NYILATKOZAT

Név: Fazekas Péter László

ELTE Természettudományi Kar, szak: matematika

NEPTUN azonosító: SL45K6

Szakdolgozat címe: Rácsok, parkettázások, és bázisredukciós algoritmusok

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2024. 06. 03.

Fazekas Péter

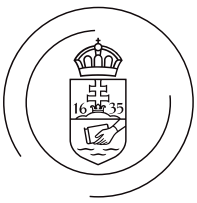
a hallgató aláírása

Rácsok, parkettázások, és bázisredukciós algoritmusok

BSc szakdolgozat

Fazekas Péter László

Témavezető
Dr. Grolmusz Vince
Számítógéptudományi tanszék



ELTE | TTK

Budapest, 2024

Tartalomjegyzék

0. Bevezető

Rácsokkal kapcsolatos problémákkal már a középkortól kezdődően sok matematikus foglalkozott, azonban a rácsokat először Minkowski tárta fel mélyebben, amikor az 1890-es években megalkotta az úgynevezett számok geometriáját. Az általa kidolgozott tételeknek rengeteg számelméleti alkalmazása született, például a diofantikus approximáció terén, és a kvadratikus alakok tanulmányozásában. [Lek87]

A rácsok viszonylag modernebb alkalmazásait mutatja be Conway és Sloane a Sphere packings, Lattices and Groups című könyvükben [Slo99]. Itt a rácsokat alapvető eszközként használják a gömbpakolások és fedések, továbbá a kissing number (érintkezési szám) probléma tanulmányozásánál. Mindezek mellett előkerülnek még a hibajavító kódok, és a Steiner rendszerek.

Ezen dolgozatban az előbb említett területek mélyebb tanulmányozásától eltekintünk, és a fókuszt a rácsokkal kapcsolatos algoritmikus problémákra helyezzük. Ezen témakörben az egyik legfontosabb eredmény az 1980-as évek végén született híres LLL (Lenstra, Lenstra, Lovász) algoritmus, amely polinomiális megoldást nyújt több klasszikus problémára a számítástudományban. Ilyen például egy IP (Integer programming) feladat megoldása fix dimenzióban, és a racionális számtest feletti polinomok faktorizálása.

A számítástudományban egy algoritmikus probléma akkor nehéz, ha az nehéz a legrosszabb esetben. Kriptográfiában az átlagos eset nehézségét célszerű vizsgálni. Ajtai 1990-es munkájában megmutatja, hogy hogyan kell olyan kriptográfiai függvényt építeni, amely feltörése annyira nehéz az átlagos esetben, mint bizonyos nehéz rácsproblémák megoldása a legrosszabb esetben. A rácsalgoritmusok mélyebb megértése kulcsfontosságú, ugyanis a modern kriptográfia ezeken a nehezen megoldható rácsproblémákon alapszik.

Ezen dolgozat fő célja, hogy bevezetést adjon a rácsalgoritmusok világába. Bemutatjuk a legfontosabb algoritmikus problémákat rácsokon, és megpróbáljuk összefoglalni az ezen problémákat megoldó legalapvetőbb algoritmusok geometriai hátterét. Az 1. fejezetben összefoglaljuk a szükséges előismereteket. A 2. fejezetben bemutatjuk a fő algoritmikus problémákat, bemutatjuk a híres LLL algoritmust mint Hermit egy korábbi algoritmusának relaxált verzióját, majd Kannan algoritmusát vizsgáljuk meg megmutatva, hogy az milyen összefüggésben áll egy rácsot geometriailag jellemző ortogonalitási defektussal.

Végül a 3. és 4. fejezetekben bevezetjük a redukciós tartományok fogalmát és ennek segítségével bemutatjuk az LLL algoritmus egy kevésbé kutatott testvérét, amely minimális ortogonalitási defektusú bázist talál az első 4 dimenzióban. Ennek segítségével jobban megértjük az alacsony dimenziós esetet, és talán az LLL algoritmus működését is. Megvizsgáljuk ezen algoritmus futását magasabb dimenzióban, és az algoritmus iterációinak számára egy új felső korlátot adunk.

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Grolmusz Vincének aki ezt a roppant érdekes témát ajánlotta számomra és irányt mutatott ezen hatalmas tudásanyag megismerése felé. Mindig végighallgatott, és hasznos kérdéseket tett fel melyekkel munkámat előre lendítette.

A dolgozat eredményei bemutatásra kerültek a Szegedi AMK konferencián. A konferencián való részvételt az Innovációs és Technológiai Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával finanszírozta.

Önálló munka

A dolgozatban szereplő ábrák a GeoGebra szoftver segítségével készültek.

A leírt eredmények nagy része ismert a szakirodalomban, viszont gyakran ezen tényekre saját bizonyítást találtam. Erre két példát emelnék ki: Az egyik a rácsok determinánsának bevezetése a szakirodalomban találtaktól eltérő módon, átdarabolás segítségével. Ez az 1.2. állításban található. A másik a 3.6. állítás bizonyítása, amely összefüggésbe hozza a gyenge redukciót az alacsony dimenziós rácsok viselkedésével.

Az ortogonalitási defektus egy mérőszám arra, hogy egy rács egy bázisa mennyire „jó”, így ez használható bizonyos bázisredukciós algoritmusok elemzésénél. Habár sok helyen használják az ortogonalitási defektus fogalmát, a fogalom részletesebb bemutatására nem nagyon akad példa. A 2.1. alfejezetben összefoglaltam az ortogonalitási defektus bázisredukcióhoz kapcsolódó legfontosabb tulajdonságait.

Munkám során, amikor próbáltam bizonyos algoritmusokat megérteni, végül a tér bizonyos objektumait véltem felfedezni mögöttük. A 2.10. és 2.14. tételek segítségével összekötöm Kannan SVP-re és CVP-re adott algoritmusát az ortogonalitási defektussal, az általam bevezetett Voronoi-defektussal és az ezekhez tartozó k dimenziós téglatestekkel. A 3. fejezetben bevezettem a redukciós tartományok fogalmát. Számomra ezáltal sokkal átláthatóbbá és érthetőbbé váltak az itt tárgyalt bázisredukciós algoritmusok.

Legjobb tudásom szerint a dolgozat következő eredményei még nem voltak ismertek eddig:

A 3. fejezetben megmutatom, hogy egy alacsony dimenziós rács bázisának ortogonalitási defektusa pontosan akkor minimális, ha a bázis vektorainak hosszai rendre a szukcesszív minimumok. Ilyen, minimális ortogonalitási defektusú bázis megtalálható az LLL algoritmus egy kevésbé kutatott testvérével. Ezeket felhasználva megadom a Hermit konstanshoz hasonló 2.3. definícióban meghatározott δ_k konstans pontos értékét $k = 3$ esetén, továbbá sejtést adok a konstans értékére $k = 4$ esetén, és receptet ennek egy lehetséges bizonyítására. Ezen konstans értéke azért érdekes, mert megmutatja, hogy adott dimenzióban mekkora ortogonalitási defektusú bázis találása még nem reménytelen.

A 4. fejezetben a redukciós tartományok segítségével egy új felső korlátot szabok a 3.1. algoritmus iterációinak számára (4.1 tétel).

1. Rácsok

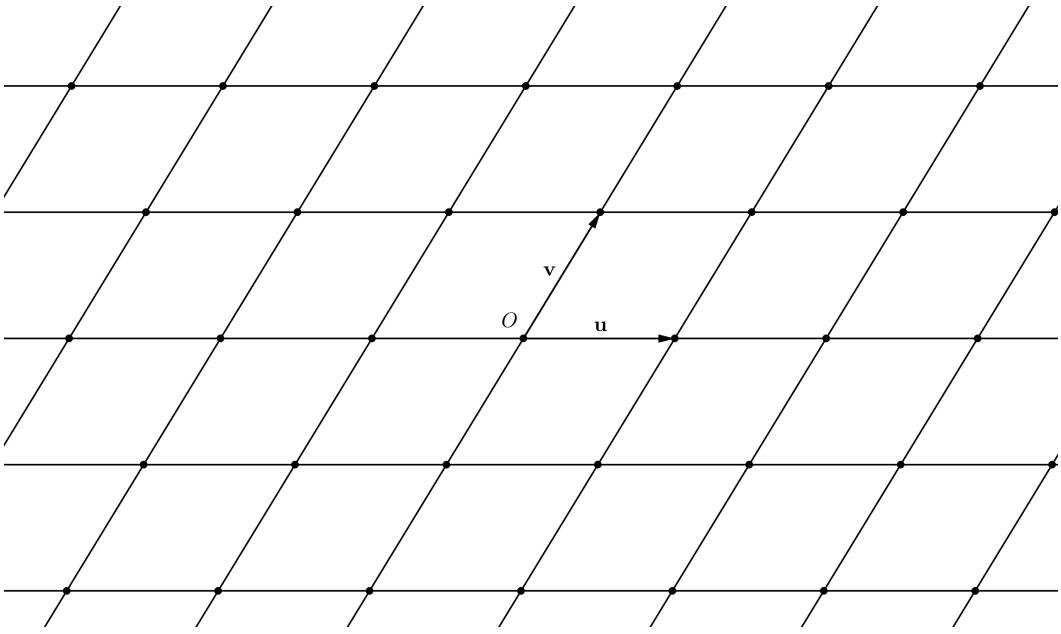
1.1. Mi az, hogy rács?

A legegyszerűbb rács, amit mindenki ismer, az nem más mint a négyzetrács. Ezt megkaphatjuk például úgy, hogy lefedjük az euklideszi síkot azonos oldalhosszúságú négyzetekkel. Persze mindenki tudja, hogy néz ki ez a rács: a négyzeteinket hézagmentesen illesztjük egymáshoz úgy, hogy két szomszédos négyzet érintkező oldalai teljesen egybeessenek.

Bontsuk fel ezt a rácsot alkotóelemeire! Maga a négyzetrács vízszintes és függőleges egyenesekből áll, és persze ne feledkezzünk meg ezen egyenesek metszéspontjairól, azaz a rács pontjairól.

A sík egy általános rácsa annyiban különbözhet az előzőtől, hogy a lefedéshez négyzetek helyett egybevágó paralelogrammákat használunk. Az alkotóelemek is ugyanezek maradnak, csak míg az előbb vízszintes és függőleges egyeneseink voltak, most két egymással nem párhuzamos egyenes szöge akár valamilyen hegyesszög is lehet.

A rácsokat meghatározzák pontjai, de szerencsére a rács ismertetéséhez nem kell mind a végtelen pontot felsorolni. Legyen a rács egyik pontja az O origó. Ez pont a lefedéshez használt egyik paralelogramma sarka. Legyenek az $\mathbf{u},\mathbf{v}$ vektorok azok, amik az O pontból a paralelogramma két O-val szomszédos csúcsába mutatnak. Ekkor a rácsunk pontjai pontosan azon pontok, amelyekbe eljuthatunk az O-ból indulva az $\mathbf{u}$ és $\mathbf{v}$ vektorokkal előre-hátra ugrálva. Az $\mathbf{u}$ és $\mathbf{v}$ vektorok meghatározzák tehát a teljes rácsot.



1.1. ábra. Egy rács a síkon.

Ugyanezen gondolatmenet működik tetszőleges n dimenziós euklideszi térben is. Ekkor terünket n-dimenziós paralelepipedonokkal fedjük le, és a pontok és síkok mellett több dimenziós affin alterek is megjelennek. A rácsot ekkor 2 helyett n darab lineárisan független vektor hatá-

rozza meg. Ahhoz, hogy ezen bonyolultnak tűnő objektumokat jól tudjuk kezelni itt az ideje, hogy fogalmainkat precízen bevezessük.

1.2. Alapok, jelölések

A továbbiakban számunkra a tér mindig n dimenziós euklideszi vektortér lesz, általában az $\mathbb{R}$ számtest felett. Ezt $\mathbb{R}^n$-el jelöljük. $n = 2$ esetén síkról, $n \geq 3$ esetén pedig térről beszélünk. Az euklideszi tér pontjai és vektorai számunkra lényegében ugyanazt fogják jelenteni. Általában vektorokkal dolgozunk, amelyeket mindig vastag kisbetűvel jelöljük, de előfordulhat, hogy pontokról beszélünk. Ekkor ezeket az abc nagybetűivel jelöljük. Ennek megfelelően $\mathbf{0}$ vagy O az origót jelöli.

Ha konkrétan meg akarunk adni egy vektort, akkor azt általában koordinátánkét tesszük meg, és ilyenkor a vektort mindig sorvektorként írjuk fel. Például

$$\mathbf{v} = (0, 0.5, \sqrt{2}, 1/2)$$

azt a $\mathbf{v} \in \mathbb{R}^4$ vektort jelöli, amely koordinátái rendre $0, 0.5, \sqrt{2}, 1/2$. Egy $\mathbf{v}$ vektor i. koordinátáját v_i-vel fogjuk jelölni. Ebben a konkrét esetben $v_1 = 0$, $v_2 = 0.5$, $v_3 = \sqrt{2}$ és $v_4 = 1/2$.

A lineáris transzformációkat/mátrixokat szintén az abc nagybetűivel jelöljük. Konkrét mátrixokat szögletes zárójelekkel adunk meg, például

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$$

és

$$B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

módon. Mátrixot-mátrixal, vektort-mátrixal értelemszerűen szorzunk. Például

$$BA = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 7 & 9 \end{bmatrix},$$

továbbá $\mathbf{v} = (1, 1, 1)$ esetén

$$A\mathbf{v} = (6, 15)$$

és $\mathbf{v} = (1, 1)$ esetén pedig

$$\mathbf{v}A = (5, 7, 9).$$

Ha adottak a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{R}^n$ vektorok akkor

$$A = \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$$

esetén A a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektorok egymás alá írásával kapott mátrixot jelöli, azaz ekkor

$$A = \begin{bmatrix} v_{1,1} & v_{1,2} & \ldots & v_{1,n} \\ v_{2,1} & v_{2,2} & \ldots & v_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ v_{k,1} & v_{k,2} & \ldots & v_{k,n} \end{bmatrix} \tag{1.2.1}$$

ahol $v_{i,j}$ a $\mathbf{v}_i$ vektor j. koordinátája.

Az új jelölések bevezetésére mostantól a $:=$ jelet használjuk. Például mi az $\mathbb{R}^n$ euklideszi téren skalárszorzás alatt a szokásos skalárszorzást értjük. Ezt a következő módon vezetjük be: az $\mathbf{u},\mathbf{v}\in\mathbb{R}^n$ vektorok skalárszorzátát

$$\mathbf{u}\cdot\mathbf{v} := u_1v_1 + u_2v_2 + \ldots + u_nv_n, \tag{1.2.2}$$

egy $\mathbf{v}\in\mathbb{R}^n$ vektor önmagával vett skalárszorzatát pedig

$$\mathbf{v}^2 := \mathbf{v}\cdot\mathbf{v} \tag{1.2.3}$$

módon jelöljük.

Egy $\mathbf{v}\in\mathbb{R}^n$ vektor hossza mindig a szokásos 2-normában értendő, amit a következő módon adunk meg:

$$\|\mathbf{v}\| := \sqrt{\mathbf{v}^2}. \tag{1.2.4}$$

A távolság fogalmát az ezen norma által indukált metrika adja meg. Adott $\mathbf{u},\mathbf{v}\in\mathbb{R}^n$ esetén ezen vektorok által meghatározott A és B pontok távolsága tehát

$$\mathrm{d}(A,B) = \mathrm{d}(\mathbf{u},\mathbf{v}) := \|\mathbf{v}-\mathbf{u}\|. \tag{1.2.5}$$

Legyenek adottak a $G,H\subset\mathbb{R}^n$ halmazok, egy $\mathbf{v}\in\mathbb{R}^n$ vektor, és egy $x\in\mathbb{R}$ konstans. A $\mathbf{v}$ vektor és G halmaz összege alatt a

$$\mathbf{v}+G = G+\mathbf{v} := \{\mathbf{v}+\mathbf{g} \mid \mathbf{g}\in G\} \tag{1.2.6}$$

halmazt, a G halmaz és x konstans szorzatán a

$$xG = Gx := \{x\mathbf{g} \mid \mathbf{g}\in G\} \tag{1.2.7}$$

a G és H halmazok összegén a

$$G+H := \{\mathbf{g}+\mathbf{h} \mid \mathbf{g}\in G,\ \mathbf{h}\in H\} \tag{1.2.8}$$

halmazt, a H halmaz ellentetjén a

$$-H := \{-\mathbf{h} \mid \mathbf{h}\in H\} \tag{1.2.9}$$

halmazt, a H és G halmazok különbségén pedig a

$$G-H := G+(-H) \tag{1.2.10}$$

halmazt értjük.

Adott $G\subset\mathbb{R}^n$ halmaz esetén a G által generált alteret

$$[G] := \{x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + \ldots + x_k\mathbf{g}_k \mid k\in\mathbb{N},\ \forall i\colon x_i\in\mathbb{R},\ \mathbf{g}_i\in G\} \tag{1.2.11}$$

módon jelöljük. Ha adottak a $\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_k\in\mathbb{R}^n$ lineárisan független vektorok, akkor az általuk generált k dimenziós alteret

$$[\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_k] := \{x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \ldots + x_k\mathbf{v}_k \mid x_1,x_2,\ldots,x_k\in\mathbb{R}\} \tag{1.2.12}$$

módon jelöljük. Az eddigi jelölések segítségével adott $\mathbf{v} \in \mathbb{R}^n$ vektor esetén felírhatjuk a $[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k]$ lineáris altér $\mathbf{v}$ vektorral való eltoltjaként kapott

$$\mathbf{v} + [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k]$$

k dimenziós affin alteret. Az $\mathbb{R}^n$ összes affin alterének halmazát jelölje $\mathscr{A}_n$. Egy $A \in \mathscr{A}_n$ affin altér dimenzióját

$$\dim A \tag{1.2.13}$$

jelöli.

Amennyiben adott egy $G \subset \mathbb{R}^n$ halmaz, akkor ezen halmaz dimenziója alatt, az őt tartalmazó legszűkebb affin altér dimenzióját értjük. Ezt precízen a következő módon definiálhatjuk:

$$\dim G := \dim \bigcap_{\substack{A \in \mathscr{A}_n \\ G \subset A}} A. \tag{1.2.14}$$

Legyen $a < b \in \mathbb{R}$. Ekkor jelöljék

$$[a,b],\ ]a,b[,\ [a,b[,\ ]a,b] \tag{1.2.15}$$

rendre a balról és jobbról zárt, balról és jobbról nyílt, balról zárt jobbról nyílt, balról nyílt jobbról zárt a és b közötti intervallumot.

Az olyan $G \subset \mathbb{R}^n$ halmazokat, amelyekre

$$-G = G \tag{1.2.16}$$

0-*szimmetrikus* halmazoknak nevezzük. Egy adott $H \subset \mathbb{R}^n$ korlátos halmaz átmérőjén a

$$\operatorname{diam}(H) := \sup_{\mathbf{u},\mathbf{v} \in H} \mathrm{d}(\mathbf{u}, \mathbf{v}) \tag{1.2.17}$$

valós számot, sugarán pedig a

$$\operatorname{rad}(H) := \operatorname{diam}(H)/2 \tag{1.2.18}$$

valós számot értjük. Amennyiben egy $G \subset \mathbb{R}^n$ korlátos halmaz **0**-szimmetrikus, akkor

$$\operatorname{rad}(H) = \sup_{\mathbf{v} \in H} \|\mathbf{v}\|. \tag{1.2.19}$$

Azt mondjuk, hogy egy $D \subset \mathbb{R}^n$ halmaz *diszkrét*, ha létezik egy $\varepsilon > 0$ valós szám, hogy tetszőleges $\mathbf{d}, \mathbf{d}' \in D$ esetén

$$\varepsilon \leq \mathrm{d}(\mathbf{d}, \mathbf{d}'). \tag{1.2.20}$$

A diszkrét halmazok elemszáma véges, vagy megszámlálhatóan végtelen. Ennek megmutatásához először vegyük a $\delta\mathbb{Z}^n$ halmazt, ahol $0 < \delta \in \mathbb{R}$. Ismert tény, hogy ezen halmaznak megszámlálhatóan végtelen eleme van. Legyen δ akkora, hogy

$$H = [-\delta/2, \delta/2[\times [-\delta/2, \delta/2[\times \ldots \times [-\delta/2, \delta/2[$$

pont az ε átmérőjű **0** súlypontú n dimenziós „balról nyílt jobbról zárt” kocka legyen. Ekkor a

$$\mathscr{H} = \{\mathbf{v} + H \mid \mathbf{v} \in \delta\mathbb{Z}^n\}$$

halmazrendszer az $\mathbb{R}^n$ tér egy partíciója, amely megszámlálhatóan végtelen sok egybevágó kockából áll. Mivel tetszőleges $H' \in \mathscr{H}$ halmazban a D halmaznak legfeljebb 1 eleme lehet, így D tényleg véges, vagy megszámlálhatóan végtelen elemszámú.

