettu ensisijaisesti tietojenkäsittelytieteen opiskelijoille, ja siksi kaikki kurssilla käsiteltävät asiat liittyvät jollain lailla tietokoneisiin ja niillä suoritettuun laskentaan. Monta diskreetin matematiikan kulmakiveä jää tarkastelematta ja lukijaa kehoitetaan tutustumaan alla mainittuihin lähteisiin.

Luentomoniste perustuu seuraaviin lähteisiin:

A. Arnold and I. Guessarian, *Mathematics for computer science*, Prentice Hall, 1996.

N.L. Biggs, *Discrete Mathematics*, Oxford Science Publ., 1989.

B.W. Jackson and D. Thoro, *Applies Combinatorics with Problem Solving*, Addison-Wesley, 1990.

E. Jurvanen, *Diskreetti matematiikka*, Turun yliopisto, 2005.

J. Truss, *Discrete Mathematics for Computer Scientists*, 2nd edition, Addison-Wesley, 1999.

J.E. Whitesitt, *Boolean Algebra and Its Applications*, Addison-Wesley, 1961.

# 1 Rakenteellinen induktio ja rekursio

## 1.1 Induktioperiaate

Luonnollisten lukujen joukko voidaan määritellä induktiivisesti käyttämällä seuraavia **aksioomia** 1, 2 ja 3.

**Määritelmä 1.1.** Luonnollisten lukujen joukko  $\mathbb{N}$  toteuttaa seuraavat kolme ehtoa:

1.  $0 \in \mathbb{N}$ ,
2. jos  $n \in \mathbb{N}$ , niin  $n + 1 \in \mathbb{N}$ , ja
3. tässä ovat kaikki luonnolliset luvut.

Tarkastellaan seuraavaksi joukon  $\mathbb{N}$  luonnollista järjestystä  $\leq$ .

**Määritelmä 1.2.** Joukko  $X$ , jossa on määritelty järjestys  $\sqsubseteq$ , on **hyvin järjestetty**, jos sen jokaisella epätyhjällä osajoukolla on pienin alkio järjestyksen  $\sqsubseteq$  suhteen.

**Lemma 1.3.** *Luonnollisten lukujen joukko  $\mathbb{N}$  on hyvin järjestetty, kun käytetään järjestystä  $\leq$ .*

*Todistus.* Olkoon  $A$  on jokin joukon  $\mathbb{N}$  epätyhjä osajoukko. Tarkastellaan joukon  $\mathbb{N}$  alkioita suuruusjärjestyksessä ( $\leq$  mukaisesti). Ensimmäinen joukon  $\mathbb{N}$  alkio joka kuuluu joukkoon  $A$ , on pienin joukon  $A$  pienin alkio.  $\square$

Luonnollisten lukujen ominaisuuksia voidaan todistaa luonnollisten lukujen määritelmää käyttämällä. Merkitään  $P(n)$ , jos luonnollisella luvulla  $n \in \mathbb{N}$  on ominaisuus  $P$ . Lisäksi, jos  $P(n)$ , niin sanotaan, että  $P(n)$  **on voimassa**.

Kun halutaan todistaa, että jokaisella luonnollisella luvulla on ominaisuus  $P$ , voidaan käyttää matemaattista induktiota.

**Lause 1.4 (Ensimmäinen induktioperiaate).** *Jos on voimassa*

1.  $P(0)$  ja
2. jos  $P(n)$ , niin  $P(n + 1)$ ,

*niin silloin  $P(n)$  on voimassa kaikilla  $n \in \mathbb{N}$ .*

*Todistus.* Oletetaan, että ominaisuudelle  $P$  ehdot 1 ja 2 ovat voimassa. Olkoon

$$A = \{n \in \mathbb{N} \mid P(n) \text{ ei ole voimassa}\},$$

siis  $A$  on niiden luonnollisten lukujen joukko, joilla ei ole ominaisuutta  $P$ . Tehdään *vasta oletus*, että  $A$  on epätyhjä.

Koska  $\mathbb{N}$  on hyvinjärjestetty ja  $A$  on epätyhjä, on joukossa  $A$  pienin alkio, sanotaan  $k$ . Selvästi  $0 \notin A$ , sillä ehdon 1 mukaan  $P(0)$  on voimassa, joten  $k \neq 0$ . On siis olemassa luku  $k - 1 \in \mathbb{N}$ , jolle  $k - 1 \notin A$ , joten  $P(k - 1)$  on voimassa. Nyt ehdosta 2 seuraa, että  $P(k)$  on voimassa. Siis  $k \notin A$ , mutta tämä on ristiriidassa sen kanssa, että  $k$  on joukon  $A$  pienin alkio. Tehty vasta oletus on siis väärä, joten väite on tosi.  $\square$

Lauseen 1.4 ehtoa 1 eli ehtoa  $P(0)$  kutsutaan **induktion lähtökohdaksi** (induction basis) ja ehtoa 2 **induktioaskeleeksi**. Induktioaskeleessa on **induktio-oletus** (induction hypothesis)  $P(n)$  ja **induktioväite**  $P(n + 1)$ . Lauseen 1.4 mukaan siis luonnollisten lukujen ominaisuuksien  $P$  induktiotodistukset ovat tosia.

**Esimerkki 1.5.** Olkoon jonossa ääretön määrä ihmisiä. Jonon ensimmäiselle kerrotaan matemaattisen induktion periaate. Tiedetään, että jos joku ihmisistä tietää induktion periaatteen, hän kertoo sen seuraavalle jonossa. Tästä voidaan päätellä, että kaikki jonossa olevat tietävät aikanaan matemaattisen induktion periaatteen.

**Esimerkki 1.6.** Lapsi lähetetään ensimmäiselle luokalle. Tässä koulussa jokainen pääsee luokalta seuraavalle aina joka syksy ja luokkia on ääretön määrä. Induktion mukaan voimme päätellä, että lapsi tulee käyneeksi jokaisen luokan.

**Esimerkki 1.7.** Todistetaan kaava

$$\sum_{i=0}^n i = \frac{n(n+1)}{2}$$

induktiolla.

Tarkastellaan luonnollisen luvun  $n$  ominaisuutta  $P$ , jolle

$$P(n) \iff \sum_{i=0}^n i = \frac{n(n+1)}{2}.$$

Osoitetaan, että Lauseen 1.4 ehdot 1 ja 2 ovat voimassa ominaisuudelle  $P$ .

Induktion lähtökohta: Kun  $n = 0$ , niin  $\sum_{i=0}^0 i = 0 = \frac{0 \cdot 1}{2}$ .

Induktioaskel: Induktio-oletus on, että  $P(n)$  on voimassa ja induktio väite, että  $P(n + 1)$  on voimassa. Nyt

$$\begin{aligned} \sum_{i=0}^{n+1} i &= (n+1) + \sum_{i=0}^n i \stackrel{\text{i.o.}}{=} \frac{n(n+1)}{2} + n+1 \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \implies P(n+1). \end{aligned}$$

Jos halutaan todistaa jokin ominaisuus lukua  $n_0$  suuremmille luvuille, voidaan käyttää seuraavaa induktioperiaatteen muunnosta. Tässä muunnoksessa induktion lähtökohta on 0:n sijaan luku  $n_0$ .

**Lause 1.8.** *Jos jollekin  $n_0 \in \mathbb{N}$  on voimassa*

1.  $P(n_0)$  ja
2. jos  $n \geq n_0$  ja  $P(n)$ , niin  $P(n + 1)$ ,

*niin silloin  $P(n)$  on voimassa kaikilla  $n \geq n_0$ ,  $n \in \mathbb{N}$ .*

*Todistus.* Oletetaan ehdot 1 ja 2 ovat voimassa. Määritellään luonnollisten lukujen ominaisuus  $S$ , jolle

$$S(n) \quad \text{joss} \quad P(n + n_0)$$

kaikilla  $n \in \mathbb{N}$ . Osoitetaan induktioperiaatteen avulla, että  $S(n)$  on voimassa kaikilla  $n \in \mathbb{N}$ .

Induktion lähtökohta:  $S(0)$  on voimassa, sillä  $P(n_0)$  on voimassa ehdon 1 mukaan.

Induktioaskel: Oletetaan, että  $S(n)$  on voimassa mistä seuraa, että  $P(n + n_0)$  on voimassa. Koska  $n + n_0 \geq n_0$ , ehdon 2 nojalla myös  $P(n + 1 + n_0)$  on voimassa. Tästä taas seuraa ominaisuuden  $S$  määritelmän mukaan  $S(n + 1)$  on voimassa. Näin ollen on voimassa: jos  $S(n)$ , niin  $S(n + 1)$ .

Nyt Lauseen 1.4 mukaan  $S(n)$  kaikilla  $n \in \mathbb{N}$ . Ominaisuuden  $S$  määritelmän mukaan tästä seuraa, että  $P(n + n_0)$  kaikilla  $n \in \mathbb{N}$ , eli  $P(n)$  kaikilla  $n \geq n_0$ .  $\square$

Seuraavaksi käsittelemme ns. toista induktioperiaatetta, jossa ehto 2 on yleistetty siten, että induktioaskeleessa oletetaan ominaisuuden  $P$  olevan voimassa kaikille  $k \leq n$ .

**Lause 1.9** (Toinen induktioperiaate). *Jos on voimassa*

1.  $P(0)$  ja
2. jos  $P(0), P(1), \dots, P(n)$ , niin  $P(n + 1)$ ,

*niin silloin  $P(n)$  on voimassa kaikilla  $n \in \mathbb{N}$ .*

*Todistus.* Oletetaan, että ehdot 1 ja 2 ovat voimassa ominaisuudelle  $P$  ja määritellään ominaisuus  $S$  seuraavasti:

$$S(n) \quad \text{joss} \quad P(0), P(1), \dots \text{ ja } P(n).$$

Osoitetaan ensimmäisen induktioperiaatteen avulla, että kaikilla  $n \in \mathbb{N}$  on ominaisuus  $S$ .

Induktion lähtökohta:  $S(0)$  on voimassa, sillä nolllalla on ominaisuus  $P$  ehdon 1 mukaan.

Induktioaskel: induktio-oletus on nyt  $S(n)$ . Ominaisuuden  $S$  määritelmän mukaan  $P(0)$ ,  $P(1)$ ,  $\dots$  ja  $P(n)$  ovat voimassa. Lisäksi ehdon 2 nojalla nyt  $P(n+1)$  on voimassa, joten  $S(n+1)$  voimassa. Täten  $S(n)$  kaikilla  $n \in \mathbb{N}$ .

Koska  $S(n)$  on voimassa kaikille  $n \in \mathbb{N}$ , niin erityisesti myös  $P(n)$  kaikilla  $n \in \mathbb{N}$ .  $\square$

Myös toisessa induktioperiaatteessa ehdon 1 alkuarvon voidaan olettaa olevan yleisesti jokin luku  $n_0$ .

**Lause 1.10.** *Jos jollakin  $n_0 \in \mathbb{N}$  on voimassa*

1.  $P(n_0)$  ja

2. jos  $P(n_0)$ ,  $P(n_0 + 1)$ ,  $\dots$ ,  $P(n_0 + n)$ , niin  $P(n_0 + n + 1)$ ,

niin silloin  $P(n)$  on voimassa kaikilla  $n \geq n_0$ .

*Todistus.* Demonstraatiot.  $\square$

**Esimerkki 1.11.** Todistetaan toista induktioperiaatetta käyttäen, että jokainen ykköstä suurempi luonnollinen luku voidaan esittää alkulukujen tulona.

Olkoon  $n \in \mathbb{N}$  ja  $n \geq 2$ .

Induktion lähtökohta: jos  $n = 2$ , niin  $n$  on itse alkuluku ja voidaan esittää tulona, jossa on vain yksi tekijä.

Induktioaskel: olkoon  $n \geq 2$ . Induktio-oletus on nyt, että jokainen lukua  $n$  pienempi luku — ei vain  $n - 1$  — voidaan esittää alkulukujen tulona.

Jos  $n$  on itse alkuluku, se voidaan jälleen esittää alkulukujen tulona. Jos taas  $n$  on yhdistetty luku, niin  $n$  on kahden luvun tulo, eli  $n = n_1 n_2$ , missä  $n_1, n_2 \in \mathbb{N}$  ja  $1 < n_1, n_2 < n$ . Induktio-oletuksen mukaan

$$n_1 = p_1 p_2 \cdots p_r \quad \text{ja} \quad n_2 = q_1 q_2 \cdots q_s,$$

missä luvut  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$  ovat alkulukuja. Tällöin myös  $n$  on alkulukujen tulo  $n = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ , ja väite on todistettu kaikille luonnollisille luvuille  $n \geq 2$ .

## 1.2 Induktiiviset määrittelyt

Induktiivisessa määrittelyssä käsite  $S(n)$  määritellään rekursiivisesti / induktiivisesti jokaiselle  $n$ :n arvolle: ensin määritellään  $S(0), S(1), \dots, S(k)$  (**lähtökohta** tai **alkuarvot**) ja  $S(n+1)$  määritellään käyttäen hyväksi joitakin aiempia arvoja  $S(i)$ ,  $i < n+1$  (**induktioaskel** tai **rekursio**). Määriteltävä käsite voi olla vaikkapa joukko, luku, kuvaus.

**Esimerkki 1.12.** Kuvaus  $f : \mathbb{N} \rightarrow \mathbb{R}$  voidaan määritellä rekursiivisesti palauttamalla arvo  $f(n)$   $k$ :hon edelliseen arvoon,  $k \in \mathbb{N}$ , seuraavalla tavalla.

1. Määritellään  $f(0), f(1), \dots, f(k-1)$ .
2. Kun  $n \geq k$ , määritellään  $f(n)$  käyttäen hyväksi lukuja  $f(n-1), \dots, f(n-k)$ .

Algoritmia tai ohjelmaa taas sanotaan **rekursiiviseksi**, jos se kutsuu itseään (jollakin "pienemmällä" syötteellä).

**Esimerkki 1.13. Kertomafunktio**  $! : \mathbb{N} \rightarrow \mathbb{N}$  määritellään kaavoilla

$$\begin{aligned} 0! &= 1, \\ (n+1)! &= (n+1)n!. \end{aligned}$$

Se on muotoa  $f(0) = 1$  ja  $f(n+1) = (n+1)f(n)$ . On helppo osoittaa, että  $n! = 1 \cdot 2 \cdot \dots \cdot n$  kaikilla  $n \in \mathbb{N}$ .

**Esimerkki 1.14.** Määritellään lukujonon  $(a_n)_{n=0}^{\infty}$  seuraavasti:

$$\begin{aligned} a_0 &= 2, \\ a_{n+1} &= 3a_n + 2. \end{aligned}$$

Yhtälö  $a_{n+1} = 3a_n + 2$  kutsutaan **rekursioksi** tai **palautuskaavaksi** ja ehtoa  $a_0 = 2$  **alkuehdoksi**. Lukujonon **jäseniä** ovat  $a_0 = 2, a_1 = 8, a_2 = 26, \dots$ .

Lukujono on siis rekursiivisesti määritelty funktio  $f : \mathbb{N} \rightarrow \mathbb{N}$ , jossa  $f(n) = a_n$ . Määrittelyehdot ovat siis:  $f(0) = 2$  ja  $f(n+1) = 3f(n) + 2$ .

**Esimerkki 1.15.** Tarkastellaan ns. **Fibonaccin lukujonoa**  $(F_n)_{n=0}^{\infty}$ . Sen jäsentä  $F_n$  kutsutaan  $n$ :neksi **Fibonaccin luvuksi** ja se on aina kahden edellisen Fibonaccin luvun summa. Alkuehdot ovat  $F_0 = 0$  ja  $F_1 = 1$  (jossain yhteyksissä myös  $F_0 = 1$ ), ja saadaan siis määritelmä

$$\begin{aligned} F_0 &= 0, & F_1 &= 1, \\ F_{n+2} &= F_n + F_{n+1}. \end{aligned}$$

Lukujono alkaa  $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$ .

**Esimerkki 1.16.** Osoitetaan, että Fibonaccin luvuilla on seuraava ominaisuus:

$$F_{n+1} \leq \left(\frac{9}{5}\right)^n, \quad \text{kaikilla } n \in \mathbb{N}.$$

Koska Fibonaccin lukujonon määritelmässä on kaksi alkuarvoa, tarvitaan induktion lähtökohdassa kaksi ehtoa, mutta toisaalta induktioaskeleessa voidaan olettaa myös kaksi ehtoa.

Induktion lähtökohta: kun  $n = 0$ , niin  $F_1 = 1 \leq \left(\frac{9}{5}\right)^0 = 1$  ja, kun  $n = 1$ , niin  $F_2 = 1 \leq \left(\frac{9}{5}\right)^1 = \frac{9}{5}$ .

Induktioaskel: Induktio-oletus on  $F_{n+1} \leq \left(\frac{9}{5}\right)^n$  ja  $F_{n+2} \leq \left(\frac{9}{5}\right)^{n+1}$ .

Induktiotodistus:

$$\begin{aligned} F_{n+3} &= F_{n+2} + F_{n+1} \leq \left(\frac{9}{5}\right)^{n+1} + \left(\frac{9}{5}\right)^n \\ &= \left(\frac{9}{5} + 1\right) \left(\frac{9}{5}\right)^n = \frac{14}{5} \left(\frac{9}{5}\right)^n < \left(\frac{9}{5}\right)^2 \left(\frac{9}{5}\right)^n = \left(\frac{9}{5}\right)^{n+2}. \end{aligned}$$

**Esimerkki 1.17.** Olkoon  $A$  jokin joukko, jossa on määritelty assosiatiiivinen operaatio  $\circ : A \times A \rightarrow A$ . Olkoon lisäksi  $e \in A$  operaation  $\circ$  suhteen ns. neutraalialkio, eli  $e \circ a = a \circ e = a$  kaikilla  $a \in A$ . Nyt voidaan määritellä alkion  $a \in A$   $n$ :s **potenssi** kaavoilla

$$\begin{aligned} a^0 &= e, \\ a^{n+1} &= a^n \circ a. \end{aligned}$$

Voidaan osoittaa, että  $a^n = \overbrace{a \circ a \circ \dots \circ a}^{nkpl}$ . Selvästi myös  $a^1 = a$ . Induktiolla voidaan todistaa esimerkiksi kaavat  $a^m \circ a^n = a^{m+n}$  ja  $(a^m)^n = a^{mn}$ .

### 1.3 Joukkojen induktiiviset määritelmät

Tietojenkäsittelyssä monet tietorakenteet määritellään induktiivisesti tai rekursiivisesti. Silloin jokin osajoukko tai -relaatio määritellään antamalla ensin sen perusjoukko tai perusjoukon alkioita ja sitten (rekursiiviset/induktiiviset) tavat, joilla joukon alkioista muodostetaan uusia alkioita.

**Määritelmä 1.18. Joukon  $A$  induktiivinen määritelmä** on seuraavaa muotoa.

Joukko  $A$  on *pienin* sellainen joukko, että

1. (*lähtökohta*)  $B \subseteq A$  ( $B$  on ns. **perusjoukko**), ja
2. (*induktioaskel*)  $a \in A$ , jos  $a$  voidaan määritellä annetuilla tavoilla joidenkin jo joukossa  $A$  olevien alkioiden  $a_1, \dots, a_n$ ,  $n \geq 1$ , avulla.

Vaatimus, että  $A$  on pienin joukko, joka toteuttaa määritelmän ehdot, takaa, että jokainen joukon  $A$  alkio saadaan perusjoukon  $B$  alkioista eli ns. **perusalkioista** soveltamalla induktioaskelta äärellisen monta kertaa.

**Esimerkki 1.19.** Määritellään kolmella jaollisten lukujen joukko  $3\mathbb{N}$  induktiivisesti.  $3\mathbb{N}$  on joukon  $\mathbb{N}$  pienin osajoukko  $A$ , joka toteuttaa ehdot

1.  $0 \in A$ , ja
2. jos  $n \in A$ , niin  $n + 3 \in A$ .

Huomataan, että myös esim. joukot  $\mathbb{N}$ ,  $\mathbb{N} \setminus \{1\}$  ja  $\mathbb{N} \setminus \{1, 2\}$  toteuttavat ehdot 1 ja 2. Yksikäsitteisyys saavutetaan nyt vaatimalla, että  $A$  on *pienin* joukko, joka toteuttaa ehdot 1 ja 2.

**Esimerkki 1.20.** Olkoon  $\Sigma$  **äärellinen aakkosto** eli joukko **kirjaimia**. Aakkoston  $\Sigma$  **sana**  $u$  on äärellinen jono  $u = a_1 \cdots a_n$  aakkoston  $\Sigma$  kirjaimia, siis  $a_1, \dots, a_n \in \Sigma$ . Määritellään lisäksi ns. **tyhjä sana**  $\epsilon$ , joka on kaikkien aakkostojen sana, johon ei kuulu yhtään kirjainta.

Kaikkien aakkoston  $\Sigma$  sanojen joukkoa merkitään  $\Sigma^*$ :llä. Esimerkiksi jos  $\Sigma = \{a, b\}$ , niin  $\Sigma^* = \{\epsilon, a, b, aa, ab, ba, bb, aaa, aab, \dots\}$ . Määritellään joukolle  $\Sigma^*$  assosiatiivinen operaatio **yhdiste**, merk.  $\cdot$ , siten, että  $u \cdot v = uv$ . Toisin sanoen,  $u \cdot v$  saadaan kun sanat  $u$  ja  $v$  kirjoitetaan peräkkäin, esim.  $ab \cdot aab = abaab$ . Tyhjän sanan yhdistäminen sanaan  $u$  ei muuta sanaa  $u$ , sillä  $u\epsilon = \epsilon u = u$ .

Sanojen joukko  $\Sigma^*$  voidaan määritellä myös induktiivisesti. Määritellään joukko  $V$ , joka on pienin joukko, jolle

1.  $\epsilon \in V$ , ja
2. jos  $a \in \Sigma$  ja  $u \in V$ , niin  $au \in V$ .

Huomataan, että joukko  $V$  kuuluvat kaikki aakkoston  $\Sigma$  sanat, joten  $V = \Sigma^*$ .

**Esimerkki 1.21.** Olkoon  $E$  sellaisten lausekkeiden joukko, joiden osalausekkeet ovat aina suluisissa ja jotka muodostuvat joukon  $X = \{x_1, \dots, x_n\}$  muuttujista ja binäärisistä operaatioista  $+$  ja  $\times$  ja unaarisesta operaatiosta  $-$ . Silloin  $E$  on aakkoston  $X \cup \{+, \times, -, (, )\}$  sanojen pienin sellainen joukko, että

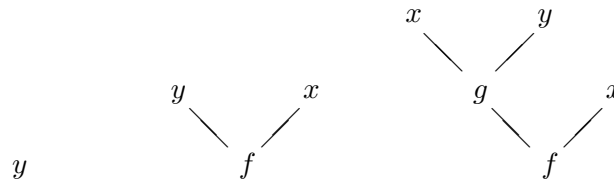
1.  $X \subseteq E$ , ja
2. jos  $e$  ja  $f \in E$ , niin  $(e + f)$ ,  $(e \times f)$  ja  $(-e) \in E$ .

Joukon  $E$  lausekkeita ovat siis esimerkiksi  $x_3$ ,  $(x_1 + (x_2 \times (-x_1)))$  ja  $(-(x_1 + x_2))$ .

**Esimerkki 1.22.** Tarkastellaan binääripuita, joiden jokaisessa jakautumiskohdassa on symboli  $f$  tai  $g$  ja jokaisessa lehdessä on symboli  $x$  tai  $y$ . Tällaisten binääripuiden joukko  $\text{Tree}$  on pienin joukko, jolle

1.  $x, y \in \text{Tree}$ , ja
2. jos  $t_1$  ja  $t_2 \in \text{Tree}$ , niin  $f(t_1, t_2)$  ja  $g(t_1, t_2) \in \text{Tree}$ .

Jokaisella binääripuulla on luonnollinen graafinen esitys. Kuvassa 1 on binääripuiden  $y$ ,  $f(y, x)$  ja  $f(g(x, y), x)$  esitykset.



Kuva 1: Binääripuut  $y$ ,  $f(y, x)$  ja  $f(g(x, y), x)$

### 1.4 Funktioiden induktiiviset määritelmät

Jos funktion lähtöjoukko on induktiivisesti määritelty, voidaan funktiokin määritellä induktiivisesti käyttäen hyväksi lähtöjoukon induktiivista rakennetta. Induktiivisten joukkojen ja funktioiden ominaisuuksia voidaan todistaa käyttäen rakenteellista induktiota, jota käsitellään seuraavassa kappaleessa. Tarkastellaan ensin kuitenkin funktioiden induktiivista määrittelyä.

**Määritelmä 1.23.** Olkoon  $A$  induktiivisesti määritelty joukko, jonka perusalkiot ovat joukossa  $B$ . Silloin **funktion**  $f : A \rightarrow C$  **induktiivinen määritelmä** joukkoon  $C$  on muotoa:

1. (*lähtökohta*) Määritellään  $f(b)$  kaikille  $b \in B$ .
2. (*induktioaskel*) Jos joukon  $A$  alkio  $a$  on määritelty alkioiden  $a_1, \dots, a_n \in A$  avulla, niin  $f(a)$  määritellään alkioiden  $f(a_1), \dots, f(a_n)$  avulla.

Koska jokainen joukon  $A$  alkio  $a$  joko on perusalkio ( $a \in B$ ) tai  $a$  on saatu rakentamalla muista (yksinkertaisemmista alkioista) niin funktio  $f$  tulee määritellyksi jokaiselle joukon  $A$  alkioille. Yksinkertaisempi tarkoittaa tässä, että alkion määrittelevät alkiot saadaan perusalkioista pienemmällä määrällä induktioaskelia kuin itse määriteltävä alkio.

**Esimerkki 1.24.** Määritellään joukossa  $3\mathbb{N}$  funktio  $f : 3\mathbb{N} \rightarrow \mathbb{Z}$  siten, että

1.  $f(0) = 2$  ja
2.  $f(n + 3) = f(n) + 2$ .

Nyt esim.  $f(3) = f(0) + 2 = 4$  ja  $f(6) = f(3) + 2 = 6$ .

**Esimerkki 1.25.** Määritellään ns. pituusfunktio aakkoston  $\Sigma$  sanoille (ks. esimerkki 1.20). Sanan  $w \in \Sigma^*$  **pituus**  $|w|$  on funktio  $|\cdot| : \Sigma^* \rightarrow \mathbb{N}$ , joka toteuttaa ehdot:

1.  $|\epsilon| = 0$ , ja
2. jos  $w = au$ , missä  $a \in \Sigma$  ja  $u \in \Sigma^*$ , niin  $|w| = 1 + |u|$ .

Pituusfunktion arvo on selvästi sanassa esiintyvien kirjainten lukumäärä. Esimerkiksi  $|abc| = 1 + |bc| = 1 + (1 + |c|) = 1 + (1 + (1 + |\epsilon|)) = 1 + (1 + (1 + 0)) = 3$ . Yleensä kirjallisuudessa pituusfunktio määritellään suoraan kirjainten lukumääränä.

**Esimerkki 1.26.** Määritellään vielä sanan peilisana. Sanan  $w \in \Sigma^*$  **peilisanana**  $w^R$  siten, että

1.  $\epsilon^R = \epsilon$ , ja
2.  $w^R = u^R a$ , jos  $w = au$ , missä  $a \in \Sigma$  ja  $u \in \Sigma^*$ .

Peilisanassa  $w^R$  sanan  $w$  kirjaimet ovat käänteisessä järjestyksessä. Esimerkiksi  $(abc)^R = (bc)^R a = c^R b a = cba$ .

**Esimerkki 1.27.** Tarkastellaan esimerkin 1.21 lausekkeiden joukkoa  $E$ . Määritellään funktio  $v$ , joka laskee lausekkeessa esiintyvien vasempien sulkujen määrän:

1.  $v(e) = 0$ , jos  $e \in X$ , ja
2.  $v(e+f) = 1+v(e)+v(f)$ ,  $v(e \times f) = 1+v(e)+v(f)$  ja  $v(-e) = 1+v(e)$ .

