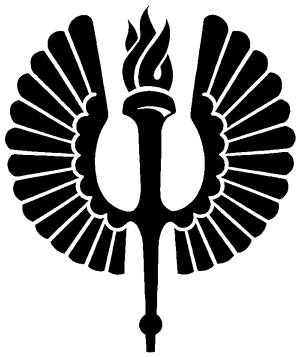


# Automaattiryhmien algebrallisia tuloksia ja ratkeavuusongelmia

Toni Hotanen

Pro gradu -tutkielma
Lokakuu 2017

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

HOTANEN, TONI: Automaattiryhmien algebrallisia tuloksia ja ratkeavuusongelmia
Pro gradu -tutkielma, 50 s.
Matematiikka
Lokakuu 2017

---

Tässä teoksessa esitetään kaksi ryhmäteoriaa koskevaa ongelmaa ja niiden ratkaisu käyttäen hyväksi erästä automaattiryhmää, joka tunnetaan nimellä Grigorchukin ryhmä. Nähdään, että kyseinen ryhmä on ääretön 2-ryhmä ja sillä on keskitason kasvu.

Lisäksi esitetään automaattiryhmiä ja -puoliryhmiä koskevia päätösongelmia. Nähdään, että sanaongelma on automaattipuoliryhmien joukossa ratkeava, kun taas muut teoksessa esitetyt päätösongelmat ovat ratkeamattomia.

Johdannon jälkeen ensimmäisessä luvussa käydään läpi esitystä seuraamiseen tarvittavat ryhmäteorian tiedot. Kolmannessa luvussa esitetään automaattiryhmien ja -puoliryhmien määritelmät ja muutamia tuloksia.

Neljännessä luvussa esitetään Grigorchukin ryhmä ja sen avulla ratkaisut sekä Burnsiden ongelmaan että Milnorin ongelmaan.

Viimeisessä luvussa esitetään automaattiryhmiä ja -puoliryhmiä koskevia päätösongelmia.

Asiasanat: automaattiryhmä, automaattipuoliryhmä, Grigorchukin ryhmä, Burnsiden ongelma, Milnorin ongelma, ryhmän kasvu, päätösongelma, ratkeamattomuus.

# Sisältö

# 1 Johdanto

Mealyn koneet ovat deterministisiä tilamuuntimia. Formaalisti Mealyn koneen määrittelee neljä-tupla $(Q, \Sigma, \delta, \sigma)$, missä $Q$ on äärellinen tilajoukko, $\Sigma$ on äärellinen aakkosto, $\delta$ on siirtymäfunktio ja $\sigma$ on tulostusfunktio. Jokainen Mealyn kone määrittelee automaattipuoliryhmän ja lisäksi kääntyvä Mealyn kone määrittelee automaattiryhmän.

Automaattiryhmien tutkimus on johtanut useiden tärkeiden avointen ryhmäteorian ongelmien ratkaisuun. William Burnside kysyi vuonna 1902 artikkelissa [4], että onko jokainen sellainen äärellisesti generoitu ryhmä, jonka jokaisen alkion kertaluku on äärellinen, välttämättä äärellinen. Kysymys on kuuluisa ja se tunnetaan nykyään nimellä Burnsiden ongelma. Burnsiden ongelma pysyi avoimena noin 60 vuotta ja sen ratkaisi ensimmäisenä Evgeny Golod artikkelissa [7] käyttäen hyväksi artikkelin [6] Golod - Shafarevich lausetta. Kuuluisimman ja eniten tutkitun automaattiryhmän on konstruoinut Rostislav Grigorchuk vuonna 1980 artikkelissa [8]. Kyseisessä artikkelissa Grigorchuk osoittaa, että hänen konstruoima ryhmä on ääretön 2-ryhmä ja näin ollen se on eräs vastaesimerkki Burnsiden ongelmaan. Kolme vuotta myöhemmin ilmestyneessä artikkelissa [16] Narain Gupta ja Said Sidki näyttivät, että jokaista alkulukua $p$ kohti on olemassa automaattiryhmä, joka on ääretön $p$-ryhmä. Samoihin aikoihin Grigorchuk näytti artikkelissa [13], että Grigorchukin ryhmällä on keskitason kasvu. Näin ollen se on ensimmäinen ratkaisu Milnorin ongelmaan, jonka John Milnor esitti artikkelissa [21] vuonna 1968. Näiden ongelmien lisäksi mainittakoon vielä kaksi tärkeää ongelmaa, jotka ratkaistiin automaattiryhmien avulla, mutta joita ei tässä teoksessa käydä läpi. Olkoot $M$ suljettu monisto, $b_i^{(2)}(M)$ moniston $M$ $i$:nnes $L^2$-Betti luku, ja $G$ sellainen ryhmä, että se on isomorfinen fundamentaalisen ryhmän $\pi_1(M)$ kanssa. Olkoon lisäksi $H$ sellainen rationaalilukujen aliryhmä, jonka generoivat ryhmän $G$ äärellisten aliryhmien kertalukujen käänteisluvut. Tällöin vahvan Atiyahin konjektuurin mukaan $b_i^{(2)}(M) \in H$ aina, kun $i \in \mathbb{N}$. Artikkelissa [10] Grigorchuk yhdessä Peter Linnelin, Thomas Schickin ja Andrzej Zukin kanssa todisti vahvan Atiyahin konjektuurin vääräksi. Kasvufunktio on tasaisesti eksponentiaalinen jos $\inf_H \lim_{n\to\infty}(\gamma_G^H(n))^{\frac{1}{n}} > 1$. Eräs Gromovin ongelma kysyy onko olemassa sellainen äärellisesti generoitu ryhmä, jonka kasvufunktio on eksponentiaalinen, mutta ei kuitenkaan tasaisesti eksponentiaalinen. Artikkelissa [26] John Wilson ratkaisi kyseisen Gromovin ongelman konstruoimalla ryhmän, jolla on edellä mainittu ominaisuus.

Rostislav Grigorchuk esitti artikkelissa [9] useita automaattiryhmiä ja automaattipuoliryhmiä koskevia päätösongelmia. Näistä muutamia on lähivuo-

sina ratkaistu joko kokonaan tai osittain. Artikkelissa [23] vuodelta 2012 Zoran Šunić ja Enric Ventura osoittivat automaattiryhmiä koskevan konjugaattiongelman ratkeamattomaksi. Samana vuonna he luennoivat isomorfisuusongelman ratkeamattomuudesta, käyttäen hyväkseen artikkelissaan saamaansa tulosta. Artikkelissa [5] vuodelta 2014 Pierre Gillibert osoitti äärellisyysongelman ratkeamattomaksi automaattipuoliryhmien luokassa. Vielä ei kuitenkaan tiedetä onko äärellisyysongelma ratkeava vai ratkeamaton automaattiryhmien joukossa.

# 2 Esitietoja

## 2.1 Aakkostot, sanat ja kielet

**Määritelmä 2.1.** Olkoon $\Sigma$ äärellinen ja epätyhjä joukko. Sanotaan, että $\Sigma$ on *aakkosto* ja sen *koko* on $|\Sigma|$, mikä tarkoittaa sen alkioiden lukumäärää. Määritellään

$$\Sigma^* = \{a_1 a_2 \cdots a_n \mid a_i \in \Sigma \text{ ja } n \in \mathbb{N}\}.$$

Merkitään sanaa, jonka pituus on nolla, symbolilla $\epsilon$ ja annetaan sille nimeksi *tyhjä sana*. Olkoon $w = a_1 a_2 \cdots a_n \in \Sigma^*$. Tällöin $w$ on aakkoston $\Sigma$ *sana* ja $|w| = n$ on sanan $w$ *pituus*. Määritellään

$$\Sigma^\omega = \{a_1 a_2 \cdots \mid a_i \in \Sigma\}.$$

Nähdään, että $\Sigma^\omega$ sisältää kaikki äärettömät sanat, yli aakkoston $\Sigma$. Määritellään myös

$$\Sigma^n = \{a_1 a_2 \cdots a_n \mid a_i \in \Sigma\}$$

aina, kun $n \in \mathbb{N}$. Olkoot $t \in \Sigma^*$, $u \in \Sigma^*$, $v \in \Sigma^* \cup \Sigma^\omega$ ja $w \in \Sigma^* \cup \Sigma^\omega$. Jos $w = utv$, niin $u$ on sanan $w$ *prefiksi*, $t$ on sanan $w$ *osasana* ja $v$ on sanan $w$ *suffiksi*.

## 2.2 Ryhmät ja puoliryhmät

**Määritelmä 2.2.** *Puoliryhmä* on pari $(G, *)$, missä $G$ on epätyhjä joukko ja $* : G^2 \longrightarrow G$ on *assosiatiivinen* kuvaus, eli se toteuttaa ehdon:

$$(a * b) * c = a * (b * c) \text{ aina, kun } a, b \text{ ja } c \text{ kuuluvat joukkoon } G.$$

Puoliryhmä $(G, *)$ on *monoidi*, jos siihen kuuluu *ykkösalkio* $1_G$, eli alkio joka toteuttaa ehdon:

$$a * 1_G = a = 1_G * a \text{ aina, kun } a \text{ kuuluu joukkoon } G.$$

Monoidi $(G, *)$ on ryhmä, jos sen jokaista alkiota $a$ kohti on olemassa joukkoon $G$ kuuluva alkio $a^{-1}$, joka toteuttaa ehdon:

$$a * a^{-1} = 1_G = a^{-1} * a.$$

Alkiota $a^{-1}$ kutsutaan alkion $a$ *käänteisalkioksi*. Ryhmä $(G, *)$ on *Abelin ryhmä*, jos sen alkiot *kommutoivat* keskenään, mikä tarkoittaa seuraavaa ehtoa:

$$a * b = b * a \text{ aina, kun } a \text{ ja } b \text{ kuuluvat ryhmään } G.$$

Jos kuvaus $*$ on kontekstista selvä, niin se voidaan jättää merkitsemättä. Ryhmän $G$ *kertaluku* $|G|$ on sen alkioiden lukumäärä. Jos $|G| \in \mathbb{N}$, niin ryhmä $G$ on *äärellinen*, muutoin se on *ääretön*.

**Määritelmä 2.3.** Olkoot $(G, *)$ monoidi, $H \subseteq G$ ja $H \neq \emptyset$. Tällöin $H$ on ryhmän $G$ *aliryhmä*, jos se on suljettu operaation $*$ suhteen ja jokaista joukkoon $H$ kuuluvaa alkiota kohti on olemassa käänteisalkio, joka kuuluu myös joukkoon $H$. Merkitään $H \leq G$, jos $H$ on ryhmän $G$ aliryhmä.

Vastaavasti määritellään *alimonoidi* ja *alipuoliryhmä*, poislukien vaatimus, joka koskee käänteisalkioita. Alimonoidin tapauksessa vaaditaan tietysti, että ykkösalkio kuuluu siihen.

**Lause 2.4** (Aliryhmäkriteeri)**.** Ryhmän $G$ osajoukko $H$ on ryhmän $G$ aliryhmä jos ja vain jos $H \neq \emptyset$ ja $ab^{-1} \in H$ aina, kun $a \in H$ ja $b \in H$.

*Todistus.* ($\Rightarrow$) Oletetaan, että $H \leq G$. Tällöin Määritelmän 2.3 nojalla, $H \neq \emptyset$ ja aina, kun $a \in H$ ja $b \in H$, niin $b^{-1} \in H$ ja siten myös $ab^{-1} \in H$.
($\Leftarrow$) Oletetaan sitten, että $H \neq \emptyset$ ja $ab^{-1} \in H$ aina, kun $a \in H$ ja $b \in H$. Koska $H \neq \emptyset$, niin on olemassa $a \in H$. Tällöin $1_G = aa^{-1} \in H$, joten myös $a^{-1} = 1_G a^{-1} \in H$. Jos myös $b \in H$, niin $ab = a(b^{-1})^{-1} \in H$. □

**Esimerkki 2.5.** Olkoon $X$ mikä tahansa joukko. Tällöin joukko
$\mathcal{T}_X = \{f \mid f : X \to X\}$ muodostaa monoidin, kun operaatioksi otetaan kuvausten yhdistäminen, jolloin tunnetusti assosiatiivisuus on voimassa. Ykkösalkiona monoidissa $\mathcal{T}_X$ on identiteettikuvaus. Joukko
$Sym(X) = \{f \mid f : X \to X,\ f \text{ on bijektio}\}$ on monoidin $\mathcal{T}_X$ aliryhmä, mikä nähdään suoraan määritelmästä.

**Esimerkki 2.6.** Seuraava taulukko määrittelee ryhmän $(G, *)$, missä

$$G = \{1, a, b, c\}.$$

Jokainen joukon $G$ alkio on itsensä käänteisalkio ja $1_G = 1$. Assosiatiivisuus on myös helppo tarkistaa. Ryhmän $G$ alkiot kommutoivat keskenään, joten kyseessä on Abelin ryhmä. Ryhmässä $G$ on neljä alkiota ja sitä kutsutaan nimellä *Kleinin neliryhmä*.

| $*$ | 1 | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ |
| $a$ | $a$ | 1 | $c$ | $b$ |
| $b$ | $b$ | $c$ | 1 | $a$ |
| $c$ | $c$ | $b$ | $a$ | 1 |

**Lause 2.7.** Olkoot $G$ ryhmä, $I$ indeksijoukko ja $H_i \leq G$ aina, kun $i \in I$. Tällöin

$$\bigcap_{i \in I} H_i \leq G.$$

*Todistus.* Merkitään

$$A = \bigcap_{i \in I} H_i.$$

Koska $1_G \in H_i$ aina, kun $i \in I$, niin $1_G \in A$, joten $A \neq \emptyset$. Oletetaan, että $a \in A$ ja $b \in A$. Tällöin aliryhmäkriteerin nojalla $ab^{-1} \in H_i$ aina, kun $i \in I$ ja näin ollen myös $ab^{-1} \in A$, joten aliryhmäkriteerin nojalla $A \leq G$. □

**Määritelmä 2.8.** Olkoot $G$ ryhmä ja $H \subseteq G$. Määritellään

$$< H >= \bigcap_{\substack{H \subseteq A \\ A \leq G}} A,$$

joka edellisen Lauseen nojalla on ryhmän $G$ aliryhmä. Sanotaan tällöin, että $< H >$ on osajoukon $H$ *generoima* aliryhmä ja $H$ on aliryhmän $< H >$ *generaattori*.

**Lause 2.9.** Olkoot $G$ ryhmä ja $H \subseteq G$. Tällöin $< H >$ on pienin ryhmän $G$ aliryhmä, joka sisältää joukon $H$.

*Todistus.* Oletetaan, että $H \subseteq A$ ja $A \leq G$. Tällöin suoraan Määritelmän 2.8 nojalla $< H > \subseteq A$, joten $< H >$ on pienin ryhmän $G$ aliryhmä, joka sisältää joukon $H$. □

On selvää, että

$$< H > \;=\; \{h_1 h_2 \cdots h_n \in G \mid h_i \in H \text{ tai } h_i^{-1} \in H \text{ ja } n \in \mathbb{N}\}.$$

Jos $H = \{h_1, h_2, ..., h_n\}$, niin voidaan merkitä

$$< H > \;=\; < h_1, h_2, ..., h_n > .$$

Tällöin $< H >$ on *äärellisesti generoitu*. Erityisesti, jos $H = \{h\}$, niin aliryhmä $< h >$ on *syklinen* ja alkion $h \in G$ kertaluku on aliryhmän $< h >$ alkioiden lukumäärä.

**Määritelmä 2.10.** Ryhmä $G$ on *p-ryhmä*, jos jokaisen ryhmään $G$ kuuluvan alkion kertaluku on muotoa $p^n$, missä $n \in \mathbb{N}$ ja $p$ on alkuluku.

**Määritelmä 2.11.** Olkoon $\Sigma$ aakkosto ja $\Sigma^{-1}$ sellainen, että $a^{-1} \in \Sigma^{-1}$ aina, kun $a \in \Sigma$. Oletetaan, että alkioille $a$ ja $a^{-1}$ on voimassa kumoutumislaki: $aa^{-1} = 1$ ja $a^{-1}a = 1$. Oletetaan, että $|\Sigma| = |\Sigma^{-1}|$ ja $\Sigma \cap \Sigma^{-1} = \emptyset$ ja merkitään $S = \Sigma \cup \Sigma^{-1}$. Tällöin joukon $S$ generoima ryhmä on *vapaa ryhmä* $F_\Sigma$, jonka operaationa $*$ on katenointi, eli $a_1a_2 \cdots a_n * b_1b_2 \cdots b_m = a_1a_2 \cdots a_nb_1b_2 \cdots b_m$ aina, kun $a_1a_2 \cdots a_n \in S^*$ ja $b_1b_2 \cdots b_m \in S^*$.

**Määritelmä 2.12.** Olkoot $G$ ryhmä ja $H \leq G$. Tällöin joukko $gH = \{gh \in G \mid h \in H\}$ on aliryhmän $H$ *vasen sivuluokka* aina, kun $g \in G$. Vastaavasti määritellään aliryhmän $H$ *oikea sivuluokka* $Hg$ aina, kun $g \in G$. Aliryhmän $H$ *indeksi* $[G : H]$ on sen sivuluokkien lukumäärä. Aliryhmä $H$ on *normaali aliryhmä*, jos $gH = Hg$ aina, kun $g \in G$, jolloin merkitään $H \trianglelefteq G$.

**Lause 2.13.** Olkoon $G$ ryhmä ja $H \leq G$. Tällöin $H$ on normaali aliryhmä jos ja vain jos $gHg^{-1} \subseteq H$ aina, kun $g \in G$.

*Todistus.* Oletetaan, että $H \trianglelefteq G$. Olkoot $g \in G$ ja $h \in H$. Tällöin on olemassa sellainen $h' \in H$, että $gh = h'g$, jolloin $ghg^{-1} = h' \in H$. Oletetaan sitten, että $gHg^{-1} \subseteq H$ aina, kun $g \in G$. Olkoot $g \in G$ ja $h \in H$. Tällöin on olemassa sellainen $h' \in H$, että $ghg^{-1} = h'$, jolloin $gh = h'g$, joten $gH \subseteq Hg$. Vastaavasti nähdään, että $Hg \subseteq gH$, joten $H$ on normaali aliryhmä. □

**Määritelmä 2.14.** Olkoot $G$ ryhmä, $S \subseteq G$ ja

$$N_S = \bigcap_{\substack{S \subseteq N \\ N \trianglelefteq G}} N.$$

Tällöin $N_S$ on joukon $S$ *normaalisulkeuma*.

Normaalisulkeuma $N_S$ on aina ryhmän $G$ normaali aliryhmä. Väite todistetaan hyvin samanlaisesti kuten lause 2.7.

**Lemma 2.15.** Olkoon $G$ ryhmä ja $H \leq G$. Tällöin $gH = g'H$ jos ja vain jos $g'^{-1}g \in H$.

*Todistus.* Oletetaan, että $gH = g'H$. Tällöin on olemassa sellaiset joukkoon $H$ kuuluvat alkiot $h$ ja $h'$, että $gh = g'h'$, josta saadaan $g'^{-1}g = h'h^{-1} \in H$. Oletetaan sitten, että $g'^{-1}g \in H$. Tällöin on olemassa sellainen joukkoon $H$ kuuluva alkio $h$, että $g'^{-1}g = h$, jolloin $g = g'h \in g'H$. Tällöin $gH \subseteq g'H$ ja vastaavasti nähdään, että $g'h \subseteq gH$, joten $gH = g'H$. □

Olkoot $G$ ryhmä ja $H \leq G$. Jos $g' \in gH$, niin sanotaan, että alkio $g'$ on sivuluokan $gH$ *edustaja*. Joukko $S \subseteq G$, joka sisältää yhden alkion jokaisesta ryhmän $H$ sivuluokasta on sivuluokkien $gH$ *edustajisto*.

**Lause 2.16.** Olkoon $G$ ryhmä ja $N \trianglelefteq G$. Tällöin aliryhmän $N$ sivuluokat muodostavat ryhmän $G/N$ operaationa $*$, joka määritellään seuraavasti: Olkoon $g \in G$ ja $h \in G$. Tällöin $gN * hN = ghN$.

*Todistus.* Operaatio $*$ on hyvin määritelty: Olkoot $g$, $g'$, $h$ ja $h'$ ryhmän $G$ sellaisia alkioita, että $gN = g'N$ ja $hN = h'N$. Tällöin Lemman 2.15 nojalla on olemassa sellaiset ryhmään $N$ kuuluvat alkiot $n$ ja $n'$, että $g'^{-1}g = n$ ja $h'^{-1}h = n'$. Tällöin

$$(g'h')^{-1}gh = h'^{-1}g'^{-1}gh = h'^{-1}nh \in h'^{-1}Nh = h'^{-1}hN = n'N = N.$$

Näin ollen Lemman 2.15 nojalla $g'h'N = ghN$.

Assosiatiivisuus on voimassa ryhmässä $G/N$, koska se on voimassa ryhmässä $G$. Ryhmän $G/N$ ykkösalkio on $N$. Alkion $gN \in G/N$ käänteisalkio $(gN)^{-1} = g^{-1}N$, joka kuuluu ryhmään $G/N$, koska $G$ on ryhmä. □

**Määritelmä 2.17.** Olkoon $G$ ryhmä ja $X$ joukko. Tällöin kuvaus

$$f : G \times X \to X$$

on *ryhmän (oikea) toiminta joukossa* $X$, jos $f$ toteuttaa seuraavat kaksi aksioomaa:

$$f(1_G, x) = x \text{ aina, kun } x \in X \text{ ja}$$
$$f(h, f(g, x)) = f(gh, x) \text{ aina, kun } g \in G, h \in G \text{ ja } x \in X.$$

Merkitään jatkossa $f(g, x) = g.x$, jos ryhmän toiminta on kontekstista selvä.

