Algebrallisia lähestymistapoja Golomb-Welch konjektuuriin

Pro gradu Mika Pohto

Pro gradu -tutkielma
Huhtikuu 2024

Tarkastajat:
Prof. Jarkko Kari
Prof. Tero Laihonen

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Mika Pohto: Algebrallisia lähestymistapoja Golomb-Welch konjektuuriin
Pro gradu -tutkielma, 39 s.
Matematiikka
Huhtikuu 2024

Tässä tutkielmassa perehdytään Golomb-Welch konjektuuriin algebrallisin keinoin käyttäen Laurentin polynomeja. Konjektuuri esitellään koodausteorian sanastolla, mutta sitä käsitellään laatoitusten ongelmana. Tutkielmassa esitellään vahvoja työkaluja, joilla saadaan pääteltyä laatoitusten ominaisuuksia laatoittavan kappaleen avulla. Työkalut ja lauseet pätevätkin kaiken muotoisiin diskreetteihin laattoihin, mutta esimerkit ja sovellukset esitellään Lee-palloilla.

Tutkielmassa kerrataan peruskäsitteitä muun muassa algebrasta ja laatoituksesta, jonka jälkeen syvennytään ihanteisiin ja Lee-koodeihin. Tämän jälkeen esitellään Golomb-Welch konjektuuri. Tutkielmassa olevat algebralliset lähestymistavat keskittyvät pääosin polynomiseen menetelmään sekä säikeillä tutkittavaan deterministisyyteen. Lopulta esitellään lyhyesti ylärajoja.

Asiasanat: Golomb-Welch konjektuuri, Lee-metriikka, Lee-koodit, algebra, Laurentin polynomi, polynominen menetelmä, säikeet.

Sisällys

1 Johdanto

Vuonna 1968 Golomb ja Welch esittivät konjektuurin täydellisien e-virheen korjaavien Lee-koodien olemattomuudesta. Monista julkaistuista tutkimuksista huolimatta konjektuuria ei ole vielä ratkaistu. Tässä tutkielmassa lähestytään konjektuuria algebrallisesti keskittyen pääasiassa polynomiseen lähestymistapaan ja säikeillä tehtävään lähestymistapaan.

Tutkielmassa kerrataan algebran, topologian ja laatoituksen peruskäsitteitä, sekä esitellään täydelliset e-virheen korjaavat Lee-koodit ja niiden käsittelyä laatoitusten avulla. Tämän jälkeen esitellään konjektuurin vahva ja heikko versio, jonka jälkeen perehdytään polynomiseen lähestymistapaan ja säikeisiin perustuvaan lähestymistapaan. Lopulta vielä esitellään lyhyesti konjektuurille saatuja ylärajoja.

Käsiteltyjä lähestymistapoja voidaan hyödyntää kaikille yhden laatan siirtolaatoituksille, mutta esimerkit ja lauseiden sovellukset on tehty Lee-palloilla.

Tutkielman pohjana ovat Golomb-Welch konjektuuria monesta eri suunnasta käsittelevä artikkeli [1], säikeisiin perustuva tutkimus [2] ja polynomista menetelmää käsittelevä artikkeli [6].

2 Laatoitus ja perusteet

Yleisesti laatoituksella tarkoitetaan tason täyttämistä jonkin muotoisilla laatoilla siten, että laatat eivät ole toistensa päällä eikä tasoon jää täyttämättömiä aukkoja [8]. Tämä voidaan yleistää korkeampiin ulottuvuuksiin. Tutkielmassa käsitellään kin n-ulotteisen Euklidisen avaruuden $\mathbb{R}^n$ täyttämistä n-ulotteisilla kappaleilla, joita kutsutaan *laatoiksi*. Laatoituksissa voidaan yleensä asettaa laatat erilaisiin asentoihin, mutta tässä tutkielmassa keskitytään *siirtolaatoituksiin* eli laatoituksiin joissa kappaleet ovat vain yhdessä tietyssä asennossa. Laatoituksissa voi myös olla useita erilaisia laattoja, mutta tässä tutkielmassa sallitaan vain yhdenlaisen laatan olemassaolo. Laatoituksiin perehdytään tarkemmin algebran keinoin kappaleessa 2.2. Seuraavaksi kerrataan vaadittavia käsitteitä.

2.1 Algebran peruskäsitteitä

Tässä kappaleessa kerrataan algebran peruskäsitteitä, joita tullaan käyttämään runsaasti tulevissa kappaleissa. Kappaleessa on käytetty lähteinä algebran luentomonisteita [10, 11].

Joukossa S määritellyllä *binäärioperaatiolla* $*$ tarkoitetaan jotain kuvausta $S \times S \to S$. Operaatiolle käytetään infiksi-merkintää: parin (a, b) kuva on $a * b$.

Määritelmä 1. Olkoon G epätyhjä joukko. Paria $(G, *)$, tai lyhyemmin G, sanotaan *ryhmäksi*, jos $*$ on joukossa G määritelty binäärioperaatio, joka täyttää seuraavat ehdot:

1. Kaikilla $a, b, c \in G$ pätee $a * (b * c) = (a * b) * c$ (*assiosiatiivilaki*),
2. on olemassa jokin sellainen alkio $e \in G$, että $a * e = e * a = a$ kaikilla $a \in G$ (*neutraalialkio*),

3. jokaista alkiota $a \in G$ kohti on olemassa sellainen alkio $a^{-1} \in G$, että $a * a^{-1} = a^{-1} * a = e$ (*käänteisalkio*).

Lisäksi pari $(G, *)$ on *kommutatiivinen ryhmä*, eli *Abelin ryhmä*, jos se toteuttaa edellisten ehtojen lisäksi vielä ehdon:

4. Jokaisella $a, b \in G$ pätee $a * b = b * a$ (*kommutatiivilaki*).

Ryhmän G alkioiden lukumäärää kutsutaan ryhmän G *kertaluvuksi*. Olkoon G ryhmä ja H sen osajoukko, joka on myös ryhmä ryhmän G binäärioperaation restriktion $H \times H \to H$ suhteen. Tällöin ryhmää H kutsutaan ryhmän G *aliryhmäksi*.

Olkoon R jokin ryhmä. Joukko S on ryhmän R *generoiva joukko*, jos ryhmän R jokainen alkio voidaan esittää joukon S äärellisen monen alkion ja käänteisalkion kombinaationa.

Määritelmä 2. Kolmikkoa $(R, +, \cdot)$ kutsutaan *renkaaksi*, jos $+$ ja $\cdot$ ovat joukossa R määriteltyjä binäärioperaatioita ja jos seuraavat ehdot ovat voimassa:

1. $(R, +)$ on Abelin ryhmä (*renkaan additiivinen ryhmä*),
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (*kertolaskun assosiatiivilaki*),
3. on olemassa sellainen alkio $1 \in R$, että kaikilla $a \in R$ pätee $1 \cdot a = a \cdot 1 = a$ (*renkaan ykkösalkio*),
4. kaikilla $a, b, c \in R$ pätee $a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + b \cdot c$ (*distributiivilait*).

Lisäksi kolmikko $(R, +, \cdot)$ on *kommutatiivinen rengas*, jos se totetuttaa edellisten ehtojen lisäksi vielä ehdon:

5. kaikilla $a, b \in R$ pätee $a \cdot b = b \cdot a$.

Operaatioita $+$ ja $\cdot$ kutsutaan yhteenlaskuksi ja kertolaskuksi.

Yhden alkion $(\{0\}, +, \cdot)$ rengasta kutsutaan *nollarenkaaksi*. Osajoukkoa $S \subseteq R$ sanotaan renkaan $(R, +, \cdot)$ *alirenkaaksi*, kun S on rengas renkaan R yhteen- ja kertolaskun restriktioiden suhteen ja sen ykkösalkio 1_S on sama kuin renkaan R ykkösalkio 1_R.

Määritelmä 3. Kolmikkoa $(F, +, \cdot)$ kutsutaan *kunnaksi*, jos

1. $(F, +, \cdot)$ on kommutatiivinen rengas, joka ei ole nollarengas
2. jokaisella joukon F nollasta eroavalla alkiolla on olemassa käänteisalkio kertolaskun suhteen joukossa F.

Kunnille käytetään myös merkintää $\mathbb{F}$. Eräitä kuntia ovat reaaliluvut $\mathbb{R}$ ja kompleksiluvut $\mathbb{C}$ lukujen tavallisten yhteen- ja kertolaskujen suhteen.

Olkoon $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ muuttujien vektori ja $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}^n$. Merkitään $\boldsymbol{x}^{\boldsymbol{y}} = x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$. Kun $\boldsymbol{y} = (y, y, \ldots, y)$ merkitään myös lyhyesti $\boldsymbol{x}^y = x_1^y x_2^y \cdots x_n^y$. Määritellään seuraavaksi *Laurentin polynomit* [12] ja *formaalit potenssisarjat*:

Määritelmä 4. Olkoon $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ muuttujien vektori ja R jokin kommutatiivinen rengas. Kutsutaan summaa

$$p = \sum_{\boldsymbol{k} \in \mathbb{Z}^n} p_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}, p_{\boldsymbol{k}} \in R$$

Laurentin polynomiksi, kun vain äärellisen monta kerrointa $p_{\boldsymbol{k}}$ on nollasta eroavia. Kaikkien Laurentin polynomien kokoelmaa yli renkaan R merkitään merkinnällä $R[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] = R[\boldsymbol{x}^{\pm 1}]$.

Kun summassa äärettömän monen kertoimen $p_{\boldsymbol{k}}$ sallitaan eroavan nollasta, niin summaa kutsutaan *muodolliseksi potenssisarjaksi*. Niiden joukosta käytetään merkintää $R[[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]] = R[[\boldsymbol{x}^{\pm 1}]]$.

Laurentin polynomit $R[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ muodostavat renkaan, jossa yhteen- ja kertolasku on kuten tavallisilla polynomeilla, mutta niissä voi olla negatiivisia eksponentteja mukana:

$$\left(\sum_{\boldsymbol{k}} a_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \right) + \left(\sum_{\boldsymbol{k}} b_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \right) = \sum_{\boldsymbol{k}} (a_{\boldsymbol{k}} + b_{\boldsymbol{k}}) \boldsymbol{x}^{\boldsymbol{k}}$$

ja

$$\left(\sum_{\boldsymbol{k}} a_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \right) \cdot \left(\sum_{\boldsymbol{k}} b_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \right) = \sum_{\boldsymbol{k}} \left(\sum_{\substack{\boldsymbol{i},\boldsymbol{j} \\ \boldsymbol{i}+\boldsymbol{j}=\boldsymbol{k}}} a_{\boldsymbol{i}} b_{\boldsymbol{j}} \right) \boldsymbol{x}^{\boldsymbol{k}}.$$

Tässä tutkielmassa Laurentin polynomeja käsitellään vain yli kunnan $\mathbb{C}$, ellei toisin mainita. Laurentin polynomeille, joiden kertoimet kuuluvat kokonaislukujen $\mathbb{Z}$ joukkoon tullaan käyttämään merkintää $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] = \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$.

Määritellään seuraavaksi renkaan ihanne. Ihanteita käsitellään lisää kappaleessa 2.4.

Määritelmä 5. Renkaan $(R, +, \cdot)$ osajoukkoa I kutsutaan *ihanteeksi*, jos

1. joukko I on ryhmän $(R, +)$ aliryhmä,
2. $ra \in I$ kaikilla $r \in R$ ja $a \in I$,
3. $ar \in I$ kaikilla $r \in R$ ja $a \in I$.

Mikäli vain toinen ehdoista 2 tai 3 täyttyy ensimmäisen lisäksi, niin osajoukkoa I kutsutaan vastaavasti *oikeanpuoleiseksi* ja *vasemmanpuoleiseksi ihanteeksi*.

Määritelmä 6. Olkoon H ryhmän G aliryhmä ja a jokin ryhmän G alkio. Osajoukkoa

$$aH = \{ah \,|\, h \in H\}$$

kutsutaan aliryhmän H *vasemmaksi sivuluokaksi* ryhmässä G ja osajoukkoa

$$Ha = \{ha \,|\, h \in H\}$$

kutsutaan *oikeaksi sivuluokaksi* ryhmässä G. Mikäli vasemmat ja oikeat sivuluokat ovat samoja joukkoja, toisin sanoen jos

$$aH = Ha$$

kaikilla $a \in G$, niin aliryhmää H kutsutaan *normaaliksi*.

Huomautus 7. Edellisessä määritelmässä ryhmää G merkittiin multiplikatiivisesti. Additiivista merkintää käyttäessä sivuluokat kirjoitetaan $a + H$ ja $H + a$.

Tässä tutkielmassa käsiteltävät ryhmät ovat pääosin Abelin ryhmiä, jolloin vasemmat ja oikeat sivuluokat ovat samoja ja täten aliryhmät normaaleja aliryhmiä. Tällöin määreet "vasen" tai "oikea" jätetään sivuluokista pois.

Jos sivuluokkien joukko $\{aH \mid a \in G\}$ on ryhmä, niin sitä kutsutaan *tekijäryhmäksi* G/H. Kun aliryhmä on normaali, niin sen sivuluokkien joukko on ryhmä. Esitellään tämä lauseena ilman todistusta.

Lause 8. *Olkoon N ryhmän G normaali aliryhmä. Tällöin joukko G/N on ryhmä seuraavan binäärioperaation suhteen:*

$$aN \cdot bN = abN$$

kaikilla $a, b \in G$.

Määritelmä 9. Olkoot $(G, \cdot)$ ja $(G', *)$ ryhmiä. Kuvausta $f : G \to G'$ kutsutaan *(ryhmä)homomorfismiksi*, jos

$$f(a \cdot b) = f(a) * f(b)$$

kaikilla $a, b \in G$.

Kun N on jonkin ryhmän G normaali aliryhmä, niin homomorfismia $\pi : G \to G/N$, missä $\pi(a) = aN$ kaikilla $a \in G$, kutsutaan *luonnolliseksi homomorfismiksi*.

2.2 Laatoitus ja translaatio

Kappaleen lähteinä käytetään [2, 8].

Tutkielmassa käytetään Laurentin polynomeja ja formaaleja potenssisarjoja solujen identifioimiseen. Soluilla tarkoitetaan jotakin n-ulotteisten kokonaislukujen joukon $\mathbb{Z}^n$ pistettä, joka voi saada arvon joukosta $\mathbb{C}$. Olkoon $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ jokin piste. Pisteet identifioidaan algebrallisesti Laurentin polynomeilla monomina $\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} \cdots x_n^{u_n} \in \mathbb{C}[\boldsymbol{x}^{\pm 1}]$, missä muuttujaan $\boldsymbol{x}$ ei aseteta arvoja. Samoin äärellinen joukko pisteitä $D \subset \mathbb{Z}^n$ voidaan esittää Laurentin polynomina $\sum_{\boldsymbol{u} \in D} \boldsymbol{x}^{\boldsymbol{u}} = \boldsymbol{x}^{\boldsymbol{u}_1} + \cdots + \boldsymbol{x}^{\boldsymbol{u}_{|D|}} \in \mathbb{C}[\boldsymbol{x}^{\pm 1}]$. Mikäli joukko D on äärettömän suuri, niin joukko esitetään formaalina potenssisarjana. Monomia, jonka kerroin on 1, kutsutaan *yksikkömonomiksi*.

Laurentin polynomien ja formaalien potenssisarjojen termien kertoimet kertovat solussa olevan arvon. Merkitään alaindeksillä $f_{\boldsymbol{u}}$ Laurentin polynomin tai formaalin potenssisarjan f termin $\boldsymbol{x}^{\boldsymbol{u}}$ kerrointa. Tästä eteenpäin kutsutaan Laurentin polynomeja ja formaaleja potenssisarjoja molempia vain potenssisarjoiksi, sillä Laurentin polynomit ovat myös formaaleja potenssisarjoja.

Olkoon $D \subset \mathbb{Z}^n$ jokin äärellinen joukko. Joukkoa D kutsutaan termillä *laatta*. Laatan D karakteristista funktiota

$$f_D(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in D} \boldsymbol{x}^{\boldsymbol{u}}$$

kutsutaan termillä *algebrallinen laatta*. Kuvausta $c : \mathbb{Z}^n \to A$ kutsutaan n-ulotteiseksi konfiguraatioksi yli äärellisen aakkoston $A \subset \mathbb{Z}$. Kuvauksen c arvoa kohdassa $\boldsymbol{u} \in \mathbb{Z}^n$ merkitään merkinnällä $c_{\boldsymbol{u}}$. Konfiguraation c *algebrallinen konfiguraatio* on potenssisarja

$$f_c(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{Z}^n} c_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}.$$

Konfiguraation c sanotaan *laatoittavan* avaruuden $\mathbb{Z}^n$ laatoilla D, kun $c \in \{0,1\}^{\mathbb{Z}^n}$ ja $f_c(\boldsymbol{x}) f_D(\boldsymbol{x}) = 1(\boldsymbol{x})$, missä

$$1(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in \mathbb{Z}^n} \boldsymbol{x}^{\boldsymbol{u}}$$

on ykköskonfiguraatio. Merkitään joukolla $T_D \subseteq \{0,1\}^{\mathbb{Z}^n}$ niitä konfiguraatioita, jotka laatoittavat avaruuden $\mathbb{Z}^n$ laatoilla D.

Edellä joukosta D saatiin muodostettua Laurentin polynomi f_D. Sama voidaan tehdä päinvastoin ja saada Laurentin polynomista f_D joukko $\mathrm{Supp}(f)$, joka on identtinen joukon D kanssa. Olkoon joukko

$$\mathrm{Supp}(f) = \{\boldsymbol{u} \in \mathbb{Z}^n \mid f_{\boldsymbol{u}} \neq 0\}$$

Laurentin polynomin f *tuki* (eng. support), joka sisältää kaikki pisteet, joissa potenssisarjan f termien kertoimien arvo ei ole nolla. Kuitenkaan $f_{\mathrm{Supp}(f)}$ ei aina ole identtinen potenssisarjan f kanssa. Näin käy mikäli potenssisarjan f jonkin nollasta eroavan termin kerroin ei ole 1. Edellisistä määritelmistä voi jättää määreen *algebrallinen* pois, kun sekaannusta ei ole.

Määritellään seuraavaksi periodisuus:

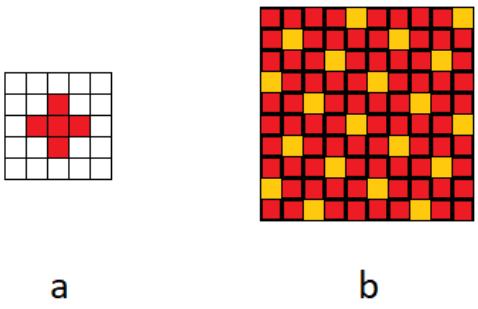
Määritelmä 10. Olkoon $\tau_{\boldsymbol{v}}(X) = \{\boldsymbol{x} + \boldsymbol{v} \mid \boldsymbol{x} \in X\}$ joukon $X \subseteq \mathbb{Z}^n$ *translaatio* suuntaan $\boldsymbol{v} \in \mathbb{Z}^n$, ja $\{\boldsymbol{e}_i \mid i \in \{1, \ldots, n\}\}$ avaruuden $\mathbb{Z}^n$ luonnollinen kanta. Translaatio on määritelty vastaavasti myös muille kuin joukoille, esimerkiksi funktioille $\mathbb{Z}^n \to A$.

- Joukko X on *periodinen*, kun $\tau_{\boldsymbol{v}}(X) = X$ jollain $\boldsymbol{v} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$. Vektoria $\boldsymbol{v}$ kutsutaan joukon *periodiksi*.

- Joukko X on *vahvasti periodinen*, kun $\tau_{\boldsymbol{v}_i}(X) = X$ kaikilla $i \in \{1, \ldots, n\}$ ja vektorit $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$ ovat lineaarisesti riippumattomia. Vahvasti periodisella joukolla X on olemassa jokin $q > 0$ siten, että $\tau_{\boldsymbol{e}_i \cdot q}(X) = X$ kaikilla $i \in \{1, \ldots, n\}$. Kun arvoa q halutaan painottaa, niin joukkoa X kutsutaan *vahvasti q-periodiseksi*.

- Joukko X on *ristikollinen* (eng. lattice), jos se on Abelin ryhmän $\mathbb{Z}^n$ aliryhmä.

- Joukkojen kokoelma Y on *translaatioinvariantti*, jos $\tau_{\boldsymbol{v}}(X) \in Y$ kaikilla $\boldsymbol{v} \in \mathbb{Z}^n$ ja $X \in Y$. Toisin sanoen $\tau_{\boldsymbol{v}}(Y) = Y$ kaikilla $\boldsymbol{v} \in \mathbb{Z}^n$.