**Esimerkki 1.28.** Määritellään esimerkissä 1.22 määriteltyjen binääripuiden korkeusfunktio, kun binääripuun **korkeus** on määritellään puun pisimmän polun pituudeksi juuresta lehteen. (Polun pituus taas on polussa esiintyvien kaarien (viivojen) lukumäärä.) Binääripuun  $t$  korkeus  $h(t)$  on määritellään nyt induktiivisesti siten, että

1.  $h(t) = 0$ , jos  $t \in \{x, y\}$ , ja
2.  $h(t) = 1 + \max \{h(t_1), h(t_2)\}$ , jos  $t = f(t_1, t_2)$  tai  $t = g(t_1, t_2)$ .

Kuvan 1 puiden korkeudet ovat 0, 1 ja 2.

## 1.5 Rakenteellinen induktio

Rakenteellinen induktio on (induktio)todistusmenetelmä induktiivisesti määriteltyjen objektien (esim. joukkojen ja funktioiden) ominaisuuksien todistamiseen. Rakenteellisessa induktiossa induktioaskel perustuu suoraan käsiteltävän objektin määritelmän induktioaskeleeseen.

**Lause 1.29 (Rakenteellinen induktio).** *Olkoon joukon  $U$  osajoukko  $A$  induktiivisesti määritelty joukko, jonka perusalkiot ovat joukossa  $B$ . Ehdoista*

1.  $P(b)$  on voimassa kaikilla  $b \in B$ , ja
2. jos  $a \in A$  on määritelty alkioiden  $a_1, \dots, a_n \in A$  avulla ja  $P(a_1), \dots, P(a_n)$  ovat voimassa, niin  $P(a)$  on voimassa,

*seuraa, että  $P(a)$  on voimassa kaikilla  $a \in A$ .*

*Todistus.* Oletetaan, että joukon  $A$  alkiot toteuttavat ehdot 1 ja 2. Olkoon

$$Z = \{a \in U \mid P(a) \text{ on voimassa}\}$$

niiden joukon  $U$  alkioiden joukko, joilla on ominaisuus  $P$ . Osoitetaan, että ehdoista 1 ja 2 seuraa, että  $A \subseteq Z$  käyttäen joukon  $A$  induktiivista määritelmää, jolloin siis jokaisella joukon  $A$  alkiolla on ominaisuus  $P$ .

Jos  $a \in B$ , niin  $P(a)$  on voimassa ehdon 1 mukaan ja siten  $a \in Z$ .

Oletetaan siis, että  $a$  on määritelty alkioiden  $a_1, \dots, a_n \in A$  avulla. Tehdään vasta oletus, että  $a \notin A$ . Ehdon 2 nojalla  $P(a)$  on voimassa, jos  $a_i \in Z$  kaikilla  $i$ . Välttämättä siis jokin  $a_i \notin Z$ . Nyt taas  $a_i$  on välttämättä määritelty alkioiden  $a'_1, \dots, a'_n$  avulla, sillä jos  $a_i \in B$ , päädytään ristiriitaan ehdon 1 kanssa. Kuten edellä, ehdon 2 nojalla jokin  $a'_j \notin Z$ . Jatketaan päättelyä, kunnes päädytään tapaukseen, jossa alkio on määritelty perusjoukon  $B$  alkioiden avulla ja alkio ei kuulu joukkoon  $Z$ . Tämä on ristiriidassa ehdon 2 kanssa, koska  $B \subseteq Z$ . Siis välttämättä  $a \in Z$ .  $\square$

Lauseen 1.29 ehtoa 1 kutsutaan **induktion lähtökohdaksi** (induction basis) ja ehtoa 2 **induktioaskeleeksi**. **Induktio-oletus** (induction hypothesis) on nyt muotoa " $a \in A$  on määritelty alkioiden  $a_1, \dots, a_n \in A$  avulla ja  $P(a_1), \dots, P(a_n)$  ovat voimassa" ja **induktioväite**  $P(a)$ .

**Esimerkki 1.30.** Näytetään, että esimerkin 1.24 funktion  $f: 3\mathbb{N} \rightarrow \mathbb{N}$  arvo on aina parillinen. Tehdään se todistamalla rakenteellisella induktiolla, että joukon  $3\mathbb{N}$  jokaisella alkiolla  $n$  on ominaisuus  $f(n)$  on parillinen.

Induktion lähtökohta:  $f(0) = 2$  on parillinen.

Induktioaskel: induktio-oletus on, että  $n \in 3\mathbb{N}$  ja  $f(n)$  on parillinen. Väite seuraa, koska  $f(n+3) = f(n) + 2$  on selvästi parillinen.

**Esimerkki 1.31.** Osoitetaan, että peilisana-funktiolla on seuraava ominaisuus:  $(uv)^R = v^R u^R$ . Käytetään rakenteellista induktiota *sanan  $u$  suhteen*. Induktion lähtökohta:  $u = \epsilon$ . Silloin  $(uv)^R = (\epsilon v)^R = v^R$ . Toisaalta  $v^R u^R = v^R \epsilon^R = v^R \epsilon = v^R$ .

Induktio-oletus:  $u = au_1$ , missä  $a \in \Sigma$ , ja  $(u_1 v)^R = v^R u_1^R$ . Induktioväite on siis  $(uv)^R = v^R u^R$ .

Käyttämällä peilisanan määritelmän kohtaa 2 ja induktio-oletusta saadaan

$$(uv)^R = (au_1 v)^R \stackrel{\text{Määr.}}{=} (u_1 v)^R a \stackrel{\text{i.o.}}{=} v^R u_1^R a \stackrel{\text{Määr.}}{=} v^R (au_1)^R = v^R u^R.$$

Huomaa, että rakenteellinen induktio tehdään **sanan  $u$  suhteen**, ei sanan pituuden suhteen kuten tavallisella induktiolla.

**Esimerkki 1.32.** Määritellään esimerkissä 1.22 määriteltyjen binääripuiden **kooksi** symbolien  $f$ ,  $g$ ,  $x$  ja  $y$  esiintymien määrä puussa. Esimerkiksi puun  $f(x, y)$  koko on 3 ja puun  $g(f(x, x), x)$  koko on 5. Silloin binääripuun  $t$  koko  $k(t)$  on

1.  $k(t) = 1$ , jos  $t \in \{x, y\}$ , ja
2.  $k(t) = 1 + k(t_1) + k(t_2)$ , jos  $t = f(t_1, t_2)$  tai  $t = g(t_1, t_2)$ .

Esimerkin 1.28 funktio  $h : \text{Tree} \rightarrow \mathbb{N}$  ilmoitti puun korkeuden. Näytetään nyt, että puun koolla ja korkeudella on seuraava yhteys: kaikilla  $t \in \text{Tree}$  on voimassa

$$k(t) \leq 2^{h(t)+1} - 1.$$

Todistetaan väite rakenteellisella induktiolla.

Induktion lähtökohta: Jos  $t$  on lehti  $x$  tai  $y$ , niin  $k(t) = 1$  ja  $h(t) = 0$ . Silloin  $2^{h(t)+1} - 1 = 1$  ja väite pitää paikkansa.

Induktioaskel: Induktio-oletus on  $t = f(t_1, t_2)$  tai  $t = g(t_1, t_2)$  ja  $k(t_1) \leq 2^{h(t_1)+1} - 1$  ja  $k(t_2) \leq 2^{h(t_2)+1} - 1$ .

Induktioväite:  $k(t) \leq 2^{h(t)+1} - 1$  (kun  $t = f(t_1, t_2)$  tai  $t = g(t_1, t_2)$ ).

Induktiodistustus: Katsotaan ensin puun  $t = f(t_1, t_2)$  korkeutta, joka on määritelmän mukaan  $1 + \max\{h(t_1), h(t_2)\}$ . Puun  $t$  alipuut  $t_1$  ja  $t_2$  ovat joko yhtä korkeita tai sitten toinen, sanotaan  $t_2$ , on korkeampi. Siis  $h(t_1) \leq h(t_2)$ . Silloin  $\max\{h(t_1), h(t_2)\} = h(t_2)$ . Täten

$$\begin{aligned}
 k(t) &= 1 + k(t_1) + k(t_2) && \text{koon määritelmä} \\
 &\leq 1 + 2^{h(t_1)+1} - 1 + 2^{h(t_2)+1} - 1 && \text{induktio-oletukset} \\
 &= 2^{h(t_1)+1} + 2^{h(t_2)+1} - 1 \\
 &\leq 2^{h(t_2)+1} + 2^{h(t_2)+1} - 1 && h(t_1) \leq h(t_2) \\
 &= 2 \cdot 2^{h(t_2)+1} - 1 \\
 &= 2 \cdot 2^{\max\{h(t_1), h(t_2)\}+1} - 1 && h(t_1) \leq h(t_2) \\
 &= 2 \cdot 2^{h(t)} - 1 && \text{korkeuden määritelmä} \\
 &= 2^{h(t)+1} - 1.
 \end{aligned}$$

Todistus tapauksessa  $h(t_1) \geq h(t_2)$  sujuu vastaavasti, kuten myös puulle  $t = g(t_1, t_2)$

## 1.6 Sovellus: Ohjelmien oikeellisuus\*

Tarkastellaan esimerkkejä, miten induktiivisia todistuksia voidaan käyttää ohjelmien oikeellisuuden todistamiseksi. Oletetaan, että ohjelman mukana annetaan myös kuvailu, millaisia syötteitä sille oletetaan annettavaksi. Näitä syötteitä kutsutaan **oikeiksi** tai **laillisiksi** syötteiksi.

Ohjelma on **oikeellinen**, jos se on korrekti, täydellinen ja päättyvä. Ohjelma on **korrekti**, se laskee tuloksen annetuille kaikille laillisille syötöille oikein, ja se on **täydellinen**, jos se antaa vastauksen kaikille laillisille syötöille. Ohjelma on **päättyvä**, jos se päättyy kaikilla laillisilla syötöillä.

Tarkastellaan seuraavaa ohjelmaa `square`, joka laskee syötteenä saamansa kokonaisluvun  $a$  neliön  $a^2$ . Ohjelman laillisia syötteitä ovat siis kaikki kokonaisluvut.

```
PROGRAM square
  VAR a,b,c: integer
BEGIN
  READ a
  IF a < 0 THEN
    a := -a
  ENDIF
  b := a
  c := 0
  WHILE b <> 0 DO
    c := c + a
    b := b - 1
  ENDWHILE
  WRITE c
END
```

Liitetään ohjelman eri kohtiin väitelauseita, jotka ovat voimassa kohdan suorituksen jälkeen. Silmukoiden kohdalla käytetään induktiivista todistusta: näytetään, että

1. väite on voimassa, ennen kuin silmukkaan mennään ensi kerran,
2. väite on voimassa yhden silmukan suorituskierron jälkeen, jos se on ollut voimassa juuri ennen kierrosta.

Ensiksi näytämme, että ohjelma pysähtyy.

**Väite.** Ohjelma `square` päättyy.

*Todistus.* Riittää näyttää, että silmukka päättyy joskus. Toteamme seuraavat tosiasiat.

1. Ennen kuin silmukkaan mennään, muuttujassa  $b$  on positiivinen kokonaislukuarvo.
2. Muuttujan  $b$  arvo vähenee yhdellä jokaisella kierroksella. Siitä tulee nolla jossain vaiheessa.
3. Kun muuttujan  $b$  arvo on nolla, silmukasta poistutaan. □

Todistuksessa käytettiin hyväksi sitä luonnollisten lukujen ominaisuutta, ettei luvun arvo voi vähetä aidosti äärettömän kauan.

Seuraavaksi näytämme, että ohjelma on korrekti.

**Väite.** Ohjelma `square` on korrekti.

*Todistus.* Liitetään väitelause  $a^2 = c + ba$  kohtaan ennen silmukan ehdon tarkistusta. Indeksoidaan muuttujat niin, että  $x_n$  merkitsee muuttujan  $x$  arvoa silmukan  $n$ :nnen kierroksen jälkeen. Silloin  $a_0$  merkitsee muuttujan  $a$  arvoa juuri ennen silmukan suoritusta. Olkoon nyt  $P(n)$  ominaisuus  $a^2 = c_n + b_n a$  ja näytetään  $P(n)$  kaikille  $n \in \mathbb{N}$  induktiolla.

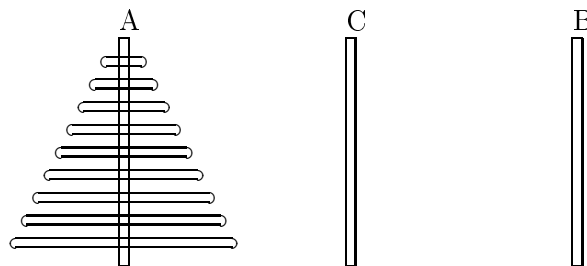
1. Aluksi alustetaan  $b_0 = a$  ja  $c_0 = 0$ , joten  $P(0)$  on voimassa.
2. Oletetaan  $P(n)$ . Täten  $a^2 = c_n + b_n a$ . Silmukan mukaan  $c_{n+1} = c_n + a$  ja  $b_{n+1} = b_n - 1$ . Tällöin  $c_{n+1} + b_{n+1} a = (c_n + a) + (b_n - 1)a = c_n + b_n a$ , joka on induktio-oletuksen mukaan yhtä suuri kuin  $a^2$ . Siis  $P(n + 1)$  on voimassa.

Kun silmukasta poistutaan kierroksella  $n$ , niin  $a^2 = c_n + b_n a$  ja  $b_n = 0$ . Siten  $a^2 = c_n$  ja ohjelma tulostaa oikean tuloksen  $a^2$ .  $\square$

**Väite.** Ohjelma **square** on täydellinen.

*Todistus.* Ohjelman lailliset syötöt ovat kokonaislukuja  $a$ . Jos  $a > 0$ , ohjelma toimii oikein. Negatiiviset syötöt korjataan ohjelman alussa positiivisiksi, mikä ei vaikuta tulokseen. Jos  $a = 0$ , silmukkaan ei mennä ja tulostetaan oikea arvo 0. Siten ohjelma on täydellinen.  $\square$

Tarkastellaan vielä rekursiivisen ohjelman oikeaksi todistamista. **Hanoin tornit** on peli, jossa on 3 tankoa:  $A$ ,  $B$  ja  $C$ , ja  $n$  erikokoista kiekkoa, jotka voidaan sijoittaa tankoihin. Aluksi kaikki kiekot ovat tangossa  $A$  kokonsa mukaan järjestyksessä suurin alimpana kuten kuvassa 2. Pelin tarkoituksena on siirtää kaikki kiekot tangosta  $A$  tankoon  $B$  niin, että suurempi kiekko ei koskaan joudu pienemmän päälle. Tankoa  $C$  voi käyttää väliasemana.



Kuva 2: Hanoin tornit ja kiekot

Ratkaisemme ongelman rekursiivisesti. Ensinnäkin jos kiekkoja on vain yksi, sen siirtämisessä ei ole ongelmaa. Toiseksi ratkaisu ei muutu oleellisesti, vaikka tangon  $B$  sijasta kiekot siirrettäisiin tankoon  $C$ . Oletetaan siis, että tiedämme, miten  $n$  kiekkoa siirretään tangosta toiseen, ja nyt pitäisi

siirtää  $n + 1$  kiekkoa. Jossain vaiheessa isoin kiekko on siirrettävä tangosta  $A$  tankoon  $B$ . Silloin tangossa  $B$  ei voi olla muita, pienempiä kiekkoja. Tietenkään muut kiekot eivät voi olla tangossa  $A$ . Silloin niiden on oltava tangossa  $C$ . Kun suurin kiekko on siirretty  $A$ :sta  $B$ :hen, pienemmät kiekot on siirrettävä tangosta  $C$  tankoon  $B$ . Saamme siis menetelmän, jossa

- $n$  ylintä kiekkoa siirretään  $A$ :sta  $C$ :hen,
- alin kiekko siirretään  $A$ :sta  $B$ :hen,
- $n$  ylintä kiekkoa siirretään  $C$ :sta  $B$ :hen.

Kirjoitetaan menetelmän mukaan rekursiivinen algoritmi  $\text{HANOI}(n, x, y)$ , jossa  $n \in \mathbb{N}_+$  on kiekkojen määrä ja  $x, y \in \{A, B, C\}$  ovat tankoja,  $x \neq y$ . Jäljelle jäävää tankoa merkitään  $z$ :lla. Tarkoitus on, että  $\text{HANOI}(n, x, y)$  siirtää ylimmät  $n$  kiekkoa tangosta  $x$  tankoon  $y$  noudattaen pelin sääntöjä. Ohjelma on

```

HANOI(1, x, y):   siirrä ylin kiekko x:stä y:hyn
HANOI(n+1, x, y): HANOI(n, x, z)
                  HANOI(1, x, y)
                  HANOI(n, z, y)

```

Keskimmäinen askel on annettu HANOI-kutsuna, vaikka se on yhden askeleen päässä varsinaisesta suorituksesta.

Todistetaan nyt algoritmin oikeellisuus käyttämällä induktiota.

**Väite.**  $\text{HANOI}(n, x, y)$  on korrekti.

*Todistus.* Näytämme siis, että pelin sääntöjä noudatetaan ja että kiekot siirtyvät  $x$ :stä  $y$ :hyn.

Jos  $n = 1$ , niin pienin kiekko siirretään  $x$ :stä  $y$ :hyn, eikä se joudu isompien kiekkojen alle.

Oletetaan sitten, että  $\text{HANOI}(n, u, v)$  osaa siirtää  $n$  ylintä kiekkoa oikein mistä tahansa tangosta  $u$  toiseen tankoon  $v$ . Nyt algoritmissa  $\text{HANOI}(n+1, x, y)$  on kolme osaa, joista ensimmäisessä ja viimeisessä siirretään  $n$  ylintä kiekkoa niin, ettei isompi joudu pienemmän päälle. Suurinta kiekkoa siirretään vain keskiosassa, ja silloin tanko  $y$  on tyhjä, sillä induktio-oletuksen mukaan pienemmät kiekot ovat tangossa  $z$ . Lopuksi pienemmät kiekot siirretään  $y$ :hyn, joten kaikki kiekot tulevat siirretyiksi oikeaan tankoon, vieläpä noudattaen pelin sääntöjä.  $\square$

**Väite.**  $\text{HANOI}(n, x, y)$  päättyy.

*Todistus.* Osoitamme itse asiassa vahvemman tuloksen, nimittäin että algoritmin  $\text{HANOI}(n, x, y)$  suoritus vie täsmälleen  $2^n - 1$  askelta.

Jos  $n = 1$ , niin pienin kiekko siirretään, tapahtuu yksi askel ja  $1 = 2^1 - 1$ . Oletetaan, että  $\text{HANOI}(n, u, v)$  päättyy  $2^n - 1$  askeleella. Silloin algoritmin  $\text{HANOI}(n+1, x, y)$  askelien määrä on

$$(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1. \quad \square$$

Kun lisäksi toteamme, että algoritmi on täydellinen: se on määritelty kaikille positiivisille kokonaisluvuille  $n \in \mathbb{N}_+$  ja tangoille  $x, y \in \{A, B, C\}$ ,  $x \neq y$ , niin algoritmi on todistettu oikeelliseksi.

Tavallisesti algoritmeja tai ohjelmia ei näytetä optimaalisiksi, mutta näin yksinkertaiselle algoritmille sekin onnistuu.

**Väite.**  $\text{HANOI}(n, x, y)$  on optimaalinen.

*Todistus.* Osoitetaan nyt, ettei  $\text{HANOI}(n, x, y)$  voi ottaa vähempää kuin  $2^n - 1$  askelta.

Jos  $n = 1$ , niin vähintään yksi askel on tehtävä. Oletetaan, että algoritmin  $\text{HANOI}(n, u, v)$  suorittamiseksi on otettava  $2^n - 1$  askelta. Algoritmin  $\text{HANOI}(n+1, x, y)$  on ainakin siirrettävä isoin kiekko tangosta  $x$  tankoon  $y$ . Sitä ennen pienemmät kiekot on siirrettävä alta pois tankoon  $z$  ja sen jälkeen tangosta  $z$  tankoon  $y$ . Kaiken kaikkiaan askelien määrä on jälleen vähintään  $(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$ .  $\square$

## 2 Rekursiiviset lukujonot

Tässä luvussa tarkastellaan lukujonoja ja niiden jäsenten esityksiä. Esimerkeissä tarkasteltavat lukujonot ovat kokonaislukujonoja, mutta koska teoria yleistyy kompleksilukujonoille ja toisaalta kompleksilukuja tarvitaan kokonaislukujononkin ratkaisussa, oletetaan, että jonot ovat kompleksilukujonoja.

### 2.1 Palautuskaava

Olkoon  $(u_n)_{n=0}^{\infty}$  jokin lukujono. Yhtälöä

$$u_{n+k} = h(u_{n+k-1}, u_{n+k-2}, \dots, u_n, n),$$

jonka jonon  $(u_n)_{n=0}^{\infty}$  jäsenet toteuttavat, kutsutaan jonon **palautuskaavaksi** tai **rekursioksi**.  $h$  on kuvaus joukkoon  $\mathbb{C}$ , se saa argumentteikseen jononjäseniä ja luvun  $n$ . Jononjäsenet lausutaan siis  $k$  edellisen jäsenen funktiona. Jäseniä  $u_0, u_1, \dots, u_{k-1}$  kutsutaan **alkuehdoiksi**. Käytetään jonosta  $(u_n)_{n=0}^{\infty}$  yksinkertaisesti merkintää  $(u_n)$ , jos sekaannuksen vaaraa ei ole.

Palautuskaava on **lineaarinen**, jos  $h$  on lineaarinen (ensimmäistä astetta) jäsenten  $u_i$  suhteen ja **vakiokertoiminen**, jos funktiossa  $h$  jäsenten  $u_i$  kertoimet ovat vakioita. Usein lineaarinen vakiokertoiminen palautuskaava annetaan muodossa

$$\begin{cases} u_0 = b_0, u_1 = b_1, \dots, u_{k-1} = b_{k-1}, \\ u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \dots + a_k u_n + f(n) \end{cases} \quad (n \geq 0), \quad (1)$$

missä  $a_i \in \mathbb{C}$  kaikilla  $1 \leq i \leq k$ ,  $a_k \neq 0$  ja  $f: \mathbb{N} \rightarrow \mathbb{C}$  on funktio. Tällöin sanotaan, että palautuskaava on **kertalukua  $k$** . Palautuskaava on **homogeeninen**, jos  $f(n) = 0$  (kaikilla  $n$ ). Sanotaan, että funktio  $g: \mathbb{N} \rightarrow \mathbb{C}$  on palautuskaavan **ratkaisu**, jos  $u_n = g(n)$  kaikille  $n \in \mathbb{N}$ .

Joskus palautuskaava (1) esitetään muodossa

$$\begin{cases} u_0 = b_0, u_1 = b_1, \dots, u_{k-1} = b_{k-1}, \\ u_n = a_1 u_{n-1} + a_2 u_{n-2} + \dots + a_k u_{n-k} + f_2(n) \end{cases} \quad (n \geq k). \quad (2)$$

Huomaa, että  $f_2(n) = f(n-k)$ , ts. epähomogeeninen osa on muuttunut.

**Esimerkki 2.1.** Olkoon  $a_n$  sellaisten  $n$ -pituisten binäärilukujen lukumäärä, joissa ei ole kahta peräkkäistä nollaa. Etsi jonolle  $(a_n)$  palautuskaava.

Tarkastellaan homogeenista palautuskaavaa

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \dots + a_k u_n, \quad (3)$$

missä  $a_k \neq 0$ .

**Määritelmä 2.2.** Palautuskaavan (3) **karakteristinen yhtälö** on

$$x^k - a_1x^{k-1} - a_2x^{k-2} - \dots - a_{k-1}x - a_k = 0 \quad (4)$$

Karakteristisen yhtälön ratkaisuja  $r_1, r_2, \dots, r_k (\in \mathbb{C})$  kutsutaan **karakteristisiksi juuriksi**. Huomaa, että  $a_k \neq 0$ , joten 0 ei voi olla karakteristinen juuri. Karakteristisen yhtälön (4) polynomia kutsutaan joskus jono **karakteristiseksi polynomiksi**.

Jokaisella rekursiolla on useita ratkaisuja, jos alkuehtoja ei oteta huomioon. Rekursion **yleisellä ratkaisulla** tarkoitetaan ratkaisua, jossa alkuehtoja ei oteta huomioon vaan vakiokertoimet ovat muuttujia ja rekursion jokainen ratkaisu voidaan esittää ratkaisemalla nämä kertoimet alkuehdoista.

## 2.2 II kertaluvun homogeenisen lineaarinen palautuskaava

Toisen kertaluvun homogeeninen lineaarinen palautuskaava on muotoa

$$\begin{cases} u_0 = c_0, u_1 = c_1, \\ u_{n+2} = a_1u_{n+1} + a_2u_n \end{cases} \quad (n \geq 0), \quad (5)$$

missä  $a_1, a_2, c_0, c_1 \in \mathbb{C}$ . Olkoot  $\alpha$  ja  $\beta$  karakteristisen yhtälön

$$x^2 - a_1x - a_2 = 0. \quad (6)$$

juuret. Jonon  $(u_n)$  ratkaisut tiedetään seuraavan lauseen perusteella.

**Lause 2.3.** *Olkoon  $(u_n)$  kuten edellä. Silloin*

(i) *jos  $\alpha \neq \beta$ , niin*

$$u_n = a\alpha^n + b\beta^n$$

*kaikille  $n \geq 0$ , missä  $a = \frac{c_1 - c_0\beta}{\alpha - \beta}$  ja  $b = \frac{c_1 - c_0\alpha}{\beta - \alpha}$*

(ii) *jos  $\alpha = \beta$ , niin*

$$u_n = (cn + d)\alpha^n$$

*kaikille  $n \geq 0$ , missä  $d = c_0$  ja  $c = \frac{c_1 - c_0\alpha}{\alpha}$ .*

*Todistus.* Todistetaan ensin tapaus (i) toisella induktioperiaatteella.

Induktion lähtökohta: Kun  $n = 0$ ,

$$\begin{aligned} a\alpha^n + b\beta^n &= a + b = \frac{c_1 - c_0\beta}{\alpha - \beta} + \frac{c_1 - c_0\alpha}{\beta - \alpha} = \frac{c_1 - c_0\beta - c_1 + c_0\alpha}{\alpha - \beta} \\ &= c_0 \frac{-\beta + \alpha}{\alpha - \beta} = c_0, \end{aligned}$$

ja kun  $n = 1$

$$\begin{aligned} a\alpha^n + b\beta^n &= a\alpha + b\beta = \frac{c_1 - c_0\beta}{\alpha - \beta}\alpha + \frac{c_1 - c_0\alpha}{\beta - \alpha}\beta = \frac{c_1\alpha - c_0\beta\alpha - c_1\beta + c_0\alpha\beta}{\alpha - \beta} \\ &= c_1 \frac{\alpha - \beta}{\alpha - \beta} = c_1, \end{aligned}$$

joten induktion lähtökohta on kunnossa.

Induktioaskel: Induktio-oletus on nyt, että  $u_n = a\alpha^n + b\beta^n$  ja  $u_{n+1} = a\alpha^{n+1} + b\beta^{n+1}$ . Nyt

$$\begin{aligned} u_{n+2} &= a_1u_{n+1} + a_2u_n = a_1(a\alpha^{n+1} + b\beta^{n+1}) + a_2(a\alpha^n + b\beta^n) \\ &= (a_1\alpha + a_2)a\alpha^n + (a_1\beta + a_2)b\beta^n = a\alpha^{n+2} + b\beta^{n+2}, \end{aligned}$$

koska  $\alpha$  ja  $\beta$  ovat yhtälön (6) juuria, ts.  $a_1\alpha + a_2 = \alpha^2$  ja  $a_1\beta + a_2 = \beta^2$ .

Tapaus (ii) todistetaan myös induktiolla.

