Hadamardin matriiseista Steinerin systeemeihin

LuK Atte Virtanen

Pro gradu -tutkielma
Toukokuu 2022

Tarkastajat:
Prof. Vesa Halava
Prof. Tero Harju

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

ATTE VIRTANEN: Hadamardin matriiseista Steinerin systeemeihin
Pro gradu -tutkielma, 34 s.
Matematiikka
Toukokuu 2022

Tämän kirjallisuuteen perustuvan pro gradu -tutkielman pääaiheita ovat Hadamardin matriisit ja lohkosommitelmat. Tutkimuksen kohteina ovat myös äärelliset projektiiviset tasot ja Steinerin systeemit, jotka ovat tietynlaisia lohkosommitelmia. Työ kuuluu diskreetin matematiikan, lineaarialgebran ja kombinatoriikan alaan. Tärkeimmät lähdeteokset ovat olleet Ian Andersonin kirja *Combinatorial Designs: Construction Methods*, Marshall Hall Juniorin kirja *Combinatorial Theory* sekä Ian Andersonin ja Iiro Honkalan luentomoniste *A Short Course in Combinatorial Mathematics*.

Tutkielman alkupuolella tarkastellaan Hadamardin matriiseja. Ne ovat neliömatriiseja, joiden alkiot ovat positiivisia ja negatiivisia ykkösiä sopivassa järjestyksessä. Kun Hadamardin matriisi ja sen transpoosi kerrotaan keskenään, tuloksena on diagonaalimatriisi, jonka jokainen diagonaalialkio on matriisin asteluku. Alkuosan keskeisimpänä asiana esitellään kaksi Hadamardin matriisien konstruointimenetelmää ja muutamia esimerkkitapauksia.

Keskiosassa siirrytään tutkimaan lohkosommitelmia. Ne ovat matemaattisia esiintyvyysjärjestelmiä, joissa äärellisen perusjoukon alkiot jaetaan lohkoihin eli osajoukkoihin sellaisella tavalla, että lohkot ja alkiot ovat toistensa kanssa erityisessä relaatiossa. Sommitelmassa on tietty määrä lohkoja, joissa jokainen alkio ja jokainen alkiopari tai yleisemmin t-alkioinen osajoukko esiintyy. Lisäksi kaikissa lohkoissa on tietty määrä alkioita. Kolmannessa luvussa tutkitaan sommitelmien ominaisuuksia, muodostetaan yksinkertaisia esimerkkejä ja löydetään luonnollinen yhteys Hadamardin matriisien ja sommitelmien välille.

Työn loppupuolella tutustutaan äärellisiin projektiivisiin tasoihin ja Steinerin systeemeihin. Projektiivisia tasoja muodostetaan äärellisen geometrian avulla. Osoittautuu, että pisteet voidaan tulkita alkioiksi ja suorat lohkoiksi, ja näin projektiivinen taso on myös sommitelma. Steinerin systeemit puolestaan ovat lohkosommitelmia, joissa jokainen perusjoukon t-alkioinen osajoukko kuuluu täsmälleen yhteen lohkoon. Loppuosan tärkein teoreettinen asia on Steinerin kolmikkosysteemin konstruoiminen Skolemin menetelmällä. Lisäksi viidennen luvun lopussa laajennetaan Hadamardin 2-sommitelma 3-sommitelmaksi ja tarkastellaan hieman Steinerin nelikkosysteemeitä.

Asiasanat: matriisi, lohkosommitelma, äärellinen geometria, Steinerin systeemi.

Sisällys

1 Johdanto

Tutkielman lähtökohta on ollut Turun yliopiston kombinatoriikan jatkokurssi, jonka sisällöstä tarkastelun kohteiksi ovat valikoituneet Hadamardin matriisit, lohkosommitelmat, äärelliset projektiiviset tasot ja Steinerin systeemit. Tarkoitus on yhtäältä esitellä aiheet omina kokonaisuuksinaan ja toisaalta löytää yhteydet näiden välille. Käsitteet määritellään täsmällisesti ja lauseet todistetaan syvällisesti. Lukijalle näytetään myös havainnollistavia esimerkkejä helpottamaan tulosten ymmärtämistä.

Tarkastelu aloitetaan Hadamardin matriiseista. Ne ovat neliömuotoisia, jokainen alkio on -1 tai 1 ja rivit sekä sarakkeet ovat keskenään ortogonaaliset eli niiden sisätulo on nolla. Hadamardin matriisien avulla voidaan löytää esimerkiksi virheitä korjaavia koodeja. Niitä voidaan käyttää hyödyksi myös tilastotieteessä estimoitaessa parametriestimaattorin varianssia. Tässä tutkielmassa ei kuitenkaan käsitellä näitä sovelluskohteita vaan tarkastellaan keskeisiä ominaisuuksia sekä konstruoimista Paleyn ja Williamsonin menetelmillä. Paleyn metodin käyttämiseen tarvitaan myös äärellisiä kuntia ja matriisilaskennassa toisinaan esiintyvää Kroneckerin suoraa tuloa. Raymond Paley ($1907 - 1933$) julkaisi menetelmänsä kuolinvuonnaan 1933.

Lohkosommitelmat muodostavat tutkielman toisen laajan kokonaisuuden. Sommitelmat ovat tietyn kokoisista lohkoista koostuvia kokoelmia. Lohkoihin valitaan sellaiset äärellisen perusjoukon alkiot, että kokoelmasta tulee symmetrinen. Tämä tarkoittaa, että on oltava tietty määrä lohkoja, joihin alkio tai alkiopari ilmaantuu. Lähemmän tarkastelun kohteina ovat sommitelman matriisi, symmetrinen sommitelma ja Hadamardin sommitelma, josta löydetään yhteys Hadamardin matriiseihin. Tärkeimpiä esimerkkitapauksia on $(7, 3, 1)$-sommitelma, sillä samankaltainen konstruktio tulee vastaan myöhemmissäkin luvuissa.

Luvussa 4 tarkastellaan äärellisiä projektiivisia tasoja, ja sitä voidaan pitää eräänlaisena väliosuutena, koska tässä tutkielmassa aiheen käsittely on hieman suppeampaa. Projektiiviset tasot yhdistetään heti määritelmässä sommitelmiin ja vasta tämän jälkeen esitellään tason konstruktio pisteiden ja lohkojen eli suorien avulla. Pisteet ovat perusjoukon alkiokolmikoiden muodostamia ekvivalenssiluokkia. Mikäli jokin kolmikko on toisen kolmikon monikerta, niitä vastaavat pisteet tulkitaan samoiksi. Esimerkkeinä tarkastellaan toisen ja neljännen asteen projektiivisia tasoja. Luvun merkittävä päätelmä on, että 2-asteinen projektiivinen taso on myös 2-asteinen Hadamardin sommitelma ja $(7, 3, 1)$-sommitelma.

Tutkielman loppuosassa keskitytään niihin sommitelmiin, joita kutsutaan Steinerin systeemeiksi. Myös nämä määritellään aluksi sommitelmien avulla, mutta sitten esitellään yksityiskohtaisesti nimenomaan Steinerin kolmikkosysteemien suora konstruointimenetelmä, Skolemin metodi. Steinerin systeemit ovat siis sommitelmia, joita konstruoitaessa ei välttämättä tutkita perusjoukon alkioparien esiintyvyyttä lohkoissa vaan yleisemmin t-alkioisen osajoukon esiintyvyyttä ja joissa jokainen tällainen osajoukko esiintyy täsmälleen yhdessä lohkossa. Kolmikkosysteemi puolestaan tarkoittaa, että jokaisessa lohkossa on kolme alkiota. Kun Skolemin metodilla kootaan kolmikkosysteemi $S(2, 3, 7)$, huomataan, että kyseessä on jälleen $(7, 3, 1)$-sommitelma sekä 2-asteinen Hadamardin sommitelma ja projektiivinen taso. Myöhemmin pystytään todistamaan, että kaikki Hadamardin 2-sommitelmat voidaan laajentaa 3-sommitelmiksi. Tämä merkitsee sitä, että alkioparien sijaan tarkastel-

laan alkiokolmikoiden esiintyvyyttä lohkoissa. Aivan lopuksi laajennetaan myös yleinen Steinerin nelikkosysteemi hajoavien sommitelmien ja Hananin tuplausmenetelmän avulla.

Lukijalta edellytetään tuntemusta yliopistomatematiikan perusasioista, erityisesti matriisilaskennasta ja kombinatoriikasta. Matriisin $\mathbf{A}$ determinantista käytetään tässä työssä merkintää $|\mathbf{A}|$. Lisäksi $\mathbf{I}$ tarkoittaa matriisia, jonka diagonaalialkiot ovat ykkösiä ja muut alkiot nollia, ja $\mathbf{J}$ tarkoittaa kokonaan ykkösistä koostuvaa matriisia.

Suurin osa tutkielman teoriaosuuksista on kirjoitettu Ian Andersonin teoksen [1] pohjalta. Tutkittaessa Paleyn ja Williamsonin metodeja sekä lohkosommitelmien määritelmää ja perusominaisuuksia päälähde on Marshall Hall Juniorin teos [3]. Iiro Honkalan ja Ian Andersonin luentomoniste [2] on tiettyjen esitysten lähde. Se on lisäksi myös ollut yleinen tuki pohjatyöskentelyssä. Osa esimerkeistä on poimittu lähdekirjallisuudesta niiden havainnollistavuuden vuoksi, mutta kirjoittaja on myös pyrkinyt lisäämään työhön omia esimerkkejään. Myös vastuu aiheen rajaamisesta ja käännöstyöstä on ollut kirjoittajan.

2 Hadamardin matriisit

2.1 Perustietoa, esimerkkejä ja ominaisuuksia

Tämän luvun alkuosa perustuu lähteeseen [1], ellei toisin mainita. Ensimmäiseksi määritellään Hadamardin matriisi. Niiden olemassaolo liittyy oleellisesti myöhemmin tarkasteltavien Hadamardin sommitelmien olemassaoloon.

Määritelmä 1. Olkoon $\mathbf{H}$ neliömatriisi, jonka dimensio eli aste on m ja jonka alkiot kuuluvat joukkoon $\{-1, 1\}$. Olkoon $\mathbf{I}_m$ m-asteinen identiteettimatriisi. Matriisi $\mathbf{H}$ on *Hadamardin matriisi*, jos se toteuttaa ehdon

$$\mathbf{H}^T\mathbf{H} = m\mathbf{I}_m. \tag{1}$$

Käytetään tästä eteenpäin Hadamardin matriisista lyhennettä H-matriisi. Niiden tutkimuksen voidaan katsoa alkaneen vuonna 1867, kun James Joseph Sylvester $(1814-1897)$ tarkasteli tiilitysongelman ja H-matriisien välistä yhteyttä. Hän myös löysi tavan muodostaa 2^n-asteisia H-matriiseja. Tähän palataan seuraavassa alaluvussa. Myöhemmin vuonna 1893 Jacques Hadamard $(1865-1963)$ havaitsi, että m-asteisen neliömatriisin $\mathbf{A} = (a_{ij})$ determinantti on korkeintaan $m^{m/2}$, kun $|a_{ij}| \leq 1$ kaikilla indekseillä i, j. Erityisesti $|\mathbf{A}| = m^{m/2}$ tarkalleen silloin kun $\mathbf{A}^T\mathbf{A} = m\mathbf{I}_m$.

Tarkastellaan seuraavaksi yksinkertaisia esimerkkitapauksia.

Esimerkki 1. Ensimmäisen, toisen ja neljännen asteen H-matriiseja ovat

$$(1),\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ ja } \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Äkkiseltään saattaa luulla, että on olemassa myös esimerkiksi tyyppiä (3×3) oleva H-matriisi. Osoittautuu kuitenkin, että jos H-matriisi on olemassa, niin sen asteluvun on oltava yksi, kaksi tai jokin neljän monikerta. Tehdään seuraavaksi muutama havainto määritelmän 1 pohjalta ja todistetaan kaksi aputulosta, minkä jälkeen päästään edellä mainittuun tulokseen.

Tarkastellaan H-matriisin diagonaalin ulkopuolisia alkioita. Ehdon (1) perusteella seuraa, että matriisin $\mathbf{H}^T$ i:nnen rivin ja matriisin $\mathbf{H}$ j:nnen sarakkeen sisätulo on nolla, kun i ja j eroavat toisistaan. Toisin sanoen minkä tahansa kahden eri rivin tai sarakkeen sisätulo on nolla. Matriisin $\mathbf{H}$ rivit ja sarakkeet ovat siis *ortogonaaliset*. Ehdosta (1) nähdään lisäksi, että kyseinen matriisi on kääntyvä ja $\mathbf{H}^{-1} = \frac{1}{m}\mathbf{H}$. Näin ollen $\mathbf{H}$ kommutoi sekä käänteismatriisinsa että transpoosinsa kanssa, ja myös matriisin $\mathbf{H}^T$ mitkä tahansa kaksi riviä ja sarakketta ovat ortogonaalisia. Tämä perustelee seuraavan aputuloksen.

Lemma 1. *Neliömatriisi* $\mathbf{H}$*, jonka asteluku on* m *ja jonka alkiot kuuluvat joukkoon* $\{-1, 1\}$ *on Hadamardin matriisi täsmälleen silloin kun sen rivit tai sarakkeet ovat parittain ortogonaaliset.*

Seuraavaksi huomataan, että ehto (1) pysyy voimassa, vaikka rivejä ja sarakkeita permutoitaisiin tai joitain rivejä ja sarakkeita kerrottaisiin luvulla -1. Tällä tavalla saadaan siis aikaan uusia ja alkuperäisen matriisin kanssa ekvivalentteja H-matriiseja.

Huomautus 1. Jos $\mathbf{H}'$ ja $\mathbf{H}''$ ovat ekvivalentteja H-matriiseja, niin

$$\mathbf{H}'' = \mathbf{P}\mathbf{H}'\mathbf{Q},$$

missä $\mathbf{P}$ ja $\mathbf{Q}$ ovat monomisia permutaatiomatriiseja. Tässä tapauksessa matriisien $\mathbf{P}$ ja $\mathbf{Q}$ jokainen rivi ja sarake sisältää täsmälleen yhden nollasta eroavan alkion, joka on ± 1. Mainitaan vielä, että $\mathbf{P}$ määrää matriisin $\mathbf{H}'$ *rivien* permutaatiot sekä etumerkkimuunnokset ja $\mathbf{Q}$ määrää *sarakkeiden* vastaavat muunnokset. [3]
Esimerkiksi

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

Jos H-matriisi järjestetään muotoon, jossa ensimmäinen rivi ja sarake koostuvat pelkästään positiivisista ykkösistä, matriisia kutsutaan *normalisoiduksi* H-matriisiksi. Todetaan, että esimerkin 1 matriisit ovat normalisoidussa muodossa. Todistetaan sitten H-matriisin alkioiden järjestystä koskeva aputulos.