**Määritelmä 2.18.** Oletetaan, että ryhmä $G$ toimii joukossa $X$. Tällöin alkion $x \in X$ *stabilisaattori* on joukko

$$Stab_G(x) = \{g \in G \mid g.x = x\} \tag{1}$$

ja *rata* on joukko

$$\mathcal{O}_G(x) = \{g.x \mid g \in G\}. \tag{2}$$

Ryhmän toiminnan määritelmän nojalla $1_G \in Stab_G(x)$, joten $Stab_G(x) \neq \emptyset$. Olkoot $g \in Stab_G(x)$ ja $h \in Stab_G(x)$. Tällöin

$$\begin{aligned} x &= 1_G.x \\ &= gg^{-1}.x \\ &= g^{-1}.x, \end{aligned}$$

joten $g^{-1} \in Stab_G(x)$ ja selvästi tällöin $x = hg^{-1}.x$, joten $hg^{-1} \in Stab_G(x)$. Näin ollen aliryhmäkriteerin nojalla $Stab_G(x) \leq G$ aina, kun $x \in X$.

**Määritelmä 2.19.** Ryhmän $G$ alkiot $g$ ja $g'$ ovat *konjugaatteja*, jos on olemassa sellainen $h \in G$, että $g' = h^{-1}gh$.

**Esimerkki 2.20.** Näytetään, miten ryhmä $G$ toimii itsessään konjugoimalla. Olkoon $f : G \times G \to G$ määritelty siten, että $g.h = g^{-1}hg$ aina, kun $g \in G$ ja $h \in G$. Tällöin Määritelmän 2.17 ehdot ovat voimassa:

$$1_G.h = 1_G^{-1}h1_G = h$$
$$g'.(g.h) = g'.g^{-1}hg = g'^{-1}g^{-1}hgg' = (gg')^{-1}hgg' = gg'.h$$

**Määritelmä 2.21.** Ryhmän $G$ toiminta joukossa $X$ on *uskollinen*, jos aina, kun $g \in G$, $h \in G$ ja $g \neq h$ on olemassa sellainen $x \in X$, että $g.x \neq h.x$.

**Määritelmä 2.22.** Olkoon $Y = X^* \cup X^\omega$. Ryhmän $G$ uskollinen toiminta joukossa $Y$ on *itsensä kaltainen*, jos aina, kun $g \in G$, $w \in Y$ ja $a \in X$ on olemassa sellaiset $h \in G$ ja $b \in X$, että $g.aw = bh.w$.

**Määritelmä 2.23.** Olkoon $G$ ryhmä. Jos on olemassa joukko $Y = X^* \cup X^\omega$ ja itsensä kaltainen toiminta $f : G \times Y \to Y$, niin $G$ on *itsensä kaltainen ryhmä*.

**Määritelmä 2.24.** Olkoot $(X, *)$ ja $(Y, \cdot)$ joukkoja varustettuna jollakin operaatiolla. Tällöin kuvaus $f : X \to Y$ on *homomorfismi*, jos

$$f(x * y) \quad = \quad f(x) \cdot f(y),$$

aina, kun $x \in X$ ja $y \in X$. Jos $f$ on lisäksi bijektio, niin $f$ on *isomorfismi* ja tällöin $X$ ja $Y$ ovat *isomorfisia*, jolloin merkitään $X \cong Y$. Jos $X = Y$ ja $* = \cdot$, niin $f$ on *automorfismi*.

**Lause 2.25.** Olkoot $G$ ja $G'$ ryhmiä ja $\varphi : G \to G'$ homomorfismi. Tällöin $\varphi(1) = 1$, $\varphi(g^{-1}) = \varphi(g)^{-1}$ ja jos $H \leq G$, niin $\varphi(H) \leq G'$.

*Todistus.* Ensimmäinen väite seuraa siitä, että $\varphi(1) = \varphi(1 * 1) = \varphi(1)\varphi(1)$, jolloin kertomalla molemmat puolet alkiolla $\varphi(1)^{-1}$ nähdään, että $1 = \varphi(1)$.

Vastaavasti saadaan, että $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1$, jolloin kertomalla molemmat puolet oikealta alkiolla $\varphi(g)^{-1}$ nähdään, että $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Olkoot sitten $g_1' \in \varphi(H)$ ja $g_2' \in \varphi(H)$. Tällöin on olemassa sellaiset $g_1 \in H$ ja $g_2 \in H$, että $\varphi(g_1) = g_1'$ ja $\varphi(g_2) = g_2'$. Näin ollen saadaan, että $g_1'g_2' = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in \varphi(H)$. Lisäksi jo todistetun nojalla $\varphi(g)^{-1} \in \varphi(H)$ aina, kun $\varphi(g) \in \varphi(H)$ ja $1 \in \varphi(H)$, joten väite on todistettu. □

**Esimerkki 2.26.** Olkoon $(X, *)$ joukko varustettuna jollakin operaatiolla. Tällöin

$$Aut(X) = \{\varphi : X \to X \mid \varphi \text{ on automorfismi}\} \leq Sym(X).$$

Ryhmää $Aut(X)$ sanotaan joukon $X$ *automorfismiryhmäksi*. Osoitetaan, että $Aut(X)$ täyttää aliryhmäkriteerin. Identiteettikuvaus on automorfismi, joten $Aut(X)$ on epätyhjä. Olkoot $\varphi \in Aut(X)$, $\phi \in Aut(X)$, $x \in X$ ja $y \in X$. Tällöin seuraava yhtälöketju on voimassa:

$$\begin{aligned} \varphi \circ \phi(x * y) &= \varphi(\phi(x * y)) \\ &= \varphi(\phi(x) * \phi(y)) \\ &= \varphi(\phi(x)) * \varphi(\phi(y)) \\ &= \varphi \circ \phi(x) * \varphi \circ \phi(y), \end{aligned}$$

joten kahden automorfismin yhdistetty kuvaus on automorfismi. Automorfismi on bijektio, joten automorfismin $\phi$ käänteiskuvaus $\phi^{-1}$ on olemassa. Saadaan:

$$\begin{aligned} & x * y && = \phi(\phi^{-1}(x)) * \phi(\phi^{-1}(y)) \\ & && = \phi(\phi^{-1}(x) * \phi^{-1}(y)) \\ \Leftrightarrow \quad & \phi^{-1}(x * y) && = \phi^{-1}(x) * \phi^{-1}(y). \end{aligned}$$

Näin ollen automorfismin käänteiskuvaus on myös automorfismi, joten myös yhdistetty kuvaus $\varphi \circ \phi^{-1} \in Aut(G)$.

Kahden homomorfismin yhdistetty kuvaus on homomorfismi, mikä nähdään samalla tavalla kuin edellisessä todistuksessa automorfismien tapauksessa. Tätä tietoa käytetään seuraavassa esimerkissä.

**Esimerkki 2.27.** Olkoot $\Sigma = \{a_1, a_2, ..., a_n\}$ ja $\Delta = \{b_1, b_2, ..., b_n\}$ aakkostoja. Tällöin $F_\Sigma \cong F_\Delta$, mikä nähdään seuraavasti: Määritellään kuvaus $f : \Sigma \to \Delta$, $f(a_i) = b_i$ aina, kun $i \in \{1, 2, ..., n\}$. Koska $F_\Sigma$ on vapaa, kuvaus $f$ laajenee yksikäsitteisesti sellaiseksi homomorfismiksi $\varphi : F_\Sigma \to F_\Delta$, että $\varphi(a_i) = f(a_i) = b_i$ aina, kun $i \in \{1, 2, ..., n\}$. Samoin $f$ laajenee yksikäsitteisesti sellaiseksi homomorfismiksi $\phi : F_\Delta \to F_\Sigma$, että $\phi(b_i) = f^{-1}(b_i) = a_i$ aina, kun $i \in \{1, 2, ..., n\}$. Tällöin

$$\begin{aligned} \phi \circ \varphi(a_{i_1} a_{i_2} ... a_{i_k}) &= \phi \circ \varphi(a_{i_1}) \phi \circ \varphi(a_{i_2}) ... \phi \circ \varphi(a_{i_k}) \\ &= \phi(b_{i_1}) \phi(b_{i_2}) ... \phi(b_{i_k}) \\ &= a_{i_1} a_{i_2} ... a_{i_k}. \end{aligned}$$

Samoin nähdään, että $\varphi \circ \phi(w) = w$ aina, kun $w \in F_\Delta$, joten $\phi$ on homomorfismin $\varphi$ käänteiskuvaus. Näin ollen $\varphi : F_\Sigma \to F_\Delta$ on isomorfismi, joten $F_\Sigma \cong F_\Delta$. Näin ollen vapaata ryhmää, jonka generoi $n$ alkiota voidaan merkitä symbolilla $F_n$.

**Määritelmä 2.28.** Olkoot $\Sigma$ aakkosto, $F_\Sigma$ vapaa ryhmä ja $R \subseteq F_\Sigma$. Samaistetaan ykkösalkio $1_{F_\Sigma}$ jokaisen alkion, joka kuuluu joukkoon $R$ kanssa. Määritellään $< \Sigma | R >= F_\Sigma / N_R$, missä $N_R$ on joukon $R$ normaalisulkeuma. Olkoon $G$ sellainen ryhmä, että $G \cong < \Sigma | R >$. Tällöin $< \Sigma | R >$ on ryhmän $G$ *esitys*. Jos lisäksi $\Sigma$ ja $R$ ovat molemmat äärellisiä, niin $G$ on *äärellisesti esitetty ryhmä*.

**Esimerkki 2.29.** Tarkastellaan esimerkkinä Diedriryhmää
$D_n \cong < s, r | r^n, s^2, (sr)^2 >$. Esityksestä nähdään, että $rs = sr^{n-1}$ aina, kun $n > 2$, joten jokainen ryhmän $F_\Sigma / N_R$ alkio on muotoa $s^m r^k$, koska kirjaimet $s$ voidaan siirtää aina vasemmalle. Toisaalta, koska $s^2 = 1$, niin edellä $0 \leq m \leq 1$ ja $0 \leq k \leq n$. Nähdään, että $|D_n| \leq 2n$.

Olkoon $\mathcal{G}$ kaikkien ryhmien joukko ja $\mathcal{H} \subseteq \mathcal{G}$. Tällöin $\mathcal{P}$ on joukon $\mathcal{H}$ *ominaisuus*, jos jokaisella joukkoon $\mathcal{H}$ kuuluvalla ryhmällä on ominaisuus $\mathcal{P}$ ja millään ryhmällä joukossa $\mathcal{G} \setminus \mathcal{H}$ ei ole ominaisuutta $\mathcal{P}$. Jos ryhmällä on jokin ominaisuus $\mathcal{P}$, sanotaan yksinkertaisesti, että ryhmä on $\mathcal{P}$.

**Määritelmä 2.30.** Olkoon $G$ ryhmä ja $\mathcal{P}$ jokin ominaisuus. Tällöin ryhmä $G$ on *residuaalisesti* $\mathcal{P}$, jos jokaista epätriviaalia alkiota $g \in G$ kohti on olemassa ryhmä $H$, jolla on ominaisuus $\mathcal{P}$ ja sellainen homomorfismi $f : G \to H$, että $f(g) \neq 1_H$.

## 2.3 Yleiset lineaariset ryhmät

**Määritelmä 2.31.** Olkoon $R$ joukko ja olkoot $+$ sekä $\cdot$ binäärikuvauksia joukossa $R$. Tällöin $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot ovat voimassa:

$$
\begin{aligned}
&(R, +) \text{ on Abelin ryhmä,} \\
&(R, \cdot) \text{ on monoidi,} \\
&a \cdot (b + c) = a \cdot b + a \cdot c \text{ ja} \\
&(a + b) \cdot c = a \cdot c + b \cdot c
\end{aligned}
$$

aina, kun $a$, $b$ ja $c$ kuuluvat joukkoon $R$. Kutsutaan kahta jälkimmäistä ehtoa *distributiivilaeiksi*. Merkitään rengasta $(R, +, \cdot)$ lyhyemmin symbolilla $R$ jos operaatiot ovat kontekstista selvät. Jos alkiota $a \in R$ kohti on olemassa sellainen alkio $a^{-1}$, että $a \cdot a^{-1} = 1_R = a^{-1} \cdot a$, missä $1_R$ on monoidin $(R, \cdot)$ ykkösalkio, niin $a$ on renkaan $R$ *yksikkö*.

**Esimerkki 2.32.** Kokonaislukujen joukko $\mathbb{Z}$ on rengas tavallisen yhteenlaskun ja tulon suhteen Renkaan $\mathbb{Z}$ ainoat yksiköt ovat 1 ja $-1$. Olkoon $n \in \mathbb{Z}_+$,

tällöin *n-adiset kokonaisluvut* $\mathbb{Z}_n$ muodostavat renkaan. Joukon $\mathbb{Z}_n$ alkiot ovat äärettömiä formaaleja summia

$$\sum_{i=0}^{\infty} a_i n^i, \quad \text{missä} \quad a_i \in \{0, 1, ..., n-1\}.$$

Olkoot $X_n = \{0, 1, ..., n-1\}$, $a_i \in X_n$, $b_i \in X_n$ ja $i \in \mathbb{N}$. Tällöin

$$a_i n^i + b_i n^i + \epsilon_{i-1} n^i = c_i n^i + \epsilon_i n^{i+1},$$

missä $c_i \in X_n$ ja $\epsilon_i \in X_n$ aina, kun $i \in \mathbb{N}$ ja $\epsilon_{-1} = 0$. Tällöin yhteenlasku voidaan määritellä seuraavasti:

$$\sum_{i=0}^{\infty} a_i n^i + \sum_{i=0}^{\infty} b_i n^i \quad = \sum_{i=0}^{\infty} (c_i + \epsilon_{i-1}) n^i.$$

Helposti nähdään, että näin muodostettu yhteenlasku muodostaa Abelin ryhmän. Olkoot $m \in \mathbb{N}$ ja $\alpha \in \mathbb{Z}_n$, tällöin

$$m\alpha = \sum_{i=1}^{m} \alpha.$$

Näin ollen tulo voidaan määritellä seuraavasti:

$$(\sum_{i=0}^{\infty} a_i n^i) \cdot (\sum_{i=0}^{\infty} b_i n^i) \quad = \sum_{i=0}^{\infty} \beta_i,$$

missä

$$\beta_i = a_i n^i \sum_{j=0}^{\infty} b_j n^j.$$

Monoidin assosiatiivisuus ja renkaan distributiivilait voidaan nähdä suoraviivaisesti. Tulon määritelmästä nähdään myös suoraviivaisesti, että alkio

$$\sum_{i=0}^{\infty} a_i n^i$$

on renkaan $\mathbb{Z}_n$ yksikkö jos ja vain jos $a_0 \neq 0$.

Olkoon $a \in \mathbb{N}$, tällöin luvulla $a$ on yksikäsitteinen esitys muodossa

$$\sum_{i=0}^{k} a_i n^i,$$

missä $k \in \mathbb{N}$. Voidaan määritellä injektiivinen homomorfismi $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ asettamalla

$$\varphi(a) = \sum_{i=0}^{\infty} a_i n^i,$$

missä $a_i = 0$ aina, kun $i > k$ ja

$$\varphi(-a) = -\sum_{i=0}^{\infty} a_i n^i.$$

Erityisesti

$$\varphi(1) = 1 + \sum_{i=1}^{\infty} 0n^i \text{ ja}$$

$$\varphi(-1) = \sum_{i=0}^{\infty} (n-1)n^i$$

ovat renkaan $Z_n$ yksiköitä.

Olkoon $R$ rengas. Lineaarialgebran teoriasta muistetaan, että matriisi $M \in R^{n\times n}$ on kääntyvä jos ja vain jos $det(M)$ on renkaan $R$ yksikkö. Selvästi renkaan yksikköjen tulo on edelleen renkaan yksikkö. Näin ollen kääntyvien matriisien joukko muodostaa ryhmän matriisien kertolaskun suhteen.

**Määritelmä 2.33.** Olkoon $R$ rengas. Määritellään ryhmä

$$GL_n(R) = \{M \in R^{n\times n} \mid det(M) \text{ on renkaan } R \text{ yksikkö}\}.$$

Sanotaan, että $GL_n(R)$ on *yleinen lineaarinen ryhmä* yli renkaan $R$.

Olkoon $R$ rengas. Määritellään kuvaus $\tau_v : R^n \to R^n$ siten, että $\tau_v(u) = v + u$ aina, kun $v \in R^n$. Olkoon $M \in R^{n\times n}$ kääntyvä, tällöin kuvaukset, jotka ovat muotoa $M_v : R^n \to R^n$, missä $M_v(u) = v + Mu$, muodostavat ryhmän kuvausten yhdistämisen suhteen. Helposti nähdään, että $M_v = \tau_v \circ M_0$.

**Määritelmä 2.34.** Olkoon $R$ rengas. Määritellään ryhmä

$$Aff_n(R) = \{M_v \mid det(M) \text{ on renkaan } R \text{ yksikkö ja } v \in R^n\}.$$

Sanotaan, että $Aff_n(R)$ on *affiinikuvausten ryhmä* yli renkaan $R$.

## 2.4 Puolisuora tulo ja kehätulo

**Lause 2.35.** Olkoot $H$ ja $K$ ryhmiä, ja $\varphi : K \to Aut(H)$ homomorfismi. Tällöin $(H \times K, *)$ on ryhmä, missä

$$(h, k) * (h', k') = (h\varphi(k)(h'), kk').$$

*Todistus.* Olkoot $(h,k)$, $(h',k')$ ja $(h'',k'')$ joukkoon $H \times K$ kuuluvia alkioita. Merkitään $\varphi(k) = \varphi_k$, jotta merkinnät pysyvät selkeinä. Osoitetaan, että assosiatiivisuus on voimassa:

$$\begin{aligned}(h,k) * ((h',k') * (h'',k'')) &= (h,k) * (h'\varphi_{k'}(h''), k'k'') \\ &= (h\varphi_k(h'\varphi_{k'}(h'')), kk'k'') \\ &= (h\varphi_k(h')\varphi_k(\varphi_{k'}(h'')), kk'k'') \\ &= (h\varphi_k(h')\varphi_{kk'}(h''), kk'k'') \\ &= (h\varphi_k(h'), kk') * (h'',k'') \\ &= ((h,k) * (h',k')) * (h'',k'').\end{aligned}$$

Neutraalialkio on $(1_H, 1_K)$:

$$\begin{aligned}(h,k) * (1_H, 1_K) &= (h\varphi_k(1_H), k1_K) \\ &= (h,k) \\ &= (1_H\varphi_{1_K}(h), 1_K k) \\ &= (1_H, 1_K) * (h,k).\end{aligned}$$

Alkion $(h,k)$ käänteisalkio on $(\varphi_{k^{-1}}(h^{-1}), k^{-1})$:

$$\begin{aligned}(h,k) * (\varphi_{k^{-1}}(h^{-1}), k^{-1}) &= (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) \\ &= (h\varphi_{1_K}(h^{-1}), 1_K) \\ &= (1_H, 1_K) \\ &= (\varphi_{k^{-1}}(1_H), 1_K) \\ &= (\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), k^{-1}k) \\ &= (\varphi_{k^{-1}}(h^{-1}), k^{-1}) * (h,k).\end{aligned}$$

□

**Määritelmä 2.36.** Olkoon $(H \times K, *)$ Lauseen 2.35 ryhmä. Merkitään sitä $H \rtimes_\varphi K$ tai $H \rtimes K$, jos $\varphi$ on kontekstista selvä. Ryhmä $H \rtimes K$ on ryhmien $H$ ja $K$ *ulkoinen puolisuora tulo*. Jos funktion $\varphi$ kuvajoukkoon kuuluu ainoastaan identiteettikuvaus, niin saadaan *ulkoinen suora tulo*, jota merkitään $H \times K$.

Ulkoinen suora tulo yleistyy helposti *n-kertaiseksi ulkoiseksi suoraksi tuloksi*, missä $n \in \mathbb{N}$: Olkoon $G_i$ ryhmä aina, kun $i \in \{1, 2, ..., n\}$. Merkitään $G = G_1 \times G_2 \times ... \times G_n$. Määritellään operaatio $* : G \times G \to G$ siten, että $(g_1, g_2, ..., g_n) * (h_1, h_2, ..., h_n) = (g_1h_1, g_2h_2, ..., g_nh_n)$ aina, kun $g_i \in G_i$ ja $h_i \in G_i$. Soveltamalla Lausetta 2.35 $n-1$ kertaa nähdään, että $(G, *)$ on ryhmä. Jos tässä $G_i = H$ aina, kun $i \in \{1, 2, ..., n\}$, niin merkitään $G_1 \times G_2 \times ... \times G_n = H^n$.

**Määritelmä 2.37.** Olkoot $G$ ryhmä, $N \trianglelefteq G$ ja $H \leq G$. Jos $G = NH$ ja $N \cap H = \{1\}$, niin $G$ on ryhmien $N$ ja $H$ *sisäinen puolisuora tulo*.

**Lemma 2.38.** Olkoon $G$ ryhmien $N$ ja $H$ sisäinen puolisuora tulo. Tällöin jokainen alkio $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = nh$, missä $n \in N$ ja $h \in H$.

*Todistus.* Suoraan sisäisen puolisuoran tulon määritelmästä seuraa, että jokaisella alkiolla $g \in G$ on vähintään yksi esitys muodossa $nh$. Oletetaan sitten, että $g = n_1h_1 = n_2h_2$. Tällöin $n_2^{-1}n_1 = h_2h_1^{-1}$, joten koska $N \cap H = 1$, niin on oltava, että $n_1 = n_2$ ja $h_1 = h_2$. □

**Lause 2.39.** Olkoon $G = K \rtimes_\varphi H$. Tällöin on olemassa sellaiset $N \trianglelefteq G$ ja $H' \leq G$, että $N \cap H' = 1$, $G = NH'$, $K \cong N$ ja $H \cong H'$.

