Pienten kokonaislukumatriisien kuolevuusongelman ratkeavuudesta

Reino Niskanen

Pro gradu -tutkielma
Heinäkuu 2013

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

NISKANEN, REINO: Pienten kokonaislukumatriisien kuolevuusongelman ratkeavuudesta
Pro gradu -tutkielma, 59 s.
Matematiikka
Heinäkuu 2013

Tämä tutkielma käsittelee kokonaislukumatriisien kuolevuusongelman ratkeavuutta. Kuolevuusongelmassa kysytään onko annettujen matriisien jokin tulo nollamatriisi. Ongelma todistettiin ratkeamattomaksi 3×3 matriiseille vuonna 1970, mutta 2×2 matriiseille ongelma on kiinnostuksesta huolimatta edelleenkin avoin.

Tutkielman pääpainona on 2×2 matriisien kuolevuusongelman kahden erikoistapauksen ratkeavaksi osoittaminen. Ensimmäisessä erikoistapauksessa rajoitutaan matriiseihin, joiden determinantti on 0 tai ± 1. Toisessa erikoistapauksessa tarkastellaan kahden matriisin kuolevuutta. Lisäksi tarkastellaan yleisesti, miten matriisijoukon koko vaikuttaa kuolevuusongelman ratkeavuuteen.

Asiasanat: ratkeavuus, ratkeamattomuus, matriisipuoliryhmät, lineaarialgebra.

Sisältö

1 Johdanto

Tämä tutkielma käsittelee algoritmista ratkeavuutta. Pääpainona on pienten kokonaislukumatriisien kuolevuusongelman ratkeavuus. Sanotaan, että matriisijoukko on kuoleva, jos nollamatriisi sisältyy joukon generoimaan puoliryhmään.

Lukijalta ei odoteta muita esitietoja kuin lineaarialgebran ja ryhmäteorian alkeita, sillä tarvittavat käsitteet ja lauseet käydään riittävän tarkasti läpi. On kuitenkin suotavaa, että lukija hallitsee algoritmista ajattelua.

Tämän tutkielman ensimmäisessä luvussa käydään tutkielman kannalta tarpeelliset perusteet läpi. Ensimmäisessä alaluvussa käydään läpi matriisialgebran tuloksia, joita käytetään tutkielman päätuloksien todistuksissa. Toisessa alaluvussa käydään läpi formaalisten kielten teoriaa, jossa tutustutaan äärellisiin automaatteihin ja rationaalisiin lausekkeisiin. Kolmannessa alaluvussa tarkastellaan äärellisiä automaatteja algebrallisesta näkökulmasta.

Toisessa luvussa tarkastellaan päätäntäongelmien ratkeavuutta. Ratkeamattomuudella tarkoitetaan, että ei voida muodostaa algoritmia, joka antaisi vastauksen kyseiselle ongelmalle. Ennen kuin voidaan puhua ratkeamattomuudesta, on määriteltävä tarkasti mitä algoritmilla tarkoitetaan. Tässä tutkielmassa algoritmin määritelmänä käytetään A. Turingin kehittämää Turingin konetta. Turingin koneita ei kuitenkaan konstruoida eksplisiittisesti, vaan algoritmit tyydytään esittämään sanallisesti. Churchin-Turingin teesin nojalla mielivaltainen algoritmi voidaan toteuttaa Turingin koneen avulla, joten epätarkatkin kuvaukset on mahdollista esittää myös tarkasti. Luvussa todistetaan, että niin kutsuttu pysähtymisongelma on ratkeamaton Turingin koneille. Tämä tarkoittaa sitä, että ei voida muodostaa algoritmia, joka vastaa pysähtyykö annettu Turingin kone tyhjällä syötteellä vai ei. Käyttämällä tätä tulosta todistetaan, että Postin vastaavuusongelma on myös ratkeamaton.

Kolmannessa luvussa tarkastellaan tutkielman pääaihetta eli matriisien kuolevuusongelmaa. Postin vastaavuusongelman avulla osoitetaan, että 3×3 kokonaislukumatriisien kuolevuus ei ole ratkeavaa. Tämän jälkeen tarkastellaan 2×2 kokonaislukumatriisien kuolevuusongelman kahta erikoistapausta,

ja osoitetaan, että ne ovat ratkeavia. Ensimmäisessä erikoistapauksessa annettujen matriisien determinantit ovat 0 tai ± 1 ja toisessa erikoistapauksessa annettu joukko koostuu vain kahdesta matriisista. Jälkimmäisessä tapauksessa todistetaan vahvempi tulos, jossa sallitaan, että annettu matriisipari on rationaalinen. Viimeisessä alaluvussa tarkastellaan $n \times n$ matriisien lukumäärän vaikutusta kuolevuusongelman ratkeavuuteen. Pienille matriiseille tarkkoja rajoja ei tunneta, vaan ongelma on edelleenkin auki. Vähintäin 21×21 matriiseille tarkat rajat ovat tiedossa. Tunnetut rajat perustuvat suurimmaksi osaksi 3×3 matriisien kuolevuuteen, sillä 2×2 matriisien kuolevuuden ratkeavuus on avoin ongelma.

Viimeisessä luvussa on yhteenveto tutkielman tuloksista sekä muutama aiheeseen liittyvä tulos.

2 Perusteet

Tässä luvussa esitetään tutkielmassa käytetyt merkinnät ja pohjataan päätuloksissa luvussa 4 käytettävää matriisiryhmien ja formaalisten kielten teoriaa. Ensimmäisessä alaluvussa tarkastellaan matriisien teoriaa ja todistetaan, että ryhmä $PSL_2(\mathbb{Z})$ on isomorfinen syklisten ryhmien C_2 ja C_3 vapaan tulon kanssa. Lisäksi todistetaan Jordanin normaalimuodon olemassaolo kompleksisille matriiseille. Toisessa alaluvussa tarkastellaan formaalisten kielten teoriaa, ja esitellään deterministiset äärelliset automaatit ja niitä koskevat sulkeumaominaisuudet. Viimeisessä alaluvussa tarkastellaan monoidiesityksiä äärellisten automaattien näkökulmasta.

Tässä tutkielmassa käytetään lukujoukoista seuraavanlaisia merkintöjä. Luonnollisten lukujen joukosta käytetään merkintää $\mathbb{N} = \{0, 1, 2, \ldots\}$. Kokonaislukujen joukosta käytetään merkintää $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ ja positiivisten kokonaislukujen joukosta $\mathbb{Z}_+ = \{1, 2, \ldots\}$. Rationaalilukujen joukosta käytetään merkintää $\mathbb{Q}$, reaalilukujen joukosta $\mathbb{R}$ ja kompleksilukujen joukosta $\mathbb{C}$.

Olkoon $f : X \to Y$ homomorfismi. Sanotaan, että f on *endomorfismi*, jos $X = Y$. Homomorfismi on injektio, jos kaikille $x, x' \in X$ on voimassa $f(x) \neq f(x')$, aina kun $x \neq x'$. Injektiivista homomorfismia sanotaan *upotukseksi* ja siitä käytetään merkintää $X \hookrightarrow Y$. Sanotaan, että homomorfismi on epimorfismi, jos se on surjektio eli jokaiselle $y \in Y$ on olemassa $x \in X$, jolle $f(x) = y$. Epimorfismista käytetään merkintää $X \twoheadrightarrow Y$. Jos homomorfismi f on sekä injektio, että surjektio, niin sanotaan, että se on *isomorfismi*.

2.1 Matriisiryhmistä

Käydään ensin tutkielmassa käytettyjä matriiseja koskevia perusmerkintöjä läpi. Kaikkien $n \times n$ matriisien joukosta yli lukurenkaan $\mathbb{K}$ käytetään merkintää $\mathcal{M}_n(\mathbb{K})$. Yleensä tarkastellaan joukkoa $\mathcal{M}_n(\mathbb{Z})$, jonka matriisit muodostavat monoidin tavallisen matriisikertolaskun suhteen. Kokoa $n \times n$ olevasta identiteettimatriisista käytetään merkintää I_n ja nollamatriisista $\mathcal{O}_n$. Jos matriisin koko on asiayhteydestä selvä, niin usein jätetään alaindeksi kirjoittamatta. *Yleinen lineaarinen ryhmä* $GL_2(\mathbb{Z})$ on kääntyvistä 2×2 ko-

konaislukumatriiseista koostuva ryhmä. Tavallisesti joukon $\mathbb{F}$ ollessa kunta, $GL_2(\mathbb{F})$ määritellään joukoksi, johon kuuluvat kaikki matriisit, joiden determinantti eroaa nollasta. Tässä tutkielmassa kuitenkin määritellään kyseinen joukko renkaan $\mathbb{Z}$ yli, jolloin se koostuu matriiseista, joiden determinantti on yksikkö eli ± 1. Ryhmän $GL_2(\mathbb{Z})$ aliryhmä on *erityinen lineaarinen ryhmä* $SL_2(\mathbb{Z})$ ja se sisältää kaikki matriisit, joiden determinantti on 1. Aliryhmän $SL_2(\mathbb{Z})$ tekijäryhmä on *projektiivinen erityinen lineaarinen ryhmä* $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{I, -I\}$. Siis

$$\begin{aligned} \mathcal{M}_n(\mathbb{K}) &= \{(a_{ij})_{n\times n} \mid a_{ij} \in \mathbb{K}, i, j \in \{1, \ldots, n\}\}, \\ GL_2(\mathbb{Z}) &= \{A \in \mathcal{M}_2(\mathbb{Z}) \mid \det(\mathrm{A}) = \pm 1\}, \\ SL_2(\mathbb{Z}) &= \{A \in GL_2(\mathbb{Z}) \mid \det(\mathrm{A}) = 1\}. \end{aligned}$$

Olkoon $A \in \mathcal{M}_n(\mathbb{K})$. Silloin endomorfismin $\varphi_A : \mathbb{R}^n \to \mathbb{R}^n$,

$$\varphi_A((x_1, \ldots, x_n)^T) = A(x_1, \ldots, x_n)^T$$

kuva on $\mathrm{Im}_A = \{A(x_1, \ldots, x_n)^T \mid (x_1, \ldots, x_n)^T \in \mathbb{R}^n\}$ ja ydin on $\mathrm{Ker}_A = \{(x_1, \ldots, x_n)^T \in \mathbb{R}^n \mid A(x_1, \ldots, x_n)^T = (0, \ldots, 0)^T\}$. Tällöin sanotaan, että Im_A ja Ker_A ovat matriisin A kuva ja ydin. Jos matriisin A aste on 1, niin sen ydin Ker_A ja kuva Im_A ovat yksiulotteisia aliavaruuksia.

Esimerkki 2.1. Olkoon

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}).$$

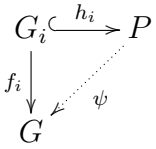
Nyt $\mathrm{Im}_A = \{(x + 3y)(1, 2)^T \mid x, y \in \mathbb{R}\}$ ja $\mathrm{Ker}_A = \{(x, y)^T \mid x = -3y\}$.

Seuraavaksi osoitetaan tekijäryhmän $PSL_2(\mathbb{Z})$ isomorfia kahden syklisen ryhmän vapaan tulon kanssa. Vapaasta tulosta voi lukea lisää esimerkiksi kirjoista [25] tai [23].

Määritelmä 2.1. Olkoot $G_1, G_2, \ldots, G_n$ ryhmiä. Ryhmä P on ryhmien $G_1, G_2, \ldots, G_n$ *vapaa tulo*, $P = G_1 * G_2 * \ldots * G_n$, jos se toteuttaa seuraavat ehdot:

(i) Ryhmä P sisältää ryhmien $G_1, G_2, \ldots, G_n$ isomorfiset kuvat. Siis on olemassa injektiiviset homomorfismit $h_i : G_i \hookrightarrow P$ kaikille $i = 1, \ldots, n$.

(ii) Olkoon G mielivaltainen ryhmä ja $f_i : G_i \to G$ homomorfismi kaikille $i = 1, \ldots, n$. On olemassa yksikäsitteinen homomorfismi $\psi : P \to G$ siten, että $\psi h_i = f_i$, kullekin $i = 1, \ldots, n$.



Jos P on ryhmien $G_1, G_2, \ldots, G_n$ vapaa tulo, niin ryhmiä $G_1, G_2, \ldots, G_n$ sanotaan vapaan tulon *vapaiksi tekijöiksi*.

Lause 2.2. *Syklisten ryhmien C_2 ja C_3 vapaa tulo on isomorfinen tekijäryhmän $PSL_2(\mathbb{Z})$ kanssa. Siis $PSL_2(\mathbb{Z}) \cong C_2 * C_3$.*

Todistus. Osoitetaan ensin, että matriisit

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

generoivat ryhmän $SL_2(\mathbb{Z})$. Matriisien A ja B generoima ryhmä $\langle A, B \rangle = H$ on selvästi ryhmän $SL_2(\mathbb{Z})$ aliryhmä, siis $H \leq SL_2(\mathbb{Z})$. Tehdään vastaoletus, että H on aito aliryhmä eli $SL_2(\mathbb{Z}) \setminus H \neq \emptyset$. Olkoon matriisi

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \setminus H,$$

missä $|a|+|c|$ on minimaalinen. Oletetaan ensin, että $a \neq 0$, $c \neq 0$ ja $|a| \geq |c|$. Nyt $AB = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ja

$$(AB)^k X = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + kc & b + kd \\ c & d \end{pmatrix} \notin H.$$

Luku k voidaan valita siten, että $|a+kc| < |a|$, jolloin $|a+kc|+|c| < |a|+|c|$, mikä on ristiriidassa matriisin X valinnan kanssa.

Oletetaan sitten, että $|a| < |c|$. Tällöin $BA = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ ja

$$(BA)^{-m}X = \begin{pmatrix} a & b \\ ma+c & mb+d \end{pmatrix} \notin H.$$

Nyt luku m voidaan valita siten, että $|ma+c| < |c|$, jolloin $|a| + |ma+c| < |a| + |c|$, mikä on jälleen ristiriidassa matriisin X valinnan kanssa.

Siis joko $a = 0$ tai $c = 0$. Jos $a = 0$, niin

$$X = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & d \end{pmatrix}.$$

Nyt $B^{-1} = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ ja

$$\begin{aligned} B^{-1}X &= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix} \\ &= \begin{pmatrix} -1 & -d-1 \\ 0 & -1 \end{pmatrix} = A^2(AB)^{-(d+1)} \end{aligned}$$

tai

$$\begin{aligned} B^{-1}X &= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix} \\ &= \begin{pmatrix} 1 & d-1 \\ 0 & 1 \end{pmatrix} = (AB)^{d-1}. \end{aligned}$$

Jos $c = 0$, niin $X = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$, jolloin $X = (AB)^b$ tai $X = A^2(AB)^{-b}$. Siispä $\langle A, B\rangle = SL_2(\mathbb{Z})$.

Osoitetaan sitten, että on olemassa isomorfismi ryhmästä $C_2 * C_3$ ryhmään $PSL_2(\mathbb{Z})$. Olkoon $h : \ SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z})$ luonnollinen homomorfismi ja merkitään $h(A) = \bar{A}$ ja $h(B) = \bar{B}$. Koska $A^2 = -I$ ja $B^3 = I$, on matriisien $\bar{A}$ ja $\bar{B}$ kertaluvuille voimassa $\mathrm{ord}(\bar{A}) = 2$ ja $\mathrm{ord}(\bar{B}) = 3$. Olkoot $\langle a\rangle = C_2$ ja $\langle b\rangle = C_3$ ja $G = \langle a\rangle * \langle b\rangle$. Vapaan tulon ominaisuuden (ii) nojalla homomorfismit $a \mapsto \bar{A}, b \mapsto \bar{B}$ määräävät surjektiivisen homomorfismin $\psi : G \to PSL_2(\mathbb{Z})$. Osoitetaan, että homomorfismin ψ ydin $\ker(\psi) = \{1\}$, mistä seuraa, että kuvaus ψ on haluttu isomorfismi.

Olkoon $y \in G$. Voidaan olettaa, että $y = b^j x a^k$, missä x on alkioiden ab, ab^{-1} epätyhjä tulo, $j \in \{-1, 0, 1\}$ ja $k \in \{0, 1\}$. Jos sallitaan, että termi x on tyhjä tulo, niin silloin $y = b^j a^k$ ja $y \in \ker(\psi)$ jos ja vain jos $j = 0 = k$. Merkitään

$$X = \psi(x) = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}.$$

Oletetaan ensin, että $j = 1$ ja $k = 1$. Nyt

$$\psi(y) = BXA = \begin{pmatrix} x_4 & -x_3 \\ -x_2 - x_4 & x_1 + x_3 \end{pmatrix},$$

mistä seuraa, että jos $y \in \ker(\psi)$, on matriisin X oltava muotoa $X = \left(\begin{smallmatrix} \pm 1 & \mp 1 \\ 0 & \pm 1 \end{smallmatrix}\right)$. Mutta tällöin $X = \mp B^{-1}A$, jolloin $y = 1$. Vastaavasti osoitetaan, että jos $j = -1$ ja $k = 1$, niin matriisi $X = BA$ ja $y = 1$.

Oletetaan sitten, että toinen luvuista i, j on 0. Nyt

$$(AB)^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \quad \text{ja} \quad (AB^{-1})^s = (-1)^s \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix},$$

kaikilla $r, s \geq 0$. Siis näiden matriisien epätyhjä tulo ei voi sisältää sekä positiivisia että negatiivisia alkioita ja siten matriisin X alkiot ovat joko kaikki ei-negatiivisia tai kaikki ei-positiivisia. Jotta $y \in \ker(\psi)$, matriisin X on oltava $\pm A$ tai $\pm B^{\pm 1}$, mutta tämä ei ole mahdollista.

Siis jos $y \in \ker(\psi)$, niin $y = 1$ ja homomorfismi ψ on injektio. Näin ollen $C_2 * C_3 \cong PSL_2(\mathbb{Z})$, mikä oli todistettava. □

Edellisestä lauseesta huomataan mielenkiintoinen ominaisuus. Nimittäin kahden äärellisen ryhmän vapaa tulo voi olla ääretön.

Matriisin $A \in \mathcal{M}_2(\mathbb{C})$ *pystyvektoriavaruutta* merkitään $P(A)$. Matriisit

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}_{k \times k}$$

ja $J_1(\lambda) = (\lambda)$ ovat *Jordanin lohkoja. Jordanin matriisi* J on matriisi, jonka päädiagonaalilla on Jordanin lohkoja. Siis

$$J = \begin{pmatrix} J_{i_1} & & 0 & \\ & J_{i_2} & & \\ & 0 & \ddots & \\ & & & J_{i_n} \end{pmatrix}.$$

Seuraava tulos on voimassa kaikille $n \times n$ matriiseille, mutta merkintöjen helpottamiseksi rajoitutaan 2×2 matriiseihin. Lauseen todistus $n \times n$ matriiseille löytyy artikkelista [31].

Lause 2.3. *Olkoon $A \in \mathcal{M}_2(\mathbb{C})$. On olemassa kääntyvä matriisi $P \in \mathcal{M}_2(\mathbb{C})$ siten, että*

$$P^{-1}AP = J \tag{1}$$

missä

$$J = \begin{pmatrix} J_1(\lambda_1) & 0 \\ 0 & J_1(\lambda_2) \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

tai $J = J_2(\lambda_1)$, ja λ_1 sekä λ_2 ovat matriisin A ominaisarvot.

Todistus. Olkoon

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Jos Jordanin matriisi J on ensimmäistä muotoa, silloin tulos on suoraviivainen. Nimittäin nyt matriisilla A on kaksi eri ominaisarvoa ja se on diagonalisoituva.

