AUTOMAATTIEN SYNKRONISAATIOSTA

Johan Kopra

Pro gradu -tutkielma
Huhtikuu 2015

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

KOPRA, JOHAN: Automaattien synkronisaatiosta
Pro gradu -tutkielma, 46 s.
Matematiikka
Huhtikuu 2015

Tässä tutkielmassa tarkastellaan eräitä synkronisoituviin automaatteihin liittyviä ongelmia. Pääpaino on Černýn konjektuurissa ja tienväritysongelmassa, joiden lisäksi käsitellään myös hybridikonjektuuria.

Černýn konjektuuri on otaksuma, jonka mukaan jokainen synkronisoituva n-tilainen automaatti voidaan synkronisoida enintään pituutta $(n-1)^2$ olevalla sanalla. Ongelma on ollut avoin 1970-luvulta asti, mutta useita osatuloksia on todistettu. Tutkielmassa esitetään niistä tärkeimmät.

Tienväritysongelma koskee sitä, millaisista suunnatuista graafeista voidaan muodostaa synkronisoituvia automaatteja. Vuonna 2009 todistetun tienvärityslauseen mukaan synkronisoituvia automaatteja voidaan muodostaa ns. primitiivisistä graafeista. Tutkielmassa esitetään tienvärityslauseen todistus.

Hybridikonjektuuri on vuonna 2010 esitetty otaksuma, jossa on yhdistetty elementtejä Černýn konjektuurista ja tienvärityslauseesta. Hybridikonjektuurin mukaan jokaisesta n solmua sisältävästä primitiivisestä graafista voidaan muodostaa synkronisoituva automaatti, jonka lyhimmän synkronisoivan sanan pituus on enintään $n^2 - 3n + 3$. Tutkielmassa esitetään tunnettuja osatuloksia sekä johdetaan uusi alaraja Eulerin graafeille.

Asiasanat: automaattien teoria, synkronisoituvat automaatit, Černýn konjektuuri, tienväritysongelma, hybridikonjektuuri, Perronin-Frobeniuksen lause.

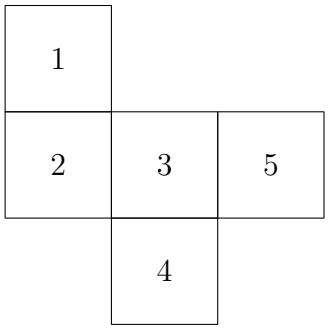
Sisältö

1 Johdanto

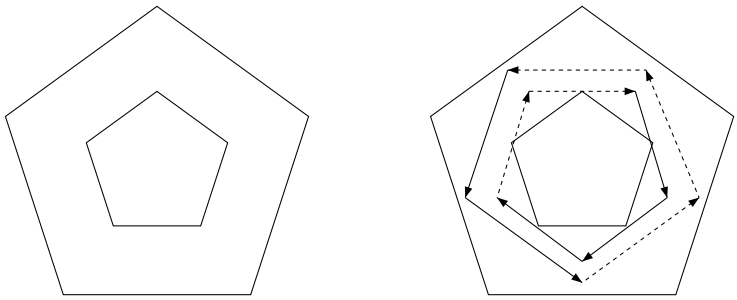
Automaattien teoriassa tutkimuksen kohteena ovat systeemit, joille annetaan komentoja (esimerkiksi kaukosäätimellä), ja jotka muuttavat tilaansa saamiensa komentojen perusteella. Tilalla voidaan tarkoittaa konkreettista sijaintia (esimerkiksi teollisuusrobotti voi sijaita kaukosäätimen välityksellä annetuista komennoista riippuen eri kohdissa tuotantolinjan varrella) tai jotakin abstraktia tilaa (esimerkiksi tietokoneen virtapiireissä voi tapahtua jännitemuutoksia näppäimistöllä kirjoittamisen seurauksena). Tärkeän automaattien luokan muodostavat synkronisoituvat automaatit, joiden tutkimus on alkanut vuonna 1964 Černý:n artikkelista [4]. Karkeasti sanottuna synkronisoituvalla automaatilla tarkoitetaan systeemiä, joka voidaan jollakin toimintosarjalla "synkronisoida", eli saattaa haluttuun tilaan riippumatta siitä, mikä systeemin tila on aloitettaessa. Havainnollistetaan tätä esimerkillä, jonka idea on kirjan [15] luvusta 4.4.

Tarkastellaan robottipölynimuria, jonka tarkoituksena on siivota huone, jonka pohjapiirustus on kuvassa 1. Huone on jaettu ruutuihin ja jokainen imurille annettava komento (oikea, vasen, ylös, alas) siirtää imuria yhden ruudun verran vastaavaan suuntaan. Jos komennon määrämässä suunnassa on seinä, niin imuri yrittää liikkua seinää päin eikä sen olinpaikka siis muutu. Oletetaan nyt, että imurilla ei ole sensoreita ja että se on ennen käynnistämistä päätynyt satunnaiseen paikkaan. (Sensoreiden lisääminen kasvattaa imurin valmistuskustannuksia, joten niiden puuttuminen on realistinen oletus.) Imurin on hyödyllistä olla selvillä omasta sijainnistaan. Sijainnin selvittämiseksi ohjelmoidaan imuri etukäteen suorittamaan käynnistyksen yhteydessä toimintosarja alas-oikea-ylös-oikea, joka siirtää imurin ruutuun 5 riippumatta siitä, mistä ruudusta se aloittaa.

Esimerkissä imuri saa varman tiedon sijainnistaan neljästä komennosta koostuvan toimintosarjan seurauksena. Tutkielman luvussa 4 tarkastellaan



Kuva 1: Huoneen pohjapiirustus.



Kuva 2: Silmukka ennen ja jälkeen maalauksen. Yhtenäinen nuoli tarkoittaa mustaa väriä, katkonainen nuoli valkoista.

sitä, kuinka pitkiä lyhimmät synkronisoivat toimintosarjat voivat olla sellaisissa systeemeissä, joissa niitä ylipäätään on olemassa.

Jatketaan imuriesimerkkiä ja tarkastellaan tilannetta kuvan 2 viiden käytävän muodostamassa silmukassa. Jos mahdolliset komennot ovat "myötäpäivään"ja "vastapäivään", niin on selvää, että synkronisoivaa toimintosarjaa ei voi olla olemassa. Oletetaan siis, että tällä kertaa imurilla onkin yksinkertainen sensori, jolla se pystyy erottamaan kaksi väriä toisistaan, esim. mustan ja valkoisen. Maalataan sitten kustakin käytävästä nuolet viereisiin käytäviin (yksi myötäpäivään ja yksi vastapäivään), toinen mustalla ja toinen valkoisella värillä. Jos nyt imurille annettavat komennot ovatkin muotoa "seuraa valkoista nuolta"ja "seuraa mustaa nuolta"(lyhennetään v ja m), niin nuolet voidaan mahdollisesti maalata niin, että synkronisoiva toimintosarja on olemassa. Kuvassa on esitetty tällainen maalaus; toimintosarjan $mmvv$ jälkeen imuri on yläoikealla olevassa käytävässä riippumatta siitä, mistä käytävästä se aloittaa.

Tutkielman luvussa 5 tutkitaan sitä, millä edellytyksillä voidaan nuolia maalaamalla muodostaa sellainen systeemi, että siinä on olemassa synkronisoivia toimintosarjoja. Kiinnostavaa on myös se, kuinka lyhyeksi lyhin mahdollinen synkronisoiva toimintosarja voidaan saada kun nuolet on maalattu optimaalisesti; tätä käsitellään luvussa 6.

2 Peruskäsitteitä

Määritellään tässä luvussa automaattien teorian peruskäsitteitä.

Määritelmä 2.1. Luonnollisten lukujen joukko $\mathbb{N} = \{1, 2, 3, \dots\}$.

Määritelmä 2.2. Äärellistä epätyhjää joukkoa Σ kutsutaan *aakkostoksi*. Sen alkioita kutsutaan *merkeiksi* tai *kirjaimiksi*.

Jos Σ on jokin aakkosto, niin sen kirjaimista muodostettujen äärellisten merkkijonojen eli *sanojen* joukkoa merkitään symbolilla Σ^*. Joukko Σ^* voidaan tulkita monoidiksi, jonka kertolaskuna on kahden merkkijonon kirjoittaminen yhteen. Identiteettialkiona on ns. tyhjä sana, jota merkitään ϵ. Sanan w merkkien lukumäärää merkitään $|w|$.

Esimerkki 2.3. Jos $\Sigma = \{a, b\}$, niin joukon Σ^* sanoja ovat esim. abb, ba ja niiden tulo $(abb)(ba) = abbba$. Sanassa $w = abbba$ on viisi merkkiä, eli $|w| = 5$.

Johdannossa käytettiin epämuodollista käsitettä "systeemi"ja annettiin havainnollistavia esimerkkejä systeemeistä. Esitetään seuraavaksi tämän käsitteen formaali vastine.

Määritelmä 2.4. *Automaatiksi* kutsutaan 3-tuplaa $A = (Q, \Sigma, *)$, missä

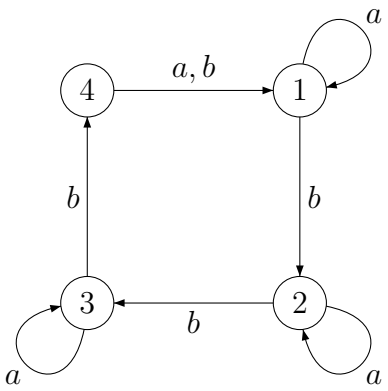
- Q on äärellinen epätyhjä joukko, jonka alkioita kutsutaan *tiloiksi*,
- Σ on aakkosto ja
- $*$ on kuvaus $Q \times \Sigma \to Q$ (alkion $(q, a) \in Q \times \Sigma$ kuvaa merkitään $q * a$).

Esimerkki 2.5. Muodostetaan automaatti $A = (Q, \Sigma, *)$, joka vastaa ensimmäistä johdannossa esitettyä systeemiä. Tilajoukko $Q = \{1, 2, 3, 4, 5\}$ vastaa niitä ruutuja, joissa imuri voi olla ja aakkosto $\Sigma = \{o, v, y, a\}$ vastaa komentoja "oikea", "vasen", "ylös"ja "alas". Määritellään kuvaus $*$ niin, että $q * a = s$ jos sovellettaessa komentoa a imurin ollessa ruudussa q imuri siirtyy ruutuun s, esim. $2 * o = 3$.

Automaatti voidaan esittää suunnattuna graafina, jonka solmuja ovat joukon Q alkiot ja jossa on kirjaimella a merkitty nuoli solmusta q solmuun $q * a$ kaikilla $q \in Q$ ja $a \in \Sigma$.

Esimerkki 2.6. Kuvassa 3 on automaatin $A = (Q, \Sigma, *)$ graafiesitys, missä $Q = \{1, 2, 3, 4\}$, $\Sigma = \{a, b\}$ ja

$$q * a = \begin{cases} 1 & \text{kun } q = 4 \\ q & \text{muulloin} \end{cases} \quad \text{ja} \quad q * b = \begin{cases} 1 & \text{kun } q = 4 \\ q + 1 & \text{muulloin} \end{cases}.$$



Kuva 3: Erään automaatin graafiesitys.

Solmusta 4 solmuun 1 menee itse asiassa kaksi nuolta, mutta kuvan yksinkertaistamiseksi nämä on korvattu yhdellä nuolella, joka on merkitty kahdella eri kirjaimella.

Operaatio $*$ voidaan induktiivisesti jatkaa kuvaukseksi $\hat{*} : Q \times \Sigma^* \to Q$, missä

- $q\hat{*}\epsilon = q$ kaikilla $q \in Q$ ja
- $q\hat{*}aw = (q * a)\hat{*}w$ kaikilla $q \in Q$, $a \in \Sigma$ ja $w \in \Sigma^*$.

Jatkossa näistä molemmista operaatioista käytetään merkintää $*$.

Olkoon $A = (Q, \Sigma, *)$ automaatti. Jos $S \subseteq Q$ ja $w \in \Sigma^*$, niin merkitään

$$S * w = \{s * w \mid s \in S\} \quad \text{ja} \quad S * w^{-1} = \{q \in Q \mid q * w \in S\}.$$

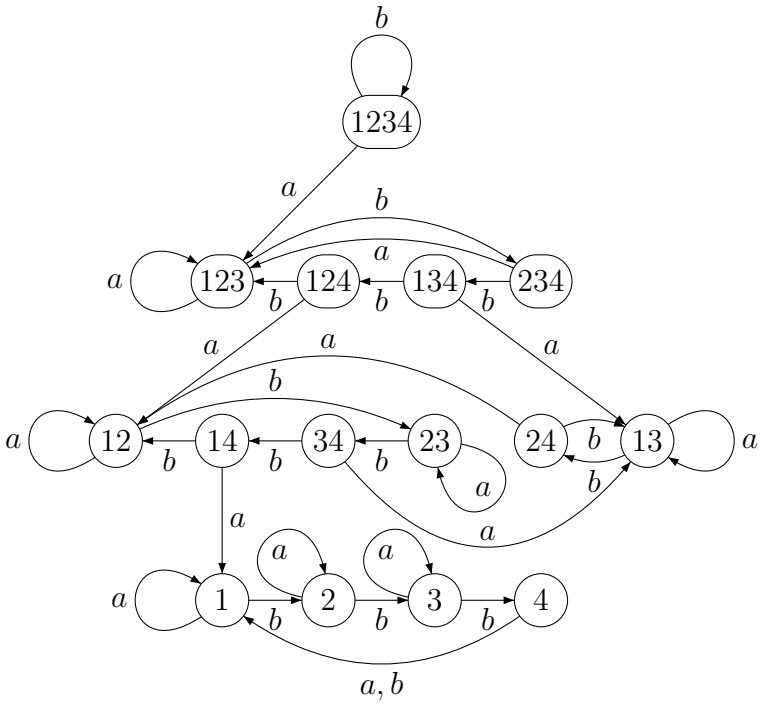
Jos $S * w = \{q\}$, niin voidaan merkitä myös $S * w = q$.

Määritelmä 2.7. Automaattia $A = (Q, \Sigma, *)$ sanotaan *synkronisoituvaksi*, jos on olemassa sellainen sana $w \in \Sigma^*$, että $|Q * w| = 1$. Tällainen sana w *synkronisoi* automaatin. Joukkoa $S \subseteq Q$ sanotaan synkronisoituvaksi, jos on olemassa sana w, jolla $|S * w| = 1$. (Erityisesti $\emptyset$ ei ole synkronisoituva.)

Esimerkki 2.8. Kuvan 3 automaatti on synkronisoituva, sillä esim. sana *abbbabbba* synkronisoi sen.

Synkronisoivia sanoja etsittäessä seuraavanlainen konstruktio on joskus hyödyllinen.

Määritelmä 2.9. Olkoon $A = (Q, \Sigma, *)$ automaatti. Sen *potenssijoukkoautomaatti* on $\mathcal{P}(A) = (2^Q, \Sigma, \cdot)$, missä 2^Q on joukon Q epätyhjien osajoukkojen joukko ja kaikilla $S \in 2^Q$, $a \in \Sigma$ on $S \cdot a = S * a$.



Kuva 4: Potenssijoukkoautomaatti.

Potenssijoukkoautomaatin idea on, että se seuraa kerralla koko joukon $S \subseteq Q$ muutosta sanan w vaikutuksesta. Erityisesti automaatissa $\mathcal{P}(A)$ on kirjaimilla $a_1, \ldots, a_k$ merkitty polku tilasta Q johonkin tilaan S, jossa $|S| = 1$, tarkalleen silloin kun $w = a_1 \ldots a_k$ synkronisoi automaatin A.

Esimerkki 2.10. Kuvassa 4 on kuvan 3 automaatin potenssijoukkoautomaatti. Sen avulla synkronisoivien sanojen löytäminen on helppoa. Näiden joukossa on myös edellisessä esimerkissä mainittu *abbbabbba*.

3 Lineaarialgebraa

Esitetään Perronin-Frobeniuksen lauseen todistus kirjan [14] luvusta yhdeksän.

Määritelmä 3.1. Jos $A = (a_{ij})$ on reaalinen matriisi, jossa kaikilla i ja j on $a_{ij} > 0$ (vast. $a_{ij} \geq 0$), niin matriisia kutsutaan *positiiviseksi* (vast. *epänegatiiviseksi*), merk. $A > 0$ (vast. $A \geq 0$).

Käytetään jatkossa merkintää $A > B$ (vast. $A \geq B$) tarkoittamaan sitä, että $A - B > 0$ (vast. $A - B \geq 0$).

Määritelmä 3.2. Jos $A = (a_{ij})$ on epänegatiivinen neliömatriisi ja jokaista paria (i, j) kohti on olemassa sellainen luku $k \in \mathbb{N}$, että matriisin A^k koordinaatissa (i, j) oleva alkio on nollaa suurempi, niin matriisia A kutsutaan *redusoitumattomaksi*.

Lemma 3.3. Jos A on redusoitumaton, niin on olemassa sellainen luku $k \in \mathbb{N}$, että $(I + A)^k > 0$.

Todistus. Valitaan kutakin matriisin A koordinaattia (i, j) kohti luku $k_{ij} \in \mathbb{N}$ niin, että matriisin $A^{k_{ij}}$ koordinaatissa (i, j) oleva alkio on nollaa suurempi. Valitaan lisäksi $k = \max k_{ij}$. Kertomalla $(I + A)^k$ auki

$$(I + A)^k = I + kA + \binom{k}{2} A^2 + \cdots + A^k$$

nähdään, että $(I + A)^k > 0$. □

Olkoon A redusoitumaton $n \times n$-matriisi ja merkitään symbolilla $\mathfrak{L}$ kaikkien epänegatiivisten nollasta poikkeavien pystyvektorien joukkoa. Vektoreille $\mathbf{x} = (x_1, \ldots x_n)^T \in \mathfrak{L}$, voidaan määritellä funktio

$$r(\mathbf{x}) = \min_{\substack{1 \leq i \leq n \\ x_i \neq 0}} \frac{(A\mathbf{x})_i}{x_i},$$

missä $(A\mathbf{x})_i$ on vektorin $A\mathbf{x}$ i:s alkio. Määritelmästä seuraa, että kaikilla luvuilla i on voimassa $r(\mathbf{x})x_i \leq (A\mathbf{x})_i$ ja jollakin i:n arvolla $r(\mathbf{x})x_i = (A\mathbf{x})_i$. Voidaan siis sanoa, että $r(\mathbf{x})$ on suurin sellainen luku ρ, että $A\mathbf{x} \geq \rho\mathbf{x}$.

Olkoon $\mathfrak{B} = \{\mathbf{x} = (x_1, \ldots x_n)^T \in \mathfrak{L} \mid \sum_i x_i^2 = 1\}$ ja $\mathfrak{B}' = \{(I + A)^k\mathbf{x} \mid \mathbf{x} \in \mathfrak{B}\}$, missä k on edellisen lemman mukainen kiinnitetty luku. Selvästi $\mathfrak{B}$ on kompakti joukko, ja koska $\mathfrak{B}'$ on joukon $\mathfrak{B}$ kuva jatkuvassa kuvauksessa $(I+A)^k$, myös se on kompakti. Koska joukon $\mathfrak{B}'$ alkiot ovat kaikki positiivisia,

niin kuvauksen $r(\mathbf{x})$ rajoittuma kompaktille joukolle $\mathfrak{B}'$ on jatkuva ja sillä on siis suurin arvo.