Lemma 2. *Olkoon* $\mathbf{H}$ *normalisoitu* m*-asteinen* H*-matriisi. Tarkastellaan muita kuin ensimmäistä riviä ja saraketta. Nyt niillä on* $m/2$ *positiivista ykköstä ja* $m/2$ *negatiivista ykköstä. Jos lisäksi* $m > 2$*, parittaisilla riveillä on* $m/4$*:ssä sarakkeessa yhtä aikaa* $+1$ *ja vastaavasti* $m/4$*:ssä sarakkeessa yhtä aikaa* -1*.*

Todistus. Olkoon R_1 ensimmäinen rivi, jonka kaikki alkiot ovat positiivisia ykkösiä. Olkoon R_2 jokin toinen rivi, jolla on x positiivista ykköstä ja y negatiivista ykköstä. Tällöin $R_1 \cdot R_2 = x - y$. Koska rivit ovat parittain ortogonaaliset, $x - y = 0$ eli $x = y$. Tiedetään, että $x + y = m$, joten väistämättä $x = y = m/2$.

Olkoon $m > 2$ ja R_3 mikä tahansa toinen rivi. Oletetaan, että matriisissa $\mathbf{H}$ on λ saraketta, joissa riveillä R_2 ja R_3 on $+1$ yhtä aikaa. Tällöin todistuksen ensimmäisen osan nojalla on $m/2 - \lambda$ saraketta, joissa rivillä R_2 on $+1$ ja rivillä R_3 on -1. Oletetaan myös, että matriisissa $\mathbf{H}$ on μ saraketta, joissa riveillä R_2 ja R_3 on -1 yhtä aikaa. Tällöin vastaavasti on $m/2 - \mu$ saraketta, joissa rivillä R_2 on -1 ja rivillä R_3 on $+1$. Koska rivin R_3 positiivisten ykkösten lukumäärän on oltava $m/2$, saadaan yhtälö

$$\lambda + (m/2 - \mu) = m/2 \Leftrightarrow \lambda = \mu.$$

Tiedetään, että R_2 ja R_3 ovat ortogonaaliset, joten

$$0 = 1 \cdot 1 + 1 \cdot (-1) + (-1) \cdot 1 + (-1) \cdot (-1). \tag{2}$$

Koska tiedetään myös, kuinka monta kertaa jokainen yhtälön (2) neljästä eri tulosta tapahtuu, voidaan merkitä

$$0 = \lambda - (m/2 - \lambda) + \mu - (m/2 - \mu) = 2\lambda + 2\mu - m = 4\lambda - m.$$

Lopulta saadaan

$$\lambda = \mu = m/4.$$

□

Lemmoista 1 ja 2 seuraa nyt merkittävä lause:

Lause 1. *Jos m-asteinen H-matriisi on olemassa, niin $m = 1$, $m = 2$ tai $m = 4n$ ($n \in \mathbb{N}_1$).*

2.2 Paleyn metodi

Siirrytään tarkastelemaan Hadamardin matriisien konstruoimista. Esitellään ensin Sylvesterin löytämä ääretön H-matriisiperhe. Olkoot $\mathbf{H}_0 = (1)$ ja $\mathbf{H}_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Nyt voidaan määritellä

$$\mathbf{H}_n = \begin{pmatrix} \mathbf{H}_{n-1} & \mathbf{H}_{n-1} \\ \mathbf{H}_{n-1} & -\mathbf{H}_{n-1} \end{pmatrix}, \text{ kun } n \geq 1. \tag{3}$$

Osoitetaan, että näin rekursiivisesti saatujen H-matriisien asteluvut ovat luvun 2 potensseja.

Lause 2. *$\mathbf{H}_n$ on 2^n-asteinen Hadamardin matriisi.*

Todistus. Todistetaan induktiolla indeksin n suhteen. Induktion alkuaskeleeksi voidaan valita edellä määritetty $\mathbf{H}_0$ tai $\mathbf{H}_1$. Oletetaan, että väite on voimassa indeksillä $n-1$. Tällöin $\mathbf{H}_n$ on varmasti neliömatriisi, jonka alkiot kuuluvat joukkoon $\{-1, 1\}$. Lisäksi sen asteluvun on oltava 2^n. Olkoot R_i ja R_j kaksi riviä ja $i > j$. Olkoon $\mathbf{x}_i$ rivin R_i ensimmäinen puolikas ja $\mathbf{y}_i$ jälkimmäinen puolikas. Määritellään samoin $\mathbf{x}_j$ ja $\mathbf{y}_j$ rivin R_j tapauksessa. Jos $i \neq j + 2^{n-1}$, niin $\mathbf{x}_i \cdot \mathbf{x}_j = 0 = \mathbf{y}_i \cdot \mathbf{y}_j$, jolloin R_i ja R_j ovat ortogonaaliset. Jos taas $i = j + 2^{n-1}$, niin $\mathbf{x}_i = \mathbf{x}_j$ ja $\mathbf{y}_i = -\mathbf{y}_j$ ja

$$R_i \cdot R_j = \mathbf{x}_i \cdot \mathbf{x}_j + \mathbf{y}_i \cdot \mathbf{y}_j = \mathbf{x}_i \cdot \mathbf{x}_i - \mathbf{y}_i \cdot \mathbf{y}_i = 2^{n-1} - 2^{n-1} = 0.$$

Lemman 1 ja induktioperiaatteen nojalla väite saatiin todistettua. □

Näytetään esimerkki edellisen lauseen avulla muodostetusta 8-asteisesta H-matriisista.

Esimerkki 2. Olkoon $\mathbf{H}_2$ esimerkin 1 neljännen asteen H-matriisi. Tällöin

$$\mathbf{H}_3 = \begin{pmatrix} \mathbf{H}_2 & \mathbf{H}_2 \\ \mathbf{H}_2 & -\mathbf{H}_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

Huomataan, että koska $\mathbf{H}_2$ oli normalisoitu, $\mathbf{H}_3$ on myös.

Sylvesterin tapa konstruoida H-matriiseja on itse asiassa erikoistapaus yleisemmästä *Paleyn metodista*, jonka yhteydessä tarvitaan Kroneckerin tulon käsitettä. Määritellään se seuraavaksi. Luvun loppuosa perustuu lähteeseen [3], ellei toisin mainita.

Määritelmä 2. Olkoon $\mathbf{A} = (a_{ij})$ m-asteinen neliömatriisi ja $\mathbf{B} = (b_{rs})$ n-asteinen neliömatriisi. Tällöin niiden *Kroneckerin tulo* eli *suora tulo* on mn-asteinen neliömatriisi

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \dots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \dots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & a_{m2}\mathbf{B} & \dots & a_{mn}\mathbf{B} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \dots & a_{11}b_{1n} & \dots & a_{1m}b_{11} & a_{1m}b_{12} & \dots & a_{1m}b_{1n} \\ a_{11}b_{21} & a_{11}b_{22} & \dots & a_{11}b_{2n} & \dots & a_{1m}b_{21} & a_{1m}b_{22} & \dots & a_{1m}b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{11}b_{n1} & a_{11}b_{n2} & \dots & a_{11}b_{nn} & \dots & a_{1m}b_{n1} & a_{1m}b_{n2} & \dots & a_{1m}b_{nn} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \dots & a_{m1}b_{1n} & \dots & a_{mm}b_{11} & a_{mm}b_{12} & \dots & a_{mm}b_{1n} \\ a_{m1}b_{21} & a_{m1}b_{22} & \dots & a_{m1}b_{2n} & \dots & a_{mm}b_{21} & a_{mm}b_{22} & \dots & a_{mm}b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{n1} & a_{m1}b_{n2} & \dots & a_{m1}b_{nn} & \dots & a_{mm}b_{n1} & a_{mm}b_{n2} & \dots & a_{mm}b_{nn} \end{pmatrix}.$$

Matriisikertolaskua käyttäen saadaan

$$\mathbf{A} \otimes \mathbf{B} = (\mathbf{A} \otimes \mathbf{I}_n)(\mathbf{I}_m \otimes \mathbf{B}) = (\mathbf{I}_m \otimes \mathbf{B})(\mathbf{A} \otimes \mathbf{I}_n).$$

Kroneckerin tulo on assosiatiivinen eli $(\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C} = \mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C})$. Tulomatriisit $\mathbf{B} \otimes \mathbf{A}$ ja $\mathbf{A} \otimes \mathbf{B}$ ovat ekvivalentit, kun rivejä ja sarakkeita permutoidaan sopivasti. Oletetaan sitten, että $\mathbf{A}$, $\mathbf{A}_1$, $\mathbf{A}_2$ sekä $\mathbf{C}$ ovat m-asteisia neliömatriiseja ja $\mathbf{B}$, $\mathbf{B}_1$, $\mathbf{B}_2$ ja $\mathbf{D}$ n-asteisia neliömatriiseja. Silloin seuraavat ominaisuudet ovat voimassa:

$$s((\mathbf{A} \otimes \mathbf{B}) = (s\mathbf{A}) \otimes \mathbf{B} = \mathbf{A} \otimes (s\mathbf{B}), \text{ missä } s \text{ on skalaari}; \tag{4}$$

$$(\mathbf{A}_1 + \mathbf{A}_2) \otimes \mathbf{B} = \mathbf{A}_1 \otimes \mathbf{B} + \mathbf{A}_2 \otimes \mathbf{B}, \tag{5}$$

$$\mathbf{A} \otimes (\mathbf{B}_1 + \mathbf{B}_2) = \mathbf{A} \otimes \mathbf{B}_1 + \mathbf{A} \otimes \mathbf{B}_2, \tag{6}$$

$$(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = \mathbf{AC} \otimes \mathbf{BD}, \tag{7}$$

$$(\mathbf{A} \otimes \mathbf{B})^T = \mathbf{A}^T \otimes \mathbf{B}^T. \tag{8}$$

Sovelletaan Kroneckerin tulon määritelmää Hadamardin matriisien tapauksessa.

Lause 3. *Oletetaan, että on olemassa m- ja n-asteiset H-matriisit. Tällöin niiden Kroneckerin tulo on mn-asteinen H-matriisi.*

Todistus. Olkoon $\mathbf{H}$ m-asteinen ja $\mathbf{H}'$ n-asteinen H-matriisi. Laskusääntöjä (7) ja (8) käyttämällä saadaan

$$\begin{aligned}(\mathbf{H} \otimes \mathbf{H}')(\mathbf{H} \otimes \mathbf{H}')^T &= (\mathbf{H} \otimes \mathbf{H}')(\mathbf{H}^T \otimes \mathbf{H}'^T) \\ &= \mathbf{H}\mathbf{H}^T \otimes \mathbf{H}'\mathbf{H}'^T = m\mathbf{I}_m \otimes n\mathbf{I}_n = mn\mathbf{I}_{mn}.\end{aligned}$$

□

Esimerkiksi Sylvesterin H-matriiseja (3) voidaan nyt muodostaa myös tulona: $\mathbf{H}_n = \mathbf{H}_1 \otimes \mathbf{H}_{n-1}$. (ks. [1])

Kroneckerin tulon lisäksi jatkoa varten tarvitaan äärellisiä kuntia ja niihin kuuluvia neliöitä. Olkoon $\mathbb{F}_{p^r}$ äärellinen kunta, missä p on pariton alkuluku. Määritellään kuvaus χ seuraavasti:

$$\begin{aligned}&\chi(0) = 0, \\ &\chi(x) = 1, \text{ jos } x \text{ on neliö kunnassa } \mathbb{F}_{p^r}, \\ &\chi(x) = -1, \text{ jos } x \text{ ei ole neliö kunnassa } \mathbb{F}_{p^r}.\end{aligned}$$

Nyt jos $\theta \in \mathbb{F}_{p^r}$ on primitiivialkio, $\chi(\theta^i) = (-1)^i$. (ks. [1]) Lisäksi yleisesti $\chi(xy) = \chi(x)\chi(y)$ äärellisten kuntien ominaisuuksien nojalla.

Seuraavaksi tutkitaan kolmea aputulosta, joiden avulla Paleyn metodina tunnettu tulos voidaan todistaa.

Lemma 3. *Olkoon $q = p^r$. Nyt $\sum_{b=1}^{q-1} \chi(b)\chi(b+c) = -1$, jos $c \neq 0$.*

Todistus. Jos $b = 0$, niin $\chi(0)\chi(0+c) = 0$, joten olkoon $b \neq 0$. Tällöin on olemassa sellainen yksikäsitteinen $z \neq 1$, että $b + c = bz$. Nyt b käy läpi kunnan nollasta eroavat alkiot ja z ykkösestä eroavat alkiot. Huomataan, että kun $b = -c$, $z = 0$. Näin ollen

$$\begin{aligned}\sum_{b\neq 0} \chi(b)\chi(b+c) &= \sum_{b=1}^{q-1} \chi(b)\chi(b+c) = \sum_{b=1}^{q-1} \chi(b)^2\chi(z) = \sum_{z\neq 1} \chi(z) \\ &= \sum_{z\neq 1} \chi(z) - \chi(1) = 0 - 1 = -1.\end{aligned}$$

□

Ennen seuraavaa aputulosta otetaan käyttöön muutama merkintä. Olkoon q alkuluvun potenssi. Numeroidaan kunnan $\mathbb{F}_q$ alkiot $a_0, a_1, \ldots, a_{q-1}$ niin, että $a_0 = 0$ ja $a_{q-1} = -a_i$, missä $i = 1, \ldots, q-1$. Määritellään matriisi $\mathbf{Q} = (q_{ij})$, missä $q_{ij} = \chi(a_i - a_j)$. Tällöin $q_{ji} = \chi(a_j - a_i) = \chi(-1)\chi(a_i - a_j)$. Tarkastellaan tilannetta modulo 4. Nyt -1 on neliö, jos $q \equiv 1 \pmod 4$. Vastaavasti se ei ole neliö, jos $q \equiv 3 \pmod 4$. Tästä seuraa, että ensimmäisessä tapauksessa $\mathbf{Q}$ on symmetrinen ja jälkimmäisessä vinosti symmetrinen.

Olkoon tästä eteenpäin $\mathbf{J} = (a_{ij})$ neliömatriisi, missä $a_{ij} = 1$ kaikilla indekseillä i, j.

Lemma 4. *Olkoot matriisit* $\mathbf{Q} = (q_{ij})$ *ja* $\mathbf{J} = (a_{ij})$ *kuten edellä. Tällöin* $\mathbf{QQ}^T = q\mathbf{I}_q - \mathbf{J}$ *ja* $\mathbf{QJ} = \mathbf{JQ} = 0$. *Jos merkitään* $\mathbf{QQ}^T = \mathbf{B}(b_{ij})$, *niin*

$$\begin{aligned} b_{ij} &= \sum_t \chi(a_i - a_t)\chi(a_j + a_t) \\ &= \begin{cases} q-1, \textit{ jos } i = j \\ -1, \textit{ jos } i \neq j. \end{cases} \end{aligned}$$

Todistus. Viimeksi mainittu relaatio saadaan sijoittamalla lemman 3 yhtälöön $b = a_i - a_t$ ja $c = a_j - a_i$, mikä todistaa väitteen $\mathbf{QQ}^T = q\mathbf{I}_q - \mathbf{J}$. Väite $\mathbf{QJ} = \mathbf{JQ} = 0$ seuraa siitä, että $\sum_z \chi(z) = 0$. □

Otetaan jälleen käyttöön lisää merkintöjä. Olkoon $e = e_q = (1, \ldots, 1)$ vektori, jossa on q kappaletta ykkösiä. Jos nyt $q = p^r \equiv -1 \pmod 4$, matriisilla

$$\mathbf{S} = \begin{pmatrix} 0 & e \\ -e^T & \mathbf{Q} \end{pmatrix}$$

on ominaisuudet $\mathbf{S}^T = -\mathbf{S}$ ja $\mathbf{SS}^T = q\mathbf{I}_{q+1}$. Tämän matriisin avulla voidaan muodostaa $q+1$-asteinen H-matriisi

$$\mathbf{H}_{q+1} = \mathbf{I}_{q+1} + \mathbf{S},$$

sillä jokainen alkio on kuuluu joukkoon $\{-1, 1\}$ ja

$$\begin{aligned} \mathbf{H}_{q+1}\mathbf{H}_{q+1}^T &= (\mathbf{I}_{q+1} + \mathbf{S})(\mathbf{I}_{q+1} + \mathbf{S}^T) = \mathbf{I}_{q+1} + \mathbf{S} + \mathbf{S}^T + \mathbf{SS}^T \\ &= \mathbf{I}_{q+1} + q\mathbf{I}_{q+1} = (q+1)\mathbf{I}_{q+1}. \end{aligned}$$

H-matriisia kutsutaan *vinoksi*, jos se on muotoa $\mathbf{H}_m = \mathbf{I}_m + \mathbf{S}_m$, $\mathbf{S}_m^T = -\mathbf{S}_m$. Esitellään vielä J. Williamsonin todistama aputulos.