Az előzőekből az is látszik, hogy amennyiben adott egy $K \subset \mathbb{R}^n$ korlátos halmaz, és egy $D \subset \mathbb{R}^n$ diszkrét halmaz, akkor a

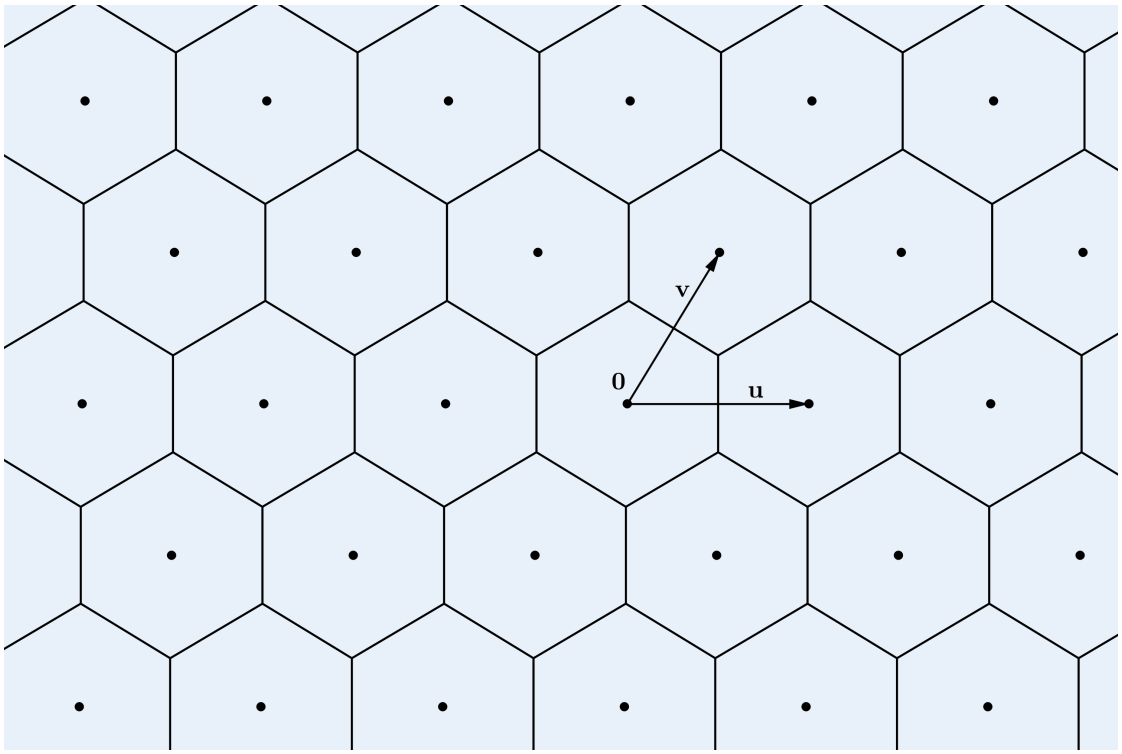
$$D \cap K$$

halmaz véges elemű, ugyanis tetszőleges K korlátos halmaz lefedhető véges sok $\mathscr{H}$-beli kockával.

Általában, ha adott egy k dimenziós $L \subset \mathbb{R}^n$ rács, és egy olyan $G \subset [L]$ halmaz, hogy a

$$G + \mathbf{b} \qquad \mathbf{b} \in L \tag{1.2.21}$$

módon adott halmazrendszer halmazai legfeljebb a határukon érintkeznek, továbbá lefedik a teljes $[L]$ alteret, akkor ezt a halmazrendszert az $[L]$ altér egy *parkettázásának* hívjuk. Erre látható egy egyszerű példa az 1.2. ábrán.



1.2. ábra. A sík egy parkettázása.

A $\mathbf{0} \neq \mathbf{u} \in \mathbb{R}^n$ és $\mathbf{0} \neq \mathbf{v} \in \mathbb{R}^n$ vektorok által bezárt $\alpha \in [0, \pi]$ szöget

$$\arg(\mathbf{u}, \mathbf{v}) := \alpha = \arccos \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|} \tag{1.2.22}$$

módon definiáljuk (A Cauchy–Schwarz-egyenlőtlenség szerint $|\mathbf{u} \cdot \mathbf{v}| \leq \|\mathbf{u}\| \|\mathbf{v}\|$, így ez a kifejezés értelmes). Ha ezt el akarjuk képzelni, akkor erre gondolhatunk úgy, mint az $\mathbf{u}, \mathbf{v}$ vektorok által az $[\mathbf{u}, \mathbf{v}]$ síkban bezárt szög. Ha $\mathbf{u} = \mathbf{0}$ vagy $\mathbf{v} = \mathbf{0}$ akkor az általuk bezárt szög legyen $\pi/2$.

Ezek szerint egy $\mathbf{u}$ és $\mathbf{v}$ vektor pontosan akkor merőleges egymásra, ha $\mathbf{u} \cdot \mathbf{v} = 0$. Az $\mathbf{u}$ és $\mathbf{v}$ vektorok merőlegességét jelölje

$$\mathbf{u} \perp \mathbf{v}. \tag{1.2.23}$$

Amennyiben adott egy $W \subset \mathbb{R}^n$ halmaz, akkor legyen

$$W^\perp := \{\mathbf{u} \in \mathbb{R}^n \mid \forall \mathbf{w} \in W \colon \mathbf{u} \perp \mathbf{w}\} \tag{1.2.24}$$

a W-re merőleges altér. Ismert tény, hogy amennyiben a $W \subset \mathbb{R}^n$ halmaz egy k dimenziós altér, akkor $W^\perp$ egy $n-k$ dimenziós altér, továbbá tetszőleges $\mathbf{v} \in \mathbb{R}^n$ vektor esetén $\exists! \, \mathbf{w} \in W$ és $\exists! \, \mathbf{w}^\perp \in W^\perp$, hogy

$$\mathbf{v} = \mathbf{w} + \mathbf{w}^\perp. \tag{1.2.25}$$

Ekkor a $\mathbf{w}$ vektort a $\mathbf{v}$ vektor W altérbe eső komponensének hívjuk, és erre a

$$\mathrm{proj}_W(\mathbf{v}) \tag{1.2.26}$$

jelölést, a $\mathbf{w}^\perp$ vektort pedig a W altérre merőleges komponensének hívjuk és erre a

$$\mathrm{proj}_W^\perp(\mathbf{v}) \tag{1.2.27}$$

jelölést használjuk. Legyenek adottak a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{R}^n$ lineárisan független vektorok és egy tetszőleges $\mathbf{v} \in \mathbb{R}^n$ vektor. Adott i index esetén legyen $W_i = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i]$. Az egyszerűség kedvéért bevezetjük a

$$\mathrm{proj}_i(\mathbf{v}) := \mathrm{proj}_{W_i}(\mathbf{v}) \tag{1.2.28}$$

és

$$\mathrm{proj}_i^\perp(\mathbf{v}) := \mathrm{proj}_{W_i}^\perp(\mathbf{v}) \tag{1.2.29}$$

jelöléseket.

Legyenek adottak a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{R}^n$ lineárisan független vektorok. Ekkor a

$$\begin{aligned}
\mathbf{v}_1^* &:= \mathbf{v}_1 \\
\mathbf{v}_2^* &:= \mathrm{proj}_1^\perp(\mathbf{v}_2) \\
\mathbf{v}_3^* &:= \mathrm{proj}_2^\perp(\mathbf{v}_3) \\
&\ldots \\
\mathbf{v}_k^* &:= \mathrm{proj}_{k-1}^\perp(\mathbf{v}_k)
\end{aligned} \tag{1.2.30}$$

módon definiált $\mathbf{v}_1^*, \mathbf{v}_2^*, \ldots, \mathbf{v}_k^*$ lineárisan független vektorokat a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektorok Gram-Schmidt ortogonalizált vektorainak hívjuk. ($k = n$ esetén gyakran a Gram-Schmidt ortogonalizált bázis elnevezést használjuk) Ekkor

$$\begin{aligned}
\mathbf{v}_1 &= \mu_{1,1}\mathbf{v}_1^* \\
\mathbf{v}_2 &= \mu_{2,1}\mathbf{v}_1^* + \mu_{2,2}\mathbf{v}_2^* \\
\mathbf{v}_3 &= \mu_{3,1}\mathbf{v}_1^* + \mu_{3,2}\mathbf{v}_2^* + \mu_{3,3}\mathbf{v}_3^* \\
&\ldots \\
\mathbf{v}_k &= \mu_{k,1}\mathbf{v}_1^* + \mu_{k,2}\mathbf{v}_2^* + \mu_{k,3}\mathbf{v}_3^* + \ldots + \mu_{k,k}\mathbf{v}_k^*,
\end{aligned} \tag{1.2.31}$$

ahol minden i index esetén $\mu_{i,i} = 1$. Az így kapott $(\mu_{i,j})_{0<j\leq i}$ együtthatókat a bázis Gram-Schmidt együtthatóinak hívjuk, a $\mu_{i,j}$ együtthatót pedig a $\mathbf{v}_i$ vektor j. Gram-Schmidt együtthatójának nevezzük.

Legyen adott egy $W \subset \mathbb{R}^n$ altér és egy $\mathbf{v} \in \mathbb{R}^n$ vektor. Legyen $\mathbf{v}^* = \text{proj}_W^{\perp}(\mathbf{v})$ a $\mathbf{v}$ vektor W altérre merőleges komponense, és $\mathbf{w} = \text{proj}_W(\mathbf{v})$ a $\mathbf{v}$ vektor W altérbe eső komponense. Ekkor a $\mathbf{v}$ vektor és W altér által bezárt α szöget a következő módon értelmezzük:

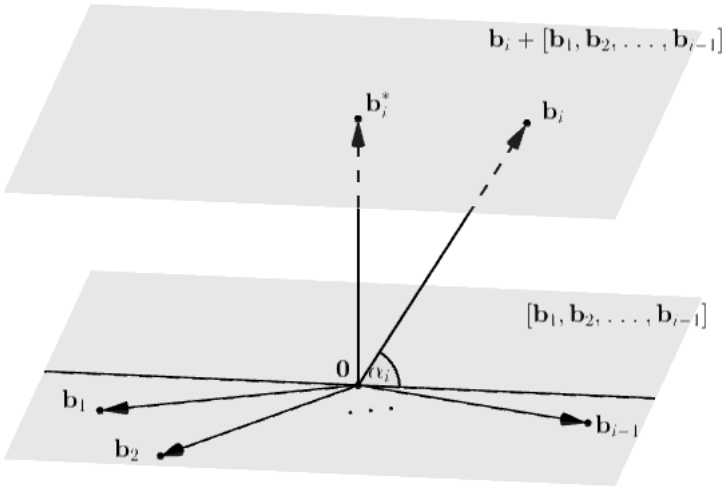
$$\alpha = \arg(W, \mathbf{v}) = \arg(\mathbf{v}, W) := \arg(\mathbf{v}, \mathbf{w}) = \pi/2 - \arg(\mathbf{v}, \mathbf{v}^*). \tag{1.2.32}$$

Ekkor

$$\sin\alpha = \frac{\mathbf{v}\cdot\mathbf{v}^*}{\|\mathbf{v}\|\|\mathbf{v}^*\|} = \frac{\|\mathbf{v}^*\|^2}{\|\mathbf{v}\|\|\mathbf{v}^*\|} = \frac{\|\mathbf{v}^*\|}{\|\mathbf{v}\|}, \tag{1.2.33}$$

és

$$\cos\alpha = \frac{\mathbf{w}\cdot\mathbf{v}}{\|\mathbf{v}\|\|\mathbf{w}\|} = \frac{\|\mathbf{w}\|^2}{\|\mathbf{v}\|\|\mathbf{w}\|} = \frac{\|\mathbf{w}\|}{\|\mathbf{v}\|}. \tag{1.2.34}$$



1.3. ábra. A $\mathbf{b}_i$ vektor Gram-Schmidt ortogonalizáltja, és az α_i szög.

A térfogat mérésére a Jordan-mértéket használjuk. Legyenek adottak a $a_1, a_2, \ldots, a_n \in \mathbb{R}$ és a $b_1, b_2, \ldots, b_n \in \mathbb{R}$ valós számok ahol minden i index esetén $a_i \leq b_i$. Egy

$$[a_1, b_1] \times [a_2, b_2] \times \ldots \times [a_n, b_n] \subset \mathbb{R}^n$$

n dimenziós téglatest térfogata ezen mérték szerint a

$$(b_1 - a_1) \cdot (b_2 - a_2) \cdot \ldots \cdot (b_n - a_n)$$

szorzat. Adott $K \subset \mathbb{R}^n$ halmaz pontosan akkor Jordan-mérhető, ha a K-ba írt n dimenziós diszjunkt téglatestek össztérfogatának felső határa megegyezik a K halmazt lefedő diszjunkt n dimenziós téglatestek össztérfogatának alsó határával. Ebben az esetben K térfogatát

$$\text{vol}\, K \tag{1.2.35}$$

jelöli, amely megegyezik ezen határokkal (Precízebb definícióért lásd [Ver07]). Ismert tény, hogy tetszőleges $K \subset \mathbb{R}^n$ konvex és korlátos halmaz Jordan-mérhető. Amennyiben adott egy k dimenziós $A \subset \mathbb{R}^n$ affin altér, ahol $k < n$, és egy $K \subset A$ halmaz, akkor

$$\operatorname{vol} K$$

alatt a K halmaz A affin altérbeli k dimenziós térfogatát értjük, azaz azonosítjuk az affin alterünket a k dimenziós $\mathbb{R}^k$ euklideszi térrel, és K térfogatát itt mérjük. Habár ez a jelölés ellentmondásra adhatna okot, ugyanis K „igazi" térfogata ebben az esetben 0 volna, mi ezen dolgozatban csak olyan halmazok térfogatát fogjuk vizsgálni, ahol ez egyáltalán nem fog problémát okozni. Ezen dolgozatban a Jordan-mérhető halmazokat az egyszerűség kedvéért csak mérhető halmazoknak fogjuk nevezni.

Az $\mathbb{R}^n$ euklideszi tér $\mathbf{0}$ középpontú $r \in \mathbb{R}$ sugarú zárt gömbjét

$$\mathrm{B}(r) := \{\mathbf{v} \in \mathbb{R}^n \mid \|\mathbf{v}\| \leq r\} \tag{1.2.36}$$

módon jelöljük. Általában a tér n dimenziója egyértelműen kiderül a szövegkörnyezetből, viszont ha hangsúlyozni akarjuk a dimenziószámot, akkor a

$$\mathrm{B}_n(r) \tag{1.2.37}$$

jelölést használjuk.

Adott $x \in \mathbb{R}$ valós szám esetén az

$$\lfloor x \rfloor, \lceil x \rceil, \lfloor x \rceil \tag{1.2.38}$$

jelölések rendre x alsó egészrészét, felső egészrészét, és egészrészét jelentik. (x egész része az x valós számhoz legközelebb eső egész szám. Amennyiben x pont két egész szám között helyezkedik el, akkor $\lfloor x \rceil$ jelentse x felső egészrészét.)

Ismert tény, hogy

$$\operatorname{vol} \mathrm{B}_n(r) = \frac{\pi^{\lfloor n/2 \rfloor} r^n}{(n/2)!} \tag{1.2.39}$$

ahol $(n/2)! := (n/2) \cdot (n/2-1) \cdot \ldots \cdot (n/2 - \lfloor n/2 - 1/2 \rfloor)$.

Ismert még, hogy a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in \mathbb{R}^n$ lineárisan független vektorok által kifeszített

$$P = \{x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \ldots + x_k\mathbf{v}_k \mid \forall i\colon x_i \in \mathbb{R},\ 0 \leq x_i \leq 1\}$$

paralelepipedon térfogatát megkaphatjuk a következő módokon:

$$\operatorname{vol} P = \|\mathbf{v}_1^*\|\|\mathbf{v}_2^*\| \ldots \|\mathbf{v}_k^*\| = \sqrt{\det AA^T} \tag{1.2.40}$$

ahol $A = \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$, és $\mathbf{v}_1^*, \mathbf{v}_2^*, \ldots, \mathbf{v}_k^*$ a $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ bázis Gram-Schmidt ortogonalizáltja.

1.3. Rácsok

1.1. Definició. Legyen adott az $\mathbb{R}^n$ euklideszi tér k darab $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektora. Ezen vektorok egész együtthatós lineáris kombinációinak halmazát *rácsnak* nevezzük, és ezt a halmazt

$$L = L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) := \{s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \ldots + s_k\mathbf{b}_k \mid s_1, s_2, \ldots, s_k \in \mathbb{Z}\}$$

módon jelöljük. Ekkor L a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok által *generált* rács, és a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorokat az L rács *bázisának* hívjuk.

Előfordulhat, hogy néhány egymástól nem feltétlen független $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ vektor egész együtthatós lineáris kombinációinak halmaza is egy rácsot ad eredményül, sőt ez még akkor is megtörténhet, ha megszámlálhatóan végtelen sok vektor áll rendelkezésünkre. Általában amennyiben adott egy $D \subset \mathbb{R}^n$ diszkrét halmaz, akkor az ez által generált „rácsra" a

$$L(D) := \{s_1\mathbf{d}_1 + s_2\mathbf{d}_2 + \ldots + s_m\mathbf{d}_m \mid m \in \mathbb{N},\ \mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_m \in D,\ s_1, s_2, \ldots, s_m \in \mathbb{Z}\} \quad (1.3.1)$$

jelölést használjuk.

Egy rács dimenziója (1.2.14) szerint az őt generáló lineárisan független vektorok száma. Amennyiben egy $L \subset \mathbb{R}^n$ rács dimenziója n, akkor azt mondjuk, hogy L *teljes dimenziós*. A k dimenziós rácsok halmazára mostantól az

$$\mathscr{L}_k := \{L \mid L \text{ egy } k \text{ dimenziós rács.}\} \quad (1.3.2)$$

jelölést használjuk.

A fejezet legelején leírt példa a $\mathbb{Z}^2 \subset \mathbb{R}^2$ egész koordinátájú pontok által meghatározott rács. Ezt a

$$\mathbf{e}_1 = (1,0)$$
$$\mathbf{e}_2 = (0,1)$$

vektorok generálják, de láthatóan ugyanezen rács megkapható, mint a

$$\mathbf{u} = (1,0)$$
$$\mathbf{v} = (s,1)$$

vektorok által generált rács is, ahol $s \in \mathbb{Z}$ tetszőleges egész szám. Ezek szerint a $\mathbb{Z}^2$ rácsnak végtelen sok különböző bázisa van. Ehhez hasonlóan meggondolható, hogy általában a legalább 2 dimenziós rácsoknak is végtelen sok különböző bázisa van.

Most, hogy pontjainak segítségével megadtunk egy rácsot, írjuk le a rács többi alkotóelemét is! Legyen adott egy k dimenziós L rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Ekkor a bázishoz tartozó

$$P = \{x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \ldots + x_k\mathbf{b}_k \mid \forall i\colon x_i \in \mathbb{R},\ 0 \le x_i \le 1\}$$

fundamentális paralelepipedon $\mathbf{b} + P$ eltoltjai ahol $\mathbf{b} \in L$ lefedik a teljes $[L]$ alteret, továbbá két ilyen politóp csak a határukon érintkezhet, azaz

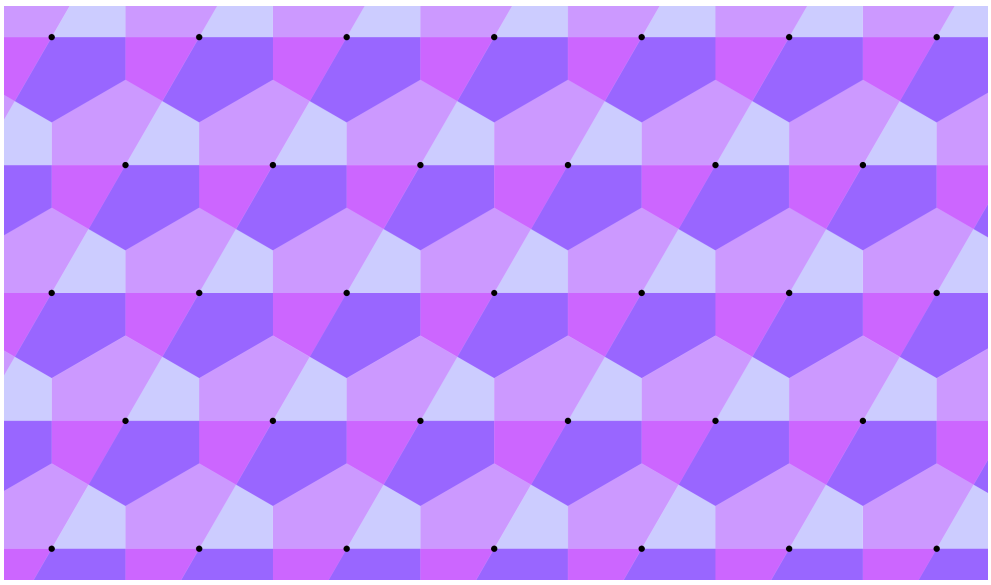
$$\mathbf{b} + P \qquad \mathbf{b} \in L$$

az $[L]$ altér egy parkettázása.

Általában egy rács determinánsát P-hez tartozó bázis determinánsának abszolút értékeként szokták definiálni. Ezt általában úgy teszik meg, hogy először belátják, hogy két bázis pontosan akkor feszíti ki ugyanazon rácsot, ha egy ± 1 determinánsú (unimoduláris) lineáris transzformáció segítségével az egyik a másikba vihető. Ekkor két különböző bázis determinánsának abszolút értéke meg kell hogy egyezzen, tehát a rács determinánsa jól definiált. Egy ilyen bizonyítás például megtalálható a [Lek87] könyvben, számunkra azonban többet mond, ha egy kicsit más irányból közelítjük meg ezen fogalmat.

A következő állításban megmutatjuk, hogy ha leparkettázuk az euklideszi terünket egybevágó testekkel úgy, hogy ezen testeket egy rács pontjaiba illesztjük, akkor ezen testek térfogata

csakis egy értéket vehet fel. Ezt úgy mutatjuk meg, hogy belátjuk, hogy két ilyen test mindig átdarabolható egymásba. Erre a 1.4. ábrán egy konkrét példa látható egy síkbeli rács esetén.



1.4. ábra. Két különböző parkettázás átdarabolása egymásba.