Olkoon nyt $\mathbf{x} \in \mathfrak{B}$ mielivaltainen. Tällöin $\mathbf{y} = (I + A)^k \mathbf{x} \in \mathfrak{B}'$ ja

$$r(\mathbf{x})\mathbf{y} = r(\mathbf{x})(I + A)^k \mathbf{x} \leq (I + A)^k A\mathbf{x} = A(I + A)^k \mathbf{x} = A\mathbf{y}.$$

Koska $r(\mathbf{y})$ on suurin luku ρ, jolla $\rho\mathbf{y} \leq A\mathbf{y}$, niin $r(\mathbf{x}) \leq r(\mathbf{y})$. Siis $\sup_{\mathbf{x}\in\mathfrak{B}} r(\mathbf{x}) \leq \max_{\mathbf{y}\in\mathfrak{B}'} r(\mathbf{y})$. Määritellään

$$r = \sup_{\mathbf{x}\in\mathfrak{L}} r(\mathbf{x}).$$

Jos α on positiivinen reaaliluku ja $\mathbf{x} \in \mathfrak{L}$, niin $r(\mathbf{x}) = r(\alpha\mathbf{x})$. Voidaan siis kirjoittaa

$$r = \sup_{\mathbf{x}\in\mathfrak{L}} r(\mathbf{x}) = \sup_{\mathbf{x}\in\mathfrak{B}} r(\mathbf{x}) \leq \max_{\mathbf{y}\in\mathfrak{B}'} r(\mathbf{y}).$$

Koska kuitenkin $\mathfrak{B}' \subseteq \mathfrak{L}$, niin

$$\max_{\mathbf{y}\in\mathfrak{B}'} r(\mathbf{y}) \leq \sup_{\mathbf{x}\in\mathfrak{L}} r(\mathbf{x}) = r,$$

eli $r = \max_{\mathbf{y}\in\mathfrak{B}'} r(\mathbf{y})$. Siis on olemassa vektoreita $\mathbf{z} \in \mathfrak{L}$, joilla $r(\mathbf{z}) = r$ tai ekvivalentisti $r\mathbf{z} \leq A\mathbf{z}$. Kaikkia tällaisia vektoreita kutsutaan matriisin A *äärivektoreiksi*.

Lemma 3.4. Olkoon A redusoitumaton matriisi. Siihen liittyvä edellä määritelty luku r on sen positiivinen ominaisarvo. Lisäksi kaikki matriisin A äärivektorit ovat positiivisia ominaisvektoreita, jotka kuuluvat ominaisarvoon r.

Todistus. Mikään matriisin $A = (a_{ij})$ vaakarivi ei muodostu pelkästään nollista, koska nollarivi pysyisi nollarivinä myös matriisissa A^l kaikilla $l \in \mathbb{N}$ vastoin redusoitumattomuuden määritelmää. Siis jos $\mathbf{u} = (1, \ldots, 1)^T$, niin $r \geq r(\mathbf{u}) = \min_{1\leq i\leq n} \sum_{j=1}^n a_{ij} > 0$.

Olkoon $\mathbf{z}$ äärivektori ja $\mathbf{x} = (I + A)^k \mathbf{z}$, missä k on kuten edellisessä lemmassa, siis $\mathbf{x} > 0$. Koska $\mathbf{z}$ on äärivektori, niin $A\mathbf{z} - r\mathbf{z} \geq 0$, ja jos olisi $A\mathbf{z} - r\mathbf{z} \neq 0$, niin

$$A\mathbf{x} - r\mathbf{x} = (I + A)^k (A\mathbf{z} - r\mathbf{z}) > 0.$$

Tästä seuraisi, että $r < r(\mathbf{x})$, mikä olisi vastoin luvun r valintaa. Siis $A\mathbf{z} = r\mathbf{z}$, joten $\mathbf{z}$ on ominaisarvoon r kuuluva ominaisvektori. Tästä seuraa, että $\mathbf{x} = (I + A)^k \mathbf{z} = (1 + r)^k \mathbf{z}$. Koska $\mathbf{x} > 0$ ja $r > 0$, niin myös $\mathbf{z} > 0$. □

Lause 3.5 (Perron-Frobenius)**.** Jos A on redusoitumaton matriisi, niin sillä on positiivinen ominaisarvo r, jonka itseisarvo on vähintään yhtä suuri kuin muilla ominaisarvoilla. Lisäksi on olemassa positiivinen vektori, joka virittää ominaisarvoon r kuuluvan ominaisavaruuden.

Todistus. Olkoon r kuten edellisessä lemmassa. Lemman mukaan r on matriisin A positiivinen ominaisarvo. Olkoon α jokin toinen ominaisarvo, eli $A\mathbf{y} = \alpha\mathbf{y}$, missä $\mathbf{y} \neq 0$. Käytetään merkintää $|\mathbf{x}|$ vektorista, joka on saatu vektorista $\mathbf{x}$ ottamalla itseisarvo komponenteittain. Koska $A \geq 0$, niin

$$|\alpha||\mathbf{y}| = |A\mathbf{y}| \leq A|\mathbf{y}|.$$

Siis $|\alpha| \leq r(|\mathbf{y}|) \leq r$.

Olkoon $\mathbf{z}$ jokin ominaisarvoon r kuuluva ominaisvektori, siis $A\mathbf{z} = r\mathbf{z}$ ja $\mathbf{z} \neq 0$. Todetaan kuten edellä, että $r|\mathbf{z}| \leq A|\mathbf{z}|$. Siis $|\mathbf{z}|$ on äärivektori ja edellisen lemman nojalla $|\mathbf{z}| > 0$ ja erityisesti vektorin $\mathbf{z}$ ensimmäinen komponentti ei ole 0. Tästä seuraa, että ominaisarvoon r kuuluvan ominaisavaruuden dimensio on 1, sillä muutoin voitaisiin valita lineaarisesti riippumattomat ominaisarvoon r kuuluvat ominaisvektorit $\mathbf{z_1}$ ja $\mathbf{z_2}$ ja luvut $\alpha, \beta \neq 0$ niin, että ominaisvektorin $\alpha\mathbf{z_1} + \beta\mathbf{z_2}$ ensimmäinen komponentti olisi 0. Edellisen lemman nojalla $|\mathbf{z}|$ on positiivinen vektori, joka virittää kyseisen ominaisavaruuden. □

4 Černý konjektuuri

Jos automaatti A on synkronisoituva, niin on luonnollista kysyä, kuinka lyhyt voi olla lyhin mahdollinen sana, joka synkronisoi sen. Artikkelissa [5] esitetty *Černýn konjektuuri* ottaa kantaa tähän kysymykseen.[1]

Käytetään jatkossa merkintää $\boldsymbol{S}$ kaikkien synkronisoituvien automaattien joukosta ja merkintää $\boldsymbol{S}_n$ kaikkien n-tilaisten synkronisoituvien automaattien joukosta.

Määritelmä 4.1. Jos $A \in \boldsymbol{S}$, niin käytetään merkintää $\mathfrak{C}(A)$ automaatin A lyhimmän synkronisoivan sanan pituudesta. Määritelmä laajennetaan kaikille $\boldsymbol{T} \subseteq \mathbf{S}$ seuraavasti:

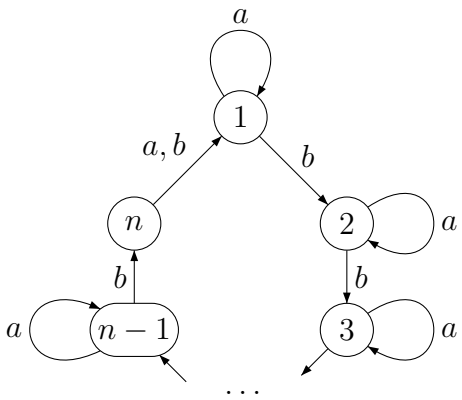
$$\mathfrak{C}(\boldsymbol{T}) = \max\{\mathfrak{C}(A) \mid A \in \boldsymbol{T}\} \quad \text{(jos olemassa)}.$$

Tapauksessa $\boldsymbol{T} = \boldsymbol{S}_n$ merkitään $\mathfrak{C}(\boldsymbol{T}) = \mathfrak{C}(n)$.

Konjektuuri 4.2 (Černýn konjektuuri)**.** Kaikilla $n \in \mathbb{N}$ on $\mathfrak{C}(n) = (n-1)^2$.

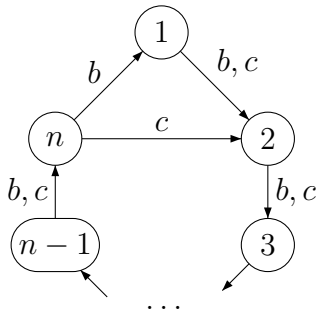
Tiedetään, että $\mathfrak{C}(n) \geq (n-1)^2$, sillä lähteessä [4] esitetään jokaista luonnollista lukua n kohti synkronisoituva automaatti, jolla on n tilaa ja jonka lyhin synkronisoiva sana on pituudeltaan $(n-1)^2$. Nämä automaatit ovat $C_n = (Q, \Sigma, *)$ (ks. kuva 5), missä $Q = \{1, 2, \ldots, n\}$, $\Sigma = \{a, b\}$ sekä

$$q * a = \begin{cases} 1 & \text{kun } q = n \\ q & \text{muulloin} \end{cases} \quad \text{ja} \quad q * b = \begin{cases} 1 & \text{kun } q = n \\ q+1 & \text{muulloin} \end{cases}.$$



Kuva 5: Automaatti C_n.

[1] Kirjallisuudessa on tyypillisesti esitetty konjektuurin lähteeksi artikkeli [4], jossa kuitenkin vain todistetaan Lause 4.5. Artikkelissa [5] konjektuuri mainitaan ohimennen ja todistetaan muutamassa erikoistapauksessa.



Kuva 6: Automaatti W_n.

Tapauksessa $n = 1$ nimittäin lyhin synkronisoiva sana on ϵ, ja kun $n > 1$, niin voidaan todeta, että $Q * (ab^{n-1})^{n-2}a = 1$, joten $\mathfrak{C}(C_n) \leq (n-1)^2$. Osoitetaan seuraavaksi lähteen [2] esityksen mukaisesti, että automaatilla C_n ei ole lyhyempää synkronisoivaa sanaa. Aluksi on tarkasteltava automaattia $W_n = (Q, \Delta, \cdot)$ $(n > 1)$ (ks. kuva 6), missä $Q = \{1, 2, \ldots, n\}$, $\Delta = \{c, b\}$ sekä

$$q \cdot c = \begin{cases} 2 & \text{kun } q \in \{1, n\} \\ q+1 & \text{muulloin} \end{cases} \quad \text{ja} \quad q \cdot b = \begin{cases} 1 & \text{kun } q = n \\ q+1 & \text{muulloin} \end{cases}.$$

Lemma 4.3. Olkoon n ja m positiivisia kokonaislukuja, joiden suurin yhteinen tekijä on 1. Lukua $nm - n - m$ ei voi kirjoittaa muodossa $kn + lm$, missä k ja l ovat epänegatiivisia kokonaislukuja.

Todistus. Tehdään vastaoletus, että $nm-n-m = kn+lm$. Jakamalla yhtälön molemmat puolet luvulla n ja uudelleen ryhmittelemällä saadaan $m - 1 - k = \frac{l+1}{n}m$. Koska tämän yhtälön molemmat puolet ovat kokonaislukuja, ja koska lukujen n ja m suurin yhteinen tekijä on 1, niin $\frac{l+1}{n}$ on positiivinen kokonaisluku. Siis $m - 1 - k < m \leq \frac{l+1}{n}m$ vastoin oletusta. □

Lause 4.4. $\mathfrak{C}(W_n) = n^2 - 3n + 3$.

Todistus. Voidaan helposti todeta, että $(cb^{n-2})^{n-2}c$ on synkronisoiva sana, jonka pituus on $n^2 - 3n + 3$. Vielä on osoitettava, että lyhyempiä synkronisoivia sanoja ei ole.

Olkoon w lyhin mahdollinen synkronisoiva sana ja $q = Q \cdot w$. Jos $q \neq 2$, niin tilaan q saapuu nuolia vain yhdestä tilasta, joten w olisi synkronisoiva sana myös ilman viimeistä kirjaintaan. Tämä on mahdotonta, koska w on lyhin synkronisoiva sana, joten $q = 2$.

Kaikilla $u \in \Delta^*$ myös uw on sana jolla $Q \cdot uw = 2$. Täten kaikilla $l \geq |w|$ automaatin W_n graafissa on polku solmusta 2 siihen itseensä, jonka pituus

on l. Jokainen tällainen polku muodostuu silmukoista, joiden pituus on n tai $n-1$, joten Lemman 4.3 nojalla on $|w| > n(n-1)-n-(n-1) = n^2-3n+1$.

Koska solmusta 1 on pituutta w oleva polku solmuun 2 ja koska solmun 1 molemmat nuolet menevät solmuun 2, niin solmusta 2 on pituutta $|w|-1$ oleva polku siihen itseensä. Lemman 4.3 nojalla $|w|-1 \neq n^2-3n+1$. Siis $|w| > n^2-3n+2$. □

Lause 4.5. $\mathfrak{C}(C_n) = (n-1)^2$.

Todistus. Olkoon w lyhin mahdollinen synkronisoiva sana. Kaikilla $S \subseteq Q$ on $|Q*b| = |Q|$, joten w päättyy kirjaimeen a ja voidaan kirjoittaa $w = w'a$, missä $Q*w' = \{1,n\}$.

Koska kaikilla $S \subseteq Q$ on $S*aa = S*a$ ja koska w on lyhin mahdollinen synkronisoiva sana, niin sanassa w' jokaista kirjaimen a esiintymää seuraa b. Siis korvaamalla sanassa w' kaikki sanan ab esiintymät kirjaimella c saadaan sana $v \in \Delta^*$. Vertaamalla automaatteja C_n ja W_n todetaan, että $q*ab = q\cdot c$ ja $q*b = q\cdot b$ kaikilla $q \in Q$. Siis $Q\cdot v = \{1,n\}$ ja vc on automaatin W_n synkronisoiva sana. Edellisen lauseen nojalla $|vc| \geq n^2-3n+3$, joten $|v| \geq n^2-3n+2$. Koska kaikilla $S \subseteq Q$ on $|S\cdot c| \geq |S|-1$, niin sanassa v on vähintään $n-2$ kirjaimen c esiintymää. Koska c vastaa kahta merkkiä sanassa w', niin $|w'| \geq |v|+n-2 \geq n^2-2n$ ja $|w| \geq n^2-2n+1 = (n-1)^2$. □

Synkronisoituvat automaatit A, joilla $\mathfrak{C}(A) = (n-1)^2$, ovat harvinaisia; itse asiassa äärettömän perheen C_n lisäksi tällaisia tunnetaan vain kahdeksan erilaista. Ne on kuvattu artikkelissa [18].

4.1 Yläraja-arvio lukujonolle $\mathfrak{C}(n)$

Černýn konjektuurin mukaan lukujono $\mathfrak{C}(n)$ on neliöllinen luvun n suhteen, mutta parhaat todistetut ylärajat tälle lukujonolle ovat kuutiollisia. Esitetään artikkelin [16] todistus sille, että $\mathfrak{C}(n) \leq \frac{n^3-n}{6}$.

Olkoon $A = (Q,\Sigma,*)$ jokin synkronisoituva automaatti, jossa $|Q| = n$. Muodostetaan sen synkronisoiva sana seuraavasti. Etsitään lyhin mahdollinen sana w_1, jolla $|Q*w_1| < |Q|$. Etsitään sitten lyhin mahdollinen sana w_2, jolla $|Q*w_1w_2| < |Q*w_1|$. Jatketaan vastaavasti, kunnes on muodostettu sellainen sana $w = w_1\dots w_k$ ($k \leq n-1$), että $|Q*w| = 1$. Olennaista on saada selville, kuinka pitkiä sanat w_i voivat pisimmillään olla.

Olkoon $S \subseteq Q$, $|S| = k > 1$ ja $w = a_1\dots a_l$, $a_i \in \Sigma$ lyhin sellainen sana, että $|S*w| < |S|$. Merkitään $S_1 = S$ ja $S_{i+1} = S_i * a_i$ ($1 \leq i < l$). Koska $|S*w| < |S|$, niin on olemassa tilat $x,y \in S$ ($x \neq y$), joilla $x*w = y*w$. Merkitään $T_1 = \{x,y\}$ ja $T_{i+1} = T_i*a_i$. Sanan w määritelmän nojalla $|S_i| = k$,

$|T_i| = 2$ ja $T_i \subseteq S_i$ kaikilla $i \leq l$. Lisäksi aina kun $1 \leq i < j \leq l$, niin $T_j \not\subseteq S_i$, koska muutoin olisi $|S * a_1 \dots a_{i-1} a_j \dots a_l| < |S|$ vastoin sanan w valintaa.

Jatkossa tarvitaan tunnettua lineaarialgebran lemmaa, jolle esitetään tässä todistus kirjasta [21] (lause 5.9).

Lemma 4.6.

$$V(x_1, \dots, x_n) \overset{määr.}{=} \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{i<j} (x_j - x_i).$$

Todistus. Todistetaan väite induktiolla muuttujien lukumäärän n suhteen. Tapaus $n = 1$ on triviaali, joten oletetaan että väite on todistettu tapauksessa $n = k$ ja todistetaan se tapauksessa $n = k + 1$.

Lisäämällä allaolevassa determinantissa k:s sarake sen oikealla puolella olevaan sarakkeeseen kerrottuna luvulla $-x_1$, $k-1$:s sarake sen oikealla puolella olevaan sarakkeeseen kerrottuna luvulla $-x_1$ jne. (tässä järjestyksessä) saadaan

$$\begin{aligned} V(x_1, \dots, x_{k+1}) &= \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^k \\ 1 & x_2 & x_2^2 & \dots & x_2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k+1} & x_{k+1}^2 & \dots & x_{k+1}^k \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & x_2 - x_1 & x_2(x_2 - x_1) & \dots & x_2^{k-1}(x_2 - x_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k+1} - x_1 & x_{k+1}(x_{k+1} - x_1) & \dots & x_{k+1}^{k-1}(x_{k+1} - x_1) \end{vmatrix}. \end{aligned}$$

Kehitetään tämä determinantti ylimmän vaakarivin suhteen, otetaan jokaiselta vaakarivilta i tekijä $x_{i+1} - x_1$ determinantin ulkopuolelle ja sovelletaan induktio-oletusta.

$$\begin{aligned} &\begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \dots & x_2^{k-1}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \dots & x_3^{k-1}(x_3 - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_{k+1} - x_1 & x_{k+1}(x_{k+1} - x_1) & \dots & x_{k+1}^{k-1}(x_{k+1} - x_1) \end{vmatrix} \\ =& V(x_2, \dots, x_{k+1}) \prod_{1<j} (x_j - x_1) = \prod_{i<j} (x_j - x_i). \end{aligned}$$

□

Seuraava aputulos, joka antaa ylärajan sanan w pituudelle l edellä esitetyssä menetelmässä, on ensimmäisenä todistettu (yleisemmässä tapauksessa) artikkelissa [8]. Lemmalle esitetään artikkelin [13] todistus seuraten lähteen [12] esitystä.