Kuva 1: a) 2-ulotteinen Lee pallo säteellä 1, esimerkin 11 laatta D. b) Laatoitus esimerkin 11 laatalla D. Konfiguraatio saa arvon 1 keltaisella värjätyissä kohdissa.

Esimerkki 11. Olkoon $D = \{(-1,0),(0,-1),(0,0),(0,1),(1,0)\} \subset \mathbb{Z}^2$ laatta, ja olkoon kuvaus $c : \mathbb{Z}^2 \to \{0,1\}$ sellainen konfiguraatio, että $\mathrm{Supp}(f_c) = \{(x,y) \in \mathbb{Z}^2 \,|\, x \in \mathbb{Z}, y = 2x + 5a, a \in \mathbb{Z}\}$ (katso kuva 1). Osoitetaan, että konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^2$ laatoilla D. Algebrallinen laatta ja konfiguraatio ovat $f_D(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in D} \boldsymbol{x}^{\boldsymbol{u}} = x_1^{-1} + x_1^1 + x_2^{-1} + x_2^1 + 1$ ja $f_c(\boldsymbol{x}) = \sum_{x,a \in \mathbb{Z}} x_1^x x_2^{2x+5a}$. Nyt kertomalla algebralliset funktiot f_D ja f_c keskenään saadaan

$$\begin{aligned}
&\sum_{x,a\in\mathbb{Z}} x_1^{x-1}x_2^{2x+5a} + \sum_{x,a\in\mathbb{Z}} x_1^{x+1}x_2^{2x+5a} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a-1} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a+1} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a} \\
&= \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a+2} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a-2} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a-1} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a+1} + \sum_{x,a\in\mathbb{Z}} x_1^{x}x_2^{2x+5a} \\
&= \sum_{x,y\in\mathbb{Z}} x_1^x x_2^y,
\end{aligned}$$

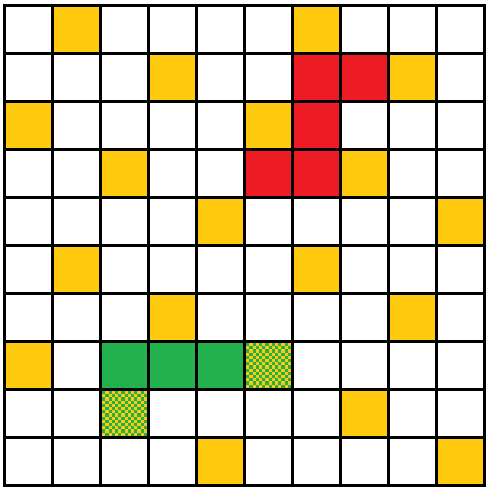
eli ykköskonfiguraatio.

Olkoon $\boldsymbol{v} = (v_1, v_2) \in \mathbb{Z}^2$ mielivaltainen vektori. Tällöin konfiguraatio $\tau_{\boldsymbol{v}}(c)$ saa arvon 1 kohdassa $\boldsymbol{t} \in \mathbb{Z}^2$ jos ja vain jos konfiguraatio c saa arvon 1 kohdassa $\boldsymbol{t} - \boldsymbol{v}$. Siis $\tau_{\boldsymbol{v}}(c)_{\boldsymbol{t}} = c_{\boldsymbol{t}-\boldsymbol{v}}$ kaikilla $\boldsymbol{v}, \boldsymbol{t} \in \mathbb{Z}^2$. Samoin algebrallisella konfiguraatiolla saadaan

$$\tau_{\boldsymbol{v}}(f_c) = \sum_{x,a\in\mathbb{Z}} x_1^{x+v_1}x_2^{2x+5a+v_2} = x_1^{v_1}x_2^{v_2} \sum_{x,a\in\mathbb{Z}} x_1^x x_2^{2x+5a}.$$

Nyt sijoittamalla vektoriin $\boldsymbol{v}$ arvot $(1,2)$ ja $(2,-1)$ vastaavasti saadaan $\tau_{(1,2)}(f_c) = f_c$ ja $\tau_{(2,-1)}(f_c) = f_c$. Täten konfiguraatio c on vahvasti periodinen, sillä $\tau_{(1,2)}(c) = c$ ja $\tau_{(2,-1)}(c) = c$, ja vektorit $(1,2)$ ja $(2,-1)$ ovat lineaarisesti riippumattomia. Se on myös ristikollinen, sillä kuvaus c saa vain arvoja 0 ja 1 sekä $\mathrm{Supp}(f_c)$ on Abelin ryhmän $\mathbb{Z}^2$ aliryhmä.

Seuraavaksi esitetään lause, jolla voidaan tarkistaa laatoittaako annettu laatta avaruuden annetulla konfiguraatiolla, eli päteekö $f_D(\boldsymbol{x})f_c(\boldsymbol{x}) = 1(\boldsymbol{x})$. Lause sanoo, että asetettaessa laatta $-D$ mihin hyvänsä avaruuden pisteeseen, niin se osuu tarkalleen vain yhteen konfiguraatiopisteeseen.



Kuva 2: Konfiguraatio on sama kuin kuvassa 1. Punaisella laatalla ei voi laatoittaa avaruutta kyseisellä konfiguraatiolla, sillä sen voi sijoittaa niin, ettei se osu yhteenkään konfiguraatipisteeseen. Vihreä laatta taas osuu kahteen pisteeseen, joten silläkään ei voi laatoittaa avaruutta kyseisellä konfiguraatiolla.

Lause 12. *Olkoon D laatta ja $c \in \{0,1\}^{\mathbb{Z}^n}$ konfiguraatio. Konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D jos ja vain jos $|(-D+\boldsymbol{x}) \cap Supp(f_c)| = 1$ kaikilla $\boldsymbol{x} \in \mathbb{Z}^n$.*

Todistus. Oletetaan ensin, että konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Olkoon $\boldsymbol{x} \in \mathbb{Z}^n$ jokin vektori. Tällöin vektorin voi esittää yksikäsitteisesti summana $\boldsymbol{x} = \boldsymbol{d} + \boldsymbol{e}$, missä $\boldsymbol{d} \in D$ ja $\boldsymbol{e} \in \mathrm{Supp}(f_c)$, sillä avaruus $\mathbb{Z}^n$ partitioituu laatan D muotoisiin osiin. Siis $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = |(-D+\boldsymbol{d}+\boldsymbol{e}) \cap \mathrm{Supp}(f_c)| \geq 1$, sillä $\boldsymbol{e} \in (-D+\boldsymbol{d}+\boldsymbol{e})$ ja $\boldsymbol{e} \in \mathrm{Supp}(f_c)$. Jos $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| \geq 2$, niin on olemassa toisista eroavat $\boldsymbol{e}_1 = \boldsymbol{x} + \boldsymbol{d}_1$ ja $\boldsymbol{e}_2 = \boldsymbol{x} + \boldsymbol{d}_2$, missä $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathrm{Supp}(f_c)$ ja $\boldsymbol{d}_1, \boldsymbol{d}_2 \in D$, josta seuraa $\boldsymbol{e}_1 + \boldsymbol{d}_2 = \boldsymbol{e}_2 + \boldsymbol{d}_1$. Tämä on ristiriita, sillä jokaisen vektorin esitys konfiguraation ja laatan alkion summana on yksikäsitteinen. Siis $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$.

Oletetaan seuraavaksi, että $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$ kaikilla $\boldsymbol{x} \in \mathbb{Z}^n$. Konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D, jos jokainen $\boldsymbol{x} \in \mathbb{Z}^n$ voidaan esittää yksikäsitteisesti muodossa $\boldsymbol{x} = \boldsymbol{d} + \boldsymbol{e}$, jossa $\boldsymbol{d} \in D$ ja $\boldsymbol{e} \in \mathrm{Supp}(f_c)$.

Olkoon $\boldsymbol{x} \in \mathbb{Z}^n$ mielivaltainen vektori. Nyt tarkalleen yhdellä $\boldsymbol{d} \in D$ pätee, että $-\boldsymbol{d} + \boldsymbol{x} = \boldsymbol{e}$, jossa $\boldsymbol{e} \in \mathrm{Supp}(f_c)$ on yksikäsitteinen, sillä $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$. Siis jokainen $\boldsymbol{x} \in \mathbb{Z}^n$ voidaan esittää yksikäsitteisesti muodossa $\boldsymbol{x} = \boldsymbol{d} + \boldsymbol{e}$, jossa $\boldsymbol{d} \in D$ ja $\boldsymbol{e} \in \mathrm{Supp}(f_c)$. □

Myöhemmin todistetaan, että konfiguraatio c laatoittaa avaruuden laatoilla D jos ja vain jos c laatoittaa avaruuden laatoilla $-D$. Tämän seurauksena saadaan suoraan, että edellisen lauseen ehdon $|(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$ voi korvata ehdolla $|(D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$. Usein on kuitenkin helpompi todistaa algebrallisesti, laatoittaako jokin konfiguraatio c avaruuden laatalla D.

2.3 Topologiaa ja siirtoaliavaruus

Tässä kappaleessa lähteinä käytetään töitä [2, 9]. Kerrataan seuraavaksi topologiaa, jonka jälkeen sovelletaan sitä laatoituksien teoriaan. Tässä kappaleessa kerrataan vain oleellisimmat määritelmät ja lauseet. Lisäksi käydään lyhyesti läpi laatoitusten teoriaa. Lisätietoja laatoitusten topologiasta saa esimerkiksi lähteestä [8].

Määritelmä 13. Olkoon X jokin joukko ja τ jokin kokoelma sen osajoukkoja. Kokoelma τ on avaruuden X *topologia* jos sille pätee seuraavat kolme ehtoa:

1. $\emptyset \in \tau$ ja $X \in \tau$,

2. kokoelman τ mielivaltaisen aliperheen unioni kuuluu kokoelmaan τ,

3. kokoelman τ äärellisen monen jäsenen leikkaus kuuluu kokoelmaan τ.

Kokoelman τ alkioita kutsutaan *avoimiksi joukouksi* ja niiden komplementteja suljetuiksi joukoiksi. Paria (X, τ), tai lyhyemmin X, sanotaan *topologiseksi avaruudeksi*.

Edellisestä määritelmästä saadaan suoraan samankaltaiset ehdot suljetuille joukoille De Morganin kaavoista.

Lause 14. *Suljetuille joukoille pätevät seuraavat kolme ominaisuutta:*

1. *$\emptyset$ on suljettu ja X on suljettu,*

2. *suljettujen joukkojen leikkaus on suljettu,*

3. *äärellisen monen suljetun joukon unioni on suljettu.*

Määritelmien perusteella joukko voi olla joko suljettu, avoin, suljettu ja avoin (eng. clopen) tai ei kumpikaan. Joukon A *sulkeuma* on leikkaus kaikista suljetuista joukoista, jotka sisältävät joukon A ja on täten pienin suljettu joukko, joka sisältää joukon A. Merkitään joukon A sulkeumaa merkinnällä $\overline{A}$.

Kokoelma $\mathcal{B}$ avoimia joukkoja on topologian *kanta* jos ja vain jos jokainen avoin joukko on kokoelman $\mathcal{B}$ jonkin osakokoelman joukkojen unioni. Jos kokoelma $\mathcal{B}$ on topologian kanta, niin tällöin tämä topologia on yksikäsitteisesti määritelty: kaikki avoimet joukot ovat perheen $\mathcal{B}$ alkioiden unioneja.

Määritellään seuraavaksi kompaktisuus. Olkoon X topologinen avaruus. Kokoelmaa avoimia joukkoja U_i kutsutaan joukon A *avoimeksi peitteeksi*, jos jokainen joukon A alkio kuuluu johonkin joukkoon U_i. Siis A on joukkojen U_i unionin osajoukko. Avoimen peitteen aliperhettä kutsutaan *avoimeksi osapeitteeksi*, jos se on myös joukon A avoin peite. Joukkoa $A \subseteq X$ kutsutaan *kompaktiksi*, jos sen jokaisella avoimella peitteellä on äärellinen avoin osapeite. Topologiaa kutsutaan kompaktiksi, jos koko avaruus X on kompakti.

Lause 15. *Jos X on kompakti topologinen avaruus, niin jokainen suljettu joukko $A \subseteq X$ on kompakti.*

Todistus. Olkoon joukko $A \subseteq X$ suljettu. Olkoon $\mathcal{S}$ sen jokin avoin peite. Koska A on suljettu, niin sen komplementti on avoin. Nyt joukon A komplementti yhdessä perheen $\mathcal{S}$ kanssa luovat koko avaruuden X avoimen peitteen. Joukko X on kompakti, joten on olemassa äärellinen avoin osapeite. Poistamalla tästä osapeitteestä joukon A komplementti saadaan suljetulle joukolle A äärellinen avoin osapeite. Siis A on kompakti. □

Jono $x_1, x_2, x_3, \ldots$ avaruuden X alkioita *suppenee* kohti alkiota $x \in X$, jos jokaista avointa joukkoa U kohti, joka sisältää alkion x, on olemassa jokin positiivinen kokonaisluku m siten että x_i kuuluu joukkoon U kaikilla $i \geq m$.

Määritellään seuraavaksi metriikka ja metrinen avaruus, ja sitten palloympäristö, jonka avulla saadaan määriteltyä metrisen avaruuden avoimet ja suljetut joukot.

Määritelmä 16. Olkoon X jokin joukko ja $d : X \times X \to \mathbb{R}$ kuvaus, joka täyttää seuraavat ehdot, kun $x, y, z \in X$:

1. $d(x, y) \geq 0$,
2. $d(x, y) = 0$ jos ja vain jos $x = y$,
3. $d(x, y) = d(y, x)$,
4. $d(x, z) \leq d(x, y) + d(y, z)$ (kolmioepäyhtälö).

Tällöin funktiota d sanotaan *metriikaksi* ja paria (X, d), tai lyhyemmin X, *metriseksi avaruudeksi*.

Määritelmä 17. Olkoon (X, d) metrinen avaruus, $a \in X$ ja $r > 0$. Sanotaan, että $B(a, r) = \{x \in X \mid d(a, x) < r\}$ on pisteen a *avoin r-palloympäristö* tai (a-keskinen) *avoin r-pallo*.

Metrisessä avaruudessa joukkoa $U \subseteq X$ kutsutaan *avoimeksi*, jos jokaista joukon U pistettä x kohti on olemassa jokin $r > 0$ siten, että $B(a, r) \subseteq U$. Nämä avoimet joukot muodostavat avaruuden X topologian. Topologinen avaruus (X, τ) on *metristyvä*, jos on olemassa sellainen metriikka d avaruudessa X, että τ on sama kuin metriikan d suhteen avoimien joukkojen kokoelma.

Lause 18. *Olkoon X metrinen avaruus. Joukko $A \subseteq X$ on kompakti jos ja vain jos jokaisella joukon A jonolla on osajono, joka suppenee jotain joukon A alkiota kohti.*

Määritellään seuraavaksi laatoitusavaruuksien topologiaa ja tärkeitä konsepteja. Aloitetaan ensin kaavoilla ja kaavakompleksisuudella. Käsitellään sen jälkeen joukon $A^{\mathbb{Z}^n}$ kompaktia topologiaa.

Olkoon $D \subset \mathbb{Z}^n$ jokin äärellinen osajoukko ja A jokin äärellinen aakkosto. Funktio $p \in A^D$ on *D-kaava* ja D on kaavan p *muoto*. Jos muotoa ei ole määritelty tai se on mielivaltainen, niin etuliitteen D voi jättää pois. Tällöin siis funktiota p kutsutaan *kaavaksi*. D-kaava p *esiintyy* konfiguraatiossa $c \in A^{\mathbb{Z}^n}$, jos $\tau_{\boldsymbol{v}}(c) \restriction_D = p$ jollain $\boldsymbol{v} \in \mathbb{Z}^n$. Voidaan myös sanoa, että konfiguraatio c sisältää D-kaavan p kohdassa $-\boldsymbol{v}$.

Kaikkien D-kaavojen joukkoa, jotka esiintyvät konfiguraatiossa c, merkitään $\mathcal{L}_D(c)$. Merkinnällä $\mathcal{L}(c)$ tarkoitetaan kaikkien kaavojen joukkoa, jotka esiintyvät konfiguraatiossa c. Siis $\mathcal{L}(c) = \bigcup_D \mathcal{L}_D(c)$.

Konfiguraation c *kaavakompleksisuus* muotoa D kohden on niiden D-kaavojen määrä, jotka esiintyvät konfiguraatiossa c. Se on siis luku $|\mathcal{L}_D(c)|$. Konfiguraatiolla c on *matala kompleksisuus* muotoa D kohti, kun $|\mathcal{L}_D(c)| \leq |D|$. Jos konfiguraatiolla c on matala kompleksisuus jotain muotoa kohti, niin konfiguraatiolla c sanotaan olevan *matala kompleksisuus*.

Kaikilla konfiguraatioilla, jotka laatoittavat avaruuden jollain laatalla, on matala kompleksisuus. Nimittäin olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatalla D. Nyt Lauseen 12 mukaan $-D$-kaavoja on tarkalleen $|-D|$ kappaletta. Siis $|\mathcal{L}_{-D}(c)| \leq |-D|$.

Olkoon $p \in A^D$ jokin D-kaava ja $[p] = \{c \in A^{\mathbb{Z}^n} \mid c \restriction_D = p\}$. Joukkoa $[p]$ kutsutaan termillä *p-sylinteri*. Sylinterien $[p]$ kokoelma on erään joukon $A^{\mathbb{Z}^n}$ kompaktin topologian kanta. Sylinterit ovat tässä topologiassa sekä avoimia että suljettuja. Topologia $A^{\mathbb{Z}^n}$ on myös metristyvä, joten sille voidaan käyttää metrisen avaruuden ominaisuuksia.

Osajoukkoa $X \subseteq A^{\mathbb{Z}^n}$ kutsutaan termillä *siirtoaliavaruus* (eng. subshift), kun se on topologisesti suljettu ja se on translaatio-invariantti. Usein siirtoaliavaruuden määritelmässä siirtoaliavaruus ei saa olla tyhjä, mutta tässä tutkielmassa se kuitenkin sallitaan.

Kompaktisuuden perusteella on olemassa joukko kaavoja, jotka estävät konfiguraatiota c kuulumasta siirtoaliavaruuteen X, jos jokin kaavoista esiintyy kyseisessä konfiguraatiossa. Täten siirtoaliavaruudet voidaan määritellä kiellettyjen kaavojen avulla. Olkoon P jokin joukko äärellisiä kaavoja. Tällöin

$$\mathcal{X}_P = \{c \in A^{\mathbb{Z}^n} \mid \mathcal{L}(c) \cap P = \emptyset\},$$

on joukko konfiguraatioita, jotka eivät sisällä mitään kaavoja joukosta P. Jos $X = \mathcal{X}_P$ jollain äärellisellä P, niin siirtoaliavaruus X on *äärellistä tyyppiä*, tai lyhyemmin SFT (eng. subshift of finite type).

Olkoon X siirtoaliavaruus. Määritellään sen kieli. Olkoon $\mathcal{L}(X)$ joukko kaikista kaavoista, jotka esiintyvät jossain siirtoaliavaruuden X konfiguraatiossa. Siis $\mathcal{L}(X) = \bigcup_{c \in X} \mathcal{L}(c)$. Samoin sen *D-kieli* on $\mathcal{L}(X) \cap A^D$ muodolla D.

Samoin kuin konfiguraatioilla niin myös siirtoaliavaruuksilla on matala kompleksisuus muotoa D kohti, jos $|\mathcal{L}_D(X)| \leq |D|$. Olkoon D jokin muoto ja olkoon joukon $P \subseteq A^D$ alkiot hyväksytyt kaavat, joita on enintään $|D|$ kappaletta. Tällöin $X = \mathcal{X}_{A^D \setminus P} = \{c \in A^{\mathbb{Z}^n} \mid \mathcal{L}_D(c) \subseteq P\}$ on matala kompleksinen SFT, sillä $\mathcal{L}_D(X) \subseteq P$ ja $|P| \leq |D|$. Täten konfiguraatioiden joukko T_D, jotka laatoittavat avaruuden $\mathbb{Z}^n$ laatoilla D, on matala kompleksinen SFT.

2.4 Annihilaattori- ja periodisoijaihanteet

Jatketaan Laurentin polynomien ominaisuuksista laatoituksessa. Kappaleen lähteinä ovat teokset [2, 4, 5].

