TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Saana Wallius

Paleyn graafit laajennusaksioomien malleina

Luonnontieteiden tiedekunta
Matematiikka
Toukokuu 2018

Tampereen yliopisto
Luonnontieteiden tiedekunta
WALLIUS, SAANA: Paleyn graafit laajennusaksioomien malleina
Pro gradu -tutkielma, 37 s.
Matematiikka
Toukokuu 2018

Tiivistelmä

Tutkielmassa tarkastellaan Paleyn graafeja ja laajennusaksioomia. Erityisesti osoitetaan, että Paleyn graafit ovat laajennusaksioomien malleja.

Graafien käsittelyä tutkielmassa pohjustetaan esittelemällä tarpeellista käsitteistöä. Esitellään satunnaisgraafin käsite, jonka avulla tarkastellaan graafien ominaisuuksia. Graafien ominaisuuksista tarkastellaan erityisesti laajennusaksioomia. Laajennusaksioomissa yleisesti ottaen vaaditaan, että jokaiselle graafin tietyn kaltaiselle solmujen osajoukolle on olemassa eri solmu, joka on liitetty osajoukon solmuihin vaaditulla tavalla. Laajennusaksioomista tutkielmassa erityisesti käsitellään k-laajennusaksioomia, ja osoitetaan, että k-laajennusaksioomien toteuttavia graafeja on aina olemassa ja että tämän ominaisuuden asymptoottinen todennäköisyys on 1.

Paleyn graafien käsittelyä varten määritellään neliönjäännös ja siihen liittyvä Legendren symboli. Käydään läpi näihin liittyviä tuloksia ja tarvittavia arvioita. Esitellään myös karakterin käsite, joka on tarpeellinen pääväittämämme todistuksessa. Määritellään Paleyn graafit, jonka jälkeen lopuksi todistetaan pääväite, että riittävän suuret Paleyn graafit toteuttavat k-laajennusaksioomat.

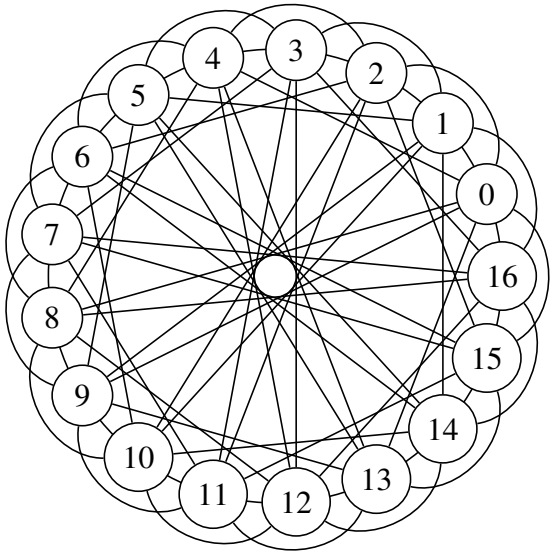
Sisältö

1 Johdanto

Paleyn graafi määritellään seuraavasti: Olkoon q alkuluku, jolle $q \equiv 1 \pmod 4$. Paleyn graafin P_q solmujen joukko on kunta $\mathbb{Z}_q$ ja särmät määräytyvät siten, että kahden mielivaltaisesti valitun solmun x ja y välillä on särmä, mikäli $x - y$ on neliö joukossa $\mathbb{Z}_q$ [3, s. 315]. Paleyn graafit ovat nimetty englantilaisen matemaatikon Raymond Paleyn (1907–1933) mukaan. Kuviossa 1.1 on kuvattu Paleyn graafi P_{17}.

Paleyn graafit ovat siitä erityinen graafien perhe, että riittävän suuret Paleyn graafit toteuttavat graafien ominaisuuden, jota kutsutaan k-laajennusaksioomiksi. Laajennusaksioomissa yleisesti ottaen vaaditaan, että jokaiselle graafin tietyn kaltaiselle solmujen osajoukolle on olemassa eri solmu, joka on liitetty osajoukon solmuihin vaaditulla tavalla [4]. Laajennusaksioomakäsitteen ovat alun perin esitelleet matemaatikot Alfréd Rényi ja Paul Erdős.

Erityisesti graafi toteuttaa k-laajennusaksiooman, jos seuraava ehto toteutuu: jokaiselle solmujen osajoukoille X ja Y, joille $|X| = |Y| = k$, on olemassa eri solmu, joka on naapuri joukon X solmujen kanssa, mutta ei minkään joukon Y solmun kanssa [2]. Edelleen, vaikka k-laajennusaksiooma on yksinkertaista määritellä, ominaisuuden toteuttavia graafeja on todettu olevan vaikeaa konstruoida. Tutkielman tehtävänä on todistaa, että Paleyn graafit toteuttavat tämän ominaisuuden.



Kuvio 1.1: Tutkielman kirjoittajaa on innoittanut
myös Paleyn graafien esteettinen puoli. Paleyn graafi P_{17}. (Vrt. [17].)

Tutkielman tekninen toteutus ja esittäminen etenevät niin, että ensin esitellään graafeihin liittyvää peruskäsitteistöä, jonka jälkeen perehdytään tarkemmin laajennusaksioomiin ja lopulta Paleyn graafeihin. Luvussa 2 esitellään graafien peruskäsitteistön lisäksi käsite satunnaisgraafi. Satunnaisgraafi on reaalista satunnaismuuttujaa

muistuttava käsite, ja tämän avulla tarkastellaan graafien ominaisuuksia ja ominaisuuksien todennäköisyyksiä. Esitellään myös asymptoottisen todennäköisyyden käsite. Luvun lopuksi perehdytään erityisesti k-laajennusaksioomiin.

Luvussa 3 osoitetaan satunnaisgraafin käsitteen avulla, että k-laajennusaksiooman toteuttavia graafeja on aina olemassa. Osoitamme myös, että k-laajennusaksioomien asymptoottinen todennäköisyys on 1.

Luvussa 4 perehdytään tarkemmin Paleyn graafeihin. Aloitetaan käymällä läpi Paleyn graafien käsittelyssä hyödyllistä käsitteistöä, kuten neliönjäännökset ja niihin liittyvä käsite Legendren symboli. Esitellään esimerkki Paleyn graafista ja osoitetaan lopuksi, että Paleyn graafit toteuttavat k-laajennusaksioomat, eli ovat k-laajennusaksioomien malleja.

Lukijalta edellytetään perustietämystä todennäköisyyslaskennasta ja lukuteoriasta. Erityisesti lukuteorian osalta tietämystä edellytetään modulaariaritmetiikasta. Graafiteorian osalta esitys pohjautuu Diestelin teokseen *Graph Theory* [5] ja lukuteorian osalta Rosenin teokseen *Elementary number theory and its applications* [13]. Päälähteenä tutkielmassa toimii Blassin, Exoon ja Hararyn artikkeli *Paley Graphs Satisfy All First-Order Adjacency Axioms* [2]. Tutkielmassa esitetyt kuviot ovat saaneet innoituksen WolframMathWorld -verkkosivustolta [17]. Esimerkit ja lauseiden todistukset, joissa ei ole lähdeviittausta, ovat tutkielman kirjoittajan itsensä kirjoittamia.

2 Graafit

Luvussa 2 käydään läpi graafien peruskäsitteistöä ja perehdytään graafeihin liittyviin todennäköisyyksiin. Esitellään satunnaisgraafin käsite, jonka avulla tarkastellaan graafien ominaisuuksia ja niiden asymptoottista todennäköisyyttä. Lopuksi perehdytään tarkemmin graafien ominaisuuteen, jota kutsutaan laajennusaksioomiksi.

2.1 Graafien peruskäsitteitä

Luvussa päälähteenä on käytetty Diestelin teosta *Graph Theory* [5, s. 2–13] ja Koiviston ja Niemistön luentomonistetta *Graafiteoriaa* [7]. Aloitetaan määrittelemällä graafin käsite.

Määritelmä 2.1. *Yksinkertainen graafi* on pari $G = (V, E)$, joka rakentuu äärellisestä joukosta $V \neq \emptyset$ ja järjestämättömien parien joukosta E, jolle

$$E \subseteq \{\{x, y\} \mid x, y \in V \text{ ja } x \neq y\}.$$

Joukon V alkioita kutsutaan *solmuiksi* ja joukon E alkioita kutsutaan *särmiksi*.

Huomautus. Koska tässä tutkielmassa tarkastellaan ainoastaan yksinkertaisia graafeja, voidaan jatkossa käyttää ainoastaan termiä graafi.

Määritellään lisäksi muita tarpeellisia käsitteitä graafeille, ja olkoon sitä varten $G = (V, E)$ graafi. Graafin G solmujen joukkoa on tapana merkitä $V = V(G)$ ja särmien joukkoa $E = E(G)$. Graafin *koko*, jota merkitään $\text{card}(G)$, on graafin solmujen lukumäärä eli $\text{card}(G) = |V|$.

Jos graafille G pätee $E = \emptyset$ eli graafissa ei ole särmiä, sitä kutsutaan *tyhjäksi graafiksi*. Jos taas graafille G pätee $E = \{\{x, y\} \mid x, y \in V \text{ ja } x \neq y\}$ eli jokainen solmupari muodostaa särmän, sitä kutsutaan *täydelliseksi graafiksi*.

Olkoot sitten $x, y \in V$ solmuja. Solmujen x ja y välinen *polku* on äärellinen jono

$$p = (s_0, e_0, s_1, e_1, s_2, \ldots, s_{k-1}, e_{k-1}, s_k),$$

jossa on vuorotellen merkitty solmut $s_i \in V$, $0 \leq i \leq k$, joiden kautta polku p kulkee, ja särmät $e_j \in E$, $0 \leq j \leq k-1$, jotka yhdistävät solmuja s_j ja s_{j+1}. Jos solmujen välillä on polku, sanotaan, että solmut ovat *yhdistetyt*. Erityisesti mikäli solmuille $x, y \in V$ pätee $\{x, y\} \in E$, niin solmuja x ja y kutsutaan toistensa *naapureiksi*. Jos graafin mitkä tahansa kaksi solmua ovat yhdistetyt, sanotaan, että graafi on *yhtenäinen*.

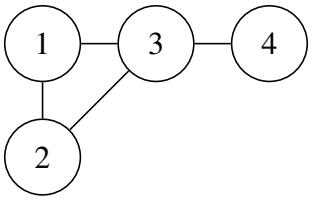
Graafin ominaisuus on sellainen graafien luokka, joka on suljettu isomorfismin suhteen. Jos siis graafilla G on ominaisuus A, eli $G \in A$, niin myös kaikilla sen kanssa isomorfisilla graafeilla on sama ominaisuus.

Esimerkki 2.2. Olkoon $G = (V, E)$ graafi, jolle $V = \{1, 2, 3, 4\}$ ja $E = \{\{1, 2\}, \{1, 3\}, \{3, 4\}, \{2, 3\}\}$. Graafi G on kuvattu kuviossa 2.1.

Graafin G koko on card(G) = 4 ja se on esimerkki yhtenäisestä graafista. Esimerkiksi solmut 1 ja 3 ovat naapureita, ja solmut 2 ja 4 ovat yhdistetty polulla

$$p = (2,\ \{2,3\},\ 3,\ \{3,4\},\ 4).$$

Siis, jos merkitään, että ominaisuus A on "graafi on yhtenäinen", niin $G \in A$.



Kuvio 2.1: Yksinkertainen graafi $G = (V, E)$, missä $V = \{1, 2, 3, 4\}$ ja $E = \{\{1, 2\}, \{1, 3\}, \{3, 4\}, \{2, 3\}\}$.

Graafi on siis pari $G = (V, E)$, joka koostuu äärellisestä solmujen joukosta V ja särmien joukosta E. Merkitään nyt symbolilla $\mathcal{G}_n$ sellaista yksinkertaisten ja kokoa n olevien graafien joukkoa, jossa graafien solmujen joukko on nimettyjen solmujen joukko $V = \{v_1, v_2, \ldots, v_n\}$. Huomattakoon, että tällaisia graafeja on olemassa $2^{\binom{n}{2}}$ kappaletta, sillä graafissa, jossa on n solmua, solmupareja on yhteensä $\binom{n}{2}$ kappaletta.

2.2 Satunnaisgraafit

Jatketaan graafien joukon $\mathcal{G}_n$ tarkastelua. Tavoitteena on pystyä todistamaan graafeille erilaisia ominaisuuksia, ja tätä varten esitellään käsite *satunnaisgraafi*. Ideana on muodostaa graafien joukolle $\mathcal{G}_n$ todennäköisyysavaruus ja tarkastella graafien ominaisuuksia tämän avulla. Tällöin halutunlaisen graafin olemassaolo voidaan todistaa osoittamalla graafin olemassaolon todennäköisyys positiiviseksi. Päälähteenä luvussa on käytetty Diestelin teosta *Graph Theory* [5, s. 294–295].