Lemma 4.7. Olkoon Q joukko, $|Q| = n$ ja $\{S_1, \ldots, S_l\}$ sekä $\{T_1, \ldots, T_l\}$ joukon Q osajoukkojen kokoelmia, missä $|S_i| = k$, $|T_i| = 2$, $T_i \subseteq S_i$ ja $T_j \not\subseteq S_i$ aina kun $1 \leq i < j \leq l$. Silloin $l \leq \binom{n-k+2}{2}$.

Todistus. Rajoituksetta voidaan olettaa, että $Q = \{1, \ldots, n\}$. Liitetään jokaiseen joukon Q k-alkioiseen osajoukkoon $S = \{s_1, \ldots, s_k\}$ reaalikertoiminen polynomi

$$D(S) = \begin{vmatrix} 1 & s_1 & s_1^2 & \ldots & s_1^{k-3} & x_{s_1} & x_{s_1}^2 \\ 1 & s_2 & s_2^2 & \ldots & s_2^{k-3} & x_{s_2} & x_{s_2}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & s_k & s_k^2 & \ldots & s_k^{k-3} & x_{s_k} & x_{s_k}^2 \end{vmatrix}.$$

Polynomit $D(S_1), \ldots, D(S_l)$ ovat lineaarisesti riippumattomia n:n muuttujan reaalikertoimisten polynomien muodostamassa $\mathbb{R}$-vektoriavaruudessa. Todistetaan tämä tekemällä vastaoletus, että jokin polynomi $D(S_j)$ voidaan esittää polynomien $D(S_1), D(S_2), \ldots, D(S_{j-1})$ lineaarikombinaationa. Tiedetään, että $T_j = \{t_1, t_2\} \subseteq S_j$ mutta $T_j \not\subseteq S_i$ kun $i < j$. Sijoituksella $x_{t_1} = t_1$, $x_{t_2} = t_2$ ja $x_t = 0$ kun $t \notin \{t_1, t_2\}$ polynomit $D(S_1), \ldots, D(S_{j-1})$ (ja niiden lineaarikombinaatiot) saavat arvon nolla, sillä vastaavissa determinanteissa tulee kahteen viimeiseen sarakkeeseen pelkästään nollia (mahdollisesti yhtä riviä lukuunottamatta). Toisaalta samalla sijoituksella determinantin $D(s_j)$ arvo saadaan etumerkkiä vaille kertomalla kahdesta viimeisestä sarakkeesta saatava determinantti $\begin{vmatrix} t_1 & t_1^2 \\ t_2 & t_2^2 \end{vmatrix}$ jollakin lemman 4.6 tyyppiä olevalla determinantilla, joten $D(S_j)$ ei saa arvoa nolla. Tämä on ristiriita.

Polynomien $D(S_1), \ldots, D(S_l)$ lineaarisesta riippumattomuudesta seuraa, että l ei voi ylittää sen $\mathbb{R}$-vektoriavaruuden V dimensiota, jonka virittää joukko $P = \{D(S) | S \subseteq Q, |S| = k\}$. Määritellään nyt joukko $W = \{1, \ldots, k-2\}$, muodostetaan lista, jossa on jossain järjestyksessä kaikki joukon $Q \setminus W$ 2-alkioiset osajoukot ja muodostetaan joukko P_i joukkojen W ja listan i:nnen joukon unionina kun $1 \leq i \leq \binom{n-k+2}{2}$. Väitetään, että polynomit $D(P_1), \ldots, D(P_{\binom{n-k+2}{2}})$ virittävät vektoriavaruuden V, eli avaruuden dimensio on enintään $\binom{n-k+2}{2}$. Riittää osoittaa, että joukon P mielivaltainen alkio $D(S)$ (missä $S = \{s_1, \ldots, s_k\}$) voidaan esittää polynomien

$D(P_1), \ldots, D(P_{\binom{n-k+2}{2}})$ lineaarikombinaationa. Todistetaan väite induktiolla luvun $|S \setminus W|$ suhteen.

Tapauksessa $|S \setminus W| = 2$ on $W \subseteq S$, joten jollakin i on $S = P_i$ ja siis $D(S) = D(P_i)$.

Tapauksessa $|S \setminus W| > 2$ valitaan jokin alkio $s_0 \in W \setminus S$ ja määritellään $S' = S \cup \{s_0\}$. Määritellään lisäksi polynomi $p(x) = c \prod_{w \in W \setminus s_0}(x - w)$, missä $c \in \mathbb{R}$ on sellainen luku, että $p(s_0) = 1$, ja tarkastellaan determinanttia

$$\Delta = \begin{vmatrix} p(s_0) & 1 & s_0 & s_0^2 & \ldots & s_0^{k-3} & x_{s_0} & x_{s_0}^2 \\ p(s_1) & 1 & s_1 & s_1^2 & \ldots & s_1^{k-3} & x_{s_1} & x_{s_1}^2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p(s_k) & 1 & s_k & s_k^2 & \ldots & s_k^{k-3} & x_{s_k} & x_{s_k}^2 \end{vmatrix}.$$

Polynomi $p(x)$ on astetta $k - 3$, joten determinantin ensimmäinen pystyrivi voidaan ilmaista muiden pystyrivien lineaarikombinaationa ja siis $\Delta = 0$. Kehittämällä Δ ensimmäisen pystyrivin suhteen saadaan yhtälö

$$\sum_{i=0}^{k} (-1)^i p(s_i) D(S' \setminus \{s_i\}) = 0.$$

Siirretään termi $p(s_0)D(S' \setminus \{s_0\})$ yhtälön toiselle puolelle. Koska $p(s_0) = 1$ ja $S' \setminus \{s_0\} = S$, niin saadaan

$$D(S) = \sum_{i=1}^{k} (-1)^{i+1} p(s_i) D(S' \setminus \{s_i\}).$$

Koska $p(s_i) = 0$ kun $s_i \in W \setminus \{s_0\}$, niin induktioaskeleen todistamiseksi riittää osoittaa, että $D(S' \setminus \{s_i\})$ voidaan esittää polynomien $D(P_1), \ldots, D(P_{\binom{n-k+2}{2}})$ lineaarikombinaationa, kun $s_i \notin W$. Tämän osoittamiseen voidaan käyttää induktio-oletusta, sillä kun $s_i \notin W$, niin $|(S' \setminus \{s_i\}) \setminus W| = |(S' \setminus W) \setminus \{s_i\}| = |(S \setminus W) \setminus \{s_i\}| = |S \setminus W| - 1$. □

Lause 4.8. $\mathfrak{C}(n) \leq \frac{n^3-n}{6}$.

Todistus. Kun rakennetaan n-tilaisen automaatin synkronisoiva sana edellä esitetyllä menetelmällä, niin edellisen lemman mukaan sen pituus on enintään

$$\sum_{k=2}^{n} \binom{n-k+2}{2} = \sum_{i=2}^{n} \binom{i}{2}.$$

Induktiolla on helppo todistaa, että tämän summan arvo on $\frac{n^3-n}{6}$. Tapaus $n = 1$ on nimittäin triviaali, ja jos oletetaan, että yhtäsuuruus on voimassa

kun $n = k - 1$, niin

$$\sum_{i=2}^{k} \binom{i}{2} = \sum_{i=2}^{k-1} \binom{i}{2} + \binom{k}{2} = \frac{(k-1)^3 - (k-1)}{6} + \frac{k(k-1)}{2}$$
$$= \frac{k^3 - 3k^2 + 2k}{6} + \frac{3k^2 - 3k}{6} = \frac{k^3 - k}{6}.$$

□

4.2 Sykliset automaatit

Černýn konjektuurin edellyttämä yläraja lyhimmän synkronisoivan sanan pituudelle on pystytty todistamaan useille äärettömille automaattien perheille; esimerkiksi artikkelissa [7] on todistettu yläraja $(n-1)^2$ ns. syklisille automaateille, joita ovat mm. kaikki Černýn automaatit C_n. Esitetään kuitenkin tässä osiossa 20 vuotta vanhempi todistus lähteestä [17], joka kattaa sykliset automaatit, joissa tilojen lukumäärä n on alkuluku. Tässä erikoistapauksessa saadaan lisäksi yksinkertainen kriteeri sille, milloin automaatti on synkronisoituva.

Määritelmä 4.9. Automaatti $A = (Q, \Sigma, *)$ on *syklinen*, jos on olemassa sellainen kirjain $c \in \Sigma$, että $Q = \{q * c^r \mid r \in \mathbb{N}\}$ kaikilla $q \in Q$.

Rajoituksetta voidaan olettaa, että $Q = \{1, \ldots, n\}$ ja että kaikilla $q \in Q$ on $q * c \equiv q + 1 \pmod{n}$.

Lemma 4.10. Olkoon $A = (Q, \Sigma, *)$ ja c kuten määritelmässä ja $n = |Q|$ alkuluku. Oletetaan, että on sellainen kirjain $a \in \Sigma$, että $|Q * a| < |Q|$. Jos $S \subseteq Q$ ja $S \notin \{\emptyset, Q\}$ niin on olemassa luku $r \in \mathbb{N} \cup \{0\}$, jolla $|(S * c^r) * a^{-1}| > |S|$.

Todistus. Tehdään vastaoletus, että kaikilla r on $|(S * c^r) * a^{-1}| \leq |S|$. Silloin yhtälöstä

$$\sum_{r=0}^{n-1} |(S * c^r) * a^{-1}| = \sum_{r=0}^{n-1} \sum_{q \in S * c^r} |q * a^{-1}| = |S| \sum_{q \in Q} |q * a^{-1}| = |S||Q * a^{-1}| = |S|n$$

seuraa, että $|(S * c^r) * a^{-1}| = |S|$ kaikilla r.

Valitaan $\zeta \in \mathbb{C}$ niin, että n on pienin positiivinen kokonaisluku, jolla $\zeta^n = 1$ (eli ζ on n:s primitiivinen ykkösenjuuri). Käytetään merkintää $\mathbb{Q}(\zeta)$ kunnan $\mathbb{C}$ suppeimmasta alikunnasta, joka sisältää kunnan $\mathbb{Q}$ ja luvun ζ. Luvun ζ minimaalipolynomi on $\sum_{i=0}^{n-1} x^i$, joten $\mathbb{Q}$-vektoriavaruuden $\mathbb{Q}(\zeta)$ dimensio on $n-1$ ja sillä on kanta $\{\zeta^i \mid 0 \leq i \leq n-2\}$. Siis $V = \mathbb{Q} \times \mathbb{Q}(\zeta)$ on

n-dimensioinen $\mathbb{Q}$-vektoriavaruus. Liitetään nyt jokaiseen tilaan $q \in Q$ vektoriavaruuden V vektori $\overline{q} = (1, \zeta^q)$ ja jokaiseen osajoukkoon $T \subseteq Q$ vektori $\overline{T} = \sum_{q \in T} q'$.

Vektorit $\overline{q}$ virittävät avaruuden V, sillä $(1,0) = |Q|^{-1}(\sum_{q \in Q} \overline{q})$ ja $(0, \zeta^q) = \overline{q} - (1,0)$ kaikilla $q \in Q$. Koska avaruuden V dimensio on n, niin tästä seuraa, että vektorit $\overline{q}$ muodostavat V:n kannan. Määritellään lineaarikuvaukset $A : V \to V$ ja $B : V \to \mathbb{R}$ kantavektoreiden avulla: $A(\overline{q}) = \overline{(q * a^{-1})}$ ja $B(\overline{q}) = 1$ kaikilla $q \in Q$.

Merkitään nyt $u = \sum_{q \in S} \zeta^q$ ja osoitetaan seuraavaksi, että joukkojen $S * c^r$ $(0 \leq r \leq n-1)$ vastinvektorit $\overline{S * c^r} = (|S|, u\zeta^r)$ muodostavat avaruuden V kannan. Vektori $(1,0)$ voidaan esittää muodossa $(|S|n)^{-1}(\sum_{r=0}^{n-1}(\overline{S * c^r}))$, joten riittää osoittaa, että vektorit $u\zeta^r$ virittävät avaruuden $\mathbb{Q}(\zeta)$. Luku $u = \sum_{q \in S} \zeta^q$ ei ole nolla, koska luvun ζ minimaalipolynomi ei jaa polynomia $\sum_{q \in S} x^q$. Siis luvulla u on käänteisalkio $\sum_{r=0}^{n-1} k_i \zeta^i$, eli $1 = \sum_{r=0}^{n-1} k_i (u\zeta^i)$. Kertomalla tämä puolittain avaruuden $\mathbb{Q}(\zeta)$ mielivaltaisella kantavektorilla ζ^r saadaan $\zeta^r = \sum_{r=0}^{n-1} k_i (u\zeta^{i+r})$, josta väite seuraa.

Koska kaikilla $r \in \mathbb{N} \cup \{0\}$ on $|(S * c^r) * a^{-1}| = |(S * c^r)|$, niin vastaavasti $B(A(\overline{S * c^r})) = B(\overline{S * c^r})$. Koska vektorit $\overline{S * c^r}$ muodostavat joukon V kannan, niin kaikilla $v \in V$ on $B(A(v)) = B(v)$; erityisesti $B(A(\overline{q})) = B(\overline{q}) = 1$ kaikilla $q \in Q$. Tällöin $|q * a^{-1}| = 1$, mikä on ristiriidassa sen kanssa, että $|Q * a| < |Q|$. □

Lause 4.11. Olkoon $A = (Q, \Sigma, *)$ syklinen automaatti, jonka tilojen lukumäärä n on alkuluku. Jos on olemassa $a \in \Sigma$, jolla $|Q * a| < |Q|$, niin A on synkronisoituva ja $\mathfrak{C}(A) \leq (n-1)^2$.

Todistus. Olkoon kirjain c kuten edellisessä lemmassa ja $q \in Q$ sellainen tila, että $|q * a^{-1}| > 1$. Osoitetaan induktiolla, että kun $0 \leq k \leq n-2$, niin on olemassa sellainen sana w, että $|w| \leq 1 + kn$ ja $|q * w^{-1}| \geq k + 2$. Tapauksessa $k = 0$ voidaan valita $w = a$. Oletetaan nyt, että sana u toteuttaa väitteen tapauksessa $k = t < n-2$ ja todistetaan väite tapauksessa $k = t+1$. Jos $|q * u^{-1}| \geq t+3$, niin voidaan valita $w = u$. Muutoin edellisen lemman nojalla on olemassa sellainen luku r $(0 \leq r \leq n-1)$, että $|((q * u^{-1}) * (c^r)^{-1}) * a^{-1}| > |q * u^{-1}| = t + 2$ ja voidaan siis valita $w = ac^r u$ $(|w| \leq 1 + (t+1)n)$.

Nyt todistetusta voidaan tapauksessa $k = n-2$ päätellä, että on olemassa sellainen sana w, että $|w| = 1 + (n-2)n = (n-1)^2$ ja $|q * w^{-1}| \geq n$, eli $q * w^{-1} = Q$. Tästä seuraa, että $|Q * w| = 1$. □

4.3 Vahvasti yhtenäiset automaatit

Automaattia $A = (Q, \Sigma, *)$ sanotaan *vahvasti yhtenäiseksi*, jos jokaista kahta tilaa $q, s \in Q$ kohti on olemassa sana w, jolla $q * w = s$. Černý konjektuu-

rin tutkimisessa riittää rajoittua vahvasti yhtenäisiin automaatteihin. Tämä nähdään seuraavan lemman avulla, joka on esitetty yleisemmässä muodossa artikkelissa [20]. Käytetään lemman muotoilussa merkintää $\mathbf{V}_n$ niiden n-tilaisten automaattien joukosta, jotka ovat synkronisoituvia ja vahvasti yhtenäisiä.

Lemma 4.12. Jos $f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ on sellainen funktio, että $\mathfrak{C}(\mathbf{V}_n) \leq f(n)$ kaikilla $n \in \mathbb{N}$, ja jos $A = (Q, \Sigma, *) \in \mathbf{S}_n \setminus \mathbf{V}_n$ (siis $n > 1$), niin $\mathfrak{C}(A)$ on enintään

$$\max\left\{\binom{n-m+1}{2} + f(m) \mid 1 \leq m < n\right\}.$$

Todistus. Olkoon u jokin automaatin A synkronisoiva sana ja q sellainen tila, että $Q * u = q$. Merkitään $S = \{q * w \mid w \in \Sigma^*\}$, $|S| = m < n$ ja $S' = Q \setminus S$. Etsitään ensin sellainen sana w, että $S' * w \subseteq S$. Olkoon $T \subseteq S'$ epätyhjä, $|T| = i$. Lyhin sellainen sana w', että jollakin $t \in T$ on $t * w' \in S$ (siis $|T * w' \cap S'| < |T|$), on enintään pituutta $n - m - i + 1$. Jos nimittäin $w' = a_1 \dots a_j$, $a_1, \dots, a_j \in \Sigma$, niin $t * a_1 \dots a_l \notin S$ kaikilla $l < j$ ja $t * a_1 \dots a_p \neq t * a_1 \dots a_r$ kun $p \neq r$.

Muodostetaan sana $w = w_1 \dots w_t$ niin että sanat w_l ovat lyhimmät mahdolliset, joilla $|S' * w_1 \cap S'| < |S'|, |S' * w_1 w_2 \cap S'| < |S' * w_1 \cap S'|, \dots, |S' * w \cap S'| = 0$. Edellä todetun nojalla sanan w pituus on enintään $1 + 2 + \dots + (n - m) = \binom{n-m+1}{2}$.

Kolmikko $B = (S, \Sigma, *)$, missä $*$ on sama operaatio kuin automaatissa A, on vahvasti yhtenäinen synkronisoituva automaatti. Olkoon u sen lyhin synkronisoiva sana; sen pituus on enintään $f(m)$. Sana wu on automaatin A synkronisoiva sana. □

Lause 4.13. Jos $\mathfrak{C}(\mathbf{V}_n) = (n-1)^2$ kaikilla $n \in \mathbb{N}$, niin $\mathfrak{C}(n) = (n-1)^2$ kaikilla $n \in \mathbb{N}$.