Olkoon $c(\boldsymbol{x})$ jokin potenssisarja ja olkoon $\boldsymbol{x}^{\boldsymbol{t}}$ monomi, jossa $\boldsymbol{t} \in \mathbb{Z}^n$. Potenssisarjan $c(\boldsymbol{x})$ kertominen monomilla $\boldsymbol{x}^{\boldsymbol{t}}$ lisää potenssisarjan $c(\boldsymbol{x})$ jokaisen monomin eksponenttiin arvon $\boldsymbol{t}$. Potenssisarjan $c(\boldsymbol{x})$ translaation $\tau_{\boldsymbol{t}}(c)$ voikin nyt ilmoittaa sarjojen kertolaskuna: $\tau_{\boldsymbol{t}}(c) = \boldsymbol{x}^{\boldsymbol{t}} c(\boldsymbol{x})$. Täten $c(\boldsymbol{x})$ on periodinen jos ja vain jos $\boldsymbol{x}^{\boldsymbol{t}} c(\boldsymbol{x}) = c(\boldsymbol{x})$

eli $(\boldsymbol{x}^{\boldsymbol{t}} - 1)c(\boldsymbol{x}) = 0$. Kutsutaan binomia $(\boldsymbol{x}^{\boldsymbol{t}} - 1)$ termillä *differenssibinomi*, ja kutsutaan Laurentin polynomia $f(\boldsymbol{x})$ potenssisarjan $c(\boldsymbol{x})$ *annihilaattoriksi*, jos $fc = 0$. Laurentin polynomin $f(\boldsymbol{x})$ sanotaan myös *annihiloivan* konfiguraation c, kun $fc = 0$.

Olkoon joukko

$$\mathrm{Ann}(c) = \{f \in \mathbb{C}[\boldsymbol{x}^{\pm 1}] \mid fc = 0\}$$

potenssisarjan c *annihilaattori-ihanne*, joka sisältää kaikki ne polynomit, jotka annihiloivat potenssisarjan c. Kun X on siirtoaliavaruus, niin joukko $\mathrm{Ann}(X)$ sisältää ne Laurentin polynomit, jotka annihiloivat kaikki konfiguraatiot siirtoaliavaruudessa X.

Mikäli konfiguraatiolla c on kompleksikertoiminen annihilaattori f, niin tällöin sillä on myös kokonaislukukertoiminen annihilaattori f', jolla $\mathrm{Supp}(f') = \mathrm{Supp}(f)$. Nimittäin olkoon $f \in \mathrm{Ann}(c)$ jokin annihilaattori ja olkoon $f_i \in \mathbb{C}$, $i \in \{1, \ldots, m\}$ sen monomien kerroinosat, eli $f_1\boldsymbol{x}^{\boldsymbol{t}_1} + \cdots + f_m\boldsymbol{x}^{\boldsymbol{t}_m} = f$. Tällöin $(f_1\boldsymbol{x}^{\boldsymbol{t}_1} + \cdots + f_m\boldsymbol{x}^{\boldsymbol{t}_m}) \cdot c = f_1 \cdot \tau_{\boldsymbol{t}_1}(c) + \cdots + f_m \cdot \tau_{\boldsymbol{t}_m}(c) = 0$. Siis kaikissa pisteissä $\boldsymbol{t} \in \mathbb{Z}^n$ konfiguraatio saa arvon $f_1 \cdot \tau_{\boldsymbol{t}_1}(c)_{\boldsymbol{t}} + \cdots + f_m \cdot \tau_{\boldsymbol{t}_m}(c)_{\boldsymbol{t}} = 0$. Kun $\boldsymbol{t}$ käy läpi kaikki arvot ja kertoimet f_i korvataan muuttujilla h_i, saadaan homogeeninen lineaarinen yhtälöryhmä. Konfiguraatiolla c on vain äärellisen monta eri kerrointa, joten yhtälöryhmä on äärellinen. Saadaan siis yhtälöryhmä muuttujilla $h_1, h_2, \ldots, h_m$

$$\begin{cases} h_1 \cdot a_{11} + \cdots + h_m \cdot a_{1m} = 0 \\ \vdots \\ h_1 \cdot a_{k1} + \cdots + h_m \cdot a_{km} = 0, \end{cases}$$

jossa $a_{ij} \in A$ kaikilla i, j. Koska yhtälöt ovat lineaarisia, kertoimet a_{ij} ovat kokonaislukuja, ja yhtälöllä on nollasta eroava ratkaisu $(h_1, h_2, \ldots, h_m) = (f_1, f_2, \ldots, f_m)$, niin yhtälöryhmällä on olemassa myös jokin kokonaislukuratkaisu f', jolla $\mathrm{Supp}(f) = \mathrm{Supp}(f')$. Tämä johtuu siitä, että kompleksilukujen summassa reaaliosat eivät vaikuta imaginaariosien summaan ja päinvastoin sekä siitä, että yhtälöryhmän kertoimet ovat kokonaislukuja, jolloin kaikki ratkaisut voidaan esittää kokonaisluvuilla skalaareilla kerrottuina.

Määritellään seuraavaksi *periodisoijaihanne*

$$\mathrm{Per}(c) = \{f \in \mathbb{C}[\boldsymbol{x}^{\pm 1}] \mid fc \text{ on vahvasti periodinen}\},$$

joka sisältää vain ne Laurentin polynomit, joiden tulo konfiguraation c kanssa on vahvasti periodinen. Kun X on siirtoaliavaruus, niin $\mathrm{Per}(X)$ sisältää ne Laurentin polynomit, jotka periodisoivat kaikki konfiguraatiot siirtoaliavaruudessa X.

Potenssisarjan c annihilaattori- ja periodisoijaihanteet on helppo osoittaa renkaan $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ ihanteiksi. Nimittäin riittää osoittaa, että joukot ovat renkaan $\mathbb{C}[\boldsymbol{x}^{\pm 1}]$ additiivisia aliryhmiä, sekä se, että joukkojen ja renkaan alkioden tulot kuuluvat vastaaviin joukkoihin.

Koska nollakonfiguraatio on vahvasti periodinen, niin $\mathrm{Ann}(c) \subseteq \mathrm{Per}(c)$. Jos $f \in \mathrm{Per}(c)$, niin $\boldsymbol{x}^{\boldsymbol{t}} - 1$ annihiloi konfiguraation fc jollain sen periodilla $\boldsymbol{t}$, ja siten $f(\boldsymbol{x})(\boldsymbol{x}^{\boldsymbol{t}} - 1)$ annihiloi konfiguraation c. Täten jos $\mathrm{Per}(c)$ sisältää nollasta eroavan polynomin, niin $\mathrm{Ann}(c)$ sisältää nollasta eroavan polynomin.

Seuraavaksi esitellään kuuluisa Hilbertin Nullstellensatz-lause ilman todistusta. Sitä tullaan soveltamaan muissa lauseissa. Lause koskee tavallisia polynomeja ilman

negatiivisia muuttujien potensseja. Sille esitetään Laurentin polynomien vastine kappaleessa 4.1. Määritellään kuitenkin ensin kolme joukkoa:

Olkoon J jokin polynomirenkaan $\mathbb{C}[\boldsymbol{x}]$ ihanne, ja olkoon $S \subseteq \mathbb{C}^n$ jokin joukko. Joukkoa

$$\mathcal{I}(S) = \{f \in \mathbb{C}[\boldsymbol{x}] \mid f(\boldsymbol{x}) = 0 \text{ kaikilla } \boldsymbol{x} \in S\}$$

kutsutaan *joukon S ihanteeksi*. Se on siis joukko kaikista polynomeista renkaassa $\mathbb{C}[\boldsymbol{x}]$, jotka saavat arvon 0 kaikilla joukon S arvoilla. Joukkoa

$$\mathcal{V}(J) = \{\boldsymbol{x} \in \mathbb{C}^n \mid f(\boldsymbol{x}) = 0 \text{ kaikilla } f \in J\}$$

kutsutaan termillä *varisto*. Se on siis kompleksilukujen $\mathbb{C}^n$ osajoukko, johon kuuluvat vain ja ainoastaan kaikki ihanteen J Laurentin polynomien yhteiset nollakohdat. Joukkoa

$$\sqrt{J} = \{f \in \mathbb{C}[\boldsymbol{x}] \mid f^k \in J \text{ jollain } k \geq 1\}$$

kutsutaan ihanteen J *radikaaliksi*. Ihannetta J kutsutaan *radikaaliksi ihanteeksi*, jos $J = \sqrt{J}$.

Lause 19 (Nullstellensatz)**.** *Olkoon J jokin renkaan $\mathbb{C}[\boldsymbol{x}]$ ihanne. Tällöin*

$$\mathcal{I}(\mathcal{V}(J)) = \sqrt{J}.$$

Seuraavaksi todistetaan, että kaikilla konfiguraatioilla, jotka laatoittavat avaruuden $\mathbb{Z}^n$ jollain laatalla D, on olemassa epätriviaali Laurentin polynomi, joka annihiloi kyseisen konfiguraation.

Lemma 20. *Olkoon konfiguraatiolla c matala kompleksisuus. Tällöin $Ann(c)$ sisältää nollasta eroavan polynomin. Tarkemmin sanoen, jos konfiguraatiolla c on matala kompleksisuus muodon $D \subset \mathbb{Z}^n$ suhteen, niin on olemassa sellainen nollasta eroava Laurentin polynomi $f \in Per(c)$, että $-Supp(f) \subseteq D$.*

Todistus. Olkoon $D = \{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_k\}$. Muodostetaan joukko

$$\{(1, c_{\boldsymbol{d}_1+\boldsymbol{t}}, \ldots, c_{\boldsymbol{d}_k+\boldsymbol{t}}) \mid \boldsymbol{t} \in \mathbb{Z}^n\},$$

joka sisältää kompleksivektoreita, joiden dimensio on $k+1$. Koska konfiguraatiolla c on matala kompleksisuus muodon D suhteen, niin joukossa on enintään $|D| = k$ alkiota. Täten on olemassa vektori $(a_0, a_1, \ldots, a_k)$, joka on kohtisuorassa kaikkia joukon vektoreita kohtaan ja $a_i \neq 0$ jollain $1 \leq i \leq k$.

Olkoon $f(\boldsymbol{x}) = \overline{a_1}\boldsymbol{x}^{-\boldsymbol{d}_1} + \cdots + \overline{a_n}\boldsymbol{x}^{-\boldsymbol{d}_n} \neq 0$, missä merkinnällä $\overline{a}$ tarkoitetaan luvun $a \in \mathbb{C}$ kompleksikonjugaattia. Nyt Laurentin polynomin fc kerroin sijainnissa $\boldsymbol{t} \in \mathbb{Z}^n$ on

$$(fc)_{\boldsymbol{t}} = \overline{a_1}c_{\boldsymbol{d}_1+\boldsymbol{t}} + \cdots + \overline{a_k}c_{\boldsymbol{d}_k+\boldsymbol{t}} = -\overline{a_0},$$

sillä vektori $(a_0, a_1, \ldots, a_k)$ on kohtisuorassa vektoria $b = (1, c_{\boldsymbol{d}_1+\boldsymbol{t}}, \ldots, c_{\boldsymbol{d}_k+\boldsymbol{t}})$ kohtaan, jolloin niiden sisätulo $\sum_{i=0}^{k} \overline{a_i} \cdot b_i = 0$. Nyt millä vain nollasta eroavalla vektorilla $\boldsymbol{t} \in \mathbb{Z}^n$ saadaan $(\boldsymbol{x}^{\boldsymbol{t}} - 1)fc = 0$.

Siis $f \in \mathrm{Per}(c)$ on nollasta eroava ja $-\mathrm{Supp}(f) \subseteq D$, sekä $(\boldsymbol{x}^{\boldsymbol{t}} - 1)f \in \mathrm{Ann}(c)$, jolloin $\mathrm{Ann}(c)$ sisältää nollasta eroavan Laurentin polynomin.

□

Tämän kappaleen päälauseena (Lause 27) saadaan, että annihilaattori-ihanteeseen kuuluu Laurentin polynomi, joka on differenssibinomien tulo. Lauseen todistukseen tarvitaan kuitenkin paljon apulauseita: seuraavat kaksi lemmaa muodostavat annetusta annihilaattorista polynomin, joka saa arvon 0 kaikissa annihilaattori-ihanteen yhteisissä nollakohdissa. Myöhemmin Nullstellensatzin lauseella osoitetaan, että tämä polynomi kuuluu myös annihilaattori-ihanteeseen.

Lemma 21. *Olkoon c jokin konfiguraatio ja $f(\boldsymbol{x}) \in Ann(c)$ jokin epätriviaali kokonaislukukertoiminen Laurentin polynomi. Tällöin on olemassa sellainen kokonaisluku r, että jokaisella positiivisella luvulla h, joka on luvun r suhteen alkuluku, pätee $f(\boldsymbol{x}^h) \in Ann(c)$.*

Todistus. Olkoon $f_{\boldsymbol{u}} \in \mathbb{Z}$ polynomin $f(\boldsymbol{x})$ monomin kerroin kohdassa $\boldsymbol{u} \in \mathbb{Z}^n$, ja olkoon $m \in \mathbb{Z}$ jokin mielivaltainen kokonaisluku. Todistetaan ensin, että jos $f(\boldsymbol{x}^m)$ on annihilaattori, niin $f(\boldsymbol{x}^{pm})$ on annihilaattori jokaisella tarpeeksi suurella alkuluvulla p.

Olkoon p jokin alkuluku. Tällöin $f^p(\boldsymbol{x}) \equiv f(\boldsymbol{x}^p) \pmod p$ ja erityisesti $f^p(\boldsymbol{x}^m) \equiv f(\boldsymbol{x}^{pm}) \pmod p$. Koska polynomi $f(\boldsymbol{x}^m)$ annihiloi konfiguraation c, niin kertomalla molemmat puolet konfiguraatiolla $c(\boldsymbol{x})$ saadaan

$$0 \equiv f(\boldsymbol{x}^{pm})c(\boldsymbol{x}) \pmod p.$$

Potenssisarjan $f(\boldsymbol{x}^{pm})c(\boldsymbol{x})$ kertoimet ovat itseisarvoltaan enintään

$$s = c_{max} \sum |f_{\boldsymbol{u}}|,$$

missä c_{max} on itseisarvoltaan suurin kerroin konfiguraatiossa c. Täten jos $p > s$, niin saadaan $f(\boldsymbol{x}^{pm})c(\boldsymbol{x}) = 0$ ja täten $f(\boldsymbol{x}^{pm}) \in \mathrm{Ann}(c)$.

Olkoon seuraavaksi $r = s!$. Nyt kaikki positiiviset luvut h, jotka ovat luvun r suhteen alkulukuja, ovat muotoa $p_1 \cdots p_k$ missä jokainen p_i on alkuluku, joka on suurempi kuin s. Koska $f(\boldsymbol{x})$ on annihilaattori, niin induktiolla seuraa suoraan, että $f(\boldsymbol{x}^{p_1 \cdots p_k}) = f(\boldsymbol{x}^h)$ on annihilaattori. □

Lemma 22. *Olkoon c jokin konfiguraatio ja $f = \sum a_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}$ jokin epätriviaali kokonaislukukertoiminen Laurentin polynomiannihilaattori. Olkoon*

$$g(\boldsymbol{x}) = x_1 \cdots x_n \prod_{\substack{\boldsymbol{u} \in Supp(f) \\ \boldsymbol{u} \neq \boldsymbol{u}_0}} (\boldsymbol{x}^{r\boldsymbol{u}} - \boldsymbol{x}^{r\boldsymbol{u}_0}),$$

jossa r on kokonaisluku Lemmasta 21 ja $\boldsymbol{u}_0 \in Supp(f)$ mielivaltainen. Tällöin $g(\boldsymbol{z}) = 0$ kaikilla ihanteen $Ann(c)$ yhteisillä nollakohdilla $\boldsymbol{z} \in \mathbb{C}^n$.

Todistus. Olkoon $\boldsymbol{z}$ jokin ihanteen $\mathrm{Ann}(c)$ yhteisistä nollakohdista. Jos jokin sen koordinaatti on 0, niin $g(\boldsymbol{z}) = 0$. Olkoon siten kaikki sen koordinaatit nollasta eroavia.

Muodostetaan seuraavanlaiset joukot ja funktiot kompleksiluvulle $\alpha \in \mathbb{C}$:

$$S_\alpha = \{\boldsymbol{u} \in \mathrm{Supp}(f) \mid \boldsymbol{z}^{r\boldsymbol{u}} = \alpha\},$$
$$f_\alpha(\boldsymbol{x}) = \sum_{\boldsymbol{u} \in S_\alpha} a_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}.$$

Koska $\mathrm{Supp}(f)$ on äärellinen, niin tällöin on olemassa äärellinen määrä epätyhjiä joukkoja $S_{\alpha_1}, \ldots, S_{\alpha_m}$. Nämä joukot muodostavat joukon $\mathrm{Supp}(f)$ partition, josta saadaan $f = f_{\alpha_1} + \cdots + f_{\alpha_m}$.

Koska luvut $1 + r \cdot a$ ovat suhteellisia alkulukuja lukuun r kaikilla ei-negatiivisilla kokonaisluvuilla a, niin Lemman 21 perusteella $f(\boldsymbol{x}^{1+r\cdot a}) \in \mathrm{Ann}(c)$. Nyt koska $\boldsymbol{z}$ oli annihilaattori-ihanteen yhteinen nollakohta, niin $f(\boldsymbol{z}^{1+r\cdot a}) = 0$. Sijoitetaan $\boldsymbol{z}^{1+r\cdot a}$ funktioon $f_\alpha(\boldsymbol{x})$, jolloin saadaan

$$f_\alpha(\boldsymbol{z}^{1+r\cdot a}) = \sum_{\boldsymbol{u}\in S_\alpha} a_{\boldsymbol{u}} \boldsymbol{z}^{(1+r\cdot a)\boldsymbol{u}} = \sum_{\boldsymbol{u}\in S_\alpha} a_{\boldsymbol{u}} \boldsymbol{z}^{\boldsymbol{u}} \alpha^a = f_\alpha(\boldsymbol{z})\alpha^a.$$

Summataan funktiot $f_{\alpha_1}, \ldots, f_{\alpha_m}$ yhteen:

$$0 = f(\boldsymbol{z}^{1+r\cdot a}) = f_{\alpha_1}(\boldsymbol{z})\alpha_1^a + \cdots + f_{\alpha_m}(\boldsymbol{z})\alpha_m^a.$$

Edellinen yhtälö täyttää kohtisuoruuden määritelmän pistetulolla avaruudessa $\mathbb{C}^m$, joten saadaan

$$\left(\overline{f_{\alpha_1}(\boldsymbol{z})}, \ldots, \overline{f_{\alpha_m}(\boldsymbol{z})}\right) \perp (\alpha_1^a, \ldots, \alpha_m^a).$$

Edellisistä vektoreista $(\alpha_1^a, \ldots, \alpha_m^a)$ arvoilla $a \in \{0, 1, \ldots, m-1\}$ voidaan muodostaa Vandermonden matriisi, jonka determinantti $\prod_{0\le i<j\le n}(\alpha_j - \alpha_i)$ ei ole nolla. Tästä saadaan, että vektori $\left(\overline{f_{\alpha_1}(\boldsymbol{z})}, \ldots, \overline{f_{\alpha_m}(\boldsymbol{z})}\right)$ on nollavektori ja erityisesti sellaisella α, jolla $\boldsymbol{u}_0 \in S_\alpha$, pätee

$$0 = f_\alpha(\boldsymbol{z}) = \sum_{\boldsymbol{u}\in S_\alpha} a_{\boldsymbol{u}} \boldsymbol{z}^{\boldsymbol{u}}.$$

Vektorissa $\boldsymbol{z}$ ei ole nollakoordinaatteja, joten yhtälön oikean puolen jokainen termi on nollasta eroava. Kuitenkin summa on 0, joten tällöin joukkoon S_α kuuluu vähintään kaksi vektoria $\boldsymbol{u}$ ja $\boldsymbol{u}_0$. Joukon S_α määritelmän perusteella $\boldsymbol{z}^{r\boldsymbol{u}} = \boldsymbol{z}^{r\boldsymbol{u}_0} = \alpha$, joten $\boldsymbol{z}$ on Laurentin polynomin $\boldsymbol{x}^{r\boldsymbol{u}} - \boldsymbol{x}^{r\boldsymbol{u}_0}$ nollakohta. □

Nyt Nullstellensatzin lauseella voitaisiin todistaa Lauseet 26 ja 27, mutta ilman lineaarista riippumattomuutta. Seuraavaksi esiteltävillä *suorilla Laurentin polynomeilla* saadaan todistettua haluttu lineaarinen riippumattomuus.