Lemma 5. *Olkoon* $\mathbf{S}$ *sellainen* n*-asteinen neliömatriisi, että* $\mathbf{S}^T = \epsilon\mathbf{S}$, $\epsilon = \pm 1$ *ja* $\mathbf{SS}^T = (n-1)\mathbf{I}_{n-1}$. *Oletetaan, että* $\mathbf{A}$ *ja* $\mathbf{B}$ *ovat* m*-asteisia neliömatriiseja, jotka toteuttavat ehdot*

$$\mathbf{AA}^T = \mathbf{BB}^T = m\mathbf{I}_m \textit{ ja } \mathbf{AB}^T = -\epsilon\mathbf{BA}^T.$$

Tällöin matriisi $\mathbf{K} = \mathbf{A} \otimes \mathbf{I}_n + \mathbf{B} \otimes \mathbf{S}$ *toteuttaa ehdon* $\mathbf{KK}^T = mn\mathbf{I}_{mn}$.

Todistus. Suoraan laskemalla saadaan

$$\begin{aligned} \mathbf{KK}^T &= (\mathbf{A} \otimes \mathbf{I}_n + \mathbf{B} \otimes \mathbf{S})(\mathbf{A}^T \otimes \mathbf{I}_n + \mathbf{B}^T \otimes \mathbf{S}^T) \\ &= \mathbf{AA}^T \otimes \mathbf{I}_n + \mathbf{AB}^T \otimes \mathbf{S}^T + \mathbf{BA}^T \otimes \mathbf{S} + \mathbf{BB}^T \otimes \mathbf{SS}^T \\ &= m\mathbf{I}_m \otimes \mathbf{I}_n + (-\epsilon\mathbf{BA}^T) \otimes (\epsilon\mathbf{S}) + \mathbf{BA}^T \otimes \mathbf{S} + m\mathbf{I}_m \otimes (n-1)\mathbf{I}_n \\ &= m\mathbf{I}_{mn} + m(n-1)\mathbf{I}_{mn} = mn\mathbf{I}_{mn}. \end{aligned}$$

□

Jos $q = p^r \equiv 1 \pmod 4$, niin indeksillä $n = q + 1$ saadaan matriisi

$$\mathbf{S}_n = \begin{pmatrix} 0 & e \\ e^T & \mathbf{Q} \end{pmatrix}, \text{ missä } e = e_{n-1} \text{ ja } \mathbf{Q} \text{ symmetrinen.} \tag{9}$$

Lemman 4 nojalla näin määriteltyllä matriisilla on ominaisuudet

$$\mathbf{S}_n^T = -\mathbf{S}_n \text{ ja } \mathbf{S}_n\mathbf{S}_n^T = (n-1)\mathbf{I}_n. \tag{10}$$

Olkoon $\mathbf{A}$ mikä tahansa H-matriisi, jonka asteluku $m > 1$ on parillinen. Nyt voidaan konstruoida matriisi $\mathbf{U}_m$, jonka päädiagonaalin alapuolella on $m/2$ kappaletta alimatriiseja $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Merkitään Kroneckerin tulona

$$\mathbf{U}_m = \mathbf{I}_{m/2} \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Olkoon $\mathbf{B} = \mathbf{U}_m\mathbf{A}$. Saadaan yhtälöt

$$\begin{aligned} \mathbf{B}\mathbf{B}^T &= \mathbf{U}_m\mathbf{A}\mathbf{A}^T\mathbf{U}_m^T = \mathbf{U}_m m\mathbf{I}_m\mathbf{U}_m^T = m\mathbf{I}_m, \\ \mathbf{A}\mathbf{B}^T &= \mathbf{A}\mathbf{A}^T\mathbf{U}_m^T = m\mathbf{I}_m\mathbf{U}_m^T = -m\mathbf{U}_m \text{ ja} \\ \mathbf{B}\mathbf{A}^T &= \mathbf{U}_m\mathbf{A}\mathbf{A}^T = \mathbf{U}_m m\mathbf{I}_m = m\mathbf{U}_m. \end{aligned}$$

Nyt matriisit $\mathbf{A}$ ja $\mathbf{B}$ sopivat lemman 5 kaavoihin. Jos $\mathbf{S}_n$ vastaa määrittelyä (9), päädiagonaalin alkiot ovat nollia ja muut alkiot ± 1. Näin ollen lemman 5 matriisin $\mathbf{K}$ kaikki alkiot ovat ± 1, joten sen on oltava mn-asteinen H-matriisi. On siis todistettu seuraava lause:

Lause 4. *Olkoon p alkuluku ja $h > 1$ Hadamardin matriisin asteluku. Jos $p^r \equiv 1 \pmod 4$, niin on olemassa H-matriisi, jonka asteluku on $h(p^r + 1)$.*

Paleyn metodissa, joka on oikeastaan tämän Williamsonin tuloksen erikoistapaus, tarvitaan määrittelyn (9) mukaista matriisia $\mathbf{S}_n$. Sen avulla konstruoidaan H-matriisi

$$\mathbf{H}_{2n} = \mathbf{S}_n \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} + \mathbf{I}_n \otimes \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}. \tag{11}$$

Yhtälöistä (10) seuraa, että $\mathbf{H}_{2n}$ on symmetrinen H-matriisi. Paleyn tuloksen mukaan on siis olemassa H-matriisi, jonka asteluku on $2(p^r + 1)$, kun $p^r \equiv 1 \pmod 4$. Konstruoidaan nyt tällä metodilla 12-asteinen H-matriisi.

Esimerkki 3. Valitaan alkuluku $q = 5$. Merkitään kunnan $\mathbb{F}_5$ alkioita seuraavasti: $a_0 = 0$, $-a_1 = a_4 = 4$, $-a_2 = a_3 = 3$, $-a_3 = a_2 = 2$ ja $-a_4 = a_1 = 1$. Kootaan matriisi $\mathbf{Q} = (q_{ij})$, missä siis $q_{ij} = \chi(a_i - a_j)$. Tulkitaan, että ensimmäisen rivin ja sarakkeen järjestysluku on 0 ja viimeisten 4. Tällöin kaikki diagonaalialkiot ovat

nollia. Jos tietyssä sijainnissa rivin ja sarakkeen järjestyslukujen erotus on ± 1 tai ± 4, kyseinen alkio on positiivinen ykkönen. Loput alkiot ovat negatiivisia ykkösiä. Saadaan

$$\mathbf{Q} = \begin{pmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{pmatrix}, \mathbf{S}_6 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

ja lopulta kaavan (11) mukaan (ks. [1])

$$\mathbf{H}_{12} = \begin{pmatrix} 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}.$$

2.3 Williamsonin metodi

Lauseen 4 ja sitä aiempien tulosten pohjalta on ollut mahdollista konstruoida $4n$-asteisia H-matriiseja, kun $4n \leq 100$. Asteluku 92 on poikkeus. Kyseisen tapauksen konstruointiin tarvitaan muita menetelmiä, esimerkiksi *Williamsonin metodia*, joka on nimetty John Williamsonin $(1901 - 1949)$ mukaan. Tässä metodissa pyritään käyttämään hyödyksi *Lagrangen lausetta*, jonka mukaan jokainen luonnollinen luku voidaan esittää neljän neliön summana. Siis jos $m \in \mathbb{N}_0$, on olemassa sellaiset $a, b, c, d \in \mathbb{N}_0$, että $m = a^2 + b^2 + c^2 + d^2$. Esimerkiksi $77 = 8^2 + 3^2 + 2^2 + 0^2$ ja $90 = 9^2 + 3^2 + 0^2 + 0^2$.

Olkoon matriisi

$$\mathbf{H} = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}. \tag{12}$$

Jos A, B, C ja D ovat skalaareja, niin

$$\mathbf{H}\mathbf{H}^T = (A^2 + B^2 + C^2 + D^2)\mathbf{I}_4.$$

Williamsonin ajatus oli, että A, B, C ja D olisivatkin n-asteisia neliömatriiseja. Oletetaan, että ne ovat symmetrisiä ja kommutoivat keskenään. Tällöin

$$\mathbf{H}\mathbf{H}^T = (A^2 + B^2 + C^2 + D^2) \otimes \mathbf{I}_4.$$

Seuraavaksi tarvitaan permutaatio- ja kiertomatriiseja. Olkoon

$$\mathbf{U} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

n-asteinen permutaatiomatriisi, jolla on ominaisuus $\mathbf{U}^n = \mathbf{I}_n$, ja olkoon

$$\mathbf{C} = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix}$$

n-asteinen kiertomatriisi. Nyt jos A, B, C ja D ovat polynomeja matriisissa $\mathbf{U}$, ne varmasti kommutoivat. Hyödynnetään matriisin $\mathbf{C}$ alkioita ja merkitään

$$\begin{aligned} A &= a_0\mathbf{I}_n + a_1\mathbf{U} + \ldots + a_{n-1}\mathbf{U}^{n-1}, \\ B &= b_0\mathbf{I}_n + b_1\mathbf{U} + \ldots + b_{n-1}\mathbf{U}^{n-1}, \\ C &= c_0\mathbf{I}_n + c_1\mathbf{U} + \ldots + c_{n-1}\mathbf{U}^{n-1}, \\ D &= d_0\mathbf{I}_n + d_1\mathbf{U} + \ldots + d_{n-1}\mathbf{U}^{n-1}. \end{aligned} \tag{13}$$

Koska $\mathbf{U}\mathbf{U}^T = \mathbf{I}_n$ eli $\mathbf{U}^T = \mathbf{U}^{-1}$, matriisit A, B, C ja D ovat symmetrisiä, jos

$$a_{n-i} = a_i,\ b_{n-i} = b_i,\ c_{n-i} = c_i,\ d_{n-i} = d_i \tag{14}$$

kaikilla indekseillä $i = 1, \ldots, n-1$. Jos jokainen kerroin a, b, c, d on ± 1, matriisin $\mathbf{H}$ jokainen alkio on ± 1, jolloin saadaan

$$\mathbf{H}\mathbf{H}^T = 4n\mathbf{I}_{4n} \text{ ja } A^2 + B^2 + C^2 + D^2 = 4n\mathbf{I}_n.$$

Williamsonin metodin idea siis on, että lähtötilanteen (12) matriisi $\mathbf{H}$ on $4n$-asteinen H-matriisi, jos A, B, C ja D ovat tiettyjä polynomeja (13) ja kertoimet täyttävät ehdot (14). Näytetään seuraavaksi esimerkki tapauksesta $n = 3$.

Esimerkki 4. Olkoon

$$A = \mathbf{J}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \text{ ja } B = C = D = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

Tällöin A, B, C ja D ovat symmetrisiä ja kommutoivat. Todetaan, että asteluvusta johtuen $A^2 = 3A$ ja $B^2 = C^2 = D^2 = 4\mathbf{I}_3 - A$, joten $A^2 + B^2 + C^2 + D^2 = 3A + 3(4\mathbf{I}_3 - A) = 12\mathbf{I}_3$. Yhtälöstä (12) saadaan 12-asteinen H-matriisi

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{pmatrix}. \quad [1]$$

Esitellään vielä, miten H-matriisin konstruoinnissa päästään alkuun tapauksessa $n = 23$. Baumert *et al.* löysi tämän ratkaisun vuonna 1962. Samalla tavalla voidaan konstruoida astelukujen 116 ja 172 H-matriisit.

Esimerkki 5. (ks. [1]) Muodostetaan 92-asteinen H-matriisi. Koska $n = 23$, voidaan valita, että A, B, C ja D ovat 23-asteisia kiertomatriiseja, joiden ensimmäiset rivit ovat

$A : 1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1$
$B : 1, -1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, -1$
$C : 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1$
$D : 1, 1, 1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1.$

3 Lohkosommitelmat

3.1 Määritelmä ja olemassaolo

Lähestytään tämän luvun aihetta Hallin [3] mukaisesti. Oletetaan, että on olemassa äärellinen perusjoukko. Tarkoituksena on jakaa joukon alkiot pienempiin joukkoihin eli lohkoihin, joita on oltava tietty määrä. Kuhunkin lohkoon ryhmitellään tietty määrä alkioita. Lisäksi on tietty määrä sellaisia lohkoja, joissa jokainen alkiopari, -kolmikko tai vastaava alkioiden yhdistelmä esiintyy. Tällaisesta ryhmittelystä voidaan käyttää yleisnimitystä *esiintyvyysjärjestelmä* (engl. *incidence system*). Määritellään luvun aluksi tasapainoinen vajaa lohkosommitelma, joka on eräänlainen esiintyvyysjärjestelmä.

Määritelmä 3. Olkoon perusjoukon S alkioiden lukumäärä v. *Tasapainoinen vajaa lohkosommitelma* (engl. *balanced incomplete block design*) on sellainen kokoelma, että alkiot jaetaan lohkoihin, joita on b kappaletta, seuraavasti: jokaisessa lohkossa on täsmälleen k eri alkiota, jokainen alkio esiintyy täsmälleen r:ssä lohkossa ja jokainen erillisten alkioiden a_i, a_j muodostama pari esiintyy täsmälleen λ:ssa lohkossa.

Tässä määritelmässä tasapainoisuus tarkoittaa viimeisen ehdon toteutumista ja vajaus sitä, että $k < v$ eli yksikään lohko ei ole perusjoukko itse. Merkittävää on, että kaikki lohkot ovat samankokoisia, mutta eri lohkot voivat sisältää samoja alkioita. Sommitelmaa ei siis tule pitää pelkkänä osajoukkojen kokoelmana vaan edellä kuvatulla tavalla määriteltynä järjestelmänä, jossa alkiot ja lohkot ovat tietyssä relaatiossa toisiinsa nähden. Käytännössä sommitelmia voidaan hyödyntää vaikkapa testattaessa jonkin tuotteen eri laatuja. Jos nimittäin näiden vertailtavien laatujen lukumäärä on suuri, on järkevää muodostaa lohkoja eri testaajia varten.