Todistus. Lauseen oletuksin edellisestä lemmasta seuraa, että jos $A \in \mathbf{S}_n \setminus \mathbf{V}_n$ (siis $n > 1$), niin sen lyhin synkronisoiva sana on enintään pituutta $\max\{\binom{n-m+1}{2} + (m-1)^2 \mid 1 \leq m < n\}$. Polynomin $g(m) = \binom{n-m+1}{2} + (m-1)^2$ korkea-asteisin termi on $\frac{3}{2}m^2$, joten $g(m)$ saavuttaa maksiminsa välillä $[1, n-1]$ kun $m = 1$ tai $m = n - 1$. Molemmilla sijoituksilla $g(m) \leq (n-1)^2$. □

Olkoon nyt $A = (Q, \Sigma, *)$, $|\Sigma| = k$, vahvasti yhtenäinen automaatti. Rajoituksetta voidaan olettaa, että $Q = \{1, \dots, n\}$. Liitetään automaattiin A $n \times n$-matriisi $B = (b_{ij})$, jossa alkio b_{ij} on nuolien lukumäärä tilasta j tilaan i. Induktiolla on helppo todeta, että kaikilla $k \in \mathbb{N}$ matriisin B^k koordinaatissa (i, j) oleva alkio kertoo, kuinka monta pituutta k olevaa polkua

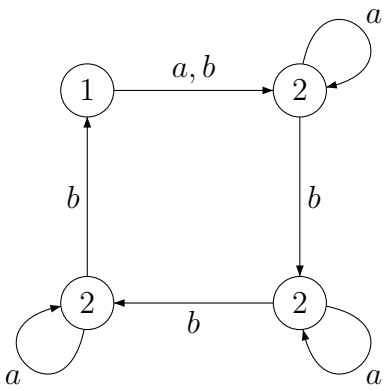
graafissa on tilasta j tilaan i. Koska automaatin A graafi on vahvasti yhtenäinen, niin B on redusoitumaton. Siis myös matriisi B^T on redusoitumaton. Perronin-Frobeniuksen lauseen nojalla matriisilla B^T on positiivinen ominaisarvo r, jonka itseisarvo on vähintään yhtä suuri kuin muilla ominaisarvoilla, ja johon kuuluu positiivinen ominaisvektori $\mathbf{x} = (x_1, \ldots, x_n)^T$. Olkoon α sellainen luku, että vektorin $\alpha\mathbf{x}$ suurin luku on $x_i = 1$. Tästä seuraa, että $k \geq (B^T\alpha\mathbf{x})_i = (r\alpha\mathbf{x})_i = r$. Valitaan toisalta luku β niin, että vektorin $\beta\mathbf{x}$ pienin luku on 1. Päätellään kuten edellä, että $k \leq r$ ja siis $r = k$. Koska matriiseilla B^T ja B on samat ominaisarvopolynomit, niillä on samat ominaisarvot. Siis matriisilla B on ominaisarvo k, jonka itseisarvo on vähintään yhtä suuri kuin muilla ominaisarvoilla.

Matriisilla B on ominaisarvoon k kuuluva ominaisvektori, jonka komponentit ovat rationaalisia. Tämä nähdään tarkastelemalla yhtälöä $B\mathbf{x} = k\mathbf{x}$, missä $\mathbf{x} = (x_1, \ldots, x_n)^T$. Tiedetään, että positiivisia ominaisvektoreita on olemassa, joten voidaan tehdä sijoitus $x_1 = 1$. Saadaan n:n yhtälön yhtälöryhmä, jossa on $n - 1$ muuttujaa $x_2, \ldots x_n$. Koska ominaisarvoon k kuuluvan ominaisavaruuden dimensio on 1, niin yhtälöryhmä määrää muuttujille yksikäsitteiset arvot. Yhtälöistä voidaan siis valita $n - 1$:n lineaarisesti riippumattoman yhtälön joukko. Näiden muodostama yhtälöryhmä on muotoa $B'\mathbf{x}' = \mathbf{c}$, missä B' on kääntyvä kokonaislukumatriisi, $\mathbf{x}' = (x_2, \ldots, x_n)^T$ ja $\mathbf{c}$ on kokonaislukuvektori. Koska B' on kokonaislukumatriisi, sen käänteismatriisin alkiot ovat rationaalilukuja. Siis ratkaisemalla yhtälöstä $\mathbf{x}'$ selviää, että $x_2, \ldots, x_n$ ovat rationaalilukuja.

Kertomalla ominaisarvoon k kuuluva rationaalinen ominaisvektori sopivalla luvulla saadaan ominaisvektori $\mathbf{w}^T = (w_1, \ldots, w_n)^T$, jonka komponentit ovat luonnollisia lukuja, joiden suurin yhteinen tekijä on 1. Tällainen vektori on yksikäsitteinen. Vektorin $\mathbf{w}$ avulla voidaan määritellä painofunktio $w : Q \to \mathbb{N}$, $w(i) = w_i$ kuten artikkelissa [9] on tehty. Lukua $w(i)$ kutsutaan tilan i *painoksi*. Joukon $S \subseteq Q$ painon määritellään olevan $\sum_{i \in S} w(i)$ ja siitä käytetään merkintää $w(S)$.

Painon määrittelystä ominaisvektorin $\mathbf{w}^T$ avulla seuraa, että kaikilla $i \in Q$ luvun $kw(i)$ arvo on niiden tilojen painojen summa, joista tulee nuoli tilaan i. (Jos jostakin tilasta saapuu useampi nuoli, niin summauksessa tilan paino kerrotaan siitä saapuvien nuolien lukumäärällä.) Tämän tiedon avulla on joskus helppo arvata pelkästään automaatin graafia katsomalla, mikä sen painofunktio on.

Esimerkki 4.14. Kuvan 7 automaatissa on merkitty tiloihin niiden painot. Edellisen kappaleen mukaisesti on helppo tarkistaa, että painot ovat juuri nämä.



Kuva 7: Automaatti ja tilojen painot.

Painon käsitteen avulla voidaan muotoilla yksi mahdollinen tapa etsiä synkronisoituvan ja vahvasti yhtenäisen automaatin $A = (Q, \Sigma, *)$ synkronisoivaa sanaa. Aloitetaan mielivaltaisesta tilasta $q \in Q$ ja etsitään lyhin mahdollinen sana w_1, jolla $w(q * w_1^{-1}) > w(q)$. Etsitään sitten lyhin mahdollinen sana, jolla $w(q*(w_2w_1)^{-1}) > w(q*w_1^{-1})$. Jatketaan vastaavasti, kunnes on löydetty sellainen sana $w = w_k \dots w_1$, että $q*w^{-1} = Q$. Tällöin $Q*w = q$, eli w on synkronisoiva sana. On selvitettävä, kuinka pitkiä sanat w_i voivat pisimmillään olla. Tehdään sanojen w_i pituutta koskevat tarkastelut artikkelin [11] esitystä seuraten.

Jokaiseen joukkoon $S \subseteq Q$ voidaan liittää vektori $[S] = (s_1, .., s_n)$, missä

$$s_i = \begin{cases} 1 & \text{kun } q \in S \\ 0 & \text{muulloin.} \end{cases}$$

Jokaiseen kirjaimeen $a \in \Sigma$ voidaan liittää $n \times n$ matriisi $[a] = (a_{ij})$, missä

$$a_{ij} = \begin{cases} 1 & \text{kun } i * a = j \\ 0 & \text{muulloin.} \end{cases}$$

Vastaavasti sanaan $w \in \Sigma^*$ voidaan liittää matriisi $[w] = (w_{ij})$, missä

$$w_{ij} = \begin{cases} 1 & \text{kun } i * w = j \\ 0 & \text{muulloin.} \end{cases}$$

Induktiolla on helppo todistaa, että jos $w = a_1...a_k$, niin $[w] = [a_1]...[a_k]$. Matriisi $[w]^T$ vastaa lineaarikuvausta $\mathbb{R}^n \to \mathbb{R}^n$, jonka rajoittuma joukolle $\{[S] \mid S \subseteq Q\}$ on varsin luonteva:

$$[S][w]^T = [S * w^{-1}].$$

Määritellään lineaarikuvaus $\hat{w} : \mathbb{R}^n \to \mathbb{R}$, $\hat{w}(\mathbf{x}) = \mathbf{x}\mathbf{w}^T$, missä $\mathbf{w}^T$ on edellä mainittu ominaisvektori. Sen rajoittuma joukolle $\{[S] \mid S \subseteq Q\}$ yhtyy painofunktioon w:

$$\hat{w}([S]) = w(S).$$

Jatkossa näistä molemmista funktioista käytetään merkintää w.

Kaikilla $\mathbf{x} \in \mathbb{R}^n$

$$\sum_{a\in\Sigma} w(\mathbf{x}[a]^T) = w(\mathbf{x}\sum_{a\in\Sigma}[a]^T) = \mathbf{x}(\sum_{a\in\Sigma}[a]^T)\mathbf{w}^T = k\mathbf{x}\mathbf{w}^T = kw(\mathbf{x}). \quad (1)$$

On kaksi vaihtoehtoa: joko kaikilla $a \in \Sigma$ on $w(\mathbf{x}[a]^T) = w(\mathbf{x})$ tai jollakin $a \in \Sigma$ on $w(\mathbf{x}[a]^T) > w(\mathbf{x})$. Vastaavasti voidaan osoittaa, että jos on sana u, jolla $w(\mathbf{x}[u]^T) \neq w(\mathbf{x})$, niin on olemassa yhtä pitkä sana u', jolla $w(\mathbf{x}[u']^T) > w(\mathbf{x})$.

Määritellään joukot

$$Z_0 = \{\mathbf{x} \in \mathbb{R}^n \mid w(\mathbf{x}) = 0\} \text{ ja } Z_1 = \{(r, \ldots, r) \in \mathbb{R}^n \mid r \in \mathbb{R}\}.$$

Jos $\mathbf{y} \in \mathbb{R}^n$ on mielivaltainen, niin valitsemalla $\mathbf{z} \in Z_1$ sopivasti saadaan vektorin $\mathbf{x} = \mathbf{y} - \mathbf{z}$ paino nollaksi, eli vektorilla $\mathbf{y}$ on esitys $\mathbf{y} = \mathbf{x} + \mathbf{z}$, missä $\mathbf{x} \in Z_0$ ja $\mathbf{z} \in Z_1$. Tämä esitys on yksikäsitteinen, sillä $Z_0 \cap Z_1 = \{0\}$. Koska $\mathbf{z}[w]^T = \mathbf{z}$ kaikilla sanoilla w, niin $w(\mathbf{y}[w]^T) \neq w(\mathbf{y})$ tarkalleen silloin kun $w(\mathbf{x}[w]^T) \neq w(\mathbf{x}) = 0$, eli silloin kun $\mathbf{x}[w]^T \notin Z_0$. Yhdistämällä tämä edellisen kappaleen havaintoon voidaan todeta, että jos $\mathbf{x}[w]^T \notin Z_0$ jollakin $w \in \Sigma^*$, niin on olemassa yhtä pitkä sana $u \in \Sigma^*$, jolla $w(\mathbf{y}[u]^T) > w(\mathbf{y})$.

Seuraavaksi todistettava lemma on yleisemminkin hyödyllinen.

Lemma 4.15. Liitetään kuhunkin kirjaimeen $a \in \Sigma$ jokin reaalinen n-neliömatriisi $\overline{a}$ ja jokaiseen sanaan $w = a_1 \ldots a_t$ matriisi $\overline{w} = \overline{a_1} \ldots \overline{a_t}$. Jos $V \subseteq \mathbb{R}^n$ on vektoriavaruus, $\mathbf{x} \in V$, ja on olemassa sellainen sana w, että $\mathbf{x}\overline{w} \notin V$, niin lyhin tällainen sana on pituudeltaan enintään $\dim(V)$.

Todistus. Olkoon U_i $(i \geq 0)$ vektoriavaruus, jonka generoi joukko

$$G_i = \begin{cases} \{\mathbf{x}\} & \text{kun } i = 0 \\ \{\mathbf{x}_{i-1}\overline{a} \mid \mathbf{x}_{i-1} \in G_{i-1}, a \in \Sigma\} \cup G_{i-1} & \text{muulloin.} \end{cases}$$

Jos jollakin luvulla i on $U_{i+1} = U_i$, niin $U_j = U_i$ kaikilla $j \geq i$. Tämä nähdään induktiolla: jos $U_k = U_i$, niin

$$\begin{aligned} G_{k+1} &= \{\mathbf{x}_k\overline{a} \mid \mathbf{x}_k \in G_k, a \in \Sigma\} \cup G_k \subseteq \{\mathbf{x}_k\overline{a} \mid \mathbf{x}_k \in U_k, a \in \Sigma\} \cup U_k \\ &= \{\mathbf{x}_k\overline{a} \mid \mathbf{x}_k \in U_i, a \in \Sigma\} \cup U_i \subseteq U_{i+1} \cup U_i = U_i. \end{aligned}$$

Siis $U_{k+1} = U_i$.

Olkoon w lyhin sana, jolla $\mathbf{x}\overline{w} \notin V$ ja $i = |w|$. Koska kaikilla j joukon G_j vektorit ovat $\mathbf{x}\overline{u}$, missä u on enintään pituutta j, niin i on pienin luku, jolla $G_i \not\subseteq V$ ja samalla pienin luku, jolla $U_i \not\subseteq V$. Vektoriavaruusketjussa $U_0 \subset U_1 \subset \cdots \subset U_i$ sisältymiset ovat aitoja, joten

$$1 = \dim(U_0) < \dim(U_1) < \cdots < \dim(U_{i-1}) \leq \dim(V).$$

Siis $i \leq \dim(V)$. □

Sovelletaan lemmaa nyt tämän luvun tapaukseen.

Lemma 4.16. Kaikilla $\mathbf{x} \in Z_0 \setminus \{0\}$ on olemassa enintään pituutta $n-1$ oleva sana w, jolla $\mathbf{x}[w]^T \notin Z_0$.

Todistus. Ensiksi osoitetaan, että on olemassa jokin sana w, jolla $\mathbf{x}[w]^T \notin Z_0$. Olkoon nimittäin vektorin $\mathbf{x}$ koordinaattissa i luku $r \neq 0$. Koska automaatti on synkronisoituva ja vahvasti yhtenäinen, niin on olemassa sellainen sana w, että $Q * w = \{i\}$. Siis matriisin $[w]^T$ i:s rivi koostuu ykkösistä ja muut rivit nollista, joten $\mathbf{x}[w]^T = (r, \ldots, r) \notin Z_0$.

Väite seuraa nyt edellisestä lemmasta valinnalla $V = Z_0$ ja $\overline{a} = [a]^T$ kaikilla $a \in \Sigma$. □

Seuraus 4.17. Kaikilla $S \subset Q$, $S \neq \emptyset$ on olemassa enintään pituutta $n-1$ oleva sana u, jolla $w(S * u^{-1}) > w(S)$.

Todistus. Esitetään vektori $[S]$ muodossa $\mathbf{x} + \mathbf{z}$, missä $\mathbf{x} \in Z_0$ ja $\mathbf{z} \in Z_1$. Edellä on todettu, että on olemassa pituutta i oleva sana u jolla $w(S * u^{-1}) > w(S)$ (eli $w([S][u]^T) > w([S])$) jos on olemassa yhtä pitkä sana w, jolla $\mathbf{x}[w]^T \notin Z_0$. Koska $[S] \notin Z_1$, niin $\mathbf{x} \neq 0$ ja väite seuraa edellisestä lemmasta. □

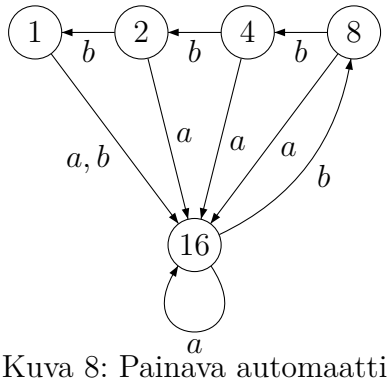
Lause 4.18. Jos $A = (Q, \Sigma, *) \in \mathbf{V}_n$ ja W_{max} on sen painavimman tilan paino, niin $\mathfrak{C}(A) \leq (w(Q) - W_{max})(n-1)$.

Todistus. Muodostetaan synkronisoiva sana w sivun 18 menetelmällä aloittamalla tilasta, jonka paino on W_{max}. Edellisen seurauslauseen nojalla kunkin osasanan w_i pituus on enintään $n-1$, joten koko sanan w pituus on enintään $(w(Q) - W_{max})(n-1)$. □

Lauseesta seuraa, että lyhimmän synkronisoivan sanan pituus on enintään $(n-1)^2$ sellaisilla vahvasti yhtenäisillä synkronisoituvilla automaateilla, joilla yhden tilan paino on mielivaltainen ja jokaisen muun tilan paino on 1. Erikoistapauksen tällaisista automaateista muodostavat ns. Eulerin automaatit.

Määritelmä 4.19. Automaatti $A = (Q, \Sigma, *)$ on *Eulerin automaatti*, jos sen jokaiseen tilaan saapuu $|\Sigma|$ nuolta.

Voidaan helposti todeta, että Eulerin automaatin jokaisen tilan paino on 1. Tämä mahdollistaa sen, että edellisen lauseen tulosta voidaan Eulerin automaattien tapauksessa hieman parantaa. Käytetään merkintää $\mathbf{E}_n$ synkronisoituvien n-tilaisten Eulerin automaattien joukosta.



Kuva 8: Painava automaatti

Lause 4.20. Jos $A = (Q, \Sigma, *) \in \mathbf{E}_n$, niin $\mathfrak{C}(A) \leq 1 + (n-2)(n-1) = n^2 - 3n + 3$.

Todistus. On olemassa $q \in Q$ ja $a \in \Sigma$, joilla $|q{*}a^{-1}| > |q| = 1$. Muodostetaan synkronisoiva sana w edellä esitetyllä menetelmällä aloittamalla tilasta q. □

Černýn konjektuuri on siis todistettu Eulerin automaattien tapauksessa. Ei kuitenkaan tiedetä, kuinka paljon ylärajaa $\mathfrak{C}(\mathbf{E}_n) \leq n^2 - 3n + 3$ voidaan parantaa. Esitetään tähän kysymykseen liittyen todistuksetta tulos lähteestä [10].

Lause 4.21. Jos $n \geq 5$ on pariton, niin $\mathfrak{C}(\mathbf{E}_n) \geq \frac{n^2-3n+4}{2}$.

Lause 4.18 ei yleisesti anna hyviä ylärajoja lyhimmän synkronisoivan sanan pituudelle. Kuvassa 8 on 5-tilainen automaatti, jolle lause antaa ylärajan 60 (vrt. lause 4.8: $\mathfrak{C}(5) \leq 20$), mutta itse asiassa jo sana a synkronisoi sen. Vastaavalla tavalla voidaan kaikilla $n > 1$ muodostaa n-tilainen automaatti, jolle lause antaa eksponentiaalisen ylärajan

$$\left(\left(\sum_{i=0}^{n-1} 2^i\right) - 2^{n-1}\right)(n-1) = \left(\sum_{i=0}^{n-2} 2^i\right)(n-1) = (2^{n-1} - 1)(n-1).$$

4.4 L-yhtenäiset automaatit

Tarkastellaan tässä artikkeliin [3] pohjautuvassa luvussa ns. L-yhtenäisten automaattien lyhimmän synkronisoivan sanan pituutta. Esitettävistä tuloksista osoittautuu olevan hyötyä myös luvun 6 konjektuurin tutkimisessa.

Määritelmä 4.22. Olkoon $A = (Q, \Sigma, *)$ automaatti. Jos $L = \{w_1, \ldots, w_t\} \subseteq \Sigma^*$ ja $R = \{q_1, \ldots, q_t\} \subseteq Q$ ovat sellaiset joukot, että kaikilla $s \in Q$ on $s * L = \{s * w_1, \ldots, s * w_t\} = \{q_1, \ldots, q_t\}$, niin automaattia A kutsutaan *L-yhtenäiseksi*. Tällöin joukkoa L kutsutaan *riippumattomaksi* ja joukkoa R kutsutaan L:n *kuvaksi*.

Käytetään jatkossa määritelmän merkintöjä ilman erillistä mainintaa.

Lemma 4.23. Kaikilla $v \in \Sigma^*$ joukko $vL = \{vw_1, \ldots, vw_t\}$ on riippumaton ja sen kuva on R.