*Todistus.* Olkoot $N = \{(n, 1) \in G \mid n \in K\}$ ja $H' = \{(1, h) \in G \mid h \in H\}$. Selvästi $N$ ja $H'$ ovat ryhmän $G$ aliryhmiä, $K \cong N$ ja $H \cong H'$. Olkoon $(k, h) \in G$. Tällöin

$$\begin{aligned}(k,h)(n,1)(k,h)^{-1} &= (k\varphi_h(n), h)(\varphi_{h^{-1}}(k^{-1}), h^{-1}) \\ &= (k\varphi_h(n)\varphi_h(\varphi_{h^{-1}}(k^{-1})), hh^{-1}) \\ &= (k\varphi_h(n)k^{-1}, 1) \in N.\end{aligned}$$

Lisäksi selvästi $N \cap H' = 1$ ja $G = NH'$, joten väite on todistettu. □

**Lause 2.40.** Olkoon $G$ ryhmien $N$ ja $H$ sisäinen puolisuora tulo. Tällöin on olemassa sellainen homomorfismi $\varphi : H \to Aut(N)$, että $G \cong N \rtimes_\varphi H$.

*Todistus.* Määritellään $\varphi : H \to Aut(N)$ siten, että $\varphi_h(n) = hnh^{-1}$ aina, kun $h \in H$ ja $n \in N$. Määritellään kuvaus $\varphi' : G \to N \times H$ siten, että $\varphi'(g) = (n, h)$, missä $g = nh$. Lemman 2.38 mukaan $\varphi'$ on hyvin määritelty ja selvästi bijektio. Olkoot $n_1h_1 = g_1 \in G$ ja $n_2h_2 = g_2 \in G$. Tällöin

$$\begin{aligned}g_1g_2 &= n_1h_1n_2h_2 \\ &= n_1h_1n_2h_1^{-1}h_1h_2 \\ &= n_1\varphi_{h_1}(n_2)h_1h_2,\end{aligned}$$

jolloin saadaan, että

$$\begin{aligned}\varphi'(g_1)\varphi'(g_2) &= (n_1, h_1)(n_2, h_2) \\ &= (n_1\varphi_{h_1}(n_2), h_1h_2) \\ &= \varphi'(g_1g_2),\end{aligned}$$

joten kuvaus $\varphi'$ on isomorfismi. □

**Lemma 2.41.** Olkoot $G$ ryhmä, $X = \{x_1, x_2, ..., x_n\}$ äärellinen joukko ja $\sigma \in Sym(X)$. Määritellään kuvaus $\rho_\sigma : G^X \to G^X$ siten, että

$$\rho_\sigma((g_{x_1}, g_{x_2}, ..., g_{x_n})) = (g_{y_1}, g_{y_2}, ..., g_{y_n}),$$

missä $\sigma(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n)$. Tällöin $\rho_\sigma \in Aut(G^X)$.

*Todistus.* Olkoon $\sigma((x_1, x_2, ..., x_n)) = (y_1, y_2, ..., y_n)$, tällöin:

$$\begin{aligned}\rho_\sigma((gg'_{x_1}, gg'_{x_2}, ..., gg'_{x_n})) &= (gg'_{y_1}, gg'_{y_2}, ..., gg'_{y_n}) \\ &= (g_{y_1}, g_{y_2}, ..., g_{y_n})(g'_{y_1}, g'_{y_2}, ..., g'_{y_n}) \\ &= \rho_\sigma((g_{x_1}, g_{x_2}, ..., g_{x_n}))\rho_\sigma((g'_{x_1}, g'_{x_2}, ..., g'_{x_n}))\end{aligned}$$

joten $\rho_h$ on homomorfismi. Koska $\sigma \in Sym(X)$, niin selvästi $\rho_\sigma$ on bijektio ja näin ollen se on automorfismi. □

**Lemma 2.42.** Olkoot $G$ ryhmä ja $X = \{x_1, x_2, ...x_n\}$ äärellinen joukko. Määritellään kuvaus $\varphi : H \to Aut(G^X)$ siten, että $\varphi(\sigma) = \rho_\sigma$, missä $H \leq Sym(X)$ ja $\rho_\sigma$ on määritelty kuten Lemmassa 2.41. Tällöin kuvaus $\varphi$ on homomorfismi.

*Todistus.* Olkoot $\tau \in H$ ja $\sigma \in H$. Tällöin

$$\begin{aligned}\rho_{\sigma\tau}((g_{x_1}, g_{x_2}, ..., g_{x_n})) &= (g_{\sigma\tau(x_1)}, g_{\sigma\tau(x_2)}, ..., g_{\sigma\tau(x_n)}) \\ &= \rho_\tau((g_{\sigma(x_1)}, g_{\sigma(x_2)}, ..., g_{\sigma(x_n)})) \\ &= \rho_\tau(\rho_\sigma((g_{x_1}, g_{x_2}, ..., g_{x_n}))).\end{aligned}$$

Näin ollen $\varphi(\sigma\tau) = \rho_{\sigma\tau} = \rho_\tau \circ \rho_\sigma = \varphi(\tau) \circ \varphi(\sigma) = \varphi(\sigma)\varphi(\tau)$. □

**Määritelmä 2.43.** Olkoot $G$ ryhmä, $X = \{x_1, x_2, ...x_n\}$ äärellinen joukko, $H \leq Sym(X)$ ja $\varphi$, kuten Lemmassa 2.42. Lauseen 2.35 nojalla $G^X \rtimes_\varphi H$ on ryhmä, jota merkitään $G \wr H$, jos $X$ on selvä kontekstista. Sanotaan, että ryhmä $G \wr H$ on ryhmien $G$ ja $H$ *kehätulo*.

## 2.5 Ryhmän kasvu

**Määritelmä 2.44.** Olkoot $G$ äärellisesti generoitu ryhmä, $H$ sen generaattori ja $g \in G$. Pienin sellainen luku $n \in \mathbb{N}$, että $g = h_1 h_2 \cdots h_n$, on alkion $g$ *pituus* $l_G^H(g)$, missä $h_i \in H$ tai $h_i^{-1} \in H$ aina, kun $i \in \{1, 2, ..., n\}$.

**Määritelmä 2.45.** Olkoot $G$ äärellisesti generoitu ryhmä ja $H$ sen generaattori. Kuvaus

$$\gamma_G^H : \mathbb{N} \to \mathbb{N}$$

on ryhmän $G$ *kasvufunktio* generaattorin $H$ suhteen, missä

$$\gamma_G^H(n) = |G_H^{l \leq n}|$$

ja

$$G_H^{l \leq n} = \{g \in G \mid l_G^H(g) \leq n\}$$

aina, kun $n \in \mathbb{N}$. Jos ryhmä tai generaattori on kontekstista selvä, niin jätetään kasvufunktiosta ja alkion pituudesta vastaava merkintä pois. Merkitään myös

$$G_H^{l=n} = \{g \in G \mid l_G^H(g) = n\}.$$

Selvästi kasvufunktio on aina ylhäältä rajoitettu: Olkoot $G$ äärellisesti generoitu ryhmä, $H$ sen generaattori ja $|H| = m$. Tällöin

$$\gamma(n) = \sum_{n=0}^{n} |G_H^{l=n}| \leq \sum_{n=0}^{n} (2m)^n \leq (2m)^{n+1}$$

aina, kun $n \in \mathbb{N}$.

**Lause 2.46.** Äärettömän äärellisesti generoidun ryhmän $G$ kasvufunktio on aidosti kasvava.

*Todistus.* Olkoot $G$ ääretön ryhmä ja $H =< g_1, g_2, ..., g_s >$ sen generaattori. Oletetaan, että on olemassa sellainen $m \in \mathbb{N}$, että $\gamma(m+1) = \gamma(m)$. Jos $g = g_{i_1} g_{i_2} \cdots g_{i_{m+1}}$, missä $g_{i_k} \in H$ tai $g_{i_k}^{-1} \in H$, niin on oltava sellaiset $g_{j_1}, g_{j_2}, ..., g_{j_r}$, että $g_{j_k} \in H$ tai $g_{j_k}^{-1} \in H$, $0 \leq r < m+1$ ja $g = g_{j_1} g_{j_2} \cdots g_{j_r}$. Näin ollen jokainen muotoa $g = g_{i_1} g_{i_2} \cdots g_{i_l}$ oleva alkio, missä $l > m$, voidaan induktiivisesti lyhentää muotoon $g = g_{j_1} g_{j_2} \cdots g_{j_r}$, missä $0 \leq r < m+1$. Tällöin $G$ on äärellinen ryhmä mikä on ristiriita. □

**Lause 2.47.** Äärellisesti generoidun ryhmän $G$ kasvufunktio $\gamma$ toteuttaa epäyhtälön $\gamma(m+n) \leq \gamma(m)\gamma(n)$ aina, kun $m \in \mathbb{N}$ ja $n \in \mathbb{N}$.

*Todistus.* Olkoot $G$ ryhmä ja $H =< g_1, g_2, ..., g_s >$ sen generaattori. Olkoon $l(g) \leq m+n$, tällöin on olemassa sellaiset $m' \leq m$ ja $n' \leq n$, että $g = g_{i_1} g_{i_2} \cdots g_{i_{m'}} g_{i_{m'+1}} \cdots g_{i_{m'+n'}}$, missä $g_{i_k} \in H$ tai $g_{i_k}^{-1} \in H$. Koska $g_{i_1} g_{i_2} \cdots g_{i_{m'}} \in G^{l \leq m}$ ja $g_{i_{m'+1}} g_{i_{m'+2}} \cdots g_{i_{m'+n'}} \in G^{l \leq n}$, niin $g \in G^{l \leq m} G^{l \leq n}$. Näin ollen $G^{l \leq m+n} \subseteq G^{l \leq m} G^{l \leq n}$, joten väite seuraa. □

**Määritelmä 2.48.** Olkoot $f : \mathbb{N} \to \mathbb{R}_+$ ja $g : \mathbb{N} \to \mathbb{R}_+$. Määritellään relaatio $\preceq$ siten, että $f \preceq g$ jos on olemassa sellaiset $C > 0$ ja $\alpha > 0$, että $f(n) \leq C g(\alpha n)$ aina, kun $n > 0$. Sanotaan, että $f$ ja $g$ ovat *ekvivalentit* jos $f \preceq g$ ja $g \preceq f$, jolloin merkitään $f \sim g$.

**Lause 2.49.** Olkoon $G$ äärellisesti generoitu ryhmä. Olkoot $H$ ja $H'$ ryhmän $G$ kaksi äärellistä generaattoria. Tällöin $\gamma^H \sim \gamma^{H'}$.

*Todistus.* Merkitään

$$\alpha = max\{l^{H'}(h) \in \mathbb{N} \mid h \in H\}.$$

Näin ollen $l^H(g) \leq \alpha l^{H'}(g)$ aina, kun $g \in G$. Tästä seuraa, että $G_H^{l \leq n} \subseteq G_{H'}^{l \leq \alpha n}$, mistä saadaan, että $\gamma^H(n) \leq \gamma^{H'}(\alpha n)$ aina, kun $n \in \mathbb{N}$. Ollaan osoitettu, että $\gamma^H \preceq \gamma^{H'}$. Symmetrisesti saadaan, että $\gamma^{H'} \preceq \gamma^H$, joten $\gamma^H \sim \gamma^{H'}$. □

Samoin voidaan todistaa, että jos $G$ ja $G'$ ovat äärellisesti generoituja ryhmiä ja $\varphi : G \to G'$ on injektiivinen homomorfismi, niin $\gamma_G \preceq \gamma_{G'}$. Erityisesti jos $G$ ja $G'$ ovat isomorfisia, niin $\gamma_G \sim \gamma_{G'}$.

**Määritelmä 2.50.** Olkoon $f : \mathbb{N} \to \mathbb{R}_+$. Tällöin funktio $f$ on *polynomiaalinen* jos on olemassa sellainen $\alpha > 0$, että $f(n) \sim n^\alpha$. Funktio $f$ on *ylipolynomiaalinen* jos

$$\lim_{n\to\infty} \frac{\ln(f(n))}{\ln(n)} = \infty.$$

Funktio $f$ on *eksponentiaalinen* jos $f(n) \sim e^n$ ja *alieksponentiaalinen* jos

$$\lim_{n\to\infty} \frac{\ln(f(n))}{n} = 0.$$

Jos $f$ on sekä ylipolynomiaalinen että alieksponentiaalinen, niin sillä on *keskitason kasvu*.

On helppo nähdä, että funktio $e^{n^\alpha}$ on ylipolynomiaalinen aina, kun $\alpha > 0$ ja alieksponentiaalinen aina, kun $\alpha < 1$.

Ryhmän $G$ generaattori $H$ on *symmetrinen* jos $g^{-1} \in H$ aina, kun $g \in H$.

**Lemma 2.51.** Olkoot $G$ äärellisesti generoitu ryhmä, $G' \leq G$ ja $[G : G'] < \infty$. Olkoot $H$ ryhmän $G$ äärellinen symmetrinen generaattori ja $S$ aliryhmän $G'$ sellainen sivuluokkien edustajisto, johon kuuluu alkio $1_G$. Tällöin joukko $S^{-1}HS \cap G'$ generoi ryhmän $G'$. Erityisesti $G'$ on äärellisesti generoitu.

*Todistus.* Merkitään $H' = S^{-1}HS \cap G'$ ja olkoon $g' \in G'$. Tällöin on olemassa sellaiset alkiot $g_i \in H$, että $g' = g_1 g_2 \cdots g_n$, missä $1 \leq i \leq n$. Koska $S$ on edustajisto, niin on olemassa sellaiset alkiot $g'_n \in G'$ ja $s_n \in S$, että $g_n = s_n g'_n$, jolloin $g'_n = s_n^{-1} g_n \in H'$. Vastaavasti jokaista alkiota $g_i s_{i+1}$ kohti on olemassa sellaiset alkiot $g'_i \in G'$ ja $s_i \in S$, että $g_i s_{i+1} = s_i g'_i$, jolloin $g'_i = s_i^{-1} g_i s_{i+1} \in H'$ aina, kun $2 \leq i \leq n-1$. Saadaan, että

$$\begin{aligned}
g' \quad &= g_1 g_2 \cdots g_n \\
&= g_1(s_2 s_2^{-1}) g_2 (s_3 s_3^{-1}) \cdots g_{n-1}(s_n s_n^{-1}) g_n \\
&= (g_1 s_2)(s_2^{-1} g_2 s_3) \cdots (s_{n-1}^{-1} g_{n-1} s_n)(s_n^{-1} g_n) \\
&= (g_1 s_2) g'_2 g'_3 \cdots g'_n \\
\text{missä} & \\
g_1 s_2 \quad &= g'(g'_2 g'_3 \cdots g'_n)^{-1} \in G'.
\end{aligned}$$

Nähdään, että $H'$ generoi ryhmän $G'$. Lisäksi koska $H$ ja $S$ ovat äärellisiä, niin myöskin $H'$ on äärellinen. □

**Lause 2.52.** Olkoot $G$ äärellisesti generoitu ryhmä, $G' \leq G$ ja $[G : G'] < \infty$. Tällöin $\gamma_{G'} \sim \gamma_G$.

*Todistus.* Olkoot $H$ ryhmän $G$ äärellinen symmetrinen generaattori ja $H'$ ryhmän $G'$ generaattori. Merkitään

$$\alpha = max\{l_G^H(h') \in \mathbb{N} \mid h' \in H'\}.$$

Olkoon $g' \in G'$, tällöin $l_{G'}^{H'}(g') \leq \alpha l_G^H(g')$, joten $\gamma_{G'}^{H'}(n) \leq \gamma_G^H(\alpha n)$ aina, kun $n \in \mathbb{N}$.

Olkoon $H'' = S^{-1}HS \cap G'$, missä $S$ on aliryhmän $G'$ sellainen sivuluokkien edustajisto, johon kuuluu alkio $1_G$. Lemman 2.51 nojalla $H''$ on ryhmän $G'$ äärellinen generaattori. Olkoon $g = g_1 g_2 \cdots g_n \in G$, missä $g_i \in H$ aina, kun $1 \leq i \leq n$. Kuten Lemman 2.51 todistuksessa nähdään, että on olemassa sellaiset alkiot $s_1 \in S$, $s_2 \in S$, ... , $s_{n-1} \in S$ ja $s_n \in S$, että

$$g = s_1(s_1^{-1}g_1s_2)(s_2^{-1}g_2s_3)\cdots\ (s_{n-1}^{-1}g_{n-1}s_n)(s_n^{-1}g_n),$$

missä $s_n^{-1}g_n \in H''$ ja $s_i^{-1}g_is_{i+1} \in H''$ aina, kun $1 \leq i \leq n-1$. Näin ollen $G_H^{l\leq n} \subseteq SG_{H''}^{\prime l\leq n}$, jolloin $\gamma_G^H(n) \leq [G : G']\gamma_{G'}^{H''}(n)$ aina, kun $n \in \mathbb{N}$. Ollaan todistettu, että $\gamma_{G'} \sim \gamma_G$. □

**Lause 2.53.** [Alaraja lemma] Olkoon $f : \mathbb{N} \to \mathbb{R}_+$ aidosti kasvava ja $\lim_{n\to\infty} f(n) = \infty$. Jos on olemassa sellainen $m > 1$, että $f^m \preceq f$, niin on olemassa sellainen $\alpha > 0$, että $e^{n^\alpha} \preceq f$.

*Todistus.* Laajennetaan funktion $f$ määritelmää siten, että $f : \mathbb{R}_+ \to \mathbb{R}_+$ ja $f(n) = f(\lfloor n \rfloor)$. Voidaan olettaa, että $f(1) \geq 3$, muussa tapauksessa voidaan funktio kertoa riittävän suurella vakiolla. Voidaan myös olettaa, että $m \geq 2$, koska ketjusta $f \succeq f^m \succeq f^{m^2} \succeq f^{m^3} \succeq ...$ saadaan lopulta, että $f \succeq f^{m'}$, missä $m' \geq 2$.

Määritellään $\pi : \mathbb{R}_+ \to \mathbb{R}_+$ siten, että $\pi(n) = \ln f(n)$. Tällöin $\pi$ on aidosti kasvava, $\pi(1) = \ln(3) > 1$ ja $\lim_{n\to\infty} \pi(n) = \infty$. Koska oletuksen nojalla $f \succeq f^m$, niin on olemassa sellaiset $C > 0$ ja $\alpha > 0$, että $f(n) \geq Cf^m(\alpha n)$ aina, kun $n \in \mathbb{R}_+$. Tästä saadaan, että

$$\pi(n) \geq m\pi(\alpha n) + c,$$

missä $c = \ln(C)$. Jos $\alpha \geq 1$, niin

$$-c \geq m\pi(\alpha n) - \pi(n) \geq m\pi(n) - \pi(n) = (m-1)\pi(n),$$

mikä on ristiriita koska funktio $\pi$ kasvaa rajatta kohti ääretöntä. Toistamalla aiempaa epäyhtälöä saadaan, että

$$\begin{aligned}\pi(n) &\geq m\pi(\alpha n) + c \\ &\geq m(m\pi(\alpha^2 n) + c) + c = m^2\pi(\alpha^2 n) + c(1+m) \\ &\geq m^2(m\pi(\alpha^3 n) + c) + c(1+m) = m^3\pi(\alpha^3 n) + c(1+m+m^2) \\ &. \\ &. \\ &. \\ &\geq m^k\pi(\alpha^k n) + c(1+m+m^2+...+m^{k-1}).\end{aligned}$$

Oletetaan, että $c \geq 0$ ja valitaan $k = \lfloor \log_{\frac{1}{\alpha}}(n) \rfloor$. Tällöin

$$\alpha^k \geq \alpha^{\log_{\frac{1}{\alpha}}(n)} = \frac{1}{n},$$

joten $\pi(\alpha^k n) \geq \pi(1) > 1$. Toisaalta

$$\begin{aligned}m^k &= (\tfrac{1}{\alpha})^{\log_{\frac{1}{\alpha}}(m)\lfloor \log_{\frac{1}{\alpha}}(n) \rfloor} \\ &= (\tfrac{1}{\alpha})^{\log_{\frac{1}{\alpha}}(n)\log_{\frac{1}{\alpha}}(m) + d\log_{\frac{1}{\alpha}}(m)} \\ &= n^v(\tfrac{1}{\alpha})^{vd} \\ &= n^v m^d \\ &\geq An^v,\end{aligned}$$

missä $d = (\lfloor \log_{\frac{1}{\alpha}}(n) \rfloor - \log_{\frac{1}{\alpha}}(n))$, $v = \log_{\frac{1}{\alpha}}(m)$ ja $A = m^{-(1+\ln(\frac{1}{\alpha}))}$. Tällöin saadaan, että $\pi(n) \geq m^k \geq An^v$, missä $A > 0$ ja $v > 0$.

Oletetaan sitten, että $c < 0$. Koska $m \geq 2$, niin

$$1 + m + m^2 + ... + m^{k-1} < m^k,$$

joten

$$\pi(n) > m^k(\pi(\alpha^k n) + c).$$

Valitaan pienin sellainen kokonaisluku $s \geq 1$, että $\pi(s) > 1 - c$. Valitaan $k = \lfloor \log_{\frac{1}{\alpha}}(\frac{n}{s}) \rfloor$, jolloin $\alpha^k n \geq s$ ja edelleen $\pi(\alpha^k n) + c \geq \pi(s) + c \geq 1$. Tällöin

$$\pi(n) > m^k(\pi(\alpha^k n) + c) \geq m^k = (\frac{1}{\alpha})^{vk} \geq (\frac{A}{s^v})n^v,$$

missä $A$ ja $v$ on kuten tapauksessa $c \geq 0$. Kummassakin tapauksessa saadaan tulokseksi, että on olemassa sellainen $B > 0$, että

$$f(n) = e^{\pi(n)} \geq e^{Bn^v} = e^{(\sqrt[v]{B}n)^v}.$$

Näin ollen $f(n) \succeq e^{n^v}$, joten väite on todistettu. □

Muistetaan, että funktio $f : \mathbb{R} \to \mathbb{R}$ on konkaavi välillä $I$, jos epäyhtälö

$$f(tx + (1-t)y) \geq tf(x) + (1-t)f(y)$$

on voimassa aina, kun $x \in I$, $y \in I$ ja $t \in [0,1]$.