Oletetaan, että matriisi J on jälkimmäistä muotoa, jolloin $\lambda = \mathrm{tr}(A)/2 = \frac{a+d}{2}$ on matriisin A ainoa ominaisarvo. Olkoon P matriisi, jonka pystyrivit ovat $x_1 = (x_{11}, x_{12})^T$ ja $x_2 = (x_{21}, x_{22})^T$. Nyt sijoittamalla pystyvektorit yhtälöön (1) saadaan

$$\begin{aligned} A(x_1 \mid x_2) &= (x_1 \mid x_2)J = \begin{pmatrix} x_{11} & x_{21} \\ x_{12} & x_{22} \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \\ &= \begin{pmatrix} x_{11}\lambda & x_{11} + x_{21}\lambda \\ x_{12}\lambda & x_{12} + x_{22}\lambda \end{pmatrix} = (x_1\lambda \mid x_1 + x_2\lambda), \end{aligned}$$

eli yhtälö (1) on ekvivalentti yhtälöiden

$$\begin{aligned} Ax_1 &= \lambda x_1 \\ Ax_2 &= \lambda x_2 + x_1 \end{aligned}$$

kanssa. Merkitään $B = A - \lambda I$. Edellisistä yhtälöistä seuraa

$$Bx_2 = (A - \lambda I)x_2 = Ax_2 - \lambda x_2 = \lambda x_2 + x_1 - \lambda x_2 = x_1$$

ja

$$Bx_1 = (A - \lambda I)x_1 = Ax_1 - \lambda x_1 = \lambda x_1 - \lambda x_1 = 0.$$

Siis $x_1 \in \mathrm{Ker}_B \cap P(B)$ ja $x_2 \in \mathrm{Ker}_{B^2}$. Koska λ on matriisin A ominaisarvo, niin $\dim(\mathrm{Im}_B) < 2$ ja täten $\dim(\mathrm{Ker}_B) = 1$. Ominaisarvo λ on karakteristisen polynomin $(a - \lambda)(d - \lambda) - bc$ kaksinkertainen juuri, joten diskriminantti on 0. Siis $(a + d)^2 - 4ad + 4bc = (a - d)^2 + 4bc = 0$. Olkoon $(x, y)^T \in \mathbb{C}^2$. Nyt

$$\begin{aligned} (A - \lambda I)^2 \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} \frac{a-d}{2} & b \\ c & \frac{d-a}{2} \end{pmatrix}^2 \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{4}((a-d)^2 + 4bc) & 0 \\ 0 & \frac{1}{4}((a-d)^2 + 4bc) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \mathcal{O} \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Eli $(x, y)^T \in \mathrm{Ker}_{B^2}$ ja $\dim \mathrm{Ker}_{B^2} = 2$. Voidaan siis löytää lineaarisesti riippumattomat pystyvektorit x_1 ja x_2, joista muodostettu matriisi P on kääntyvä ja toteuttaa yhtälön (1). □

Jordanin normaalimuodosta voi lukee lisää kirjasta [1].

2.2 Säännöllisistä kielistä

Käydään ensin formaalisten kielten peruskäsitteitä läpi ennen kuin siirrytään tarkastelemaan säännöllisiä kieliä. Aiheeseen tutustumaton lukija voi löytää lisää esimerkkejä ja teoriaa luentomonisteesta [15] tai kirjasta [17].

Aakkosto Σ on epätyhjä joukko, jonka alkiot ovat *kirjaimia*. Aakkosto voi olla ääretön tai äärellinen, mutta tässä tutkielmassa aakkostot ovat aina

äärellisiä, ellei toisin mainita. *Sana* on äärellinen jono aakkoston kirjaimia ja *tyhjä sana* ε on sana, jossa ei ole yhtään kirjainta. Sanan w *pituus* $|w|$ on siinä esiintyvien kirjaimien lukumäärä ja sopimuksena tyhjän sanan ε pituus on 0. Kun $u = a_1a_2 \cdots a_n$ ja $w = b_1b_2 \cdots b_m$ ovat sanoja, joissa jokainen $a_i, b_j \in \Sigma$, niin binäärioperaatio *katenaatio* yhdistää sanat seuraavalla tavalla

$$u \cdot w = a_1a_2 \cdots a_n \cdot b_1b_2 \cdots b_m = a_1a_2 \cdots a_nb_1b_2 \cdots b_m.$$

Katenaatio on selvästi assosiatiivinen ja tyhjä sana ε on neutraalialkio. Kun sana w katenoidaan itsensä kanssa n kertaa, siitä käytetään merkintää $\underbrace{w \cdots w}_{n \text{ kpl}} = w^n$ ja sopimuksena $w^0 = \varepsilon$.

Formaalinen kieli on joukko sanoja kiinnitetyn aakkoston yli. Kieli voi olla äärellinen tai ääretön. Esimerkiksi

$$\begin{aligned}
&\{a, aa, ab\},\\
&\{a, aa, aaa, \ldots\} = \{a^n \mid n \geq 1\},\\
&\{ab, aabb, aaabbb, \ldots\} = \{a^nb^n \mid n \geq 1\},\\
&\{\varepsilon, a, b, aa, ab, ba, bb, aaa, \ldots\} = \Sigma^*,\\
&\{a, b, aa, ab, ba, bb, aaa, \ldots\} = \Sigma^+
\end{aligned}$$

ovat kieliä aakkoston $\Sigma = \{a, b\}$ yli. Näistä kaksi viimeistä ovat erityisen tärkeitä, toiseksi viimeinen on kaikkien sanojen joukko Σ^* ja viimeinen on kaikkien epätyhjien sanojen joukko $\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$. Joukko Σ^* (vast. Σ^+) ja katenaatio muodostavat vapaan monoidin $(\Sigma^*, \cdot)$ (vast. puoliryhmän $(\Sigma^+, \cdot)$), jonka generaattorijoukko on Σ. Lisää monoideista voi lukea luvussa 2.3.

Määritellään seuraavaksi kielille joitakin operaatioita. Olkoot L, L_1 ja L_2 kieliä aakkoston Σ yli. Kielten L_1 ja L_2 katenaatio on kieli

$$L_1L_2 = \{uv \mid u \in L_1, v \in L_2\}.$$

Jokaiselle $n \geq 0$ määritetään kieli L^n, jossa kieli L on katenoituna itsensä kanssa n kertaa. Toisin sanoen

$$\begin{aligned}
L^0 &= \{\varepsilon\},\\
L^n &= L^{n-1}L \text{ , kaikille } n \geq 1.
\end{aligned}$$

Kielen L *Kleenen sulkeuma* on

$$L^* = \bigcup_{i=0}^{\infty} L^i$$

ja *positiivinen sulkeuma* on

$$L^+ = \bigcup_{i=1}^{\infty} L^i.$$

Selvästi $L^* = L^+ \cup \{\varepsilon\}$ ja $L^+ = LL^*$. Lisäksi $L^* = L^+$ jos ja vain jos $\varepsilon \in L$.

Siirrytään seuraavaksi säännöllisten kielten teoriaan. *Rationaaliset* (tai säännölliset) kielet ovat perhe formaalisia kieliä, jotka voidaan määrittää *rationaalisilla lausekkeilla* tai *äärellisillä automaateilla*. Myöhemmin todistettavan Kleenen lauseen nojalla rationaaliset lausekkeet ja äärelliset automaatit määrittävät tarkalleen samat kielet. Rationaaliset kielet voidaan esittää myös Chomskin hierarkian tyyppiä 3 olevan kieliopin avulla, mutta sitä ei käydä tässä tutkielmassa läpi.

Epädeterminististinen äärellinen automaatti NFA on automaatti, joka tarkistaa kuuluuko sana kieleen vai ei. Tätä varten NFA käy syötteen läpi kirjain kerralla ja jokaisen kirjaimen kohdalla automaatin tila muuttuu tai pysyy ennallaan riippuen sen hetken tilasta ja kirjaimesta. Syöte hyväksytään, jos viimeisen kirjaimen jälkeen automaatti on hyväksyvässä tilassa. Tarkemmin sanottuna, NFA on viisikko $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$, missä:

(i) Q on äärellinen joukko tiloja. Jokaisella hetkellä automaatti on jossain tilassa $q \in Q$.

(ii) Σ on syötteen aakkosto. Automaatti osaa käsitellä vain sanoja yli aakkoston Σ.

(iii) δ on siirtymäfunktio. Siirtymäfunktio kertoo miten automaatin tila muuttuu. Hieman tarkemmin,

$$\delta : Q \times (\Sigma \cup \{\varepsilon\}) \to 2^Q$$

siten, että $\delta(q, a)$ on joukko tiloja p, joihin automaatti voi siirtyä tilasta q syötteellä a ja $\delta(q, \varepsilon)$ on joukko tiloja p, joihin automaatti voi siirtyä tilasta q lukematta syötettä. Erityisesti $q \in \delta(q, \varepsilon)$.

(iv) q_0 on alkutila, jossa automaatti on ennen kuin syötettä on luettu.

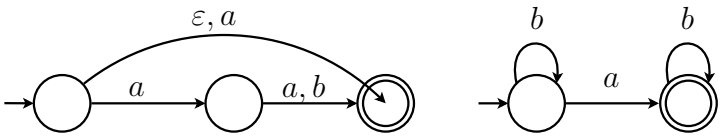
(v) $F \subseteq Q$ on joukko lopputiloja.

Syötteellä w automaatti aloittaa toiminnan alkutilasta q_0. Tämän jälkeen automaatti vaihtaa tiloja siirtymäfunktion mukaisesti. Jos automaatti käyttää siirrosta $\delta(q, a)$, siirtyy se syötteen seuraavaan kirjaimeen. Jos automaatti on lopputilassa $f \in F$ joillain siirtymäfunktion määrittämillä tilanmuutoksilla, kun koko syöte on luettu, niin automaatti hyväksyy syötteen. Jos millään siirtymäfunktion määrittämillä tilanmuutoksilla automaatti ei ole lopputilassa $f \in F$, kun koko syöte on luettu, niin automaatti hylkää syötteen.

Kieli, joka koostuu kaikista sanoista, jotka automaatti $\mathcal{A}$ hyväksyy on $L(\mathcal{A})$.

Automaatti voidaan esittää suunnattuna graafina, jossa solmut vastaavat tiloja ja kaaret siirroksia eri syötteillä. Siis kun $a \in \Sigma \cup \{\varepsilon\}$, siirros $p \in \delta(q, a)$ on ilmaistu kaarena solmusta q solmuun p ja kaaren leima on a. Lisäksi lopputilat on merkattu tuplaympyröillä ja alkutila on osoitettu lyhyellä nuolella. Automaatti hyväksyy sanan w jos ja vain jos on olemassa polku alkutilasta lopputilaan, minkä leima on w.

Esimerkki 2.2. Kieliä $L_1 = \{\varepsilon, a, aa, ab\}$ ja $L_2 = \{b^n a b^m \mid n, m \geq 0\}$ vastaavat automaatit ovat kuvassa 1.



Kuva 1: Kieliä L_1 ja L_2 vastaavat automaatit.

Siirtymäfunktion määritelmän nojalla, jokaisesta solmusta voi lähteä useampi kaari samalla kirjaimella tai ε–siirroksella. Jos siirtymäfunktiossa jokaista tilaa kohti on korkeintaan yksi siirros kutakin kirjainta kohti, niin automaatti on *deterministinen äärellinen automaatti* eli DFA. Erityisesti deterministisessä äärellisessä automaatissa ei ole ε–siirroksia.

Lause 2.4. *Olkoon L kieli. Silloin on olemassa DFA $\mathcal{A}_1$, joka hyväksyy kielen L jos ja vain jos on olemassa NFA $\mathcal{A}_2$, joka hyväksyy kielen L.*

Todistus. Toiseen suuntaan väite on ilmeinen, sillä DFA on epädeterminististen äärellisen automaatin erikoistapaus. Oletetaan sitten, että on olemassa NFA $\mathcal{A}$, joka hyväksyy kielen L. Olkoon NFA $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$, joka hyväksyy kielen L. Muodostetaan joukot $E_i(q)$ induktiivisesti. Määritellään $E_1(q) = \delta(q, \varepsilon)$ ja $E_i(q)$, kun $i \geq 2$, on $E_i(q) = \{r \mid r \in \delta(p, \varepsilon),\ p \in E_{i-1}(q)\}$. Nyt joukko $E(q) = \bigcup_{i \in \mathbb{N}} E_i(q)$ on ne tilat, joihin pääsee tilasta q pelkällä ε–siirroksella. Määritellään vielä osajoukolle $S \subseteq Q$ joukko $E(S) = \bigcup_{q \in S} E(q)$.

Muodostetaan DFA $\mathcal{A}' = (Q', \Sigma, \delta', q_0', F')$, missä $Q' = 2^Q$, $q_0' = E(q_0)$, $F' = \{S \subseteq Q \mid E(S) \cap F \neq \emptyset\}$ ja siirtymäfunktio

$$\delta'(S, a) = \bigcup_{q \in S} \{\delta(p, a) \mid p \in E(q)\},$$

joka on määritelty kaikille $S \subseteq Q$ ja $a \in \Sigma$. Tilasta S on määritelty vain yksi siirros kullakin kirjaimella $a \in \Sigma$ eikä ε–siirroksia ole määritelty. Riittää siis osoittaa, että siirtymäfunktiot vastaavat toisiaan. Eli osoitetaan induktiolla syöteen w pituuden suhteen, että automaatin $\mathcal{A}'$ siirtymäfunktiolla δ' on voimassa

$$\delta'(q_0', w) = \delta(q_0, w),$$

kun automaatin $\mathcal{A}'$ tila samaistetaan vastaavan joukon kanssa. Väite on voimassa, kun $w = \varepsilon$, sillä

$$\delta'(q_0', \varepsilon) = q_0' = E(q_0) = \delta(q_0, \varepsilon).$$

Oletetaan, että väite pätee kaikille korkeintaan pituutta l oleville syötteille. Olkoon $|w| = l + 1$. Silloin $w = ua$, jollekin l pituiselle sanalle u ja kirjaimelle $a \in \Sigma$. Induktio-oletuksen nojalla $\delta'(q_0', u) = \delta(q_0, u)$. Merkitään $S = \delta'(q_0', u) = \delta(q_0, u)$. Nyt

$$\delta'(q_0', ua) = \delta'(S, a) = \bigcup_{q \in S} \{\delta(p, a) \mid p \in E(q)\} = \delta(q_0, ua).$$

Automaatti $\mathcal{A}'$ hyväksyy sanan w jos ja vain jos joukko $\delta'(q_0, w)$ sisältää alkion joukosta $E(F)$. Tila $\delta(q_0, w)$ on tässä joukossa ja automaatti $\mathcal{A}$ hyväksyy sanan w jos ja vain jos $\delta(q_0, w)$ on lopputila. Siis automaatit $\mathcal{A}$ ja $\mathcal{A}'$ hyväksyvät saman kielen L, mikä oli todistettava. □

Edellisen lauseen nojalla voidaan samaistaa epädeterministiset ja deterministiset äärelliset automaatit. On kuitenkin syytä huomata, että deterministisessä äärellisessä automaatissa on exponentiaalinen määrä tiloja verrattuna sitä vastavaan epädeterministiseen automaattiin. Luentomonisteessa [15] on todistettu sama tulos esittämällä muunnokselle konkreettisen algoritmin.

Voidaan olettaa, että epädeterministisessä automaatissa on vain yksi lopputila. Nimittäin automaatista $\mathcal{A}$ muodostetaan automaatti $\mathcal{A}'$ lisäämällä ε-siirrokset jokaisesta alkuperäisestä lopputilasta uuteen lopputilaan f_0 ja muuttamalla alkuperäiset lopputilat tavallisiksi tiloiksi. Selvästi $L(\mathcal{A}) = L(\mathcal{A}')$ ja automaatissa $\mathcal{A}'$ on vain yksi lopputila.

Rationaaliset lausekkeet ovat toinen tapa ilmaista rationaalisia kieliä. Toisin kuin automaatit, jotka hyväksyvät kieleen kuuluvat sanat, rationaaliset lausekkeet kuvaavat kieltä. Jos r on rationaalinen lauseke, niin $L(r)$ on sitä vastaava kieli. Rationaaliset lausekkeet määritellään rekursiivisesti.

(i) Lauseke $\emptyset$ vastaa tyhjää kieltä.

(ii) Lauseke ε vastaa kieltä $\{\varepsilon\}$.

(iii) Jokaiselle $a \in \Sigma$, lauseke a vastaa kieltä $\{a\}$.

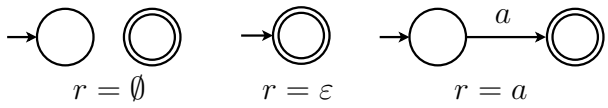
(iv) Kun r ja s ovat rationaalisia lausekkeita, niin $r + s$, rs ja r^* ovat rationaalisia lausekkeita. Tällöin

$$\begin{aligned} L(r+s) &= L(r) \cup L(s), \\ L(rs) &= L(r)L(s), \\ L(r^*) &= L(r)^*. \end{aligned}$$

Usein samaistetaan rationaalinen lauseke r ja sitä vastaava kieli $L(r)$ ja sanotaan, että rationaalinen lauseke r määrittää kielen $L(r)$. Rationaalisesta lausekkeesta r yli aakkoston $\{a_1, \ldots, a_n\}$ voidaan myös käyttää merkintää $\mathcal{R}(a_1, \ldots, a_n)$.

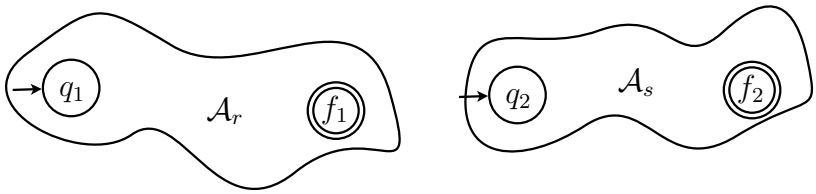
Lause 2.5 (Kleene)**.** *Rationaalisen lausekkeen määrittämä kieli on rationaalinen jos ja vain jos on olemassa äärellinen automaatti, joka hyväksyy saman kielen.*

Todistus. Oletetaan ensin vasen puoli. Olkoon L rationaalisen lausekkeen r määrittämä kieli. Muodostetaan nyt rationaalista lauseketta r vastaava äärellinen automaatti. Väite todistetaan induktiolla rationaalisen lausekkeen operaatioiden lukumäärän suhteen. Rationaalisia lausekkeita $\emptyset$, ε ja $a \in \Sigma$ vastaavat automaatit ovat kuvassa 2.



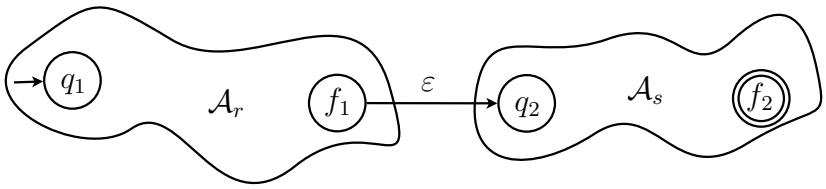
Kuva 2: Atomaarisia rationaalilausekkeita vastaavat automaatit.

Olkoot r ja s rationaalisia lausekkeita, joissa on korkeintaan $n-1$ operaatiota ja $\mathcal{A}_r$ ja $\mathcal{A}_s$ niitä vastaavat automaatit, joiden tilajoukot voidaan olettaa erillisiksi.



Kuva 3: Automaatit $\mathcal{A}_r$ ja $\mathcal{A}_s$.

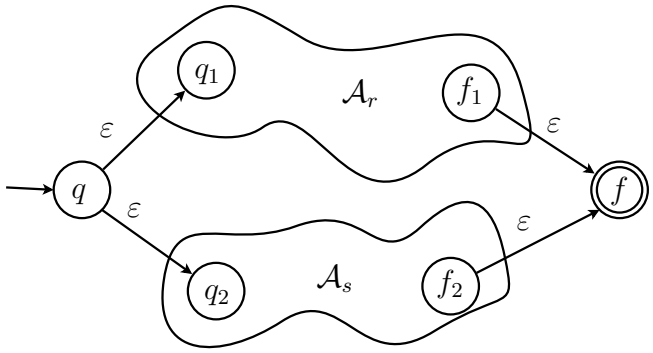
Lauseketta rs vastaavassa automaatissa alkutilana on q_1 ja lopputilana on f_2. Lisäksi siinä on ε–siirros automaatin $\mathcal{A}_r$ lopputilasta f_1 automaatin $\mathcal{A}_s$ alkutilaan q_2. Tämä automaatti on esitetty kuvassa 4.



Kuva 4: Rationaalista lauseketta rs vastaava automaatti.

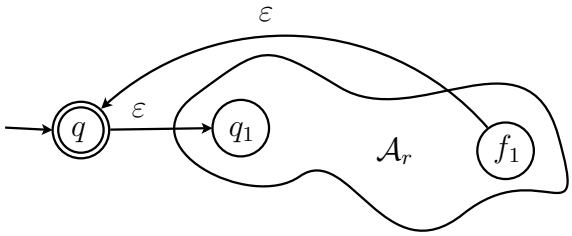
Lauseketta $r + s$ vastaavassa automaatissa on alkutila q, josta ε–siirroksella pääsee tiloihin q_1 ja q_2 ja automaattien $\mathcal{A}_r$ ja $\mathcal{A}_s$ lopputiloista

f_1 ja f_2 päästään ε–siirroksella uuteen lopputilaan f. Tämä automaatti on esitetty kuvassa 5.