Induktion lähtökohta: Kun  $n = 0$  on  $(cn + d)\alpha^n = d = c_0$ . Kun  $n = 1$  on

$$(cn + d)\alpha^n = (c + d)\alpha = c_1 - c_0\alpha + c_0\alpha = c_1.$$

Induktioaskel: Induktio-oletus on  $u_n = (cn + d)\alpha^n$  ja  $u_{n+1} = (c(n + 1) + d)\alpha^{n+1}$ . Koska  $\alpha = \beta$ , tiedetään, että  $(x - \alpha)^2 = x^2 - 2\alpha x + \alpha^2 = x^2 - a_1x - a_2$ , josta taas seuraa, että  $a_1 = 2\alpha$  ja  $a_2 = -\alpha^2$ . Nyt

$$\begin{aligned} u_{n+2} &= a_1u_{n+1} + a_2u_n = a_1(c(n + 1) + d)\alpha^{n+1} + a_2(cn + d)\alpha^n \\ &= 2\alpha(c(n + 1) + d)\alpha^{n+1} - \alpha^2(cn + d)\alpha^n = (2c(n + 1) + 2d - cn - d)\alpha^{n+1} \\ &= (c(n + 2) + d)\alpha^{n+2}. \end{aligned}$$

Väitteet seuraavat nyt induktioperiaatteen nojalla. □

Käytännössä kertoimet  $a$  ja  $b$  kannattaa ratkaista yksinkertaisesta yhtälöryhmästä kuten seuraavassa esimerkissä.

**Esimerkki 2.4. Fibonaccin luvut**  $F_i$  voidaan määritellä palautuskaavalla

$$\begin{cases} F_0 = 0, F_1 = 1, \\ F_{n+2} = F_{n+1} + F_n \end{cases} \quad (n \geq 0).$$

Lukujono alkaa siis 0, 1, 1, 2, 3, 5, 8, 13, 21, ... . Ratkaistaan Fibonaccin lukujen palautuskaava.

Karakteristinen yhtälö on  $x^2 - x - 1 = 0$ , jonka juuret ovat

$$r_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Yleinen ratkaisu on

$$F_n = a \cdot \left(\frac{1 + \sqrt{5}}{2}\right)^n + b \cdot \left(\frac{1 - \sqrt{5}}{2}\right)^n.$$

## 2.2 II kertaluvun homogeenisen lineaarinen palautuskaava 19

---

Sijoitetaan yleiseen ratkaisuun  $n = 0$  ja  $n = 1$ , jolloin alkuehtojen avulla saadaan yhtälöryhmä

$$\begin{cases} a + b = 0 \\ a \cdot \frac{1 + \sqrt{5}}{2} + b \cdot \frac{1 - \sqrt{5}}{2} = 1 \end{cases}$$

josta kertoimet  $a$  ja  $b$  ratkaistaan. Saadaan, että  $a = \frac{1}{\sqrt{5}}$  ja  $b = -\frac{1}{\sqrt{5}}$ . Nyt

$$F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right).$$

**Esimerkki 2.5.** Ratkaise rekursio  $u_n = 2u_{n-1} - u_{n-2}$ ,  $u_0 = 1$  ja  $u_1 = 2$ .

Kertalukua  $k$  olevien lineaaristen homogeenisten palautuskaavojen ratkaisulle esitetään seuraava lause. Karakteristisen juuren  $r_i$  **kertaluku** on  $j_i$ , jos  $r_i$  on karakteristisen yhtälön  $j_i$  kertainen juuri. Esimerkiksi Lauseen 2.3 tapauksessa (ii) karakteristisen juuren  $\alpha$  kertaluku on kaksi, kun taas kohdassa (i) molempien karakteristen juurien kertaluku on yksi.

**Lause 2.6.** *Olkoot  $r_1, r_2, \dots, r_m$  rekursioon karakteristisen yhtälön erisuuret juuret,  $r_i$  kertalukua  $j_i$ , kaikilla  $1 \leq i \leq m$ , ja  $j_1 + j_2 + \dots + j_m = k$ . Tällöin rekursioon yleinen ratkaisu on*

$$\begin{aligned} u_n &= c_{11}r_1^n + c_{12}nr_1^n + \dots + c_{1j_1}n^{j_1-1}r_1^n + \dots + c_{m1}r_m^n + \dots + c_{mj_m}n^{j_m-1}r_m^n \\ &= \sum_{i=1}^m \sum_{\ell=1}^{j_i} c_{i\ell} n^{\ell-1} r_i^n. \end{aligned}$$

*Todistus.* Sivutetaan □

Homogeenisen lineaarisen vakiokertoimisen palautuskaavan ratkaisu löydetään karakteristen juurten avulla. Käytännössä, kun kertaluku on riittävän suuri, ongelmaksi muodostuu näiden juurien löytäminen.

Edellinen lause antaa myös menetelmän rekursioon yksittäisen ratkaisun etsimiseen, kun alkuehdot tunnetaan. Silloin kertoimet  $c_i$  löydetään ratkaisemalla yhtälöryhmä, joka muodostetaan alkuehdoista.

**Esimerkki 2.7.** Etsi yleinen ratkaisu rekursiolle  $u_n = 5u_{n-1} - 6u_{n-2} - 4u_{n-3} + 8u_{n-4}$ .

Rekursioon karakteristinen yhtälö on  $x^4 - 5x^3 + 6x^2 + 4x - 8 = 0$ , jonka juuret ovat  $-1$  ja  $2$ , nimittäin  $x^4 - 5x^3 + 6x^2 + 4x - 8 = (x - 2)^3(x + 1)$ . Yleinen ratkaisu on siis

$$u_n = c_1 2^n + c_2 n 2^n + c_3 n^2 2^n + c_4 (-1)^n.$$

**Esimerkki 2.8.** Ratkaise rekursio  $u_0 = 1$ ,  $u_1 = 0$ ,  $u_2 = 1$ , ja  $u_{n+3} = -2u_{n+2} + u_{n+1} + 2u_n$ , kun  $n \geq 0$ .

**Esimerkki 2.9.** Ratkaise Esimerkin 2.1 palautuskaava.

**Esimerkki 2.10.** Ratkaise rekursio  $u_n = 2u_{n-1} - u_{n-2} + 2u_{n-3}$ ,  $u_0 = 3$ ,  $u_1 = 2$  ja  $u_2 = 2$ .

### 2.3 Epähomogeenisen lineaarisen palautuskaavan ratkaisu

Tarkastellaan nyt epähomogeenisen lineaarisen vakiokertoimisen palautuskaavan

$$\begin{cases} u_0 = b_0, u_1 = b_1, \dots, u_{k-1} = b_{k-1}, \\ u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \dots + a_k u_n + f(n) \end{cases} \quad (n \geq 0), \quad (7)$$

määrittelemää lukujonoa  $(u_n)_{n=0}^{\infty}$ . Palautuskaavan (7) **homogeeninen osa** on

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \dots + a_k u_n. \quad (8)$$

**Lemma 2.11.** *Jos jonot  $(x_n)$  ja  $(y_n)$  toteuttavat palautuskaavan (7) (siis ilman alkuehtoja), niin jono  $(x_n - y_n)$  toteuttaa homogeenisen lineaarisen palautuskaavan (8).*

*Todistus.* Sivutetaan □

Edellinen lemma siis tarkoittaa, että kun on löydetty yksi epähomogeenisen rekursioon ratkaisu, muut ratkaisut poikkeavat siitä vain homogeenisen osan ratkaisulla. Toisin sanoen, epähomogeeninen lineaarinen palautuskaava voidaan ratkaista seuraavalla tavalla:

- (i) Etsi jokin **yksittäisratkaisu**.
- (ii) Etsi homogeenisen osan yleinen ratkaisu.
- (iii) Yhdistä kaksi edellistä ja ratkaise kertoimet alkuehdoista.

Kohdat (ii) ja (iii) ovat jo tuttuja juttuja, tarkastellaan nyt yksittäisratkaisun etsimistä tapauksissa, joissa  $f(n)$  on polynomi tai eksponenttifunktio. Yksittäisratkaisu etsitään (kuten differentiaaliyhtälöissä) ratkaisemalla ns. **yrite**.

#### $f(n)$ on polynomi

Jos  $f(n)$  on astetta  $m$  oleva polynomi, yrite on myös  $m$ -asteinen polynomi, jonka kertoimet ratkaistaan ns. määräämättömien kertoimien menetelmällä sijoittamalla se palautuskaavaan.

**Esimerkki 2.12.** Etsi rekursion  $a_n = a_{n-1} + a_{n-2} + 2n$  yksittäisratkaisu.

Koska  $f(n) = 2n$  on astetta yksi oleva polynomi, yrite on siis  $p(n) = bn + c$ . Nyt sijoitetaan  $p(n)$  rekursioon, saadaan

$$bn + c = (b(n-1) + c) + (b(n-2) + c) + 2n \iff -bn + (3b - c) = 2n$$

mistä saadaan, että  $b = -2$  ja  $c = -6$ , joten yksittäisratkaisu on  $p(n) = -2n - 6$ .

**Esimerkki 2.13.** Ratkaise rekursio  $a_n = a_{n-1} + 2a_{n-2} - 4$ ,  $a_0 = 6$  ja  $a_1 = 7$ .

Yrite on  $p(n) = d$ , koska  $f(n)$  on vakio. Sijoittamalla saadaan

$$d = d + 2d - 4 \iff d = 2,$$

joten  $p(n) = 2$ . Homogeenisen osan  $a_n = a_{n-1} + 2a_{n-2}$  yleinen ratkaisu on  $a'_n = b(-1)^n + c2^n$ . Rekursion ratkaisu on siis  $a_n = b(-1)^n + c2^n + 2$ . Kertoimet  $b$  ja  $c$  ratkaistaan nyt alkuehdoista ja saadaan

$$a_n = (-1)^n + 3 \cdot 2^n + 2.$$

### $f(n)$ on eksponenttifunktio

Jos  $f(n) = b \cdot r^n$ , niin yrite on  $p(n) = c \cdot r^n$ . Jos  $r$  on homogeenisen osan karakteristisen yhtälön juuri, niin tämä yrite ei toimi. Voidaan osoittaa, että jos  $r$  on  $m$ -kertainen karakteristinen juuri, niin jono  $v_n = cn^m r^n$  on yksittäisratkaisu jollakin  $c \in \mathbb{C}$ , ts. yrite on  $p(n) = cn^m r^n$ .

**Esimerkki 2.14.** Ratkaise rekursio  $u_n = u_{n-1} + 6u_{n-2} + 2^n$ ,  $u_0 = 0$  ja  $u_1 = 1$ .

Yrite on  $p(n) = c \cdot 2^n$  ja homogeenisen osan karakteristinen yhtälö on  $x^2 - x - 6 = 0$ , joten karakteristiset juuret ovat  $-2$  ja  $3$ . Saadaan, että ratkaisu on muotoa

$$u_n = a \cdot (-2)^n + b \cdot 3^n + c \cdot 2^n.$$

Kertoimet voidaan ratkaista alkuehdoista, kun vielä huomataan, että  $u_2 = 5$ . Saadaan, että

$$u_n = 3^n - 2^n.$$

Huomaa, että tässä yrite ja itse rekursio ratkaistiin samalla kertaa. Jos yrite on väärä, vastauskin on väärä, siksi yrite kannattaa ratkaista ensin.

**Esimerkki 2.15.** Ratkaise rekursio  $u_n = 4u_{n-1} - 4u_{n-2} + 2^n$ ,  $u_0 = 1$ ,  $u_1 = -1$ .

**Esimerkki 2.16.** Ratkaise rekursio  $u_n = 3u_{n-1} - 4n + 3 \cdot 2^n$ ,  $u_0 = 4$ .

**Esimerkki 2.17.** Tasossa on  $n$  suoraa, jotka kaikki leikkaavat toisensa, mutta mitkään kolme eivät leikkaa samassa pisteessä. Kuinka moneen osaan taso on jaettu?

## 2.4 Sovellus: Matriisit ja rekursiot\*

Tässä pykälässä esitetään homogeenisen lineaarisen vakiokertoimisen rekursion ja matriisien välinen yhteys.

Tarkastellaan  $n \times n$ -(neliö)matriiseja, joiden alkiot ovat kompleksilukuja ja merkitään näiden matriisien joukkoa  $\mathbb{C}^{n \times n}$ . Palautetaan aluksi mieleen muutamia matriisien peruskäsitteitä.

Matriisi

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}_{n \times n}$$

on ns. **identiteetti matriisi**.

Olkoon  $A \in \mathbb{C}^{n \times n}$ . Matriisin  $A$  **ominaisarvo**  $\lambda \in \mathbb{C}$  ja **ominaisvektori**  $\mathbf{x} \in \mathbb{C}^n$ ,  $\mathbf{x} \neq (0, \dots, 0)$ , toteuttavat yhtälön

$$A\mathbf{x}^T = \lambda\mathbf{x}^T, \quad (9)$$

missä  $\mathbf{x}^T$  on vektorin  $\mathbf{x}$  transpoosi (ts.  $\mathbf{x}$  pystyvektorina).

Yhtälö (9) voidaan kirjoittaa muotoon

$$(A - \lambda I)\mathbf{x}^T = \mathbf{0}^T.$$

Tämä taas voidaan tutkia yhtälö(ryhmä)nä, jolla on epätriviaali ratkaisu  $\mathbf{x}^T$  silloin ja vain silloin, kun

$$\det(A - \lambda I) = 0.$$

Tätä yhtälöä kutsutaan matriisin  $A$  **karakteristiseksi yhtälöksi**. Yhtälön vasenta puolta kutsutaan **karakteristiseksi polynomiksi**, merkitään matriisin  $A$  karakteristista polynomia  $c_A(\lambda)$ :lla (tässä  $\lambda$  on muuttuja),

$$c_A(\lambda) = (-1)^n(\lambda^n + c_1\lambda^{n-1} + \dots + c_n).$$

Karakteristinen polynomi on astetta  $n$ , jos  $A \in \mathbb{C}^{n \times n}$ , ja kertoimet  $c_i \in \mathbb{C}$ . Jos  $z \in \mathbb{C}$  on  $A$ :n ominaisarvo, niin siis  $c_A(z) = 0$ .

Olkoon  $p(x)$  polynomi, jonka kertoimet ovat kompleksilukuja, sanotaan  $p(x) = c_1x^k + c_2x^{k-1} + \dots + c_{k+1}$ . Nyt matriisille  $A \in \mathbb{C}^{n \times n}$  määritellään

$$p(A) = c_1A^k + c_2A^{k-1} + \dots + c_{k+1}I.$$

Seuraava lause on ns. **Cayleyn–Hamiltonin** lause.

**Lause 2.18.** *Jos  $A$  on neliömatriisi ja  $c_A$  on sen karakteristinen polynomi, niin*

$$c_A(A) = 0,$$

missä  $0 = (0)_{n \times n}$  on ns. **nollamatriisi**.

Olkoon  $A \in \mathbb{C}^{k \times k}$  ja  $\mathbf{u}, \mathbf{v} \in \mathbb{C}^k$ . Määritellään jono  $(a_n)_{n=0}^{\infty}$  yhtälöllä

$$a_n = \mathbf{u}A^n\mathbf{v}^T, \quad (n \geq 0). \quad (10)$$

Osoitetaan seuraavaksi, että tämä lukujono toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion.

**Lause 2.19.** *Jono (10) toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion.*

*Todistus.* Olkoon

$$c_A(\lambda) = (-1)^k(\lambda^k + c_1\lambda^{k-1} + \cdots + c_k),$$

$A$ :n karakteristinen polynomi. Cayleyn–Hamiltonin lauseen mukaan

$$(c_A(A))A^k + c_1A^{k-1} + \cdots + c_kI = 0.$$

Kerrotaan tämä yhtälö vasemmalta  $\mathbf{u}A^n$ :llä ja oikealta pystyvektorilla  $\mathbf{v}^T$ , saadaan

$$a_{n+k} + c_1a_{n+k-1} + \cdots + c_ka_n = 0, \quad (11)$$

joten jono  $(a_n)_{n=0}^{\infty}$  toteuttaa siis tämän rekursion. Rekursion alkuehdot saadaan laskemalla  $k$  ensimmäistä arvoa määritelmästä (10).  $\square$

Voidaan myös osoittaa, että jokaisella homogeenisella lineaarisella vakiokertoimisella rekursiolla on matriisiesitys (10).

**Lause 2.20.** *Olkoon  $(a_n)_{n=0}^{\infty}$  jono, joka toteuttaa homogeenisen lineaarisen vakiokertoimisen rekursion*

$$\begin{cases} a_0 = b_0, a_1 = b_1, \dots, a_{k-1} = b_{k-1}, \\ a_{n+k} = c_1a_{n+k-1} + c_2a_{n+k-2} + \cdots + c_ka_n \end{cases} \quad (n \geq 0),$$

missä  $c_k \neq 0$ . Tällöin on olemassa sellainen  $k \times k$  matriisi  $A$  ja sellaiset vektorit  $\mathbf{u}, \mathbf{v} \in \mathbb{C}^k$ , että

$$a_n = \mathbf{u}A^n\mathbf{v}^T$$

kaikilla  $n \geq 0$ .

*Todistus.* Sivuuutetaan.  $\square$

### 3 Boolean algebrat ja matriisit

Boolean algebra on algebrallinen systeemi, jonka *George Boole* kehitti logiikan systemaattiseen esitykseen. Boolean algebran ensimmäinen sovellus oli propositiologiikka ja nykyään niiden keskeinen sovellusalue on elektroniikan piirisuunnittelu. Boolean matriisien alkiot taas ovat Boolean algebran alkiota. Niillä voidaan kuvata diskreetteja joukkoja ja relaatioita.

#### 3.1 Boolean algebra

Olkoon  $B$  on jokin epätyhjä joukko ja 0 ja 1 sen kaksi erisuurta alkiota. Lisäksi joukossa  $B$  on määritelty kaksi binääristä operaatiota,

**yhdiste**  $+$ :  $B \times B \rightarrow B$  ja

**kohtaus**  $\cdot$ :  $B \times B \rightarrow B$ .

Lisäksi joukossa  $B$  on määritelty unaarinen operaatio

**komplementti**  $\bar{\phantom{x}}$ :  $B \rightarrow B$ .

**Määritelmä 3.1.** Kuusikko  $\mathcal{B} = (B, +, \cdot, \bar{\phantom{x}}, 0, 1)$  on **Boolean algebra** jos seuraavat ehdot ovat voimassa kaikille  $x, y, z \in B$ :

$$\begin{array}{ll}
 \text{(B1)} & x + (y + z) = (x + y) + z, & \text{(B2)} & x \cdot (y \cdot z) = (x \cdot y) \cdot z, \\
 \text{(B3)} & x + y = y + x & \text{(B4)} & x \cdot y = y \cdot x \\
 \text{(B5)} & x + (y \cdot z) = (x + y) \cdot (x + z), & \text{(B6)} & x \cdot (y + z) = (x \cdot y) + (x \cdot z) \\
 \text{(B7)} & x + 0 = x & \text{(B8)} & x \cdot 1 = x \\
 \text{(B9)} & x + \bar{x} = 1 & \text{(B10)} & x \cdot \bar{x} = 0.
 \end{array}$$

Alkiota 0 kutsutaan Boolean algebran  $\mathcal{B}$  **nolla-alkioksi** ja alkiota 1 sen **ykkösalkioksi**.

Lakien (B1) ja (B2) mukaan yhdiste ja kohtaus ovat assosiatiivisia, lakien (B3) ja (B4) mukaan ne ovat kommutatiivisia ja lakien (B5) ja (B6) mukaan ne ovat keskenään distributiivisia operaatioita. Lain (B7) mukaan nolla-alkio on yhdisteen identiteettialkio (neutraalialkio) ja lain (B8) mukaan ykkösalkio on kohtauksen identiteettialkio (neutraalialkio). Lain (B9) mukaan alkion yhdiste komplementtinsa kanssa on ykkösalkio ja lain (B10) mukaan alkion kohtaus komplementtinsa kanssa on nolla-alkio.

Seuraavaksi tarkastellaan Boolean algebroiden tärkeää sovellusta, joka koskee joukkoja ja niiden operaatioita unioni, leikkaus ja komplementti.

**Esimerkki 3.2.** Joukon  $X$  **potenssijoukko**  $\mathcal{P}(X)$  on joukon  $X$  kaikkien osajoukkojen joukko eli

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

$(\mathcal{P}(X), \cup, \cap, ^C, \emptyset, X)$  muodostaa Boolean algebran. Alkioina ovat siis joukon  $X$  osajoukot, yhdisteenä on unioni  $\cup$ , kohtauksena on leikkaus  $\cap$ , komplementiksi on valittu joukko-opin komplementti  $^C$ , nolla-alkioksi  $\emptyset$  ja ykkösalkioksi  $X$ .

Unioni ja leikkaus ovat selvästi assosiativisia, ts. lait (B1)–(B4) ovat selvästi voimassa. Osoitetaan lait (B5), (B7), (B9), loput jätetään harjoitustehtäviksi. Oletetaan, että  $A, B, C \in \mathcal{P}(X)$  (siis  $A, B, C \subseteq X$ ),

$$\begin{aligned} \text{(B5)} \quad & (A \cup B) \cap (A \cup C) \\ &= \{x \in X \mid (x \in A \text{ tai } x \in B) \text{ ja } (x \in A \text{ tai } x \in C)\} \\ &= \{x \in X \mid x \in A \text{ tai } (x \in B \text{ ja } x \in C)\} = A \cup (B \cap C). \end{aligned}$$

$$\text{(B7)} \quad A \cup \emptyset = A$$

$$\text{(B9)} \quad A \cup A^C = X.$$

Oletetaan, että Boolean algebran operaatioista vahvimmin sitoo komplementti, sitten  $\cdot$  ja heikoimmin  $+$ . Boolean algebran kaavat voidaan nyt kirjoittaa muodossa, jossa turhat sulkuja on jätetty pois. Lisäksi kohtaus operaatiossa  $\cdot$  voidaan jättää kirjoittamatta, eli merkitään  $xy = x \cdot y$ . Nyt esimerkiksi Boolean algebran kaava  $(x \cdot y) + (x \cdot z)$  muuttuu muotoon  $xy + xz$ .

Kun tarkastellaan edellisellä sivulla esitetyn Boolean algebran määritelmän lakeja pareittain, huomataan seuraavan lauseen mukainen vastaavuus. Tämä ns. **duaaliperiaate** on Boolean algebran keskeinen ominaisuus.

**Lause 3.3** (Dualiteettiperiaate). *Jos  $\mathcal{B} = (B, +, \cdot, ', 0, 1)$  on Boolean algebra, niin sen duaali  $\mathcal{B}^d = (B, \cdot, +, ', 1, 0)$  on myös Boolean algebra.*

*Todistus.* **Dualiteettimuunnoksella**

$$+ \rightarrow \cdot, \quad \cdot \rightarrow +, \quad 0 \rightarrow 1, \quad 1 \rightarrow 0$$

kaava muuttuu duaalikseen. Boolean algebran määritelmän listassa B1–B10 jokainen laki on viereisen lain duaali. Näemme, että jokainen duaalilta  $\mathcal{B}^d$  vaadittava laki on voimassa, koska algebran  $\mathcal{B}$  lait ovat voimassa.  $\square$

Duaaliteettiperiaatteesta seuraa, että jos jokin annettu väite voidaan johtaa laskusäännöillä (B1)–(B10), sen duaaliväite voidaan johtaa vastaavilla duaalisäännöillä. Kahdesta keskenään duaalista väitteistä riittää siis todistaa vain toinen.

Tarkastellaan seuraavaksi Boolean algebran ominaisuuksia. Näytetään ensin, että yhdiste ja kohtaus ovat **idempotenttisia**.

**Lause 3.4.** *Boolean algebrassa  $x + x = x$  ja  $xx = x$ .*

*Todistus.* Väitteen ensimmäinen todistetaan seuraavasti:

$$x + x \stackrel{B8}{=} (x + x)1 \stackrel{B9}{=} (x + x)(x + \bar{x}) \stackrel{B5}{=} x + x\bar{x} \stackrel{B10}{=} x + 0 \stackrel{B7}{=} x.$$

Koska toinen väitteen kaava on ensimmäisen duaali, se seuraa duaaliperiaatteen nojalla, mutta todistetaan se silti.

$$xx \stackrel{B7}{=} xx + 0 \stackrel{B10}{=} xx + x\bar{x} \stackrel{B6}{=} x(x + \bar{x}) \stackrel{B9}{=} x1 \stackrel{B8}{=} x.$$

Huomaa, että käytetyt säännöt ovat toistensa duaalit.  $\square$

Samoin osoitetaan seuraavat identiteetit.

**Lause 3.5.** *Boolean algebrassa seuraavat kaavat ovat voimassa:*

1.  $x + 1 = 1$ ,  $x0 = 0$ ,
2.  $x + xy = x$ ,  $x(x + y) = x$ ,
3.  $x + \bar{x}y = x + y$ ,  $x(\bar{x} + y) = xy$ .

Näytetään seuraavaksi, että alkion komplementti on yksikäsitteinen. Jos tosiaan jokin alkio  $b$  toteuttaa  $\bar{x}$ :ltä vaadittavat säännöt (B9) ja (B10), niin  $b = \bar{x}$ .

**Lemma 3.6.** *Olkoon  $a \in B$ . Jos  $a + b = 1$  ja  $ab = 0$  jollekin  $b \in B$ , niin  $b = \bar{a}$ .*

*Todistus.* Koska  $a + b = 1$ , niin  $\bar{a}b = 0 + \bar{a}b = a\bar{a} + \bar{a}b = \bar{a}a + \bar{a}b = \bar{a}(a + b) = \bar{a}1 = \bar{a}$ . Toisaalta koska  $ab = 0$ , niin  $b = b1 = b(a + \bar{a}) = ba + b\bar{a} = ab + \bar{a}b = 0 + \bar{a}b = \bar{a}b$ . Yhteensä  $\bar{a} = \bar{a}b = b$ .  $\square$

Esellisen lemmän avulla voidaan todistaa muita komplementin ominaisuuksia. Seuraavan lauseen kohdassa 3 ovat ns. **De Morganin säännöt**.

**Lause 3.7.** *Boolean algebrassa seuraavat kaavat ovat voimassa:*

1.  $\bar{\bar{x}} = x$ ,
2.  $\bar{0} = 1$ ,  $\bar{1} = 0$ ,
3.  $\overline{a + b} = \bar{a}\bar{b}$ ,  $\overline{ab} = \bar{a} + \bar{b}$ .

### 3.2 Totuusfunktiot ja propositiot

Merkitään joukkoa  $\{0, 1\}^n = \mathcal{V}_n$ . Funktiota  $\varphi: \mathcal{V}_n \rightarrow \{0, 1\}$  kutsutaan (*n-paikkaiseksi*) **totuusfunktioiksi**. Joukko  $\mathcal{V}_n = \{0, 1\}^n$  on *n*-pituisten binäärivektoreiden joukko eli

$$\mathcal{V}_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \{0, 1\}, 1 \leq i \leq n\}.$$

Selvästi  $|\mathcal{V}_n| = 2^n$ . Merkitään joukon  $\mathcal{V}_n$  alkioita  $\mathbf{v} = (v_1, v_2, \dots, v_n)$ . Maalijoukon  $\{0, 1\}$  alkioista 0 vastaa nyt totuusarvoa **epätosi** ja 1 totuusarvoa

**tosi.** Totuusfunktio  $\varphi$  antaa siis kaikille joukon  $\mathcal{V}_n$  vektoreille  $\mathbf{v}$  totuusarvon  $\varphi(\mathbf{v})$ .

Merkitään  $\mathcal{F}_n$ :llä kaikkien  $n$ -paikkaisten totuusfunktioiden joukkoa, siis

$$\mathcal{F}_n = \{\varphi: \mathcal{V}_n \rightarrow \{0, 1\} \mid \varphi \text{ on funktio}\}.$$

Osoitetaan, että  $\mathcal{F}_n$  muodostaa Boolean algebran. Valitaan yhdisteeksi **disjunktio**  $\vee$ , kohtaukseksi **konjunktio**  $\wedge$ , komplementiksi **negaatio**  $\neg$ . Olkoon  $\varphi, \psi \in \mathcal{F}_n$ ,  $\varphi \vee \psi$ , nyt  $\varphi \wedge \psi$  ja  $\neg\varphi$  ovat joukon  $\mathcal{F}_n$  totuusfunktioita, joiden arvot vektoreille  $\mathbf{v} \in \mathcal{V}_n$  määritellään seuraavasti:

$$\begin{aligned} (\varphi \vee \psi)(\mathbf{v}) &= \max\{\varphi(\mathbf{v}), \psi(\mathbf{v})\}, \\ (\varphi \wedge \psi)(\mathbf{v}) &= \min\{\varphi(\mathbf{v}), \psi(\mathbf{v})\}, \\ (\neg\varphi)(\mathbf{v}) &= 1 - \varphi(\mathbf{v}), \end{aligned}$$

missä  $-$  negaation määritelmässä on tavallinen kokonaislukujen erotus. Nolla-alkiona toimii aina epätosi totuusfunktio  $\perp$ , jolle  $\perp(\mathbf{v}) = 0$  kaikilla  $\mathbf{v} \in \mathcal{V}_n$ , ja ykkösalkiona aina tosi totuusfunktio  $\top$ ,  $\top(\mathbf{v}) = 1$  kaikilla  $\mathbf{v} \in \mathcal{V}_n$ .