Todistus. Jos $s \in Q$, niin $s * (vL) = \{s * vw_1, \ldots, s * vw_t\} = \{(s * v) * w_1, \ldots, (s * v) * w_t\} = R$. □

Lause 4.24. Jos $A = (Q, \Sigma, *)$ on L-yhtenäinen, niin kaikilla $P \subseteq R$ on

$$\sum_{i=1}^{t} |P * w_i^{-1} \cap R| = |P|t.$$

Todistus. Jos P on tyhjä joukko, niin väite on triviaali. Oletetaan siis, että $P = \{p_1, \ldots, p_m\}$, $m \geq 1$ jolloin

$$\sum_{i=1}^{t} |P * w_i^{-1} \cap R| = \sum_{i=1}^{t} \left| \bigcup_{j=1}^{m} p_j * w_i^{-1} \cap R \right| = \sum_{i=1}^{t} \sum_{j=1}^{m} |p_j * w_i^{-1} \cap R|.$$

L-yhtenäisyyden määritelmän nojalla kaikilla $s \in Q$ ja $p \in R$ on tarkalleen yksi sana $w_i \in L$, jolla $s \in p * w_i^{-1}$. Joukot $p * w_i^{-1}$ muodostavat siis joukon Q partition, joten $t = |R| = \sum_{i=1}^{t} |p * w_i^{-1} \cap R|$. Nyt

$$\sum_{i=1}^{t} \sum_{j=1}^{m} |p_j * w_i^{-1} \cap R| = \sum_{j=1}^{m} \sum_{i=1}^{t} |p_j * w_i^{-1} \cap R| = |P|t.$$

□

Seuraus 4.25. Jos $P \subseteq R$, niin kaikilla i on $|P * w_i^{-1} \cap R| = |P|$ tai jollakin i on $|P * w_i^{-1} \cap R| > |P|$

Lause 4.26. Olkoon $K \subseteq R$ synkronisoituva ja M suurimman joukkoon R sisältyvän synkronisoituvan joukon koko. Seuraavat ovat ekvivalentteja.

1. $|K| = M$.
2. Kaikilla $w \in L$ ja $v \in \Sigma^*$ on $|K * (vw)^{-1} \cap R| \leq |K|$.
3. Kaikilla $w \in L$ ja $v \in \Sigma^*$ on $|K * (vw)^{-1} \cap R| = |K|$.
4. K on maksimaalinen joukon R synkronisoituva osajoukko.

Todistus. 1 $\implies$ 2: Seuraa suoraan siitä, että $K * (vw)^{-1} \cap R$ on myös synkronisoituva joukko.

2 $\implies$ 3: Koska vL on riippumaton joukko, jonka kuva on R, niin tämä implikaatio seuraa Seurauksesta 4.25.

3 $\implies$ 4: Olkoon $X \subseteq R$ synkronisoituva, $|X| = M$. On olemassa sanat $v \in \Sigma^*$ ja $w \in L$ sekä tila $q \in Q$, joilla $X * v = q$ ja $q * w \in K$. Siis $X * vw \subseteq K$ ja $X \subseteq K * (vw)^{-1} \cap R$. Tästä ja oletuksesta 3 seuraa, että $|K| = |K * (vw)^{-1} \cap R| \geq M$. Luvun M valinnan nojalla $|K| = M$ ja K on maksimaalinen.

4 $\implies$ 1: Olkoon X kuten edellä. On olemassa sanat $v \in \Sigma^*$ ja $w \in L$ sekä tila $q \in Q$, joilla $K * v = q$ ja $q * w \in X$. Siis $K \subseteq X * (vw)^{-1} \cap R$. Koska $X * (vw)^{-1} \cap R$ on synkronisoituva, niin joukon K maksimaalisuudesta seuraa, että $K = X * (vw)^{-1} \cap R$. Implikaatio 1 $\implies$ 3 on jo todistettu, joten tiedetään, että $|X * (vw)^{-1} \cap R| = |X| = M$. Siis $|K| = M$. □

Lemma 4.27. Olkoon $K \subseteq R$ ja $v \in \Sigma^*$. Ehto

$$|K * (vw_i)^{-1} \cap R| = |K|$$

on voimassa kaikilla $w_i \in L$ tarkalleen silloin, kun vektori $([R][v])^T$ on yhtälöryhmän

$$\left([K * w_i^{-1}] - \frac{|K|}{|R|}[Q]\right)\mathbf{x} = 0,\ 1 \leq i \leq t \tag{2}$$

ratkaisu (sijoitus muuttujaan x).

Todistus. Tekemällä mainittu sijoitus saadaan

$$\left([K * w_i^{-1}] - \frac{|K|}{|R|}[Q]\right)([R][v])^T = ([K * w_i^{-1}][v]^T)[R]^T - \frac{|K|}{|R|}([Q][v]^T)[R]^T$$

$$= |K * (vw_i)^{-1} \cap R| - \frac{|K|}{|R|}|Qv^{-1} \cap R| = |K * (vw_i)^{-1} \cap R| - |K|.$$

Tämä on nolla tarkalleen silloin kun $|K * (vw_i)^{-1} \cap R| = |K|$. □

Käytetään merkintää $\text{rank}(A)$ matriisin A asteesta ja merkintää $\overline{A}$ matriisin A pystyrivialiavaruudesta.

Lemma 4.28. Jos A on t-rivinen reaalilukumatriisi, jossa ei ole nollarivejä ja jonka kussakin sarakkeessa on enintään $x > 0$ nollasta eroavaa alkiota, niin $\text{rank}(A) \geq t/x$.

Todistus. Matriisin A sarakkeista voidaan valita vektoriavaruuden $\overline{A}$ kanta $B = \{\mathbf{a}_1, \ldots, \mathbf{a}_r\}$, missä $r = \text{rank}(A)$. Näissä vektoreissa on yhteensä enintään rx nollasta eroavaa alkiota.

Väitteen osoittamiseksi tehdään vastaoletus, että $rx < t$. Tällöin jossakin koordinaatissa i on kaikissa kannan B vektoreissa nollia. Koska B virittää avaruuden $\overline{A}$, niin matriisin A rivi i koostuu pelkästään nollista, mikä on vastoin lemman oletusta. □

Lemma 4.29. Jos A ja B ovat reaalilukumatriiseja, jotka voidaan laskea yhteen, niin

$$\text{rank}(A) + \text{rank}(B) \geq \text{rank}(A + B).$$

Todistus. Olkoon V suppein vektoriavaruus, joka sisältää avaruudet $\overline{A}$ ja $\overline{B}$. Näiden avaruuksien kannat yhdessä virittävät avaruuden V, joten $\text{rank}(A) + \text{rank}(B) \geq \dim(V)$. Avaruus V sisältää kaikki avaruuden $\overline{A+B}$ vektorit, joten $\dim(V) \geq \text{rank}(A + B)$. □

Lemma 4.30. Olkoon $K \subseteq R$ ja oletetaan, että $\emptyset \neq K * w^{-1} \neq Q$ kaikilla $w \in L$ (erityisesti $K \neq R$). Sivun 24 yhtälöryhmän (2) matriisin aste on vähintään

$$\max\left\{\frac{|R \setminus K|}{|K|}, \frac{|K|}{|R \setminus K|}\right\}.$$

Todistus. Yhtälöryhmän matriisi on

$$C = A - \frac{|K|}{|R|}Y,$$

missä matriisi Y koostuu pelkästään ykkösistä ja matriisin A vaakariveinä on vektorit $[K * w_i^{-1}]$ $(1 \leq i \leq t)$.

Koska $K * w_i^{-1} \neq \emptyset$, niin matriissa A ei ole nollarivejä. Lisäksi joukon L määritelmästä seuraa, että jos $q \in Q$ on mielivaltainen, niin joukossa L on $|K|$ sanaa w, joilla $q * w \in K$. Siis matriisin A jokaisessa sarakkeessa on tarkalleen $|K|$ nollasta eroavaa alkiota, joten lemman 4.28 nojalla $\text{rank}(A) \geq t/|K|$. Lemman 4.29 nojalla $\text{rank}(C) + \text{rank}((|K|/|R|)Y) \geq \text{rank}(A)$, joten

$$\text{rank}(C) \geq \text{rank}(A) - \text{rank}\left(\frac{|K|}{|R|}Y\right) \geq t/|K| - 1 = \frac{|R \setminus K|}{|K|}.$$

Matriisi C voidaan myös esittää muodossa $C = (A - Y) + (1 - |K|/|R|)Y$. Matriisin $A - Y$ alkio on erisuuri kuin nolla tarkalleen silloin kun matriisin A vastinalkio on nolla. Siis matriisin $A - Y$ jokaisessa sarakkeessa on tarkalleen

$t - |K|$ nollasta eroavaa alkiota. Lisäksi matriisissa $A - Y$ ei ole nollarivejä (koska $K * w_i^{-1} \neq Q$), joten $\operatorname{rank}(A - Y) \geq t/(t - |K|)$ ja

$$\operatorname{rank}(C) \geq \operatorname{rank}(A - Y) - \operatorname{rank}\left(-\left(1 - \frac{|K|}{|R|}\right) Y\right) \geq \frac{t}{t - |K|} - 1 = \frac{|K|}{|R \setminus K|}.$$

□

Lemma 4.31. Olkoon K synkronisoituva, ei-maksimaalinen joukon R osajoukko. Tälloin on olemassa sanat $v \in \Sigma^*$ ja $w \in L$, joilla

$$|K * (vw)^{-1} \cap R| > |K| \quad \text{ja} \quad |v| \leq n - \max\left\{\frac{|R \setminus K|}{|K|}, \frac{|K|}{|R \setminus K|}\right\},$$

missä n on automaatin tilojen lukumäärä.

Todistus. Seurauksen 4.25 ja Lemman 4.23 nojalla riittää osoittaa, että on olemassa vaadittua pituutta oleva sana v ja jokin $w \in L$, joilla $|K * (vw)^{-1} \cap R| \neq |K|$. Voidaan olettaa, että $\emptyset \neq K * w^{-1} \neq Q$, sillä muutoin väite seuraa helposti valitsemalla $v = \epsilon$.

Olkoon N sivun 24 yhtälöryhmän 2 ratkaisujen muodostama vektoriavaruus (tulkitaan ratkaisut nyt pystyvektoreina). Koska K ei ole maksimaalinen, niin lauseesta 4.26 ja lemmasta 4.27 seuraa, että on olemassa sana $v \in \Sigma^*$, jolla $[R][v] \notin N$. Lemman 4.15 nojalla sana v voidaan vieläpä valita niin, että $|v| \leq \dim N$. Jos $f : \mathbb{R}^n \to \mathbb{R}^t$ on lineaarikuvaus, niin tunnetun lineaarialgebran tuloksen mukaan $n = \dim(f^{-1}(0)) + \dim(f(\mathbb{R}^n))$. Siis tulkitsemalla yhtälöryhmän matriisi C lineaarikuvauksen matriisina voidaan päätellä, että, $\dim(N) = n - \operatorname{rank}(C)$ (sillä matriisissa C on n pystyriviä). Tästä seuraa yhdessä lemman 4.30 kanssa, että sana v on vaadittua pituutta, ja koska $[R][v] \notin N$, niin lemman 4.27 nojalla jollakin $w \in L$ on $|K * (vw)^{-1} \cap R| \neq |K|$. □

Lause 4.32. Olkoon $A = (Q, \Sigma, *)$ n-tilainen synkronisoituva L-yhtenäinen automaatti ja $|L| = t$. Jos merkitään joukon L lyhimmän sanan pituutta L_ω ja pisimmän sanan pituutta L_Ω, niin

$$\mathfrak{C}(A) \leq (t - 1)(n + 1 + L_\Omega) - 2t \ln \frac{t + 1}{2} + L_\omega.$$

Todistus. Tapauksessa $t = 1$ joukon L ainoa sana synkronisoi automaatin. Sen pituus on L_ω, joten väite toteutuu tässä tapauksessa. Oletetaan siis, että $t > 1$, valitaan mielivaltainen $q \in R$ ja merkitään $K_0 = \{q\}$. Määritellään

joukkojen K_i ketju induktiivisesti: jos $K_i \neq R$, niin edellisen lemman mukaan voidaan valita sanat $v_i \in \Sigma^*$ ja w_{γ_i}, joilla

$$|K_i * (v_i w_{\gamma_i})^{-1} \cap R| > |K_i| \quad \text{ja} \quad |v_i| \leq n - \max\left\{\frac{|R \setminus K_i|}{|K_i|}, \frac{|K_i|}{|R \setminus K_i|}\right\}.$$

Merkitään $K_{i+1} = K_i * (v_i w_{\gamma_i})^{-1} \cap R$ ja olkoon r indeksi, jolla $K_r = R$. Valitsemalla $v = v_{r-1} w_{\gamma_{r-1}} \dots v_0 w_{\gamma_0} \in \Sigma^* L$ saadaan $R * v = q$ ja

$$\begin{aligned}
|v| &\leq \sum_{i=0}^{r-1} \left(n - \max\left\{\frac{|R \setminus K_i|}{|K_i|}, \frac{|K_i|}{|R \setminus K_i|}\right\} + L_\Omega \right) \\
&\leq \sum_{j=1}^{t-1} \left(n - \max\left\{\frac{t-j}{j}, \frac{j}{t-j}\right\} + L_\Omega \right) \\
&= (t-1)(n + L_\Omega) - \sum_{j=1}^{t-1} \max\left\{\frac{t}{j} - 1, \frac{t}{t-j} - 1\right\} \\
&= (t-1)(n + L_\Omega + 1) - t \sum_{j-1}^{t-1} \frac{1}{\min\{j, t-j\}}.
\end{aligned}$$

Jos $w \in L$, niin $|Q * wv| = 1$. Jos valitaan w niin, että $|w| = L_\omega$, niin lauseen todistamiseksi riittää osoittaa, että

$$\sum_{j=1}^{t-1} \frac{1}{\min\{j, t-j\}} \geq 2 \ln \frac{t+1}{2}.$$

Olkoon $h = \lfloor (t-1)/2 \rfloor$. Integroimalla todetaan, että $\sum_{j=1}^{h} 1/j = \sum_{j=t-h}^{t-1} 1/(t-j) \geq \ln(h+1)$, joten

$$S = \sum_{j=1}^{h} \frac{1}{j} + \sum_{j=t-h}^{t-1} \frac{1}{t-j} \geq 2 \ln(h+1).$$

Jos t on pariton, niin $h = (t-1)/2$ ja $\sum_{j=1}^{t-1} 1/\min\{j, t-j\} = S \geq 2\ln(h+1) = 2\ln((t+1)/2)$. Jos taas t on parillinen, niin $h = (t-2)/2$ ja $\sum_{j=1}^{t-1} 1/\min\{j, t-j\} = S + 2/t \geq 2\ln(h+1) + 2/t$. Epäyhtälöstä $\ln((t+1)/2) - \ln(h+1) = \ln((t+1)/(2(h+1))) = \ln(1 + 1/t) \leq 1/t$ seuraa, että $2\ln(h+1) + 2/t = 2(\ln(h+1) + 2/t) \geq 2\ln((t+1)/2)$, joten $\sum_{j=1}^{t-1} \frac{1}{\min\{j,t-j\}} \geq 2\ln((t+1)/2)$. □

Edellistä lausetta sovellettaessa joukon L valinta on tärkeässä roolissa. Jos nimittäin A on synkronisoituva automaatti ja w on sen lyhin synkronisoiva sana, niin A on L-yhtenäinen, kun valitaan $L = \{w\}$. Tällöin kuitenkin edellinen lause redusoituu muotoon $\mathfrak{C}(A) \leq \mathfrak{C}(A)$. Tarkastellaan nyt erästä automaattien luokkaa, missä joukko L voidaan valita paremmin.

Määritelmä 4.33. Automaatti $A = (Q, \Sigma, *)$ on *1-klusteriautomaatti*, jos sen graafissa jollakin kirjaimella $a \in \Sigma$ merkityt nuolet muodostavat tarkalleen yhden syklin ja (mahdollisesti) joukon puita, jotka johtavat tähän sykliin. Tällaista sykliä kutsutaan *a-pääsykliksi*.

Lause 4.34. Jos $A = (Q, \Sigma, *)$ on synkronisoituva 1-klusteriautomaatti ja $|Q| = n \geq 2$, niin

$$\mathfrak{C}(A) \leq 2n^2 - 4n + 1 - 2(n-1)\ln\frac{n}{2}.$$

Todistus. Olkoon $a \in \Sigma$ kuten määritelmässä 4.33, $R \subseteq W$ a-pääsykliin kuuluvien tilojen joukko ja $|R| = t$. Automaatti A on L-yhtenäinen, missä $L = \{a^{n-1}, a^{n-2}, \ldots, a^{n-t}\}$. Nimittäin $q * a^{n-t} \in R$ kaikilla $q \in Q$, ja kun i käy luvut $0 \leq i \leq t-1$, niin $(q * a^{n-t}) * a^i$ käy läpi kaikki joukon R tilat.

Jos $t = n$, niin automaatti on syklinen ja tässä tapauksessa artikkelissa [7] on todistettu, että $\mathfrak{C}(A) \leq (n-1)^2$. Epäyhtälö

$$(n-1)^2 \leq 2n^2 - 4n + 1 - 2(n-1)\ln\frac{n}{2}$$

on ekvivalentti epäyhtälön

$$f(n) = n^2 - 2n - 2(n-1)\ln\frac{n}{2} \geq 0$$

kanssa. Koska $\ln x \leq x - 1$ kun $x > 0$, niin $f(n) = n(n - 2 - 2\ln(n/2)) + 2\ln(n/2) \geq n(n - 2 - 2(n/2 - 1)) + 2\ln(n/2) = 2\ln(n/2) \geq 0$ kun $n \geq 2$.

Keskitytään nyt tapaukseen $t < n$. Lauseen 4.32 merkintöjä käyttämällä $l_\omega = n - t$ ja $L_\Omega = n - 1$, joten saman lauseen nojalla

$$\mathfrak{C}(A) \leq 2nt - n - t - 2t\ln\frac{t+1}{2}.$$

Lauseen todistamiseksi osoitetaan, että

$$2nt - n - t - 2t\ln\frac{t+1}{2} \leq 2n^2 - 4n + 1 - 2(n-1)\ln\frac{n}{2}.$$

Tämä epäyhtälö on ekvivalentti epäyhtälön

$$2(n-1)\ln n - 2t\ln(t+1) \leq (2n - 1 + 2\ln 2)(n - t - 1)$$

kanssa. Käyttämällä taas arviota $\ln x \leq x - 1$ saadaan

$$\begin{aligned}
&2(n-1)\ln n - 2t\ln(t+1) = 2t\ln\frac{n}{t+1} + 2(n-t-1)\ln n \\
\leq &2t\frac{n-t-1}{t+1} + 2(n-t-1)(n-1) \leq 2n(n-t-1) \\
\leq &(2n - 1 + 2\ln 2)(n - t - 1);
\end{aligned}$$

kahdessa viimeisessä epäyhtälössä tarvitaan oletusta $t < n$. □

5 Tienväritysongelma

Olkoon Γ suunnattu graafi, jonka jokaisesta solmusta lähtee sama määrä nuolia ja jossa kahden solmun välillä voi olla useita nuolia. Jos Σ on aakkosto, jossa on kirjaimia yhtä monta kuin kussakin solmussa on lähteviä nuolia, niin voidaan muodostaa automaatti merkitsemällä jokainen graafin nuoli jollakin kirjaimella niin, että mistään solmusta ei lähde kahta samalla kirjaimella merkittyä nuolta. Tällaista graafin nuolien merkintää kutsutaan graafin *väritykseksi*. (Nimitys tulee siitä, että joskus aakkoston Σ alkioiden mielletään olevan värejä kirjainten sijasta.) Väritykseksi voidaan kutsua myös väritystä vastaavaa automaattia. Jos värityksellä saadaan muodostettua synkronisoituva automaatti, niin väritystä kutsutaan *synkronisoivaksi*. Kysymystä siitä, millaisilla graafeilla on olemassa synkronisoiva väritys, kutsutaan *tienväritysongelmaksi*.