Määritelmä 23. Laurentin polynomia $f \in \mathbb{C}[\boldsymbol{x}^{\pm 1}]$ kutsutaan *suoraksi Laurentin polynomiksi*, jos sen tuki sisältää ainakin kaksi pistettä ja tuen kaikki pisteet ovat samalla suoralla.

Vektoria $\boldsymbol{v}$ kutsutaan *primitiiviseksi*, jos sen koordinaateilla ei ole yhteistä epätriviaalia kokonaislukutekijää. Kaikki suorat Laurentin polynomit voidaan esittää muodossa

$$f(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{v}'}(a_m \boldsymbol{x}^{m\boldsymbol{v}} + \cdots + a_1 \boldsymbol{x}^{\boldsymbol{v}} + a_0)$$

joillain $a_i \in \mathbb{C}, m \ge 1, a_m \ne 0, a_0 \ne 0, \boldsymbol{v}', \boldsymbol{v} \in \mathbb{Z}^n$, jossa $\boldsymbol{v}$ on primitiivinen.

Lemma 24. *Olkoon c yksiulotteinen konfiguraatio, jolla $f^m c = 0$ jollain epätriviaalilla polynomilla f ja kokonaisluvulla $m \in \mathbb{N}$. Tällöin myös $fc = 0$.*

Todistus. Konfiguraatiota c voidaan käsitellä sarjana, jolla on vain äärellisen monta eri arvoa. Olkoon $f^m(x) = \sum_{i \in \mathrm{Supp}(f)} a_i x^i$. Kirjoittamalla kertolasku $f^m c = 0$ auki saadaan

$$a_{i_1} x^{i_1} c + \cdots + a_{i_d} x^{i_d} c = 0$$

ja kaikilla sarjan arvoilla c_n saadaan differenssiyhtälö

$$a_{i_1} c_{n-i_1} + \cdots + a_{i_d} c_{n-i_d} = 0.$$

Koska konfiguraatio c voi saada vain äärellisen monta arvoa ja sillä on yllä oleva differenssiyhtälö, niin se on periodinen. Täten on siis olemassa sellainen luku $k \in \mathbb{N}$, että $x^k - 1 \in \mathrm{Ann}(c)$.

Koska $\mathrm{Ann}(c)$ on ihanne niin saadaan, että $g = \gcd(x^k - 1, f^m) \in \mathrm{Ann}(c)$. Koska polynomilla $x^k - 1$ on vain yksinkertaisia juuria ja polynomi g jakaa sen, niin polynomilla g on myös vain yksinkertaisia juuria. Täten siis kun g jakaa polynomin f^m, niin se jakaa myös polynomin f. Koska polynomi g jakaa polynomin f ja $g \in \mathrm{Ann}(c)$, niin $f \in \mathrm{Ann}(c)$. □

Lemma 25. *Olkoon c jokin konfiguraatio ja $f_1, \ldots, f_k$ sellaisia suoria Laurentin polynomeja, että $f_1^{m_1} \cdots f_k^{m_k}$ annihiloi konfiguraation c. Tällöin myös $f_1 \cdots f_k$ annihiloi sen.*

Todistus. Näytetään ensin, että kun f on suora Laurentin polynomi ja f^m annihiloi konfiguraation c, niin tällöin myös f annihiloi sen. Voidaan olettaa, että suora Laurentin polynomi kulkee origon kautta, eli $\boldsymbol{v}' = 0$ ja

$$f(\boldsymbol{x}) = a_d \boldsymbol{x}^{d\boldsymbol{v}} + \cdots + a_1 \boldsymbol{x}^{\boldsymbol{v}} + a_0$$

joillain $a_i \in \mathbb{C}$ ja $\boldsymbol{v} \in \mathbb{Z}^n$. Määritellään yksiulotteinen polynomi $g(t) = a_d t^d + \cdots + a_1 t + a_0 \in \mathbb{C}[t]$ siten että $f^m(\boldsymbol{x}) = g^m(\boldsymbol{x}^{\boldsymbol{v}})$.

Nyt millä vain $\boldsymbol{u} \in \mathbb{Z}^n$ sarja kertoimista $(c_{\boldsymbol{u}+i\boldsymbol{v}})_{i \in \mathbb{Z}}$ voidaan käsittää yksiulotteisena konfiguraationa, jonka polynomi g^m annihiloi. Lemman 24 perusteella sen annihiloi myös polynomi g, joten $g(\boldsymbol{x}^{\boldsymbol{v}}) = f(\boldsymbol{x})$ annihiloi konfiguraation c.

Nyt $f_2^{m_2} \cdots f_k^{m_k} c$ on myös jokin konfiguraatio, jonka suora Laurentin polynomi $f_1^{m_1}$ annihiloi ja täten sen siis annihiloi myös polynomi f_1 ja $f_1 f_2^{m_2} \cdots f_k^{m_k} c = 0$. Sama päättely voidaan toistaa kaikille f_i, josta saadaan $f_1 f_2 \cdots f_k c = 0$. □

Lause 26. *Olkoon c konfiguraatio ja $f \in Ann(c)$. Jokaista $\boldsymbol{u} \in Supp(f)$ kohti on olemassa pareittain lineaarisesti riippumattomat $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m \in \mathbb{Z}^n$ siten, että jokainen $\boldsymbol{t}_i$ on yhdensuuntainen $\boldsymbol{u}_i - \boldsymbol{u}$ kanssa jollain $\boldsymbol{u}_i \in Supp(f) \setminus \{\boldsymbol{u}\}$ ja*

$$(\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in Ann(c). \tag{1}$$

Todistus. Olkoon $g(\boldsymbol{x})$ kuten Lemmassa 22. Koska $g(\boldsymbol{x}) = 0$ kaikilla ihanteen $\mathrm{Ann}(c)$ yhteisillä nollakohdilla, niin Nullstellensatzin lauseen mukaan jollain $k \in \mathbb{N}$ polynomi $g^k(\boldsymbol{x})$ kuuluu annihilaattori-ihanteeseen $\mathrm{Ann}(c)$. Koska $g^k(\boldsymbol{x})$ koostuu suorista Laurentin polynomeista, niin Lemman 25 mukaan myös $g(\boldsymbol{x}) \in \mathrm{Ann}(c)$.

Koska $g(\boldsymbol{x})$ kuuluu ihanteeseen, niin myös

$$\frac{g(\boldsymbol{x})}{x_1 \cdots x_n \cdot \boldsymbol{x}^{r\boldsymbol{u}_0(|\mathrm{Supp}(f)-1|)}} = \prod (\boldsymbol{x}^{r(\boldsymbol{u}-\boldsymbol{u}_0)} - 1) = \prod (\boldsymbol{x}^{\boldsymbol{t}_i} - 1)$$

kuuluu ihanteeseen $\mathrm{Ann}(c)$. Jos jollain indekseillä $j_1 \neq j_2$ vektorit $\boldsymbol{t}_{j_1} = a\boldsymbol{t}$ ja $\boldsymbol{t}_{j_2} = b\boldsymbol{t}$ ovat lineaarisesti riippuvia, niin termi $(\boldsymbol{x}^{a\boldsymbol{t}} - 1)(\boldsymbol{x}^{b\boldsymbol{t}} - 1)$ voidaan korvata termillä $(\boldsymbol{x}^{ab\boldsymbol{t}} - 1)$. Nimittäin polynomi $(\boldsymbol{x}^{a\boldsymbol{t}} - 1)(\boldsymbol{x}^{b\boldsymbol{t}} - 1)$ jakaa polynomin $(\boldsymbol{x}^{ab\boldsymbol{t}} - 1)^2$, eli $(\boldsymbol{x}^{a\boldsymbol{t}} - 1)(\boldsymbol{x}^{b\boldsymbol{t}} - 1)h(\boldsymbol{x}) = (\boldsymbol{x}^{ab\boldsymbol{t}} - 1)^2$ jollain polynomilla $h(\boldsymbol{x})$, jolloin $h(\boldsymbol{x}) \prod(\boldsymbol{x}^{\boldsymbol{t}_i} - 1) = (\boldsymbol{x}^{ab\boldsymbol{t}} - 1)^2 \prod_{i \neq j_1, j_2}(\boldsymbol{x}^{\boldsymbol{t}_i} - 1)$ kuuluu ihanteeseen $\mathrm{Ann}(c)$ ja Lemman 25 mukaan $(\boldsymbol{x}^{ab\boldsymbol{t}} - 1) \prod_{i \neq j_1, j_2}(\boldsymbol{x}^{\boldsymbol{t}_i} - 1) \in \mathrm{Ann}(c)$. □

Sama pätee myös siirtoaliavaruuksille.

Lause 27. *Olkoon X siirtoaliavaruus ja $f \in Ann(X)$. Jokaista $\boldsymbol{u} \in Supp(f)$ kohti on olemassa pareittain lineaarisesti riippumattomat $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m \in \mathbb{Z}^n$ siten, että jokainen $\boldsymbol{t}_i$ on yhdensuuntainen $\boldsymbol{u}_i - \boldsymbol{u}$ kanssa jollain $\boldsymbol{u}_i \in Supp(f) \setminus \{\boldsymbol{u}\}$ ja*

$$(\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in Ann(X). \tag{2}$$

Todistus. Olkoon $f \in \mathrm{Ann}(X)$, tällöin myös polynomi $f \in \mathrm{Ann}(c)$ kaikilla $c \in X$. Edellisten lauseiden mukaan Laurentin polynomien

$$(\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in \mathrm{Ann}(c)$$

vektorit $\boldsymbol{t}_i$ määräytyvät täysin Laurentin polynomista f ja Lemmassa 21 olevassa arvosta

$$s = c_{max} \sum |f_{\boldsymbol{u}}|.$$

Valitsemalla arvon c_{max} sijaan arvo X_{max}, missä X_{max} on itseisarvoltaan suurin kerroin siirtoaliavaruuden X konfiguraatioissa, saadaan haluttu yhteinen annihilaattori kaikille konfiguraatioille $c \in X$. □

2.5 Lee-koodit

Tässä kappaleessa perehdytään täydellisiin e-virheen korjaaviin Lee-koodeihin ja miten niitä voidaan käsitellä laatoitusten avulla. Lähteenä on [1].

Määritelmä 28. Metriikkaa

$$\delta_L(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^{n} \min(|u_i - v_i|, q - |u_i - v_i|), \text{ kun } \boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}_q^n,$$
$$\delta_L(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^{n} |u_i - v_i|, \text{ kun } \boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}^n$$

kutsutaan *Lee-metriikaksi*, joka tunnetaan myös *Manhattan-* ja *ℓ^1-metriikkana.*

Määritelmä 29. Metrisen avaruuden $(\mathbb{Z}^n, \delta_L)$ tai $(\mathbb{Z}_q^n, \delta_L)$ osajoukkoa C kutsutaan *Lee-koodiksi.* Lee koodia C kutsutaan *e-virheen korjaavaksi koodiksi*, jos kaikilla $\boldsymbol{u}, \boldsymbol{v} \in C$ pätee $\delta_L(\boldsymbol{u}, \boldsymbol{v}) \geq 2e + 1$, kun $\boldsymbol{u} \neq \boldsymbol{v}$. Toisin sanoen, joukon C kahden erillisen alkion etäisyys toisistaan on vähintään $2e + 1$.

e-virheen korjaavaa Lee koodia C kutsutaan *täydelliseksi*, jos jokaista $\boldsymbol{x} \in \mathbb{Z}^n$ tai $\boldsymbol{x} \in \mathbb{Z}_q^n$ kohti on olemassa yksikäsitteinen $\boldsymbol{c} \in C$ siten, että $\delta_L(\boldsymbol{x}, \boldsymbol{c}) \leq e$. Toisin

sanoen jokainen metrisen avaruuden $(\mathbb{Z}^n, \delta_L)$ tai $(\mathbb{Z}_q^n, \delta_L)$ piste on enintään etäisyyden e päässä yhdestä joukon C pisteestä. Täydellisestä e-virheen korjaavaavasta Lee koodista käytetään merkintää $PL(n, e, q)$ avaruudessa $\mathbb{Z}_q^n$ ja $PL(n, e)$ avaruudessa $\mathbb{Z}^n$.

$PL(n, e)$-koodi C on *periodinen*, *vahvasti periodinen* tai *lineaarinen*, jos joukko C on vastaavasti *periodinen*, *vahvasti periodinen* tai *ristikollinen*.

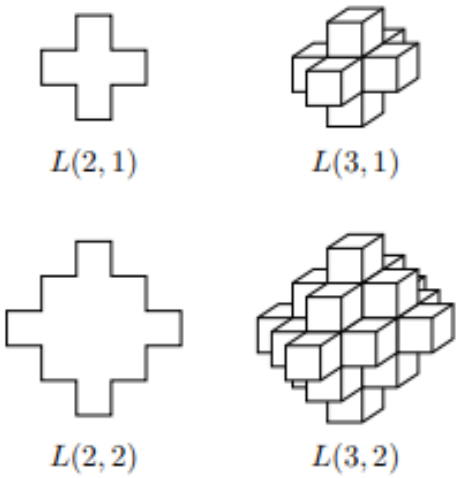
Kun periodi $q \geq 2e + 1$, niin $\mathrm{PL}(n, e, q)$-koodien sanotaan olevan yli *suuren aakkoston*, muuten ne ovat yli *pienen aakkoston*. Oletetaan tästä eteenpäin, että $\mathrm{PL}(n, e, q)$-koodit ovat yli suuren aakkoston, ellei toisin mainita.

Määritellään seuraavaksi *Lee-pallo*. Tällöin täydellisiä e-virheen korjaavia Lee koodeja voidaan käsitellä laatoitusten avulla.

Määritelmä 30. Kutsutaan seuraavia joukkoja e-säteisiksi *Lee-palloiksi*:

$$S(n, e, q) = \{\boldsymbol{x} \in \mathbb{Z}_q^n \mid \delta_L(\boldsymbol{x}, \mathbf{0}) \leq e\},$$
$$S(n, e) = \{\boldsymbol{x} \in \mathbb{Z}^n \mid \delta_L(\boldsymbol{x}, \mathbf{0}) = |x_1| + \cdots + |x_n| \leq e\}.$$

Usein suljettuja palloja kutsutaan topologiassa kuuliksi ja vain pallon reunaa kutsutaan palloksi, mutta tässä tutkielmassa poiketaan käytännöstä Lee-pallojen suhteen.



Kuva 3: Reaaliavaruuden $\mathbb{R}^n$ Lee-pallot $L(n, e)$ ovat n-ulotteisten yksikkökuutioiden unioneja, jotka on asetettu Lee-pallon $S(n, e)$ pisteiden päälle. Kuvassa on määritelmän 30 Lee-palloja esitettynä reaaliavaruudessa [1].

Nyt $\mathrm{PL}(n, e)$-koodit voidaan luonnollisesti esittää avaruuden $\mathbb{Z}^n$ laatoituksena laatalla $S(n, e)$. Nimittäin $\mathrm{PL}(n, e)$-koodin kaikki pisteet ovat vähintään etäisyyden $2e + 1$ päässä toisistaan, jolloin jokaisen pisteen kohdalle sijoitettu e-säteinen Lee-pallo ei ole päällekkäin minkään toisen Lee-pallon kanssa. Koska $\mathrm{PL}(n, e)$-koodi on täydellinen, niin jokainen avaruuden $(\mathbb{Z}^n, \delta_L)$ piste on enintään etäisyyden e päässä jostain $\mathrm{PL}(n, e)$-koodin pisteestä. Täten kun $\mathrm{PL}(n, e)$-koodin kaikkien pisteiden

päälle asetetaan laatta $S(n, e)$, niin avaruuteen $\mathbb{Z}^n$ ei jää tyhjiä kohtia. Nämä ominaisuudet yhdessä siis tarkoittavat sitä, että PL(n, e)-koodi laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla $S(n, e)$. PL(n, e)-koodeja voidaan siis käsitellä laatoitusten avulla.

Vahvasti periodiset PL(n, e)-koodit voidaan samaistaa PL(n, e, q)-koodien kanssa. Olkoon $f : \mathbb{Z}^n \to \mathbb{Z}_q^n$ luonnollinen projektio. Sivuluokkien avulla projektio on $f(\boldsymbol{x}) = \boldsymbol{x} + q\mathbb{Z}^n = \boldsymbol{x} \pmod q$. Tällöin joukkojen $S(n, e)$ ja $S(n, e, q)$ välillä on bijektio luonnollisen projektion restriktiolla. Tällöin jokainen avaruuden $\mathbb{Z}^n$ laatoitus laatoilla $S(n, e, q)$ saadaan luonnollisella projektiolla jostain q-periodiesta laatoituksesta laatoilla $S(n, e)$. Vastaavasti jokainen q-periodinen PL(n, e)-koodi saadaan jostain PL(n, e, q)-koodista.

Lause 31. *PL(n, e, q)-koodien ja q-periodisten PL(n, e)-koodien välillä on olemassa luonnollinen bijektio.*

Koska PL(n, e, q)-koodien ja q-periodisten PL(n, e)-koodien välillä on olemassa luonnollinen bijektio ja q-periodiset PL(n, e)-koodit ovat PL(n, e)-koodien osajoukko, niin täten kun puhutaan kaikista PL(n, e)-koodeista ilman, että periodisuutta on mainittu, niin samalla puhutaan PL(n, e, q)-koodeista.

Nyt saadaan seuraava lause:

Lause 32. *PL(n, e)-koodi on olemassa jos ja vain jos on olemassa laatoitus Lee-pallolla $S(n, e)$. Samoin PL(n, e, q)-koodi on olemassa jos ja vain jos on olemassa vahvasti q-periodinen laatoitus laatoilla $S(n, e)$.*

Esitellään lopuksi vielä Lee-pallojen koko [13]:

$$|S(n, e)| = \sum_{i=0}^{\min\{n,e\}} 2^i \binom{n}{i} \binom{e}{i}.$$

3 Golomb-Welch konjektuuri

Esitellään seuraavaksi Golomb-Welch konjektuurin vahva ja heikko versio [13]:

Konjektuuri 33 (Golomb-Welch, heikko versio)**.** *Ei ole olemassa sellaista* $PL(n, e, q)$*-koodia, jossa* $q \geq 2e + 1$*,* $n \geq 3$ *ja* $e \geq 2$*.*

Konjektuuri 34 (Golomb-Welch, vahva versio)**.** *Ei ole olemassa sellaista* $PL(n, e)$*-koodia, jossa* $n \geq 3$ *ja* $e \geq 2$*.*

Golomb ja Welch esittivät konjektuurit jo vuonna 1968, eikä niitä ole vielä ratkaistu. Seuraavissa kappaleissa tullaan käsittelemään algebrallisia lähestymistapoja konjektuureihin.

Mikäli seuraava Lagarias-Wang konjektuuri [21] olisi totta, niin Konjektuurit 33 ja 34 olisivat ekvivalentit:

Konjektuuri 35 (Lagarias-Wang)**.** *Olkoon* $V \subset \mathbb{Z}^n$ *jokin laatta. Jos konfiguraatio* c_1 *laatoittaa avaruuden* $\mathbb{Z}^n$ *laatoilla* V*, niin on olemassa vahvasti periodinen konfiguraatio* c_2*, joka laatoittaa avaruuden* $\mathbb{Z}^n$ *laatoilla* V*.*

Lagarias-Wang konjektuuri osoitettiin vääräksi vuoden 2022 loppupuolella. Katso lisätietoja lähteestä [3]. Kuitenkin tämän tutkielman kappaleessa 4.2 osoitetaan, että Konjektuuri 35 pitää paikkaansa kun $|V|$ on alkuluku. Tämän todisti ensimmäiseksi Szegedy [20].