**Lause 2.54.** [Jensenin epäyhtälö] Olkoon funktio $f : \mathbb{R} \to \mathbb{R}$ konkaavi välillä $I$. Tällöin

$$f(\frac{\sum_{i=1}^{n} a_i x_i}{\sum_{i=1}^{n} a_i}) \geq \frac{\sum_{i=1}^{n} a_i f(x_i)}{\sum_{i=1}^{n} a_i}$$

missä $a_i > 0$ ja $x_i \in I$ aina, kun $1 \leq i \leq n$ ja $n > 0$.

*Todistus.* Riittää todistaa, että $f(\sum_{i=1}^{n} b_i x_i) \geq \sum_{i=1}^{n} b_i f(x_i)$ aina, kun $\sum_{i=1}^{n} b_i = 1$. Muulloin voidaan asettaa $b_i = \frac{a_i}{\sum_{i=1}^{n} a_i}$. Todistetaan väite induktiolla muuttujan $n$ suhteen.

Induktioaskel: Kun $n = 1$ väite on triviaalisti voimassa.

Induktio-oletus: Väite on voimassa aina, kun $n < k$.

Todistetaan induktioväite. Voidaan olettaa, että $b_k \in (0,1)$, muulloin epäyhtälö on voimassa suoraan induktioaskeleen nojalla. Määritellään $c_i = \frac{b_i}{1-b_k}$ aina, kun $1 \leq i < k$. Tällöin $\sum_{i=1}^{k-1} c_i = 1$. Induktio-oletuksen ja funktion $f$ konkaavisuuden nojalla saadaan, että

$$\begin{aligned} f(\textstyle\sum_{i=1}^{n} b_i x_i) &= f((1-b_k)\sum_{i=1}^{k-1} c_i x_i + b_k x_k) \\ &\geq (1-b_k) f(\textstyle\sum_{i=1}^{k-1} c_i x_i) + b_k f(x_k) \\ &\geq (1-b_k)\textstyle\sum_{i=1}^{k-1} c_i f(x_i) + b_k f(x_k) \\ &= \textstyle\sum_{i=1}^{k-1} b_i f(x_i) + b_k f(x_k) \\ &= \textstyle\sum_{i=1}^{k} b_i f(x_i). \end{aligned}$$

□

Muistetaan, että kahdesti derivoituva funktio $f : \mathbb{R} \to \mathbb{R}$ on konkaavi välillä $I$ jos ja vain jos $f''(x) \leq 0$ aina, kun $x \in I$. Tällöin nähdään helposti, että funktio $f(x) = x^a$ on konkaavi aina, kun $0 < a < 1$:
$f''(x) = (a-1)ax^{a-2} \leq 0$ aina, kun $x \in [0, \infty)$.

Olkoon $f : \mathbb{N} \to \mathbb{R}_+$ aidosti kasvava funktio. Määritellään kuvaus $f^{*k}(n) : \mathbb{N} \to \mathbb{R}_+$ siten, että

$$f^{*k}(n) = \sum_{(n_1, n_2, \ldots, n_k) \in N_{k,n}} f(n_1) f(n_2) \cdots f(n_k),$$

missä

$$N_{k,n} = \{(n_1, n_2, ..., n_k) \in \mathbb{N}^k \mid n_1 + n_2 + ... + n_k \leq n\}.$$

**Lause 2.55.** [Yläraja lemma] Olkoon $f : \mathbb{N} \to \mathbb{R}_+$ sellainen aidosti kasvava funktio, että $\lim_{n\to\infty} f(n) = \infty$. Jos on olemassa sellaiset $k \geq 2$, $C > 0$ ja $0 < \alpha < 1$, että $f(n) \leq Cf^{*k}(\alpha n)$ aina, kun $n \in \mathbb{N}$, niin on olemassa sellainen $\beta < 1$, että $f \preceq e^{n^\beta}$.

*Todistus.* Olkoon $\pi(n) = \ln f(n)$. Todistetaan induktiolla muuttujan $n$ suhteen, että on olemassa sellaiset $A > 0$ ja $0 < v < 1$, että $\pi(n) \leq An^v$ aina, kun $n \in \mathbb{N}$. Oletuksen nojalla on olemassa sellaiset $k \geq 2$, $C > 0$ ja $0 < \alpha < 1$, että $f(n) \leq Cf^{*k}(\alpha n)$. Olkoon $\epsilon > 0$ sellainen, että $0 < v = \log_{\frac{\alpha}{k}} \frac{1-\epsilon}{k} < 1$. Valikoidaan $A > 0$ siten, että

$$\ln C + k\ln\alpha + k\ln n + An^v(1-\epsilon) \leq An^v$$

aina, kun $n \in \mathbb{N}$ ja $\pi(1) \leq A = A1^v$, jolloin induktiolähtökohta on voimassa. Tehdään induktio-oletus: Väite on voimassa jokaisella lukua $n$ aidosti pienemmellä luvulla.

Todistetaan induktioväite. Olkoot luvut $n_i$ sellaisia, että $n_1 + ... + n_k \leq \alpha n < n$, missä $1 \leq i \leq k$. Induktio-oletuksen ja Jensenin epäyhtälön nojalla saadaan, että

$$\begin{aligned}
\ln(f(n_1)\cdots f(n_k)) &= \pi(n_1) + ... + \pi(n_k) \\
&\leq A(n_1^v + ... + n_k^v) \\
&\leq Ak(\textstyle\sum_{i=1}^k \frac{n_i}{k})^v \\
&\leq Ak(\frac{\alpha n}{k})^v \\
&= An^v k(\frac{\alpha}{k})^v \\
&= An^v(1-\epsilon)
\end{aligned}$$

missä toinen epäyhtälö seuraa Jensenin epäyhtälöstä 2.54 asettamalla $f(x) = x^v$ ja $a_i = 1$ aina, kun $1 \leq i \leq k$. Kun $n \neq 1$, niin summassa $Cf^{*k}(\alpha n)$ on selvästi korkeintaan $(\alpha n)^k$ termiä. Tästä saadaan, että

$$\begin{aligned}
\pi(n) &= \ln f(n) \\
&\leq \ln Cf^{*k}(\alpha n) \\
&= \ln C \textstyle\sum_{(n_1,n_2,...,n_k)\in N_{k,\alpha n}} f(n_1)f(n_2)\cdots f(n_k) \\
&\leq \ln C(\alpha n)^k e^{An^v(1-\epsilon)} \\
&= \ln C + \ln(\alpha n)^k + An^v(1-\epsilon) \\
&= \ln C + k\ln\alpha + k\ln n + An^v(1-\epsilon) \\
&\leq An^v.
\end{aligned}$$

Näin ollen väite seuraa samoin, kuten alaraja lemman todistuksessa. □

# 3 Automaattiryhmät ja -puoliryhmät

Mealyn koneet ovat deterministisiä, synkronisoituja tilamuuntimia. Tässä luvussa määritellään automaattiryhmät ja -puoliryhmät, sekä esitetään muutamia perustuloksia. Syvemmin automaattiryhmien teoriaan voidaan tutustua esimerkiksi artikkeleissa [9] ja [22].

**Määritelmä 3.1.** *Mealyn kone* on neljä-tupla $A = (Q, \Sigma, \delta, \sigma)$, missä

$$Q \text{ on äärellinen } \textit{tilajoukko},$$
$$\Sigma \text{ on äärellinen aakkosto},$$
$$\delta : Q \times \Sigma \to Q \text{ on } \textit{siirtymäfunktio} \text{ ja}$$
$$\sigma : Q \times \Sigma \to \Sigma \text{ on } \textit{tulostusfunktio}.$$

Samaistetaan tässä esityksessä käsitteet Mealyn kone ja *automaatti*.

Automaatti voidaan esittää suunnattuna multigraafina, jonka viivat on leimattu seuraavasti: Asetetaan pisteiden joukoksi automaatin tilajoukko ja viivoiksi joukko $\{(q, \delta(q, a)) \mid \text{aina, kun } q \in Q \text{ ja } a \in \Sigma\}$. Viivan $(q, \delta(q, a))$ leimaksi asetetaan $a|\sigma(q, a)$. Sanotaan näin muodostettua multigraafia sitä vastaavan automaatin *graafiesitykseksi*.

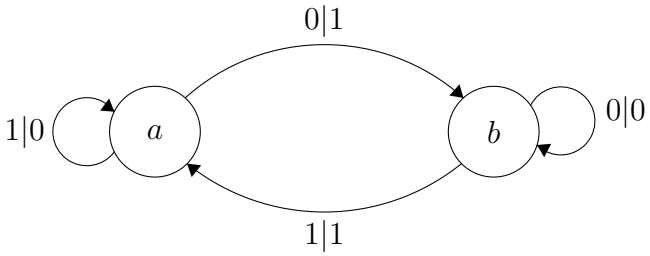
Laajennetaan siirtymä- ja tulostusfunktio luonnollisella tavalla seuraavasti:

$$\delta : Q \times \Sigma^* \to Q$$
$$\delta(q, ut) = \delta(\delta(q, u), t) \text{ ja}$$
$$\sigma : Q \times \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega$$
$$\sigma(q, uv) = \sigma(q, u)\sigma(\delta(q, u), v)$$

aina, kun $q \in Q$, $u \in \Sigma^*$, $t \in \Sigma^*$ ja $v \in \Sigma^* \cup \Sigma^\omega$. Merkitään tästä eteenpäin $\delta_u(q) = \delta(q, u)$ ja $\sigma_q(v) = \sigma(q, v)$, jolloin saadaan kuvaukset $\delta_u : Q \to Q$ ja $\sigma_q : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega$.

**Esimerkki 3.2.** Määritellään $A = (Q, \Sigma, \delta, \sigma)$ siten, että $Q = \{a, b\}$, $\Sigma = \{0, 1\}$ ja siirtymäfunktio sekä tulostusfunktio on määritelty seuraavasti:

$$\begin{aligned} \delta_0(a) &= b, \quad \sigma_a(0) = 1, \\ \delta_1(a) &= a, \quad \sigma_a(1) = 0, \\ \delta_0(b) &= b, \quad \sigma_b(0) = 0, \\ \delta_1(b) &= a, \quad \sigma_b(1) = 1. \end{aligned}$$




Kuva 1: Esimerkin 3.2 automaatin graafiesitys.

Esimerkiksi jos syöte on 10010, niin

$$\begin{aligned}
\sigma_a(10010) &= 0\sigma_{\delta_1(a)}(0010) \\
&= 0\sigma_a(0010) \\
&= 01\sigma_{\delta_0(a)}(010) \\
&= 01\sigma_b(010) \\
&= 010\sigma_{\delta_0(b)}(10) \\
&= 010\sigma_b(10) \\
&= 0101\sigma_{\delta_1(b)}(0) \\
&= 0101\sigma_a(0) \\
&= 01011.
\end{aligned}$$

Automaatin $A$ graafiesitys voidaan nähdä Kuvassa 1. Artikkelissa [10] osoitettiin, että kyseinen automaatti määrittelee ryhmän, joka on vastaesimerkki vahvaan Atiyahin konjektuuriin.

**Määritelmä 3.3.** Mealyn kone $(Q, \Sigma, \delta, \sigma)$ on *kääntyvä*, jos $\sigma_q$ on bijektio aina, kun $q \in Q$.

**Määritelmä 3.4.** Kuvaus $f : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega$ on *automaattinen*, jos on olemassa sellainen Mealyn kone $(Q, \Sigma, \delta, \sigma)$ ja tila $q \in Q$, että $f = \sigma_q$.

**Lemma 3.5.** Kahden Mealyn koneen määrittelemien automaattisten kuvausten yhdistetty kuvaus on automaattinen.

*Todistus.* Olkoot $(Q, \Sigma, \delta, \sigma)$ ja $(Q', \Sigma, \delta', \sigma')$ Mealyn koneita ja olkoot $q \in Q$ ja $q' \in Q'$. Tällöin yhdistetyn kuvauksen $\sigma_{q'} \circ \sigma_q : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega$ määrittelee Mealyn kone $(Q \times Q', \Sigma, \delta'', \sigma'')$, missä

$$\delta''_a((q, q')) = (\delta_a(q), \delta'_{\sigma_q(a)}(q'))$$

ja

$$\sigma''_{(q,q')}(a) = \sigma'_{q'}(\sigma_q(a))$$

aina, kun $a \in \Sigma$. Olkoot $u \in \Sigma^*$ ja $a \in \Sigma$. Tällöin induktio-oletuksen nojalla saadaan seuraavat yhtälöketjut:

$$\begin{aligned}
\delta''_{ua}((q,q')) &= \delta''_a(\delta''_u(q,q')) \\
&= \delta''_a(\delta_u(q), \delta'_{\sigma_q(u)}(q')) \\
&= (\delta_a(\delta_u(q)), \delta'_{\sigma_{\delta_u(q)}(a)}(\delta'_{\sigma_q(u)}(q'))) \\
&= (\delta_{ua}(q), \delta'_{\sigma_q(ua)}(q'))
\end{aligned}$$

$$\begin{aligned}
\sigma''_{(q,q')}(ua) &= \sigma''_{(q,q')}(u)\sigma''_{\delta''_u((q,q'))}(a) \\
&= \sigma'_{q'}(\sigma_q(u))\sigma''_{\delta''_u((q,q'))}(a) \\
&= \sigma'_{q'}(\sigma_q(u))\sigma''_{(\delta_u(q),\delta'_{\sigma_q(u)}(q'))}(a) \\
&= \sigma'_{q'}(\sigma_q(u))\sigma'_{\delta'_{\sigma_q(u)}(q')}(\sigma_{\delta_u(q)}(a)) \\
&= \sigma'_{q'}(\sigma_q(u)\sigma_{\delta_u(q)}(a)) \\
&= \sigma'_{q'}(\sigma_q(ua))
\end{aligned}$$

Ollaan osoitettu, että $\sigma''_{(q,q')} = \sigma_{q'} \circ \sigma_q$. □

Edellisen lemman nojalla nähdään, että joukko

$$\mathcal{S}(\mathcal{A}_\Sigma) = \{f \mid f : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega,\ f \text{ on automaattinen funktio}\}$$

on puoliryhmä operaatiolla kuvausten yhdistäminen varustettuna. Yhdistetylle kuvaukselle $\sigma_{q'} \circ \sigma_q$ käytetään merkintää $\sigma_{qq'}$ ja yleisemmin $\sigma_{q_k} \circ \sigma_{q_{k-1}} \circ \ldots \circ \sigma_{q_1} = \sigma_{q_1 q_2 \cdots q_k}$. Laajennetaan kuvaus $\delta : Q^* \times \Sigma^* \to Q^*$ siten, että $\delta_u(qq') = \delta_{(u)}(q)\delta_{\sigma_q(u)}(q')$ aina, kun $u \in \Sigma^*$, $q \in Q^*$ ja $q' \in Q^*$.

**Lemma 3.6.** Kääntyvän Mealyn koneen määrittelemän automaattisen kuvauksen käänteiskuvaus on automaattinen.

*Todistus.* Olkoon $A = (Q, \Sigma, \delta, \sigma)$ kääntyvä Mealyn kone ja olkoon $q \in Q$. Tällöin automaattisen kuvauksen $\sigma_q$ käänteiskuvauksen määrittelee Mealyn kone $A^{-1} = (Q', \Sigma, \delta', \sigma')$, missä $Q' = \{q^{-1} \mid q \in Q\}$,

$$\begin{aligned}
\delta'_a(q^{-1}) &= \delta_{\sigma_q^{-1}(a)}(q)^{-1} \text{ ja} \\
\sigma'_{q^{-1}}(a) &= \sigma_q^{-1}(a)
\end{aligned}$$

aina, kun $q \in Q$ ja $a \in \Sigma$. Olkoot $u \in \Sigma^*$ ja $a \in \Sigma$ Tällöin induktio-oletuksen

nojalla saadaan seuraavat yhtälöketjut:

$$\begin{aligned}
\delta'_{ua}(q^{-1}) &= \delta'_a(\delta'_u(q^{-1})) \\
&= \delta'_a(\delta_{\sigma_q^{-1}(u)}(q)^{-1}) \\
&= \delta_{\sigma^{-1}_{\delta_{\sigma_q^{-1}(u)}(q)}(a)}(\delta_{\sigma_q^{-1}(u)}(q))^{-1} \\
&= \delta_{\sigma_q^{-1}(ua)}(q)^{-1}
\end{aligned}$$

$$\begin{aligned}
\sigma'_{q^{-1}}(ua) &= \sigma'_{q^{-1}}(u)\sigma'_{\delta'_u(q^{-1})}(a) \\
&= \sigma_q^{-1}(u)\sigma'_{\delta'_u(q^{-1})}(a) \\
&= \sigma_q^{-1}(u)\sigma'_{\delta_{\sigma_q^{-1}(u)}(q)^{-1}}(a) \\
&= \sigma_q^{-1}(u)\sigma^{-1}_{\delta_{\sigma_q^{-1}(u)}(q)}(a) \\
&= \sigma_q^{-1}(ua)
\end{aligned}$$

Ollaan osoitettu, että $\sigma'_{q^{-1}} = \sigma_q^{-1}$. □

Tarkastelemalla kääntyvän Mealyn koneen $A$ graafiesitystä voidaan Mealyn kone $A^{-1}$ konstruoida yksinkertaisesti vaihtamalla jokaisen viivan leiman $a|b$ leimaksi $b|a$.

Lemmojen 3.5 ja 3.6 nojalla nähdään, että joukko

$$\mathcal{G}(\mathcal{A}_\Sigma) = \{f \mid f : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega,\ f \text{ on automaattinen kääntyvä funktio}\}$$

on ryhmä kuvausten yhdistämisen suhteen.

**Määritelmä 3.7.** Olkoon $A = (Q, \Sigma, \delta, \sigma)$ Mealyn kone. Tällöin

$$\mathcal{S}(A) =< \{\sigma_q : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega \mid q \in Q\} >$$

muodostaa puoliryhmän $\mathcal{S}(\mathcal{A}_\Sigma)$ alipuoliryhmän ja sanotaan, että $\mathcal{S}(A)$ on *automaattipuoliryhmä*. Jos lisäksi $A$ on kääntyvä, niin

$$\mathcal{G}(A) =< \{g : \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega \mid g = \sigma_q \text{ tai } g = \sigma_q^{-1} \text{ ja } q \in Q\} >$$

muodostaa ryhmän $\mathcal{G}(\mathcal{A}_\Sigma)$ aliryhmän ja sanotaan, että $\mathcal{G}(A)$ on *automaattiryhmä*.

Määrittelemällä $\varphi : \mathcal{G}(A) \times \Sigma^* \cup \Sigma^\omega \to \Sigma^* \cup \Sigma^\omega$ siten, että $\varphi(g, u) = g(u) = g.u$ nähdään helposti, että $\mathcal{G}(A)$ toimii joukossa $\Sigma^* \cup \Sigma^\omega$: $gh.u = h.(g.u)$ aina, kun $g \in \mathcal{G}(A)$, $h \in \mathcal{G}(A)$, ja $u \in \Sigma^* \cup \Sigma^\omega$. Selvästi toiminta on uskollinen, koska jos $g.u = h.u$ aina, kun $u \in \Sigma^* \cup \Sigma^\omega$, niin $g = h$. Toiminta on itsensä kaltainen, koska aina, kun $g \in \mathcal{G}(A)$, $a \in \Sigma$

ja $u \in \Sigma^* \cup \Sigma^\omega$ on olemassa sellaiset $h \in \mathcal{G}(A)$ ja $b \in \Sigma$, että $g.au = bh.u$. Näin ollen jokainen automaattiryhmä on itsensä kaltainen ryhmä.

Toisaalta jokaisen itsensä kaltaisen ryhmän $G$ generoi *ääretön Mealyn kone*, mikä on määritelty samoin kuin äärellinen versio, mutta tilajoukko on ääretön. Tämä nähdään seuraavasti: Oletetaan, että $G$ toimii joukossa $Y = \Sigma^* \cup \Sigma^\omega$. Otetaan tilajoukoksi $G$ ja aakkostoksi joukko $\Sigma$. Jos $g \in G$, $a \in \Sigma$, $u \in Y$ ja $g.au = b.hu$, niin määritellään $\delta_a(g) = h$ ja $\sigma_g(a) = b$. Koska $G$ on ryhmä, niin toiminnan määritelmän nojalla jokainen $\sigma_g$ on bijektio. Jos lisäksi $G$ on äärellisesti generoitu ja tilajoukko on äärellinen, niin saadaan automaattiryhmä.

**Määritelmä 3.8.** Olkoon $A = (Q, \Sigma, \delta, \sigma)$ automaatti. Määritellään joukko

$$LStab_{\mathcal{G}(A)}(n) = \bigcap_{\substack{w \in \Sigma^* \\ |w| \leq n}} Stab_{\mathcal{G}(A)}(w) = \bigcap_{\substack{w \in \Sigma^* \\ |w| = n}} Stab_{\mathcal{G}(A)}(w)$$

aina, kun $n \in \mathbb{N}$. Sanotaan, että $LStab_{\mathcal{G}(A)}(n)$ on *tason n stabiloija* yli ryhmän $\mathcal{G}(A)$.