Oletetaan jatkossa, että tarkasteltavat graafit ovat *vahvasti yhtenäisiä*, eli graafin mistä tahansa solmusta pääsee mihin tahansa toiseen solmuun seuraamalla graafin nuolia oikeaan suuntaan. Helposti saadaan seuraava välttämätön ehto synkronisoivan värityksen olemassaololle.

Lause 5.1. Jos graafilla Γ on synkronisoiva väritys, niin graafin syklien pituuksien suurin yhteinen tekijä on 1.

Todistus. Tehdään vastaoletus, että graafin syklien pituuksien suurin yhteinen tekijä on $d > 1$. Olkoon graafilla kiinnitetty synkronisoiva väritys $A = (Q, \Sigma, *)$ ja olkoon v jokin synkronisoiva sana. Kaikilla sanoilla u myös uv on synkronisoiva sana, joten on olemassa synkronisoiva sana w, jonka pituus l ei ole jaollinen luvulla d. Olkoon $Q * w = q$. Sana w indusoi automaatissa pituutta l olevan polun tilasta q siihen itseensä. Tämä polku voidaan muodostaa syklejä yhdistelemällä, joten vastaoletuksen nojalla d jakaa luvun l, mikä on mahdotonta luvun l valinnan nojalla. □

Artikkelissa [1] esitetään konjektuuri, jonka mukaan tämä välttämätön ehto on myös riittävä.

Konjektuuri 5.2 (Tienväritysluause)**.** Jos Γ on suunnattu, vahvasti yhtenäinen graafi, jonka jokaisesta solmusta lähtee yhtä monta nuolta ja jonka syklien pituuksien suurin yhteinen tekijä on 1, niin sillä on synkronisoiva väritys.

Konjektuuri todistetaan artikkelissa [19]. Esitetään tässä kyseinen todistus. Kutsutaan jatkossa konjektuurin ehdot täyttävää graafia *primitiiviseksi*. Tarkasteluissa käytetään stabiilisuusrelaation käsitettä lähteestä [6].

Määritelmä 5.3. Automaatin $A = (Q, \Sigma, *)$ tilajoukon Q ekvivalenssirelaatiota $\sim$ kutsutaan *kongruenssiksi*, jos kaikilla $p, q, \in Q$ ja $a \in \Sigma$

$$p \sim q \implies p * a \sim q * a.$$

Määritelmä 5.4. Automaatin $A = (Q, \Sigma, *)$ tilapari $p, q \in Q$ on stabiili, merkitään $p \equiv q$, jos kaikilla $u \in \Sigma^*$ on olemassa sellainen $w \in \Sigma^*$, että $p * uw = q * uw$.

Lause 5.5. Automaatin $A = (Q, \Sigma, *)$ stabiilisuusrelaatio on kongruenssi.

Todistus. Selvästi relaatio $\equiv$ on refleksiivinen ja symmetrinen.

Olkoon $p, q, r \in Q$ sellaiset tilat, että $p \equiv q$ ja $q \equiv r$ ja olkoon $u \in \Sigma^*$ mielivaltainen. Koska $p \equiv q$, niin on olemassa $w_1 \in \Sigma^*$, jolla $p*uw_1 = q*uw_1$. Koska $q \equiv r$, niin on olemassa $w_2 \in \Sigma^*$, jolla $q * uw_1w_2 = r * uw_1w_2$. Kun $w = w_1w_2$, niin $p * uw = q * uw = r * uw$. Siis $p \equiv r$ ja relaatio $\equiv$ on ekvivalenssirelaatio.

Stabiilisuuden määritelmästä seuraa helposti, että jos $p \equiv q$, niin $p * w \equiv q * w$ kaikilla $w \in \Sigma^*$. Siis relaatio $\equiv$ on kongruenssi. □

Olkoon $A = (Q, \Sigma, *)$ automaatti, jolle on määritelty kongruenssi $\sim$ ja käytetään merkintää $[p]$ tilan p määräämästä ekvivalenssiluokasta. Automaatin A *tekijäautomaatti kongruenssin* $\sim$ *suhteen* on $A/\sim = (Q/\sim, \Sigma, \cdot)$, missä $Q/\sim = \{[p] \mid p \in Q\}$ ja kaikilla $[p] \in Q', w \in \Sigma^*$ on

$$[p] \cdot w = [p * w].$$

Koska $\sim$ on kongruenssi, niin operaatio $\cdot$ on hyvin määritelty.

Lemma 5.6. Olkoon Γ primitiivinen graafi ja $A = (Q, \Sigma, *)$ jokin graafin Γ väritys. Silloin automaatin $A/\equiv$ graafi Γ' on myös primitiivinen, ja jos graafilla Γ' on synkronisoiva väritys, niin myös graafilla Γ on synkronisoiva väritys.

Todistus. Koska Γ' on automaatin $A/\equiv = (Q/\equiv, \Sigma, \cdot)$ graafi, niin sen jokaisesta tilasta lähtee yhtä monta nuolta, ja koska Γ on vahvasti yhtenäinen, niin myös Γ' on vahvasti yhtenäinen. Jos C on graafin Γ sykli, niin sitä vastaa suljettu polku graafissa Γ, joten syklin C pituus voidaan ilmaista jonakin graafin Γ' syklien pituuksien summana. Siis graafin Γ' kaikkien syklien pituuksien suurin yhteinen tekijä on 1 ja Γ' on primitiivinen graafi.

Oletetaan sitten, että $B' = (Q/\equiv, \Sigma, \cdot')$ on synkronisoituva automaatti, joka on saatu graafin Γ' jollakin värityksellä. Automaatin B' voidaan myös ajatella muodostetun automaatista $A/\equiv$ permutoimalla kustakin tilasta $[p] \in$

$Q/\equiv$ lähtevien nuolten kirjaimia bijektiolla $\pi_{[p]} : \Sigma \to \Sigma$, joka toteuttaa ehdon $[p]\cdot'\pi_{[p]}(a) = [p]\cdot a$ kun $a \in \Sigma$. Muodostetaan graafin Γ uudelleenväritys $A' = (Q, \Sigma, *')$ määrittelemällä $p *' \pi_{[p]}(a) = p * a$ kaikilla $p \in Q$ ja $a \in \Sigma$.

Olkoon w jokin automaatin B' synkronisoiva sana eli $Q \cdot' w = [p] \in Q/\equiv$. Tällöin automaatissa A' on $Q *' w \subseteq [p]$. Koska joukon $[p]$ tilat ovat keskenään stabiileja automaatissa A, niin on olemassa sellainen sana $u' = a_1 \dots a_m$, $a_i \in \Sigma$, että $|[p] * u'| = 1$. Jos merkitään $P_i = [p] \cdot a_1 \dots a_i$, niin sana $u = \pi_{[p]}(a_1)\pi_{P_1}(a_2) \dots \pi_{P_{m-1}}(a_m)$ toteuttaa ehdon $|[p] *' u| = 1$. Siis sana wu synkronisoi automaatin A', joten graafilla Γ on synkronisoiva väritys. □

Lemma antaa seuraavan mahdollisen tavan konjektuurin ratkaisemiseen.

Lause 5.7. Oletetaan, että jokaisella primitiivisellä graafilla, jolla on vähintään kaksi solmua, on olemassa väritys A, jossa on epätriviaali stabiili tilapari $p, q \in Q$ (eli $p \neq q$ ja $p \equiv q$). Tällöin jokaisella primitiivisellä graafilla on synkronisoiva väritys.

Todistus. Todistetaan induktiolla primitiivisen graafin Γ tilojen lukumäärän n suhteen. Selvästi synkronisoiva väritys on olemassa jos $n = 1$. Oletetaan, että $n = k > 1$ ja että väite on todistettu pienemmille graafeille.

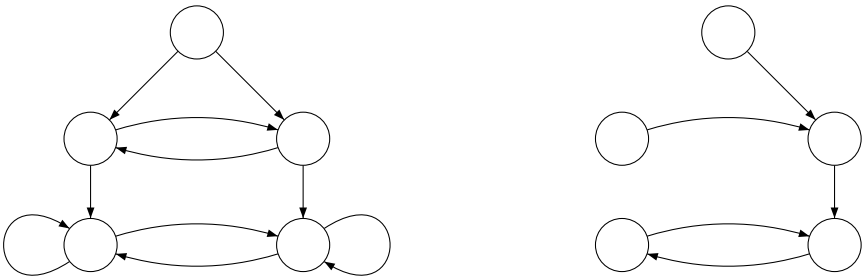
Lauseen oletuksen nojalla graafilla Γ on väritys A, jolla on epätriviaali stabiili tilapari. Silloin automaatin $A/\equiv$ tilojen lukumäärä on pienempi kuin k, joten induktio-oletuksen nojalla automaattiin $A/\equiv$ liittyvällä graafilla Γ' on synkronisoiva väritys. Lemman nojalla myös graafilla Γ on synkronisoiva väritys. □

Seuraavaksi esitettävät tulokset tähtäävät lauseen oletuksen todistamiseen.

Määritelmä 5.8. Olkoon $A = (Q, \Sigma, *)$ automaatti. Joukkoa $S \subseteq Q$ sanotaan *klikiksi*, jos kaikilla $w \in \Sigma^*$ on $|S * w| = |S|$.

Lemma 5.9. Olkoon $A = (Q, \Sigma, *)$ automaatti, S klikki jonka alkioiden lukumäärä on maksimaalinen ja w sellainen sana, että $|S \setminus (S * w)| = 1$. Silloin automaatissa A on epätriviaali stabiili tilapari.

Todistus. Oletetaan vastoin väitettä, että automaatissa ei ole epätriviaaleja stabiileja tilapareja. Merkitään $S * w = T$. Koska S on klikki, niin $|S| = |T|$ ja $|T \setminus S| = 1$. Olkoon $s \in S \setminus T$ ja $t \in T \setminus S$ näiden joukkojen uniikit alkiot. Koska $s \not\equiv t$, niin on olemassa sellainen sana u, että joukko $\{s * u, t * u\}$ ei ole synkronisoituva. Koska lisäksi joukot $S * u$ ja $T * u$ ovat klikkejä, niin mitkään joukon $(S \cup T) * u$ tilaparit eivät muodosta synkronisoituvaa joukkoa, eli $(S \cup T) * u$ on klikki. Koska $s * u \neq t * u$, niin $|(S \cup T) * u| = |A| + 1$, mikä on vastoin joukon S maksimaalisuusoletusta. □



Kuva 9: Virittävä graafi.

Määritelmä 5.10. Olkoon Γ primitiivinen graafi. Graafia Δ kutsutaan graafin Γ *virittäväksi* graafiksi, jos niillä on samat solmut ja graafin Δ nuolina on jokaisesta graafin Γ solmusta tarkalleen yksi lähtevä nuoli.

Esimerkki 5.11. Kuvassa 9 on eräs primitiivinen graafi ja sen virittävä graafi. Yleisestikin virittävät graafit muodostuvat sykleistä ja puista, joiden juuret ovat sykleillä.

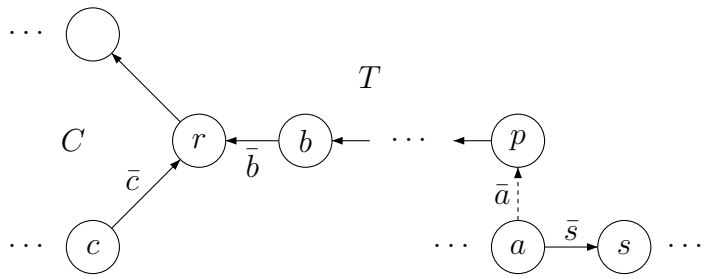
Jos s on jokin virittävän graafin solmu, niin lyhimmän polun pituutta solmusta s johonkin syklillä olevaan solmuun kutsutaan solmun s *syvyydeksi*. Erityisesti kaikkien sykleillä olevien solmujen syvyys on nolla.

Lemma 5.12. Olkoon Γ primitiivinen graafi, jossa on $n > 1$ solmua, ja Δ sen virittävä graafi. Jos graafi Δ koostuu vain sykleistä (eli kaikkien solmujen syvyys on nolla), niin graafilla Γ on myös sellainen virittävä graafi, jossa on vain yksi suurinta, positiivista syvyyttä oleva solmu.

Todistus. Graafissa Γ on jokin solmu s, josta lähtee nuolia ainakin kahteen eri solmuun, sillä muutoin graafin kaikki syklit olisivat pituutta n. Olkoon t se solmu, johon solmusta s lähtevä nuoli saapuu graafissa Δ. Muodostetaan uusi virittävä graafi Δ', joka on muuten samanlainen kuin Δ, paitsi että solmusta s solmuun t lähtevä nuoli on korvattu jollakin toiseen solmuun menevällä nuolella. Tässä virittävässä graafissa solmu t on ainoa suurinta syvyyttä oleva solmu. □

Jos jostain graafin solmusta s lähtee kaikki nuolet samaan solmuun, kutsutaan näiden nuolien joukkoa *kimpuksi*.

Lemma 5.13. Olkoon Γ primitiivinen graafi, jossa on $n > 1$ solmua ja jonka mihinkään solmuun ei saavu kahta kimppua. Graafilla Γ on virittävä graafi, jonka kaikki maksimaalista syvyyttä olevat solmut ovat samassa puussa.



Kuva 10: Graafin Δ osa.

Todistus. Valitaan graafin Γ virittävä graafi Δ niin, että maksimaalinen määrä solmuja (ekvivalentisti: maksimaalinen määrä nuolia) on osana syklejä. Jos graafi Δ koostuu vain sykleistä, niin väite seuraa edellisen lemman nojalla. Oletetaan siis, että maksimaalista syvyyttä olevan solmun syvyys d on positiivinen ja että kaikki tällaiset solmut eivät ole samassa puussa.

Olkoon p jokin maksimaalista syvyyttä oleva solmu, T puu, joka sisältää solmun p ja C sykli, johon puu T on yhteydessä. Olkoon r puun juurisolmu, c se syklin solmu, josta on nuoli juurisolmuun ja b se puun solmu, josta on nuoli juurisolmuun. Koska Γ on primitiivinen graafi, niin siinä on solmu, josta on nuoli solmuun p; olkoon jonkin tällaisen solmun nimi a. Tämä tilanne, joidenkin lisämerkintöjen ohella, on esitetty kuvassa 10. Kuvassa tavalliset nuolet kuuluvat graafiin Δ. Katkoviivalla merkitty nuoli ei kuulu graafiin Δ, mutta kuuluu graafiin Γ. Tarkoituksena on muodostaa graafin Δ pohjalta uusi virittävä graafi, joka toteuttaa väitteen.

Tapaus 1. Oletetaan, että solmusta c lähtevät nuolet eivät muodosta kimppua. Muodostetaan graafi Δ' graafista Δ korvaamalla nuoli $\bar{c}$ jollakin solmusta c lähtevällä nuolella $\bar{u}$, joka ei johda solmuun r, vaan solmuun, jonka nimi olkoon u. Solmu u ei voi kuulua puuhun T, sillä muutoin graafissa Δ' olisi sykli C', joka sisältää kaikki syklin C solmut ja lisäksi joitakin puun T solmuja, mikä on vastoin graafin Δ valintaa.

Koska u ei kuulu puuhun T, niin solmun p syvyys on graafissa Δ' suurempi kuin d ja kaikki maksimaalista syvyyttä olevat solmut ovat samassa puussa kuin p.

Tapaus 2. Oletetaan, että solmusta c lähtevät nuolet muodostavat kimpun. Muodostetaan graafi Δ' graafista Δ korvaamalla nuoli $\bar{s}$ nuolella $\bar{a}$. Oletetaan aluksi, että solmu a ei ole syklillä C. Jos a kuuluisi solmujen p ja r väliseen polkuun P, niin nuolen $\bar{a}$ lisäämisen myötä kaikki graafin Δ syklit säilyisivät graafissa Δ', mutta a tulisi osaksi uutta sykliä. Tämä on vastoin graafin Δ valintaa, joten a ei kuulu polkuun P. Siis a tulee liitetyksi puuhun T solmun p perään ja solmun a syvyydeksi tulee $d + 1$. Nyt kaikki

maksimaalista syvyyttä olevat solmut ovat puussa, jonka juuri on r.

Oletetaan nyt, että a on syklillä C. Tällöin graafissa Δ' on sykli C', joka sisältää solmun a, polun P ja nuolen $\bar{a}$. Jos syklissä C polun pituus solmusta r solmuun a on x, niin syklin C' pituus on $d+x+1$. Jos syklissä C polun pituus solmusta s solmuun r on y, niin syklin C pituus on $x+y+1$. Graafissa Δ' on muuten samat syklit kuin graafissa Δ, mutta sykli C on korvattu syklillä C'. Graafi Δ on valittu niin, että $x+y+1 \geq d+x+1$, eli $y \geq d$. Jos $y > d$, niin graafissa Δ' solmun s syvyys on $y \geq d+1$. Nyt kaikki maksimaalista syvyyttä olevat solmut ovat puussa, joka sisältää solmun s. Jäljelle jää tapaus $y = d$. Tällöin graafissa Δ' on maksimaalinen määrä solmuja sykleillä ja solmut s ja b ovat samassa roolissa kuin solmut p ja c graafissa Δ. Koska solmusta c lähtevät nuolet muodostavat kimpun, niin solmusta b lähtevät nuolet eivät muodosta kimppua, joten graafiin Δ' voidaan soveltaa tapausta 1. □

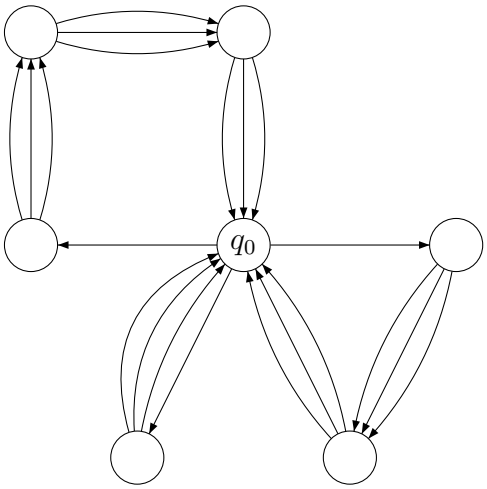
Lemma 5.14. Olkoon Γ primitiivinen graafi, jossa on vähintään kaksi solmua ja jonka jossain virittävässä graafissa Δ kaikki maksimaalista syvyyttä olevat solmut ovat samassa puussa. Olkoon lisäksi $A = (Q, \Sigma, *)$ graafista Γ muodostettu automaatti, jonka kaikki graafiin Δ kuuluvat nuolet on merkitty samalla kirjaimella $a \in \Sigma$. Tällöin automaatilla A on epätriviaali stabiili tilapari.