Kuva 5: Rationaalista lauseketta $r + s$ vastaava automaatti.

Lauseketta r^* vastaavassa automaatissa on uusi tila q, joka on sekä alkutila, että lopputila. Tilasta q on ε–siirros tilaan q_1 ja tilasta f_1 on ε–siirros tilaan q. Tämä automaatti on esitetty kuvassa 6.



Kuva 6: Rationaalista lauseketta r^* vastaava automaatti.

Toiseen suuntaan väite todistetaan induktiolla automaatin siirrosten lukumäärän suhteen. Jos automaatissa on 0 siirrosta, niin sitä vastaava rationaalinen lauseke on $\emptyset$ tai ε, riippuen siitä onko $q_0 \in F$. Oletetaan, että väite on tosi kaikille automaateille, joissa on $n - 1$ siirrosta jollain $n \geq 1$. Olkoon $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ automaatti, jossa on n siirrosta. Kiinnitetään $p \in Q$ ja valitaan mielivaltainen siirros $q \in \delta(p, a)$. Tämä siirros on olemassa, sillä

$n > 0$. Muodostetaan uudet automaatit

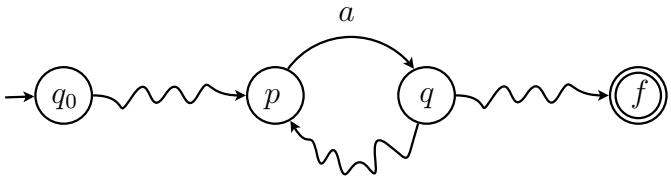
$$\begin{aligned}
\mathcal{A}_1 &= (Q, \Sigma, \delta', q_0, F), \\
\mathcal{A}_2 &= (Q, \Sigma, \delta', q_0, \{p\}), \\
\mathcal{A}_3 &= (Q, \Sigma, \delta', q, \{p\}), \\
\mathcal{A}_4 &= (Q, \Sigma, \delta', q, F),
\end{aligned}$$

missä δ' sisältää samat siirroksen kuin δ, lukuunottamatta siirrosta $q \in \delta(p, a)$. Merkitään $L_i = L(\mathcal{A}_i)$, missä $i = 1, \ldots, 4$. Konstruktioidensa takia automaateissa $\mathcal{A}_i$ on $n-1$ siirrosta, joten induktio-oletuksen nojalla kutakin niistä vastaa jokin rationaalinen lauseke. Osoitetaan, että

$$L(\mathcal{A}) = L_1 + (L_2a)(L_3a)^*L_4.$$

Selvästi $L_1 \subseteq L$, sillä kieli L_1 koostuu tarkalleen niistä sanoista, jotka $\mathcal{A}$ hyväksyy ja joissa ei käytetä siirrosta $q \in \delta(p, a)$. Olkoon $w \in (L_2a)(L_3a)^*L_4$. Automaatissa $\mathcal{A}$ on polut kaikille sanoille, jotka automaatit $\mathcal{A}_2$, $\mathcal{A}_3$ ja $\mathcal{A}_4$ hyväksyvät, sillä δ' oli määritelty siirtymäfunktion δ avulla. Käyttämällä sääntöä $p \xrightarrow{a} q$ saadaan polku automaatin $\mathcal{A}$ alkutilasta lopputilaan. Näin ollen myös $(L_2a)(L_3a)L_4 \subseteq L_{\mathcal{A}}$.

Olkoon $x \in L$. Jos sanan x käsittelyssä ei käytetä sääntöä $p \xrightarrow{a} q$, niin silloin $x \in L_1$. Muutoin sana x voidaan jakaa tekijöihin, joiden käsittelyssä ei käytetä sääntöä $p \xrightarrow{a} q$, $x = (ua)(v_1a)\cdots(v_na)w$. Selvästi $u \in L_2$, $v_i \in L_3$ kaikilla indekseillä $i = 1, \ldots, n$ ja $w \in L_4$, jolloin sana $x \in (L_2a)(L_3a)^*L_4$.



Kuva 7: Automaatti $\mathcal{A}$.

Siis rationaaliset lausekkeet ja äärelliset automaatit määräävät täsmälleen samat kielet. □

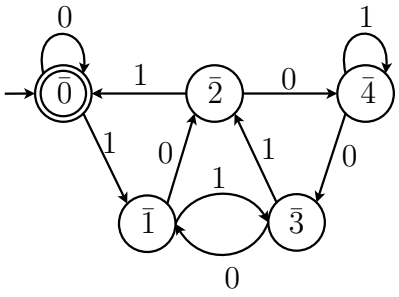
Edellisen lauseen todistus ei antanut algoritmista tapaa muodostaa rationaalista lauseketta äärellisestä automaatista. Aiheesta kiinnostunut lukija löytää algoritmisen todistuksen luentomonisteesta [15] tai kirjasta [17].

Esimerkki 2.3. Kun aakkosto on $\{0,1\}$, voidaan ajatella että sana $w \in \{0,1\}^*$ on binääriluku, jossa vähemmän merkitsevä numero on oikealla. Tällöin viidellä jaolliset binääriluvut muodostavat säännöllisen kielen. Olkoon

$$L_5 = \{w \in \{0,1\}^* \mid w \text{ on binääriluku, joka on jaollinen viidellä}\}.$$

Sitä vastaava automaatti on kuvassa 8. Tilat vastaavat jakojäännöksiä modulo 5 ja siirrokset $\delta(q,i) = p$ vastaavat laskua $2q + i = p \mod 5$ kaikilla $p, q \in Q$. Kielen L_5 määrittävä rationaalinen lauseke on

$$\mathcal{R}(0,1) = (0 + 101 + 1(1 + 001^*0)(101^*0 + 0(1 + 001^*0))^*(11 + 001))^*.$$



Kuva 8: Kieltä L_5 vastaava automaatti.

Määritelmänsä nojalla rationaaliset kielet ovat suljettuja unionin ja katenaation suhteen. Seuraavaksi osoitetaan, että kahden rationaalisen kielen leikkaus on myös rationaalinen kieli.

Lemma 2.6. *Olkoot L_1 ja L_2 rationaalisia kieliä aakkoston Σ yli. Silloin*

(i) $\overline{L_1} = \{w \in \Sigma^* \mid w \notin L_1\}$ *on rationaalinen kieli,*

(ii) $L_1 \cap L_2$ *on rationaalinen kieli.*

Todistus. Olkoon $\mathcal{A}$ deterministinen äärellinen automaatti, joka hyväksyy kielen L_1. Sana w vie automaatin tilaan q ja sana hyväksytään jos ja vain jos tila q on lopputila. Muutetaan automaatin lopputilat tavallisiksi tiloiksi ja päinvastoin. Näin muodostettu automaatti hyväksyy sanan jos ja vain jos alkuperäinen automaatti ei hyväksynyt sitä. Siis on muodostettu automaatti, joka hyväksyy kielen $\overline{L_1}$ sanat.

De Morganin lain mukaan $L_1 \cap L_2 = \overline{\overline{L_1} \cup \overline{L_2}}$. Koska L_1 ja L_2 ovat rationaalisia, niin edellisen kohdan nojalla myös $\overline{L_1}$ ja $\overline{L_2}$ ovat rationaalisia. Siispä myös $\overline{L_1} \cup \overline{L_2}$ ja $\overline{\overline{L_1} \cup \overline{L_2}}$ ovat rationaalisia. □

2.3 Monoidiesityksistä

Tässä alaluvussa käydään monoidiesitysteoriaa läpi ja osoitetaan, että äärellisen automaatin syötefunktio on vapaan monoidin Σ^* kongruenssi. Monoidiesityksistä voi lukea lisää luentomonisteesta [14] ja syötemonoideista kirjasta [2].

Monoidi $(M, \cdot)$ on algebrallinen rakenne, joka on suljettu assosiatiivisen binäärioperaation $\cdot$ suhteen. Lisäksi monoidissa on binäärioperaation neutraalialkio. Siis monoidi on neutraalialkiolla varustettu puoliryhmä.

Määritelmä 2.7. Ekvivalenssirelaatio $\equiv$ on monodin M *kongruenssi*, jos kaikille $x, y, z \in M$ ehdosta $x \equiv y$ seuraa $(zx) \equiv (zy)$ ja $(xz) \equiv (yz)$.

Olkoon M puoliryhmä. Osajoukko $1_M \notin X \subseteq M$ *generoi monoidin* M *vapaasti*, jos $X \cup \{1_M\}$ generoi monoidin M ja jokainen kuvaus α_0 joukosta X monoidiin P voidaan laajentaa homomorfismiksi $\alpha : M \to P$, jonka rajoittuma $\alpha|_X = \alpha_0$ ja $\alpha(1_M) = 1_P$. Sanotaan, että monoidi on *vapaa*, jos joku osajoukko generoi sen vapaasti.

Lause 2.8. *Olkoon M monoidi. On olemassa äärellinen tai ääretön aakkosto Σ ja epimorfismi $\psi : \Sigma^* \twoheadrightarrow M$.*

Todistus. Olkoon X monoidin M generoiva joukko ja olkoon Σ aakkosto, jonka koko on $|X|$. Olkoon $\psi_0 : \Sigma^* \to X$ bijektiivinen kuvaus. Koska Σ^* on vapaa, kuvaus ψ_0 voidaan laajentaa homomorfismiksi $\psi : \Sigma^* \to M$. Tämä

homomorfismi on surjektiivinen, sillä joukko $X \cup \{1_M\}$ generoi monoidin M. □

Seuraus 2.9. *Jokainen monoidi M on vapaan monoidin tekijämonoidi.*

Todistus. Edellisen lauseen nojalla on olemassa epimorfismi $\psi : \Sigma^* \twoheadrightarrow M$. Isomorfialauseen nojalla

$$M \cong \Sigma^* / \ker(\psi).$$

□

Olkoon M monoidi. Silloin

$$M = \langle a_1, a_2, \ldots \mid u_i = v_i (i \in I) \rangle \text{ tai } M = \langle \Sigma \mid R \rangle$$

on monoidin M *esitys*, jos $\ker(\psi)$, missä ψ on lauseen 2.8 epimorfismi, on sanamonoidin Σ^* pienin kongruenssi, joka sisältää relaation R. Siis monoidin generaattorijoukko on $\Sigma = \{a_1, a_2, \ldots\}$ ja $u_i = v_i (i \in I)$ on joukko relaatioita sanoille $u_i, v_i \in \Sigma^*$. Esityksessä voi olla muotoa $u = 1$ olevia relaatiota, mikä tarkoittaa, että sana u voidaan lisätä sanan keskelle tai se voidaan pyyhkiä sanasta.

Nyt sanamonoidin avulla voidaan antaa vaihtoehtoinen määritelmä kongruenssille. Olkoot $u, v \in \Sigma^*$. Merkitään $u =_R v$ monoidissa M, jos $u = xu_iy$ ja $v = xv_iy$, joillain sanoilla $x, y \in \Sigma^*$ ja relaatiolla $u_i = v_i$ joukossa R. Edelleen, sanat $u, v \in \Sigma^*$ ovat ekvivalentit monoidissa M, jota merkitään $u = v$, jos on olemassa äärellinen jono $u = u_1, u_2, \ldots, u_n = v$, missä $u_i =_R u_{i+1}$ jokaisella $i = 1, 2, \ldots, n-1$.

Sanotaan, että monoidi M on *äärellisesti esitetty*, jos sekä generaattorijoukko Σ että relaatioiden joukko R ovat äärellisiä.

Koska jokainen ryhmä on monoidi, ryhmälle $G = \{1, g_1, g_2, \ldots\}$ saadaan esitys

$$\left\langle g_1, g_2 \ldots \mid g_i^{\mathrm{ord}(g_i)} = 1, g_i g_j = g_k (i, j \in I) \right\rangle,$$

jossa $\mathrm{ord}(g)$ on alkion g kertaluku ja $g_i g_j = g_k$ ryhmässä G.

Tarkastellaan syklisten ryhmien vapaan tulon esitystä.

Lemma 2.10. *Olkoon* $G \cong C_{p_1} * C_{p_2} * \ldots * C_{p_n}$. *Merkitään* $\langle c_i \rangle = C_{p_i}$ *kaikille* $i = 1, 2, \ldots, n$. *Tällöin ryhmällä* G *on äärellinen esitys*

$$\langle c_1, c_2, \ldots, c_n \mid c_1^{p_1} = c_2^{p_2} = \ldots = c_n^{p_n} = 1 \rangle .$$

Todistus. Olkoon $G \cong C_{p_1} * C_{p_2} * \ldots * C_{p_n}$. Kaikilla $i = 1, \ldots, n$ vapailla tekijöillä C_i on esitys $\langle c_i \mid c_i^{p_i} = 1 \rangle$. Vapaan tulon määritelmän nojalla ryhmä G sisältää ryhmien C_i isomorfiset kuvat. Joten ryhmän G esityksen generaattorijoukossa on oltava jokaisen ryhmän C_{p_i} generaattori. Samoin jokaisen relaation $c_i^{p_i}$ on oltava ryhmän G relaatioiden joukossa, sillä muuten ryhmän C_i isomorfinen kuva ei sisältyisi ryhmään G. □

Edellinen lemma pätee yleisemminkin. Olkoon $G = G_1 * G_2 * \ldots * G_n$, jossa $G_i = \langle S_i \mid R_i \rangle$ kaikilla $i = 1, \ldots, n$. Silloin ryhmällä G on esitys $\langle S_1 \cup S_2 \cup \ldots \cup S_n \mid R_1 \cup R_2 \cup \ldots \cup R_n \rangle$. Vapaan tulon esityksistä voi lukea lisää kirjasta [18].

Palataan takaisin deterministisiin äärellisiin automaatteihin. Siirtymäfunktion δ sijaan tarkastellaan *syötefunktioita* $\delta_a : Q \to Q$, jotka kuvaavat tilan muutosta tietyllä syötteellä. Siis $\delta_a(q) = q'$ jos ja vain jos $\delta(q, a) = q'$. Syötefunktio voidaan myös määritellä luonnollisella tavalla epädeterministisille automaateille, mutta tässä tarkastelussa sille ei ole tarvetta.

Esimerkki 2.4. Esimerkin 2.2 kieltä $L_2 = \{b^n a b^m \mid n, m \geq 0\}$ vastaavan deterministisen automaatin syötefunktio on $\delta_a(q_0) = f$, $\delta_b(q_0) = q_0$ ja $\delta_b(f) = f$, kun q_0 on alkutila ja f on lopputila.

Syötefunktio δ yleistyy mielivaltaisille syötejonoille luonnollisella tavalla: kun $w = au$, silloin $\delta_w(q) = \delta_u(\delta_a(q))$. Vaikka erilaisia syötejonoja on ääretön määrä, nimittäin $|\Sigma^*|$ verran, erilaisia syötefunktioita on kuitenkin vain äärellinen määrä, sillä ne ovat kuvauksia äärellisestä joukosta Q äärelliseen joukkoon. Tätä tarkastellaan tarkemmin seuraavassa lemmassa.

Lemma 2.11. *Olkoot* $\mathcal{A}$ *deterministinen äärellinen automaatti ja* $u, v \in \Sigma^*$. *Silloin relaatio* $\equiv$ *säännöllä* $u \equiv v$ *jos ja vain jos* $\delta_u(q) = \delta_v(q)$ *kaikilla tiloilla* $q \in Q$ *on joukon* Σ^* *ekvivalenssirelaatio.*

Todistus. Relaatio $\equiv$ on refleksiivinen, sillä $\delta_u(q) = \delta_u(q)$ kaikilla $q \in Q$ ja $u \in \Sigma^*$, jolloin $u \equiv u$ kaikilla $u \in \Sigma^*$. Jos $u \equiv v$ ja $v \equiv w$, joillain $u, v, w \in \Sigma^*$, niin $\delta_u(q) = \delta_v(q)$ ja $\delta_v(q) = \delta_w(q)$ kaikilla $q \in Q$, jolloin $\delta_u(q) = \delta_w(q)$. Eli relaatio $\equiv$ on transitiivinen. Se on lisäksi symmetrinen, sillä jos $u \equiv v$, niin $\delta_u(q) = \delta_v(q)$ kaikilla $q \in Q$ ja $v \equiv u$. Siispä relaatio $\equiv$ on ekvivalenssirelaatio. □

Koska $\equiv$ on ekvivalenssirelaatio, se partitioi joukon Σ^* ekvivalenssiluokkiin $[u]$. Kaikkien sanojen joukko Σ^* on vapaa monoidi, joten seuraavaksi tarkastellaan miten sen rakenne muuttuu partitioinnin jälkeen.

Lause 2.12. *Olkoot $\mathcal{A}$ deterministinen äärellinen automaatti yli aakkoston Σ ja $\equiv$ ekvivalenssirelaatio joukossa Σ^*, jonka syötefunktio määrittää. Olkoon I^ε kaikkien relaation $\equiv$ ekvivalenssiluokkien joukko. Kun määritellään ekvivalenssiluokille tulo $[u][v] = [uv]$ kaikille $[u], [v] \in I^\varepsilon$, niin I^ε on monoidi.*

Todistus. Osoitetaan ensin, että tulo on hyvinmääritelty funktio. Olkoot $u' \in [u]$ ja $v' \in [v]$. Nyt ekvivalenssiluokan määritelmän nojalla $u' \equiv u, v' \equiv v$ ja siten $\delta_{u'}(q) = \delta_u(q), \delta_{v'}(q) = \delta_v(q)$ kaikilla $q \in Q$. Osoitetaan, että $[u'][v'] = [u'v'] = [uv]$. Nyt jokaiselle $q \in Q$ pätee

$$\delta_{u'v'}(q) = \delta_{v'}(\delta_{u'}(q)) = \delta_v(\delta_u(q)) = \delta_{uv}(q),$$

sillä $u' \equiv u$ ja $v' \equiv v$. Siispä $\delta_{u'v'} = \delta_{uv}$. Joukko I^ε on suljettu, sillä ekvivalenssiluokkien tulo on ekvivalenssiluokka, johon edustajien katenaatio kuuluu. Joukko on selvästi assosiatiivinen, nimittäin olkoot $[u], [v], [w] \in I^\varepsilon$. Silloin

$$([u][v])[w] = [uv][w] = [uvw] = [u][vw] = [u]([v][w]).$$

Ykkösalkiona toimii ekvivalenssiluokka $[\varepsilon]$. Nimittäin olkoon $[u] \in I^\varepsilon$, silloin

$$[u][\varepsilon] = [u\varepsilon] = [u]$$

ja

$$[\varepsilon][u] = [\varepsilon u] = [u].$$

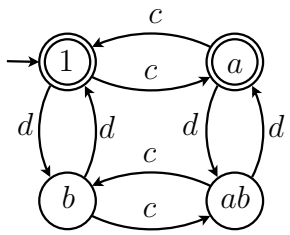
Siis I^ε on monoidi, mikä oli todistettava. □

Edellisen lauseen nojalla ekvivalenssirelaatio $\equiv$ on vapaan monoidin Σ^* kongruenssi. Kun $\mathcal{A}$ on DFA, niin silloin sanotaan, että $I^\varepsilon = \Sigma^*/\equiv$ on automaatin $\mathcal{A}$ *syötemonoidi* ja $I = \Sigma^+/\equiv$ on *syötepuoliryhmä*. Koska ekvivalenssiluokkaan $[\varepsilon]$ voi sisältyä muitakin sanoja kuin tyhjä sana ε, myös I voi olla monoidi.

Olkoon M äärellisesti esitetty monoidi, jonka generaattorijoukko on Σ. Sen *rationaalinen osajoukko* H on syötemonoidi, joka on monoidin M osajoukko. Toisin sanoen se on määritelty deterministisen äärellisen automaatin $\mathcal{A}$ avulla. Jokainen sana yli aakkoston Σ, jonka $\mathcal{A}$ hyväksyy, on osajoukon H alkion edustaja ja jokainen H:n alkio on edustettu jollain sanalla, jonka automaatti $\mathcal{A}$ hyväksyy.

Rationaalinen osajoukko voidaan määrittää ekvivalentisti käyttäen rationaalisia lausekkeita. Olkoon $Q \subseteq M$, jossa M on monoidi. Osajoukko Q on rationaalinen, jos $Q = \varphi(\mathcal{R}(a_1, \ldots, a_n))$, missä $\mathcal{R}(a_1, \ldots, a_n)$ rationaalinen lauseke ja φ on sijoitus, joka kuvaa jokaisen kirjaimen a_i alkioksi monoidista M.