4 Algebralliset lähestymistavat Golomb-Welch konjektuuriin

4.1 Polynominen menetelmä

Kappaleen lähteinä ovat teokset [1, 5, 6]. Olkoon c jokin avaruuden $\mathbb{Z}^n$ konfiguraatio, joka saa vain arvoja 0 ja 1. Määritellään sellainen lineaarikuvaus

$$T_c : \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \to \mathbb{Z},$$

että kaikilla $(a_1, \ldots, a_n) \in \mathbb{Z}^n$

$$T_c(x_1^{a_1} \ldots x_n^{a_n}) = c(a_1, \ldots, a_n).$$

Lineaarikuvaus T_c kertoo kuinka monta annettua pistettä kuuluu konfiguraatioon c. Jos polynomin $f \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ termien kertoimet ovat kaikki 1, niin $T_c(f) = |\mathrm{Supp}(f) \cap \mathrm{Supp}(f_c)|$. Ehto $T_c(x_1^{v_1} \ldots x_n^{v_n} f_{-D}) = 1$ onkin ekvivalentti ehdon $|(-D + \boldsymbol{v}) \cap \mathrm{Supp}(f_c)| = 1$ kanssa. Lause 12 saadaankin seuraavaan muotoon: konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D jos ja vain jos $T_c(M f_{-D}) = 1$ kaikilla yksikkömonomeilla $M \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Oletetaan seuraavaksi, että konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Myöhemmin nähdään, että konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ myös laatoilla $-D$. Tämän seurauksena saadaan, että $T_c(f_{-D}) = T_c(f_D) = 1$ jolloin kuvauksen T_c argumentiksi voidaan suoraan antaa laatan D karakteristinen funktio f_D. Koska polynomi on lineaarikombinaatio yksikkömonomeista, niin $T_c(P f_{-D}) = P(1, \ldots, 1)$ jokaisella Laurentin polynomilla $P \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Monissa seuraavissa todistuksissa käytetään seuraavaa ominaisuutta laatan D karakteriselle polynomille:

$$f_D(x_1^a, \ldots, x_n^a) = \sum_{\boldsymbol{d} \in D} x_1^{a \cdot d_1} \cdots x_n^{a \cdot d_n} = f_{aD}(x_1, \ldots, x_n).$$

Erityisesti kun $a = -1$, niin saadaan $f_D(x_1^{-1}, \ldots, x_n^{-1}) = f_{-D}(x_1, \ldots, x_n)$.

Seuraavaksi esitellään tuloksia, joissa käytetään hyödyksi lineaarikuvaksen T_c ja Laurentin polynomin f_{-D} ominaisuuksia. Tutkimuksen [6] kirjoittajat ovat nimenneet lähestymistavat *polynomiseksi menetelmäksi* (eng. Polynomial Method).

Lemma 36. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Tällöin*

$$T_c(P f_{-D}(x_1^{-1}, \ldots, x_n^{-1})) = P(1, \ldots, 1)$$

kaikilla kokonaislukukertoimisilla Laurentin polynomeilla $P \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Todistus. Koska T_c on lineaarikuvaus, niin riittää todistaa, että

$$T_c(M f_{-D}(x_1^{-1}, \ldots, x_n^{-1})) = 1$$

kaikilla yksikkömonomeilla $M \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$.

Todistetaan ensin, että $T_c(Mf_{-D}(x_1^{-1},\dots,x_n^{-1})) \leq 1$. Jos näin ei ole, niin on olemassa $\boldsymbol{u},\boldsymbol{v} \in -D$, $\boldsymbol{u} \neq \boldsymbol{v}$, joilla

$$T_c(M \cdot x_1^{-v_1} \cdots x_n^{-v_n}) = T_c(M \cdot x_1^{-u_1} \cdots x_n^{-u_n}) = 1.$$

Olkoon $M' = M \cdot x_1^{-v_1-u_1} \cdots x_n^{-v_n-u_n}$. Nyt

$$\begin{aligned} 1 = T_c(M' f_{-D}) &\geq T_c(M' \cdot x_1^{u_1} \cdots x_n^{u_n}) + T_c(M' \cdot x_1^{v_1} \cdots x_n^{v_n}) \\ &= T_c(M \cdot x_1^{-v_1} \cdots x_n^{-v_n}) + T_c(M \cdot x_1^{-u_1} \cdots x_n^{-u_n}) = 2, \end{aligned}$$

mikä on ristiriita. Täten $T_c(Mf_{-D}(x_1^{-1},\dots,x_n^{-1})) \leq 1$ kaikilla yksikkömonomeilla M.

Koska $T_c(Mf_{-D}(x_1^{-1},\dots,x_n^{-1})f_{-D}) = f_{-D}(1^{-1},\dots,1^{-1}) = |D|$ ja

$$\begin{aligned} T_c(Mf_{-D}(x_1^{-1},\dots,x_n^{-1})f_{-D}) &= \sum_{\boldsymbol{d}\in -D} T_c(M \cdot x_1^{d_1} \cdots x_n^{d_n} \cdot f_{-D}(x_1^{-1},\dots,x_n^{-1})) \\ &\leq \sum_{\boldsymbol{d}\in -D} 1 = |D|, \end{aligned}$$

niin summan kaikilla termeillä pätee yhtäsuuruus. Täten kaikilla yksikkömonomeilla M saadaan $T_c(Mf_{-D}(x_1^{-1},\dots,x_n^{-1})) = 1$. □

Edellisestä lauseesta seuraa suoraan, että $T_c(Mf_{-D}) = T_c(Mf_D)$ kaikilla yksikkömonomeilla $M \in \mathbb{Z}[x_1^{\pm 1},\dots,x_n^{\pm 1}]$.

Seuraus 37. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Tällöin c laatoittaa avaruuden $\mathbb{Z}^n$ myös laatoilla $-D$. Myös $T_c(Mf_{-D}) = T_c(Mf_D)$ kaikilla yksikkömonomeilla M.*

Todistus. Nyt kaikilla yksikkömonomeilla $M \in \mathbb{Z}[x_1^{\pm 1},\dots,x_n^{\pm 1}]$ pätee

$$T_c(Mf_D(x_1,\dots,x_1)) = T_c(Mf_{-D}(x_1^{-1},\dots,x_1^{-1})) = T_c(Mf_{-D}(x_1,\dots,x_1)) = 1.$$

Täten $|(D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = |(-D+\boldsymbol{x}) \cap \mathrm{Supp}(f_c)| = 1$ kaikilla $\boldsymbol{x} \in \mathbb{Z}^n$, joten konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla $-D$. □

Edellisen seurauksen perusteella nyt merkinnästä $T_c(Mf_{-D})$ voi jättää miinusmerkin pois tehden todistuksista ja lauseista selkeämpiä.

Seuraava lemma, lause ja seuraus todistavat, että jos konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatalla D, niin sama konfiguraatio laatoittaa avaruuden myös laatalla $aD = \{a \cdot \boldsymbol{d} \,|\, \boldsymbol{d} \in D\}$, kun a on kokonaisluku, jolla $\gcd(a,|D|) = 1$.

Lemma 38. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D ja olkoon $p = 1$ tai alkuluku, joka ei jaa laatan kokoa $|D|$. Tällöin*

$$T_c(Pf_D(x_1^p,\dots,x_n^p)) = P(1,\dots,1)$$

kaikilla kokonaislukukertoimisilla Laurentin polynomeilla $P \in \mathbb{Z}[x_1^{\pm 1},\dots,x_n^{\pm 1}]$.

Todistus. Koska T_c on lineaarikuvaus, niin riittää todistaa, että

$$T_c(Mf_D(x_1^p, \ldots, x_n^p)) = 1$$

jokaisella yksikkömonomilla $M \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Saadaan

$$\begin{aligned} T_c(Mf_D(x_1^p, \ldots, x_n^p)) &\equiv T_c(Mf_D(x_1, \ldots, x_n)^p) = T_c(Mf_D(x_1, \ldots, x_n)^{p-1} f_D) \\ &= (f_D(1, \ldots, 1))^{p-1} = |D|^{p-1} \equiv 1 \pmod{p}, \end{aligned}$$

sillä $T_c(Rf_D) = R(1, \ldots, 1)$ kaikilla Laurentin polynomeilla $R \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Täten $T_c(Mf_D(x_1^p, \ldots, x_n^p)) \geq 1$ kaikilla yksikkömonomeilla M.

Edelleen saadaan

$$T_c(Mf_D(x_1^p, \ldots, x_n^p) f_D) = \sum_{\boldsymbol{d} \in D} T_c(M \cdot x_1^{d_1} \cdots x_n^{d_n} \cdot f_D(x_1^p, \ldots, x_n^p)) \geq \sum_{\boldsymbol{d} \in D} 1 = |D|, \quad (3)$$

mutta myös

$$T_c(Mf_D(x_1^p, \ldots, x_n^p) f_D) = f_D(1^p, \ldots, 1^p) = |D|.$$

Täten siis yhtälössä (3) pätee yhtäsuuruus kaikilla summan termeillä. Koska yksikkömonomi $M \cdot x_1^{d_1} \cdots x_n^{d_n}$ on mielivaltainen, niin

$$T_c(Mf_D(x_1^p, \ldots, x_n^p)) = 1.$$

□

Edellisistä lemmoista seuraa suoraan seuraava lause:

Lause 39. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D ja olkoon $a \in \mathbb{Z}$ laatan koon $|D|$ suhteen alkuluku. Siis $gcd(a, |D|) = 1$. Nyt jokaisella kokonaislukukertoimisella Laurentin polynomilla $P \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ pätee*

$$T_c(Pf_D(x_1^a, \ldots, x_n^a)) = P(1, \ldots, 1).$$

Todistus. Luvun a voi esittää alkulukujen tulona, jotka eivät jaa lukua $|D|$. Siis $a = p_1 \cdots p_m$. Edellisen lemman perusteella, jos konfiguraatio c laatoittaa avaruuden laatoilla D, se laatoittaa avaruuden myös laatoilla $p_1 D$. Jatkamalla samalla logiikalla saadaan, että c laatoittaa avaruuden myös laatoilla $p_1 \cdots p_m D = aD$ ja siten

$$T_c(Pf_D(x_1^a, \ldots, x_n^a)) = P(1, \ldots, 1).$$

□

Kun edellisessä lauseessa korvataan polynomi P mielivaltaisella yksikkömonomilla M, niin saadaan suoraan seuraava lause:

Seuraus 40. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D ja olkoon $a \in \mathbb{Z}$ laatan koon $|D|$ suhteen alkuluku. Siis $gcd(a, |D|) = 1$. Tällöin c laatoittaa avaruuden $\mathbb{Z}^n$ "räjähtäneillä" laatoilla $aD = \{a\boldsymbol{d} \mid d \in D\}$ (eng. "blowout" tile).*

Todistus. $T_c(Mf_{aD}(x_1,\ldots,x_n)) = T_c(Mf_D(x_1^a,\ldots,x_n^a)) = 1$ kaikilla yksikkömonomeilla M, joten konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla aD. □

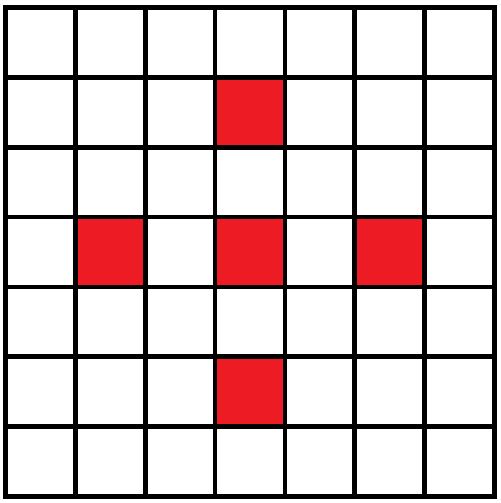
Nyt saadaan seuraus, mikä kertoo mihin pisteisiin laattaa ei voi missään konfiguraatioissa asettaa. Nämä pisteet ovat niitä pisteitä, joissa "räjähtäneet" laatat menisivät päällekkäin.

Seuraus 41. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D ja olkoon $a \in \mathbb{Z}$ laatan koon $|D|$ suhteen alkuluku. Siis $gcd(a,|D|) = 1$. Tällöin $\boldsymbol{l} + a(\boldsymbol{v}-\boldsymbol{w}) \notin Supp(f_c)$, kun $\boldsymbol{l} \in Supp(f_c)$ ja $\boldsymbol{v} \neq \boldsymbol{w} \in D$.*

Todistus. Tehdään vastaoletus $\boldsymbol{l} + a(\boldsymbol{v}-\boldsymbol{w}) = \boldsymbol{k} \in \mathrm{Supp}(f_c)$. Nyt

$$\boldsymbol{l} + a\boldsymbol{v} = a\boldsymbol{w} + \boldsymbol{k} \text{ ja}$$
$$\boldsymbol{l} + a\boldsymbol{v} = a\boldsymbol{v} + \boldsymbol{l}.$$

Seurauksen 40 perusteella konfiguraatio c laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla aD, mutta pisteen $\boldsymbol{l}+a\boldsymbol{v}$ esitys ei ole yksikäsitteinen, jolloin c ei laatoita avaruutta $\mathbb{Z}^n$ laatoilla aD, mikä on ristiriita. □



Kuva 4: "Räjähtänyt" Lee-pallo $S(2,1)$.

Esimerkki 42. Lee-pallojen koko $|S(n,e)| = \sum_{i=0}^{\min\{n,e\}} 2^i \binom{n}{i}\binom{e}{i}$ on pariton, jolloin $\gcd(2,|S(n,e)|) = 1$ ja täten $T_{S(n,e)} \subseteq T_{2S(n,e)}$.

Todistetaan seuraavaksi Laurentin polynomien vastine Hilbertin Nullstellensatz lauseesta.

Lemma 43. *Olkoon $\{f_i\}_{i\in I} \subseteq \mathbb{C}[x_1^{\pm 1},\ldots,x_n^{\pm 1}]$ joukko sellaisia Laurentin polynomeja, että ei ole olemassa sellaista $(x_1,\ldots,x_n) \in (\mathbb{C}\setminus\{0\})^n$, jolla $f_i(x_1,\ldots,x_n) = 0$ kaikilla $i \in I$. Tällöin on olemassa Laurentin polynomit $p_1,\ldots,p_k$ ja indeksit $i_1,\ldots,i_k \in I$ siten, että*

$$f_{i_1}p_1 + \cdots + f_{i_k}p_k = 1.$$

Todistus. Valitaan jokaista $i \in I$ kohti jokin tarpeeksi suuri kokonaisluku $n_i \in \mathbb{N}$, että $(x_1 \cdots x_n)^{n_i - 1} f_i \in \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Olkoon $g_i = (x_1 \cdots x_n)^{n_i} f_i$, jolloin g_i on polynomi, joka on jaollinen monomilla $x_1 \cdots x_n$.

Olkoon seuraavaksi $J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ polynomien g_i generoima ihanne. Koska ei ole sellaista $(x_1, \ldots, x_n) \in (\mathbb{C} \setminus \{0\})^n$, että $f_i(x_1, \ldots, x_n) = 0$ kaikilla $i \in I$, niin ei ole sellaista $(x_1, \ldots, x_n) \in (\mathbb{C} \setminus \{0\})^n$, jolla $g_i(x_1, \ldots, x_n) = 0$ kaikilla $i \in I$. Toisaalta jos jokin $x_i, \ldots, x_n$ on nolla, niin $g_i(x_1, \ldots, x_n) = 0$, sillä $x_1 \cdots x_n$ jakaa polynomin g_i. Täten

$$\mathcal{V}(J) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_1 \cdots x_n = 0\}.$$

Siis Hilbertin Nullstellensatz Lauseen 19 mukaan $x_1 \cdots x_n \in \mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$, eli $(x_1 \cdots x_n)^m \in J$ jollain positiivisella kokonaisluvulla m.

Koska polynomit g_i generoivat ihanteen J, niin on olemassa sellaiset polynomit $q_1, \ldots, q_k$ ja indeksit $i_1, \ldots, i_k \in I$, että

$$(x_1 \cdots x_n)^m = g_{i_1} q_1 + \cdots + g_{i_k} q_k = (x_1 \cdots x_n)^{n_{i_1}} f_{i_1} q_1 + \cdots + (x_1 \cdots x_n)^{n_{i_k}} f_{i_k} q_k.$$

Jakamalla molemmat puolet polynomilla $(x_1 \cdots x_n)^m$ saadaan

$$1 = f_{i_1} \frac{q_1}{(x_1 \cdots x_n)^{m - n_{i_1}}} + \cdots + f_{i_k} \frac{q_k}{(x_1 \cdots x_n)^{m - n_{i_k}}}.$$

□

Seuraavaksi todistetaan välttämätön ehto laatoituksen olemassaoloon:

Lause 44. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D ja olkoon laatan D koko $|D| \geq 2$. Tällöin on olemassa sellainen $(x_1, \ldots, x_n) \in (\mathbb{C} \setminus \{0\})^n$, että $f_D(x_1^a, \ldots, x_n^a) = 0$ kaikilla $a \in \mathbb{Z}$, joilla $gcd(a, |D|) = 1$.*

Todistus. Tehdään vastaoletus: ei ole olemassa sellaista $(x_1, \ldots, x_n) \in (\mathbb{C} \setminus \{0\})^n$, että $f_D(x_1^a, \ldots, x_n^a) = 0$ kaikilla $a \in \mathbb{Z}$, jotka ovat laatan koon $|D|$ suhteen alkulukuja. Nyt Lemman 43 perusteella on olemassa Laurentin polynomit $p_1, \ldots, p_k$ ja kokonaisluvut $a_1, \ldots, a_k$, jotka ovat laatan koon $|D|$ suhteen alkulukuja, joilla pätee

$$p_1 f_D(x_1^{a_1}, \ldots, x_n^{a_1}) + \cdots + p_k f_D(x_1^{a_k}, \ldots, x_n^{a_k}) = 1.$$

Asettamalla kaikkiin muuttujiin $x_1, \ldots, x_n$ arvon 1 saadaan

$$p_1(1, \ldots, 1)|D| + \cdots + p_k(1, \ldots, 1)|D| = 1$$

ja siten

$$p_1(1, \ldots, 1) + \cdots + p_k(1, \ldots, 1) = \frac{1}{|D|}.$$

Nyt Lauseen 39 perusteella jokaisella yksikkömonomilla M

$$\begin{aligned} T_c(M) &= T_c(M(p_1 f_D(x_1^{a_1}, \ldots, x_n^{a_1}) + \cdots + p_k f_D(x_1^{a_k}, \ldots, x_n^{a_k}))) \\ &= T_c(M p_1 f_D(x_1^{a_1}, \ldots, x_n^{a_1})) + \cdots + T_c(M p_k f_D(x_1^{a_k}, \ldots, x_n^{a_k})) \\ &= p_1(1, \ldots, 1) + \cdots + p_k(1, \ldots, 1) \\ &= \frac{1}{|D|}, \end{aligned}$$

mikä on mahdotonta, sillä $\frac{1}{|D|}$ ei ole kokonaisluku. Täten on olemassa sellainen $(x_1, \ldots, x_n) \in (\mathbb{C} \setminus \{0\})^n$, että $f_D(x_1^a, \ldots, x_n^a) = 0$ kaikilla luvuilla $a \in \mathbb{Z}$, jotka ovat laatan koon $|D|$ suhteen alkulukuja. □

Edelliselle lauseelle voidaan todistaa vahvempi versio. Lause on kuten edellä, mutta vektorille $(x_1, \ldots, x_n) \in \mathbb{C}^n$ pätee $|x_i| = 1$ kaikilla $i \in \{1, \ldots, n\}$. Sivuutetaan tämän todistus.

Lause 45. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D, ja olkoon laatan D koko $|D| \geq 2$. Tällöin on olemassa sellainen $(x_1, \ldots, x_n) \in \mathbb{C}^n$, missä $|x_i| = 1$ kaikilla i, että $f_D(x_1^a, \ldots, x_n^a) = 0$ kaikilla $a \in \mathbb{Z}$, joilla $gcd(a, |D|) = 1$.*

Yllä olevat lauseet ovat kuitenkin vain välttämättömiä ehtoja. Vaikka yhteinen nollakohta löytyisi, niin se ei takaa, että laatoitusta olisi olemassa.

Esimerkki 46. PL(3, 2)-koodia ei ole olemassa, mutta yhtälöillä $f_{S(3,2)}(x^a, y^a, z^a) = 0$ on yhteinen nollakohta kaikilla kokonaisluvuilla a, joita luku 5 ei jaa. Esimerkiksi $x = 1, y = e^{2\pi i/5}, z = e^{4\pi i/5}$ on tällainen nollakohta.

4.2 Alkulukujen kokoiset laatat

Kappaleen lähteinä ovat teokset [5, 6].

Edellisen kappaleen Seuraus 41 viittaa siihen, että mitä vähemmän tekijöitä laatan koolla on, niin sitä enemmän rajoituksia laatoituksella on. Täten tässä kappaleessa keskitytään laattoihin, joiden koko kuuluu alkulukujen joukkoon. Heti ensimmäiseksi todistetaan, että laatoituksella on olemassa tällöin jokin periodi.