1.2. Állítás. *Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. Legyenek $G,H \subset [L]$ olyan mérhető halmazok, hogy a*

$$\mathscr{H} = \{\mathbf{b}+H \mid \mathbf{b} \in L\}$$

és

$$\mathscr{G} = \{\mathbf{b}+G \mid \mathbf{b} \in L\}$$

halmazrendszerek az $[L]$ altér egy-egy parkettázását (lásd (1.2.21)) alkotják. Ekkor

$$\operatorname{vol} G = \operatorname{vol} K.$$

Bizonyítás. Az állítást úgy bizonyítjuk, hogy megmutatjuk, hogy a H halmaz átdarabolható a G halmazba. Mivel $\mathscr{G}$ egy parkettázás, így

$$H = \bigcup_{\mathbf{v}\in L} (\mathbf{v}+G) \cap H.$$

Legyen

$$H_{\mathbf{v}} := (\mathbf{v}+G) \cap H$$

és

$$G_{\mathbf{v}} := H_{\mathbf{v}} - \mathbf{v} \subset G.$$

Indirekt tegyük fel, hogy léteznek $\mathbf{u} \neq \mathbf{v}$ rácsvektorok, hogy a $G_{\mathbf{u}}$ és $G_{\mathbf{v}}$ halmazoknak van egy $\mathbf{g}$ közös belső pontjuk. Ekkor a

$$\mathbf{h}_1 := \mathbf{g}+\mathbf{u}$$

és

$$\mathbf{h}_2 := \mathbf{g}+\mathbf{v}$$

pontok a H halmaz két különböző belső pontjai. Ez nem lehet, mivel ekkor $\mathbf{h}_1 = \mathbf{h}_2 + \mathbf{u} - \mathbf{v}$ és így $\mathbf{h}_1$ nemcsak a H, hanem a $H + \mathbf{u} - \mathbf{v}$ halmaznak is belső pontja lenne. Ez nem teljesülhet, ugyanis $\mathscr{H}$ egy parkettázás.

Ezek szerint tetszőleges $\mathbf{u} \neq \mathbf{v}$ rácsvektorok esetén a $G_\mathbf{u}$ és $G_\mathbf{v}$ halmazok legfeljebb a határukon érintkezhetnek és így

$$\operatorname{vol} H = \sum_{\mathbf{v}\in L} \operatorname{vol} H_\mathbf{v} = \sum_{\mathbf{v}\in L} \operatorname{vol} G_\mathbf{v} \leq \operatorname{vol} G.$$

Ugyanezt a H és G halmazok szerepcseréjével újra végigjátszva a fordított egyenlőtlenséget is megkapjuk, tehát az állítást beláttuk. □

Ezek szerint értelmes a következő definíció:

1.3. Definició. Legyen adott egy k dimenziós L rács, és egy G korlátos mérhető halmaz, hogy

$$\mathbf{b} + G \qquad \mathbf{b} \in L$$

az $[L]$ egy parkettázását adja. Ekkor az L rács *térfogata* alatt a G halmaz térfogatát értjük és ezt

$$\operatorname{vol} L := \operatorname{vol} G \tag{1.3.3}$$

módon jelöljük.

Ezt szokás még az L rács determinánsának is hívni. Mi viszont most a rácsokat jobban geometriai, mint algebrai objektumként kezeljük, ezért beszélünk inkább térfogatról.

A bevezetőben leírtuk, hogy mik is egy rács fő alkotóelemei. Ezek közül már csak egyet nem öntöttünk precíz formába.

1.4. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Ekkor adott $0 < i < k$ index és $s_{i+1}, s_{i+2}, \ldots, s_k \in \mathbb{Z}$ egész számok esetén a

$$F = \mathrm{F}(s_{i+1}, s_{i+2}, \ldots, s_k) := [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i] + s_{i+1}\mathbf{b}_{i+1} + s_{i+2}\mathbf{b}_{i+2} + \ldots + s_k\mathbf{b}_k$$

módon meghatározott affin alteret a rács egy *lapjának* nevezzük. $i = 1$ esetén lap helyett inkább az él kifejezést használjuk.

1.5. Állítás. *Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen adott egy i index és legyenek adottak az $s_{i+1}, s_{i+2}, \ldots, s_k \in \mathbb{Z}$ egész számok. Legyen adott a rács*

$$F = \mathrm{F}(s_{i+1}, s_{i+2}, \ldots, s_k)$$

lapja. Legyen $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis Gram-Schmidt ortogonalizáltja, és legyenek $x_1, x_2, \ldots, x_k \in \mathbb{R}$ olyan valós számok, hogy

$$s_{i+1}\mathbf{b}_{i+1} + s_{i+2}\mathbf{b}_{i+2} + \ldots + s_k\mathbf{b}_k = x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^*.$$

Ekkor F minimális hosszúságú vektora

$$x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*.$$

Bizonyítás. Mivel

$$\begin{aligned} F &= [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i] + s_{i+1}\mathbf{b}_{i+1} + s_{i+2}\mathbf{b}_{i+2} + \ldots + s_k\mathbf{b}_k &= \\ &= [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i] + x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^* &= \\ &= [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i] + x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*, \end{aligned}$$

így tetszőleges $\mathbf{v} \in F$ előáll, mint

$$\mathbf{v} = \mathbf{v}' + x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*$$

ahol $\mathbf{v}' \in [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i]$. Ezek szerint

$$\begin{aligned} \|\mathbf{v}\|^2 = \|\mathbf{v}' + x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*\|^2 = \|\mathbf{v}'\|^2 + \|x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*\|^2 \geq \\ \geq \|x_{i+1}\mathbf{b}_{i+1}^* + x_{i+2}\mathbf{b}_{i+2}^* + \ldots + x_k\mathbf{b}_k^*\|^2 \end{aligned}$$

így az állítást beláttuk. □

Ha a fenti állításban s_m a maximális indexű egész szám amely nem 0, akkor a Gram-Schmidt ortogonalizált definíciója szerint $x_m = s_m$, és $j > m$ esetén $x_j = 0$. Ezek szerint ekkor tetszőleges $\mathbf{v} \in F$ esetén

$$\|\mathbf{v}\| \geq |s_m| \cdot \|\mathbf{b}_m^*\| \geq \|\mathbf{b}_m^*\|. \tag{1.3.4}$$

1.6. Állítás. *Az $\mathbb{R}^n$ halmaz rácsai pontosan az $\mathbb{R}^n$ halmaz diszkrét (lásd (1.2.20)) additív részcsoportjai.*

Bizonyítás. Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. Legyen az L rács egy bázisa $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$, és legyen ezen bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$.

Az, hogy L az $\mathbb{R}^n$ egy additív részcsoportja a rácsok definíciójából azonnal adódik. Amit be szeretnénk látni, hogy diszkrét is. Mivel $\mathbf{0} \in L$ így elég megmutatni, hogy $\exists 0 < \varepsilon \in \mathbb{R}$, hogy a $\mathrm{B}(\varepsilon)$ gömb csak a $\mathbf{0}$ rácspontot tartalmazza, ekkor ugyanis két különböző rácspont távolságának legalább ε-nak kell lennie. Legyen

$$0 < \varepsilon < \min_i \|\mathbf{b}_i^*\|.$$

Ekkor (1.3.4) szerint tetszőleges $\mathbf{0} \neq \mathbf{b} \in L$ rácspontra

$$\|\mathbf{b}\| > \varepsilon$$

teljesül, így ezzel az állítás egyik irányát beláttuk.

Most legyen adott az $\mathbb{R}^n$ egy $k > 0$ dimenziós L diszkrét addítív részcsoportja. Úgy bizonyítjuk be az állítás másik irányát, hogy rekurzív megadjuk a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorokat, amelyekre

$$L = L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

teljesül. Mivel L egy additív részcsoport, így az $\mathbf{0} \in L$, és mivel $\dim L > 0$ így létezik egy $\mathbf{0} \neq \mathbf{v} \in L$ vektor is. Mivel L diszkrét, így $L \cap \mathrm{B}(\|\mathbf{v}\|)$ halmaz véges elemszámú. Legyen $\mathbf{b}_1 \in L$ az a vektor amelyre

$$\|\mathbf{b}_1\| = \min_{\mathbf{b} \in L \cap \mathrm{B}(\|\mathbf{v}\|)} \|\mathbf{b}\|$$

teljesül. Ekkor $\mathbf{b}_1$ az L halmaz legrövidebb nem $\mathbf{0}$ vektora. Most tegyük fel, hogy már meghatároztuk a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$ vektorokat, ahol $i-1 < k$. Legyen

$$P = \{x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \ldots + x_{i-1}\mathbf{b}_{i-1} \mid \forall j\colon 0 \leq x_j \leq 1\}$$

a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$ vektorok által generált rács alappolitópja. Tetszőleges $\mathbf{b} \in L$ vektor

$$\mathbf{b} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \ldots + x_{i-1}\mathbf{b}_{i-1} + \mathbf{b}^{\perp}$$

alakba írható, ahol $\mathbf{b}^{\perp} \in [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]^{\perp}$. Vezessük be a

$$P(\mathbf{b}) := (x_1 - \lfloor x_1 \rfloor)\mathbf{b}_1 + (x_2 - \lfloor x_2 \rfloor)\mathbf{b}_2 + \ldots (x_{i-1} - \lfloor x_{i-1} \rfloor)\mathbf{b}_{i-1} + \mathbf{b}^{\perp}$$

jelölést. Mivel L egy additív részcsoport így $\mathbf{b} \in L$ esetén $P(\mathbf{b}) \in L$.

Legyen $\mathbf{v} \in L \setminus [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ tetszőleges, és legyen

$$P' := P + \mathrm{B}(\|\mathbf{v}\|).$$

Mivel a P' egy korlátos halmaz, és L diszkrét, így a

$$Q := P' \cap L \setminus [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$$

halmaznak véges sok eleme van. Válasszuk meg a $\mathbf{b}_i \in L \setminus [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ vektort úgy, hogy

$$\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\| = \min_{\mathbf{b} \in Q} \|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b})\|$$

teljesüljön. Ekkor mivel tetszőleges $\mathbf{b} \in L$ esetén

$$\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b})\| = \|\mathrm{proj}_{i-1}^{\perp}(P(\mathbf{b}))\| \geq \min_{\mathbf{b} \in Q} \|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b})\|$$

így

$$\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\| = \min_{\mathbf{b} \in L} \|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b})\| \tag{1.3.5}$$

is teljesül, tehát ezek szerint $\mathbf{b}_i$ az L rács $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ altérhez legközelebb eső vektora.

Rekurzív meghatároztuk a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in L$ lineárisan független vektorokat. Mivel L egy k dimenziós halmaz, így tetszőleges $\mathbf{b} \in L$ esetén léteznek $s_1, s_2, \ldots, s_k \in \mathbb{R}$ valós számok, hogy

$$\mathbf{b} = s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \ldots + s_k\mathbf{b}_k.$$

Amit meg szeretnénk mutatni, hogy az $s_1, s_2, \ldots, s_k$ számok igazából egészek. Tegyük fel indirekt, hogy ez nem teljesül és legyen m maximális index, hogy $s_m \in \mathbb{R} \setminus \mathbb{Z}$. Ekkor

$$\mathbf{b}' := \mathbf{b} - \lfloor s_m \rfloor \mathbf{b}_m - s_{m+1}\mathbf{b}_{m+1} - s_{m+2}\mathbf{b}_{m+2} - \ldots - s_k\mathbf{b}_k \in L$$

és

$$\|\mathrm{proj}_{m-1}^{\perp}(\mathbf{b}')\| = (s_m - \lfloor s_m \rfloor)\|\mathrm{proj}_{m-1}^{\perp}(\mathbf{b}_m)\| < \|\mathrm{proj}_{m-1}^{\perp}(\mathbf{b}_m)\|,$$

így (1.3.5) szerint ellentmondásra jutottunk. □

Ezáltal az a nem meglepő tény is kiderült, hogy tetszőleges L rácsnak van legrövidebb nem $\mathbf{0}$ vektora. Ezen vektor hosszát jelöljük

$$\lambda(L) := \min_{\mathbf{b} \in L} \|\mathbf{b}\| \tag{1.3.6}$$

módon.

Most már egy kicsit közelebbről megismertük ezen dolgozat legfontosabb struktúráját: a rácsokat. A következő fejezetben megismerkedünk egy klasszikus problémával, ami a mai napig rengeteg nyílt kérdést vet fel. Ezt a problémát természetesen a rácsok szemszögéből közelítjük majd meg. Vágjunk hát bele!

1.4. Gömbpakolási feladatok, és a Voronoi cella

Klasszikus kérdés ami már Keplert is foglalkoztatta, hogy milyen sűrűn lehet lefedni a 3 dimenziós teret egybevágó diszjunkt gömbök segítségével. 1611-ben Kepler megsejtette, hogy nincs jobb gömbpakolás, mint az úgynevezett fcc (face-centered cubic) pakolás (lásd 1.5. ábra). Gauss bebizonyította, hogy az olyan pakolások esetén, amikor a gömbök középpontjai egy rács pontjai, ez a legsűrűbb fedés. Kepler sejtése az általános esetről számos próbálkozás után is bizonyítás nélkül maradt, egészen a 2000-es évek elejéig. Thomas Callister Hales egy számítógép által asszisztált bizonyítást adott, amely helyességében hosszas ellenőrzési folyamat után sem bizonyosodtak meg teljesen.

1.5. ábra. Almák fcc pakolása.

Erre válaszul Hales 2003-ban elindította az úgynevezett Flyspeck projektet (Formal Proof of Kepler projekt), melynek célja az volt, hogy Kepler sejtésére befejezze a formális bizonyítást. A projekt 2014-ben sikerrel lezárult, így pont került egy akkorra már négyszáv éves probléma végére.

Hales bámulatos eredményének ellenére még rengeteg nyitott kérdés van ezzel kapcsolatban. Ezen dolgozatban a gömbpakolási problémát tetszőleges dimenzióban tekintjük, viszont a probléma azon változatával foglalkozunk csak, amikor gömbjeink középpontjai egy rács pontjai. Ezen témából kiragadjuk a számunkra fontos fogalmakat, viszont a témát nem tárgyaljuk részletesen. A fogalmak bevezetését az [Slo99] könyv alapján írjuk le.

Legyen adott az $\mathbb{R}^n$ tér egy teljes dimenziós L rácsa, és egy $0 < r \in \mathbb{R}$ valós szám. Ekkor a

$$\mathbf{b} + \mathrm{B}(r) \qquad \mathbf{b} \in L \tag{1.4.1}$$

halmazrendszert *gömbpakolásnak* hívjuk.

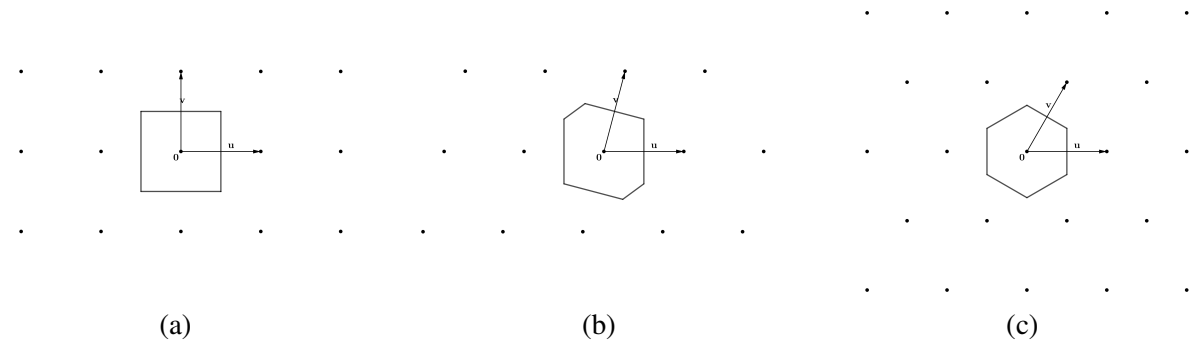
Mivel L egy diszkrét részhalmaz, így megválaszthatjuk az r sugár értékét egy 0-nál nagyobb valós számnak úgy, hogy gömbjeink legfeljebb a határukon érintkezzenek. Ezt *diszjunkt* gömbpakolásnak nevezzük. A maximális ilyen sugár $\lambda(L)/2$. Ezt az L rács *pakolási sugarának* hívjuk, és

$$r(L) := \lambda(L)/2 \tag{1.4.2}$$

módon jelöljük. Egy L rácshoz tartozó olyan gömbpakolás, ahol gömbjeink legfeljebb a határukon érintkeznek akkor fedi le a tér legnagyobb hányadát, ha a gömbök sugara a pakolási sugár.

A következő kérdés, hogy mekkora az a minimális r sugár, amivel gömbpakolásunk nem diszjunkt, és még a teljes teret lefedi. Mielőtt ezt megadnánk, először meg kell ismernünk, hogy mi egy rács Voronoi cellája.

Ez nem más mint azon pontok halmaza, amelyek legalább olyan közel vannak $\mathbf{0}$-hoz mint bármely másik rácsponthoz.



(a) (b) (c)

1.6. ábra. A sík 3 rácsának Voronoi cellája.

1.7. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. Ekkor a

$$\operatorname{vor} L := \{\mathbf{v} \in [L] \mid \forall \mathbf{b} \in L\colon \mathrm{d}(\mathbf{v},\mathbf{0}) \leq \mathrm{d}(\mathbf{v},\mathbf{b})\} \tag{1.4.3}$$

halmazt az L rács *Voronoi cellájának* hívjuk.

A

$$\mathbf{b} + \operatorname{vor} L \qquad \mathbf{b} \in L$$

alakú halmazok lefedik a teljes $[L]$ alteret, továbbá két ilyen halmaz csak a határán érintkezhet, tehát ez a $[L]$ egy parkettázása. Az 1.2. állítás szerint, tetszőleges L rács esetén

$$\operatorname{vol}(\operatorname{vor} L) = \operatorname{vol} L. \tag{1.4.4}$$

Figyeljük meg, hogy ha $\mathbf{v} \in \operatorname{vor} L$, akkor $-\mathbf{v} \in \operatorname{vor} L$ is teljesül. Ezek szerint $\operatorname{vor} L$ $\mathbf{0}$-szimmetrikus.

A definícióból azonnal adódik, hogy

$$\operatorname{vor} L = \bigcap_{\mathbf{b} \in L \setminus \{\mathbf{0}\}} \{\mathbf{v} \in [L] \mid \mathbf{v} \cdot \mathbf{b} \leq \mathbf{b}^2/2\} \tag{1.4.5}$$

ugyanis

$$\{\mathbf{v} \in [L] \mid \mathbf{v} \cdot \mathbf{b} \leq \mathbf{b}^2/2\} \tag{1.4.6}$$

a **0** és **b** pontokat összekötő szakaszt elfelező merőleges hipersík által meghatározott a **0** irányába eső féltér. Ez azon $[L]$ altérbeli **v** pontok halmaza, amelyek közelebb vannak **0**-hoz mint **b**-hez.

Valójában egy rács Voronoi cellája előáll véges sok féltér metszeteként, és mivel korlátos is, így egy politóp.

1.8. Definició. Legyen adott egy k dimenziós L rács. Egy olyan **b** rácspontot, amelyekre a

$$\operatorname{vor} L \cap \{\mathbf{v} \in [L] \mid \mathbf{v} \cdot \mathbf{b} = \mathbf{b}^2/2\}$$

halmaz nem üres, a rács *Voronoi vektorának* hívjuk. Amennyiben ez a halmaz a Voronoi cella egy $k-1$ dimenziós lapja, akkor azt mondjuk, hogy a vektor *Voronoi-releváns*.

A Voronoi-releváns vektorok azok, amelyek által meghatározott félterekre ténylegesen szükség van a Voronoi cella „előállításához". A következő Voronoi-tól származó klasszikus állítás leírja, hogy adott rácsvektor mikor Voronoi/Voronoi-releváns.

1.9. Állítás. *Legyen adott egy k dimenziós L rács, és egy* $\mathbf{b} \in L \setminus \{\mathbf{0}\}$ *rácspont. Ekkor* **b** *pontosan akkor Voronoi vektora a rácsnak, ha ő az* $L/2L$ *faktorcsoport*

$$\mathbf{b} + 2L$$

osztályának egyik legrövidebb vektora, és pontosan akkor Voronoi-releváns, ha ezen osztály legrövidebb vektorai csak **b** *és* $-\mathbf{b}$.

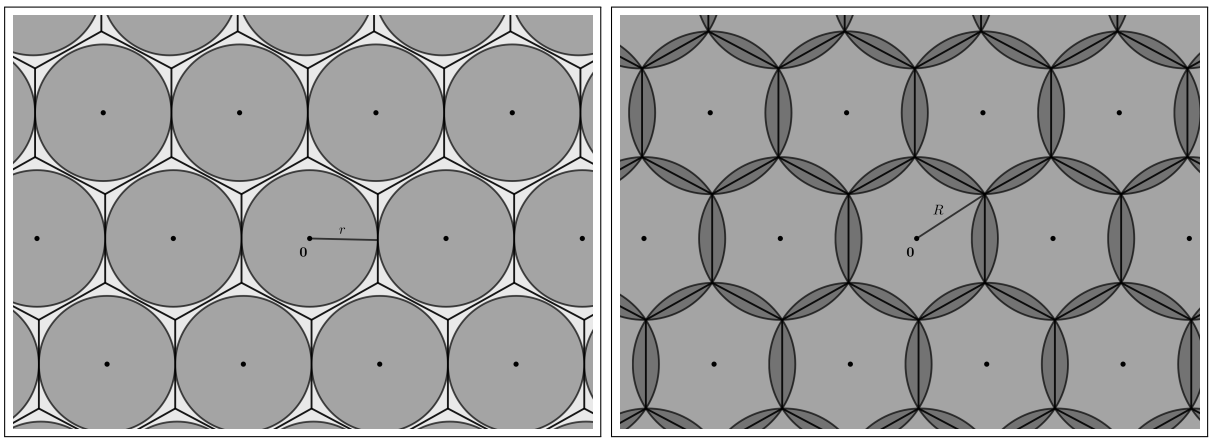
Mi ezen dolgozatban az állítás bizonyítását nem tárgyaljuk.