Esimerkki 2.5. Olkoot $D_4 = \langle a, b \mid a^2 = b^2 = 1,\ ab = ba \rangle$ dihedraaliryhmä ja $Q = \{1, a\}$ sen osajoukko. Nyt Q on rationaalinen osajoukko. Nimittäin olkoot $\mathcal{R}(c, d) = c^* + (c^*d(d^2)^*c^*d(d^2)^*c^*)^*$ ja $\varphi :\ c \mapsto a, d \mapsto b$. Tällöin $Q = \varphi(\mathcal{R}(c, d))$. Kuvassa 9 on esitetty rationaalisen osajoukon Q hyväksyvä automaatti yli aakkoston $\{c, d\}$, jossa on siirros $\delta(q, c) = q'$ (vast. $\delta(q, d) = q'$) jos ja vain jos ryhmässä D_4 on $qa = q'$ (vast. $qb = q'$).



Kuva 9: Rationaalisen osajoukon Q hyväksyvä automaatti.

3 Ratkeavuudesta

Tässä luvussa tarkastellaan päätäntäongelmia ja niiden ratkeavuutta. Päätäntäongelma koostuu syötteistä ja kuhunkin syötteeseen liittyvästä KYLLÄ tai EI vastauksesta. Voidaan siis ajatella, että se on kuvaus syötteiden joukosta I joukkoon $\{0, 1\}$. Algoritmilla tarkoitetaan mekaanista menetelmää, jolla tarkastettava ongelma voidaan ratkaista. Algoritmi koostuu äärellisestä määrästä ohjeita, mutta sen suorittaminen saattaa vaatia mielivaltaisen pitkän ajan tai määrän muistia. Ongelmaa sanotaan *ratkeavaksi*, jos on olemassa joku algoritmi, joka ratkaisee sen. Tämän algoritmin ei tarvitse olla tehokas, vaan pelkkä olemassaolo riittää. Kaikki päätäntäongelmat eivät ole ratkeavia, vaan on olemassa *ratkeamattomia* ongelmia. K. Gödel [10] osoitti, että ratkeamattomia ongelmia on olemassa ja A. Church [9] antoi ensimmäisen konkreettisen ratkeamattoman ongelman. Turingin koneista ja ratkeamattomuudesta voi lukea lisää luentomonisteesta [15] tai kirjasta [29].

Jos päätäntäongelmalla on vain äärellinen määrä syötteitä, niin se ei voi olla ratkeamaton. Nimittäin jos syötteitä on n kappaletta, niin on olemassa 2^n erilaista algoritmia, joissa on kaikki mahdolliset eri kombinaatiot KYLLÄ ja EI vastauksia kaikille syötteille. Näistä algoritmeista jokin on oikea, sillä kaikki mahdolliset vastausvaihtoehdot on käyty läpi. Ei kuitenkaan ole ilmeistä mikä näistä algoritmeista on se oikea, ainoastaan, että jokin on.

Esimerkki 3.1. Osoitetaan, että ongelma ”Onko annettu rationaalinen kieli L tyhjä?” on ratkeava.

Olkoon $\mathcal{A}$ äärellinen automaatti, joka hyväksyy kielen L. Selvästi L ei ole tyhjä jos ja vain jos automaatissa on polku alkutilasta q_0 johonkin lopputilaan $f \in F$. Polun olemassaolo voidaan tarkistaa esimerkiksi graafin syvyyshaulla.

Esimerkki 3.2. Osoitetaan, että ongelma ”Onko $L_1 \subseteq L_2$ annetuille rationaalisille kielille L_1, L_2?” on ratkeava.

Tämä voidaan ratkaista käyttämällä edellisen esimerkin algoritmia kielen tyhjyydelle ja lemman 2.6 algoritmeja. Joukko-opista tiedetään seuraavat ekvivalenssit:

$$L_1 \subseteq L_2 \Leftrightarrow L_1 \setminus L_2 = \emptyset \Leftrightarrow L_1 \cap \overline{L_2} = \emptyset.$$

Turingin kone on A. Turingin kehittämä teoreettinen automaatti, jota käytetään algoritmin määritelmänä. Artikkelissaan [30] Turing osoitti, että on olemassa *universaali Turingin kone*, joka pystyy simuloimaan mielivaltaista Turingin konetta ja että niin kutsuttu *pysähtymisongelma* on ratkeamaton. Turingin kone koostuu äärettömästä, ruutuihin jaetusta työnauhasta ja lukupäästä, joka lukee nauhalta symboleja, kirjoittaa sille ja liikkuu nauhalla. Tarkemmin sanottuna, Turingin kone on seitsikko $M = (Q, \Sigma, \Gamma, \delta, q_0, B, h)$, missä:

(i) Q on äärellinen joukko tiloja.

(ii) Σ on syöteaakkosto.

(iii) Γ on nauha-aakkosto. Oletetaan, että $\Sigma \subset \Gamma$, sillä syöte kirjoitetaan nauhalle, ja että $Q \cap \Gamma = \emptyset$.

(iv) δ on siirtymäfunkio eli kuvaus $Q \setminus \{h\} \times \Gamma \to Q \times \Gamma \times \{L, R\}$. Siirtymä $\delta(q, X) = (p, Y, L)$ tarkoittaa, että kun kone on tilassa q ja lukee symbolin X, koneen tila muuttuu tilaksi p, nauhalle kirjoitetaan symboli Y ja lukupää siirtyy vasemmalle. Samoin määritellään $\delta(q, X) = (p, Y, R)$, mutta lukupää siirtyy oikealle.

(v) q_0 on alkutila.

(vi) $B \in \Gamma \setminus \Sigma$ on tyhjän ruudun symboli.

(vii) h on lopetustila.

Alussa syöte w kirjoitetaan työnauhalle ja kaikkialle sen ympärille kirjoitetaan tyhjä symboli B. Kone on tilassa q_0 ja lukee syötteen ensimmäistä kirjainta, jonka jälkeen toimitaan siirtymäfunktion δ ohjeiden mukaan. Kone M hyväksyy syötteen, jos se pysähtyy lopputilassa h, muuten hylkää. Huomataan, että kone ei välttämättä pysähdy kaikilla syötteillä, mutta algoritmi käyttää määritelmänsä nojalla äärellisen määrän aikaa. Siispä algoritmit määritellään Turingin koneiksi, jotka pysähtyvät kaikilla syötteillä.

Olkoot koneen lukupää tilassa q kirjaimen a kohdalla ja nauha muotoa xay, jossa x on vasemmalle ja y oikealle äärettömiä. Selvästi kullakin hetkellä

nauhalla on vain äärellinen määrä tyhjästä symbolista B eroavia symboleita, joten esitetään koneen konfiguraatio sanalla $\alpha = uqav$, jossa sana u (vast. v) on sanan x (vast. y) lyhin suffiksi (vast. prefiksi), joka sisältää kaikki tyhjästä symbolista eroavat kirjaimet. Tarkemmin,

$$\alpha \in (\{\varepsilon\} \cup (\Gamma \setminus \{B\})\Gamma^*)Q\Gamma(\Gamma^*(\Gamma \setminus \{B\} \cup \{\varepsilon\})).$$

Jos kone on konfiguraatiossa $\alpha = uqav$ hetkellä t ja seuraava konfiguraatio on β, niin silloin merkitään $\alpha \vdash \beta$. Merkitään $\alpha \vdash^* \beta$ jos on olemassa äärellinen jono $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n = \beta$, missä $\alpha_i \vdash \alpha_{i+1}$ jokaisella $i = 1, 2, \ldots, n-1$. Kieli, jonka Turingin kone M hyväksyy on

$$L(M) = \{w \mid w \in \Sigma^* \text{ ja } q_0 w \vdash^* uhv, \text{ joillekin } u, v \in \Gamma^*\}.$$

Esimerkki 3.3. Olkoon $M = (\{q, p, h\}, \{a, B\}, \{a, B\}, \delta, q, B, h)$ Turingin kone, jossa siirtymäfunktio δ on

$$\begin{aligned} \delta(q, a) &= (p, a, L), \quad \delta(q, B) = (p, a, R), \\ \delta(p, a) &= (h, a, L), \quad \delta(p, B) = (q, a, L). \end{aligned}$$

Kone M toimii tyhjällä syötteellä seuraavasti:

$$qB \vdash apB \vdash qaa \vdash pBaa \vdash qBaaa \vdash apaaa \vdash haaaa.$$

Määritellään koodaukset Turingin koneelle M. Voidaan olettaa, että koneen M syöteaakkosto on $\{0, 1\}$, sillä suurempi aakkosto voidaan koodata binäärisanoiksi. Lisäksi oletetaan, että tilat $Q = \{q_1, \ldots, q_n\}$, jossa q_1 on alkutila, q_n on lopputila ja aakkosto $\Gamma = \{X_1, X_2, \ldots, X_m\}$, jossa $X_1 = 1, X_2 = 0$ ja $X_3 = B$. Merkitään $D_1 = L$ ja $D_2 = R$. Olkoon $\delta(q_i, X_j) = (q_k, X_l, D_s)$ siirtymäfuktion sallima siirros. Sitä vastaa yksikäsitteinen sana $c_{i,j} = 1^i 0 1^j 0 1^k 0 1^l 0 1^s$. Nyt koko konetta M vastaava binäärisana on

$$c(M) = 0001^n 001^m 00 c_{1,1} 00 c_{1,2} 00 \cdots c_{n-1,m} 000.$$

On luontevaa samaistaa Turingin kone M koodauksensa $c(M)$ kanssa.

Esimerkki 3.4. Edellisen esimerkin Turingin koneelle M koodaus

$$\begin{aligned} c(M) \;=\; & 00011001100\underbrace{1010110101}_{c_{1,1}}00\underbrace{101101101011}_{c_{1,2}}00 \\ & \underbrace{110101110101}_{c_{2,1}}00\underbrace{11011010101}_{c_{2,2}}000. \end{aligned}$$

Nyt voidaan muodostaa universaali Turingin kone, joka pystyy simuloimaan mielivaltaisen Turingin koneen koodauksen. Universaalin Turingin koneen rakennetta ei käydä tässä tutkielmassa läpi. A. Turingin suunnitteleman universaalin koneen rakenne löytyy artikkelista [30]. Artikkelissaan [24] Y. Rogozhin käy läpi universaaleja Turingin koneita, joissa on mahdollisimman pienet tilajoukko Q ja aakkosto Γ.

Lause 3.1. *Olkoon* $L_d = \{c(M) \mid M \text{ ei hyväksy sanaa } c(M)\}$. *Ongelma* "Onko $w \in L_d$?" *ei ole ratkeava.*

Todistus. Oletetaan, että ongelma on ratkeava ja olkoon M_d Turingin kone, joka hyväksyy kielen L_d sanat. Annetaan koneelle M_d syötteeksi $c(M_d)$. Oletetaan ensin, että kone M_d ei hyväksy sanaa $c(M_d)$. Silloin kielen L_d määritelmän nojalla $c(M_d) \in L_d$. Tämä ei ole mahdollista, sillä silloin kone M_d hyväksyy sanan $c(M_d)$. Oletetaan sitten, että kone M_d hyväksyy sanan $c(M_d)$. Silloin $c(M_d) \notin L_d$ ja siis kone M_d ei hyväksy sanaa $c(M_d)$. Molemmissa tapauksissa päädytään ristiriitaan, joten ongelma on ratkeamaton. □

Edellinen lause antoi ensimmäisen ratkeamattoman ongelman, jonka avulla todistetaan seuraavat ongelmat ratkeamattomiksi käyttäen reduktiota. *Reduktiolla* tarkoitetaan, että ongelma voidaan ratkaista käyttäen toista ongelmaa. Tarkemmin, jos ongelma P *redusoituu* ongelmaan P', niin mikä tahansa ongelman P instanssi i voidaan muuttaa ongelman P' instanssiksi i' siten, että i on ongelman P positiivinen instanssi jos ja vain jos i' on ongelman P' positiivinen instanssi. Jos ongelma P redusoituu ongelmaan P', niin käytetään merkintää $P \leq P'$. Reduktiossa voidaan myös muuttaa ongelman P positiiviset instanssit muutetaan ongelman P' negatiivisiksi instansseiksi ja päinvastoin. Jos halutaan osoittaa ongelma P' ratkeamattomaksi, niin se redusoidaan johonki tunnettuun ratkeamattomaan ongelmaan P. Tällöin on-

gelman P' on oltava ratkeamaton, sillä muuten sen avulla voitaisiin ratkaista ongelma P, joka tiedetään ratkeamattomaksi.

Määritellään pysähtymisongelma HALT(M, w).

HALT(M,w)	
SYÖTE:	Turingin kone M ja syöte w.
ONGELMA:	Hyväksyykö Turingin kone M syötteen w?

Edellisen lauseen seurauksena saadaan luonnollisempi tulos. Nimittäin nyt voidaan osoittaa, että ongelma HALT(M, w) ei ole ratkeava.

Seuraus 3.2. *Pysähtymisongelma* HALT(M, w) *ei ole ratkeava.*

Todistus. Tehdään vastaoletus, että HALT(M, w) on ratkeava. Olkoot

$$L_u = \{(M, w) \mid M \text{ on Turingin kone, joka hyväksyy sanan } w\}$$

ja M_u Turingin kone, joka hyväksyy kielen L_u sanat. Muodostetaan Turingin kone M_d, joka hyväksyy lauseen 3.1 kielen L_d sanat. Syötteellä w kone M_d tarkistaa onko sana w jonkin Turingin koneen koodaus. Jos ei ole, silloin kone M_d ei hyväksy sanaa w. Jos $w = c(M)$, jollekin Turingin koneelle M, silloin kone M_d simuloi koneen M_u syötteellä (w, w).

Jos M_u hyväksyy syötteen (w, w), silloin M_d hylkää sanan w ja jos M_u ei hyväksy syötettä (w, w), niin silloin M_d hyväksyy sanan w.

Eli kone M_d hyväksyy sanan w jos ja vain jos se on jonkun Turingin koneen M koodaus, joka ei hyväksy omaa koodaustaan. Siis M_d hyväksyy kielen L_d sanat, mikä ei ole mahdollista. Siispä HALT(M, w) ei ole ratkeava. □

Seuraavaksi osoitetaan, että *Postin vastaavuusongelma* PCP(L_1, L_2) ei ole ratkeava. Tämän tuloksen E. Post todisti artikkelissaan [22]. Määritellään ongelma PCP(L_1, L_2).

PCP(L_1, L_2)	
SYÖTE:	Listat sanoja $L_1 = \{u_1, u_2, \ldots, u_k\}$, $L_2 = \{v_1, v_2, \ldots, v_k\}$.
ONGELMA:	Onko $u_{i_1}u_{i_2}\cdots u_{i_j} = v_{i_1}v_{i_2}\cdots v_{i_j}$ jollain indeksijonolla $i_1, i_2 \ldots, i_j$?

Kuten Turingin koneiden koodauksessakin, voidaan olettaa, että kaikki sanat u_i ja v_j ovat yli aakkoston $\{a, b\}$, sillä suurempi aakkosto voidaan koodata binäärimuotoon.

Toinen tapa määritellä Postin vastaavuusongelma on, että listojen L_1 ja L_2 sanaparit muodostavat dominoita, joiden ylä- ja alapuoliskoilla on vastaavat sanat. Siis syötteenä on joukko

$$\left\{ \left[\frac{u_1}{v_1}\right], \left[\frac{u_2}{v_2}\right], \ldots, \left[\frac{u_k}{v_k}\right] \right\}$$

ja kysytään, saadanko näistä dominojono, jossa ylä- ja alapuoliskoilla on samat sanat.

Esimerkki 3.5. Olkoot

$$P_1 = \left\{ \left[\frac{ab}{abb}\right], \left[\frac{bb}{baa}\right], \left[\frac{aaa}{aa}\right] \right\}$$

ja

$$P_2 = \left\{ \left[\frac{aa}{a}\right], \left[\frac{aba}{ab}\right], \left[\frac{ba}{b}\right] \right\}.$$

Joukolla P_1 on ratkaisu, nimittäin

$$\left[\frac{ab}{abb}\right] \left[\frac{bb}{baa}\right] \left[\frac{aaa}{aa}\right] \left[\frac{aaa}{aa}\right],$$

jossa molemmilla riveillä on sana *abbbaaaaaa*. Joukolla P_2 ei ole ratkaisua, sillä jokaisessa dominossa ylärivillä on enemmän kirjaimia kuin alarivillä.

Lemma 3.3. *Muokattu Postin vastaavuusongelma MPCP, jossa vaaditaan, että joukon ensimmäinen domino on ratkaisussa ensimmäisenä ei ole ratkeava.*

Todistus. Oletetaan, että muokattu Postin vastaavuusongelma on ratkeava. Muodostetaan Turingin kone M_u, joka määrää kielen

$$L_u = \{(M, w) \mid M \text{ on Turingin kone, joka hyväksyy sanan } w\}.$$

Olkoon $M = (Q, \Sigma, \Gamma, \delta, q_0, B, h)$ Turingin kone. Tavoitteena on muodostaa sellainen dominojoukko P, jolle voidaan muodostaa muokatun Postin vastavuusongelman mukainen sana jos ja vain jos kone M hyväksyy sanan w. Voidaan olettaa, että koneen M lukupää ei ikinä siirry syötteen ensimmäisen kirjaimen vasemmalle puolelle.

(i) Lisätään domino $\left[\frac{\#}{\#q_0w\#}\right]$ joukon P ensimmäiseksi dominoksi. Positiivisen instanssin on alettava tällä dominolla, joten alapuoli alkaa koneen M ensimmäisellä konfiguraatiolla.

(ii) Jokaiselle $a, b \in \Gamma$ ja jokaiselle $q, p \in Q$. Jos $\delta(q, a) = (p, b, R)$, niin silloin lisätään domino $\left[\frac{qa}{bp}\right]$ joukkoon P. Tällä simuloidaan lukupään siirtymiset oikealle.

(iii) Jokaiselle $a, b, c \in \Gamma$ ja jokaiselle $q, p \in Q$. Jos $\delta(q, a) = (p, b, L)$, niin silloin lisätään domino $\left[\frac{cqa}{pcb}\right]$ joukkoon P. Tällä simuloidaan lukupään siirtymiset vasemmalle.

(iv) Jokaiselle $a \in \Gamma$ lisätään domino $\left[\frac{a}{a}\right]$ joukkoon P. Tämän avulla ne ruudut, joissa ei ole lukupäätä, pysyvät muuttumattomina.

(v) Lisätään dominot $\left[\frac{\#}{\#}\right]$ ja $\left[\frac{\#}{B\#}\right]$ joukkoon P. Näillä dominoilla päätetään konfiguraatio.

(vi) Jokaiselle $a \in \Gamma$ lisätään $\left[\frac{ah}{h}\right]$ ja $\left[\frac{ha}{h}\right]$ joukkoon P. Nämä dominot mahdollistavat työnauhan tyhjentämisen sen jälkeen kun kone on siirtynyt lopputilaan.

(vii) Lisätään $\left[\frac{h\#\#}{\#}\right]$ joukkoon P. Tällä dominolla saadaan ylä- ja alarivit täsmäämään.