Lause 47. *Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Jos laatan koko $|D| = p$ on alkuluku, niin $p(\boldsymbol{v} - \boldsymbol{w})$ on konfiguraation c periodi kaikilla $\boldsymbol{v}, \boldsymbol{w} \in D$.*

Todistus. Jokaisella yksikkömonomilla M pätee

$$\begin{aligned} T_c(Mf_D(x_1^p, \ldots, x_n^p)) &\equiv T_c(Mf_D^p) = T_c(Mf_D^{p-1} f_D) \\ &= (f_D(1, \ldots, 1))^{p-1} = p^{p-1} \equiv 0 \pmod{p}, \end{aligned} \tag{4}$$

sillä $T_c(Pf_D) = P(1, \ldots, 1)$ kaikilla Laurentin polynomeilla P. Toisaalta

$$T_c(Mf_D(x_1^p, \ldots, x_n^p)) = \sum_{\boldsymbol{d} \in D} T_c(Mx_1^{pd_1} \cdots x_n^{pd_n}).$$

Täten yhtälössä (4) summataan $|D| = p$ lukua yhteen, jotka ovat joko 0 tai 1, ja summa on luvun p moninkerta. Täten nämä summattavat luvut ovat kaikki samanaikaisesti joko 0 tai 1. Nyt siis kaikilla $\boldsymbol{v}, \boldsymbol{w} \in D$ ja kaikilla yksikkömonomeilla M

$$T_c(Mx_1^{pv_1} \cdots x_n^{pv_n}) = T_c(Mx_1^{pw_1} \cdots x_n^{pw_n}).$$

Tästä seuraa, että kaikilla $\boldsymbol{x} \in \mathbb{Z}^n$ piste $\boldsymbol{x}$ kuuluu laatoituksen tukeen jos ja vain jos $\boldsymbol{x} + p(\boldsymbol{v} - \boldsymbol{w})$ kuuluu laatoituksen tukeen. Täten $p(\boldsymbol{v} - \boldsymbol{w})$ on laatoituksen c periodi. □

Edellisessä lauseessa saatiin vahvalle periodisuudelle lause. Todistetaan seuraavaksi lause ristikollisille laatoituksille. Jos laatan alkiot generoivat Abelin ryhmän $\mathbb{Z}^n$, ja jos on olemassa jokin laatoitus, niin tällöin on olemassa myös ristikollinen laatoitus. Todistetaan ensin apulause [16] jolla ristikolliset laatoitukset voidaan esittää ryhmähomomorfismilla:

Lemma 48. *Olkoon D jokin laatta, jonka koko on $k = |D|$. Tällöin on olemassa ristikollinen konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D, jos ja vain jos on olemassa kertaluvun k Abelin ryhmä G ja ryhmähomomorfismi $\phi : \mathbb{Z}^n \to G$, jonka rajoittuma $\phi : D \to G$ on bijektio.*

Todistus. Olkoon G kertaluvun k Abelin ryhmä ja olkoon $\phi : \mathbb{Z}^n \to G$ sellainen ryhmähomomorfismi, jonka rajoittuma $\phi : D \to G$ on bijektio. Olkoon konfiguraatio c sellainen, että $\mathrm{Supp}(f_c) = \mathrm{Ker}(\phi)$. Kuvauksen ydin $\mathrm{Ker}(\phi)$ on ryhmän $\mathbb{Z}^n$ aliryhmä ja $\mathbb{Z}^n / \mathrm{Ker}(\phi) = G$. Suoraan homomorfismin määritelmästä seuraa, että kaksi alkiota $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}^n$ kuuluvat samaan sivuluokkaan jos ja vain jos $\boldsymbol{u} - \boldsymbol{v} \in \mathrm{Ker}(\phi)$.

Osoitetaan, että $|(-D + \boldsymbol{t}) \cap \mathrm{Ker}(\phi)| = 1$ kaikilla $\boldsymbol{t} \in \mathbb{Z}^n$. Olkoon $\boldsymbol{t} \in \mathbb{Z}^n$ mielivaltainen. Koska $\phi : D \to G$ on bijektio, niin jollain $\boldsymbol{d} \in D$ saadaan $\phi(\boldsymbol{d}) = \phi(\boldsymbol{t})$. Tällöin $\boldsymbol{t} - \boldsymbol{d} = \boldsymbol{l} \in \mathrm{Ker}(\phi)$. Saadaan siis $|(-D + \boldsymbol{t}) \cap \mathrm{Ker}(\phi)| \geq 1$. Oletetaan seuraavaksi, että jollain $\boldsymbol{t} \in \mathbb{Z}^n$ pätee $|(-D + \boldsymbol{t}) \cap \mathrm{Ker}(\phi)| \geq 2$. Tällöin on olemassa sellaiset keskenään eroavat alkiot $\boldsymbol{d}_1, \boldsymbol{d}_2 \in D$, että $\boldsymbol{t} - \boldsymbol{d}_1 \in \mathrm{Ker}(\phi)$ ja $\boldsymbol{t} - \boldsymbol{d}_2 \in \mathrm{Ker}(\phi)$. Mutta tällöin alkiot $\boldsymbol{d}_1, \boldsymbol{d}_2 \in D$ kuuluvat samaan sivuluokkaan, mikä on mahdotonta, sillä ryhmähomomorfismin restriktio $\phi : D \to G$ on bijektio.

Olkoon seuraavaksi c ristikollinen konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Tällöin $\mathrm{Supp}(f_c)$ on siis ryhmän $\mathbb{Z}^n$ normaali aliryhmä ja saadaan tekijäryhmä $G = \mathbb{Z}^n / \mathrm{Supp}(f_c) = \{\boldsymbol{x} + \mathrm{Supp}(f_c) \,|\, \boldsymbol{x} \in \mathbb{Z}^n\}$. Olkoon $\phi : \mathbb{Z}^n \to G$ sellainen kuvaus, että $\phi(\boldsymbol{x}) = g = \boldsymbol{x} + \mathrm{Supp}(f_c)$. Kyseinen kuvaus on luonnollinen homomorfismi. Osoitetaan, että kuvauksen rajoittuma $\phi : D \to G$ on bijektio. Jos se ei ole, niin joillain $\boldsymbol{x}, \boldsymbol{y} \in D$, $\boldsymbol{x} \neq \boldsymbol{y}$, pätee $\phi(\boldsymbol{x}) = \phi(\boldsymbol{y})$. Tällöin $\boldsymbol{x} - \boldsymbol{y} \in \mathrm{Ker}(\phi) = \mathrm{Supp}(f_c)$. Nyt $|(-D + \boldsymbol{x}) \cap \mathrm{Supp}(f_c)| \geq 2$, sillä $-\boldsymbol{y} + \boldsymbol{x} \in \mathrm{Supp}(f_c)$ ja $-\boldsymbol{x} + \boldsymbol{x} \in \mathrm{Supp}(f_c)$. Täten c ei ole avaruuden $\mathbb{Z}^n$ laatoitus laatalla D. Kuvauksen rajoittuma $\phi : D \to G$ on siis bijektio. □

Huomautus 49. Kun k on alkuluku, niin edellisessä lemmassa ryhmäksi G käy ryhmä $\mathbb{Z}_k$.

Nyt edellisestä lemmasta saadaan todistettua, että jos alkuluvun kokoisilla laatoilla voi laatoittaa avaruuden, niin sen voi laatoittaa ristikollisesti. Esitellään ensin *Newtonin identiteetit*, joita käytetään todistuksessa. Lause käyttää avukseen alkeellisia symmetrisia polynomeja.

Alkeellisiksi symmetrisiksi polynomeiksi kutsutaan polynomeja

$$e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k},$$

kun $n \geq k \geq 0$ ja

$$e_k(x_1, \ldots, x_n) = 0,$$

kun $k > n$.

Lause 50. *Olkoot polynomit* $p_k(x_1, \ldots, x_n) = \sum_{i=1}^{k} x_i^k = x_1^k + \cdots + x_n^k$ *ja olkoot polynomit* $e_k(x_1, \ldots, x_n)$ *alkeellisia symmetrisiä polynomeja. Tällöin*

$$ke_k(x_1, \ldots, x_n) = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n),$$

kun $n \geq k \geq 1$.

Todistus [22] sivuutetaan.

Lause 51. *Olkoon* $D = \{\boldsymbol{v}_0 = \mathbf{0}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p-1}\}$ *laatta, jonka koko* $|D| = p$ *on alkuluku, ja jonka alkiot* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p-1}$ *generoivat Abelin ryhmän* $\mathbb{Z}^n$ *yhteenlaskun suhteen. Tällöin on olemassa konfiguraatio* c_1*, joka laatoittaa avaruuden* $\mathbb{Z}^n$ *laatoilla* D *jos ja vain jos on olemassa konfiguraatio* c_2*, joka laatoittaa avaruuden* $\mathbb{Z}^n$ *ristikollisesti. Toisin sanoen on olemassa ryhmähomomorfismi* $\phi : \mathbb{Z}^n \to \mathbb{Z}_p$*, joka rajoittuu bijektioon* $D \to \mathbb{Z}_p$.

Todistus. Kun $p = 2$, niin tapaus on triviaali, koska ainoat mahdolliset laatat ovat $\{0, 1\}$ ja $\{0, -1\}$. Olkoon $p \geq 3$. Oletetaan, että on olemassa jokin laatoitus laatalla D. Todistetaan, että tällöin on olemassa jokin ristikollinen laatoitus laatalla D. Lauseen 44 perusteella on olemassa jokin $(y_1, \ldots, y_n) \in (\mathbb{C} \setminus \{0\})^n$, jolla algebrallinen laatta saa arvon $f_D(y_1^a, \ldots, y_n^a) = 0$ kaikilla arvoilla a, jotka eivät ole jaollisia laatan koolla p. Merkitään polynomin $f_D(x_1, \ldots, x_n)$ termejä monomeilla $m_1, m_2, \ldots, m_p$, jossa $m_1 = 1$. Sijoittamalla luku $(y_1, \ldots, y_n) \in \mathbb{C}^n$ polynomeihin $f_D(x_1^a, \ldots, x_n^a)$, kun $1 < a < p - 1$ saadaan siis

$$h_1^a + h_2^a + \cdots + h_p^a = 0$$

kaikilla $a = 1, 2, \ldots, p - 1$, jossa h_i on monomin m_i arvo luvulla $(y_1, \ldots, y_n)$.

Nyt Lauseen 50 mukaan

$$e_k(h_1, \ldots, h_p) = 0$$

kaikilla $1 \leq k < p$.

Luvut $h_1, h_2, \ldots, h_p$ ovat seuraavan polynomin juuria:

$$(x - h_1) \cdots (x - h_p) = \sum_{k=0}^{p} (-1)^k x^{p-k} e_k(h_1, \ldots, h_p) = x^p - e_p(h_1, \ldots, h_p) = x^p - 1.$$

Tässä $e_p(h_1, \ldots, h_p) = 1$, sillä $h_1 = 1$, josta seuraa $0 = 1^p - e_p(h_1, \ldots, h_p)$. Täten luvut $h_1, \ldots, h_p \in \mathbb{C}$ ovat jokin permutaatio ykkösenjuurista $1, \xi, \ldots, \xi^{p-1}$, jossa $\xi = e^{2\pi i/p}$.

Koska laatan alkiot $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p-1}$ generoivat ryhmän $\mathbb{Z}^n$, niin tällöin jokainen $x_1, x_2, \ldots, x_n$ voidaan esittää monomien $m_1, m_2, \ldots, m_p$ potenssien tuloina. Toisin sanoen kaikille x_i saadaan jokin kaava $x_i = m_1^{a_{i,1}} \cdot m_2^{a_{i,2}} \cdots m_p^{a_{i,p}}$. Täten luku $y_i = h_1^{a_{i,1}} \cdot h_2^{a_{i,2}} \cdots h_p^{a_{i,p}}$, eli y_i on ykkösenjuurien tulo ja siten myös ykkösenjuuri. Siis on sellaiset $b_i \in \mathbb{Z}$, että $y_i = \xi^{b_i}$ jokaisella i. Koska luvut $h_1, h_2, \ldots, h_p$ ovat permutaatio luvuista $1, \xi, \ldots, \xi^{p-1}$, niin tästä seuraa, että homomorfismi

$$\phi : \mathbb{Z}^n \to \mathbb{Z}/p\mathbb{Z},\ \phi(z_1, z_2, \ldots, z_n) = b_1 z_1 + b_2 z_2 + \cdots + b_n z_n$$

on joukon D rajoittumassa bijektio. Nimittäin laatan vektoreilla $\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p-1}$ arvo $\xi^{\phi(\boldsymbol{v}_i)}$ on ykkösenjuuri h_{i+1}. □

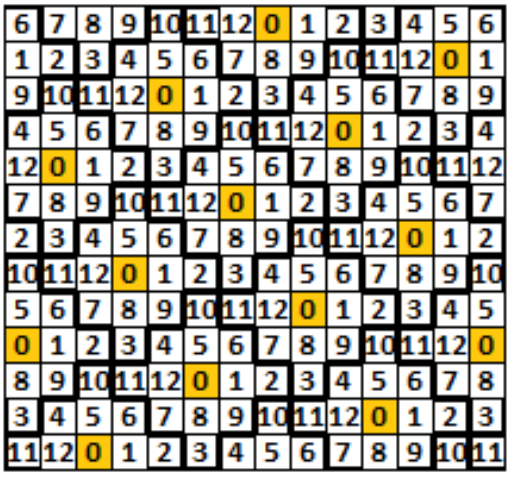
Koska Lee-pallossa on mukana jokainen luonnollisen kannan alkio $\boldsymbol{e}_i$, $i \in \{1, \ldots, n\}$, niin se generoi Abelin ryhmän $\mathbb{Z}^n$. Jos siis Lee-pallo on alkuluvun kokoinen, niin Lauseen 47 perusteella kaikki laatoitukset ovat periodisia ja Lauseen 51 perusteella ainakin osa laatoituksista on ristikollisia.

Seuraus 52. *Olkoon $n, e \geq 1$ ja $|S(n,e)| = p$ alkuluku. Tällöin jokainen $PL(n,e)$-koodi on vahvasti p-periodinen. Lisäksi, on olemassa $PL(n,e)$-koodi jos ja vain jos on olemassa lineaarinen $PL(n,e)$-koodi*

Todistus. Lauseen 47 mukaan $\mathrm{PL}(n,e)$-koodi on p-periodinen jokaiseen suuntaan, eli vahvasti p-periodinen. Lisäksi $\mathbf{0} \in \mathrm{S}(n,e)$ ja Lee-pallo generoi koko avaruuden $\mathbb{Z}^n$, sillä avaruuden $\mathbb{Z}^n$ luonnollinen kanta $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ kuuluu joukkoon $\mathrm{S}(n,e)$. □

Lähteessä [15] osoitetaan, että kaksisäteisellä Lee-pallolla ei ole olemassa ristikollista laatoitusta, ja täten Golomb-Welch konjektuuri pätee Lee-koodeille $\mathrm{PL}(n,2)$, kun $|S(n,2)| = 2n^2 + 2n + 1$ on alkuluku. Todistus on jaettu kolmeen tapaukseen: ulottuvuuden n kolmen jakojäännöksille osoitetaan erikseen, ettei ristikollista laatoitusta ole. Ohitetaan todistus sen pituuden vuoksi. Useimmissa todistuksissa tapaus $S(n,2)$ on osoittautunut tärkeimmäksi, joten tulos luo hyvää pohjaa Golomb-Welch konjektuurille. Kuitenkaan ei tiedetä, onko $2n^2+2n+1$ alkuluku äärettömän monella kokonaisluvulla n.

Lause 53. *Olkoon $n \geq 3$. Tällöin ei ole olemassa ristikollista laatoitusta kaksisäteisellä Lee-palloilla $S(n,2)$. Lisäksi jos kaksisäteisen Lee-pallon koko $|S(n,2)| = 2n^2 + 2n + 1$ on alkuluku, niin tällöin ei ole olemassa laatoitusta kaksisäteisellä Lee-pallolla.*



Kuva 5: Esimerkin 54 homomorfismi $\phi : \mathbb{Z}^2 \to \mathbb{Z}_{13}$. Konfiguraation $c = \phi^{-1}(0)$ pisteet ovat keltaisella.

Esimerkki 54. Osoitetaan, että laatalla $S(2,2)$ on olemassa ristikollinen konfiguraatio sopivalla homomorfismilla. Seurauksen 52 perusteella riittää löytää homomorfismi $\mathbb{Z}^n \to G$, jonka restriktio $S(n,e) \to G$ on bijektio. Koska laatan koko $|S(2,2)| = 13$ on alkuluku, niin joukoksi G kelpaa joukko $\mathbb{Z}_{13}$. Olkoon ϕ :

$\mathbb{Z}^2 \to \mathbb{Z}_{13}$, $\phi(x,y) = x + 5y \pmod{13}$. Nyt funktio ϕ on homomorfismi ja sen restriktio $S(2,2) \to \mathbb{Z}_{13}$ on bijektio. Kyseinen konfiguraatio on homomorfismin ydin $\mathrm{Supp}(f_c) = \mathrm{Ker}(\phi)$.

Lause 51 luo pohjaa seuraavalle konjektuurille:

Konjektuuri 55. *Olkoon $D = \{\boldsymbol{v}_0 = \mathbf{0}, \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p-1}\}$ laatta, jonka koko $|D| = p$ on alkuluku ja vektorit $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p-1}$ sellaisia, että ne generoivat Abelin ryhmän $\mathbb{Z}^n$ yhteenlaskun suhteen. Tällöin kaikki konfiguraatiot, jotka laatoittavat avaruuden $\mathbb{Z}^n$ laatoilla D, ovat ristikollisia.*

Seuraavaksi saadaan tulos, että konjektuuria ratkaistaessa voi tarkastella tietynlaista kappaletta.

Lause 56. *Olkoon p jokin alkuluku ja $D_{p-1} = \{\mathbf{0}, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{p-1}\}$ semiristilaatta. Jos jokainen avaruuden $\mathbb{Z}^{p-1}$ laatoitus semiristeillä D_{p-1} on ristikollinen, niin tällöin jokainen avaruuden $\mathbb{Z}^n$ laatoitus laatalla $D = \{\mathbf{0}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{p-1}\}$, jossa vektorit $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p-1}\}$ generoivat avaruuden $\mathbb{Z}^n$, on ristikollinen.*

Todistus. Olkoon c konfiguraatio, joka laatoittaa avaruuden $\mathbb{Z}^n$ laatoilla D. Näytetään, että konfiguraatiolla c voidaan muodostaa konfiguraatio c_0, joka laatoittaa avaruuden $\mathbb{Z}^{p-1}$ semiristeillä D_{p-1}.

Olkoon $\phi : \mathbb{Z}^{p-1} \to \mathbb{Z}^n$ se homomorfismi, jolla

$$(x_1, x_2, \ldots, x_{p-1}) \mapsto \sum_{i=1}^{p-1} x_i \boldsymbol{v}_i.$$

Koska vektorit $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{p-1}\}$ generoivat avaruuden $\mathbb{Z}^n$, niin homomorfismi ϕ on surjektiivinen. Olkoon c_0 konfiguraatio, jolla

$$\mathrm{Supp}(c_0) = \phi^{-1}(\mathrm{Supp}(c)).$$

Koska tarkalleen yksi vektori joukosta $\{\boldsymbol{x}, \boldsymbol{x} + \boldsymbol{v}_1, \ldots, \boldsymbol{x} + \boldsymbol{v}_{p-1}\}$ kuuluu joukkoon $\mathrm{Supp}(c)$ kaikilla $\boldsymbol{x} \in \mathbb{Z}^n$, niin vain yksi vektori joukosta $\{\boldsymbol{x}, \boldsymbol{x} + \boldsymbol{e}_1, \ldots, \boldsymbol{x} + \boldsymbol{e}_{p-1}\}$ kuuluu joukkoon $\mathrm{Supp}(c_0)$ kaikilla $\boldsymbol{x} \in \mathbb{Z}^{p-1}$. Täten konfiguraatio c_0 on avaruuden $\mathbb{Z}^{p-1}$ laatoitus semiristeillä, ja siten c_0 on ristikollinen.

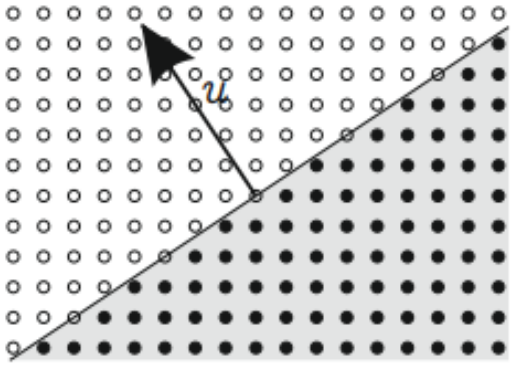
Koska homomorfismi ϕ on surjektiivinen, niin $\phi(\mathrm{Supp}(c_0)) = \mathrm{Supp}(c)$. Koska $\mathrm{Supp}(c_0)$ on ryhmän $\mathbb{Z}^{p-1}$ aliryhmä, niin myös $\mathrm{Supp}(c)$ on ryhmän $\mathbb{Z}^n$ aliryhmä. Täten konfiguraatio c on ristikollinen. □

Lisää tietoa konjektuurista ja siihen liittyvistä lauseista löytyy artikkelin [6] kappaleesta 5.