Funktioiden  $\varphi \vee \psi$ ,  $\varphi \wedge \psi$  ja  $\neg\varphi$  arvot voidaan esittää myös ns. totuus-  
taulukoiden avulla.

$\varphi(\mathbf{v})$	$\psi(\mathbf{v})$	$(\varphi \vee \psi)(\mathbf{v})$	$(\varphi \wedge \psi)(\mathbf{v})$		$\varphi(\mathbf{v})$	$(\neg\varphi)(\mathbf{v})$
0	0	0	0		0	1
0	1	1	0		1	0
1	0	1	0		1	0
1	1	1	1		1	0

**Lause 3.8.**  $(\mathcal{F}_n, \vee, \wedge, \neg, \top, \perp)$  on Boolean algebra (kaikilla  $n$ ).

*Todistus.* Osoitetaan, että Boolean algebran lait (B1) -(B10) ovat voimassa. Oletetaan, että  $\varphi, \psi, \chi \in \mathcal{F}_n$ .

(B1)  $\varphi \vee (\psi \vee \chi) = (\varphi \vee \psi) \vee \chi$ , koska kaikilla  $\mathbf{v} \in \mathcal{V}_n$ ,  $\max\{\varphi(\mathbf{v}), \max\{\psi(\mathbf{v}), \chi(\mathbf{v})\}\} = \max\{\varphi(\mathbf{v}), \psi(\mathbf{v}), \chi(\mathbf{v})\} = \max\{\max\{\varphi(\mathbf{v}), \psi(\mathbf{v})\}, \chi(\mathbf{v})\}$

(B2)  $\varphi \wedge (\psi \wedge \chi) = (\varphi \wedge \psi) \wedge \chi$ , koska kaikilla  $\mathbf{v} \in \mathcal{V}_n$ ,  $\min\{\varphi(\mathbf{v}), \min\{\psi(\mathbf{v}), \chi(\mathbf{v})\}\} = \min\{\varphi(\mathbf{v}), \psi(\mathbf{v}), \chi(\mathbf{v})\} = \min\{\min\{\varphi(\mathbf{v}), \psi(\mathbf{v})\}, \chi(\mathbf{v})\}$

Lait (B3) ja (B4) ovat selvästi voimassa, koska joukon maksimi tai minimi ei riipu alkioiden järjestyksestä.

Lait (B5)-(B10) voidaan todistaa totuustaulukoiden avulla. (B5) ja (B6) seuraavat seuraavista totuustaulukoista.

$\varphi(\mathbf{v})$	$\psi(\mathbf{v})$	$\chi(\mathbf{v})$	$(\varphi \vee (\psi \wedge \chi))(\mathbf{v})$	$((\varphi \vee \psi) \wedge (\varphi \vee \chi))(\mathbf{v})$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

$\varphi(\mathbf{v})$	$\psi(\mathbf{v})$	$\chi(\mathbf{v})$	$(\varphi \wedge (\psi \vee \chi))(\mathbf{v})$	$((\varphi \wedge \psi) \vee (\varphi \wedge \chi))(\mathbf{v})$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Lait (B7)-(B10) seuraavat taulukosta

$\varphi(\mathbf{v})$	$(\varphi \vee \perp)(\mathbf{v})$	$(\varphi \wedge \top)(\mathbf{v})$	$(\varphi \vee \neg\varphi)(\mathbf{v})$	$(\varphi \wedge \neg\varphi)(\mathbf{v})$
0	0	0	1	0
1	1	1	1	0

□

Tarkastellaan seuraavaksi propositioita ja osoitetaan niiden yhteys totuusfunktioihin. Aloitetaan propositioiden määritelmällä kun käytössä ovat konnektiivit **konjunktio**  $\wedge$ , **disjunktio**  $\vee$  ja **negaatio**  $\neg$ .

Olkoon  $P_n = \{p_1, p_2, \dots, p_n\}$  propositiomuuttujien joukko. Määritellään joukko **Prop** seuraavasti

1.  $P_n \subset \mathbf{Prop}$ , ja
2. jos  $p, q \in \mathbf{Prop}$ , niin  $(p \vee q), (p \wedge q)$  ja  $(\neg p) \in \mathbf{Prop}$ .

Kuvaus  $v$ , jossa jokaiselle funktiolle annetaan totuusarvo 1 tai 0 on ns. **totuusarvosijoitus** (valuaatio, totuusarvotus)  $v : P_n \rightarrow \{0, 1\}$ . Totuusarvosijoitus  $v$  voidaan ajatella vektorina  $(v(p_1), v(p_2), \dots, v(p_n)) \in \{0, 1\}^n$ . Jokaista totuusarvosijoitusta vastaa siis jokin joukon  $\mathcal{V}_n$  vektori. Jokainen totuusarvosijoitus vastaa siis totuustaulukon yhtä vaakariviä.

Propositiomuuttujien totuusarvot saadaan totuusarvosijoituksesta. Määritellään propositioiden totuusarvot (induktiivisesti) eri totuusarvosijoituksille seuraavien totuustaulukoiden avulla. Oletetaan, että  $p, q \in \mathbf{Prop}$ .

$p$	$q$	$(p \vee q)$	$(p \wedge q)$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

$p$	$(\neg p)$
0	1
1	0

Selvästi siis jokainen propositio (jonka muuttujien joukko on  $P_n$ ) määrittää joukon  $\mathcal{F}_n = \{\varphi: \{0, 1\}^n \rightarrow \{0, 1\}\}$  totuusfunktion.

Määritellään nyt propositioiden yhtäsuuruus  $\equiv$  nyt siten, että

$$P \equiv Q \quad \text{joss} \quad v(P) = v(Q) \text{ kaikilla } v \in \mathcal{V}_n.$$

Jos  $P \equiv Q$ , sanotaan, että propositiot ovat **loogisesti ekvivalentit**. *Propositiot ovat siis ekvivalentit, jos ne saavat saman totuusarvon kaikissa totuusarvosijoituksissa.* Tarkemmin sanottuna,  $P \equiv Q$  jos ja vain jos  $P$  ja  $Q$  määräävät saman totuusfunktion.

**Lemma 3.9.** *Jokainen propositio määrittää totuusfunktion. Jokainen totuusfunktio voidaan esittää propositiona.*

*Todistus.* Väitteen ensimmäinen osa perusteltiin jo edellä. Osoitetaan nyt, että jokainen totuusfunktio  $\varphi: \mathcal{V}_n \rightarrow \{0, 1\}$  voidaan esittää propositiona, joka määrittelee totuusfunktion  $\varphi$ .

Tarkastellaan funktion  $\varphi$  totuustaulukkoa. Jokainen taulukon vaakarivin vektori  $\mathbf{v} = (a_1, a_2, \dots, a_n)$  määrittelee totuusarvosijoituksen  $v$ , jolle  $v(p_i) = a_i$  kaikilla  $i$ .

$\mathbf{v}$	$\varphi(\mathbf{v})$
$\mathbf{v}_0 = 0 \ 0 \ \dots \ 0 \ 0$	$\varphi(\mathbf{v}_0)$
$\mathbf{v}_1 = 0 \ 0 \ \dots \ 0 \ 1$	$\varphi(\mathbf{v}_1)$
$\mathbf{v}_2 = 0 \ 0 \ \dots \ 1 \ 0$	$\varphi(\mathbf{v}_2)$
$\mathbf{v}_3 = 0 \ 0 \ \dots \ 1 \ 1$	$\varphi(\mathbf{v}_3)$
$\vdots$	$\vdots$
$\mathbf{v}_{2^n-1} = 1 \ 1 \ \dots \ 1 \ 1$	$\varphi(\mathbf{v}_{2^n-1})$
$p_1 \ p_2 \ \dots \ p_{n-1} \ p_n$	$\varphi(v(p_1), v(p_2), \dots, v(p_n))$

Olkoon  $J = \{j \mid \varphi(\mathbf{v}_j) = 1\}$ , toisin sanoen  $J$  on niiden indeksien  $j$  joukko, joille  $\varphi(\mathbf{v}_j) = 1$ . Olkoon  $\mathbf{v}_i = (v_{i1}, v_{i2}, \dots, v_{in})$ , sitä vastaava **alkeiskonjunktio** on

$$(q_{i1} \wedge q_{i2} \wedge \dots \wedge q_{in}),$$

missä  $q_{ij} = p_j$ , jos  $v_{ij} = 1$ , ja  $q_{ij} = \neg p_j$ , jos  $v_{ij} = 0$ . Esimerkiksi vektoria  $(0, 1, 1, 0)$  vastaava alkeiskonjunktio on  $(\neg p_1 \wedge p_2 \wedge p_3 \wedge \neg p_4)$ . Nyt kun joukon  $J$  alkioita vastaavat alkeiskonjunktiot yhdistetään operaation  $\vee$  avulla, saadaan aikaan propositio, joka vastaa totuusfunktiota  $\varphi$ . □

Määritellään vielä kaksi erikoispropositiota,  $\top$  ja  $\perp$ , jotka vastaavat kyseisiä totuusfunktioita. Siis  $\top$  on aina tosi ja  $\perp$  aina epätosi. Tarkastellaan nyt propositioita "modulo looginen ekvivalenssi", ts. jos  $p, q \in \mathbf{Prop}$  ja  $p \equiv q$ , niin  $p$  ja  $q$  ovat yksi ja sama propositio. Merkitään propositioiden joukkoa "modulo looginen ekvivalenssi"  $\mathbf{Prop}_{\equiv}$ :llä.

**Lause 3.10.**  $(\mathbf{Prop}_{\equiv}, \vee, \wedge, \neg, \top, \perp)$  on Boolean algebra.

*Todistus.* Seuraa Lauseesta 3.8 ja Lemmasta 3.9 ja loogisen ekvivalenssin määritelmästä.  $\square$

Huomaa, että  $\mathbf{Prop}$  ei ole Boolean algebra vaan  $\mathbf{Prop}_{\equiv}$  on. Esimerkiksi,  $p_1 \wedge \neg p_1 \equiv p_2 \wedge \neg p_2 \equiv \perp$ , joukossa  $\mathbf{Prop}$  kaksi ensimmäistä ovat eri alkioita, mutta joukossa  $\mathbf{Prop}_{\equiv}$  ne ovat sama alkio, koska ne ovat ekvivalentit eli määräävät saman totuusfunktion. Voidaan osoittaa, että Boolean algebrassa nolla-alkio on aina yksikäsitteinen, siksi  $\mathbf{Prop}$  ei voi olla Boolean algebra.

Koska  $\mathbf{Prop}_{\equiv}$  on Boolean algebra, ovat kaikki Boolean algebran yleiset kaavat tosia myös propositiolle, kun yhtäsuuruutena on looginen ekvivalenssi. Esimerkiksi Lauseen 3.7 kohdan (iii) mukaan ns. De Morganin kaavat ovat voimassa propositioille, eli jos  $p, q \in \mathbf{Prop}$ , niin

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad \text{ja} \quad \neg(p \wedge q) \equiv \neg p \vee \neg q.$$

Huomaa myös, että tutut konnektiivit  $\rightarrow$  ja  $\leftrightarrow$  voidaan määritellä konnektiivien  $\vee, \wedge$  ja  $\neg$  avulla seuraavasti:

$$p \rightarrow q \equiv \neg p \vee q \quad \text{ja} \quad p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q).$$

Jos propositiomuuttujien joukko  $P_n$  on tyhjä, saadaan pienin mahdollinen Boolean algebra, sillä alkioista jäljelle jäävät vain funktiot  $\perp$  ja  $\top$ . Ne ovat toistensa komplementtja:  $\bar{\perp} = \top$  ja  $\bar{\top} = \perp$ . Merkitään  $0 = \perp$  ja  $1 = \top$ . Nimetään tämä Boolean algebra:  $\mathcal{B}_2 = (\{0, 1\}, +, \cdot, \neg, 0, 1)$ . Operaatiot  $+$  ja  $\cdot$  määritellään seuraavasti.

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

Huomaa, että  $1 + 1 = 1$  päinvastoin kuin yhteenlaskussa modulo 2.

### 3.3 Boolean algebra ja osittainen järjestys

**Määritelmä 3.11.** Joukon  $B$  relaatio  $\leq$  on **osittainen järjestys**, jos se on

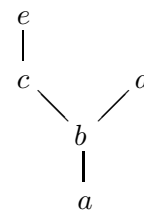
- **refleksiivinen** eli  $b \leq b$  kaikilla  $b \in B$ ,
- **antisymmetrinen** eli jos  $a \leq b$  ja  $b \leq a$ , niin  $a = b$ , ja

- **transitiivinen** eli jos  $a \leq b$  ja  $b \leq c$ , niin  $a \leq c$ .

Osittainen termi viittaa siihen, että välttämättä kahta alkioita ei voi järjestää: voi olla  $a \not\leq b$  ja  $b \not\leq a$ . Jos alkioita  $a$  ja  $b$  ei voida järjestää merkitään  $a \parallel b$ .

Alkio  $a$  on joukon  $B$  **pienin alkio**, jos  $a \leq b$  kaikilla  $b \in B$ . Vastaavasti  $a \in B$  on **suurin alkio**, jos  $y \leq a$  kaikilla  $y \in B$ . Alkio  $a \in B$  on **minimaalinen**, jos joko  $a \parallel b$  tai  $a \leq b$  kaikilla  $b \in B$ .

Osittainen järjestys voidaan esittää ns. **Hassen kaavion** avulla. Siinä suurempi alkio kirjoitetaan pienemmän yläpuolelle ja ne yhdistetään viivalla. Vieressä on joukon  $A = \{a, b, c, d, e\}$  osittainen järjestys, jossa  $a \leq b$ ,  $b \leq c$ ,  $b \leq d$  ja  $c \leq e$ . Transitiivisuudesta seuraa esimerkiksi  $a \leq c$  ja refleksiivisyydestä  $a \leq a$ , joten näitä ei piirretä kaavioon näkyviin.



Boolean algebrassa voidaan määritellä osittainen järjestys seuraavalla tavalla.

**Määritelmä 3.12.** Boolean algebrassa joukon  $B$  relaatio  $\leq$  määritellään kaavalla

$$a \leq b \quad \text{joss} \quad a \cdot b = a.$$

Selvästi edellisen määritelmän relaatio on osittainen, sillä välttämättä kahden alkion kohtaaminen ei ole jompikumpi alkioista. Määritelmä voidaan tulkitella niin, että kohtaaminen valitsee kahdesta alkioista pienemmän. Seuraavan lauseen mukaan vastaavasti yhdiste valitsee kahdesta alkioista suuremman.

**Lause 3.13.** *Olkkoon  $\leq$  Boolean algebran  $B$  Määritelmän 3.12 mukainen järjestys relaatio. Silloin kaikille  $a, b, c, d \in B$  on voimassa seuraavat ominaisuudet:*

1. Relaatio  $\leq$  on osittainen järjestys.
2.  $a \leq b$  joss  $a \cdot b = a$  joss  $a + b = b$  joss  $\bar{b} \leq \bar{a}$ .
3.  $a \cdot b \leq a$ .
4.  $a \leq a + b$ .
5. Jos  $x \leq a$  ja  $x \leq b$ , niin  $x \leq a \cdot b$ .
6. Jos  $a \leq y$  ja  $b \leq y$ , niin  $a + b \leq y$ .
7. Jos  $a \leq b$  ja  $c \leq d$ , niin  $a + c \leq b + d$  ja  $a \cdot c \leq b \cdot d$ .

*Todistus.* Kohdat (iii), (iv) ja (vi) jätetään harjoitustehtäviksi.

(i) Relaatio  $\leq$  on refleksiivinen, koska Lauseen 3.4 mukaan  $bb = b$ . Se on antisymmetrinen, koska, jos  $a \leq b$  ja  $b \leq a$ , niin  $b = ab = a$ . Jos  $a \leq b$  ja  $b \leq c$ , niin  $ac = abc = ab = a$ , joten  $\leq$  on transitiivinen.

(ii) Oletetaan, että  $a \leq b$ , joten  $ab = a$ . Silloin Lauseen 3.5 kohdan (ii) mukaan

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

Samoin nähdään, että ehdosta  $a + b = b$  seuraa  $ab = a$ . Käyttämällä De Morganin sääntöjä saadaan

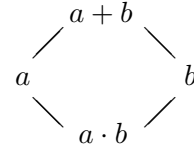
$$a \leq b \quad \text{joss} \quad ab = a \quad \text{joss} \quad \bar{a} + \bar{b} = \bar{a} \quad \text{joss} \quad \bar{b} \leq \bar{a}.$$

(v) Jos  $x \leq a$  ja  $x \leq b$ , niin  $xa = xb = x$ . Silloin  $x(ab) = (xa)b = xb = x$ , joten  $x \leq ab$ . Samoin päätellään toinen väite.

(vi) jätetään harjoitustehtäväksi.

(vii) Jos  $a \leq b$  ja  $c \leq d$ , niin  $(a + c) \cdot (b + d) = ab + bc + ad + cd = a + bc + ad + c = a(1 + d) + c(b + 1) = a + c$ , joten  $a + c \leq b + d$ . Toisaalta  $(ac) \cdot (bd) = ac$ , joten  $ac \leq bd$ . □

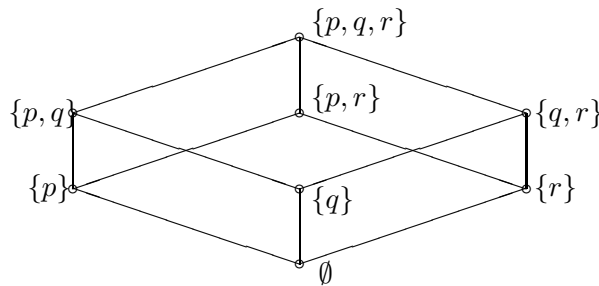
Kohdan (iii) mukaan  $a \cdot b \leq a$  ja  $a \cdot b \leq b$ . Siis  $a \cdot b$  on  $a$ :n ja  $b$ :n yhteinen **alaraja**. Kohta (v) mukaan taas  $a \cdot b$  on suurin alkioiden  $a$  ja  $b$  alarajoista. Jos nimittäin myös  $x$  on alaraja, niin  $x \leq a \cdot b$ . Vastaavasti kohtien (iv) ja (vi) mukaan  $a + b$  on pienin alkioiden  $a$  ja  $b$  **ylärajoista**.



**Esimerkki 3.14.** Olkoon  $X = \{p, q, r\}$  ja tarkastellaan Boolean algebraa  $\mathcal{P}(X)$ . Joukon  $X$  osajoukkojen välille saadaan nyt lauseen 3.13 nojalla osittainen järjestys, kun määritellään

$$A \leq B \quad \text{joss} \quad A \cap B = A.$$

Mutta  $A \cap B = A$  silloin ja vain silloin, kun  $A \subseteq B$ . Osittainen järjestys  $\leq$  on siis sama kuin osajoukkojen sisältymisjärjestys  $\subseteq$ . Koska  $\mathcal{P}(X)$  on äärellinen joukko, voidaan piirtää Hassen kaavio sisältymisrelaation suhteen.



Kuva 3: Boolean algebra  $\mathcal{P}(\{p, q, r\})$

On tärkeää huomata, että Boolean algebrassa  $\mathcal{B} = (B, +, \cdot, \bar{\phantom{x}}, 0, 1)$  pienin alkio on aina 0 ja suurin aina 1. Esimerkin 3.14 potenssialgebrassa pienin alkio on  $\emptyset$  ja suurin on  $X$ .

### 3.4 Esityslause

Tässä kappaleessa osoitetaan, että jokainen äärellinen Boolean algebra on **isomorfinen** jonkun joukon  $X$  potenssijoukon  $\mathcal{P}(X)$  muodostaman Boolean algebran kanssa. Näin saamme nopean keinon tarkistaa, milloin annettu äärellinen joukko operaatioineen on Boolean algebra.

**Määritelmä 3.15.** Olkoon  $\leq$  osittainen järjestys Boolean algebran joukossa  $B$ . Alkio  $x \in B$  on **atomi**, jos  $x \neq 0$  ja ehdosta  $0 < y \leq x$  seuraa  $y = x$ .

Atomi on siis minimaalinen nollasta eroava joukon  $B$  alkio. Esimerkin 3.14 Boolean algebrassa atomit ovat  $\{p\}$ ,  $\{q\}$  ja  $\{r\}$ . Lauseen 3.19 todistuksessa Boolean algebran atomit ovat keskeisessä roolissa.

**Määritelmä 3.16.** Olkoot  $\mathcal{B} = (B, +, \cdot, ^-, 0, 1)$  ja  $\mathcal{C} = (C, \cup, \cap, ^C, \emptyset, X)$  kaksi Boolean algebraa. Kuvaus  $f : B \rightarrow C$  on **Boolean algebrojen isomorfismi**, jos  $f$  on bijektio ja kaikilla  $a, b \in B$

- $f(a + b) = f(a) \cup f(b)$ ,
- $f(a \cdot b) = f(a) \cap f(b)$ ,
- $f(\bar{a}) = (f(a))^C$ , ja
- $f(0) = \emptyset$  ja  $f(1) = X$ .

Silloin Boolean algebrat  $\mathcal{B}$  ja  $\mathcal{C}$  ovat **isomorfiset**.

Boolean algebrojen isomorfismi on siis bijektio, joka säilyttää kohtauksen, yhdisteen, komplementin, nolla- ja ykkösalkion.

**Lemma 3.17.** Jos  $a + b = 1$ , niin  $\bar{a} \leq b$ . Jos  $a \cdot b = 0$ , niin  $a \leq \bar{b}$ .

*Todistus.* Nähdään Lemman 3.6 todistuksesta. □

**Lemma 3.18.** Olkoon  $x$  atomi. Silloin

1.  $x \leq \bar{a}$  jos ja vain jos  $x \not\leq a$ .
2. Jos  $x \leq a + b$ , niin  $x \leq a$  tai  $x \leq b$ .

*Todistus.* (i) Oletetaan, että  $x \leq \bar{a}$ . Silloin  $x \cdot \bar{a} = x$ . Jos nyt  $x \leq a$ , niin  $xa = x$ , jolloin  $x = xa = (x \cdot \bar{a})a = x(\bar{a} \cdot a) = x \cdot 0 = 0$ , mikä ei käy, sillä  $x$  on atomi. Siis  $x \not\leq a$ .

Oletetaan sitten, että  $x \not\leq a$ . Silloin  $x \cdot a \neq x$ . Täten  $x = x \cdot 1 = x(a + \bar{a}) = (x \cdot a) + (x \cdot \bar{a}) \geq x \cdot a \geq 0$ . Koska  $x \cdot a \neq x$ , niin  $x > x \cdot a$ . Koska lisäksi  $x$  on atomi, niin  $x \cdot a = 0$ . Edellisen lemmän mukaan  $x \leq \bar{a}$ .

2. Olkoon  $x \leq a + b$ . Silloin  $x = x(a + b) = (x \cdot a) + (x \cdot b)$ . Jos molemmat  $x \cdot a$  ja  $x \cdot b$  olisivat nollia, niin myös  $x$  olisi nolla. Siis jompi kumpi, sanotaan  $x \cdot a$  ei ole nolla. Lauseen 3.13 kohdan (iii) mukaan  $0 < x \cdot a \leq x$ , joten  $x \cdot a = x$ , sillä  $x$  on atomi. Siis  $x \leq a$ . □

**Lause 3.19** (Esityslause). *Jokainen äärellinen Boolean algebra on isomorfinen jonkin potenssialgebran  $\mathcal{P}(X)$  kanssa.*

*Todistus.* Olkoon  $\mathcal{B} = (B, +, \cdot, \bar{\phantom{x}}, 0, 1)$  äärellinen Boolean algebra. Valitaan joukoksi  $X$  Boolean algebran  $\mathcal{B}$  atomit. Joukko  $X$  ei ole tyhjä, sillä äärellisessä Boolean algebrassa täytyy olla ainakin yksi atomi. Nimittäin,  $0 \leq 1$ , ja joko  $1$  on atomi tai niiden välissä on vähintään yksi atomi.

Määritellään kuvaus  $f$  joukosta  $B$  joukkoon  $\mathcal{P}(X)$  kaavalla

$$f(b) = \{x \in X \mid x \leq b\}.$$

Tällöin  $b$  kuvautuu niiden atomien  $x$  joukoksi, joille  $x \leq b$ . Näytetään, että  $f$  on isomorfismi Boolean algebrasta  $\mathcal{B} = (B, +, \cdot, \bar{\phantom{x}}, 0, 1)$  Boolean algebraan  $(\mathcal{P}(X), \cup, \cap, \bar{\phantom{x}}, \emptyset, X)$ .

*Injektiiivisyys:* Oletetaan, että  $b_1 \neq b_2$ . Silloin joko  $b_1 \not\leq b_2$  tai  $b_2 \not\leq b_1$ . Oletetaan, että  $b_1 \not\leq b_2$ , toinen tapaus todistetaan samalla tavalla.

Lemman 3.17 mukaan  $b_1 \cdot \bar{b}_2 \neq 0$ . On siis olemassa sellainen atomi  $x$ , että  $x \leq b_1 \cdot \bar{b}_2$ . Lauseen 3.13 kohdan (iii) mukaan  $b_1 \cdot \bar{b}_2 \leq b_1$  ja  $b_1 \cdot \bar{b}_2 \leq \bar{b}_2$ , joten  $x \leq b_1$  ja  $x \leq \bar{b}_2$ . Tästä seuraa, että  $x \not\leq b_2$  Lemman 3.18 mukaan. Nyt  $x \in f(b_1)$ , mutta  $x \notin f(b_2)$ , joten  $f(b_1) \neq f(b_2)$ .

*Surjektiiivisyys:* Olkoon  $\{x_1, x_2, \dots, x_k\} \subseteq X$ . Merkitään  $b = x_1 + x_2 + \dots + x_k$ , jos  $k \geq 1$ , ja  $b = 0$ , jos  $k = 0$ . Osoitetaan, että  $\{x_1, x_2, \dots, x_k\} = f(b)$ .

Lauseen 3.13 kohdan (iv) mukaan jokainen  $x_i \leq x_1 + x_2 + \dots + x_k = b$ , joten  $\{x_1, x_2, \dots, x_k\} \subseteq f(b)$ .

Toisaalta, jos  $x \in f(b)$ , niin  $x \in X$  ja  $x \leq b$ , eli  $x \leq x_1 + \dots + x_k$ . Lemman 3.18 mukaan jollakin  $i$ llä  $0 < x \leq x_i$ . Koska  $x_i$  on atomi, niin  $x = x_i$  eli  $x \in \{x_1, \dots, x_k\}$ . Tästä seuraa, että  $f(b) \subseteq \{x_1, \dots, x_k\}$ .

*Nolla- ja ykkösalkio:* Koska  $0$  on pienin alkio,  $f(0) = \emptyset$ , ja  $f(1) = X$ , sillä  $x \leq 1$  kaikille atomeille  $x$  (tai  $X = \{1\}$  Boolean algebrassa  $\mathcal{B}_2$ ).

*Yhdiste ja kohtaus:* On osoitettava, että  $f(b_1 \cdot b_2) = f(b_1) \cap f(b_2)$  ja  $f(b_1 + b_2) = f(b_1) \cup f(b_2)$ .

*Kohtaus:* Koska  $b_1 \cdot b_2 \leq b_1$  ja  $b_1 \cdot b_2 \leq b_2$ , niin  $f(b_1 \cdot b_2) \subseteq f(b_1)$  ja  $f(b_1 \cdot b_2) \subseteq f(b_2)$ . Tästä seuraa, että  $f(b_1 \cdot b_2) \subseteq f(b_1) \cap f(b_2)$ . Toisaalta jos  $x \in f(b_1) \cap f(b_2)$ , niin  $x \leq b_1$  ja  $x \leq b_2$ . Silloin lauseen 3.13 kohdan (v) mukaan  $x \leq b_1 \cdot b_2$ , ja  $x \in f(b_1 \cdot b_2)$ . Näin ollen  $f(b_1 \cdot b_2) = f(b_1) \cap f(b_2)$ .