Konstruktiosta nähdään, että kone M hyväksyy sanan w jos ja vain jos joukko P on muokatun Postin vastaavuusongelman positiivinen instanssi. Joten ongelma MPCP ei ole ratkeava. □

Lause 3.4. *Ongelma* PCP *ei ole ratkeava.*

Todistus. Edellisen lemman konstruktio ei suoraan käy tämän tuloksen todistamiseen, sillä vaiheessa (iv) muodostetut dominot ovat itsessään positiivinen ratkaisu. Olkoon $w = w_1w_2 \cdots w_n$. Määritellään sanat $\star w$, $w\star$ ja $\star w\star$ seuraavasti

$$\begin{aligned} \star w &= *w_1 * w_2 * \cdots * w_n, \\ w\star &= w_1 * w_2 * \cdots * w_n*, \\ \star w\star &= *w_1 * w_2 * \cdots * w_n*, \end{aligned}$$

joissa $*$ on uusi symboli. Olkoon

$$P = \left\{ \left[\frac{u_1}{v_1}\right], \left[\frac{u_2}{v_2}\right], \ldots, \left[\frac{u_k}{v_k}\right] \right\}$$

MPCP:n instanssi. Olkoon

$$P' = \left\{ \left[\frac{\star u_1}{\star v_1 \star}\right], \left[\frac{\star u_1}{v_1 \star}\right], \left[\frac{\star u_2}{v_2 \star}\right], \ldots, \left[\frac{\star u_k}{v_k \star}\right], \left[\frac{*\Diamond}{\Diamond}\right] \right\},$$

missä $\Diamond$ on uusi symboli. Nyt P' on ongelman PCP syöte. Positiivisen vastauksen on pakko alkaa dominolla $\left[\frac{\star u_1}{\star v_1 \star}\right]$, sillä se on ainoa domino, jossa molemmat puolet alkaavat samalla symbolilla. Dominon $\left[\frac{*\Diamond}{\Diamond}\right]$ avulla saadaan puuttuva $*$ ylärivin loppuun. Siispä ongelma PCP on ratkeava jos ja vain jos ongelma MPCP on ratkeava. Näin ollen ongelma PCP on ratkeamaton. □

Esimerkki 3.6. Olkoon $M = (\{q, p, h\}, \{a\}, \{a, b\}, \delta, q, b, h)$, jossa siirtymäfunktio δ on $\delta(q, a) = (p, a, R)$, $\delta(q, b) = (h, b, R)$, $\delta(p, a) = (q, a, R)$, siis kone, joka hyväksyy parillisen pituiset sanat. Koneen toimintaa syötteellä $w = aa$ vastaava muokatun Postin vastaavuusongelman dominojoukko on

$$\begin{aligned} P \;=\; & \left\{ \left[\frac{\#}{\#qaa\#}\right], \left[\frac{qa}{ap}\right], \left[\frac{qb}{bh}\right], \left[\frac{pa}{aq}\right], \left[\frac{a}{a}\right], \right. \\ & \left. \left[\frac{b}{b}\right], \left[\frac{\#}{\#}\right], \left[\frac{\#}{b\#}\right], \left[\frac{ah}{h}\right], \left[\frac{bh}{h}\right], \left[\frac{h\#\#}{\#}\right] \right\}. \end{aligned}$$

Koska sanan aa pituus on 2, niin voidaan muodostaa virheetön dominoketju

$$\begin{aligned} & \left[\frac{\#}{\#qaa\#}\right] \left[\frac{qa}{ap}\right] \left[\frac{a}{a}\right] \left[\frac{\#}{\#}\right] \left[\frac{a}{a}\right] \left[\frac{pa}{aq}\right] \left[\frac{\#}{b\#}\right] \left[\frac{a}{a}\right] \left[\frac{a}{a}\right] \left[\frac{qb}{bh}\right] \left[\frac{\#}{\#}\right] \\ & \quad \left[\frac{a}{a}\right] \left[\frac{a}{a}\right] \left[\frac{bh}{h}\right] \left[\frac{\#}{\#}\right] \left[\frac{a}{a}\right] \left[\frac{ah}{h}\right] \left[\frac{\#}{\#}\right] \left[\frac{ah}{h}\right] \left[\frac{\#}{\#}\right] \left[\frac{h\#\#}{\#}\right]. \end{aligned}$$

Tämän dominoketjun molemmilla riveillä on sana

$$\#qaa\#apa\#aaqb\#aabh\#aah\#ah\#h\#\#.$$

4 Matriisien ratkeavuustuloksia

Tässä luvussa tarkastellaan matriisien kuolevuusongelmaa ja sen variaatioiden ratkeavuutta. Määritellään kokonaislukumatriisien kuolevuusongelma MORT(n).

MORT(n)	
SYÖTE:	Äärellinen matriisijoukko $\{M_1, M_2, \ldots, M_k\}$, jossa jokainen matriisi on kokoa $n \times n$.
ONGELMA:	Onko $M_{i_1} M_{i_2} \cdots M_{i_j} = \mathcal{O}$ jollain indeksijonolla $i_1, i_2, \ldots, i_j$?

Siis kuolevuusongelmassa kysytään sisältyykö nolla-alkio annettujen alkioiden generoituun puoliryhmään.

Esimerkki 4.1. Olkoon $F = \{M_1, M_2, \ldots, M_k\}$, missä jokainen matriisi $M_i \in \mathcal{M}_2(\mathbb{Z}_+)$. Olkoot

$$M_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in F$$

ja

$$M_j = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in F.$$

Näiden kahden matriisien tulo on

$$M_i M_j = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + db' & cb' + dd' \end{pmatrix},$$

jossa jokainen alkio on suurempi kuin nolla. Siispä joukko F ei ole kuoleva.

Esimerkki 4.2. Olkoon $F = \{A, B\}$, missä $A = \left(\begin{smallmatrix} 0 & 0 \\ -1 & k \end{smallmatrix}\right)$ ja $B = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Joukko F on kuoleva, sillä

$$AB^k = \begin{pmatrix} 0 & 0 \\ -1 & k \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$$

ja

$$AB^k AB^k = \mathcal{O}.$$

Olkoon $w = a_1 a_2 \cdots a_m \in \{1,2,3\}^*$ ja $\sigma(w)$ sen esitys kannassa 4. Siis

$$\sigma(w) = a_m + 4a_{m-1} + \ldots + 4^{m-1}a_1.$$

On selvää, että kuvaus σ on injektio ja sanoille u ja v on voimassa

$$\sigma(uv) = \sigma(v) + 4^{|v|}\sigma(u).$$

Seuraavaksi yhdistetään 3×3 matriisi sanoihin u, v:

$$M_{u,v} = \begin{pmatrix} 4^{|u|} & 0 & 0 \\ 0 & 4^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}.$$

Lemma 4.1. *Kaikille $u, v, x, y \in \{1,2,3\}^*$ on voimassa $M_{u,v}M_{x,y} = M_{ux,vy}$.*

Todistus. Suoraan laskemalla nähdään, että

$$\begin{aligned} M_{u,v}M_{x,y} &= \begin{pmatrix} 4^{|u|} & 0 & 0 \\ 0 & 4^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix} \begin{pmatrix} 4^{|x|} & 0 & 0 \\ 0 & 4^{|y|} & 0 \\ \sigma(x) & \sigma(y) & 1 \end{pmatrix} \\ &= \begin{pmatrix} 4^{|u|}4^{|x|} & 0 & 0 \\ 0 & 4^{|v|}4^{|y|} & 0 \\ 4^{|x|}\sigma(u) + \sigma(x) & 4^{|y|}\sigma(v) + \sigma(y) & 1 \end{pmatrix} \\ &= \begin{pmatrix} 4^{|ux|} & 0 & 0 \\ 0 & 4^{|vy|} & 0 \\ \sigma(ux) & \sigma(vy) & 1 \end{pmatrix} = M_{ux,vy}. \end{aligned}$$

□

Edellisen lemman nojalla kuvaus $(u, v) \mapsto M_{u,v}$ on monoidihomomorfismi.

Lause 4.2. *Ongelma* MORT(3) *ei ole ratkeava.*

Todistus. Osoitetaan, että jos ongelma MORT(3) on ratkeava, niin silloin ongelma PCP on ratkeava. Lauseen 3.4 nojalla PCP ei ole ratkeava, kun sanat ovat binääriaakkoston yli. Olkoot

$$\begin{aligned} L_1 &= \{u_1, u_2, \ldots, u_k\}, \\ L_2 &= \{v_1, v_2, \ldots, v_k\}, \end{aligned}$$

ongelman PCP syöte, jossa kaikki sanat ovat aakkoston $\{2,3\}$ yli. Muodostetaan matriisijoukko F, jossa on matriisit $M_i = M_{u_i,v_i}$, $M'_i = M_{u_i,1v_i}$ kaikille $i = 1, 2, \ldots, k$ ja matriisi

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

Matriisi A on idempotentti, siis $A^2 = A$ ja

$$AM_{x,y}A = (4^{|x|} + \sigma(x) - \sigma(y))A. \tag{2}$$

Huomataan, että $AM_{x,y}A = \mathcal{O}$ jos ja vain jos

$$\sigma(y) = 4^{|x|} + \sigma(x) = \sigma(1x),$$

toisin sanoen jos ja vain jos $y = 1x$. Osoitetaan, että joukko F on kuoleva jos ja vain jos tälle ongelman PCP syötteelle on ratkaisu.

Oletetaan ensin, että $i_1, i_2, \ldots, i_m$ on ratkaisu. Siis $u_{i_1}u_{i_2}\cdots u_{i_m} = v_{i_1}v_{i_2}\cdots v_{i_m}$. Silloin

$$M'_{i_1}M_{i_2}M_{i_3}\cdots M_{i_m} = M_{x,y},$$

jossa $x = u_{i_1}u_{i_2}\cdots u_{i_m}$ ja $y = 1v_{i_1}v_{i_2}\cdots v_{i_m}$. Nyt $y = 1x$, joten $AM_{x,y}A = \mathcal{O}$. Siispä joukko F on kuoleva.

Seuraavaksi oletetaan, että joukko F on kuoleva. Siis

$$AW_1AW_2A\cdots AW_mA = \mathcal{O},$$

jossa

$$W_j \in \{K_{i_1}\cdots K_{i_n} \mid n \geq 1, K_{i_j} \in F \setminus \{A\}\}$$

kaikilla indekseillä j. Toisin sanoen matriisi W_j on matriisien M_i, M'_i epätyhjä tulo. Jokainen matriisi W_j on muotoa $M_{x,y}$ joillekin sanoille $x, y \in \{1,2,3\}^*$, joten yhtälön (2) nojalla matriisit AW_jA ovat matriisin A skalaarimonikertoja. Siis $AW_jA = a_jA$, jollekin luvulle a_j. Nyt

$$\begin{aligned} \mathcal{O} &= AW_1AW_2A\cdots AW_mA = a_1AW_2A\cdots AW_mA \\ &= a_1a_2AW_3A\cdots AW_mA = a_1a_2\cdots a_mA. \end{aligned}$$

Siispä jokin kertoimista on nolla. Olkoon $a_j = 0$ ja siis $AW_jA = \mathcal{O}$. Olkoon $W_j = M_{x,y}$. Yhtälön (2) nojalla $x = 1y$. Koska sana u on yli aakkoston $\{2, 3\}$, niin on oltava

$$W_j = M'_{i_1} M_{i_2} M_{i_3} \cdots M_{i_m},$$

joillekin luvuille $i_1, i_2, \ldots, i_m$. Nyt

$$\begin{aligned} x &= u_{i_1} u_{i_2} \cdots u_{i_m} \\ y &= v_{i_1} v_{i_2} \cdots v_{i_m} \end{aligned}$$

ja $x = 1y$, joten $i_1, i_2, \ldots, i_m$ on ongelman PCP kyseisen instanssin ratkaisu. □

Seuraus 4.3. *Ongelma* MORT(n)*, jossa* $n > 3$*, ei ole ratkeava.*

Todistus. Tehdään vastaoletus, että $n \times n$ matriisien kuolevuus on ratkeavaa, kun $n > 3$. Silloin myös 3×3 matriisien kuolevuus on ratkeavaa. Nimittäin joukko $F = \{M_1, M_2, \ldots, M_k\}$, jossa jokainen matriisi M_i on 3×3 kokonaislukumatriisi, on kuoleva jos ja vain jos joukko $F' = \{M'_1, M'_2, \ldots, M'_k\}$ on kuoleva, missä

$$M'_i = \begin{pmatrix} M_i & \mathcal{O}_{r\times 3} \\ \mathcal{O}_{3\times r} & \mathcal{O}_{r\times r} \end{pmatrix}$$

kaikilla indekseillä $i = 1, \ldots, k$ ja $r = n - 3$. □

Tarkastellaan ongelmaa MORT$_+$(n), jossa annettujen matriisien alkiot ovat ei-negatiivisia.

Lause 4.4. *Ongelma* MORT$_+$(n) *on ratkeava.*

Todistus. Olkoon $F = \{A_1, \ldots, A_m\}$. Määritellään kuvaus $\rho(A) = A'$, jossa matriisin A' alkio on 0 (vast. 1) jos ja vain jos matriisissa A vastaava alkio on 0 (vast. suurempi kuin 0). Nyt $S = \langle F \rangle$, missä binäärioperaatio $*$ on määritelty siten, että $A * B = \rho(AB)$, on puoliryhmä. Erilaisia binäärimatriiseja on 2^{n^2} kappaletta, joten $|S| \leq 2^{n^2}$. Tästä johtuen jos matriisi $A \in S$, niin se on alle 2^{n^2} generaattorin tulo. Muodostamalla kaikki mahdolliset tulot, voidaan todeta onko $\mathcal{O} \in S$, jolloin joukon F matriisien tulo on nollamatriisi samoilla indekseillä. □

Tällä hetkellä ei tiedetä onko ongelma MORT(2) ratkeava vai ei. Seuraavissa alaluvuissa osoitetaan, että ongelman MORT(2) jotkut erikoistapaukset ovat ratkeavia. Nämä erikoistapaukset ovat MORT(2, 2), jossa syötteenä on kaksi matriisia, ja MORT′(2), jossa matriisien determinantti on 0 tai ±1. Määritellään ongelmat MORT(2, 2) ja MORT′(2).

MORT(2, 2)	
SYÖTE:	Matriisijoukko $\{M_1, M_2\}$, jossa molemmat matriisit ovat kokoa 2×2.
ONGELMA:	Onko $M_{i_1} M_{i_2} \cdots M_{i_j} = \mathcal{O}$ joillain indekseillä $i_1, \ldots, i_j$?

MORT′(2)	
SYÖTE:	Äärellinen matriisijoukko $\{M_1, M_2, \ldots, M_k\}$, jossa jokainen matriisi on kokoa 2×2 ja determinantti on 0 tai ±1.
ONGELMA:	Onko $M_{i_1} M_{i_2} \cdots M_{i_j} = \mathcal{O}$ joillain indekseillä $i_1, \ldots, i_j$?

4.1 Ongelman MORT′(2) ratkeavuudesta

Tässä alaluvussa osoitetaan, että 2×2 matriisien kuolevuus on ratkeavaa, kun rajoitutaan matriiseihin, joiden determinantti on 0 tai ±1. Esitys seuraa artikkelia [20].

Seuraavan lemman avulla 2×2 rationaalisen matriisin A kuvalle Im_A ja ytimelle Ker_A voidaan valita tiettyä tyyppiä olevat generaattorit.

Lemma 4.5. *Olkoon $A \in \mathcal{M}_2(\mathbb{Q})$ siten, että* $\mathrm{rank}(A) = 1$. *Silloin* Im_A (*vast.* Ker_A) *sisältää vektorin $(x, y) \in \mathbb{Z}^2$, jolle pätee* $\mathrm{syt}(x, y) = 1$.

Todistus. Olkoon $A \in \mathcal{M}_2(\mathbb{Q})$ ja $\mathrm{rank}(A) = 1$. Koska matriisin A aste on 1, se on muotoa

$$A = \begin{pmatrix} a & b \\ \lambda a & \lambda b \end{pmatrix},$$

jollekin $a, b, \lambda \in \mathbb{Q}$. Molemmat a ja b eivät voi olla 0, sillä muuten matriisin A aste olisi 0. Voidaan rajoituksetta olettaa, että $a \neq 0$. Merkitään $\lambda = p/q$ joillekin $p, q \in \mathbb{Z}$ ja $\mathrm{syt}(p, q) = 1$. Nyt kuva Im_A on

$$A \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} au + bv \\ \lambda(au + bv) \end{pmatrix}.$$

Valitsemalla $u = 1/a$ ja $v = 0$, saadaan haluttu kuvavektori $q(1, \lambda)^T = (q, p)^T$. Ytimen tapauksessa ratkaisemalla yhtälö $A\binom{u}{v} = \binom{0}{0}$ nähdään, että vektori $(u, v)^T$ voidaan valita siten, että $(u, v)^T \in \mathbb{Q}$. Nimittäin

$$\begin{pmatrix} a & b \\ \lambda a & \lambda b \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} au + bv \\ \lambda au + \lambda bv \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

jos ja vain jos $u = -\frac{b}{a}v$. Siis on olemassa minimaalinen $n \in \mathbb{N}$ siten, että $n(u, v)^T \in \mathbb{Z}^2$ ja tämä on haluttu vektori. □

Tutkittaessa matriisien kuolevuutta ei tarvitse tarkastella kaikkia mahdollisia tuloja, vaan voidaan rajoittua seuraavan lemman mukaisiin tuloihin. Seuraava lemma todistetaan rationaalisille matriiseille lausetta 4.17 varten.

Lemma 4.6. *Äärellinen joukko* 2×2 *matriiseja* $F = \{A_1, \ldots, A_m\} \subseteq \mathcal{M}_2(\mathbb{Q})$ *on kuoleva jos ja vain jos on olemassa* $k \in \mathbb{Z}$ *ja kokonaisluvut* $i_1, \ldots, i_k \in \{1, \ldots, m\}$*, joille on voimassa*

$$\begin{aligned} A_{i_1} \cdots A_{i_k} &= \mathcal{O}, \\ \operatorname{rank}(A_{i_j}) &= 2, \textit{ jos } 1 < j < k, \\ \operatorname{rank}(A_{i_j}) &< 2, \textit{ jos } j = 1 \textit{ tai } j = k. \end{aligned}$$

Todistus. Oletetaan, että F on kuoleva. Silloin on olemassa minimaalinen $k \geq 2$, jolle $A_{i_1} \cdots A_{i_k} = \mathcal{O}$. Matriisit A_{i_1} ja A_{i_k} ovat singulaarisia, sillä muuten

$$\begin{aligned} A_{i_1} \cdots A_{i_k} &= \mathcal{O} \\ \Leftrightarrow A_{i_1}^{-1} A_{i_1} \cdots A_{i_k} A_{i_k}^{-1} &= \mathcal{O} \\ \Leftrightarrow A_{i_2} \cdots A_{i_{k-1}} &= \mathcal{O}, \end{aligned}$$

mikä on ristiriidassa luvun k minimaalisuuden kanssa.

Olkoon $j \geq 2$ pienin kokonaisluku, jolle $\operatorname{rank}(A_{i_j}) < 2$. Merkitään, $A_{i_1} \cdots A_{i_{j-1}} = B$ ja $A_{i_j} \cdots A_{i_k} = C$. Koska $A_{i_1} \cdots A_{i_k} = BC = \mathcal{O}$, matriisi B kuvaa matriisin C kuvan Im_C nollaksi. Lisäksi, Im_C on matriisin A_{i_j}

kuva ja sen dimensio on 1. Selvästi $\mathrm{Im}_C \subseteq \mathrm{Im}_{A_{i_j}}$. Lisäksi luvun k määritelmän nojalla, kuvan Im_C dimensio ei voi olla 0 ja se on korkeintaan 1, sillä $\mathrm{rank}(A_{i_j}) < 2$. Nyt sekä Im_C että $\mathrm{Im}_{A_{i_j}}$ ovat yksiulotteisia ja niillä on generaattorit x ja y. Lemman 4.5 nojalla generaattorin alkioiden suurin yhteinen tekijä on 1 ja koska $x \in \mathrm{Im}_{A_{i_j}}$, niin välttämättä $x = y$, jolloin $\mathrm{Im}_C = \mathrm{Im}_{A_{i_j}}$. Siispä $BA_{i_j} = A_{i_1} \cdots A_{i_{j-1}} A_{i_j} = \mathcal{O}$. Luvun k minimaalisuuden nojalla $j = k$, mikä todistaa väitteen. Toiseen suuntaan väite on ilmeinen. □

Joukko F voidaan jakaa kahteen erilliseen joukkoon

$$S = \{A \in F \mid \mathrm{rank}(A) < 2\} = \{S_1, \ldots, S_k\}$$

ja

$$R = \{A \in F \mid \mathrm{rank}(A) = 2\} = \{R_1, \ldots, R_n\}.$$

Voidaan olettaa, että molemmat joukot ovat epätyhjiä. Nimittäin, jos $S = \emptyset$, niin edellisen lemman nojalla F ei ole kuoleva. Jos taas $R = \emptyset$, niin lemman nojalla riittää tarkastella parittaisia tuloja joukon S matriiseista. Lisäksi voidaan olettaa, että $\mathrm{rank}(S_i) = 1$ kaikille $i \in \{1, \ldots, k\}$, sillä muuten $\mathcal{O} \in S$, jolloin F on triviaalisti kuoleva.

Merkintöjen helpottamiseksi, jokaiselle matriisille $S_i \in S$, merkitään $\mathrm{Im}_i = \mathrm{Im}_{S_i}$ ja $\mathrm{Ker}_i = \mathrm{Ker}_{S_i}$. Lisäksi merkitään ι_i (vast. κ_i) lemman 4.5 mukainen generaattori kuvalle Im_i (vast. ytimelle Ker_i).