4.3 Säikeet

Kappaleen lähteenä toimii [2].

Olkoon $\boldsymbol{u} \in \mathbb{R}^n$ jokin nollasta eroava vektori ja $H_{\boldsymbol{u}} = \{\boldsymbol{v} \in \mathbb{Z}^n \mid \langle \boldsymbol{v}, \boldsymbol{u} \rangle < 0\}$ avoin diskreetti puoliavaruus suuntaan $\boldsymbol{u}$. Merkinnällä $\langle \boldsymbol{v}, \boldsymbol{u} \rangle$ tarkoitetaan sisätuloa. Siirtoaliavaruus X on deterministinen suuntaan $\boldsymbol{u}$, jos kaikilla $c, c' \in X$ pätee



Kuva 6: Värjätyt pisteet kuuluvat avoimeen 2-ulotteiseen diskreettiin puoliavaruuteen $H_{\boldsymbol{u}}$ [2].

$c \restriction_{H_{\boldsymbol{u}}} = c' \restriction_{H_{\boldsymbol{u}}} \Rightarrow c = c'$, eli puoliavaruuden $H_{\boldsymbol{u}}$ sisältö yksikäsitteisesti määrittää konfiguraation sisällön koko avaruudelle $\mathbb{Z}^n$. Deterministisyyttä ja pian määriteltyä ekspansiivisuutta voidaan käyttää tutkittaessa, onko jokin siirtoaliavaruus X äärellinen eli vahvasti periodinen.

Joukko $A \subseteq \mathbb{Z}^n$ *koodaa* joukon $B \subseteq \mathbb{Z}^n$ siirtoaliavaruudessa X, jos kaikilla $c, c' \in X$ pätee $c \restriction A = c' \restriction A \Rightarrow c \restriction B = c' \restriction B$. Todistetaan seuraavaksi, että jos jokin joukko $A \subseteq \mathbb{Z}^n$ koodaa pisteen $\boldsymbol{t} \in \mathbb{Z}^n$, niin tällöin on olemassa jokin äärellinen joukko $A_0 \subseteq A$, joka koodaa pisteen $\boldsymbol{t}$ [7].

Lemma 57. *Olkoon X jokin n-ulotteinen siirtoaliavaruus ja $A \subseteq \mathbb{Z}^n$. Jos jollain $\boldsymbol{t} \in \mathbb{Z}^n$ ja kaikilla $c, c' \in X$ pätee $c \restriction_A = c' \restriction_A \Rightarrow c_{\boldsymbol{t}} = c'_{\boldsymbol{t}}$, niin on olemassa jokin äärellinen joukko $A_0 \subseteq A$, jolla pätee $c \restriction_{A_0} = c' \restriction_{A_0} \Rightarrow c_{\boldsymbol{t}} = c'_{\boldsymbol{t}}$:*

Todistus. Tehdään vastaoletus: ei ole olemassa äärellistä joukkoa A_0. Valitaan jokaista $m \geq 0$ kohti sellaiset konfiguraatiot $x_m, y_m \in X$, että $x_m(\boldsymbol{t}) \neq y_m(\boldsymbol{t})$, mutta $x_m(\boldsymbol{v}) = y_m(\boldsymbol{v})$ kaikilla $\boldsymbol{v} \in A$, joilla $|\boldsymbol{v}| \leq m$. Koska X on kompakti, niin jokin osajono $x_{m_1}, x_{m_2}, x_{m_3}, \ldots$ suppenee kohti jotain konfiguraatiota $x' \in X$. Samoin $y_{m_1}, y_{m_2}, y_{m_3}, \ldots$ suppenee kohti jotain konfiguraatiota $y' \in X$. Nyt $x'(\boldsymbol{t}) \neq y'(\boldsymbol{t})$, mutta $x'(\boldsymbol{v}) = y'(\boldsymbol{v})$ kaikilla $\boldsymbol{v} \in A$, mikä on ristiriita. □

Nyt edellisen lemman perusteella saadaan helposti, että jos puoliavaruus $H_{\boldsymbol{u}}$ koodaa jonkin pisteen sen ulkopuolelta, niin se koodaa koko avaruuden $\mathbb{Z}^n$.

Lemma 58. *Olkoon X jokin n-ulotteinen siirtoaliavaruus ja $\boldsymbol{u} \in \mathbb{R}^n, \boldsymbol{u} \neq \boldsymbol{0}$. Jos jollain $\boldsymbol{t} \in \mathbb{Z}^n \setminus H_{\boldsymbol{u}}$ ja kaikilla $c, c' \in X$ pätee $c \restriction_{H_{\boldsymbol{u}}} = c' \restriction_{H_{\boldsymbol{u}}} \Rightarrow c_{\boldsymbol{t}} = c'_{\boldsymbol{t}}$, niin tällöin kaikilla $c, c' \in X$ pätee $c \restriction_{H_{\boldsymbol{u}}} = c' \restriction_{H_{\boldsymbol{u}}} \Rightarrow c = c'$, eli X on deterministinen suuntaan $\boldsymbol{u}$.*

Todistus. Olkoon $\boldsymbol{v} \in \mathbb{Z}^n$ mielivaltainen alkio ja $A_0 \subset H_{\boldsymbol{u}}$ äärellinen joukko, joka koodaa pisteen $\boldsymbol{t} \in \mathbb{Z}^n \setminus H_{\boldsymbol{u}}$.

Jos $\langle \boldsymbol{v}, \boldsymbol{u} \rangle \leq \langle \boldsymbol{t}, \boldsymbol{u} \rangle$, niin

$$c \restriction_{H_{\boldsymbol{u}}} = c' \restriction_{H_{\boldsymbol{u}}} \Rightarrow \tau_{\boldsymbol{t}-\boldsymbol{v}}(c) \restriction_{H_{\boldsymbol{u}}} = \tau_{\boldsymbol{t}-\boldsymbol{v}}(c') \restriction_{H_{\boldsymbol{u}}} \Rightarrow \tau_{\boldsymbol{t}-\boldsymbol{v}}(c)_{\boldsymbol{t}} = \tau_{\boldsymbol{t}-\boldsymbol{v}}(c')_{\boldsymbol{t}} \Rightarrow c_{\boldsymbol{v}} = c'_{\boldsymbol{v}}.$$

Jos $\langle \boldsymbol{v}, \boldsymbol{u} \rangle > \langle \boldsymbol{t}, \boldsymbol{u} \rangle$, niin $c_{\boldsymbol{v}} = c'_{\boldsymbol{v}}$ jos $c \restriction_{\tau_{\boldsymbol{t}-\boldsymbol{v}}(A_0)} = c' \restriction_{\tau_{\boldsymbol{t}-\boldsymbol{v}}(A_0)}$. Jos $\langle \boldsymbol{a}, \boldsymbol{u} \rangle \geq 0$ jollain $\boldsymbol{a} \in \tau_{\boldsymbol{t}-\boldsymbol{v}}(A_0)$, niin selvitetään alkiot $\tau_{\boldsymbol{t}-\boldsymbol{v}}(A_0)$. Koska A_0 on äärellinen ja $A_0 \subset H_{\boldsymbol{u}}$,

niin jollain $m \in \mathbb{R}_+$ pätee $\langle \boldsymbol{a}, \boldsymbol{u} \rangle \leq -m$ kaikilla $\boldsymbol{a} \in A_0$. Siis $\langle \boldsymbol{v}, \boldsymbol{u} \rangle / m$ askeleen jälkeen kaikki selvitettävät alkiot kuuluvat puoliavaruuteen $H_{\boldsymbol{u}}$, jolloin $c_{\boldsymbol{v}} = c'_{\boldsymbol{v}}$.

Koska $\boldsymbol{v} \in \mathbb{Z}^n$ oli mielivaltainen, niin $c = c'$. □

Nyt seuraavassa lemmassa riittää tarkastella vain, että puoliavaruus koodaa pisteen $\mathbf{0}$.

Lemma 59. *Olkoot X jokin n-ulotteinen siirtoaliavaruus, Laurentin polynomi $f \in Per(X)$ sellainen, että $\mathbf{0} \in Supp(f)$ ja $\boldsymbol{u} \in \mathbb{R}^n$ jokin sellainen nollasta eroava vektori, että $-Supp(f) \setminus \{\mathbf{0}\} \subset \boldsymbol{H_u}$. Tällöin X on deterministinen suuntaan u.*

Todistus. Olkoon $c, c' \in X$ sellaiset konfiguraatiot, että $c \upharpoonright_{H_{\boldsymbol{u}}} = c' \upharpoonright_{H_{\boldsymbol{u}}}$. Koska $f(\boldsymbol{x})$ periodisoi konfiguraatiot c ja c', niin on olemassa sellainen $\boldsymbol{t} \in -H_{\boldsymbol{u}}$, että $\boldsymbol{t}$ on konfiguraatioiden $f \cdot c$ ja $f \cdot c'$ yhteinen periodi. Olkoon $g(\boldsymbol{x}) = f(\boldsymbol{x}) \cdot (\boldsymbol{x}^{\boldsymbol{t}} - 1)$, jolloin $g(\boldsymbol{x}) \in \mathrm{Ann}(c)$, $g(\boldsymbol{x}) \in \mathrm{Ann}(c')$ ja yhä $-\mathrm{Supp}(g) \setminus \{\mathbf{0}\} \subset H_{\boldsymbol{u}}$. Nyt saadaan

$$0 = (gc)_{\mathbf{0}} - (gc')_{\mathbf{0}} = \sum_{\boldsymbol{v} \in \mathrm{Supp(g)}} g_{\boldsymbol{v}} c_{-\boldsymbol{v}} - \sum_{\boldsymbol{v} \in \mathrm{Supp(g)}} g_{\boldsymbol{v}} c'_{-\boldsymbol{v}}.$$

Kun $\boldsymbol{v} \neq \mathbf{0}$, niin $-\boldsymbol{v} \in H_{\boldsymbol{u}}$, jolloin $c_{-\boldsymbol{v}} = c'_{-\boldsymbol{v}}$. Saadaan

$$\sum_{\boldsymbol{v} \in \mathrm{Supp(g)} \setminus \{\mathbf{0}\}} g_{\boldsymbol{v}} c_{-\boldsymbol{v}} = \sum_{\boldsymbol{v} \in \mathrm{Supp(g)} \setminus \{\mathbf{0}\}} g_{\boldsymbol{v}} c'_{-\boldsymbol{v}},$$

ja yhdistämällä edellä olevat yhtälöt saadaan

$$g_{\mathbf{0}} c_{\mathbf{0}} - g_{\mathbf{0}} c'_{\mathbf{0}} = 0.$$

Nyt jakamalla yhtälön molemmat puolet luvulla $g_{\mathbf{0}} \neq 0$ saadaan $c_{\mathbf{0}} = c'_{\mathbf{0}}$. Edellisen lemman perusteella $c = c'$, ja siten X on deterministinen suuntaan $\boldsymbol{u}$. □

Kun siirtoaliavaruus on deterministinen suuntaan $\boldsymbol{u}$ ja $-\boldsymbol{u}$, niin $(n-1)$-ulotteinen aliavaruus $S = \langle \boldsymbol{u} \rangle^{\perp} = \{\boldsymbol{v} \in \mathbb{R}^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0\}$ on *ekspansiivinen* siirtoaliavaruudelle X. Muuten se on *epäekspansiivinen*. Lemman 57 perusteella konfiguraation sisältö rajallisella etäisyydellä ekspansiivisesta avaruudesta määrittää yksikäsitteisesti koko konfiguraation. Toisin sanoen on olemassa jokin $\delta > 0$ siten, että kaikilla $c, c' \in X$ pätee

$$c \upharpoonright B = c' \upharpoonright B \Rightarrow c = c',$$

jossa $B = \{\boldsymbol{v} \in \mathbb{Z}^n \mid |\langle \boldsymbol{v}, \boldsymbol{u} \rangle| < \delta\}$.

Lause 60. *[17] Siirtoaliavaruus, joka on deterministinen jokaiseen suuntaan, on äärellinen ja siten sisältää vain vahvasti periodisia konfiguraatioita.*

Todistetaan seuraavaksi, että Lausesta 27 saatavalla Laurentin polynomilla $f(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in \mathrm{Ann}(X)$ voidaan näyttää lineaarisen aliavaruuden $\langle \boldsymbol{u} \rangle^{\perp}$ olevan ekspansiivinen, jos $\langle \boldsymbol{u}, \boldsymbol{t}_i \rangle \neq 0$ kaikilla $i \in \{1, \ldots, m\}$.

Lemma 61. *Olkoon X jokin n-ulotteinen siirtoaliavaruus ja olkoon $f(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in Ann(X)$. Olkoon $S \subset \mathbb{R}^n$ jokin $(n-1)$-ulotteinen lineaarinen aliavaruus. Jos $\boldsymbol{t}_i \notin S$ kaikilla $i \in \{1, \ldots, m\}$, niin S on ekspansiivinen siirtoaliavaruudelle X.*

Todistus. Olkoon $\boldsymbol{u} \in \mathbb{R}^n$ sellainen, että $S = \langle \boldsymbol{u} \rangle^\perp$. Koska $\boldsymbol{x}^{\boldsymbol{t}} - 1 = -\boldsymbol{x}^{\boldsymbol{t}}(\boldsymbol{x}^{-\boldsymbol{t}} - 1)$, niin vektorin $\boldsymbol{t}_i$ voi korvata vektorilla $-\boldsymbol{t}_i$ annihilaattorissa $f(\boldsymbol{x}) = (\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1)$.

Voidaan siis olettaa, että $\langle \boldsymbol{u}, \boldsymbol{t}_i \rangle > 0$ kaikilla $i \in \{1, \ldots, m\}$, sillä kaikki vektorit $\boldsymbol{t}_i$, joilla $\langle \boldsymbol{u}, \boldsymbol{t}_i \rangle < 0$ korvataan vektorilla $-\boldsymbol{t}_i$. Mutta nyt $\boldsymbol{0} \in \mathrm{Supp}(f)$ ja $-\mathrm{Supp}(f) \setminus \{\boldsymbol{0}\} \subset H_{\boldsymbol{u}}$. Nyt siis Lemman 59 perusteella siirtoaliavaruus X on deterministinen suuntaan $\boldsymbol{u}$. Mutta koska myös $S = \langle -\boldsymbol{u} \rangle^\perp$, niin X on myös deterministinen suuntaan $-\boldsymbol{u}$. Täten S on ekspansiivinen siirtoaliavaruudelle X. □

Seuraava lause on kappaleen päälause, jota käytetään myöhemmin määritellyissä S-säikeissä. Sillä saadaan riittävä ehto ekspansiivisuuteen periodisoivien polynomien avulla. Seuraavassa todistuksessa käytetään sitä tulosta lähteestä [18], että siirtoaliavaruus, jossa on vain vahvasti periodisia konfiguraatioita on äärellinen.

Lause 62. *Olkoon X jokin n-ulotteinen siirtoaliavaruus ja olkoon S avaruuden $\mathbb{R}^n$ aito lineaarinen aliavaruus. Jos $f \in Per(X)$ on sellainen, että*

$$Supp(f) \cap S = \{\boldsymbol{0}\},$$

niin on olemassa pareittain lineaarisesti riippumattomat $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_m \in \mathbb{Z}^n$ siten, että $\boldsymbol{t}_i \notin S$ kaikilla $i \in \{1, \ldots, m\}$ ja $(\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1) \in Ann(X)$. Erityisesti jos S on $(n-1)$ ulotteinen, niin S on ekspansiivinen siirtoaliavaruudelle X.

Todistus. Todistetaan ensin, että on olemassa sellainen $g \in \mathrm{Ann}(X)$, jolle pätee $\mathrm{Supp}(g) \cap S = \{\boldsymbol{0}\}$. Joukko $Y = \{fc \,|\, c \in X\}$ on siirtoaliavaruus, johon kuuluu vain vahvasti periodisia konfiguraatioita, ja on siten äärellinen. Koska S on aito aliavaruus, niin on olemassa jokin yksikkökoordinaattivektori $\boldsymbol{e}_i$, joka ei sisälly avaruuteen S. Koska siirtoaliavaruus Y on äärellinen joukko vahvasti periodisia konfiguraatioita, niin niillä on jokin yhteinen periodi suuntaan $\boldsymbol{e} = \boldsymbol{e}_i$. Tämän periodin moninkerta on myös siirtoaliavaruuden Y periodi, joten on olemassa mielivaltaisen suuria kokonaislukuja k, joilla $(\boldsymbol{x}^{k\boldsymbol{e}} - 1)f(\boldsymbol{x}) \in \mathrm{Ann}(X)$. Koska $\boldsymbol{e} \notin S$, niin tarpeeksi suurella kokonaisluvulla k pätee $\mathrm{Supp}(\boldsymbol{x}^{k\boldsymbol{e}} f) \cap S = \varnothing$. Täten siis jollain $g(\boldsymbol{x}) = (\boldsymbol{x}^{k\boldsymbol{e}} - 1)f(\boldsymbol{x})$ pätee $\mathrm{Supp}(g) \cap S = \{\boldsymbol{0}\}$ ja $g \in \mathrm{Ann}(X)$.

Nyt Lauseen 27 mukaan annihilaattorilla g ja vektorilla $\boldsymbol{u} = \boldsymbol{0} \in \mathrm{Supp}(g)$ saadaan haluttu differenssiannihilaattori $(\boldsymbol{x}^{\boldsymbol{t}_1} - 1) \cdots (\boldsymbol{x}^{\boldsymbol{t}_m} - 1)$, sillä $\boldsymbol{u}_i - \boldsymbol{u} \notin S$ koska $\boldsymbol{u}_i \in \mathrm{Supp}(g) \setminus \{\boldsymbol{u}\}$. Nyt edellisen Lemman 61 avulla saadaan, että S on ekspansiivinen siirtoaliavaruudelle X. □

Edelliset lauseet suoraan antavat seuraavan yksinkertaisen seurauksen. Se demonstroi hyvin edellisen menetelmän tehokkuutta.

Seuraus 63. *Olkoon X jokin n-ulotteinen siirtoaliavaruus siten, että jokaista nollasta eroavaa $\boldsymbol{u} \in \mathbb{R}^n$ kohti on olemassa $f \in Per(X)$ ja $\boldsymbol{v} \in Supp(f)$ siten, että $\langle \boldsymbol{v}, \boldsymbol{u} \rangle \neq \langle \boldsymbol{v}', \boldsymbol{u} \rangle$ kaikilla $\boldsymbol{v}' \in Supp(f) \setminus \{\boldsymbol{v}\}$. Tällöin X on äärellinen ja siten sisältää vain vahvasti periodisia konfiguraatioita.*

Todistus. Valitaan jokaista $(n-1)$-ulotteista aliavaruutta S kohti sellainen $\boldsymbol{u} \in \mathbb{R}^n$, että $S = \langle \boldsymbol{u} \rangle^\perp$ ja olkoot f ja $\boldsymbol{v}$ kuten yllä. Nyt $\boldsymbol{x}^{-\boldsymbol{v}} f(\boldsymbol{x}) \in \mathrm{Per}(X)$ ja $\mathrm{Supp}(\boldsymbol{x}^{-\boldsymbol{v}} f(\boldsymbol{x})) \cap S = \{\boldsymbol{0}\}$. Nyt Lauseen 62 perusteella aliavaruus S on ekspansiivinen siirtoaliavaruudelle X. Koska $\boldsymbol{u}$ oli mielivaltainen, niin Lauseen 60 perusteella siirtoaliavaruus X on äärellinen ja siten sisältää vain vahvasti periodisia konfiguraatioita. □

Seuraavaksi esitellään tapa käyttää Lausetta 62 periodisoijaihanteen avulla. Koska periodisoijaihanne on suljettu yhteen- ja kertolaskun suhteen, niin periodisoijasta f voidaan yrittää löytää sellainen lineaarikombinaatio, että $\mathrm{Supp}(\boldsymbol{x}^{\boldsymbol{t}_1} f(\boldsymbol{x}) \pm \boldsymbol{x}^{\boldsymbol{t}_2} f(\boldsymbol{x}) \pm \cdots \pm \boldsymbol{x}^{\boldsymbol{t}_m} f(\boldsymbol{x})) \cap S = \{\boldsymbol{0}\}$.

