ALGEBRALLINEN NÄKÖKULMA PEITTOKOODEIHIN

Elias Heikkilä

Pro gradu -tutkielma
Toukokuu 2020

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck-järjestelmällä.

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

HEIKKILÄ, ELIAS: Algebrallinen näkökulma peittokoodeihin
Pro gradu -tutkielma, 48 s.
Matematiikka
Toukokuu 2020

Tässä tutkielmassa käsitellään algebrallista symbolidynamiikkaa ja sovelletaan sitä peittokoodien tutkimiseen. Algebrallisessa symbolidynamiikassa kombinatoriset ja topologiset ongelmat muutetaan polynomeja koskeviksi kysymyksiksi, jolloin ongelmaan saadaan algebrallinen näkökulma. Algebrallisella lähestymistavalla saadaan helppoja todistuksia neliöhilan ja kuningasgraafin peittokoodituloksille.

Tutkielma alkaa symbolidynamiikan perinteisten käsitteiden määrittelyllä ja perustulosten esittelyllä. Tämän jälkeen määritellään kommutatiivisen algebran ja algebrallisen geometrian peruskäsitteet, joilla saadaan uusi näkökulman symbolidynamiikan tutkimukseen. Näin saadaan perinteisen topologisen rakenteen lisäksi myös algebrallista rakennetta käyttöön. Perustietojen jälkeen esitellään työkaluiksi erilaisia polynomihajotelmia ja todistetaan tutkielman kannalta olennaisten ihanteiden rakennetuloksia. Tutkielmassa pyritään rakentamaan tarvittava teoria mahdollisimman suppeilla esitietovaatimuksilla.

Kun teoriapohja on rakennettu, sovelletaan polynomihajotelmia peittokooditulosten todistamiseen. Lopuksi annetaan vielä algoritmi peittokoodien etsimiseen tietyssä erikoistapauksessa.

Asiasanat: peittokoodi, algebra, algebrallinen geometria, algoritmi, kommutatiivinen algebra, polynomi, ihanne, symbolidynamiikka.

Sisältö

1 Johdanto

Olkoon $w\colon \mathbb{Z} \to \Sigma$ kahteen suuntaan ääretön sana ja merkitään siinä esiintyvien n-pituisten yhtenäisten osasanojen lukumäärää $p_n(w)$. Morsen-Hedlundin lause kertoo, että w on jaksollinen jos ja vain jos on olemassa sellainen $n \in \mathbb{N}$, että $p_n(w) \leqslant n$. Tämä tunnettu sanojen kombinatoriikan tulos luokittelee äärettömät sanat jaksollisiin ja ei-jaksollisiin paikallisen ominaisuuden, kuviokompleksisuuden, avulla. Kutsutaan niitä sanoja, joilla on sellainen $n \in \mathbb{N}$, että $p_n(w) \leqslant n$, *matalan kompleksisuuden* sanoiksi.

Kun tunnetaan tämä tulos, on luontevaa tarkastella matalan kompleksisuuden sanoja useampiulotteisessa tapauksessa. Määritellään tätä varten d-ulotteinen konfiguraatio $c\colon \mathbb{Z}^d \to \Sigma$. Olkoot $n_1, ..., n_d \in \mathbb{N}$ ja määritellään $E = \times_{i=1}^{n} \{\, 1, ..., n_i \,\}$. Tekijäkompleksisuus joukon E suhteen $p_E(c)$ on niiden d-ulotteisten sanojen lukumäärä, jotka saadaan siirtelemällä joukon E määräämää ikkunaa konfiguraation c yllä. Kutsutaan konfiguraatiota c samalla tavalla matalan kompleksisuuden konfiguraatioksi, jos voidaan valita sellaiset luvut $n_1, ..., n_d$, että $p_E(c) \leqslant |E|$.

On olemassa helppoja vastaesimerkkejä ei-jaksollisisista matalan kompleksisuuden konfiguraatioista aina, kun $d \geqslant 3$. [3] Rajatapaus $d = 2$ on yhä avoin, mutta sen uskotaan pitävän paikkansa. Tämä väite on nimetty ranskalaisen Maurice Nivat'n mukaan Nivat'n konjektuuriksi vuonna 1997. [17]

Algebrallinen lähestymistapa symbolidynamiikan tutkimukseen sai alkunsa artikkelissa [14], jossa esiteltiin moniulotteisten sanojen tulkinta polynomeina ja todistettiin algebrallisen geometrian avulla uusia tuloksia matalan kompleksisuuden konfiguraatioista. Tällä lähestymistavalla edistyttiin myös Nivat'n konjektuurissa huomattavasti. Artikkelit [14, 15, 13] ovat osa väitöskirjaa [18], jossa on lisäksi laajennettu tavanomaista polynomien käsittelyä Laurentin polynomeille.

Alunperin Nivat'n konjektuuria varten rakennettua algebrallista koneistoa on myöhemmin yhdistelty perinteiseen symbolidynamiikan topologiseen käsitteistöön ja rakennettu teoriaa uudesta näkökulmasta. [11, 12] Eri näkökulmista on koottu artikkeli [9], jossa mainitaan myös mahdollinen yhteys

peittokoodeihin.

Tässä tutkielmassa todistetaan peittokoodien jaksollisuustuloksia viivapolynomihajotelmilla, jotka avaavat jälleen uuden kehityssuunnan vanhan teorian pohjalle. Näiden hajotelmien avulla saadaan yksinkertaisia todistuksia peittokoodien jaksollisuusominaisuuksille, joita on käsitelty esimerkiksi artikkelissa [2]. Lopuksi esitetään myös yksinkertainen algoritmi, jolle voidaan syöttää kuvio ja tietyssä tapauksessa osataan sanoa, voidaanko sillä peittää taso annettujen ehtojen mukaisesti.

2 Konfiguraatioavaruus

Yleisesti ottaen dynaaminen systeemi on pari (X, f), jossa X on kompakti metrinen avaruus ja f on monoidin M toiminta joukossa X. Lisäksi f^m tulee olla jatkuva kaikilla $m \in M$. Monoidin M voidaan ajatella olevan ajan käsitteen yleistys, jonka paikalle voidaan asettaa esimerkiksi jatkuvassa ja kääntyvässä systeemissä ryhmä $\mathbb{R}$ tai diskreettiaikaisessa kääntymättömässä systeemissä monoidi $\mathbb{N}$. Ei ole kuitenkaan mitään syytä rajoittua yksiulotteiseen tapaukseen.

Tässä tutkielmassa käsitellään moniulotteista symbolidynamiikkaa, jossa X on d-ulotteisten äärettömien sanojen joukko, f on siirto ja $M = \mathbb{Z}^d$. Määritellään nyt käsitteitä hieman täsmällisemmin. Tässä kappaleessa lähteinä on käytetty luentomonisteita [10, 8] ja topologian kirjaa [20].

Määritelmä 2.1. *(aakkosto, konfiguraatio)* Äärellistä epätyhjää joukkoa T kutsutaan *aakkostoksi*. Mielivaltaista kuvausta $c\colon \mathbb{Z}^d \to T$ kutsutaan *konfiguraatioksi* tai *äärettömäksi d-ulotteiseksi sanaksi*. Merkitään sanojen kombinatoriikasta tutulla tavalla $c_{\mathbf{v}} = c(\mathbf{v})$, kun $\mathbf{v} \in \mathbb{Z}^d$.

Määritelmä 2.2. *(konfiguraatioavaruus)* Konfiguraatioavaruus on kaikkien konfiguraatioiden joukko, jolle käytetään tyypillistä joukko-opin merkintätapaa $T^{\mathbb{Z}^d}$.

Määritelmä 2.3. *(kuvio)* Olkoon $D \subseteq \mathbb{Z}^d$ äärellinen ja $p\colon D \to T$. *Äärellinen kuvio*, tai yksinkertaisesti *kuvio*, aakkoston T yli on pari (p, D). Kuvio on luonteva yleistys äärellisen sanan käsittelle.

Määritelmä 2.4. *(sylinteri, alikuvio)* Olkoon (p, D) äärellinen kuvio. Määritellään kuvion (p, D) määräämä *sylinteri* joukkona

$$\mathrm{Cyl}(p, D) = \{\, c \in T^{\mathbb{Z}^d} \mid c|_D = p \,\}.$$

Sanotaan, että kuvio (p, D) on konfiguraation c *alikuvio*, jos $c \in \mathrm{Cyl}(p, D)$.

Annetaan tiilijoukolle T diskreetti metriikka. Tällöin avaruus T on kompakti metrinen avaruus ja T^{Z^d} voidaan ajatella tuloavaruutena, jonne saadaan luonnollisesti tulotopologia, jolla on sylinterikanta

$$\mathcal{B} = \{ \operatorname{Cyl}(p, D) \mid (p, D) \text{ on äärellinen kuvio} \}.$$

Konfiguraatioavaruus on metristyvä, koska se on metristen avaruuksien numeroituva tulo. Lisäksi konfiguraatioavaruus on kompaktien avaruuksien tulona kompakti. [20]

Määritelmä 2.5. *(siirto)* Olkoot $c \in T^{\mathbb{Z}^d}$ ja $\mathbf{u} \in \mathbb{Z}^d$. Vektorin $\mathbf{u}$ määräämä *siirto* on kuvaus $\tau_{\mathbf{u}} \colon T^{\mathbb{Z}^d} \to T^{\mathbb{Z}^d}$, jossa $c \mapsto e$ ja $e(\mathbf{v}) = c(\mathbf{v} - \mathbf{u})$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$.

Määritelmä 2.6. *(jaksollisuus, k-jaksollisuus, täysin jaksollinen)* Ajatellaan kokonaislukuhilaa $\mathbb{Z}^d$ vektoriavaruuden $\mathbb{Q}^d$ alihilana. Konfiguraatio $c \in T^{\mathbb{Z}^d}$ on *jaksollinen* vektorin $\mathbf{u}$ suuntaan, jos $\tau_{\mathbf{u}}(c) = c$ jollekin $\mathbf{u} \in \mathbb{Z}^d \setminus \{ \mathbf{0} \}$. Konfiguraatio c on k-jaksollinen, jos k on suurin sellainen luku, että c on jaksollinen lineaarisesti riippumattomiin suuntiin $\mathbf{u}_1, ..., \mathbf{u}_k$. Yleensä 1-jaksollista konfiguraatiota kutsutaan *yhteen suuntaan jaksolliseksi*. Lisäksi d-jaksollista konfiguraatiota kutsutaan *täysin jaksolliseksi*.

Lause 2.7. *Merkitään* $\mathbf{e}_1 = (1, 0, ..., 0), \mathbf{e}_2 = (0, 1, ..., 0), ..., \mathbf{e}_d = (0, 0, ..., 1)$. *Konfiguraatio c on täysin jaksollinen jos ja vain jos on olemassa sellaiset luvut* $n_i \in \mathbb{Z} \setminus \{ 0 \}$, *että c jaksollinen kaikkiin suuntiin* $n_i \mathbf{e}_i$, *missä* $i = 1, ..., d$.

Todistus.

$\Longleftarrow$ Oletetaan, että c on jaksollinen kaikkiin suuntiin $n_i \mathbf{e}_i$. Koska vektorit $n_i \mathbf{e}_i$ ovat lineaarisesti riippumattomia yli kunnan $\mathbb{Q}$, c on täysin jaksollinen.

$\Longrightarrow$ Oletetaan nyt, että c on täysin jaksollinen. Otetaan ne lineaarisesti riippumattomat vektorit $\mathbf{v}_i$, $i = 1, ..., d$, joille $\tau_{\mathbf{v}_i}(c) = c$. Olkoon $j \in \{ 1, .., d \}$ mielivaltainen. Nyt joukko $\{ \mathbf{v}_i \mid i = 1, .., d \} \cup \{ \mathbf{e}_j \}$ on

lineaarisesti riippuva yli kunnan $\mathbb{Q}$, joten on olemassa rationaaliluvut $q_1, ..., q_{d+1}$, missä $q_{d+1} \neq 0$ ja

$$q_1\mathbf{v}_1 + \cdots q_d\mathbf{v}_d + q_{d+1}\mathbf{e}_j = 0.$$

Otetaan sellainen luku $k \in \mathbb{Z} \setminus \{ 0 \}$, että $kq_i \in \mathbb{Z}$ kaikilla $i = 1, ..., d+1$. Nyt siis $-kq_{d+1}\mathbf{e}_j = kq_1\mathbf{v}_1 + \cdots + kq_d\mathbf{v}_d$ ja edelleen

$$\tau_{-kq_{d+1}\mathbf{e}_j}(c) = \tau_{kq_1\mathbf{v}_1+\cdots+kq_d\mathbf{v}_d}(c) = \tau_{kq_1\mathbf{v}_1} \cdots \tau_{kq_d\mathbf{v}_d}(c) = c.$$

□

Lause 2.8. *Olkoon $c \in T^{\mathbb{Z}^d}$ täysin jaksollinen konfiguraatio. On olemassa sellainen luku $n \in \mathbb{Z} \setminus \{ 0 \}$, että $\tau_{n\mathbf{v}}(c) = c$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$.*

Todistus. Olkoon luvut $n_1, ..., n_d$ lauseesta 2.7 ja merkitään $n = \prod n_i$. Olkoon $\mathbf{v} \in \mathbb{Z}^d$ mielivaltainen. Nyt $n\mathbf{v} = (nv_1, ..., nv_d)$, missä $n_i \mid nv_i$. Merkitään $k_i = \frac{nv_i}{n_i}$. Saadaan siis

$$n\mathbf{v} = \sum_{i=1}^{d} k_i n_i \mathbf{e}_i$$

ja täten $\tau_{n\mathbf{v}}(c) = \tau_{k_1 n_1 \mathbf{e}_1} \cdots \tau_{k_d n_d \mathbf{e}_d}(c) = c$.

□

Lause 2.9. *Siirtokuvaus $\tau_{\mathbf{v}}$ on jatkuva kaikilla $\mathbf{v} \in \mathbb{Z}^d$.*

Todistus. Seuraa luonnollisesti, kun tarkastellaan konfiguraatioavaruuden topologian sylinterikantaa. Yksityiskohtainen todistus lähteessä [8]. □

2.1 Siirtoaliavaruus

Joukko $A \subseteq T^{\mathbb{Z}^d}$ on *translaatioinvariantti* jos $\tau_{\mathbf{u}}(A) = A$ kaikilla $\mathbf{u} \in \mathbb{Z}^d$.

Määritelmä 2.10. *(siirtoaliavaruus)* Translaatioinvarianttia ja topologisesti suljettua joukkoa A kutsutaan *siirtoaliavaruudeksi (subshift)*. Erikoistapausta $A = T^{\mathbb{Z}^d}$ voidaan kutsua yksinkertaisesti *siirtoavaruudeksi (full shift)*. Siirtoavaruus on siis konfiguraatioavaruuden synonyymi hieman eri vivahteella.

Määritelmä 2.11. *(kuvion esiintyminen konfiguraatiossa)* Kuvio (p, D) *esiintyy* konfiguraatiossa c, jos on olemassa vektori $\mathbf{v} \in \mathbb{Z}^d$, jolle $\tau_{\mathbf{v}}(u)|_D = p$. Merkitään kaikkien konfiguraatiossa c esiintyvien kuvioiden joukkoa

$$\mathrm{Patt}(c) = \{\, (p, D) \mid \text{kuvio } (p, D) \text{ esiintyy konfiguraatiossa } c \,\}.$$

Kuviojoukossa on kaikki konfiguraation alikuviot ja niiden siirretyt versiot. Konfiguraation c alikuvioiden avulla saadaan kaikki sylinterit, joihin c kuuluu ja kuviojoukon avulla saadaan sellaiset sylinterit, joihin konfiguraatio voidaan siirtää. Tämä on tärkeä asetelma symbolidynamiikan kannalta, koska sylinterit muodostavat topologian kannan ja ryhmän $(\mathbb{Z}^d, +)$ toiminta konfiguraatioavaruudessa määritellään siirtojen avulla.

Kuviojoukon määritelmää voidaan laajentaa konfiguraatiojoukoille $A \subseteq T^{\mathbb{Z}^d}$ luonnollisella tavalla:

$$\mathrm{Patt}(A) = \bigcup_{c \in A} \mathrm{Patt}(c).$$

Määritelmä 2.12. *(kuvioita välttävät konfiguraatiot)* Määritellään kuviojoukolle $P \subseteq \mathrm{Patt}(T^{\mathbb{Z}^d})$ konfiguraatiojoukko, jossa ei esiinny kuvioita joukosta P:

$$\Sigma(P) = \{\, c \in T^{\mathbb{Z}^d} \mid \mathrm{Patt}(c) \cap P = \varnothing \,\}.$$

Sanotaan, että joukon $\Sigma(P)$ konfiguraatiot *välttävät* joukon P kuviot.

Siirtoavaruudessa esiintyy kaikki mahdolliset kuviot ja siksi onkin luontevaa ajatella, että siirtoaliavaruudessa esiintyy vain jokin osajoukko kaikista kuvioista. Seuraava tulos muotoilee täsmällisesti tämän ajatuksen.