Az állítás szerint, egy rács Voronoi-releváns vektorainak száma legfeljebb $2(2^n-1)$, ugyanis minden osztályból legfeljebb 2 Voronoi-releváns vektor kerülhet ki, és a nem **0**-hoz tartozó osztályok száma 2^n-1.

Egy L rács pakolási sugara pont a rács Voronoi cellájának beírható körének sugara. A Voronoi cella köréírható körének sugarát a rács *fedési sugarának* hívjuk és

$$R(L) := \operatorname{rad}(\operatorname{vor} L) \tag{1.4.7}$$

módon jelöljük. Ez a legkisebb akkora sugár amekkora sugarú gömbökkel a 1.4.1. gömbpakolás a teljes $[L]$ alteret lefedi. Ilyenkor gömbpakolás helyett a *gömbfedés* kifejezést használjuk.



(a) A pakolási sugár (b) A fedési sugár

1.7. ábra. A sík egy rácsának pakolási és fedési sugara.

A fejezet elején leírtuk Kepler gömbpakolási feladatát. A cél az, hogy megtaláljunk egy olyan diszjunkt gömbpakolást, amely sűrűsége a lehető legkisebb, azaz amely a tér lehető legnagyobb hányadát lefedi. A kérdés csak az, hogy hogyan írjuk le precízen egy gömbpakolás sűrűségét?

Adott $L \subset \mathbb{R}^n$ teljes dimenziós rács és r sugarú gömbök esetén a pakolás sűrűsége

$$\frac{\mathrm{vol}\,\mathrm{B}(r)}{\mathrm{vol}\,L} = \frac{\pi^{\lfloor n/2 \rfloor}}{(n/2)!} \cdot \frac{r^n}{\mathrm{vol}\,L}, \tag{1.4.8}$$

tehát a legsűrűb L rácshoz tartozó diszjunkt pakolás sűrűsége

$$\frac{\pi^{\lfloor n/2 \rfloor}}{(n/2)!} \cdot \frac{(r(L))^n}{\mathrm{vol}\,L}, \tag{1.4.9}$$

a legkevésbé sűrű gömbfedés sűrűsége pedig

$$\frac{\pi^{\lfloor n/2 \rfloor}}{(n/2)!} \cdot \frac{(R(L))^n}{\mathrm{vol}\,L}. \tag{1.4.10}$$

Eddig a legsűrűbb diszjunkt gömbpakolás csak az első 8 dimenzióban, és a 24. dimenzióban ismert. Hasonló a helyzet a legkevésbé sűrű gömbfedésekkel: az első 5 dimenzióban tudjuk, hogy melyek a legjobb fedések, magasabb dimenzióban azonban a válasz sajnos nem ismert. [Slo99]

1.5. Szukcesszív minimumok, Minkowski tételei, és a Hermit konstans

Az 1.3. alfejezetben láthattuk, hogy minden rácsnak található legrövidebb vektora. Ezen fogalom tovább általánosítható, és megtalálhatjuk egy rács első valahány legrövidebb vektorát.

Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. Növeljük fokozatosan egy $\mathbf{0}$ középpontú n dimenziós gömb sugarát egészen addig a pillanatig, amíg a gömbünk az eddigi nem $\mathbf{0}$ rácspontoktól lineárisan független új rácsponttal nem bővül. Ha a kezdeti sugár olyan kicsi volt, hogy a gömb nem tartalmazott $\mathbf{0}$-tól különböző rácspontokat, akkor a bővülés után kapott rácspont lesz a rácsunk legrövidebb nem $\mathbf{0}$ vektora. Ha folytatjuk ezt a bővítési folyamatot, akkor mindig a következő kapott vektor lesz az, ami szemünkben a következő legrövidebb rácsvektor. Ez alapján a következő definíciót kapjuk az i. „legrövidebb” vektor hosszára:

1.10. Definició. Legyen $L \subset \mathbb{R}^n$ egy k dimenziós rács. A

$$\lambda_i(L) := \inf\{r \in \mathbb{R} \mid \exists \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i \in L \cap \mathrm{B}(r) \text{ lineárisan független vektorok}\} \quad (1 \leq i \leq k)$$

valós számot az L rács i. *szukcesszív minimumának* hívjuk.

Adott L rács esetén mindig van olyan rácspont aminek hossza pont $\lambda_i(L)$, továbbá ahogy azt megfigyeltük, $\lambda_1(L)$ a rács legrövidebb nem $\mathbf{0}$ vektorának hossza, és

$$\lambda_1(L) \leq \lambda_2(L) \leq \ldots \leq \lambda_n(L), \tag{1.5.1}$$

teljesül. (Az egyenlőséget azért engedhetjük meg, mert a definíció előtt leírt gömb egyszerre akár több független rácsvektorral is bővülhet.)

Ezen alfejezetben bemutatunk egy fontos felső becslést a szukcesszív minimumok szorzatának nagyságára. Mint ahogy azt látni fogjuk, ennek segítségével korlátot szabunk a legsűrűbb diszjunkt gömbpakolás sűrűségére is. A következő három tétel bizonyítását, amely ezen tényhez vezet, egy az egyben a [Gol02] könyv alapján írjuk le.

1.11. Tétel (Blichfeldt tétele)**.** *Legyen adott egy $L \subset \mathbb{R}^n$ rács, és egy $G \subset [L]$ mérhető halmaz. Ha*

$$\operatorname{vol} L < \operatorname{vol} G$$

akkor léteznek a $\mathbf{g}_1, \mathbf{g}_2 \in G$ pontok, hogy

$$\mathbf{g}_2 - \mathbf{g}_1 \in L.$$

Bizonyítás. Legyen K egy mérhető halmaz, hogy

$$\mathbf{b} + K \qquad \mathbf{b} \in L$$

az $[L]$ altér egy parkettázását adja. Legyen $\mathbf{v} \in L$,

$$K_{\mathbf{v}} := \mathbf{v} + K$$

és

$$G_{\mathbf{v}} = K_{\mathbf{v}} \cap G.$$

Ekkor

$$G_{\mathbf{v}} - \mathbf{v} \subset K,$$

és

$$\operatorname{vol} G = \sum_{\mathbf{v} \in L} \operatorname{vol} G_{\mathbf{v}},$$

így léteznie kell $\mathbf{u} \neq \mathbf{v}$ rácsvektoroknak, hogy a $G_{\mathbf{v}} - \mathbf{v}$ és $G_{\mathbf{u}} - \mathbf{u}$ halmazok metszetének belseje nem üres, mivel különben

$$\operatorname{vol} G = \sum_{\mathbf{v} \in L} \operatorname{vol} G_{\mathbf{v}} = \sum_{\mathbf{v}} \operatorname{vol} (G_{\mathbf{v}} - \mathbf{v}) \leq \operatorname{vol} K$$

teljesülne ami ellent mondana a $\operatorname{vol} G > \operatorname{vol} L = \operatorname{vol} K$ kezdeti feltételnek. Legyen tehát $\mathbf{g}$ a $G_{\mathbf{u}} - \mathbf{u}$ és $G_{\mathbf{v}} - \mathbf{v}$ halmazok belsejének közös eleme. Legyen $\mathbf{g}_1 = \mathbf{g} + \mathbf{u}$, és $\mathbf{g}_2 = \mathbf{g} + \mathbf{v}$. Ekkor $\mathbf{g}_1, \mathbf{g}_2 \in G$ és $\mathbf{g}_2 - \mathbf{g}_1 = \mathbf{v} - \mathbf{u} \in L$ így az állítást beláttuk. □

Ezen tételből szinte azonnal következik Minkowski nevezetes tétele:

1.12. Tétel (Minkowski első tétele)**.** *Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács, és egy $S \subset [L]$ konvex és $\mathbf{0}$-szimmetrikus halmaz. Ha $\operatorname{vol} S > 2^k \operatorname{vol} L$, akkor az S halmaz tartalmaz egy nem $\mathbf{0}$ rácspontot.*

Bizonyítás. Legyen adott egy $S \subset [L]$ halmaz amely teljesíti a tétel feltételeit. Legyen

$$S' = (1/2) \cdot S.$$

Ekkor mivel

$$\operatorname{vol} S' = (1/2)^k \operatorname{vol} S > \operatorname{vol} L$$

így Blichfeldt tétele szerint létezik $\mathbf{s}_1 \neq \mathbf{s}_2 \in S'$, hogy $\mathbf{s}_2 - \mathbf{s}_1 \in L$. S' definíciója szerint

$$2\mathbf{s}_1, 2\mathbf{s}_2 \in S,$$

és mivel S $\mathbf{0}$-szimmetrikus így

$$-2\mathbf{s}_1 \in S.$$

Végül S konvexitása miatt

$$L \setminus \{\mathbf{0}\} \ni \mathbf{s}_2 - \mathbf{s}_1 = \frac{2\mathbf{s}_2 - 2\mathbf{s}_1}{2} \in S$$

tehát $\mathbf{s}_2 - \mathbf{s}_1$ egy S-beli rácspont. □

Végül ebből be tudjuk látni Minkowski másik nevezetes tételét:

1.13. Tétel (Minkowski második tétele)**.** *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács. Ekkor*

$$\frac{\lambda_1(L) \cdot \lambda_2(L) \cdot \ldots \cdot \lambda_k(L)}{\operatorname{vol} L} < k^{k/2}.$$

Bizonyítás. Indirekt tegyük fel, hogy

$$\frac{\lambda_1(L) \cdot \lambda_2(L) \cdot \ldots \cdot \lambda_k(L)}{\operatorname{vol} L} \geq k^{k/2}.$$

Legyen $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in L$ az L rács olyan vektorai, hogy tetszőleges i index esetén

$$\|\mathbf{b}_i\| = \lambda_i(L).$$

Legyen ezen vektorok Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. Legyen

$$B = \{\mathbf{v} \in [L] \mid \|\mathbf{v}\| < 1\}$$

az $[L]$ altér 1 sugarú nyílt egységgömbje, és legyen $T\colon [L] \to [L]$ az a lineáris transzformáció amelyre

$$T(\mathbf{b}_i^*) = \lambda_i(L)\mathbf{b}_i^*.$$

Ekkor a T transzformációt a B gömbre alkalmazva egy $\mathbf{0}$-szimmetrikus konvex halmazt kapunk amely térfogatára a következő becslés áll fenn:

$$\operatorname{vol} T(B) = \lambda_1(L) \cdot \lambda_2(L) \cdot \ldots \cdot \lambda_k(L) \operatorname{vol} B \geq (k^{k/2} \operatorname{vol} L) \operatorname{vol} B = \operatorname{vol} L (\operatorname{vol} \sqrt{k} B).$$

Mivel $\sqrt{k}B$ tartalmazza a 2 oldalhosszúságú origó súlypontú kockát, így térfogata legalább 2^n, és ezek szerint

$$\operatorname{vol} T(B) \geq 2^n \cdot \operatorname{vol} L$$

így Minkowski első tétele szerint létezik egy $\mathbf{v} \in T(B) \cap L$ nem $\mathbf{0}$ rácspont. Legyen $\mathbf{u} \in B$ az a pont amelyre

$$T(\mathbf{u}) = \mathbf{v}.$$

Mivel $\mathbf{u} \in B$ így $\|\mathbf{u}\| \leq 1$. Írjuk fel az $\mathbf{u}$ és $\mathbf{v}$ vektorokat a $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ vektorok lineáris kombinációjaként. Ha

$$\mathbf{u} = c_1\mathbf{b}_1^* + c_2\mathbf{b}_2^* + \ldots + c_k\mathbf{b}_k^*$$

akkor T definíciója szerint

$$\mathbf{v} = c_1\lambda_1(L)\mathbf{b}_1^* + c_2\lambda_2(L)\mathbf{b}_2^* + \ldots + c_k\lambda_k(L)\mathbf{b}_k^*.$$

Legyen i maximális index, hogy c_i nem 0, és legyen i' minimális index amire $\lambda_{i'}(L) = \lambda_i(L)$. Mivel $\mathbf{b}_i^* \cdot \mathbf{v} = \|\mathbf{b}_i^*\|^2 c_i\lambda_i(L) \neq 0$ így a $\mathbf{v}$ rácspont lineárisan független a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i'-1}$ vektoroktól, így $\mathbf{v}$ nincs benne a $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i'-1}]$ altérben, tehát $\mathbf{v}$ egy a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i'-1}$ vektoroktól független rácspont. A bizonyítás befejezéséhez megmutatjuk, hogy $\|\mathbf{v}\| < \lambda_L(i) = \lambda_L(i')$:

$$\begin{aligned}\|\mathbf{v}\|^2 &= \lambda_1(L)^2\|c_1\mathbf{b}_1^*\|^2 + \lambda_2(L)^2\|c_2\mathbf{b}_2^*\|^2 + \ldots + \lambda_i(L)^2\|c_i\mathbf{b}_i^*\|^2 \leq \\ &\leq \lambda_i(L)^2\|c_1\mathbf{b}_1^*\|^2 + \lambda_i(L)^2\|c_2\mathbf{b}_2^*\|^2 + \ldots + \lambda_i(L)^2\|c_i\mathbf{b}_i^*\|^2 = \\ &= \lambda_i(L)^2\|\mathbf{u}\| < \lambda_i(L)^2.\end{aligned}$$

Ezzel az i'. szukcesszív minimum definíciója szerint ellentmondásra jutottunk, és így a tételt beláttuk. □

Most eljött az idő, hogy megvizsgáljuk, mi köze ennek a diszjunkt gömbfedésekhez. Ehhez először is be kell vezetnünk egy rács Hermit defektusának a fogalmát.

1.14. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. Ekkor a

$$\gamma(L) := \frac{\lambda(L)^k}{\mathrm{vol}\, L} = \frac{\lambda(L)^k}{\|\mathbf{b}_1^*\| \cdot \|\mathbf{b}_2^*\| \cdot \ldots \cdot \|\mathbf{b}_k^*\|}$$

valós számot az L rács *Hermit defektusának* hívjuk.

Minkowski második tétele szerint egy k dimenziós rács Hermit defektusára a

$$\gamma(L) = \frac{\lambda(L)^k}{\mathrm{vol}\, L} < k^{k/2} \tag{1.5.2}$$

felső becslést kapjuk. Hermit egy ennél valamivel rosszabb felső becslést használt fel annak megmutatására, hogy értelmes a

$$\gamma_k := \sup_{L \in \mathscr{L}_k} \gamma(L) \tag{1.5.3}$$

kifejezés. Ez az úgynevezett k dimenziós *Hermit konstans*. A Hermit konstanst sok helyen

$$\gamma_k^{2/k}$$

módon definiálják, nekünk azonban ezt kényelmesebb a (1.5.3)-nél látható módon bevezetni. Ismert tény, hogy létezik olyan k dimenziós L rács, amelyen a Hermit konstans értéke felvétetik, azaz amelyre

$$\gamma_k = \gamma(L).$$

Az ilyen rácsokat *kritikus rácsoknak hívjuk*. A Hermit konstans pontos értéke csak az első 8 és a 24. dimenzióban ismert, továbbá ezen dimenziókban még ismert az összes kritikus rács is. [Ngu10]

Megfigyelhetjük, hogy a Hermit defektus szoros összefüggésben áll a lehető legsűrűbb n-dimenziós diszjunkt gömbpakolás meghatározásával. Nevezetesen (1.4.9) alapján, egy ilyen pakolás sűrűsége

$$\frac{\pi^{\lfloor n/2 \rfloor}}{(n/2)!2^n} \cdot \gamma_n. \tag{1.5.4}$$

így a legsűrűbb gömbpakolást pont a kritikus rácsok adják.

2. Algoritmikus problémák rácsokon

2.1. Elemi algoritmusok

A bevezetőben leírtuk, hogy az $\mathbb{R}^n$ tetszőleges k darab $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorához tartozik k darab egymásra merőleges $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ vektor, hogy

$$\begin{aligned}
\mathbf{b}_1 &= \mu_{1,1}\mathbf{b}_1^* \\
\mathbf{b}_2 &= \mu_{2,1}\mathbf{b}_1^* + \mu_{2,2}\mathbf{b}_2^* \\
\mathbf{b}_3 &= \mu_{3,1}\mathbf{b}_1^* + \mu_{3,2}\mathbf{b}_2^* + \mu_{3,3}\mathbf{b}_3^* \\
&\ldots \\
\mathbf{b}_k &= \mu_{k,1}\mathbf{b}_1^* + \mu_{k,2}\mathbf{b}_2^* + \mu_{k,3}\mathbf{b}_3^* + \ldots + \mu_{k,k}\mathbf{b}_k^*,
\end{aligned}$$

A $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ vektorokat a kezdeti vektorok Gram-Schmidt ortogonalizáltjának hívjuk, a $\mu_{i,j}$ együtthatókat pedig a Gram-Schmidt együtthatóknak. Ezek a következő klasszikus algoritmus segítségével megkaphatóak:

2.1. Algoritmus Gram-Schmidt ortogonalizáció

Név: `GS_ort` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
Be: $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok
Ki: A kezdeti vektorokhoz tartozó $(\mu_{i,j})_{0<j<i\leq n}$ Gram-Schmidt együtthatók, és $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ Gram-Schmidt ortogonalizált

1: $\mathbf{b}_1^* \leftarrow \mathbf{b}_1$
2: **Ciklus** $i = 2..k$ (+1)
3: **Ciklus** $j = 1..i-1$ (+1)
4: $\mu_{ij} \leftarrow \mathbf{b}_i \cdot \mathbf{b}_j^* / \|\mathbf{b}_j^*\|^2$
5: **Ciklus vége**
6: $\mathbf{b}_i^* \leftarrow \mathbf{b}_i - \mu_{i,1}\mathbf{b}_1^* - \mu_{i,2}\mathbf{b}_2^* - \ldots - \mu_{i,i-1}\mathbf{b}_{i-1}^*$
7: **Ciklus vége**

Itt az i. iterációban megkeressük azt a

$$\mathbf{b}_i + [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$$

affin altér belsejébe eső $\mathbf{b}_i^*$ vektort, amely merőleges az első $i-1$ vektor által kifeszített altérre. Ezt úgy adjuk meg, hogy a $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_{i-1}^*$ megfelelő lineáris kombinációját kivonjuk a $\mathbf{b}_i$ vektorból. Ezek a megfelelő együtthatók pont a Gram-Schmidt együtthatók lesznek, amiket az algoritmus 3. sorában kezdődő ciklusban határozunk meg.

Most bemutatunk egy másik elemi algoritmus, amelyet már Gauss is megfogalmazott. Egyesek úgy gondolják, hogy Lagrange már Gauss előtt felfedezte ezt az algoritmust, és így sok helyen a Lagrange algoritmus elnevezést használják. Mi végül a Lagrange-Gauss algoritmus elnevezés mellett döntöttünk. Az algoritmust [Gal12] alapján mutatjuk itt be.

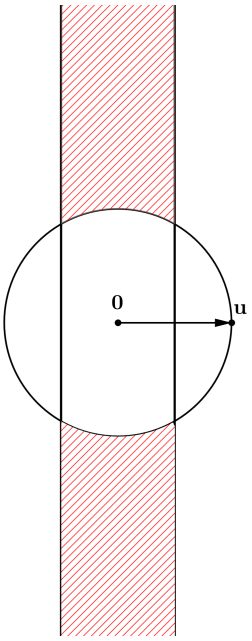
Ezen algoritmus (egy tetszőleges dimenzióba általánosított változatának) részletes elemzését a 4. fejezetben tárgyaljuk majd. Itt most csak felvázoljuk az algoritmus működése mögött rejlő alap gondolatokat.

Legyen adott egy 2 dimenziós $L \subset \mathbb{Q}^n$ rács és ennek egy $\mathbf{u}, \mathbf{v}$ bázisa. Legyen μ a $\mathbf{v}$ vektor $\mathbf{u}$ vektorhoz tartozó Gram-Schmidt együtthatója. Ekkor, amennyiben a

$$\begin{aligned} \|\mathbf{u}\| &\leq \|\mathbf{v}\| \\ |\mu| &\leq 1/2 \end{aligned} \tag{2.1.1}$$

feltételek teljesülnek, akkor azt mondjuk, hogy a bázis *Lagrange-Gauss* redukált.

A redukáltság ezen fogalma a $\mathbf{v}$ vektort a 2.1. ábrán látható tartományba kényszeríti. Mint azt később látni fogjuk, kettő dimenzióban ezen redukáltság a lehető legjobb amit csak találhatunk, olyan értelemben, hogy egy kettő dimenziós rács Lagrange Gauss redukált bázisa a lehető legmerőlegesebb az ő összes bázisa közül.



2.1. ábra. A Lagrange-Gauss redukáltság tartománya.

Ezt tudva adódik a 2.2. algoritmus, amely megtalál egy Lagrange-Gauss redukált bázist.

2.2. Algoritmus Lagrange-Gauss redukció

Név: `LG_alg_2d(`$\mathbf{u}, \mathbf{v}$`)`
Be: Egy $L \subset \mathbb{Q}^n$ rács egy $\mathbf{u}, \mathbf{v}$ bázisa, ahol $\|\mathbf{v}\| \leq \|\mathbf{u}\|$
Ki: Az L rács $\mathbf{u}, \mathbf{v}$ Lagrange-Gauss redukált bázisa

1: **Ciklus**
2: $\quad x \leftarrow \mathbf{u} \cdot \mathbf{v} / \|\mathbf{v}\|^2$
3: $\quad \mathbf{r} \leftarrow \mathbf{u} - \lfloor x \rceil \mathbf{v}$ ▷ $\lfloor x \rceil$ a x valós számhoz (egyik) legközelebb eső egész szám
4: $\quad \mathbf{u} \leftarrow \mathbf{v}$
5: $\quad \mathbf{v} \leftarrow \mathbf{r}$
6: **Ciklus amíg** $\|\mathbf{v}\| < \|\mathbf{u}\|$ **vége**

A 3. sorban pont azt érjük el, hogy az iteráció végére kapott $\mathbf{u}, \mathbf{v}$ bázis Gram-Schmidt együtthatójának abszolútértéke legfeljebb $1/2$ legyen. A leállási feltétel és ezen megfigyelés miatt az algoritmus muszáj, hogy leálláskor Lagrange-Gauss redukált bázist adjon eredményül.

