Hilat: katsaus hiloista ja niiden sovelluskohteista eri matematiikan osa-alueilla sekä kouluopetuksessa

Juho Gröhn
ohjaaja: Louna Seppälä

22. huhtikuuta 2021

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen osasto

Tekijä — Författare — Author
Juho Gröhn

Työn nimi — Arbetets titel — Title

Hilat: katsaus hiloista ja niiden sovelluskohteista eri matematiikan osa-alueilla sekä kouluopetuksessa

Oppiaine — Läroämne — Subject		
Matematiikka		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Maisterintutkielma	22. huhtikuuta 2021	40

Tiivistelmä — Referat — Abstract

Tässä tutkielmassa käsitellään hiloja ja niiden sovelluskohteita eri matematiikan osa-alueilla.
Työn ensimmäisessä puolikkaassa esitellään hilat käsitteenä ja todistetaan hiloihin liittyvät kaikkein keskeisimmät tulokset. Kappaleessa 2 esitellään useita hilojen helposti todistettavia ominaisuuksia. Tällaisia ominaisuuksia ovat esimerkiksi hilan perussuunnikkaan koon riippumattomuus kannan valinnasta sekä Minkowskin ensimmäinen lause. Kappaleessa 3 esitellään ja todistetaan Minkowskin toinen lause. Lisäksi esitellään kaikki se teoria, joka täytyy tuntea todistuksen ymmärtämiseksi ja jota ei voi olettaa yleissivistykseksi. Tällainen on esimerkiksi Jordan-sisällön käsite.
Työn jälkimmäisessä puolikkaassa esitellään, miten hilat ja niihin liittyvä teoria yhdistyy moniin sellaisiin aiheisiin, joiden yhteys hiloihin ei ole aivan ilmeinen. Kappaleessa 4 esitellään Gaussin kokonaisluvut ja niihin liittyvä ympyräongelma. Ympyräongelmalle johdetaan muutama kohtalaisen alkeellinen tulos. Kappaleessa 6 esitellään ympyräpakkausongelmat ja ympyräongelmien tunnetut ratkaisut. Kaikki tunnetut ratkaisut ovat hilapakkauksia. Kappaleessa 7 esitellään, miten hiloihin liittyvä teoria sidostuu tietojenkäsittelytieteeseen. Esitellään virheenkorjausalgoritmien ja optimaalisten hilapakkausten välistä suhdetta. Esitellään myös lyhimmän ja lähimmän hilapisteen ongelmat ja todistetaan ongelmille muutama alkeellinen tulos.
Aivan työn lopuksi, yhteenvetokappaleessa 8, pohditaan mitä yhtymäkohtia hilateorialla on yläasteen ja lukion matematiikan oppimääriin ja miten hilateoriaa voisi hyödyntää näiden oppilaitosten matematiikan opetuksessa.

Avainsanat — Nyckelord — Keywords
hilat, lukuteoria, Minkowskin toinen lause, pakkausongelmat

Säilytyspaikka — Förvaringsställe — Where deposited
sähköinen

Muita tietoja — Övriga uppgifter — Additional information

Sisällys

1 Johdanto

Tässä työssä tutkitaan hiloja, niiden ominaisuuksia, ja hilateorian sovelluskohteita lukion ja ylä-asteen matematiikkaan. Tämä johdanto pyrkii perustelemaan, miksi aiheenvalinta on mielekäs ja kiinnostava.

Hilan käsite määritellään tässä työssä heti luvussa 2. Hilat aiheena on mielenkiintoinen, sillä hilan käsite liittyy yhtä lailla lukuteoriaan, lineaarialgebraan kuin geometriaankin. Monilla hiloihin liittyvillä ongelmilla on lisäksi mittateoreettisia ulottuvuuksia. Käytännössä tämä tarkoittaa, että hiloihin liittyvät lauseet ovat usein helppoja esittää mutta haastavia ratkaista, että ratkaisut sisältävät runsaasti vektorilaskentaa, että havainnollistavien kuvien piirtäminen on pääsääntöisesti helppoa, ja että pinta-aloja ja tilavuuksia käsitellään varsin usein. Hilat aiheena on siis hedelmällinen monenlaisen matematiikan kekseliääseen soveltamiseen.

Useat hiloihin liittyvät lauseet luokitellaan ns. "lukugeometrian" lauseiksi, ja näissä lauseissa yhdistyy juuri tällaisella luovalla tavalla eri matematiikan osa-alueiden tuloksia. Esimerkiksi Minkowskin ensimmäinen ja toinen lause ovat lukuteorian peruslauseita[1, s. 2], ja näiden lauseiden todistukset vaativat kumpikin ovelaa ongelmanratkaisua, jossa yhdistyy niin algebrallinen, analyyttinen, kuin geometrinenkin päättely. Minkowskin ensimmäinen lause esitellään alaluvussa 2.4; Minkowskin toinen lause on niin suuri ja haastava, että sille varataan koko kappale 3.

Hiloihin käsitteenä liittyy olennaisesti ajatus loputtomasta, samanlaisena toistuvasta äärettömästä tasosta tai tätä moniulotteisemmasta avaruudesta. Näin ollen hilat liittyvät useisiin sellaisiin ongelmiin, joihin liittyy keskeisesti toisto ja moniulotteisuus. Tällaisia ovat esimerkiksi pakkausongelmat: ongelmat, joissa n-kuulia pyritään pakkamaan suureen astiaan mahdollisimman tiiviisti. Kaikissa niissä avaruuksissa $\mathbb{R}^n$, joissa optimaalinen pakkaus tiedetään, tämä pakkaus on ollut paitsi säännöllinen, myös ns. hilapakkaus, eli pakkaus, jonka n-kuulien keskipisteet ovat hilapisteitä. Pakkausongelmista kerrotaan lisää kappaleessa 6.

Hilat tuovat myös uusia näkökulmia vanhastaan tunnettuihin lukuteorian ongelmiin ja sama pätee myös toiseen suuntaan. Kappaleessa 4 esitellään Gaussin ympyräongelma hilojen näkökulmasta ja samalla tutustutaan ajatukseen, että myös Gaussin kokonaisluvut on itse asiassa hila. Kappaleessa 5 todistetaan Dirichlet'n epäyhtälö lukugeometrisesti origokeskisen suunnikkaan avulla.

Eräs puhtaan matematiikan ulkopuolinen aihe, johon hiloilla on yhtymäkohtia, on tietojenkäsittelytiede. Kappaleessa 7 esitellään, miten virheenkorjausalgoritmit ovat aiheena lähisukua pakkausongelmille. Esitellään myös lyhimmän ja lähimmän hilapisteen ongelmat, sekä se miten ongelmat ovat näennäisestä yksinkertaisuudestaan huolimatta tosiasiassa erittäin vaikeiksi – tarkemmin, NP-vaikeiksi – epäiltyjä ratkaisuongelmia.

Aivan työn lopussa, yhteenvetokappaleessa 8 esitellään useita esimerkkejä siitä, miten hiloihin liittyvää monipuolista matematiikkaa voisi sisällyttää yläasteen ja lukion opetukseen.

Merkintäkäytäntöjä ja usein käytettyjä määritelmiä

- Tässä työssä merkintä $\mathbb{R}^n$ tarkoittaa mitä tahansa reaalivektoriavaruutta, eli n on mielivaltainen, jos ei erikseen toisin mainita.

- Reaalivektoreita merkitään yläviivalla varustetuilla pienillä kirjaimilla, tyyllillä $\bar{v}, \bar{w}, \bar{x}, \bar{y}, \bar{z}$, jne.
- Poikkeus edelliseen on kompleksitulolla varustettujen avaruuksien vektorit. Tällaisia vektoreita merkitään kuten reaalilukuja – pienillä yläviivattomilla kirjaimilla – ja näistä vektoreista saatetaan puhua myös lukuina. Kompleksitulolla varustettuja avaruuksia tässä työssä ovat esimerkiksi kompleksitaso, Gaussin kokonaisluvut, ja oktonioavaruus.
- Matriiseja merkitään isoilla kirjaimilla M, N, jne.
- "Vektorijono" ja "matriisi" ovat synonyymit.
- Kuitenkin kun matriiseihin viitataan matriiseina, ne ovat lähtökohtaisesti neliömatriiseja $\mathbb{R}^{n\times n}$, mutta jos niistä puhutaan vektorijonoina, näin ei välttämättä ole.
- Hilasta ja sitä määrittävästä vektorijonosta(=matriisista) käytetään samaa merkintää silloin, kun sekaannuksen vaaraa ei ole. Esimerkiksi yhdessä kontekstissa voidaan merkitä $\Lambda\bar{x}$ merkitsemään lineaarikuvausta hilan kantamatriisilla, kun taas toisessa asiayhteydessä voidaan merkitä $\bar{x} \in \Lambda$ osoittamaan, että $\bar{x}$ on hilapiste. Hiloja merkitään samoin kuin matriiseja tai, tavallisemmin, symbolilla Λ.
- Kun hilan kantaa ei ole täsmennetty, voidaan olettaa, että käsiteltävä ominaisuus ei riipu kannan valinnasta.
- Sana "symmetrinen" viittaa origon suhteen symmetrisyyteen, jos ei toisin täsmennetä. Symmetrinen kappale sisältää vektorin tasan silloin, kun se sisältää myös tämän vastavektorin.
- Konveksi kappale tarkoittaa ei missään koveraa kappaletta: jokainen kappaleen pisteiden välinen jana on kappaleen osajoukko.
- Mitalla tarkoitetaan tavallista Lebesque-mittaa. Avaruudessa $\mathbb{R}^2$ tämä tarkoittaa pinta-alaa, avaruudessa $\mathbb{R}^3$ tilavuutta, jne. Kussakin tapauksessa mittaa merkitään pystyviivamerkinnällä $|\cdot|$, tyylillä "$|K| > 2^n, K \subset \mathbb{R}^n$".

2 Hilojen ominaisuuksia

Tässä kappaleessa määritellään hilan käsite sekä esitellään joitain hilojen perusominaisuuksista.

Intuition tasolla hilojen voidaan ajatella koostuvan tasavälisiin riveihin ja sarakkeisiin järjestetyistä, diskreeteistä, avaruuden $\mathbb{R}^n$ pisteistä. Esimerkiksi joukot $\mathbb{Z}^n$ ovat kaikki hiloja. Rivien ei kuitenkaan täydy olla yhtä korkeat kuin sarakkeet ovat leveät, ja kummatkin saavat olla vinossa suhteessa toisiinsa sekä suhteessa avaruuden luonnoliseen kantaan.

Määritellään seuraavaksi hila tarkemmin. Lainataan Wolfgang M. Schmidtin teoksessa *"Diophantine Approximation"* käytettyä määritelmää [2, s. 111].

Määritelmä 2.1. *Λ on hila, jos on olemassa lineaarisesti riippumattomien vektorien $(\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n), \bar{v}_i \in \mathbb{R}^n$ jono, jolla*

$$\Lambda = \{z_1\bar{v}_1 + z_2\bar{v}_2 + \ldots z_n\bar{v}_n | z_1, z_2, \ldots z_n \in \mathbb{Z}\}.$$

Toisin sanottuna hila on riippumattomien reaalivektorien kokonaislukukombinaatioista rakentuva ryhmä.

2.1 Perusominaisuuksia

Koska jokaisen hilan virittää n riippumatonta vektoria avaruudessa $\mathbb{R}^n$, virittää jokainen hila avaruuden $\mathbb{R}^n$.

Jokainen hila, jonka virittää n riippumatonta vektoria, on lisäksi isomorfinen ryhmän $(\mathbb{Z}^n, +)$ kanssa. Tämä on helppo nähdä ryhmäisomorfismista f:

$$f : \Lambda \to \mathbb{Z}^n, f(z_1v_1 + z_2v_2 + \cdots + z_nv_n) = (z_1, z_2, \ldots, z_n).$$

Tästä isomorfismista seuraa myös se, että jokainen hila on ryhmän $(\mathbb{R}^n, +)$ aliryhmä.

Huomataan lisäksi, että isomorfismi f on homeomorfismi. Tästä seuraa se, että koska jokainen joukko $\mathbb{Z}^n$ on diskreetti, jokainen hila on diskreetti.

2.2 Kannan determinantti

Lause 2.1. *Mille tahansa hilalle $\Lambda \in \mathbb{R}^n$ pätee, että jos vapaa jono $V = (\bar{v}_1, \ldots, \bar{v}_n)$ muodostaa hilan Λ kannan, ja myös vapaa jono $W = (\bar{w}_1, \ldots, \bar{w}_n)$ muodostaa tämän hilan kannan, niin*

$$|\det(V)| = |\det(W)|.$$

Todistetaan tämä seuraavaksi.

Todistus. Olkoon $V = \begin{bmatrix} \bar{v}_1 & \ldots & \bar{v}_n \end{bmatrix} \in \mathbb{R}^{n\times n}, W = \begin{bmatrix} \bar{w}_1 & \ldots & \bar{w}_n \end{bmatrix} \in \mathbb{R}^{n\times n}$ ja sekä V että W muodostavat kannan hilalle Λ.

Koska V on kanta hilalle Λ, niin $\bar{v}_1, \ldots, \bar{v}_n \in \Lambda$.

Toisaalta, koska W on kanta hilalle Λ, on olemassa kokonaislukukombinaatio $\bar{z}_1 = \begin{bmatrix} z_{11} \\ \vdots \\ z_{n1} \end{bmatrix} \in \mathbb{Z}^{n\times 1}$, jolla

$$W\bar{z}_1 = \bar{w}_1z_{11} + \cdots + \bar{w}_nz_{n1} = \bar{v}_1.$$

Vastaavasti on olemassa $\bar{z}_2 = \begin{bmatrix} z_{12} \\ \vdots \\ z_{n2} \end{bmatrix} \in \mathbb{Z}^{n\times 1}$, jolla $W\bar{z}_2 = \bar{w}_1 z_{12} + \cdots + \bar{w}_n z_{n2} = \bar{v}_2$,

jne.

Yleisesti, on olemassa kokonaislukumatriisi

$$Z = \begin{bmatrix} \bar{z}_1 & \bar{z}_2 & \dots & \bar{z}_n \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1n} \\ z_{21} & z_{22} & \dots & z_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1} & z_{n2} & \dots & z_{nn} \end{bmatrix} \in \mathbb{Z}^{n\times n},$$

jolla

$$WZ = \begin{bmatrix} W\bar{z}_1 & W\bar{z}_2 \dots & W\bar{z}_n \end{bmatrix} = \begin{bmatrix} \bar{v}_1 & \bar{v}_2 & \dots & \bar{v}_n \end{bmatrix} = V.$$

Symmetrisesti on olemassa $Z^{-1} \in \mathbb{Z}^{n\times n}$ jolla $VZ^{-1} = W$. On helppo huomata, että Z ja Z^{-1} ovat toistena käänteismatriisit.

Olennaisesti, koska $Z \in \mathbb{Z}^{n\times n}$, niin $\det(Z) \in \mathbb{Z}$. Kuitenkin, myös $Z^{-1} \in \mathbb{Z}^{n\times n}$. Siispä, koska $Z^{-1} \in \mathbb{Z}^{n\times n}$, niin myös $\det(Z^{-1}) \in \mathbb{Z}$.

Muistetaan nyt, että $\det(A)\det(A^{-1}) = 1$ kaikilla kääntyvillä neliömatriiseilla A. Tämä yhdessä edellisten huomioiden kanssa tarkoittaa, että

$$\det(Z) = \det(Z^{-1}) = \pm 1.$$

Tästä seuraa päättely

$$\begin{aligned} WZ &= V \\ |\det(WZ)| &= |\det(V)| \\ |\det(W)\det(Z)| &= |\det(V)| \\ |\det(W)||\det(Z)| &= |\det(V)| \\ |\det(W)| \cdot 1 &= |\det(V)| \\ |\det(W)| &= |\det(V)|. \end{aligned}$$

Tämä viimeistelee todistuksen.

□

Lause 2.1 on todistettu hyvin samankaltaisella päättelyllä myös mm. Evertsen vuoden 2017 kurssimuistiinpanoissa[3, kpl 2., s. 9].

Hilalle avaruudessa $\mathbb{R}^2$ tämä determinantin itseisarvo vastaa kantavektorien määräämän suunnikkaan pinta-alaa. Avaruuden $\mathbb{R}^3$ hilalle tämä on kantavektorien määräämän suuntaissärmiön tilavuus. Yleisesti avaruudessa $\mathbb{R}^n$ kantavektorien determinantin itseisarvo on vektorien määräämän hypersuunnikkaan mitta. Kirjallisuudessa tätä kappaletta kutsutaan hilan "perussuunnikkaaksi" (eng. "fundamental parallelepiped").

Lause 2.1 siis kertoo, että kaikki ne hilan hypersuunnikkaat, joiden sivut muodostavat jonkun kannan hilalle, ovat mitaltaan yhtä suuret, ja voivat täten kukin yhtä hyvin olla hilan perussuunnikas.

2.3 Hilan suhde kaimakäsitteeseensä

Hilalla on olemassa tunnettu kaimakäsite – myös nimeltään "hila" – jonka määritelmä on täysin erilainen kuin määritelmä 2.1. Tämä toisenlainen hilan määritelmä esiintyy järjestettyjen joukkojen kontekstissa. Kaimakäsite esitellään tässä työssä käsitteiden erojen ja yhtäläisyyksien vertailun vuoksi.

Määritelmä 2.2. *Hila on osittain järjestetty joukko* $(S, \leq)$*, jossa jokaisella alkioparilla on*

- *supremum,* $\wedge : S \times S \to S$*, jolla* $a, b \leq a \wedge b$*, ja*
- *infimum,* $\vee : S \times S \to S$*, jolla* $a, b \geq a \vee b$*.*

Supremum ja infimum ovat vaihdannaiset ja liitännäiset ja lisäksi niille pätevät absorptiolait

- $(a \wedge b) \vee a = a$
- $(a \vee b) \wedge a = a$.