Koska sommitelmalla on viisi edellä mainittua parametria, se on viisikko (v, k, λ, b, r). Usein sommitelma kuitenkin ajatellaan kolmikkona (v, k, λ), koska näiden kolmen parametrin perusteella b ja r määräytyvät yksikäsitteisesti. Seuraavassa lauseessa esitellään parametrien välinen yhteys.

Lause 5. *Yhtälöt*

$$bk = vr, \tag{15}$$

$$r(k-1) = \lambda(v-1) \tag{16}$$

ovat voimassa kaikissa (v, k, λ)-sommitelmissa.

Todistus. Yhtälössä (15) lasketaan esiintyvyyksien kokonaismäärä kahdella tavalla: Lohkoja on b kappaletta ja niissä on k alkiota. Toisaalta perusjoukossa on alkioita v kappaletta ja lohkoja, joissa jokainen yksittäinen alkio esiintyy, on r kappaletta.

Yhtälössä (16) puolestaan lasketaan sellaiset parittaiset esiintyvyydet, joissa on mukana tietty alkio a_1. Tiedetään, että a_1 esiintyy r:ssä lohkossa, joista jokaiseen kuuluu jäljelle jäävien $(k-1)$ lohkon alkion kanssa muodostetut parit. Toisaalta a_1 voi muodostaa parin λ kertaa jäljelle jäävien $(v-1)$ perusjoukon alkion kanssa. □

Lauseen 5 yhtälöt antavat sommitelman konstruointiin välttämättömät ehdot, jotka eivät kuitenkaan ole riittäviä. Käänteisesti voidaan tällöin päätellä, että jos

yhtälöihin sijoitetaan sellaiset kokonaislukuparametrit v, k ja λ, että b ja r eivät ole kokonaislukuja, kyseisten parametrien pohjalta ei voi muodostaa sommitelmaa. Näytetään esimerkki tilanteesta.

Esimerkki 6. Ei ole olemassa $(13, 8, 3)$-sommitelmaa, koska yhtälön (16) mukaan $r = \frac{3\cdot(13-1)}{(8-1)} = \frac{36}{7}$. Myöskään $(13, 7, 3)$-sommitelmaa ei ole olemassa. Nyt $r = \frac{3\cdot(13-1)}{(7-1)} = 6$, mutta yhtälön (15) mukaan $b = \frac{13\cdot 6}{7} = \frac{78}{7}$.

3.2 $(7, 3, 1)$-sommitelma, sommitelman matriisi ja symmetrisyys

Tutkitaan erästä yksinkertaista sommitelmaa ja tapoja kuvata sitä. Olkoon perusjoukko $S = \{a, b, c, d, e, f, g\}$, jolloin $v = 7$. Tarkoitus on, että jokaiseen lohkoon tulisi kolme alkiota ja jokainen alkiopari ilmaantuisi tarkalleen yhteen lohkoon. Siis $k = 3$ ja $\lambda = 1$. Lauseen 5 mukaan $b = 7$ ja $r = 3$, mikä tarkoittaa, että lohkoja on seitsemän ja jokainen alkio esiintyy täsmälleen kolmessa lohkossa. Merkitään lohkoja $B_1, \ldots, B_7$ ja kootaan sommitelma:

$$\begin{aligned} &B_1 = \{a, b, d\};\ B_2 = \{b, c, e\};\ B_3 = \{c, d, f\};\ B_4 = \{d, e, g\};\ B_5 = \{e, f, a\}; \\ &B_6 = \{f, g, b\};\ B_7 = \{g, a, c\}. \end{aligned} \tag{17}$$

Sommitelman rakenne voidaan siis esittää luettelemalla lohkot ja alkiot, mutta myös sommitelman matriisi havainnollistaa tilannetta erinomaisesti.

Määritelmä 4. Olkoon matriisi $\mathbf{A} = (a_{ij})$, missä $i = 1, \ldots, v$ ja $j = 1, \ldots, b$. Tulkitaan rivit sommitelman lohkoiksi $B_1, \ldots, B_b$ ja sarakkeet perusjoukon alkioiksi $a_1, \ldots, a_v$. Matriisi $\mathbf{A}$ on *sommitelman matriisi*, jos

$$a_{ij} = \begin{cases} 1, \text{ kun } a_i \in B_j \\ 0 \text{ muulloin.} \end{cases}$$

Näin saadaan $(7, 3, 1)$-sommitelman matriisiksi

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

Tehdään muutama havainto matriisista $\mathbf{A}$. Ensinnäkin nähdään, että on mahdollista luoda $(7, 3, 1)$-sommitelma siirtämällä ensimmäisen rivin ykkösiä syklisesti aina

yhden sarakkeen verran oikealle. Sommitelman matriisi ei ole yksikäsitteinen, koska rivien ja sarakkeiden järjestystä voidaan muuttaa. Oleelliset ominaisuudet kuitenkin säilyvät permutoinnista huolimatta. On esimerkiksi mahdollista muuttaa $\mathbf{A}$ symmetriseksi:

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

Huomautus 2. Sommitelman matriisin symmetrisyys ei ole sama asia kuin sommitelman symmetrisyys, joka seuraa siitä, että sommitelman matriisi on neliömatriisi. Tällöin $v = b$ tai yhtäpitävästi $k = r$. Sommitelman symmetrisyys tarkoittaa seuraavia asioita:

1. Jokaisessa lohkossa on k alkiota.
2. Jokainen alkio esiintyy k:ssa lohkossa.
3. Jokainen alkiopari esiintyy λ:ssa lohkossa.
4. Jokaisen lohkoparin leikkauksessa on λ alkiota. Todistetaan tämä myöhemmin.

Tarkastellaan seuraavaksi, millainen tulos saadaan, kun sommitelman matriisi ja sen transpoosi kerrotaan keskenään. Vastaavaa tuloa käytetään Hadamardin matriisin määritelmässä.

Lause 6. *Olkoon* $\mathbf{A}$ (v, k, λ)*-sommitelman matriisi. Tällöin*

$$\mathbf{A}^T\mathbf{A} = \mathbf{B} = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix} = (r - \lambda)\mathbf{I}_v + \lambda\mathbf{J}_v. \tag{18}$$

Lisäksi jos $\mathbf{w}_v$ *ja* $\mathbf{w}_b$ *ovat vektoreita, joissa on* v *ja* b *kappaletta ykkösiä, niin* $\mathbf{w}_v\mathbf{A} = k\mathbf{w}_b$.

Todistus. Matriisin $\mathbf{B}$ alkio b_{ij} on matriisin $\mathbf{A}$ i:nnen rivin ja j:nnen sarakkeen sisätulo. Tällöin matriisin $\mathbf{B}$ diagonaalille muodostuu matriisin $\mathbf{B}$ i:nnen rivin ykkösten lukumäärä, jonka on oltava r. Merkitään siis $b_{ii} = r$. Kun $i \neq j$, sekä i:nnellä että j:nnellä rivillä on ykkönen t:nnessä sarakkeessa, jos ja vain jos sekä a_i että a_j kuuluvat lohkoon B_t. Diagonaalin ulkopuolinen alkio b_{ij} kuvaa siis, kuinka monta kertaa alkiopari (a_i, a_j) esiintyy. Sommitelman määritelmän mukaan saadaan $b_{ij} = \lambda$. Yhtälö $\mathbf{w}_v\mathbf{A} = k\mathbf{w}_b$ seuraa siitä, että jokaisessa sarakkeessa on k ykköstä. □

Voidaan siis todeta kääntäen, että jos binäärimatriisi $\mathbf{A}$ toteuttaa ehdon (18), se on (v, k, λ, b, r)-sommitelman matriisi. Todistetaan seuraavaksi *Fisherin epäyhtälönä* tunnettu tulos.

Lause 7. *Kaikissa (v, k, λ)-sommitelmissa $b \geq v$ ja $r \geq k$.*

Todistus. Lasketaan ensin tulon (18) determinantti. Olkoon $\mathbf{A}$ sommitelman matriisi. Vähennetään matriisin $\mathbf{A}^T\mathbf{A}$ ensimmäinen sarake kaikista muista sarakkeista ja lisätään ensimmäiseen riviin kaikki muut rivit. Tällöin päädiagonaalin yläpuoliset alkiot ovat nollia. Ensimmäinen diagonaalialkio on $r + (v-1)\lambda$ ja loput ovat $r - \lambda$. Determinantin laskusääntöjen mukaan alakolmiomatriisin determinantti on diagonaalialkioiden tulo eli

$$|\mathbf{A}^T\mathbf{A}| = (r + (v-1)\lambda)(r-\lambda)^{v-1} = rk(r-\lambda)^{v-1} \neq 0.$$

Jos $r = \lambda$, sommitelma on triviaali, koska silloin alkio a_i esiintyy λ kertaa sekä muodostaa parin kaikkien muiden alkioiden a_j kanssa ja jokainen lohko koostuu kaikista perusjoukon alkoista. Kun sommitelma oletetaan epätriviaaliksi, $r > \lambda$ ja matriisi $\mathbf{A}^T\mathbf{A}$ ei ole singulaarinen. Koska tulomatriisin $\mathbf{A}^T\mathbf{A}$ asteluku v ei voi olla suurempi kuin kummankaan tekijän asteluku b, saadaan haluttu tulos $v \leq b$. □

Todistetaan vielä, että symmetrisen sommitelman matriisi ja sen transpoosi kommutoivat. Tuloksesta seuraa myös huomatuksen 2 viimeinen kohta.

Lause 8. *Jos $\mathbf{A}$ on symmetrisen sommitelman matriisi, niin $\mathbf{A}\mathbf{A}^T = (k-\lambda)\mathbf{I} + \lambda\mathbf{J} = \mathbf{A}^T\mathbf{A}$. Näin ollen jokaisen lohkoparin leikkauksessa on λ alkiota.*

Todistus. Sovelletaan tietoa, että kaikki matriisit kommutoivat käänteismatriisinsa kanssa. Todetaan, että $\mathbf{A}\mathbf{J} = \mathbf{J}\mathbf{A} = k\mathbf{J}$ ja $\mathbf{A}^T\mathbf{J} = \mathbf{J}\mathbf{A}^T = k\mathbf{J}$. Samoin $\mathbf{J}\mathbf{A}^T = k\mathbf{J}$ ja triviaalisti $\mathbf{J}^2 = v\mathbf{J}$. Koska kyseessä on symmetrinen sommitelma, $r = k$, jolloin yhtälön (18) nojalla

$$\begin{aligned}\left(\mathbf{A}^T - \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right)\left(\mathbf{A} + \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right) &= \mathbf{A}^T\mathbf{A} + \sqrt{\left(\frac{\lambda}{v}\right)}(\mathbf{A}^T\mathbf{J} - \mathbf{J}\mathbf{A}) - \frac{\lambda}{v}\mathbf{J}^2 \\ &= \mathbf{A}^T\mathbf{A} - \lambda\mathbf{J} = (k-\lambda)\mathbf{I}.\end{aligned}$$

Matriisit $\frac{1}{k-\lambda}\left(\mathbf{A} + \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right)$ ja $\left(\mathbf{A}^T - \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right)$ ovat siis toistensa käänteismatriisit, joten erityisesti ne kommutoivat. Saadaan

$$\begin{aligned}(k-\lambda)\mathbf{I} &= \left(\mathbf{A} + \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right)\left(\mathbf{A}^T - \sqrt{\left(\frac{\lambda}{v}\right)}\mathbf{J}\right) \\ &= \mathbf{A}\mathbf{A}^T + \sqrt{\left(\frac{\lambda}{v}\right)}(\mathbf{J}\mathbf{A}^T - \mathbf{A}\mathbf{J}) - \frac{\lambda}{v}\mathbf{J}^2 = \mathbf{A}\mathbf{A}^T - \lambda\mathbf{J}\end{aligned}$$

ja lopulta $\mathbf{A}\mathbf{A}^T = (k-\lambda)\mathbf{I} + \lambda\mathbf{J} = \mathbf{A}^T\mathbf{A}$.

Koska $\mathbf{A}$ on symmetrisen (v, k, λ)-sommitelman matriisi, sekä jokaisella rivillä että jokaisessa sarakkeessa on k ykköstä. Samoin sekä parittaisilla riveillä että parittaisissa sarakkeissa on λ yhteistä ykköstä. Tämä luku on siis lohkoparin leikkauksessa olevien alkioiden määrä. Huomataan vielä, että myös $\mathbf{A}^T$ on jonkin (v, k, λ)-sommitelman matriisi. (ks. [2]) □

Konstruoidaan alaluvun lopuksi sommitelma, jota voi soveltaa musiikissa.

Esimerkki 7. Olkoon perusjoukko $S = \{a, b, c, d, e, f, g\}$. Tulkitaan alkiot a-molliasteikon säveliksi. Halutaan muodostaa sommitelma, jonka eräinä lohkoina ovat tavalliset duuri- ja mollikolmisoinnut. Nyt siis $v = 7$ ja $k = 3$. Tässä tilanteessa $(7, 3, 1)$-sommitelma ei ole sopiva, koska jokainen sävelpari esiintyy kahdessa soinnussa. Merkitään siis $\lambda = 2$, jolloin $r = 6$ ja $b = 14$. Muodostetaan ensin $(7, 3, 2)$-sommitelman "sointulohkot"

$Am = \{a, c, e\}$; $C = \{c, e, g\}$; $Dm = \{d, f, a\}$; $Em = \{e, g, b\}$; $F = \{f, a, c\}$ ja $G = \{g, b, d\}$.

Muut lohkot ovat

$\{a, b, c\}$; $\{b, c, d\}$; $\{c, d, e\}$; $\{d, e, f\}$; $\{e, f, g\}$; $\{b, d, f\}$; $\{a, f, g\}$ ja $\{a, b, g\}$.

3.3 Hadamardin sommitelma

Jatketaan sommitelmien tarkastelua Andersonin [1] mukaisesti. Tavoitteena on löytää yhteys Hadamardin matriisien ja lohkosommitelmien välillä. Aluksi määritellään Hadamardin sommitelma.

Määritelmä 5. Olkoon $n \geq 2$. Tällöin $(4n-1, 2n-1, n-1)$-sommitelmaa kutsutaan n-asteiseksi *Hadamardin sommitelmaksi.*

Huomataan, että jos valitaan $n = 2$, saadaan edellä konstruoitu $(7, 3, 1)$ -sommitelma, joten kyseessä on H-sommitelma.

Lauseen 1 mukaan H-matriisin asteluku on aina 1, 2 tai luvun 4 monikerta. Otaksutaan, että olisi voimassa ekvivalenssi eli jokaisella asteluvulla $m = 4k$ olisi olemassa H-matriisi. Lisäksi otaksutaan, että olisi olemassa H-sommitelma jokaisella asteluvulla $n \geq 2$. Todistetaan seuraavaksi lause, josta näiden otaksumien yhtäpitävyys seuraa.

Lause 9. *Hadamardin $(4n-1, 2n-1, n-1)$-sommitelma on olemassa silloin ja vain silloin kun on olemassa $4n$-asteinen Hadamardin matriisi.*

Todistus. Oletetaan ensin, että $4n$-asteinen H-matriisi on olemassa. Olkoon $\mathbf{H}$ normalisoitu $4n$-asteinen H-matriisi. Poistetaan siitä ensimmäinen rivi ja sarake sekä vaihdetaan jokainen -1 nollaksi. Olkoon näin saatu binäärimatriisi $\mathbf{A}$. Tulkitaan se jonkin sommitelman matriisiksi. Lemman 2 mukaan jokaisella matriisin $\mathbf{A}$ rivillä on ykkösiä $2n-1$ kappaletta, joten sommitelman kunkin lohkon koon on oltava $2n-1$.