Tarkastellaan nimettyjen solmujen joukkoa $V = \{v_1, v_2, \ldots, v_n\}$. Käydään läpi joukon V solmuparit ja määritetään jokaisen parin kohdalla kolikkoa heittämällä muodostavatko ne särmän; jos tulos on klaava, solmupari muodostaa särmän. Kolikko on harhainen, ja klaavan todennäköisyys on p ja kruunan $1-p$, missä $p \in]0, 1[$. Tällöin todennäköisyys muodostaa kolikkoa heittämällä kiinteä graafi, jossa on N särmää, on $p^N(1-p)^{\binom{n}{2}-N}$, sillä mahdolliset särmien paikat voidaan valita yhteensä $\binom{n}{2}$ eri tavalla. Intuitiivisella tasolla näin saadaan liitettyä jokaiseen graafiin $G \in \mathcal{G}_n$ todennäköisyys, ja muodostuu todennäköisyysavaruus graafien joukolle $\mathcal{G}_n$ eli *satunnaisgraafin* $G_{n,p}$ malli. [5, s. 294]

Satunnaisgraafi on reaalista satunnaismuuttujaa muistuttava käsite ja tämän tapaan satunnaisgraafi $G_{n,p}$ on kuvaus. Kuvaus $G_{n,p}$ liittää jokaiseen perusjoukon $\mathcal{G}_n$ alkeistapaukseen eli graafiin arvon, joka tässä tapauksessa on graafi itse. Alkeistapauksien todennäköisyydet muodostetaan edellä esitellyllä tavalla, ja näin saadaan satunnaisgraafille $G_{n,p}$ todennäköisyysjakauma.

Määritelmä 2.3 (Satunnaisgraafi)**.** Olkoot $n > 0$ kokonaisluku ja $0 < p < 1$ reaaliluku. *Satunnaisgraafi* $G_{n,p}$ rakentuu nimettyjen solmujen joukosta $V(G_{n,p}) = \{v_1, v_2, \ldots, v_n\}$, jossa jokaisen solmuparin välille muodostuu toisistaan riippumatta särmä todennäköisyydellä p. Satunnaisgraafi $G_{n,p}$ on siis kuvaus $G_{n,p} : \mathcal{G}_n \to \mathcal{G}_n$, jolle $G_{n,p}(G) = G$, kun $G \in \mathcal{G}_n$. Satunnaisgraafin $G_{n,p}$ jakauma määräytyy todennäköisyysfunktiosta $\mathbb{P} : \mathcal{P}(\mathcal{G}_n) \to [0, 1]$, jolle

$$\mathbb{P}(\{G\}) = \mathbb{P}(\{G' \in \mathcal{G}_n \mid G_{n,p}(G') = G\}) = p^N(1-p)^{\binom{n}{2}-N},$$

kun $G \in \mathcal{G}_n$ on graafi, jossa on N särmää. Jatkossa todennäköisyyttä $\mathbb{P}$ merkitään lyhyesti $\mathbb{P}(\{G\}) = \mathbb{P}\{G\}$.

Edellä määriteltyä satunnaisgraafia kutsutaan myös Erdős-Rényin satunnaisgraafiksi. Satunnaisgraafi on saanut nimensä matemaatikoiden Paul Erdős ja Alfréd Rényin mukaan, jotka esittelivät satunnaisgraafien mallin ensimmäisen kerran vuonna 1959 artikkelissaan *On random graphs I.* [18]

Tässä tutkielmassa tarkastellaan satunnaisgraafista ainoastaan erikoistapausta $p = \frac{1}{2}$, eli satunnaisgraafia $G_{n,\frac{1}{2}}$. Tästä seuraa, että satunnaisgraafin $G_{n,\frac{1}{2}}$ kaikilla alkeistapauksilla on sama todennäköisyys eli satunnaisgraafin jakauma on symmetrinen: mikäli $G_0 \in \mathcal{G}_n$ on graafi, jossa on N särmää, niin graafin todennäköisyys on

$$\mathbb{P}\{G_0\} = \left(\frac{1}{2}\right)^N \left(\frac{1}{2}\right)^{\binom{n}{2}-N} = \left(\frac{1}{2}\right)^{\binom{n}{2}} = \frac{1}{2^{\binom{n}{2}}}. \tag{2.1}$$

Tämä todennäköisyys riippuu ainoastaan muuttujasta n, joka on graafin koko.

Perusjoukon $\mathcal{G}_n$ osajoukkoja kutsutaan *tapahtumiksi*. Koska nyt kaikki alkeistapaukset ovat toisistaan riippumattomia ja yhtä todennäköisiä, niin tällöin tapahtuman $A \subseteq \mathcal{G}_n$ todennäköisyys $\mathbb{P}(A)$, eli todennäköisyys, että satunnaisgraafi $G_{n,\frac{1}{2}}$ kuuluu tapahtumaan A, voidaan laskea myös yksinkertaisella tavalla joukon A osuutena perusjoukosta $\mathcal{G}_n$ (vrt. [15, s. 13]):

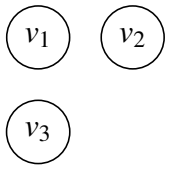
$$\begin{aligned} \mathbb{P}(A) &= \mathbb{P}\{G_{n,\frac{1}{2}} \in A\} \\ &= \mathbb{P}\{G \in \mathcal{G}_n \,|\, G \in A\} \\ &= \frac{|\,\{G \in \mathcal{G}_n \,|\, G \in A\}\,|}{|\,\mathcal{G}_n\,|} = \frac{|A|}{2^{\binom{n}{2}}}. \end{aligned} \tag{2.2}$$

Esimerkki 2.4. Tarkastellaan satunnaisgraafia $G_{3,\frac{1}{2}}$. Perusjoukossa $\mathcal{G}_3$ on nyt yhteensä $2^{\binom{3}{2}} = 2^3 = 8$ graafia. Merkitään näitä graafeja seuraavasti: G_1 on tyhjä graafi, G_2, G_3 ja G_4 ovat yksisärmäiset graafit, G_5, G_6 ja G_7 ovat kaksisärmäiset graafit ja G_8 on täydellinen graafi. Graafit ovat kuvattuina kuviossa 2.2. Alkeistapahtuman $\{G_1\}$ todennäköisyys on kaavan 2.1 nojalla

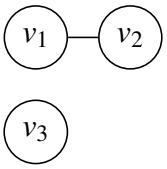
$$\mathbb{P}\{G_1\} = \frac{1}{8}.$$

Olkoon sitten tapahtuma $A = \{G_1, G_2, G_3\}$. Nyt kaavan 2.2 nojalla tapahtuman A todennäköisyys on

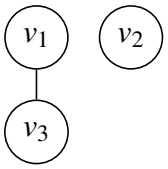
$$\mathbb{P}(A) = \mathbb{P}\{G_{3,\frac{1}{2}} \in A\} = \frac{|A|}{8} = \frac{3}{8}.$$



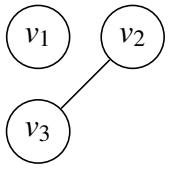
(a) Tyhjä graafi G_1.



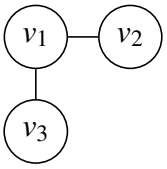
(b) Graafi G_2.



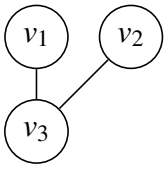
(c) Graafi G_3.



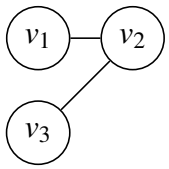
(d) Graafi G_4.



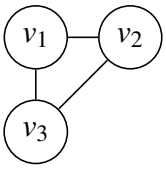
(e) Graafi G_5.



(f) Graafi G_6.



(g) Graafi G_7.



(h) Täydellinen graafi G_8.

Kuvio 2.2: Joukon $\mathcal{G}_3$ graafit.

2.3 Graafien ominaisuudet ja asymptoottinen todennäköisyys

Kuten luvussa 2.1 määriteltiin, *graafin ominaisuus* on sellainen graafien luokka, joka on suljettu isomorfismin suhteen. Kun tarkastellaan satunnaisgraafia $G_{n,\frac{1}{2}}$, graafin ominaisuus on perusjoukon $\mathcal{G}_n$ osajoukkona tapahtuman erikoistapaus. Tarkastellaan nyt ominaisuuksien todennäköisyyksiä ja erityisesti mitä tarkoitetaan ominaisuuden asymptoottisella todennäköisyydellä. Lähteenä luvussa on toiminut Diestelin teos *Graph Theory* [5, s. 302] ja Spencerin teos *The Strange Logic of Random Graphs* [15, s. 3–4, 13].

Olkoon A jokin graafien ominaisuus. Jotta voidaan osoittaa, että ominaisuuden A toteuttavia graafeja on olemassa, voidaan tarkastella ominaisuuden todennäköisyyt-

tä, joka on vastaavan tapahtuman A todennäköisyys $\mathbb{P}(A)$. Mikäli ominaisuuden A todennäköisyys on positiivinen, ominaisuuden toteuttavia graafeja on olemassa.

On kiinnostavaa tarkastella, mitä graafin ominaisuuden todennäköisyydelle tapahtuu, kun graafin koon annetaan kasvaa rajatta. Tämän vuoksi on hyödyllistä ottaa käyttöön merkintä, jossa graafin koko n on muuttujana. Kun $n > 0$ on kokonaisluku ja tarkastellaan satunnaisgraafia $G_{n,\frac{1}{2}}$, merkitään ominaisuuden A todennäköisyyttä

$$\mathbb{P}_n(A) = \mathbb{P}_n\{G_{n,\frac{1}{2}} \in A\}.$$

Seuraavaksi määritellään asymptoottisen todennäköisyyden käsite käyttäen edellä esitettyä merkintää ja lisäksi käydään läpi mitä tarkoitetaan sillä, että graafilla on asymptoottisesti melkein varmasti jokin ominaisuus.

Määritelmä 2.5. Tarkastellaan satunnaisgraafia $G_{n,\frac{1}{2}}$. Olkoon A jokin graafien ominaisuus. Ominaisuuden A *asymptoottinen todennäköisyys* on raja-arvo

$$\lim_{n\to\infty} \mathbb{P}_n(A),$$

mikäli raja-arvo on olemassa. Erityisesti,

(i) jos $\lim_{n\to\infty} \mathbb{P}_n(A) = 1$, niin sanotaan, että *satunnaisgraafilla on asymptoottisesti melkein varmasti ominaisuus A*,

(ii) ja jos $\lim_{n\to\infty} \mathbb{P}_n(A) = 0$, niin sanotaan, että *satunnaisgraafilla asymptoottisesti melkein varmasti ei ole ominaisuutta A*.

Käydään läpi konkreettinen esimerkki graafien ominaisuuksista ja asymptoottisesta todennäköisyydestä.

Esimerkki 2.6 (vrt. [15, s. 3–4])**.** Osoitetaan, että satunnaisgraafi $G_{n,\frac{1}{2}}$ sisältää asymptoottisesti melkein varmasti kolmion. Kolmio on sellainen solmujen kolmikko, jossa kaikki solmut ovat keskenään naapureita. Merkitään, että A on ominaisuus "graafi sisältää kolmion", ja osoitetaan, että $\lim_{n\to\infty} \mathbb{P}_n(A) = 1$.

Jaetaan graafin $G_{n,\frac{1}{2}}$ solmujen joukko $V = V(G_{n,\frac{1}{2}})$ 3 alkion joukkoihin; jos n ei ole jaollinen luvulla 3, korkeintaan 2 solmua voi jäädä ylimääräiseksi. Saadaan kuitenkin muodostettua vähintään $s = \lfloor \frac{n}{3} \rfloor$ kappaletta kolmikoita.

Satunnaisesti valittu solmujen kolmikko $\{x, y, z\} \subseteq V$ muodostaa kolmion todennäköisyydellä $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$, ja näin ollen todennäköisyys, että mikään solmujen kolmikoista ei muodosta kolmiota on $\left(\frac{7}{8}\right)^s$. Siis todennäköisyys, että yksi valituista kolmikoista on kolmio on $1 - \left(\frac{7}{8}\right)^s$.

Muodostettu jako voitaisiin kuitenkin tehdä lukuisilla eri tavoilla, joten saatu todennäköisyys on alaraja todennäköisyydelle $\mathbb{P}_n(A)$, että satunnaisgraafi $G_{n,\frac{1}{2}}$ sisältää kolmion. Ensinnäkin, todennäköisyys saa aina positiivisia arvoja, joten ominaisuuden toteuttavia graafeja on aina olemassa. Toisaalta, kun $n \to \infty$, niin $s \to \infty$, joten saadaan

$$\lim_{n\to\infty} \mathbb{P}_n(A) \geq \lim_{s\to\infty} \left(1 - \left(\frac{7}{8}\right)^s\right) = 1.$$

Siis määritelmän 2.5 nojalla satunnaisgraafi $G_{n,\frac{1}{2}}$ sisältää asymptoottisesti melkein varmasti kolmion.

2.4 Laajennusaksioomat

Laajennusaksioomiksi[1] kutsutut ominaisuudet ovat graafien erityisiä ominaisuuksia, joissa yleisesti ottaen vaaditaan, että jokaiselle graafin tietyn kaltaiselle solmujen osajoukolle on olemassa eri solmu, joka on liitetty osajoukon solmuihin vaaditulla tavalla. Tässä tutkielmassa tarkastellaan erityisesti niin kutsuttuja k-laajennusaksioomia, mutta aloitetaan määrittelemällä laajennusaksioomat yleisemmällä tasolla. Luvussa on käytetty lähteenä Bollobàsin teosta *Random Graphs* [3, s. 41] ja Blassin, Exoon ja Hararyn artikkelia *Paley graphs satisty all first-order adjacency axioms* [2].