Käytetään jatkossa määritelmän 2.2 mukaisesta hilasta nimitystä "järjestyshila" ja määritelmän 2.1 mukaisesta hilasta nimitystä "algebrallinen hila" tai vain "hila". Järjestyshiloja ei tulla käsittelemään tässä työssä tämän kappaleen ulkopuolella.

Esimerkkejä järjestyshiloista ovat kaikki täysin järjestetyt joukot; näissä supremum on yksinkertaisesti alkioparien maksimi ja infimum alkioparien minimi. Kuitenkin, kiinnostavammin, myös esimerkiksi $(\mathbb{N}, |)$, eli luonnolliset luvut jaollisuusrelaatiolla on järjestyshila. Tässä järjestyshilassa alkioiden supremum on niiden pienin yhteinen moninkerta ja infimum niiden suurin yhteinen tekijä.

Kaikille algebrallisille hiloille voidaan määritellä järjestys, supremum, ja infimum, jotka täydentäisivät kyseisen hilan järjestyshilaksi. Esimerkki tälläisesta täydentävästä määritelmästä hilassa $\mathbb{Z}^n$ olisi seuraava:

- $(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n) \Leftrightarrow (x_1 \leq y_1) \wedge \ldots \wedge (x_n \leq y_n)$.
- $(x_1, \ldots, x_n) \wedge (y_1, \ldots, y_n) = (\max(x_1, y_1), \ldots, \max(x_n, y_n))$.
- $(x_1, \ldots, x_n) \vee (y_1, \ldots, y_n) = (\min(x_1, y_1), \ldots, \min(x_n, y_n))$.

Esimerkki kaikille muille hiloille puolestaan saadaan isomorfismilla edellisestä. Näin ollen kaikkia algebrallisia hiloja on mahdollista käsitellä järjestyshiloina.

Sama ei kuitenkaan ole totta toisin päin: kaikkia järjestyshiloja ei voi käsitellä algebrallisina hiloina. Esimerkiksi $(\mathbb{R}, \leq)$ on järjestyshila, mutta ei ylinumeroituvuutensa vuoksi voi olla isomorfinen minkään algebrallisen hilan kanssa: algebralliset hilat ovat kaikki numeroituvia.

Järjestyshila on käsitteenä mielenkiintoinen, mutta koska sen yhteys algebrallisiin hiloihin on harmillisen yksipuolinen, rajataan käsitteen tarkempi tarkastelu tämän työn ulkopuolelle.

Tässä kappaleessa johdetaan kaikille hiloille yhteisiä ominaisuuksia. Ominaisuuksista jotkut ovat nopeasti ilmeisiä, ja ne esitellään kootusti kappaleessa 2.1. Muille ominaisuuksille on omistettu omat kappaleensa.

2.4 Minkowskin konveksien kappaleiden lause

Minkowskin konveksien kappaleiden lause – tai lyhyemmin vain *Minkowskin lause* – sitoo avaruuden $\mathbb{R}^n$ kappaleet tämän avaruuden hiloihin. Minkowskin lause todistaa, että tietynlaiset kappaleet avaruudessa $\mathbb{R}^n$ sisältävät aina vähintään kolme hilapistettä.

Lause 2.2 (Minkowskin lause)**.** *Avaruuden $\mathbb{R}^n$ kappale, joka on*

- *konveksi,*
- *symmetrinen origon suhteen,*
- *ja mitaltaan suurempi kuin 2^n*

sisältää origon ohella vähintään yhden toisen hilan $\mathbb{Z}^n$ pisteen.

Luonnollisesti kaikki lauseen 2.2 ehdot täyttävä kappale sisältää myös kolmannen hilapisteen: origosta poikkeavan hilapisteen vastavektorin.

Lisäksi huomataan, että konvekseille, symmetrisille kappaleille 2^n on mitan pienin yläraja, joka varmistaa ylimääräisten hilapisteiden olemassaolon: Esimerkiksi origonkeskinen avoin neliö, kuutio, tai hyperkuutio, jonka sivun pituus on 2, on mitaltaan tasan 2^n mutta sisältää hilan $\mathbb{Z}^n$ pisteistä vain origon.

Minkowskin lauseelle on useita todistuksia[2, s. 32]. Todistetaan seuraavaksi Minkowskin lause Evertsen algebrallista todistusta [3, kappale 2, s. 14] mukaillen, mutta käyttäen sivuluokka-algebrallisia merkintätapoja.

Todistus. Olkoon K konveksi, symmetrinen joukko avaruudessa $\mathbb{R}^n$. Olkoon $|K| > 2^n$.

$2\mathbb{Z}^n$ parillisten kokonaislukuvektorien muodostama hila. Kuvatkoon funktio f kunkin kappaleen K vektorin $\bar{x}$ omalle ekvivalenssiluokalleen hilan $2\mathbb{Z}^n$ suhteen, eli

$$f : K \to \mathbb{R}^n/2\mathbb{Z}^n : f(\bar{x}) = \{\bar{x} + 2\bar{q} | 2\bar{q} \in 2\mathbb{Z}^n\}.$$

Visuaalisesti tulkittuna f jakaa avaruuden $\mathbb{R}^n$ ja sen kappaleen K hyperkuutioihin, joiden sivujen pituudet ovat 2, ja kuvaa kunkin vektorin sijainnilleen oman kuutionsa suhteen.

Huomataan, että f on lokaalisti mitan säilyttävä funktio, eli $|fA| = |A|$ kaikilla riittävän pienillä $A \subset K$. Lisäksi huomataan, että f maalijoukko, eli ekvivalenssiluokkien $\bar{x} + 2\mathbb{Z}^n$ muodostama tekijäavaruus $\mathbb{R}^n/2\mathbb{Z}^n$ on kuutio, jonka mitta on 2^n. Kuitenkin määritelmällisesti $|K| > 2^n$. Nämä seikat yhdessä johtavat siihen, että f ei voi olla injektio: Jos f olisi injektio, sille olisi olemassa mitan säilyttävä käänteiskuvaus f^{-1}. Tämä ei kuitenkaan ole mahdollista, sillä $|fK| \leq 2^n$ mutta $|f^{-1}(fK)| = |K| > 2^n$.

Koska f ei ole injektio, on olemassa ainakin kaksi pistettä, $\bar{x} \in K$ ja $\bar{y} \in K, \bar{x} \neq \bar{y}$, joilla $f(\bar{x}) = f(\bar{y})$, eli on olemassa $2\bar{z} \in 2\mathbb{Z}^n$, jolla $\bar{y} = \bar{x} + 2\bar{z}$.

Koska K on origon suhteen symmetrinen, sisältyy näiden ohella myös piste $-\bar{x}$ joukkoon K.

Koska K on konveksi, sisältyy jokainen piste janalla pisteestä $-\bar{x}$ pisteeseen $\bar{y}$ joukkoon K. Erityisesti tämän janan keskipiste $\bar{v}$ kuuluu joukkoon. $\bar{v}$ on hilapiste, sillä

$$\begin{aligned}\bar{v} &= \frac{1}{2}(-\bar{x} + \bar{y}) \\ &= \frac{1}{2}\left(-\bar{x} + \bar{x} + 2\bar{z}\right) \\ &= \frac{1}{2}(2\bar{z}) \\ &= \bar{z} \in \mathbb{Z}^n.\end{aligned}$$

$\bar{v} \neq \bar{0}$, sillä $\bar{y} = \bar{x} + 2\bar{z}$ ja $\bar{x} \neq \bar{y}$.

Täten on löydetty joukon K piste, joka ei ole $\bar{0}$ ja joka sisältyy joukkoon $\mathbb{Z}^n$. Tämä viimeistelee Minkowskin lauseen todistuksen.

□

Minkowskin ensimmäinen lause mielivaltaisessa hilassa Λ Minkowskin lause yleistyy muille hiloille kuin $\mathbb{Z}^n$.

Lause 2.3 (Minkowskin ensimmäisen lauseen korollaari)**.** *Mielivaltaisessa hilassa $\Lambda \subset \mathbb{R}^n$, symmetrinen ja konveksi kappale K sisältää ainakin yhden origosta poikkeavan hilapisteen, jos $|K| \geq 2^n |\det \Lambda|$.*

Tämän osoittamiseen tarvitaan seuraavat kaksi aputulosta:

Lause 2.4. *Jos L on lineaarikuvaus, $|LK| = |\det(L)||K|$.*

Lause 2.5. *Jos K on konveksi ja symmetrinen, ja L on lineaarikuvaus, myös LK on konveksi ja symmetrinen.*

Lauseelle 2.4 on olemassa valmis todistus olemassaolevassa kirjallisuudessa[4, s. 389]. Todistus menee mittateorian puolelle, joten jätetään se todistamatta uudelleen.

Lauseen 2.5 todistus sen sijaan on hyvin helppo:

Todistus. Olkoon K symmetrinen ja konveksi kappale ja olkoon L lineaarikuvaus. Nyt

- $\bar{x} \in K \Rightarrow L\bar{x} \in LK$ ja $-\bar{x} \in K \Rightarrow -L\bar{x} \in LK$, joten

  $$(\bar{x} \in K \Leftrightarrow -x \in K) \Rightarrow (L\bar{x} \in LK \Leftrightarrow -L\bar{x} \in LK).$$

  Näin ollen jos K on symmetrinen, LK on symmetrinen.

- Jos kaikki janapisteet $p\bar{x} + q\bar{y}, p + q = 1$ pisteiden $\bar{x}, \bar{y} \in K$ välillä kuuluvat kappaleeseen K, niin pisteet $L(p\bar{x} + q\bar{y})$ kuuluvat kappaleeseen LK. Mutta

  $$L(p\bar{x} + q\bar{y}) = p(L\bar{x}) + q(L\bar{y}),$$

  jolloin nämä pisteet ovat siis tasan ne janapisteet, jotka ovat pisteiden $L\bar{x}$ ja $L\bar{y}$ välissä. Tämä tulos ei riipu pisteiden $\bar{x}$ ja $\bar{y}$ valinnasta. Näin ollen jos K on konveksi, LK on konveksi.

□

Lauseiden 2.4 ja 2.5 turvin ollaan valmiita todistamaan lause 2.3

Todistus. Olkoon K konveksi ja symmetrinen kappale ja olkoon Λ mielivaltainen hila. Olkoon kappaleen K mitta ainakin $2^n|\det(\Lambda)|$.

Lauseesta 2.4 seuraa, että kappaleen $\Lambda^{-1}K$ mitta on ainakin $|\det(\Lambda^{-1})|2^n|\det(\Lambda)| = 2^n$. Lauseen 2.5 nojalla $\Lambda^{-1}K$ on symmetrinen ja konveksi, jolloin lauseen 2.2 nojalla $\Lambda^{-1}K$ sisältää ainakin yhden origosta poikkeavan pisteen $\bar{x}$ hilasta $\mathbb{Z}^n$. Tämä piste kuvautuu pisteeksi $\Lambda\bar{x}$ kappaleessa $\Lambda(\Lambda^{-1}K) = K$. $\Lambda\bar{x}$ on origosta poikkeava hilapiste hilassa Λ. Näin ollen K sisältää ainakin yhden origosta poikkeavan hilan Λ pisteen. □

3 Minkowskin toinen lause

Tässä kappaleessa esitellään ja todistetaan Minkowskin toinen lause. Minkowskin lauseita pidetään lukugeometrian – lukuteoriaa ja geometriaa yhdistävän matematiikan haaran, eng. "geometry of numbers" – peruslauseina, joista koko lukugeometria lähti käyntiin[1, s. 2]. Minkowskin ensimmäinen lause esiteltiin kappaleessa 2.4.

Minkowskin toinen lause, kuten ensimmäinenkin lause, koskee konvekseja, origon suhteen symmetrisiä kappaleita. Toisessa lauseessa kappaleen mitta ei kuitenkaan ole kiinnitetty. Sen sijaan toinen lause on muotoiltu ns. perättäisiä minimejä käyttäen (esitellään kappaleessa 3.1.1). Jos kappaleen kaikki perättäiset minimit tiedetään, sen mitalle voidaan asettaa ylä- ja alaraja.

Minkowskin toiselle lauseelle on useita todistuksia – esimerkiksi [5], [1] ja [6, s. 204] – ja yleinen konsensus on, että varsinkin lauseen varhaiset todistukset ovat pääsääntöisesti pitkiä ja vaikealukuisia.[1, s. 203][6, s. 3]. Tämän kappaleen tarkoituksena on todistaa lause verrattain helposti ymmärrettävällä päättelyllä.

3.1 Minkowskin toiseen lauseeseen liittyvää käsitteistöä

Tässä kappaleessa esitellään Minkowskin toiseen lauseeseen, sen ymmärtämiseen, ja sen todistukseen olennaisesti liittyvät käsitteet ja lauseet.

3.1.1 Perättäiset minimit

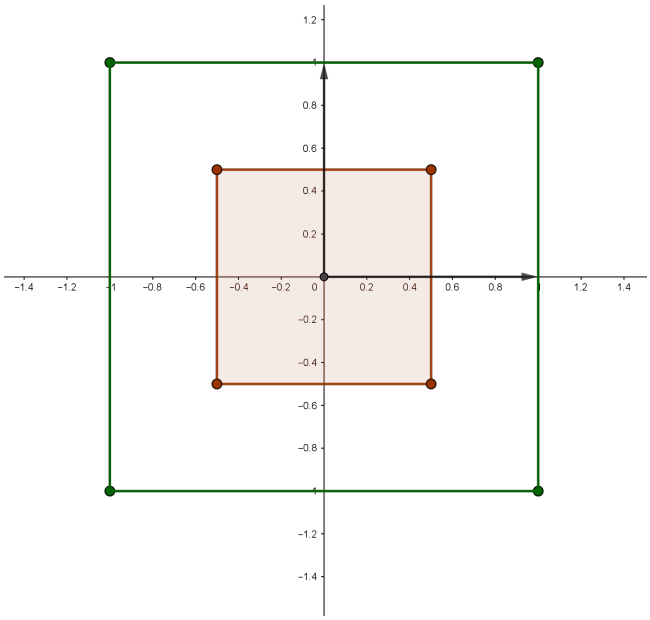
Minkowskin toinen lause tutkii, kuinka monta lineaarisesti riippumatonta hilan vektoria konveksiin ja symmetriseen kappaleeseen sisältyy, ja miten tämä luku muuttuu, kun kappaletta skaalataan lineaarisesti jollain kertoimella. Tarkemmin, Minkowskin toinen lause ei käsittele mitä tahansa kertoimia, vaan *perättäisiä minimejä* λ kappaleelle K.

Tässä kappaleessa esitellään perättäisten minimien käsite sekä käsitteeseen liittyviä hyödyllisiä apulauseita.

Määritelmä 3.1 (Perättäinen minimi)**.** *Positiivinen reaaliluku λ_n on n. perättäinen minimi kappaleelle K, jos*

- *lineaariskaalattu kappale $\lambda_n K$ sisältää ainakin n lineaarisesti riippumatonta hilan vektoria sisä- tai reunapisteinään, ja*

- *ei ole olemassa pienempää positiivista reaalilukua, jolla edellinen olisi totta.*



Kuva 1: Hilassa $\mathbb{Z}^2$ yksikköneliötä täytyy skaalata kaksinkertaiseksi, jotta se sisältäisi edes yhden hilan vektorin. Samalla se tosin tulee sisältäneeksi kaksi lineaarisesti riippumatonta hilan vektoria. Näin ollen $\lambda_1 = \lambda_2 = 2$.

Esimerkki 3.1. *Origokeskisessä yksikköneliössä* $K = [-\frac{1}{2}, \frac{1}{2}]^2$ *ja hilassa* $\mathbb{Z}^2$ *huomataan, että* $\lambda_1 = 2$*, sillä* $(1, 0) \in 2K = [-1, 1]^2$ *ja toisaalta myös* $\lambda_2 = 2$ *sillä* $(0, 1) \in 2K$*. Muita kertoimia* λ_n *ei ole, sillä hilassa* $\mathbb{Z}^2$ *ei voi olla kolmen tai useamman lineaarisesti riippumattoman vektorin jonoja.*

Lause 3.1. *Kaikkien konveksien, symmetristen, positiivismitallisten kappaleiden* K *perättäisille minimeille* λ_i *on voimassa*

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < \infty$$

missä n *on hilan dimensio.*

Lause 3.1 on yksinkertainen todistaa.

Todistus. Olkoon K symmetrinen ja konveksi kappale. Olkoon sen perättäiset minimit $\lambda_1, \ldots, \lambda_n$. Olkoon $\Lambda = \text{span}(v_1, \ldots, v_n)$ hila avaruudessa $\mathbb{R}^n$.

- $0 < \lambda_i$, sillä $0K = \{\bar{0}\}$ ja tämä joukko ei sisällä yhtään vapaata hilan vektoria.
- $\lambda_i \leq \lambda_{i+1}$ sillä kappale, joka sisältää $i + 1$ riippumatonta hilan vektoria, sisältää i riippumatonta hilan vektoria.

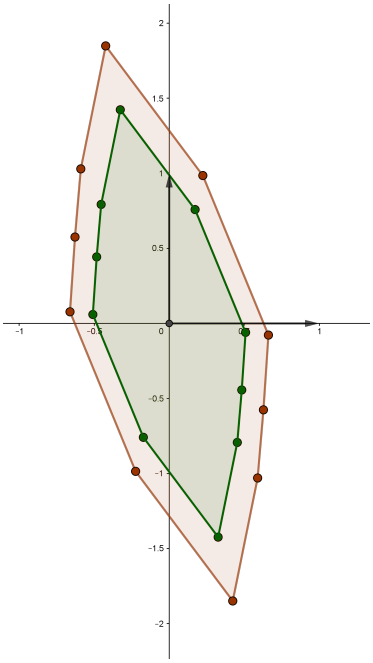
- $\lambda_i < \infty$ sillä positiivismitalliseen kappaleeseen K on sisällyttävä osajoukkona ainakin yksi avoin kuula, $B(\bar{x}, r), r > 0$. Koska K on symmetrinen, se sisältää myös kuulan $B(-\bar{x}, r)$. Toisaalta, koska K on konveksi, se sisältää siis myös origokeskeisen kuulan $K' = B(\bar{0}, r)$. Olkoon $d = \max(|v_1|, \ldots, |v_n|)$. $\frac{d}{r}K' = B(\bar{0}, d)$ sisältää kaikki hilan virittäjävektorit, joten $\frac{d}{r}K$ sisältää kaikki hilan virittäjävektorit ja täten siis ainakin n riippumatonta hilan vektoria. Näin ollen $\lambda_n \leq \frac{d}{r} < \infty$.