Todistus. Olkoon $C \subseteq Q$ niiden solmujen joukko, jotka kuuluvat johonkin sykliin graafissa Δ ja N niiden solmujen joukko, jotka ovat maksimaalista syvyyttä d. Olkoon lisäksi K jokin klikki, jossa on maksimaalinen määrä alkioita. Koska A on vahvasti yhtenäinen automaatti, on olemassa sellainen sana w, että klikki $K' = K * w$ sisältää jonkin solmun joukosta N. Koska kaikki joukon N alkiot ovat samassa graafin Δ puussa, niin $|N * a^d| = 1$. Koska klikissä ei voi tapahtua synkronisaatiota, niin $|K' \cap N| = 1$. Tästä seuraa, että $|(K' * a^{d-1}) \setminus C| = 1$; merkitään $S = K' * a^{d-1}$.

Olkoon m positiivinen kokonaisluku, joka on graafin Δ kaikkien syklien pituuksien monikerta. Klikkien S ja $T = S * a^m$ yhteiset alkiot ovat tarkalleen joukon $S \cap C$ alkiot. Koska $|S \setminus C| = 1$, niin $|S \setminus T| = 1$. Klikissä S on maksimaalinen määrä alkioita, joten lemman 5.9 nojalla automaatilla on epätriviaali stabiili tilapari. □

Lause 5.15. Jos Γ on primitiivinen graafi, jossa on vähintään kaksi solmua, niin sillä on väritys, jossa on epätriviaali stabiili tilapari.

Todistus. Jos graafissa Γ on solmut u ja v, joista lähtee kimput samaan solmuun, niin solmut u ja v muodostavat stabiilin tilaparin kaikissa värityksissä. Voidaan siis olettaa, että Γ toteuttaa lemman 5.13 ehdot ja että Δ on virittävä graafi, jossa kaikki maksimaalista syvyyttä olevat solmut ovat samassa puussa. Nyt väite seuraa edellisestä lemmasta. □



Kuva 11: Graafi, jonka syklien pituudet ovat 2, 3 ja 4.

Tämä lause yhdessä lauseen 5.7 kanssa todistaa tienvärityslauseen.

Esimerkki 5.16. Olkoon $a_1, \ldots, a_t \in \mathbb{N}$ $(t > 1)$ lukuja, joiden suurin yhteinen tekijä on 1. Joukon $\{a_1, \ldots, a_t\}$ *Frobeniuksen luvuksi* kutsutaan lukua

$$F(a_1, \ldots, a_t) = \max\{n \in \mathbb{N} \mid k_1a_1 + \ldots k_ta_t \neq n \text{ kaikilla } k_1, \ldots, k_t \in \mathbb{N} \cup \{0\}\},$$

joka toisin sanoen on suurin luku, jota ei voida esittää lukujen $a_1, \ldots, a_t$ epänegatiivisten monikertojen summana. Tällaisen luvun olemassaololle on olemassa alkeislukuteoreettinen todistus. Esitetään nyt vaihtoehtoinen todistus luvun $F(2, 3, 4)$ olemassaololle, jossa sovelletaan tienvärityslausetta. Tähän tapaukseen rajoitutaan havainnollisuuden vuoksi, mutta samaa todistusta voidaan soveltaa myös yleiseen tapaukseen.

Muodostetaan primitiivinen graafi Γ, jonka syklien pituudet ovat $2, 3$ ja 4, kuten kuvassa 11. Koska graafin syklien pituuksien suurin yhteinen tekijä on 1, niin tienvärityslauseen nojalla sillä on synkronisoiva väritys $A = (Q, \Sigma, *)$. Olkoon q_0 automaatin "keskustila"(ks. kuva) ja w sellainen synkronisoiva sana, että $Q * w = q_0$. Kaikilla sanoilla $u \in \Sigma^*$ myös uw on synkronisoiva sana ja $Q * uw = q_0$. Erityisesti $q_0 * uw = q_0$ kaikilla $u \in \Sigma^*$ ja sanan uw määräämä tilasta q_0 lähtevä polku voidaan muodostaa yhdistämällä syklejä, joiden pituus on $2, 3$ tai 4. Siis polun pituus $|uw|$ voidaan esittää lukujen $2, 3$ ja 4 epänegatiivisten monikertojen summana ja $F(2, 3, 4) < |w|$.

6 Hybridikonjektuuri

Nyt kun tiedetään, että jokaisella primitiivisellä graafilla on synkronisoiva väritys, niin voidaan Černýn konjektuurin hengessä kysyä, kuinka lyhyeksi lyhin synkronisoiva sana voidaan saada, kun graafin väritys valitaan sopivasti. Tähän kysymykseen liittyen on lähteessä [2] esitetty seuraava ns. *hybridikonjektuuri*.[2]

Käytetään merkintää $\mathbf{\Pi}$ kaikkien primitiivisten graafien joukosta ja merkintää $\mathbf{\Pi}_n$ kaikkien n solmua sisältävien primitiivisten graafien joukosta.

Määritelmä 6.1. Jos $\Gamma \in \mathbf{\Pi}$, niin käytetään merkintää $\mathfrak{H}(\Gamma)$ lyhimmän sellaisen sanan pituudesta, joka synkronisoi jonkin graafin Γ värityksen. Määritelmä laajennetaan kaikille $\mathbf{\Lambda} \subseteq \mathbf{\Pi}$ seuraavasti:

$$\mathfrak{H}(\mathbf{\Lambda}) = \max\{\mathfrak{H}(\Gamma) \mid \Gamma \in \mathbf{\Lambda}\} \quad \text{(jos olemassa)}.$$

Tapauksessa $\mathbf{\Lambda} = \mathbf{\Pi}_n$ merkitään $\mathfrak{H}(\mathbf{\Lambda}) = \mathfrak{H}(n)$.

Konjektuuri 6.2 (Hybridikonjektuuri)**.** Kaikilla kokonaisluvuilla $n > 1$ on $\mathfrak{H}(n) = n^2 - 3n + 3$.

Huomattavaa on, että vaikka Černýn konjektuuri ja hybridikonjektuuri ovat hyvin samantapaisia, niin kumpikaan ei välittömästi seuraa toisesta (vaikkakin triviaalisti $\mathfrak{H}(n) \leq \mathfrak{C}(n)$).

Esitetään lähteen [2] todistus sille, että konjektuuria ei voi tiukentaa.

Lause 6.3. Kun $n > 1$, niin $\mathfrak{H}(n) \geq n^2 - 3n + 3$.

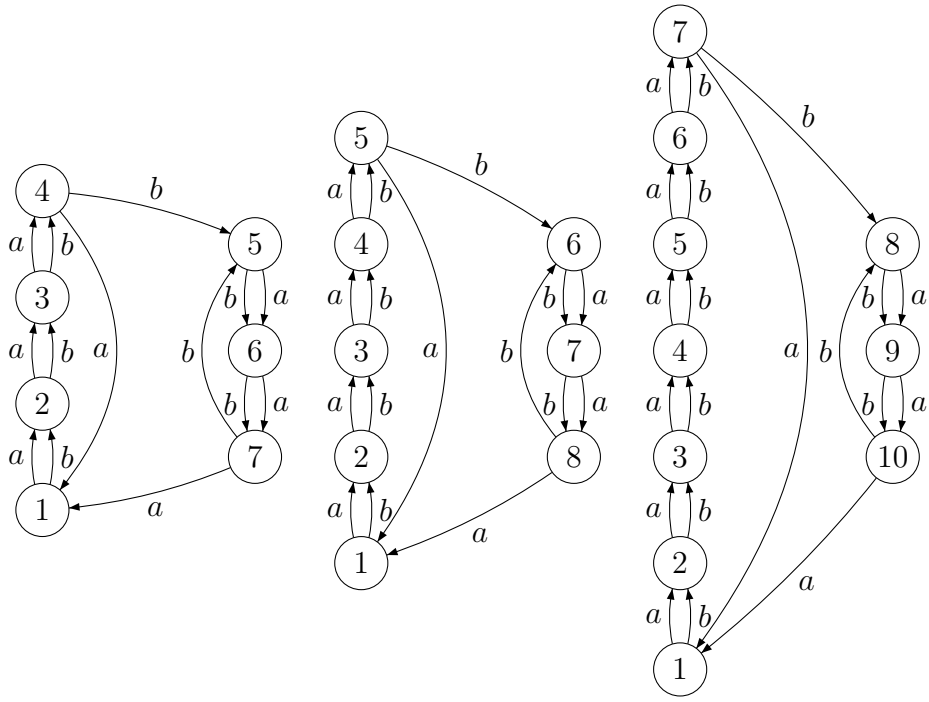
Todistus. Lauseen 4.4 mukaan kuvan 6 automaatin lyhin synkronisoiva sana on pituudeltaan $n^2 - 3n + 3$. Väite seuraa siitä, että selvästi kyseiseen automaattiin liittyvän graafin kaikki mahdolliset väritykset ovat olennaisesti samanlaiset. □

6.1 Eulerin graafit

Olkoon $\boldsymbol{O}_n$ niiden graafien $\Gamma \in \mathbf{\Pi}_{\boldsymbol{n}}$ joukko, missä jokaiseen solmuun tulee yhtä monta nuolta. Kutsutaan tällaisia graafeja jatkossa *Eulerin graafeiksi*. Selvästi Eulerin graafien kaikki väritykset ovat Eulerin automaatteja. Seuraava tulos seuraa suoraan lauseesta 4.20.

Lause 6.4. Kaikilla $n \in \mathbb{N}$ on $\mathfrak{H}(\boldsymbol{O}_n) \leq n^2 - 3n + 3$.

[2]Englanninkielisessä kirjallisuudessa ongelmasta on käytetty kuvaavaa, mutta epäkäytännöllisen pitkää nimitystä *Hybrid Černý-Road coloring problem*.



Kuva 12: Automaatit E_7, E_8 ja E_{10}.

Hybridikonjektuuri siis pätee Eulerin graafien osalta. Ei kuitenkaan tiedetä, kuinka paljon ylärajaa n^2-3n+3 voidaan parantaa. Yritetään seuraavaksi arvioida lukua $\mathfrak{H}(\boldsymbol{O}_n)$ alhaaltapäin.

Määritellään jokaisella luonnollisella luvulla $n \geq 3$ automaatti $E_n = (Q, \Sigma, *)$, missä $Q = \{1, 2, \ldots, n\}$, $\Sigma = \{a, b\}$ sekä

$$q * a = \begin{cases} 1 & \text{kun } q \in \{\frac{n+1}{2}, n\} \\ q+1 & \text{muulloin} \end{cases} \quad \text{ja} \quad q * b = \begin{cases} \frac{n+1}{2}+1 & \text{kun } q = n \\ q+1 & \text{muulloin} \end{cases}$$

jos n on pariton,

$$q * a = \begin{cases} 1 & \text{kun } q \in \{\frac{n+2}{2}, n\} \\ q+1 & \text{muulloin} \end{cases} \quad \text{ja} \quad q * b = \begin{cases} \frac{n+2}{2}+1 & \text{kun } q = n \\ q+1 & \text{muulloin} \end{cases}$$

jos n on neljällä jaollinen ja

$$q * a = \begin{cases} 1 & \text{kun } q \in \{\frac{n+4}{2}, n\} \\ q+1 & \text{muulloin} \end{cases} \quad \text{ja} \quad q * b = \begin{cases} \frac{n+4}{2}+1 & \text{kun } q = n \\ q+1 & \text{muulloin} \end{cases}$$

jos n on parillinen luku, joka ei ole neljällä jaollinen (ks. kuva 12).

Lemma 6.5. Kun $n \geq 3$ on pariton, niin $\mathfrak{C}(E_n) = \frac{(n-1)^2}{4} + 1$.

Todistus. Voidaan helposti todeta, että $b(a^{\frac{n-1}{2}-1}b)^{\frac{n-1}{2}}$ on synkronisoiva sana, jonka pituus on $\frac{(n-1)^2}{4}+1$. Vielä on osoitettava, että lyhyempiä synkronisoivia sanoja ei ole. Koska synkronisoiva sana pysyy synkronisoivana, jos sen loppuun lisätään kirjaimia, niin riittää osoittaa, että ei ole olemassa synkronisoivaa sanaa, jonka pituus on $\frac{(n-1)^2}{4}$. Tämä on helppo tarkistaa tapauksessa $n = 3$, joten voidaan rajoittua tapaukseen $n \geq 5$.

Tehdään vastaoletus, että wd on pituutta $\frac{(n-1)^2}{4}$ oleva synkronisoiva sana, missä $w \in \Sigma^*$ ja $d \in \Sigma$. Selvästi $Q * w = \{\frac{n+1}{2}, n\}$, joten wa ja wb ovat molemmat synkronisoivia sanoja. Kirjain d voidaan siis valita niin, että $wd = udvd$, missä $u, v \in \Sigma^*$ ja $|u| = \frac{n+1}{2} - 1$.

Oletetaan ensin, että $d = a$. Tällöin $1 = 1 * ud \in Q * ud$, ja koska $(Q * ud) * vd = Q * wd = \{\frac{n+1}{2}, n\} * d = 1$, niin $1 * vd = 1$. Automaatin E_n graafissa on siis pituutta $|vd| = \frac{n^2-4n-1}{4}$ oleva polku solmusta 1 siihen itseensä. Tämä polku koostuu pituutta $\frac{n+1}{2}$, $\frac{n-1}{2}$ ja $n = \frac{n+1}{2} + \frac{n-1}{2}$ olevista sykleistä, joten $\frac{n^2-4n-1}{4}$ voidaan kirjoittaa muodossa $k\frac{n+1}{2} + l\frac{n-1}{2}$, missä k ja l ovat epänegatiivisia kokonaislukuja. Tämä on kuitenkin mahdotonta Lemman 4.3 nojalla.

Oletetaan sitten, että $d = b$. Vastaavalla tavalla voidaan osoittaa, että automaatin E_n graafissa on pituutta $|vd|$ oleva polku solmusta $\frac{n+1}{2} + 1$ siihen itseensä, mikä on mahdotonta. □

Lemma 6.6. Olkoon $n \geq 4$ parillinen.

(a) Jos n on neljällä jaollinen, niin $\mathfrak{C}(E_n) = \left\lfloor \frac{(n-1)^2}{4} \right\rfloor + 1$.

(b) Jos n ei ole neljällä jaollinen, niin $\mathfrak{C}(E_n) = \left\lfloor \frac{(n-1)^2}{4} \right\rfloor - 1$.

Todistus. Voidaan helposti todeta, että kun n on neljällä jaollinen, niin $b(a^{\frac{n-2}{2}-1}b)^{\frac{n}{2}}$ on synkronisoiva sana, ja kun n ei ole neljällä jaollinen, niin $b(a^{\frac{n-4}{2}-1}b)^{\frac{n+2}{2}}$ on synkronisoiva sana. Se, että lyhyempiä synkronisoivia sanoja ei ole, voidaan todistaa kuten edellisessä lemmassa. □

Lause 6.7. Olkoon $n \geq 3$ luonnollinen luku. Jos n on parillinen mutta ei jaollinen neljällä, niin $\mathfrak{H}(\boldsymbol{O}_n) \geq \left\lfloor \frac{(n-1)^2}{4} \right\rfloor - 1$. Muussa tapauksessa $\mathfrak{H}(\boldsymbol{O}_n) \geq \left\lfloor \frac{(n-1)^2}{4} \right\rfloor + 1$.

Todistus. Automaatin E_n graafilla Γ on kaksi olennaisesti erilaista väritystä; toinen on E_n itse ja toinen, $G_n = (Q, \Sigma, \cdot)$, saadaan automaatista E_n vaihtamalla solmusta n lähtevät nuolet keskenään. Automaatti G_n ei ole synkronisoituva, sillä $Q \cdot a = Q$ ja $Q \cdot b = Q$. Lauseen väite seuraa nyt kahdesta edellisestä lemmasta. □

6.2 Hamiltonin polut

Esitetään tässä osiossa hybridikonjektuuriin liittyvä tulos artikkelista [3] primitiivisille graafeille Γ, joissa on ns. *Hamiltonin polku*. Tässä tapauksessa artikkelin tulos antaa luvulle $\mathfrak{H}(\Gamma)$ neliöllisen ylärajan, joskin kysymys siitä, onko $\mathfrak{H}(\Gamma) \leq n^2 - 3n + 3$, jää avoimeksi.

Määritelmä 6.8. Graafin polkua kutsutaan Hamiltonin poluksi, jos polku käy jokaisessa graafin solmussa tarkalleen kerran.

Päätuloksen todistamiseksi jatketaan aiemmin aloitettua L-yhtenäisten automaattien tarkastelua. Käytetään jatkossa määritelmän 4.22 merkintöjä ilman erillistä mainintaa. Käytetään lisäksi jatkossa merkintää M suurimman joukkoon R sisältyvän synkronisoituvan joukon koosta ja merkintää L_Ω joukon L pisimmän sanan pituudesta.

Lemma 6.9. Olkoon $q \in R$ mielivaltainen. On olemassa $K \subseteq R$ ja sellainen sana $v \in \{w_1 w_2 \mid w_1 \in \Sigma^*, w_2 \in L\} \cup \{\epsilon\} = \Sigma^* L \cup \{\epsilon\}$, että

$$|K| = M, \quad K * v = q \quad \text{ja} \quad |v| \leq (M-1)(n+1+L_\Omega) - t \ln M,$$

missä n on automaatin tilojen lukumäärä.

Todistus. Tapauksessa $M = 1$ voidaan valita $v = \epsilon$, joten oletetaan, että $M \geq 2$ ja merkitään $K_0 = \{q\}$. Määritellään joukkojen K_i ketju induktiivisesti: jos $|K_i| < M$, niin lemman 4.31 mukaan voidaan valita sanat $v_i \in \Sigma^*$ ja $w_{\gamma_i} \in L$, joilla

$$|K_i * (v_i w_{\gamma_i})^{-1} \cap R| > |K_i| \quad \text{ja} \quad |v_i| \leq n - \frac{|R \setminus K_i|}{|K_i|}.$$

Merkitään $K_{i+1} = K_i * (v_i w_{\gamma_i})^{-1} \cap R$ ja olkoon m indeksi, jolla $|K_m| = M$.

Valitsemalla $K = K_m$ ja $v = v_{m-1} w_{\gamma_{m-1}} \dots v_0 w_{\gamma_0} \in \Sigma^* L$ saadaan $|K| = M$, $K * v = q$ ja

$$|v| \leq \sum_{i=0}^{m-1} \left(n - \frac{|R \setminus K_i|}{|K_i|} + L_\Omega \right) \leq \sum_{j=1}^{M-1} \left(n - \frac{t-j}{j} + L_\Omega \right)$$

$$= (M-1)(n+1+L_\Omega) - t \sum_{j=1}^{M-1} \frac{1}{j} \leq (M-1)(n+1+L_\Omega) - t \ln M.$$

□

Lemma 6.10. Jos K on joukon R maksimaalinen synkronisoituva osajoukko, niin ei ole stabiilia paria $(p, q) \in K \times (R \setminus K)$.

Todistus. Tehdään vastaoletus, että stabiili pari $(p, q) \in K \times (R \setminus K)$ on olemassa ja olkoon w joukon K synkronisoiva sana. Koska (p, q) on stabiili pari, niin on olemassa sana u, jolla $p * wu = q * wu$. Nyt $|(K \cup \{q\}) * wu| = |K * wu \cup q * wu| = |p * wu \cup q * wu| = 1$, mikä on ristiriidassa joukon K maksimaalisuuden kanssa. □

Lemma 6.11. Jos epätyhjän tilajoukon $C \subseteq Q$ alkiot ovat parittain stabiileja, niin on olemassa sana u, jolla $|C * u| = 1$ ja $|u| \leq (M-1)(n+1+L_\Omega) - t \ln M + L_\Omega$.