Lause 4.7. *Jos $\mathcal{O} \notin F$, niin F on kuoleva jos ja vain jos $K\mathrm{Im}_i = \mathrm{Ker}_j$, joillain $i, j \in \{1, \ldots, k\}$ ja $K \in \langle R_1, \ldots, R_n \rangle$.*

Todistus. Oletetaan, että F on kuoleva. Väite seuraa lemmasta 4.6. Nimittäin sen nojalla on olemassa $K \in \langle R_1, \ldots, R_n \rangle$ ja $i, j \in \{1, \ldots, k\}$ joille pätee $S_j K S_i = \mathcal{O}$. Olkoon $(x, y)^T \in K\mathrm{Im}_i$, siis $(x, y)^T = KS_i(u, v)^T$, jollain $(u, v)^T \in \mathbb{R}^2$. Nyt

$$S_j \begin{pmatrix} x \\ y \end{pmatrix} = S_j K S_i \begin{pmatrix} u \\ v \end{pmatrix} = \mathcal{O} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

eli $(x, y)^T \in \mathrm{Ker}_j$ ja siten myös $K\mathrm{Im}_i \subseteq \mathrm{Ker}_j$. Selvästi $\mathrm{Ker}_j \subseteq K\mathrm{Im}_i$, eli $K\mathrm{Im}_i = \mathrm{Ker}_j$.

Oletetaan seuraavaksi oikea puoli. Jos on olemassa $i, j \in \{1, \ldots, k\}$ ja $K \in \langle R_1, \ldots, R_n \rangle$, joille $K\mathrm{Im}_i = \mathrm{Ker}_j$, niin selvästi $S_j K S_i = \mathcal{O}$. □

Jatkossa oletetaan, että edellä määritellylle joukolle R on $R \subseteq GL_2(\mathbb{Z})$. Tämän oletuksen jälkeen edellisen lauseen väite on ekvivalentti seuraavan kuvan ja ytimen generaattorien tarkastelun kanssa.

Lemma 4.8. *Olkoon $K \in \langle R_1, \ldots, R_n \rangle$. Silloin $K\mathrm{Im}_i = \mathrm{Ker}_j$, joillain $i, j \in \{1, \ldots, k\}$ jos ja vain jos $K\iota_i^T = \pm\kappa_j^T$.*

Todistus. Oletetaan väitteen vasen puoli. Olkoot $(x, y)^T \in \mathrm{Im}_i$ ja $(u, v)^T \in \mathrm{Ker}_j$ siten, että $K(x, y)^T = (u, v)^T$. Lisäksi $(x, y)^T = \alpha\iota_i$ ja $(u, v)^T = \beta\kappa_j$ joillain $\alpha, \beta \in \mathbb{R}$. Nyt sijoittamalla arvot yhtälöön $K\binom{x}{y} = \binom{u}{v}$ saadaan yhtälö $\alpha K\iota_i = \beta\kappa_j$, josta saadaan edelleen yhtälö $K\iota_i = \lambda\kappa_j$, kun $\lambda = \frac{\beta}{\alpha}$. Itse asiassa $\lambda \in \mathbb{Z}$, sillä $\kappa_j, \iota_i \in \mathbb{Z}^2$, $K \in \mathcal{M}_2(\mathbb{Z})$ ja $\kappa_j = (z, t)^T$, jossa $\mathrm{syt}(z, t) = 1$. Siispä

$$\iota_i = \lambda K^{-1}\kappa_j,$$

missä $K^{-1} \in \mathcal{M}_2(\mathbb{Z})$. Jos $\iota_i = (r, s)^T$, niin λ jakaa komponentit r ja s, jolloin $\lambda = \pm 1$, koska lemman 4.5 nojalla $\mathrm{syt}(r, s) = 1$. Väite seuraa tästä.

Oletetaan sitten oikea puoli. Olkoot $\alpha\iota_i = (x, y)^T \in \mathrm{Im}_i$ ja $\beta\kappa_j = (u, v)^T \in \mathrm{Ker}_j$, joillain $\alpha, \beta \in \mathbb{R}$. Nyt

$$K\begin{pmatrix} x \\ y \end{pmatrix} = \alpha K\iota_i = \pm\alpha\kappa_j$$

ja

$$\begin{pmatrix} u \\ v \end{pmatrix} = \beta\kappa_j = \pm\beta K\iota_i.$$

Siis $K\mathrm{Im}_i = \mathrm{Ker}_j$, mikä oli todistettava. □

Seuraavissa tuloksissa luonnollisesta kantavektorista $(1, 0)^T$ käytetään merkintää e_1.

Lemma 4.9. *Olkoon $c = (x, y)^T \in \mathbb{Z}^2$ siten, että $\mathrm{syt}(x, y) = 1$. Silloin on olemassa $U \in GL_2(\mathbb{Z})$, jolle $Ue_1 = c$.*

Todistus. Koska $\mathrm{syt}(x, y) = 1$, on olemassa kokonaisluvut $\lambda, \mu \in \mathbb{Z}$ siten, että $\lambda x + \mu y = 1$. Jos valitaan

$$U = \begin{pmatrix} x & -\mu \\ y & \lambda \end{pmatrix},$$

niin $Ue_1 = (x, y)^T$ ja $\det(U) = 1$, eli $U \in GL_2(\mathbb{Z})$. □

Lemman 4.9 nojalla sen sijaan, että tarkistetaan onko $K\iota_i^T = \pm\kappa_j^T$, joillekin $K \in \langle R_1, \ldots, R_n \rangle$ ja $i, j \in \{1, \ldots, k\}$, voidaan tarkistaa onko $U^{-1}KUe_1 = \pm U^{-1}\kappa_j^T$, jollekin $U^{-1}KU \in \langle U^{-1}R_1U, \ldots, U^{-1}R_nU \rangle$, missä U on lemman 4.9 matriisi, kun $c = \iota_i$.

Lause 4.10. *Olkoot $a, b \in \mathbb{Z}$ suhteellisia alkulukuja ja $K \in GL_2(\mathbb{Z})$. Silloin*

$$Ke_1 = \begin{pmatrix} a \\ b \end{pmatrix}$$

jos ja vain jos K on muotoa AT^λ jollain $\lambda \in \mathbb{Z}$, missä

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

ja

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \quad tai \quad A = \begin{pmatrix} a & -c \\ b & -d \end{pmatrix},$$

missä c, d ovat kokonaisluvut, joille on voimassa $ad - bc = 1$.

Todistus. Oletetaan, että $Ke_1 = (a, b)^T$. Selvästi K on muotoa $\left(\begin{smallmatrix} a & x \\ b & y \end{smallmatrix}\right)$, missä $x, y \in \mathbb{Z}$ ja $ay - bx = \pm 1$. Koska nyt $\mathrm{syt}(a, b) = 1$, on olemassa luvut $c, d \in \mathbb{Z}$, joille $ad - bc = 1$. Jos $ay - bx = 1$, niin a jakaa erotuksen $(c - x)$ ja b jakaa erotuksen $(d - y)$. Olkoon $\lambda \in \mathbb{Z}$ siten, että $c - x = \lambda a$ ja $d - y = \lambda b$. Nyt

$$K = \begin{pmatrix} a & c \\ b & d \end{pmatrix} - \lambda \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}.$$

Jos merkitään

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \quad \text{ja} \quad B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix},$$

niin $K = A(I - \lambda A^{-1}B) = AT^{-\lambda}$.

Jos $ay - bx = -1$, niin a jakaa summan $(c+x)$ ja b jakaa summan $(d+y)$. Olkoon $\lambda \in \mathbb{Z}$ siten, että $c + x = \lambda a$ ja $d + y = \lambda b$. Nyt

$$K = \begin{pmatrix} a & -c \\ b & -d \end{pmatrix} - \lambda \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}.$$

Jos merkitään

$$A = \begin{pmatrix} a & -c \\ b & -d \end{pmatrix} \quad \text{ja} \quad B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix},$$

niin $K = A(I - \lambda A^{-1}B) = AT^{\lambda}$.

Toiseen suuntaan väite on ilmeinen, mikä nähdään suoraan laskemalla:

$$\begin{aligned} K \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} a & \pm c \\ b & \pm d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\lambda} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} a & \lambda a \pm c \\ b & \lambda b \pm d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}. \end{aligned}$$

□

Jos halutaan näyttää, että joukko F on kuoleva, riittää tarkistaa onko joillekin kokonaisluvuille $i, j \in \{1, 2, \ldots, k\}$ olemassa kokonaislukua λ, jolle $AT^{\lambda} \in \langle R_1, \ldots, R_n \rangle$, missä A on luvuista i ja j riippuvainen matriisi, jonka determinantti on ± 1 ja T on edellä määritelty matriisi.

Lause 4.11. *Olkoon $G \cong \mathbb{Z}_{p_1} * \ldots * \mathbb{Z}_{p_n}$ syklisten ryhmien $\mathbb{Z}_{p_i}$ vapaa tulo ja H sen rationaalinen osajoukko, joka on määritelty jonkun äärellisen automaatin avulla. Silloin ryhmän G yksikön sisältyminen rationaaliseen osajoukkoon H on ratkeavaa.*

Todistus. Lemman 2.10 nojalla ryhmällä G on monoidiesitys

$$\langle a_1, a_2, \ldots, a_n \mid a_1^{p_1} = a_2^{p_2} = \ldots = a_n^{p_n} = 1 \rangle.$$

Olkoon w sana yli generaattorien $a_1, a_2, \ldots, a_n$. Selvästi sitä vastaa yksikäsitteinen redusoitu sana u, jossa ei esiinny osasanaa $a_i^{p_i}$ millään $i \in \{1, \ldots, n\}$. Tämä sana u voidaan muodostaa soveltamalla sääntöä $a_i^{p_i} \to 1$ eli poistamalla osasanat $a_i^{p_i}$.

Olkoon $\mathcal{A}$ äärellinen automaatti, joka määrittelee ryhmän G rationaalisen osajoukon H. Riittää osoittaa, että jos automaatti hyväksyy sanan w, niin automaattia $\mathcal{A}$ voidaan muokata siten, että muokattu automaatti hyväksyy myös redusoidun sanan u. Tämä toteutetaan lisäämällä ε–siirros tilojen q ja q' välille, jos näiden kahden tilan välillä on polku sanalle $a_i^{p_i}$, jollain $i \in \{1, \ldots, n\}$. Siis kun $L \subset \{a_1, a_2, \ldots, a_n\}^*$ on osajoukko, jonka muutettu automaatti hyväksyy, silloin redusoitujen sanojen osajoukko on rationaalinen osajoukko $L \setminus (\{a_1, a_2, \ldots, a_n\}^*(a_1^{p_1} + \ldots + a_n^{p_n})\{a_1, a_2, \ldots, a_n\}^*)$. □

Seuraus 4.12. *Olkoon $G \cong \mathbb{Z}_{p_1} * \ldots * \mathbb{Z}_{p_n}$ syklisten ryhmien $\mathbb{Z}_{p_i}$ vapaa tulo. Olkoot $\mathcal{A}$, $\mathcal{B}$ automaatit, jotka hyväksyvät rationaaliset osajoukot $H, K \subseteq G$. Silloin on ratkeavaa onko leikkaus $H \cap K$ tyhjä vai ei.*

Todistus. Edellisen lauseen nojalla voidaan muodostaa automaatit $\mathcal{A}_H$ ja $\mathcal{A}_K$, jotka hyväksyvät ainoastaan vastaavien joukkojen redusoidut sanat. Nyt, koska jokaista sanaa vastaa yksikäsitteinen redusoitu sana, osajoukkojen H ja K leikkaus on epätyhjä jos ja vain jos automaatteja $\mathcal{A}_H$ ja $\mathcal{A}_K$ vastaavien rationaalisten kielten $L(\mathcal{A}_H)$ ja $L(\mathcal{A}_K)$ leikkaus on epätyhjä, joka on esimerkin 3.1 nojalla päätettävissä.. □

Lause 4.13. *Olkoon $Q \subseteq \mathcal{M}_2(\mathbb{Z})$ rationaalinen osajoukko ja matriisi $A \in GL_2(\mathbb{Z})$. On ratkeavaa onko $\{AT^m \mid m \in \mathbb{Z}\} \cap Q \neq \emptyset$, missä $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.*

Todistus. Osajoukko Q on rationaalinen lauseke $\mathcal{R}(X_1, \ldots, X_n)$ aakkoston $\{X_1, \ldots, X_n\}$ yli, johon on sovellettu sijoitusta φ, joka kuvaa jokaisen kirjaimen X_i matriisiksi joukosta $\mathcal{M}_2(\mathbb{Z})$. Sanotaan, että kirjaimen X determinantti on $\det(\varphi(X))$. Siispä, annetulle osajoukolle $\{AT^m \mid m \in \mathbb{Z}\}$ halutaan selvittää onko

$$\{AT^m \mid m \in \mathbb{Z}\} \cap \varphi(\mathcal{R}(X_1, \ldots, X_n)) \neq \emptyset \tag{3}$$

vai ei. Väite todistetaan peräkkäisillä yksinkertaistamisilla.

Väite 1. Voidaan rajoituksetta olettaa, että $A = I$. Nimittäin, jos X on uusi kirjain ja kuvaukseen φ lisätään $\varphi(X) = A^{-1}$, niin ehto (3) on ekvivalentti ehdon $\{T^m \mid m \in \mathbb{Z}\} \cap \varphi(X \cdot \mathcal{R}(X_1, \ldots, X_n)) \neq \emptyset$ kanssa. ■

Väite 2. Voidaan rajoituksetta olettaa, että jokaisen kirjaimen X_i determinantti on 1 tai -1, sillä $\det(T^m) = 1$ kaikille $m \in \mathbb{Z}$. ■

Väite 3. Voidaan rajoituksetta olettaa, että jokaisen kirjaimen X_i determinantti on 1. Nimittäin, voidaan olettaa, että kaikissa sanoissa, jotka lauseke $\mathcal{R}(X_1, \ldots, X_n)$ määrittelee on parillinen määrä kirjaimia X_i, joiden determinantti on -1.

Olkoon J osajoukko, joka koostuu indekseistä $1 \leq i \leq n$, joille $\det(\varphi(X_i)) = -1$. Silloin ehto (3) on ekvivalentti ehdon

$$\begin{aligned}\{T^m \mid m \in \mathbb{Z}\} \quad \cap \quad & \varphi(X \cdot \mathcal{R}(X_1, \ldots, X_n) \\ & \cap((\{X_i \mid i \notin J\}^*\{X_i \mid i \in J\}^*\{X_i \mid i \notin J\}^*)^2)) \neq \emptyset\end{aligned}$$

kanssa. Kuvauksen φ argumenttina oleva lauseke on rationaalinen. Lisäksi huomataan, että jokaiselle X_i ja X_k, missä $i \in J$ ja $k \notin J$, on olemassa yksikäsitteinen matriisi $Y_{i,k}$, jonka determinantti on 1 siten, että $\varphi(X_i)Y_{i,k} = \varphi(X_k)\varphi(X_i)$ on voimassa. Olkoon $X_{i,k}$ uusi kirjain, kun $i \in J$ ja $k \notin J$ ja laajennetaan kuvaus φ siten, että $\varphi(X_{i,k}) = Y_{i,k}$ kaikille uusille kirjaimille.

Olkoon τ kuvaus, joka muuntaa jokaisen rationaalisen lausekkeen $\mathcal{R}$ määräämän sanan seuraavanlaisesti. Olkoot X_{k_i} ja X_{k_j} mahdollisimman vasemmalla olevat kirjaimet, joille $k_i, k_j \in J$. Nyt sanan tekijä $X_{k_i}X_{k_i+1}\cdots X_{k_j-1}X_{k_j}$ korvataan tekijällä $X_{k_i,k_i+1}\cdots X_{k_i,k_j-1}X_{k_i}X_{k_j}$. Tätä toistetaan, niin kauan kuin sanasta löytyy termi X_{k_i}, $k_i \in J$, johon ei ole käytetty kuvausta τ. Esimerkiksi, kun $n = 4$, $J = \{2, 4\}$ ja sana $W = X_3X_2X_1X_3X_4X_3X_4X_1X_2$, niin $\tau(W) = X_3X_{2,1}X_{2,3}X_2X_4X_3X_{4,1}X_4X_2$.

On olemassa rationaalinen lauseke $\mathcal{R}'$ aakkoston $\{X_i \mid i = 1, \ldots n\} \cup \{X_{i,k} \mid i \in J, k \notin J\}$ yli, joka määrittää tarkalleen ne sanat, jotka saadaan, kun lauseketta $\mathcal{R}$ kuvataan funktiolla τ. Huomataan, että lausekkeen $\mathcal{R}'$ määritellyissä sanoissa kirjaimet X_i, missä $i \in J$ esiintyvät peräkkäisinä pareina. Lisäämällä uudet symbolit $Z_{i,k}$ kaikille tekijöille X_iX_k, kun $i, k \in J$ saadaan ekvivalentti rationaalinen lauseke $\mathcal{R}''$, jossa kirjaimet ovat X_i, kun $i \notin J$, $X_{i,k}$, kun $i \in J, k \notin J$ ja $Z_{i,k}$, kun $i, k \in J$. Kirjaimia $Z_{i,k}$ varten kuvaukseen φ lisätään säännöt $\varphi(Z_{i,k}) = \varphi(X_i)\varphi(X_k)$ kaikille $i, k \in J$. Tämä todistaa väitteen. ■

Edelliset kolme väitettä osoittavat, että voimme aloittaa rationaalisesta lausekkeesta $\mathcal{R}$ ja morfismista φ, joka kuvaa jokaisen kirjaimen X_i matriisiksi ryhmästä $SL_2(\mathbb{Z})$, joten voimme olettaa, että $\varphi(\mathcal{R})$ on ryhmän $SL_2(\mathbb{Z})$ rationaalinen osajoukko. Seurauksen 4.12 nojalla voimme tarkistaa onko leikkauksen $\{T^m \mid m \in \mathbb{Z}\} \cap \varphi(\mathcal{R})$ kuva ryhmässä $PSL_2(\mathbb{Z})$ epätyhjä. Jotta voidaan osoittaa, että $\{T^m \mid m \in \mathbb{Z}\} \cap \varphi(\mathcal{R}) \neq \emptyset$, pitää poistaa moniselitteisyys matriisien T^m ja $-T^m$ väliltä. Olkoon ψ kuvaus ryhmästä $SL_2(\mathbb{Z})$ ryhmään $\mathcal{M}_2(\mathbb{Z}/3\mathbb{Z})$, joka redusoi matriisin alkiot modulo 3. Nyt

$$\{T^m| \ m \in \mathbb{Z}\} \subseteq H = \left\{ A \in SL_2(\mathbb{Z}) \mid \psi(A) = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \bmod 3, i = 0, 1, 2 \right\}$$

ja $-T^m \notin H$. Joukko

$$Q = \left\{ W \in \{X_1, \ldots, X_n\}^* \mid \psi(\varphi(W)) = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \bmod 3, i = 0, 1, 2 \right\}$$

on rationaalinen joukko, sillä se on äärellisen joukon

$$\left\{ \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \bmod 3 \mid i = 0, 1, 2 \right\}$$

alkukuva. Siis $\{T^m \mid m \in \mathbb{Z}\} \cap \varphi(\mathcal{R}(X_1, \ldots, X_n)) = \emptyset$ jos ja vain jos

$$\{T^m \mid m \in \mathbb{Z}\} \cap \varphi(\mathcal{R}(X_1, \ldots, X_n) \cap Q) = \emptyset,$$

missä $\mathcal{R}(X_1, \ldots, X_n) \cap Q$ on rationaalinen, sillä se on kahden rationaalisen joukon leikkaus. Tämä todistaa väitteen. □

Nyt ollaan todistettu seuraava lause.

Lause 4.14. *Ongelma* MORT′(2) *on ratkeava.*

4.2 Ongelman MORT(2, 2) ratkeavuudesta

Tässä alaluvussa osoitetaan, että kahden 2×2 matriisin kuolevuus on ratkeavaa jopa silloin kun alkiot ovat rationaalilukuja. Artikkelissaan [26] Y. Saouter todisti, että ongelma on ratkeava, silloin kun matriisien ominaisarvot ovat reaalisia. O. Bournez ja M. Branicky todistivat ongelman ratkeavaksi kaikille rationaalisille matriiseille artikkelissaan [5].

Seuraava ratkeavuustulos on artikkelista [28].

Lemma 4.15. *Seuraava ongelma on ratkeava:*

SYÖTE:	*Rationaaliluvut* $p, q \in [-1, 1]$.
ONGELMA:	*Onko joillekin luvuille* $\theta \in \mathbb{R}$ *ja* $n \in \mathbb{N}$ *voimassa* $\cos(\theta) = p$ *ja* $\cos(n\theta) = q$*?*

Todistus. Olkoot $p = r/s$, $q = u/v$, missä luvut $r, s, u, v \in \mathbb{Z}$ ja $\text{syt}(r, s) = \text{syt}(u, v) = 1$. Jos $p \in \{0, \frac{1}{2}, 1\}$, niin niitä vastaavat kuvaukset säännöllä $n \mapsto \cos(n\theta)$ saavat vain äärellisen määrän eri arvoja. Tarkemmin sanottuna, vastaavat kuvajoukkot ovat $\{-1, 0, 1\}, \{-1, -\frac{1}{2}, \frac{1}{2}, 1\}$ ja $\{1\}$. Jos q on jokin näistä arvoista, niin kyseessä on positiivinen instanssi.