*Yhdiste:* Koska  $b_2 \leq b_1 + b_2$  ja  $b_1 \leq b_1 + b_2$ , niin  $f(b_2) \subseteq f(b_1 + b_2)$  ja  $f(b_1) \subseteq f(b_1 + b_2)$ . Tästä seuraa, että  $f(b_1) \cup f(b_2) \subseteq f(b_1 + b_2)$ .

Toisaalta jos taas  $x \in f(b_1 + b_2)$ , niin  $x \leq b_1 + b_2$ . Lemman 3.18 nojalla  $x \leq b_1$  tai  $x \leq b_2$ , joten  $x \in f(b_1) \cup f(b_2)$ .

*Komplementti:* Lemman 3.18 mukaan kaikille atomeille  $x \in X$ ,  $x \leq b$  jos ja vain jos  $x \not\leq \bar{b}$ . Täten  $f(\bar{b}) = X \setminus f(b) = (f(b))^C$ .  $\square$

Esityslauseen avulla voidaan testata, muodostaako annettu äärellinen joukko operaatioineen Boolean algebran. Käytännössä piirretään vastaavan

järjestyksen mukainen Hassen kaavio ja verrataan sitä jonkin potenssijoukon sisältymisrelaation mukaiseen Hassen kaavioon. Näin tehdään seuraavassa esimerkissä luvun tekijäjoukolle.

**Esimerkki 3.20.** Joukossa

$$A = \{a \in \mathbb{N} \mid a \text{ jakaa luvun } 30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

on kaikki luvun 30 positiiviset tekijät. Joukossa  $A$  on tavalliseen tapaan binääriset operaatiot: suurin yhteinen tekijä  $\text{syt}$  ja pienin yhteinen jaettava  $\text{pyj}$ . Tarkastellaan, saataisiinko joukosta  $A$  näillä operaatioilla Boolean algebra. Operaatiot  $\text{syt}$  ja  $\text{pyj}$  ovat assosiatiivisia ja kommutatiivisia, ja ne ovat myös keskenään distributiivisia. Valitaan kohtaukseksi  $\text{syt}$  ja yhdisteeksi  $\text{pyj}$ . Nolla-alkioksi 0 on valittava luku, joka toteuttaa ehdon  $\text{pyj}(a, 0) = a$  kaikilla  $a \in A$ . Silloin nolla-alkion on jaettava jokainen joukon  $A$  alkio, joten sen täytyy olla 1. Koska ykkösalkiolle pätee  $\text{syt}(a, 1) = a$  kaikilla  $a \in A$ , niin jokainen joukon  $A$  alkio jakaa ykkösalkion, joten sen täytyy olla 30. Alkion  $a \in A$  komplementti  $\bar{a}$  löydetään ratkaisemalla yhtälöt  $\text{pyj}(a, \bar{a}) = 30$  ja  $\text{syt}(a, \bar{a}) = 1$ . Esimerkiksi  $\bar{3} = 10$  ja  $\bar{6} = 5$ . Täten  $\mathcal{B}_{30} = (A, \text{pyj}, \text{syt}, \bar{\phantom{x}}, 1, 30)$  on Boolean algebra.

Etsitään esityslauseen mukainen joukko  $X$  ja sen Boolean algebra  $\mathcal{P}(X)$ . Se on olemassa, sillä  $A$  on äärellinen. Todistuksessa  $X$  valittiin atomien joukoksi. Tätä varten on etsittävä operaatioihin liittyvä osittainen järjestys. Silloin

$$a \leq b \quad \text{joss} \quad a \cdot b = a \quad \text{joss} \quad \text{syt}(a, b) = a \quad \text{joss} \quad a \mid b.$$

Siis  $a$  on pienempi tai yhtä suuri kuin  $b$ , jos ja vain jos  $a$  jakaa  $b$ :n. Tässä järjestyksessä joukon  $A$  pienin alkio on 1 ja suurin 30. Atomi on nyt sellainen luvun 30 tekijä, joka on ykköistä suurempi, mutta jota pienempää lukua ei joukossa  $A$  ole. Atomit ovat siis 2, 3 ja 5. Isomorfismikuvaus  $f$  on nyt siis joukolta  $A$  joukolle  $\mathcal{P}(X)$ , jossa  $X = \{2, 3, 5\}$ , ja se määritellään kaavalla

$$f(a) = \{x \in X \mid x \leq a\}$$

jokaiselle  $a \in A$ . Silloin  $f(a) = \{x \in \{2, 3, 5\} \mid x \text{ jakaa } a:n\}$ . Esimerkiksi  $f(6) = \{2, 3\}$ . Kun merkitään  $p = 2$ ,  $q = 3$  ja  $r = 5$ , saadaan kuvan 3 mukainen Hassen kaavio.

### 3.5 Boolean matriisit

Boolean matriisien alkiot kuuluvat Boolean algebraan  $\mathcal{B}_2 = (\{0, 1\}, +, \cdot, \bar{\phantom{x}}, 0, 1)$ .

**Määritelmä 3.21.** Matriisia

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

jossa on  $m$  vaakariviä ja  $n$  pystyriviä, kutsutaan **Boolean**  $m \times n$ -**matriisiksi** (tai **tyyppiä**  $m \times n$  **olevaksi Boolean matriisiksi**), jos  $a_{ij} \in \{0, 1\}$  kaikilla  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ . Matriisille  $\mathbf{A}$  käytetään myös merkintää  $(a_{ij})_{m \times n}$  tai lyhyemmin  $(a_{ij})$ . Matriisin  $\mathbf{A}$  rivin  $i$  sarakkeen  $j$  alkiota  $a_{ij}$  sanotaan **kohdan**  $i, j$  **alkioksi** ja merkitään myös  $(\mathbf{A})_{ij}$ :llä. Kaikkien tyyppiä  $m \times n$  olevien Boolean matriisien joukko on  $\mathbb{B}_{m \times n}$ .

Saman tyyppisille Boolean matriiseille määritellään binäärioperaatiot yhdiste  $+$  ja kohtaus  $\odot$  ottamalla alkioittaiset yhdisteet ja kohtaukset Boolean algebran  $\mathcal{B}_2$  mukaan. Boolean algebrassa  $\mathcal{B}_2$  yhdiste  $+$ , kohtaus  $\cdot$  ja komplementti  $-$  määriteltiin seuraavasti.:

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

**Määritelmä 3.22.** Olkoot  $\mathbf{A} = (a_{ij})$  ja  $\mathbf{B} = (b_{ij})$  Boolean  $m \times n$ -matriiseja. Silloin niiden yhdisteen  $\mathbf{A} + \mathbf{B}$  ja kohtauksen  $\mathbf{A} \odot \mathbf{B}$  kohdan  $i, j$  alkioit ovat

$$(\mathbf{A} + \mathbf{B})_{ij} = a_{ij} + b_{ij} \quad \text{ja} \quad (\mathbf{A} \odot \mathbf{B})_{ij} = a_{ij} \cdot b_{ij},$$

missä  $1 \leq i \leq m$  ja  $1 \leq j \leq n$ , ja matriisin  $\mathbf{A}$  komplementin  $\overline{\mathbf{A}}$  kohdan  $i, j$  alkio on

$$(\overline{\mathbf{A}})_{ij} = \overline{a_{ij}}.$$

Boolean matriisien yhdiste, kohtaus ja komplementti saadaan siis alkioittain käyttäen Boolean algebran  $\mathcal{B}_2$  operaatioita.

**Esimerkki 3.23.** Olkoot

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad \mathbf{B} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Silloin  $(\mathbf{A} + \mathbf{B})_{12} = a_{12} + b_{12} = 0 + 1 = 1$  ja

$$\mathbf{A} + \mathbf{B} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathbf{A} \odot \mathbf{B} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \overline{\mathbf{A}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

**Määritelmä 3.24.** Nollamatriisin  $\mathbf{0}_{m \times n} = (0)_{m \times n}$  kaikki alkioit ovat nollija ja ykkösmatriisin  $\mathbf{1}_{m \times n} = (1)_{m \times n}$  ykkösiä. Merkinnät voi lyhentää:  $\mathbf{0} = \mathbf{0}_{m \times n}$  ja  $\mathbf{1} = \mathbf{1}_{m \times n}$ .

**Lause 3.25.** Olkoon  $m, n \geq 1$ . Silloin  $(\mathbb{B}_{m \times n}, +, \cdot, -, \mathbf{0}_{m \times n}, \mathbf{1}_{m \times n})$  on Boolean algebra, jossa on  $2^{mn}$  alkioita.

*Todistus.* Joukon  $\mathbb{B}_{m \times n}$  yhdisteen ja kohtauksen assosiativisuus, kommutatiivisuus ja keskinäiset distributiivisuudet seuraavat Boolean algebran  $\mathcal{B}_2$  yhdisteen ja kohtauksen ominaisuuksista. Nollamatriisi on yhdisteen neutraalialkio ja ykkösmatriisi kohtauksen. Komplementille pätee lait  $\mathbf{A} + \overline{\mathbf{A}} = \mathbf{1}$  ja  $\mathbf{A} \odot \overline{\mathbf{A}} = \mathbf{0}$ .  $\square$

Huomaa, että Boolean matriisien kohtausta  $\odot$  ei ole vastaa matriisien tavallista kertolaskua. Boolean matriisien tulo lasketaan samalla periaatteella kuin tavallisten matriisien tulo. Tulossa käytetään alkioiden yhteenlaskuna  $\mathcal{B}_2$ :n yhdistettä ja kertolaskuna  $\mathcal{B}_2$ :n kohtausta.

**Määritelmä 3.26.** Olkoon  $\mathbf{A} = (a_{ij})$  Boolean  $m \times n$ -matriisi ja  $\mathbf{B} = (b_{ij})$  Boolean  $n \times p$ -matriisi. Matriisien  $\mathbf{A}$  ja  $\mathbf{B}$  tulo  $\mathbf{AB} = (c_{ij})$  on Boolean  $m \times p$ -matriisi, missä

$$c_{ij} = (a_{i1} \cdot b_{1j}) + (a_{i2} \cdot b_{2j}) + \cdots + (a_{in} \cdot b_{nj}) \stackrel{\text{merk.}}{=} \sum_{k=1}^n (a_{ik} \cdot b_{kj}),$$

kun  $1 \leq i \leq m$  ja  $1 \leq j \leq p$ . Huomaa, että summa merkintä  $\sum$  vastaa tässä Boolean algebran  $\mathcal{B}_2$  yhdistettä  $+$ , ja  $\cdot$  on  $\mathcal{B}_2$ :n kohtausta.

**Esimerkki 3.27.** Olkoot

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{ja} \quad \mathbf{B} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Boolean  $2 \times 3$ -matriisi ja  $3 \times 4$ -matriisi. Niiden tulo on  $2 \times 4$ -matriisi

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

Esimerkiksi alkio  $c_{24}$  on  $\sum_{k=1}^3 (a_{2k} \cdot b_{k4}) = (a_{21} \cdot b_{14}) + (a_{22} \cdot b_{24}) + (a_{23} \cdot b_{34}) = (1 \cdot 1) + (0 \cdot 1) + (0 \cdot 1) = 1 + 0 + 0 = 1$ .

**Määritelmä 3.28.** Olkoon  $\mathbf{A} = (a_{ij})$  Boolean  $m \times n$ -matriisi. Sen **transpoosi**  $\mathbf{A}^T = (c_{ij})$  on Boolean  $n \times m$ -matriisi, jossa

$$c_{ij} = a_{ji},$$

kun  $1 \leq i \leq n$  ja  $1 \leq j \leq m$ .

**Esimerkki 3.29.** Matriisin  $\mathbf{A}$  transpoosi  $\mathbf{A}^T$  saadaan yksinkertaisesti vaihtamalla matriisin  $\mathbf{A}$  rivit transpoosin sarakkeiksi:

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad \mathbf{A}^T = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

Samantyyppisten matriisien välillä on pienempi tai yhtä kuin -relaatio.

**Määritelmä 3.30.** Olkoot  $\mathbf{A} = (a_{ij})$  ja  $\mathbf{B} = (b_{ij})$  Boolean  $m \times n$ -matriiseja. Silloin

$$\mathbf{A} \leq \mathbf{B} \quad \text{joss} \quad a_{ij} \leq b_{ij} \quad \text{kaikilla } 1 \leq i \leq m, 1 \leq j \leq n.$$

Huomaa, että koska  $a_{ij}, b_{ij} \in \{0, 1\}$ , niin ehto  $a_{ij} \leq b_{ij}$  on yhtäpitävä ehdon ( $a_{ij} = 0$  tai  $b_{ij} = 1$ ) kanssa.

**Esimerkki 3.31.** Joukossa  $\mathbb{B}_{2 \times 3}$  on voimassa

$$\mathbf{0}_{2 \times 3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \leq \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \leq \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \leq \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \mathbf{1}_{2 \times 3}.$$

Boolean algebrassa ovat voimassa olevat ns. yleistetyt distribuutiivilait, jotka esitetään seuraavaksi. Käytetään lyhennysmerkintää kohtaukselle

$$b_1 \cdot b_2 \cdots b_n \stackrel{\text{merk.}}{=} \prod_{k=1}^n b_k.$$

**Lemma 3.32** (Yleistetyt distribuutiivilait). *Kun  $a, b_1, \dots, b_n \in B$ , niin*

$$a \cdot \left( \sum_{k=1}^n b_k \right) = \sum_{k=1}^n (a \cdot b_k) \quad \text{ja} \quad a + \left( \prod_{k=1}^n b_k \right) = \prod_{k=1}^n (a + b_k). \quad \square$$

Seuraavat laskulait ovat voimassa Boolean matriisien tulolle.

**Lause 3.33.** *Kun  $\mathbf{A}, \mathbf{B}$  ja  $\mathbf{C}$  ovat kussakin kohdassa sopivaa tyyppiä olevia matriiseja, on voimassa*

1.  $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$  *assosiatiivisuus,*
2.  $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$  *distributiivisuus,*
3.  $(\mathbf{A}^T)^T = \mathbf{A}$  *kaksoistranspoosi,*
4.  $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$  *summan transpoosi,*
5.  $(\mathbf{AB})^T = \mathbf{B}^T \mathbf{A}^T$  *tulon transpoosi.*

*Todistus.* Todistetaan kohdat (i) ja (iv) ja jätetään muut harjoitustehtäviksi.

(i) Jotta kertolaskut voidaan suorittaa, matriisin  $\mathbf{A}$  on oltava tyyppiä  $m \times n$ , matriisin  $\mathbf{B}$  tyyppiä  $n \times p$  ja matriisin  $\mathbf{C}$  tyyppiä  $p \times q$ .

Osoitetaan matriisin  $\mathbf{A}(\mathbf{BC})$  kohdan  $i, j$  alkio samaksi kuin matriisin  $(\mathbf{AB})\mathbf{C}$  kohdan  $i, j$  alkio, missä  $1 \leq i \leq m$  ja  $1 \leq j \leq q$ , käyttämällä yleistä distribuutiivilakia:

$$\begin{aligned} (\mathbf{A}(\mathbf{BC}))_{ij} &= \sum_{k=1}^n ((\mathbf{A})_{ik} \cdot (\mathbf{BC})_{kj}) = \sum_{k=1}^n ((\mathbf{A})_{ik} \cdot \sum_{\ell=1}^p ((\mathbf{B})_{k\ell} \cdot (\mathbf{C})_{\ell j})) \\ &= \sum_{k=1}^n \sum_{\ell=1}^p ((\mathbf{A})_{ik} \cdot (\mathbf{B})_{k\ell} \cdot (\mathbf{C})_{\ell j}) = \sum_{\ell=1}^p \sum_{k=1}^n ((\mathbf{A})_{ik} \cdot (\mathbf{B})_{k\ell} \cdot (\mathbf{C})_{\ell j}) \\ &= \sum_{\ell=1}^p ((\mathbf{AB})_{i\ell} \cdot (\mathbf{C})_{\ell j}) = ((\mathbf{AB})\mathbf{C})_{ij}. \end{aligned}$$

(iv) Nyt  $\mathbf{A}$  ja  $\mathbf{B}$  ovat  $m \times n$ -matriiseja ja tarkastellaan kohdan  $i, j$  alkioita, jossa  $1 \leq i \leq n$  ja  $1 \leq j \leq m$ :

$$\begin{aligned} ((\mathbf{A} + \mathbf{B})^T)_{ij} &= (\mathbf{A} + \mathbf{B})_{ji} = (\mathbf{A})_{ji} + (\mathbf{B})_{ji} \\ &= (\mathbf{A}^T)_{ij} + (\mathbf{B}^T)_{ij} = (\mathbf{A}^T + \mathbf{B}^T)_{ij}. \end{aligned}$$

□

### 3.6 Sovellus: Relaation esitys Boolean matriisin avulla\*

Boolean matriisien avulla voidaan esittää äärellisiä binäärisiä **relaatioita**. Kun  $A$  ja  $B$  ovat joukkoja, mikä tahansa karteesisen tulon  $A \times B$  osajoukko  $R$  on binäärinen relaatio joukosta  $A$  joukkoon  $B$ . Kun  $(a, b) \in R$ , merkitään myös  $a R b$ . Ts.

$$R = \{(a, b) \mid a \in A, b \in B, a R b\}.$$

Relaation  $R$  **käänteisrelaatiota** merkitään  $R^{-1}$  ja se on  $\{(b, a) \mid (a, b) \in R\}$ . Jos  $R$  on relaatio joukosta  $A$  joukkoon  $B$  ja  $S$  relaatio joukosta  $B$  joukkoon  $C$ , relaatioiden **yhdiste** on  $R \circ S = \{(a, c) \mid (a, b) \in R \text{ ja } (b, c) \in S \text{ jollakin } b \in B\}$ .

Jos  $R$  on relaatio joukossa  $A$  (eli  $R \subseteq A \times A$ ), niin määritellään relaation  $R$  potenssit:

1.  $R^0 = I_A = \{(a, a) \mid a \in A\}$ , ja
2.  $R^{n+1} = R^n \circ R$ .

Relaatioista saadaan uusia relaatioita joukko-opin operaatioilla unioni, leikkaus ja komplementti. Näiden matriisit voidaan laskea myös suoraan matriiseja käyttämällä. Huomaa, että  $R^C = A \times B \setminus R$ .

**Määritelmä 3.34.** Olkoot  $A = \{a_1, \dots, a_m\}$  ja  $B = \{b_1, \dots, b_n\}$  äärellisiä joukkoja. Oletetaan, että joukkojen alkioilla on indeksoinnin mukainen järjestys, ts.  $a_1 \leq a_2 \leq \dots \leq a_m$  ja  $b_1 \leq \dots \leq b_n$ . Olkoon  $R$  binäärinen relaatio joukosta  $A$  joukkoon  $B$ . Silloin relaation  $R$  **matriisi**  $\mathbf{M}_R = (r_{ij})$  on Boolean  $m \times n$ -matriisi, jolle

$$r_{ij} = \begin{cases} 1, & \text{jos } a_i R b_j, \\ 0 & \text{muuten.} \end{cases}$$

**Esimerkki 3.35.** Olkoon  $A = \{x, y, z\}$  ja  $B = \{a, b, c, d, e, f\}$ . Relaatiossa  $R \subseteq A \times B$  on voimassa  $x R a, y R c, y R f$  ja  $z R e$ . Silloin relaation matriisi on

$$\mathbf{M}_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

**Lause 3.36.** *Olkoon joukot  $A = \{a_1, \dots, a_m\}$  ja  $B = \{b_1, \dots, b_n\}$  järjestetty indeksoinnin mukaan. Kun  $R$  ja  $S$  ovat relaatioita joukosta  $A$  joukkoon  $B$ , niin*

1.  $\mathbf{M}_R = \mathbf{M}_S$ , jos ja vain jos  $R = S$ ,
2.  $\mathbf{M}_R \leq \mathbf{M}_S$ , jos ja vain jos  $R \subseteq S$ ,
3.  $\mathbf{M}_{R \cup S} = \mathbf{M}_R + \mathbf{M}_S$ ,
4.  $\mathbf{M}_{R \cap S} = \mathbf{M}_R \odot \mathbf{M}_S$ ,
5.  $\mathbf{M}_{R^c} = \overline{\mathbf{M}_R}$ ,
6.  $\mathbf{M}_\emptyset = \mathbf{0}_{m \times n}$  ja  $\mathbf{M}_{A \times B} = \mathbf{1}_{m \times n}$ .

*Todistus.* Todistetaan esimerkkinä kohta (ii), muut kohdat jätetään harjoitustehtäväksi:

$$\begin{array}{ll}
 \mathbf{M}_R \leq \mathbf{M}_S & \text{joss } (\mathbf{M}_R)_{ij} \leq (\mathbf{M}_S)_{ij} \text{ kaikilla } i, j \\
 & \text{joss } (\mathbf{M}_R)_{ij} = 0 \text{ tai } (\mathbf{M}_S)_{ij} = 1 \text{ kaikilla } i, j \\
 & \text{joss } a_i \bar{R} b_j \text{ tai } a_i S b_j \text{ kaikilla } i, j \\
 & \text{joss } a_i R b_j \Rightarrow a_i S b_j \text{ kaikilla } i, j \\
 & \text{joss } (a_i, b_j) \in R \Rightarrow (a_i, b_j) \in S \text{ kaikilla } i, j \\
 & \text{joss } R \subseteq S.
 \end{array}$$

□

Myös käänteisrelaation ja yhdistetyn relaation matriisit saadaan alkuperäisten relaatioiden matriiseista.

**Lause 3.37.** *Olkoon  $A = \{a_1, \dots, a_m\}$ ,  $B = \{b_1, \dots, b_n\}$  ja  $C = \{c_1, \dots, c_p\}$  joukkoja, joilla on indeksoinnin mukainen järjestys, ja olkoon  $R$  relaatio joukosta  $A$  joukkoon  $B$  ja  $S$  relaatio joukosta  $B$  joukkoon  $C$ . Silloin*

1.  $\mathbf{M}_{R^{-1}} = \mathbf{M}_R^T$  ja
2.  $\mathbf{M}_{R \circ S} = \mathbf{M}_R \mathbf{M}_S$ .

*Todistus.* Osoitetaan kohta (ii), kohta (i) jätetään harjoitustehtäväksi.

Matriisi  $\mathbf{M}_{RS}$  on tyyppiä  $m \times p$  ja matriisit  $\mathbf{M}_R$  ja  $\mathbf{M}_S$  vastaavasti tyyppiä  $m \times n$  ja  $n \times p$ , joten tyypit sopivat yhteen. Olkoon  $1 \leq i \leq m$  ja  $1 \leq j \leq p$ .

Silloin

$$\begin{aligned}
 (\mathbf{M}_{R \circ S})_{ij} = 1 & \quad \text{joss} \quad a_i R \circ S c_j \\
 & \quad \text{joss} \quad a_i R b_k, \quad b_k S c_j \quad \text{jollakin } b_k \in B \\
 & \quad \text{joss} \quad (\mathbf{M}_R)_{ik} = 1, \quad (\mathbf{M}_S)_{kj} = 1 \quad \text{jollakin } 1 \leq k \leq n \\
 & \quad \text{joss} \quad (\mathbf{M}_R)_{ik} \cdot (\mathbf{M}_S)_{kj} = 1 \quad \text{jollakin } 1 \leq k \leq n \\
 & \quad \text{joss} \quad \sum_{k=1}^n ((\mathbf{M}_R)_{ik} \cdot (\mathbf{M}_S)_{kj}) = 1 \\
 & \quad \text{joss} \quad (\mathbf{M}_R \mathbf{M}_S)_{ij} = 1.
 \end{aligned}$$

Näin ollen matriisien  $\mathbf{M}_{R \circ S}$  ja  $\mathbf{M}_R \mathbf{M}_S$  kohdan  $i, j$  alkioit ovat molemmat 1 tai molemmat 0, joten matriisit ovat samat.  $\square$

Tarkastellaan lopuksi binäärisiä relaatioita joukossa  $A = \{a_1, \dots, a_n\}$ . Relaation  $R \subseteq A \times A$  matriisi on  $n \times n$ -matriisi.

**Määritelmä 3.38.** Boolean  $n \times n$ -identiteettimatriisi on

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Joukon  $A$  identiteettirelaatioissa  $I_A$  on voimassa  $a I_A b$ , jos ja vain jos  $a = b$ . Identiteettirelaation matriisi on siis  $\mathbf{I}_n$ .

Kun  $R$  on joukon  $A$  relaatio, sen potenssit  $R^i$  ovat myös joukon  $A$  relaatioita. Olkoon  $|A| = n$ . Relaation  $R \subseteq A \times A$  transitiivinen sulkeuma on relaatio  $R^+ = R \cup R^2 \cup \dots \cup R^n$  ja sen refleksiivinen transitiivinen sulkeuma on relaatio  $R^* = I_A \cup R^+$ .

**Lause 3.39.** Olkoon  $A$  joukko, jossa on  $n$  alkioita, ja olkoon  $R$  relaatio joukossa  $A$ . Silloin

1.  $\mathbf{M}_{I_A} = \mathbf{I}_n$ ,
2.  $\mathbf{M}_{R^m} = \mathbf{M}_R^m$  kaikilla  $m \geq 0$ ,
3.  $\mathbf{M}_{R^+} = \mathbf{M}_R^1 + \mathbf{M}_R^2 + \dots + \mathbf{M}_R^n$ ,
4.  $\mathbf{M}_{R^*} = \mathbf{I}_n + \mathbf{M}_R^1 + \mathbf{M}_R^2 + \dots + \mathbf{M}_R^n$ .

*Todistus.* Kohta (i) on selvä.

Lauseen 3.37 mukaan  $\mathbf{M}_{R^2} = \mathbf{M}_R \mathbf{M}_R$ . Induktiolla yleistämällä saadaan tulos  $\mathbf{M}_{R^m} = \mathbf{M}_R^m$ , kun  $m \geq 1$ . Lisäksi, koska  $R^0 = I_A$ , saadaan  $\mathbf{M}_{R^0} = \mathbf{M}_{I_A} = \mathbf{I}_n = \mathbf{M}_R^0$ . Tästä seuraa kohta (ii).

Kohdat (iii) ja (iv) seuraavat nyt relaatioiden  $R^+$  ja  $R^*$  määritelmistä:  $\square$

**Esimerkki 3.40.** Olkoon joukon  $A = \{a, b, c\}$  relaatio  $R$  seuraava:  $a R a$ ,  $b R c$  ja  $c R a$ . Silloin relaation transitiivisen sulkeuman matriisi  $\mathbf{M}_{R^+}$  ja refleksiivisen transitiivisen sulkeuman matriisi  $\mathbf{M}_{R^*}$  lasketaan näin:

$$\mathbf{M}_R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \mathbf{M}_{R^2} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \mathbf{M}_{R^3} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{M}_{R^+} = \mathbf{M}_R + \mathbf{M}_{R^2} + \mathbf{M}_{R^3} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \mathbf{M}_{R^*} = \mathbf{I}_3 + \mathbf{M}_{R^+} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

## 4 Kielet ja äärelliset automaattit

Tässä luvussa tutustutaan formaalisten kielten ja automaattien terorian perusteisiin.