□

Esimerkki 3.2. *Hilassa* $\mathbb{Z}^2$ *suorakaiteen* $K = [-\frac{1}{2}, \frac{1}{2}] \times [-2, 2]$ *ensimmäinen perättäinen minimi on* $\lambda_1 = \frac{1}{2}$*, sillä* $(0, 1) \in \frac{1}{2}K = [-\frac{1}{4}, \frac{1}{4}] \times [-1, 1]$*. Suorakaiteen toinen perättäinen minimi on* $\lambda_2 = 2$*, sillä tällöin ja vasta tällöin* $(1, 0) \in \lambda_2 K = 2K = [-1, 1] \times [-4, 4]$.

Huomionarvoisesti kappaleen perättäiset minimit ovat verrannollisia sekä kappaleen kokoon että hilan rakenteeseen:

- Jos kappaleen K perättäiset minimit ovat $\lambda_1, \ldots, \lambda_n$, niin kappaleen rK perättäiset minimit ovat $\frac{\lambda_1}{r}, \ldots, \frac{\lambda_n}{r}$.
- Jos kappaleen K perättäiset minimit ovat $\lambda_1, \ldots, \lambda_n$ hilassa Λ, niin hilassa $r\Lambda$ ne ovat $r\lambda_1, \ldots, r\lambda_n$.



Kuva 2: Kuvassa mielivaltainen konveksi, origon suhteen symmetrinen kappale K (oranssi) sekä kappale $0.77K$ (vihreä). Huomataan, että $\lambda_1 = 0.77$ on pienin luku, jolla $\lambda_1 K$ sisältää ainakin yhden riippumattoman hilan $\mathbb{Z}^2$ vektorin.

Perättäisten minimien suuruus on siis kääntäen verrannollinen kappaleen kokoon ja suoraan verrannollinen hilan perussuunnikkaan kokoon. Muiden perättäisten minimien suuruuteen vaikuttavien tekijöiden voi karkeasti ottaen ajatella liittyvän kappaleen muotoon sekä hilan itsensä muotoon.

Lause 3.2. *Hilan Λ kanta $(\bar{v}_1, \ldots, \bar{v}_n)$ voidaan aina valita niin, että $\bar{v}_i \in \lambda_i K$ kaikilla indekseillä i ja kappaleilla K.*

Todistus. Todistetaan rakentamalla mielivaltaiselle kappaleelle K esimerkkikanta $(\bar{v}_1, \ldots, \bar{v}_n)$, jolle pätee $\bar{v}_i \in \lambda_i K$ kaikilla i.

Määritelmällisesti kappale $\lambda_1 K$ sisältää ainakin yhden origosta poikkeavan hilavektorin. Olkoon yksi niistä kantavektori $\bar{v}_1$.

Olkoon $(\bar{v}_1, \ldots, \bar{v}_i)$ vapaa jono joukossa $\lambda_i K$. Symmetrisyyden ja konveksisuuden nojalla $\lambda_i K \subset \lambda_{i+1} K$. Lisäksi, määritelmällisesti, $\lambda_{i+1} K$ sisältää ainakin $i+1$ riippumatonta hilapistettä. Valitaan yksi niistä, joka ei sisälly jonoon $(\bar{v}_1, \ldots, \bar{v}_i)$ kantavektoriksi $\bar{v}_{i+1}$.

Nyt on konstruoitu kanta $(\bar{v}_1, \ldots, \bar{v}_n)$, joka on vapaa, ja jonka jokaiselle jäsenelle $\bar{v}_i$ pätee, että $\bar{v}_i \in \lambda_i K$. Tämä viimeistelee todistuksen. □

Annetaan lauseessa 3.2 esitellylle kannalle nimi.

Määritelmä 3.2 (Järjestetty kanta)**.** *Kappaleen K järjestetty kanta hilassa Λ on sellainen hilan Λ kanta $V_K = (\bar{v}_1, \ldots, \bar{v}_n)$, jolla*

$$\bar{v}_i \in \lambda_i K$$

kaikilla $i \in \{1, \ldots, n\}$.

Lause 3.3. *Järjestetyn kannan hilavektori $\bar{v}_i$ on aina kappaleen $\lambda_i K$ reunapiste, eikä koskaan sisäpiste.*

Todistus. Todistetaan ristiriidalla.

Jos $\bar{v}_i$ olisi kappaleen $\lambda_i K$ sisäpiste, olisi pisteellä $\varepsilon|\bar{v}_i|$-säteinen kuulaympäristö, jonka sisällä kaikki pisteet kuuluisivat joukkoon $\lambda_i K$. Erityisesti, piste $(1+\varepsilon)\bar{v}_i$ kuuluisi joukkoon $\lambda_i K$. Kuitenkin tästä seuraa, että $\bar{v}_i \in \frac{\lambda_i}{1+\varepsilon} K$, mutta $\frac{\lambda_i}{1+\varepsilon} < \lambda_i$. Tämä taas on ristiriita, sillä kerroin λ_i on määritelmällisesti pienin kerroin, jolla $\bar{v}_i \in \lambda_i K$.

Näin ollen pisteen $\bar{v}_i$ on oltava kappaleen $\lambda_i K$ reunapiste. □

Korollaari 3.3.1. *Kaikki kappaleen $\lambda_{i+1} K$ sisäpisteet, jotka ovat hilapisteitä, ovat muotoa $n_1\bar{v}_1 + \ldots n_i\bar{v}_i$, missä $(\bar{v}_1, \ldots, \bar{v}_i)$ ovat järjestetyn kannan V_K ensimmäiset i jäsentä.*

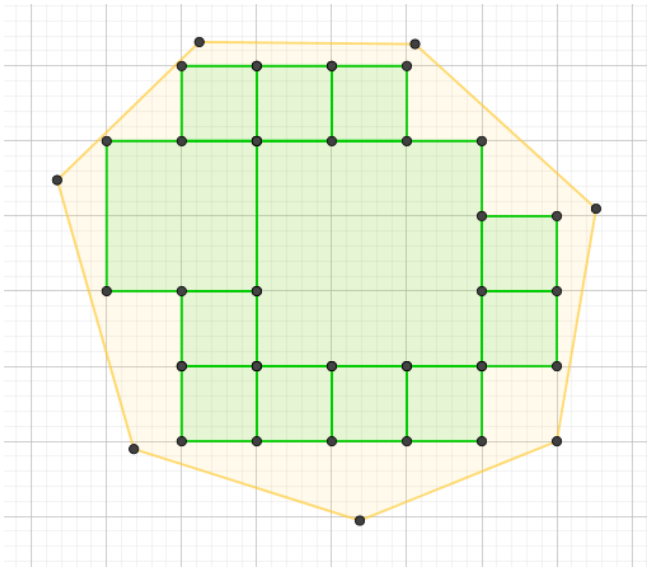
Todistus. Todistetaan ristiriidalla.

Jos $\lambda_{i+1} K$ sisältäisi sisäpisteen $\bar{x} \neq n_1\bar{v}_1 + \ldots n_i\bar{v}_i$, olisi tämä piste riippumaton vektoreista $(\bar{v}_1, \ldots, \bar{v}_i)$. Näin ollen se kelpaisi jonkun järjestetyn kannan V'_K jäseneksi $\bar{v}'_{i+1}$. Lauseen 3.3 nojalla tällainen piste ei voi olla kappaleen $\lambda_{i+1} K$ sisäpiste, mutta $\bar{x}$ on sisäpiste. Tämä on ristiriita. □

3.1.2 Jordan-sisältö

Jordan-sisältö on joillekin avaruuden $\mathbb{R}^n$ osajoukoille määritelty pseudomitta, $J : W \to \mathbb{R}, W \subset \mathbb{R}^n$. Jordan-sisällön käsite tulee olemaan myöhemmin hyödyllinen Minkowskin toisen lauseen todistuksessa. Siispä se esitellään nyt.

Jordan-sisällön perusidea on arvioida kappaleen K mittaa pilkkomalla kappale suorakulmaisiin särmiöihin ja sitten laskemalla näiden särmiöiden yhteismitta. Jordan-sisältö saadaan, kun särmiöiden koko ja täten myös arvion mittausvirhe, lähestyy nollaa.



Kuva 3: Eräs tasokuvio ja sille eräs epäsäännöllinen Jordan-alaraja-arvio.

Määritelmä 3.3 (Jordan-sisältö)**.** *Koostukoot joukot A_i leikkaamattomista suorakulmaisista särmiöistä $s = [r_1, r_1 + w_1) \times [r_2, r_2 + w_2) \times \cdots \times [r_n, r_n + w_n)$ ja olkoon $A_1 \subset A_2 \subset \cdots \subset K$. Olkoon $K = \lim_{i\to\infty} A_i$.*

Koostukoot toisaalta joukot Y_i myös suorakulmaisista särmiöistä, mutta $Y_1 \supset Y_2 \supset \cdots \supset K$ ja $\lim_{i\to\infty} Y_i = K$.

Jos kappaleelle K on olemassa sekä jono A_i että jono Y_i, jotka toteuttavat edellä mainitut ehdot, on kappaleella K olemassa Jordan-sisältö, ja tämä sisältö on

$$J(K) = \lim_{i\to\infty} |A_i| = \lim_{i\to\infty} |Y_i|$$

ja

$$|A_i| = \sum_{s\in A_i} |s|$$

missä suorakaide $s = [r_1, r_1 + w_1) \times [r_2, r_2 + w_2) \times \cdots \times [r_n, r_n + w_n)$ ja

$$|s| = w_1 \dots w_n.$$

Käytännössä Jordan-sisältö on kuin Lebesque-mitta, paitsi suppeammalla määrittelyjoukolla: Jordan-mitta on määritelty tasan niille $\mathbb{R}^n$ osajoukoille,

joiden reuna on nollamitallinen. Lisäksi Jordan-sisältö ei ole täysadditiivinen. Jordan-sisällön käsite on yhtä kaikki mielekäs, sillä se mahdollistaa tiettyjen hyödyllisten yhtälöiden muodostamisen.

3.2 Minkowskin toisen lauseen muotoilu ja todistus

Minkowskin toinen lause antaa ylä- ja alarajan konveksin ja symmetrisen kappaleen K tilavuuden ja siihen liittyvien perättäisten minimien $\lambda_1, \ldots, \lambda_n$ tulolle. Ylä- ja alaraja ovat suhteessa hilan dimensioon sekä perussuunnikkaan tilavuuteen.

Lause 3.4 (Minkowskin toinen lause)**.** *Olkoon $\Lambda \subset \mathbb{R}^n$ n-ulotteinen hila ja olkoon $K \subset \mathbb{R}^n$ suljettu, symmetrinen ja konveksi kappale. Olkoon $\lambda_1, \ldots, \lambda_n$ kappaleen K perättäiset minimit. Tällöin*

$$\frac{2^n}{n!}|\det(\Lambda)| \leq \lambda_1 \ldots \lambda_n |K| \leq 2^n |\det(\Lambda)|.$$

Tässä $|\det(\Lambda)|$ tarkoittaa hilan perussuunnikkaan mittaa. Perussuunnikkaista puhuttiin edellisen kerran kappaleessa 2.2 ja niiden mitat todistettiin yhtä suuriksi lauseessa 2.1.

Todistetaan Minkowskin toinen lause. Riittää todistaa Minkowskin toinen lause hiloille $\mathbb{Z}^n$, eli että näissä hiloissa

$$\frac{2^n}{n!} \leq \lambda_1 \lambda_2 \ldots \lambda_n |K| \leq 2^n.$$

Yleinen muoto seuraa tästä lauseen 2.4 kautta, kun kerrotaan koko epäyhtälö mielivaltaisen hilan Λ perussuunnikkaan mitalla $|\det(\Lambda)|$ ja uudelleenmerkitään $|\Lambda K| := |K|$.

Lauseen todistus on varsin pitkä, joten todistetaan lause yksi puoli kerrallaan, alakohdat erikseen otsikoituina.

3.2.1 Vasemman puolen todistus

Todistetaan ensin Minkowskin toisen lauseen vasen puoli. Tämä on työvaiheista selkeästi nopeampi ja yksinkertaisempi.

Todistus. Tarkastellaan hilaa $\mathbb{Z}^n$. Olkoon $K \subset \mathbb{R}^n$ konveksi, origon suhteen symmetrinen, suljettu kappale. Olkoon $V = (\bar{v}_1, \ldots, \bar{v}_n)$ kappaleen K järjestetty kanta.

Matriisi $L = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{bmatrix}$ kuvaa kappaleen K reunapisteet $\frac{v_1}{\lambda_1}, \ldots, \frac{v_n}{\lambda_n}$ pisteiksi $v_1, \ldots, v_n$.

Käänteismatriisi V^{-1} kuvaa vektorit $v_1, \ldots, v_n$ luonnollisen kannan vektoreiksi $e_1, \ldots, e_n$. Koska $\det(V) \in \mathbb{Z}$ niin $\det(V^{-1}) \in \frac{1}{\mathbb{Z}}$. Merkitään

$$K' = LV^{-1}K$$

ja huomataan, että tämä joukko sisältää koko luonnollisen kannan I reunapisteinään.

Huomataan, että kärkineliö ($n = 2$), oktaedri ($n = 3$), tai hyperoktaedri ($n \geq 4$), jonka kärkipisteet ovat luonnollisen kannan vektorit vastavektoreineen, on varmasti kappaleen K' osajoukko. Tällaisen säännöllisen hyperoktaedrin mitan tiedetään olevan $\frac{2^n}{n!}$.[1] Näin ollen

$$\begin{aligned}
\frac{2^n}{n!} &\leq |K'| \\
&= |LV^{-1}K|, \text{ josta lauseen 2.4 nojalla} \\
&= |\det(LV^{-1})||K| \\
&= |\det(L)||\det(V^{-1})||K| \\
&= (\lambda_1\lambda_2\dots\lambda_n)\frac{1}{z}|K|, z \geq 1 \\
&\leq \lambda_1\lambda_2\dots\lambda_n|K|.
\end{aligned}$$

Tämä viimeistelee epäyhtälön vasemman puolen.

□

3.2.2 Oikean puolen todistus

Todistetaan nyt Minkowskin toisen lauseen oikea puoli. Tämä on todistuksen vaiheista pidempi. Todistetaan oikea puoli Daninicin Jordan-sisältöä hyödyntävää todistusta[7] tiiviisti jäljitellen.

Ongelman redusoiminen Jordan-sisällön avulla Olkoon K symmetrinen ja konveksi kappale ja olkoon M jokin suuri kokonaisluku. Olkoon Λ tarkoitushakuisesti valittu hila, joka koostuu pisteistä

$$\bar{v} = \left(\frac{\lambda_1 2v_1}{M\lambda_1}, \frac{\lambda_1 2v_2}{M\lambda_2}, \dots, \frac{\lambda_1 2v_n}{M\lambda_n}\right)_V, (v_1, \dots, v_n) \in \mathbb{Z}^n$$

ja V on kappaleen K järjestetty kanta. Olkoon $N(M)$ joukon $\Lambda \cap \lambda_1 K$ alkioiden lukumäärä.

Kun tarkastellaan avaruuden laatoittavia suorakulmaisia särmiöitä, joiden keskipisteet ovat muotoa $(\frac{\lambda_1 2v_1}{M\lambda_1}, \frac{\lambda_1 2v_2}{M\lambda_2}, \dots, \frac{\lambda_1 2v_n}{M\lambda_n})$, ja jotka sisältyvät joukkoon $\lambda_1 K$, on selvää, että joukon $\lambda_1 K$ Jordan-sisältö on

$$J(\lambda_1 K) = \lim_{M\to\infty} \frac{N(M)\lambda_1^n 2^n}{M^n \lambda_1 \dots \lambda_n}.$$

Tämä arvo on toisaalta sama kuin kappaleen $\lambda_1 K$ mitta $|\lambda_1 K|$. Näin ollen

$$|\lambda_1 K| = \lambda_1^n |K| = \lim_{M\to\infty} \frac{N(M)\lambda_1^n 2^n}{M^n \lambda_1 \dots \lambda_n},$$

jolloin

$$\lim_{M\to\infty} \frac{N(M)}{M^n} = \frac{\lambda_1 \dots \lambda_n |K|}{2^n}.$$

[1] Induktiolla yhtälöparista $|O_2| = 2, |O_{n+1}| = \int_{-1}^{1}(1 - |x|)^n |O_n| dx$.

Tästä huomataan, että Minkowskin toisen lauseen oikea puoli on ekvivalentti ehdon

$$\lim_{M\to\infty} \frac{N(M)}{M^n} \leq 1$$

kanssa.

Hyvät ja huonot hilapisteet Muodostakoot kuutiot, joiden keskipisteet ovat muotoa

$$\left(\frac{\lambda_1 2v_1}{(\lambda_{i+1}-\lambda_i)M}, \ldots, \frac{\lambda_1 2v_n}{(\lambda_{i+1}-\lambda_i)M} \right), (v_1, \ldots, v_n) \in \mathbb{Z}^n$$

tesselaation T_i avaruudelle $\mathbb{R}^n$ jollain indeksillä $i \in \{1, \ldots, n-1\}$, jolla $\lambda_{i+1} - \lambda_i \neq 0$.