**Lause 3.9.** Olkoon $A = (Q, \Sigma, \delta, \sigma)$ automaatti. Tällöin

$$LStab_{\mathcal{G}(A)}(n) \trianglelefteq \mathcal{G}(A) \text{ ja } [\mathcal{G}(A) : LStab_{\mathcal{G}(A)}(n)] < \infty.$$

*Todistus.* Aiemmin ollaan todettu, että $Stab_{\mathcal{G}(A)}(w) \leq \mathcal{G}(A)$ aina, kun $w \in \Sigma^*$, joten Lauseen 2.7 nojalla

$$LStab_{\mathcal{G}(A)}(n) \leq \mathcal{G}(A).$$

Olkoot sitten $\sigma_r \in LStab_{\mathcal{G}(A)}(n)$, $\sigma_q \in \mathcal{G}(A)$ ja $u \in \Sigma^n$. Tällöin

$$\begin{aligned} \sigma_q^{-1} \circ \sigma_r \circ \sigma_q(u) &= \sigma_{q^{-1}}(\sigma_r(\sigma_q(u))) \\ &= \sigma_{q^{-1}}(\sigma_q(u)) \\ &= u. \end{aligned}$$

Saadaan, että $\sigma_q^{-1} \circ \sigma_r \circ \sigma_q \in LStab_{\mathcal{G}(A)}(n)$ joten Lauseen 2.13 nojalla

$$LStab_{\mathcal{G}(A)}(n) \trianglelefteq \mathcal{G}(A).$$

Olkoot $\sigma_q \in \mathcal{G}(A)$ ja $\sigma_r \in \mathcal{G}(A)$. Lemman 2.15 nojalla

$$\sigma_q LStab_{\mathcal{G}(A)}(n) = \sigma_r LStab_{\mathcal{G}(A)}(n)$$

jos ja vain jos $\sigma_r^{-1}\sigma_q \in LStab_{\mathcal{G}(A)}(n)$. Toisaalta $\sigma_r^{-1}\sigma_q \in LStab_{\mathcal{G}(A)}(n)$ jos ja vain jos $\sigma_{r|\Sigma^n} = \sigma_{q|\Sigma^n}$. Näin ollen

$$[\mathcal{G}(A) : LStab_{\mathcal{G}(A)}(n)] \leq |\Sigma^n|!.$$

□

**Lause 3.10.** Olkoon $A = (Q, \Sigma, \delta, \sigma)$ automaatti. Tällöin automaattiryhmä $\mathcal{G}(A)$ on residuaalisesti äärellinen.

*Todistus.* Merkitään

$$\mathcal{G}_n(A) = \{\sigma_{q|\Sigma^n} \mid \sigma_q \in \mathcal{G}(A)\},$$

jolloin $\mathcal{G}_n(A)$ on äärellinen ryhmä. Olkoon $\sigma_q \in \mathcal{G}(A)$, $\sigma_q \neq 1_{\mathcal{G}(A)}$. Tällöin on olemassa sellainen $n \in \mathbb{N}$ ja $w \in \Sigma^n$, että $\sigma_q(w) \neq w$. Määritellään kuvaus

$$\varphi : \mathcal{G}(A) \to \mathcal{G}_n(A)$$

siten, että $\varphi(\sigma_q) = \sigma_{q|\Sigma^n}$, jolloin $\varphi(\sigma_q) \neq 1_{\mathcal{G}_n(A)}$. Automaattiryhmien määritelmästä seuraa suoraan, että $\varphi$ on homomorfismi, joten Määritelmän 2.30 nojalla ryhmä $\mathcal{G}(A)$ on residuaalisesti äärellinen. □

**Lause 3.11.** Olkoon $\mathcal{G}(A)$ automaattiryhmä, missä $A = (Q, \Sigma, \delta, \sigma)$. Tällöin on olemassa isomorfismi $\varphi : \mathcal{G}(A) \to \mathcal{G}(A) \wr \mathcal{G}_1(A)$.

*Todistus.* Olkoot $q \in Q^*$ ja $\Sigma = \{a_1, a_2, ..., a_n\}$. Määritellään kuvaus $\varphi : \mathcal{G}(A) \to \mathcal{G}(A) \wr \mathcal{G}_1(A)$ siten, että

$$\varphi(\sigma_q) \quad = ((g_{a_1}, ..., g_{a_n}), \sigma_{q|\Sigma}),$$

missä $g_{a_i} = \delta_{a_i}(q)$ aina, kun $i \in \{1, ..., n\}$. Selvästi näin määritelty kuvaus on bijektio. Tarkistetaan, että $\varphi$ on homomorfismi. Olkoot $q \in Q^*$, $r \in Q^*$, $h_{a_i} = \delta_{a_i}(r)$ ja $f_{a_i} = \delta_{a_i}(rq)$ aina, kun $i \in \{1, ..., n\}$. Tällöin:

$$\begin{aligned}
\varphi(\sigma_r)\varphi(\sigma_q) &= ((h_{a_1}, ..., h_{a_n}), \sigma_{r|\Sigma})((g_{a_1}, ..., g_{a_n}), \sigma_{q|\Sigma}) \\
&= ((h_{a_1}, ..., h_{a_n})(g_{\sigma_{r|\Sigma}(a_1)}, ..., g_{\sigma_{r|\Sigma}(a_n)}), \sigma_{r|\Sigma}\sigma_{q|\Sigma}) \\
&= ((h_{a_1} g_{\sigma_{r|\Sigma}(a_1)}, ..., h_{a_n} g_{\sigma_{r|\Sigma}(a_n)}), \sigma_{rq|\Sigma}) \\
&= ((\delta_{a_1}(r)\delta_{\sigma_{r|\Sigma}(a_1)}(q), ..., \delta_{a_n}(r)\delta_{\sigma_{r|\Sigma}(a_n)}(q)), \sigma_{rq|\Sigma}) \\
&= ((\delta_{a_1}(rq), ..., \delta_{a_n}(rq)), \sigma_{rq|\Sigma}) \\
&= ((f_{a_1}, ..., f_{a_n}), \sigma_{rq|\Sigma}) \\
&= \varphi(\sigma_r\sigma_q).
\end{aligned}$$

□

Jos sekaannuksen vaaraa ei ole, niin merkitään jatkossa $q = \sigma_q = \varphi(\sigma_q) = ((\delta_{a_1}(q), ..., \delta_{a_n}(q)), \sigma_{q|\Sigma}) = (\delta_{a_1}(q), ..., \delta_{a_n}(q))\sigma_{q|\Sigma}$, jolloin ryhmien $\mathcal{G}(A)$ ja $\mathcal{G}(A) \wr \mathcal{G}_1(A)$ alkiot tulevat samaistetuksi. Lisäksi merkintä $\sigma_{q|\Sigma}$ jätetään pois, jos se on identiteettikuvaus.

Ryhmän $\mathcal{G}(A) \wr \mathcal{G}_1(A)$ alkiot toimivat joukossa $\Sigma^\omega$ säännöllä $(\delta_{a_1}(q), ..., \delta_{a_n}(q))\sigma_{q|\Sigma}.a_i u = \sigma_q(a_i)\sigma_{\delta_{a_i}(q)}(u)$ missä $u \in \Sigma^\omega$.

**Esimerkki 3.12.** Jatketaan Esimerkkiä 3.2 tarkastelemalla ryhmän $\mathcal{G}(A) \wr \mathcal{G}_1(A)$ alkioita. Kyseisen Mealyn koneen määritelmästä nähdään, että

$$\begin{array}{ll} a & = (\delta_0(a), \delta_1(a))\sigma_{a|_\Sigma} \quad = (b,a)\tau \text{ ja} \\ b & = (\delta_0(b), \delta_1(b))\sigma_{b|_\Sigma} \quad = (b,a) \end{array}$$

missä $\tau = (01)$. Nähdään, että $((b,a)\tau).10010 = 0\sigma_{\delta_1(a)}(0010) = 01011$. Merkitään $(b,a)\tau = (g_0, g_1)\tau$. Tällöin ryhmän $\mathcal{G}(A) \wr \mathcal{G}_1(A)$ kertolaskun määritelmän nojalla nähdään, että

$$\begin{aligned} a^2 &= (g_0, g_1)\tau(g_0, g_1)\tau \\ &= (g_0 g_{\tau(0)}, g_1 g_{\tau(1)})\tau^2 \\ &= (g_0 g_1, g_1 g_0) \\ &= (ba, ab). \end{aligned}$$

**Lause 3.13.** Olkoon $\mathcal{G}(A)$ automaattiryhmä. Määritellään jokaista alkiota $u \in \Sigma^*$ kohti kuvaus

$$\varsigma_u : LStab_{\mathcal{G}(A)}(|u|) \to \mathcal{G}(A)$$

siten, että

$$\varsigma_{a_i}((q_{a_1}, q_{a_2}, ..., q_{a_{|\Sigma|}})) = q_{a_i}$$

aina, kun $i \in \{1, 2, ...., |\Sigma|\}$ ja yleisemmin

$$\varsigma_u = \varsigma_{a_{i_n}} \circ \varsigma_{a_{i_{n-1}}} \circ ... \circ \varsigma_{a_{i_1}},$$

aina, kun $u = a_{i_1} \cdots a_{i_n}$ ja $a_{i_j} \in \Sigma$ ja $n \geq 1$. Tällöin $\varsigma_u$ on homomorfismi.

*Todistus.* Väite seuraa helposti, sillä $\varsigma_a(LStab_{\mathcal{G}(A)}(n+1)) \subseteq LStab_{\mathcal{G}(A)}(n)$ aina, kun $a \in \Sigma$. Lisäksi

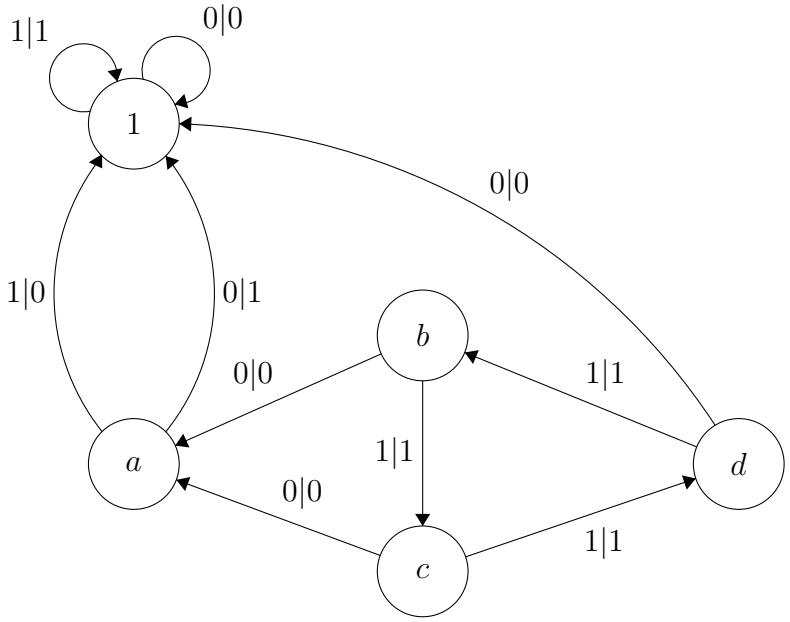
$$\begin{aligned} \varsigma_{a_i}((q_{a_1}, q_{a_2}, ..., q_{a_n}))\varsigma_{a_i}((r_{a_1}, r_{a_2}, ..., r_{a_n})) &= q_{a_i} r_{a_i} \\ &= \varsigma_{a_i}((q_{a_1} r_{a_1}, q_{a_2} r_{a_2}, ..., q_{a_n} r_{a_n})), \end{aligned}$$

joten kuvaus $\varsigma_{a_i}$ on homomorfismi. Induktiivisesti väite seuraa kuvaukselle $\varsigma_u$ aina, kun $u \in \Sigma^n$. □

# 4 Ryhmäteoreettisia tuloksia

Kuvassa 2 esitetään automaatti, joka generoi Grigorchukin ryhmän $G_{rig}$. Rostislav Grigorchuk konstruoi kyseisen ryhmän vastaesimerkkinä Burnsiden ongelmaan artikkelissa [8] vuonna 1980. Kolme vuotta myöhemmin Yurii Merzlyakov näytti artikkelissa [19], että Grigorchukin ryhmä on hyvin saman kaltainen vuonna 1972 konstruoidun Aleshinin ryhmän kanssa [1]. Vuoden 1983

artikkelissa [13], Grigorchuk näytti, että ryhmällä $G_{rig}$ on keskitason kasvu ja näin ollen se on ensimmäinen ratkaisu Milnorin ongelmaan. Tästä lähtien kyseistä ryhmää on tutkittu paljon ja on osoittautunut, että sillä on monia muitakin mielenkiintoisia ominaisuuksia. Aliluvussa 4.1 osoitetaan, että $G_{rig}$ on ääretön 2-ryhmä. Sitä pidetäänkin monissa lähteissä yksinkertaisimpana vastaesimerkkinä Burnsiden ongelmaan. Aliluvussa 4.2 osoitetaan, että ryhmällä $G_{rig}$ on keskitason kasvu.




Kuva 2: Grigorchukin ryhmän generoivan automaatin graafiesitys.

## 4.1 Burnsiden ongelma

Tässä aliluvussa esitetään ratkaisu Burnsiden ongelmaan, joka kysyy onko olemassa ääretöntä ryhmää, joka on äärellisesti generoitu ja jonka jokainen alkio on äärellinen.

**Lause 4.1.** Grigorchukin ryhmä $G_{rig}$ on ääretön 2-ryhmä [8].

*Todistus.* Todistetaan ensin, että Grigorchukin ryhmä on ääretön osoittamalla, että kuvaus $\varsigma_0 : LStab_{G_{rig}}(1) \to G_{rig}$ on surjektiivinen. Tämä todistaa väitteen, koska $a \notin LStab_{G_{rig}}(1)$, joten $LStab_{G_{rig}}(1)$ on Grigorchukin ryhmän

aito aliryhmä. Merkitään $\tau = (01)$, jolloin helposti nähdään, että Grigorchukin ryhmän määrittelee seuraava kehärekursio:

$$\begin{aligned} 1 &= (1,1) \\ a &= (1,1)\tau \\ b &= (a,c) \\ c &= (a,d) \\ d &= (1,b) \end{aligned}$$

Tästä saadaan laskettua, että:

$$\begin{aligned} aba &= (1,1)\tau((a,c)(1,1)\tau) &&= (1,1)\tau(a,c)\tau &&= (c,a) \\ aca &= (1,1)\tau((a,d)(1,1)\tau) &&= (1,1)\tau(a,d)\tau &&= (d,a) \\ ada &= (1,1)\tau((1,b)(1,1)\tau) &&= (1,1)\tau(1,b)\tau &&= (b,1) \end{aligned}$$

Saadaan, että $\{c, d, aba, aca, ada\} \subseteq LStab_{G_{rig}}(1)$, ja nähdään, että:

$$\begin{aligned} \varsigma_0(d) &= 1 & \varsigma_0(aba) &= c \\ \varsigma_0(c) &= a & \varsigma_0(aca) &= d \\ \varsigma_0(ada) &= b. \end{aligned}$$

Näin ollen $\varsigma_0 : LStab_{G_{rig}}(1) \to G_{rig}$ on surjektio. Todistetaan sitten, että $G_{rig}$ on 2-ryhmä. Grigorchukin ryhmän määrittelemästä kehärekursiosta nähdään heti, että $a^2 = 1$, mistä seuraa:

$$b^2 = (1, c^2) \quad c^2 = (1, d^2) \quad d^2 = (1, b^2)$$

Koska $\{b^2, c^2, d^2\} \subseteq LStab_{G_{rig}}(1)$, niin induktiolla yllä olevista yhtälöistä seuraa, että $\{b^2, c^2, d^2\} \subseteq LStab_{G_{rig}}(n)$ aina, kun $n \in \mathbb{N}$. Tästä seuraa, että $b^2 = c^2 = d^2 = 1$. Lisäksi

$$\begin{aligned} cd &= (a, db) & dc &= (a, bd) \\ db &= (a, bc) & bd &= (a, cb) \\ bc &= (1, cd) & cb &= (1, dc), \end{aligned}$$

mistä nähdään, että alkiot $\{b, c, d\}$ toteuttavat saman kehärekursion, kuin alkiot $\{cd, db, bc\}$ ja $\{dc, bd, cb\}$. Koska kehärekursio määrittelee sitä vastaavan automaattiryhmän ryhmänalkiot yksikäsitteisesti, niin

$$\begin{aligned} cd &= b & &= dc \\ db &= c & &= bd \\ bc &= d & &= cb \end{aligned}$$

Kokonaisuudessaan siis:

| $\circ$ | 1 | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| 1 | 1 | $b$ | $c$ | $d$ |
| $b$ | $b$ | 1 | $d$ | $c$ |
| $c$ | $c$ | $d$ | 1 | $b$ |
| $d$ | $d$ | $c$ | $b$ | 1 |

Mistä nähdään, että $< b, c, d >$ on isomorfinen Kleinin neliryhmän kanssa. Tästä seuraa, että jos $g \in G_{rig}$, niin $g = e_1 a e_2 a \cdots e_{k-1} a e_k$, missä $e_i \in \{b, c, d\}$ aina, kun $1 < i < k$ ja $e_j \in \{1, b, c, d\}$, kun $j = 1$ tai $j = k$.

Todistetaan sitten induktiolla alkion pituuden suhteen, että jokaista $g \in G_{rig}$ kohti on olemassa sellainen $n \in \mathbb{N}$, että $g^{2^n} = 1$.

Induktioaskel: $a^2 = b^2 = c^2 = d^2 = 1$.

Induktio-oletus: Väite on voimassa aina, kun $|g| < k$.

Todistetaan induktioväite. Olkoon $g \in G_{rig}$ ja $|g| = k$, jolloin $g = e_1 a e_2 a \cdots a e_m$. Jos $e_1 = e_m = 1$, niin $aga = e_2 a \cdots a e_{m-1}$ ja näin ollen on olemassa sellainen $n$, että $(aga)^{2^n} = 1$, koska $|aga| < k$. Näin ollen konjugoimalla $aga$ alkiolla $a$ saadaan, että $g^{2^n} = 1$. Samoin, jos $e_1 \in \{b, c, d\}$ ja $e_m \in \{b, c, d\}$, niin on olemassa sellainen $f \in \{b, c, d\}$, että $|fgf| < k$, jolloin on olemassa sellainen $n$, että $(fgf)^{2^n} = 1$. Tällöin jälleen konjugoinnin nojalla $g^{2^n} = 1$.

Olkoon sitten

$$g = a e_1 a \cdots a e_{\frac{k}{2}}.$$

Tarvittaessa konjugoidaan jollakin alkiolla joukosta $\{b, c, d\}$. Jos $\frac{k}{2}$ on parillinen, niin saadaan:

$$g = (a e_1 a) e_2 (a e_3 a) e_4 \cdots (a e_{\frac{k}{2}-1} a) e_{\frac{k}{2}} = (g_0, g_1),$$

missä $a e_i a \in \{b, c, d\} \times \{a, 1\}$ ja $e_j \in \{a, 1\} \times \{b, c, d\}$, joten $|g_0| \leq \frac{k}{2}$ ja $|g_1| \leq \frac{k}{2}$. Induktio-oletuksen nojalla, on olemassa sellainen $n \in \mathbb{N}$, että $g_0^{2^n} = 1 = g_1^{2^n}$, joten myös $g^{2^n} = 1$. Jos $\frac{k}{2}$ on pariton, niin

$$g^2 = (a e_1 a) e_2 \cdots (a e_{\frac{k}{2}-2} a) e_{\frac{k}{2}-1} (a e_{\frac{k}{2}} a) e_1 \cdots (a e_{\frac{k}{2}-1} a) e_{\frac{k}{2}} = (h_0, h_1),$$

missä samoin perusteluin kuten edellä nähdään, että $|h_0| \leq k$ ja $|h_1| \leq k$.

Jos on olemassa sellainen $i \in \{1, 2, ..., \frac{k}{2}\}$, että $e_i = d = (1, b)$, niin $a e_i a = (b, 1)$, joten $|h_0| \leq k-1$ ja $|h_1| \leq k-1$. Näin ollen induktio-oletuksen nojalla on olemassa sellainen $n \in \mathbb{N}$, että $h_0^{2^n} = 1 = h_1^{2^n}$, joten $g^{2^{n+1}} = 1$.

Jos on olemassa sellainen $i \in \{1, 2, ..., \frac{k}{2}\}$, että $e_i = c = (a, d)$, niin $a e_i a = (d, a)$, mutta tällöin, joko $|h_0| \leq k-1$ ja $|h_1| \leq k-1$ tai väite palautuu edelliseen tapaukseen. Molemmissa tapauksissa on olemassa sellainen $n \in \mathbb{N}$, että $g^{2^n} = 1$.

Jos $e_i = b$ aina, kun $i \in \{1, 2, ..., \frac{k}{2}\}$, niin $g = abab \cdots ab$. Lasketaan mikä on alkion $ab$ kertaluku:

$$\begin{array}{lll} (ab)^{16} & = ((a,c)\tau(a,c)\tau)^8 & = ((a,c)(c,a))^8 \quad = (ac,ca)^8 \\ (ac)^8 & = ((a,d)\tau(a,d)\tau)^4 & = ((a,d)(d,a))^4 \quad = (ad,da)^4 \\ (ad)^4 & = ((1,b)\tau(1,b)\tau)^2 & = ((1,b)(b,1))^2 \quad = (b,b)^2. \end{array}$$

Koska konjugaateilla on sama kertaluku ja $b^2 = 1$, niin $(ab)^{16} = 1$. Näin ollen Lagrangen lauseen nojalla alkion $g$ kertaluku jakaa luvun 16, joten on olemassa sellainen $n \in \mathbb{N}$, että $g^{2^n} = 1$. □

## 4.2 Milnorin ongelma

Tässä aliluvussa osoitetaan ensin, että Grigorchukin ryhmän kasvufunktio on ylipolynomiaalinen. Tämän jälkeen osoitetaan, että kyseinen kasvufunktio on myös alieksponentiaalinen, jolloin Grigorchukin ryhmällä on keskitason kasvu.

**Määritelmä 4.2.** Olkoot $G_1$ ja $G_2$ ryhmiä. Jos on olemassa sellaiset

$$H_1 \leq G_1 \text{ ja } H_2 \leq G_2,$$

että

$$H_1 \cong H_2,\ [G_1 : H_1] < \infty \text{ ja } [G_2 : H_2] < \infty$$

niin sanotaan, että $G_1$ ja $G_2$ ovat *yhteismitallisia*. Jos $G_1$ ja $G_2$ ovat yhteismitallisia, niin merkitään $G_1 \approx G_2$.

**Määritelmä 4.3.** Olkoon $G$ ääretön ryhmä. Tällöin $G$ on *multilateraalinen* jos on olemassa sellainen $m > 1$, että $G \approx G^m$.