Määritelmä 2.7 (l, m-Laajennusaksioomat)**.** Olkoot l ja m sellaisia positiivisia kokonaislukuja, joille $l + m > 0$, ja olkoon G graafi. Tällöin sanotaan, että graafi G toteuttaa l, m*-laajennusaksiooman*, mikäli seuraava ehto toteutuu:

> Olkoot $X, Y \subset V(G)$ mielivaltaiset ja erilliset solmujen joukot, joille $|X| = l$ ja $|Y| = m$. Tällöin on olemassa sellainen solmu $z \in V(G) \setminus (X \cup Y)$, että solmu z on naapuri jokaisen solmun $x \in X$ kanssa, mutta ei yhdenkään solmun $y \in Y$ kanssa.

Merkitään l, m-laajennusaksioomaa merkinnällä $\eta_{l,m}$.

Huomautus. Laajennusaksiooman toteutumista on luonnollisesti luontevaa tarkastella vain tapauksissa, joissa graafin G koolle $\text{card}(G)$ pätee $\text{card}(G) > l + m$.

Huomautus. Laajennusaksiooma on graafien ominaisuus, joten mikäli graafi G toteuttaa l, m-laajennusaksiooman $\eta_{l,m}$, niin merkitään $G \in \eta_{l,m}$.

Huomautus. Mikäli jokin graafien perhe toteuttaa l, m-laajennusaksiooman, sitä kutsutaan l, m*-laajennusaksiooman malliksi*.

Laajennusaksioomille pätee seuraava tärkeä ominaisuus.

Lause 2.8. *Olkoot l, l', m ja m' sellaisia kokonaislukuja, joille $l \geq l' \geq 0$ ja $m \geq m' \geq 0$ ja $l' + m' > 0$. Olkoon G sellainen graafi, jolle* $\text{card}(G) > l + m$ *ja joka toteuttaa l, m-laajennusaksiooman $\eta_{l,m}$. Tällöin graafi G toteuttaa myös l', m'-laajennusaksiooman $\eta_{l',m'}$.*

Todistus. Olkoot $X', Y' \subset V(G)$ sellaisia mielivaltaisia graafin G solmujoukon $V(G)$ osajoukkoja, että $|X'| = l'$ ja $|Y'| = m'$. Osoitetaan, että on olemassa sellainen solmu $z \in V(G) \setminus (X' \cup Y')$, että solmu z on naapuri jokaisen solmun $x \in X'$ kanssa, mutta ei yhdenkään solmun $y \in Y'$ kanssa.

Valitaan nyt sellaiset erilliset joukot $X, Y \subset V(G)$, että $X' \subset X$ ja $Y' \subset Y$ ja lisäksi $|X| = l$ ja $|Y| = m$. Tällaiset joukot voidaan löytää, koska $\text{card}(G) > l + m$ ja graafi G toteuttaa l, m-laajennusaksiooman $\eta_{l,m}$.

Edelleen, koska graafi G toteuttaa l, m-laajennusaksiooman, niin on olemassa sellainen solmu $z \in V(G) \setminus (X \cup Y)$, että solmu z on naapuri jokaisen solmun $x \in X$ kanssa, mutta ei yhdenkään solmun $y \in Y$ kanssa. Huomataan, että solmu z on erityisesti

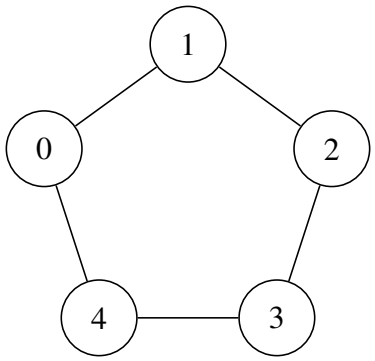
[1] Laajennusaksioomia kutsutaan englannin kielisissä lähteissä usein termeillä *extension axioms* tai *adjacency properties*.

naapuri jokaisen solmun $x \in X'$ kanssa, mutta ei yhdenkään solmun $y \in Y'$ kanssa. Siis määritelmän 2.7 nojalla graafi G toteuttaa myös l', m'-laajennusaksiooman $\eta_{l',m'}$. □

Lauseen 2.8 nojalla, mikäli graafi G toteuttaa k, k-laajennusaksiooman $\eta_{k,k}$, ja lisäksi l ja m ovat sellaisia kokonaislukuja, joille $l, m < k$, niin G toteuttaa myös l, m-laajennusaksiooman $\eta_{l,m}$. Näin ollen k, k-laajennusaksiooman tarkastelu tutkielmassa ei ole rajoittava tekijä. Tarkastellaan jatkossa ainoastaan k, k-laajennusaksioomaa ja kutsutaan sitä yksinkertaisesti k-laajennusaksioomaksi.

Esitetään seuraavaksi yksinkertainen esimerkki 1-laajennusaksioomasta $\eta_{1,1}$.

Esimerkki 2.9. Olkoon G graafi, missä solmujen joukko on $V(G) = \{0, 1, 2, 3, 4\}$ ja särmien joukko on $E(G) = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 0\}\}$. Graafi G on kuvattu kuviossa 2.3.



Kuvio 2.3: Graafi G, missä $V(G) = \{0, 1, 2, 3, 4\}$ ja $E(G) = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 0\}\}$. (Vrt. [17].)

Kuviosta 2.3 nähdään, että graafi G toteuttaa 1-laajennusaksiooman. Valittiinpa mitkä tahansa 2 solmua x ja y, on aina olemassa näistä eroava solmu z, joka on naapuri solmun x kanssa, mutta ei naapuri solmuun y kanssa. Esimerkiksi, jos valitaan solmut 0 ja 1, löydetään solmu 4, joka on naapuri solmun 0 kanssa, mutta ei solmun 1. Siis 1-laajennusaksiooma pätee eli $G \in \eta_{1,1}$.

Graafia G kutsutaan myös *Paleyn graafiksi* P_5. Paleyn graafeja tarkastellaan tarkemmin luvussa 4.

3 Laajennusaksioomat ja satunnaisgraafit

Tässä luvussa tarkastellaan luvussa 2.4 määriteltyihin laajennusaksioomiin liittyen kahta asiaa. Aloitetaan osoittamalla, että k-laajennusaksiooman $\eta_{k,k}$ täyttäviä graafeja on aina olemassa. Tämä osoitetaan näyttämällä, että ominaisuuden $\eta_{k,k}$ todennäköisyys $\mathbb{P}(\eta_{k,k})$ on positiivinen. Toiseksi osoitetaan, että satunnaisgraafi toteuttaa asymptoottisesti melkein varmasti k-laajennusaksiooman. Tämä osoitetaan näyttämällä, että ominaisuuden $\eta_{k,k}$ asymptoottinen todennäköisyys on 1. Lähteenä luvussa on toiminut pääasiallisesti Bonaton artikkeli *The search for n-e.c. graphs* [4].

Aloitetaan todistamalla kaksi tarvittavaa arviota. On osoitettavissa, että $2^n < n!$, kunhan $n \geq 4$, mutta aloitetaan esittelemällä tästä hieman muunneltu versio.

Lemma 3.1. *Olkoon $n \geq 4$ kokonaisluku. Tällöin $2^n \cdot (1 - \frac{1}{2^n})^{-n} < n!$.*

Todistus. Todistetaan väite induktiolla luvun n suhteen. Perusaskeleessa tarkastellaan tapausta $n = 4$. Tällöin

$$\begin{aligned} 2^4 \cdot \left(\frac{15}{16}\right)^{-4} &= 16 \cdot \frac{16^4}{15^4} \approx 20.7 \\ &< 24 = 4 \cdot 3 \cdot 2 \cdot 1 = 4!, \end{aligned}$$

eli väite on selvä. Oletetaan sitten, että väite pätee luvulle n eli $2^n \cdot (1 - \frac{1}{2^n})^{-n} < n!$ ja väitetään, että tällöin myös $2^{n+1} \cdot (1 - \frac{1}{2^{n+1}})^{-n-1} < (n+1)!$. Oletuksen nojalla $n \geq 4$ ja induktio-oletusta käyttämällä saadaan

$$\begin{aligned} 2^{n+1} \cdot \left(1 - \frac{1}{2^{n+1}}\right)^{-n-1} &= 2^n \cdot \left(1 - \frac{1}{2^{n+1}}\right)^{-n} \cdot 2 \cdot \left(1 - \frac{1}{2^{n+1}}\right)^{-1} \\ &< 2^n \cdot \left(1 - \frac{1}{2^n}\right)^{-n} \cdot 2 \cdot \left(1 - \frac{1}{2^n}\right)^{-1} \\ &< n! \cdot 2 \cdot \left(1 - \frac{1}{2^n}\right)^{-1} \\ &= n! \cdot 2 \cdot \left(\frac{2^n}{2^n - 1}\right) \\ &< n! \cdot 2 \cdot 2 \\ &< n! \cdot (n+1) \\ &= (n+1)!. \end{aligned}$$

Siis väite pätee induktioperiaatteen nojalla kaikille luvuille $n \geq 4$. □

Toisen tarvittavan arvion todistus sivuutetaan:

Lemma 3.2. *Kun $x \geq 0$ on reaaliluku, niin $1 + x \leq e^x$.*

Todistus. Sivuutetaan. □

Nyt voidaan osoittaa, että k-laajennusaksiooman toteuttavia graafeja on aina olemassa.

Lause 3.3. *Olkoon $k > 0$ kokonaisluku. Tällöin on olemassa sellainen graafi G, jolle* $\mathrm{card}(G) \geq 8k^2 2^{2k}$ *ja joka toteuttaa k-laajennusaksiooman.*

Todistus (vrt. [4, Theorem 1]). Olkoon $n \geq 8k^2 2^{2k}$ kokonaisluku ja tarkastellaan satunnaisgraafia $G_{n,\frac{1}{2}}$. Lauseen väite on nyt yhtäpitävää sen kanssa, että k-laajennusaksiooman todennäköisyys on positiivinen, eli

$$\mathbb{P}(\eta_{k,k}) = \mathbb{P}\{G_{n,\frac{1}{2}} \in \eta_{k,k}\} > 0.$$

Merkitään $V = V(G_{n,\frac{1}{2}}) = \{v_1, v_2, \ldots, v_n\}$ ja $E = E(G_{n,\frac{1}{2}})$. Tarkastellaan ominaisuuden $\eta_{k,k}^{\complement}$ todennäköisyyttä $\mathbb{P}(\eta_{k,k}^{\complement})$, eli todennäköisyyttä, että satunnaisgraafi $G_{n,\frac{1}{2}}$ ei toteuta k-laajennusaksioomaa. Tällöin tavoitteena on osoittaa, että todennäköisyys $\mathbb{P}(\eta_{k,k}^{\complement})$ on aidosti pienempi kuin 1.

Olkoot $X, Y \subset V$ sellaiset mielivaltaiset ja erilliset solmujen osajoukot, joille pätee $|X| = |Y| = k$. Merkitään $X = \{x_1, x_2, \ldots, x_k\}$ ja $Y = \{y_1, y_2, \ldots, y_k\}$. Todennäköisyys, että mielivaltaisesti valittu solmu $z \in V \setminus (X \cup Y)$ on liitetty oikein joukkoihin X ja Y on $(\frac{1}{2})^{2k}$, ja näin ollen todennäköisyys, että solmu z on liitetty väärin, on $1 - (\frac{1}{2})^{2k}$. Toisaalta solmu z voidaan valita $n - 2k$ eri tavalla, jotka ovat toisistaan riippumattomia, joten todennäköisyys, että mikään solmu $z \in V \setminus (X \cup Y)$ ei ole liitetty oikein joukkoihin X ja Y on $(1 - (\frac{1}{2})^{2k})^{n-2k}$.

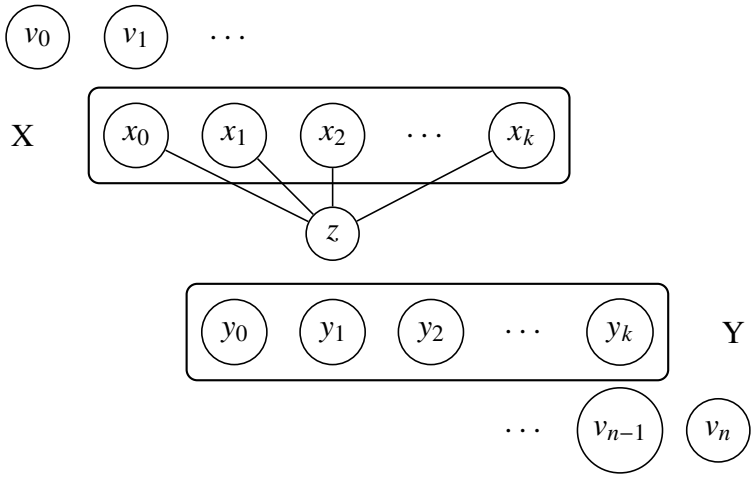
Joukko $X \cup Y$ voidaan valita solmujen joukosta V yhteensä $\binom{n}{2k}$ eri tavalla, ja tästä joukot X ja Y voidaan muodostaa korkeintaan 2^{2k} eri tavalla. Siispä todennäköisyys, että graafi G ei toteuta k-laajennusaksioomaa on

$$\mathbb{P}(\eta_{k,k}^{\complement}) \leq \binom{n}{2k} 2^{2k} \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n-2k}. \tag{3.1}$$

Kuviossa 3.1 on havainnollistettu k-laajennusaksiooman mukaista tilannetta satunnaisgraafille $G_{n,\frac{1}{2}}$.