Olkoon tällaisen tesselaation T_i kuutio C "huono", jos se on kappaleen K reunalla, eli se sisältää pisteitä sekä kappaleesta K että sen komplementista. Olkoon tällainen kuutio "hyvä", jos sen pisteet ovat kaikki kappaleessa K, eli $C \subset K$.

Olkoon hilan Λ piste $\bar{v}$ "hyvä", jos se sisältyy hyvään kuutioon kaikissa tesselaatioissa T, ja "huono", jos se sisältyy huonoon kuutioon ainakin yhdessä tesselaatiossa T.

Erotellaan $N(M)$ tekijöihin $G(M)$ ja $B(M)$, missä $N(M) = G(M) + B(M)$ ja missä $G(M)$ on hyvien hilapisteiden Λ ja $B(M)$ huonojen hilapisteiden Λ lukumäärä. Huomataan, että lukuun $B(M)$ vaikuttavat hilapisteet ovat jatkuvasti lähempänä $\lambda_1 K$ reunaa luvun M kasvaessa rajatta, joten huonojen kuutioiden Jordan-sisältö on kappaleen K reunan mitta. Kappaleen K reunan mitta puolestaan on 0. Näin ollen

$$J(\partial K) = \lim_{M\to\infty} \frac{B(M)\lambda_1^n 2^n}{M^n \lambda_1 \ldots \lambda_n} = 0$$

joten

$$\lim_{M\to\infty} \frac{B(M)}{M^n} = 0.$$

Lisäksi, koska $N(M) = G(M) + B(M)$, niin

$$\lim_{M\to\infty} \frac{N(K)}{M^n} = \lim_{M\to\infty} \frac{G(M)}{M^n} + \frac{B(M)}{M^n} = \lim_{M\to\infty} \frac{G(M)}{M^n}.$$

Siispä Minkowskin toisen lauseen todistamiseksi riittää osoittaa, että

$$\lim_{M\to\infty} \frac{G(M)}{M^n} \leq 1.$$

Tämä tullaan osoittamaan todeksi, kun osoitetaan, että $G(M) \leq M^n$.

Hyvien pisteiden jonot $\bar{x}_i$ Olkoon

$$\bar{x}_1 = \left(\frac{\lambda_1 2x_1}{M\lambda_1}, \frac{\lambda_1 2x_2}{M\lambda_2}, \ldots, \frac{\lambda_1 2x_n}{M\lambda_n} \right) \tag{1}$$

joku hyvä piste.

Koska $\bar{x}_1$ on hyvä piste, sisältyvät kaikki sen kanssa samassa kuutiossa $C \in T_i$ olevat pisteet kappaleeseen $\lambda_1 K$.

Tällainen on esimerkiksi piste

$$\left(\frac{\lambda_1 2v_1}{(\lambda_{i+1}-\lambda_i)M},\dots\frac{\lambda_1 2v_i}{(\lambda_{i+1}-\lambda_i)M},\frac{\lambda_1 2x_{i+1}}{M\lambda_n},\dots,\frac{\lambda_1 2x_n}{M\lambda_n}\right)$$

missä $v_1,\dots,v_i$ ovat kokonaislukuja, jotka vastaavat kuution $C \in T_i$ keskipisteen $(v_1,\dots,v_n)$ ensimmäistä i. komponenttia.

Merkitään tällaisia pisteitä lyhyesti

$$\left(\frac{2\lambda_1 \bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right),$$

missä $\bar{v}_i = (v_1,\dots,v_i)$ ja $\bar{x}_i^* = (\frac{\lambda_1 2x_{i+1}}{M\lambda_n},\dots,\frac{\lambda_1 2x_n}{M\lambda_n})$.

Edellistenkaltaisten pisteiden ohella myös pisteet

$$(\bar{0}_i, \bar{x}_i^*)$$

sisältyvät joukkoon $\lambda_1 K$, jos $\lambda_{i+1}-\lambda_i = 0$.

Näin ollen hyvän pisteen $\bar{x}_1$ kaikille hännille $\bar{x}_i^*$ on olemassa ainakin yksi pää $\bar{v}_i \in \mathbb{Z}^i$, jolla

$$\left(\frac{2\lambda_1 \bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right) \in \lambda_1 K.$$

Olennaisesti $\bar{v}_i$ voidaan valita pelkän hännän $\bar{x}_i^*$ perusteella, ilman tietoa vektorin $\bar{x}_1$ päästä $(x_1,\dots,x_i)$. Siispä on olemassa funktio, joka kuvaa jokaisen hännän $\bar{x}_i^*$ joksikin tasan yhdeksi pääksi $\bar{v}_i$. Oletetaan jatkossa, että $\bar{v}_i$ on yksikäsitteinen hännän $\bar{x}_i^*$ suhteen. Tämä on ratkaisevaa alla esiteltävän yhtälön (5) todistuksen kannalta.

Määritellään nyt vektorijono $(\bar{x}_1,\dots,\bar{x}_n)$ seuraavanlaisesti:

$$\begin{aligned}\bar{x}_1 &= \left(\frac{\lambda_1 2x_1}{M\lambda_1}, \frac{\lambda_1 2x_2}{M\lambda_2},\dots,\frac{\lambda_1 2x_n}{M\lambda_n}\right)\\ \bar{x}_{i+1} &= \frac{\lambda_{i+1}}{\lambda_i}\left(\frac{\lambda_i}{\lambda_{i+1}}\bar{x}_i + \frac{\lambda_{i+1}-\lambda_i}{\lambda_{i+1}}\cdot\frac{\lambda_i}{\lambda_1}\left(\frac{2\lambda_1\bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right)\right)\end{aligned}$$

Määritelmästä voidaan nähdä, että kukin $\bar{x}_i$ kuuluu indeksiään vastaavaan kappaleeseen $\lambda_i K$: Todistettavasti

$$\left(\frac{2\lambda_1 \bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right) \in \lambda_1 K.$$

Siispä

$$\frac{\lambda_i}{\lambda_1}\left(\frac{2\lambda_1 \bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right) \in \lambda_i K.$$

Induktio-olettamalla $\bar{x}_i \in \lambda_i$ joten painotettu keskiarvo

$$\left(\frac{\lambda_i}{\lambda_{i+1}}\bar{x}_i + \frac{\lambda_{i+1}-\lambda_i}{\lambda_{i+1}}\cdot\frac{\lambda_i}{\lambda_1}\left(\frac{2\lambda_1\bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right)\right) \in \lambda_i K,$$

ja näin ollen

$$\frac{\lambda_{i+1}}{\lambda_i}\left(\frac{\lambda_i}{\lambda_{i+1}}\bar{x}_i + \frac{\lambda_{i+1}-\lambda_i}{\lambda_{i+1}}\cdot\frac{\lambda_i}{\lambda_1}\left(\frac{2\lambda_1\bar{v}_i}{(\lambda_{i+1}-\lambda_i)M}, \bar{x}_i^*\right)\right) \in \lambda_{i+1} K.$$

Lisäksi seuraavat lauseet seuraavat määritelmästä joko suoraan tai nopeasti induktiolla:

$$\bar{x}_{i+1} = \bar{x}_i + \left(\frac{2\bar{v}_i}{M}, \frac{(\lambda_{i+1} - \lambda_i)\bar{x}_i^*}{\lambda_1}\right) \tag{2}$$

$$\bar{x}_i = \left(\frac{2x_1}{M}, \ldots, \frac{2x_i}{M}, \frac{\lambda_i 2x_i}{\lambda_{i+1}M}, \ldots, \frac{\lambda_i 2x_n}{\lambda_n M}\right) + \frac{2}{M}\left(\bar{v}_1 + \cdots + \bar{v}_{i-1}\right) \tag{3}$$

$$\bar{x}_n = \frac{2}{M}\left(\bar{x}_1 + \bar{v}_1 + \cdots + \bar{v}_{n-1}\right) \tag{4}$$

$$\bar{x}_{i+1} = \bar{y}_{i+1} \Rightarrow \bar{x}_i = \bar{y}_i \tag{5}$$

Näissä yhtälöissä vektorien $\bar{v}_i$ puuttuvat komponentit tulkitaan nolliksi.

Ekvivalenssiluokat $[k_1, \ldots, k_n]_M$ Osoitetaan nyt, että kullekin ekvivalenssiluokalle $[k_1, \ldots, k_n]_M \in \mathbb{Z}^n/M\mathbb{Z}^n$ on olemassa enintään yksi $\frac{M}{2}\bar{x}_n$, joka kuuluu luokkaan, eli että

$$\frac{M}{2}\bar{x}_n \equiv \frac{M}{2}\bar{y}_n \mod M \Rightarrow \bar{x}_1 = \bar{y}_1. \tag{6}$$

Jos näin on, niin myös hyviä pisteitä $\bar{x}_1$ on enintään yksi per ekvivalenssiluokka, jolloin $G(M) \leq M^n$ ja todistus on valmis.

Tiedetään $\bar{x}_1$ määrittelevästä yhtälöstä (1) sekä yhtälöstä (4), että jokainen $\frac{M}{2}\bar{x}_n$ on kokonaislukuvektori, joten jokainen tällainen vektori kuuluu johonkin ekvivalenssiluokista.

Olkoon vektorit $\bar{x}_n, \bar{y}_n \in \lambda_n K$ joitain hyviä pisteitä $\bar{x}_1$ ja $\bar{y}_1$ vastaavia lukujonojen viimeisiä jäseniä ja olkoon

$$\frac{M}{2}\bar{x}_n \equiv \frac{M}{2}\bar{y}_n \mod M.$$

Tällöin

$$\bar{z} = \frac{\bar{x}_n - \bar{y}_n}{2}$$

on piste joukossa $\lambda_n K$ ja hilassa $\mathbb{Z}^n$. Pisteet $\bar{x}_n$ ja $\bar{y}_n$ sisältyvät kummatkin johonkin $\lambda_n K$ hyvistä kuutioista, joten ne eivät voi olla reunapisteitä. Siispä myöskään $\bar{z}$ ei ole reunapiste. Tämä tarkoittaa lauseen 3.3.1 nojalla, että vektorin $\bar{z}$ viimeinen komponentti z_n on 0.

Toisaalta $z_n = \frac{x_n - y_n}{2}$ sillä vektoreilla $(\bar{v}_1, \ldots, \bar{v}_{n-1})$ ei ole n. komponenttia. Siispä $x_n = y_n$. Mutta tämä tarkoittaa, että $\bar{x}_{n-1}^* = \bar{y}_{n-1}^*$ jolloin yhtälön (5) nojalla myös $\bar{v}_{n-1} = \bar{w}_{n-1}$, missä siis $\bar{w}_{n-1}$ on vastaavanlainen hilavektori kuin $\bar{x}_n$ hilavektori $\bar{v}_n$. Tästä taas on helppo nähdä, että

$$z_{n-1} = \frac{x_{n-1} + v_{n-1,n-1} - y_{n-1} - w_{n-1,n-1}}{2} = \frac{x_{n-1} - y_{n-1}}{2} = 0$$

eli myös $x_{n-1} = y_{n-1}$.

Nyt taas on helppo nähdä induktiivisesti, että päättelyketjun jatkaminen johtaa siihen, että $x_j = y_j$ kaikilla j, jolloin siis $\bar{x}_1 = \bar{y}_1$. Näin on todistettu yhtälö (6).

Yhtälön (6) nojalla jokaiselle ekvivalenssiluokalle $[k_1, \ldots, k_n] \in \mathbb{Z}^n/M\mathbb{Z}^n$ on olemassa enintään yksi hyvä piste $\bar{x}_1$. Ekvivalenssiluokkia taas on tasan M^n kappaletta. Siispä

$$G(M) \leq M^n.$$

Tästä taas seuraa

$$\lim_{M\to\infty} \frac{G(M)}{M^n} \leq 1$$

mistä seuraa Minkowskin toisen lauseen oikea puoli. □

3.2.3 Todistuksen viimeistely

On todistettu, että hiloissa $\mathbb{Z}^n$ pätee $\frac{2^n}{n!} \leq \lambda_1\lambda_2\ldots\lambda_n|K|$ ja toisaalta $\lambda_1\lambda_2\ldots\lambda_n|K| \leq 2^n$. Siispä

$$\frac{2^n}{n!} \leq \lambda_1\lambda_2\ldots\lambda_n|K| \leq 2^n.$$

Vastaavalla argumentilla kuin Minkowskin ensimmäisen lauseen todistuksessa (kappaleessa 2.4) tämäkin lause yleistyy mille tahansa hilalle isomorfismin kautta. Yleiselle hilalle Λ lause muuttuu muotoon

$$\frac{2^n}{n!}|\det(\Lambda)| \leq \lambda_1\ldots\lambda_n|K| \leq 2^n|\det(\Lambda)|.$$

Tämä viimeistelee Minkowskin toisen lauseen todistuksen. □

4 Erityinen hila: Gaussin kokonaisluvut ja ympyräongelma

Tässä luvussa tarkastellaan hilan erityistapausta, Gaussin kokonaislukuja, joka mallina yhdistää hilan omainaisuudet joihinkin kompleksitason algebrallisiin ominaisuuksiin.

Gaussin kokonaisluvut on hila kompleksitasossa.

Määritelmä 4.1. *Gaussin kokonaisluvut on joukko $\mathbb{Z}[i]$, missä*

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Toinen yhtäpitävä muotoilu on, että Gaussin kokonaisluvut on hila $\mathbb{Z}^2$ mutta varustettuna kompleksitulolla. Kompleksitulo ei ole tässä kappaleessa erityisen tärkeä työkalu, mutta se on olennainen ympyräongelmaan läheisesti liittyvän aiheen, *Gaussin alkulukujen*, tarkastelussa. Myöhemmin tässä työssä kompleksituloa käytetään kappaleessa 6.4 Leech-hilan määritelmän yhteydessä.

Ympyräongelma on Gaussin kokonaislukuihin liittyvä ongelma, joka kysyy, kuinka monta hilan $\mathbb{Z}[i]$ pistettä sisältyy origokeskeiseen suljettuun kuulaan, jonka säde on $r \in \mathbb{R}_{\geq 0}$. Toisin sanottuna, kuinka monta Gaussin kokonaislukua $z = a + bi$ on, joilla

$$|z| = a^2 + b^2 \leq r^2.$$

Hilapisteiden määrän r-säteisessä ympyrässä ilmoittaa funktio $N : \mathbb{R} \to \mathbb{N}$.

Esimerkki 4.1. *Lasketaan $N(\sqrt{14})$. Ratkaistaan etsimällä kaikki ne pisteet*

(x, y) *joilla* $x^2 + y^2 \leq 14$. *Tehdään taulukko:*

x	*suotuisat* y	*hilapisteiden lukumäärä sarakkeessa*
-4		0
-3	$-2, -1, 0, 1, 2$	5
-2	$-3, \ldots, 3$	7
-1	$-3, \ldots, 3$	7
0	$-3, \ldots, 3$	7
1	$-3, \ldots, 3$	7
2	$-3, \ldots, 3$	7
3	$-2, -1, 0, 1, 2$	5
4		0

Siispä, nopean yhteenlaskun jälkeen, on selvitetty, että $N(\sqrt{14}) = 45$.

Vaikuttaisi, että $N(r) \approx \pi r^2$. Itse asiassa, jos palautetaan mieleen Jordan-sisällön määritelmä (esitelty kappaleessa 3.1.2), niin likiarvo on ilmeinen: Muodostetaan Jordan-sisältö niistä $\frac{1}{r} \times \frac{1}{r}$-neliöistä, joiden keskipisteet kuuluvat hilaan $\frac{1}{r}\mathbb{Z}[i]$ ja joiden keskipiste sisältyy yksikköympyrään. Tällaisten neliöiden lukumäärä olkoon $N'(r)$. Nyt raja-arvo

$$\lim_{r\to\infty} \frac{N'(r)}{r^2}$$

määrittää yksikköympyrän Jordan-sisällön, eli

$$\lim_{r\to\infty} \frac{N'(r)}{r^2} = \pi \cdot 1^2.$$

Huomataan lisäksi määritelmiä tarkastelemalla, että $N(r) = N'(r)$ kaikilla r, jolloin siis

$$\lim_{r\to\infty} \frac{N(r)}{r^2} = \pi \cdot 1^2$$

ja tämä yhtälö voidaan edelleen muokata muotoon

$$\lim_{r\to\infty} \frac{N(r) - \pi r^2}{r^2} = 0.$$

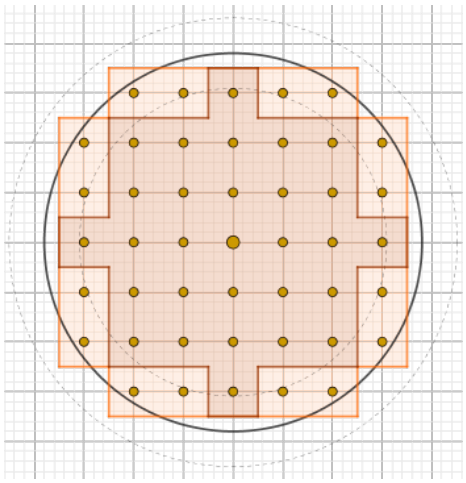
Näin ollen, jos määritellään, että "virhefunktio" $\varepsilon(r) := N(r) - \pi r^2$, niin huomataan välittömästi, että tämä funktio kasvaa hitaammin kuin yksikään toisen asteen polynomi. Asymptoottinotaatiolla: $\varepsilon(r) = o(r^2)$. Tämä virhetermin verrattain hidas kasvu taas perustelee likiarvon $N(r) \approx \pi r^2$.

Virhetermin kasvunopeuden ylärajaa on mahdollista kaventaa osoittamalla, että ε kasvaa ja pienenee enintään lineaarisesti; että $\varepsilon(r) = \Theta(r)$.

Lause 4.1. *Kun* $N(r) = \pi r^2 + \varepsilon(r)$, *niin* $|\varepsilon(r) - \frac{\pi}{2}| < \pi\sqrt{2}r$.