Lause 2.13. *Joukko Σ on siirtoaliavaruus jos ja vain jos $\Sigma = \Sigma(P)$ jollekin $P \subseteq Patt(T^{\mathbb{Z}^d})$.*

Todistus. Luentomonisteessa [8]. □

Määritelmä 2.14. (*Wang-laatta, Wang-laatoitus) Wang-laatta* on yksikköneliö, jonka reunat on värjätty. Tässä yhteydessä laatoitus on sellainen konfiguraatio Wang-laattoja, että kaikki toisiaan koskevat reunat ovat samaa väriä.

Siirtoaliavaruus Σ on *äärellistä tyyppiä* tai SFT *(subshift of finite type)*, jos on olemassa äärellinen P, jolle $\Sigma = \Sigma(P)$. Kun rajoitutaan kahteen ulottuvuuteen, saadaan äärellisen tyypin siirtoaliavaruuksien ja tiilitysten välille luonteva yhteys. Kaikki Wang-tiilitykset voidaan ajatella äärellisen tyypin siirtoaliavaruuksina ja toisaalta äärellisen tyypin siirtoaliavaruuksista voidaan algoritmisesti rakentaa samoilla ominaisuuksilla varustettu Wang-tiilijoukko. [10] Wang-laatoituksille esiteltyjä algoritmeja voidaan soveltaa siis äärellisen tyypin siirtoavaruuksille. Esitellään vielä kaksi tutkielman myöhemmässä vaiheessa tarvittavaa tulosta.

Lause 2.15. *Jos Wang-tiilijoukolla T voidaan tiilittää taso yhteen suuntaan jaksollisesti, on samalla tiilijoukolla olemassa myös 2-jaksollinen tiilitys.*

Todistus. Luentomonisteessa [10]. □

Lause 2.16. *Olkoon siirtoaliavaruus $\Sigma \subseteq T^{\mathbb{Z}^2}$ äärellistä tyyppiä. Jos tiedetään, että Σ sisältää jaksollisen alkion tai $\Sigma = \varnothing$, kysymys joukon Σ tyhjyydestä on algoritmisesti ratkeava.*

Todistus. Rakennetaan algoritmisesti tiilijoukko T, joka tiilittää tason jaksollisesti jos ja vain jos $\Sigma \neq \varnothing$. Tähän on esitelty algoritmi luentomonisteessa [10]. Ajetaan kahta puolialgoritmia samaan aikaan:

1) Arvataan sellainen $k \in \mathbb{N}$, jolle aluetta $\{ 0, 1, ..., k \}^2$ ei pystytä tiilittämään ilman virhettä. Tällöin $\Sigma = \varnothing$.

2) Lauseen 2.15 nojalla riittää etsiä 2-jaksollisia tiilityksiä. Arvataan sellainen $k \in \mathbb{N}$, että alue $\{ 0, 1, ..., k \}^2$ pystytään tiilittämään ilman virhettä ja kuvion alarivin värit sopivat ylärivin väreihin sekä vasemman reunan värit sopivat oikean reunan väreihin. Nyt ollaan löydetty jaksollinen tiilitys. Tällöin $\Sigma \neq \varnothing$.

□

3 Kommutatiivista algebraa

Määritellään kommutatiivisen algebran työkaluja, jotta voidaan käsitellä d muuttujan Laurentin polynomeja, jotka avaavat yhteyden polynomialgebran ja symbolidynamiikan välille. Käytetään lähteinä kirjoja [1, 4] ja luentomonistetta [16]. Algebrallisen geometrian osuudessa käytetään kirjaa [5] ja väitöskirjaa [18].

Määritelmä 3.1. *(rengas)* Kolmikkoa $(R, +, *)$ kutsutaan *renkaaksi*, jos binäärioperaatioille $+ \colon R \times R \to R$ ja $* : R \times R \mapsto R$ pätee seuraavat ehdot:

1. $(R, +)$ on Abelin ryhmä

2. $(R, *)$ on monoidi

3. $a * (b + c) = a * b + a * c$ ja $(a + b) * c = a * c + b * c$ kaikilla $a, b, c \in R$.

Kommutatiiviselle renkaalle pätee lisäksi $a * b = b * a$ kaikilla $a, b \in R$. Tästä eteenpäin renkaasta käytetään lyhennemerkintää R, koska binäärioperaatiot voidaan päätellä asiayhteydestä. Lyhennetään myös kertolaskun merkintää tyypilliseen tapaan $a * b = ab$. Tässä koko tutkielmassa oletetaan, että R on kommutatiivinen rengas.

Määritelmä 3.2. *(yksikkö, jaoton alkio)* Alkio $a \in R$ on *yksikkö*, jos sillä on olemassa kertolaskun suhteen käänteisalkio. Alkiota $a \neq 0$ sanotaan *jaottomaksi* jos a ei ole yksikkö ja

$$a = bc \implies b \text{ on yksikkö tai } c \text{ on yksikkö.}$$

Esimerkki 3.3. Kokonaislukujen renkaassa $\mathbb{Z}$ yksiköitä ovat 1 ja -1. Täten kokonaislukurenkaan jaottomat alkiot ovat alkuluvut ja niiden vastaluvut.

Esimerkki 3.4. Kunnassa ei ole jaottomia alkioita, koska kaikki nollasta poikkeavat alkiot ovat yksiköitä.

3.1 Polynomirenkaat ja muodolliset potenssisarjat

Olkoon R kommutatiivinen rengas ja $x_1, ..., x_d$ muuttujia. Käytetään muuttujien monikolle merkintää $X = (x_1, ..., x_d)$ ja määritellään $X^{\mathbf{v}} = x_1^{v_1} x_2^{v_2} \cdots x_d^{v_d}$ vektorille $\mathbf{v} \in \mathbb{Z}^d$.

Määritelmä 3.5. *(Laurentin polynomi) Laurentin polynomi* renkaan R yli on summa $\sum_{\mathbf{v} \in D} a_{\mathbf{v}} X^{\mathbf{v}}$, missä $D \subseteq \mathbb{Z}^d$ on äärellinen ja $a_{\mathbf{v}} \in R$. Merkitään Laurentin polynomien joukkoa

$$R[x_1^{\pm 1}, ..., x_d^{\pm 1}] \text{ tai } R[X^{\pm 1}].$$

Määritelmä 3.6. *(muodollinen potenssisarja)* Kun sallitaan Laurentin polynomille ääretön määrä nollasta poikkeavia kertoimia, saadaan *muodollinen potenssisarja* yli renkaan R. Merkitään muodollisten potenssisarjojen joukkoa

$$R[[x_1^{\pm 1}, ..., x_d^{\pm 1}]] = R[[X^{\pm 1}]] = \{ \sum_{\mathbf{v} \in \mathbb{Z}^d} a_{\mathbf{v}} X^{\mathbf{v}} \mid a_{\mathbf{v}} \in R \}.$$

Joukko $R[X^{\pm 1}]$ on kommutatiivinen rengas tavanomaisen polynomikertolaskun suhteen ja lisäksi voidaan määritellä Laurentin polynomin ja muodollisen potenssisarjan kertolasku paikallisena polynomikertolaskuna. Tällöin muodollisten potenssisarjojen joukko muodostaa modulin Laurentin polynomien renkaan yli.

Määritelmä 3.7. *(kantaja)* Olkoon $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ Laurentin polynomi tai muodollinen potenssisarja. Määritellään *kantaja*:

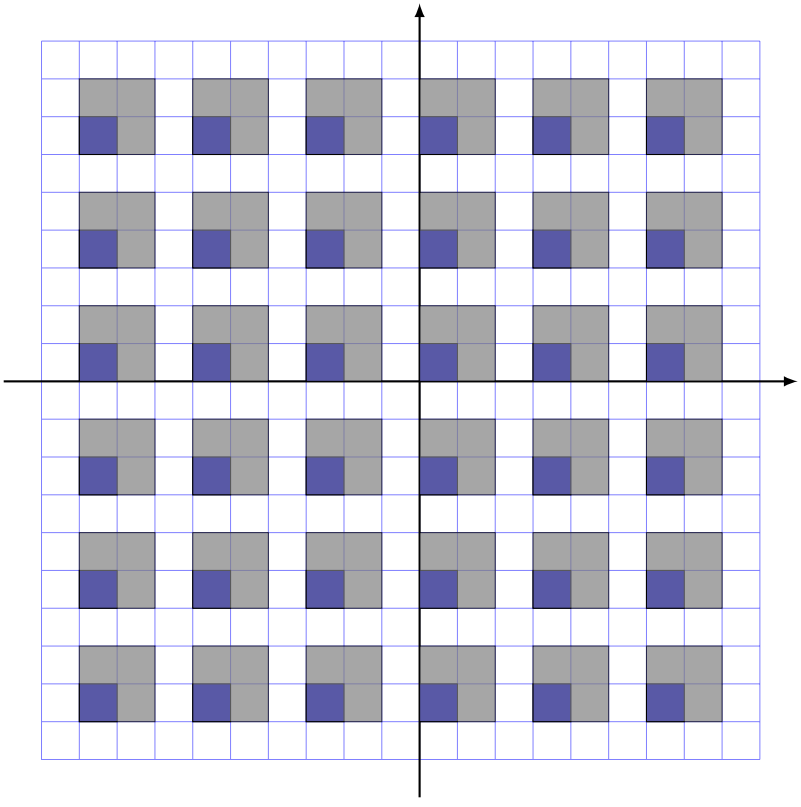
$$\text{supp}(f) = \{ \mathbf{v} \in \mathbb{Z}^d \mid a_{\mathbf{v}} \neq 0 \}.$$

Tässä tutkielmassa käsitellään Laurentin polynomeja ja muodollisia potenssisarjoja lähinnä kunnan $\mathbb{C}$ yli, koska se on algebrallisesti suljettu. Toinen kiinnostava vaihtoehto olisi tarkastella polynomeja yli äärellisen kunnan $\mathbb{F}_q$, missä $q = p^n$ jollekin alkuluvulle p. [11] Tätä ajatusta sivutaan peittokoodien sovelluksissa, koska siellä rajoitutaan binääriaakkostoon.

Esimerkki 3.8. Olkoon $f = \sum_{\mathbf{v}\in D} a_{\mathbf{v}} X^{\mathbf{v}}$ Laurentin polynomi ja $c = \sum_{\mathbf{v}\in\mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$ muodollinen potenssisarja. Lasketaan tulo fc ensin kahdella tavalla.

$$fc = \sum_{\mathbf{v}\in\mathbb{Z}^d} f c_{\mathbf{v}} X^{\mathbf{v}} = \sum_{\mathbf{v}\in\mathbb{Z}^d} \sum_{\mathbf{u}\in D} a_{\mathbf{u}} c_{\mathbf{v}} X^{\mathbf{v}+\mathbf{u}} = \sum_{\mathbf{v}\in\mathbb{Z}^d} \sum_{\mathbf{u}\in D} a_{\mathbf{u}} c_{\mathbf{v}-\mathbf{u}} X^{\mathbf{v}}.$$

Tämä antaa kaksi visuaalista ajattelutapaa. Joko Laurentin polynomi f asetetaan kaikkiin potenssisarjan c osoittamiin kohtiin tai tarkastellaan ikkunassa $-D$ havaittavia potenssisarjan c merkkejä. Havainnollistetaan nyt konfiguraation $c = \sum_{\mathbf{v}\in\mathbb{Z}^d} X^{3\mathbf{v}}$ ja polynomin $f = 1 + x + y + xy$ kertolaskua kuvalla.



Kuva 1: Polynomin f ja potenssisarjan c kertolasku.

3.2 Konfiguraatio, tiili ja tiilittäjä

Määritellään nyt symbolidynamiikan käsitteitä algebrallisessa kontekstissa väitöskirjan [18] kanssa yhteensopivasti.

Määritelmä 3.9. *(algebrallinen konfiguraatio)* Mikä tahansa muodollinen potenssisarja $c \in \mathbb{C}[[X^{\pm 1}]]$ on *algebrallinen konfiguraatio.*

Määritelmä 3.10. *(äärellisen aakkoston konfiguraatio, äärellisen kokonaisaakkoston konfiguraatio, konfiguraatio aakkoston T yli)*
Olkoon $c = \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$ algebrallinen konfiguraatio. Määritellään symbolidynamiikan kannalta olennaisia alakäsitetteitä.

- c on *äärellisen aakkoston konfiguraatio*, jos on olemassa äärellinen $T \subseteq \mathbb{C}$, jolle $c_{\mathbf{v}} \in T$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$.
- Konfiguraatio on *äärellisen kokonaisaakkoston konfiguraatio*, jos lisäksi $T \subseteq \mathbb{Z}$.
- Joskus halutaan myös kiinnittää aakkosto T valmiiksi. Jos konfiguraatiolle c pätee $c_{\mathbf{v}} \in T$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$, sanotaan, että c on konfiguraatio *aakkoston T yli*. Samoin voidaan puhua Laurentin polynomeista aakkoston T yli.

Potenssisarjamääritelmä konfiguraatiolle on yleisempi kuin perinteinen symbolidynamiikan versio, koska tässä tapauksessa sallitaan ääretön aakkosto. Jonkin äärellisen aakkoston konfiguraatiot samaistuvat kuitenkin symbolidynamiikan käsitteistöön luontevasti. Tulkitaan aluksi, että aakkoston kirjaimet ovat kompleksilukuja ja tämän jälkeen tehdään injektiivinen kuvaus $T^{\mathbb{Z}^d} \to \mathbb{C}[[x_1^{\pm 1}, ..., x_d^{\pm 1}]]$, missä $c \mapsto \sum_{\mathbf{v} \in \mathbb{Z}^d} c_{\mathbf{v}} X^{\mathbf{v}}$. Koska virhepäätelmien vaaraa ei ole, tästä eteenpäin puhutaan algebrallisista konfiguraatioista yksinkertaisesti konfiguraatioina. Tämä vastaavuus avaa algebrallisen näkökulman symbolidynamiikan tutkimukseen.

Voidaan siis määritellä vastaavia symbolidynamiikan käsitteitä algebrallisella lähestymistavalla. Siirto vektorilla $\mathbf{v}$ saa muodon $\tau_{\mathbf{v}}(c) = X^{\mathbf{v}} c$. Lisäksi c on jaksollinen jos $X^{\mathbf{v}} c = c$ eli $(X^{\mathbf{v}} - 1)c = 0$ jollakin $\mathbf{v} \neq \mathbf{0}$. Vastaavasti c on täysin jaksollinen jos c on jaksollinen lineaarisesti riippumattomiin suuntiin $\mathbf{v}_1, ..., \mathbf{v}_d$.

Lause 3.11. *Olkoot c ja e täysin jaksollisia konfiguraatioita ja f polynomi. Konfiguraatiot $c+e$ ja fc ovat täysin jaksollisia.*

Todistus. Olkoon $i \in \{1, ..., d\}$.

$(c+e)$ Lauseen 2.7 mukaan konfiguraatiot e ja c ovat jaksollisia suuntiin $n_i\mathbf{e}_i$ ja $m_i\mathbf{e}_i$ joillekin $n_i, m_i \in \mathbb{Z}\backslash\{0\}$. Nyt siis konfiguraatioilla c ja e on yhteinen jakso $n_i m_i \mathbf{e}_i$, joten myös $c+e$ on jaksollinen suuntaan $n_i m_i \mathbf{e}_i$.

(fc) Tarkastellaan nyt kertolaskua fc. Konfiguraation c jaksollisuudesta seuraa, että $c_{\mathbf{v}} = c_{\mathbf{v}+m_i\mathbf{e}_i}$ kaikille $\mathbf{v} \in \mathbb{Z}^d$. Laskemalla saadaan

$$X^{m_i\mathbf{e}_i} fc = X^{m_i\mathbf{e}_i} \sum_{\mathbf{v}\in\mathbb{Z}^d} \sum_{\mathbf{u}\in\mathrm{supp}(f)} a_{\mathbf{u}} c_{\mathbf{v}+\mathbf{u}} X^{\mathbf{v}} = \sum_{\mathbf{v}\in\mathbb{Z}^d} \sum_{\mathbf{u}\in\mathrm{supp}(f)} a_{\mathbf{u}} c_{\mathbf{v}+\mathbf{u}} X^{\mathbf{v}+m_i\mathbf{e}_i} =$$

$$\sum_{\mathbf{v}\in\mathbb{Z}^d} \sum_{\mathbf{u}\in\mathrm{supp}(f)} a_{\mathbf{u}} c_{\mathbf{v}+m_i\mathbf{e}_i+\mathbf{u}} X^{\mathbf{v}+m_i\mathbf{e}_i} = fc.$$

□

Täten siis täysin jaksolliset konfiguraatiot muodostavat alimodulin muodollisten potenssisarjojen modulille. Jos sallitaan mukaan myös yhteen suuntaan jaksollisia konfiguraatioita, vastaavaa alimodulirakennetta ei synny.