### 4.1 Aakkosto, sana ja kieli

**Määritelmä 4.1.** *Aakkosto*  $\Sigma$  on äärellinen joukko, jonka alkioita kutsutaan *kirjaimiksi* tai *symboleiksi*. *Sana*  $w$  on äärellinen jono  $w = x_1x_2 \cdots x_m$  symboleita  $x_1, x_2, \dots, x_m$  aakkostosta  $\Sigma$ . *Tyhjässä sanassa*  $\varepsilon$  ei ole yhtään kirjainta. Kaikkien aakkoston  $\Sigma$  sanojen joukko on  $\Sigma^*$ . Siis

$$\Sigma^* = \{x_1x_2 \cdots x_m \mid m \in \mathbb{N}, x_1, x_2, \dots, x_m \in \Sigma\}.$$

**Esimerkki 4.2.** Jos aakkosto on  $\Sigma = \{a, b, c\}$ , niin sen sanoja ovat  $\varepsilon, a, b, c, ab, acacabbb, \dots$

**Esimerkki 4.3.** *Binääriaakkoston*  $\Sigma = \{0, 1\}$  sanoja ovat kaikenlaiset bit-tijonot  $\varepsilon, 0, 1, 00, 10011101, \dots$

**Määritelmä 4.4.** Sanan  $w = x_1x_2 \cdots x_m$  *pituus*  $|w|$  on  $m$ , kun  $x_1, x_2, \dots, x_m \in \Sigma$ . Jokainen  $x_i$  *esiintyy* sanassa  $x_1x_2 \cdots x_m$ . Kirjaimen  $a$  esiintymien määrä sanassa  $w$  on  $|w|_a$ .

**Esimerkki 4.5.**  $|\varepsilon| = 0$  ja  $|abbcc| = 5$ . Sanassa  $w = abbcaac$  kirjaimet  $b$  ja  $c$  esiintyvät kahdesti, ja kirjaimella  $b$  on kaksi esiintymää sanassa  $w$ .  $|abbcaac|_a = 3$

Jos sama kirjain esiintyy peräkkäin, voidaan merkintää lyhentää. Kun  $a \in \Sigma$ ,  $a^i$  on sana  $aa \dots a$ , missä kirjaimia  $a$  on  $i$  kappaletta. Merkitään myös  $a^0 = \varepsilon$ .

**Määritelmä 4.6.** Sanojen  $u = x_1 \cdots x_m$  ja  $v = y_1 \cdots y_n$  *yhdiste* eli *katenaatio*  $u \cdot v$  on  $x_1 \dots x_m y_1 \dots y_n$ . Piste voidaan jättää pois ja silloin  $uv = u \cdot v$ .

katenoitavat sanat kirjoitetaan yksinkertaisesti peräkkäin. Huomaa, että sanojen yhdistäminen on assosiatiivinen operaatio. Lisäksi tyhjän sanan katenoiminen mihin tahansa sanaan ei muuta sanaa:  $\varepsilon \cdot w = w \cdot \varepsilon = w$ .

**Esimerkki 4.7.** Jos  $u = abbcc$  ja  $v = abc$ , niin  $u \cdot v = abbccabc$ .

**Määritelmä 4.8.** *Kieli*  $L$  on jokin joukko aakkoston  $\Sigma$  sanoja. Siis  $L \subseteq \Sigma^*$ .

**Esimerkki 4.9.**  $\{abc, ac\}$ ,  $\Sigma^*$  ja  $\emptyset$  ovat aakkoston  $\Sigma = \{a, b, c\}$  kieliä. Samoin  $\{b^i \mid i \in \mathbb{N}\} = \{\varepsilon, b, bb, bbb, \dots\}$  on kieli.

Sana-jonoja voidaan määritellä induktiivisesti. Näiden ominaisuuksia voidaan sitten todistaa käyttämällä induktiota.

**Esimerkki 4.10.** Olkoon  $\Sigma = \{a, b\}$ . Sanat  $w_0, w_1, \dots$ , määritellään kaavoilla  $w_0 = a$ ,  $w_{i+1} = w_i \cdot b$ . Silloin  $w_1 = w_0b = ab$ ,  $w_2 = w_1b = abb$ , jne. Näytetään, että kun  $i \geq 0$ , niin  $w_i = ab^i$ .

Induktion lähtökohta on  $i = 0$ . Silloin  $w_0 = a = a \cdot \varepsilon = ab^0$  pitää paikkansa. Oletetaan sitten, että  $w_k = ab^k$  jollakin  $k \geq 0$ , ja näytetään  $w_{k+1} = ab^{k+1}$ . Induktio-todistus: määritelmän mukaan  $w_{k+1} = w_k b$ . Induktio-oletuksesta seuraa, että  $w_k b = ab^k b$ , joka on  $ab^{k+1}$ .

**Määritelmä 4.11.** Olkoot  $u$  ja  $w \in \Sigma^*$ . Silloin  $u$  on sanan  $w$  *tekijä*, jos on olemassa sellaiset sanat  $x$  ja  $y \in \Sigma^*$ , että  $w = xuy$ . Jos tässä  $x = \varepsilon$ , niin  $u$  on sanan  $w$  *prefiksi*, ja jos  $y = \varepsilon$ , niin  $u$  on sanan  $w$  *suffiksi*. Tekijä  $u$  on *aito*, jos  $u \neq w$ . Sanan  $w$  tekijä on siis jokin sanan  $w$  yhtenäinen osasana. Jos tekijä sijaitsee sanan alussa, se on prefiksi, jos taas lopussa, se on suffiksi. Sanan  $w \in \Sigma^*$  *peilisana* eli *käänteissana*  $w^R$  on sana, joka luettuna oikealta vasemmalle on  $w$ .

**Esimerkki 4.12.** Sanan *aabbccddd* tekijöitä ovat *aab*, *bccd* ja *dd*. Näistä *aab* on prefiksi ja *dd* on suffiksi. Sanan *acbb* peilisana on  $(acbb)^R = bbca$ .

## 4.2 Kielten operaatioita

Kieli on kaikkien sanojen joukon  $\Sigma^*$  osajoukko ja siten se voi olla ääretön tai äärellinen. Pieni äärellinen kieli voidaan esittää luettelemalla kaikki siihen kuuluvat sanat. Kielet voidaan esittää myös jonkin niiden ominaisuuden avulla, esim.  $L = \{w \in \Sigma^* \mid w:ssä \text{ ei esiinny kirjainta } a\}$ . Kolmas mahdollisuus on käyttää erilaisia operaatioita.

Ensinnäkin kieliä voi käsitellä joukkoina. Silloin kielille  $L$  ja  $K \subseteq \Sigma^*$  voidaan määritellä seuraavat operaatiot:

unioni	$L \cup K = \{w \mid w \in L \text{ tai } w \in K\}$	Esimerkiksi jos $K = \{abc, cc\}$
leikkaus	$L \cap K = \{w \mid w \in L \text{ ja } w \in K\}$	
komplementti	$L^c = \Sigma^* \setminus L = \{w \in \Sigma^* \mid w \notin L\}$	
erotus	$L \setminus K = \{w \mid w \in L, w \notin K\}$	

$\{abc, aac, cc\}$  ja  $L = \{abc, cc, ccc\}$ , niin  $K \cup L = \{abc, aac, cc, ccc\}$ ,  $K \cap L = \{abc, cc\}$  ja  $K \setminus L = \{aac\}$ .

Kahden kielen  $L$  ja  $K$  *tulo* eli *katenaatio*  $LK$  on kieli, jonka jokainen sana saadaan aikaan yhdistämällä mikä tahansa kielen  $L$  sana mihin tahansa kielen  $K$  sanaan:

$$LK = \{uv \mid u \in L, v \in K\}.$$

Esimerkiksi jos  $L = \{ab^i \mid i \in \mathbb{N}\}$  ja  $K = \{c^j \mid c \in \mathbb{N}\}$ , niin

$$LK = \{ab^i c^j \mid i, j \in \mathbb{N}\}.$$

Kun kieli  $L$  katenoidaan itsensä kanssa, saadaan kielen  $L$  toinen potenssi  $LL$ , jota voidaan merkitä  $L^2$ . Jos  $n \in \mathbb{N}$ , niin kielen  $L$   $n$ :s potenssi saadaan katenoimalla kieli itsensä kanssa  $n$  kertaa. Rekursiivisesti sama voidaan määritellä  $L^0 = \{\varepsilon\}$  ja  $L^{n+1} = L^n L$ . Esimerkiksi kielen  $L = \{ab^i \mid i \in \mathbb{N}\}$  kolmas potenssi on  $L^3 = \{ab^i ab^j ab^k \mid i, j, k \in \mathbb{N}\}$ .

Kielen  $L$  *iteraatio* sisältää kaikki kielen  $L$  potenssit:

$$L^* = \bigcup_{i \geq 0} L^i = \{u_1 \dots u_n \mid n \geq 0, u_i \in L\}.$$

Iteraation jokainen sana saadaan siis katenoimalla kielen  $L$  sanoja äärellisen monta kertaa. Huomaa, että myös eri sanat voidaan yhdistää peräkkäin. Esimerkiksi jos  $L = \{ab, bb, ccc\}$ , niin

$$L^* = \{\varepsilon, ab, bb, ccc, abab, abbb, abccc, bbab, bbbb, bbccc, cccab, cccbb, cccccc, ababab, ababbb, \dots\}.$$

Huomaa myös, että iteraatioon kuuluu aina  $L^0$ , joten tyhjä sana  $\varepsilon$  kuuluu aina iteraatioon.

Edellisistä operaatioista unioni, leikkaus ja komplementti ovat *joukko-opillisia* ja unioni, tulo ja iteraatio *säännöllisiä operaatioita*.

**Esimerkki 4.13.** Merkintä  $\Sigma^*$  on selvästi johdonmukainen iteraatiotähden kanssa. Voidaan ajatella, että aakkosto  $\Sigma$  onkin kieli  $L$ , jossa on yksikirjaimisia sanoja. Sen iteraation  $L^*$  sanat ovat muotoa  $w_1 \cdot w_2 \cdot \dots \cdot w_n$ , jossa  $n \in \mathbb{N}$  ja  $w_1, \dots, w_n \in L$ . Koska sanat  $w_1, \dots, w_n$  ovat vain kirjaimia joukosta  $\Sigma$ , niin kieli  $L^*$  on kaikkien sanojen joukko, jonka kirjaimet kuuluvat joukkoon  $\Sigma$ .

**Esimerkki 4.14.** Oletetaan, että  $L = \emptyset$ . Jos sana on muotoa  $w_1 \cdot w_2 \cdot \dots \cdot w_n$ , jossa  $n \in \mathbb{N}$  ja  $w_1, \dots, w_n \in \emptyset$ , ainoa mahdollisuus on, että  $n = 0$ . Silloin sana on katenoitu nolasta kappaleesta sanoja ja on siten tyhjä  $\varepsilon$ . Siis  $\emptyset^* = \{\varepsilon\}$ .

**Lause 4.15.** Jos  $L \subseteq K$ , niin  $L^* \subseteq K^*$ .

*Todistus.* Demonsraatiot. □

**Esimerkki 4.16.** Olkoon  $L$  binääriaakkoston  $\Sigma = \{0, 1\}$  kieli, jonka sanoissa nolliä on eri määrä kuin ykkösiä:  $L = \{w \in \{0, 1\}^* \mid |w|_0 \neq |w|_1\}$ . Näytetään, että  $L^* = \Sigma^*$ . Ensinnäkin  $L^* \subseteq \{0, 1\}^*$ , koska  $L$  on binääriaakkoston kieli. Toisaalta  $\{0, 1\} \subseteq L$ , sillä kummassakin sanassa 0 ja 1 nolliä ja ykkösiä esiintyy eri määrä. Silloin edellisen lauseen nojalla  $\{0, 1\}^* \subseteq L^*$ . Yhteensä siis  $L^* = \{0, 1\}^*$ .

**Lause 4.17.** Mille tahansa kielelle  $L \subseteq \Sigma^*$  pätee  $L^* = \{\varepsilon\} \cup L^* L$ .

*Todistus.* Olkoon  $w \in L^*$ . Silloin  $w$  voidaan jakaa joiksikin sanoiksi  $u_1 \in L, \dots, u_n \in L$  niin, että  $w = u_1 \dots u_n$ . Jos  $n = 0$ , niin sana  $u_1 \dots u_n = \varepsilon$ . Jos taas  $n \geq 1$ , niin sana  $u_1 \dots u_{n-1} \in L^*$  ja sana  $u_n \in L$ , joten  $w \in L^*L$ .

Toisaalta jos  $w = \varepsilon$ , niin  $w \in L^*$ . Jos  $w \in L^*L$ , niin  $w$  voidaan jakaa kahteen sanaan  $u$  ja  $v$ , joista  $u \in L^*$  ja  $v \in L$ . Tällöin  $u$  on muotoa  $u = u_1 \dots u_n$ , missä  $n \geq 0$  ja  $u_1, \dots, u_n \in L$ . Silloin  $w = uv = u_1 \dots u_n v$ , missä  $u_1, \dots, u_n, v \in L$ , joten  $w \in L^*$ .  $\square$

Kielet ovat usein äärettömiä, mutta ne pitäisi pystyä esittämään äärellisessä tilassa. Tarkastelemme tällä kurssilla kahta tapaa kielen esittämiseen: 1) esittämistä kielten operaatioiden avulla kuten edellä, ja 2) esittämistä hyväksyvän automaatin avulla. Huomaa, että kaikkia kieliä ei voida esittää käyttäen näitä tapoja. Nimittäin kieli  $L$  on mikä tahansa äärettömän joukon  $\Sigma^*$  osajoukko ja näitä osajoukkoja on ylinumeroituva määrä.

### 4.3 Säännölliset ilmaisut

**Esimerkki 4.18.** Esitetään seuraava kieli  $L$  muodostamalla se kolmen eri operaation avulla pienemmistä kielistä. Olkoon  $L \in \Sigma^*$ ,  $\Sigma = \{a, b\}$ , kieli, johon kuuluvat ensinnäkin ne sanat, joissa  $b$  esiintyy kaksi kertaa ja  $b$ :n esiintymät eivät saa olla vierekkäin, ja toiseksi ne sanat, joissa  $b$  esiintyy ensimmäisenä kirjaimena ja muut kirjaimet ovat  $a$ -kirjaimia. Silloin  $L$  voidaan esittää muodossa

$$L = (\{a\}^* \cdot \{b\} \cdot \{a\}^* \cdot \{a\} \cdot \{b\} \cdot \{a\}^*) \cup (\{b\} \cdot \{a\}^*)$$

käyttäen ainoastaan kieliä, joissa on yksi yksikirjaiminen sana, ja säännöllisiä operaatioita, eli unionia, katenaatiota ja iteraatiota. Kun sulut ja piste jätetään pois, saadaan säännöllinen ilmaisu  $a^*ba^*aba^* \cup ba^*$ , joka esittää kieltä  $L$ .

**Määritelmä 4.19.** *Säännöllinen ilmaisu* (regular expression) aakkostossa  $\Sigma$  määritellään seuraavasti.

1.  $\emptyset$  ja  $a$  ovat säännöllisiä ilmaisuja, kun  $a \in \Sigma$ .
2. Jos  $\alpha$  ja  $\beta$  ovat säännöllisiä ilmaisuja, niin myös  $(\alpha \cup \beta)$ ,  $(\alpha\beta)$  ja  $\alpha^*$  ovat.
3. Tässä ovat kaikki säännölliset ilmaisut.

Vähentääksemme sulkujen määrää sovimme operaatioiden presedenssin niin, että iteraatiota sovelletaan ensiksi, sitten katenaatiota ja viimeiseksi unionia. Silloin esimerkiksi  $\alpha \cup \beta\gamma^*$  tarkoittaa ilmaisua  $\alpha \cup (\beta(\gamma)^*)$ .

**Esimerkki 4.20.** Olkoon  $\Sigma = \{a, b, c\}$ . Säännöllisiä ilmaisuja ovat  $\emptyset$ ,  $a$ ,  $ab$ ,  $abcc$ ,  $a \cup abcc$ ,  $(a \cup abcc)aa$ ,  $(ab)^*$  ja  $ab^*$ .

Säännöllinen ilmaisu on nyt vain sana, mutta sen on tarkoitus edustaa kokonaista kieltä. Määritellään seuraavaksi, mitä kieltä säännöllinen ilmaisu esittää, vaikka se käykin melko selvästi ilmi esimerkistä.

**Määritelmä 4.21.** Säännöllinen ilmaisu  $\alpha$  *esittää* kieltä  $L(\alpha)$  seuraavasti.

1.  $L(\emptyset) = \emptyset$  ja  $L(a) = \{a\}$ , kun  $a \in \Sigma$ .
2.  $L(\alpha \cup \beta) = L(\alpha) \cup L(\beta)$ ,  $L(\alpha\beta) = L(\alpha)L(\beta)$  ja  $L(\alpha^*) = L(\alpha)^*$ .

Tässä  $L$  on funktio säännöllisten ilmaisujen joukolta kielten joukkoon. Esimerkin 4.18 kieli voidaan kirjoittaa uudestaan muotoon  $L(a^*ba^*aba^* \cup ba^*) = L$ .

**Esimerkki 4.22.** Mitä kieltä esittää säännöllinen ilmaisu  $a^*(b \cup c)$ ? Lasketaan siis  $L(a^*(b \cup c))$ .

$$\begin{aligned} L(a^*(b \cup c)) &= L(a^*)L(b \cup c) = L(a)^*L(b \cup c) \\ &= L(a)^*(L(b) \cup L(c)) = \{a\}^*(\{b\} \cup \{c\}) = \{a\}^*\{b, c\}. \end{aligned}$$

Tuloksena saadaan kieli, jonka sanat alkavat nolalla tai useammalla  $a$ -kirjaimella ja päättyvät  $b$ - tai  $c$ -kirjaimeseen.

**Määritelmä 4.23.** Olkoot  $\alpha$  ja  $\beta$  säännöllisiä ilmaisuja. Jos ne esittävät samaa kieltä eli  $L(\alpha) = L(\beta)$ , niin  $\alpha$  ja  $\beta$  ovat *ekvivalentit* ja merkitään  $\alpha \equiv \beta$ .

**Esimerkki 4.24.** Ilmaisu  $a(aa)^*$  esittää kieltä, jonka sanat ovat paritonta pituutta, ja  $(aa)^*$  kieltä, jonka sanat ovat parillista pituutta. Siksi voidaan kirjoittaa  $a(aa)^* \cup (aa)^* \equiv a^*$ .

**Määritelmä 4.25.** Kieli  $L$  on *säännöllinen*, jos jokin säännöllinen ilmaisu  $\alpha$  esittää sitä. Kaikkien aakkoston  $\Sigma$  säännöllisten kielten joukko on  $\mathcal{REG}(\Sigma)$ .

Määritelmän mukaan siis kieli  $L \subseteq \Sigma^*$  on säännöllinen, jos a)  $L = \emptyset$ , b)  $L = \{a\}$  jollekin  $a \in \Sigma$ , c)  $L = L_1 \cup L_2$ , d)  $L = L_1L_2$  tai e)  $L = L_1^*$  joillekin säännöllisille kielille  $L_1$  ja  $L_2$ .

**Esimerkki 4.26.** Kieli  $\{\varepsilon\}$  on säännöllinen, sillä  $\emptyset^*$  esittää sitä.

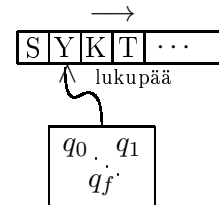
**Esimerkki 4.27.** Olkoon  $\Sigma = \{a, b, c\}$ . Kieli, jossa on kaikki sanat, joiden prefiksi on  $aa$ , on säännöllinen, sillä  $aa(a \cup b \cup c)^*$  esittää sitä.

Myöhemmin näytämme, että kieli  $\{a^n b^n \mid n \geq 0\}$  ei ole säännöllinen kieli.

#### 4.4 Epädeterministinen äärellinen automaatti

Säännölliset kielet voidaan tunnistaa äärellisten automaattien avulla. Äärellinen automaatti on laskentamalli, jolla on äärellinen muisti.

Äärellisessä automaatissa on syöttönauha, sitä lukeva lukupää ja äärellinen määrä sisäisiä tiloja. Se lukee syöttöä symboli kerrallaan ja valitsee uuden tilan lukemansa kirjaimen ja nykyisen tilan mukaan. Alussa automaatti on tiettyssä alkutilassa. Se hyväksyy lukemansa syöttösanan, jos se pystyy saavuttamaan jonkin erityisistä lopputiloista lukemalla koko syöttösanan. Kaikki sanat, jotka automaatti hyväksyy, muodostavat automaatin hyväksymän kielen.



**Määritelmä 4.28.** *Epädeterministinen äärellinen automaatti* on viisikko

$$\mathcal{A} = (Q, \Sigma, \Delta, q_0, F),$$

missä

1.  $Q$  on äärellinen joukko *tiloja*,
2.  $\Sigma$  on äärellinen *syöttöaakkosto*,
3.  $\Delta \subseteq Q \times (\Sigma \cup \{\varepsilon\}) \times Q$  on *siirtymärelaatio*,
4.  $q_0 \in Q$  on *alkutila* ja
5.  $F \subseteq Q$  on *lopputilojen* joukko.

Siirtymärelaatio  $\Delta$  on joukko kolmikkoja muotoa  $(q, a, r)$ , jossa  $q$  ja  $r \in Q$  ja  $a \in \Sigma$ . Se määrää automaatin toiminnan. Jos  $(q, a, r) \in \Delta$  ja automaatti on tilassa  $q$  ja seuraavaksi luettava kirjain syöttönauhalla on  $a$ , niin automaatti voi siirtyä tilaan  $r$ . Siirtymää  $(q, a, r)$  voidaan nimittää *a-siirtymäksi*. Jos siirtymässä  $(q, \varepsilon, r)$  ei ole kirjainta vaan  $\varepsilon$ , niin automaatti voi siirtyä tilasta  $q$  tilaan  $r$  lukematta yhtään kirjainta. Tällaista siirtymää sanotaan  *$\varepsilon$ -siirtymäksi*. Merkitään  $a$ - ja  $\varepsilon$ -siirtymää seuraavasti:

$$q \xrightarrow{a} r \quad \text{ja} \quad q \xrightarrow{\varepsilon} r.$$

Kun epädeterministinen automaatti  $\mathcal{A}$  lukee sanan  $w \in \Sigma^*$ , niin se kulkee joidenkin tilojen  $q_1, \dots, q_n$  kautta. Aina, kun se kulkee tilasta  $q_{i-1}$  tilaan  $q_i$ , se joko lukee syöttösanan yhden kirjaimen tai siirtyy uuteen tilaan lukematta mitään. Voidaan sanoa, että se lukee syöttösanan osan  $x_i \in (\Sigma \cup \{\varepsilon\})$ . Täten  $w$  voidaan jakaa sellaisiin osiin  $w = x_1 \dots x_n$ , että

$$(q_{i-1}, x_i, q_i) \in \Delta,$$

kun  $i = 1, \dots, n$ . Nyt sanan  $w$  lukeva *lasku* on siirtymien jono alkutilasta  $q_0$  johonkin tilaan  $q_n$ , jossa jokainen sanan  $w$  kirjain tulee luetuksi. Se voidaan kirjoittaa muodossa

$$q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \dots \xrightarrow{x_{n-1}} q_{n-1} \xrightarrow{x_n} q_n$$

ja voidaan lyhentää muotoon

$$q_0 \xrightarrow{x_1 \dots x_n} q_n.$$

Jos viimeinen tila  $q_n$  on lopputila, lasku on *hyväksyvä*, muuten *hylkäävä*.

Merkitään myös  $q \xrightarrow{\varepsilon} q$ , kun  $q \in Q$ . Jos halutaan korostaa, että  $p \xrightarrow{w} q$  on automaatin  $\mathcal{A}$  lasku, merkitään  $p \xrightarrow[\mathcal{A}]{w} q$ .

Yhdellä sanalla voi olla monta laskua: kun automaatti on tilassa  $q$  ja lukee kirjaimen  $a$  ja relaatiossa  $\Delta$  on kolmikot  $(q, a, r)$  ja  $(q, a, s)$ , automaatti voi siirtyä tilaan  $r$  tai  $s$ . Tässä lasku haarautuu kahdeksi laskuksi. Samoin jos lisäksi relaatiossa  $\Delta$  on kolmikko  $(q, \varepsilon, t)$ , automaatti voikin siirtyä tilaan  $t$  lukematta mitään, ja saadaan kolmas lasku. Myös voi käydä niin, että syöttösanan seuraavaksi luettava kirjain on  $a$  ja tilasta  $q$  ei ole yhtään  $a$ - eikä  $\varepsilon$ -siirtymää. Silloin lasku on keskeytettävä ja lasku on hylkäävä. Sana  $w$  hyväksytään, jos ainakin yksi laskuista  $q_0 \xrightarrow{w} q_n$  on hyväksyvä.

Epädeterministinen automaatti  $\mathcal{A}$  *tunnistaa* eli *hyväksyy* sanan, jos sanalla on ainakin yksi hyväksyvä lasku. Epädeterministisen automaatin  $\mathcal{A}$  *tunnistama* eli *hyväksymä* kieli on sen hyväksymien sanojen joukko

$$L(\mathcal{A}) = \{w \in \Sigma^* \mid q_0 \xrightarrow{w} q_n \text{ jollekin } q_n \in F\}.$$

Automaatti voidaan esittää *siirtymägraafin* avulla, jossa jokaista tilaa kohti on ympyrä ja jokaista siirtymää  $(q, x, r)$  kohti on symbolilla  $x$  merkitty nuoli tilasta  $q$  tilaan  $r$ . Alkutila merkitään siihen tulevalla lyhyellä nuolella ja jokainen lopputila siitä lähtevällä lyhyellä nuolella.

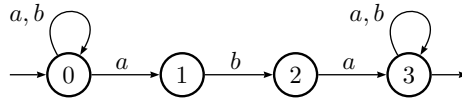
**Esimerkki 4.29.** Olkoon  $\mathcal{A} = (\{0, 1, 2, 3\}, \{a, b\}, \Delta, 0, \{3\})$  automaatti, jonka siirtymärelaatio on

$$\Delta = \{(0, a, 0), (0, b, 0), (0, a, 1), (1, b, 2), (2, a, 3), (3, a, 3), (3, b, 3)\}.$$

Automaatin  $\mathcal{A}$  siirtymägraafi on alla. Sanalla *baba* on seuraavat laskut:

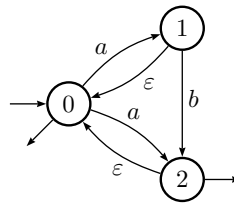
$$\begin{aligned} 0 &\xrightarrow{b} 0 \xrightarrow{a} 0 \xrightarrow{b} 0 \xrightarrow{a} 0, \\ 0 &\xrightarrow{b} 0 \xrightarrow{a} 0 \xrightarrow{b} 0 \xrightarrow{a} 1, \\ 0 &\xrightarrow{b} 0 \xrightarrow{a} 1 \xrightarrow{b} 2 \xrightarrow{a} 3. \end{aligned}$$

Näistä vain viimeinen on hyväksyvä, sillä se päättyy tilaan 3. Mutta se riittää, ja sana *baba* kuuluu kieleen  $L(\mathcal{A})$ . Sen sijaan kaikki sanan *aab* laskut päättyvät tilaan 0 tai 2, joten sanaa *aab* ei hyväksytä. Voidaan näyttää, että  $\mathcal{A}$  hyväksyy kaikki sanat, joilla on tekijä *aba*.



**Esimerkki 4.30.** Automaatilla  $\mathcal{A} = (\{0, 1, 2\}, \{a, b\}, \Delta, 0, \{0, 2\})$  on siirtymärelaatio  $\Delta = \{(0, a, 1), (0, a, 2), (1, b, 2), (1, \varepsilon, 0), (2, \varepsilon, 0)\}$ . Sen siirtymägraafi on vieressä. Sanalla  $aab$  on hyväksyvä lasku

$$0 \xrightarrow{a} 2 \xrightarrow{\varepsilon} 0 \xrightarrow{a} 1 \xrightarrow{b} 2.$$



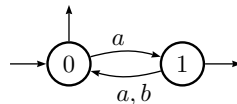
Sen sijaan sanaa  $abb$  ei hyväksytä, sillä sen kaikki laskut ovat hylkääviä:

$$\begin{aligned} 0 &\xrightarrow{a} 1 \xrightarrow{b} 2 \xrightarrow{\varepsilon} 0, \\ 0 &\xrightarrow{a} 1 \xrightarrow{\varepsilon} 0, \\ 0 &\xrightarrow{a} 2 \xrightarrow{\varepsilon} 0. \end{aligned}$$

Myös kaikki sanat, jotka alkavat kirjaimella  $b$  hylätään, sillä niillä ei ole yhtään laskua. Automaatin hyväksymä kieli on  $L(\mathcal{A}) = L((a \cup ab)^*)$ .