**Lemma 4.4.** Olkoon $G$ multilateraalinen ryhmä. Tällöin ryhmän $G$ kasvufunktio on ylipolynomiaalinen.

*Todistus.* Multilateraalisuudesta seuraa, että on olemassa sellaiset $H \leq G$ ja $H' \leq G^m$, että $[G : H] < \infty$, $[G^m : H'] < \infty$ ja $H \cong H'$. Näin ollen Lauseen 2.52 nojalla

$$\gamma_G \sim \gamma_H \sim \gamma_{H'} \sim \gamma_{G^m}.$$

Tällöin $\gamma_{G^m} \preceq \gamma_G$, joten Lemman 2.53 nojalla $G$ on ylipolynomiaalinen. □

Olkoon $B = N_{G_{rig}}(b) =< g^{-1}bg | g \in G_{rig} >$.

**Lemma 4.5.** Olkoon $B$ kuten edellä. Tällöin $[G_{rig} : B] \leq 8$.

*Todistus.* Lauseen 4.1 todistuksessa nähtiin, että $< b, c, d >$ on isomorfinen Kleinin neliryhmän kanssa, joten

$$< b, c, d >=< b, d >$$

ja näin ollen $G_{rig} =< a, b, d >$. Saman lauseen todistuksessa nähtiin, että $a^2 = d^2 = (ad)^4 = 1$. Näin ollen Esimerkin 2.29 nojalla $< a, d > \leq D_4$. Lemman 2.15 nojalla $[G_{rig} : B] \leq |D_4| \leq 8$. □

Merkitään $H = LStab_{G_{rig}}(1)$ ja määritellään kuvaus $\phi : H \to G_{rig}^2$ siten, että $\phi(h) = (\varsigma_0(h), \varsigma_1(h))$, missä $\varsigma_i$ on kuten Lauseessa 3.13 ja $h \in H$.

**Lemma 4.6.** Joukko $B^2$ on ryhmän $\phi(H)$ aliryhmä.

*Todistus.* Lauseen 4.1 nojalla $< b, c, d, aba, aca, ada > \leq H$ ja:

$$\begin{array}{llllll} \phi(b) & = (a, c) & \text{ja} & \phi(aba) & = (c, a) \\ \phi(c) & = (a, d) & \text{ja} & \phi(aca) & = (d, a) \\ \phi(d) & = (1, b) & \text{ja} & \phi(ada) & = (b, 1). \end{array}$$

Olkoon $g \in H$ ja $\phi(g) = (g_0, g_1)$. Tällöin

$$\begin{aligned} \phi(g^{-1}dg) &= \phi(g^{-1})\phi(d)\phi(g) \\ &= (g_0^{-1}, g_1^{-1})(1, b)(g_0, g_1) \\ &= (1, g_1^{-1}bg_1) \end{aligned}$$

ja

$$\begin{aligned} \phi(g^{-1}adag) &= \phi(g^{-1})\phi(ada)\phi(g) \\ &= (g_0^{-1}, g_1^{-1})(b, 1)(g_0, g_1) \\ &= (g_0^{-1}bg_0, 1). \end{aligned}$$

Koska $\varsigma_0(H) = G = \varsigma_1(H)$, niin yllä $g_0$ ja $g_1$ voivat saada kaikki mahdolliset arvot joukosta $G_{rig}$. Näin ollen $\{1\} \times B \leq \phi(H)$ ja $B \times \{1\} \leq \phi(H)$, joten myös $B^2 \leq \phi(H)$. □

**Lause 4.7.** Grigorchukin ryhmä on multilateraalinen.

*Todistus.* Lauseen 3.9 nojalla $[G_{rig} : H]$ on äärellinen. Lemmojen 4.5 ja 4.6 nojalla

$$[G_{rig}^2 : \phi(H)] \leq [G_{rig}^2 : B^2] = [G_{rig} : B]^2 \leq 8^2 = 64.$$

Koska lisäksi $H \leq G_{rig}$, $\phi(H) \leq G_{rig}^2$ ja $H \cong \phi(H)$, niin $G_{rig}$ ja $G_{rig}^2$ ovat yhteismitallisia. Lauseen 4.1 nojalla $G_{rig}$ on ääretön ryhmä, joten Grigorchukin ryhmä on multilateraalinen. □

**Seuraus 4.8.** Grigorchukin ryhmällä on ylipolynomiaalinen kasvu.

Lauseen 4.1 todistuksessa nähtiin, että jokainen ryhmän $G_{rig}$ alkio voidaan esittää jossakin seuraavassa muodossa:

$$\begin{array}{ll} (i) & ae_1ae_2a\cdots e_{n-1}ae_na \\ (ii) & ae_1ae_2a\cdots e_{n-1}ae_n \\ (iii) & e_1ae_2a\cdots e_{n-1}ae_na \\ (iv) & e_1ae_2a\cdots e_{n-1}ae_n, \end{array}$$

missä $n \in \mathbb{N}$ ja $e_i \in \{b, c, d\}$ aina, kun $1 \leq i \leq n$. Kutsutaan näitä muotoja ryhmän alkion *redusoiduiksi ryhmäsanoiksi*. Määritellään kaksi uudelleenkirjoitussääntöä $\Phi_i : Q^* \to Q^*$ siten, että

$$\begin{array}{llll} \Phi_0(1) & = 1, & \Phi_1(1) & = 1, \\ \Phi_0(a) & = 1, & \Phi_1(a) & = 1, \\ \Phi_0(b) & = a, & \Phi_1(b) & = c, \\ \Phi_0(c) & = a, & \Phi_1(c) & = d, \\ \Phi_0(d) & = 1, & \Phi_1(d) & = b, \end{array}$$

$$\Phi_0 : \begin{cases} u1 \to \Phi_0(u)1, \\ ua \to \Phi_0(u)1, \\ ub \to \Phi_0(u)a, uc \to \Phi_0(u)a, ud \to \Phi_0(u)1 \text{ jos } |u|_a \text{ on parillinen}, \\ ub \to \Phi_0(u)c, uc \to \Phi_0(u)d, ud \to \Phi_0(u)b \text{ jos } |u|_a \text{ on pariton}, \end{cases}$$

ja

$$\Phi_1 : \begin{cases} u1 \to \Phi_1(u)1, \\ ua \to \Phi_1(u)1, \\ ub \to \Phi_1(u)a, uc \to \Phi_1(u)a, ud \to \Phi_1(u)1 \text{ jos } |u|_a \text{ on pariton}, \\ ub \to \Phi_1(u)c, uc \to \Phi_1(u)d, ud \to \Phi_1(u)b \text{ jos } |u|_a \text{ on parillinen} \end{cases}$$

aina, kun $u \in Q^*$.

Määritelmästä seuraa, että $\Phi_i(ua) = \Phi_i(u)\Phi_i(a)$, jos $|u|_a$ on parillinen ja $\Phi_i(ua) = \Phi_i(u)\Phi_j(a)$, jos $|u|_a$ on pariton aina, kun $i \in \{0, 1\}$, $j \in \{0, 1\}$ ja $i \neq j$.

**Lemma 4.9.** Olkoon $g \in G_{rig}$. Tällöin sen jokainen pituudeltaan pienin redusoitu ryhmäsana on tyyppiä $(i)$, $(iv)$ tai kumpaa vain tyyppiä $(ii)$ tai $(iii)$.

*Todistus.* Olkoon $g \in G_{rig}$. Jos $\sigma_g(0) = 1$, niin helposti nähdään, että jokaisessa sitä vastaavassa ryhmäsanassa on oltava pariton määrä $a$ kirjaimia. Vastaavasti jos $\sigma_g(0) = 0$, niin nähdään, että jokaisessa sitä vastaavassa ryhmäsanassa on oltava parillinen määrä $a$ kirjaimia.

Olkoon $g \in G_{rig}$ sellainen, että $\sigma_g(0) = 0$. Olkoot $w$ ja $w'$ sellaisia alkion $g$ redusoituja ryhmäsanoja, että $|w| = |w'| = l(g)$. Tällöin on olemassa sellaiset $r \in \mathbb{N}$ ja $s \in \mathbb{N}$, että $|w|_a = 2r$ ja $|w'|_a = 2s$. Olkoon $w$ tyyppiä $(i)$. Tällöin $|w| = 2|w|_a - 1 = 4r - 1$. Jos $w'$ on tyyppiä $(iv)$, niin $|w'| = 2|w'|_a + 1 = 4s + 1$. Toisaalta yhtälöllä $4r - 1 = 4s + 1$ ei ole yhtään ratkaisua kokonaislukujen joukossa, mikä johtaa ristiriitaan, joten $w'$ ei voi olla tyyppiä $(iv)$. Jos $w'$ on tyyppiä $(ii)$ tai $(iii)$, niin $|w'| = 2|w'|_a = 4s$. Tämä johtaa myös ristiriitaan, sillä yhtälöllä $4r - 1 = 4s$ ei ole yhtään ratkaisua kokonaislukujen joukossa. Muut tapaukset käsitellään vastaavasti, joten väite seuraa. □

Seuraavassa oletetaan ryhmän $G_{rig}$ generaattoriksi $\{a, b, c, d\}$.

**Lemma 4.10.** Olkoot $g \in G_{rig}$, $g = (g_0, g_1)\sigma$ ja $w$ alkion $g$ mikä tahansa ryhmäsana. Tällöin $\Phi_i(w) = g_i$ aina, kun $i \in \{0, 1\}$. Jos lisäksi $w$ on alkion $g$ pituudeltaan pienin redusoitu ryhmäsana, niin

$$\begin{aligned} l(g_i) &\leq \tfrac{1}{2}(l(g) - 1), \text{ jos w on tyyppiä (i)}, \\ l(g_i) &\leq \tfrac{1}{2} l(g), \text{ jos w on tyyppiä (ii) tai (iii)}, \\ l(g_i) &\leq \tfrac{1}{2}(l(g) + 1), \text{ jos w on tyyppiä (iv)} \end{aligned}$$

aina, kun $i \in \{0, 1\}$.

*Todistus.* Todistetaan väite induktiolla alkion $g$ ryhmäsanan $w$ pituuden $|w|$ suhteen. Oletetaan ensin, että $|w| = 1$. Tällöin $w$ on joko tyyppiä $(i)$ tai $(iv)$. Muistetaan, että kehärekursio

$$\begin{aligned} 1 &= (1, 1) \\ a &= (1, 1)\tau \\ b &= (a, c) \\ c &= (a, d) \\ d &= (1, b) \end{aligned}$$

määrittelee ryhmän $G_{rig}$. Toisaalta

$$\begin{aligned} \Phi_0(1) &= 1, & \Phi_1(1) &= 1, \\ \Phi_0(a) &= 1, & \Phi_1(a) &= 1, \\ \Phi_0(b) &= a, & \Phi_1(b) &= c, \\ \Phi_0(c) &= a, & \Phi_1(c) &= d, \\ \Phi_0(d) &= 1, & \Phi_1(d) &= b. \end{aligned}$$

Nähdään, että tällöin $\Phi_i(w) = g_i$ aina, kun $i \in \{0, 1\}$ ja pituutta koskeva väite on voimassa, joten induktiolähtökohta on kunnossa. Oletetaan sitten, että väite on voimassa aina, kun $|w| < n$.

Olkoon sitten $w$ sellainen alkion $g \in G_{rig}$ ryhmäsana, että $|w| = n$. Tällöin on olemassa sellaiset alkiot $h \in G_{rig}$ ja $e \in \{a, b, c, d\}$, että $g = he$ ja $w = ue$, missä $u$ on alkion $h$ ryhmäsana ja $|u| = n - 1$. Merkitään $h = (h_0, h_1)\tau$ ja $e = (e_0, e_1)\delta$. Jos $\tau = (01)$, niin välttämättä $|u|_a$ on pariton. Tällöin $\Phi_i(ue) = \Phi_i(u)\Phi_j(e)$, missä $i \neq j$ ja $he = (h_0e_1, h_1e_0)\tau\delta$. Toisaalta jos $\tau$ on identiteettikuvaus, niin välttämättä $|u|_a$ on parillinen. Tällöin $\Phi_i(ue) = \Phi_i(u)\Phi_i(e)$ ja $he = (h_0e_0, h_1e_1)\delta$. Näin ollen induktio-oletuksen nojalla $\Phi_i(g) = g_i$ aina, kun $i \in \{0, 1\}$.

Käytetään edelleen samoja merkintöjä. Oletetaan nyt lisäksi, että $w = ue$ on alkion $g$ pituudeltaan pienin ryhmäsana. Jos $u$ on tyyppiä $(i)$, niin $ue$ on tyyppiä $(ii)$. Tällöin

$$l(h_ie_j) \leq \frac{1}{2}(l(h) - 1) + 1 = \frac{1}{2}(l(h) + 1) = \frac{1}{2}l(he),$$

missä $i = j$ tai $i \neq j$ riippuen kirjainten $a$ lukumäärästä. Jos $u$ on tyyppiä $(ii)$, niin $ue$ on tyyppiä $(i)$, joten $e = a$. Tällöin

$$l(h_ie_j) = l(h_i) \leq \frac{1}{2}l(h) = \frac{1}{2}(l(he) - 1),$$

missä $i = j$ tai $i \neq j$ riippuen kirjainten $a$ lukumäärästä. Tapaukset, missä $u$ on tyyppiä $(iii)$ tai $(iv)$ käsitellään samoin. □

Merkitään lyhennetysti $H_3 = LStab_{G_{rig}}(3)$.

**Lemma 4.11.** Olkoot $h \in H_3$ ja $\varsigma_u(h) = h_u$. Tällöin

$$l(h_{000}) + l(h_{001}) + ... + l(h_{111}) \leq \frac{5}{6}l(h) + 8.$$

*Todistus.* Olkoot $h \in H_3$ ja sana $w$ alkion $h$ mikä tahansa pituudeltaan pienin redusoitu ryhmäsana. Käyttämällä uudelleenkirjoitussääntöjä $\Phi_0$ ja $\Phi_1$ saadaan sanat $w_0$ ja $w_1$. Toistamalla uudelleenkirjoitussääntöä sanoihin $w_0$ ja $w_1$ saadaan sanat $w_{00}$, $w_{01}$, $w_{10}$ ja $w_{11}$. Toistamalla uudelleenkirjoitussääntöä vielä viimeisen kerran juuri saatuihin sanoihin saadaan sanat $w_{000}$, $w_{001}$, ... , $w_{110}$ ja $w_{111}$. Näin saadut sanat ovat Lemman 4.10 nojalla alkioiden $h_0$, $h_1$, $h_{01}$, ... , $h_{110}$ ja $h_{111}$ ryhmäsanoja, mutta ei välttämättä redusoituja. Näin ollen

$$\begin{aligned} l(h_i) &\leq |w_i|, \\ l(h_{ij}) &\leq |w_{ij}|, \\ l(h_{ijk}) &\leq |w_{ijk}| \end{aligned}$$

aina, kun $i \in \{0, 1\}$, $j \in \{0, 1\}$ ja $k \in \{0, 1\}$. Lisäksi Lemman 4.10 seurauksena saadaan, että

$$\begin{aligned} l(h_0) + l(h_1) &\leq l(h) + 1, \\ l(h_{00}) + ... + l(h_{11}) &\leq l(h_0) + l(h_1) + 2 \text{ ja} \\ l(h_{000}) + ... + l(h_{111}) &\leq l(h_{00}) + ... + l(h_{11}) + 4. \end{aligned}$$

Otetaan käyttöön merkinnät

$$w' = w_0 w_1, w'' = w_{00} \cdots w_{11} \text{ ja } w''' = w_{000} w_{001} \cdots w_{111},$$

jolloin saadaan, että

$$l(h_{000}) + ... + l(h_{111}) \leq min\{|w'''|, |w''| + 4, |w'| + 6\}.$$

Uudelleenkirjoitussäännön nojalla sanan pituus lyhenee, jos siihen kuuluu kirjain $d$. Näin ollen

$$|w'| \leq |w| + 1 - |w|_d.$$

Toisaalta kirjain $c$ uudelleenkirjoitetaan kirjaimeksi $d$, joten

$$|w''| \leq |w'| + 2 - |w'|_d \leq |w| + 3 - |w|_c.$$

Edelleen kirjain $b$ uudelleenkirjoitetaan kirjaimeksi $c$, joten

$$|w'''| \leq |w''| + 4 - |w''|_d \leq |w'| + 6 - |w'|_c \leq |w| + 7 - |w|_b.$$

Koska $w$ on redusoitu ryhmäsana, niin $|w|_b + |w|_c + |w|_d \geq \frac{1}{2}(|w| - 1)$, joten on olemassa ainakin yksi sellainen kirjain $e \in \{b, c, d\}$, että $w_e > \frac{|w|}{6} - 1$. Näin ollen saadaan, että

$$\begin{aligned} l(h_{000}) + ... + l(h_{111}) &\leq min\{|w'''|, |w''| + 4, |w'| + 6\} \\ &\leq |w| + 7 - max_{e \in \{b,c,d\}} |w|_e \\ &< |w| + 7 - (\tfrac{|w|}{6} - 1) \\ &= \tfrac{5}{6} l(h) + 8. \end{aligned}$$

□

**Lause 4.12.** Ryhmällä $G_{rig}$ on alieksponentiaalinen kasvu.

*Todistus.* Jokainen alkio $g \in G_{rig}$ voidaan kirjoittaa muodossa $g = uh$, missä $h \in H_3$ ja $u$ on tekijäryhmän $G_{rig}/H_3$ edustaja. Lauseen 3.9 nojalla on olemassa sellainen $C > 0$, että $[G_{rig} : H_3] \leq C$. Olkoon $\alpha$ edustajiston pisimmän alkion pituus. Koska $g = uh$, niin $h = u^{-1}g$, joten $l(h) \leq l(g) + \alpha$ aina, kun $h \in H_3$. Näin ollen Lemman 4.11 nojalla

$$\begin{aligned} \textstyle\sum_{ijk} l(h_{ijk}) &\leq \tfrac{5}{6} l(h) + 8 \\ &\leq \tfrac{5}{6}(l(g) + \alpha) + 8 \\ &< \tfrac{5}{6} l(g) + \beta, \end{aligned}$$

missä $\beta > \frac{5}{6}\alpha + 8$ ja $\varsigma_u(h) = h_u$. Kuvausten $\varsigma_{ijk} : H_3 \to G_{rig}$ määritelmistä seuraa helposti, että kuvaus $\chi : H_3 \to G_{rig}^8$ on injektiivinen homomorfismi, missä $\chi(h) = (\varsigma_{000}(h), ..., \varsigma_{111}(h))$. Näin ollen

$$\gamma(n) \leq C\gamma^{*8}(\frac{5}{6} + \beta).$$

Olkoon $m = n + \delta$ sellainen, että $\frac{5}{6}n + \beta < \frac{5}{6}m$. Tällöin

$$\begin{aligned} \gamma(m) &= \gamma(n + \delta) \\ &\leq 4^\delta \gamma(n). \end{aligned}$$

Näin ollen on olemassa sellainen $\epsilon > 0$, että

$$\begin{aligned} \gamma(m) &\leq 4^\delta \gamma(n) \\ &\leq 4^\delta C\gamma^{*8}(\tfrac{5}{6}n + \beta) \leq \epsilon\gamma^{*8}(\tfrac{5}{6}m). \end{aligned}$$

Näin ollen yläraja Lemman 2.55 nojalla ryhmä $G_{rig}$ on alieksponentiaalinen. □

**Lause 4.13.** Ryhmällä $G_{rig}$ on keskitason kasvu [13].

*Todistus.* Seurauksen 4.8 nojalla ryhmällä $G_{rig}$ on ylipolynomiaalinen kasvu ja Lauseen 4.8 nojalla sillä on alieksponentiaalinen kasvu, joten Määritelmän 2.50 nojalla sillä on keskitason kasvu. □

# 5 Ratkeavuusongelmia

*Algoritmi* on prosessi, jonka määrittelee äärellinen joukko komentoja ja joka ottaa vastaan *syötteen* ja antaa vastauksena *tulosteen*. Syöte ja tuloste ovat äärellisiä kuvauksia jostakin objektista. Ryhmien tapauksessa äärellinen kuvaus voi olla esimerkiksi sen äärellinen esitys tai automaattiryhmien tapauksessa sen generoiva Mealyn kone. Automaattiryhmän yksittäisen alkion äärelliseksi kuvaukseksi käy mikä tahansa kyseistä alkiota vastaava ryhmäsana yli generaattoriaakkoston. *Päätösongelma* on kysymys, johon on tasan kaksi mahdollista vastausta: "kyllä" tai "ei". Päätösongelma on *ratkeava*, jos on olemassa algoritmi, joka antaa kysymykseen oikean vastauksen äärellisen ajan kuluessa, sen jokaisella syötteellä. Esitetään seuraavaksi ongelmat, jotka tässä luvussa käsitellään.

*Puoliryhmän $S$ sanaongelma*
**Syöte:** Alkion $w \in S$ äärellinen kuvaus.
**Kysymys:** Onko $w$ ykkösalkio?

*Ryhmän $G$ konjugaattiongelma*
**Syöte:** Alkioiden $u \in G$ ja $v \in G$ äärelliset kuvaukset.
**Kysymys:** Onko olemassa sellainen alkio $t \in G$, että $u = t^{-1}vt$?

*Isomorfisuusongelma*
**Syöte:** Ryhmien $G$ ja $H$ äärelliset kuvaukset.
**Kysymys:** Ovatko ryhmät $G$ ja $H$ isomorfisia?

*Äärellisyysongelma*
**Syöte:** Ryhmän $G$ äärellinen kuvaus.
**Kysymys:** Onko ryhmä $G$ äärellinen?

## 5.1 Sanaongelma

**Lause 5.1.** Sanaongelma on ratkeava automaattipuoliryhmien luokassa.

*Todistus.* Olkoon $A = (Q, \Sigma, \delta, \sigma)$ Mealyn kone. Annettu syöte $w = \sigma_{q_1}\sigma_{q_2} \cdots \sigma_{q_n}$ on automaattinen kuvaus Lemman 3.5 nojalla. Kuvausta vastaava Mealyn kone $A' = (Q', \Sigma, \delta', \sigma')$ voidaan konstruoida äärellisen ajan kuluessa toistamalla induktiivisesti Lemman 3.5 konstruktiota kahden automaattisen kuvauksen yhdistetylle kuvaukselle. Nyt $w = 1$ jos ja vain jos $\sigma'_{q'}(a) = a$ aina, kun $q' \in Q'$ ja $a \in \Sigma$. □

## 5.2 Konjugaattiongelma

Oleg Bogopolski, Armando Martino ja Enric Ventura todistivat Lauseen 5.2 artikkelissa [3] vuonna 2010. Tämän jälkeen Zoran Šunić ja Ventura pystyivät todistamaan konjugaattiongelman ratkeamattomaksi artikkelissa [23] vuonna 2012. Oli riittävää osoittaa, että Lauseen 5.2 tyyppiset ryhmät ovat automaattiryhmiä.