Esimerkki 3.12. Kahden 1-jaksollisen konfiguraation summa ei välttämättä ole jaksollinen.

Määritellään konfiguraatiot $c_1, c_2 \in \mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ seuraavalla tavalla:

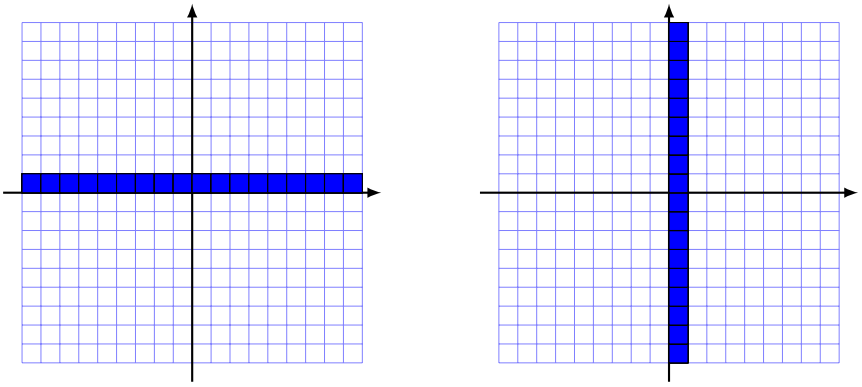
$$c_{1(x,y)} = \begin{cases} 1 & y = 0 \\ 0 & \text{muutoin} \end{cases}$$

$$c_{2(x,y)} = \begin{cases} 1 & x = 0 \\ 0 & \text{muutoin.} \end{cases}$$

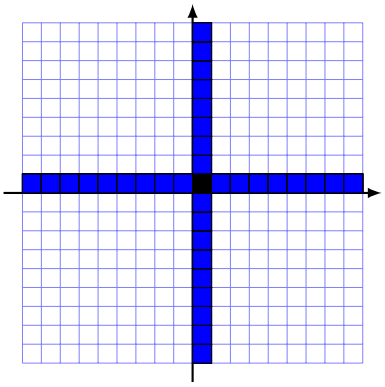
Nämä konfiguraatiot ovat selvästi yhteen suuntaan jaksollisia, mutta niiden summa $c = c_1 + c_2$ on konfiguraatio

$$c_{(x,y)} = \begin{cases} 2 & (x,y) = \mathbf{0} \\ 1 & xy = 0 \text{ ja } (x,y) \neq \mathbf{0} \\ 0 & \text{muutoin.} \end{cases}$$

Havainnollistetaan tilannetta kuvalla.



(a) c_1 (b) c_2



(c) $c_1 + c_2$

Kuva 2: Konfiguraatiot c_1 ja c_2 sekä niiden summa $c_1 + c_2$

Tässä tutkielmassa pakataan kokonaislukuhila äärellisillä $\mathbb{Z}^d$ kuvioilla tiettyjen ehtojen toteutuessa. Algebrallisella lähestymistavalla kuviot samaistuvat Laurentin polynomeiksi ja tätä kautta saadaan tuloksia siitä, miten laattoja on aseteltava hilaan annettujen ehtojen toteutumiseksi. Merkitään ensin $\mathbb{1} = \sum_{\mathbf{v}\in\mathbb{Z}^d} X^{\mathbf{v}}$.

Määritelmä 3.13. *(tiili)* Mikä tahansa nollasta poikkeava Laurentin polynomi f yli kunnan $\mathbb{C}$ on *tiili*.

Määritelmä 3.14. *(n-pakkaaja)* Äärellisen kokonaisaakkoston konfiguraatio c on *n-pakkaaja* tiilelle f, jos $fc = n\mathbb{1}$. Kaksiulotteisessa tapauksessa voidaan puhua myös *n-tiilittäjästä*.

Lause 3.15. *Olkoon $n \in \mathbb{N}$ ja $T \subseteq \mathbb{Z}$ äärellinen. Laattaa f vastaavien n-pakkaajien joukko yli aakkoston T on SFT.*

Todistus. Olkoon nyt $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ ja merkitään $D = \mathrm{supp}(f)$. Olkoon $P = \{(p, -D) \mid \sum_{\mathbf{u} \in D} a_{\mathbf{u}} p_{-\mathbf{u}} \neq n\}$. Nyt P on äärellinen ja $\Sigma(P)$ on n-pakkaajien joukko. □

Tutkielman loppuosassa hyödynnetään edellistä tulosta erityisesti kaksiulotteisessa tapauksessa, jossa lisäksi tiilen f ja pakkaajan c aakkosto on $\{0, 1\}$. Silloin riittää, että kaikilla $\mathbf{v} \in \mathbb{Z}^2$ pätee

$$\sum_{\mathbf{u} \in -D + \mathbf{v}} c_{\mathbf{u}} = n.$$

Toinen tärkeä huomio on, että tässä tutkielmassa ei olla suljettuja äärellisen aakkoston T sisälle. Vaikka siis laatta f ja sen n-pakkaaja c olisivat aakkoston T sisällä, ei tulo fc ole välttämättä enää aakkoston T yli.

3.3 Ihanteista

Määritelmä 3.16. *(Ihanne)* Joukkoa $I \subseteq R$ kutsutaan *ihanteeksi*, jos se toteuttaa seuraavat ehdot:

1. $I \neq \varnothing$

2. $a + b \in I$ kaikille $a, b \in I$

3. $ra \in I$ kaikille $r \in R$ ja $a \in I$.

Määritelmä 3.17. *(triviaali ja epätriviaali ihanne)* Ihanteelle käytetään merkintää $I \leqslant R$. Ihanne I on *triviaali* jos $I = \{0\}$. Muutoin I on *epätriviaali*. Määritellään kaksi tutkielman kannalta olennasta Laurentin polynomien renkaan ihannetta konfiguraation c avulla.

Määritelmä 3.18. *(annihilaattori-ihanne)* Joukko $\mathrm{Ann}(c) = \{ f \in \mathbb{C}[X^{\pm 1}] \mid fc = 0 \}$ on konfiguraation c *annihilaattori-ihanne* ja sanotaan, että f *annihiloi* konfiguraation c.

Määritelmä 3.19. *(jaksollistaja-ihanne)* Joukko $\mathrm{Per}(c) = \{\, f \in \mathbb{C}[X^{\pm 1}] \mid fc \text{ on täysin jaksollinen} \,\}$ on konfiguraation c *jaksollistaja-ihanne.*

Lause 3.20. *Joukot Ann(c) ja Per(c) ovat renkaan* $\mathbb{C}[X^{\pm 1}]$ *ihanteita.*

Todistus.

Ann(c) Selvästi $0 \in \mathrm{Ann}(c)$. Olkoot nyt $f, g \in \mathrm{Ann}(c)$. Tällöin $(f+g)c = fc + gc = 0$, joten $f + g \in \mathrm{Ann}(c)$. Olkoon nyt r jokin polynomi. Tällöin $(rf)c = r(fc) = 0$, joten $rf \in \mathrm{Ann}(c)$. Täten $\mathrm{Ann}(c)$ on ihanne.

Per(c) Ensinnäkin $0 \in \mathrm{Per}(c)$. Valitaan mielivaltaiset $f, g \in \mathrm{Per}(c)$ ja polynomi r. Nyt $(f+g)c = fc+gc$ on kahden täysin jaksollisen konfiguraation summana täysin jaksollinen. Lisäksi rfc on täysin jaksollinen.

□

Määritelmä 3.21. *(nollanjakaja, kokonaisalue)* Alkio $a \in R$ on *nollanjakaja*, jos $a \neq 0$ ja on olemassa sellainen $b \neq 0$, jolle $ab = 0$. Rengas R on *kokonaisalue*, jos R ei sisällä nollanjakajia.

Lause 3.22. *Olkoon* (I_i) *mielivaltainen perhe ihanteita renkaassa R. Tällöin leikkaus* $\bigcap I_i$ *on ihanne.*

Todistus. Olkoon $a, b \in \bigcap I_i$. Valitaan mielivaltainen I_i. Koska I_i on ihanne, voidaan päätellä $a + b \in I_i$ ja $ra \in I_i$. Koska i oli mielivaltainen, saadaan $a + b, ra \in \bigcap I_i$. □

Määritelmä 3.23. *(osajoukon generoima ihanne)* Olkoon $S \subseteq R$. Joukon S generoima ihanne määritellään $\langle S \rangle = \bigcap_{S \subseteq I \leqslant R} I$. Toisin sanoen $\langle S \rangle$ on pienin ihanne, joka sisältää joukon S.

Lause 3.24. *Joukon S generoima ihanne sisältää täsmälleen ne alkiot, jotka ovat muotoa $r_1s_1 + ... + r_ns_n$, missä $r_i \in R$ ja $s_i \in S$.*

Todistus. Olkoot $s_1, ..., s_n \in S$ ja $r_1, ..., r_n \in R$ mielivaltaisia. Nyt selvästi $s_i \in \langle S \rangle$ kaikille i, joten $s_ir_i \in \langle S \rangle$. Koska ihanne suljettu summien suhteen, myös $s_1r_1 + ... + s_nr_n \in \langle S \rangle$. Täten $\{ s_1r_1 + ... + s_nr_n \mid s_i \in S, r_i \in R \} \subseteq \langle S \rangle$. Toisaalta joukko $\{ s_1r_1 + ... + s_nr_n \mid s_i \in S, r_i \in R \}$ on ihanne, koska alkioiden esitysmuoto sallii summauksen ja renkaan alkiolla kertomisen. Täten $\{ s_1r_1 + ... + s_nr_n \mid s_i \in S, r_i \in R \} = \langle S \rangle$.

□

Määritelmä 3.25. (*Noetherin rengas*) Rengas R on *Noetherin rengas* jos jokainen ihanne $I \leqslant R$ on äärellisen joukon generoima.

Lause 3.26 (Hilbertin kantalause)**.** *Jos R on Noetherin rengas, niin $R[X]$ on Noetherin rengas.*

Todistus. Kirjassa [5]. □

Lemma 3.27. *Olkoon R Noetherin rengas ja $S \subseteq R$. On olemassa äärellinen $F \subseteq S$, jolle $\langle F \rangle = \langle S \rangle$.*

Todistus. Merkitään $I = \langle S \rangle$. Koska R on Noetherin rengas, on olemassa äärellinen $G \subseteq I$, jolle $I = \langle G \rangle$. Merkitään $G = \{ g_1, ..., g_n \}$ ja otetaan kaikille g_i esitys joukon S alkioiden äärellisenä kombinaationa:

$$g_i = \sum_{j=1}^{m_i} r_j s_j.$$

Olkoon nyt $F_i = \{ s_1, ..., s_{m_i} \}$. Kun merkitään $F = F_1 \cup \cdots \cup F_n$, saadaan $\langle F \rangle = I$ ja $F \subseteq S$ on äärellinen.

□

Määritelmä 3.28. *(ihanteiden summa ja tulo)* Kahden ihanteen $I, J \leqslant R$ *summa* on $I + J = \{\, a + b \mid a \in I \text{ ja } b \in J \,\}$ ja *tulo* on $IJ = \langle\, ab \mid a \in I \text{ ja } b \in J \,\rangle$. Nämä ovat myös ihanteita renkaassa R.

Määritelmä 3.29. *(pääihanne, alkuihanne, maksimaalinen ihanne, radikaali, pareittain maksimaaliset ihanteet)*

- Yhden alkion $a \in R$ generoimaa ihannetta $\langle a \rangle$ kutsutaan *pääihanteeksi*. Rengas R on *pääihannealue* jos kaikki ihanteet $I \leqslant R$ ovat pääihanteita.
- Ihanne $I \leqslant R$ on *alkuihanne*, jos $ab \in I \implies a \in I$ tai $b \in I$.
- Ihanne $I \leqslant R$ on *maksimaalinen*, jos

$$I \subseteq J \leqslant R \implies J = I \text{ tai } J = R.$$

- Ihanteet $I, J \leqslant R$ ovat *pareittain maksimaaliset*, jos $I + J = R$.
- Ihanteen I *radikaali* on joukko $\sqrt{I} = \{\, a \mid a^n \in I \text{ jollekin } n \in \mathbb{N} \,\}$ ja ihannetta kutsutaan *radikaaliksi* jos $I = \sqrt{I}$.

Renkaasta voidaan muodostaa *tekijärengas* jonkin ihanteen suhteen. Määritellään tekijärengas $R/I = \{\, r + I \mid r \in R \,\}$ sivuluokkien joukkona. Tekijärenkaassa on käytössä renkaan R laskuoperaatiot, mutta kahta samaan sivuluokkaan kuuluvaa alkiota ei erotella keskenään.

Lause 3.30. *Tekijärengas R/I on kunta jos ja vain jos I on maksimaalinen ihanne.*

Todistus. Kirjassa [1]. □

Lause 3.31. *Joukko $\sqrt{I}$ on ihanne.*

Todistus. Olkoot $a, b \in \sqrt{I}$ ja $r \in R$. On siis olemassa luvut $n, m \in \mathbb{N}$, joille $a^n \in I$ ja $b^m \in I$. Nyt

$$(a+b)^{n+m} = \sum_{\substack{i,j \geqslant 0 \\ i+j=n+m}} \binom{n+m}{i} a^i b^j,$$

joten kaikissa summattavissa termeissä pätee $i \geqslant n$ tai $j \geqslant m$. Tästä seuraa, että kaikki summattavat termit kuuluvat ihanteesen I ja täten myös $(a+b)^{n+m} \in I$ ja edelleen $a + b \in \sqrt{I}$. Tulo saadaan kommutatiivisuuden nojalla $(ra)^n = r^n a^n \in I$ eli $ra \in \sqrt{I}$. □

Lause 3.32. *Tekijärengas R/I on kokonaisalue jos ja vain jos I on alkuihanne.*

Todistus.

$\Longrightarrow$ Oletetaan, että R/I on kokonaisalue. Olkoot $a, b \in R$ sellaiset, että $ab \in I$. Täten $(a+I)(b+I) = 0_{R/I}$, josta seuraa $a + I = 0_{R/I}$ tai $b + I = 0_{R/I}$ ja edelleen $a \in I$ tai $b \in I$.

$\Longleftarrow$ Olkoon nyt I alkuihanne. Valitaan sellaiset $a + I, b + I \in R/I$, että $(a+I)(b+I) = 0_{R/I}$. Nyt siis $ab \in I$ ja edelleen $a \in I$ tai $b \in I$. Nyt siis $a + I = 0_{R/I}$ tai $b + I = 0_{R/I}$.

□

Lemma 3.33. *Maksimaaliset ihanteet ovat alkuihanteita*

Todistus. Olkoon $M \leqslant R$ maksimaalinen. Tekijärengas R/M on kunta ja täten kokonaisalue. Nyt voidaan soveltaa edellistä tulosta ihanteeseen M. □

Lause 3.34. *Alkuihanteet ovat radikaaleja*

Todistus. Olkoon P alkuihanne. Tietysti $P \subseteq \sqrt{P}$. Olkoon $r \in \sqrt{P}$. Valitaan sellainen $n \in \mathbb{N}$, jolle $r^n \in P$. Koska P on alkuihanne, saadaan $r^n = rr^{n-1} \implies r \in P$ tai $r^{n-1} \in P$. Helpolla induktiolla todetaan, että $r \in P$. □

Korollaari 3.35. *Maksimaaliset ihanteet ovat radikaaleja*

Todistus. Maksimaalinen ihanne on alkuihanne ja alkuihanne on radikaali. □

Lause 3.36. *Radikaalien ihanteiden mielivaltainen leikkaus on radikaali*

Todistus. Olkoon (I_j) perhe radikaaleja ihanteita. Olkoon $a \in R$ ja $n \in \mathbb{N}$. Jos $a^n \in \bigcap I_j$, niin $a^n \in I_j$ ja edelleen $a \in \sqrt{I_j} = I_j$ kaikilla j. Nyt siis $a \in \bigcap I_j$ ja väite seuraa. □

3.4 Algebrallista geometriaa

Yleensä algebrallisessa geometriassa käsitellään polynomirengasta $\mathbb{C}[X]$. Tässä tutkielmassa ollaan konfiguraation ja laatan määritelmien takia kiinnostuneita ihanteista Laurentin polynomien renkaassa $\mathbb{C}[X^{\pm 1}]$. Olennaiset tulokset ovat kuitenkin voimassa myös tässä hieman yleisemmässä kontekstissa. [18] Määritellään aluksi algebrallisen geometrian olennaisia käsitteitä Laurentin polynomien yhteydessä. Merkitään tavanomaiseen tapaan $\mathbb{C}^* = \mathbb{C} \setminus \{ 0 \}$.

Määritelmä 3.37. (*varisto, polynomijoukon määräämä ihanne, polynomin häviäminen*)

- Polynomijoukon $K \subseteq \mathbb{C}[X^{\pm 1}]$ määräämä *varisto* on joukko $\mathbf{V}(K) = \{ x \in (\mathbb{C}^*)^d \mid f(x) = 0 \text{ kaikilla } f \in K \}$.
- Määritellään joukolle $S \subseteq (\mathbb{C}^*)^d$ ihanne $\mathbf{I}(S) = \{ f \in \mathbb{C}[X^{\pm 1}] \mid f(x) = 0 \text{ kaikilla } x \in S \}$. Sanotaan, että polynomi $f \in \mathbf{I}(S)$ *häviää* joukossa S.