Todistus. Olkoon $K \subseteq M$ ja $v \in \Sigma^*$ kuten lemmassa 6.9. Koska C on epätyhjä, niin on olemassa sana $w \in L$, jolla $C * w \cap K \neq \emptyset$. Koska joukon C alkiot ovat parittain stabiileja, niin täytyy olla $C * w \subseteq K$ ja siis $C * wv \subseteq K * v = q$ jollakin $q \in Q$. Siis valinnalla $u = wv$ saadaan $|C * u| = 1$. □

Lemma 6.12. Olkoon $1 \leq h \leq \lceil t/M \rceil$. On olemassa h eri tilaa $q_1, \ldots, q_h \in R$ ja sana $u \in \Sigma^* L \cup \{\epsilon\}$, joilla $|q_i * u^{-1} \cap R| = M$ kun $1 \leq i \leq h$.

Todistus. Todistetaan väite induktiolla luvun h suhteen. Tapauksessa $h = 1$ väite seuraa lemmasta 6.9.

Oletetaan seuraavaksi, että $h > 1$ ja että on olemassa tilat $q_1, \ldots, q_{h-1} \in R$ ja sana $u' \in \Sigma^* L \cup \{\epsilon\}$, joilla $|q_i * u'^{-1} \cap R| = M$ kun $1 \leq i \leq h-1$. Koska $h \leq \lceil t/M \rceil$, niin $(h-1)M < t$ ja joukko $R \setminus (\bigcup_{i=1}^{h-1} q_i * u'^{-1})$ on epätyhjä. Valitaan tästä joukosta jokin alkio q. Lemman 6.9 nojalla on olemassa kokoa M oleva joukko $K \subseteq R$ ja sana $v \in \Sigma^* L \cup \{\epsilon\}$, joilla $K * v = q$. Määritellään nyt $q_h = q * u' \in R$ ja $u = vu'$. Koska $q_h * u'^{-1} \supseteq \{q\}$ ja $q * v^{-1} \supseteq K$, niin $q_h * u^{-1} \cap R \supseteq K$ ja joukon K maksimaalisuuden takia tämä sisältyminen on itse asiassa yhtäsuuruus. Jos taas $1 \leq i \leq h-1$, niin $|q_i * u'^{-1} \cap R| = M$ ja lemman 4.26 nojalla $|(q_i * u'^{-1} \cap R) * v^{-1} \cap R| = M$. Tästä seuraa, että $|q_i * u^{-1} \cap R| = M$. □

Lemma 6.13. $\min\{|Q * w| \mid w \in \Sigma^*\} = t/M$.

Todistus. Sovelletaan edellistä lemmaa tapauksessa $h = \lceil t/M \rceil$ ja olkoon q_i $(1 \leq i \leq h)$ ja u kuten lemmassa. Joukot $q_i * u^{-1} \cap R$ ovat joukon R alkiovieraita osajoukkoja, joissa kussakin on M alkiota. Koska $h \geq t/M$, niin $hM \geq t$ ja joukot $q_i * u^{-1} \cap R$ muodostavat joukon R partition. Tästä seuraa, että $h = t/M$.

Jos $w \in L$ on mielivaltainen, niin $Q * wu \subseteq \{q_i \mid 1 \leq i \leq h\}$, eli $h \geq \min\{|Q * w| \mid w \in \Sigma^*\}$. Osoitetaan nyt, että $h = \min\{|Q * w| \mid w \in \Sigma^*\}$ tekemällä vastaoletus, että $|Q * u'| < h$ jollakin sanalla u'. Tällöin on olemassa indeksit i ja j, joilla $q_i * u' = q_j * u'$. Tästä seuraa, että $(q_i * u^{-1} \cup q_j * u^{-1}) \cap R$ on kertalukua $2M$ oleva synkronisoituva joukko, jonka synkronisoi sana uu', mikä on ristiriidassa luvun M valinnan kanssa. □

Lemma 6.14. Olkoon $A = (Q, \Sigma, *)$ n-tilainen 1-klusteriautomaatti, t sen jonkin pääsyklin tilojen lukumäärä ja $h = \min\{|Q * w| \mid w \in \Sigma^*\}$. Jos $C \subseteq Q$ on epätyhjä tilajoukko, jonka alkiot ovat parittain stabiileja, niin on olemassa sellainen sana v, että

$$|C * v| = 1 \quad \text{ja} \quad |v| \leq \frac{2nt}{h} - n - 1 - t \ln \frac{t}{h}.$$

Todistus. Lauseen 4.34 todistuksessa nähtiin, että automaatin A riippumattomaksi joukoksi voidaan valita $L = \{a^{n-1}, a^{n-2}, \ldots, a^{n-t}\}$. Edellisen lemman mukaan $M = t/h$, joten väite seuraa suoraan lemmasta 6.11. □

Lemma 6.15. Olkoon $A = (Q, \Sigma, *)$ n-tilainen 1-klusteriautomaatti, joka ei ole synkronisoituva. Jos $C \subseteq Q$ on epätyhjä tilajoukko, jonka alkiot ovat parittain stabiileja, niin on olemassa sellainen sana v, että

$$|C * v| = 1 \quad \text{ja} \quad |v| \leq n^2 - n - 1 - n \ln \frac{n}{2}.$$

Todistus. Väite seuraa edellisestä lemmasta, kun osoitetaan, että

$$\frac{2nt}{h} - t \ln \frac{t}{h} \leq n^2 - n \ln \frac{n}{2}$$

kun $n > 1$ ja $h > 1$. Tämä on ekvivalentti epäyhtälön

$$n \ln \frac{n}{2} - t \ln \frac{t}{h} \leq n^2 - \frac{2nt}{h}$$

kanssa. Aloitetaan soveltamalla epäyhtälöä $\ln x \leq x - 1$:

$$\begin{aligned} n \ln \frac{n}{2} - t \ln \frac{t}{h} &= (n-t) \ln \frac{n}{2} + t \ln \frac{n}{t} + t \ln \frac{h}{2} \\ &\leq (n-t) \left(\frac{n}{2} - 1 \right) + t \left(\frac{n}{t} - 1 \right) + t \left(\frac{h}{2} - 1 \right). \end{aligned}$$

Todistettavaksi jää epäyhtälö

$$(n-t) \left(\frac{n}{2} - 1 \right) + t \left(\frac{n}{t} - 1 \right) + t \left(\frac{h}{2} - 1 \right) \leq n^2 - \frac{2nt}{h} :$$

tämä on ekvivalentti epäyhtälön

$$\frac{2nt}{h} + \frac{th}{2} \leq t + \frac{nt}{2} + \frac{n^2}{2}$$

kanssa. Epäyhtälö on voimassa tapauksessa $h \geq 4$, sillä tällöin $2nt/h \leq nt/2$ ja $th/2 \leq n^2/2$. Tapauksessa $h = 2$ epäyhtälö redusoituu muotoon

$$nt \leq \frac{nt}{2} + \frac{n^2}{2},$$

joka on voimassa, sillä $t \leq n$. Tapauksessa $h = 3$ saadaan

$$\frac{nt}{6} + \frac{t}{2} \leq \frac{n^2}{2}.$$

Tämä on voimassa, sillä

$$\frac{nt}{6} + \frac{t}{2} \leq \frac{n^2}{6} + \frac{n}{2} \leq \frac{n^2}{4} + \frac{2n}{4} \leq \frac{n^2}{4} + \frac{n^2}{4} = \frac{n^2}{2}.$$

□

Lemma 6.16. Olkoon Γ vähintään kaksi solmua sisältävä primitiivinen graafi, jossa on Hamiltonin polku. Graafilla Γ on väritys $A = (Q, \Sigma, *)$, jossa on epätriviaali stabiili tilapari ja jossa kaikki Hamiltonin polun nuolet on merkitty samalla kirjaimella $a \in \Sigma$.

Todistus. Oletetaan, että Hamiltonin polku käy solmut läpi järjestyksessä $q_1, q_2, \ldots, q_n$ ja annetaan solmusta q_i solmuun q_{i+1} menevälle nuolelle nimi e_i, kun $1 \leq i \leq n-1$. Jos solmusta q_n menee nuoli e_n solmuun $q \neq q_1$, niin nuolet $e_1, \ldots, e_n$ muodostavat graafin Γ virittävän graafin Δ, jossa maksimaalista syvyyttä olevat solmut ovat samassa puussa. Tällöin väite seuraa lemmasta 5.14.

Jos puolestaan solmusta q_n menee nuoli e_n solmuun q_1, niin nuolet $e_1, \ldots, e_n$ muodostavat syklin, jonka pituus on n. Koska Γ on primitiivinen graafi, niin on solmu, josta lähtevät nuolet eivät muodosta kimppua. Rajoituksetta voidaan olettaa, että q_n on tällainen solmu, joten voidaan valita nuoli e'_n, joka lähtee solmusta q_n solmuun $q \neq q_1$. Tällöin nuolet $e_1, \ldots, e_n$ muodostavat graafin Γ virittävän graafin Δ, jossa maksimaalista syvyyttä olevat solmut ovat samassa puussa. Väite seuraa taas lemmasta 5.14. □

Lemma 6.17. Olkoon $A = (Q, \Sigma, *)$ automaatti, jossa on Hamiltonin polku, jonka kaikki nuolet on merkitty samalla kirjaimella $a \in \Sigma$. Kaikilla kongruensseilla $\sim$ myös automaatissa $A/\sim$ on kirjaimella a merkitty Hamiltonin polku.

Todistus. Kongruenssi $\sim$ on kongruenssi myös automaatissa $A' = (Q, \{a\}, *')$, missä $*'$ on kuvauksen $*$ rajoittuma joukolle $Q \times \{a\}$. Tässä automaatissa on myös kirjaimella a merkitty Hamiltonin polku. Automaateissa,

joiden aakkostossa on vain yksi kirjain, on Hamiltonin polku tarkalleen silloin kun niiden jostakin tilasta on polku kaikkiin muihin tiloihin. Tästä seuraa, että myös automaatissa $A'/\sim$ on Hamiltonin polku. Koska automaatti $A'/\sim$ saadaan poistamalla automaatista $A/\sim$ kaikki nuolet, joita ei ole merkitty kirjaimella a, niin automaatissa $A/\sim$ on kirjaimella a merkitty Hamiltonin polku. □

Lause 6.18. Jos Γ on primitiivinen graafi, jossa on Hamiltonin polku ja $n > 1$ solmua, niin

$$\mathfrak{H}(\Gamma) \leq f(n) = 2n^2 - 4n + 1 - 2(n-1)\ln\frac{n}{2}.$$

Todistus. Todistetaan väite induktiolla solmujen määrän n suhteen. Tapaus $n = 2$ on triviaali, joten oletetaan jatkossa, että $n > 2$. Olkoon $A = (Q, \Sigma, *)$ lemman 6.16 mukaisella värityksellä graafista Γ saatu automaatti. Se on erityisesti 1-klusteriautomaatti. Jos se on synkronisoituva, niin väite seuraa lauseesta 4.34, joten oletetaan jatkossa, että A ei ole synkronisoituva.

Tarkastellaan automaatin $A/\equiv\ = (Q/\equiv, \Sigma, \cdot)$ graafia Γ'. Automaatti A ei ole synkronisoituva mutta siinä on epätriviaali stabiili tilapari, joten $1 < |Q/\equiv| < n$; merkitään $|Q/\equiv| = m$. Lemman 5.6 mukaan Γ on primitiivinen graafi ja edellisen lemman mukaan siinä on Hamiltonin polku. Induktio-oletuksen mukaan graafilla Γ' on synkronisoiva väritys $B' = (Q/\equiv, \Sigma, \cdot')$, jonka lyhimmän synkronisoivan sanan w pituus on enintään $f(m)$. Lemman 5.6 todistuksessa esitetyllä tavalla saadaan graafille Γ uusi väritys $A' = (Q, \Sigma, *')$. Joukon $C = Q *' w$ alkiot kuuluvat samaan automaatin A stabiilisuusluokkaan, joten on olemassa sana u', jolla $|C * u'| = 1$. Lemman 5.6 todistuksesta nähdään, että on olemassa yhtä pitkä sana u, jolla $|Q *' wu| = 1$. Jaetaan todistuksen loppu kahteen tapaukseen luvun m koon perusteella.

Tapaus 1. Oletetaan, että $n < 2m$. Tällöin on olemassa sellainen joukko $[q] \in Q/\equiv$, että $|[q]| = 1$. Koska automaatti A on vahvasti yhtenäinen, niin voidaan valita enintään pituutta $m-1$ oleva sana u', jolla $C * u' \subseteq [q]$, eli $|C * u'| = 1$. Siis automaatilla A' on synkronisoiva sana wu, jonka pituus on enintään $f(m) + m - 1$. Differentiaalilaskennan väliarvolauseen nojalla voidaan valita $\xi \in [m, n]$ niin, että $f(n) - f(m) = (n-m)f'(\xi)$, joten $|wu| \leq f(n) - (n-m)f'(\xi) + m - 1$. Funktion $f(x)$ kasvunopeudelle tarvitaan arvio, jonka avulla voidaan todeta, että $|wu| \leq f(n)$.

Väitetään nyt, että $f'(x) \geq x$ kun $x > 0$. Ensiksikin $f'(x) = 4x - 6 - 2\ln(x/2) + 2/x$, joten väite on ekvivalentti epäyhtälön $3x - 6 - 2\ln(x/2) + 2/x \geq 0$ kanssa. Koska $\ln x \leq x - 1$ kun $x > 0$, niin väite seuraa epäyhtälöstä $g(x) = 2x + 2/x \geq 4$. Funktion $g'(x) = 2 - 2/x^2$ ainoa nollakohta joukossa $x > 0$ on $x = 1$, joten tässä pisteessä on funktion $g(x)$ ainoa ääriarvo.

Koska $g(1/2) = g(2) = 5$ ja $g(1) = 4$, niin ääriarvo on lokaali minimi ja $g(x) \geq g(1) = 4$, kun $x > 0$.

Koska $f'(\xi) \geq \xi \geq m$ ja $n - m \geq 1$, niin $|wu| \leq f(n) - m + m - 1 = f(n) - 1 < f(n)$.

Tapaus 2. Oletetaan, että $n \geq 2m$. Lemman 6.15 mukaan sana u' jolla $|C * u'| = 1$ voidaan valita niin, että $|u'| \leq n^2 - n - 1 - n\ln(n/2)$, jolloin $|wu| \leq f(m) + n^2 - n - 1 - n\ln(n/2)$. Koska $f(x)$ on kasvava kun $x > 0$ ja $m \leq n/2$, niin

$$\begin{aligned} f(n) - |wu| &\geq f(n) - f\left(\frac{n}{2}\right) - n^2 + n + 1 + n\ln\left(\frac{n}{2}\right) \\ &= \frac{n^2}{2} - n(1 + \ln 2) + 1 + \ln 4 = h(n). \end{aligned}$$

Funktion $h(x)$ kuvaaja on ylöspäin aukeava paraabeli ja se saa pienimmän arvonsa derivaatan $h'(x) = n - 1 - \ln 2$ nollakohdassa $1 + \ln 2 < 2$. Koska $n \geq 3$, niin $h(n) > h(2) = 1 > 0$ ja $|wu| < f(n)$. □

Lähteet

[1] R. L. Adler, L. W. Goodwyn, B. Weiss: Equivalence of topological Markov shifts. *Israel J. Math.* Vol. 27, 1977. s. 49-63.

[2] D. Ananichev, V. Gusev, M. Volkov: Slowly synchronizing automata and digraphs. Kirjassa Mathematical Foundations of Computer Science (toim. P. Hlineny, A. Kucera). *Lecture Notes in Computer Science*. Vol. 6281. Springer Berlin Heidelberg, 2010. s. 55-64.

[3] A. Carpi, F. D'Alessandro: Independent sets of words and the synchronization problem. *Advances in Applied Mathematics*. Vol. 50, 2013. s. 339-355.

[4] J. Černý: Poznámka k homogénnym eksperimentom s konečnými automatami. *Matematicko-fyzikálny Časopis*. Slovenská akadémia vied. Vol. 14 , 1964. s. 208-216.

[5] J. Černý, A. Pirická, B. Rosenauerová: On directable automata. *Kybernetika*. No. 4, 1971. s. 289-298.

[6] K. Culik II, J. Karhumäki, J. Kari: A note on synchronized automata and Road Coloring Problem. *Int. J. Found. Comp. Sci*. Vol. 13, 2002. s. 459-471.

[7] L. Dubuc: Sur les automates circulaires et la conjecture de Černý. *RAIRO Inform. Théor. App.* Vol. 32, 1998. s. 21-34.

[8] P. Frankl: An extremal problem for two families of sets. *European J. Combinatorics*. Vol. 3, 1982. s. 125-127.

[9] J. Friedman: On the road coloring problem. *Proceedings of the American Mathematical Society*. Vol. 110, 1990. s. 1133-1135.

[10] V. Gusev: Lower bounds for the length of reset words in Eulerian automata. Kirjassa Reachability Problems (toim. G. Delzanno, I. Potapov). *Lecture Notes in Computer Science*. Vol. 6945. Springer Berlin Heidelberg, 2011. s. 180-190.

[11] J. Kari: Synchronizing finite automata on Eulerian digraphs. *Theoretical Computer Science*. Vol. 295, 2003. s. 223-232.

[12] J. Kari, M. Volkov: Černý's conjecture and the road coloring problem. Julkaistaan kirjassa *Handbook of Automata*. European Science Foundation.

[13] A. A. Klyachko, I. K. Rystsov, M. A. Spivak. An extremal combinatorial problem associated with the bound of the length of a synchronizing word in an automaton. *Cybernetics and System Analysis*. Vol. 23, 1987. s. 165-171. Käännetty lehdestä *Kibernetika*. No. 2, 1987. s. 16-20, 25.

[14] P. Lancaster: *Theory of Matrices*. Academic Press, 1969.

[15] P. Norvig, S. Russell: *Artificial Intelligence: A Modern Approach (Third Edition)*. Prentice Hall, 2009.

[16] J.-É. Pin: On two combinatorial problems arising from automata theory. *Ann. Disc. Math.* Vol. 17, 1983. s. 535-548.

[17] J.-É. Pin: Sur un cas particulier de la conjecture de Černý. Kirjassa Proc. 5th Colloq. on Automata, Languages and Programming (toim. G. Ausiello, C. Böhm). *Lecture Notes in Computer Science*. Vol. 62. Springer Berlin Heidelberg, 1978. s. 345-352.

[18] A. Trahtman: Notable trends concerning the synchronization of graphs and automata. *Electronic Notes Discr. Math.* Vol. 25, 2006. s. 173-175.

[19] A. Trahtman: The Road Coloring Problem. *Israel J. Math.* Vol. 172, 2009. s. 51-60.

[20] M. Volkov: Synchronizing automata preserving a chain of partial orders. Kirjassa Implementation and Application of Automata (toim. J. Holub, J. Zdárek). *Lecture Notes in Computer Science*. Vol. 4783. Springer Berlin Heidelberg, 2007. s. 27-37.

[21] F. Zhang: *Matrix Theory: Basic Results and Techniques*. Springer New York, 2011.