**Lause 5.2.** Jokaista kokonaislukua $d \geq 4$ kohti on olemassa sellainen äärellisesti generoitu ryhmä $\Gamma \leq GL_d(\mathbb{Z})$, että konjugaattiongelma on ratkeamaton ryhmässä $\mathbb{Z}^d \rtimes \Gamma$.

*Todistus.* Todistettu artikkelissa [3]. □

Olkoon $\mathcal{M} = \{M_1, M_2, ..., M_m\}$ joukko $d \times d$ kokonaislukumatriiseja, joiden determinantit ovat jaottomia luvun $n \geq 2$ kanssa. Tällöin selvästi jokainen matriisi $M_i$ on kääntyvä yli $n$-adisten lukujen renkaan $\mathbb{Z}_n$, joka määriteltiin Esimerkissä 2.32. Olkoon $v \in \mathbb{Z}_n^d$ ja $M_v : \mathbb{Z}_n^d \to \mathbb{Z}_n^d$, missä $M_v(u) = v + Mu$. Määritellään ryhmä

$$G_{\mathcal{M},n} =< \{M_v \mid M \in \mathcal{M}, v \in \mathbb{Z}_n^d\} >,$$

joka selvästi on ryhmän $Aff_d(\mathbb{Z}^n)$ aliryhmä. Olkoon $e_i = (a_1, a_2, ..., a_d)$, missä $a_j = 0$, jos $i \neq j$ ja $a_i = 1$. Määritellään kuvaus $\tau_u : \mathbb{Z}_n^d \to \mathbb{Z}_n^d$ jokaista alkiota $u \in \mathbb{Z}_n^d$ kohti siten, että $\tau_u(v) = u + v$ aina, kun $v \in \mathbb{Z}_n^d$. Tällöin

$$G_{\mathcal{M},n} =< \{M_0 \mid M \in \mathcal{M}\} \cup \{\tau_{e_i} \mid i \in \{1, 2, ..., d\}\} > .$$

**Lemma 5.3.** Olkoon $\mathcal{M}$ joukko kääntyviä matriiseja yli renkaan $\mathbb{Z}$. Tällöin $G_{\mathcal{M},n} \cong \mathbb{Z}^d \rtimes \Gamma$, missä $\Gamma =< \mathcal{M} >\leq GL_d(\mathbb{Z})$ aina, kun $n \geq 2$.

*Todistus.* Olkoot $M$ kääntyvä matriisi yli renkaan $\mathbb{Z}$ ja $v \in \mathbb{Z}^d$. Tällöin kuvaus $M_v \in Aff_d(\mathbb{Z}_n)$ rajoittuu bijektiiviseen affiinikuvaukseen $M_v \in Aff_d(\mathbb{Z})$. Näin ollen ryhmä $G_{\mathcal{M},n}$ voidaan ajatella ryhmän $Aff_d(\mathbb{Z})$ aliryhmänä. Näin ollen riippuvuus luvusta $n \geq 2$ katoaa ja voidaan merkitä $G_{\mathcal{M}} = G_{\mathcal{M},n}$.

Merkitään $T =< \tau_{e_1}, \tau_{e_2}, ..., \tau_{e_d} >$. Määritellään kuvaus $\varphi : T \to \mathbb{Z}^d$ siten, että $\varphi(\tau_{e_i}) = e_i$, jolloin nähdään, että $T \cong \mathbb{Z}^d$. Selvästi myös ryhmät $\Gamma$ ja $< M_0 \mid M \in \mathcal{M} >$ ovat isomorfisia, joten ne voidaan samaistaa.

Olkoot $\tau_v \in T$ ja $M \in \Gamma$. Tällöin $M0 = 0$, mutta $\tau_v(0) = v$, joten $T \cap \Gamma = 1$. Olkoon $M$ joko joukon $\mathcal{M}$ alkio tai käänteisalkio. Tällöin

$$\begin{aligned} M_0 \circ \tau_{e_j} \circ M_0^{-1}(u) &= M_0(\tau_{e_j}(M^{-1}u)) \\ &= M_0(e_j + M^{-1}u) \\ &= Me_j + u \\ &= \tau_{e_1}^{m_{1,j}} \circ \tau_{e_2}^{m_{2,j}} \circ ... \circ \tau_{e_d}^{m_{d,j}}(u), \end{aligned}$$

aina, kun $j \in \{1, 2, ..., d\}$ ja $u \in \mathbb{Z}^d$ ja missä $m_{i,j}$ on matriisin $M$ alkio positiossa $(i, j)$. Nähdään, että $\mathbb{Z}^d \cong T \trianglelefteq G_{\mathcal{M}}$. Näin ollen Määritelmän 2.37 nojalla $G_{\mathcal{M}} \cong \mathbb{Z}^d \rtimes \Gamma$. □

Renkaan $\mathbb{Z}_n$ alkiot voidaan esittää äärettöminä sanoina yli aakkoston $\Sigma_n = \{0, 1, ..., n-1\}$ siten, että sana $a_0a_1a_2 \cdots \in \Sigma_n^\omega$ vastaa alkiota $\sum_{i=1}^{\infty} a_i n^i$. Yleistämällä tätä luonnollisella tavalla saadaan jokainen alkio $u \in \mathbb{Z}_n^d$ esitettyä äärettöminä sanoina yli aakkoston $\Sigma_{n,d} = \{(b_1, b_2, ..., b_d)^T \mid b_i \in \Sigma_n\}$.

Olkoon $v \in \mathbb{Z}^d$. Määritellään jakojäännös $\mathrm{Mod}(v)$ ja osamäärä $\mathrm{Div}(v)$ siten, että $v = \mathrm{Mod}(v) + n\mathrm{Div}(v)$, missä $Mod(v) \in \Sigma_n^d$.

**Lemma 5.4.** Olkoot $v \in \mathbb{Z}^d$ ja $u_1u_2u_3 \cdots \in \Sigma_{n,d}^\omega$. Tällöin

$$M_v(u_1u_2u_3 \cdots) = \mathrm{Mod}(v + Mu_1) + nM_{\mathrm{Div}(v+Mu_1)}(u_2u_3u_4 \cdots).$$

*Todistus.* Väite seuraa yhtälöketjusta:

$$\begin{aligned} M_v(u_1u_2u_3 \cdots) &= v + Mu_1u_2u_3 \cdots \\ &= v + M(u_1 + n(u_2u_3u_4 \cdots)) \\ &= v + Mu_1 + nMu_2u_3u_4 \cdots \\ &= \mathrm{Mod}(v + Mu_1) + n\mathrm{Div}(v + Mu_1) + nMu_2u_3u_4 \cdots \\ &= \mathrm{Mod}(v + Mu_1) + n(\mathrm{Div}(v + Mu_1) + Mu_2u_3u_4 \cdots) \\ &= \mathrm{Mod}(v + Mu_1) + nM_{\mathrm{Div}(v+Mu_1)}(u_2u_3u_4 \cdots). \end{aligned}$$

□

Merkitään $||M|| = max_i \sum_{j=1}^{d} |m_{i,j}|$, missä $m_{i,j}$ on matriisin $M$ alkio positiossa $(i,j)$. Määritellään joukko

$$V_M = \{(v_1, v_2, ..., v_d) \in \mathbb{Z}^d \mid -||M|| \leq v_i \leq ||M|| - 1 \text{ ja } i \in \{1, 2, ..., d\}\},$$

jolloin $|V_M| \leq (2||M||)^d$.

Olkoot $v \in V_M$ ja $u \in \Sigma_{n,d}$. Tällöin

$$\begin{aligned}(v + Mu)_i &= v_i + \sum_{i=1}^{d} m_{i,j}u_j \\ &\leq ||M|| - 1 + \sum_{i=1}^{d} |m_{i,j}||u_j| \\ &\leq ||M|| - 1 + \sum_{i=1}^{d} |m_{i,j}|(n-1) \\ &\leq ||M|| - 1 + (n-1)||M|| \\ &\leq n||M|| - 1\end{aligned}$$

ja

$$\begin{aligned}(v + Mu)_i &= v_i + \sum_{i=1}^{d} m_{i,j}u_j \\ &\geq -||M|| + \sum_{i=1}^{d} -|m_{i,j}||u_j| \\ &\geq -||M|| + \sum_{i=1}^{d} -|m_{i,j}|(n-1) \\ &\geq -||M|| - (n-1)||M|| \\ &\geq -n||M||\end{aligned}$$

aina, kun $i \in \{1, 2, ..., d\}$. Näin ollen $\text{Div}(v+Mu) \in V_M$, joten Määritelmässä 5.5 konstruoitu Mealyn kone on hyvin määritelty.

**Määritelmä 5.5.** Olkoon $M$ kokonaislukumatriisi. Määritellään Mealyn kone $A_{M,n} = (Q, \Sigma, \delta, \sigma)$ siten, että $Q = \{m_v | v \in V_M\}$, $\Sigma = \Sigma_{n,d}$,

$$\delta_u(m_v) = m_{\text{Div}(v+Mu)} \text{ ja } \sigma_{m_v(u)} = \text{Mod}(v + Mu)$$

aina, kun $u \in \Sigma$ ja $m_v \in Q$.

Selvästi Mealyn kone $A_{M,n}$ on kääntyvä jos $M$ on kääntyvä.

**Lemma 5.6.** Olkoon Mealyn kone $A_{M,n} = (Q, \Sigma, \delta, \sigma)$, kuten Määritelmässä 5.5. Tällöin $\sigma_{m_v(u)} = M_v(u)$ aina, kun $m_v \in Q$ ja $u \in \Sigma^\omega$.

*Todistus.* Väite seuraa suoraan Lemmasta 5.4 ja Määritelmästä 5.5. □

**Määritelmä 5.7.** Olkoon $\mathcal{M} = \{M_1, M_2, ..., M_m\}$ joukko $(d \times d)$-kokonaislukumatriiseja. Määritellään $A_{\mathcal{M},n}$ automaattien $A_{M_1,n}$, $A_{M_2,n}$, ... , $A_{M_{m-1},n}$ ja $A_{M_m,n}$ unionina.

**Lause 5.8.** Ryhmä $G_{\mathcal{M},n}$ on isomorfiaa vaille automaattiryhmä.

*Todistus.* Olkoon $\mathcal{M}$ joukko kääntyviä $(d \times d)$-kokonaislukumatriiseja. Osoitetaan, että $G_{\mathcal{M},n} \cong \mathcal{G}(A_{\mathcal{M},n})$. Määritelmän 5.5 nojalla $\sigma_{m_0} \in Q$ ja Lemman 5.4 nojalla $\sigma_{m_0} = M_0$ aina, kun $M \in \mathcal{M}$. Toisaalta
$\tau_{e_i} = M_0 \circ (M_0)^{-1} \circ \tau_{e_i} = M_0 \circ (M_{-e_i})^{-1} = \sigma_{m_0} \circ \sigma_{m_{-e_i}}^{-1} \in Q$, joten koska

$$G_{\mathcal{M},n} =< \{M_0 \mid M \in \mathcal{M}\} \cup \{\tau_{e_i} \mid i \in \{1, 2, ..., d\}\} >,$$

niin Lemman 5.4 nojalla $G_{\mathcal{M},n} \cong \mathcal{G}(A_{\mathcal{M},n})$. □

**Lause 5.9.** Konjugaattiongelma on ratkeamaton automaattiryhmien luokassa. [23]

*Todistus.* Koska ryhmien $G_{\mathcal{M},n}$ joukossa on Lauseen 5.2 nojalla olemassa sellainen ryhmä, että konjugaattiongelma on ratkeamaton ja koska Lauseen 5.8 nojalla $G_{\mathcal{M},n} \cong \mathcal{G}(A_{\mathcal{M},n})$, niin väite seuraa. □

## 5.3 Isomorfisuusongelma

Lauseesta 5.8 seuraa myös isomorfisuusongelman ratkeamattomuus.

**Määritelmä 5.10.** Olkoon $U =< x_1, x_2, ..., x_n | r_1, r_2, ..., r_m >$ jonkin ryhmän äärellinen esitys. Määritellään ryhmä

$$M(U) = \{(v, u) \in F_n \times F_n \mid v =_U u\}$$

ja sanotaan, että $M(U)$ on ryhmää $U$ vastaava *Mihailovan ryhmä.*

**Lause 5.11.** Olkoot $U =< x_1, x_2, ..., x_n | r_1, r_2, ..., r_m >$ jonkin ryhmän äärellinen esitys ja $M(U)$ Mihailovan ryhmä. Tällöin

$$M(U) =< \{(x_1, x_1), (x_2, x_2), ..., (x_n, x_n), (1, r_1), (1, r_2), ..., (1, r_m)\} > .$$

*Todistus.* Merkitään yhtälön oikeaa puolta symbolilla $H$. Selvästi $H \subseteq M(U)$. Todistetaan väite toiseen suuntaan. Jos $w =_U 1$, niin

$$w =_U \prod_{i=1}^{k} u_i^{-1} r_{j_i}^{e_i} u_i,$$

missä $u_i \in U$ ja $e_i \in \{-1, 1\}$ aina, kun $i \in \{1, 2, ..., k\}$. Tällöin

$$(1, w) =_{U \times U} \prod_{i=1}^{k} (u_i, u_i)^{-1} (1, r_{j_i})^{e_i} (u_i, u_i) \in H.$$

Yleisemmin, jos $v =_U u$, niin $vu^{-1} =_U 1$, joten $(1, vu^{-1}) \in H$. Lisäksi selvästi $(u, u) \in H$, joten $(u, v) \in H$ ja näin ollen $M(U) \subseteq H$, joten väite on todistettu. □

**Lause 5.12.** Olkoot $U =< x_1, x_2, ..., x_n | r_1, r_2, ..., r_m >$ jonkin ryhmän äärellinen esitys ja $M(U)$ Mihailovan ryhmä. Tällöin $M(U)$ on äärellisesti esitetty jos ja vain jos $U$ on äärellinen.

*Todistus.* Todistettu artikkelissa [15]. □

**Määritelmä 5.13.** Olkoot $U =< x_1, x_2, ..., x_n | r_1, r_2, ..., r_m >$ jonkin ryhmän äärellinen esitys ja $w \in U$. Määritellään ryhmä $L_w$ siten, että

$$L_w =< x_1, x_2, ..., x_n, a, b, c | r_1, r_2, ..., r_m, R_1 R_1^{'-1}, R_2 R_2^{'-1}, R_3 R_3^{'-1}, T >,$$

missä

$$\begin{array}{llll} R_1 & = a^{-1}ba, & R_1^{'} & = c^{-1}b^{-1}cbc, \\ R_2 & = a^{-2}b^{-1}aba^{-2}, & R_2^{'} & = c^{-2}b^{-1}cbc^2, \\ R_3 & = a^{-3}[w,b]a^3, & R_3^{'} & = c^{-3}bc^3, \\ T_i & = a^{-(3+i)}x_i ba^{3+i}, & T_i^{'} & = c^{-(3+i)}bc^{3+i} \end{array}$$

aina, kun $i \in \{1, 2, ..., n\}$ ja missä $[w, b] = w^{-1}b^{-1}wb$ ja

$$T = \{T_i T_i^{'-1} \mid i \in \{1, 2, ..., n\}\}.$$

**Lause 5.14.** Olkoot $U$ ja $L_w$ kuten Määritelmässä 5.13. Tällöin seuraavat kolme väitettä ovat voimassa:

Jos $w =_U 1$, niin on olemassa injektiivinen homomorfismi $\varphi : U \to L_w$.
Normaalisulkeuma $N_w = L_w$, erityisesti $L_w \cong \{1\}$, jos $w =_U 1$.
Alkiot $b$ ja $ca^{-1}$ generoivat ryhmän $L_w$.

*Todistus.* Todistettu kirjassa [20]. □

Kirjan [20] nojalla on olemassa sellainen äärellisesti esitetty ryhmä $U$, että sanaongelma on kyseisessä ryhmässä ratkeamaton.

**Lause 5.15.** Isomorfisuusongelma on ratkeamaton muotoa $\mathbb{Z}^d \rtimes \Gamma$ olevien ryhmien luokassa, missä $\Gamma \leq GL_d(\mathbb{Z})$.

*Todistus.* Valitaan mikä tahansa sellainen äärellisesti esitetty kahden alkion generoima ryhmä $U$, että sanaongelma on kyseisessä ryhmässä ratkeamaton. Konstruoidaan syötesanaa $w \in U$ vastaava Määritelmän 5.13 ryhmä $L_w$. Konstruoidaan ryhmää $L_w$ vastaava Mihailovan ryhmä $H_w = M(L_w)$. Nähdään, että

$$\begin{array}{ll} H_w = F_2 \times F_2 & \text{jos ja vain jos } u =_{L_w} v \text{ aina, kun } u \in F_2 \text{ ja } v \in F_2 \\ & \text{jos ja vain jos } L_w = \{1\} \text{ [20]} \\ & \text{jos ja vain jos } w =_U 1. \end{array}$$

Koska $F_2 \leq GL_2(\mathbb{Z})$, niin voidaan valita $\Gamma = H_w \leq GL_4(\mathbb{Z})$ ja $\Delta = F_2 \times F_2 \leq GL_4(\mathbb{Z})$. Merkitään $G_w = \mathbb{Z}^4 \rtimes \Gamma$ ja $G = \mathbb{Z}^4 \rtimes \Delta$. Tällöin jos $w =_U 1$, niin $G_w = G$, joka on äärellisesti esitetty. Toisaalta jos $w \neq_U 1$, niin on olemassa injektiivinen homomorfismi $\varphi : U \to L_w$, jolloin $L_w$ on välttämättä ääretön. Lauseen 5.12 nojalla $H_w$ ei ole äärellisesti esitetty, jolloin myöskään $G_w$ ei ole äärellisesti esitetty. Näin ollen $G_w$ ei ole isomorfinen ryhmän $G$ kanssa, joten väite seuraa. □

**Lause 5.16.** Isomorfisuusongelma on ratkeamaton automaattiryhmien luokassa [24].

*Todistus.* Lauseen 5.8 nojalla jokainen muotoa $\mathbb{Z}^d \rtimes \Gamma$ oleva ryhmä, missä $\Gamma \leq GL_d(\mathbb{Z})$ ja $\Gamma$ on äärellisesti generoitu, on automaattiryhmä. Näin ollen väite seuraa Lauseesta 5.15. □

## 5.4 Äärellisyysongelma

Hao Wang määritteli Wang-tiilijoukot artikkelissa [25] ja otaksui, että tiilitysongelma on ratkeava. Robert Berger todisti ongelman kuitenkin ratkeamattomaksi artikkelissa [2]. Jarkko Kari määritteli NW-deterministiset tiilijoukot artikkelissa [18] ratkaistaakseen yksi-ulotteisia soluautomaatteja koskevan nilpotenttisuusongelman ja todisti, että tiilitysongelma on ratkeamaton myös kun ollaan rajoituttu NW-deterministisiin tiilijoukkoihin. Tässä aliluvussa todistetaan automaattipuoliryhmiä koskevan äärellisyysongelman ratkeamattomuus redusoimalla sen NW-determinististen Wang-tiilijoukkojen tiilitysongelmaan. Ratkaisu on peräisin Pierre Gillibertin artikkelista [5].

*Tiilitysongelma*
**Syöte:** Wang-tiilijoukko $T$.
**Kysymys:** Onko olemassa konfiguraatio $c : \mathbb{Z}^2 \to T$, joka on validi tiilitys?

**Määritelmä 5.17** (Wang-tiili ja -tiilijoukko)**.** Olkoon $S$ äärellinen joukko. *Wang-tiili* on yksikköneliö, joka esitetään neljä-tuplana $t = (t^n, t^e, t^s, t^w)$, jossa $t^n$, $t^e$, $t^s$ ja $t^w$ kuuluvat *värien* joukkoon $S$. *Wang-tiilijoukko* $T$ on äärellinen joukko Wang-tiiliä. *Konfiguraatio* on kuvaus $c : \mathbb{Z}^2 \longrightarrow T$ ja se on *virheetön* osajoukossa $F \subseteq \mathbb{Z}^2$, jos

$$\begin{array}{rcll} c(i,j)^n & = & c(i,j+1)^s, & \\ c(i,j)^e & = & c(i+1,j)^w, & \\ c(i,j)^s & = & c(i,j-1)^n & \text{ja} \\ c(i,j)^w & = & c(i-1,j)^e & \end{array}$$

aina, kun $(i,j)$, $(i+1,j)$, $(i,j+1)$, $(i-1,j)$ ja $(i,j-1)$ kuuluvat joukkoon $F$, muutoin se on *virheellinen* joukossa $F$. Konfiguraatio on *validi tiilitys*, jos se on virheetön tasossa $\mathbb{Z}^2$.

**Määritelmä 5.18.** Merkitään kaikkien mahdollisten konfiguraatioiden joukkoa tavalliseen tapaan $T^{\mathbb{Z}^2}$. Olkoon $(c_n)$ konfiguraatioiden *jono* joukossa $T^{\mathbb{Z}^2}$. Sanotaan, että $(c_n)$ *suppenee* kohti sen *raja-arvoa* $c \in T^{\mathbb{Z}^2}$, jos jokaista $(i,j) \in \mathbb{Z}^2$ kohti on olemassa sellainen $k \in \mathbb{N}$, että $c_m(i,j) = c(i,j)$ aina, kun $m \geq k$.

Joukon $S$ *enumeraatio* on sen alkioiden täydellinen listaus.