Hilbertin nollakohtalause antaa luontevan yhteyden ihanteiden ja varistojen välille. Kiinnitetyssä varistossa häviävä ihanne on radikaali.

Lause 3.38 (Hilbertin nollakohtalause Laurentin polynomeille)**.**
Olkoon $I \leqslant \mathbb{C}[X^{\pm 1}]$. *Tällöin* $\boldsymbol{IV}(I) = \sqrt{I}$.

Todistus. Kirjat [4] ja [5] sisältävät klassisen polynomirenkaita koskevan version. Laajennus Laurentin polynomeille on todistettu väitöskirjassa [18]. □

Lause 3.39 (Hilbertin kantalauseen sovellus Laurentin polynomeille)**.** $\mathbb{C}[X^{\pm 1}]$ *on Noetherin rengas.*

Todistus. Väitöskirjassa [18]. □

Lause 3.40. *Ihanne* $I \leqslant \mathbb{C}[X^{\pm 1}]$ *on radikaali jos ja vain jos se on alkuihanteiden leikkaus* $I = P_1 \cap \cdots \cap P_n$*, missä* $P_i \nsubseteq P_j$*, kun* $i \neq j$*.*

Todistus.

$\Longrightarrow$ Kirja [4] sisältää todistuksen polynomirenkaassa ja väitöskirjassa [18] on laajennus Laurentin polynomeille.

$\Longleftarrow$ Alkuihanteet ovat radikaaleja lauseen 3.34 nojalla ja radikaalien ihanteiden leikkaus on radikaali lauseen 3.36 mukaan.

□

Lause 3.41. *Epätriviaalille alkuihanteelle* $P \leqslant \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ *pätee yksi seuraavista:*

- P *on jaottoman polynomin* ϕ *generoima pääihanne*
- P *on maksimaalinen ihanne ja* $P = \langle x - \alpha, y - \beta \rangle$ *joillekin* $\alpha, \beta \in \mathbb{C}^*$*.*

Todistus. Kirjassa [5] on polynomeja koskeva versio. Laajennus Laurentin polynomeille on esitetty väitöskirjassa [18]. □

Lause 3.42. *Olkoon* $A \leqslant \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ *epätriviaali radikaali ihanne. On olemassa jaottomien polynomien generoimat pääihanteet* $R_1, ..., R_s$ *ja maksimaaliset ihanteet* $M_1, ..., M_t$*, joille* $M_i \neq M_j$ *ja* $R_i \nsubseteq M_j$ *ja*

$$A = R_1 \cdots R_s M_1 \cdots M_t.$$

Lisäksi ihanteet ovat yksikäsitteisesti määrätyt ja ihanteet $R = R_1 \cdots R_s, M_1, ..., M_t$ *ovat pareittain maksimaalisia.*

Todistus. Väitöskirjassa [18]. □

4 Annihilaattori- ja jaksollistajaihanne

Tässä kappaleessa ollaan pääasiassa kiinnostuneita renkaista $\mathbb{C}[x^{\pm 1}]$ ja $\mathbb{C}[x^{\pm 1}, y^{\pm 1}]$. Tavoitteena on todistaa, että $\mathrm{Ann}(c)$ ja $\mathrm{Per}(c)$ ovat radikaaleja renkaassa $\mathbb{C}[x^{\pm 1}, y^{\pm 1}]$. Annihilaattori-ihanteen alkuihannehajotelmasta saadaan viivapolynomit käyttöön ja yksittäisen annihilaattorin normaalihajotelma antaa koko annihilaattori-ihanteelle rakenteellisia tuloksia. Tätä kautta saadaan itse annihiloitavasta konfiguraatiosta tietoa, erityisesti sen jaksollisuudesta. Jotta tutkielma olisi mahdollisimman itsenäinen kokonaisuus, ihanteiden rakennetodistukset on esitetty yksityiskohtaisesti tässä kappaleessa. Lähteenä on käytetty väitöskirjaa [18] ja joitain todistuksia on muunnettu asianyhteyteen sopivammaksi.

4.1 Perusominaisuuksia

Lemma 4.1. *Olkoon c äärellisen kokonaisaakkoston konfiguraatio ja $f \in \mathrm{Ann}(c)$ kokonaiskertoiminen nollasta poikkeava polynomi. On olemassa sellainen $r \in \mathbb{N}$, että kaikille ehdon $\mathrm{syt}(n, r) = 1$ toteuttaville luvuille $n \in \mathbb{N}$ on voimassa $f(X^n) \in \mathrm{Ann}(c)$.*

Todistus. Merkitään $f(X) = \sum_{\mathbf{v} \in D} a_{\mathbf{v}} X^{\mathbf{v}}$ ja olkoon $m \in \mathbb{Z}$ mielivaltainen. Määritellään $s = \max\{\, |c_{\mathbf{u}}| \sum_{\mathbf{v} \in D} |a_{\mathbf{v}}| \mid \mathbf{u} \in \mathbb{Z}^d \,\}$. Nyt pätee $|(f(X^m)c)_{\mathbf{v}}| \leqslant s$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$.

Olkoon $p > s$ alkuluku. Binomikaavasta seuraa, että kaikille $g \in \mathbb{Z}[X^{\pm 1}]$ on voimassa $g(X)^p \equiv g(X^p) \pmod p$. Oletetaan, että $f(X^m) \in \mathrm{Ann}(c)$ jollekin $m \in \mathbb{N}$. Nyt

$$0 = f(X^m)^p c(X) \equiv f(X^{mp}) c(X) \pmod p,$$

mistä seuraa $f(X^{mp})c(X) = 0$.

Olkoon $r = s!$ ja valitaan sellainen $n \in \mathbb{N}$, jolle $\mathrm{syt}(n, r) = 1$. Hajotetaan $n = p_1 p_2 \cdots p_k$ alkutekijöihin. Nyt jokaiselle alkuteikijälle pätee $p_i > s$. Helpolla induktiolla saadaan $f(X) \in \mathrm{Ann}(c) \implies f(X^{p_1 p_2 \cdots p_k}) = f(X^n) \in \mathrm{Ann}(c)$.

□

Merkitään kompleksiluvun $x = a + bi$ kompleksikonjugaattia $\bar{x} = a - bi$.

Lemma 4.2. *Olkoon c äärellisen kokonaisaakkoston konfiguraatio. Tällöin on olemassa äärellinen $F \subseteq \mathbb{Z}[X^{\pm 1}]$, jolle pätee $Ann(c) = \langle F \rangle$.*

Todistus. Etsitään aluksi mielivaltaiselle annihilaattorille esitys kokonaislukukertoimisten annihilaattorien avulla. Olkoon $f \in \mathrm{Ann}(c)$ ja merkitään

$$f = \sum_{i=1}^{n} f_{\mathbf{u}_i} X^{\mathbf{u}_i}, \text{ missä } f_{\mathbf{u}_i} \in \mathbb{C}.$$

Määritellään joukko $P = \{ (c_{\mathbf{v}-\mathbf{u}_1}, ..., c_{\mathbf{v}-\mathbf{u}_n}) \mid \mathbf{v} \in \mathbb{Z}^d \} \subseteq \mathbb{Z}^n$. Kerätään siis joukkoon jokaiselle $\mathbf{v} \in \mathbb{Z}^d$ se kuvio, joka määrää kertolaskun fc tuloksen kohdassa $\mathbf{v}$. Tarkastellaan vektorialiavaruutta $V = \langle P \rangle \subseteq \mathbb{C}^n$. Olkoon $g = \sum_{i=1}^{n} g_{\mathbf{u}_i} X^{\mathbf{u}_i}$. Nyt on voimassa

$$(\overline{g_{\mathbf{u}_1}}, ..., \overline{g_{\mathbf{u}_n}}) \in V^{\perp} \iff g \in \mathrm{Ann}(c).$$

Joukosta P voidaan valita äärellinen osajoukko $\mathcal{B}_V$, joka on kokonaislukukertoimisista vektoreista koostuva kanta aliavaruudelle V. Avaruudelle $V^{\perp}$ voidaan laskea rationaalikoordinaattinen kanta helposti luonnollisen $\mathbb{C}^n$ kannan ja $\mathcal{B}_V$ avulla. Skaalaamalla saadaan kokonaiskertoiminen kanta $\mathcal{B}_{V^{\perp}} = \{ \mathbf{b}^{(1)}, ..., \mathbf{b}^{(m)} \} \subseteq \mathbb{Z}^n$. Merkitään edelleen $\mathbf{b}^{(i)} = (b_1^{(i)}, ..., b_n^{(i)})$ ja määritellään polynomit $g^{(1)}, ..., g^{(m)}$ seuraavalla tavalla:

$$g^{(i)} = \sum_{j=1}^{n} b_j^{(i)} X^{\mathbf{u}_j}, \text{ missä } i = 1, ..., m.$$

Koska $\overline{\mathbf{b}^{(i)}} = \mathbf{b}^{(i)} \in V^{\perp}$, tiedetään että $g^{(i)} \in \mathrm{Ann}(c)$ kaikilla $i = 1, ..., m$. Nyt vektorille $\overline{\mathbf{a}} = (\overline{f_{\mathbf{u}_1}}, ..., \overline{f_{\mathbf{u}_n}}) \in V^{\perp}$ on olemassa kantaesitys $\sum_{i=1}^{m} c_i \mathbf{b}^{(i)}$, missä $c_i \in \mathbb{C}$. Edelleen $\mathbf{a} = \sum_{i=1}^{m} \overline{c_i} \mathbf{b}^{(i)}$. Nyt siis polynomille f pätee

$$f = \sum_{i=1}^{m} \overline{c_i} g^{(i)}.$$

Jokaiselle $\mathrm{Ann}(c)$ alkiolle löydetään vastaava esitys kokonaiskertoimisien annihilaattorien avulla. Tällöin joukolle $S = \mathrm{Ann}(c) \cap \mathbb{Z}[X^{\pm 1}]$ pätee $\langle S \rangle = \mathrm{Ann}(c)$. Lauseen 3.39 mukaan $\mathbb{C}[X^{\pm 1}]$ on Noetherin rengas ja lemman 3.27 mukaan on olemassa äärellinen $F \subseteq S$, jolla on voimassa $\langle F \rangle = \mathrm{Ann}(c)$. $\square$

Lemma 4.3. *Olkoon c äärellisen kokonaisaakkoston konfiguraatio ja $f = \sum a_{\mathbf{v}} X^{\mathbf{v}}$ sen epätriviaali kokonaisaakkoston annihilaattori. Olkoon r lauseen 4.1 luku ja $\mathbf{v}_0 \in supp(f)$. Määritellään*

$$g(X) = \prod_{\substack{\mathbf{v} \in supp(f) \\ \mathbf{v} \neq \mathbf{v}_0}} (X^{r(\mathbf{v}-\mathbf{v}_0)} - 1).$$

Tällöin $g \in \boldsymbol{IV}(Ann(c))$.

Todistus. Olkoon $\mathbf{Z} \in \mathbf{V}(\mathrm{Ann}(c))$. Osoitetaan, että $g(\mathbf{Z}) = 0$. Määritellään kompleksiluvun $\alpha \in \mathbb{C}$ avulla joukko $S_\alpha = \{\, \mathbf{v} \in \mathrm{supp}(f) \mid \mathbf{Z}^{r\mathbf{v}} = \alpha \,\}$ ja lisäksi polynomi

$$f_\alpha(X) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} X^{\mathbf{v}}.$$

Olkoot $\alpha_1, ..., \alpha_n$ ne luvut, joille $S_{\alpha_i} \neq \varnothing$. Näitä on vain äärellinen määrä, koska $\mathrm{supp}(f)$ on äärellinen. Huomataan myös, että $S_0 = \varnothing$, koska $\mathbf{Z} \in (\mathbb{C}^*)^d$. Täten joukot $S_{\alpha_1}, ..., S_{\alpha_n}$ muodostavat kantajan äärellisen partition. Todetaan, että

$$f(X) = f_{\alpha_1}(X) + \cdots + f_{\alpha_n}(X).$$

Olkoon nyt $k \in \mathbb{N}$. Nyt on voimassa $\mathrm{syt}(1 + kr, r) = 1$, joten 4.1 perusteella $f(X^{1+kr}) \in \mathrm{Ann}(c)$. Nyt siis $(f(X^{1+kr}))(\mathbf{Z}) = f(\mathbf{Z}^{1+kr}) = 0$. Valitaan mielivaltainen $\alpha \in \mathbb{C}$ ja lasketaan

$$f_\alpha(\mathbf{Z}^{1+kr}) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} (\mathbf{Z}^{\mathbf{v}(1+kr)}) = \sum_{\mathbf{v} \in S_\alpha} a_{\mathbf{v}} \mathbf{Z}^{\mathbf{v}} \alpha^k = f_\alpha(\mathbf{Z}) \alpha^k$$

Täten siis

$$0 = f(\mathbf{Z}^{1+kr}) = \sum_{i=1}^{n} f_{\alpha_i}(\mathbf{Z}^{1+kr}) = \sum_{i=1}^{n} f_{\alpha_i}(\mathbf{Z}) \alpha_i^k$$

Havaitaan, että edellinen kaava voidaan tulkita kahden vektorin kohtisuoruutena:

$$(\overline{f_{\alpha_1}(\mathbf{Z})}, \overline{f_{\alpha_2}(\mathbf{Z})}, ..., \overline{f_{\alpha_n}(\mathbf{Z})}) \perp (\alpha_1^k, \alpha_2^k, ..., \alpha_n^k)$$

Kohtisuoruus pätee siis kaikille $k \in \mathbb{N}$. Nyt tiedetään $\alpha_i \neq \alpha_j$ ja $\alpha_i, \alpha_j \neq 0$ kaikille $i, j \in \{ 1, \dots, n \}$, missä $i \neq j$. Nyt matriisi

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

muodostaa avaruuden $\mathbb{C}^n$ kannan, koska

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i) \neq 0.$$

Nyt täytyy siis olla $(\overline{f_{\alpha_1}(\mathbf{Z})}, \overline{f_{\alpha_2}(\mathbf{Z})}, ..., \overline{f_{\alpha_n}(\mathbf{Z})}) = \mathbf{0}$, joten erityisesti $f_{\alpha_i}(\mathbf{Z}) = 0$ sellaiselle i, jossa $\mathbf{v}_0 \in S_{\alpha_i}$. Muistetaan, että $f_{\alpha_i} = \sum_{\mathbf{v} \in S_{\alpha_i}} a_{\mathbf{v}} X^{\mathbf{v}}$ ja todetaan, että $a_{\mathbf{v}} \mathbf{Z}^{r\mathbf{v}} \neq 0$ kaikilla $\mathbf{v} \in S_{\alpha_i}$. Täten joukon S_{α_i} täytyy sisältää vähintään kaksi eri vektoria $\mathbf{v}, \mathbf{v}_0 \in S_{\alpha_i}$. Nyt $\mathbf{Z}^{r(\mathbf{v}-\mathbf{v}_0)} - 1 = 0$ ja täten siis $g(\mathbf{Z}) = 0$. □

4.2 Viivapolynomit

Tämän kappaleen lopussa todistetaan, että kaksiulotteisen konfiguraation jaksollistaja-ihanne voidaan muodostaa sellaisten polynomien avulla, joiden kantajat ovat yhdellä suoralla. Jos kiinnitetään yksi tietty suora ja tarkastellaan tämän suoran suuntaisia polynomeja, tarvitaan käyttöön vain yksi muuttuja. Tämä motivoi tässä alikappaleessa esitettävät uudet määritelmät ja hajotelmat.

Määritelmä 4.4. *(viivapolynomi, primitiivinen vektori, suunta)* Laurentin polynomia $\phi \in \mathbb{C}[X^{\pm 1}]$ kutsutaan *viivapolynomiksi*, jos $|\mathrm{supp}(\phi)| \geqslant 2$ ja on olemassa sellaiset vektorit $\mathbf{u} \in \mathbb{Z}^d, \mathbf{u}_0 \in \mathrm{supp}(\phi)$, joille $\mathrm{supp}(\phi) \subseteq \langle \mathbf{u} \rangle + \mathbf{u}_0$. Vektorin $\mathbf{u}$ koordinaateista voidaan jakaa yhteiset tekijät pois ja saadaan merkkiä vaille yksikäsitteinen $\mathbf{v} = (v_1, ..., v_d) \in \mathbb{Z}^d$, jolle $\mathrm{supp}(\phi) \subseteq \langle \mathbf{v} \rangle + \mathbf{u}_0$ ja $\mathrm{syt}(v_1, ..., v_d) = 1$. Tällaista vektoria $\mathbf{v}$ kutsutaan *primitiiviseksi* ja sen generoimaa alimodulia $\langle \mathbf{v} \rangle \subseteq \mathbb{Z}^d$ kutsutaan polynomin ϕ *suunnaksi*.