Lemmaa 2 voidaan soveltaa myös tarkasteltavan H-matriisin transpoosiin: matriisin $\mathbf{H}^T$ parittaisilla riveillä on n:ssä sarakkeessa positiivinen ykkönen. Näin ollen matriisin $\mathbf{A}$ parittaisissa sarakkeissa on positiivinen ykkönen samalla rivillä $n-1$ kertaa. On siis $n-1$ sellaista lohkoa, joissa mitkä tahansa kaksi alkiota esiintyvät yhdessä. Siis $\mathbf{A}$ on $(4n-1, 2n-1, n-1)$-sommitelman matriisi.

Oletetaan sitten, että on olemassa $(4n-1, 2n-1, n-1)$-sommitelma. Olkoon $\mathbf{A}$ sen matriisi. Vaihdetaan jokaisen nollan paikalle -1 sekä lisätään uusi rivi ja sarake, joiden kaikki alkiot ovat positiivisia ykkösiä. Saadaan $4n$-asteinen neliömatriisi $\mathbf{H}$, jonka alkiot kuuluvat joukkoon $\{-1, 1\}$. Tarkastellaan kahden erillisen sarakkeen sisätuloa. Näissä sarakkeissa on $+1$ samalla rivillä $1 + (n-1) = n$ kertaa, koska kyseisessä sommitelmassa $\lambda = n-1$. Todetaan myös, että jokaisessa sarakkeessa on $r + 1 = 2n$ positiivista ykköstä, joten matriisissa $\mathbf{H}$ on $2(2n-n) = 2n$ solua, joissa kahden sarakkeen alkiot eroavat toisistaan. Nyt kahden sarakkeen sisätulo on $2n(+1) + 2n(-1) = 0$, joten sarakkeet ovat parittain ortogonaaliset. Lemman 1 mukaan $\mathbf{H}$ on Hadamardin matriisi. □

Seuraavassa esimerkissä valitaan $n = 2$ ja konstruoidaan H-matriisi sommitelman matriisin avulla.

Esimerkki 8. Jos

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

on $(7, 3, 1)$-sommitelman matriisi, 8-asteiseksi H-matriisiksi saadaan

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}.$$

Palataan nyt tarkastelemaan edellisessä luvussa esiteltyä Williamsonin metodia. H-matriisien konstruointiin voidaan nimittäin käyttää myös sellaisia symmetrisiä sommitelmia, jotka *eivät ole* Hadamardin sommitelmia. Oletetaan, että $\mathbf{A}$ on symmetrisen sommitelman matriisi, ja vaihdetaan -1 jokaisen nollan tilalle. Tutkitaan, milloin näin saatu matriisi on H-matriisi. Seuraava aputulos perustuu havaintoon siitä, että kun nollien tilalle vaihdetaan -1, tullaan muodostaneeksi matriisi $\mathbf{H} = 2\mathbf{A} - \mathbf{J}$.

Lemma 6. *Olkoon* $\mathbf{A}$ *symmetrisen* (v, k, λ)*-sommitelman matriisi. Tällöin* $\mathbf{H} = 2\mathbf{A} - \mathbf{J}$ *on* H*-matriisi, jos ja vain jos* $v = 4(k - \lambda)$*.*

Todistus. Todistetaan laskemalla

$$\begin{aligned}\mathbf{H}\mathbf{H}^T &= (2\mathbf{A} - \mathbf{J})(2\mathbf{A}^T - \mathbf{J}) = 4\mathbf{A}\mathbf{A}^T - 2\mathbf{A}\mathbf{J} - 2\mathbf{J}\mathbf{A}^T + \mathbf{J}^2 \\ &= 4((k-\lambda)\mathbf{I} + \lambda\mathbf{J}) - 2k\mathbf{J} - 2k\mathbf{J} + v\mathbf{J} = 4(k-\lambda)\mathbf{I} + (v - 4(k-\lambda))\mathbf{J} = v\mathbf{I},\end{aligned}$$

joka toteutuu, jos ja vain jos $v = 4(k - \lambda)$. □

Yksinkertaisen esimerkin avulla löydetään nyt ainoa tunnettu Hadamardin kiertomatriisi.

Esimerkki 9. Olkoon $S = \{1, 2, 3, 4\}$ perusjoukko, jolloin $v = 4$ ja $k - \lambda = 1$. Kootaan $(4, 3, 2)$-sommitelma lohkoista $\{2, 3, 4\}$, $\{1, 3, 4\}$, $\{1, 2, 4\}$ ja $\{1, 2, 3\}$. Sommitelman matriisi on siis

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \text{ ja } H\text{-kiertomatriisi } \mathbf{H} = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Ennen toista esimerkkiä selvitetään, milloin ehdon $v = 4(k - \lambda)$ on mahdollista toteutua. Seuraavan lauseen pohjalta löydetään sopivat parametrien arvot.

Lause 10. *Olkoon* v *parillinen luonnollinen luku. Jos on olemassa symmetrinen* (v, k, λ)*-sommitelma, erotuksen* $k - \lambda$ *on oltava neliöluku eli* $\sqrt{k - \lambda} \in \mathbb{N}$*.*

Todistus. Olkoon $\mathbf{A}$ sommitelman matriisi. Koska sommitelma on symmetrinen, niin $k = r$. Fisherin epäyhtälön todistuksen perusteella $|\mathbf{A}|^2 = k^2(k-\lambda)^{v-1}$, jolloin $|\mathbf{A}| = k(k-\lambda)^{(v-1)/2}$. Koska $|\mathbf{A}|$ ja k ovat kokonaislukuja, $(k-\lambda)^{(v-1)/2}$ on rationaaliluku. Tämä on mahdollista sillä ehdolla, että $k-\lambda$ on neliöluku, sillä eksponentin osoittaja $v - 1$ on pariton. □

Merkitään nyt, että $v = 4(k - \lambda) = 4m^2$. Sijoittamalla $k = 2m^2 \pm m$ ja $\lambda = m^2 \pm m$ yhtälö toteutuu. Seuraavassa Spencen esimerkissä vuodelta 1971 käytetään Williamsonin metodia tapauksessa $m = 3$.

Esimerkki 10. Olkoot parametrit $v = 4 \cdot 3^2 = 36$, $k = 2 \cdot 3^2 - 3 = 15$ ja $\lambda = 3^2 - 3 = 6$. Tavoitteena on siis löytää $(36, 15, 6)$-sommitelman matriisi. Kiertomatriisin asteluvun on oltava $v/4$, joten olkoot A, B, C ja D 9-asteisia kiertomatriiseja, joiden ensimmäiset rivit ovat

$$\begin{aligned} A &: 1, -1, -1, -1, 1, 1, -1, -1, -1 \\ B &: 1, -1, -1, 1, -1, -1, 1, -1, -1 \\ C &: 1, -1, 1, -1, -1, -1, -1, 1, -1 \\ D &: 1, 1, -1, -1, -1, -1, -1, -1, 1. \end{aligned}$$

Muutetaan yhtälön (12) matriisi muotoon

$$\mathbf{H}' = \begin{pmatrix} -A & B & C & D \\ B & A & D & -C \\ C & -D & A & B \\ D & C & -B & A \end{pmatrix},$$

joka on yhtä lailla Williamsonin metodin kannalta sopiva. Nyt matriisissa $\mathbf{H}'$ on 15 positiivista ykköstä joka rivillä ja sarakkeessa, jolloin $\mathbf{H}'\mathbf{J} = -6\mathbf{J} = \mathbf{J}\mathbf{H}'$. Olkoon $\mathbf{K} = \frac{(\mathbf{H}'+\mathbf{J})}{2}$. Tällöin $\mathbf{K}$ on sellainen binäärimatriisi, että

$$\mathbf{K}\mathbf{K}^T = \frac{(\mathbf{H}' + \mathbf{J})(\mathbf{H}'^T + \mathbf{J})}{4} = \frac{1}{4}(36\mathbf{I} - 6\mathbf{J} - 6\mathbf{J} + 36\mathbf{I}) = 9\mathbf{I} + 6\mathbf{J} \text{ ja}$$
$$\mathbf{J}\mathbf{K} = \frac{1}{2}(-6\mathbf{J} + 36\mathbf{J} = 15\mathbf{J} = \mathbf{K}\mathbf{J}.$$

Täten $\mathbf{K}$ on $(36, 15, 6)$-sommitelman matriisi.

Huomautus 3. Kaikista $4m$-asteisista H-matriiseista ei voi johtaa symmetristä sommitelmaa. Oleellista on, että H-matriisi on *täsmällinen* (engl. *regular*). Se tarkoittaa, että rivien alkioiden summa on vakio. Jos siis $\mathbf{H}\mathbf{J} = \mathbf{J}\mathbf{H} = t\mathbf{J}$ jollakin kokonaisluvulla t, edellä kuvattu metodi toimii.

4 Äärelliset projektiiviset tasot

Luvun päälähde on Andersonin teos [1]. Aloitetaan määrittelemällä lyhyesti äärellinen projektiivinen taso ja tutkitaan sen jälkeen taustaa sekä yhteyttä lohkosommitelmiin.

Määritelmä 6. *Äärellinen projektiivinen taso*, jonka asteluku on $n \geq 2$, on $(n^2 + n + 1, n + 1, 1)$-sommitelma.

Thomas Penyngton Kirkman $(1806 - 1895)$ todisti vuonna 1850, että kun kiinnitetään $\lambda = 1$, millä tahansa alkuluvulla p on olemassa sommitelma, jossa $v = p^2 + p + 1$ ja $k = p + 1$. Vuonna 1906 O. Veblen ja W. H. Bussey puolestaan osoittivat, että on olemassa $(q^2 + q + 1, q + 1, 1)$-sommitelma kaikilla alkulukujen potensseilla q. Tässä luvussa tarkoitus on konstruoida äärellisten kuntien avulla joitakin projektiivisia tasoja ja näin myös sommitelmia.

Tarkastellaan joukkoa S, joka koostuu kolmikoista $\mathbf{x} = (x_0, x_1, x_2)$. Jokainen x_i kuuluu äärelliseen kuntaan $\mathbb{F}_q$ ja ainakin jokin niistä eroaa nollasta. Näin ollen joukossa S on $q^3 - 1$ alkiota, mutta ajatuksena on samaistaa kolmikot $\mathbf{x}$ ja $\mathbf{y}$, jos toinen niistä on toisen skalaarimonikerta. Määritellään siis sellainen ekvivalenssirelaatio, että $\mathbf{x}$ ja $\mathbf{y}$ ovat *ekvivalentit*, jos $\mathbf{x} = \lambda\mathbf{y}$, kun $\lambda \in \mathbb{F}_q^*$. Skalaarilla λ on siis $q - 1$ mahdollista arvoa, joten eri ekvivalenssiluokkien määrä on $\frac{q^3-1}{q-1} = q^2 + q + 1$. Olkoon kolmikon $\mathbf{x}$ ekvivalenssiluokka $[\mathbf{x}]$. Tällöin voidaan merkitä $[\mathbf{x}] = [\mathbf{y}]$, jos $\mathbf{x}$ ja $\mathbf{y}$ ovat ekvivalentit kolmikot. Lisäksi jos $\mathbf{y} \in [\mathbf{x}]$, kolmikko $\mathbf{y}$ on luokan $[\mathbf{x}]$ *vektoriedustaja* (engl. *representing vector*).

Edetään niin, että tulkitaan ekvivalenssiluokat $[\mathbf{x}]$, joita siis on $q^2 + q + 1$ kappaletta, äärellisen projektiivisen tason alkioiksi eli *pisteiksi*. Määritellään sitten lohkot eli *suorat* seuraavasti: Olkoon $\mathbf{a} = (a_0, a_1, a_2)$, missä $a_i \in \mathbb{F}_q$ ja $\mathbf{a} \neq 0$. Tällöin suora $[\mathbf{a}]$ kaikkien sellaisten pisteiden $[\mathbf{x}]$ joukko, että $a_0x_0 + a_1x_1 + a_2x_2 = 0$. Huomataan, että $[\mathbf{a}] = [\lambda\mathbf{a}]$ kaikilla $\lambda \neq 0$ eikä suoran $[\mathbf{a}]$ määrittely riipu siitä, mitkä vektoriedustajat luokasta $[\mathbf{x}]$ valitaan.

Edellä perusteltiin, miksi projektiivisella tasolla on tarkalleen $q^2 + q + 1$ pistettä. Samalla perusteella suoria on yhtä monta. Selvitetään, kuinka monta pistettä on suoralla. Tarkastellaan suoraa $[\mathbf{a}]$, missä $\mathbf{a} = (a_0, a_1, a_2)$. Voidaan olettaa, että $a_1 \neq 0$. Jos piste $[\mathbf{x}]$ on suoralla $[\mathbf{a}]$, komponentit x_0 ja x_2 määräävät yksikäsitteisesti komponentin x_1. Koska komponenteista x_0 ja x_2 ainakin toinen eroaa nollasta, mahdollisia arvoja on $q^2 - 1$ kappaletta. On siis $q^2 - 1$ nollasta eroavaa vektoria $\mathbf{x}$, jotka toteuttavat yhtälön $a_0x_0 + a_1x_1 + a_2x_2 = 0$. Näin ollen suoralla $[\mathbf{a}]$ on $\frac{q^2-1}{q-1} = q + 1$ erillistä pistettä $[\mathbf{x}]$. Tutkitaan vielä erillisiä pisteitä $[\mathbf{x}]$ ja $[\mathbf{y}]$. Ne ovat suoralla $[\mathbf{a}]$, jos ja vain jos $\sum_i a_ix_i = 0 = \sum_i a_iy_i$. Tässä $\mathbf{a}$ on mikä tahansa suoran vektoriedustaja. Koska vektorit $\mathbf{x}$ ja $\mathbf{y}$ ovat lineaarisesti riippumattomat kunnassa $\mathbb{F}_q$, yhtälön ratkaisut $\mathbf{a}$ muodostavat yksiulotteisen aliavaruuden. Vektori $\mathbf{a}$ määräytyy näin yksikäsitteisesti skalaarikertolaskun mielessä, jolloin myös suora $[\mathbf{a}]$ on yksikäsitteinen. Johtopäätöksenä mitkä tahansa kaksi pistettä määräävät suoran. Määritellään nyt projektiivinen taso hieman eri merkinnöin.

Määritelmä 7. Merkitään, että $PG(m, q)$ on q-asteinen äärellinen projektiivinen taso. Luku $m + 1$ on perusjoukon alkioiden komponenttien lukumäärä.

Tämän luvun konstruktiossa tarkastellaan siis tapausta $m = 2$, eli perusjoukon alkiot ovat kolmikoita. Esitellään seuraavaksi 2-asteinen projektiivinen taso.