Arvioidaan nyt todennäköisyyttä 3.1, ja osoitetaan lopulta, että se saa arvoja, jotka ovat pienempiä kuin 1. Ensinnäkin

$$\begin{aligned}
\mathbb{P}(\eta_{k,k}^{\complement}) &= \binom{n}{2k} 2^{2k} \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n-2k} \\
&= \frac{n!}{(2k)!(n-2k)!} \cdot 2^{2k} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{-2k} \\
&= \frac{2^{2k}}{(2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{-2k} \cdot \frac{n!}{(n-2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n},
\end{aligned}$$



Kuvio 3.1: k-Laajennusaksiooman mukainen tilanne satunnaisgraafille $G_{n,\frac{1}{2}}$, jossa solmujen joukoille X ja Y löydetään niihin halutulla tavalla liitetty solmu z.

ja kun $k \geq 2$ eli $2k \geq 4$, niin lauseen 3.1 nojalla saadaan

$$\frac{2^{2k}}{(2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{-2k} \cdot \frac{n!}{(n-2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n} < \frac{n!}{(n-2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n}.$$

Toisaalta

$$\frac{n!}{(n-2k)!} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n} = (n \cdot (n-1) \cdot \cdots \cdot (n-2k+1)) \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n} \leq n^{2k} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n},$$

jolloin lauseen 3.2 nojalla saadaan arvio

$$\begin{aligned} n^{2k} \cdot \left(1 - \left(\frac{1}{2}\right)^{2k}\right)^{n} &< n^{2k} \cdot \left(e^{-\frac{1}{2^{2k}}}\right)^{n} \\ &= n^{2k} \cdot e^{-\frac{n}{2^{2k}}} \\ &= e^{2k\ln(n) - n2^{-2k}}. \end{aligned}$$

Siis todennäköisyydelle pätee $\mathbb{P}(\eta_{k,k}^{\complement}) < e^{2k\ln(n) - n2^{-2k}}$. On osoitettavissa, että funktio $n \mapsto 2k\ln(n) - n2^{-2k}$ on vähenevä, ja kun oletetaan, että $n \geq 8k^2 2^{2k}$,

saadaan

$$\begin{aligned} e^{2k\ln(n)-n2^{-2k}} &\leq e^{2k\cdot\ln(8k^2 2^{2k})-8k^2 2^{2k}2^{-2k}} \\ &= e^{2k\cdot\left(\ln(8)+2\ln(k)+2k\cdot\ln(2)\right)-8k^2} \\ &= e^{2k\cdot\ln(8)+4k\cdot\ln(k)+4k^2\cdot\ln(2)-8k^2} \\ &= e^{\ln(16)k^2+4k\ln(k)+\ln(64)k-8k^2} \\ &\leq e^{3k^2+4k^2+5k-8k^2} \\ &= e^{-k^2+5k}. \end{aligned}$$

Nyt eksponentissa oleva funktio saa negatiivisia arvoja, kunhan $k > 5$. Siis, kun $k > 5$, niin ominaisuuden $\eta_{k,k}^{\complement}$ todennäköisyydelle pätee $\mathbb{P}(\eta_{k,k}^{\complement}) < e^0 = 1$. Näin ollen ominaisuuden $\eta_{k,k}$ todennäköisyys, eli todennäköisyys, että satunnaisgraafi $G_{n,\frac{1}{2}}$ toteuttaa k-laajennusaksiooman on

$$\mathbb{P}(\eta_{k,k}) = 1 - \mathbb{P}(\eta_{k,k}^{\complement}) > 1 - 1 = 0.$$

Siis k-laajennusaksiooman $\eta_{k,k}$ toteuttavia graafeja on aina olemassa, kun $k > 5$.

Erikoistapauksiksi tarkasteluun jäävät k-laajennusaksiooman tapaukset, joissa $k = 1, 2, 3, 4$ ja 5. Luvussa 2 esimerkissä 2.9 esiteltiin eräs 1-laajennusaksiooman toteuttava graafi, ja käydään esimerkkinä läpi tapaus $k = 2$. Aiemmin todistuksessa todettiin, että

$$\mathbb{P}(\eta_{k,k}^{\complement}) \leq e^{\ln(16)k^2+4k\ln(k)+\ln(64)k-8k^2},$$

kunhan $k \geq 2$, ja sijoittamalla tähän $k = 2$, voidaan osoittaa, että myös tässä tapauksessa ominaisuuden $\eta_{2,2}$ todennäköisyys on positiivinen. Nyt

$$\begin{aligned} &\ln(16)k^2 + 4k\ln(k) + \ln(64)k - 8k^2 \\ &= \ln(16)\cdot 4 + 8\cdot\ln(2) + \ln(64)\cdot 2 - 8\cdot 4 \\ &= \ln(16)\cdot 4 + \ln(16)\cdot 2 + \ln(16)\cdot 3 - 32 \\ &= \ln(16)\cdot 9 - 32 \\ &< 3\cdot 9 - 32 \\ &= -5 < 0, \end{aligned}$$

joten $\mathbb{P}(\eta_{2,2}^{\complement}) < e^0 = 1$. Siis tapauksessa $k = 2$, ominaisuuden $\eta_{2,2}$ todennäköisyys on

$$\mathbb{P}(\eta_{2,2}) = 1 - \mathbb{P}(\eta_{2,2}^{\complement}) > 1 - 1 = 0,$$

joten 2-laajennusaksiooman toteuttavia graafeja on olemassa. Tapaukset $k = 3$, 4 ja 5 voidaan käsitellä samaan tapaan. □

Edellä esitetyn todistuksen avulla on helppo todistaa, että satunnaisgraafi toteuttaa asymptoottisesti melkein varmasti k-laajennusaksiooman.

Lause 3.4. *Olkoon $k \geq 1$ kokonaisluku. Tällöin*

$$\lim_{n\to\infty} \mathbb{P}_n(\eta_{k,k}) = 1.$$

Todistus (vrt. [4, Theorem 1]). Osoittaaksemme väitteen, osoitetaan, että $\lim_{n\to\infty} \mathbb{P}_n(\eta_{k,k}^{\complement}) = 0$. Lauseen 3.3 todistuksessa todettiin, että ominaisuuden $\eta_{k,k}^{\complement}$ todennäköisyydelle pätee

$$\mathbb{P}_n(\eta_{k,k}^{\complement}) < e^{2k\ln(n) - n2^{-2k}},$$

kun $k \geq 2$. Tarkastellaan raja-arvoa $\lim_{n\to\infty} e^{2k\ln(n)-n2^{-2k}}$. Nyt logaritmifunktio kasvaa hitaammin kuin polynominen, joten

$$\lim_{n\to\infty} \left(2k\ln(n) - n2^{-2k}\right) = -\infty.$$

Siis

$$\lim_{n\to\infty} \left(e^{2k\ln(n)-n2^{-2k}}\right) = 0,$$

joten suppiloperiaatteen nojalla $\lim_{n\to\infty} \mathbb{P}_n(\eta_{k,k}^{\complement}) = 0$, ja edelleen $\lim_{n\to\infty} \mathbb{P}_n(\eta_{k,k}) = 1$. Siis väite on todistettu, ja määritelmän 2.5 nojalla satunnaisgraafilla on asymptoottisesti melkein varmasti ominaisuus $\eta_{k,k}$.

□

k-Laajennusaksioomat toteuttavia graafeja on siis aina olemassa, mutta käytännössä niiden konstruointi voi kuitenkin olla hankalaa. [4] Seuraavassa luvussa käydään kuitenkin läpi eräs tunnettu graafien joukko, jonka riittävän suuret graafit toteuttavat tämän ominaisuuden. Tätä joukkoa kutsutaan *Paleyn graafeiksi*.

4 Laajennusaksioomat ja Paleyn graafit

Tunnettuja k-laajennusaksioomien malleja ovat Paleyn graafit. Luvun aluksi käydään läpi Paleyn graafien määrittelyssä ja käsittelyssä tarvittavia käsitteitä sekä esitellään niihin liittyviä tuloksia. Tämän jälkeen määritellään Paleyn graafit. Luvun lopuksi osoitetaan, että Paleyn graafit toteuttavat k-laajennusaksioomat, eli ovat k-laajennusaksioomien malleja.

4.1 Neliönjäännökset

Ensin määritellään käsite neliönjäännös ja käydään läpi siihen liittyviä perusominaisuuksia. Tämän jälkeen määritellään käsite Legendren symboli, jonka avulla voidaan merkitä, onko kokonaisluku luvun p neliönjäännös. Todistetaan myös myöhemmin tarvittavia tuloksia liittyen Legendren symboliin. Luvussa päälähteenä toimii Rosenin teos *Elementary number theory and its applications* [13, s. 375–380] ja termistön tukena Väisälän teos *Lukuteorian ja korkeamman algebran alkeet* [16].

4.1.1 Perusominaisuuksia

Määritelmä 4.1. Olkoot m ja a kokonaislukuja. Kokonaisluku a on luvun m *neliönjäännös*, jos $a \not\equiv 0 \pmod{m}$ ja kongruenssiyhtälöllä $x^2 \equiv a \pmod{m}$ on ratkaisu. Jos kongruenssiyhtälöllä $x^2 \equiv a \pmod{m}$ ei ole ratkaisua, luku a on luvun m *neliönepäjäännös*.

Esimerkki 4.2 (vrt. [13, s. 376])**.** Määritetään luvun 7 neliönjäännökset. Lasketaan neliöt joukon $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ alkioille:

$$1^2 \equiv 1 \pmod 7, \qquad 2^2 \equiv 4 \pmod 7, \qquad 3^2 = 9 \equiv 2 \pmod 7,$$
$$4^2 = 16 \equiv 2 \pmod 7, \quad 5^2 = 25 \equiv 4 \pmod 7 \text{ ja } \quad 6^2 = 36 \equiv 1 \pmod 7.$$

Siis luvun 7 neliönjäännöksiä ovat 1, 2 ja 4, ja neliönepäjäännöksiä ovat 3, 5 ja 6.

Seuraava lause toimii apuna selvitettäessä jatkossa neliönjäännösten lukumäärää.

Lause 4.3. *Olkoot $p > 2$ alkuluku ja a kokonaisluku, jolle $a \not\equiv 0 \pmod{p}$. Tällöin kongruenssiyhtälöllä*

$$x^2 \equiv a \pmod{p} \tag{4.1}$$

on joko ei yhtään ratkaisua tai täsmälleen kaksi keskenään ei-kongruenttia ratkaisua modulo p.

Todistus (vrt. [13, s. 376–377]). Jos kongruenssiyhtälöllä (4.1) ei ole ratkaisua, väite on selvä. Oletetaan siis, että yhtälöllä on ainakin yksi ratkaisu $x = x_0$. Koska

$$(-x_0)^2 = x_0^2 \equiv a \pmod{p},$$

niin selvästi myös $-x_0$ on kongruenssiyhtälön ratkaisu. Mikäli olisi $x_0 \equiv -x_0 \pmod{p}$, saataisiin $2x_0 \equiv 0 \pmod{p}$. Tämä on kuitenkin ristiriita, sillä muuten olisi voimassa $p \mid 2x_0$; koska $p > 2$ ja alkuluku, niin $p \nmid 2$. Lisäksi, koska $a \not\equiv 0 \pmod{p}$ ja $x_0^2 \equiv a \pmod{p}$, niin $p \nmid x_0$. Kongruenssiyhtälöllä (4.1) on siis vähintään kaksi keskenään ei-kongruenttia ratkaisua.

Osoitetaan sitten, että kongruenssiyhtälöllä (4.1) on korkeintaan kaksi ratkaisua. Oletetaan, että yhtälöllä on ratkaisun $x = x_0$ lisäksi myös toinen ratkaisu, $x = x_1$. Osoitetaan, että nyt ratkaisun $x = x_1$ on oltava kongruentti toisen ratkaisuista $x = x_0$ tai $x = -x_0$ kanssa. Nyt $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$, joten

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}.$$

Tästä seuraa $p \mid (x_0 - x_1)(x_0 + x_1)$ eli edelleen $p \mid (x_0 - x_1)$ tai $p \mid (x_0 + x_1)$. Siis $x_1 \equiv x_0 \pmod{p}$ tai $x_1 \equiv -x_0 \pmod{p}$. Siispä kongruenssiyhtälöllä $x^2 \equiv a \pmod{p}$ ei voi olla kuin kaksi keskenään ei-kongruenttia ratkaisua. □

Seuraavaksi voidaan todistaa lause neliönjäännösten lukumäärästä.

Lause 4.4. *Olkoon $p > 2$ alkuluku. Luvun p suhteen on olemassa täsmälleen $\frac{p-1}{2}$ neliönjäännöstä ja $\frac{p-1}{2}$ neliönepäjäännöstä. Lisäksi kaikki luvun p neliönjäännökset saadaan määritettyä laskemalla neliöt luvuille $1, 2, \ldots, \frac{p-1}{2}$.*

Todistus (vrt. [13, s. 378] ja [9]). Ensin huomataan, että korottamalla luvut $1, 2, \ldots,$ ja $\frac{p-1}{2}$ toiseen potenssiin, saadaan korkeintaan $\frac{p-1}{2}$ eri lopputulosta:

$$\begin{aligned} 1^2 &\equiv (-1)^2 \equiv (p-1)^2 \pmod{p} \\ 2^2 &\equiv (-2)^2 \equiv (p-2)^2 \pmod{p} \\ &\ldots \\ \left(\frac{p-1}{2}\right)^2 &\equiv \left(-\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2 \pmod{p}. \end{aligned}$$

Siis luvun p neliönjäännöksiä on korkeintaan $\frac{p-1}{2}$ kappaletta.