Määritelmä 4.5. (*normaalimuotoinen viivapolynomi*) Viivapolynomi ϕ, jonka suunta on $\langle \mathbf{v} \rangle$, voidaan esittää muodossa

$$\phi = X^{\mathbf{u}_0}(a_0 + a_1 X^{\mathbf{v}} + \cdots + a_n X^{n\mathbf{v}}),$$

missä $a_i \in \mathbb{C},\ n \geqslant 1,\ a_0 \neq 0$ ja $a_n \neq 0$. Kun sijoitetaan $t = X^{\mathbf{v}}$ ja unohdetaan siirtotermi, saadaan polynomista ϕ hyödyllinen yksinkertaistus yhdelle muuttujalle.

$$\phi' = a_0 + a_1 t + \cdots + a_n t^n.$$

Viivapolynomi ϕ' on *normaalimuodossa*, jos se on yhden muuttujan polynomi, jossa on nollasta poikkeava vakiotermi ja lisäksi pätee $\phi = X^{\mathbf{u}_0}\phi'(X^{\mathbf{v}})$. Normaalimuotoinen viivapolynomi on siis yhden muuttujan yksinkertaistus, joka sisältää usean muuttujan viivapolynomin olennaisen tiedon. Viivapolynomin ϕ normaalimuotoista esitystapaa merkataan ϕ'.

4.2.1 Viivapolynomihajotelmia

Määritelmä 4.6. ($\mathbf{v}$-*säie*) Konfiguraation $c = \sum_{\mathbf{v} \in \mathbb{Z}^d} a_{\mathbf{v}} X^{\mathbf{v}}$ määräämä $\mathbf{v}$-*säie* kohdassa $\mathbf{u}$ määritellään $\operatorname{fib}_{\mathbf{v}}(c, \mathbf{u}) = \sum_{i \in \mathbb{Z}} a_{\mathbf{u}+i\mathbf{v}} t^i$.

Säikeen määritelmää voidaan käyttää luontevasti myös Laurentin polynomille, kun se samaistetaan vastaavaan äärellisen kantajan konfiguraatioon.

Määritelmä 4.7. *(säiehajotelma)* Olkoon $c \in \mathbb{C}[[X^{\pm 1}]]$ konfiguraatio ja $\mathbf{v} \in \mathbb{Z}^d$ vektori. *Säiehajotelma* on erilaisten säikeiden joukko

$$S_{\mathbf{v}}(c) = \{\, \operatorname{fib}_{\mathbf{v}}(c, \mathbf{u}) \mid \mathbf{u} \in \mathbb{Z}^d \,\}.$$

Lause 4.8. *Konfiguraatio c on täysin jaksollinen jos ja vain jos $S_{\mathbf{v}}(c)$ on äärellinen kaikilla $\mathbf{v} \in \mathbb{Z}^d$.*

Todistus.

$\Longleftarrow$ Valitaan mielivaltainen suunta $\mathbf{v} \in \mathbb{Z}^d$. Olkoon $n = |S_{\mathbf{v}}(c)|$. Kiinnitetään jokin kohta $\mathbf{u} \in \mathbb{Z}^d$. Tarkastellaan säikeitä $\mathrm{fib}_{\mathbf{v}}(c, k\mathbf{v} + \mathbf{u})$, missä $k = 0, ..., n$. Lokeroperiaatteen mukaan on olemassa luvut $0 \leqslant k_1 < k_2 \leqslant n$, joille $\mathrm{fib}_{\mathbf{v}}(c, k_1\mathbf{v} + \mathbf{u}) = \mathrm{fib}_v(c, k_2\mathbf{v} + \mathbf{u})$. Laskemalla saadaan

$$(t^{k_2-k_1} - 1)\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}) = t^{k_2}\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u} + k_1\mathbf{v}) - \mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}) =$$
$$t^{k_2}\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u} + k_2\mathbf{v}) - \mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}) = 0.$$

Säie $\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u})$ on siis jaksollinen suuntaan $\mathbf{v}$. Eri vektorien $u \in \mathbb{Z}^d$ antamien säikeiden jaksoilla on yläraja n, joten mielivaltaisella säikeellä $\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u})$ on jakso $n!\mathbf{v}$. Koska suunta $\mathbf{v}$ on mielivaltainen, konfiguraatio c on täysin jaksollinen.

$\Longrightarrow$ Oletetaan nyt, että konfiguraatio c on täysin jaksollinen. Lauseen 2.8 mukaan on olemassa $n \in \mathbb{Z} \setminus \{ 0 \}$, jolle pätee $(X^{n\mathbf{v}} - 1)c = 0$ kaikilla $\mathbf{v} \in \mathbb{Z}^d$. Tietysti mielivaltaiselle säikeelle pätee siis $(t^n - 1)\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}) = 0$. Olkoon $K = \{ (u_1, u_2, ..., u_d) \in \mathbb{Z}^d \mid 0 \leqslant u_i < n \text{ kaikilla } i = 1, .., d \}$. Nyt saadaan

$$S_{\mathbf{v}}(c) = \bigcup_{\mathbf{u} \in K} \{ \mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}),\ t\,\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}),\ t^2\,\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}),\ ...,\ t^{n-1}\,\mathrm{fib}_{\mathbf{v}}(c, \mathbf{u}) \}.$$

□

Määritelmä 4.9. *(normaalihajotelma)* Olkoon f Laurentin polynomi ja $\mathbf{v}$ primitiivinen vektori. Polynomin f *normaalihajotelma* suuntaan $\mathbf{v}$ määritellään $\mathrm{N}_{\mathbf{v}}(f) = \{ \mathrm{fib}_{\mathbf{v}}(f, \mathbf{u}) \mid \mathrm{fib}_{\mathbf{v}}(f, \mathbf{u}) \text{ on normaalimuodossa} \}$.

Seuraavaksi tulos, joka näyttää että normaalihajotelman tekeminen on hyvinmääritelty operaatio.

Lause 4.10. *Normaalihajotelma on aina olemassa ja se määräytyy yksikäsitteisesti polynomista f ja suunnasta* $\mathbf{v}$

Todistus. Olkoon $\mathbf{u} \in \text{supp}(f)$. Olkoon $k \in \mathbb{N}$ suurin luonnollinen luku, jolle pätee $\mathbf{u} - k\mathbf{v} \in \text{supp}(f)$. Nyt polynomi $\text{fib}_{\mathbf{v}}(f, \mathbf{u} - k\mathbf{v})$ on yksikäsitteinen normaalimuotoinen säie, joka sisältää vektorin $\mathbf{u}$. □

Määritelmä 4.11. (*siirtovakiot*) Määritellään *siirtovakiot* joukkona $O_{\mathbf{v}}(f) = \{\, \mathbf{u} - k\mathbf{v} \mid \mathbf{u} \in \text{supp}(f), k = \max\{\, n \in \mathbb{N} \mid \mathbf{u} - k\mathbf{v} \in \text{supp}(f) \,\} \,\}$. Nämä ovat siis ne kohdat, joista luetaan normaalihajotelman säikeet.

Määritelmä 4.12. (*normaaliesitys*) Olkoon $O_{\mathbf{v}}(f) = \{\, \mathbf{u}_1, ..., \mathbf{u}_n \,\}$. Otetaan kaikille $i = 1, ..., n$ siirtovakiota vastaava säie $\phi'_i = \text{fib}_{\mathbf{v}}(c, \mathbf{u}_i) \in N_{\mathbf{v}}(f)$. Kutsutaan Laurentin polynomin esitystä muodossa $f = \sum_{i=1}^{n} X^{\mathbf{u}_i} \phi'_i(X^{\mathbf{v}})$ polynomin f *normaaliesitykseksi.*

Lause 4.13. *Polynomin f normaaliesitys on aina olemassa järjestystä vaille yksikäsitteisesti.*

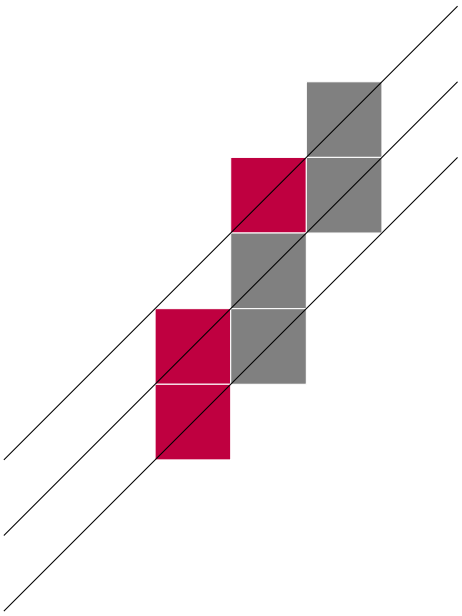
Todistus. Normaalihajotelman määritelmästä seuraa, että normaaliesitys on aina olemassa. Siirtovakioiden yksikäsitteisyydestä seuraa normaaliesityksen yksikäsitteisyys. □

Lause 4.14. *On olemassa algoritmi polynomin f normaaliesityksen ja normaalihajotelman muodostamiseen.*

Todistus. Merkitään $f = \sum a_{\mathbf{u}} X^{\mathbf{u}}$. Olkoon nyt $\mathbf{v}$ primitiivinen vektori ja $\mathbf{u} \in \text{supp}(f)$. Lasketaan suurin $k \in \mathbb{N}$ jolle $\mathbf{u} - k\mathbf{v} \in \text{supp}(f)$. Merkitään $\mathbf{z} = \mathbf{u} - k\mathbf{v}$. Nyt säie kohdassa $\mathbf{z}$ voidaan laskea hakemalla suurin $n \in \mathbb{N}$, jolle $\mathbf{z} + n\mathbf{v} \in \text{supp}(f)$. Nyt polynomi $X^{\mathbf{z}}(a_{\mathbf{z}} + a_{\mathbf{z}+\mathbf{v}} X^{\mathbf{v}} + \cdots + a_{\mathbf{z}+n\mathbf{v}} (X^{\mathbf{v}})^n)$ on haluttu normaaliesityksen termi. Kun jätetään siirtovakio huomioimatta ja sijoitetaan $t = X^{\mathbf{v}}$, saadaan tämän kohdan normaalihajotelman säie $a_{\mathbf{z}} + a_{\mathbf{z}+\mathbf{v}} t + \cdots + a_{\mathbf{z}+n\mathbf{v}} t^n$. Tallennetaan muistiin saadut polynomit sekä siirtovakio $\mathbf{z}$ ja toistetaan operaatio kaikille polynomin f kantajan vektoreille. Jos vektoria vastaava siirtovakio löytyy tallennettujen siirtovakioiden joukosta, tämä säie on jo käyty läpi ja siirrytään seuraavaan. □

Käytetään tätä algoritmia esimerkkipolynomin normaalihajotelman ja normaaliesityksen muodostamiseen.

Esimerkki 4.15. Tarkastellaan polynomin $f = 1 + y + xy + xy^2 + xy^3 + x^2y^3 + x^2y^4$ normaalihajotelmaa suuntaan $\mathbf{v} = (1, 1)$.



Etsitään aluksi siirtovakiot kun oletetaan origon olevan vasemmassa alakulmassa. Suoraviivaisella laskemisella huomataan, että siirtovakioiden joukko on $\{ (0,0), (0,1), (1,3) \}$. Nämä kohdat polynomin kantajassa näkyvät kuvassa punaisina soluina. Polynomi voidaan sieventää siirtovakioiden avulla normaaliesitykseksi:

$$f = 1 + xy + y(1 + xy + x^2y^2) + xy^3(1 + xy),$$

joten normaalihajotelma on $N_{\mathbf{v}}(f) = \{ 1 + t, 1 + t + t^2 \}$.

Esimerkki 4.16. Olkoon ϕ viivapolynomi suuntaan $\mathbf{v}$. Tällöin $N_{\mathbf{v}}(\phi) = \{ \phi' \}$.

Lause 4.17. *Tulo $\phi_1\phi_2$ on viivapolynomi suuntaan* $\mathbf{v}$ *jos ja vain jos ϕ_1 ja ϕ_2 ovat viivapolynomeja suuntaan* $\mathbf{v}$ *tai toinen on monomi.*

Todistus.

$\Longleftarrow$ Jos toinen on monomi, väite pätee. Olkoot $\phi_1, \phi_2 \in \mathbb{C}[X^{\pm 1}]$ viivapolynomeja suuntaan $\langle \mathbf{v} \rangle$. Otetaan normaaliesitykset $\phi_1 = X^{\mathbf{u}_1}\phi_1'(X^{\mathbf{v}})$ ja $\phi_2 = X^{\mathbf{u}_2}\phi_2'(X^{\mathbf{v}})$. Kahden normaaliesityksen tulo viivapolynomien tapauksessa on myös normaaliesitys. Täten $\phi_1\phi_2 = X^{\mathbf{u}_1+\mathbf{u}_2}\phi_1'(X^{\mathbf{v}})\phi_2'(X^{\mathbf{v}})$ on viivapolynomi suuntaan $\langle \mathbf{v} \rangle$.

$\Longrightarrow$ Oletetaan nyt, että $\phi = \phi_1\phi_2$ on viivapolynomi suuntaan $\langle \mathbf{v} \rangle$. Otetaan normaaliesitys $\phi = X^{\mathbf{u}}(a_0 + a_1X^{\mathbf{v}} + \cdots + a_n(X^{\mathbf{v}})^n)$. Hajotetaan polynomi $\phi' = a_0 + a_1t + \cdots + a_nt^n$ jaottomiin lineaarisiin tekijöihin

$$a_0 + a_1t + \cdots + a_nt^n = \psi_1'\psi_2' \cdots \psi_n',$$

missä $\psi_i' = a_0^{(i)} + a_1^{(i)}t$. Kun sijoitetaan $t = X^v$, saadaan

$$a_0 + a_1X^{\mathbf{v}} + \cdots + a_nX^{n\mathbf{v}} = \psi_1'(X^{\mathbf{v}})\psi_2'(X^{\mathbf{v}}) \cdots \psi_n'(X^{\mathbf{v}}),$$

missä $\psi_i'(X^{\mathbf{v}}) = a_0^{(i)} + a_1^{(i)}X^{\mathbf{v}}$ ovat selvästi jaottomia polynomeja ja ne ovat viivapolynomeja suuntaan $\langle \mathbf{v} \rangle$ tai monomeja. Näistä jaottomista tekijöistä ja monomeista $X^{\mathbf{u}}$ voidaan rakentaa kaikki polynomin ϕ tekijät. Erityisesti ϕ_1 ja ϕ_2 ovat viivapolynomeja suuntaan $\langle \mathbf{v} \rangle$ tai toinen on monomi.

□

Määritellään polynomijoukoulle A ja polynomille f kertolasku luonnolliseen tapaan $fA = \{\, fg \mid g \in A \,\}$. Kahden polynomijoukon A ja B kertolasku määritellään $AB = \{\, fg \mid f \in A, g \in B \,\}$.