Mivel az algoritmus minden iterációjában csökken az $\mathbf{u}$ vektor hossza, és a $\mathrm{B}(\|\mathbf{u}\|)$ gömbben csak véges sok rácspont van így az algoritmus szükségszerűen véges sok lépésben le is áll. Később majd belátjuk, hogy ezen algoritmus iterációinak száma polinomiális.

2.2. Az ortogonalitási defektus, és Hermit algoritmusa

A síkon viszonylag könnyű volt megfogalmazni a célunk: olyan bázisát akartuk megtalálni egy rácsnak, melynek vektorai a lehető legközelebb vannak a merőlegeshez. Ugyanezt akarjuk megvalósítani most n dimenziós terek esetén, ehhez azonban először is be kell vezetnünk az *ortogonalitási defektus* fogalmát. Ez egy mérőszám arra, hogy egy rács egy adott bázisa mennyire tér el az ő Gram-Schmidt ortogonalizáltjától.

2.1. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen ezen bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. A

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) := \frac{\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\|}{\mathrm{vol}\, L}$$

valós számot a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ független vektorok *ortogonalitási defektusának* nevezzük.

Mivel $\mathrm{vol}\, L = \|\mathbf{b}_1^*\| \cdot \|\mathbf{b}_2^*\| \cdot \ldots \cdot \|\mathbf{b}_k^*\|$ és $\mathbf{b}_1^* = \mathbf{b}_1$, így az ortogonalitási defektust felírhatjuk egy kicsit másképp is:

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \frac{\|\mathbf{b}_2\| \cdot \|\mathbf{b}_3\| \cdot \ldots \cdot \|\mathbf{b}_k\|}{\|\mathbf{b}_2^*\| \cdot \|\mathbf{b}_3^*\| \cdot \ldots \cdot \|\mathbf{b}_k^*\|}. \tag{2.2.1}$$

Ez alapján már látni fogjuk, hogy az ortogonalitási defektus ténylegesen azt jelenti, amit a neve sugall: megmutatja, hogy a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ független vektorok mennyire térnek el az ortogonálistól.

2.2. Állítás (Hadamard egyenlőtlenség)**.** $1 \leq \delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ *ahol pontosan akkor teljesül az egyenlőség, ha a* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ *vektorok egymásra merőlegesek.*

Bizonyítás. Mivel tetszőleges i esetén $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$ és az egyenlőség pontosan akkor teljesül, ha $\mathbf{b}_i = \mathbf{b}_i^*$, ezért (2.2.1) alapján megkaptuk az állítást. □

Az ortogonalitási defektus (2.2.1) alakjából ennél többet is ki tudunk olvasni. Mivel $\|\mathbf{b}_i^*\|/\|\mathbf{b}_i\|$ pont a $\mathbf{b}_i$ vektor és $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ altér által bezárt $0 < \alpha_i \leq \pi/2$ szög színusza (lásd (1.2.33)), így az ortogonalitási defektus új alakját kaptuk:

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \frac{1}{\sin\alpha_2 \cdot \sin\alpha_3 \cdot \ldots \cdot \sin\alpha_k}. \tag{2.2.2}$$

Végül arra jutottunk, hogy az ortogonalitási defektus nagyobb vagy egyenlő mint 1, pontosan akkor egyenlő 1-el, ha a vektoraink egymásra merőlegesek, és minél közelebb van az ortogonalitási defektus 1-hez, annál közelebb kell lenni az $\alpha_2, \alpha_3, \ldots, \alpha_k$ szögek szinuszának 1-hez, tehát a szögek annál közelebb vannak a merőlegeshez.

Adódik tehát a probléma, hogy megtaláljuk egy rács egy olyan $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisát, amely ortogonalitási defektusa minimális. Ahogy ezt a következő példa illusztrálja, nem várhatjuk el, hogy mindig ortogonális bázist találjunk, ugyanis ilyen nem feltétlen létezik.

Legyenek adottak a síkon az

$$\begin{aligned}\mathbf{u} &= (1,0)\\ \mathbf{v} &= (1/2,\sqrt{3}/2)\end{aligned} \tag{2.2.3}$$

vektorok. Az ezek által generált szabályos hatszög rács (lásd 2.2. ábra) későbbi kitüntetett szerepe miatt külön jelölést kap:

$$A_2 := L(\mathbf{u},\mathbf{v}) \tag{2.2.4}$$

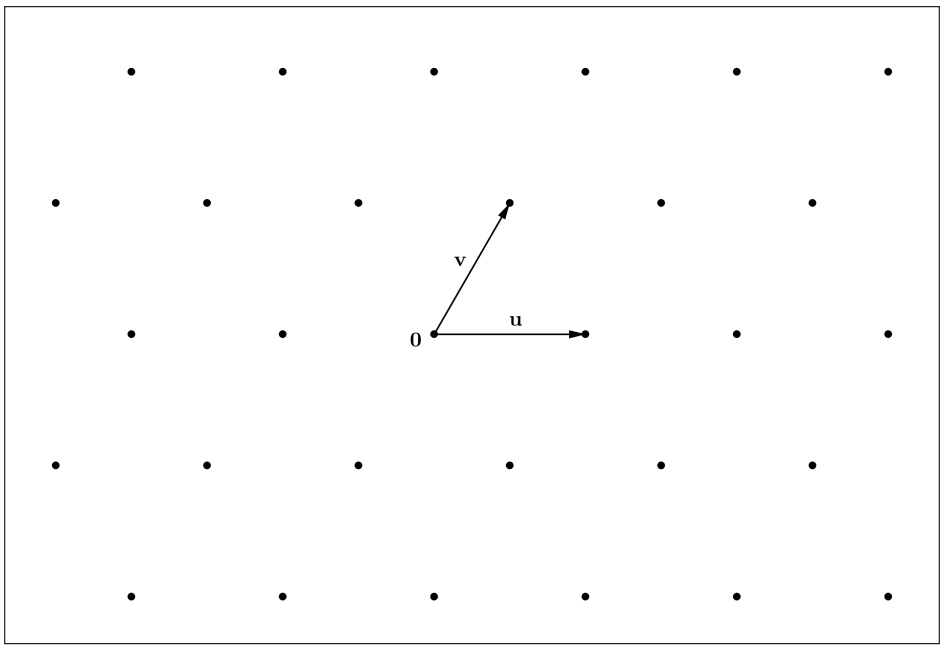
Mivel $\mathrm{vol} A_2 = \sqrt{3}/2$ és $\|\mathbf{u}\| = \|\mathbf{v}\| = 1$, így

$$\delta(\mathbf{u},\mathbf{v}) = \frac{2}{\sqrt{3}}. \tag{2.2.5}$$

Tudunk ennél jobbat? Az A_2 rács egy $\mathbf{b}_1,\mathbf{b}_2$ bázisának ortogonalitási defektusa pontosan akkor minimális, ha a

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\|$$

szorzat minimális. Az A_2 rács minimális hosszúságú nem $\mathbf{0}$ vektorai az egységkörön helyezkednek el. Nyilván $\mathbf{u}$ és $\mathbf{v}$ is ilyenek. Ezek szerint az A_2 rács $\mathbf{u},\mathbf{v}$ bázisa minimalizálja az ortogonalitási defektust.



2.2. ábra. A szabályos hatszög rács.

Most megmutatjuk, tetszőleges rácsban található minimális ortogonalitási defektusú bázis.

Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács és ennek egy $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ bázisa. Először az egyszerűség kedvéért tegyük fel, hogy $\lambda_1(L) \geq 1$. Később majd ettől a feltételtől megszabadulunk. Mivel a

$$B = \mathrm{B}(\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\|)$$

gömbben csak véges sok rácspont van, így ezen gömbbe L bázisai közül is csak véges sok eshet. Legyen $\mathbf{b}'_1,\mathbf{b}'_2,\ldots,\mathbf{b}'_k \in B$, a B gömbbeli bázisok közül minimális ortogonalitási defektusú. Akkor ez L összes bázisa közül is minimális ortogonalitási defektusú, ugyanis

$$\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k \in B$$

és amennyiben adott az L egy olyan $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ bázisa, amelynél van olyan i index amire $\mathbf{c}_i \notin B$, akkor

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) < \delta(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k).$$

Amennyiben $\lambda_1(L) < 1$, akkor az L rács helyett nézzük az átskálázott

$$\frac{1}{\lambda_1(L)} L$$

rácsot. Az előzőek szerint itt található minimális ortogonalitási defektusú bázis, így ilyen a kezdeti L rácsban is volt.

2.3. Definició. Megmutattuk tehát, hogy minden k dimenziós $L \subset \mathbb{R}^n$ rácsnak található minimális ortogonalitási defektusú bázisa. Ezen ortogonalitási defektus nagyságát az L rács *ortogonalitási defektusának* hívjuk, és

$$\delta(L) := \min_{\substack{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \\ \text{az } L \text{ bázisa}}} \delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

módon jelöljük.

Hermit (a kvadratikus formák nyelvén) megadott egy algoritmust, amely tetszőleges dimenzióba általánosítja a Lagrange-Gauss algoritmust, és habár minimális ortogonalitási defektusú bázist nem talál, de azt megközelíti. Ehhez először is megfogalmazta az úgynevezett gyenge redukáltság fogalmát. Az algoritmus itt található kifejtését [Ngu10] és [Lov86] alapján írjuk le.

2.4. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Amennyiben tetszőleges $j < i$ indexek esetén a bázis $\mu_{i,j}$ Gram-Schmidt együtthatójára

$$|\mu_{i,j}| \leq 1/2$$

teljesül, akkor azt mondjuk, hogy a bázis *gyengén redukált*.

A 2.3. algoritmus segítségével tetszőleges kiindulási bázis esetén található egy gyengén redukált bázis, amely Gram-Schmidt ortogonalizáltja ugyanaz, mint a kezdetinek.

Vizsgáljuk meg, hogy mi történik amikor az algoritmus 4. sorában megváltoztatjuk $\mathbf{b}_i$ értékét. Először vegyük észre, hogy a változtatás a bázis Gram-Schmidt ortogonalizáltját változatlanul hagyja, így ha $k \neq i$ akkor tetszőleges l esetén μ_{kl} ugyanaz marad.

Legyen $\mathbf{b}_i'$ a kapott új vektor, $(\mu_{il}')_{1 \leq l < i}$ az új Gram-Schmidt együtthatók, $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*$ pedig a bázis Gram-Schmidt ortogonalizáltja. Ekkor

$$\mathbf{b}_i' = \mathbf{b}_i - \lfloor \mu_{ij^*} \rceil \mathbf{b}_{j^*} = \sum_{l=1}^{i} \mu_{il} \mathbf{b}_l^* - \lfloor \mu_{ij^*} \rceil \sum_{l=1}^{i} \mu_{j^*l} \mathbf{b}_l^* = \sum_{l=1}^{i} (\mu_{il} - \lfloor \mu_{ij^*} \rceil \mu_{j^*l}) \mathbf{b}_l^*,$$

így

$$\mu_{il}' = \mu_{il} - \lfloor \mu_{ij^*} \rceil \mu_{j^*l} = \begin{cases} \mu_{il} & \text{ha } j^* < l, \\ \mu_{ij^*} - \lfloor \mu_{ij^*} \rceil & \text{ha } l = j^*, \\ \mu_{il} - \lfloor \mu_{ij^*} \rceil \mu_{j^*l} & \text{különben.} \end{cases} \tag{2.2.6}$$

2.3. Algoritmus Gyenge Redukció

Név: `gyenge_redukció` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
Be: Egy $L \subset \mathbb{Q}^n$ rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa
Ki: Az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ gyengén redukált bázisa

1: `GS_ort` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
2: **Ciklus** $i = 2..n$ $(+1)$
3: **Ciklus amíg** $\exists j\colon 1 \leq j < i,\ |\mu_{ij}| > 1/2$
4: Legyen j^* a ciklus felételének megfelelő j-k közül maximális
5: $\mathbf{b}_i \leftarrow \mathbf{b}_i - \lfloor \mu_{ij^*} \rceil \mathbf{b}_{j^*}$
6: Frissítsük a Gram-Schmidt együtthatókat
7: **Ciklus vége**
8: **Ciklus vége**

Ezek szerint $|\mu'_{ij}| \leq 1/2$, így a ciklus feltételét teljesítő maximális j index legalább egyel kisebb lett. Innen látszik, hogy az i. külső ciklusban legfeljebb $i-1$-szer fut le a belső ciklus azaz az algoritmus iterációinak száma legfeljebb

$$1+2+\ldots+(n-1) = \binom{n}{2}.$$

Végül azt kaptuk, hogy a 2.3. algoritmus eredményül egy gyengén redukált bázist ad vissza, és legfeljebb $\binom{n}{2}$ belső iteráció alatt véget ér.

Az algoritmus 6. sorában a Gram-Schmidt együtthatók frissítését persze (2.2.6) szerint gyorsan elvégezhetjük, így nem kell mindig újra elvégezni egy Gram-Schmidt ortogonalizációt.

Adott k dimenziós $L \subset \mathbb{Q}^n$ rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisához, található annak egy $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$ gyengén redukált bázisa. Ezt a kezdeti bázis *gyengén redukáltjának* hívjuk, a $\mathbf{b}'_i$ vektort pedig a $\mathbf{b}_i$ vektor $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$ szerinti *gyengén redukáltjának* nevezzük. Egy rács bázisának gyengén redukáltjára gondolhatunk úgy, mint a bázis diszkrét Gram-Schmidt ortogonalizáltjára, ugyanis itt is mint az ortogonalizálásnál, a $\mathbf{b}_i$ vektorunkat a

$$\mathbf{b}_i + [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$$

affin altéren belül visszük közelebb az ortogonálishoz. A különbség, hogy így általában nem tudunk a $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ altérre teljesen merőleges vektort találni, mivel az affin altéren belül nincs feltétlen ilyen rácsvektor.

Az igazság az, hogy gyengén redukált bázis ortogonalitási defektusa tetszőlegesen nagy lehet. Hermit úgy tette erősebbé a gyenge redukáltság fogalmát, hogy a gyenge redukáltság mellett egy extra feltételt adott.

2.5. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Amennyiben a bázis gyengén redukált, és tetszőleges $i < j$ indexek esetén

$$\|\mathrm{proj}^{\perp}_{i-1}(\mathbf{b}_i)\| \leq \|\mathrm{proj}^{\perp}_{i-1}(\mathbf{b}_j)\|$$

teljesül, akkor azt mondjuk, hogy a bázis *Hermit-redukált*.

Most megmutatjuk, hogy egy k dimenziós Hermit-redukált bázis ortogonalitási defektusa nem lehet nagyobb egy bizonyos felső határnál. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ Hermit-redukált bázisa, és ennek a $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ Gram-Schmidt ortogonalizáltja. Figyeljük meg, hogy a Hermit-redukáltság miatt

$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^* + \mu_{i+1,i}\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2 + \|\mathbf{b}_i^*\|^2/4 \tag{2.2.7}$$

és így

$$\|\mathbf{b}_i^*\|^2 \leq \frac{4}{3}\|\mathbf{b}_{i+1}^*\|^2 \tag{2.2.8}$$

teljesül. Ezek szerint tetszőleges $i < j$ indexek esetén

$$\|\mathbf{b}_i^*\|^2 \leq (4/3)^{j-i}\|\mathbf{b}_j^*\|^2 \tag{2.2.9}$$

és így

$$\begin{aligned}
\frac{\|\mathbf{b}_i\|^2}{\|\mathbf{b}_i^*\|^2} &= \frac{\|\mu_{i,1}\mathbf{b}_1^* + \mu_{i,2}\mathbf{b}_2^* + \ldots + \mu_{i,i-1}\mathbf{b}_{i-1}^* + \mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} &&= \\
&= \frac{\mu_{i,1}^2\|\mathbf{b}_1^*\|^2 + \mu_{i,2}^2\|\mathbf{b}_2^*\|^2 + \ldots + \mu_{i,i-1}^2\|\mathbf{b}_{i-1}^*\|^2 + \|\mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} &&\leq \\
&\leq \frac{(\|\mathbf{b}_1^*\|^2 + \|\mathbf{b}_2^*\|^2 + \ldots + \|\mathbf{b}_{i-1}^*\|^2)/4 + \|\mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} &&\leq \\
&\leq \frac{(4/3 + (4/3)^2 + \ldots + (4/3)^{i-1})\|\mathbf{b}_i^*\|^2/4 + \|\mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} &&= \\
&= (4/3 + (4/3)^2 + \ldots + (4/3)^{i-1})/4 + 1 = (4/3)^{i-1}.
\end{aligned} \tag{2.2.10}$$

Ezek szerint egy k dimenziós L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ Hermit-redukált bázisának ortogonalitási defektusára a következő felső becslést kapjuk (Hermit egyenlőtlenség):

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_1^*\|} \cdot \frac{\|\mathbf{b}_2\|}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot \frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} \leq \left(\frac{2}{\sqrt{3}}\right)^{1+2+\ldots+k-1} = \left(\frac{2}{\sqrt{3}}\right)^{(k-1)k/2} \tag{2.2.11}$$

Hermit algoritmust is adott egy ilyen bázis megtalálására, ami megtalálható Jacobinak írt levelében [Ngu10]. Az eredeti algoritmusnak mi egy iteratív változatát írjuk le a 2.4. algoritmusban. Ez az algoritmus véges sok iterációban leáll, és végül Hermit-redukált bázist ad vissza. Ezek szerint tetszőleges rácsnak található Hermit-redukált bázisa, és így adott k dimenziós $L \subset \mathbb{Q}^n$ rács esetén mindig található olyan bázis, mely ortogonalitási defektusára az (2.2.11) egyenlőtlenség teljesül.

Ezek szerint értelmes a

$$\delta_k := \sup_{L \in \mathscr{L}_k} \delta(L) \tag{2.2.12}$$

konstans. Egy k dimenziós rácsnak δ_k ortogonalitási defektusú bázisa mindig található, viszont ennél kisebb ortogonalitási defektussal rendelkező bázis nem feltétlen.

Hermit algoritmusa nem csak az ortogonalitási defektusra ad felső becslést. (2.2.8) alapján azt kapjuk, hogy

$$\|\mathbf{b}_1\| = \|\mathbf{b}_1^*\| \leq (2/\sqrt{3})^{i-1}\|\mathbf{b}_j^*\|. \tag{2.2.13}$$

2.4. Algoritmus Hermit redukció

Név: `Hermit_redukció` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
Be: Egy $L \subset \mathbb{Q}^n$ rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa
Ki: Az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ Hermit-redukált bázisa.

$i \leftarrow k-1$
`GS_ort` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
Ciklus amíg $i > 0$
    Ciklus $j = (i+1)..k$ $(+1)$
        $\mathbf{b}_j \leftarrow \mathbf{b}_j - \lfloor \mu_{j,i} \rceil \mathbf{b}_i$
    Ciklus vége
    Frissítsük a Gram-Schmidt együtthatókat
    Ha $\forall j > i$: $\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\| \leq \|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_j)\|$ **akkor**
        $i \leftarrow i-1$
    különben
        Válasszunk egy $j > i$ indexet amire $\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\| > \|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_j)\|$ teljesül.
        `csere` $(\mathbf{b}_i, \mathbf{b}_j)$
        Ha $j < k$ **akkor**
            $i \leftarrow j$
        különben
            $i \leftarrow k-1$
        Elágazás vége
    Elágazás vége
Ciklus vége

Ezek szerint

$$\|\mathbf{b}_1\| \leq (2/\sqrt{3})^{k-1} \min_j \|\mathbf{b}_j^*\|,$$

és így (1.3.4) szerint azt is megkapjuk, hogy

$$\|\mathbf{b}_1\| \leq (2/\sqrt{3})^{k-1} \lambda(L), \tag{2.2.14}$$

azaz a Hermit redukció segítségével megközelítjük az L rács legrövidebb vektorát is.

Az eddigi számolások eredményeit a következő tételben foglalhatjuk össze:

2.6. Tétel. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy Hermit-redukált $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen a bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. Ekkor $i < j$ esetén*

$$\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_j^*\|} \leq (4/3)^{(j-i)/2}$$

továbbá a

$$\|\mathbf{b}_1\| \leq (4/3)^{(k-1)/2} \lambda(L),$$

és

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \leq (4/3)^{\binom{k}{2}/2}$$

becslések teljesülnek.

Ezen felső becslések jelentőségét a következő fejezetben jobban megvizsgáljuk.

2.3. Algoritmikus problémák rácsokon, és a Lenstra-Lenstra-Lovász algoritmus

Ezen fejezetben először bemutatunk néhány alapvető algoritmikus problémát. Ezen problémák bonyolultságáról, és a köztük levő összefüggésekről már rengeteg tény ismert. [Gol02] Mi most a bonyolultság szempontjából csak egy kis ízelítőt adunk, és bemutatunk néhány egyszerű de elegáns összefüggést.

Ezen alfejezetben, mivel algoritmusok futásidejét vizsgáljuk, így rácsainkat az $\mathbb{R}$ számtest helyett a $\mathbb{Q}$ számtest fölött nézzük. Ez azért fontos, mert az algoritmusaink inputjának végesnek kell lenni. Algoritmusaink inputja általában egy k dimenziós $L \subset \mathbb{Q}^n$ rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Ekkor az input $k \cdot n$ egész számpárból áll (a vektorok minden koordinátája egy racionális szám, amit egy egész számokból álló számpár reprezentál). A valóságban persze a számok bitenként vannak megadva, így az input mérete alatt az inputban szereplő bitek számát értjük.