**Lause 5.19.** Jokaista konfiguraatioiden jonoa kohti on olemassa suppeneva osajono.

*Todistus.* Olkoot $T$ Wang-tiilijoukko ja $(c_n)$ konfiguraatioiden jono joukossa $T^{\mathbb{Z}^2}$. Olkoon $r_0$, $r_1$, ... joukon $\mathbb{Z}^2$ enumeraatio. Valikoidaan $i_0$ siten, että se on pienin sellainen luonnollinen luku, että joukko $\{i \in \mathbb{N} \mid c_i(r_0) = c_{i_0}(r_0)\}$ on ääretön. Valinta voidaan tehdä, koska $T$ on äärellinen. Oletetaan sitten, että $i_{k-1}$ on valittu ja valitaan $i_k$ siten, että se on pienin luonnollinen luku, joka toteuttaa seuraavat kolme ehtoa:

$(A_k)$ $\quad i_k > i_{k-1}$,
$(B_k)$ $\quad c_{i_k}(r_j) = c_{i_{k-1}}(r_j)$ aina, kun $j \in \mathbb{N}$ ja $j < k$ ja
$(C_k)$ $\quad$ Joukko $\{i \in \mathbb{N} \mid c_i(r_j) = c_{i_k}(r_j)$ aina, kun $j \in \mathbb{N}$ ja $j \leq k\}$ on ääretön.

Olkoon $I_k$ indeksijoukko, joka toteuttaa ehdon $(B_k)$. Koska ehto $(C_{k-1})$ oli voimassa, kun $i_{k-1}$ valittiin, niin $I_k$ on ääretön. Koska $T^k$ on äärellinen, niin on olemassa sellainen osajoukko $J_k \subseteq I_k$, että $J_k$ on ääretön ja
$J_k = \{i \in \mathbb{N} \mid c_i(r_j) = c_{i_k}(r_j)$ aina, kun $j \in \mathbb{N}$ ja $j \leq k\}$, jolloin ehto $(C_k)$ on myös voimassa. Joukosta $J_k$ löytyy myös triviaalisti ehdon $(A_k)$ täyttävä luku. Ehdosta $(B_k)$ seuraa, että osajono $(c_{i_n})$ suppenee. □

**Seuraus 5.20** (Kompaktisuusperiaate)**.** Olkoon $T$ Wang-tiilijoukko. Jos on olemassa virheetön konfiguraatio joukossa $F$ aina, kun $F \subseteq \mathbb{Z}^2$ ja $F$ on äärellinen, niin on olemassa konfiguraatio, joka on validi tiilitys.

*Todistus.* Olkoon $r_0$, $r_1$, ... joukon $Z^2$ enumeraatio. Merkataan
$F_n = \{r_0, r_1, ..., r_n\}$ aina, kun $n \in \mathbb{N}$. Oletuksen nojalla jokaista $n \in \mathbb{N}$ kohti on olemassa konfiguraatio $c_n$, joka on virheetön joukossa $F_n$. Lauseesta 5.19 seuraa, että näin saatujen konfiguraatioiden jonolla $(c_n)$ on suppeneva osajono. Osajonon raja-arvo on selvästi validi tiilitys. □

**Määritelmä 5.21** (NW-deterministinen Wang-tiilijoukko)**.** Wang-tiilijoukko $T$ on *NW-deterministinen* jos $t_0 = t_1$ aina, kun $t_0^n = t_1^n$, $t_0^w = t_1^w$, $t_0 \in T$ ja $t_1 \in T$.

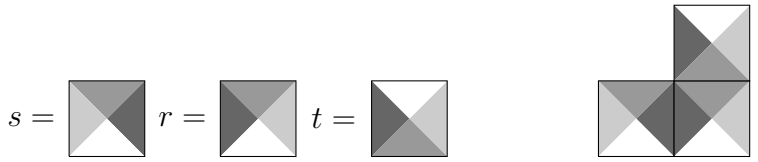
**Lause 5.22.** Tiilitysongelma on ratkeamaton NW-deterministisisten Wang-tiilijoukkojen luokassa.

*Todistus.* Todistettu artikkelissa [18]. □

**Määritelmä 5.23.** Olkoon $T$ NW-deterministinen tiilijoukko. Olkoon $\perp$ symboli, joka ei kuulu joukkoon $T$. Määritellään Mealyn kone $A_T = (Q, \Sigma, \delta, \sigma)$ siten, että $Q = \Sigma = T \cup \{\perp\}$. Siirtymäfunktio $\delta : Q \cup \Sigma \to Q$ on määritelty siten, että $\delta_a(q) = a$ aina, kun $a \in \Sigma$ ja $q \in Q$. Tulostusfunktio $\sigma : Q \cup \Sigma \to \Sigma$ on määritelty siten, että

$$\begin{aligned} \sigma_\perp(a) &= \perp \text{ aina, kun } a \in \Sigma, \\ \sigma_s(t) &= r \text{ jos } r^n = t^s, r^w = s^e \text{ ja } r \in T, \\ \sigma_s(t) &= \perp \text{ muissa tapauksissa.} \end{aligned}$$

Konstruktion vastaavuutta tason $\mathbb{Z}^2$ tiilitykseen voidaan havainnoida seuraavasti. Syötesana $u \in \Sigma^* \cup \Sigma^\omega$ kirjoitetaan tason diagonaalille $((i,i))_{i \in \mathbb{N}}$ ja tuloste $\sigma_q(u)$ kirjoitetaan vastaavasti tason diagonaalille $((i, i-1))_{i \in \mathbb{N}}$. Symboli $\perp$ tarkoittaa virhettä. Jos sellaista tiiltä $r \in T$ ei ole olemassa, että $r^n = t^s$ ja $r^w = s^e$, niin tulostusfunktio $\sigma_s$ antaa syötteellä $t$ tulosteena virheen $\perp$. Tulostusfunktiota on havainnoitu Kuvassa 3.




Kuva 3: Määritelmässä 5.23 konstruoidun Mealyn koneen tulostus- ja siirtymäfunktioiden havainnointi. Tässä $\sigma_s(t) = r$ ja $\delta_t(s) = t$.

**Määritelmä 5.24.** Olkoot $A = (Q, \Sigma, \delta, \sigma)$ Mealyn kone ja $\varphi : \Sigma \to Q$ injektiivinen kuvaus. Jos $\delta_a(q) = \varphi(a)$ aina, kun $q \in Q$, niin $A$ on *reset-automaatti*.

Reset-automaateille on voimassa seuraava yhtälö:

$$\sigma_q(u) = \sigma_q(u_1)\sigma_{\varphi(u_1)}(u_2)\sigma_{\varphi(u_2)}(u_3) \cdots$$

aina, kun $u = u_1 u_2 \cdots \in \Sigma^* \cup \Sigma^\omega$. Selvästi Määritelmässä 5.23 konstruoitu Mealyn kone on reset-automaatti.

**Lemma 5.25.** Olkoot $T$ NW-deterministinen Wang-tiilijoukko, $c : \mathbb{Z}^2 \to T$ validi tiilitys ja $w_n = (c(i+n, i))_{i\in\mathbb{N}}$. Tällöin $\sigma_{\perp^m}(w_n) = \perp^m w_{m+n}$ aina, kun $n \in \mathbb{N}$ ja $m \in \mathbb{N}$. Erityisesti $\mathcal{S}(A_T)$ on ääretön.

*Todistus.* Suoraan puoliryhmän $\mathcal{S}(A_T)$ määritelmästä seuraa, että

$$\sigma_{c(i,j)}(c(i+1, j+1)) = c(i+1, j)$$

aina, kun $i \in \mathbb{N}$ ja $j \in \mathbb{N}$. Todistetaan väite induktiolla muuttujan $m$ suhteen. Jos $m = 1$ niin saadaan, että

$$\begin{aligned}\sigma_\perp(w_n) &= \sigma_\perp(c(n, 0))(\sigma_{c(i+n,i)}(c(i+1+n, i+1)))_{i\in\mathbb{N}} \\ &= \perp (c(i+1+n, i))_{i\in\mathbb{N}} \\ &= \perp w_{n+1}.\end{aligned}$$

Tällöin induktio-oletuksen nojalla

$$\begin{aligned}\sigma_{\perp^m}(w_n) &= \sigma_\perp(\sigma_{\perp^{m-1}}(w_n)) \\ &= \sigma_\perp(\perp^{m-1} w_{m+n-1}) \\ &= \perp^{m-1} \sigma_\perp(w_{m+n-1}) \\ &= \perp^m w_{m+n}.\end{aligned}$$

Tällöin $\sigma_{\perp^i} \neq \sigma_{\perp^j}$ aina, kun $i \in \mathbb{N}$, $j \in \mathbb{N}$ ja $i \neq j$, joten puoliryhmä $\mathcal{S}(A_T)$ on ääretön. □

**Lemma 5.26.** Olkoon $T$ sellainen NW-deterministinen Wang-tiilijoukko, että ei ole olemassa kuvausta $c : \mathbb{Z}^2 \to T$, joka olisi validi tiilitys. Tällöin puoliryhmä $\mathcal{S}(A_T)$ on äärellinen.

*Todistus.* Kompaktisuusperiaatteen 5.20 nojalla on olemassa sellainen $n \in \mathbb{N}$, että ei ole olemassa virheetöntä kuvausta $c : \{1, 2, ..., n\}^2 \to T$.

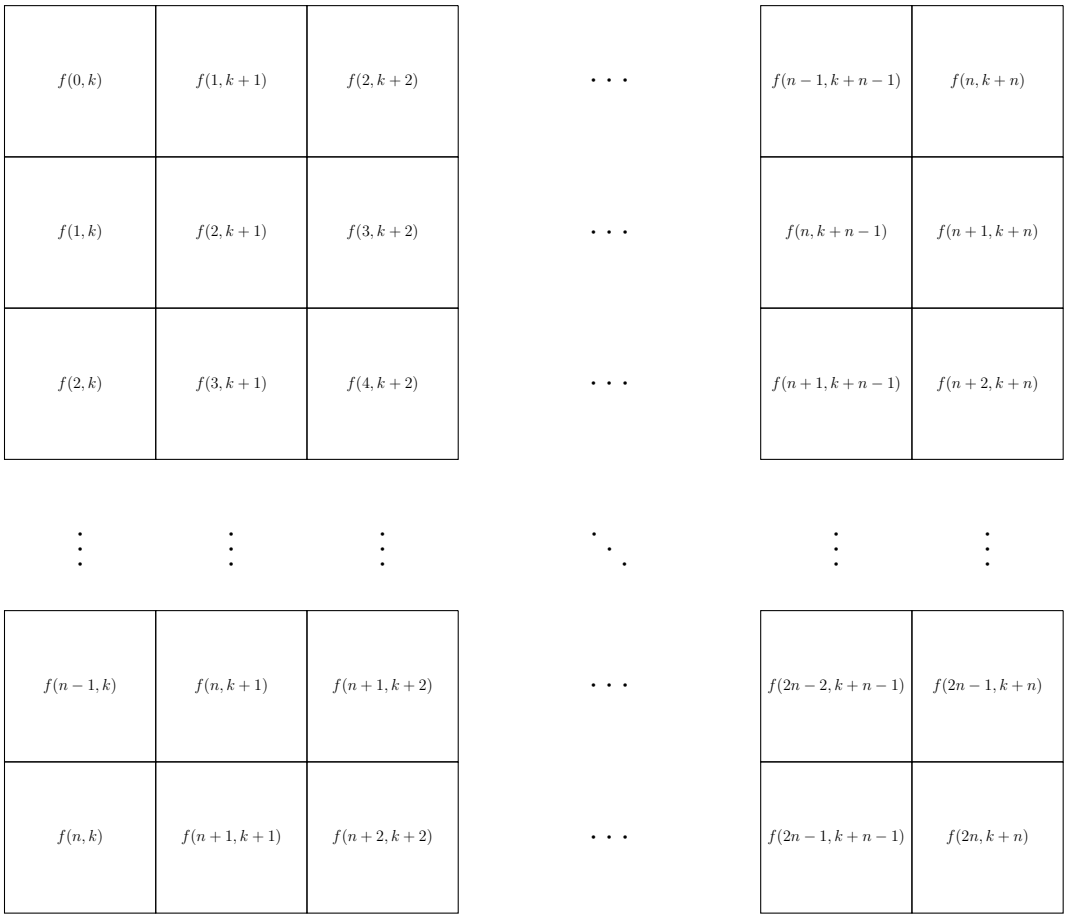
Olkoon $u = u_1 u_2 \cdot ... \cdot u_{2n} \in Q^{2n}$. Otetaan käyttöön lyhennysmerkintä $\tau_k = \sigma_{u_1 u_2 \cdot ... \cdot u_k}$ aina, kun $1 \leq k \leq 2n$ ja olkoon $\tau_0$ identiteettikuvaus. Tällöin $\tau_{k+1} = \sigma_{u_{k+1}} \circ \tau_k$ aina, kun $0 \leq k \leq 2n-1$. Olkoot $t \in \Sigma^n$ ja $v \in \Sigma^\omega$. Määritellään jokaista ehdon $0 \leq i \leq 2n$ täyttävää lukua $i$ kohti jono $f_i : \mathbb{N} \to \Sigma$ siten, että

$$(f(i, j))_{j\in\mathbb{N}} = \tau_i(tv) \text{ missä } f(i, j) = f_i(j).$$

Saadaan, että

$$\begin{aligned}(f(i+1, j))_{j\in\mathbb{N}} &= \tau_{i+1}(tv) \\ &= \sigma_{u_{i+1}}(\tau_i(tv)) \\ &= \sigma_{u_{i+1}}((f(i, j))_{j\in\mathbb{N}}) \\ &= \sigma_{u_{i+1}}(f(i, 0))(\sigma_{f(i,j)}(f(i, j+1)))_{j\in\mathbb{N}},\end{aligned}$$

joten $\sigma_{f(i,j)}(f(i,j+1)) = f(i+1,j+1)$ aina, kun $0 \leq i < 2n$. Jos on olemassa sellainen $k \in \mathbb{N}$, että $f(2n, n+k) \neq \perp$, niin edellisen ja Määritelmän 5.23 nojalla saadaan, että $f(i+j, j+k) \neq \perp$ aina, kun $0 \leq i \leq n$ ja $0 \leq j \leq n$. Tämä käy selväksi Kuvasta 4. Näin ollen kuvaus $c : \mathbb{Z}^2 \to T$ on virheetön joukossa $\{0,1,...,n\}^2$, missä $c(j,i) = f(i+j, j+k)$ aina, kun $0 \leq i \leq n$ ja $0 \leq j \leq n$.




Kuva 4: Määrittelemällä $c(j,i) = f(i+j, j+k)$ aina, kun $0 \leq i \leq n$ ja $0 \leq j \leq n$ saadaan kuvaus, joka on virheetön joukossa $\{0,1,...,n\}^2$.

Tämä on ristiriita, joten $\sigma_u(tv) = \sigma_u(t)\ \perp^\omega$ aina, kun $t \in \Sigma^n$ ja $v \in \Sigma^\omega$. Olkoon sitten $w = uq$, missä $u \in Q^{2n}$ ja $q \in Q^*$. Tällöin

$$\begin{aligned} \sigma_w(tv) &= \sigma_q(\sigma_u(tv)) \\ &= \sigma_q(\sigma_u(t)\ \perp^\omega) \\ &= \sigma_{uq}(t)\ \perp^\omega \\ &= \sigma_w(t)\ \perp^\omega \end{aligned}$$

aina, kun $t \in \Sigma^n$ ja $v \in \Sigma^\omega$. Näin ollen joukko

$$H = \{\sigma_u \in \mathcal{S}(A_T) \mid u \in \Sigma^* \text{ ja } |u| \geq 2n\}$$

on äärellinen ja sen koko on korkeintaan $|(\Sigma^n)^{\Sigma^n}|$. Koska

$$\mathcal{S}(A_T) = H \cup \{\sigma_u \in \mathcal{S}(A_T) \mid u \in \Sigma^* \text{ ja } |u| < 2n\},$$

niin

$$|\mathcal{S}(A_T)| \leq |(\Sigma^n)^{\Sigma^n}| + \sum_{i=0}^{2n-1} |Q|^i.$$

Näin ollen puoliryhmä $\mathcal{S}(A_T)$ on äärellinen.

□

**Lause 5.27.** Äärellisyysongelma on ratkeamaton automaattipuoliryhmien luokassa [5].

*Todistus.* Olkoon $T$ NW-deterministinen Wang-tiilijoukko. Tällöin Lemmojen 5.25 ja 5.26 nojalla on olemassa validi tiilitys jos ja vain jos automaattipuoliryhmä $\mathcal{S}(A_T)$ on ääretön. Koska tiilitysongelma on ratkeamaton NW-determinististen Wang-tiilijoukkojen luokassa, niin välttämättä myös äärellisyysongelma on ratkeamaton automaattipuoliryhmien joukossa. □

**Seuraus 5.28.** Päätösongelma "Annettuna puoliryhmä ja kaksi mitä tahansa puoliryhmän alkiota $g$ ja $h$, päätä onko olemassa sellainen luonnollinen luku $n \in \mathbb{N}$, että $g^n = h$." on ratkeamaton automaattipuoliryhmien luokassa.

*Todistus.* Olkoon $T$ NW-deterministinen Wang-tiilijoukko. Olkoon $A_T$ Määritelmässä 5.23 konstruoitu automaattipuoliryhmä. Lisätään tilajoukkoon $Q$ uusi tila $c$ ja laajennetaan siirtymäfunktio siten, että $\delta_a(c) = c$ aina, kun $a \in \Sigma$ ja laajennetaan tulostusfunktio siten, että $\sigma_c(a) = \perp$ aina, kun $a \in \Sigma$. Olkoon näin saatu Mealyn kone $A'_T$. Tällöin $\sigma_c(w) = \perp^\omega$ aina, kun $w \in \Sigma^\omega$. Lemmojen 5.25 ja 5.26 nojalla on olemassa sellainen luonnollinen luku $n$, että $\sigma_\perp^n = \sigma_c$ jos ja vain jos ei ole olemassa kuvausta, joka olisi tason validi tiilitys. □

# Lähteet

[1] S. V. Aleshin: Finite automata and Burnside's problem for periodic groups. *Mat. Zametki, 11:3.* 1972. s. 319 – 328.

[2] R. Berger. *The undecidability of the Domino problem.* Mem. Amer. Math. Soc. 1966.

[3] O. Bogopolski, A. Martino, E. Ventura: Orbit decidability and the conjugacy problem for some extensions of groups. *Trans. Amer. Math. Soc. 362.* 2010. s. 2003 – 2036.

[4] W. Burnside: On an Unsettled Question in the Theory of Discontinuous Groups. *Quart. J. Pure Appl. Math. 33.* 1902. s. 230 - 238.

[5] P. Gillibert: The finiteness problem for automaton semigroups is undecidable. *Int. J. Algebra Comput., 24, 1.* 2014. s. 1 - 9.

[6] E. S. Golod, I. R. Shafarevich: On the class field tower. *Izv. Akad. Nauk SSSR 28, no. 2.* 1964. s. 261 – 272.

[7] E. S. Golod: On nil algebras and residually finite p-groups. *Izv. Akad. Nauk SSSR 28, no. 2.* 1964. s. 273 – 276.

[8] R. I. Grigorchuk: On Burnside's problem on periodic groups *Funktsional. Anal. i Prilozhen. 14.* 1980. s. 53 – 54.

[9] R. I. Grigorchuk, V.V. Nekrashevich, V.I. Sushchanskii: Automata, dynamical systems, and groups. *Tr. Mat. Inst. Steklova 231.* 2000. 134 – 214.

[10] R. I. Grigorchuk, P. Linnel, T. Schick, A. Zuk: On a Conjecture of Atiyah. *C. R. Acad. Sci. Paris Sér. I Math. 331.* 2000. s. 663 - 668.

[11] R. I. Grigorchuk: Growth Rates of Finitely Generated Groups and Theory of Invariant Means. *Izv. Akad. Nauk SSSR, Ser. Mat., vol. 48, no. 5* 1984. s. 939 - 985.

[12] R. I. Grigorchuk, A. Zuk: The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geom. Dedicata 87, no. 1 - 3.* 2001. s. 209 – 244

[13] R. I. Grigorchuk: On the Milnor problem of group growth. *Dokl. Akad. Nauk SSSR 271 no. 1.* 1983. s. 30 - 33.

[14] R. I. Grigorchuk, I. Pak: Groups of intermediate growth: an introduction. *Enseign. Math. (2), 54:3 - 4.* 2008. 251 – 272.

[15] F. J. Grunewald: On Some Groups which cannot be Finitely Presented. *J. London Math. Soc. Vol. Issue 3.* 1978. s. 2 - 17.

[16] N. Gupta, S. Sidki: On the Burnside problem for periodic groups. *Math. Z.*. 1983. s. 385 - 388.

[17] J. Kari: *Tilings and Patterns*. Luentomoniste. Turun yliopisto. 2015.

[18] J. Kari: The nilpotency problem of one-dimensional cellular automata. *SIAM J. Comput. 21*. 1992. s 571 – 586.

[19] Yu. I. Merzlyakov: On infinite finitely generated periodic groups. *Dokl. Akud. Nauk 268*. 1983. s. 803 - 805.

[20] C. F. Miller: Decision Problems for Groups - Survey and Reflections. *Algorithms and Classification in Combinatorial Group Theory*. 1992. s. 1 - 59.

[21] J. Milnor: Problem 5603. *Amer. Math. Monthly 75*. 1968.

[22] V. V. Nekrashevych: *Self-similar groups, Mathematical Surveys and Monographs, vol. 117*. American Mathematical Society, Providence, RI. 2005.

[23] Z. Šunić, E. Ventura: The conjugacy problem in automaton groups is not solvable. *J. Algebra 364*. 2012. s. 148 – 154.

[24] E. Ventura: *Unsolvability of the CP and IP for automaton groups*. Luento. GAGTA-6, Dusseldorf. 2012.

[25] H. Wang: Proving theorems by pattern recognition–II. *Bell System Tech. 40*. 1961. s. 1 – 42.

[26] J. S. Wilson: On exponential growth and uniformly exponential growth for groups. *Invent. Math. 155, no. 2*. 2004. s. 287 - 303.