Lause 4.18. *Olkoon f Laurentin polynomi ja ϕ viivapolynomi suuntaan $\langle \mathbf{v} \rangle$. Tällöin $N_{\mathbf{v}}(\phi f) = \phi' N_{\mathbf{v}}(f)$.*

Todistus. Otetaan polynomien f ja ϕ normaaliesitykset $f = \sum_{i=1}^{n} X^{\mathbf{u}_i} \phi_i'(X^{\mathbf{v}})$, $\phi = X^{\mathbf{u}} \phi'(X^{\mathbf{v}})$. Kerrotaan polynomin f normaaliesitys puolittain polynomilla ϕ. Saadaan normaaliesitys tulolle

$$\phi f = \phi \sum_{i=1}^{n} X^{\mathbf{u}_i} \phi_i'(X^{\mathbf{v}}) = \sum_{i=1}^{n} X^{\mathbf{u}_i + \mathbf{u}} \phi'(X^{\mathbf{v}}) \phi_i'(X^{\mathbf{v}}).$$

Täten normaalihajotelmalle pätee $N_{\mathbf{v}}(\phi f) = \{\, \phi' \phi_i' \mid i = 1, ..., n \,\} = \phi' N_{\mathbf{v}}(f)$. □

4.2.2 Viivapolynomiannihilaattorit

Lause 4.19. *Äärellisen aakkoston konfiguraatio c on jaksollinen jos ja vain jos sillä on viivapolynomiannihilaattori.*

Todistus. Jos c on jaksollinen, niin viivapolynomi $X^{\mathbf{v}} - 1 \in \mathrm{Ann}(c)$ jollekin $\mathbf{v} \in \mathbb{Z}^d$. Oletetaan nyt, että $\phi \in \mathrm{Ann}(c)$ ja olkoon $\langle \mathbf{v} \rangle$ sen suunta. Olkoon $e \in S_{\mathbf{v}}(c)$ mielivaltainen. Merkitään $\phi' = a_0 + a_1 t + \cdots a_n t^n$. Olkoon $k \in \mathbb{Z}$. Nyt

$$(\phi' e)_k = \sum_{i=0}^{n} e_{k-i} a_i = 0,$$

mistä saadaan

$$e_k = -\frac{1}{a_0} \sum_{i=1}^{n} e_{k-i} a_i$$

ja

$$e_{k-n} = -\frac{1}{a_n} \sum_{i=0}^{n-1} e_{k-i} a_i.$$

Sana $w = e_{[k-n,\ldots,k-1]}$ määrittelee yksikäsitteisesti kohdan e_k arvon ja vastaavasti $e_{[k-n+1,\ldots,k]}$ määrittelee kohdan e_{k-n}. Induktiolla saadaan, että koko konfiguraatio määräytyy yksikäsitteisesti sanasta $e_{[k-n,\ldots,k]}$. Huomataan myös, että sanan w pituus riippuu ainoastaan polynomin ϕ' asteesta. Koska aakkosto on äärellinen, lokeroperiaatteen nojalla on olemassa sellaiset kokonaisluvut $k_1 < k_2$, joille $e_{[k_1-n,\ldots,k_1-1]} = e_{[k_2-n,\ldots,k_2-1]}$ eli $e_{k_1+q} = e_{k_2+q}$ kaikilla $q \in \mathbb{Z}$, joten $(t^{k_2-k_1} - 1)e = 0$. Merkitään $p_w = k_2 - k_1$. Jaksoa voidaan

kasvattaa, jotta se saadaan riippumattomaksi säikeestä e. Määritellään siis

$$p = \prod_{w \in \Sigma^n} p_w$$

ja todetaan, että $(t^p - 1)e = 0$. Koska $e \in S_{\mathbf{v}}(c)$ on mielivaltainen, saadaan $(X^{p\mathbf{v}} - 1)c = 0$. □

Korollaari 4.20. *Äärellisen aakkoston konfiguraatio $c \in \mathbb{C}[[x^{\pm 1}]]$ on jaksollinen jos ja vain jos sillä on epätriviaali annihilaattori.*

Todistus. Kaikki yhden muuttujan polynomit voidaan tulkita viivapolynomeiksi. Sovelletaan nyt lausetta 4.19. □

Todistetaan tulos, jota hyödynnetään myöhemmin kaksiulotteisille konfiguraatioille. Yksiulotteisten äärellisen kokonaisaakkoston konfiguraatioiden annihilaattori-ihanne on radikaali.

Lemma 4.21. *Olkoon $c \in \mathbb{C}[[x^{\pm 1}]]$ äärellisen kokonaisaakkoston konfiguraatio ja $f^m \in Ann(c)$. Tällöin $f \in Ann(c)$.*

Todistus. Tapauksessa $f = 0$ väite pätee. Oletetaan, että $f \neq 0$. Nyt korollaarin 4.20 nojalla c on jaksollinen, joten on olemassa sellainen $n \in \mathbb{N}$, jolle $x^n - 1 \in \mathrm{Ann}(c)$. Eukleideen algoritmilla saadaan $g = \mathrm{syt}(x^n - 1, f^m) \in \mathrm{Ann}(c)$. Tiedetään, että polynomilla $x^n - 1$ on vain yksinkertaisia nollakohtia, joten $\mathrm{syt}(x^n - 1, f^m) = \mathrm{syt}(x^n - 1, f)$ ja tästä saadaan $g \mid f$. Nyt siis $f = hg \in \mathrm{Ann}(c)$. □

Lemma 4.22. *Olkoon c äärellisen kokonaisaakkoston konfiguraatio, $\phi_1, ..., \phi_n$ viivapolynomeja ja luvut $k_1, ..., k_n$, joille $\phi_1^{k_1}\phi_2^{k_2}\cdots\phi_n^{k_n} \in Ann(c)$. Tällöin $\phi_1\phi_2\cdots\phi_n \in Ann(c)$.*

Todistus. Olkoon $\mathbf{v}_1$ viivapolynomin ϕ_1 suunta ja otetaan jokin $e \in S_{\mathbf{v}_1}(\phi_2^{k_2}\cdots\phi_n^{k_n}c)$. Merkitään $\phi_1' \in N_{\mathbf{v}}(\phi_1)$. Nyt tietysti $(\phi_1')^{k_1} \in \mathrm{Ann}(e)$ ja lemman 4.21 nojalla $\phi_1' \in \mathrm{Ann}(e)$. Koska valittu säie oli mielivaltainen, saadaan $\phi_1 \in \mathrm{Ann}(\phi_2^{k_2}\cdots\phi_n^{k_n}c)$ eli $\phi_1\phi_2^{k_2}\cdots\phi_n^{k_n} \in \mathrm{Ann}(c)$. Helpolla induktiolla saadaan edelleen $\phi_1\cdots\phi_n \in \mathrm{Ann}(c)$. □

4.3 Radikaalisuus

Lemma 4.23. *Olkoon c äärellisen kokonaisaakkoston konfiguraatio, jolla on epätriviaali annihilaattori. Tällöin on olemassa keskenään erisuuntaiset vektorit $\boldsymbol{v}_1, ..., \boldsymbol{v}_m \in \mathbb{Z}^d$, joille*

$$(X^{\boldsymbol{v}_1} - 1) \cdots (X^{\boldsymbol{v}_m} - 1) \in Ann(c).$$

Todistus. Olkoon $g \in \mathbf{IV}(\mathrm{Ann}(c))$ lemman 4.3 mukainen polynomi. Nyt Hilbertin nollakohtalauseen nojalla $g \in \sqrt{\mathrm{Ann}(c)}$. Otetaan nyt sellainen $m \in \mathbb{N}$, jolle $g^m \in \mathrm{Ann}(c)$. Koska g^m on viivapolynomien eksponenttien tulo, voidaan soveltaa lemmaa 4.22 ja todeta, että $g \in \mathrm{Ann}(c)$.

Jos polynomissa g on kaksi viivapolynomitekijää $(X^{a\mathbf{u}} - 1)$ ja $(X^{b\mathbf{u}} - 1)$ samaan suuntaan, voidaan tarkastella polynomin $X^{ab\mathbf{u}} - 1$ kahta tekijöihinjakoa:

$$X^{ab\mathbf{u}} - 1 = (X^{a\mathbf{u}} - 1)(1 + X^{a\mathbf{u}} + \cdots + {}^{(b-1)a\mathbf{u}}) = (X^{b\mathbf{u}} - 1)(1 + X^{b\mathbf{u}} + \cdots + X^{(a-1)b\mathbf{u}}).$$

Molemmat tekijät $X^{a\mathbf{u}} - 1$ ja $X^{b\mathbf{u}} - 1$ jakavat siis polynomin $X^{ab\mathbf{u}} - 1$. Korvataan siis tekijä $(X^{a\mathbf{u}} - 1)(X^{b\mathbf{u}} - 1)$ polynomilla $(X^{ab\mathbf{u}} - 1)^2$ ja lemman 4.22 nojalla eksponentti voidaan hävittää. Samansuuntaiset tekijät voidaan siis korvata yhdellä tekijällä $X^{abu} - 1$. Jatketaan polynomitekijöiden korvaamista, kunnes kaikki tekijät ovat eri suuntiin. □

Lause 4.24. *Olkoon $c \in \mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ äärellisen kokonaisaakkoston konfiguraatio, jolla on epätriviaali annihilaattori. Tällöin $Ann(c)$ on radikaali ja lisäksi $Ann(c)$ alkuihannehajotelman jokainen alkuihanne P on muotoa*

$$P = \langle x^a y^b - \omega \rangle \text{ tai } P = \langle x - \omega_x, y - \omega_y \rangle$$

missä $(a, b) \in \mathbb{Z}^2$ on primitiivinen ja $\omega, \omega_x, \omega_y \in \mathbb{C}$ ovat ykkösenjuuria.

Todistus. Merkitään $A = \sqrt{\mathrm{Ann}(c)}$. Konfiguraatiolla c on epätriviaali annihilaattori, joten A on myös epätriviaali. Koska A on radikaali, voidaan lauseen 3.40 avulla tehdä alkuihannehajotelma

$$A = P_1 \cap P_2 \cap \cdots \cap P_n.$$

Olkoon $i \in \{1, ..., n\}$ ja merkitään $P = P_i$. Muistetaan lauseesta 3.41 renkaan $\mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ alkuihanteet. Oletetaan ensin, että $P = \langle \varphi \rangle$ jollekin jaottomalle φ. Lemman 4.23 nojalla on olemassa sellaiset eri suuntaiset vektorit $\mathbf{v}_1, ..., \mathbf{v}_n$, että

$$f = (X^{\mathbf{v}_1} - 1) \cdots (X^{\mathbf{v}_n} - 1) \in \mathrm{Ann}(c).$$

Tiedetään, että $\mathrm{Ann}(c) \subseteq A \subseteq P$, joten $f \in P$. Koska P on pääihanne, saadaan $\varphi \mid f$. Polynomin φ jaottomuudesta voidaan päätellä edelleen, että

$$\varphi \mid (X^{\mathbf{v}} - 1)$$

jollekin $\mathbf{v} \in \mathbb{Z}^2$. Olkoon nyt $d > 0$ se luonnollinen luku, jolle $\mathbf{v} = d\mathbf{w}$ ja $\mathbf{w}$ on primitiivinen. Nyt hajotetaan jaottomiin tekijöihin

$$X^{\mathbf{v}} - 1 = X^{d\mathbf{w}} - 1 = (X^{\mathbf{w}} - \omega_1) \cdots (X^{\mathbf{w}} - \omega_d)$$

ja todetaan, että $\varphi = X^{\mathbf{w}} - \omega = x^a y^b - \omega$ jollekin primitiiviselle $(a, b) \in \mathbb{Z}^2$.

Oletetaan nyt, että $P = \langle x - \alpha, y - \beta \rangle$. Osoitetaan, että α ja β ovat ykkösenjuuria. Valitaan mielivaltainen $g \in \prod_{j \neq i} (P_j \setminus P)$. Todetaan, että $g(x - \alpha) \in A$. Täten siis $g^m (x - \alpha)^m \in \mathrm{Ann}(c)$ jollekin $m \in \mathbb{N}$. Koska P on alkuihanne ja polynomin g kaikki tekijät ovat ihanteen P ulkopuolella, tiedetään, että $g \notin P$. Lisäksi helpolla induktiolla saadaan $g^m \notin P$ ja edelleen $g^m \notin \mathrm{Ann}(c)$. Nyt siis $(x - \alpha)^m$ annihiloi äärellisen aakkoston konfiguraation $c' = g^m c$. Lemman 4.22 nojalla myös $(x - \alpha) \in \mathrm{Ann}(c')$. Nyt siis

$$c'_{i,j} = c'_{0,j} \alpha^{-i}$$

ja jotta konfiguraatio c' pysyy äärellisen aakkoston konfiguraationa, on luvun α oltava ykkösenjuuri. Sama päättely pystytään toistamaan kun tarkastellaan lukua β. Voidaan siis merkitä $\alpha = \omega_x$ ja $\beta = \omega_y$.

Pitää vielä todistaa, että $\mathrm{Ann}(c)$ on radikaali ihanne. Lauseen 3.42 nojalla $A = P_1 P_2 \cdots P_n$. Kaikki ihanteet P_i ovat viivapolynomien generoimia. Täten ihanteelle A on olemassa polynomit $s_1, ..., s_k$, missä jokainen s_i on viivapolynomien tulo ja

$$A = \langle s_1, ..., s_k \rangle.$$

Jokaiselle s_i on olemassa luku $m \in \mathbb{N}$, jolle $s_i^m \in \mathrm{Ann}(c)$. Nyt lemman 4.22 nojalla $s_i \in \mathrm{Ann}(c)$. Tällöin siis $A \subseteq \mathrm{Ann}(c)$ ja todetaan, että $\mathrm{Ann}(c) = A$. $\mathrm{Ann}(c)$ on siis radikaali. □

Maksimaaliset ihanteet sisältävät viivapolynomeja kaikkiin suuntiin. Tämä on olennainen tulos jaksollistajaihanteen $\mathrm{Per}(c)$ rakenteen kannalta.

Lause 4.25. *Olkoon $M \leqslant \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ maksimaalinen ihanne ja v primitiivinen vektori. Tällöin M sisältää viivapolynomin suuntaan v.*

Todistus. Merkitään $\mathbf{v} = (v_x, v_y)$. Lauseen 3.41 mukaan $M = \langle x - \alpha, y - \beta \rangle$. Nyt selvästi $\mathbf{V}(M) = \{ (\alpha, \beta) \}$ ja edelleen $\mathbf{IV}(M) = \{ f \mid f(\alpha, \beta) = 0 \}$. Hilbertin nollakohtalauseen mukaan $\mathbf{IV}(M) = \sqrt{M}$ ja koska M on maksimaalinen, saadaan $\sqrt{M} = M$. Merkitään $\phi = x^{v_x} y^{v_y} - \alpha^{v_x} \beta^{v_y}$ ja todetaan, että $\phi(\alpha, \beta) = 0$. Nyt siis $\phi \in \mathbf{IV}(M) = M$ ja se on viivapolynomi suuntaan $\mathbf{v}$. □

Yleistetään edellistä tulosta mielivaltaisille maksimaalisten ihanteiden tuloille

Lause 4.26. *Olkoon $H = M_1 \cdots M_n$, missä $M_i \leqslant \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ ovat maksimaalisia ihanteita ja $\boldsymbol{v}$ primitivinen vektori. Tällöin H sisältää viivapolynomin suuntaan $\boldsymbol{v}$.*

Todistus. Valitaan edellisen lauseen avulla $\phi_1, ..., \phi_m$, missä ϕ_i on viivapolynomi suuntaan $\mathbf{v}$ ja $\phi_i \in M_i$. Nyt $\phi = \phi_1 \cdots \phi_m$ on viivapolynomi suuntaan $\mathbf{v}$ ja $\phi \in H$. □

Lause 4.27. *Olkoon $c \in \mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ äärellisen kokonaisaakkoston konfiguraatio, jolla on epätriviaali annihilaattori. Tällöin $Per(c) = \langle \phi \rangle$, missä $\phi = \phi_1 \cdots \phi_m$ ja ϕ_i ovat viivapolynomeja eri suuntiin. Lisäksi $\phi = \psi_1 \cdots \psi_k$, missä ψ_i ovat jaottomia erisuuria viivapolynomeja.*

Todistus. Olkoon $\mathrm{Ann}(c) = P_1 \cdots P_k M_1 \cdots M_n$ alkuihannnehajotelma. Merkitään $P = P_1 \cdots P_k$ ja $H = M_1 \cdots M_n$. Tarkastellaan jaottomia viivapolynomeja $\psi_1, ..., \psi_k$, joille $P_i = \langle \psi_i \rangle$. Nyt viivapolynomit ψ_i ovat korkeintaan m eri suuntaan $\mathbf{v}_1, ..., \mathbf{v}_m$, jossa $m \leqslant k$. Nyt alkuihannehajotelman 3.40 sisältymisehdosta seuraa, että $\psi_i \neq \psi_j$ aina, kun $i \neq j$. Olkoon nyt ϕ_i tulo kaikista polynomeista ψ_j suuntaan $\mathbf{v}_i$. Nyt polynomit $\phi_1, ..., \phi_m$ ovat viivapolynomeja eri suuntiin ja lisäksi $P = \langle \phi_1 \cdots \phi_m \rangle = \langle \psi_1 \cdots \psi_k \rangle$. Merkitään $\phi = \phi_1 \cdots \phi_m$. Lauseen 4.26 mukaan voidaan ottaa kaksi erisuuntaista viivapolynomia $h_1, h_2 \in H$. Nyt $\phi h_1 \in \mathrm{Ann}(c)$ ja $\phi h_2 \in \mathrm{Ann}(c)$. Nyt siis ϕc on täysin jaksollinen ja täten $\langle \phi \rangle \subseteq \mathrm{Per}(c)$.

Oletetaan nyt, että $f \in \mathrm{Per}(c)$. Valitaan primitiivinen vektori $\mathbf{v} \in \mathbb{Z}^2 \setminus \{ \mathbf{v}_1, -\mathbf{v}_1, ..., \mathbf{v}_m, -\mathbf{v}_m \}$. Valitaan viivapolynomi $\psi \in \mathrm{Ann}(fc)$, joka on suuntaan $\mathbf{v}$. Tällainen ψ on olemassa, koska fc on täysin jaksollinen. Nyt siis $\psi f \in \langle \phi \rangle H$. Kaikki polynomin ϕ jaottomat tekijät l ovat viivapolynomeja johonkin suuntaan $\mathbf{v}_i$, missä $i \in \{1, ..., m\}$, joten $l \nmid \psi$. Koska kuitenkin $\phi \mid \psi f$, saadaan $\phi \mid f$. Täten $f \in \langle \phi \rangle$.