Legyenek például a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ vektorok egy algoritmus inputjai. Ekkor az inputban $2 \cdot n \cdot k$ egész szám szerepel. Ha a legnagyobb abszolút értékű szám abszolút értéke M, akkor az input bitjeinek száma nem több mint

$$2nk(\log M + 1),$$

ahol a $+1$ bit az előjel miatt kell. Ez az algoritmus pontosan akkor polinomiális, ha a futás során elvégzett bitműveletek száma

$$\mathcal{O}\left(p(n, k, \log M)\right)$$

ahol p egy polinom.

Most, hogy a futásidővel kapcsolatos dolgokat tisztáztuk, bemutatjuk ezen dolgozat fő problémáit. A két legalapvetőbb probléma a következő:

SVP (Shortest Vector Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok és legyen L az ezen vektorok által generált rács. Találjuk meg az L rács (egyik) legrövidebb nem $\mathbf{0}$ vektorát.

CVP (Closest Vector Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám, és egy $\mathbf{v} \in \mathbb{Q}^n$ vektor. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok, és legyen L az ezen vektorok által generált rács. Találjuk meg a vektorhoz (egyik) legközelebb eső $\mathbf{b} \in L$ rácspontot.

Egy néhány sorban leírható összefüggés, hogy CVP legalább olyan nehéz mint SVP, tehát SVP visszavezethető polinomiálisan sok CVP elvégzésére. Az itt található bizonyítást Noah Stephens-Davidowitz előadása [SD20] alapján írjuk fel. A bizonyítás eredeti változata Oded

Goldreich, Daniele Micciancio, Muli Safra és Jean-Pierre Seifert cikkéből származik. Az összefüggés megmutatásához nézzük az SVP egy példányát. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok és legyen L az ezen vektorok által generált rács. Definiáljuk az

$$L_i := L(\mathbf{b}_1, \mathbf{b}_2, \ldots, 2\mathbf{b}_i, \ldots, \mathbf{b}_k)$$

rácsot. Ekkor a CVP feladat segítségével megtalálhatjuk az L_i rács $\mathbf{b}_i$ vektorhoz legközelebb eső vektorát. Ez a legrövidebb olyan L rácsbeli vektor, amelynek a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis szerinti i. koordinátája páratlan. Jelölje ezt a vektort $\mathbf{b}'_i$. Mivel a L rács legrövidebb vektorának nem lehet minden $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis szerinti koordinátája páros (ugyanis ekkor 2-vel leosztva rövidebb rácsvektort kapnánk), így a

$$\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$$

vektorok közül a legrövidebb vektor pont az L rács legrövidebb vektora. Ezzel megkaptuk a kívánt visszavezetést.

A CVP NP-nehéz. Ezen tény eredetileg Peter van Emde Boas-tól származik. Mi a bizonyítást megint Noah Stephens-Davidowitz előadása [SD20] alapján írjuk fel. A bizonyítás úgy történik, hogy a CVP-t visszavezetjük az úgynevezett SUBSETSUM problémára, amely egy klasszikus NP-teljes probléma. A SUBSETSUM problémában az a feladat, hogy adott $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ és $s \in \mathbb{Z}$ egész számok esetén eldöntsük, hogy létezik-e úgy egy $S \subset \{1, 2, \ldots, k\}$ halmaz, hogy

$$\sum_{i \in S} a_i = s.$$

Ekkor a CVP problémát a

$$\begin{aligned} \mathbf{b}_1 &= (a_1, 2, 0, 0, \ldots, 0) \\ \mathbf{b}_2 &= (a_2, 0, 2, 0, \ldots, 0) \\ &\ldots \\ \mathbf{b}_k &= (a_k, 0, 0, 0, \ldots, 2) \\ \mathbf{v} &= (s, 1, 1, 1 \ldots, 1) \end{aligned} \tag{2.3.1}$$

kiindulási vektorokon megoldva kapunk egy $\mathbf{b} \in L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ vektort amely távolsága $\mathbf{v}$-től minimális. Egy kevés ideig tanulmányozva (2.3.1)-et megfigyelhetjük, hogy a SUBSETSUM problémánknak pontosan akkor van megoldása, ha

$$\mathrm{d}(\mathbf{b}, \mathbf{v}) = \sqrt{k}.$$

Ezzel be is láttuk a CVP NP-nehézségét. Habár SVP-ről még nincs bebizonyítva, hogy NP-nehéz viszont sokan úgy gondolják, hogy az. Emellett ami ismert, hogy randomizált visszavezetésre nézve NP-nehéz.

Az előző fejezetben láttuk, hogy tetszőleges rácsnak található minimális ortogonalitási defektusú bázisa. Ez a következő problémát sugallja:

BRP (Basis Reduction Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok, és legyen L az ezen vektorok által generált rács. Találjuk meg az L rács egy olyan $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$ bázisát, amely ortogonalitási defektusa minimális.

Ez a probléma szintén NP-nehéz, tehát az eddig felsorolt problémák valamilyen értelemben mind nehezek. Persze ezen problémákat valamivel könyebbé tehetjük, ha tekintjük az ő approximációs változatukat:

ASVP (Approximate Shortest Vector Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok és legyen L az ezen vektorok által generált rács. Találjuk egy olyan $\mathbf{b} \in L$ rácsvektort, hogy

$$\|\mathbf{b}\| \leq s_k \lambda(L),$$

ahol $s_k \in \mathbb{R}$ csak a dimenziótól függő konstans.

ACVP (Approximate Closest Vector Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám, és egy $\mathbf{v} \in \mathbb{Q}^n$ vektor. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok, és legyen L az ezen vektorok által generált rács. Találjuk egy olyan $\mathbf{b} \in L$ rácsvektort, hogy

$$\mathrm{d}(\mathbf{b}, \mathbf{v}) \leq c_k \min_{\mathbf{b}' \in L} \mathrm{d}(\mathbf{b}', \mathbf{v}),$$

ahol $c_k \in \mathbb{R}$ csak a dimenziótól függő konstans.

ABRP (Approximate Basis Reduction Problem)

Legyen adott egy $k \in \mathbb{N}$ természetes szám. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{Q}^n$ lineárisan független vektorok, és legyen L az ezen vektorok által generált rács. Találjuk meg az L rács egy olyan $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$ bázisát, amelyre

$$\delta(\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k) \leq b_k \delta(L),$$

ahol $b_k \in \mathbb{R}$ csak a dimenziótól függő konstans.

Hermit korábban leírt 2.4. algoritmusa megoldja ASVP-t $s_k = (4/3)^{(k-1)/2}$ esetén, ABRP-t pedig $b_k = (4/3)^{(k-1)k/4}$ esetén. Habár nem teljesen egyértelmű, de Babai közeli sík kereső algoritmusát [Bab86] felhasználva az ACVP is megoldható $c_k = (4/3)^{k/2}$ választással.

Az, hogy Hermit algoritmusának futásideje polinomiális-e váltakozó dimenzióban, nyitott kérdés. Ezt a problémát oldja fel Lovász László, H. Lenstra és A. Lenstra a híres LLL algoritmussal. Ennek segítségével ASVP, ACVP és ABRP megoldható $s_k = (2)^{(k-1)/2}$, $c_k = (2)^{k/2}$ és $b_k = (2)^{(k-1)k/4}$ választásokkal polinomiális időben. Az első észrevétel ami ezen algoritmushoz vezet, az az, hogy a Hermit redukáltság erejét meg tudjuk őrizni úgy, hogy valamivel gyengébb feltételeket szabunk.

2.7. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Amennyiben a bázis gyengén redukált, és tetszőleges $i < k$ index esetén

$$\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\|^2 \leq (4/3)\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_{i+1})\|^2 \tag{2.3.2}$$

akkor azt mondjuk, hogy a bázis *LLL-redukált*.

Ekkor ugyanazon számolások elvégzésével a korábbi 2.6. tételhez hasonló tételt kapunk:

2.8. Tétel. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy LLL-redukált $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen a bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. Ekkor $i < j$ esetén*

$$\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_j^*\|} \leq 2^{(j-i)/2}$$

továbbá a

$$\|\mathbf{b}_1\| \leq 2^{(k-1)/2}\lambda(L)$$

és

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \leq 2^{\binom{k}{2}/2}$$

becslések teljesülnek.

Az LLL-redukáltság definíciója alapján a 2.5. algoritmust kapjuk egy LLL-redukált bázis megtalálására.

2.5. Algoritmus Lenstra-Lenstra-Lovász redukció

Név: `LLL` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k, \mathbf{v})$
Be: Egy $L \subset \mathbb{Q}^n$ rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa
Ki: Az L rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ LLL-redukált bázisa

1: **Ciklus amíg** $\exists i$: $\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_i)\|^2 > (4/3)\|\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}_{i+1})\|^2$
2: `csere` $(\mathbf{b}_i, \mathbf{b}_{i+1})$
3: `gyenge_redukció` $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
4: **Ciklus vége**

2.9. Tétel. *A 2.5. algoritmus iterációinak száma az input méretében polinomiális.*

Bizonyítás. Legyen

$$D(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) := \prod_{i=1}^{k} \|\mathbf{b}_i^*\|^{k-i},$$

ahol $\mathbf{b}_i^*$ a $\mathbf{b}_i$ vektor Gram-Schmidt ortogonalizáltja. A tétel azon a megfigyelésen alapszik, hogy amikor az algoritmus 2. sorában megcseréljük a $\mathbf{b}_i$ és $\mathbf{b}_{i+1}$ vektorokat, akkor $D(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ értéke legalább $2/\sqrt{3}$-al csökken, a gyenge redukció által viszont változatlan marad. A bizonyítás további részében alsó és felső korlátot szabunk $D(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ nagyságára, ezzel belátva a tételt.

Jelölje L_i a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i$ vektorok által generált rácsot. Ekkor

$$D(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \prod_{i=1}^{n-1} \mathrm{vol}\, L_i.$$

Minkowki 2. tétele (1.13. tétel) szerint

$$\frac{\lambda_1(L_i)\cdot\lambda_2(L_i)\cdot\ldots\cdot\lambda_i(L_i)}{i^{i/2}} < \operatorname{vol} L_i.$$

Jelölje az L rács szukcesszív minimumait rendre $\lambda_1,\lambda_2,\ldots,\lambda_k$. Mivel $\lambda_j \le \lambda_j(L_i)$ így azt kaptuk, hogy

$$\frac{\lambda_1\cdot\lambda_2\cdot\ldots\cdot\lambda_i}{i^{i/2}} < \operatorname{vol} L_i.$$

Ezek szerint az L rács tetszőleges $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ bázisa esetén

$$\left(\frac{\lambda_1^2}{k}\right)^{\binom{k}{2}/2} < \frac{\lambda_1^{k-1}\cdot\lambda_2^{k-2}\cdot\ldots\cdot\lambda_k}{(2^2\cdot 3^3\cdot\ldots\cdot(k-1)^{(k-1)})^{1/2}} < D(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k).$$

Mivel $\|\mathbf{b}_i^*\| \le \|\mathbf{b}_i\|$, így

$$\left(\frac{\lambda_1^2}{k}\right)^{\binom{k}{2}/2} < D(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k) \le (\max_i \|\mathbf{b}_i\|)^{\binom{k}{2}},$$

tehát az algoritmus N iterációinak számára a következő felső becslést kapjuk:

$$N < \binom{k}{2}((1/2)\cdot\log k + \log\max_i \|\mathbf{b}_i\| - \log\lambda_1)$$

Legyen az inputban szereplő legnagyobb abszolút értékű egész szám abszolútértéke M. Ekkor $1/M^{nk} \le \lambda_1$, és $\max_i \|\mathbf{b}_i\| \le \sqrt{n}M$, tehát

$$N < \binom{n}{k}((1/2)\log k + (1/2)\log n + (nk+1)\log M).$$

Innen ahhoz, hogy lássuk, hogy az algoritmus polinomiális futásidejű, még azt kell megmutatni, hogy az inputban szereplő számok mérete nem nő túl nagyra. Mi ezt ezen dolgozatban nem fejtjük ki. □

Megjegyeznénk, hogy az LLL-redukáltság definíciójában 4/3 helyett tetszőleges 1-nél nagyobb de 3/2-nél kisebb konstans választható. Ezzel Lovász algoritmusa változatlanul polinomiális időben lefutna (bár akár lényegesen lasabban), viszont a 2.8. tétel felső becsléseiben a 2 hatványalapot tetszőlegesen közel vihetnénk $2/\sqrt{3}$-hoz. Nyitott kérdés, hogy leáll-e az algoritmus váltakozó dimenzióra polinomiális időben, ha 4/3 helyett 1-et írunk.

Lovász algoritmusát felhasználhatjuk arra, hogy megtaláljuk egy rács legrövidebb vektorát fix dimenzióban polinomiális időben. Erre Kannan algoritmusa [Kan83] szolgál. Mi most az algoritmust nem részletezzük, viszont megmutatjuk, hogy az milyen összefüggésben áll az ortogonalitási defektussal és az ahhoz tartozó téglatesttel.

2.10. Tétel. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ bázisa. Legyen a bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*,\mathbf{b}_2^*,\ldots,\mathbf{b}_k^*$. Legyen*

$$H = \{x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^* \mid \forall i\colon |x_i| \le \|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|\}$$

és ζ a H-beli rácspontok száma. Ekkor

$$\delta(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k) \le \zeta \le 3^k\delta(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k). \tag{2.3.3}$$

Megjegyzés. H egy $[L]$ altérbeli origó súlypontú k dimenziós kocka $2\|\mathbf{b}_1\|, 2\|\mathbf{b}_2\|, \ldots, 2\|\mathbf{b}_k\|$ élhosszúságokkal, melynek lapjai a bázis Gram-Scmidth ortogonalizált vektoraira merőlegesek.

Bizonyítás. Vizsgáljuk meg, hogy legfeljebb hány $\mathbf{b} \in L$ rácspont esik H-ba. Minden rácspont

$$\mathbf{b} = s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \ldots + s_k\mathbf{b}_k = x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^*$$

alakú ahol $s_i \in \mathbb{Z}$. Az a kérdés, hogy hányféleképp választhatjuk meg az $s_1, s_2, \ldots, s_k$ egész számokat, hogy $\mathbf{b} \in H$ teljesüljön.

Először nézzük meg, hogy hányféleképp választhatjuk meg s_k értékét, hogy a

$$H_k := ([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}] + s_k\mathbf{b}_k) \cap H$$

halmaz ne legyen üres. Jelölje ezt a számot ζ_k. Mivel $s_k = x_k$, így ehhez az $|s_k| \leq \|\mathbf{b}_k\|/\|\mathbf{b}_k^*\|$ egyenlőtlenségnek kell teljesülnie. Ezek szerint

$$\zeta_k = 2\left\lfloor \frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} \right\rfloor + 1$$

így a

$$\frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} \leq \zeta_k \leq 3\frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|}$$

becsléseket kapjuk. Ha s_k értékét már megválasztottuk úgy, hogy a H_k halmaz ne legyen üres, nézzük meg, hányféleképp választható meg s_{k-1} értéke úgy, hogy a

$$H_{k-1} := ([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-2}] + s_{k-1}\mathbf{b}_{k-1} + s_k\mathbf{b}_k) \cap H$$

halmaznak is legyen eleme. Jelölje ezt a számot ζ_{k-1}. Most pontos értéket nem tudunk adni ζ_{k-1}-nek. Ezt az előző esetben azért tudtuk megtenni, mivel az alterünket a $\mathbf{0}$-ból kiindulva toltuk el, most viszont a „kiindulási pont" $s_k\mathbf{b}_k$. Ekkor mivel $x_{k-1} = s_k \cdot \mu_{k,k-1} + s_{k-1}$, így a kérdés, hogy hány olyan s_{k-1} egész szám van amivel $|s_k \cdot \mu_{k,k-1} + s_{k-1}| \leq \|\mathbf{b}_{k-1}\|/\|\mathbf{b}_{k-1}^*\|$ teljesül. Ezek szerint

$$\frac{\|\mathbf{b}_{k-1}\|}{\|\mathbf{b}_{k-1}^*\|} \leq \frac{2\|\mathbf{b}_{k-1}\|}{\|\mathbf{b}_{k-1}^*\|} - 1 \leq \zeta_{k-1} \leq \left\lfloor \frac{2\|\mathbf{b}_{k-1}\|}{\|\mathbf{b}_{k-1}^*\|} \right\rfloor + 1 \leq 3\frac{\|\mathbf{b}_{k-1}\|}{\|\mathbf{b}_{k-1}^*\|}$$

becslések még így is fennálnak. Most, hogy az eddigieket folytatni tudjuk, vezessünk be egy általános jelölést. Legyen

$$H_i := ([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}] + s_i\mathbf{b}_i + s_{i+1}\mathbf{b}_{i+1} + \ldots + s_k\mathbf{b}_k) \cap H.$$

Legyenek $s_{i+1}, s_{i+2}, \ldots, s_k$ fix egész számok úgy, hogy H_{i+1} nem üres. Nézzük meg, hogy legfeljebb hányféleképp választható meg s_i, hogy H_i se legyen üres. Jelölje ezt a számot ζ_i. Ekkor

$$\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|} \leq \frac{2\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|} - 1 \leq \zeta_i \leq \left\lfloor \frac{2\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|} \right\rfloor + 1 \leq 3\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|},$$

így végül a következőt kapjuk:

$$\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_1^*\|} \cdot \frac{\|\mathbf{b}_2\|}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot \frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} \leq \zeta \leq 3\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_1^*\|} \cdot 3\frac{\|\mathbf{b}_2\|}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot 3\frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} = 3^k\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

tehát a tételt beláttuk. □

Ortogonális bázis és azonos hosszúságú bázisvektorok esetén $\zeta = 3^k$. Ekkor ζ értéke az állításbeli felső becslés. Az állítás alapján látható, hogy $\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ korlátot szab a H-beli rácspontok számára. Miért jó ez nekünk?

Legyen m olyan index amire $\|\mathbf{b}_m\|$ hossza minimális a bázissvektorok közül. Mivel

$$\mathrm{B}(\|\mathbf{b}_m\|) \subset H,$$

így az összes H-beli rácspontot átnézve megtalálható a legrövidebb nem $\mathbf{0}$ rácsvektor. Ehhez az állítás szerint legfeljebb

$$3^k \cdot \delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

vektor hosszát kell megnézni. Ha először elvégezzük az 2.5. algoritmust, és utána vizsgáljuk át H vektorait akkor ezek szerint legfeljebb

$$3^k \cdot 2^{k(k-1)/4}$$

vektor hosszát kell átvizsgálni.

Hasonló gondolatok alapján eljuthatunk a CVP pontos megoldásához is.

2.11. Lemma. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen az első i bázisvektor által kifeszített rács L_i. Legyen $\mathbf{v} \in [L]$ tetszőleges, és legyen*

$$V_i := \mathrm{proj}_i(\mathbf{v}) + \mathrm{vor}\, L_i.$$

Legyen adott egy $\mathbf{b} \in L$ rácspont. A következők ekvivalensek

(i) *A $\mathbf{b}$ vektor az L rács $\mathbf{v}$ vektorhoz eső egyik legközelebbi vektora.*

(ii) *Tetszőleges i index esetén* $\mathrm{proj}_i(\mathbf{b}) \in V_i$

(iii) $\mathbf{b} \in \mathbf{v} + \mathrm{vor}\, L$.

Bizonyítás. $(i) \Rightarrow (ii)$ megmutatásához indirekt tegyük fel, hogy $\mathrm{proj}_i(\mathbf{b}) \notin V_i$. Ekkor

$$\mathrm{proj}_i(\mathbf{b} - \mathbf{v}) \notin \mathrm{vor}\, L_i$$

és ezek szerint létezik egy $\mathbf{r}_i \in L_i$, hogy

$$\|\mathrm{proj}_i(\mathbf{b} - \mathbf{v}) - \mathbf{r}_i\| < \|\mathrm{proj}_i(\mathbf{b} - \mathbf{v})\|.$$

Ezzel ellentmondásra jutottunk, ugyanis ekkor $\mathbf{b} - \mathbf{r}_i \in L$ egy a $\mathbf{v}$ vektorhoz a $\mathbf{b}$ rácspontnál közelebb eső rácspont.

Az, hogy $(ii) \Rightarrow (iii)$ következik abból, hogy $V_k = \mathbf{v} + \mathrm{vor}\, L$.

Végül az, hogy $(iii) \Rightarrow (i)$ következik abból, hogy

$$\mathbf{b} \in \mathbf{v} + \mathrm{vor}\, L \Leftrightarrow \mathbf{b} - \mathbf{v} \in \mathrm{vor}\, L \Leftrightarrow \forall \mathbf{b}' \in L\colon\ \|\mathbf{b} - \mathbf{v} - \mathbf{b}'\| \geq \|\mathbf{b} - \mathbf{v}\|,$$

azaz $\mathbf{b} \in \mathbf{v} + \mathrm{vor}\, L$ esetén $\mathbf{b}$ legalább olyan közel van $\mathbf{v}$-hez, mint bármely másik rácspont. Ezzel a lemmát beláttuk. □

Legyen R_i a $\mathrm{vor}L_i$ Voronoi cella köré írt gömb sugara. Legyen $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis Gram-Schmidt ortogonalizáltja. Legyen

$$\mathbf{v} = x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^*.$$

Az előző lemma szerint a $\mathbf{v}$ vektorhoz legközelebb eső rácspont megtalálásához elég az olyan

$$\mathbf{b} = y_1\mathbf{b}_1^* + y_2\mathbf{b}_2^* + \ldots + y_k\mathbf{b}_k^*$$

vektorokat átvizsgálni, ahol minden i indexre $|x_i - y_i| \leq R_i/\|\mathbf{b}_i^*\|$, mivel különben $\mathrm{proj}_i(\mathbf{b}) \notin V_i$ teljesülne.