Todistetaan lause 4.1.

Todistus. Olkoon r-säteisen, origonkeskeisen suljetun kuulan $B(r)$ sisäpisteet avaruudessa $\mathbb{Z}[i]$ pisteet $G(r)$ ja $N(r) = |G(r)|$.



Kuva 4: Ympyrän sisältämien hilapisteiden lukumäärä on sama kuin hilapisteiden määräämien yksikköneliöiden yhteispinta-ala. Osa näistä neliöistä on kokonaan ympyrän sisällä, toiset osittain sisällä ja osittain ulkopuolella. Yksikään neliö ei voi olla kokonaan ympyrän ulkopuolella.

Huomataan, että joukon $G(r)$ pisteiden lukumäärä on sama kuin joukon $H(r)$ pinta-ala avaruudessa $\mathbb{C}$, kun määritellään, että joukko $H(r)$ koostuu tasan niistä yksikköneliöistä, joiden keskipisteet sisältyvät joukkoon $G(r)$.

Koska $|H(r)|_{\mathbb{R}^2} = |G(r)|_{\mathbb{Z}[i]} = N(r)$, on joukon $H(r)$ pinta-alan ylä- ja alaraja-arviot samalla funktion N ylä- ja alaraja-arvioita.

Huomataan, että kunkin yksikköneliön kukin piste on enintään etäisyyden $\sqrt{\frac{1}{2}}$ päässä keskipisteestään.

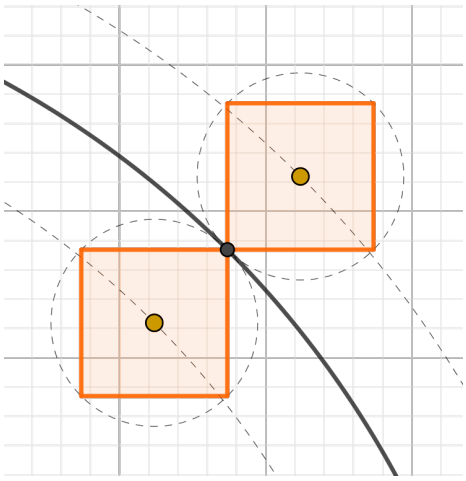
Näin ollen origoa lähin neliö, joka ei ole yksikään joukon $H(r)$ neliöistä, voi olla origosta alimmillaan etäisyyden $r - \sqrt{\frac{1}{2}}$ päässä. Jos neliö olisi yhtään lähempänä origoa, olisi sen keskipiste vääjäämättä kuulan $B(r)$ sisällä, jolloin piste kuuluisi yhteen neliöistä $H(r)$. Tämä taas on ristiriita.

Vastaavasti origosta kauimmaisin piste, joka kuuluu ainakin yhteen neliöistä $H(r)$, on enintään etäisyyden $r + \sqrt{\frac{1}{2}}$ päässä origosta. Jälleen, jos neliön kauimmaisin piste olisi origosta yhtään kauempana, olisi neliön keskipiste kuulan $B(r)$ ulkopuolella.

Näistä päättelyistä seuraa, että

$$B(r - \sqrt{\frac{1}{2}}) \subset H(r) \subset B(r + \sqrt{\frac{1}{2}}).$$

Tähän puolestaan voidaan soveltaa tunnettuja pinta-alakaavoja, ja päätyä



Kuva 5: Yksikköneliö, jonka keskipisteen etäisyys ympyrän keskipisteestä on enintään $r - \sqrt{\frac{1}{2}}$ on varmasti kokonaan ympyrän sisällä. Vastaavasti yksikköneliö, jonka keskipisteen etäisyys ympyrän keskipisteestä on ainakin $r+\sqrt{\frac{1}{2}}$ on varmasti kokonaan ympyrän ulkopuolella.

ylä- ja alaraja-arvioihin pinta-alalle $|H(r)|$:

$$\begin{aligned} B(r-\sqrt{\frac{1}{2}}) \quad &\subset H(r) \subset B(r+\sqrt{\frac{1}{2}}) \\ \Rightarrow |B(r-\sqrt{\frac{1}{2}})| &\leq |H(r)| \leq |B(r+\sqrt{\frac{1}{2}})| \\ \Rightarrow \pi(r-\sqrt{\frac{1}{2}})^2 &\leq |H(r)| \leq \pi(r+\sqrt{\frac{1}{2}})^2. \end{aligned}$$

Muistetaan nyt, että $|H(r)| = |G(r)| = N(r) = \pi r^2 + \varepsilon(r)$ ja sijoitetaan:

$$\begin{aligned} \pi(r-\sqrt{\frac{1}{2}})^2 \leq |H(r)| \quad &\leq \pi(r+\sqrt{\frac{1}{2}})^2 \\ \pi r^2 - \pi\sqrt{2}r + \frac{\pi}{2} \leq \pi r^2 + \varepsilon(r) &\leq \pi r^2 + \pi\sqrt{2}r + \frac{\pi}{2} \\ -\pi\sqrt{2}r \leq \varepsilon(r) - \frac{\pi}{2} \quad &\leq +\pi\sqrt{2}r \\ |\varepsilon(r) - \frac{\pi}{2}| &\leq \pi\sqrt{2}r. \end{aligned}$$

Tämä päättelyketju viimeistelee todistuksen.

□

Yleistys useampaan ulottuvuuteen Gaussin ympyräongelma voidaan yleistää useampaan ulottuvuuteen. Näissä avaruuksissa kysymyksen muotoilu on, kuinka monta kokonaislukujonoa $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ on olemassa, joilla

$$x_1^2 + \cdots + x_n^2 \leq r^2$$

jollain annetulla säteellä r.

Yleistetylle ongelmalle pätee sama päättely kuin perustapauksessakin, eli että $N(r) \approx |B(r)|$, missä n-ulotteisen kuulan mitta $|B(r)|$ tiedetään olevan

$$|B(r)| = \frac{\pi^{\frac{n}{2}}}{(\frac{n}{2})!} r^n$$

ja missä $(\frac{n}{2})!$ tarkoittaa Bernoullin gammafunktion arvoa $\Gamma(\frac{n}{2}+1)$ kun n on pariton.

Lisäksi näissäkin avaruuksissa on mahdollista rajata yksikkökuutiopäättelyllä, että

$$|B(r - \frac{1}{2}\sqrt{n})| \leq |H(r)| \leq |B(r + \frac{1}{2}\sqrt{n})|$$

missä luonnollisesti $\frac{1}{2}\sqrt{n}$ on n-ulotteisen yksikkökuution lävistäjän puolikas ja kaksoisepäyhtälön todistus yleistyy suoraan alkuperäisestä todistuksesta.

On myös selvää, että näissä avaruuksissa $\varepsilon(r) = \Theta(r^{n-1})$, sillä ε minorantti ja majorantti,

$$m(r) = |B(r \pm \sqrt{\frac{1}{2}})| - |B(r)|,$$

ovat molemmat $n-1$ asteen polynomifunktioita.

5 Diofanttinen approksimaatio

Tässä kappaleessa esitellään diofanttisen approksimaation käsite sekä aihealueeseen liittyviä tärkeitä lauseita.

5.1 Diofanttinen approksimaatio käsitteenä

Diofanttinen approksimaatio on lukuteorian aihealue, joka tutkii reaalilukujen rationaalilikiarvoja, ja kuinka tarkkoja likiarvot voivat olla, kun rationaaliarvioita rajoitetaan erilaisin kriteerein.

Tällaisten ongelmien ohella diofanttisen approksimaation alle luokitellaan kaikki sellaiset ongelmat, jotka yleistävät edellisenkaltaisia ongelmia esimerkiksi useaan ulottuvuuteen tai ovat muuten luonteeltaan hyvin samanhenkisiä.

Tässä kappaleessa esitellään joitain diofanttisen approksimaation lauseita sekä näiden todistukset.

5.2 Dirichlet'n approksimaatiolause

Dirichlet'n approksimaatiolause on yksi diofanttisen approksimaation hyödyllisimpiä lauseita. Dirichlet'n approksimaatiolause on reaalilukuja r, näiden rationaaliapproksimaatioita $\frac{p}{q}$ ja reaalisia apumuuttujia $R \geq 1$ koskeva lause. Lause todistaa, että kullekin reaaliluvulle on olemassa joitain erityisen hyviä rationaalilikiarvoja.

Lause 5.1 (Dirichlet'n approksimaatiolause)**.** *Kaikilla reaaliluvuilla r ja kaikilla apumuuttujilla $R \geq 1$ on olemassa lukupari (p, q), jolla*

$$1 \leq q \leq R \text{ ja } |qr - p| < \frac{1}{R}.$$

Lauseesta seuraa muun muassa, että kaikilla reaaliluvuilla r on olemassa äärettömän monta lukuparia (p, q) joilla

$$|r - \frac{p}{q}| < \frac{1}{q^2}.$$

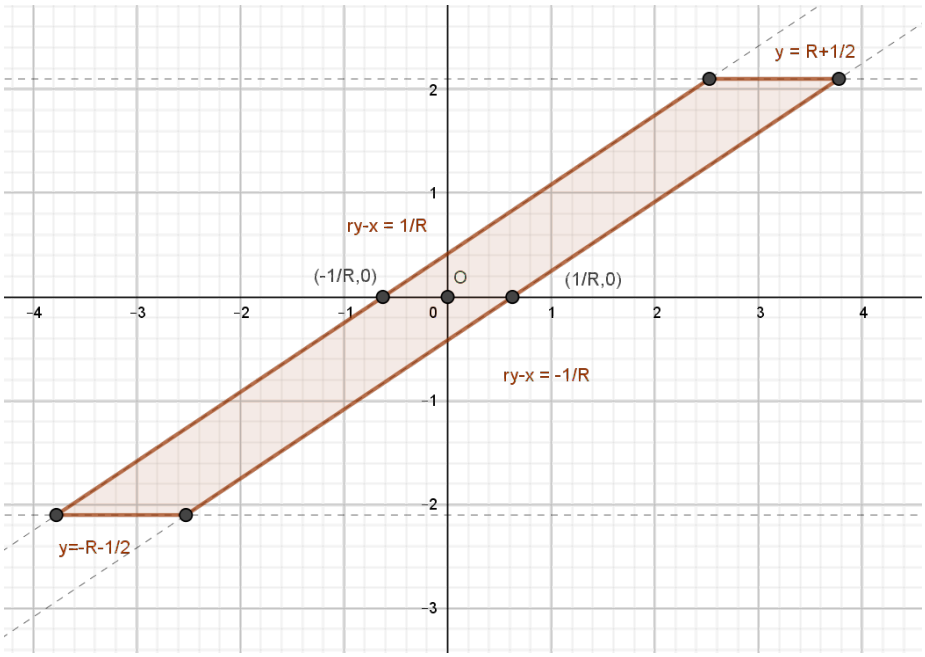
Tällaisia lukuja $\frac{p}{q}$ kutsutaan luvun r *konvergenteiksi*.

Todistetaan Dirichlet'n approksimaatiolause.

Todistus lauseelle 5.1. Olkoon

$$S_\varepsilon = \left\{ (x, y) \in \mathbb{R}^2; |y| < R + \varepsilon, |ry - x| < \frac{1}{R} \right\}, \varepsilon > 0.$$

Tämä joukko on origon suhteen symmetrinen avoin suunnikas. Suunnikas ra-



Kuva 6: Joukko S_ε on origon suhteen symmetrinen suunnikas. Tässä esimerkissä $\varepsilon = \frac{1}{2}$.

jautuu ylä- ja alapuolelta suoriin $y = -R - \varepsilon$ ja $y = R + \varepsilon$. Siispä sen korkeus on $2R + 2\varepsilon$. Suunnikas rajautuu vasemmalta ja oikealta suoriin $ry - x = \frac{1}{R}$ ja $ry - x = -\frac{1}{R}$. Suunnikkaan leveys on siis $2/R$. Suunnikkaan ala on

$$|S_\varepsilon| = (2R + 2\varepsilon)\frac{2}{R} = 4 + \frac{4\varepsilon}{R}.$$

Olennaisesti $|S| > 4$ kaikilla $\varepsilon > 0$, jolloin Minkowskin ensimmäisen lauseen (esitelty kappaleessa 2.4) nojalla jokainen S_ε sisältää ainakin yhden origosta poikkeavan hilapisteen vastavektoreineen sisäpisteenään. Koska joukot S_ε ovat toistensa osajoukkoja, ainakin yksi näistä hilapistepareista on yhteinen jokaiselle näistä joukoista.

Olkoon (p, q) kaikille joukoille S_ε yhteinen, origosta poikkeava hilapiste, jolla $q \geq 0$.

Koska $(p, q) \in S_\varepsilon$ kaikilla ε, se toteuttaa määritelmällisesti yhtälön $|qr - p| < \frac{1}{R}$.

Toiseksi $q \neq 0$, sillä origon $1/R$-säteinen kuulaympäristö ei voi sisältää yhtään toista hilapistettä mutta jana $\{(x, y); y = 0\} \cap S_\varepsilon$ on tämän ympäristön aito osajoukko.

Kolmanneksi $q \leq R$. Jos q olisi yhtään suurempi, olisi olemassa ε, jolla $(p, q) \notin S_\varepsilon$.

Näin on todistettu, että

$$|qr - p| < \frac{1}{R}$$

jollain p ja q, $1 \leq q \leq R$.

Tämä viimeistelee todistuksen.

□

5.3 Dirichlet'n approksimaatiolauseen yhtäaikainen versio

Dirichlet'n approksimaatiolauseesta on olemassa versio, joka sanoo, että äärelliselle joukolle reaalilukuja $r_1, \ldots, r_n$ on olemassa nimittäjä q jota jälleen rajoittaa apumuuttuja R, ja tämän nimittäjän omaavat rationaaliluvut arvioivat kutakin näistä reaaliluvuista kohtalaisen hyvin.

Lause 5.2. *Kullekin äärelliselle lukujonolle $(r) = (r_1, \ldots, r_n) \in \mathbb{R}^n$ ja apumuuttujalle $R \geq 1$ on olemassa yhteinen nimittäjä $q \in \mathbb{Z}_+$ ja osoittajat $(p_1, \ldots, p_n) \in \mathbb{Z}^n$, joilla*

$$1 \leq q \leq R \text{ ja } |qr_i - p_i| < \sqrt[n]{\frac{1}{R}} \text{ kaikilla } i \in \{1, \ldots, n\}.$$

Riittäköön todeta, että tämän lauseen todistus yleistyy suoraan lauseen 5.1 todistuksesta kun tarkastellaan hypersuunnikasta

$$T_\varepsilon = \left\{ (x_1, \ldots, x_n, y); |y| < R + \varepsilon, |r_i y - x_i| < \sqrt[n]{\frac{1}{R}} \right\}, \varepsilon > 0$$

ja tehdään vastaavanlaiset päättelyt kuin edellä.

5.4 Lineaarimuodot

Lineaarimuodot ovat lineaarifunktioita vektoriavaruudelta reaaliluvuille, eli lyhyesti funktiot muotoa $L : V \to \mathbb{R}$. Diofanttisen approksimaation kontekstissa lineaarimuodot ovat useimmiten reaalioperaatioita $L : \mathbb{R}^n \to \mathbb{R}$. Kaikki tällaiset lineaarimuodot on mahdollista ilmoittaa pistetulolla muodossa $L(\bar{x}) = \bar{r} \cdot \bar{x}$ jollain $\bar{r} \in \mathbb{R}^n$. Todistetaan tämä väittämä.

Todistus. Olkoon $L : \mathbb{R}^n \to \mathbb{R}$ lineaarimuoto ja olkoon $\bar{x} = x_1\bar{e_1} + \cdots + x_n\bar{e_n} \in \mathbb{R}^n$. Nyt

$$\begin{aligned} L(\bar{x}) &= L(x_1\bar{e_1} + \cdots + x_n\bar{e_n}) \\ &= L(x_1\bar{e_1}) + \cdots + L(x_n\bar{e_n}) \\ &= x_1L(\bar{e_1}) + \cdots + x_nL(\bar{e_n}) \\ &= (L(\bar{e_1}), \ldots, L(\bar{e_n})) \cdot \bar{x} \qquad\qquad |\bar{r} := (L(\bar{e_1}), \ldots, L(\bar{e_n})) \\ &= \bar{r} \cdot \bar{x} \end{aligned}$$

millä tahansa valinnalla $\bar{x} \in \mathbb{R}^n$ ja millä tahansa valinnalla $L \in \mathfrak{L}(\mathbb{R}^n \to R)$. Siispä kaikki lineaarimuodot, jotka ovat reaalioperaatioita, voidaan ilmoittaa pistetulomuodossa. □

Lineaarimuodot esiintyvät useissa diofanttisen approksimaation ongelmissa. Esitellään yksi tällaisista ongelmista kappaleessa 5.5.

5.5 Lause reaalivektoreiden ja hilavektorien pistetuloista

On todistettavissa, että kaikille reaalivektoreille $\bar{r} \in \mathbb{R}^n$ on olemassa hilavektori $\bar{q} \in \mathbb{Z}^n$, joka varmistaa, että vektorien pistetulo on lähellä jotain kokonaislukua $p \in \mathbb{Z}$. Kaukaa origosta on mahdollista löytää parempia hilavektoreita kuin origon läheltä. Ilmaistaan lause seuraavaksi eksaktisti:

Lause 5.3. *Kaikilla reaalivektoreilla $\bar{r} \in \mathbb{R}^n$ ja suorakulmaisilla hilasärmiöillä $H = [-h_1, h_1] \times \cdots \times [-h_n, h_n] \subset \mathbb{R}^n; h_1, \ldots, h_n \in \mathbb{Z}_+$ on olemassa hilapiste $\bar{q} \in H$ ja kokonaisluku $p \in \mathbb{Z}$, jolla*

$$|\bar{r} \cdot \bar{q} - p| < \frac{1}{h_1 \ldots h_n}.$$

Huomataan, että lauseen yksiulotteinen erikoistapaus on Dirichlet'n approksimaatiolause.