Väitteet seuraavat kahdesta esitystavasta $\phi = \phi_1 \cdots \phi_m = \psi_1 \cdots \psi_k$. □

Lause 4.28. *Äärelliselle kokonaisaakkoston konfiguraatiolle $c \in \mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ ihanne $Per(c)$ on radikaali.*

Todistus. Jatketaan edellisen lauseen merkinnöillä. Muistetaan, että $\mathrm{Per}(c) = \langle \psi_1 \rangle \cdots \langle \psi_k \rangle$, missä ψ_i ovat erisuuria jaottomia viivapolynomeja. Jaottomuudesta ja erisuuruudesta seuraa, että $\langle \psi_i \rangle \cap \langle \psi_j \rangle = \langle \psi_i \rangle \cdot \langle \psi_j \rangle$. Täten $\mathrm{Per}(c) = \langle \psi_1 \rangle \cap \cdots \cap \langle \psi_k \rangle$. Alkuihanteet ovat radikaaleja ja radikaalien ihanteiden leikkaus on radikaali. □

Määritellään äärellisen kokonaisaakkoston konfiguraation c kertaluvuksi $\mathrm{ord}(c)$ lauseen 4.27 luku m.

Lause 4.29. *Tarkastellaan kertalukua ord(c).*

- *ord$(c) = 0$ jos ja vain jos c on täysin jaksollinen.*
- *ord$(c) = 1$ jos ja vain jos c on yhteen suuntaan jaksollinen.*
- *ord$(c) \geqslant 2$ jos ja vain jos c ei ole jaksollinen.*

Todistus.

1) Jos $\mathrm{ord}(c) = 0$ niin $\mathrm{Per}(c) = \langle 1 \rangle$, joten konfiguraatio $1c = c$ on kahteen suuntaan jaksollinen. Oletetaan nyt, että c on täysin jaksollinen ja valitaan kaksi erisuuntaista normaalimuotoista viivapolynomia $\phi_1, \phi_2 \in \mathrm{Ann}(c)$. Nyt siis $\mathrm{syt}(\phi_1, \phi_2) = 1 \in \mathrm{Ann}(c) \subseteq \mathrm{Per}(c)$. Täten $\mathrm{ord}(c) = 0$.

2 Olkoon nyt $\mathrm{ord}(c) = 1$. Tällöin $\mathrm{Per}(c) = \langle \psi \rangle$ jollekin viivapolynomille ψ suuntaan v. Nyt siis ψc on täysin jaksollinen ja on olemassa sellainen viivapolynomi γ suuuntaan v, jolle $\psi\gamma c = 0$. Koska $\psi\gamma$ on viivapolynomiannihilaattori, konfiguraatio c on jaksollinen. Toisaalta koska $\mathrm{Ann}(c) \subseteq \langle \psi \rangle$ sisältää vain yhdensuuntaisia viivapolynomeja, konfiguraatio c on täsmälleen yhteen suuntaan jaksollinen. Jos c on yhteen suuntaan jaksollinen, on jaksollistaja-ihanteessa viivapolynomeja ainoastaan yhteen suuntaan. Tällöin lauseesta 4.27 saadaan $m = 1$.

3) Olkoon nyt $\mathrm{ord}(c) \geqslant 2$. Tällöin mikään viivapolynomi $X^{\mathbf{v}} - 1$ ei voi annihiloida konfiguraatiota c. Jos oletetaan, että c ei ole jaksollinen, on lauseen 4.27 luku $m \geqslant 2$, koska $m \leqslant 1$ takaa viivapolynomiannihilaattorin olemassalon.

□

4.4 Diskreetin geometrian työkaluja

Määritellään hieman diskreetin geometrian käsitteitä, jotta tuloksista saa algoritmisesti käyttökelpoisempia. Olkoon $\mathbf{v} = (v_x, v_y) \in \mathbb{Z}^2$ jokin suunta ja määritellään $\mathbf{v}^\perp = (-v_y, v_x)$.

Määritelmä 4.30. (*suljettu puolitaso, avoin puolitaso, puolitason reuna*)

- *Suljettu puolitaso* on $\overline{H_\mathbf{v}} = \{\, \mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{x} \cdot \mathbf{v}^\perp \geqslant 0 \,\}$.
- *Avoin puolitaso* määritellään $H_\mathbf{v} = \{\, \mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{x} \cdot \mathbf{v}^\perp > 0 \,\}$.
- *Puolitason reuna* on $\partial\overline{H_\mathbf{v}} = \overline{H_\mathbf{v}} \backslash H_\mathbf{v} = \{\, \mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{x} \cdot \mathbf{v}^\perp = 0 \,\}$.
- Äärellisellä joukolla $D \subseteq \mathbb{Z}^2$ on *ulkoreuna suuntaan* $\mathbf{v} \in \mathbb{Z}^2$ jos on olemassa sellainen $\mathbf{x} \in \mathbb{Z}^2$, että $D \subseteq \overline{H_\mathbf{v}} + \mathbf{x}$ ja joukossa $D \cap (\mathbf{x} + \partial\overline{H_\mathbf{v}})$ on ainakin kaksi pistettä.

Lemma 4.31. *Olkoot g ja h nollasta poikkeavia Laurentin polynomeja. Oletetaan, että joukolla $\mathrm{supp}(g)$ on ulkoreuna suuntaan $\boldsymbol{v}$. Tällöin myös joukolla $\mathrm{supp}(gh)$ on ulkoreunta suuntaan $\boldsymbol{v}$.*

Todistus. On olemassa vektori $\mathbf{x} \in \mathbb{Z}^2$ viivapolynomi ϕ suuntaan $\mathbf{v}$, jolle $\mathrm{supp}(g) \subseteq \overline{H_\mathbf{v}} + \mathbf{x}$ ja $\mathrm{supp}(g - \phi) \subseteq H_\mathbf{v} + \mathbf{x}$. On myös olemassa vektori $\mathbf{y}$ ja $\psi \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$, joka on viivapolynomi suuntaan $\mathbf{v}$ tai monomi, joille $\mathrm{supp}(h) \subseteq \overline{H_\mathbf{v}} + \mathbf{y}$ ja $\mathrm{supp}(h - \psi) \subseteq H_\mathbf{v} + \mathbf{y}$. Nyt saadaan $\mathrm{supp}(gh) \subseteq \overline{H_\mathbf{v}} + \mathbf{x} + \mathbf{y}$ ja $\mathrm{supp}(gh - \psi\phi) \subseteq H_\mathbf{v} + \mathbf{x} + \mathbf{y}$, jossa $\psi\phi$ on viivapolynomi suuntaan $\mathbf{v}$. Täten polynomilla gh on ulkorena suuntaan $\mathbf{v}$. □

Lause 4.32. *Olkoon g Laurentin polynomi, jolla on viivapolynomitekijä suuntaan $\boldsymbol{v}$. Tällöin joukolla $\mathrm{supp}(g)$ on ulkoreuna suuntaan $\boldsymbol{v}$.*

Todistus. Hajotetaan polynomi $g = \phi f$, missä ϕ on viivapolynomi suuntaan v. Nyt joukolla $\mathrm{supp}(\phi)$ on ulkoreuna suuntaan v, joten edellisen lauseen nojalla myös tulolla ϕf on ulkoreuna suuntaan v. □

Lause 4.33. *Olkoon f Laurentin polynomi. On olemassa algoritmi joukon $supp(f)$ ulkoreunojen etsimiseen.*

Todistus. Olkoon $\mathbf{x}, \mathbf{y} \in \text{supp}(f)$ mielivaltainen pari vektoreita ja etsitään primitiivinen vektori $\mathbf{v}$, jolle $k\mathbf{v} = \mathbf{x} - \mathbf{y}$ jollekin $k \in \mathbb{Z}$. Tarkastetaan nyt, onko joukolla $\text{supp}(f)$ vektorin $\mathbf{v}$ suuntaista ulkoreunaa. Toistetaan tämä kaikille pareille $\mathbf{x}, \mathbf{y} \in \text{supp}(f)$. □

Lause 4.34. *Olkoon $f \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ polynomi ja $c \in \mathbb{C}[[x^{\pm 1}, y^{\pm 1}]]$ sellainen äärellisen kokonaisaakkoston konfiguraatio, että $f \in Per(c)$.*

- *Jos normaalihajotelmassa $N_{\boldsymbol{v}}(f)$ ei ole yhteisiä tekijöitä millekään $\boldsymbol{v} \in \mathbb{Z}^2$, missä $\boldsymbol{v}$ on joukon $supp(f)$ reunan suuntainen primitiivinen vektori, niin c on täysin jaksollinen.*
- *Jos normaalihajotelmassa $N_{\boldsymbol{v}}(f)$ on yhteisiä tekijöitä täsmälleen yhdelle joukon $supp(f)$ reunan suuntaiselle primitiiviselle vektorille $\boldsymbol{v}$, niin c on jaksollinen suuntaan $\boldsymbol{v}$*

Todistus. Sovelletaan todistuksessa lemmaa 4.31. Ensimmäisessä tapauksessa $\text{ord}(c) = 0$, joten väite seuraa. Jos normaalihajotelmassa $N_{\mathbf{v}}(f)$ on yhteinen tekijä etumerkkiä lukuunottamatta täsmälleen yhdelle primitiiviselle vektorille $\mathbf{v}$, on $\text{ord}(c) \leqslant 1$ ja täten c on jaksollinen. □

Yleisesti ottaen jos $f \in \text{Per}(c)$ ja polynomilla f on viivapolynomitekijöitä vähintään kahteen suuntaan, ei konfiguraation c jaksollisuutta tai jaksottomuutta pysty suoraan päättelemään näillä tiedoilla. Yhden tietyn jaksollistajan f viivapolynomitekijöiden lukumäärä on ainoastaan yläraja kertaluvulle.

5 Sovellukset peittokoodeihin

Tässä kappaleessa ajatellaan koodausteoriassa käsiteltäviä peittokoodeja tietyn laatan asetteluina konfiguraation osoittamiin kohtiin. Peittokoodin laatasta saadaan siis pienellä muokkauksella konfiguraation jaksollistaja. Toisaalta, kun rajotutaan binääriaakkostoon, kiinnitettyä laattaa vastaavat peittokoodit muodostavat äärellistä tyyppiä olevan siirtoaliavaruuden. Kappaleessa käytetään koodausteorian käsitteistön lähteinä luentomonisteita [6, 7]. Annetaan uusi todistus artikkelin [2] neliöhilatulokselle ja todistetaan uutena tuloksena kuningasgraafia koskeva peittokoodien jaksollisuustulos.

5.1 Peittokoodien peruskäsitteitä

Määritelmä 5.1. (*graafi, pistejoukko, viivajoukko, pallo*) *Graafi* on pari $G = (V, E)$, missä $V \neq \varnothing$ on *pistejoukko* ja $E \subseteq \{ \{ u, v \} \mid u, v \in V, u \neq v \}$ on *viivajoukko*. Tässä yhteydessä graafit ovat siis suuntaamattomia. Graafissa kahden pisteen $u, v \in V$ etäisyys $d(u, v)$ määritellään näitä yhdistävän lyhimmän polun viivojen lukumääräksi. Määritellään graafissa *r-säteinen pallo* $B_r(u) = \{ v \in V \mid d(u, v) \leqslant r \}$. [7]

Olkoot $a, b, r \in \mathbb{N}$. Epätyhjä joukko $C \subseteq V$ on $(r, a, b) - peittokoodi$, jos kaikille $c \in C$ ja $x \in V \setminus C$ pätee $|B_r(c) \cap C| = a$ ja $|B_r(x) \cap C| = b$. Tässä kappaleessa rajoitutaan $kokonaislukugraafeihin$, jossa $V = \mathbb{Z}^2$. Neliöhila on graafi, jossa kahden pisteen välillä on viiva jos vain jos pisteestä saadaan toinen muuttamalla koordinaattia yhdellä. Kuningasgraafissa otetaan mukaan myös diagonaalit ja sen nimi kuvastaa kuninkaan liikkumista shakissa.

Määritelmä 5.2. (*neliöhila, kuningasgraafi*) Olkoon pistejoukko $V = \mathbb{Z}^2$ ja $d_E : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{R}$ tavanomainen Euklidinen etäisyys. Graafia $G = (V, E)$ kutsutaan

- *neliöhilaksi*, jos $\{ u, v \} \in E \iff d_E(u, v) = 1$ tai
- $kuningasgraafiksi$, jos $\{ u, v \} \in E \iff d_E(u, v) \leqslant \sqrt{2}$.

Määritellään kokonaislukugraafissa myös yleisempi peittokoodien perhe, joka avaa luontevan yhteyden peittokoodien ja polynomien välille.

Määritelmä 5.3. (*(S,a,b)-peittokoodi*) Olkoon $S \subseteq \mathbb{Z}^2$ äärellinen joukko ja $C \subseteq \mathbb{Z}^2$. Koodi C on $(S, a, b) - peittokoodi$, jos kaikille $\mathbf{c} \in C$ ja $\mathbf{x} \in \mathbb{Z}^2 \setminus C$ pätee $|(\mathbf{c} + S) \cap C| = a$ ja $|(\mathbf{x} + S) \cap C| = b$.

Lause 5.4. *Kokonaislukugraafissa (r, a, b)-peittokoodi on (S, a, b)-peittokoodi, missä $S = B_r(0)$.*

Todistus. Olkoon $\mathbf{v} \in \mathbb{Z}^2$. Selvästi $B_r(\mathbf{v}) = B_r(0) + \mathbf{v}$ ja väite seuraa, kun merkitään $S = B_r(0)$. □

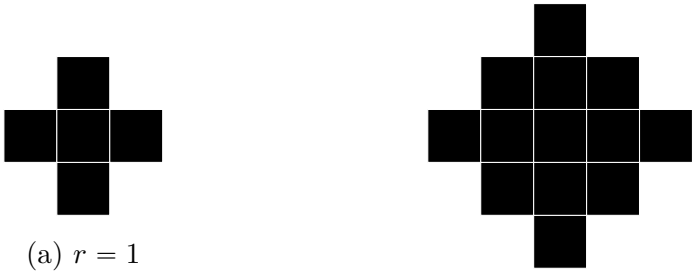
Määritellään nyt äärelliselle joukolle $S \subseteq \mathbb{Z}^2$ polynomi $f_S = \sum_{\mathbf{v} \in S} X^{\mathbf{v}}$. Muutetaan (S, a, b)-peittokoodi C konfiguraatioksi $c(X) = \sum_{\mathbf{v} \in C} X^v$. Peittokoodin määritelmästä seuraa, että $f_S c(X) = (a-b)c(X) + b\mathbb{1}$. Sieventämällä saadaan $(f_S + a - b)c(X) = a\mathbb{1}$, eli toisin sanoen konfiguraatio $c(X)$ on polynomin $f_S + a - b$ eräs a-laatoittaja. Lisäksi voidaan päätellä $f_S + a - b \in \mathrm{Per}(c)$. Lause 4.34 antaa polynomin $f_S + a - b$ viivapolynomitekijöiden avulla tuloksia konfiguraation c jaksollisuudesta. Tämä avaa uudenlaisen algebrallisen näkökulman peittokoodien tutkimukseen.

Koodausteoriassa peittokoodien yhteydessä käytetään binääriaakkostoa, joten myös laatat ja konfiguraatiot tässä kappaleessa ovat aakkoston $\{0, 1\}$ yli. Nyt siis kiinnitettyä laattaa $f_S + a - b$ vastaavien a-laatoittajien joukko on SFT, missä kiellettyjä kuvioita ovat $\{(-S, p) \mid \sum_{\mathbf{v} \in -S} p_{\mathbf{v}} \neq a\}$. Eli jos $S \subseteq \mathbb{Z}^2$ on äärellinen joukko, niin (S, a, b)-peittokoodien joukko on SFT.

Tässä kappaleessa on todistettu neliöhilan ja kuningasgraafin peittokoodituloksia yksinkertaisesti viivapolynomien avulla. Lopuksi esitetään muita peittokoodiesimerkkejä ja tarkastellaan erikoistapauksia, joissa on viivapolynomitekijöitä kahteen suuntaan.

5.2 Neliöhila

Esitellään artikkelin [2] neliöhilan peittokoodituloksille uudet todistukset algebrallisella näkökulmalla.



(a) $r = 1$

(b) $r = 2$

Kuva 3: Neliöhilan laatat säteillä $r = 1$ ja $r = 2$.