Esimerkki 11. Konstruoidaan projektiivinen taso $PG(2, 2)$. Tähän tarvitaan kuntaa $\mathbb{F}_2 = \{0, 1\}$, jonka ainoa nollasta eroava alkio on selvästi $\lambda = 1$ ja jossa on voimassa laskusääntö $1 + 1 = 0$. Tällöin jokainen nollasta eroava kolmikko $\mathbf{x} = (x_0, x_1, x_2)$ muodostaa yksin oman ekvivalenssiluokan. Pisteitä on $2^3 - 1 = 2^2 + 2 + 1 = 7$ kappaletta: $(0, 0, 1)$; $(0, 1, 0)$; $(1, 0, 0)$; $(0, 1, 1)$; $(1, 0, 1)$; $(1, 1, 0)$; $(1, 1, 1)$. Suorat on mahdollista kuvata samalla tavalla: Jos suoran yhtälö on esimerkiksi $x_2 = 0$, niin väistämättä $a_0 = a_1 = 0$ ja $a_2 = 1$, jolloin voidaan kuvata suoraa merkinnällä $B[0, 0, 1]$. Saadaan seitsemän suoraa, joista kuhunkin kuuluu $2+1 = 3$ pistettä:

$$\begin{aligned}
x_0 = 0 &\leftrightarrow (0, 0, 1);\ (0, 1, 0);\ (0, 1, 1)\\
x_1 = 0 &\leftrightarrow (0, 0, 1);\ (1, 0, 0);\ (1, 0, 1)\\
x_2 = 0 &\leftrightarrow (1, 0, 0);\ (0, 1, 0);\ (1, 1, 0)\\
x_0 + x_1 = 0 &\leftrightarrow (0, 0, 1);\ (1, 1, 0);\ (1, 1, 1)\\
x_0 + x_2 = 0 &\leftrightarrow (0, 1, 0);\ (1, 0, 1);\ (1, 1, 1)\\
x_1 + x_2 = 0 &\leftrightarrow (1, 0, 0);\ (0, 1, 1);\ (1, 1, 1)\\
x_0 + x_1 + x_2 = 0 &\leftrightarrow (1, 0, 1);\ (0, 1, 1);\ (1, 1, 0).
\end{aligned}$$

Vaihdetaan nyt merkintöjä:

$$\begin{aligned}
&(0, 1, 0) \leftrightarrow a;\ (1, 0, 0) \leftrightarrow b;\ (0, 1, 1) \leftrightarrow c;\ (1, 1, 0) \leftrightarrow d;\\
&(1, 1, 1) \leftrightarrow e;\ (1, 0, 1) \leftrightarrow f \text{ ja } (0, 0, 1) \leftrightarrow g.
\end{aligned}$$

Nähdään, että muodostetun tason suorat ovat täsmälleen sommitelman (17) lohkot $B_1, \ldots, B_7$ ja tason pisteet ovat perusjoukon sekä lohkojen alkiot. Projektiivinen taso, jonka asteluku on 2, on siis $(7, 3, 1)$-sommitelma eli 2-asteinen H-sommitelma aivan kuten määritelmässä 6 todettiin.

Toisena esimerkkinä esitellään 4-asteinen projektiivinen taso.

Esimerkki 12. Muodostetaan projektiivinen taso $PG(2, 4)$, joka on siis $(21, 5, 1)$-sommitelma, käyttämällä kuntaa $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, missä $\alpha^2 = \alpha + 1$. Tällöin $\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 1$ ja $\alpha^4 = (\alpha + 1)^2 = \alpha^2 + 1 = \alpha$. Nyt esimerkiksi pisteet $(0, 1, \alpha^2)$ ja $(0, \alpha, 1)$ ovat ekvivalentit, koska $(0, \alpha, 1) = \alpha(0, 1, \alpha^2)$. Vastaavasti esimerkiksi $(\alpha^2, 1, \alpha) = \alpha^2(1, \alpha, \alpha^2)$. Tasoon kuuluu 21 erillistä pistettä:

$$\begin{aligned}
&(0, 0, 1);\ (0, 1, 0);\ (0, 1, 1);\ (0, 1, \alpha);\ (0, 1, \alpha^2);\ (1, 0, 0);\ (1, 0, 1);\\
&(1, 0, \alpha);\ (1, 0, \alpha^2);\ (1, 1, 0);\ (1, 1, 1);\ (1, 1, \alpha);\ (1, 1, \alpha^2);\ (1, \alpha, 0);\\
&(1, \alpha, 1);\ (1, \alpha, \alpha);\ (1, \alpha, \alpha^2);\ (1, \alpha^2, 0);\ (1, \alpha^2, 1);\ (1, \alpha^2, \alpha);\ (1, \alpha^2, \alpha^2).
\end{aligned}$$

Suoria on myös 21 kappaletta. Niistä jokaiseen kuuluu $4+1 = 5$ pistettä. Luetellaan

tässä esimerkissä 7 suoraa pisteineen:

$B[0,1,0]$: $(0,0,1)$; $(1,0,0)$; $(1,0,1)$; $(1,0,\alpha)$; $(1,0,\alpha^2)$
$B[1,1,0]$: $(0,0,1)$; $(1,1,0)$; $(1,1,1)$; $(1,1,\alpha)$; $(1,1,\alpha^2)$
$B[0,1,\alpha^2]$: $(0,1,\alpha)$; $(1,1,\alpha)$; $(1,\alpha^2,1)$; $(1,\alpha,\alpha^2)$; $(1,0,0)$
$B[1,0,\alpha]$: $(0,1,0)$; $(1,1,\alpha^2)$; $(1,0,\alpha^2)$; $(1,\alpha,\alpha^2)$; $(1,\alpha^2,\alpha^2)$
$B[1,1,1]$: $(0,1,1)$; $(1,0,1)$; $(1,1,0)$; $(1,\alpha,\alpha^2)$; $(1,\alpha^2,\alpha)$
$B[1,\alpha,1]$: $(0,1,\alpha)$; $(1,0,1)$; $(1,1,\alpha^2)$; $(1,\alpha^2,0)$; $(1,\alpha,\alpha)$
$B[1,\alpha^2,\alpha^2]$: $(0,1,1)$; $(1,0,\alpha)$; $(1,\alpha,0)$; $(1,1,\alpha^2)$; $(1,\alpha^2,1)$.

5 Steinerin systeemit

5.1 Yhteys sommitelmiin ja konstruointi

Tarkennetaan tasapainoisen vajaan lohkosommitelman määrittelyä niin, että määritelmän 3 mukaiset sommitelmat ovat 2-sommitelmia, koska niissä tutkitaan *parittaisia* erillisiä alkioita. Yhtä hyvin voidaan tutkia osajoukkoja, joissa on t alkiota. Määritellään luvun aluksi t-sommitelma ja Steinerin systeemi lähteen [2] tapaan.

Määritelmä 8. Olkoon $S = \{1, \ldots, v\}$ perusjoukko. Sen erillisten k-alkioisten osajoukkojen kokoelma $\mathcal{D}$ on $t-(v,k,\lambda)$-sommitelma, jos $0 < t \leq k < v$, $\lambda > 0$ ja jokainen perusjoukon t-alkioinen osajoukko kokoelman $\mathcal{D}$ joukoissa täsmälleen λ kertaa. *Steinerin systeemi* $S(t,k,v)$ tarkoittaa $t-(v,k,1)$-sommitelmaa.

Käytetään jatkossa lähteenä teosta [1], ellei toisin mainita. Määritellään erikseen vielä kolmikkosysteemi, jota tutkitaan tässä ja seuraavassa alaluvussa tarkemmin.

Määritelmä 9. *Steinerin kolmikkosysteemi* $S(2,3,v)$, merkitään myös $STS(v)$, on $(v,3,1)$-sommitelma.

Historiallisesta näkökulmasta Steinerin kolmikkosysteemeitä tulisi kutsua *Kirkmanin kolmikkosysteemeiksi.* Thomas Kirkman nimittäin todisti kolmikkosysteemien olemassaoloehdon vuonna 1847 eli kuusi vuotta ennen kuin Jakob Steiner $(1796-1863)$ esitti ongelman geometrisessä yhteydessä. Nykyisin yleensä määritellään, että jos kolmikkosysteemi on hajoava, sitä kutsutaan Kirkmanin kolmikkosysteemiksi. Hajoavaan sommitelmaan palataan luvun lopussa.

Selvitetään nyt, mitä arvoja parametrilla v voi olla.

Lemma 7. *Jos kolmikkosysteemi $STS(v)$ on olemassa, niin $v \equiv 1$ tai 3 (mod 6).*

Todistus. Oletetaan siis, että on olemassa $(v,k,1)$-sommitelma. Tällöin lauseen 5 yhtälöiden mukaan siinä on $b = \frac{1}{6}v(v-1)$ lohkoa. Lisäksi $r = \frac{1}{2}(v-1)$. Jotta nämä parametrit olisivat luonnollisia lukuja, v on väistämättä pariton. Merkitään $v = 2r+1$, jolloin $b = \frac{1}{3}r(2r+1)$ ja $r \equiv 0$ tai $1 \pmod 3$. Merkitään edelleen $r = 3n$ tai $r = 3n+1$. Nyt $v = 6n+1$ tai $v = 6n+3$ kuten väitettiin. □

Seuraavaksi tavoitteena on muodostaa yleinen Steinerin kolmikkosysteemi käyttämällä *Skolemin metodia.* Konstruktiossa on kaksi osaa johtuen parametrin v mahdollisista arvoista.

Tapaus $\mathbf{v = 6m+3}$:
Etsitään sopivia kolmikoita, joita on $b = \frac{1}{6}v(v-1) = (2m+1)(3m+1)$ kappaletta. Taulukoidaan luvut $0, 1, \ldots, 6m+2$ kolmelle riville, jolloin jokaiselle riville tulee $2m+1$ lukua:

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & \ldots & 2m-1 & 2m \\ 2m+1 & 2m+2 & 2m+3 & 2m+4 & \ldots & 4m & 4m+1 \\ 4m+2 & 4m+3 & 4m+4 & 4m+5 & \ldots & 6m & 6m+2. \end{array}$$

Valitaan taulukon sarakkeet ensimmäisiksi kolmikoiksi ja merkitään

$$A_i = \{i, i+2m, i+4m+2\}, \text{ missä } 0 \leq i \leq 2m.$$

Tarkastellaan sitten millä tahansa rivillä olevaa lukuparia $\{a, b\}$. Olkoon c sellainen seuraavan rivin luku, että $2c \equiv a+b \pmod{2m+1}$ tai vastaavasti $c \equiv (m+1)(a+b) \pmod{2m+1}$. Seuraava rivi tarkoittaa alempaa riviä ja viimeisen rivin tapauksessä ylintä riviä. Huomataan, että c ei voi olla samassa sarakkeessa kuin a ja b. Jos nimittäin c ja a olisivat samassa sarakkeessa eli $c \equiv a \pmod{2m+1}$, niin $2a = a+b$ eli $a \equiv b \pmod{2m+1}$, jolloin a ja b olisivat samassa sarakkeessa ja itse asiassa sama alkio. Koska joka rivillä on $\binom{2m+1}{2} = m(2m+1)$ lukuparia, voidaan valita $3m(2m+1)$ kolmikkoa $\{a, b, c\}$. Osoitetaan, että nämä sekä kolmikot A_i muodostavat kolmikkosysteemin $STS(6m+3)$.

Nähdään, että tulevassa kokoelmassa kolmikoita on yhteensä $2m+1+3m(2m+1) = (2m+1)(3m+1)$ kappaletta, mikä oli tarkoituskin. Pitää vielä näyttää, että luvuista $0, 1, \ldots, 6m+2$ koostuva pari esiintyy täsmälleen yhdessä kolmikossa. Selvästi mitkä tahansa kaksi samassa sarakkeessa olevaa lukua kuuluvat yhteen ja vain yhteen kolmikkoon A_i. Vastaavasti kaksi samalla rivillä olevaa lukua kuuluvat tarkalleen yhteen kolmikkoon. Tutkitaan kahta lukua a ja c, joista jälkimmäinen on seuraavalla rivillä ja eri sarakkeessa kuin edellinen eli $a \neq c \pmod{2m+1}$. Nämä luvut esiintyvät samassa kolmikossa, jos ja vain jos luvun a kanssa samalla rivillä on sellainen luku b, että $a+b \equiv 2c \pmod{2m+1}$ eli $b \equiv 2c-a \pmod{2m+1}$. Lopulta todetaan, että samalla rivillä kuin a on vain yksi tämän kongruenssin toteuttava b.

Tapaus $\mathbf{v = 6m+1}$:
Pyritään jälleen löytämään sopivia kolmikoita, joita on nyt $b = \frac{1}{6}v(v-1) = m(6m+1)$ kappaletta. Asetetaan rinnakkain kaksi taulukkoa:

$$\begin{array}{cccccccc} 0 & 1 & \ldots & m-1 & m & m+1 & \ldots & 2m-1 \\ 2m & 2m+1 & \ldots & 3m-1 & \text{ja } 3m & 3m+1 & \ldots & 4m-1 \\ 4m & 4m+1 & \ldots & 5m-1 & 5m & 5m+1 & \ldots & 6m-1. \end{array}$$

Huomataan, että taulukosta puuttuu luku $6m$, joka olisi $(6m+1)$:s alkio. Valitaan taulukon m ensimmäistä saraketta systeemin $STS(6m+1)$ tyypin 1 kolmikoiksi ja merkitään

$$B_i = \{i, 2m+i, 4m+i\}, \text{ missä } 0 \leq i \leq m-1.$$

Tämän jälkeen valitaan tyypin 2 kolmikot

$$C_i = \{m+i, 2m+i, 6m\};\ D_i = \{3m+i, 4m+i, 6m\};\ E_i = \{5m+i, i, 6m\}$$

kaikilla $0 \leq i \leq m-1$. Lopuksi valitaan tyypin 3 kolmikot $\{a, b, c\}$, joissa a ja b ovat samalla rivillä ja c seuraavalla. Jos $a+b$ on parillinen eli $2c \equiv a+b \pmod{2m}$, niin c on vasemmanpuoleisessa taulukossa. Jos taas $a+b$ on pariton eli $2c \equiv a+b-1 \pmod{2m}$, niin c on oikeanpuoleisessa taulukossa. On siis löydetty tarvittavat $4m + 3\binom{2m}{2} = m(6m+1)$. Viimeistellään systeemin konstruointi osoittamalla, että mikä tahansa lukupari esiintyy täsmälleen yhdessä kolmikossa.

Tyypin 2 kolmikoiden määrittelystä nähdään suoraan, että taulukosta puuttuva luku $6m$ esiintyy jokaisen luvun parina tarkalleen kerran. Koska tyypin 1 ja 2 kolmikoissa luvut ovat taulukossa eri riveillä, on välttämätöntä, että samalla rivillä olevat luvut esiintyvät parina täsmälleen yhdessä tyypin 3 kolmikossa. Jos kaksi lukua esiintyy jossakin vasemmanpuoleisen taulukon sarakkeessa, ne esiintyvät täsmälleen yhdessä tyypin 1 kolmikossa. Perustellaan, miksi ne eivät voi esiintyä tyypin

3 kolmikossa: Jos $a \equiv c \pmod{2m}$ ja sekä a että c ovat vasemmanpuoleisessa taulukossa, niin $2c \equiv a + b \pmod{2m}$, mikä on ristiriita sen kanssa, että a ja b ovat samalla rivillä. Siten kaksi vasemman puoliskon sarakkeen lukua kuuluvat yksikäsitteiseen kolmikkoon. Tarkastellaan sitten kahta lukua, jotka ovat jossain oikeanpuoleisen taulukon sarakkeessa. Olkoon luku c luvusta a seuraavalla rivillä eli $a \equiv c \pmod{2m}$. Nämä luvut esiintyvät tietyssä tyypin 3 kolmikossa $\{a, b, c\}$, jossa b saadaan kongruenssista $2a \equiv a + b - 1 \pmod{2m}$ eli $b \equiv a + 1 \pmod{2m}$. Tällöin ne eivät voi esiintyä yhdessä missään muun tyypin kolmikossa.