**Määritelmä 4.31.** Automaatit  $\mathcal{A}_1$  ja  $\mathcal{A}_2$  ovat *ekvivalentit*, jos  $L(\mathcal{A}_1) = L(\mathcal{A}_2)$ .

**Esimerkki 4.32.** Olkoon  $\mathcal{B} = (\{0, 1, 2\}, \{a, b\}, \Delta, 0, \{0, 1\})$  automaatti, jonka siirtymärelaatio on  $\Delta = \{(0, a, 1), (1, a, 0), (1, b, 0)\}$ . Sen hyväksymä kieli on myös  $L(\mathcal{B}) = L((a \cup ab)^*)$ . Automaatti  $\mathcal{B}$  on ekvivalentti esimerkin 4.30 automaatin  $\mathcal{A}$  kanssa.



### 4.5 Deterministinen äärellinen automaatti

Kun epädeterministisellä automaatilla voi olla yhtä syöttösanaa kohti yksi tai useampi lasku tai jopa ei yhtään laskua, niin deterministisellä automaatilla on täsmälleen yksi lasku jokaista syöttösanaa kohti. Silloin siirtymärelaatio  $\Delta \subseteq Q \times (\Sigma \cup \{\varepsilon\}) \times Q$  voidaan muuttaa *funktioksi*  $\delta : Q \times \Sigma \rightarrow Q$ . Tämä tarkoittaa, että kun automaatti lukee tilassa  $q$  syöttökirjaimen  $a$ , sillä on täsmälleen yksi vaihtoehto siirtyä seuraavaan tilaan, jota merkitään  $\delta(q, a)$ :lla. Deterministisellä automaatilla ei ole myöskään  $\varepsilon$ -siirtymiä, joten sen on aina pakko lukea yksi kirjain jokaisella askeleella.

**Määritelmä 4.33.** *Deterministisellä äärellisellä automaatilla*  $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$  on samat komponentit  $Q, \Sigma, q_0$  ja  $F$  kuin epädeterministisellä automaatilla, mutta

3'.  $\delta : Q \times \Sigma \rightarrow Q$  on *siirtymäfunktio*.

Deterministinen automaatti eroaa epädeterministisestä vain siinä, että siirtymärelaation tilalla on siirtymäfunktio. Siirtymäfunktio siirtyy vain yhden kirjaimen kerrallaan. Laajennetaan sitä niin, että se voi siirtyä sanan kerrallaan. Jos luetaan tyhjä sana, tila ei vaihdu. Jos luetaan sana  $wa$ , jossa  $a$  on viimeinen kirjain, niin luetaan ensin tilassa  $q$  sana  $w$ , jolloin saavutaan tilaan  $\delta(q, w)$ . Tässä tilassa luetaan sitten viimeinen kirjain  $a$ , jolloin tullaan tilaan  $\delta(\delta(q, w), a)$ . Silloin  $\delta$  laajenee funktioksi  $\delta : Q \times \Sigma^* \rightarrow Q$ , jolle

$$\begin{aligned} \delta(q, \varepsilon) &= q, \\ \delta(q, wa) &= \delta(\delta(q, w), a), \quad \text{kun } w \in \Sigma^*, a \in \Sigma. \end{aligned}$$

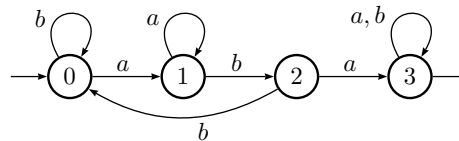
Deterministisellä automaatilla on jokaista syöttösanaa kohti tarkalleen yksi lasku, joka alkaa alkutilasta  $q_0$ . Jos syöttösana on  $w$ , laskun lopussa automaatti on tilassa  $\delta(q_0, w)$ . Jos tämä tila on lopputila, eli jokin joukon  $F$  tiloista, lasku on *hyväksyvä* ja sana  $w$  hyväksytään. Jos tila  $\delta(q_0, w)$  ei ole lopputila, sana  $w$  hylätään. Automaatin  $\mathcal{A}$  *tunnistama* tai *hyväksymä* kieli on sen hyväksymien sanojen joukko

$$L(\mathcal{A}) = \{w \in \Sigma^* \mid \delta(q_0, w) \in F\}.$$

**Esimerkki 4.34.** Olkoon  $\mathcal{A} = (\{0, 1, 2, 3\}, \{a, b\}, \delta, 0, \{3\})$  automaatti, jonka siirtymäfunktio  $\delta$  ilmoitetaan seuraavan *siirtymätaulukon* avulla.

$\delta$	$Q \backslash \Sigma$	a	b
$\rightarrow 0$		1	0
1		1	2
2		3	0
$\leftarrow 3$		3	3

automaatin  $\mathcal{A}$  siirtymägraafi



Sanalla *baabaa* on nyt lasku

$$\begin{aligned}\delta(0, baabaa) &= \delta(\delta(0, b), aabaa) = \delta(0, aabaa) \\ &= \delta(1, abaa) = \delta(1, baa) = \delta(2, aa) = \delta(3, a) = 3.\end{aligned}$$

Koska 3 on hyväksyvä tila, sana *baabaa* hyväksytään. Sen sijaan sanalla *abb* on lasku

$$\delta(0, abb) = \delta(1, bb) = \delta(2, b) = 0.$$

Mutta koska 0 ei ole lopputila, sana *abb* hylätään. Voidaan päätellä, että automaatin  $\mathcal{A}$  tunnistama kieli on

$$L(\mathcal{A}) = \{a, b\}^* \{aba\} \{a, b\}^* = \{w \in \{a, b\}^* \mid aba \text{ on } w\text{:n tekijä}\}.$$

Asia tulee selvemmäksi, jos korvaamme tilojen nimet 0, 1, 2 ja 3 sanoilla  $\varepsilon$ ,  $a$ ,  $ab$  ja  $aba$ . Silloin tila muistaa, miten pitkälle olemme jo löytäneet tekijää *aba*! Huomaa, että olemme löytäneet esimerkin 4.29 automaatin kanssa ekvivalentin deterministisen automaatin.

**Siirtymämerkintä.** Deterministisen automaatin lasku voidaan kirjoittaa myös käyttäen epädeterministisen automaatin siirtymämerkintää. Kun luetetaan sana  $w = a_1 \dots a_n$ , missä  $a_i \in \Sigma$ , automaatti käy joissakin tiloissa  $q_1, \dots, q_n$ , joilla

$$\delta(q_{i-1}, a_i) = q_i,$$

kun  $i = 1, \dots, n$ . Tämä lasku voidaan kirjoittaa samassa muodossa kuin epädeterministisillä automaateilla:

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \dots \xrightarrow{a_{n-1}} q_{n-1} \xrightarrow{a_n} q_n.$$

Kun jätetään välitilat pois, edellinen lasku voidaan esittää muodossa

$$q_0 \xrightarrow{a_1 \dots a_n} q_n.$$

Silloin automaatin hyväksymä kieli on

$$L(\mathcal{A}) = \{w \in \Sigma^* \mid q_0 \xrightarrow{w} q_n \text{ jollekin } q_n \in F\}.$$

**Esimerkki 4.35.** Esimerkin 4.34 lasku  $\delta(0, abb) = \delta(1, bb) = \delta(2, b) = 0$  voidaan kirjoittaa muodossa

$$0 \xrightarrow{a} 1 \xrightarrow{b} 2 \xrightarrow{b} 0.$$

## 4.6 Deterministisen ja epädeterministisen automaatin ekvivalenssi

Osoitamme nyt, että vaikka epädeterministinen automaatti näyttää yleisemmältä kuin deterministinen, niin se ei silti pysty tunnistamaan enempää kieliä kuin deterministinen automaatti. Seuraavaksi osoitetaan, että jokainen epädeterministinen automaatti voidaan muuntaa ekvivalentiksi deterministiseksi automaattiksi. Tämä muunnos tapahtuu kahdessa askeleessa, ensin poistetaan  $\varepsilon$  siirrot ja sen jälkeen tehdään ns. osajoukkokonstruktio, jolla päästään eroon epädeterministisyydestä eli tapauksista joissa  $(q, a, p), (q, a, r) \in \Delta$  ja  $p \neq r$ .

### $\varepsilon$ -siirtymien poistaminen

Näytetään ensin, että siirtymät, joissa luetaan vain tyhjä sana, voidaan korvata yhden symbolin lukevilla siirtymillä, eikä tunnistettu kieli muutu.

**Lause 4.36.** *Epädeterministinen automaatti on ekvivalentti sellaisen epädeterministisen automaatin kanssa, jossa ei ole  $\varepsilon$ -siirtymiä.*

*Todistus.* Näytetään, että kielen  $L$  tunnistavan epädeterministisen automaatin  $\mathcal{A} = (Q, \Sigma, \Delta, q_0, F)$  siirtymärelaatio  $\Delta \subseteq Q \times (\Sigma \cup \{\varepsilon\}) \times Q$  voidaan korvata relaatiolla  $\Delta' \subseteq Q \times \Sigma \times Q$  ja saatu automaatti tunnistaa saman kielen  $L$ .

Tarvitsemme uuden käsitteen: tilan  $p \in Q$   $\varepsilon$ -sulkeuman  $\text{clos}(p)$ , joka on

$$\text{clos}(p) = \{ q \in Q \mid p \xrightarrow{\varepsilon} q \}.$$

Joukkoon  $\text{clos}(p) \subseteq Q$  kuuluvat siis kaikki tilat, jotka voidaan saavuttaa  $p$ :sta  $\varepsilon$ -siirtymillä. Määritellään uusi epädeterministinen automaatti  $\mathcal{B} = (Q, \Sigma, \Delta'', q_0, F')$ , joka eroaa  $\mathcal{A}$ :sta siirtymäjoukoltaan ja mahdollisesti myös lopputilajoukoltaan. Korvataan ensin alkutilasta lähtevät  $\varepsilon$ -siirtymät ja sitten muut  $\varepsilon$ -siirtymät.

Jos on olemassa  $\varepsilon$ -siirtymien jono  $q_0 \xrightarrow{\varepsilon} q_f$  johonkin lopputilaan  $q_f \in F$ , niin lisätään  $q_0$  lopputilojen joukkoon:  $F' = F \cup \{q_0\}$ . Sitten kaikki muotoa  $q_0 \xrightarrow{\varepsilon} p$  olevat siirtymät otetaan pois ja tilalle vaihdetaan siirtymät

$$\{ (q_0, a, q) \mid (p, a, q) \in \Delta \text{ jollekin } p \in \text{clos}(q_0) \}.$$

Muut siirtymät jätetään ennalleen. Silloin  $\mathcal{A}$ :n lasku muotoa  $q_0 \xrightarrow{\varepsilon} q_1 \xrightarrow{a} q_2 \xrightarrow{x} \dots$  muuttuu muotoon  $q_0 \xrightarrow{a} q_2 \xrightarrow{x} \dots$ . Merkitään saatua siirtymäjoukkoa  $\Delta'$ :llä.

Uusi siirtymäjoukko  $\Delta''$  saadaan  $\Delta'$ :sta yhdistämällä  $\varepsilon$ -siirtymät kirjain-siirtymiin seuraavasti:

$$(p, a, q) \in \Delta'' \quad \text{jos ja vain jos} \quad (p, a, r) \in \Delta' \quad \text{joillekin } r \in Q \text{ ja } q \in \text{clos}(r),$$

missä  $p, q \in Q$  ja  $a \in \Sigma$ . Nyt  $\mathcal{A}$ :n lasku muotoa  $q_0 \xrightarrow{a} q_1 \xrightarrow{\varepsilon} q_2 \xrightarrow{b} q_3 \xrightarrow{\varepsilon} q_4 \longrightarrow \dots$  muuttuu muotoon  $q_0 \xrightarrow{a} q_2 \xrightarrow{b} q_4 \longrightarrow \dots$ .

Selvästi  $\mathcal{A}$  ja  $\mathcal{B}$  tunnistavat saman kielen, joten  $L(\mathcal{A}) = L(\mathcal{B})$ .  $\square$

## 4.6 Deterministisen ja epädeterministisen automaatin ekvivalenssi

**Esimerkki 4.37.** Poistetaan  $\varepsilon$ -siirtymät automaatista  $\mathcal{A} = (\{0, 1, 2, 3, 4\}, \{a, b, c, d\}, \Delta, 0, \{3, 4\})$ , missä

$$\Delta = \{(0, \varepsilon, 1), (0, a, 2), (1, b, 2), (2, c, 3), (2, d, 4), (3, \varepsilon, 4), (4, \varepsilon, 1)\}.$$

Tunnistetaan ensin  $\varepsilon$ -sulkeumat:  $\text{clos}(0) = \{0, 1\}$ ,  $\text{clos}(1) = \{1\}$ ,  $\text{clos}(2) = \{2\}$ ,  $\text{clos}(3) = \{3, 4, 1\}$  ja  $\text{clos}(4) = \{4, 1\}$ .

Ensin yhdistetään alkutilasta lähtevä  $\varepsilon$ -siirtymä  $(0, \varepsilon, 1)$  ainoaan tilasta 1 lähteviin kirjainsiirtymään  $(1, b, 2)$ . Saadaan uusi siirtymä  $(0, b, 2)$ . Tietysti siirtymä  $(0, \varepsilon, 1)$  jätetään pois. Siirtymärelaatio  $\Delta'$  on siis

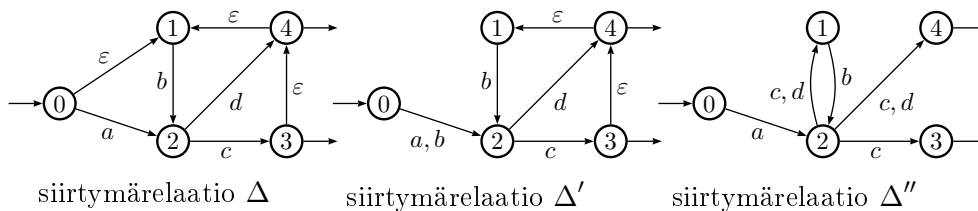
$$\Delta' = \{(0, a, 2), (0, b, 2), (1, b, 2), (2, c, 3), (2, d, 4), (3, \varepsilon, 4), (4, \varepsilon, 1)\}.$$

Lopputilojen joukkoa ei tarvitse muuttaa, koska 1 ei ole lopputila.

Sitten yhdistetään tilat joukosta  $\text{clos}(r)$   $r$ -tilaan tuleviin kirjainsiirtymiin. Alkutilaan 0 ei tule yhtään siirtymää, joten mitään ei tarvitse tehdä. Tilojen 1 ja 2  $\varepsilon$ -sulkeumissa ei ole muita tiloja kuin ne itse, joten niitäkään varten ei tarvitse muuttaa mitään. Tilaan 3 tulee vain siirtymä  $(2, c, 3)$ , joka yhdistetään joukon  $\text{clos}(3)$  tiloihin 3, 4 ja 1. Täten saadaan siirtymät  $(2, c, 3)$ ,  $(2, c, 4)$  ja  $(2, c, 1)$ , joista jälkimmäiset ovat uusia.

Vielä yhdistetään tilat joukosta  $\text{clos}(4) = \{4, 1\}$  4-tilaan tuleviin kirjainsiirtymiin, joita on vain  $(2, d, 4)$ , jolloin saadaan siirtymät  $(2, d, 4)$  ja  $(2, d, 1)$ , joista jälkimmäinen on uusi. Kun jätetään  $\varepsilon$ -siirtymät pois, automaatin siirtymärelaatioksi tulee

$$\Delta'' = \{(0, a, 2), (0, b, 2), (1, b, 2), (2, c, 1), (2, d, 1), (2, c, 3), (2, c, 4), (2, d, 4)\}.$$



### Epädeterministisyyden poistaminen

Seuraavaksi poistetaan epädeterministiset siirtymät, siis siirtymät, joilla tilasta pääsee samalla kirjaimella kahteen eri tilaan, ja lisätään puuttuvia siirtymiä. Tämä tehdään seuraavasti.

Ajatellaan, että epädeterministinen automaatti  $\mathcal{A}$  ei ole tietyllä hetkellä yhdessä tilassa vaan joukossa tiloja: nimittäin kaikkien niiden tilojen joukossa, jotka voidaan saavuttaa alkutilasta siihen mennessä luetulla syöttösanan osalla. Jos esimerkiksi automaatti  $\mathcal{A}$  jonkin syöttösanan luettuaan voi olla tiloissa  $q_0, q_2$  tai  $q_3$  mutta ei tiloissa  $q_1$  ja  $q_4$ , niin ajatellaankin  $\mathcal{A}$ :n olevan yhdessä yhteisessä tilassa  $\{q_0, q_2, q_3\}$  eikä vain jossakin näistä tiloista. Jos seuraava syöttösymboli veisi  $\mathcal{A}$ :n tilasta  $q_0$  tilaan  $q_1$  tai  $q_2, q_3$ :sta  $q_0$ :aan ja

#### 4.6 Deterministisen ja epädeterministisen automaatin ekvivalenssi

$q_3$ :sta  $q_2$ :een, niin  $\mathcal{A}$ :n seuraavaksi tilaksi ajatellaan  $\{q_0, q_1, q_2\}$ . Uutta systeemiä kutsutaan *osajoukkokonstruktioksi*, koska tilojen joukosta  $Q$  siirrytään tilojen osajoukkojen joukkoon  $\mathcal{P}(Q) = \{H \mid H \subseteq Q\}$ .

**Lause 4.38.** *Jokaista epädeterminististä äärellistä automaattia kohti on olemassa ekvivalentti deterministinen äärellinen automaatti.*

*Todistus.* Esitetään deterministinen automaatti  $\mathcal{B}$ , joka hyväksyy epädeterministisen automaatin  $\mathcal{A} = (Q, \Sigma, \Delta, q_0, F)$  hyväksymän kielen  $L$ . Voidaan olettaa, että automaatin  $\mathcal{A}$  siirtymärelaatiosta  $\Delta$  on edellisen lauseen mukaan jo poistettu  $\varepsilon$ -siirtymät.

Määritellään automaatti  $\mathcal{B} = (P, \Sigma, \delta, Q_0, G)$  seuraavasti:

$$\begin{aligned} P &= 2^Q = Q\text{:n potenssijoukko,} \\ \delta(H, a) &= \{q \in Q \mid (p, a, q) \in \Delta \text{ jollekin } p \in H\} \\ &= \{q \in Q \mid p \xrightarrow{\mathcal{A}}^a q \text{ jollekin } p \in H\}, \quad \text{kun } H \in P, a \in \Sigma, \\ Q_0 &= \{q_0\} \quad \text{ja} \\ G &= \{H \subseteq Q \mid H \cap F \neq \emptyset\}. \end{aligned}$$

Selvästi  $\mathcal{B}$  on deterministinen. Näytetään ensin seuraava väite kaikille  $H \subseteq Q$  ja  $w \in \Sigma^*$  induktiolla  $w$ :n pituuden suhteen:

$$\delta(H, w) = \{q \in Q \mid p \xrightarrow{\mathcal{A}}^w q \text{ jollekin } p \in H\}.$$

Jos  $|w| = 0$  eli jos  $w = \varepsilon$ , niin  $\delta(H, \varepsilon) = H$  siirtymäfunktion  $\delta$  määritelmän mukaan. Edelleen  $H$  voidaan esittää muodossa  $H = \{q \in Q \mid p \xrightarrow{\mathcal{A}}^\varepsilon q \text{ jollekin } p \in H\}$ , sillä  $\Delta$ :ssä ei ole oletuksen mukaan  $\varepsilon$ -siirtymiä eri tilojen välillä.

Olkoon sitten  $|w| > 0$  eli  $w = ua$ ,  $a \in \Sigma$  ja  $u \in \Sigma^*$ . Induktio-oletuksen mukaan  $\delta(H, u) = \{q \in Q \mid p \xrightarrow{\mathcal{A}}^u q \text{ jollekin } p \in H\}$ . Merkitään tätä joukkoa  $Q'$ :lla. Nyt

$$\begin{aligned} \delta(H, ua) &= \delta(\delta(H, u), a) = \delta(Q', a) \\ &= \{r \in Q \mid \text{jollekin } q \in Q' : q \xrightarrow{\mathcal{A}}^a r\} \\ &= \{r \in Q \mid \text{jollekin } q \in Q', p \in H : p \xrightarrow{\mathcal{A}}^u q \text{ ja } q \xrightarrow{\mathcal{A}}^a r\} \\ &= \{r \in Q \mid \text{jollekin } p \in H : p \xrightarrow{\mathcal{A}}^{ua} r\}. \end{aligned}$$

Nyt väite on todistettu. Lauseen todistus seuraa nyt väitteestä

$$\begin{aligned} L(\mathcal{B}) &= \{w \in \Sigma^* \mid \delta(Q_0, w) \in G\} = \{w \in \Sigma^* \mid \delta(Q_0, w) \cap F \neq \emptyset\} \\ &= \{w \in \Sigma^* \mid \text{jollekin } q \in \delta(Q_0, w) \cap F\} \\ &= \{w \in \Sigma^* \mid \text{jollekin } p \in Q_0, q \in F : p \xrightarrow{\mathcal{A}}^w q\} \\ &= \{w \in \Sigma^* \mid \text{jollekin } q \in F : q_0 \xrightarrow{\mathcal{A}}^w q\} = L(\mathcal{A}). \end{aligned}$$

□

## 4.6 Deterministisen ja epädeterministisen automaatin ekvivalenssi

**Esimerkki 4.39.** Tehdään osajoukkokonstruktio automaatille  $\mathcal{A} = (\{0, 1, 2, 3, 4, 5\}, \{a, b\}, \Delta, 0, \{2, 4\})$ , missä

$$\Delta = \{(0, a, 1), (0, a, 2), (0, b, 2), (0, b, 3), (1, a, 4), (1, b, 2), (2, a, 4), (2, a, 5), (2, b, 3), (3, b, 2), (4, b, 4), (5, b, 5)\}.$$

Uuden automaatin alkutila on  $\{0\}$ . Tilasta 0 päästään  $a$ -kirjaimella tiloihin 1 ja 2. Saamme siis uuden tilan  $\{1, 2\}$  ja siirtymän  $\delta(\{0\}, a) = \{1, 2\}$ . Tilasta 0 on siirtymät tiloihin 2 ja 3 kirjaimella  $b$ : saamme siirtymän  $\delta(\{0\}, b) = \{2, 3\}$ .

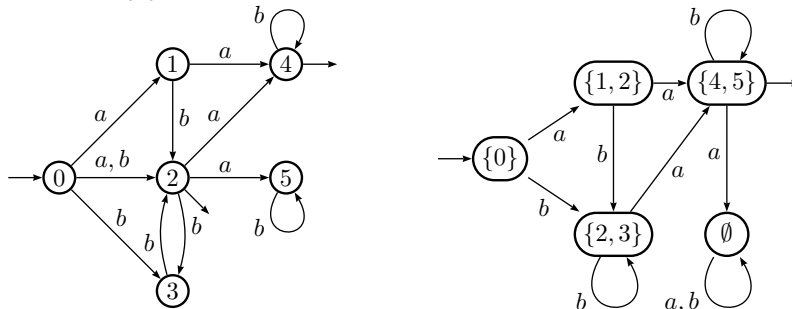
Tilasta  $\{1, 2\}$  päästään  $a$ -kirjaimella tilaan  $\{4, 5\}$ , sillä tilasta 1 on  $a$ -kirjaimella siirtymä tilaan 4 ja tilasta 2 on siirtymät tiloihin 4 ja 5. Siis  $\delta(\{1, 2\}, a) = \{4, 5\}$ . Tilasta 1 päästään  $b$ -kirjaimella tilaan 2 ja tilasta 2 tilaan 3, siis  $\delta(\{1, 2\}, b) = \{2, 3\}$ .

Jatketaan samoin uusista tiloista  $\{2, 3\}$  ja  $\{4, 5\}$  lähtien. Silloin  $\delta(\{2, 3\}, a) = \{4, 5\}$ ,  $\delta(\{2, 3\}, b) = \{2, 3\}$ ,  $\delta(\{4, 5\}, b) = \{4, 5\}$ . Entä  $\delta(\{4, 5\}, a)$ ? Tiloista 4 ja 5 ei ole  $a$ -kirjaimella siirtymää mihinkään tilaan. Silloin siirrytään tilasta  $\{4, 5\}$  tyhjiin joukkoon  $\emptyset$ . Sehän on joukon  $Q$  osajoukko myös. Siis  $\delta(\{4, 5\}, a) = \emptyset$ .

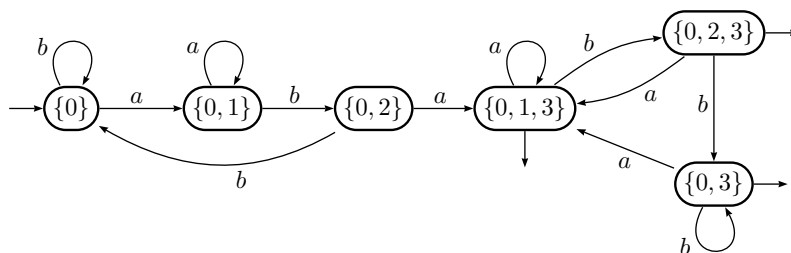
Tilassa  $\emptyset$  ei ole yhtään tilaa, joten siitä ei voi siirtyä myöskään mihinkään tilaan millään kirjaimella. Mutta jotta automaatista tulisi deterministinen, täytyy tälläkin tilalla olla siirtymät. Tyhjästä joukosta siirrytään siis ei mihinkään eli tyhjiin joukkoon:  $\delta(\emptyset, a) = \emptyset$  ja  $\delta(\emptyset, b) = \emptyset$ .

Uuden automaatin muita tiloja olisivat esimerkiksi  $\{1, 3\}$ , mutta niitä ei kannata käsitellä, sillä tällaiseen tilaan ei saavuta lukemalla mitään sanaa. Tilaa sanotaankin *saavuttamattomaksi*. Saavuttamattomat tilat voidaan jättää automaatista pois tunnistettavan kielen muuttumatta.

Uuden automaatin tilat ovat  $\{0\}$ ,  $\{1, 2\}$ ,  $\{2, 3\}$ ,  $\{4, 5\}$  ja  $\emptyset$ . Näistä lopputiloja ovat ne tilat, joissa on yksikin alkuperäisen automaatin lopputila 2 tai 4. Lopputiloja ovat siis  $\{1, 2\}$ ,  $\{2, 3\}$  ja  $\{4, 5\}$ . Alkutila on pelkän alkutilan sisältävä  $\{0\}$ . Siirtymäfunktio olikin jo edellä.



**Esimerkki 4.40.** Esimerkin 4.29 automaatin osajoukkokonstruktio on alla:



Vertaa tätä esimerkin 4.34 automaattiin.

Kieli  $L$  on *tunnistuva* (recognizable), jos on olemassa epädeterministinen äärellinen automaatti  $\mathcal{A}$ , joka hyväksyy sen. Silloin  $L = L(\mathcal{A})$ . Kaikkien tunnistuvien kielten joukko aakkostossa  $\Sigma$  on  $\mathcal{REC}(\Sigma)$ . Koska jokainen epädeterministinen automaatti voidaan muuttaa deterministiseksi automaatiksi, joka tunnistaa saman kielen, voidaan yhtä hyvin määritellä, että kieli on tunnistuva, kun jokin deterministinen automaatti hyväksyy sen.

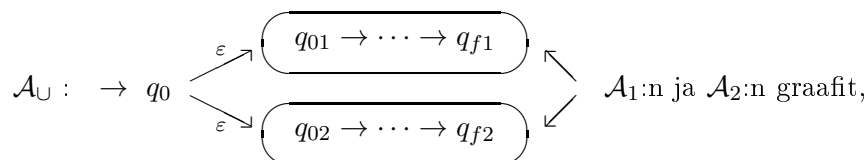
#### 4.7 Tunnistuvien kielten sulkeumaominaisuuksia

Näytetään nyt, että tunnistuvista kielistä voi usealla tavalla rakentaa uusia tunnistuvia kieliä. Käytetään hyväksi sitä tietoa, että jokaista tunnistuvaa kieltä kohti on olemassa deterministinen (ja siten myös epädeterministinen) automaatti, joka hyväksyy sen.