Lause 5.5. *Neliöhilassa kaikki* $(1, a, b)$*-peittokoodit, missä* $b - a \neq 1$*, ovat täysin jaksollisia.*

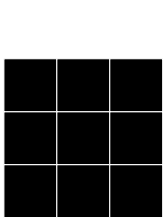
Todistus. Olkoon ensin $S = \{ (x, y) \in \mathbb{Z}^2 \mid |x| + |y| \leqslant 1\}$. Jos $b - a \neq 1$, niin joukon S reunojen suuntaiselle vektorille $\mathbf{v} \in \{ (1, 1), (-1, 1) \}$ pätee $N_{\mathbf{v}}(f_S + a - b) = \{ 1 + t, 1 + a - b \}$ ja täten polynomilla f ei ole viivapolynomitekijöitä minkään reunan suuntaisesti. Eli mielivaltainen peittokoodi on jaksollinen. □

Lause 5.6. *Neliöhilassa* (r, a, b) *koodit, missä* $r \geqslant 2$*, ovat täysin jaksollisia.*

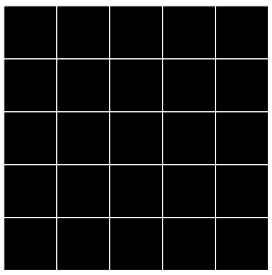
Todistus. Olkoon $S = \{ (x, y) \in \mathbb{Z}^2 \mid |x| + |y| \leqslant r \}$, missä $r \geqslant 2$. Olkoon $\mathbf{v}$ joukon S reunan suuntainen, eli $\mathbf{v} \in \{ (1, 1), (-1, 1) \}$. Kun tarkastellaan kahta säiettä siirtovakioilla $\mathbf{u}_1 = (0, -r), \mathbf{u}_2 = (0, -r+1)$, havaitaan $\mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_1) = 1 + t + \cdots + t^r \in N_{\mathbf{v}}(f_S + a - b)$ ja $\mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_2) = 1 + t + \cdots + t^{r-1} \in N_{\mathbf{v}}(f_S + a - b)$. Koska $\mathrm{syt}(\mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_1), \mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_2)) = 1$, ei normaalihajotelmalla ole yhteisiä tekijöitä ja täten mielivaltainen peittokoodi on jaksollinen. □

5.3 Kuningasgraafi

Esitellään jaksollisuustulos peittokoodeille kuningasgraafissa.



(a) $r = 1$



(b) $r = 2$

Kuva 4: Kuningasgraafin laatat säteillä $r = 1$ ja $r = 2$.

Lause 5.7. *Kuningasgraafissa kaikki (r, a, b)-koodit, missä $a \neq b$, ovat täysin jaksollisia.*

Todistus. Olkoon $r \geqslant 1$, $a \neq b$ ja $S = \{\, (x, y) \in \mathbb{Z}^2 \mid \max\{|x|, |y|\} \leqslant r \,\}$. Olkoon $\mathbf{v}$ jälleen joukon S reunan suuntainen, eli $\mathbf{v} \in \{\, (0, 1), (1, 0) \,\}$. Jos $\mathbf{v} = (1, 0)$, voidaan valita siirtovakiot $\mathbf{u}_1 = (-r, 0)$ ja $\mathbf{u}_2 = (-r, 1)$ ja todetaan, että $\mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_1) = 1 + t + \cdots + t^{r-1} + (1 + a - b)t^r + t^{r+1} + \cdots + t^{2r}$ ja $\mathrm{fib}_{\mathbf{v}}(f_S + a - b, \mathbf{u}_2) = 1 + t + \cdots + t^{2r}$. Näillä kahdella säikeellä ei ole yhteisiä tekijöitä. Sama päättely voidaan toistaa myös pystysuunnassa, joten mielivaltainen peittokoodi C on jaksollinen. □

5.4 Muita peittokoodiesimerkkejä

Yleistetään nyt artikkelin [15] esimerkkiä n-pakkaajille. Tulos on alunperin todistettu artikkelissa [19]. Tämä tulos todistetaan d-ulotteisessa tapauksessa, joten peittokoodeja koskeva erikoistapaus seuraa korollaarina.

Lause 5.8. *Olkoon $D \subseteq \mathbb{Z}^d$ joukko, jolle $|D| = p$ jollekin alkuluvulle p ja määritellään laatta $f = \sum_{\boldsymbol{v} \in D} X^{\boldsymbol{v}}$. Tälle laatalle n-pakkaajat ovat jaksollisia kaikkiin suuntiin $p(\boldsymbol{u} - \boldsymbol{v})$, missä $\boldsymbol{u} \neq \boldsymbol{v}$ ja $\boldsymbol{u}, \boldsymbol{v} \in D$.*

Todistus. Olkoon $c(X) \in \mathbb{C}[[X^{\pm 1}]]$ jokin laatan f n-pakkaaja. Pakkausehto antaa $f(X)c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} nX^{\mathbf{v}}$. Kerrotaan puolittain polynomilla f^{p-1} ja saadaan

$$f^p(X)c(X) = \sum_{\mathbf{v} \in \mathbb{Z}^d} np^{p-1} X^{\mathbf{v}} \equiv 0 \pmod{p}.$$

Lisäksi, koska p on alkuluku, nähdään binomikaavasta

$$f^p(X) \equiv f(X^p) \pmod{p}.$$

Olkoon nyt $\mathbf{u} \in \mathbb{Z}^d$ mielivaltainen. Tällöin

$$f(X^p)c(X)_{\mathbf{u}} = \sum_{\mathbf{v} \in D} c(X)_{\mathbf{u}-\mathbf{v}} \equiv 0 \pmod{p}.$$

Nyt siis polynomi $f(X^p)$ antaa ainoastaan alkuluvulla p jaollisia kertoimia kun kerrotaan pakkaajalla $c(X)$. Olkoot $\mathbf{w} \in \operatorname{supp}(c)$ ja $\mathbf{u} \in D$ mielivaltaisia. Tällöin

$$f(X^p)c(X)_{\mathbf{w}+p\mathbf{u}} = \sum_{\mathbf{v} \in D} c(X)_{\mathbf{w}+p\mathbf{u}-p\mathbf{v}} \equiv 0 \pmod{p}.$$

Nyt summassa on ainakin termi $c(X)_{\mathbf{w}+p\mathbf{u}-p\mathbf{u}} = c(X)_{\mathbf{w}} = 1$. Koska summa on jaollinen luvulla p, tiedetään että kaikkien summattavien termien on oltava 1. Tällöin $\mathbf{w} + p(\mathbf{u} - \mathbf{v}) \in \operatorname{supp}(c)$ kaikilla $\mathbf{u}, \mathbf{v} \in D$, eli $c(X)$ on jaksollinen minkä tahansa vektorin $p(\mathbf{u} - \mathbf{v})$ suuntaan. □

Korollaari 5.9. *Olkoon $S \subseteq \mathbb{Z}^2$ joukko, jolle $|S| = p$ jollekin alkuluvulle p. Tällöin (S, a, a)-koodi on jaksollinen kaikkiin suuntiin $p(\boldsymbol{u} - \boldsymbol{v})$, missä $\boldsymbol{u} \neq \boldsymbol{v}$ ja $\boldsymbol{u}, \boldsymbol{v} \in S$.*

Todistus. Laatta f_S toteuttaa edellisen lauseen ehdot. □

Tarkastellaan nyt tapausta, jossa on yhteisiä viivapolynomitekijöitä kahteen suuntaan. Annetaan esimerkeiksi kaksi polynomia, joilla on viivapolynomitekijöitä kahteen suuntaan, mutta erilaiset jaksollisuusominaisuudet. Todistetaan nämä tapaukset tavanomaisella kombinatorisella päättelyllä.

Lause 5.10. *Olkoon* $S = \{ (0,0), (0,1), (1,0), (1,1) \}$. *Kaikki* (S, a, a)*-koodit ovat jaksollisia.*

Todistus. Nyt $f_S = 1+x+y+xy$, missä $N_{\mathbf{v}}(f) = \{ 1+t \}$ vektoreille $\mathbf{v}_1 = (0,1)$ ja $\mathbf{v}_2 = (1,0)$, joten polynomilla on viivapolynomitekijöitä kahteen suuntaan. Koska $|S| = 4$, riittää tarkastella tapaukset $a = 1, 2, 3, 4$. Jokaisessa joukossa $S + \mathbf{x}$, missä $\mathbf{x} \in \mathbb{Z}^2$, esiintyy täsmälleen a koodisanaa. Tapaukset $a = 1$ ja $a = 3$ ovat värin vaihtoa vaille sama, joten käydään kolme eri tapausta läpi.

1) $a = 4$**.** Nyt koodi on selvästi konfiguraatio $c = \sum_{\mathbf{v} \in \mathbb{Z}^2} X^{\mathbf{v}}$.

2) $a = 1$**.** Olkoon $\mathbf{u} = (u_1, u_2) \in \mathbb{Z}^2$ mielivaltainen vektori, jolle $c(X)_{\mathbf{u}} = 1$. Nyt, jotta kuviot saadaan sopimaan siirtoaliavaruuteen, konfiguraatiossa täytyy olla $c(X)_{\mathbf{u}+k(2,0)} = 1$ kaikilla $k \in \mathbb{Z}$ tai $c(X)_{\mathbf{u}+k(0,2)} = 1$ kaikilla $k \in \mathbb{Z}$. Tarkastellaan näistä toista, koska tapaukset ovat samanlaisia. Jos $c(X)_{\mathbf{u}+k(2,0)} = 1$ kaikilla $k \in \mathbb{Z}$, niin peiton mahdollistamiseksi c rakentuu pystysuuntaan jaksolliseksi. Täten $c(X)$ on jaksollinen.

3) $a = 2$**.** Huomataan, että ainakin shakkilautakuvio

$$c(X)_v = \begin{cases} 1 & v_1 + v_2 \equiv 0 \pmod 2 \\ 0 & \text{muutoin} \end{cases}$$

kuuluu koodiin. Voidaan myös vaihtaa värit ja saadaan vastakkainen shakkilautakuvio $\overline{c(X)} = 1 - c(X)$, joka myös kuuluu peittokoodiin.

Oletetaan nyt, että konfiguraatiossa $c(X)$ on kaksi samaa kerrointa vierekkäin pysty- tai vaakasuunnassa. Oletetaan, että samat bitit xx esiintyvät vierekkäin vaakasuunnassa, koska toinen tapaus menee samalla tavalla. Olkoon $w = \mathrm{fib}_{(1,0)}(c, \mathbf{u})$ sellainen vaakarivi, joka sisältää bitit xx. Nyt vierekkäisten bittien ylä- ja alapuolella lukee $\bar{x}\bar{x}$ ja tämän havainnon avulla ylä- ja alapuolella olevat rivit määräytyvät yksikäsitteisesti: $\mathrm{fib}_{(1,0)}(c, \mathbf{u} + (\pm 1, 0)) = \overline{w}$. Nyt induktiolla koko konfiguraatio määräytyy yksikäsitteisesti pystysuunnassa jaksolliseksi.

□

Lause 5.11. *Olkoon nyt* $S = \{ (\pm 1, 0), (0, \pm 1) \}$*. On olemassa jaksottomia* (S, a, a)*-koodeja.*

Todistus. Nyt $f_S = x^{-1} + y^{-1} + x + y$ ja $N_{\mathbf{v}}(f_S) = \{ 1 + t \}$ molemmille $\mathbf{v} = (1, \pm 1)$. On siis olemassa viivapolynomitekijöitä kahteen suuntaan. Olkoot $H_1 = \{ (v_1, v_2) \in \mathbb{Z}^2 \mid v_1 + v_2 \equiv 0 \bmod 2 \}$ ja $H_2 = H_1 + (1, 0)$ kaksi kokonaislukuhilan alihilaa. Nyt, jos $C \subseteq H_1$ ja $c = \sum_{\mathbf{v} \in C} X^{\mathbf{v}}$, niin $\mathrm{supp}(f_S c) \subseteq H_2$. Vastaavasti, jos $C \subseteq H_2$ ja $c = \sum_{\mathbf{v} \in C} X^{\mathbf{v}}$, niin $\mathrm{supp}(f_S c) \subseteq H_1$. Koodi voidaan siis hajottaa kahteen erilliseen osaan $H_1 \cap C$ ja $H_2 \cap C$, jotka peittävät eri alihiloihin kuuluvia pisteitä. Nämä alihilat voidaan ajatella vastaamaan lauseen 5.10 tilannetta, joten otetaan kaksi yhteen suuntaan jaksollista koodia ja asetetaan ne eri alihiloille. Jos jaksot ovat eri suuntiin, saatu $(S, 1, 1)$-peittokoodi on jaksoton. □

5.5 Algoritminen näkökulma

Lause 5.12. *On olemassa algoritmi Laurentin polynomin $f \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ viivapolynomitekijöiden löytämiseksi.*

Todistus. Tarkastellaan kantajaa $\text{supp}(f)$. Lauseen 4.34 nojalla riittää tarkastella ainoastaan reunojen suuntaisia vektoreita, joten lasketaan reunojen suuntavektorit algoritmilla 4.33 ja valitaan niistä mielivaltainen $\mathbf{v}$. Lasketaan polynomin f normaalihajotelma $N_{\mathbf{v}}(f) = \{ f_1, ..., f_n \}$. Tähän on olemassa algoritmi 4.14 nojalla. Lasketaan Eukleideen algoritmilla $\text{syt}(f_1, ..., f_n)$.

□

Lause 5.13. *Jos polynomilla $f_S + a - b \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$ on viivapolynomitekijöitä korkeintaan yhteen suuntaan, kysymys (S, a, b)-peittokoodien olemassaolosta on algoritmisesti ratkeava.*

Todistus. Lauseen 4.34 nojalla kaikki polynomin $f_S + a - b$ laatoittajat c ovat jaksollisia. Nyt algoritmi saadaan lauseesta 2.16. □

6 Yhteenveto

Tämän tutkielman alussa esiteltiin laajasti algebrallisen symbolidynamiikan peruskäsitteitä, jotta tutkielman voisi lukea mahdollisimman suppeilla esitietovaatimukslla. Tämän jälkeen rakennettiin jaksollistaja- ja annihilaattoriihanteiden teoriaa viivapolynomien avulla. Tutkielman teoriaosuus kulminoituu lauseeseen 4.29, jossa todistetaan yhteys konfiguraation jaksollisuuden ja kertaluvun välillä. Toinen tärkeä tulos on lause 4.34, joka antaa käytännöllisen ja visuaalisesti hahmotettavan työkalun konfiguraation kertaluvun rajoittamiseksi ylhäältä. Kappaleessa 5 sovelletaan tätä lausetta peittokooditulosten todistamiseen. Seuraavaksi alikappaleessa 5.4 annetaan sellaisia esimerkkejä, joiden yhteyttä algebralliseen näkökulmaan ei toistaiseksi tunneta. Lopuksi annetaan algoritmi, jolla voidaan etsiä laatoittajia siinä tapauksessa, kun viivapolynomitekijöitä on korkeintaan yhteen suuntaan. Tulevaisuudessa voisi olla mielekästä etsiä tuloksia, jotka antavat tiilen avulla alarajoja tiilittäjän kertaluvulle. Toinen mielenkiintoinen suunta olisi useampiulotteinen tapaus, jonka algebrallinen näkökulma on avoin, koska annihilaattoriihanteen radikaalisuutta ei tunneta tässä tapauksessa.

Viitteet

[1] Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969.

[2] Maria Axenovich. On multiple coverings of the infinite rectangular grid with balls of constant radius. *Discrete Mathematics*, pages 31–48, 2003.

[3] Julien Cassaigne. Subword complexity and periodicity in two or more dimensions. *Developments in Language Theory*, pages 14–21, 1999.

[4] David A. Cox, John Little, and Donal OShea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, 2007.

[5] W. Fulton. *Algebraic curves: an introduction to algebraic geometry.* Addison-Wesley Pub. Co., Advanced Book Program, 1989.

[6] Iiro Honkala. *Coding Theory I.* 2013. luentomoniste.

[7] Iiro Honkala. *Coding Theory II.* 2013. luentomoniste.

[8] Jarkko Kari. *Symbolic dynamics*. 2017. luentomoniste.

[9] Jarkko Kari. Low-complexity tilings of the plane. *Descriptional Complexity of Formal Systems - 21st*, pages 35–45, 2019.

[10] Jarkko Kari. *Tilings and Patterns*. 2019. luentomoniste.

[11] Jarkko Kari and Etienne Moutot. Nivat's conjecture and pattern complexity in algebraic subshifts. *Theoretical Computer Science*, pages 379 – 386, 2019.

[12] Jarkko Kari and Etienne Moutot. Decidability and periodicity of low complexity tilings. *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*, pages 14:1–14:12, 2020.

[13] Jarkko Kari and Michal Szabados. An algebraic geometric approach to multidimensional words. *Algebraic Informatics*, pages 29–42, 2015.

[14] Jarkko Kari and Michal Szabados. An algebraic geometric approach to nivat's conjecture. *Automata, Languages, and Programming - 42nd International Colloquium, ICALP*, pages 273–285, 2015.

[15] Jarkko Kari and Michal Szabados. An algebraic geometric approach to nivat's conjecture. *Information and Computation*, 2020.

[16] Tauno Metsänkylä. *Algebra*. 2004. luentomoniste.

[17] M Nivat. Invited talk at icalp, 1997.

[18] Michal Szabados. *An Algebraic Approach to Nivat's Conjecture*. Number 234 in TUCS Dissertations. 2018.

[19] M. Szegedy. Algorithms to tile the infinite grid with finite clusters. *Proceedings 39th Annual Symposium on Foundations of Computer Science*, pages 137–145, 1998.

[20] Jussi Väisälä. *Topologia II*. Limes ry, 2015.