Tämä lause on esitelty hieman eri muodossa mm. teoksessa *Diophantine Analysis*, jossa se esitellään todistuksineen "tyyppiesimerkkinä (lauseesta) lineaarimuotojen teoriassa"[8, s. 133].

Todistetaan lause seuraavaksi. Todistus mukailee edellämainitun teoksen todistusta.

Todistus. Olkoon $\bar{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$ ja $h_1, \ldots, h_n \in \mathbb{Z}_+^n$. Olkoon matriisi

$$L = \begin{bmatrix} -1 & r_1 & \ldots & r_{n-1} & r_n \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}.$$

Huomataan, että $|\det(L)| = |-1| = 1$. Olkoon edelleen suuntaissärmiö C joukko

$$C = \left\{ (t, x_1, \ldots, x_n) \in \mathbb{R}^{n+1} : \begin{array}{r} |-t + r_1x_1 + \cdots + r_{n-1}x_{n-1} + r_nx_n| < \frac{1}{h_1 \ldots h_n} \\ |x_i| < h_i + \frac{1}{2}, i \in \{1, \ldots, n\} \end{array} \right\}.$$

Tällöin joukko LC, eli

$$LC = \left\{ \begin{bmatrix} -t + r_1 x_1 + \cdots + r_{n-1} x_{n-1} + r_n x_n \\ x_1 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} : \cdots \right\}$$

on suorakulmainen särmiö. Selkeästi suorakulmainen särmiö on konveksi ja symmetrinen origon suhteen. Tämän suorakulmaisen särmiön mitta on myös helppo laskea:

$$|LC| = \frac{2}{h_1 \dots h_n} \cdot 2(h_1 + \frac{1}{2}) \dots 2(h_{n-1} + \frac{1}{2}) \cdot 2(h_n + \frac{1}{2}) > 2^{n+1}.$$

Koska $|\det(L)| = 1$ myös $|C| > 2^{n+1}$.

Kaikesta edellisestä seuraa, Minkowskin ensimmäisen lauseen nojalla, että C sisältää varmasti ainakin yhden origosta poikkeavan hilapisteen $(p, \bar{q}) \in \mathbb{Z}^{n+1}$. Joukkoa määrittelevistä ehdoista seuraa, että tämä piste ei voi olla $(p, \bar{0})$ millään $p \neq 0$. Siispä $\bar{q} \neq \bar{0}$. Yhtä ilmeistä on, että $|q_i| \leq h_i$ kaikilla i.

Näin ollen on todistettu, että olemassa ainakin yksi $p \in \mathbb{Z}$ ja hilavektori $\bar{q} \in \mathbb{Z}^n \backslash \{0\}$, jolla $|-p + r_1 q_1 + \cdots + r_{n-1} q_{n-1} + r_n q_n| = |\bar{r} \cdot \bar{q} - p| < \frac{1}{h_1 \dots h_n}$ ja $|q_i| \leq h_i$ kaikilla $i \in \{1, \dots, n\}$.

Tämä viimeistelee todistuksen. □

5.5.1 Ratkaisujen äärettömyydestä

Lause osoittaa, että kullekin reaalivektorille on olemassa ainakin yksi verrattain pieni hilavektori, jonka pistetulo reaalivektorin kanssa on yhtä kaikki lähellä kokonaislukua. Ratkaisuja voi toki olla useampi: Luonnollisesti kullekin p ja $\bar{q}$ myös $-p$ ja $-\bar{q}$ on ratkaisu, mutta myös muut moninkerrat tai kokonaan riippumattomat hilavektorit voivat toteuttaa lauseen ehdon.

On ilmeistä, että jos epäprimitiivinen vektori $(mp, m\bar{q}), m > 1$ toteuttaa lauseen, niin myös primitiivi $(p, \bar{q})$, missä $\gcd(p, \bar{q}) = 1$, toteuttaa lauseen.

On myös ilmeistä, että kun särmiön H mitta kasvaa rajatta, myös ratkaisujen määrä kasvaa rajatta. Vähemmän ilmeistä on, että myös primitiivisten ratkaisujen määrä kasvaa rajatta. Tämä on kuitenkin todistettavissa.

Korollaari 5.3.1. *Lauseella 5.3 on äärettömän monta primitiivistä ratkaisua $(p, \bar{q})$, kun särmiön H annetaan kasvaa rajatta.*

Todistus. Todistetaan ristiriidalla. Oletetaan, että primitiivisiä ratkaisuja $(p, \bar{q})$ epäyhtälöryhmälle $|\bar{r} \cdot \bar{q} - p| < \frac{1}{h_1 \dots h_n}, |q_i| \leq h_i$ on olemassa vain äärellinen määrä jollekin reaalivektorille $\bar{r}$. Tällöin on olemassa paras approksimaatiotarkkuus $\frac{1}{h} := \frac{1}{h_1 \dots h_n} > 0$, johon primitiivivektorit yltävät.

Olkoon nyt $(\hat{p}, \hat{q})$ ratkaisu, joka yltää parempaan tarkkuuteen $\frac{1}{k} := \frac{1}{k_1 \dots k_n} < \frac{1}{h}$. Lauseen 5.3 nojalla tällainen ratkaisu on myös varmasti olemassa.

Jos tämä uusi ratkaisu $(\hat{p}, \hat{q})$ tarkkuudelle $\frac{1}{k}$ on epäprimitiivinen, on myös ratkaisua vastaava primitiivi yhtä kaikki myös ratkaisu ja sen tarkkuus on myös

ainakin $\frac{1}{k}$. Kuitenkin kaikkien primitiivisten ratkaisujen piti olla parhaimmillaan tarkkuutta $\frac{1}{h}$. Tämä puolestaan on ristiriita.

Siispä primitiivisiä ratkaisuja on oltava äärettömän monta. □

5.5.2 Korollaari alarajoista

Kun arvioitava vektori $\bar{r}$ lauseessa 5.3 on hilapiste, on ilmiselvästi olemassa sellaiset $p, \bar{q}$, joilla $|\bar{r} \cdot \bar{q} - p| = 0$. Kuitenkin muissa tapauksissa, kuten esimerkiksi silloin kun $\bar{r}$ sisältää irrationaalikomponentteja, tällaisia vakioita ei välttämättä ole olemassa.[8, s. 137]

Korollaari 5.3.2. *Kun on olemassa vakiot $c, \varepsilon > 0$, joilla*

$$|\bar{r} \cdot \bar{q} - p| \geq \frac{c}{(h_1 \dots h_n)^\varepsilon}, h_i = \max(1, |q_i|),$$

kaikilla $p, \bar{q}$, niin $\varepsilon \geq 1$.

Lause on yleistys Dirichlet'n lauseen vastaavalle korollaarille: $|rq - p| \geq \frac{c}{q^\varepsilon} \Rightarrow \varepsilon \geq 1$.

Lauseen todistus on varsin suoraviivainen kun käytössä on korollaari 5.3.1.

Todistus. Olkoon

$$|\bar{r} \cdot \bar{q} - p| \geq \frac{c}{(h_1 \dots h_n)^\varepsilon}, h_i = \max(1, |q_i|),$$

kaikilla valinnoilla $p, \bar{q}$ jollain $\bar{r} \in \mathbb{R}^n, c > 0$ ja $\varepsilon > 0$.

On olemassa äärettömän monta primitiivistä $p, \bar{q}$ joilla

$$|\bar{r} \cdot \bar{q} - p| < \frac{1}{h_1 \dots h_n}$$

joillain $h_i \geq |q_i|$ eli siis myös valinnoilla $h_i := \max(1, |q_i|)$. Nyt voidaan muodostaa kaksoisepäyhtälö

$$\frac{c}{(h_1 \dots h_n)^\varepsilon} \leq |\bar{r} \cdot \bar{q} - p| < \frac{1}{h_1 \dots h_n}.$$

Asetetaan $h := h_1 \dots h_n$ ja ratkaistaan:

$$\begin{aligned} \frac{c}{h^\varepsilon} &\leq |\bar{r} \cdot \bar{q} - p| < \frac{1}{h} \\ \Rightarrow \frac{c}{h^\varepsilon} &< \frac{1}{h} \\ \Rightarrow c &< \frac{h^\varepsilon}{h} \\ \Rightarrow h^{\varepsilon - 1} &> c. \end{aligned}$$

Koska $h^{\varepsilon-1}$ on alhaalta rajoitettu, ja $1 \leq h < \infty$ niin eksponenttifunktioiden perusominaisuuksien nojalla tiedetään, että

$$\begin{aligned} \varepsilon - 1 &\geq 0 \qquad \text{jolloin siis} \\ \varepsilon &\geq 1. \end{aligned}$$

Tämä viimeistelee todistuksen. □

6 Erityisiä hiloja: D_3, E_8, Λ_{24} ja ympyräpakkausongelmat

Pakkausongelmat ovat geometrian klassikko-ongelmia. Pakkausongelmissa yritetään selvittää tehokkain tapa pakata yhteneviä avoimia kuulia suureen avaruuden $\mathbb{R}^n$ osajoukkoon.

Tässä kappaleessa esitellään muutamia pakkausongelmiin liittyviä tunnettuja tuloksia sekä tarkastellaan hilojen merkitystä pakkausongelmien ratkaisuyrityksissä.

6.1 Pakkausongelman määritelmä

Ympyräpakkausongelma avaruudessa $\mathbb{R}^n$ etsii avaruuden tiheintä mahdollista osajoukkoa P, joka koostuu yhtenevistä, leikkaamattomista avoimista kuulista. Tiheyden määritelmä on intuitiivisesti ilmiselvä, mutta koska joukko P on ääretön, tulee formaalissa määritelmässä käyttää raja-arvoja:

$$\rho(P) = \lim_{r\to\infty} \frac{|P \cap B(r)|}{|B(r)|}$$

missä $B(r)$ on origokeskeinen r-säteinen kuula. Kuulan voi halutessaan korvata kuutiolla tai millä tahansa muulla n-ulotteisella, symmetrisellä, ja konveksilla kappaleella K jolla $K(r) = r^n K(1)$ ja määritelmät olisivat silti ekvivalentit.

Erikoisena yksityiskohtana todettakoon, että tämä määritelmä muistuttaa yllättävän paljon ehdollisen todennäköisyyden määritelmää. Joukon P tiheyden voikin vertauskuvallisesti mieltää eräänlaiseksi todennäköisyydeksi valita satunnaisesti joukon $\mathbb{R}^n$ pisteistä sellainen piste, joka sisältyy joukkoon P. Kyseessä on kuitenkin vain vertauskuva: ρ ei toteuta Kolmogorovin täysadditiivisuusaksioomaa.[2]

6.2 Tunnettuja optimaalisia pakkauksia

Optimaaliset pakkaukset voidaan määritellä yksikäsitteisesti ympyröidensä keskipisteiden mukaan. Lisäksi, ilmiselvästi, jos P on optimaalinen pakkaus, myös joukot, jotka saadaan tätä joukkoa kääntämällä, siirtämällä, tai lineaarisesti skaalaamalla ovat optimaalisia pakkauksia. Siispä puhuttaessa optimaalisesta pakkauksesta P, tulee tiedostaa, että tosiasiassa puhutaan P:n määrittelemästä ekvivalenssiluokasta.

Avaruudessa $\mathbb{R}^1$ optimaalisen pakkauksen määrittää $\mathbb{Z}$ ja sen tiheys on 1. Tämän todistaminen on triviaalia.

Avaruudessa $\mathbb{R}^2$ optimaalisen pakkauksen määrittää tasasivuisten kolmioiden muodostama hila $\text{span}(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}\frac{1}{2}\\ \frac{\sqrt{3}}{2}\end{bmatrix})$. Tämän todistaminen on jo aavistuksen työläämpää, ja kunnollinen todistus on kompaktillakin tyylillä jo noin sivun mittainen[9, s. 142-143].

Avaruudessa $\mathbb{R}^3$ on hyvä arvaus, että optimaalinen pakkaus saadaan pakkaamalla kuulia ensin ruudukkomaisesti tasoihin ja sitten asettamalla ruudukot limittäin toistensa päälle. Formaalisti ilmaistuna tämä on ns. "shakkilautapakkaus"ja sen määrittää hila D_3, missä

$$D_3 = \{(n_1, n_2, n_3) \in \mathbb{Z}^3 | n_1 + n_2 + n_3 \equiv 0 \mod 2\} = \text{span}\left(\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{bmatrix}\right).$$

[2] Tämän todistaa vastaesimerkki $[0,1] \cup [2,3] \cup [4,5] \cup \ldots$.

Kuva 7: Havainnollistus Kepler-hypoteesin optimaalisesta ympyräpakkauksesta appelsiinein. Kuvalähde: JJ Harrison, 2009, Wikimedia Commons

Shakkilautapakkaus D_3 on pakkausongelmien kontekstissa ekvivalentti sellaisen hilan kanssa, jossa hilapisteet järjestetään ensin tasasivuisten kolmioiden muodostamiin tasoihin, ja jossa nämä tasot sitten limitetään päällekkäin. Formaalisti tämä on siis hila $\operatorname{span}\left(\begin{bmatrix} \frac{\sqrt{3}}{6} & \frac{-\sqrt{3}}{3} & \frac{\sqrt{3}}{6} \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{\sqrt{6}}{3} & \frac{\sqrt{6}}{3} & \frac{\sqrt{6}}{3} \end{bmatrix}\right)$.

Hypoteesi siitä, että ekvivalenssiluokka $[D_3]$ määrittää avaruuden $\mathbb{R}^3$ parhaan mahdollisen ympyräpakkauksen, tunnetaan Kepler-hypoteesina. Hypoteesi on nimetty esittäjänsä, 1600-luvun taitteessa eläneen matemaatikon Johannes Keplerin, mukaan.

Hypoteesi ei kuitenkaan saanut todistusta kuin vasta neljäsataa vuotta esittämisensä jälkeen. Tällöin hypoteesin todisti Thomas Hales ja todistus oli tällöin yli sata sivua pitkä sekä tietokoneavusteinen[10]. Todistuksen vaikeustaso koki siis valtavan hyppäyksen.

6.3 Hila E_8

Avaruudessa $\mathbb{R}^8$ epäiltiin pitkään, että E_8 olisi pakkauksista kaikkein paras. Lauseen todistus on kuitenkin hyvin tuore saavutus: Maryna Viazovska todisti lauseen vuonna 2017[11].

Hila E_8, epäformaalisti ilmaistuna, on kaksi päällekkäin limitettyä D_8-hilaa. Formaalimmin, E_8 sisältää ne joukon $\mathbb{Z}^8$ ja ne joukon $(\mathbb{Z}+\frac{1}{2})^8$ pisteet, joiden komponenttien summa on parillinen.

Määritelmä 6.1.

$$E_8 = \left\{(x_1,\ldots,x_8) \in \mathbb{Z}^8 \cup (\mathbb{Z}+\frac{1}{2})^8 \middle| x_1+\cdots+x_8 \equiv 0 \mod 2\right\}.$$

E_8 on helppo todistaa hilaksi: Riittää huomata, että

$$E_8 = \operatorname{span} \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

Kun tarkastellaan esimerkiksi origoa $\bar{0}$, huomataan, että kaikki tämän pisteen lähinaapurit ovat joko muotoa $(\pm 1, \pm 1, 0, \ldots, 0)$ permutaatioineen tai sitten muotoa $(\pm\frac{1}{2}, \ldots, \pm\frac{1}{2})$.

Tästä on helppo laskea, että hilan E_8 määrittämässä ympyräpakkauksessa $P(E_8)$ origokeskisen kuulan säde – ja täten myös jokaisen muun kuulan säde – on

$$\begin{aligned} r &= \frac{1}{2}\sqrt{1^2 + 1^2} && = \frac{1}{2}\sqrt{2} \text{ tai, yhtäpitävästi} \\ r &= \frac{1}{2}\sqrt{\left(\frac{1}{2}\right)^2 + \cdots + \left(\frac{1}{2}\right)^2} && = \frac{1}{2}\sqrt{2}. \end{aligned}$$

Muut vaihtoehdot origon lähinaapureiksi on helppo karsia yksitellen poissulkeamalla: Muut puolikokonaislukuvektorit kuin $(\pm\frac{1}{2}, \ldots, \pm\frac{1}{2})$ sisältävät origosta kauemmas poikkeavia komponentteja ja täten niiden euklidinen mittakin on suurempi. Muut kokonaislukuvektorit kuin $(\pm 1, \pm 1, 0, \ldots, 0)$ permutaatioineen sisältävät joko enemmän komponentteja tai ainakin yhden komponentin, jonka itseisarvo on ainakin 2. Kummassakin tapauksessa euklidinen mitta kasvaa suuremmaksi kuin r.

Origolla – ja täten myös jokaisella muulla hilapisteellä – on $2^2\binom{8}{2} + 2^8\binom{8}{8} = 368$ lähinaapuria. Kunkin kuulan mitta on

$$V = \frac{\pi^{\frac{8}{2}}}{\Gamma(8 \cdot \frac{1}{2} + 1)} r^8 = \frac{\pi^4}{4!}\left(\frac{\sqrt{2}}{2}\right)^8 = \frac{\pi^4}{392} \approx 0,25.$$

$P(E_8)$ tiheys on mahdollista päätellä kun tiedetään, että $|\det(E_8)| = 1$. Determinantin itseisarvo kertoo, että avaruus $\mathbb{R}^8$ on mahdollista osittaa puoliavoimiin suuntaissärmiöihin, joiden mitta on 1, ja jotka sisältävät tasan yhden E_8 hilapisteen. Tästä seuraa, että $\rho(E_8) = 1$, josta seuraa edelleen, että $\rho(P(E_8)) = V|\det(E_8)| = V = \frac{\pi^4}{392} \approx 0,25$.