Viimeisenä tutkitaan kahta lukua a ja c, jotka ovat taulukon eri riveillä ja sarakkeissa. Oletetaan taas, että luku c on luvusta a seuraavalla rivillä. Jos c on oikeanpuoleisessa taulukossa, olkoon b samalla rivillä kuin a ja $b \equiv 2c - a + 1 \pmod{2m}$. Tällainen luku b on yksikäsitteinen, joten muodostuu yksikäsitteinen kolmikko $\{a, b, c\}$. Jos taas c on vasemmanpuoleisessa taulukossa ja $c \equiv a \pmod{m}$, niin a ja c kuuluvat yksikäsitteiseen tyypin 2 kolmikkoon. Perustellaan, miksi ne eivät voi kuulua myös tyypin 3 kolmikkoon: Jos ne esiintyisivät tyypin 3 kolmikossa, niin $2c \equiv a + b \pmod{2m}$, missä $2c \equiv 2a \pmod{2m}$. Tällöin $a \equiv b \pmod{2m}$. Koska a ja b ovat samalla rivillä, ne olisivat nyt sama luku. Siis vasemman puoliskon sarakkeen c ja a kuuluvat yhteen tyypin 2 kolmikkoon. Päätellään lopuksi, että jos c on vasemmanpuoleisessa taulukossa ja $c \not\equiv a \pmod{m}$, niin a ja c kuuluvat yksikäsitteiseen tyypin 3 lohkoon $\{a, b, c\}$, missä b saadaan kongruenssista $2c \equiv a + b \pmod{2m}$. Näin saadaan haluttu kolmikko, kunhan $b \not\equiv a \pmod{2m}$, muuten palataan tilanteeseen $a \equiv c \pmod{m}$.

Skolemin metodin avulla on nyt todistettu, että jos $v = 6m+3$ tai $v = 6m+1$, on varmasti olemassa kolmikkosysteemi $STS(v)$. Tästä ja lemmasta 7 saadaan yhteensä seuraava tulos.

Lause 11. *Steinerin kolmikkosysteemi $STS(v)$ on olemassa silloin ja vain silloin kun $v \equiv 1$ tai 3 (mod 6).*

5.2 Steinerin systeemi $S(2, 3, 7)$

Konstruoidaan Skolemin metodilla kolmikkosysteemi $STS(7)$. Nyt $m = 1$ ja $v = 7 = 6 \cdot 1 + 1$, joten käytetään metodin jälkimmäistä osaa. Huomataan myös, että $i = 0$. Olkoon $X = \{0, \ldots, 6\}$ perusjoukko. Tehdään taulukko

$$\begin{array}{cc} 0 & 1 \\ 2 & 3 \\ 4 & 5. \end{array}$$

Etsitään $b = 1(6 \cdot 1 + 1) = 7$ kolmikkoa. Ainoa tyypin 1 kolmikko on $B_0 = \{0, 2, 4\}$. Tyypin 2 kolmikoita ovat $C_0 = \{1, 2, 6\}$, $D_0 = \{3, 4, 6\}$ ja $E_0 = \{0, 5, 6\}$. Tyypin 3 kolmikoita puolestaan ovat $\{0, 1, 3\}$, $\{2, 3, 5\}$ ja $\{1, 4, 5\}$. Näin saatiin $(7, 3, 1)$-sommitelma, joka tosin näyttää hieman erilaiselta kuin aiemmin koottu sommitelma (17). Näytetään, että kyseinen kokoelma säilyy $(7, 3, 1)$-sommitelmana, vaikka joitakin lohkoja muutettaisiin sopivasti. Käytetään kuvausta, jossa $0 \mapsto 1, 1 \mapsto 7$ ja muut joukon X alkiot kuvautuvat itselleen. Lohkoiksi saadaan

$$\{1, 2, 4\};\ \{1, 5, 6\};\ \{1, 3, 7\};\ \{2, 6, 7\};\ \{4, 5, 7\};\ \{3, 4, 6\} \text{ ja } \{2, 3, 5\}.$$

Jos vielä vaihdetaan merkintöjä

$$1 \leftrightarrow a, 2 \leftrightarrow b, 3 \leftrightarrow c, 4 \leftrightarrow d, 5 \leftrightarrow e, 6 \leftrightarrow f \text{ ja } 7 \leftrightarrow g,$$

niin tulos on juurikin sommitelma (17). Voidaan päätellä, että nyt muodostettu systeemi $S(2,3,7)$ on sen kanssa *isomorfinen* eli oleellisesti samankaltainen, vaikka kaikki lohkot eivät alkuun olleetkaan identtisiä.

5.3 Hadamardin sommitelman laajentaminen

Alaluvun tavoitteena on laajentaa Hadamardin sommitelma 3-sommitelmaksi, jota konstruoitaessa tutkitaan siis alkioparien esiintyvyyksien sijaan alkiokolmikoita. Määritellään ensiksi sommitelman komplementti.

Määritelmä 10. Olkoon $\mathcal{D}$ (v,k,λ,b,r)-sommitelma. Merkitään, että jokaisen lohkon B komplementti on $C = S\backslash B$. Tällöin sommitelman $\mathcal{D}$ komplementti $\mathcal{D}^C$ tarkoittaa sommitelmaa, joka koostuu lohkoista C.

Näytetään yksinkertainen esimerkki toistuvasti esillä olleen sommitelman pohjalta.

Esimerkki 13. Tarkastellaan edellisen alaluvun Steinerin systeemiä $STS(7)$, joka on $(7,3,1)$-sommitelma. Taulukosta saatujen kolmikoiden komplementit ovat nelikoita:

$$\{1,3,5,6\};\ \{0,3,4,5\};\ \{0,1,2,5\};\ \{1,2,3,4\};\ \{2,4,5,6\};\ \{0,1,4,6\} \text{ ja } \{0,2,3,6\}.$$

Osoitetaan sitten, että sommitelman komplementti on sommitelma.

Lause 12. *Olkoon $\mathcal{D}$ (v,k,λ,b,r)-sommitelma. Tällöin komplementti $\mathcal{D}^C$ on $(v, v-k, b-2r+\lambda, b, b-r)$-sommitelma ja $b-2r+\lambda > 0$.*

Todistus. Koska komplementin lohkoihin valitaan päinvastaiset perusjoukon alkiot kuin alkuperäisen sommitelman lohkoihin, komplementin lohkoissa on oltava $v-k$ alkiota. Selvästikään lohkojen lukumäärä b ei muutu. Sommitelmassa $\mathcal{D}$ on r kappaletta sellaisia lohkoja, joissa perusjoukon alkio x esiintyy, ja $b-r$ kappaletta sellaisia lohkoja, joissa se ei esiinny. Komplementissa on siis $b-r$ lohkoa, joissa x esiintyy. Selvitetään lopuksi, kuinka monessa komplementin lohkossa alkiot x ja y esiintyvät yhdessä. Sommitelmassa $\mathcal{D}$ on saman verran lohkoja, joista sekä x että y puuttuvat. Olkoon u niiden lohkojen lukumäärä, joissa on ainakin toinen alkioista x ja y. Seulaperiaatteen perusteella tiedetään, että u on myös lukumäärä, johon on laskettu alkion x ja alkion y esiintyvyyksien summa ja vähennetty siitä yhteisien esiintymisien määrä. Etsitty parametri on $b-u = b-(r+r-\lambda) = b-2r+\lambda$. □

Jatketaan kohti alaluvun alussa asetettua tavoitetta. Aiemmin pääteltiin, että 2-sommitelma on erikoistapaus t-sommitelmasta. Näytetään, että yleisesti parametria t voi pienentää.

Lause 13. *Jos $s < t$, niin kaikki t-sommitelmat ovat myös s-sommitelmia.*

Todistus. Oletetaan, että on olemassa λ_s kappaletta sellaisia lohkoja, jotka sisältävät tietyn s-osajoukon A. Olkoon D t-osajoukko, johon A sisältyy, ja olkoon B lohko, johon D sisältyy. Muodostetaan yhtälö, jonka kummallakin puolella lasketaan parien (D, B) lukumäärä:

$$\lambda\binom{v-s}{t-s} = \lambda_s\binom{k-s}{t-s}.$$

Luku λ_s ei näin ollen riipu siitä, miten A valitaan. Kyseinen t-sommitelma on siis myös $s-(v,k,\lambda_s)$-sommitelma. □

Tämän lauseen seurauksena saadaan hyödyllistä tietoa parametreista.

Seuraus 1. *Merkitään $\lambda = \lambda_t$, jolloin*

$$\lambda_{t-1} = \lambda_t\left(\frac{v-t+1}{k-t+1}\right).$$

Lohkojen määrä t-sommitelmassa on

$$b = \lambda_0 = \lambda\frac{\binom{v}{t}}{\binom{k}{t}}. \tag{19}$$

Jokainen perusjoukon alkio esiintyy

$$r = \lambda_1 = \lambda\frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}} \text{ lohkossa.}$$

Seuraavaksi tarvitaan johdetun ja laajennetun sommitelman käsitteitä, jotka määritellään seuraavan pohjustuksen ja aputuloksen jälkeen. Olkoon $\mathcal{D}$ jokin t-sommitelma. Tällöin on olemassa selkeä tapa esittää siihen sisältyvä $(t-1)$-sommitelma. Olkoon $\mathcal{B}$ sommitelman $\mathcal{D}$ lohkojen kokoelma ja P jokin piste. Merkitään nyt, että $\mathcal{B}_P$ on kaikkien joukkojen $B\backslash P$ kokoelma, missä B on pisteen P sisältävä lohko.

Lemma 8. *Kokoelmaan $\mathcal{B}_P$ kuuluvat joukot ovat $(t-1)-(v-1,k-1,\lambda)$-sommitelman $\mathcal{D}_P$ lohkot.*

Todistus. Mikä tahansa $(t-1)$-osajoukko A esiintyy joukossa $B\backslash\{P\}$ yhtä usein kuin $A\cup\{P\}$ esiintyy kokoelman $\mathcal{B}$ lohkossa. Tämä tapahtuu λ kertaa. □

Määritellään nyt edellä mainitut uudet käsitteet.

Määritelmä 11. Sommitelma $\mathcal{D}_P$, joka muodostetaan kuten lemmassa 8, on *johdettu sommitelma*. Määritellään käänteisesti, että jos t-sommitelma on isomorfinen johdetun sommitelman $\mathcal{D}_P$ kanssa jollakin $(t+1)$-sommitelmalla $\mathcal{D}$ ja jollakin P, niin kutsutaan sommitelmaa $\mathcal{D}$ *laajennukseksi*.

Tutkitaan, milloin t-sommitelma voidaan laajentaa $(t+1)$-sommitelmaksi.

Lemma 9. *Jos $t-(v,k,\lambda,b,r)$-sommitelma voidaan laajentaa, niin luku $k+1$ jakaa luvun $b(v+1)$.*

Todistus. Yhtälön (19) perusteella saadaan

$$b = \lambda \frac{v(v-1)\dots(v-t+1)}{k(k-1)\dots(k-t+1)},$$

ja laajennuksen lohkojen lukumäärä on

$$\lambda \frac{(v+1)v\dots(v-t+1)}{(k+1)k\dots(k-t+1)} = \frac{(v+1)b}{k+1}.$$

□

Ennen kuin voidaan tehdä päätelmä H-sommitelman laajentamisesta, tarvitaan vielä yksi aputulos.

Lemma 10. *Olkoot a, b ja c jonkin (v,k,λ)-sommitelman erillisiä alkioita. Olkoon lohkoja, joista a, b ja c puuttuvat, n_0 kappaletta. Olkoon lisäksi lohkoja, joihin a, b ja c kaikki sisältyvät, n_{abc} kappaletta. Tällöin*

$$n_0 + n_{abc} = b + 3\lambda - 3r. \tag{20}$$

Tulos ei riipu lukujen a, b ja c valinnasta.

Todistus. Olkoon lohkoja, joissa a esiintyy, n_a kappaletta. Olkoon vastaavasti lohkoja, joissa a ja b esiintyvät, n_{ab} kappaletta. Seulaperiaatteen nojalla

$$n_0 = b - (n_a + n_b + n_c) + (n_{ab} + n_{bc} + n_{ac}) - n_{abc} = b - 3r + 3\lambda - n_{abc}.$$

Huomataan, että symmetrisen sommitelman tapauksessa $n_0 + n_{abc} = v - 3k + 3\lambda$. □

Seurauksena saavutetaan alaluvun tavoite.

Seuraus 2. *Jokainen Hadamardin sommitelma voidaan laajentaa 3-sommitelmaksi.*

Todistus. Olkoon $\mathcal{H}$ Hadamardin $(4m-1, 2m-1, m-1)$-sommitelma. Muodostetaan kokoelma $\mathcal{A}$ kaikista sommitelman $\mathcal{H}$ komplementtilohkoista ja alkuperäisistä lohkoista, joihin lisätään uusi alkio ∞. Kokoelmassa $\mathcal{A}$ on nyt $8m-2$ joukkoa, joista jokaisen koko on $2m$. Osoitetaan, että joukkoja, joihin jokainen 3-osajoukko kuuluu, on täsmälleen $m-1$ kappaletta. Ensinnäkin joukko $\{\infty, a, b\}$ esiintyy lohkossa $B \cup \{\infty\}$ tarkalleen silloin kun $\{a,b\}$ esiintyy lohkossa B. Tämä toteutuu $m-1$ kertaa. Jos taas a, b ja c eroavat alkiosta ∞, on $n_0 + n_{abc}$ kappaletta lohkoja B tai $B \cup \{\infty\}$, jotka sisältävät alkiot a, b ja c. Yhtälön (20) mukaan kyseinen määrä on $4m - 1 - 3(2m-1) + 3(m-1) = m-1$. □

Mainitaan vielä, että $3-(4m, 2m, m-1)$-sommitelmaa kutsutaan *Hadamardin 3-sommitelmaksi*.

5.4 Hajoava sommitelma ja Steinerin nelikkosysteemi

Tutkielman viimeisenä asiana tarkastellaan hieman Steinerin nelikkosysteemeitä ja esitellään tapa konstruoida niitä. Tähän tarvitaan hajoavuuden käsitettä sekä muutamaa aputulosta.