2.12. Definició. Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen az első i bázisvektor által kifeszített rács L_i. Legyen R_i a $\mathrm{vor}L_i$ Voronoi cella köré írt gömb sugara. Legyen $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis Gram-Schmidt ortogonalizáltja. A

$$\nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) := \frac{2R_1}{\|\mathbf{b}_1^*\|} \cdot \frac{2R_2}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot \frac{2R_k}{\|\mathbf{b}_k^*\|}$$

valós számot az L rács *Voronoi-defektusának* hívjuk.

2.13. Lemma.

$$2R_i \geq \|\mathbf{b}_i^*\|$$

Bizonyítás. A lemma bizonyításához elég belátni, hogy $\mathbf{b}_i^*/2 \in \mathrm{vor}L_i$, azaz $\mathbf{b}_i^*/2$ közelebb van a $\mathbf{0}$-hoz mint bármely $\mathbf{b} \in L_i$ rácsponthoz. Ez abban az esetben, ha $\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}) = \mathbf{0}$, nyilvánvaló. Tegyük fel, hogy ez nem igaz és legyen

$$\mathbf{b} = x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_i\mathbf{b}_i^*.$$

Mivel $\mathbf{b} \in L_i$ így x_i egész szám, és mivel feltettük, hogy $\mathrm{proj}_{i-1}^{\perp}(\mathbf{b}) \neq \mathbf{0}$ így $|x_i| > 0$. Ezek szerint

$$\|\mathbf{b} - \mathbf{b}_i^*/2\| \geq \|\mathbf{b}_i^*/2\|$$

és ezzel a lemmát beláttuk. □

2.14. Tétel. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Legyen a bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. Legyen az első i bázisvektor által kifeszített rács L_i. Legyen R_i a* $\mathrm{vor}L_i$ *Voronoi cella köré írt gömb sugara. Legyen*

$$\mathbf{v} = x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^*.$$

Legyen

$$H = \{y_1\mathbf{b}_1^* + y_2\mathbf{b}_2^* + \ldots + y_k\mathbf{b}_k^* \mid \forall i\colon |x_i - y_i| \leq R_i/\|\mathbf{b}_i^*\|\}$$

és ζ a H-beli rácspontok száma, $\mathbf{b} \in L$ pedig a $\mathbf{v}$ vektorhoz (egyik) legközelebb eső rácspont. Ekkor

$$\zeta \leq 2^k \nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k), \tag{2.3.4}$$

és $\mathbf{b} \in H$.

Bizonyítás. Az, hogy $\mathbf{b} \in H$ következik a 2.11. lemmából. A H téglatestbe eső rácspontok számára való becslés a 2.10. tételben szereplő becslés bizonyításához teljesen hasonlóan látjuk be: Legyen

$$H_i := ([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-i}] + s_i\mathbf{b}_i + s_{i+1}\mathbf{b}_{i+1} + \ldots + s_k\mathbf{b}_k) \cap H.$$

Legyenek $s_{i+1}, s_{i+2}, \ldots, s_k$ fix egész számok úgy, hogy H_{i+1} nem üres. Nézzük meg, hogy legfeljebb hányféleképp választható meg s_i, hogy H_i se legyen üres. Jelölje ezt a számot ζ_i. Ekkor a 2.13. lemmát felhasználva azt kapjuk, hogy

$$\zeta_i \leq \left\lfloor \frac{2R_i}{\|\mathbf{b}_i^*\|} \right\rfloor + 1 \leq 2\frac{2R_i}{\|\mathbf{b}_i^*\|},$$

így végül a következőt kapjuk:

$$\zeta \leq 2\frac{2R_1}{\|\mathbf{b}_1^*\|} \cdot 2\frac{2R_2}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot 2\frac{2R_k}{\|\mathbf{b}_k^*\|} = 2^k \nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

tehát a tételt beláttuk. □

Ezek szerint a CVP megoldásához elég

$$2^k \cdot \nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$$

vektort átvizsgálni.

2.15. Tétel. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács, és ennek egy LLL-redukált $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázisa. Ekkor*

$$\nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \leq 2^{(k+1)k/4}.$$

Bizonyítás. Először is figyeljük meg, hogy

$$R_i^2 \leq (\|\mathbf{b}_1^*\|^2 + \|\mathbf{b}_2^*\|^2 + \ldots + \|\mathbf{b}_i^*\|^2)/4,$$

tehát az 2.8 tétel szerint

$$\begin{aligned}\frac{4R_i^2}{\|\mathbf{b}_i^*\|^2} &\leq \frac{\|\mathbf{b}_1^*\|^2 + \|\mathbf{b}_2^*\|^2 + \ldots + \|\mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} = \\ &= \frac{\|\mathbf{b}_1^*\|^2}{\|\mathbf{b}_i^*\|^2} + \frac{\|\mathbf{b}_2^*\|^2}{\|\mathbf{b}_i^*\|^2} + \ldots + \frac{\|\mathbf{b}_i^*\|^2}{\|\mathbf{b}_i^*\|^2} \leq \\ &\leq 1 + 2^1 + 2^2 + \ldots + 2^{i-1} \leq 2^i\end{aligned}$$

és ezek szerint

$$\nu(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \frac{2R_1}{\|\mathbf{b}_1^*\|} \cdot \frac{2R_2}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot \frac{2R_k}{\|\mathbf{b}_k^*\|} \leq 2^{(1+2+\ldots+k)/2} = 2^{(k+1)k/4}.$$

□

A fentiek alapján a CVP probléma megoldható először az LLL-algoritmust elvégezve, majd a 2.14. tételben meghatározott H halmazt ($R_i/\|\mathbf{b}_i^*\|$ helyett $2^{i/2-1}$-et írva) átkutatva. Az átvizsgált vektorok száma ekkor nem lesz több mint

$$2^k \cdot 2^{(k+1)k/4}.$$

3. Redukciós tartományok, és tökéletes bázisredukció az első 4 dimenzióban

Ezen fejezet [Ste08] alapján készült. Ott megfogalmazták a Lagrange-Gauss algoritmus egy természetes általánosítását, amely az első 4 dimenzióban tökéletesen működik. A cikkben nagy hangsúlyt kap az úgynevezett Minkowski redukáltság fogalma. Ez azért hasznos, mivel Minkowski redukált bázisból kiindulva meg lehet határozni egy rács Voronoi-releváns vektorait.

Mi megnézzük, hogy mi történik akkor, ha megfeletkezünk a Minkowski redukáltságról és megvizsgáljuk, hogy így mit tudunk mondani az algoritmusról. Az algoritmust egy kicsit más alakban írjuk fel, mint ahogy az az eredeti cikkben van, így jobban látszik a hasonlóság közte és az LLL algoritmus között. Ezeken kívül megmutatjuk, hogy hogyan használható az algoritmus alacsony dimenzióban egy rács Voronoi-releváns vektorainak meghatározására, továbbá megmutatjuk, hogy az algoritmus az első 4 dimenzióban minimális ortogonalitási defektusú bázist talál.

3.1. Állítás. *Legyen adott egy k dimenziós $L \subset \mathbb{Q}^n$ rács. Legyenek adottak a L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorai. Ekkor*

$$\|\mathbf{b}_1\| = \lambda_1(L),\ \|\mathbf{b}_2\| = \lambda_2(L),\ \ldots,\ \|\mathbf{b}_k\| = \lambda_k(L) \tag{3.1}$$

pontosan akkor teljesül, ha

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_k\|$$

és tetszőleges $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k \in L$ lineárisan független vektorok esetén

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\| \leq \|\mathbf{b}'_1\| \cdot \|\mathbf{b}'_2\| \cdot \ldots \cdot \|\mathbf{b}'_k\|.$$

Bizonyítás. ($\Rightarrow$) A szukcesszív minimumok definíciója miatt

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_k\|,$$

és tetszőleges $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$ lineárisan független vektorok esetén amelyekre

$$\|\mathbf{b}'_1\| \leq \|\mathbf{b}'_2\| \leq \ldots \leq \|\mathbf{b}'_k\|$$

teljesül,

$$\lambda_i(L) \leq \|\mathbf{b}'_i\|$$

is igaz lesz tetszőleges i index esetén. Ezek szerint

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\| \leq \|\mathbf{b}'_1\| \cdot \|\mathbf{b}'_2\| \cdot \ldots \cdot \|\mathbf{b}'_k\|$$

is igaz lesz, és így az egyik irányt beláttuk.

($\Leftarrow$) A szukcesszív minimumok definíciója szerint tetszőleges i index esetén $\lambda_i(L) \leq \|\mathbf{b}_i\|$. Tegyük fel indirekt, hogy nem teljesül (3.1). Ekkor léteznie kell i indexnek, hogy $\|\mathbf{b}_i\| > \lambda_i(L)$. Mivel léteznek $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_k$ lineárisan független rácsbeli vektorok, amelyekre

$$\|\mathbf{b}'_1\| = \lambda_1(L),\ \|\mathbf{b}'_2\| = \lambda_2(L),\ \ldots,\ \|\mathbf{b}'_k\| = \lambda_k(L),$$

így ellentmondásra jutottunk, ugyanis ekkor

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\| > \|\mathbf{b}'_1\| \cdot \|\mathbf{b}'_2\| \cdot \ldots \cdot \|\mathbf{b}'_k\|.$$

□

Ezek alapján azt gondolhatnánk, hogy egy rács minimális ortogonalitási defektusú bázis megtalálása megeggyezik az olyan rácsvektorok megtalálásával amelyek (3.1)-et teljesítik. A helyzet ennél valamennyivel bonyolultabb. Legyen L egy k dimenziós rács. Be fogjuk látni a következőket:

$1 \leq k \leq 3$ esetén, ha az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorai teljesítik (3.1)-et, akkor ezek bázist alkotnak. Ezek szerint a 3. dimenzióig mindig van az L rácsnak olyan bázisa, amely teljesíti (3.1)-et.

$k = 4$ esetén előfordulhat, hogy az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ linárisan független vektorai teljesítik (3.1)-et, viszont nem alkotják a rács bázisát. Ettől függetlenül az L rácsnak ilyenkor mindig létezik olyan bázisa amely teljesíti (3.1)-et.

$k \geq 5$ esetén meglepő módon az is előfordulhat, hogy az L rácsnak nem létezik olyan bázisa amely (3.1)-et teljesítené.

Mi okozhatja ezt a váratlan változást a 4. dimenzió után? Ahhoz, hogy ezt megértsük, először is meg kell vizsgálnunk, hogyan változik a k dimenziós r sugarú gömb és az r élhosszúságú kocka viszonya k függvényében. Legyen

$$\mathrm{B}_k(r) := \{\mathbf{v} \in \mathbb{R}^k \mid \|\mathbf{v}\| \leq r\} \tag{3.2}$$

a $\mathbf{0}$ középpontú r sugarú gömb a k dimenziós euklideszi térben. Legyen $\mathbf{e}_1,\ \mathbf{e}_2,\ \ldots\ \mathbf{e}_k$ ortonormált bázis ugyanezen térben, és legyen

$$H_k(r) := \{x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \ldots + x_n\mathbf{e}_n \mid x_i \in \mathbb{R},\ |x_i| \leq r/2\} \tag{3.3}$$

egy $\mathbb{R}^k$-beli $\mathbf{0}$ súlypontú, r élhosszúságú kocka. Ennek egy adott h_k csúcsa a következő módon írható fel:

$$h_k = \pm\frac{r}{2}\mathbf{e}_1 \pm \frac{r}{2}\mathbf{e}_2 \pm \ldots \pm \frac{r}{2}\mathbf{e}_k. \tag{3.4}$$

$H_k(r)$-nek a $\mathbf{0}$-tól legtávolabb levő pontjai pont a csúcsai, melyek távolsága $\mathbf{0}$-tól:

$$\|h_k\| = \frac{\sqrt{k}}{2} \cdot r. \tag{3.5}$$

Ez alapján a következőt kapjuk:

3.2. Állítás. $\mathrm{B}_k(r)$ és $H_k(r)$ viszonya k függvényében:

- $1 \leq k \leq 3$ *esetén* $\|h_k\| < r$, *így ekkor a* $H_k(r)$ *kocka teljes egészében a* $\mathrm{B}_k(r)$ *gömb belsejében van.*
- $k = 4$ *esetén* $\|h_k(r)\| = r$, *így ekkor a* $H_k(r)$ *kocka csúcsai pont a* $\mathrm{B}_k(r)$ *gömb felszínén helyezkednek el, míg a kocka többi pontja a gömb belsejében van.*
- $k \geq 5$ *esetén* $\|h_k(r)\| > r$, *így ebben az esetben a* $H_k(r)$ *kocka csúcsai kilógnak a* $\mathrm{B}_k(r)$ *gömbből.*

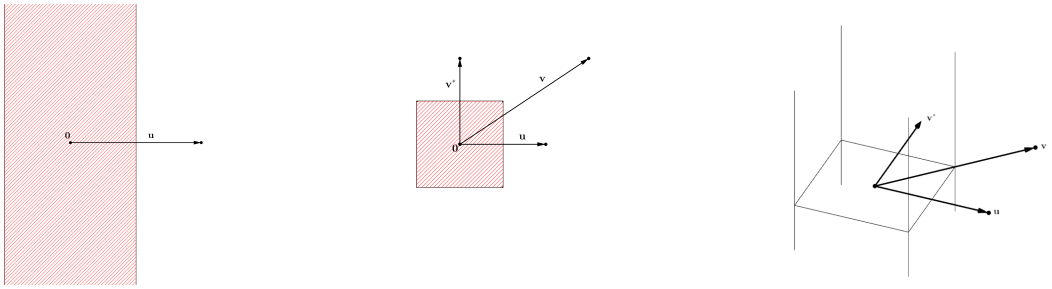
Érdekes módon ezen tény eredményezi majd a föntebb leírt változást a 4. dimenzió után. Mi köze a szukcesszív minimumoknak, a gömbök és kockák viszonyához? Ahhoz, hogy ezt megvizsgáljuk, egy új fogalomra lesz szükségünk.

Legyenek adottak $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Legyen ezek Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$.

3.3. Definició. A

$$\mathrm{GY}(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k) := \{x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^* \mid \forall j\colon |x_j| \le 1/2\} + [\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k]^\perp$$

k dimenziós „sávot” (lásd 3.1. ábra) a $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ független rácspontok *gyenge redukciós tartományának* hívjuk.



(a) $n = 2$, $k = 1$ (b) $n = 2$, $k = 2$ (c) $n = 3$, $k = 2$

3.1. ábra. Néhány gyenge redukciós tartomány.

3.4. Állítás. *Legyen* $\mathbf{v} \in \mathbb{R}^n$ *tetszőleges. Ekkor léteznek* s_1, s_2, … $s_k \in \mathbb{Z}$ *egész számok, hogy*

$$\mathbf{v} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k \in \mathrm{GY}(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k).$$

Bizonyítás. A megfelelő s_i együtthatókat a következő rekurzió segítségével határozzuk meg:

$$\begin{aligned} &\mathbf{v}[0] = \mathbf{v} \\ &\mathrm{proj}_k(\mathbf{v}[i]) = x_1[i]\mathbf{b}_1^* + x_2[i]\mathbf{b}_2^* + \ldots + x_k[i]\mathbf{b}_k^* \qquad i = 0, 1, \ldots\ k-1 \\ &\mathbf{v}[i+1] = \mathbf{v}[i] - \lfloor x_{k-i}[i] \rceil \mathbf{b}_{k-i} \end{aligned} \tag{3.6}$$

A $\mathbf{v}[i+1] = \mathbf{v}[i] - \lfloor x_{k-i}[i] \rceil \mathbf{b}_{k-i}$ rekurzióval elérjük, hogy

$$-1/2 \le x_{k-i}[i+1] \le 1/2 \tag{3.7}$$

teljesüljön. Mivel

$$x_{k-i}[i+1] = x_{k-i}[i+2] = \ldots = x_{k-i}[k],$$

így $s_i = x_i[k]$ választással az állításnak megfelelő egész számokat kapjuk. □

3.5. Definició. Az 3.4. állításban meghatározott (egyik)

$$\mathbf{v}' = \mathbf{v} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k$$

vektort a $\mathbf{v}$ vektor $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ vektorok szerinti gyenge redukáltjának hívjuk.

Most végre megérthetjük, hogy miért következik be a föntebb leírt változás a 4. dimenzióban. Legyen adott egy k dimenziós $L \subset \mathbb{R}^n$ rács. A következő bizonyítás alapgondolata a 3.4. állításon alapszik. Abból látszik, hogy ha adottak $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k \in L$ lineárisan független rácsvektorok és egy $\mathbf{b} \in L$ tetszőleges rácspont, akkor amennyiben $\mathbf{b}$ nem áll elő mint a $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ vektorok egész együtthatós lineáris kombinációja, akkor létezik egy $\mathbf{r}$ nem $\mathbf{0}$ rácspont, amely a $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ vektorok gyenge redukciós tartományába esik.

Mivel a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok lineárisan függetlenek, így a $\mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ gyenge redukciós tartomány $[L]$ altérbe eső része egy k dimenziós téglatest. A 3.2. állítás következtében $1 < k \leq 3$ esetén $\mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ szükségszerűen a $\|\mathbf{b}_m\|$ sugarú gömb belsejébe esik, ahol $0 < m \leq k$ olyan index, amire $\mathbf{b}_m$ maximális hosszúságú. Ezek szerint, ha egy $\mathbf{b}$ vektor nem áll elő, mint $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ egész együtthatós lineáris kombinációja, akkor léteznie kell egy $\mathbf{b}_m$-nél rövidebb rácsvektornak a $\mathrm{B}(\|\mathbf{b}_m\|)$ gömb belsejében. Ezen ötleteket felhasználva már be tudjuk bizonyítani a következő állítást:

3.6. Állítás. *Legyen $L \subset \mathbb{R}^n$ egy k dimenziós rács.*

- *$1 \leq k \leq 3$ esetén, ha az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független pontjai teljesítik (3.1)-et, akkor ezek bázist alkotnak.*
- *$k = 4$ esetén előfordulhat, hogy az L rács $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ linárisan független vektorai teljesítik (3.1)-et, viszont nem alkotják a rács bázisát.*
- *$k \geq 5$ esetén az is előfordulhat, hogy az L rácsnak nem létezik olyan bázisa, amely (3.1)-et teljesítené.*

Bizonyítás. Az $1 \leq k \leq 3$ esetet k szerinti indukcióval fogjuk belátni.

Az $k = 1$ eset triviális.

Nézzük a $2 \leq k \leq 3$ esetet. Indirekt tegyük fel, hogy létezik egy $\mathbf{b} \in L$ rácspont, amely nem áll elő mint $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ egész együtthatós lineáris kombinációja. Ekkor a 3.4. állítás szerint létezik egy nem $\mathbf{0}$ rácspont a $\mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ gyenge redukciós tartomány $[L]$ altérbe eső részében. Hívjuk ezt a rácspontot $\mathbf{b}'$-nek.

A 3.2. állítás miatt $\mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \cap [L]$ a $\mathrm{B}_k(\|\mathbf{b}_k\|)$ gömb belsejében van, így

$$\|\mathbf{b}'\| < \|\mathbf{b}_k\|.$$

Tegyük fel, hogy $\mathbf{b}'$ és $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}$ lineárisan függetlenek. Legyen m minimális index, amire $\|\mathbf{b}'\| < \|\mathbf{b}_m\|$. Ekkor, mivel $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-1}$ és $\mathbf{b}'$ is linárisan függetlenek, így az m. szukcesszív minimum definíciója szerint ellentmondásra jutottunk.

Ha $\mathbf{b}'$ és $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}$ lineárisan összefüggőek, akkor az indukciós feltevés szerint $\mathbf{b}'$ előáll mint $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{k-1}$ egész együtthatós lineáris kombinációja, ami pedig az indirekt feltevésnek mond ellent.

Most vizsgáljuk a $k = 4$ esetet. Az egyszerűség kedvéért tegyük fel, hogy $L \subset \mathbb{R}^4$. Ahhoz, hogy az előbbi érvelés ne működjön, szeretnénk venni úgy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_4$ független vektorokat, hogy $\mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_4)$ ne essen teljes egészében $B_4(\|\mathbf{b}_m\|)$ gömb belsejébe, ahol $\mathbf{b}_m$ maximális hosszúságú a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_4$ vektorok közül. Ez csakis akkor teljesül, ha $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_4$ egymásra merőleges azonos hosszúságú vektorok. Legyenek például

$$\begin{aligned}
\mathbf{b}_1 &= (1,0,0,0) \\
\mathbf{b}_2 &= (0,1,0,0) \\
\mathbf{b}_3 &= (0,0,1,0) \\
\mathbf{b}_4 &= (0,0,0,1).
\end{aligned}$$

Ha ezek nem alkotják rácsunk bázisát, akkor a többi rácspont csakis $\mathrm{GY}(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_4)$ csúcsainak $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_4$ egész együtthatós lineáris kombinációival való eltoltjai lehetnek, ugyanis ezek az olyan $\mathbf{b}$ rácspontok, amelyekből a $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_4$ megfelelő egész együtthatós lineáris kombinációját kivonva nem tudunk olyan rácspontot kapni, amely a $\mathrm{B}(1)$ gömbbe esne.

A $\mathrm{GY}(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_4)$ 4 dimenziós kocka csúcsai

$$h = (\pm 1/2, \pm 1/2, \pm 1/2, \pm 1/2)$$

alakúak. Legyen rácsunk az ezen csúcsok által generált rács, amit jelöljünk a következő módon:

$$D_4 := L(\{1/2,-1/2\}^4). \tag{3.8}$$

Nyilván $\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4 \in D_4$, továbbá

$$1 = \|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\| = \|\mathbf{b}_4\| = \lambda_1(D_4) = \lambda_2(D_4) = \lambda_3(D_4) = \lambda_4(D_4),$$

viszont a $\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4$ vektorok nem alkotják D_4 bázisát.