Osoitetaan nyt, että mitkään kaksi neliönjäännöksistä $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ eivät ole keskenään kongruentteja. Olkoot a ja b sellaisia kokonaislukuja $0 < a \leq b \leq \frac{p-1}{2}$, joille pätee $a^2 \equiv b^2 \pmod{p}$. Tämä on yhtäpitävää sen kanssa, että

$$a^2 - b^2 = (a - b)(a + b) \equiv 0 \pmod{p}.$$

Edelleen tästä seuraa $p \mid (a - b)$ tai $p \mid (a + b)$. Jos $p \mid (a + b)$, seuraa ristiriita, sillä $0 < a + b \leq p - 1$. Siis on oltava $p \mid (a - b)$. Koska $p \mid (a - b)$ ja $0 \leq a - b < \frac{p-1}{2}$, on oltava $a - b = 0$ eli $a = b$. Siispä neliönjäännöksiä on tasan $\frac{p-1}{2}$ kappaletta ja ne saadaan muodostettua laskemalla $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. □

Näin saatiin helpompi tapa määrittää neliönjäännöksiä, joka nähdään seuraavasta esimerkistä.

Esimerkki 4.5 (Jatkoa esimerkkiin 4.2)**.** Lauseen 4.4 perusteella esimerkissä 4.2 olisi riittänyt laskea $\frac{p-1}{2} = \frac{7-1}{2} = 3$ pienimmälle jäännökselle neliöt modulo p, jotta saadaan määritettyä kaikki luvun 7 neliönjäännökset. Nyt

$$\begin{aligned} 1^2 &\equiv 1 \pmod 7, \\ 2^2 &\equiv 4 \pmod 7 \text{ ja} \\ 3^2 = 9 &\equiv 2 \pmod 7. \end{aligned}$$

Tässä saatiin siis sama lopputulos: luvun 7 neliönjäännöksiä ovat 1, 2 ja 4, ja neliönepäjäännöksiä ovat 3, 5 ja 6.

Esimerkki 4.6. Luvun 13 neliönjäännökset ovat 1, 3, 4, 9, 10 ja 12, sillä lauseen 4.4 nojalla laskemalla saadaan

$$\begin{aligned} 1^2 &\equiv 1 \pmod{13}, & 4^2 = 16 &\equiv 3 \pmod{13}, \\ 2^2 &\equiv 4 \pmod{13}, & 5^2 = 25 &\equiv 12 \pmod{13}, \\ 3^2 &\equiv 9 \pmod{13} \text{ ja} & 6^2 = 36 &\equiv 10 \pmod{13}. \end{aligned}$$

4.1.2 Legendren symboli

Seuraavaksi esitellään Legendren symboli ja käydään läpi tähän liittyviä perusominaisuuksia. Aloitetaan määritelmällä.

Määritelmä 4.7. Olkoot $p > 2$ alkuluku ja a kokonaisluku. *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään seuraavasti:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on luvun } p \text{ neliönjäännös,} \\ 0, & \text{jos } a \equiv 0 \pmod p, \text{ ja} \\ -1, & \text{jos } a \text{ on luvun } p \text{ neliönepäjäännös.} \end{cases}$$

Esimerkki 4.8 (Jatkoa esimerkkiin 4.2, vrt. [13, s. 378])**.** Esimerkin 4.2 perusteella voidaan nyt kirjoittaa seuraavat merkinnät käyttäen Legendren symbolia:

$$\begin{aligned} \left(\frac{1}{7}\right) &= 1, & \left(\frac{2}{7}\right) &= 1, & \left(\frac{4}{7}\right) &= 1, \\ \left(\frac{3}{7}\right) &= -1, & \left(\frac{5}{7}\right) &= -1 \text{ ja} & \left(\frac{6}{7}\right) &= -1. \end{aligned}$$

Todistetaan seuraavaksi apulause, jota tarvitaan Eulerin kriteerin todistuksessa.

Lause 4.9 (Lagrange)**.** *Olkoon $n \geq 0$ kokonaisluku ja $f(x) = c_n x^n + \cdots + c_1 x + c_0$, missä c_i on kokonaisluku jokaisella $i = 0, 1, \ldots, n$. Olkoon lisäksi $p > 1$ kokonaisluku, jolle pätee $p \nmid c_n$. Tällöin kongruenssiyhtälöllä*

$$f(x) \equiv 0 \pmod p$$

on korkeintaan n ratkaisua.

Todistus (vrt. [1, s. 177]). Todistetaan väite induktiolla luvun n suhteen. Jos $n = 0$, niin kongruenssiyhtälöllä $c_0 \equiv 0 \pmod{p}$ on 0 ratkaisua, sillä oletuksen mukaan nyt $p \nmid c_0$. Siis väite pätee.

Oletetaan sitten, että väite pätee funktioille, joiden aste on pienempi kuin n. Olkoon sitten g funktio, jonka aste on n. Merkitään

$$g(x) = b_n x^n \cdots + b_1 x + b_0,$$

missä $p \nmid b_n$. Jos kongruenssiyhtälöllä $g(x) \equiv 0 \pmod{p}$ ei ole ratkaisua, väite on selvä. Oletetaan siis, että yhtälöllä on vähintään yksi ratkaisu $x = x_0$. Nyt funktio g voidaan kirjoittaa muodossa

$$g(x) \equiv (x - x_0) f(x) \pmod{p},$$

missä f on astetta $n - 1$ oleva funktio muotoa $f(x) = a_{n-1}x^{n-1} \cdots + a_1 x + a_0$. Funktiolle f pätee $p \nmid a_{n-1}$, sillä on oltava $b_n = a_{n-1}$.

Jos nyt $g(x) \equiv 0 \pmod{p}$ ja p on alkuluku, niin tulon nollasäännön perusteella $x \equiv x_0 \pmod{p}$ tai $f(x) \equiv 0 \pmod{p}$. Induktio-oletuksen mukaan kongruenssiyhtälöllä $f(x) \equiv 0 \pmod{p}$ on korkeintaan $n - 1$ ratkaisua. Nämä ovat myös yhtälön $g(x) \equiv 0 \pmod{p}$ ratkaisuja, ja näin ollen kongruenssiyhtälöllä $g(x) \equiv (x - x_0) f(x) \equiv 0 \pmod{p}$ on korkeintaan n ratkaisua. □

Nyt voidaan todistaa Eulerin kriteeri.

Lause 4.10 (Eulerin kriteeri)**.** *Olkoot $p > 2$ alkuluku ja a kokonaisluku. Tällöin*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Todistus (vrt. [13, s. 378]). Mikäli $a \equiv 0 \pmod{p}$, niin $p \mid a$. Tällöin myös $p \mid a^{\frac{p-1}{2}}$, joten $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. Siis $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ eli väite on selvä.

Oletetaan sitten, että $a \not\equiv 0 \pmod{p}$. Ensin huomataan, että Fermat'n pienen lauseen nojalla $a^{p-1} - 1 \equiv 0 \pmod{p}$, joten saadaan

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}}\right)^2 - 1^2 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Siispä luvulle a pätee joko $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ tai $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Lisäksi lauseen 4.9 nojalla kongruenssiyhtälölle $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ on olemassa korkeintaan $\frac{p-1}{2}$ ratkaisua.

Jos a on luvun p neliönjäännös eli $\left(\frac{a}{p}\right) = 1$, niin kongruenssiyhtälöllä $x^2 \equiv a \pmod{p}$ on ratkaisu $x = x_0$. Tällöin

$$x_0^{p-1} = \left(x_0^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p},$$

ja koska Fermat'n pienen lauseen perusteella $x_0^{p-1} \equiv 1 \pmod{p}$, niin

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Siis, kun a on luvun p neliönjäännös, niin $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Saatiin siis, että luvun p neliönjäännöksille a pätee $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Edellä kuitenkin todettiin, että kongruenssiyhtälöllä $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ voi olla korkeintaan $\frac{p-1}{2}$ ratkaisua. Täten, koska lauseen 4.4 todistuksen perusteella luvun p neliönjäännöksiä on tasan $\frac{p-1}{2}$ kappaletta, niin on oltava, että luvun p neliönepäjäännöset toteuttavat välttämättä toisen kongruenssiyhtälön $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Tällöin saadaan myös $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Siispä väite pätee. □

Seuraavaksi tarkastellaan Legendren symbolin käyttäytymistä muutamissa perustapauksissa.

Lause 4.11. *Olkoot $p > 2$ alkuluku ja a ja b kokonaislukuja. Tällöin*

(i) *jos $a \equiv b \pmod{p}$, niin $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(iii) *jos $a \not\equiv 0 \pmod{p}$, niin $\left(\frac{a^2}{p}\right) = 1$.*

(iv) $\left(\frac{1}{p}\right) = 1$.

Todistus (vrt. [13, s. 379]). (i) Jos $a \equiv 0 \equiv b \pmod{p}$, niin suoraan Legendren symbolin määritelmän mukaan $\left(\frac{a}{p}\right) = 0 = \left(\frac{b}{p}\right)$. Oletetaan siis $a \not\equiv 0 \not\equiv b \pmod{p}$. Jos $a \equiv b \pmod{p}$, niin kongruenssiyhtälöllä $x^2 \equiv a \pmod{p}$ on ratkaisu, jos ja vain jos yhtälöllä $x^2 \equiv b \pmod{p}$ on ratkaisu. Siis, mikäli yhtälöllä $x^2 \equiv a \pmod{p}$ on ratkaisu, niin $\left(\frac{a}{p}\right) = 1 = \left(\frac{b}{p}\right)$, ja jos ei, niin $\left(\frac{a}{p}\right) = -1 = \left(\frac{b}{p}\right)$.

(ii) Eulerin kriteerin perusteella (lause 4.10)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \text{ ja } \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}.$$

Yhdistämällä nämä kongruenssin laskusääntöjen perusteella saadaan

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p},$$

eli

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \equiv 0 \pmod{p}.$$

Nyt $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) = 2, 0$ tai -2, mutta koska $p > 2$ on alkuluku, niin on oltava $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) = 0$. Siis $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(iii) Seuraa suoraan määritelmästä 4.7.

(iv) Kongruenssiyhtälöllä $x^2 \equiv 1 \pmod{p}$ on aina ratkaisu, nimittäin $x = 1$ ja $x = -1$.

□

Lause 4.12. *Olkoon $p > 2$ alkuluku ja olkoot a_1, a_2, ..., ja a_r kokonaislukuja. Tällöin*

$$\prod_{i=1}^{r} \left(\frac{a_i}{p}\right) = \left(\frac{\prod_{i=1}^{r} a_i}{p}\right).$$

Todistus. Todistetaan väite induktiolla luvun r suhteen.

Tapaus $r = 1$ on triviaalisti tosi, ja tapaus $r = 2$ on lauseen 4.11 kohta (ii). Oletetaan sitten, että väite pätee, kun $r = n$ eli

$$\prod_{i=1}^{n} \left(\frac{a_i}{p}\right) = \left(\frac{\prod_{i=1}^{n} a_i}{p}\right).$$

Käyttämällä induktio-oletusta saadaan

$$\prod_{i=1}^{n+1} \left(\frac{a_i}{p}\right) = \left(\prod_{i=1}^{n} \left(\frac{a_i}{p}\right)\right)\left(\frac{a_{n+1}}{p}\right) = \left(\frac{\prod_{i=1}^{n} a_i}{p}\right)\left(\frac{a_{n+1}}{p}\right),$$

ja lauseen 4.11 kohdan (ii) perusteella edelleen

$$\left(\frac{\prod_{i=1}^{n} a_i}{p}\right)\left(\frac{a_{n+1}}{p}\right) = \left(\frac{\prod_{i=1}^{n+1} a_i}{p}\right).$$

Näin ollen väite pätee induktioperiaatteen nojalla kaikille positiivisille kokonaisluvuille r. □

Todistetaan seuraavaksi lause liittyen yhteen neliönjäännösten erikoistapaukseen. Kongruenssiyhtälöllä $x^2 \equiv -1 \pmod{p}$ ei aina ole ratkaisua, ja näin ollen saadaan seuraava ehto. Tämä on tarpeellinen tieto tarkasteltaessa myöhemmin Paleyn graafeja.

Lause 4.13. *Olkoon $p > 2$ alkuluku. Tällöin*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{jos } p \equiv 1 \pmod{4} \\ -1, & \text{jos } p \equiv -1 \pmod{4}. \end{cases}$$

Todistus (vrt. [13, s. 380]). Eulerin kriteerin perusteella

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Oletetaan ensin, että $p \equiv 1 \pmod 4$. Tällöin p voidaan kirjoittaa muodossa $p = 4k+1$, missä k on jokin kokonaisluku. Sijoittamalla tämä yllä olevaan kongruenssiyhtälöön, saadaan

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2k} \pmod p.$$

Nyt $(-1)^{2k} = 1$, joten

$$\left(\frac{-1}{p}\right) \equiv 1 \pmod p.$$

Tämä on yhtäpitävää sen kanssa, että $\left(\frac{-1}{p}\right) - 1 \equiv 0 \pmod p$. Koska $\left(\frac{-1}{p}\right) - 1 = 0$ tai -2 ja $p > 2$ alkuluku, niin tulee olla $\left(\frac{-1}{p}\right) - 1 = 0$. Jos olisi $\left(\frac{-1}{p}\right) - 1 = -2$, tästä seuraisi $-2 \equiv 0 \pmod p$ eli $p \mid -2$. Tämä on ristiriitaista, sillä $p > 2$ alkuluku. Siis $\left(\frac{-1}{p}\right) = 1$.