6.4 Leech-hila Λ_{24}

Leech-hila, lyhyeltä nimeltään Λ_{24}, määrittää optimaalisen ympyräpakkauksen avaruudessa $\mathbb{R}^{24}$. Leech-hilan optimaalisuus todistettiin 2017 ja todistus perustui suurelta osin samoille ideoille, kuin Viazovskan aiempi optimaalisuustodistus hilalle E_8 [12].

Leech-hilalle on useita ekvivalentteja määritelmiä. Eräs yksinkertaisimmista on Wilsonin algebrallinen, oktonioihin ja hilaan E_8 perustuva määritelmä[13].

Hila E_8 esiteltiin edellisessä kappaleessa. Oktoniot, $\mathbb{O}$, puolestaan on kompleksilukujen 8-ulotteinen yleistys. Kuten kompleksiluvuilla, myös oktonioilla on

liittoluku, käänteisluku ja normi ja kompleksiluvut ovat oktonioiden alikunta. Kertolasku ei kuitenkaan ole oktonioissa vaihdannainen eikä liitännäinen.

Esitellään seuraavaksi Wilsonin määritelmää mukaileva määritelmä Leech-hilalle.

Määritelmä 6.2. *Olkoon L joukko $\mathbb{O} \cap E_8$ ja olkoon s aidosti imaginäärinen oktonio $\frac{1}{2}(0,-1,1,1,1,1,1,1)$ ja olkoon $\bar{s}$ tämän liittoluku $\frac{1}{2}(0,1,-1,-1,-1,-1,-1,-1)$. Leech-hila on oktoniokolmikkojen (x,y,z) muodostama hila Λ_{24}, jonka kaikilla alkioilla (x,y,z) pätee*

$$x, y, z \in L, \tag{7}$$

$$x+y, y+z, z+x \in L\bar{s} \text{ ja} \tag{8}$$

$$x+y+z \in Ls. \tag{9}$$

Huomionarvoisesti $L\bar{s}$ ja Ls ovat edelleen neliömatriiseja, kun matriisikertolaskut tulkitaan toistetuiksi kompleksituloiksi

$$L\bar{s} = \begin{bmatrix} l_1\bar{s} & \dots & l_8\bar{s} \end{bmatrix}$$

ja

$$Ls = \begin{bmatrix} l_1 s & \dots & l_8 s \end{bmatrix}.$$

On myös kohtalaisen helppo huomata, että muutamat tietyssä mielessä "itseään toistavat" vektorit kuten esimerkiksi $(x,x,z) \neq \bar{0}$ eivät voi kuulua Leech-hilaan: Yhtälön (8) nojalla pitäisi olla voimassa $x+x \in L\bar{s}$ mutta toisaalta L on ryhmä, joten $x+x \in L$. Kuitenkin $L \cap L\bar{s} = \{\bar{0}\}$ ja $(x,x,z) \neq \bar{0}$. Siispä (x,x,z) ei voi kuulua Leech-hilaan.

Vastaavasti yhtälön (9) nojalla vektorit muotoa (x,x,x) voidaan sulkea Leech-hilan ulkopuolelle.

6.5 Tuntemattomia optimaalisia pakkauksia

Avaruuksille $\mathbb{R}^n$ parhaita pakkauksia ei pääsääntöisesti tunneta[14, s. 6]. Avaruudessa $\mathbb{R}^4$ shakkilautapakkaus D_4 on paras tunnettu pakkaus, ja todistettavasti paras hilapakkaus. Sama on totta avaruudessa $\mathbb{R}^5$ shakkilautapakkaukselle D_5. Avaruudessa $\mathbb{R}^6$ hilan E^6 epäillään olevan paras mahdollinen pakkaus, mutta tätä ei ole todistettu. Kukaan ei tiedä, ovatko kaikki parhaat pakkaukset säännöllisiä.[14, s. 16]

7 Hilat ja tietojenkäsittelytiede

Tietojenkäsittelytiede on eksakti tiede joka, karkeasti ottaen, käsittelee tietokoneavusteiseen laskemiseen liittyviä aiheita. Tällaisia aiheita ovat esimerkiksi tietorakenteet, algoritmit, aikavaativuudet ja vaikeusluokat. Tietokoneet – niin todelliset tietokoneet kuin teoreettiset Turingin koneetkin – varastoivat datansa diskreeteissä paketeissa ja koneiden suorittamat algoritmit suorittavat aina diskreetin määrän työvaiheita. Edellisistä havainnoista voi arvata, että lukuteorian tuloksista lienee tietojenkäsittelytieteessä usein hyötyä ja toisaalta, että tietotekniikasta on vastavuoroisesti apua lukuteorian ongelmien ratkaisussa.

Tässä kappaleessa esitellään muutama esimerkki niistä tavoista, joilla hilat esiintyvät tietojenkäsittelytieteessä. Silloin tällöin hiloihin liittyvä teoria auttaa tietoteknisten ongelmien ratkaisemisessa. Toisinaan taas käytännön ongelmista kumpuaa ihan uusia ongelmia lukuteoreetikkojen pohdittavaksi.

7.1 Hilapakkausongelmat ja virheenkorjausalgoritmit

Tietokoneiden varastoimat ja käsittelemät tietueet abstrahoidaan usein binäärimerkistön jonoiksi: tässä abstraktiossa jokainen tietokoneen käsittelemä merkki on joko 0 tai 1, ja kaikki tietueet ovat näiden merkkien jonoja, siis esimerkiksi "1100001" tai "1100110 1101111 1111000". Joillain näistä tietueista on erityisiä nimiä: esimerkiksi 8-merkkinen tietue on "tavu" ja 4-tavuinen tietue on "sana". Useimmat nykyaikaiset tietokoneet säilövät 64 bittiä, eli 8 tavua, eli 2 sanaa, jokaiseen muistipaikkaansa.

Kun tällaista binäärimuotoista tietoa lähetetään pitkien matkojen päähän, esimerkiksi langattomasti, on olemassa riski, että erilaiset häiriötekijät aiheuttavat tietueeseen satunnaisia muutoksia.

Formaalisti, jos alkuperäinen tietue $\bar{x}$ on jokin avaruuden $\{0,1\}^n = \mathbb{B}^n$ merkkijono, niin vastaanotettu tietue on

$$\bar{y} = f(\bar{x}) + \bar{\varepsilon} \in \mathbb{R}^n$$

jollain virhevektorilla $\bar{\varepsilon} \in \mathbb{R}^n$ ja kääntyvällä koodauksella $f : \mathbb{B}^n \to K \subset \mathbb{B}^m, n \leq m$. Virhevektori $\bar{\varepsilon}$ on jakautunut satunnaisesti jonkin todennäköisyysfunktion mukaisesti. Yleinen olettama on, että pienet virheet ovat todennäköisempiä kuin suuret virheet.

Kiinnostava ongelma on, miten f voidaan määritellä ovelasti niin, että $\bar{x}$ voidaan algoritmisesti arvata oikein vektorista $\bar{y}$ mahdollisimman suurella todennäköisyydellä kuitenkin niin, että kuvajoukon ulotteisuus m ei kasvaisi kovin suureksi.

Perinteinen ratkaisu: Hamming-koodit Usein virheenkorjauksessa tehdään yksinkertaistus, jossa $\bar{\varepsilon}$ voi muuttaa vain bitin 0 bitiksi 1 tai toisinpäin tai olla tekemättä mitään. Lisäksi oletetaan, että todennäköisesti jos virheitä esiintyy, niitä on tasan 1.

Tällaisessa mallissa niin sanotut Hamming-koodit ovat erinomaisen tehokas tapa korjata bittivirheitä. Hamming-koodit on nimetty keksijänsä Richard Hammingin mukaan. Hamming määritteli Hamming-koodit teoksessaan *Error detecting and error correcting codes* [15].

Määritelmä 7.1. *Hamming-koodi on funktio* $H : \mathbb{B}^{2^n-n-1} \to \mathbb{B}^{2^n-1}$ *joka rakentuu seuraavalla tavalla.*

- *Olkoon* $\bar{y} = H(\bar{x})$.
- *Komponentit* $y_1, y_2, y_4, y_8, y_{16}, \ldots$ *ovat tarkistusbittejä. Loput komponentit ovat merkkijonon* $\bar{x}$ *komponentit järjestyksessä.*
- *Tarkistusbitit valitaan niin, että*

$$\begin{aligned}
s_1 &= \mathbf{y_1} + y_3 \quad &+y_5 + y_7 + y_9 + y_{11} \quad &+y_{13} + y_{15} + \ldots \equiv 0 \mod 2 \\
s_2 &= (\mathbf{y_2} + y_3) \quad &+(y_6 + y_7) + (y_{10} + y_{11}) \quad &+(y_{14} + y_{15}) + \ldots \equiv 0 \\
s_4 &= (\mathbf{y_4} + y_5 \quad &+y_6 + y_7) + (y_{12} + y_{13} \quad &+y_{14} + y_{15}) + \ldots \underset{32}{\equiv} 0
\end{aligned}$$

jne.

Esimerkki 7.1. *Olkoon* $\bar{x} =$ "0011". *Kuvataan* $\bar{y} = H(\bar{x})$.

Varataan ensin merkkijonosta $\bar{y}$ *paikat tarkistusbiteille:*

$$\bar{y} = \text{"\_\_0\_011"}.$$

Huomataan, että $y_3 = 0, y_5 = 0$ *ja* $y_7 = 1$. *Siispä on sijoitettava* $y_1 = 1$ *jotta* $s_1 \equiv 0$.

$$\bar{y} = \text{"}\mathbf{1}\text{\_0\_011"}.$$

Seuraavaksi huomataan, että $y_3 = 0, y_6 = 1, y_7 = 1$, *joten* $y_2 = 0$*:*

$$\bar{y} = \text{"1}\mathbf{0}\text{0\_011"}.$$

Lopuksi $y_5 = 0, y_6 = 1, y_7 = 1$ *joten myös* $y_4 = 0$*:*

$$\bar{y} = \text{"100}\mathbf{0}\text{011"}.$$

Näiden välivaiheiden jälkeen on onnistuneesti laskettu, että

$$H(\text{"0011"}) = \text{"1000011"}.$$

Hamming-koodi varmistaa, että kussakin $\bar{y}$ voi tapahtua yksi bittivirhe ja virheellisestä merkkijonosta $\bar{y}'$ on silti mahdollista päätellä, mikä alkuperäinen $\bar{x}$ oli.

Esimerkki 7.2. *Olkoon vastaanotettu merkkijono* $\bar{y}' =$ "1010011". *Merkkijono* $\bar{y}'$ *on Hamming-koodattu ja siinä tiedetään olevan enintään yksi bittivirhe.*

Huomataan heti, että $s_1 = 1+1+0+1 \equiv 1$, *joten merkkijonossa on varmasti bittivirhe. Huomataan myös, että* $s_2 = 0+1+1+1 \equiv 1$ *ja että* $s_4 = 0+0+1+1 \equiv 0$.

Huomataan, että jos vaihdetaan bitti y_3' *merkistä* 1 *merkiksi* 0, *niin summat* s_1 *ja* s_2 *korjaantuvat ja summa* s_4 *ei muutu. Huomataan myös, että sama ei päde millekään muulle bitille. Siispä bittivirhe tapahtui bitissä* y_3' *ja alkuperäinen merkkijono oli siis*

$$\bar{y} = \text{"10}\mathbf{0}\text{0011"}.$$

Lause 7.1. *Jos Hamming-koodatulla merkkijonolla* $\bar{y}$ *summat* $s_{i_1}, s_{i_2}, \ldots, s_{i_k}$ *ovat parittomat, niin merkkijonossa on bittivirhe, ja bittivirhe on komponentissa* $y_{i_1+i_2+\cdots+i_k}$.

Todistus. Olkoon $\bar{y}$ Hamming-koodattu merkkijono, jossa on merkkivirhe komponentissa y_i. Olkoon merkin y_i indeksi i ilmoitettu binäärimuodossa

$$i = 2^{n-1}b_n + \cdots + 2b_2 + b_1, b_j \in \mathbb{B}.$$

Huomataan, että määritelmällisesti s_1 on pariton tasan silloin, kun $b_1 = 1$. Samoin s_2 on pariton tasan silloin, kun $b_2 = 1$. Yleisesti $s_{2^{j-1}}$ on pariton tasan silloin, kun $b_j = 1$.

Koska jokaisella indeksillä $i \in \mathbb{N}$ on tasan yksi binääriesitys, ja tämä esitys on ainutlaatuinen, niin myös jokaisessa indeksissä i tapahtunutta bittivirhettä vastaa tasan yksi ainutlaatuinen parittomien summien s joukko. Tämä ainutlaatuinen summien s joukko puolestaan on

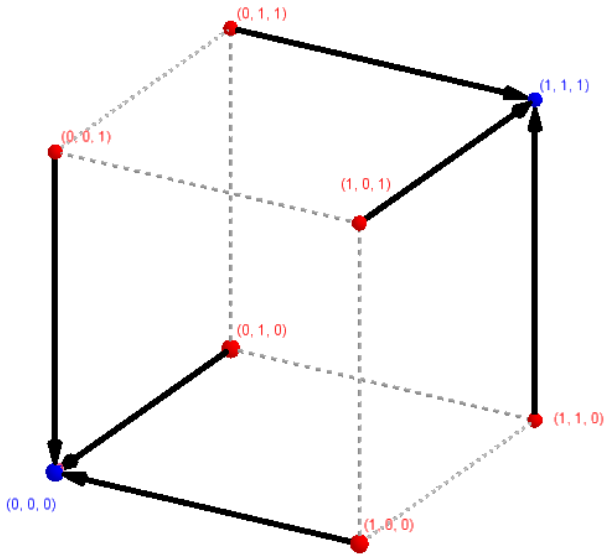
$$\{s_{2^{j-1}} : b_j = 1\}.$$

Summien $s_{2^{j-1}}$ indeksien summa puolestaan on

$$2^{j_1-1} \cdot 1 + \cdots + 2^{j_k-1} \cdot 1$$

mutta selvästi tämä on vain indeksin i binääriesitys, josta on sievennetty nollatermit pois. □

Hamming-koodin verkkoteoreettis-geometrinen tulkinta on, että koodi kuvaa $2^n - n - 1$-ulotteisen binäärikuution $\mathbb{B}^{2^n-n-1}$ kulmat binäärikuution $\mathbb{B}^{2^n-1}$ kulmapisteiksi, mutta kuitenkin niin, että kaikilla kuvajoukon kulmilla on täysin eri naapurit keskenään. Nämä naapurit edustavat tilanteita, joissa merkkijonosta on muuttunut tasan yksi bitti.



Kuva 8: Yksinkertaisin mahdollinen Hamming-koodi $\mathbb{B}^1 \to \mathbb{B}^3$ esitettynä graafisesti. Punaisella väritetyt virheelliset koodit korjautuvat valideiksi sinisiksi koodeiksi vektorinuolten osoittamalla tavalla.

$2^n - 1$-ulotteisessa avaruudessa kullakin binäärikuution kulmalla on tasan $2^n - 1$ naapuria. Kuvajoukon kulmia taas on tasan 2^{2^n-n-1} kappaletta. Siispä kuvajoukon naapureita on yhteensä $2^{2^n-n-1}(2^n-1)$ kappaletta. Yhteensä kuvajoukon kulmia sekä näiden naapureita on $2^{2^n-n-1} + 2^{2^n-n-1}(2^n-1)$ kappaletta.

Joukossa $\mathbb{B}^{2^n-1}$ puolestaan on 2^{2^n-1} alkiota. On nopeasti todennettavissa, että

$$2^{2^n-n-1} + 2^{2^n-n-1}(2^n - 1) = 2^{2^n-1}.$$

Siispä Hamming-koodi on paras mahdollinen tapa valita binäärikuutiosta $\mathbb{B}^{2^n-1}$ kulmat niin, että kunkin valitun kulman polkuetäisyys – tai, ekvivalentisti, Manhattan-etäisyys – on ainakin 3.

Virheenkorjaus pakkausongelmien näkökulmasta Jos ajatellaan, että r on sellainen säde, jolla todennäköisyys $P(|\bar{\varepsilon}| > r)$ on erittäin pieni, niin tiedetään, että alkuperäinen piste $f(\bar{x})$ on liki varmasti pisteen $\bar{y}$ r-säteisessä kuulaympäristössä. Jos tässä kuulassa olisi vain yksi kuvajoukon K piste $f(\bar{x})$, niin $\bar{x}$ voitaisiin päätellä lähes varmasti oikein.

Näin ollen yksi tapa lähestyä virheenkorjausalgoritmeja on ympyräpakkausongelmien kautta: Millainen kuvajoukko funktiolla f täytyy olla, jotta jotta joukon $K = \mathrm{Im}\, f$ määräämä ympyräpakkaus sisältäisi mahdollisimman suuren osan $\mathbb{B}^m$ hilapisteistä mutta kuitenkin niin, että pakkaus koostuu mahdollisimman monesta riittävän suuresta (=säde ainakin r) kuulasta?

7.2 Lyhimmän ja lähimmän vektorin ongelmat

Lyhimmän ja lähimmän vektorin ongelmat ovat etsintäongelmia. Näissä ongelmissa tulee annetusta – yleensä hyvin moniulotteisesta – hilan kannasta Λ etsiä mahdollisimman tehokkaasti

- hilan Λ kaikkein lyhin hilapiste $\bar{x}, |\bar{x}| = \min\{|\bar{v}| : \bar{v} \in \Lambda\}$, tai
- se hilapiste $\bar{x}$, joka on kaikkein lähimpänä annettua pistettä $\bar{v} \in \mathbb{R}^n$.

Kuten tietojenkäsittelytieteen algoritmiongelmissa yleensä, kiinnostavaa ei ole ratkaisu itse, vaan miten se voidaan löytää tehokkaasti kun hilan ulotteisuus n kasvaa hyvin suureksi ja kun käytössä on Turingin kone tai joku muu tämän kanssa ekvivalentti deterministinen laite. Ongelmat ovat siis algoritminoptimointiongelmia.