Oletetaan sitten, että $p \notin \{0, \frac{1}{2}, 1\}$. Arvo $\cos(n\theta)$ voidaan ilmaista polynomina, jossa on kokonaislukukertoimet ja luvun $\cos(\theta)$ potenssit. Nimittäin rekursiolla

$$\cos(n\theta) = 2\cos(\theta)\cos((n-1)\theta) - \cos((n-2)\theta) \tag{4}$$

hävitetään kaikki kulman θ monikerrat. Merkitään $\cos(n\theta) = p_n(r/s)$. Silloin $c_n = s^n p_n(r/s)$ on kokonaisluku, jolle on voimassa rekursioyhtälö

$$2rc_{n+1} - s^2 c_n = c_{n+2}, \tag{5}$$

kun $c_1 = r$ ja $c_2 = 2r^2 - s^2$. Tämä rekursio on yhtälö (4) kerrottuna puolittain luvulla s^2.

Oletetaan, että luku s ei ole luvun 2 potenssi. Silloin luvut s ja v voidaan esittää muodossa $s = 2^a b, v = 2^{a'} b'$, missä $a, a' \geq 0$ ja luvut $b > 1$ ja $b' \geq 1$ ovat parittomia. Yritämme löytää kokonaisluvun n, jolle on voimassa $c_n/(2^{an} b^n) = u/(2^{a'} b')$. Nyt $\text{syt}(c_n, b^n) = 1$ kaikille luonnollisille luvuille n. Nimittäin, jos joku pariton kokonaisluku d jakaa molemmat luvut s ja c_n, niin silloin d jakaa myös luvut $c_{n-1}, c_{n-2}, \ldots, c_2$ ja luvun r^2. Oletuksen nojalla $\text{syt}(r, s) = 1$, joten $d = 1$. Tämän seurauksena luku n toteuttaa ehdon $b' = b^n$.

Oletetaan sitten, että luku s on kahden potenssi eli $s = 2^k, k > 1$. Luku $k = 1$ ei käy, sillä oletimme, että $r/s \neq \frac{1}{2}$. Kirjoitetaan jokainen luku c_n muotoon $2^{\lambda_n} v_n$, jossa v_n on pariton kokonaisluku. Nyt rekursio (5) on

$$2^{\lambda_{n+1}+1} r v_{n+1} - 2^{\lambda_n + 2k} v_n = 2^{\lambda_{n+2}} v_{n+2}. \tag{6}$$

Osoitetaan, että on olemassa kokonaisluku n, jolle $\lambda_n + 1 < 2k + \lambda_{n-1}$. Nimittäin $r = c_1 = 2^{\lambda_1} v_1$, joten $\lambda_1 = 0$, ja $c_2 = 2r^2 - 2^{2k} = 2(r^2 - 2^{2k-1})$, joten $\lambda_2 = 1$. Nyt $1 + 1 < 2k + 0$ on aina voimassa, sillä $k > 1$.

Olkoon $n_0 = 1$. Se on pienin luonnollinen luku, jolle on voimassa $\lambda_{n_0+1} + 1 < 2k + \lambda_{n_0}$. Nyt yhtälö (6) saadaan muotoon

$$r v_{n_0+1} - 2^{\lambda_{n_0}+2k-\lambda_{n_0+1}-1} v_{n_0} = 2^{\lambda_{n_0+2}-\lambda_{n_0+1}-1} v_{n_0+2}.$$

Luvun n_0 valinnan nojalla, luvun v_{n_0} kerroin on parillinen, lisäksi luvut r ja v_{n_0+1} ovat parittomia, joten vasen puoli on pariton. Oikea puoli on pariton jos $\lambda_{n_0+2} - \lambda_{n_0+1} - 1 = 0$. Eli siis $\lambda_{n_0+2} = \lambda_{n_0+1} + 1$. Tästä seuraa, että $\lambda_{n_0+2} + 1 = \lambda_{n_0+1} + 2 < 2k + \lambda_{n_0+1}$. Tätä argumenttia toistamalla, kaikille kokonaisluvuille $h \geq 0$ on voimassa $\lambda_{n_0+2+h} = \lambda_{n_0+1+h} + 1$. Siispä jokaiselle positiiviselle kokonaisluvulle h on voimassa $\lambda_{n_0+h} = \lambda_{n_0} + h$.

Palataan takaisin alkuperäiseen ongelmaan, eli luvun n olemassaoloon, jolle $\cos(n\theta) = u/v$. Koska luvun $\cos(\theta)$ nimittäjä on 2^k, luvun v pitää olla luvun 2 potenssi. Oletetaan, että $v = 2^m$. On mahdollista, että on olemassa ratkaisu jollekin $n \leq n_0$. Jos $n > n_0$, ratkaisun $n = n_0 + h$ pitää toteuttaa

$$\cos((n_0 + h)\theta) = \frac{v_{n_0+h} 2^{\lambda_{n_0}+h}}{2^{k(n_0+h)}} = \frac{u}{2^m},$$

joten $k(n_0 + h) - \lambda_{n_0} - h = m$, josta voidaan ratkaista $h = (m + \lambda_{n_0} - kn_0)/(k - 1)$. Siispä ainoa mahdollinen lukua n_0 suurempi oleva ratkaisu on

$$n_0 + (m + \lambda_{n_0} - kn_0)/(k - 1),$$

jos se on kokonaisluku. □

Esimerkki 4.3. Tarkastellaan edellistä ongelmaa syötteillä $p = 3/4$ ja $q = -9/16$. Nyt $n_0 = 1$ ja $\lambda_{n_0} = 0$. Siispä ratkaisu on joko $n = 0, 1$ tai $n = 1 + \frac{4+0-2}{2-1} = 3$. Nyt

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta) = 4\left(\frac{3}{4}\right)^3 - 3 \cdot \frac{3}{4} = -\frac{9}{16} = q.$$

Olkoot $p = 5/6$ ja $q = 7/18$ ongelman syötteet. Luvun p nimittäjä $s = 2 \cdot 3$ ja luvun q nimittäjä $v = 2 \cdot 9$. Nyt $9 = 3^2$ ja

$$cos(2\theta) = 2\cos^2(\theta) - 1 = 2\left(\frac{5}{6}\right)^2 - 1 = \frac{7}{18} = q.$$

Lemma 4.16. *Olkoon A 2×2 matriisi, jonka alkiot ovat rationaalilukuja. Silloin Jordanin normaalimuodon similaarimatriisin P alkiot ovat*

(i) rationaalilukuja, jos $\operatorname{rank}(A) = 1$ *tai* $\operatorname{rank}(A) = 2$ *ja* λ *on ainoa ominaisarvo, tai*

(ii) kunnan $\mathbb{Q}(\lambda)$ *alkioita, jos matriisilla A on kaksi ominaisarvoa* λ, μ.

Todistus. Olkoon

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

ja

$$P = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

Jordanin normaalimuodon similaarimatriisi. Matriisi P toteuttaa yhtälön

$$PA = JP, \tag{7}$$

jossa matriisi J on matriisin A Jordanin normaalimuoto.

Olkoon $\operatorname{rank}(A) = 1$, silloin matriisin A ominaisarvo $\lambda = \operatorname{tr}(A) = a + d$. Luvut x, y, w ja z voidaan ratkaista yhtälöstä (7). Koska kaikki laskut tapahtuvat kunnassa $\mathbb{Q}$, myös luvut x, y, z ja w ovat rationaalilukuja.

Oletetaan sitten, että matriisin A aste on 2 ja sillä on yksi ominaisarvo λ. Silloin ominaisarvo $\lambda = tr(A)/2 = \frac{a+d}{2}$ ja siten rationaaliluku. Kuten edellisessäkin tapauksessa, similaarimatriisin alkiot ovat rationaalilukuja, sillä kaikki laskut tapahtuvat kunnassa $\mathbb{Q}$.

Oletetaan, että matriisin A aste on 2 ja sen ominaisarvot ovat λ, μ. Nyt $\lambda + \mu = tr(A) = a + d$, mutta ominaisarvot voivat olla kompleksilukuja. Ratkaisemalla ominaisarvot matriisin A karakteristisesta yhtälöstä, saadaan

$$\lambda = \frac{a + d + \sqrt{(a-d)^2 + 4bc}}{2}$$

ja

$$\mu = \frac{a + d - \sqrt{(a-d)^2 + 4bc}}{2}.$$

Nyt ominaisarvo μ voidaan esittää muodossa $\mu = a+d-\lambda$. Siis $\mu \in \mathbb{Q}(\lambda)$. Similaarimatriisin P alkiot voidaan ratkaista yhtälöstä (7), jolloin kaikki laskut tapahtuvat laajennuskunnassa $\mathbb{Q}(\lambda)$ ja täten $x, y, z, w \in \mathbb{Q}(\lambda)$. □

Lause 4.17. *Ongelma* MORT(2,2) *on ratkeava rationaalisille matriiseille.*

Todistus. Olkoon $F = \{A_1, A_2\}$ ongelman syöte. Voidaan rajoituksetta olettaa, että matriisin A_2 aste on suurempi kuin matriisin A_1. Jos molempien matriisien aste on 2, niin lemman 4.6 nojalla joukko F ei ole kuoleva. Jos matriisin A_1 aste on 0, niin F on triviaalisti kuoleva. Jos $\text{rank}(A_1) = \text{rank}(A_2) = 1$, niin lemman 4.6 nojalla riittää laskea tulot A_1^2, A_1A_2, A_2A_1 ja A_2^2.

Jäljelle jää tapaus, jossa matriisin A_2 aste on 2 ja matriisin A_1 aste on 1. Lemman 4.6 nojalla, F on kuoleva jos ja vain jos on olemassa luku $n \in \mathbb{N}$ jolle

$$A_1A_2^nA_1 = \mathcal{O}. \tag{8}$$

Tarkastellaan tätä muotoa olevaa tuloa käyttäen Jordanin normaalimuotoa matriiseista A_1 ja A_2. Merkitään $A_1 = P_1^{-1}J_1P_1$, $A_2 = P_2^{-1}J_2P_2$,

$$J_1 = \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix}$$

ja

$$J_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{tai} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},$$

jossa matriisit P_1 ja P_2 eivät ole singulaarisia. Ominaisarvo κ on rationaaliluku, sillä se on $\text{tr}(A)$. Ominaisarvot λ ja μ ovat matriisin A_2 karakteristisen polynomin kompleksiset juuret. Nyt yhtälö (8) on ekvivalentti yhtälön

$$P_1^{-1}J_1P_1P_2^{-1}J_2^nP_2P_1^{-1}J_1P_1 = \mathcal{O}$$

kanssa. Koska P_1 on kääntyvä, voidaan kirjoittaa yhtälö muotoon

$$J_1PJ_2^nP^{-1}J_1 = \mathcal{O},$$

missä

$$P = P_1P_2^{-1} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Sijoittamalla matriisien P, P^{-1}, J_1 ja J_2 arvot yhtälöön saadaan

$$\begin{aligned} J_1 P J_2^n P^{-1} J_1 &= \\ \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \lambda^n & 0 \\ 0 & \mu^n \end{pmatrix} \frac{1}{ps-qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix} &= \\ \frac{1}{ps-qr} \begin{pmatrix} ps\lambda^n\kappa^2 - qr\mu^n\kappa^2 & 0 \\ 0 & 0 \end{pmatrix} &= \mathcal{O} \end{aligned}$$

tai

$$\begin{aligned} J_1 P J_2^n P^{-1} J_1 &= \\ \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix} \frac{1}{ps-qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix} &= \\ \frac{1}{ps-qr} \begin{pmatrix} ps\lambda^n\kappa^2 - qr\lambda^n\kappa^2 - \lambda^{n-1}npr & 0 \\ 0 & 0 \end{pmatrix} &= \mathcal{O} \end{aligned}$$

riippuen matriisin J_2 muodosta. Nämä yhtälöt ovat ekvivalentit yhtälöiden

$$\begin{aligned} \begin{pmatrix} ps\lambda^n\kappa^2 - qr\mu^n\kappa^2 & 0 \\ 0 & 0 \end{pmatrix} &= \mathcal{O} \\ \begin{pmatrix} ps\lambda^n\kappa^2 - qr\lambda^n\kappa^2 - \lambda^{n-1}npr & 0 \\ 0 & 0 \end{pmatrix} &= \mathcal{O} \end{aligned}$$

kanssa.

Nyt alkuperäinen ongelma on ekvivalentti sen kanssa, että on olemassa luku $n \in \mathbb{N}$, jolle

(i) $ps\lambda^n - qr\mu^n = 0$, jos matriisilla A_2 on kaksi eri ominaisarvoa, tai

(ii) $(ps-qr)\kappa^2\lambda - rpn = 0$, jos matriisilla A_2 on yksi ominaisarvo.

Oletetaan ensin, että matriisilla A_2 on yksi ominaisarvo. Ominaisarvo λ on rationaaliluku ja lemman 4.16 nojalla myös luvut p, q, r, s ovat rationaalilukuja, jotka voidaan esittää alkuperäisten matriisien A_1 ja A_2 alkioiden avulla. Nyt luvun n olemassaolo on helposti tarkistettavissa. Nimittäin riittää tarkistaa onko $n = \frac{(ps-qr)\kappa^2\lambda}{rp}$ kokonaisluku.

Oletetaan sitten, että matriisilla A_2 on kaksi eri ominaisarvoa. Huomataan, että ominaisarvot $\lambda \neq 0$ ja $\mu \neq 0$, sillä matriisin A_2 aste on 2. Kuten lemmassa 4.16 todettiin luvut λ, μ, p, q, r ja s voivat olla kompleksilukuja ja kuuluvat laajennuskuntaan $\mathbb{Q}(\lambda)$. Toisin sanoen, ne ovat muotoa $a + \lambda b$ joillekin luvuille $a, b \in \mathbb{Q}$, jotka voidaan ratkaista matriisien A_1 ja A_2 alkioista. Nyt tapaukset $ps = 0$ tai $qr = 0$ ovat triviaalit, sillä silloin ratkaistaan $ps\lambda^n = 0$ tai $qr\mu^n = 0$ kunnassa $\mathbb{Q}(\lambda)$.

Tarkastellaan tapausta $ps \neq 0$ ja $qr \neq 0$. Tehtävänä on löytää kokonaisluku n, jolle $(\lambda/\mu)^n = (pq)/(rs)$. Selvästi $|\lambda/\mu|^n = |pq|/|rs|$. Jos $|\lambda/\mu| \neq 1$, luvun n on oltava $(\log|pq| - \log|rs|)/\log|\lambda/\mu|$. Tämä on helposti tarkastettavissa. Oletetaan, että $|\lambda/\mu| = 1$ ja ominaisarvot λ ja μ ovat reaalilukuja, silloin välttämättä $\lambda = \pm\mu$. Tällöin kokonaisluvun n on toteutettava $(\pm 1)^n = (pq/rs)$, joka on laskettavissa.

Jos $|\lambda/\mu| = 1$ ja $|pq|/|rs| \neq 1$, niin silloin ratkaisua ei ole.

Jäljelle jää tapaus, jossa ominaisarvot λ ja μ ovat kompleksilukuja, joille $|\lambda/\mu| = 1$, ja $|pq|/|rs| = 1$. Kuten lemman 4.16 todistuksessa todettiin, $\lambda = \frac{a+d+\sqrt{(a+d)^2+4bc}}{2}$ ja $\mu = \frac{a+d-\sqrt{(a+d)^2+4bc}}{2}$. Koska nämä luvut ovat kompleksisia, ne voidaan kirjoittaa muotoon $\lambda = \frac{a+d}{2} + ti$ ja $\mu = \frac{a+d}{2} - ti$, jollekin $t \in \mathbb{R}$. Huomataan, että λ ja μ ovat liittolukuja, joiden reaaliosa on rationaaliluku. Siispä myös kompleksilukujen λ/μ ja $(pq)/(rs)$ reaaliosat ovat rationaalilukuja. Olkoon θ luvun λ/μ napakoordinaattiesityksen kulma. Koska luvun λ/μ pituus on 1, niin sen reaaliosa $p' = \cos\theta$. Kokonaisluku n toteuttaa $\cos(n\theta) = r'$, jossa r' on luvun $(pq)/(rs)$ reaaliosa. Tämä on lemman 4.15 nojalla ratkeavaa. Näin on käyty kaikki tapaukset ja siis ongelma $\textsc{Mort}(2, 2)$ on ratkeava, mikä oli todistettava. □

4.3 Matriisien lukumäärän vaikutus ratkeavuuteen

Tässä osiossa tarkastellaan matriisien kuolevuuden ratkeavuutta matriisien lukumäärän näkökulmasta. Käytetään merkintää $\textsc{Mort}(n, m)$ kuoveluusongelmasta, jonka syötteenä on m kappaletta $n \times n$ kokonaislukumatriisia. Siis ongelma $\textsc{Mort}(n, m)$ määritellään seuraavanlaisesti.

MORT(n, m)	
SYÖTE:	Matriisijoukko $\{M_1, M_2, \ldots, M_m\}$,
	jossa jokainen matriisi on kokoa $n \times n$.
ONGELMA:	Onko $M_{i_1} M_{i_2} \cdots M_{i_j} = \mathcal{O}$ jollain indeksijonolla $i_1, \ldots, i_j$?

Ei tiedetä onko ongelma MORT$(2, m)$ ratkeava vai ei, mutta edellisessä alaluvussa osoitettiin, että ongelma MORT$(2, 2)$ on ratkeava.

Ongelma MORT$(3, m)$ tiedetään ratkeamattomaksi, mutta tarkkaa alarajaa luvulle m ei tiedetä. Lauseen 4.2 todistuksessa käytetään $2p+1$ matriisia, jossa p on ongelman PCP dominoiden lukumäärä. Artikkelissaan [19] Y. Matiyasevich ja G. Sénizergues osoittivat, että PCP on ratkeamaton kun syötteenä on 7 dominoa, joten ongelma MORT$(3, 15)$ on ratkeamaton. Artikkelin [5] tarkempi analyysi paljastaa, että ongelma on ratkeamaton jo kahdeksalle 3×3 matriisille. V. Halava, T. Harju ja M. Hirvensalo osoittivat artikkelissaan [12], että ongelma MORT$(3, 7)$ on ratkeamaton.

Lause 4.18 ([12])**.** *Ongelma* MORT$(3, 7)$ *on ratkeamaton.*

Seuraavaksi osoitetaan, että ongelman MORT$(3, 7)$ ratkeamattomuudesta seuraa, että myös ongelmat MORT$(21, 2)$, MORT$(12, 3)$, MORT$(9, 4)$ ja MORT$(6, 5)$ ovat ratkeamattomia.

Seuraus 4.19. *Ongelma* MORT$(21, 2)$ *on ratkeamaton.*

Todistus. Merkitään $\mathcal{O} = \mathcal{O}_3$ ja $I = I_3$. Osoitetaan, että matriisipari

$$M = \begin{pmatrix} A_1 & \mathcal{O} & \cdots & \mathcal{O} \\ \mathcal{O} & A_2 & \cdots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \cdots & A_7 \end{pmatrix}_{21x21}, \; P = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & I \\ I & \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} \\ \mathcal{O} & I & \mathcal{O} & \cdots & \mathcal{O} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathcal{O} & \cdots & \mathcal{O} & I & \mathcal{O} \end{pmatrix}_{21x21},$$

missä $A_1, \ldots, A_1 \in \mathcal{M}_3(\mathbb{Z})$, on kuoleva jos ja vain joukko $\{A_1, \ldots, A_7\}$ on kuoleva.