Oletetaan sitten, että $p \equiv -1 \pmod 4$ eli $p \equiv 3 \pmod 4$. Tällöin p voidaan kirjoittaa muodossa $p = 4k + 3$, missä k on jokin kokonaisluku. Saadaan

$$\left(\frac{-1}{p}\right) \equiv (-1)^{2k+1} \pmod p.$$

Nyt $(-1)^{2k+1} = -1$, joten

$$\left(\frac{-1}{p}\right) \equiv -1 \pmod p.$$

Tämä on yhtäpitävää sen kanssa, että $\left(\frac{-1}{p}\right) + 1 \equiv 0 \pmod p$. Koska $\left(\frac{-1}{p}\right) + 1 = 0$ tai 2 ja $p > 2$ alkuluku, niin tulee olla $\left(\frac{-1}{p}\right) + 1 = 0$. Jos olisi $\left(\frac{-1}{p}\right) + 1 = 2$, tästä seuraisi $2 \equiv 0 \pmod p$ eli $p \mid 2$. Tämä on ristiriitaista, sillä $p > 2$ alkuluku. Siis $\left(\frac{-1}{p}\right) = -1$. □

4.1.3 Karakterit

Todistettaessa, että Paleyn graafit toteuttavat k-laajennusaksiooman, tarvitaan avuksi tietoa siitä, että Legendren symboli on *karakteri*. Tässä luvussa käydään läpi karakterin käsite ja osoitetaan, että Legendren symboli täyttää tämän vaatimukset. Esitellään lopuksi jatkossa tarvittava arvio karakterisummille. Päälähteenä luvussa on käytetty Irelandin ja Rosenin teosta *A Classical Introduction to Modern Number Theory* [6, s. 88–91].

Määritelmä 4.14. Olkoon $p > 2$ alkuluku. *Multiplikatiivinen karakteri* kunnassa $\mathbb{Z}_p$ on kuvaus $\chi : \mathbb{Z}_p^* \to \mathbb{C} \setminus \{0\}$, jolle pätee

$$\chi(ab) = \chi(a)\chi(b) \text{ kaikilla } a, b \in \mathbb{Z}_p^*. \tag{4.2}$$

Jatkossa multiplikatiivisia karaktereita tullaan kutsumaan vain *karaktereiksi*, sillä tässä tutkielmassa ei käsitellä muunlaisia karaktereita. *Triviaaliksi karakteriksi* kutsutaan erityistä karakteria $\chi_0 : \mathbb{Z}_p^* \to \mathbb{C} \setminus \{0\}$, jolle pätee $\chi_0(a) = 1$ kaikilla $a \in \mathbb{Z}_p^*$.

Määritelmä 4.15. Olkoon χ karakteri ja olkoon $d > 0$ pienin sellainen kokonaisluku, jolle pätee $\chi^d = \chi_0$. Tällöin lukua d kutsutaan karakterin χ *kertaluvuksi*.

Huomattakoon, että kun p on alkuluku, niin Fermat'n pienen lauseen nojalla kaikille luvuille $a \in \mathbb{Z}_p^*$ pätee $a^{p-1} \equiv 1 \pmod{p}$. Siispä kaikille karaktereille χ pätee $\chi^{p-1} = \chi_0$, ja näin ollen kaikki kunnan $\mathbb{Z}_p$ karakterit ovat korkeintaan kertalukua $p - 1$.

Huomautus. Voi olla hyödyllistä laajentaa karakterin määritelmää siten, että merkitään $\chi(0) = 0$, ja toisaalta triviaalille karakterille merkitään $\chi_0(0) = 1$. Tällöin karakteria voidaan tarkastella koko kunnassa $\mathbb{Z}_p$.

Nyt voimme osoittaa, että luvussa 4.1.2 määritelmässä 4.7 esitelty Legendren symboli on karakteri.

Lause 4.16. *Olkoon $p > 2$ alkuluku ja tarkastellaan kuntaa $\mathbb{Z}_p$. Tällöin Legendren symboli $\left(\frac{a}{p}\right)$ on kunnan $\mathbb{Z}_p$ ei-triviaali karakteri, jonka kertaluku on 2.*

Todistus. Legendren symboli on kuvaus $f : \mathbb{Z}_p \to \{-1, 0, 1\}$, jolle $f(a) = \left(\frac{a}{p}\right)$. Kuvaukselle pätee myös karakterin määritelmässä 4.14 esitelty sääntö 4.2: jos $a, b \in \mathbb{Z}_p$, niin lauseen 4.11 nojalla

$$f(ab) = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = f(a)f(b).$$

Siis karakterin määritelmän nojalla Legendren symboli on kunnan $\mathbb{Z}_p$ karakteri.

Lauseessa 4.4 todettiin, että on olemassa täsmälleen $\frac{p-1}{2}$ neliönjäännöstä ja $\frac{p-1}{2}$ neliönepäjäännöstä modulo p. Koska $p > 2$, tästä seuraa, että on olemassa $b \in \mathbb{Z}_p$, joka on neliönepäjäännös ja näin ollen $\left(\frac{b}{p}\right) = -1$. Siispä Legendren symboli ei ole triviaali karakteri χ_0.

Edellisen perusteella Legendren symbolin kertaluku on suurempi kuin 1. Olkoon sitten $a \in \mathbb{Z}_p^*$. Tällöin lauseen 4.11 nojalla

$$\left(\frac{a}{p}\right)^2 = \left(\frac{a \cdot a}{p}\right) = \left(\frac{a^2}{p}\right) = 1,$$

ja koska a valittiin mielivaltaisesti, niin seuraa, että Legendren symbolin kertaluku on oltava 2. □

Schmidtin teoksessa *Equations over Finite Fields* [14] on todistettu arvio karakterisummille.

Lause 4.17. *Olkoon χ kunnan $\mathbb{Z}_p$ ei-triviaali karakteri, jonka kertaluku on d. Olkoon $f(x)$ kunnan $\mathbb{Z}_p$ polynomi, jolla on täsmälleen m erillistä juurta, ja joka ei ole muotoa $c(g(x))^d$, missä $c \in \mathbb{Z}_p$ ja $g(x)$ on kunnan $\mathbb{Z}_p$ polynomi. Tällöin*

$$\left| \sum_{x \in \mathbb{Z}_p} \chi(f(x)) \right| \leq (m-1)\sqrt{p}.$$

Todistus. Ks. [14, s. 43, 78–80]. □

4.2 Paleyn graafit

Paleyn graafit määritellään neliönjäännösten avulla. Lähteenä Paleyn graafien määritelmään on toiminut Blassin, Exoon ja Hararyn artikkeli *Paley Graphs Satisfy All First-Order Adjacency Axioms* [2] ja täydentävänä materiaalina on toiminut Bollobásin teos *Random graphs* [3, s. 315–316].

Määritelmä 4.18. Olkoon $q > 2$ alkuluku, jolle pätee $q \equiv 1 \pmod 4$[1]. *Paleyn graafi*, jota merkitään P_q, on graafi $P_q = (V, E)$, jossa solmujen joukko on $V = \mathbb{Z}_q$ ja särmien joukko määräytyy seuraavasti:

$$\begin{aligned} E &= \{\{a, b\} \mid a, b \in V \text{ ja } a - b \text{ on luvun q neliönjäännös}\} \\ &= \{\{a, b\} \mid a, b \in V \text{ ja } \left(\frac{a-b}{q}\right) = 1\}. \end{aligned}$$

Määritelmässä 4.18 valitaan luku q siten, että $q \equiv 1 \pmod 4$, jolloin lauseen 4.13 nojalla -1 on luvun q neliönjäännös. Tästä seuraa, että määritettäessä Paleyn graafin P_q särmien joukkoa ei ole väliä miten solmujen arvojen välinen erotus lasketaan: kun valitaan solmut $a, b \in \mathbb{Z}_q$ ja määritetään muodostavatko ne särmän, riittää tarkastella vain toista erotuksista $a - b$ tai $b - a$. Nimittäin, mikäli -1 ja c ovat luvun q neliönjäännöksiä, niin neliönjäännösten määritelmän 4.1 nojalla on olemassa sellaiset $x, y \in \mathbb{Z}_q$, että $-1 \equiv x^2 \pmod q$ ja $c \equiv y^2 \pmod q$. Tällöin luvulle $-c$ saadaan

$$-c = (-1) \cdot c \equiv x^2 \cdot y^2 = (xy)^2 \pmod q,$$

missä $xy \in \mathbb{Z}_p$, joten myös $-c$ on neliönjäännös. Mikäli oletettaisiin, että $-c$ on neliönjäännös, niin samalla päättelyllä seuraisi, että myös c on neliönjäännös. Esimerkissä 4.19 on havainnollistettu asiaa.

Esimerkki 4.19. Tarkastellaan alkulukuja 7 ja 13. Näistä luvuista ainoastaan $q = 13$ toteuttaa yhtälön $q \equiv 1 \pmod 4$.

Kuten esimerkissä 4.6 todettiin, luvut 1, 3 ja 4 ovat luvun 13 neliöjäännöksiä. Edellä todetun nojalla nyt myös -1, -3 ja -4 ovat luvun 13 neliönjäännöksiä. Tämä saadaan tarkastettua huomaamalla, että $-1 \equiv 12$, $-3 \equiv 10$ ja $-4 \equiv 9 \pmod{13}$, missä 9, 10 ja 12 ovat myös luvun 13 neliönjäännöksiä. Toisaalta esimerkin 4.5 nojalla luku 4 on luvun 7 neliönjäännös, mutta $-4 \equiv 3 \pmod 7$ ei ole.

[1] Dirichlet'n lauseen (ks. [13, s. 74]) nojalla tällaisia alkulukuja on ääretön määrä.

Seuraavassa esimerkki Paleyn graafista.

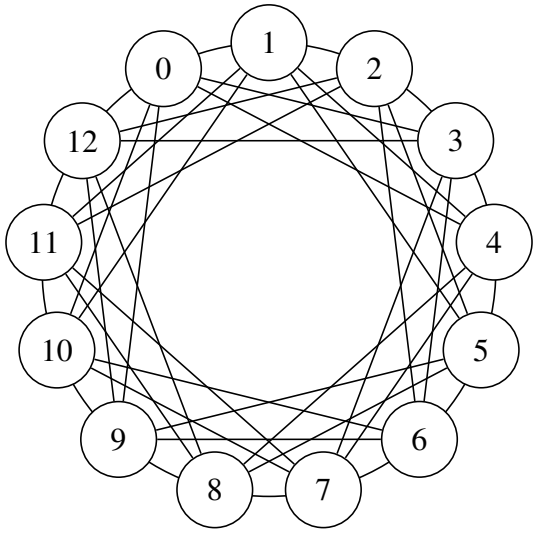
Esimerkki 4.20 (vrt. [19])**.** Valitaan edelleen $q = 13$, jolloin q on alkuluku, jolle pätee $q \equiv 1 \pmod 4$. Näin ollen voidaan muodostaa määritelmän 4.18 mukainen Paleyn graafi P_{13}. Nyt $P_{13} = (V, E)$, jossa solmujen joukko on V on jäännösluokkien joukko

$$\mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

Esimerkin 4.6 nojalla luvun $q = 13$ neliönjäännökset ovat $1, 3, 4, 9, 10$ ja 12, joten särmien joukoksi muodostuu joukko

$$\begin{aligned} E &= \{\{x, y\} \mid x, y \in \mathbb{Z}_{13} \text{ ja } x - y \text{ on luvun 13 neliönjäännös}\} \\ &= \{\{x, y\} \mid x, y \in \mathbb{Z}_{13} \text{ ja } x - y \equiv a^2 \pmod{13} \text{ jollain } a \in \mathbb{Z}_{13}\} \\ &= \{\{x, y\} \mid x, y \in \mathbb{Z}_{13} \text{ ja } x - y \equiv b \pmod{13}, \text{ missä } b \in \{1, 3, 4, 9, 10, 12\}\} \\ &= \{\{x, y\} \mid x, y \in \mathbb{Z}_{13} \text{ ja } x - y \equiv b \pmod{13}, \text{ missä } b \in \{\pm 1, \pm 3, \pm 4\}\}. \end{aligned}$$

Muodostunutta graafia P_{13} on kuvattu kuviossa 4.1. Kuten myös kuviosta 4.1 nähdään, Paleyn graafissa P_{13} jokaisesta solmusta lähtee yhteensä 6 särmää. Solmusta, jonka arvo on a lähtee särmät solmuihin $a \pm 1$, $a \pm 3$ ja $a \pm 4$.



Kuvio 4.1: Paleyn graafi P_{13}. (Vrt. [17].)

4.3 Paleyn graafit toteuttavat k-laajennusaksioomat

Kuten aiemmin luvussa 3 todistettiin, k-laajennusaksiooman toteuttavia graafeja on aina olemassa ja satunnaisgraafi toteuttaa asymptoottisesti melkein varmasti k-laajennusaksiooman. Tässä luvussa todistamme, että Paleyn graafit toteuttavat k-laajennusaksiooman. Päälähteenä luvussa on toiminut Blassin, Exoon ja Hararyn artikkeli *Paley Graphs Satisfy All First-Order Adjacency Axioms* [2].

Aloitetaan esittelemällä ensin varsinaisessa todistuksessa tarvittavia arvioita. Todistetaan ensin, että Legendren symboli toteuttaa karakterisummille lauseessa 4.17 esitellyn arvion.