Tutkitaan Steinerin systeemiä $S(2,3,9)$, joka koostuu seuraavista kolmikoista:

$$\{1,2,3\};\ \{1,5,8\};\ \{1,4,7\};\ \{1,6,9\}$$
$$\{4,8,9\};\ \{3,4,6\};\ \{2,6,8\};\ \{2,4,5\}$$
$$\{5,6,7\};\ \{2,7,9\};\ \{3,5,9\};\ \{3,7,8\}.$$

Kun katsotaan allekkain olevia kolmikoita, huomataan, että jokainen joukon $\{1,\ldots,9\}$ alkio esiintyy jossain niistä täsmälleen kerran. Kyseinen kolmikkosysteemi on siis mahdollista jakaa tällaisiin erityisiin luokkiin. Tämä on havainnollistava esimerkki hajoavasta sommitelmasta, joka määritellään seuraavaksi.

Määritelmä 12. Lohkosommitelma on *hajoava*, (engl. *resolvable*) jos lohkoista voidaan luoda r sellaista ryhmää, että jokaisen ryhmän $\frac{b}{r} = \frac{v}{k}$ lohkoa ovat erillisiä ja niiden unioni sisältää kunkin alkion täsmälleen kerran. Hajoavan sommitelman ryhmiä kutsutaan *rinnakkaisluokiksi* (engl. *parallel classes*).

Geometrisesti hajoavan sommitelman lohkoja voidaan pitää suorina ja rinnakkaisluokkia suorien kokoelmina, joista jokaiseen kuuluvat yhdensuuntaiset suorat peittävät koko perusjoukon. Toisin kuin projektiivisissa tasoissa, joissa kaikki parittaiset suorat kohtaavat toisensa, hajoava sommitelma näyttää Euklidisen geometrian mielessä nimenomaan yhdensuuntaisten suorien olemassaolon.

Hajoavia sommitelmia voidaan käyttää esimerkiksi otteluohjelmia luotaessa. Oletetaan, että lentopallojoukkueita on $2n$ kappaletta ja kaikki joukkueet pelaavat kerran toisiaan vastaan. Oletetaan lisäksi, että turnaus kestää $2n-1$ päivää ja jokaisena päivänä kukin joukkue pelaa yhden ottelun. Ratkaisu saadaan kokoamalla $(2n,2,1)$-sommitelma. Osoitetaan, että se on hajoava. Esitettävä todistus on lähteestä [2].

Lause 14. *Kun n on positiivinen kokonaisluku, $(2n,2,1)$-sommitelma on hajoava.*

Todistus. Olkoon $S = \{\infty, 1, 2, \ldots, 2n-1\}$ perusjoukko ja $\mathcal{D}$ joukon S kaikkien 2-alkioisten osajoukkojen joukko. Näytetään, miten $\mathcal{D}$ voidaan jakaa erillisiin rinnakkaisluokkiin $\mathcal{D}_1, \ldots, \mathcal{D}_{2n-1}$. Määritellään, että osajoukot $\{i,\infty\} \in \mathcal{D}_i$ ja $\{a,b\} \in \mathcal{D}_i$, jos

$$a + b \equiv 2i \pmod{2n-1},$$

missä $a, b \in S\backslash\{\infty\}$. Koska lukujen 2 ja $2n-1$ suurin yhteinen tekijä on 1, jokainen joukon S 2-osajoukko kuuluu tarkalleen yhteen rinnakkaisluokkaan $\mathcal{D}_i$. Tällöin luokan $\mathcal{D}_i$ lohko, johon a kuuluu, on $\{a,b\}$, missä $b \equiv 2i - a \pmod{2n-1}$, jos $a \neq i$ ja $a \neq \infty$, ja $\{i,\infty\}$, jos $a = i$ tai $a = \infty$. □

Jakob Steiner pyrki vuonna 1853 muodostamaan systeemeitä $S(t,k,v)$, missä $k = t+1$. Aiemmin tässä luvussa on tutkittu tapauksia $t = 2$, $k = 3$ eli kolmikkosysteemeitä, joiden löytämisessä itse asiassa Thomas Penyngton Kirkmanilla

oli merkittävä rooli. Tuolloin systeemien $S(3,4,v)$ konstruointi ei täysin onnistunut, mutta vuonna 1960 Haim Hanani $(1912-1991)$ pystyi konstruoimaan kaikki mahdolliset tapaukset. Kirkman kuitenkin näytti, että nelikkosysteemi on olemassa, kun v on luvun 2 potenssi. Ennen nelikkosysteemien varsinaista määrittelyä ja konstruointia esitellään tarvittavat aputulokset.

Lemma 11. *Steinerin systeemissä $S(t,k,v)$ on $\binom{v}{t}/\binom{k}{t}$ lohkoa.*

Todistus. Tulos saadaan yhtälöstä (19) valitsemalla $\lambda = 1$. □

Sitten hyödynnetään edellisen alaluvun aputulosta siitä, miten johdetun sommitelman lohkot muodostetaan.

Lemma 12. *Jos on olemassa Steinerin systeemi $S(t,k,v)$, niin on olemassa myös systeemi $S(t-1,k-1,v-1)$.*

Todistus. Väite seuraa, kun lemmassa 8 valitaan $\lambda = 1$. □

Systeemin parametreja voidaan siis aina pienentää, ja lohkojen lukumäärän on säilyttävä luonnollisena lukuna. Seuraava aputulos on täten varmasti voimassa.

Lemma 13. *Jos $S(t,k,v)$ on olemassa, niin luvut*

$$\binom{v}{t}/\binom{k}{t}, \binom{v-1}{t-1}/\binom{k-1}{t-1}, \ldots, \binom{v-t+1}{1}/\binom{k-t+1}{1}$$

ovat luonnollisia lukuja.

Lemman 13 perusteella hvaitaan systeemin $S(t,k,v)$ välttämättömiä voimassaoloehtoja. Jos on olemassa esimerkiksi $S(2,k,v)$, niin lukujen $\binom{v}{2}/\binom{k}{2}$ ja $\binom{v-1}{1}/\binom{k-1}{1}$ on oltava luonnollisia lukuja. Toisin sanoen $\frac{v(v-1)}{k(k-1)}$ ja $\frac{v-1}{k-1}$ ovat luonnollisia lukuja. Jotta kolmikkosysteemi $S(2,3,v)$ voisi olla olemassa, vaaditaan, että $v(v-1) \equiv 0 \pmod 6$ ja $v-1 \equiv 0 \pmod 2$ eli tiivistettynä $v \equiv 1$ tai $3 \pmod 6$, kuten aiemmin tässä luvussa osoitettiin. Tutkitaan nyt vastaavasti nelikkosysteemin $S(3,4,v)$ olemassaoloa.

Lemma 14. *Jos Steinerin nelikkosysteemi $S(3,4,v)$ on olemassa, niin $v \equiv 2$ tai 4 (mod 6).*

Todistus. Jos käytetään lemmaa 13, niin lukujen $\frac{1}{4}\binom{v}{3}$, $\frac{1}{3}\binom{v-1}{2}$ ja $\frac{1}{2}\binom{v-2}{1}$ on oltava luonnollisia lukuja. Väite voidaan todistaa myös päättelemällä, että jos $S(3,4,v)$ on olemassa, niin myös $S(2,3,v-1)$ on olemassa. Tällöin $v-1 \equiv 1$ tai $3 \pmod 6$ eli $v \equiv 2$ tai $4 \pmod 6$. □

Esitellään ennen alaluvun päätuloksia nelikkosysteemin määritelmä ja eräs merkintätapa.

Määritelmä 13. *Steinerin nelikkosysteemi* $S(3,4,v)$, merkitään myös $SQS(v)$, on $3-(v,4,1)$-sommitelma.

Tarkastellaan vielä esimerkkiä nelikkosysteemistä ja muodostetaan sen pohjalta johdettu sommitelma, joka määriteltiin aiemmin.

Esimerkki 14. Steinerin systeemi $SQS(10)$ voidaan koota perusjoukosta $\{0, \ldots, 9\}$ valitsemalla lohkoiksi $\{1, 2, 4, 5\}$, $\{1, 2, 3, 7\}$, $\{1, 3, 5, 8\}$ ja näiden translaatit eli sykliset siirrot (mod 10). Esimerkiksi lohkon $\{1, 2, 3, 7\}$ translaatit ovat $\{2, 3, 4, 8\}$, $\{3, 4, 5, 9\}$, $\{4, 5, 6, 0\}$, $\{5, 6, 7, 1\}$, $\{6, 7, 8, 2\}$, $\{7, 8, 9, 3\}$, $\{8, 9, 0, 4\}$, $\{9, 0, 1, 5\}$ ja $\{0, 1, 2, 6\}$.

Valitaan $P = 0$. Nyt johdettu sommitelma $\mathcal{D}_P$ koostuu lohkoista

$$\{1, 3, 4\};\ \{1, 7, 8\};\ \{2, 3, 9\};\ \{6, 7, 9\};\ \{1, 2, 6\};\ \{1, 5, 9\};$$
$$\{4, 8, 9\};\ \{4, 5, 6\};\ \{2, 4, 7\};\ \{2, 5, 8\};\ \{3, 6, 8\} \text{ ja } \{3, 5, 7\}.$$

Näin saatiin jälleen Steinerin systeemi $STS(9)$.

Esitellään nyt nelikkosysteemin tuplauskonstruktio. Jos siis tunnetaan jokin nelikkosysteemi, on aina mahdollista luoda uusi.

Lause 15. *Jos on olemassa Steinerin nelikkosysteemi $SQS(v)$, on olemassa myös systeemi $SQS(2v)$.*

Todistus. Olkoot X ja Y erilliset v-joukot. Olkoot $\mathcal{S}_1$ ja $\mathcal{S}_2$ systeemejä $SQS(v)$, joista ensimmäinen on koottu perusjoukon X pohjalta ja jälkimmäinen perusjoukon Y pohjalta. Lemman 14 mukaan v on parillinen, joten voidaan konstruoida kaksi hajoavaa $(v, 2, 1)$-sommitelmaa. Olkoot $F_1, \ldots, F_{v-1}$ rinnakkaisluokkia joukon X tapauksessa ja $G_1, \ldots, G_{v-1}$ rinnakkaisluokkia joukon Y tapauksessa. Muodostetaan sitten nelikkosysteemi unionin $X \cup Y$ pohjalta valitsemalla nelikoiksi kaikki systeemien $\mathcal{S}_1$ ja $\mathcal{S}_2$ nelikot sekä kaikki sellaiset nelikot $\{x_1, x_2, y_1, y_2\}$, että jollakin i osajoukko $\{x_1, x_2\} \in F_i$ ja $\{y_1, y_2\} \in G_i$. Voidaan päätellä, että joukon X mitkä tahansa kolme alkiota esiintyvät vain yhdessä systeemin $\mathcal{S}_1$ nelikossa ja vastaavasti joukon Y mitkä tahansa kolme alkiota esiintyvät vain yhdessä systeemin $\mathcal{S}_2$ nelikossa. Tarkastellaan lopuksi kolmea alkiota x_1, x_2 ja y. On vain yksi sellainen indeksi i, jolle on voimassa $\{x_1, x_2\} \in F_i$, että $\{y_1, y_2\}$ on luokan G_i yksikäsitteinen alkion y sisältävä lohko. Tällä tavalla saadaan kaikki halutut nelikot. □

Todetaan induktioperiaatteen nojalla, että nelikkosysteemi $SQS(2^n)$ on olemassa kaikilla eksponenteilla $n \geq 2$.

Tutkielman lopuksi esitellään vielä Hananin tulos, jota ei kuitenkaan todisteta tässä tarkasti. Hanani onnistui osoittamaan, että lemman 14 ehdon toteutumisesta seuraa systeemin $SQS(v)$ olemassaolo. Todistuksessa käytetään seuraavia rekursiivisia tietoja:

1. Jos on olemassa $SQS(v)$, on olemassa myös $SQS(2v)$.
2. Jos on olemassa $SQS(v)$, on olemassa myös $SQS(3v - 2)$.
3. Jos on olemassa $SQS(v)$ ja $v \equiv 10 \pmod{12}$, on olemassa myös $SQS(3v + 4)$.
4. Jos on olemassa $SQS(v)$ ja $v \equiv 8 \pmod{12}$, on olemassa myös $SQS(3v + 2)$.
5. Jos on olemassa $SQS(v)$, on olemassa myös $SQS(4v - 6)$.
6. Jos on olemassa $SQS(v)$, on olemassa myös $SQS(12v - 10)$.

Kun lisäksi tiedetään, että systeemit $SQS(14)$ ja $SQS(38)$ ovat olemassa, saadaan todistettua seuraava lause.

Lause 16. *Steinerin nelikkosysteemi $S(3,4,v)$ on olemassa, jos ja vain jos $v \equiv 2$ tai 4 (mod 6), missä $v \geq 4$.*

6 Yhteenveto

Kerrataan, millaisia tutkimustuloksia työn aikana saatiin. Ensinnäkin on olemassa useita menetelmiä Hadamardin matriisien konstruoimiseksi. Ne on saatu aikaan käyttämällä hyödyksi monenlaisia matemaattisia käsitteitä, operaattoreita ja tuloksia. Pienikokoisia lohkosommitelmia on mahdollista muodostaa päättelemällä, mutta tässäkin yhteydessä erilaiset konstruointimenetelmät ovat tarpeen. Sommitelmia voidaan koota esimerkiksi muuttamalla Hadamardin matriisi sommitelman matriisiksi, muodostamalla ekvivalenssiluokkien avulla projektiivinen taso tai keräämällä kolmikoita Skolemin metodin mukaisesti.

Tutkielman yhtenä tavoitteena oli löytää jatkumo Hadamardin matriiseista lohkosommitelmien ja projektiivisten tasojen kautta Steinerin systeemeihin. Osoittautui, että eräs yhteys kaikkien näiden välillä on $(7, 3, 1)$-sommitelma, sillä sen nähtiin olevan projektiivinen taso ja Steinerin systeemi. Kyseessä on myös Hadamardin sommitelma, joten sen avulla löydetään Hadamardin matriisi. Tällainen yksinkertainen esimerkki voi osoittaa, kuinka matematiikassa eri tavalla määritellyt asiat saattavat liittyä tai vaikuttaa toisiinsa.

Pohditaan lopuksi, miten tutkimustyötä voisi jatkaa tämän tutkielman pohjalta. Yksi vaihtoehto olisi tutkia lisää otaksumaa siitä, että jokaisella asteluvulla $m = 4k$ olisi olemassa Hadamardin matriisi ja sommitelma. Vuoteen 2014 mennessä tiedetään 12 kappaletta lukua 2000 pienempiä mahdollisia astelukuja, joiden tapauksessa Hadamardin matriiseja ei tunneta lainkaan. Olisi myös kiinnostavaa tarkastella syvällisemmin Hadamardin 3-sommitelmien ja matriisien välistä yhteyttä tai Steinerin nelikkosysteemien olemassaoloehtoa. Mainitaan vielä, että vaikka tässä tutkielmassa sivuutettiin esimerkiksi affiinit tasot eli $(n^2, n, 1)$-sommitelmat, differenssisysteemit ja parittain tasapainoiset (v, K, λ)-sommitelmat, missä parametri K on joukko, niissäkin riittäisi runsaasti tutkittavaa.

Viitteet

[1] Anderson, I.: *Combinatorial Designs: Construction Methods*. Chichester: Ellis Horwood, 1990.

[2] Anderson, I. & Honkala, I.: *A Short Course in Combinatorial Designs*. Internet Edition, Spring 1997, Revised 2012.

[3] Hall, M.: *Combinatorial Theory*. New York: Wiley, 1986 (Second Edition).