Lyhimmän vektorin ongelma on todistettu *NP-vaikeaksi* mutta ei euklidisella metriikalla vaan maksimimetriikalla[16]. Euklidisella metriikalla ongelman vaikeusluokkaa ei tiedetä. Lähimmän vektorin ongelman tiedetään olevan enintään yhtä vaikea kuin lyhimmän vektorin ongelma[17] – ne saattavat esimerkiksi molemmat olla NP-vaikeita.

NP-vaikea ongelma on mikä tahansa ongelma, joka on vähintään yhtä vaikea ratkaista kuin mikä tahansa NP-ongelma. NP-ongelma on mikä tahansa ongelma, jonka epädeterministinen Turningin kone ratkaisee polynomisessa ajassa tai, ekvivalentisti, jonka ratkaisun tavallinen Turingin kone hyväksyy polynomisessa ajassa. Salasanan arvaaminen äärellisessä aakkostossa on tunnettu esimerkki NP-ongelmasta siinä missä Kauppamatkustajan ongelma on esimerkki NP-vaikeasta ongelmasta.

Joitain havaintoja lyhimmän vektorin ongelmasta On helppo nähdä, että lähimmän vektorin ongelma ei voi olla merkittävästä vaikeampi kuin lyhimmän vektorin ongelma: On ekvivalenttia löytää vektoria $\bar{v}$ lähin hilapiste hilassa Λ kuin löytää lyhin vektori hilassa $\Lambda - \bar{v}$ ja kannan vaihtaminen tällä tavoin on selkeästi polynomisessa ajassa suoritettavissa oleva operaatio.

Lisäksi, Minkowskin ensimmäisen lauseen nojalla, hilan Λ lyhimmän nollasta poikkeavan hilavektorin täytyy sisältyä sellaiseen kuulaan, jonka tilavuus on $2^n|\det\Lambda|$. Tällaisen kuulan säde on helppo ratkaista:

$$\frac{\pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)!}r^n = 2^n|\det\Lambda|, \text{ joten}$$
$$r = \frac{2}{\sqrt{\pi}}\sqrt[n]{\left(\frac{n}{2}\right)!|\det\Lambda|}.$$

Näin ollen myös lyhimmän vektorin on oltava pituudeltaan enintään r ja kaikki tätä pidemmät hilavektorit voidaan hylätä. Tämä optimointi ei kuitenkaan yksinään auta tarkastelua merkittävästi. Esimerkiksi hila $\Lambda = \text{span}\begin{bmatrix}\frac{1}{N} & 0\\ 0 & N\end{bmatrix}$ jollain suurella N sisältää suuren määrän hilapisteitä tällaisen kuulan sisällä.

Vastaavasti Minkowskin toinen lause antaa tavan määritellä lyhimmän vektorin pituudelle alarajan: Luodaan origokeskeinen kuula, jonka säde on 1, ja olkoon tämä kuula kappale K. Minkowskin toisessa lauseessa esiintyvät viimeiset perättäiset minimit $\lambda_2, \ldots, \lambda_n$ on helppo arvioida ylöspäin kun asetetaan kuulan säteen kertoimeksi R_i kannan i. lyhimmän virittäjävektorin pituus. Kuula, jonka säde on R_i sisältää kannan i lyhintä vektoria, joten se siis sisältää varmasti i riippumatonta vektoria, ja täten siis $R_i \geq \lambda_i$. Nyt voidaan arvioida alaspäin ensimmäistä perättäistä minimiä λ_1, eli toisaalta lyhimmän hilavektorin pituutta:

$$\frac{2^n}{n!}|\det\Lambda| \leq \lambda_1 \ldots \lambda_n|K| \leq \lambda_1 R_2 \ldots R_n|K|, \text{ jolloin siis}$$
$$\lambda_1 \geq \frac{2^n|\det\Lambda|}{n!\pi R_2 \ldots R_n}.$$

Esimerkki 7.3. *Hilassa* $\Lambda = \text{span}\begin{bmatrix}\cos\alpha & \frac{1}{\sin\alpha}\\ \sin\alpha & 0\end{bmatrix}$ *jollain* α*, tiedetään, että*

$$\lambda_1 \geq \frac{4\sin\alpha}{2\pi}.$$

8 Loppumietteitä: Hilateorian suhde yläasteen ja lukion matematiikkaan

Tässä lopetuskappaleessa koostetaan aiempien kappaleiden sisältöjä ja pohditaan, miten hiloihin liittyvä teoria linkittyy eri-ikäisten matematiikan oppijoiden opintoihin. Erityisesti tarkastellaan hilateorian yhteyttä yläasteella ja lukiossa käsiteltävään matematiikkaan.

Kappaleessa 2 käsiteltiin hilojen perusominaisuuksia. Näistä ominaisuuksista monet olivat lineaarialgebrallisia: vapautta ja kannan determinanttia koskevia käsitteitä. Lisäksi seassa oli hilojen algebrallisia ominaisuuksia sekä topologiaa koskevia väitteitä. Minkowskin ensimmäinen lause oli luonteeltaan toisaalta geometrinen ja toisaalta lukuteoreettinen.

Tämän kappaleen perusteella saa hyvin vahvasti sellaisen käsityksen, että hilateorian kaikkein hedelmällisin kohdeyleisö on yliopisto-opiskelijat, joilla on matematiikka pää- tai sivuaineenaan. Hilojen lineaarialgebrallisia ominaisuuksia on hyvin haastava ymmärtää ilman kursseja *Lineaarialgebra ja matriisilaskenta I ja II* vastaavia tietoja. Samoin esimerkiksi ryhmän käsite on tuttu harvalle sellaiselle opiskelijalle, jolla ei ole ainakin kurssia *Algebralliset rakenteet I* vastaavaa tietomäärää. Osittain järjestetty joukko sekä järjestyshila ovat tuttuja käsitteitä vielä pienemmälle oppijoiden joukolle.

Minkowskin toinen lause todistuksineen kappaleessa 3 on haastava aihe vielä maisterivaiheenkin opiskelijoille.

Pakkausongelmat, ja erityisesti Kepler-hypoteesi, ovat esimerkkejä ongelmista, jotka yläastelainenkin ymmärtää, mutta joiden ratkaiseminen koettelee matemaattisen yhteisön luovuuden äärirajoja.

Toki kaikki edellinen ei ole erityisen yllättävää: Nämä aiheet valitiin tutkielmaan tarkasteltavaksi varta vasten siksi, että ne ovat maisterintutkielmaan "riittävää syvällisyyttä ja haastavuutta" osoittavia aiheita. Tämä ei kuitenkaan tarkoita, että kaiken hiloihin liittyvän teorian täytyisi olla liian vaikeaa ja syvällistä alemman asteen oppilaitoksiin.

Kepler-hypoteesia ei tarvitse todistaa koulussa, vaan jos sen haluaa mainita, sen voi mainita esimerkkinä siitä, miten matematiikassa helposti ymmärrettävä ongelma ei välttämättä ole aina helposti ratkeava ongelma.

Sivumaininta kappaleessa 2.1 siitä, miten hilat ovat diskreettejä joukkoja, avautuu varmasti kuvan avulla lukiolaisellekin, vaikka heille ei olisikaan tuttu diskreetin joukon tarkka topologinen määritelmä. Lukion pitkän matematiikan moduulissa *MAA8 Tilastot ja todennäköisyys* yksi tavoitteista on, että opiskelija "osaa havainnollistaa diskreettiä tilastollista jakaumaa sekä määrittää ja tulkita jakauman tunnuslukuja"[18, s. 227]. Tässä kontekstissa hilat voisivat olla mielenkiintoinen, tosin edistynyt, esimerkki mahdollisesta todennäköisyysfunktion perusjoukosta, joka on diskreetti mutta ääretön. Esimerkiksi erilaisia satunnaiskävelyjä voidaan mallintaa tällaisilla hilapohjaisilla todennäköisyysfunktioilla.

Hilapisteen määritelmä kokonaislukukombinaationa virittäjävektoreita on päivänselvä kenelle tahansa lukion vektorikurssin *MAA4 Analyyttinen geometria ja vektorit* käyneelle opiskelijalle.

Diofanttinen approksimaatio ja hilateorian soveltuminen Dirichlet'n lauseen todistamiseen esitellään kappaleessa 5. Diofanttinen approksimaatio on puhtaasti lukuteoreettinen aihealue, joten jos mihinkään, se sisältyy lukion pitkän matematiikan moduulin *MAA11 Algoritmit ja lukuteoria* aiheeksi. Diofanttiseen approksimaatioon liittyy hilojen ohella myös ketjumurtolukujen ja konvergent-

tien käsitteet. Kummatkin edellämainituista puolestaan on mahdollista ratkaista algoritmisesti, erityisesti tietokoneavusteisesti. Algoritmien ymmärtäminen ja toteuttaminen ovat sattumalta myös kurssin MAA11 sisältöjä[18, s. 229]. Siispä diofanttinen approksimaatio on mielekäs aihe kurssilla käsiteltäväksi. Dirichlet'n lauseen Minkowski-pohjainen todistus saattaa tosin olla liian haastava ja aikaa vievä aihe käsiteltäväksi: moduuli on tarkoitettu 2 opintopisteen kurssiksi ja sen paremmin hilat kuin todistuksetkaan eivät ole kurssin keskeisiä sisältöjä.

Minkowskin ensimmäinen lause esitellään kappaleessa 2.4. Lause ei osu nätisti minkään lukion tai peruskoulun matematiikan sisällön piiriin. Kuitenkin lause osuu erikoiseen kolmipisteeseen lukuteorian, geometrian ja analyysin välissä: Lauseen todistaminen vaatii kyyhkyslakkaperiaatteeseen vetoamista, kongruenssin käsitteen moniulotteista ja epädiskreettiä yleistämistä, janan keskipisteen vektoriyhtälön hallitsemista ja injektion käsitteen hallintaa. Näin ollen Minkowskin ensimmäisen lauseen todistus on esimerkki sovelluskohteesta useiden eri pitkän matematiikan moduulien oppisisällöille. Tällaisen monia sisältöjä yhteen nivovan, haastavan esimerkin esittely voi olla mielekästä esimerkiksi jonkinlaisella kertauskurssilla käytäväksi, mutta LOPSissa lueteltujen kurssien sisältöihin aihetta on vaikea mahduttaa.

Kappaleessa 4 esitellään Gaussin kokonaisluvut ja ympyräongelma. Gaussin kokonaislukuja ja imaginääritasoa ylipäätään ei käsitellä sen paremmin peruskoulussa[19] kuin lukiossakaan[18], mutta sen sijaan ongelman lähtökohtana toimiva Pythagoraan lause on yläasteen matematiikan sisältö[19, s. 376]. Pythagoraan lauseen esittelyn yhteydessä Gaussin ympyräongelma variaatioineen voi olla mielekäs soveltava ongelma käsiteltäväksi. Joitain funktion N arvoista voi esimerkiksi ratkaista graafisesti, laskea algoritmisesti, tai arvioida likimääräisesti. Likimääräiseen arviointiin vaaditaan ympyrän pinta-alakaavan hallinta. Myös tämä on yläasteen matematiikan sisältö[19, s. 376]. Lukiolaisille ympyräongelman käsittely sopisi luontevasti esimerkiksi kurssille MAA11, ja erityisesti tehokkaan algoritmin kirjoittaminen funktion N arvojen ratkaisemiseksi voi olla kurssin tavoitteisiin sopiva haastetehtävä.

Gaussin ympyräongelman yhteydessä sekä aiemmin kappaleessa 3 käsitellään myös Jordan-sisältöä. Jordan-sisältö puolestaan on käsitteenä lähestulkoon ekvivalentti ns. "graafisen integroinnin" käsitteen kanssa. Graafinen integrointi on työkalu, jonka avulla arvioidaan hyvin epäsäännöllisten kappaleiden – kuten kämmenien tai jalkapohjien – pinta-aloja ruutuja laskemalla. Graafinen integrointi on työkalu, joka on mahdollista opettaa muun yläasteen pinta-alalaskennan yhteydessä ylimääräisenä syventävänä sisältönä.

Tietotekniikka ja hilateoria ylipäätään sopivat hyvin yhteen. Kappaleessa 7.1 esiteltiin, miten hilateorian ja tietotekniikan yhdistäminen tuo uusia ratkaisuja esimerkiksi luotettavaan tiedonsiirtoon. Kappaleessa 7.2 esiteltiin, miten aiheita yhdistämällä saadaan aikaan uusia ongelmia. Tietotekniikka ei virallisesti ole sen paremmin yläasteella kuin lukiossakaan oma oppiaineensa, mutta niin peruskoulun[19, s. 284] kuin lukionkin[18, s. 360] laaja-alaiset tavoitteet velvoittavat oppilaitoksia huolehtimaan opiskelijoiden tietoteknisten taitojen kehittymisestä. Oppilaitoksille ei ole tavatonta tarjota erilaisia tietotekniikan kursseja, joilla näitä taitoja kehitetään. Hypoteettisen yläasteen tai lukion peliohjelmointikurssin kontekstissa hilateorialle ei ole vaikea keksiä käyttöä: Hilat $\mathbb{Z}^2$ ja $\mathbb{Z}^3$ ovat olennaisia kenelle tahansa opiskelijalle, joka yrittää toteuttaa pelin tai simulaation, jossa oliot liikkuvat aina diskreetin määrän askelia tasossa tai avaruudessa. Tällaisia pelejä ovat esimerkiksi erilaiset shakki-, Tetris-, Pacman- ja matopelikloonit. Tällaisia simulaatioita ovat esimerkiksi aiemmin tässä kappa-

leessa mainitut satunnaiskävelysimulaatiot.

Yhteen vetäen hilateoriaa esiintyy yläasteella ja lukiossa satunnaisesti niin matematiikan kuin tietotekniikan tunneillakin. Kuitenkaan omalla nimellään hiloja ei koulussa käsitellä. Sen sijaan hilojen erikoistapauksiin – aivan erityisesti hilaan $\mathbb{Z}^2$ – ja niitä koskeviin lauseisiin törmätään silloin tällöin satunnaisesti, jonkun muun aiheen yhteydessä. Nämä erikoistapaukset lauseineen esiintyvät orgaanisesti osana opetusta ilman, että hilateoriaa täytyy erikseen pakottaa osaksi tuntisuunnitelmaa. Valtaosa hilateoriasta ei esiinny alemman asteen oppilaitoksissa lainkaan. Kuitenkin koulussa harvoin käsiteltävien aiheiden joukossa on helmiä, jotka sopivat erityisesti visaisiksi haasteiksi, helpoiksi esimerkeiksi liki mahdottomista tehtävistä, sekä aiemmilla kursseilla käsiteltyjä aihealueita yhteen sitoviksi soveltaviksi esimerkeiksi.

Viitteet

[1] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1959.

[2] W. M. Schmidt, *Diophantine Approximation*, A. Dold and B. Eckmann, Eds. Springer, 2008. [Online]. Available: https://www.ebook.de/de/product/8897460/diophantine_approximation.html

[3] J.-H. Evertse. (2017, Sep.) DIOPHANTINE APPROXIMATION: Course for third year bachelor and master students - Fall 2017. Universiteit Leiden Mathematisch Instituut. [Online]. Available: http://www.math.leidenuniv.nl/ evertse/dio.shtml

[4] C. D. Aliprantis and O. Burkinshaw, *Principles of real analysis*, 3rd ed. San Diego, CA: Academic Press Inc., 1998.

[5] R. P. Bambah, A. Woods, and H. Zassenhaus, "Three proofs of Minkowski's second inequality in the geometry of numbers," *Journal of the Australian Mathematical Society*, vol. 5, no. 4, p. 453–462, 1965.

[6] M. Henk, "Successive minima and lattice points," 2002, no. 70, part I, pp. 377–384, iV International Conference in "Stochastic Geometry, Convex Bodies, Empirical Measures & Applications to Engineering Science", Vol. I (Tropea, 2001).

[7] I. Danicic, "An elementary proof of Minkowski's second inequality," *Journal of the Australian Mathematical Society*, vol. 10, no. 1-2, p. 177–181, 1969.

[8] J. Steuding, *Diophantine Analysis*, ser. Trends in Mathematics, J. Steuding, Ed. Birkhäuser, 2016. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-48817-2

[9] T. C. Hales, "Cannonballs an Honeycombs," *Notices of the AMS*, vol. 47, no. 4, pp. 440–449, Apr. 2000.

[10] ——, "A proof of the Kepler conjecture," *Annals of Mathematics*, pp. 1065–1185, 2005.

[11] M. Viazovska, "The sphere packing problem in dimension 8," *Annals of Mathematics*, vol. 185, no. 3, p. 991–1015, May 2017. [Online]. Available: http://dx.doi.org/10.4007/annals.2017.185.3.7

[12] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, "The sphere packing problem in dimension 24," *Annals of Mathematics*, vol. 185, no. 3, pp. 1017–1033, 2017. [Online]. Available: http://www.jstor.org/stable/26395748

[13] R. A. Wilson, "Octonions and the Leech lattice," *Journal of Algebra*, vol. 322, no. 6, pp. 2186–2190, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0021869309001458

[14] H. Cohn, "Packing, coding, and ground states," 2016.

[15] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[16] B. van Emde, *Another Np-complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice*, ser. Mathematical preprints series. Universiteit van Amsterdam. Mathematisch Instituut, 1981. [Online]. Available: https://books.google.fi/books?id=rRcgrgEACAAJ

[17] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert, "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors," *Information Processing Letters*, vol. 71, no. 2, pp. 55–61, 1999. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020019099000836

[18] Opetushallitus, Ed., *Lukion opetussuunnitelman perusteet 2019*. Helsinki: PunaMusta OyVerlag nicht ermittelbar, 2019.

[19] Opetushallitus, *Perusopetuksen opetussuunnitelman perusteet 2014*. Helsinki: Next Print OyVerlag nicht ermittelbar, 2016.