Lause 4.21. *Olkoon $p > 2$ alkuluku ja olkoot $y_1, y_2, \ldots,$ ja $y_s \in \mathbb{Z}_p$ eri jäännöksiä modulo p. Tällöin*

$$\left| \sum_{x=0}^{p-1} \prod_{i=1}^{s} \left(\frac{x - y_i}{p} \right) \right| \leq (s-1)\sqrt{p}.$$

Todistus. Merkitään $f(x) = \prod_{i=1}^{s}(x - y_i)$. Ensin huomataan, että Legendren symbolin ominaisuuksien nojalla (lause 4.12) voidaan kirjoittaa

$$\begin{aligned} \left| \sum_{x=0}^{p-1} \prod_{i=1}^{s} \left(\frac{x - y_i}{p} \right) \right| &= \left| \sum_{x=0}^{p-1} \left(\frac{\prod_{i=1}^{s}(x - y_i)}{p} \right) \right| \\ &= \left| \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \right|. \end{aligned}$$

Nyt haluttu arvio seuraa suoraan lauseesta 4.17, jossa on esitetty arvio karakterisummille. Lauseen 4.16 mukaan Legendren symboli toteuttaa lauseen 4.17 oletukset: Legendren symboli on kunnan $\mathbb{Z}_p$ ei-triviaali karakteri, jonka kertaluku on 2, joten riittää todeta, että $f(x)$ on sellainen kunnan $\mathbb{Z}_p$ polynomi, jolla on täsmälleen s erillistä juurta, ja joka ei ole muotoa $c(g(x))^2$, missä $c \in \mathbb{Z}_p$ ja $g(x)$ on kunnan $\mathbb{Z}_p$ polynomi.

Oletuksen mukaan $y_1, y_2, \ldots,$ ja y_s ovat eri jäännöksiä, joten funktiolla $f(x)$ on täsmälleen s juurta. Tästä seuraa myös suoraan, että $f(x)$ ei voi olla muotoa $c(g(x))^2$. Siispä lauseen 4.17 nojalla

$$\left| \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \right| \leq (s-1)\sqrt{p},$$

eli väite pätee. □

Lauseet 4.22, 4.23 ja 4.24 ovat tarpeellisia Paleyn graafeja koskevan päälauseen 4.25 todistamisessa.

Lause 4.22 (Pascalin sääntö)**.** *Olkoot n ja k sellaisia kokonaislukuja, joille pätee $1 \leq k \leq n$. Tällöin*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Todistus (vrt. [10]). Laskemalla saadaan

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \left(\frac{n!}{k!(n-k)!}\right) + \left(\frac{n!}{(k-1)!(n-k+1)!}\right) \\
&= n!\left(\frac{1}{k!(n-k)!} + \frac{1}{(k-1)!(n-k+1)!}\right) \\
&= n!\left(\frac{n-k+1}{k!(n-k+1)!} + \frac{k}{k!(n-k+1)!}\right) \\
&= n!\left(\frac{n+1}{k!(n-k+1)!}\right) \\
&= \frac{(n+1)!}{k!(n-k+1)!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

Siis väite pätee. □

Lause 4.23. *Olkoon $n \geq 0$ kokonaisluku. Tällöin*

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Todistus (vrt. [11]). Todistetaan väite induktiolla luvun n suhteen. Kun $n = 0$, niin

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{0} \binom{0}{i} = \binom{0}{0} = 1 = 2^0 = 2^n.$$

Siis väite pätee, kun $n = 0$. Muodostetaan sitten induktio-oletus, että väite pätee arvolla n eli $\sum_{i=0}^{n} \binom{n}{i} = 2^n$. Tällöin Pascalin säännön nojalla (lause 4.22) ja induktio-oletusta käyttämällä saadaan

$$\begin{aligned}
\sum_{i=0}^{n+1} \binom{n+1}{i} &= \binom{n+1}{0} + \sum_{i=1}^{n} \binom{n+1}{i} + \binom{n+1}{n+1} \\
&= \binom{n+1}{0} + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1}\right) + \binom{n+1}{n+1} \\
&= \sum_{i=1}^{n} \binom{n}{i} + \binom{n+1}{0} + \sum_{i=1}^{n} \binom{n}{i-1} + \binom{n+1}{n+1} \\
&= \sum_{i=1}^{n} \binom{n}{i} + \binom{n}{0} + \sum_{i=0}^{n-1} \binom{n}{i} + \binom{n}{n} \\
&= \sum_{i=0}^{n} \binom{n}{i} + \sum_{i=0}^{n} \binom{n}{i} \\
&= 2^n \cdot 2^n = 2^{n+1}.
\end{aligned}$$

Induktioperiaatteen nojalla väite pätee siis kaikille kokonaisluvuille $n \geq 0$. □

Lause 4.24. *Olkoon $n \geq 0$ kokonaisluku. Tällöin*

$$\sum_{i=0}^{n} \binom{n}{i} i = n2^{n-1}.$$

Todistus (vrt. [8]). Laskemalla saadaan

$$\begin{aligned}
\sum_{i=0}^{n} \binom{n}{i} i &= \sum_{i=1}^{n} \binom{n}{i} i = \sum_{i=1}^{n} \frac{n!}{i!(n-i)!} \cdot i \\
&= \sum_{i=1}^{n} \frac{(n-1)!}{(i-1)!(n-i)!} \cdot n \\
&= \sum_{i=1}^{n} \binom{n-1}{i-1} \cdot n \\
&= n \cdot \sum_{i=0}^{n-1} \binom{n-1}{i}.
\end{aligned}$$

Nyt lauseen 4.23 nojalla $\sum_{i=0}^{n-1} \binom{n-1}{i} = 2^{n-1}$, joten $\sum_{i=0}^{n} \binom{n}{i} i = n2^{n-1}$ ja näin ollen väite pätee. □

Edellä esitettyjen lauseiden avulla voidaan todistaa, että riittävän suuret Paleyn graafit toteuttavat k-laajennusaksiooman $\eta_{k,k}$.

Lause 4.25. *Olkoon $k > 0$ kokonaisluku ja olkoon q sellainen alkuluku, jolle $q \equiv 1 \pmod 4$ ja $q > k^2 2^{4k}$. Tällöin Paleyn graafi P_q toteuttaa k-laajennusaksiooman.*

Todistus (vrt. [2, Theorem 1]). Tarkastellaan Paleyn graafia P_q, missä solmujen joukko on $V = V(P_q) = \mathbb{Z}_q$ ja särmien joukko on

$$E = E(P_q) = \{\{a, b\} \mid a, b \in V \text{ ja } \left(\frac{a-b}{q}\right) = 1\}.$$

Aloitetaan muodostamalla ehto k-laajennusaksiooman toteutumiselle. Olkoot $X, Y \subset V$ sellaisia erillisiä solmun joukkoja, että $|X| = |Y| = k$, ja merkitään $X = \{x_1, x_2, \ldots, x_k\}$ ja $Y = \{y_1, y_2, \ldots, y_k\}$. Tarkastellaan summaa

$$\sum_{\substack{w=0 \\ w \notin X \cup Y}}^{q-1} \prod_{i=1}^{k} \left(1 + \left(\frac{w-x_i}{q}\right)\right)\left(1 - \left(\frac{w-y_i}{q}\right)\right). \tag{4.3}$$

Summassa 4.3 käydään yksitellen läpi jokainen solmu $w \in V \setminus (X \cup Y)$ ja verrataan miten se on yhdistetty kaikkiin joukkojen X ja Y solmuihin muodostamalla tulo

$$\prod_{i=1}^{k} \left(1 + \left(\frac{w-x_i}{q}\right)\right)\left(1 - \left(\frac{w-y_i}{q}\right)\right). \tag{4.4}$$

Mikäli solmu w on yhdistetty k-laajennusaksiooman kannalta ei-halutulla tavalla joukkojen X ja Y alkioihin, niin tulo 4.4 saa arvon 0, sillä joko

(i) solmu w ei ole naapuri vähintään yhden solmun $x_t \in X$ kanssa, $1 \leq t \leq k$, jolloin $\left(\frac{w-x_t}{q}\right) = -1$ ja edelleen $1 + \left(\frac{w-x_t}{q}\right) = 1 - 1 = 0$, ja näin ollen tulossa 4.4 esiintyy termi 0, tai

(ii) solmu w on naapuri vähintään yhden solmun $y_s \in Y$ kanssa, $1 \leq s \leq k$, jolloin $\left(\frac{w-y_s}{q}\right) = 1$ ja edelleen $1 - \left(\frac{w-y_s}{q}\right) = 1 - 1 = 0$, jolloin tulossa 4.4 esiintyy myös termi 0.

Jos taas solmu w on yhdistetty k-laajennusaksiooman kannalta oikealla tavalla joukkoihin X ja Y, niin tulo 4.4 saa arvon 2^{2k}, sillä

(i) solmu w on naapuri jokaisen joukon X solmun kanssa eli $1 + \left(\frac{w-x_i}{q}\right) = 1 + 1 = 2$ kaikilla $1 \leq i \leq k$, ja

(ii) solmu w ei ole naapuri yhdenkään joukon Y solmun kanssa eli $1 - \left(\frac{w-y_i}{q}\right) = 1 + 1 = 2$ kaikilla $1 \leq i \leq k$,

ja näin ollen saadaan

$$\prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right) = \prod_{i=1}^{k} 2^2 = \left(2^2\right)^k = 2^{2k}.$$

Käymällä siis kaikki joukon $V \setminus (X \cup Y)$ solmut läpi summassa 4.3, summattavat termit voivat saada arvon 0 tai 2^{2k}. Voidaan kirjoittaa seuraava ehto: Paleyn graafi P_q toteuttaa k-laajennusaksiooman joukkojen X ja Y kohdalla eli on olemassa solmu $z \in V \setminus (X \cup Y)$, joka on naapuri jokaisen joukon X solmun kanssa, mutta ei yhdenkään joukon Y solmun kanssa, jos ja vain jos

$$\sum_{\substack{w=0 \\ w \notin X \cup Y}}^{q-1} \prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right) > 0.$$

Osoitetaan nyt, että Paleyn graafi P_q toteuttaa k-laajennusaksiooman käyttäen edellä muodostettua ehtoa. Tarkastellaan kahta joukkojen X ja Y valinnasta riippuvaista funktiota f ja g, joista f on edellä esitetyssä ehdossa olevan epäyhtälön vasen puoli

$$f(\bar{x}, \bar{y}) = \sum_{\substack{w=0 \\ w \notin X \cup Y}}^{q-1} \prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right)$$

ja funktiossa g summataan kaikkien indeksien $w \in \mathbb{Z}_q$ suhteen eli

$$g(\bar{x}, \bar{y}) = \sum_{w=0}^{q-1} \prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right),$$

missä $\bar{x} = (x_1, x_2, \ldots, x_k)$ ja $\bar{y} = (y_1, y_2, \ldots, y_k)$. Merkitään selkeyden vuoksi jatkossa $A = X \cup Y$. Ensin huomataan, että funktio f voidaan kirjoittaa nyt muodossa

$$f(\bar{x}, \bar{y}) = g(\bar{x}, \bar{y}) - \sum_{w \in A} \prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right).$$

Arvioidaan funktiota $g(\bar{x}, \bar{y})$ ja osoitetaan sen avulla, että $f(\bar{x}, \bar{y}) > 0$. Avaamalla funktion $g(\bar{x}, \bar{y})$ lauseketta, yleisen osittelulain nojalla saadaan

$$\begin{aligned}
g(\bar{x}, \bar{y}) &= \sum_{w=0}^{q-1} \prod_{i=1}^{k} \left(1 + \left(\frac{w - x_i}{q}\right)\right)\left(1 - \left(\frac{w - y_i}{q}\right)\right) \\
&= \sum_{w=0}^{q-1} 1 + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ C \neq \emptyset}} \prod_{c \in C} (-1)^{|C \cap Y|} \left(\frac{w - c}{q}\right) \\
&= \sum_{w=0}^{q-1} 1 + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=1}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|>1}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) \\
&= q + \sum_{w=0}^{q-1} \sum_{i=1}^{k} \left(\frac{w - x_i}{q}\right) - \sum_{w=0}^{q-1} \sum_{i=1}^{k} \left(\frac{w - y_i}{q}\right) + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|>1}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right),
\end{aligned}$$

kun merkitään $\epsilon_C = (-1)^{|C \cap Y|}$. Tässä lausekkeessa kaksi keskimmäistä summattavaa termiä $\sum_{w=0}^{q-1} \sum_{i=1}^{k} \left(\frac{w-x_i}{q}\right)$ ja $\sum_{w=0}^{q-1} \sum_{i=1}^{k} \left(\frac{w-y_i}{q}\right)$ saavat arvon 0, sillä nämä summat käyvät läpi kaikki solmut $w \in \mathbb{Z}_q$, ja luvun 4.1 lauseen 4.4 nojalla luvun q neliönjäännöksiä ja neliönepäjäännöksiä on kumpiakin tasan $\frac{q-1}{2}$ kappaletta. Näin ollen verrattaessa solmuja x_i tai y_i, $1 \leq i \leq k$ solmuihin $w \in \mathbb{Z}_q$, puolet erotuksista ovat neliönjäännöksiä ja puolet eivät, ja näin ollen arvot 1 ja -1 kumoavat toisensa. Siis saadaan

$$g(\bar{x}, \bar{y}) = q + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|>1}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right).$$