**Lause 4.41.** *Olkoot  $L_1$  ja  $L_2$  tunnistuvia kieliä. Silloin myös  $L_1 \cup L_2$ ,  $L_2 \cap L_2$ ,  $L_1^c$ ,  $L_1 L_2$  ja  $L_1^*$  ovat tunnistuvia.*

*Todistus.* Oletetaan, että deterministiset automaatit  $\mathcal{A}_1 = (Q_1, \Sigma, \delta_1, q_{01}, F_1)$  ja  $\mathcal{A}_2 = (Q_2, \Sigma, \delta_2, q_{02}, F_2)$  tunnistavat kielet  $L_1$  ja  $L_2 \subseteq \Sigma^*$ . Voidaan olettaa, että automaattien tilajoukot ovat erilliset:  $Q_1 \cap Q_2 = \emptyset$ . (Jos eivät ole, vaihdetaan merkintöjä.)

Unionin  $L_1 \cup L_2$  tunnistaa epädeterministinen automaatti  $\mathcal{A}_U = (Q_U, \Sigma, \Delta, q_0, F_1 \cup F_2)$ , missä  $Q_U = Q_1 \cup Q_2 \cup \{q_0\}$  ja siirtymärelaatio  $\Delta$  sisältää molempien automaattien  $\mathcal{A}_1$  ja  $\mathcal{A}_2$  siirtymät, eli jokaisen sellaisen kolmikun  $(q, a, r)$ , että  $\delta_1(q, a) = r$  tai  $\delta_2(q, a) = r$ , sekä kaksi uutta  $\varepsilon$ -siirtymää uudesta alkutilasta  $q_0$  vanhoihin alkutiloihin. Automaatin toiminta näkyy seuraavasta kuvasta.



missä  $q_{f1} \in F_1$  ja  $q_{f2} \in F_2$ . Täten  $L_1 \cup L_2 \in \mathcal{REG}(\Sigma)$ .

Komplementin  $L_1^c$  tunnistaa deterministinen automaatti  $\mathcal{A}_1^c = (Q_1, \Sigma, \delta_1, q_{01}, Q_1 \setminus F_1)$ , joka eroaa  $\mathcal{A}_1$ :stä vain siinä, että lopputilojen joukko on vaihdettu komplementikseen. Koska  $\mathcal{A}_1$  ja  $\mathcal{A}_1^c$  ovat deterministisiä, jokaisella sanalla on

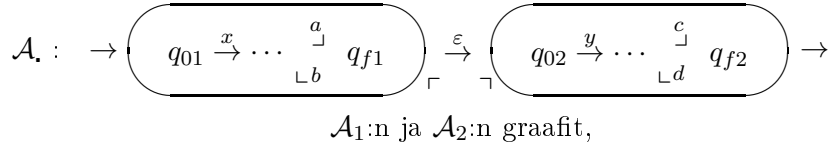
yksikäsitteinen lasku. Silloin  $A_1^c$  hyväksyy sanan, jos ja vain jos  $A_1$  hylkää sen.

Leikkauksen  $L_1 \cap L_2$  tunnistettavuus nähdään De Morganin lakien avulla:  $L_1 \cap L_2 = (L_1^c \cup L_2^c)^c$ . Toisaalta suoraan nähdään, että deterministinen automaatti  $A_\cap = (Q, \Sigma, \delta, q_0, F)$ , missä  $Q = Q_1 \times Q_2$ ,  $q_0 = (q_{01}, q_{02})$ ,  $F = F_1 \times F_2$  ja  $\delta : (Q_1 \times Q_2) \times \Sigma \rightarrow (Q_1 \times Q_2)$  on määritelty yhtälön

$$\delta((q_1, q_2), a) = (\delta_1(q_1, a), \delta_2(q_2, a))$$

avulla, tunnistaa leikkauksen. Itse asiassa  $\mathcal{A}_\cap$  simuloi molempien automaattien  $\mathcal{A}_1$  ja  $\mathcal{A}_2$  laskua yhtä aikaa, ja kun syöttösana on luettu loppuun, on saavuttava molempien automaattien lopputilaan, jotta sana voitaisiin hyväksyä.

Katenaation  $L_1 L_2$  hyväksyy seuraava yleistetty automaatti  $\mathcal{A}_\cdot$ :



Siis  $\mathcal{A}_\cdot$  simuloi ensin automaattia  $\mathcal{A}_1$  ja arvaa epädeterministisesti, milloin kielen  $L_1$  sana on luettu loppuun, siirtyy lukemalla tyhjän sanan automaatin  $\mathcal{A}_1$  lopputilasta automaatin  $\mathcal{A}_2$  alkutilaan ja simuloi sen jälkeen  $\mathcal{A}_2$ :ta. Jos päädytään  $\mathcal{A}_2$ :n lopputilaan, hyväksytään syöttösana.

Iteraation  $L_1^*$  voi tunnistaa lisäämällä  $\mathcal{A}_1$ :n siirtymäjoukkoon  $\varepsilon$ -siirtymät jokaisesta lopputilasta alkutilaan  $q_{01}$ . Lisättävät siirtymät ovat siis  $\{(p, \varepsilon, q_{01}) \mid p \in F\}$ . Lisäksi lisätään alkutila lopputilojen joukkoon (ellei se ole jo siellä), jotta automaatti hyväksyisi myös tyhjän sanan.  $\square$

**Esimerkki 4.42.** Esimerkin 4.29 tunnistuva kieli  $L$  sisälsi kaikki sanat, jotka sisältävät tekijän  $aba$ . Edellisen lauseen perusteella myös seuraavat kielet ovat tunnistuvia:

$$\begin{aligned} \{w \in \Sigma^* \mid w\text:ssä ei esiinny tekijää } aba\} &= L^c, \\ \{w \in \Sigma^* \mid aba \text{ esiintyy } w\text:ssä ainakin kahdesti, muttei päällekkäin}\} &= LL, \\ \{w \in \Sigma^* \mid w\text:ssä esiintyy tekijä } aba \text{ tai tekijä } bbb\} &= L \cup L'. \end{aligned}$$

Kieli  $L' = \Sigma^* \{bbb\} \Sigma^*$  todetaan tunnistuvaksi kieleksi samoin kuin  $L$ .

### 4.8 Äärelliset automaattit ja säännölliset ilmaisut

On helppo nähdä, että kielet  $L(a^*b^*)$  ja  $\{a, b\}^*$  voidaan esittää äärellisen automaatin ja säännöllisen ilmaisun avulla. Osoitamme nyt, että kieli voidaan esittää säännöllisellä ilmaisulla, jos ja vain jos se voidaan tunnistaa äärellisellä automaatilla.

**Lause 4.43** (Kleene). *Kieli  $L \subseteq \Sigma^*$  on säännöllinen, jos ja vain jos se on tunnistuva.*

*Todistus.* Oletetaan, että  $L$  on säännöllinen, ts. se voidaan esittää säännöllisen ilmaisun avulla, ja näytetään, että se on tunnistuva. Tyhjän kielen  $L = \emptyset$  tunnistaa mikä tahansa automaatti, jonka lopputilojen joukko on tyhjä. Kielen  $L = \{a\}$  puolestaan tunnistaa epädeterministinen automaatti, jossa on vain yksi siirtymä, joka johtaa alkutilasta lopputilaan ja joka on merkitty  $a$ :lla. Lisäksi jos  $L_1$  ja  $L_2$  ovat tunnistuvia ja  $L = L_1 \cup L_2$ ,  $L = L_1 L_2$  tai  $L = L_1^*$ , niin silloin myös  $L$  on tunnistuva lauseen 4.41 nojalla.

Oletetaan kääntäen, että  $L$  on tunnistuva. Olkoon  $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$  deterministinen automaatti, joka tunnistaa kielen  $L$ . Esitetään säännöllinen ilmaisu, joka esittää kieltä  $L$ . Numeroidaan  $\mathcal{A}$ :n tilat:  $Q = \{q_0, q_1, \dots, q_{n-1}\}$ . Määritellään sanajoukot  $L_{ij}^m$ , kun  $0 \leq m \leq n$  ja  $q_i, q_j \in Q$ . Joukossa  $L_{ij}^m$  on kaikki sanat, jotka vievät  $\mathcal{A}$ :n tilasta  $q_i$  tilaan  $q_j$  enintään tilojen  $\{q_0, \dots, q_{m-1}\}$  kautta. Siis

$$L_{ij}^m = \{w \in \Sigma^* \mid \delta(q_i, w) = q_j, \text{ ja kaikille } w\text{:n prefikseille } u \neq \varepsilon, \\ \delta(q_i, u) \in \{q_0, \dots, q_{m-1}\}\}.$$

Näytämme induktiolla  $m$ :n suhteen, että nämä joukot ovat säännöllisiä. Tästä seuraa  $L$ :n säännöllisyys, sillä

$$L = \bigcup_{q_j \in F} L_{0j}^n.$$

Induktio lähtökohta  $m = 0$ : Jos  $i \neq j$ , niin  $L_{ij}^0 = \{a \in \Sigma \mid \delta(q_i, a) = q_j\}$ . Tämä on säännöllinen, koska se on yhden symbolin kielten äärellinen unioni. Jos  $i = j$ , niin tähän joukkoon pitää lisätä tyhjä sana, joka sekin muodostaa säännöllisen kielen.

Oletetaan, että  $L_{ij}^m$  on säännöllinen kaikilla  $i, j$ , ja väitetään, että  $L_{ij}^{m+1}$  on säännöllinen kaikilla  $i, j$ .

Induktio todistus: Joukko  $L_{ij}^{m+1}$  voidaan kirjoittaa muodossa

$$L_{ij}^{m+1} = L_{ij}^m \cup L_{im}^m (L_{mm}^m)^* L_{mj}^m.$$

Tämä tarkoittaa, että päästäkseen tilasta  $q_i$  tilaan  $q_j$  kulkematta tilojen  $q_{m+1}, \dots, q_{n-1}$  kautta  $\mathcal{A}$  voi mennä a)  $q_i$ :stä  $q_j$ :hin kulkematta tilojen  $q_m, \dots, q_{n-1}$  kautta, tai b) ensin  $q_i$ :stä  $q_m$ :ään, sitten  $q_m$ :stä  $q_m$ :ään useamman kerran ja lopuksi  $q_m$ :stä  $q_j$ :hin kulkematta muuten tilojen  $q_m, \dots, q_{n-1}$  kautta. Induktio-oletuksen mukaan kaikki kielet yhtälön oikealla puolella ovat säännöllisiä, ja ne on yhdistetty säännöllisillä operaatioilla, joten  $L_{ij}^{m+1}$  on säännöllinen.  $\square$

Kleenen lauseesta seuraa, että säännöllisten kielten luokka  $\mathcal{REG}(\Sigma)$  on sama kuin tunnistuvien kielten luokka  $\mathcal{REC}(\Sigma)$ .

Kleenen lauseen todistus antaa yhden menetelmän, jolla voidaan muodostaa automaatin tunnistamaa kieltä esittävä ilmaisu. Esitetään nyt toinen menetelmä, jolla säännöllinen ilmaisu saadaan yhtälöryhmän ratkaisuna.

### Automaatista säännöllinen ilmaisu

Olko  $\alpha$  ja  $\beta$  säännöllisiä ilmaisuja. Merkintä  $\alpha \equiv \beta$  tarkoittaa, että  $\alpha$  ja  $\beta$  esittävät samaa kieltä eli  $L(\alpha) = L(\beta)$ . Säännöllisillä ilmaisuilla on ominaisuudet:

$$\begin{aligned}\alpha(\beta \cup \gamma) &\equiv \alpha\beta \cup \alpha\gamma \\ \alpha^*\alpha \cup \emptyset^* &\equiv \alpha^*.\end{aligned}$$

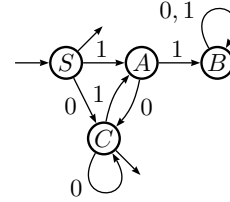
**Lemma 4.44.** *Yhtälöllä  $\gamma \equiv \gamma\alpha \cup \beta$  on ratkaisu*

$$\gamma_0 = \beta\alpha^*.$$

*Jos  $\varepsilon \notin L(\alpha)$ , niin ratkaisu on yksikäsitteinen.*

*Todistus.* Osatodistus:  $\gamma_0\alpha \cup \beta \equiv \beta\alpha^*\alpha \cup \beta \equiv \beta(\alpha^*\alpha \cup \emptyset^*) \equiv \beta\alpha^* \equiv \gamma_0$ .  $\square$

**Esimerkki 4.45.** Etsitään säännöllinen ilmaisu, joka esittää viereisen automaatin  $\mathcal{A}$  tunnistamaa kieltä. Muodostetaan yhtälöt katsomalla kuhunkin tilaan sisääntulevia nuolia. Koska alkutilaan päästään lukematta mitään, sen ilmaisussa on aina mukana tyhjää sanaa esittävä  $\emptyset^*$ .



$$\begin{cases} S &\equiv \emptyset^* && \text{alkutila} \\ A &\equiv S1 \cup C1 \\ B &\equiv A1 \cup B(0 \cup 1) \\ C &\equiv S0 \cup A0 \cup C0 \end{cases}$$

Nyt  $A \equiv \emptyset^*1 \cup C1 \equiv 1 \cup C1$ . Tällöin yhtälön

$$\begin{aligned}C &\equiv 0 \cup (1 \cup C1)0 \cup C0 \equiv 0 \cup 10 \cup C10 \cup C0 \\ &\equiv C(10 \cup 0) \cup (0 \cup 10)\end{aligned}$$

ratkaisu on edellisen lemmän mukaan on  $C \equiv (0 \cup 10)(10 \cup 0)^*$ . Se on yksikäsitteinen, sillä  $\varepsilon$  ei kuulu kieleen  $L(10 \cup 0) = \{10, 0\}$ . Koko automaatin tunnistamaa kieltä esittämä säännöllinen ilmaisu saadaan yhdistämällä lopputiloja esittävät säännölliset ilmaisut, tässä

$$\begin{aligned}L(\mathcal{A}) &= L(S) \cup L(C) \equiv L(\emptyset^*) \cup L((0 \cup 10)(10 \cup 0)^*) \\ &\equiv L(\emptyset^* \cup (0 \cup 10)(10 \cup 0)^*) \equiv L((0 \cup 10)^*).\end{aligned}$$

Automaatti  $\mathcal{A}$  tunnistaa siis kielen  $L((0 \cup 10)^*)$ .

## 4.9 Epäsäännöllinen kieli

Tähän mennessä olemme löytäneet vain säännöllisiä kieliä. Muitakin on olemassa.

**Lause 4.46.** *Kieli  $L = \{a^n b^n \mid n \geq 0\}$  ei ole säännöllinen.*

*Todistus.* Oletetaan, että  $L$  on säännöllinen. Silloin sen hyväksyy deterministinen automaatti  $\mathcal{A}$ . Automaatilla  $\mathcal{A}$  on äärellinen määrä, sanotaan  $k$ , tiloja. Tarkastellaan sanaa  $w = a^k b^k$ , joka kuuluu kieleen  $L$ . Silloin  $\mathcal{A}$  tunnistaa sen ja sanalla  $w$  on hyväksyvä lasku

$$q_0 \xrightarrow{a} q_1 \xrightarrow{a} \dots \xrightarrow{a} q_k \xrightarrow{b} q_{k+1} \xrightarrow{b} \dots \xrightarrow{b} q_{2k},$$

missä  $q_0, \dots, q_{2k} \in Q$ ,  $q_0$  on alkutila ja  $q_{2k}$  lopputila.

Koska  $\mathcal{A}$ :lla on vain  $k$  tilaa, jonossa  $q_0, q_1, \dots, q_k$  täytyy olla kaksi samaa tilaa. Olkoot ne  $q_i$  ja  $q_j$ ,  $i < j$ . Tällöin saadaan uusi lasku

$$q_0 \xrightarrow{a} \dots \xrightarrow{a} q_i \xrightarrow{a} q_{j+1} \xrightarrow{a} \dots \xrightarrow{a} q_k \xrightarrow{b} q_{k+1} \xrightarrow{b} \dots \xrightarrow{b} q_{2k}$$

sanalle  $a^{k-j+i} b^k$ . Lasku on hyväksyvä, sillä  $q_{2k}$  on lopputila, joten  $\mathcal{A}$  tunnistaa sanan  $a^{k-j+i} b^k$ . Kuitenkin  $a^{k-j+i} b^k \notin L$ , sillä  $k - j + i < k$ . Siis  $\mathcal{A}$  ei voi tunnistaa kieltä  $L$ .  $\square$

Käyttämällä säännöllisten kielten sulkeumaominaisuuksia voidaan etsiä muitakin epäsäännöllisiä kieliä.

**Esimerkki 4.47.** Kieli  $K = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\}$  ei ole säännöllinen. Oletetaan, että  $K$  on säännöllinen. Lauseen 4.41 mukaan silloin myös kieli  $K \cap L(a^* b^*)$  on säännöllinen, sillä  $L(a^* b^*)$  on säännöllinen. Kuitenkin  $K \cap L(a^* b^*) = L$ , joka ei lauseen 4.46 mukaan olekaan säännöllinen.

## 4.10 Automaatin minimointi

Halutaan etsiä tilaluvultaan pienin automaatti ekvivalenttien automaattien joukosta. Olkoon  $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$  deterministinen äärellinen automaatti. Kun  $q \in Q$ , määritellään uusi automaatti  $\mathcal{A}_q = (Q, \Sigma, \delta, q, F)$ , jonka ainut ero vanhaan on uusi alkutila. Kun  $k \geq 0$ , sanotaan, että tilat  $p$  ja  $q$  ovat  $k$ -erottuvia, jos on olemassa jokin enintään  $k$ -pituisen sana, jonka toinen automaateista  $\mathcal{A}_p$  ja  $\mathcal{A}_q$  hyväksyy ja toinen hylkää. Muuten ne ovat  $k$ -erottumattomia. Kaksi tilaa ovat ekvivalentit, jos ne ovat  $k$ -erottumattomia jokaisella arvolla  $k$ . Silloin automaatit  $\mathcal{A}_p$  ja  $\mathcal{A}_q$  tunnistavat saman kielen.

**Lemma 4.48.** *Toinen kahdesta ekvivalentista tilasta voidaan poistaa tunnustettavan kielen muuttumatta.*

*Todistus.* Oletetaan, että  $p$  ja  $q$  ovat automaatin  $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$  ekvivalentteja tiloja. Jätetään pois tila  $p$ , paitsi jos se sattuu olemaan alkutila, jolloin jätetäänkin pois tila  $q$ . Jos toinen tila olisi lopputila ja toinen ei, sanat olisivat 0-erottuvia. Siis joko kumpikin on lopputila tai kumpikaan ei ole lopputila. Muodostetaan uusi automaatti  $\mathcal{B} = (Q \setminus \{p\}, \Sigma, \delta', q_0, F \setminus \{p\})$  korvaamalla kaikki siirtymät muotoa  $\delta(r, a) = p$  siirtymällä  $\delta(r, a) = q$ . Siirretään siis tilaan  $p$  tulevat siirtymät tulemaan tilaan  $q$ .

Jos  $w = a_1 \dots a_n$ , missä  $a_i \in \Sigma$ , niin on olemassa jono sellaisia tiloja  $q_1, \dots, q_n$ , että

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \dots \xrightarrow{a_{n-1}} q_{n-1} \xrightarrow{a_n} q_n.$$

kun  $i = 1, \dots, n$ . Jos jokin tiloista  $q_1, \dots, q_n$  on tila  $p$ , sanotaan  $q_i = p$ , siirtymä  $q_{i-1} \xrightarrow{a_i} p$  voidaan korvata siirtymällä  $q_{i-1} \xrightarrow{a_i} q$ . Jos useampi tiloista  $q_1, \dots, q_n$  on  $p$ , niin tarkastellaan niistä indeksiltään pienintä. Tähän mennessä luettu sana on  $a_1 \dots a_i$  ja lukematta on sana  $a_{i+1} \dots a_n$ . Koska tilat  $p$  ja  $q$  ovat ekvivalentit, ei ole väliä, luetaanko sana  $a_{i+1} \dots a_n$  tilasta  $p$  tai tilasta  $q$  lähtien. Kummassakin tapauksessa sana hyväksytään tai hylätään. Jatkamalla tällä tavoin voidaan tilajonosta vaihtaa kaikki tilan  $p$  esiintymät tilaksi  $q$ .  $\square$

**Lemma 4.49.** *Tilat  $p$  ja  $q$  ovat  $k$ -erottumattomia, jos ja vain jos*

1.  $p$  ja  $q$  ovat molemmat lopputiloja tai kumpikaan ei ole lopputila ja
2. jos  $k > 0$ , niin tilat  $\delta(p, a)$  ja  $\delta(q, a)$  ovat  $(k-1)$ -erottumattomia kaikilla  $a \in \Sigma$ .

*Todistus.* Oletetaan siis, että  $p$  ja  $q$  ovat  $k$ -erottumattomia. Jos toinen olisi lopputila ja toinen ei, ne olisivat  $k$ -erottuvat, sillä tyhjä sana, jonka pituus on enintään  $k$ , erottaa ne. Jos  $k > 0$  ja jokin enintään  $(k-1)$ -pituinen sana  $w$  erottaisi tilat  $\delta(p, a)$  ja  $\delta(q, a)$ , niin enintään  $k$ -pituinen sana  $aw$  erottaisi tilat  $p$  ja  $q$ .

Oletetaan sitten ehdot a) ja b). Koska  $p$  ja  $q$  ovat molemmat lopputiloja tai kumpikaan ei ole lopputila,  $p$  ja  $q$  ovat ainakin 0-erottumattomat. Oletetaan sitten, että  $p$  ja  $q$  ovat  $(k-1)$ -erottumattomat. Jos jokin enintään  $k$ -pituinen sana  $au$ , jossa  $a \in \Sigma$  ja  $u \in \Sigma^*$ , erottaa tilat  $p$  ja  $q$ , niin enintään  $(k-1)$ -pituinen sana  $u$  erottaa tilat  $\delta(p, a)$  ja  $\delta(q, a)$ . Mutta ehdon b) nojalla tämä ei ole mahdollista. Siis  $p$  ja  $q$  ovat  $k$ -erottumattomat.  $\square$

**Määritelmä 4.50.** Määritellään relaatiot  $\equiv_0, \equiv_1, \dots$  tilojen joukossa  $Q$ :

$$\begin{aligned} p \equiv_0 q & \quad \text{jos ja vain jos} \quad \text{molemmat } p \text{ ja } q \text{ ovat lopputiloja tai} \\ & \quad \text{kumpikaan ei ole lopputila,} \\ p \equiv_{k+1} q & \quad \text{jos ja vain jos} \quad p \equiv_k q \text{ ja } \delta(p, a) \equiv_k \delta(q, a) \text{ kaikilla } a \in \Sigma. \end{aligned}$$

**Lemma 4.51.**  $p \equiv_k q$ , jos ja vain jos  $p$  ja  $q$  ovat  $k$ -erottumattomat.

*Todistus.* Todistetaan induktiolla indeksin  $k$  suhteen. Olkoon  $k = 0$ . Jos tyhjä sana erottaa tilat  $p$  ja  $q$ , ne ovat 0-erottuvat ja  $p \equiv_0 q$  ei päde. Muuten  $p$  ja  $q$  ovat 0-erottumattomat ja  $p \equiv_0 q$  on voimassa.

Olkoon sitten  $k > 0$ . Oletetaan, että väite pitää paikkansa arvolla  $k$ . Jos  $p \equiv_{k+1} q$ , niin  $p \equiv_k q$  ja  $\delta(p, a) \equiv_k \delta(q, a)$  kaikilla  $a \in \Sigma$ . Silloin  $p$  ja  $q$  ovat  $k$ -erottumattomat ja  $\delta(p, a)$  ja  $\delta(q, a)$  ovat  $k$ -erottumattomat kaikilla  $a \in \Sigma$ . Nyt lemmän 4.49 mukaan  $p$  ja  $q$  ovat  $(k+1)$ -erottumattomat.

Jos taas  $p$  ja  $q$  ovat  $(k+1)$ -erottumattomat, niin ne ovat  $k$ -erottumattomat. Lisäksi lemmän 4.49 mukaan tilat  $\delta(p, a)$  ja  $\delta(q, a)$  ovat  $k$ -erottumattomat kaikilla  $a \in \Sigma$ . Induktio-oletuksen mukaan  $p \equiv_k q$  ja  $\delta(p, a) \equiv_k \delta(q, a)$  kaikilla  $a \in \Sigma$ . Silloin  $p \equiv_{k+1} q$ .  $\square$

**Lemma 4.52.** *Jos  $p \equiv_{k+1} q$ , niin  $p \equiv_k q$ . Täten*

$$\equiv_0 \supseteq \equiv_1 \supseteq \equiv_2 \supseteq \dots$$

*Todistus.* Jos jokin enintään  $k$ -pituisen sana erottaa tilat  $p$  ja  $q$ , niin sama sana on enintään  $(k+1)$ -pituisen.  $\square$

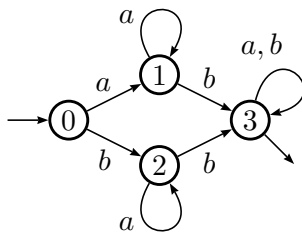
**Lemma 4.53.** *Jos  $\equiv_k = \equiv_{k+1}$ , niin  $\equiv_n = \equiv_k$  kaikilla  $n \geq k$ .*

*Todistus.* Jos  $p \equiv_k q$ , niin  $p \equiv_{k+1} q$ . Määritelmän mukaan silloin myös  $\delta(p, a) \equiv_k \delta(q, a)$  kaikilla  $a \in \Sigma$ . Silloin  $\delta(p, a) \equiv_{k+1} \delta(q, a)$  kaikilla  $a \in \Sigma$ . Relaanin  $\equiv_{k+2}$  määritelmän mukaan  $p \equiv_{k+2} q$ . Siis  $\equiv_{k+2} = \equiv_k$ . Samoin jatkamalla nähdään, että  $\equiv_n = \equiv_k$  kaikilla  $n \geq k$ .  $\square$

Edellinen sarja relaatioita ei voi pienentyä loputtomiin. Viimeistään silloin kun jokainen tila on omassa ekvivalenssiluokassaan, pienentyminen loppuu. Jos jokaisella kerralla yksi tila erottuu muista, tarvitaan enintään automaatin tilojen verran relaatioita  $\equiv_k$ . Kaikki ekvivalentit tilat löydetään siis käyttämällä relaation  $\equiv_k$  induktiivista määritelmää enintään  $|Q|$  kertaa.

**Esimerkki 4.54.** Tarkastellaan automaattia  $\mathcal{A} = (\{0, 1, 2, 3\}, \{a, b\}, \delta, 0, \{3\})$ . Aluksi 0-erottumattomat tilat ovat 0,1 ja 2, koska 3 on ainoa lopputila. Siis  $0 \equiv_0 1$ ,  $0 \equiv_0 2$  ja  $1 \equiv_0 2$ . Seuraavaksi  $a$  ei erota tiloja 0, 1 ja 2 toisistaan, sillä  $\delta(0, a) = 1$ ,  $\delta(1, a) = 1$  ja  $\delta(2, a) = 2$  ja  $1 \equiv_0 2$ . Mutta  $b$  erottaa tilan 0 tiloista 1 ja 2, sillä  $\delta(0, b) = 2$  ja  $\delta(1, b) = 3$  ja  $\delta(2, b) = 3$  ja  $2 \not\equiv_0 3$ . Siis  $1 \equiv_1 2$ , mutta  $0 \not\equiv_1 1$  ja  $0 \not\equiv_1 2$ . Seuraavaksi nähdään, että tilat 1 ja 2 eivät erotu, sillä  $\delta(1, a) = 1$  ja  $\delta(2, a) = 2$  ja  $1 \equiv_1 2$  ja  $\delta(1, b) = 3$  ja  $\delta(2, b) = 3$  ja  $3 \equiv_1 3$ . Siispä  $1 \equiv_2 2$ . Täten  $\equiv_2 = \equiv_1$ .

Minimaalisessa automaatissa tilat 1 ja 2 yhdistetään: se on siis muotoa  $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ , missä  $Q = \{0, 1, 3\}$ ,  $q_0 = 0$  ja  $F = \{3\}$ . Tila 2 jätetään pois ja tilaan 2 tulevat siirtymät siirretään tulemaan tilaan 1.



$\delta$	$a$	$b$
0	1	2
1	1	3
2	2	3
3	3	3