Tarkemmin ottaen olkoon $S \subseteq \mathbb{R}^n$ jokin aliavaruus. Laurentin polynomia f kutsutaan *S-säikeeksi* mikäli $\mathrm{Supp}(f) \subset S$. Koska S-säikeiden joukko on suljettu tulon ja summan suhteen, niin S-säikeet muodostavat Laurentin polynomien alirenkaan. Laurentin polynomin f restriktiolla aliavaruuteen S tarkoitetaan S-säiettä

$$\sum_{\boldsymbol{u} \in \mathrm{Supp}(f) \cap S} f_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}},$$

ja sitä merkitään merkinnällä $f \restriction S$. Olkoon I jokin Laurentin polynomien ihanne. Joukko $I \restriction S$ sisältää kaikki ihanteen I alkioiden restriktiot aliavaruuteen S. Siis se sisältää kaikki $f \restriction S$, missä $f \in I$. Joukko $I \restriction S$ on myös S-säikeiden renkaan ihanne. Laurentin polynomin f kaikkien translaatioiden restriktioita aliavaruuteen S kutsutaan sen *S-säikeiksi*. Joukko sisältää siis S-säikeet $\boldsymbol{x}^{\boldsymbol{t}} f(\boldsymbol{x}) \restriction S$ yli $\boldsymbol{t} \in \mathbb{Z}^n$.

Nyt Lauseen 62 ehto $\mathrm{Supp}(f) \cap S = \{\boldsymbol{0}\}$ jollain $f \in \mathrm{Per}(X)$ tarkoittaa yksinkertaisesti sitä, että monomi $1 = f \restriction S \in \mathrm{Per}(X) \restriction S$. Tällöin $\mathrm{Per}(X) \restriction S$ on koko S-säikeiden muodostama rengas. Käytännössä tämän ehdon varmistaminen periodisoijaihanteelle $\mathrm{Per}(X)$ tehdään nollasta eroavan monomin etsimisestä periodisoijien S-säikeiden lineaarikombinaationa.

Todistetaan seuraavaksi S-säikeillä, että Lee-pallon $S(3,2)$ muodostama siirtoaliavaruus $T_{S(3,2)}$ on vahvasti periodinen. Jaetaan todistus kolmeen esimerkkiin: ensimmäisessä todistetään kaikille Lee-palloille pätevä ominaisuus, toisessa todistetaan kaksisäteiselle Lee-pallolle jokin ominaisuus ja viimeisessä esimerkissä todistetaan vielä loput tarvittavat ominaisuudet Lee-pallolle $S(3,2)$. Ensimmäisessä esimerkissä Lee-pallon $S(n,e)$ pisteet $\pm e \cdot \boldsymbol{e}_i$ antavat yksistään monta S-säiettä, johon kuuluu vain monomi $\boldsymbol{x}^{\pm e \cdot \boldsymbol{e}_i}$:

Esimerkki 64. Todistetaan, että $\mathrm{PL}(n,e)$-koodit, joissa $n \geq 2$ ja $e \geq 1$ ovat deterministisiä suuntaan $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{R}^n$, kun jollain $k \in \{1, 2, \ldots, n\}$ pätee $|u_k| > |u_j|$ kaikilla $j \in \{1, \ldots, n\}$ ja $j \neq k$.

Koska Lee-pallo on symmetrinen akselien $\boldsymbol{e}_i$ suhteen, niin voidaan olettaa, että $u_i \geq 0$ kaikilla $i \in \{1, 2, \ldots, n\}$ ja voidaan myös olettaa, että $k = 1$. Koska $\langle \boldsymbol{u} \rangle^\perp = \langle a \cdot \boldsymbol{u} \rangle^\perp$, missä $a \in \mathbb{R} \setminus \{\boldsymbol{0}\}$, niin voidaan olettaa, että $u_1 = 1$ ja $0 \leq u_i < 1$, kun $i \in \{2, \ldots, n\}$.

Nyt $e \cdot \boldsymbol{e}_1$ on ainoa Lee-pallon $S(n,e)$ piste, jolla $\langle \boldsymbol{u}, e \cdot \boldsymbol{e}_1 \rangle = e$. Nimittäin olkoon $\boldsymbol{v} \in S(n,e)$ jokin muu piste kuin $e \cdot \boldsymbol{e}_1$. Tällöin

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1 \cdot v_1 + u_2 v_2 + \cdots + u_n v_n < |v_1| + |v_2| + \cdots + |v_n| \leq e$$

Lee-pallon määritelmän perusteella. Tasolle $\langle \boldsymbol{u} \rangle^\perp - e$ kuuluu siis vain yksi piste Lee-pallosta $S(n,e)$, joten $\mathrm{PL}(n,e)$-koodit ovat deterministisiä suuntaan $\boldsymbol{u}$.

Näytetään, että Lee-pallo $S(n,2)$ on deterministinen suuntaan $\boldsymbol{u} = (1, 1, \ldots, 1)$ kun $n \geq 2$:

Esimerkki 65. Olkoot $\boldsymbol{u} = (1, 1, \ldots, 1)$, ja $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, ja olkoon S hypertaso $\langle \boldsymbol{u} \rangle^\perp$. Huomaa, että Lee-pallon $S(n, e)$ eräs $(n-1)$-ulotteinen sivutahko on samansuuntainen kuin hypertaso S ja $\langle \boldsymbol{u}, \boldsymbol{v} \rangle^\perp = e$ taltioi sen uloimman osan. Tässä esimerkissä kuitenkin tarvitaan vain sisempiä osia. Lee-pallosta $S(n, 2)$ saadaan erityisesti S-säikeet

$$f(\boldsymbol{x}) = 1 + \sum_{\substack{1 \le i,j \le n \\ i \ne j}} x_i x_j^{-1}, \text{ ja}$$

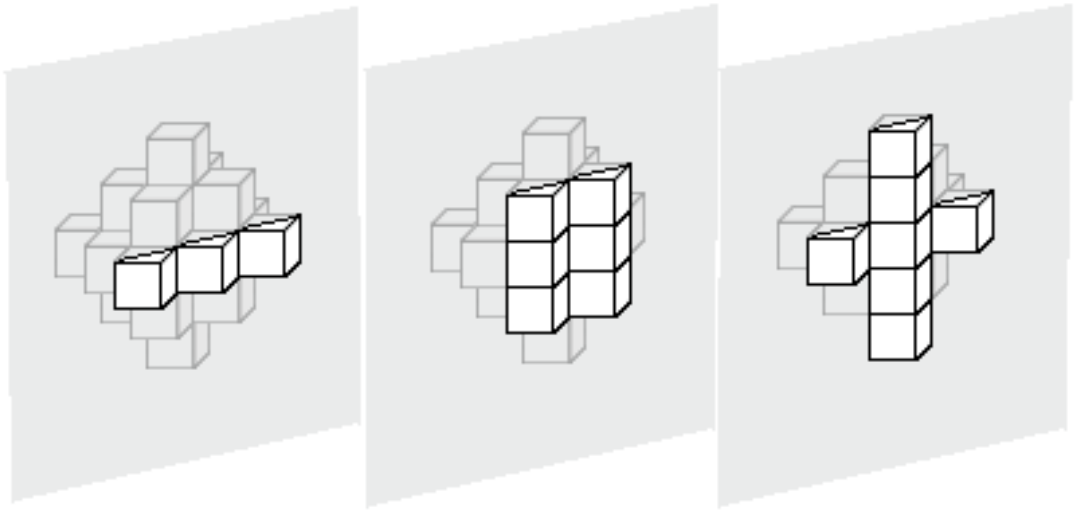
$$g(\boldsymbol{x}) = \sum_{1 \le i \le n} x_i,$$

jotka ovat vastaavasti tasoilla $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$ ja $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$. Näistä saadaan S-säie

$$(x_1^{-1} + x_2^{-1} + \cdots + x_n^{-1}) g(\boldsymbol{x}) - f(\boldsymbol{x}) = (n-1),$$

joka on nollasta eroava monomi.

Osoitetaan, että PL$(3, 2)$-koodit ovat periodisia. On todistettu, että PL$(3, 2)$-koodeja ei ole olemassa, mutta koska tässä tutkielmassa sallitaan siirtoaliavaruuden olevan tyhjä joukko, niin silloin tämä tyhjä joukko täyttää periodisuuden määritelmän. Edellisissä esimerkeissä todistettiin vektorin $\boldsymbol{u}$ tapaukset $(1, 1, 1)$ ja $(1, a, b)$, jossa $0 \le a, b < 1$, joten jäljelle jää vain todistettavaksi tapaus $(1, 1, c)$, jossa $0 \le c < 1$.



Kuva 7: Esimerkin 66 tapaus $\boldsymbol{u} = (1, 1, 0)$.

Esimerkki 66. Olkoot $\boldsymbol{x} = (x, y, z) \in \mathbb{Z}^3$ ja taso $S = \langle \boldsymbol{u} \rangle^\perp$. Oletetaan, että vektorilla $\boldsymbol{u} = (u_1, u_2, u_3)$ pätee $u_1 = u_2 = 1$ sekä $0 \le u_3 < 1$. Olkoon u_3 ensin erisuuri kuin $\frac{1}{2}$ tai 0. Tällöin on helppo osoittaa, että Lee-pallo $S(3, 2)$ on deterministinen suuntaan $\boldsymbol{u}$ ratkaisemalla yhtälö $1 \cdot x + 1 \cdot y + u_3 \cdot z = u_3$, jossa $0 \le |x| + |y| + |z| \le 2$.

Nimittäin tällä yhtälöllä on vain yksi ratkaisu $(0,0,1)$, joten tasolla $\langle \boldsymbol{u} \rangle^{\perp} - u_3$ on vain yksi piste Lee-pallosta $S(3,2)$.

Olkoon seuraavaksi $u_3 = 0$. Tällöin Laurentin polynomilla $f_{S(3,2)}$ on erityisesti S-säikeet

$$\begin{aligned} f(\boldsymbol{x}) &= x^{-1}y + xy^{-1} + z^{-2} + z^{-1} + 1 + z + z^2, \\ g(\boldsymbol{x}) &= xz^{-1} + x + xz + yz^{-1} + y + yz, \\ h(\boldsymbol{x}) &= x^2 + xy + y^2, \end{aligned}$$

jotka ovat tasoilla $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 0$, $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 1$ ja $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 2$ vastaavasti. Muodostetaan uusi S-säie

$$k(\boldsymbol{x}) = x^{-2}(z^{-1} + 1 + z)h(\boldsymbol{x}) - x^{-2}yg(\boldsymbol{x}) = z^{-1} + 1 + z.$$

Nyt

$$f(\boldsymbol{x}) = x^{-1}y^{-1}h(\boldsymbol{x}) - (z + z^{-1})k(\boldsymbol{x}) = -2,$$

joten nollasta eroava monomi kuuluu S-säikeisiin ja siten Lee-pallo $S(3,2)$ on deterministinen suuntaan $\boldsymbol{u}$.

Olkoon viimeiseksi vielä $u_3 = \frac{1}{2}$. Nyt saadaan tasoja $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = 2$ ja $\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \frac{3}{2}$ vastaavat S-säikeet

$$\begin{aligned} f(\boldsymbol{x}) &= x^2 + xy + y^2, \\ g(\boldsymbol{x}) &= xz + yz \end{aligned}$$

ja

$$f(\boldsymbol{x}) - xz^{-1}g(\boldsymbol{x}) = y^2,$$

joten nollasta eroava monomi kuuluu S-säikeisiin.

Lee-pallon $S(3,2)$ muodostama siirtoaliavaruus on siis deterministinen jokaiseen suuntaan ja siten vahvasti periodinen.

Huomautus 67. Olkoot $x_1, x_2, \ldots, x_n$ kokonaislukumuuttujia ja olkoon q sellainen reaaliluku, että yhtälöllä $x_1 + x_2 q = q$, jossa $0 \leq \sum_{i=1}^{2} |x_i| \leq 2$, on vain yksi ratkaisu muuttujilla x_1 ja x_2. Tällöin yhtälöllä $x_1 + \cdots + x_{n-1} + x_n q = q$, jossa $0 \leq \sum_{i=1}^{n} |x_i| \leq 2$, on vain yksi ratkaisu muuttujilla $x_1, x_2, \ldots, x_n$. Samalla siis saatiin todistettua, että kun $n > 3$, niin Lee-pallo $S(n,2)$ on deterministinen suuntaan $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, kun $u_1 = \cdots = u_{n-1} = 1$ ja $u_n \neq 0$, sekä $u_n \neq \frac{1}{2}$. Nämä erikoistapaukset jäävät erikseen todistettaviksi.

Vielä on jäljellä tutkittavana voiko S-säikeillä todistaa Lee-pallojen $S(n,2)$ vahvan periodisuuden. Mikäli tämä osoittautuisi todeksi, niin tämä todistaisi Golomb-Welch konjektuurit ekvivalenteiksi säteellä 2. Lauseen 53 perusteella ei kuitenkaan ole olemassa ristikollista laatoitusta säteellä 2, mikä on vahvempi muoto vahvasta periodisuudesta. Mikäli vielä tämän lisäksi todistettaisiin, että säteen 2 periodiset laatoitukset implikoisivat ristikollisia laatoituksia, niin Golomb-Welch konjektuuri pitäisi paikkansa säteellä 2.

4.4 Ylärajoja

Tässä kappaleessa esitellään lyhyesti ylärajoja ilman todistuksia. Kiinnostunut lukija voi katsoa lisätietoa alla annetuista lähteistä. Golomb ja Welch näyttivät konjektuurin tueksi, että ei ole olemassa PL$(3,2)$-koodia, ja että jokaista $n \geq 3$ kohti on olemassa jokin sellainen yläraja e_n, että PL(n,e)-koodeja ei ole olemassa, kun $e > e_n$.

Lause 68. *[13] Olkoon $n \geq 3$. On olemassa jokin luku e_n siten, että ei ole olemassa $PL(n,e)$-koodia kun $e > e_n$.*

Esitellään seuraavaksi Post'n raja ja sen jälkeen Lepistön raja PL(n,e,q)-koodeille:

Lause 69. *[19] Olkoon $n, e, q \in \mathbb{N}$ sellaiset, että $n \geq 6, e \geq \frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2}$ ja $q \geq 2e+1$. Tällöin ei ole olemassa $PL(n,e,q)$-koodia*

Lause 70. *[14] Olkoon $n, e, q \in \mathbb{N}$ sellaiset, että $n < (e+2)^2/2.1$, $e \geq 285$ ja $q \geq 2e+1$. Tällöin ei ole olemassa $PL(n,e,q)$-koodia.*

Teoksessa [1] esiteltiin yläraja täydellisille Lee-koodeille käyttäen *lineaarista optimointia*:

Lause 71. *[1] Olkoon $e \geq 18$ ja $3e+21 \leq n \leq \frac{1}{2}e^2 - 20$. Tällöin ei ole olemassa $PL(n,e)$-koodia.*

Post'n ja Lepistön rajat voidaan todistaa pätevän myös PL(n,e)-koodeille. Nämä kolme edellistä rajaa yhdistämällä saadaan seuraavanlainen raja täydellisille Lee-koodeille:

Lause 72. *[1] Ei ole olemassa $PL(n,e)$-koodia, kun n ja e toteuttavat jonkin seuraavista neljästä ehdosta:*

- $3 \leq n \leq 74$ *ja* $\max\left\{\frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2}, 2\right\} \leq e$, *tai*
- $75 \leq n \leq 405$ *ja* $\max\left\{18, \sqrt{2n+40}\right\} \leq e \leq \frac{n-21}{3}$ *tai* $\frac{\sqrt{2}}{2}n - \frac{3}{4}\sqrt{2} - \frac{1}{2} \leq e$, *tai*
- $406 \leq n \leq 876$ *ja* $\sqrt{2n+40} \leq e \leq \frac{n-21}{3}$ *tai* $285 \leq e$, *tai*
- $876 \leq n$ *ja* $\sqrt{2n+40} \leq e$.

5 Yhteenveto

Welch-Golomb konjektuuria ei vielä ole ratkaistu monista tutkimuksista huolimatta. Tässä tutkielmassa perehdyttiin algebrallisiin tapoihin lähestyä konjektuuria.

Polynomisella menetelmällä saatiin selville "räjähtäneiden" laattojen yhteys laatoituksiin ja millaisia rajoituksia tästä saadaan pääteltyä. Myös välttämätön ehto algebrallisen laatan nollakohdille esiteltiin. Tästä edettiin alkulukujen kokoisiin laattoihin ja niiden yhteydestä periodisuuteen ja ristikolliseen laatoitukseen.

S-säikeillä tutkittiin deterministisyyttä laatan periodisoijaihanteen avulla ja esimerkeillä näytettiin sen sovellusmahdollisuuksia. Muun muassa siirtolaatoitus Leepallolla $S(3, 2)$ on aina vahvasti periodinen. Myös ylärajoja esiteltiin lyhyesti.

Viitteet

[1] P. Horak, D. Kim, (2018). 50 Years of the Golomb–Welch Conjecture. IEEE Transactions on Information Theory, vol. 64, no. 4, pp. 3048-3061.

[2] J. Kari, (2023). Expansivity and Periodicity in Algebraic Subshifts. Theory of Computing Systems, vol. 67, pp. 976–994.

[3] R. Greenfeld, T. Tao, (2022). A counterexample to the periodic tiling conjecture. https://arxiv.org/abs/2211.15847

[4] J. Kari, M. Szabados, (2015). An Algebraic Geometric Approach to Nivat's Conjecture. In: M. Halldórsson, K. Iwama, N. Kobayashi, B. Speckmann (eds) Automata, Languages, and Programming. ICALP 2015. Lecture Notes in Computer Science, vol. 9135, pp. 273–285. Springer, Berlin, Heidelberg.

[5] J. Kari, M. Szabados, (2020). An Algebraic Geometric Approach to Nivat's Conjecture. Information and Computation, vol. 271, article 104481.

[6] P. Horak, D. Kim, (2018). Polynomial Method in Tilings. https://arxiv.org/pdf/1603.00051.pdf

[7] J. Franks, B. Kra, (2020). Polygonal Z2-subshifts. Proceedings of the London Mathematical Society, vol. 121, no. 2, pp. 252-286.

[8] J. Kari, (2021). Tilings and Patterns, lecture notes. Turun yliopisto.

[9] K. Ylinen, (2011). Topologian perusteet, lecture notes. Turun yliopisto.

[10] M. Koppinen, (2006). Algebran peruskurssi I, lecture notes. Turun yliopisto.

[11] M. Koppinen, (2008). Algebran peruskurssi II, lecture notes. Turun yliopisto.

[12] Laurent Polynomial, Wolfram Mathworld, (2024). https://mathworld.wolfram.com/LaurentPolynomial.html

[13] S. Golomb, L. Welch, (1970). Perfect codes in the Lee metric and the packing of polyominoes. Siam Journal on Applied Mathematics, vol. 18, pp. 302-317.

[14] T. Lepistö, (1981). A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric. Information and Control, vol. 49, no. 2, pp. 109-124.

[15] K.H. Leung, Y. Zhou, (2020). No lattice tiling of Zn by Lee sphere of radius 2. Journal of Combinatorial Theory, Series A, vol. 171, article 105157.

[16] P. Horak and B. F. AlBdaiwi, (2012). Diameter Perfect Lee Codes. IEEE Transactions on Information Theory, vol. 58, no. 8, pp. 5490-5499.

[17] M. Boyle, D. Lind, (1997). Expansive Subdynamics. Transactions of the American Mathematical Society, vol. 349 no. 1, pp. 55–102.

[18] A. Ballier, B. Durand, E. Jeandel, (2008). Structural aspects of tilings. In 25th International Symposium on Theoretical Aspects of Computer Science. Leibniz International Proceedings in Informatics (LIPIcs), vol. 1, pp. 61-72, Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[19] K. Post, (1975). Nonexistence theorems on perfect Lee codes over large alphabets. Information and Control, vol. 29, no. 4, pp. 369–380.

[20] M. Szegedy, (1998). Algorithms to tile the infinite grid with finite clusters. In: Proceedings 39th Annual Symposium on Foundations of Computer Science (FOCS). IEEE Computer Society, pp. 137-147.

[21] J. Lagarias, Y. Wang, (1996). Tiling the line with translates of one tile. Inventiones mathematicae, vol. 124, pp. 341–365.

[22] D. Zeilberger, (1984). A combinatorial proof of Newton's identities. Discrete Mathematics, vol. 49, no. 3, pp. 319.