Tarkastellaan tuloja $P^{7-k+1} M P^{k-1}$, kun $k \in \{1, \ldots, 7\}$. Matriisissa $P^{7-k+1} M P^{k-1}$ päädiagonaalilla on $A_k, \ldots, A_7, A_1, \ldots, A_{k-1}$, ja muualla on

nollaa. Esimerkiksi

$$P^6MP = \begin{pmatrix} A_2 & \mathcal{O} & \cdots & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_3 & \cdots & \mathcal{O} & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{O} & \mathcal{O} & \cdots & A_7 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & A_1 \end{pmatrix}, \; P^5MP^2 = \begin{pmatrix} A_3 & \mathcal{O} & \cdots & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_4 & \cdots & \mathcal{O} & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{O} & \mathcal{O} & \cdots & A_1 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & A_2 \end{pmatrix}.$$

Lisäksi matriisien M ja P mielivaltainen tulo C voidaan kirjoittaa muodossa

$$C = P^{7-k_1+1}MP^{k_1-1} \cdots P^{7-k_n+1}MP^{k_n-1},$$

sillä $P^7 = I_{21}$. Matriisissa C päädiagonaalin alkiot ovat matriisien $A_1, \ldots, A_7$ tuloja. Siispä $\{M, P\}$ on kuoleva jos ja vain jos $\{A_1, \ldots, A_7\}$ on kuoleva. Koska ongelma MORT$(3, 7)$ ei ole ratkeava, ongelma MORT$(21, 2)$ ei myöskään ole ratkeava. □

Seuraus 4.20. *Ongelma* MORT$(12, 3)$ *on ratkeamaton.*

Todistus. Kuten edellisen seurauksen todistuksessakin, merkitään $\mathcal{O}$ on 3×3 nollamatriisi ja I on 3×3 identiteettimatriisi. Osoitetaan, että matriisikolmikko

$$M_1 = \begin{pmatrix} A_1 & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_2 & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & A_3 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{O} & A_4 \end{pmatrix}, M_2 = \begin{pmatrix} A_5 & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_6 & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & A_7 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{O} & I \end{pmatrix}, P = \begin{pmatrix} \mathcal{O} & \mathcal{O} & \mathcal{O} & I \\ I & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & I & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & I & \mathcal{O} \end{pmatrix},$$

missä $A_1, \ldots, A_7 \in \mathcal{M}_3(\mathbb{Z})$, on kuoleva jos ja vain jos joukko $\{A_1, \ldots, A_7\}$ on kuoleva. Jälleen, tulossa $P^{4-k+1}M_1P^{k-1}$ (vast. $P^{4-k+1}M_2P^{k-1}$) päädiagonaalilla on A_1, A_2, A_3, A_4 (vast. A_5, A_6, A_7, I) syklisesti permutoituna.

Edelleen, tulossa $\prod_{i \in J} X_i$, missä jokainen $X_i \in \{P^{4-k+1}M_jP^{k-1} \mid k \in \mathbb{Z}, j \in \{1, 2\}\}$, on nollaa päädiagonaalilla jos ja vain jos joukko $\{A_1, \ldots, A_7\}$ on kuoleva samoilla indekseillä. Siispä $\{M_1, M_2, P\}$ on kuoleva jos ja vain jos $\{A_1, \ldots, A_7\}$ on kuoleva. Koska ongelma MORT$(3, 7)$ ei ole ratkeava, ongelma MORT$(12, 3)$ ei myöskään ole ratkeava. □

Seuraus 4.21. *Ongelma* MORT$(9, 4)$ *on ratkeamaton.*

Todistus. Edellisten seurauksien ideaa ja merkintöjä käyttäen osoitetaan, että matriisijoukko $\{M_1, M_2, M_3, P\}$, missä

$$M_1 = \begin{pmatrix} A_1 & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_2 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & A_3 \end{pmatrix}, \quad M_2 = \begin{pmatrix} A_4 & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & A_5 & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & A_6 \end{pmatrix},$$
$$M_3 = \begin{pmatrix} A_7 & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & I & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & I \end{pmatrix}, \qquad P = \begin{pmatrix} \mathcal{O} & \mathcal{O} & I \\ I & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & I & \mathcal{O} \end{pmatrix},$$

on kuoleva jos ja vain jos joukko $\{A_1, \ldots, A_7\}$ on kuoleva. Jälleen, tulossa $P^{3-k+1}M_iP^{k-1}$ on päädiagonaalilla matriisien (A_1, A_2, A_3), (A_4, A_5, A_6) tai (A_7, I, I) syklinen permutaatio.

Kuten edellisissäkin seurauksissa tulossa $\prod_{i\in J} X_i$, missä jokainen $X_i \in \{P^{3-k+1}M_jP^{k-1} \mid k \in \mathbb{Z}, j \in \{1,2,3\}\}$, on nollaa päädiagonaalilla jos ja vain jos joukko $\{A_1, \ldots, A_7\}$ on kuoleva samoilla indekseillä. Siispä joukko $\{M_1, M_2, M_3, P\}$ on kuoleva jos ja vain jos $\{A_1, \ldots, A_7\}$ on kuoleva. Koska ongelma MORT$(3, 7)$ ei ole ratkeava, ongelma MORT$(9, 4)$ ei myöskään ole ratkeava. □

Lause 4.22. *Ongelma* MORT$(6, 5)$ *on ratkeamaton.*

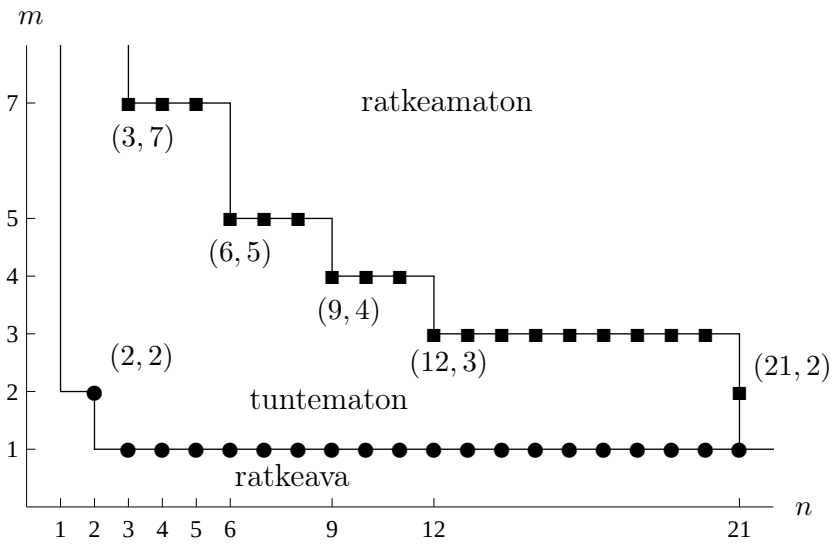
Todistus. Edellisten seurauksien ideaa ja merkintöjä käyttäen osoitetaan, että matriisijoukko $\{M_1, \ldots, M_4, P\}$, missä

$$M_1 = \begin{pmatrix} A_1 & \mathcal{O} \\ \mathcal{O} & A_2 \end{pmatrix}, \quad M_2 = \begin{pmatrix} A_3 & \mathcal{O} \\ \mathcal{O} & A_4 \end{pmatrix}, \quad M_3 = \begin{pmatrix} A_5 & \mathcal{O} \\ \mathcal{O} & A_6 \end{pmatrix},$$
$$M_4 = \begin{pmatrix} A_7 & \mathcal{O} \\ \mathcal{O} & I \end{pmatrix}, \qquad P = \begin{pmatrix} \mathcal{O} & I \\ I & \mathcal{O} \end{pmatrix},$$

on kuoleva jos ja vain jos matriisijoukko $\{A_1, \ldots, A_7\}$ on kuoleva. Tulo $\prod_{i\in J} X_i$, missä jokainen $X_i \in \{M_1P^k, \ldots, M_4P^k\}$, on nollamatriisi jos ja vain jos joukko $\{A_1, \ldots, A_7\}$ on kuoleva. Siispä $\{M_1, M_2, M_3, M_4, P\}$ on kuoleva jos ja vain jos $\{A_1, \ldots, A_7\}$ on kuoleva. Koska ongelma MORT$(3, 7)$ ei ole ratkeava, ongelma MORT$(6, 5)$ ei myöskään ole ratkeava. □

Lause 4.23. *Ongelma* MORT$(n, 1)$ *on ratkeava kaikille* $n \geq 1$.

Todistus. Olkoon $A \in \mathcal{M}_n(\mathbb{Z})$. Lineaarialgebrasta tiedetään, että jokainen neliömatriisi toteuttaa oman karakteristisen yhtälönsä. Tarkemmin $p(A) = \mathcal{O}$, missä $p(t)$ on matriisin A karakteristinen polynomi ja sen aste on korkeintaan n. Jos $p(t) = t^k$, missä $k \leq n$, niin $p(A) = A^k = \mathcal{O}$ ja siis joukko $\{A\}$ on kuoleva. Jos taas polynomi $p(t) = t^k + p'(t)$, missä $k \leq n$ ja polynomi $p'(t)$ ei ole nollapolynomi, jonka aste on korkeintaan $k - 1$, niin $p(A) = A^k = p'(A) \neq \mathcal{O}$ ja siis joukko $\{A\}$ ei ole kuoleva. Siispä ongelma MORT$(n, 1)$ on ratkeava. □



Kuva 10: Ongelman MORT(n, m) tunnetut rankeavuusrajat.

Tarkkoja ratkeavuuden ja ratkeamattomuuden rajoja ei tunneta muille kun $n \geq 21$ matriiseille. Nimittäin edellisten lauseiden nojalla kaikille $n \geq 21$ ongelma MORT$(n, 2)$ ei ole ratkeava ja ongelma MORT$(n, 1)$ on. Kuvassa 10 on esitetty tunnetut ratkeavuusrajat. Tunnetut ratkeamattomat ongelmat on merkattu neliöillä ja ratkeavat ympyröillä.

5 Lopuksi

Tässä tutkielmassa tarkasteltiin ratkeavuustuloksia keskittyen erityisesti matriisien kuolevuusongelmaan.

Lauseessa 4.2 ja seurauksessa 4.3 osoitettiin, että ongelma on ratkeamaton $n \times n$ kokonaislukumatriiseille, kun $n \geq 3$. Matriisien koon ollessa 2×2 ongelma on avoin. Julkaisussaan [7] J. Cassaigne, J. Karhumäki ja T. Harju ovat osoittaneet, että todistuksen 4.2 tekniikkaa ei voi käyttää 2×2 matriisien tapauksessa.

Luvussa 4.1 todistettiin, että 2×2 kokonaislukumatriisien kuolevuus on ratkeavaa, kun rajoitutaan matriiseihin, joiden determinantti on 0 tai ±1. On mielenkiintoista onko vastaava tulos voimassa $n \times n$ matriiseille.

Viimeisessä alaluvussa tarkasteltiin $n \times n$ matriisien kuolevuutta, kun syötteenä on m matriisia. Koon ollessa 3×3 ratkeamattomuuden paras alaraja on 7 matriisin joukko. Lisäksi todistettiin, että ongelmat $\textsc{Mort}(21, 2)$, $\textsc{Mort}(12, 3)$, $\textsc{Mort}(9, 4)$ ja $\textsc{Mort}(6, 5)$ ovat ratkeamattomia. Luvussa 4.2 todistettiin, että kahden 2×2 kokonaislukumatriisin kuolevuus on ratkeavaa. Tällä hetkellä ei tiedetä missä menee $n \times n$ matriisiparin kuolevuuden tarkka ratkeavuusraja. Kuvassa 10 on esitetty tunnetut rajat ongelmalle $\textsc{Mort}(n, m)$.

Ongelmien $\textsc{Mort}(21, 2)$, $\textsc{Mort}(12, 3)$, $\textsc{Mort}(9, 4)$ ja $\textsc{Mort}(6, 5)$ todistuksissa käytettiin ongelman $\textsc{Mort}(3, 7)$ ratkeavuutta. Artikkelissa [6] on osoitettu, että ongelman $\textsc{Mort}(3, m)$ ratkeamattomuudesta seuraa, että ongelma $\textsc{Mort}(3m, 2)$ on ratkeamaton. Tämä tulos voidaan yleistää, jolloin ongelmat $\textsc{Mort}(3k, \lceil \frac{m}{k} \rceil + 1)$ ovat ratkeamattomia jos ongelma $\textsc{Mort}(3, m)$ on ratkeamaton.

Artikkelissaan [5] O. Bournez ja M. Branicky todistivat, että kahden 2×2 reaalisen matriisin kuolevuus ei ole ratkeavaa käyttäen pelkkiä aritmeettisia laskutoimituksia.

Luvussa 3 määriteltiin deterministiset Turingin koneet. Turingin koneet voidaan myös olla epädeterministisiä samalla tavalla kuin äärelliset automaatit. Kuten äärellisten automaattien tapauksessa, deterministisella Turingin koneella voi simuloida epädeterminististä Turingin konetta. On luontevaa

puhua Turingin koneiden aikakompleksisuudesta. Olkoon f funktio $\mathbb{N} \to \mathbb{N}$. Sanotaan, että kieli L hyväksytään ajassa f, jos on olemassa Turingin kone M, joka hyväksyy sanan $w \in L$ käyttäen korkeintaan $f(|w|)$ askelta. Edelleen, kieli L voidaan hyväksyä deterministisesti tai epädeterministisesti, jolloin vastaavat luokat ovat

$$\begin{aligned} TIME(f) &= \{L \subseteq \Sigma^* \mid L \text{ hyväksytään ajassa } f \text{ käyttäen} \\ &\qquad \text{determinististä Turingin konetta}\} \\ NTIME(f) &= \{L \subseteq \Sigma^* \mid L \text{ hyväksytään ajassa } f \text{ käyttäen} \\ &\qquad \text{epädeterminististä Turingin konetta}\}. \end{aligned}$$

Erityisen tärkeät aikakompleksisuusluokat ovat determinististen polynomiaikaisten algoritmien joukko

$$\mathrm{P} = \bigcup_{i \geq 1} TIME(P_i)$$

ja epädeterminististen polynomiaikaisten algoritmien joukko

$$\mathrm{NP} = \bigcup_{i \geq 1} NTIME(P_i),$$

missä P_i on polynomi $P_i(n) = n^i$ kaikilla indekseillä i.

Määritellään seuraavaksi polynomiaikainen reduktio. Ongelma P redusoituu ongelmaan P' polynomiajassa, jos on olemassa deterministinen TM M_t siten, että

(i) M_t toimii polynomiajassa, ja

(ii) M_t muuttaa mielivaltaisen instanssin i ongelmasta P ongelman P' instanssiksi $M_t(i)$ siten, että i on ongelman positiivinen instanssi jos ja vain jos $M_t(i)$ on ongelman P' positiivinen instanssi.

Tästä käytetään merkintää $P \leq_p P'$ ja sanotaan, että ongelma P p-redusoituu ongelmaan P'.

Ongelma P' on NP-kova, jos jokainen ongelma luokasta NP p-redusoituu siihen. NP-kovien ongelmien olemassaolo ei ole ilmeistä, mutta sitä ei käydä

tässä tutkielmassa läpi. Ongelma on NP-täydellinen, jos se on NP-kova ja kuuluu luokkaan NP. Lisää kompleksisuusteoriasta voi lukea luentomonisteesta [16] tai kirjasta [29].

Artikkelissaan [3] P. Bell, M. Hirvensalo ja I. Potapov osoittivat, että kokonaislukumatriisien kuolevuusongelma on NP-kova, jopa silloin kuin rajoitutaan matriiseihin, joiden determinantit ovat $0, \pm 1$, eli ongelman MORT'(2) matriiseihin.

Ongelma k-MORT(n, m) on kuolevuusongelma, jossa vaaditaan, että matriisitulossa on k matriisia. On selvää, että tämä ongelma on ratkeava. Nimittäin on olemassa vain äärellinen määrä erilaisia tuloja, joista laskemalla voidaan todeta onko jokin niistä nollamatriisi. Tämä ongelma kuuluu luokkaan NP ja artikkelissaan [4] V. Blondel ja J. Tsitsiklis osoittivat, että ongelma k-MORT$(n, 2)$ on NP-täydellinen.

Artikkelissaan [5] O. Bournez ja M. Branicky osoittivat, että ongelma MORT$_2(\mathbb{Q})$ on ekvivalentti ongelman ZITC, jossa kysytään onko annettujen matriisien jossain tulossa 0 vasemmassa yläkulmassa, kanssa.

ZITC

SYÖTE:	Äärellinen matriisijoukko $\{M_1, M_2, \ldots, M_k\}$, jossa jokainen matriisi on kokoa 2×2.
ONGELMA:	Onko $M_{i_1} M_{i_2} \cdots M_{i_j} = C$ jollain indeksijonolla $i_1, i_2, \ldots, i_j$ siten, että $C_{11} = 0$?

Kirjallisuutta

[1] K. M. Abadir, J. R. Magnus: *Matrix Algebra*. Cambridge University Press. 2005.

[2] Z. Bavel: *Introduction to the Theory of Automata*. Reston Pub Co. 1983.

[3] P. C. Bell, M. Hirvensalo, I. Potapov: *Mortality for* 2×2 *matrices is NP-Hard*, Proceedings of the 37th international conference on Mathematical Foundations of Computer Science, ss. 148–159. 2012.

[4] V. Blondel, J. Tsitsiklis: *When is a pair of matrices mortal?*, Information Processing Letters, 63, ss. 283–286. 1997.

[5] O. Bournez, M. Branicky: *The Mortality Problem for Matrices of Low Dimensions*. Theory of Computing Systems, 35(4), ss. 433–488. 2002.

[6] J. Cassaigne, J. Karhumäki: *Examples of undecidable problems for 2-generator matrix semigroups*. TUCS Technical Reports 57. 1996.

[7] J. Cassaigne, J. Karhumäki, T. Harju: *On the decidability of the freeness of matrix semigroups*. TUCS Technical Reports 56. 1996.

[8] C. Choffrut, J. Karhumäki: *Some decision problems on integer matrices*. RAIRO Informatique Théorique et Applications, 39(1), ss. 125–131. 2005.

[9] A. Church: *An unsolvable problem of elementary number theory*. American Journal of Mathematics, 58(2), ss. 345–363. 1936.

[10] K. Gödel: *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*. Monatshefte für Mathematik und Physik 38, ss. 173-–198. 1931

[11] V. Halava: *Decidable and Undecidable Problems in Matrix Theory*. Pro Gradu - tutkielma. Turun Yliopisto. 1997.

[12] V. Halava, T. Harju, M. Hirvensalo: *Undecidability Bounds for Integer Matrices using Claus Instances*. TUCS Technical Reports 766. 2006.

[13] V. Halava, M. Hirvensalo: *Improved Matrix Pair Undecidability Results*. TUCS Technical Reports 799. 2006.

[14] T. Harju: *Semigroups*. Luentomoniste, Turun Yliopisto. 2010.

[15] J. Kari: *Automata and formal languages*. Luentomoniste, Turun Yliopisto. 2011.

[16] J. Karhumäki: *Algorithmic Complexity*. Luentomoniste, Turun Yliopisto. 2006.

[17] M. V. Lawson: *Finite Automata*. Chapman and Hall/CRC. 2004.

[18] J. M. Lee: *Introduction to Topological Manifolds*. Springer-Verlag. 2000.

[19] Y. Matiyasevich, G. Sénizergues: *Decision problems for semi-Thue systems with a few rules*. Theoretical Computer Science, 330(1), ss. 145–169. 2005.

[20] C. Nuccio, E. Rodaro: *Mortality Problem for* 2×2 *Integer Matrices*. Proceedings of the 34th conference on Current trends in theory and practice of computer science, ss. 400–405. 2008.

[21] M. S. Patterson: *Unsolvability in* 3×3 *matrices*. Studies in Applied Mathematics, 49, ss. 105–107. 1970.

[22] E. L. Post: *A variant of a recursively unsolvable problem*. Bulletin of the American Mathematical Society, 52(4), ss. 264–268. 1946

[23] D. J. S. Robinson: *A Course in the Theory of Groups*, 2. painos. Springer-Verlag. 1995.

[24] Y. Rogozhin: *Small Universal Turing Machines*. Theoretical Computer Science, 168(2), ss. 215-–240. 1996

[25] J. J. Rotman: *An Introduction to the Theory of Groups*. Ally and Bacon Inc., 1965.

[26] Y. Saouter: *The mortality of a pair of* 2×2 *matrices is decidable*. Technical Report RR-2842, Institut National de Recherche en Informatique et en Automatique. 1996.

[27] P. Schultz: *Mortality of* 2×2 *matrices*. American Mathematical Monthly, 84(2), ss. 463–464. 1977.

[28] H. S. Shank: *The rational case of a matrix problem of Harrison*. Discrete Mathematics, 28, ss. 207–212. 1979.

[29] M. Sipser: *Introduction to the Theory of Computation*. Thomson Course Technology. 2006

[30] A. M. Turing: *On computable numbers, with an application to the Entscheidungsproblem*. Proceedings of the London Mathematical Society, 42(2), ss. 230-–265. 1937.

[31] H. Väliaho: *An Elementary Approach to the Jordan Form of a Matrix*. The American Mathematical Monthly, 93(9), ss. 711–714. 1986.