Nyt kolmioepäyhtälön nojalla saadaan arvio

$$\begin{aligned}
|g(\bar{x}, \bar{y}) - q| &= \left| \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|>1}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) \right| \\
&= \left| \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=2}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=3}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) + \cdots + \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=2k}} \prod_{c \in C} \epsilon_C \left(\frac{w - c}{q}\right) \right| \\
&\leq \left| \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=2}} \prod_{c \in C} \left(\frac{w - c}{q}\right) \right| + \left| \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=3}} \prod_{c \in C} \left(\frac{w - c}{q}\right) \right| + \cdots + \left| \sum_{w=0}^{q-1} \sum_{\substack{C \subseteq A \\ |C|=2k}} \prod_{c \in C} \left(\frac{w - c}{q}\right) \right|.
\end{aligned}$$

Olkoon nyt $C \subseteq A$, sellainen, että $|C| = s$ ja merkitään $C = \{c_1, c_2, \ldots, c_s\}$. Alkiot c_1, c_2, $\ldots$, c_s ovat eri alkioita, ja koska osajoukko $C \subseteq A$ voidaan valita joukosta $A = X \cup Y$ yhteensä $\binom{2k}{s}$ eri tavalla, niin lauseen 4.21 nojalla nyt

$$\begin{aligned}\left|\sum_{w=0}^{q-1}\sum_{\substack{C\subseteq A\\|C|=s}}\prod_{c\in C}\left(\frac{w-c}{q}\right)\right| &\leq \sum_{\substack{C\subseteq A\\|C|=s}}\left|\sum_{w=0}^{q-1}\prod_{c\in C}\left(\frac{w-c}{q}\right)\right| \\ &\leq \sum_{\substack{C\subseteq A\\|C|=s}}(s-1)\sqrt{q} \\ &= \binom{2k}{s}\cdot(s-1)\sqrt{q}.\end{aligned}$$

Näin ollen $|g(\bar{x},\bar{y}) - q| \leq \sum_{s=2}^{2k}\binom{2k}{s}(s-1)\sqrt{q}$. Aiemmin todistettujen lauseiden 4.23 ja 4.24 nojalla kuitenkin

$$\begin{aligned}&\sum_{s=2}^{2k}\binom{2k}{s}\cdot(s-1)\sqrt{q} = \sqrt{q}\left(\sum_{s=2}^{2k}\binom{2k}{s}s - \sum_{s=2}^{2k}\binom{2k}{s}\right) \\ &= \sqrt{q}\left(\sum_{s=0}^{2k}\binom{2k}{s}s - \binom{2k}{0}\cdot 0 - \binom{2k}{1}\cdot 1 - \sum_{s=0}^{2k}\binom{2k}{s} + \binom{2k}{0} + \binom{2k}{1}\right) \\ &= \sqrt{q}\left(2k\cdot 2^{2k-1} - 0 - 2k - 2^{2k} + 1 + 2k\right) \\ &= \sqrt{q}\left(2k\cdot 2^{2k-1} - 2\cdot 2^{2k-1} + 1\right) \\ &= \sqrt{q}\left((2k-2)\cdot 2^{2k-1} + 1\right).\end{aligned}$$

Siis $|g(\bar{x},\bar{y}) - q| \leq \sqrt{q}\left((2k-2)\cdot 2^{2k-1}+1\right)$, eli funktiolle $g(\bar{x},\bar{y})$ saadaan arvio

$$g(\bar{x},\bar{y}) \geq q - \sqrt{q}\left((2k-2)\cdot 2^{2k-1}+1\right). \tag{4.5}$$

Huomattakoon, että kun $q > k^2 2^{4k}$, yllä olevan epäyhtälön oikeanpuoleinen lauseke on kasvava. Tämän funktiolle g muodostetun arvion avulla voidaan nyt osoittaa, että $f(\bar{x},\bar{y}) > 0$. Tarkastellaan erotusta

$$g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) = \sum_{w\in A}\prod_{i=1}^{k}\left(1+\left(\frac{w-x_i}{q}\right)\right)\left(1-\left(\frac{w-y_i}{q}\right)\right). \tag{4.6}$$

Selvästi $g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) \geq 0$. Jos $g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) = 0$ ja valitaan $q > k^2 2^{4k}$, niin arvion 4.5 nojalla saadaan

$$
\begin{aligned}
f(\bar{x},\bar{y}) = g(\bar{x},\bar{y}) &\geq q - \sqrt{q}\left((2k-2)\cdot 2^{2k-1}+1\right)\\
&> k^2 2^{4k} - \sqrt{k^2 2^{4k}}\left((2k-2)\cdot 2^{2k-1}+1\right)\\
&= k^2 2^{4k} - k2^{2k}\left(k2^{2k} - 2^{2k} + 1\right)\\
&= k^2 2^{4k} - k^2 2^{4k} + k2^{4k} - k2^{2k}\\
&= k\left(2^{4k} - 2^{2k}\right)\\
&> 0,
\end{aligned}
$$

kun $k > 0$. Tällöin väite on siis selvä.

Tarkastellaan sitten tapausta $g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) > 0$. Tällöin on olemassa vähintään yksi sellainen $w_0 \in A$, jolle

$$
\prod_{i=1}^{k}\left(1+\left(\frac{w_0 - x_i}{q}\right)\right)\left(1-\left(\frac{w_0 - y_i}{q}\right)\right) > 0. \tag{4.7}
$$

Koska $w_0 \in A$ tuottaa summaan 4.6 nollasta eroavan positiivisen termin, on oltava $\left(\frac{w_0 - x_i}{q}\right) = 1$ ja $\left(\frac{w_0 - y_i}{q}\right) = -1$ kaikilla $1 \leq i \leq k$ ja $w_0 \neq x_i, y_i$, sillä muutoin tulo 4.7 saisi arvon 0. Saadaan kaksi tapausta:

(i) jos $w_0 \in X$, niin summa 4.6 sievenee summattavaksi indeksien $w \in X$ suhteen: kaikilla $y \in Y$ summattava termi eli tulo 4.7 sisältää tekijän $1 + \left(\frac{y - w_0}{q}\right) = 1 - 1 = 0$, eli summattavan termin arvo on 0, ja

(ii) jos $w_0 \in Y$, niin summa 4.6 sievenee summattavaksi indeksien $w \in Y$ suhteen: kaikilla $x \in X$ summattava termi eli tulo 4.7 sisältää tekijän $1 - \left(\frac{x - w_0}{q}\right) = 1 - 1 = 0$, eli summattavan termin arvo on 0.

Voidaan siis olettaa, että $w_0 \in X$, sillä seuraavat päättelyt voidaan tehdä tästä valinnasta riippumatta. Summalle 4.6 saadaan

$$
\begin{aligned}
g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) &= \sum_{w\in A}\prod_{i=1}^{k}\left(1+\left(\frac{w - x_i}{q}\right)\right)\left(1-\left(\frac{w - y_i}{q}\right)\right)\\
&= \sum_{w\in X}\prod_{i=1}^{k}\left(1+\left(\frac{w - x_i}{q}\right)\right)\left(1-\left(\frac{w - y_i}{q}\right)\right)\\
&\leq \sum_{w\in X}\prod_{i=1}^{k} 2\cdot 2\\
&= k2^{2k}.
\end{aligned}
$$

Siis $g(\bar{x}, \bar{y}) - f(\bar{x}, \bar{y}) \leq k2^{2k}$. Kuten edellä huomattiin, kun valitaan $q > k^2 2^{4k}$, niin toisaalta $g(\bar{x}, \bar{y}) > k\left(2^{4k} - 2^{2k}\right)$. Yhdistämällä nämä tiedot saadaan

$$\begin{aligned} f(\bar{x}, \bar{y}) &\geq g(\bar{x}, \bar{y}) - k2^{2k} \\ &> k\left(2^{4k} - 2^{2k}\right) - k2^{2k} \\ &= k\left(2^{4k} - 2^{2k+1}\right) \\ &> 0, \end{aligned}$$

kun $k > 0$. Siis väite on voimassa tässäkin tapauksessa.

Saatiin siis osoitettua, että todistuksen alussa muodostettu ehto pätee Paleyn graafille P_q. Näin ollen alkuperäinen väite pätee eli Paleyn graafi P_q toteuttaa k-laajennusaksiooman. □

Esitetään vielä lopuksi esimerkki saatuun tulokseen liittyen. Esimerkki osoittaa kuitenkin myös, että edellä esitetyn lauseen oletuksissa olisi tarkentamisen varaa.

Esimerkki 4.26 (vrt. [2])**.** Tarkastellaan ensin 1-laajennusaksioomaa $\eta_{1,1}$. Kun valitaan $q = 17$, niin $q \equiv 1 \pmod 4$ ja $q > 1^2 \cdot 2^{4\cdot 1} = 16$, joten edellä todistetun lauseen 4.25 perusteella Paleyn graafi P_{17} toteuttaa 1-laajennusaksiooman. Mikäli siis valitaan Paleyn graafin P_{17} solmujen joukosta $\mathbb{Z}_{17}$ mitkä tahansa 2 solmua x ja y, niin solmujen joukosta löytyy aina eri solmu z, joka on naapuri solmun x kanssa, mutta ei solmun y kanssa.

Kuitenkin, kuten luvussa 2 esimerkissä 2.9 huomattiin, myös Paleyn graafi P_5 toteuttaa 1-laajennusaksiooman. Luku $q = 5$ ei kuitenkaan toteuta lauseen ehtoa $q > 1^2 \cdot 2^{4\cdot 1} = 16$.

Jos tarkastellaan 2-laajennusaksioomaa $\eta_{2,2}$, niin lauseen 4.25 nojalla P_{1033} on pienin Paleyn graafi, joka toteuttaa tämän. Toisaalta Ronald Readin artikkelissa *Prospects for graph theory algorithms* [12] on todettu, että myös Paleyn graafi P_{61} toteuttaa 2-laajennusaksiooman. Kuitenkaan myöskään luku $q = 61$ ei toteuta lauseen 4.25 ehtoa $q > 2^2 \cdot 2^{4\cdot 2} = 1024$.

Saatiin siis todistettua seuraavaa: Paleyn graafissa on oltava vähintään $k^2 2^{4k}$ solmua, jotta se toteuttaa k-laajennusaksiooman. Toisaalta luvussa 3 puolestaan todistettiin, että on olemassa kooltaan vähintään $8k^2 2^{2k}$ oleva graafi, joka toteuttaa k-laajennusaksiooman. Kuten mainittua, näissä oletuksissa on kuitenkin tarkentamisen varaa.

Lähteet

[1] Anderson J. ja Bell J., *Number Theory with Applicatons*. New Jersey: Prentice-Hall, Inc., 1997.

[2] Blass A., Exoo G. ja Harary F., *Paley Graphs Satisfy All First-Order Adjacency Axioms*. Journal of Graph Theory 5 (1981), No. 4, s. 435–439.

[3] Bollobàs B., *Random Graphs*. Orlando: Academic Press, Inc., 1985.

[4] Bonato A., *The search for n-e.c. graphs*. Contributions to Discrete Mathematics 4 (2009), No. 1, s. 40–53.

[5] Diestel R., *Graph Theory*, (3. ed.). Berlin: Springer, 2006.

[6] Ireland K. ja Rosen M., *A Classical Introduction to Modern Number Theory*. New York: Springer, 1990.

[7] Koivisto P. ja Niemistö R., *Graafiteoriaa*. Luentomoniste [verkkodokumentti], 2001 [viitattu 25.4.2018].
URL: http://www.sis.uta.fi/matematiikka/graafiteoria/graafiteoriaa.pdf

[8] ProofWiki, *Increasing Sum of Binomial Coefficients*, 2016, [viitattu 25.4.2018].
URL: https://proofwiki.org/wiki/Increasing_Sum_of_Binomial_Coefficients

[9] ProofWiki, *Number of Quadratic Residues of Prime*, 2016, [viitattu 26.4.2018].
URL: https://proofwiki.org/wiki/Number_of_Quadratic_Residues_of_Prime

[10] ProofWiki, *Pascal's Rule*, 2017, [viitattu 25.4.2018].
URL: https://proofwiki.org/wiki/Pascal%27s_Rule

[11] ProofWiki, *Sum of Binomial Coefficients over Lower Index*, 2016, [viitattu 25.4.2018].
URL: https://proofwiki.org/wiki/Sum_of_Binomial_Coefficients_over_Lower_Index

[12] Read R. C., *Prospects for Graph Theory Algorithms*. Annals of Discrete Mathematics, Vol. 55 (1993), s. 201-210.

[13] Rosen K. H., *Elementary number theory and its applications*, (4. ed.). Reading (Mass.): Addison-Wesley, 2000.

[14] Schmidt W., *Equations over Finite Fields, An Elementary Approach*. Berlin: Springer, 1976.

[15] Spencer J., *The Strange Logic of Random Graphs*. Berlin: Springer, 2001.

[16] Väisälä K., *Lukuteorian ja korkeamman algebran alkeet*. Helsinki: Otava, 1950.

[17] Weisstein E. W., *Paley Graph*, WolframMathWorld [verkkodokumentti], 2018 [viitattu 23.4.2018].
URL: http://mathworld.wolfram.com/PaleyGraph.html

[18] Wikipedia, *Erdős-Rényi model* [verkkodokumentti], 2018 [viitattu 24.4.2018].
URL: https://en.wikipedia.org/wiki/Erdős-Rényi_model

[19] Wikipedia, *Paley graph* [verkkodokumentti], 2018 [viitattu 24.4.2018].
URL: https://en.wikipedia.org/wiki/Paley_graph