A $k > 4$ eset kijön az $k = 4$ esethez hasonlóan. Az egyszerűség kedvéért most is tegyük fel, hogy $L \subset \mathbb{R}^k$. Legyen

$$D_k := L(\{1/2,-1/2\}^k) \tag{3.9}$$

a k dimenziós 1 élhosszúságú origó súlypontú kocka csúcsai által generált rács. Ekkor könnyen meggondolható, hogy

$$\begin{aligned}
\mathbf{b}_1 &= (1,0,0,\ldots,0)\\
\mathbf{b}_2 &= (0,1,0,\ldots,0)\\
\mathbf{b}_3 &= (0,0,1,\ldots,0)\\
&\ldots\\
\mathbf{b}_k &= (0,0,0,\ldots,1).
\end{aligned}$$

választással $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k \in D_k$ lineárisan független vektorok, amelyekre

$$1 = \|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \ldots = \|\mathbf{b}_k\| = \lambda_1(D_k) = \lambda_2(D_k) = \ldots = \lambda_k(D_k)$$

teljesül, viszont a $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k$ lineárisan független rácspontok nem alkotják D_k bázisát, sőt D_k-nek nincs olyan bázisa, ahol minden vektor hossza pont 1 volna. □

Ezzel azt is megmutattuk, hogy az első 3 dimenzióban minden rácsnak létezik olyan bázisa, amely vektorainak hosszai megegyeznek a rács szukcesszív minimumaival. Az is kiderült, hogy ez az 5. dimenziótól kezdve nem igaz.

Mi a helyzet a 4. dimenzióban? A válasz az, hogy minden 4 dimenziós rácsnak is található olyan bázisa, mely vektorainak hosszai a rács szukcesszív minimumai. A fejezet hátralévő részében bemutatjuk a Lagrange-Gauss algoritmus egy általánosítását és ezen algoritmus segítségével meghatározzuk δ_k értékét (lásd 2.2.12.) $1 \le k \le 4$ esetén.

3.7. Állítás. *A $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_k \in \mathbb{R}^k$ lineárisan független vektorok pontosan akkor gyengén redukáltak (lásd 2.4. definíció), ha minden $1 < i \le k$ index esetén*

$$\mathbf{b}_i \in \mathrm{GY}(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_{i-1}).$$

Bizonyítás. Az állítás azonnal következik a definíciókból. □

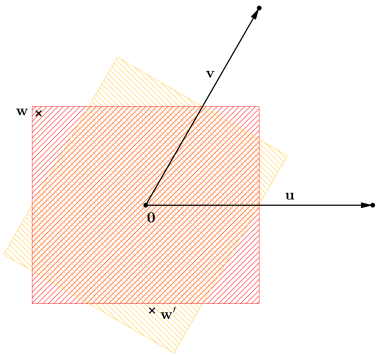
A gyenge redukáltságra gondolhatunk úgy, mint a Gram-Schmidt ortogonalizált egy diszkrét megfelelőjére. Van azonban egy lényeges eltérés a kettő között. Adott $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorok esetén a $\mathbf{b}_i$ vektor $\mathbf{b}_i^*$ komponense nem függ az előtte levő $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}$ vektorok sorrendjétől, a $\mathbf{b}_i$ vektor $\mathbf{b}_i'$ gyengén redukáltját viszont már az előtte levő vektorok sorrendje is befolyásolhatja. Ezt jól illusztrálja a következő példa. Legyenek adottak a tér

$$\mathbf{u} = (1,0,0)$$
$$\mathbf{v} = (1/2, \sqrt{3}/2, 0)$$

vektorai. Ezek jelen esetben az (2.2.4)-nél meghatározott A_2 rácsot feszítik ki a tér x és y tengelyei által meghatározott síkjában. Ezen vektorok gyenge redukciós tartománya nyilván függ a sorrendjüktől (lásd 3.2. ábra). Vegyünk most egy harmadik az $\mathbf{u}$ és $\mathbf{v}$ vektoroktól lineárisan független $\mathbf{w}$ vektort. Legyen például

$$\mathbf{w} = (-1/2 + \varepsilon, \sqrt{3}/2 - \varepsilon, 1).$$

Ahogy ez az 3.2. ábrából látszik, ha ε elég kicsi akkor az $\mathbf{u}, \mathbf{v}, \mathbf{w}$ bázis gyengén redukált, viszont a $\mathbf{v}, \mathbf{u}, \mathbf{w}$ nem az. Legyen $\mathbf{w}' = \mathbf{w} + \mathbf{u} - \mathbf{v}$ a $\mathbf{w}$ vektor gyengén redukáltja a $\mathbf{v}, \mathbf{u}$ vektorok szerint. Ekkor $\|\mathbf{w}\| \to \sqrt{2}$ és $\|\mathbf{w}'\| \to 1$ ahogy $\varepsilon \to 0$, tehát elég kicsi ε esetén $\|\mathbf{w}\| > \|\mathbf{w}'\|$.



3.2. ábra. $\mathbf{u}, \mathbf{v}$ vektorok gyenge redukciós tartományai, valamint a $\mathbf{w}$ és $\mathbf{w}'$ vektorok fölülnézetből.

Az $\mathbf{u}, \mathbf{v}, \mathbf{w}$ és a $\mathbf{v}, \mathbf{u}, \mathbf{w}'$ vektorok egy-egy gyengén redukált bázisát alkotják a $L(\mathbf{u}, \mathbf{v}, \mathbf{w})$ rácsnak. Ezek közül a $\mathbf{v}, \mathbf{u}, \mathbf{w}'$ ortogonalitási defektusa a kisebb.

Legyen most adott egy n dimenziós L rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ bázisa. Adjuk meg a redukáltság egy olyan fogalmát, amely kizárja, hogy $i > 1$ esetén a $\mathbf{b}_i$ rácsvektort egy

$$\mathbf{b}_i' \in [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}] + \mathbf{b}_i$$

rácsvektorra kicserélve a rácsunk egy kisebb ortogonalitási defektusú bázisát kapjunk.

3.8. Definició. Azt mondjuk, hogy a $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k \in \mathbb{R}^n$ lineárisan független vektorok *erősen redukáltak*, ha tetszőleges $1 < i \leq k$ index és $s_1, s_2, \ldots, s_{i-1} \in \mathbb{Z}$ egész számok esetén

$$\|\mathbf{r}_i\| \leq \|\mathbf{r}_i - s_1\mathbf{r}_1 - s_2\mathbf{r}_2 - \ldots - s_{i-1}\mathbf{r}_{i-1}\|$$

Ha egy rács bázisának vektorai erősen redukáltak, akkor azt mondjuk, hogy a bázis *erősen redukált*.

Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ linárisan független vektorok. Vegyük észre, hogy ekkor léteznek olyan $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k$ erősen redukált vektorok, hogy

$$\mathbf{r}_i = \mathbf{b}_i - s_{i,1}\mathbf{b}_1 - s_{i,2}\mathbf{b}_2 - \ldots - s_{i,i-1}\mathbf{b}_{i-1}$$

ahol az $s_{i,j}$ értékek egész számok. Ezen $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k$ vektorokat a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorokhoz tartozó *erősen redukált vektoroknak* hívjuk. Ekkor az $\mathbf{r}_i$ vektort a $\mathbf{b}_i$ vektor *erősen redukáltjának* nevezzük.

Amennyiben adott egy n dimenziós L rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ bázisa, akkor az ezen vektorokhoz tartozó erősen redukált vektorokat a bázis *erős redukáltjának* hívjuk.

Adott $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorokhoz a hozzájuk tartozó erősen redukált vektorok k darab CVP megoldásával kaphatóak meg. Ennek részleteit most nem írjuk le, viszont a fejezet céljaihoz szükséges, hogy bevezessünk egy jelölést az ezeket megtaláló algoritmusra:

$$\texttt{erős\_redukció}\,(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \tag{3.10}$$

Ez annyit jelent, hogy kicseréljük a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorokat az ő erősen redukáltjukra.

Hasonlóan a gyenge redukciós tartomány fogalmához most is be tudjuk vezetni az erős redukciós tartomány fogalmát:

3.9. Definició. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. A

$$\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) := \{\mathbf{x} \in \mathbb{R}^n \mid \forall s_1, s_2, \ldots, s_k \in \mathbb{Z}\colon \|\mathbf{x}\| \leq \|\mathbf{x} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k\|\}$$

halmazt a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok *erős redukciós tartományának* hívjuk. Könnyen meggondolható, hogy tetszőleges $\mathbf{b} \in \mathbb{R}^n$ esetén léteznek $s_1, s_2, \ldots, s_k$ egész számok, hogy

$$\mathbf{r} = \mathbf{b} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k).$$

Ekkor az $\mathbf{r}$ vektort a $\mathbf{b}$ vektor $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ szerinti *erős redukáltjának* hívjuk.

Mielőtt továbbmennénk, bevezetünk néhány jelölést az eddig leírt redukciós tartományok bizonyos részeinek jelölésére. Ez arra szolgál, hogy a továbbiakban könnyebben tudunk majd beszélni ezen tartományokról.

3.10. Definició (Redukciós tartományok részei)**.** Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Legyen ezen vektorok erős/gyenge redukciós tartománya T. A

$$T_a = T \cap [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k]$$

halmazt a gyenge/erős redukciós tartomány *alapjának* hívjuk és erős redukciós tartomány esetén $\mathrm{E}_a(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$-val, gyenge redukciós tartomány esetén pedig $\mathrm{GY}_a(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$-val jelöljük. A

$$T_t = T \setminus T_a$$

halmazt a gyenge/erős redukciós tartomány *testének* nevezzük, és erős redukciós tartomány esetén $\mathrm{E}_t(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$-val, míg gyenge redukciós tartomány esetén $\mathrm{GY}_t(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$-val jelöljük.

3.11. Állítás. *Legyenek adottak a* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ *lineárisan független vektorok. Legyen L az általuk generált k dimenziós rács.*

Ekkor

$$\mathrm{E}_a(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) = \mathrm{vor}\, L,$$

ahol vor*L, az L rács Voronoi cellája (lásd 1.7. definíció).*

Bizonyítás. Az állítás azonnal következik $\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ definíciójából, ugyanis

$$\begin{gathered}\forall s_1, s_2, \ldots, s_k \in \mathbb{Z}\colon \|\mathbf{x}\| \leq \|\mathbf{x} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k\| \\ \Leftrightarrow \\ \forall \mathbf{b} \in L\colon \mathrm{d}(\mathbf{x}, \mathbf{0}) \leq \mathrm{d}(\mathbf{x}, \mathbf{b}).\end{gathered}$$

□

Az erős redukáltságot redukciós tartományok segítségével a következő módon fogalmazhatjuk át:

3.12. Állítás. *Az* $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_k \in \mathbb{R}^n$ *vektorok pontosan akkor erősen redukáltak ha tetszőleges i index esetén*

$$\mathbf{r}_i \in \mathrm{E}(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{i-1}).$$

A térben már adtunk arra példát, hogy egy bázis gyengén redukált, viszont nem erősen redukált (lásd 3.2. ábra), és persze ez tetszőleges magasabb dimenzióban is igaz. A síkon ennél sokkal kedvezőbb a helyzet.

3.13. Állítás. *Legyenek* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$ *lineárisan független vektorok. Ekkor*

$$\mathbf{u}, \mathbf{v} \textit{ gyengén redukáltak } \Leftrightarrow \mathbf{u}, \mathbf{v} \textit{ erősen redukáltak .}$$

Bizonyítás. A bizonyításhoz elég meggondolni, hogy

$$\mathrm{E}(\mathbf{u}) = \mathrm{GY}(\mathbf{u}) = \{x\mathbf{u} + y\mathbf{v}^* \mid x, y \in \mathbb{R},\ |x| \leq 1/2\},$$

ami azonnal következik $\mathrm{E}(\mathbf{u})$ és $\mathrm{GY}(\mathbf{u})$ definíciójából. □

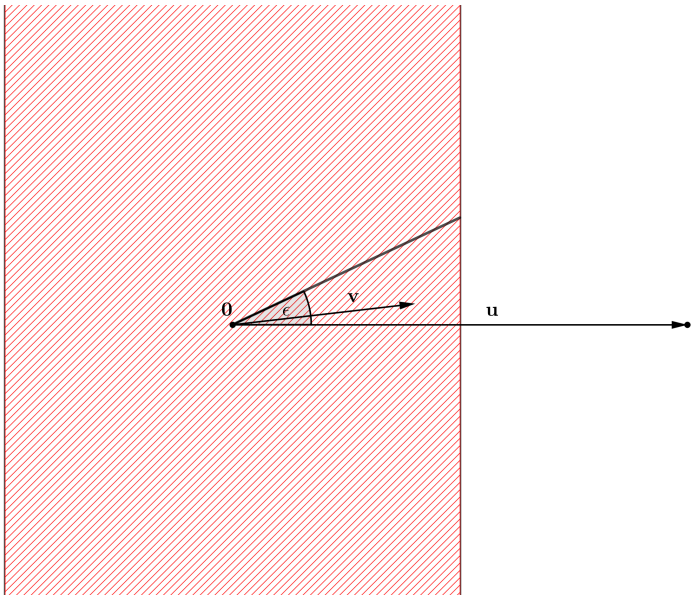
A redukáltság ezen fogalmai önmagukban még nem túl erősek. Ennek szemléltetésére vegyük a sík egy $\mathbf{u}$ vektorát. Ha $\mathbf{v} \in \mathrm{GY}(\mathbf{u})$, továbbá $\mathbf{u}$ és $\mathbf{v}$ lineárisan függetlenek, akkor az $\mathbf{u}, \mathbf{v}$ vektorok gyengén (és erősen) redukáltak. Ha az $\mathbf{u}$ által kifeszített egyenes és $\mathbf{v}$ által bezárt szög α, akkor (2.2.2) szerint

$$\delta(\mathbf{u}, \mathbf{v}) = 1/\sin\alpha.$$

Vegyük észre, hogy tetszőleges $\varepsilon > 0$ valós szám esetén, $\mathbf{v}$ megválasztható úgy $\mathrm{GY}(\mathbf{u})$-ból, hogy $0 < \alpha < \varepsilon$ teljesüljön. (lásd 3.3. ábra)

Ezek szerint gyengén vagy erősen redukált rácsbázis tetszőlegesen nagy ortogonalitási defektusú lehet.

A Lagrange-Gauss redukáltság úgy küszöböli ki a problémát, hogy a gyenge/erős redukáltság mellett veszi az $\|\mathbf{u}\| \leq \|\mathbf{v}\|$ extra feltételt. Ahhoz, hogy ez adott $\mathbf{u}$ esetén teljesüljön, a $\mathbf{v}$ vektort



3.3. ábra. Erősen/gyengén redukált bázis ortogonalitási defektusa tetszőlegesen nagy lehet.

a 2.1. ábrán látható tartományból lehet megválasztani. Az ortogonalitási defektus a maximumát minimális $\alpha > 0$ szög esetén veszi fel, ami ebben az esetben 60°.

Végül azt kaptuk, hogy $\mathbf{v} \in \mathrm{E}(\mathbf{u})$ és $\|\mathbf{u}\| \leq \|\mathbf{v}\|$ esetén

$$\delta(\mathbf{u},\mathbf{v}) \leq 1/\sin 60^\circ = 2/\sqrt{3}. \tag{3.11}$$

Mint korábban láthattuk, a Lagrange-Gauss algoritmus segítségével ilyen bázis mindig található, és ahogy azt (2.2.5)-nél megfigyeltük, $\delta(A_2) = 2/\sqrt{3}$. Ezek szerint

$$\delta_2 = 2/\sqrt{3}.$$

Vajon működik ugyanez magasabb dimenzióban? Próbáljuk meg! Általánosítsuk a Lagrange-Gauss redukáltság fogalmát a következő módon:

3.14. Definició. Azt mondjuk, hogy a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok *Lagrange-Gauss* redukáltak, vagy röviden *LG redukáltak*, ha erősen redukáltak és

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_k\|.$$

Ilyen vektorokat könnyen találhatunk az 3.1. algoritmus segítségével.

Itt `rendez(`$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$`)` annyit csinál, hogy hossz szerint növekvő sorrendbe rendezi a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorokat. Világos, hogy az 3.1. algoritmus leálláskor LG redukált bázist ad vissza. Mivel `erős_redukció(`$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$`)` az utolsó iteráció kivételével, minden iterációban csökkenti legalább egy vektor hosszát, növelni pedig biztosan nem növeli semelyik vektor hosszát sem, így az algoritmus biztosan véges sok iteráció alatt leáll, ugyanis a $\mathrm{B}(\|\mathbf{b}_m\|)$ gömbben csak véges sok vektor lehet, ahol m olyan index amire $\mathbf{b}_m$ maximális hosszúságú.

3.1. Algoritmus Lagrange-Gauss Algoritmus

Be: $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ lineárisan független vektorok.
Ki: $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ LG redukált vektorok.
Név: `LG_redukció`$(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$

1: **Ciklus**
2: `rendez`$(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
3: `erős_redukció`$(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$
4: **Ciklus amíg** $\exists i$: $\|\mathbf{b}_{i-1}\| > \|\mathbf{b}_i\|$ **vége**

3.15. Definició. Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Legyen T ezen vektorok erős/gyenge redukciós tartománya, T_a pedig ennek az alapja. (lásd 3.10. definíció) A

$$\mathrm{rad}(T_a)$$

valós számot (lásd 1.2.19. definíció), a T gyenge/erős redukciós tartomány *sugarának* hívjuk.

3.16. Állítás. *Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Az ezek által meghatározott gyenge redukciós tartomány r_{gy} sugarának hosszára a*

$$r_{gy} \leq \frac{\sqrt{k}}{2}\|\mathbf{b}_m\|$$

felső becslés adható. Amennyiben a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok azonos hosszúságúak és egymásra merőlegesek, akkor az egyenlőtlenség egyenlőséggel teljesül.

Bizonyítás. A gyenge redukciós tartomány r_{gy} sugara könnyen meghatározható a $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$ Gram-Schmidt ortogonalizált vektorok segítségével:

$$r_{gy} = \left\| \frac{1}{2}\mathbf{b}_1^* + \frac{1}{2}\mathbf{b}_2^* + \ldots + \frac{1}{2}\mathbf{b}_k^* \right\|.$$

Ezek szerint

$$r_{gy}^2 = \frac{1}{4}(\|\mathbf{b}_1^*\|^2 + \|\mathbf{b}_2^*\|^2 + \ldots + \|\mathbf{b}_k^*\|^2) \leq \frac{k}{4}\|\mathbf{b}_m\|^2, \tag{3.12}$$

amiből rögtön az állítást első felét kapjuk. Azonos hosszúságú egymásra merőleges vektorok esetén tetszőleges i indexre $\mathbf{b}_i^* = \mathbf{b}_i$, így ekkor (3.12)-ben az egyenlőtlenség egyenlőséggel teljesül, tehát az állítás második felét is megkaptuk. □

3.17. Állítás. *Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Legyen ezek gyenge redukciós tartományának sugara r_{gy}, erős redukciós tartományának sugara pedig r_e. Ekkor*

$$r_e \leq r_{gy}.$$

Ortogonális vektorok esetén az egyenlőtlenség egyenlőséggel teljesül.

Bizonyítás. Tegyük fel indirekt, hogy $r_e > r_{gy}$. Legyen $\mathbf{b} \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$ olyan, hogy $\|\mathrm{proj}_k(\mathbf{b})\| = r_e$. Legyen a $\mathbf{b}'$ vektor a $\mathbf{b}$ vektor $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok szerinti gyenge redukáltja. Ekkor

$\mathbf{b}' \in \mathrm{GY}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$, tehát $\|\mathbf{b}'\| \leq r_{gy} < r_e = \|\mathbf{b}\|$. Ekkor ellentmondásra jutottunk, ugyanis léteznek $s_1, s_2, \ldots, s_k \in \mathbb{Z}$, hogy

$$\|\mathbf{b} - s_1\mathbf{b}_1 - s_2\mathbf{b}_2 - \ldots - s_k\mathbf{b}_k\| = \|\mathbf{b}'\| < \|\mathbf{b}\|$$

teljesül viszont ekkor $\mathbf{b} \notin \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k)$. □

Ez megindokolja az *erős* redukciós tartomány elnevezést. Ezen állítások alapján azonnal a következő tételt kapjuk:

3.18. Tétel (Az erős redukciós tartomány sugarának triviális felső becslése)**.** *Legyenek adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ lineárisan független vektorok. Legyen ezek erős redukciós tartományának sugara r_e, és legyen m olyan index amire $\mathbf{b}_m$ maximális hosszúságú. Ekkor*

$$r_e \leq \frac{\sqrt{k}}{2}\|\mathbf{b}_m\|,$$

ahol azonos hosszúságú egymásra merőleges $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ vektorok esetén az egyenlőtlenség egyenlőséggel teljesül.

Most már megvizsgálhatjuk, hogy mikor jó a Lagrange-Gauss redukáltság. Legyen adott egy k dimenziós L rács egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ LG-redukált bázisa. A 3.4. ábrán látható, hogy az LG-redukáltsággal mit érünk el: először is tetszőleges i index esetén $\mathbf{b}_i \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1})$-nek kell teljesülnie, és ezek szerint $\|\mathrm{proj}_{i-1}(\mathbf{b}_i)\| \leq r_{i-1}$, ahol r_{i-1} az $\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1})$ erős redukciós tartomány sugara.

Amennyiben $r_{i-1} < \|\mathbf{b}_{i-1}\|$ akkor a $\|\mathbf{b}_{i-1}\| \leq \|\mathbf{b}_i\|$ feltétel miatt a $\mathbf{b}_i$ vektor a 3.4. ábrán látható tartományba kényszerül. Ezen gondolatokat felhasználva a következő tétel adódik:

3.19. Tétel. *Legyen adott egy k dimenziós L rács, és ennek egy $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ LG redukált bázisa. Jelölje r_i az első i bázisvektor $\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i)$ erős redukciós tartományának sugarát. Tegyük fel, hogy $r_i < \|\mathbf{b}_i\|$ ekkor*

$$\frac{\|\mathbf{b}_{i+1}\|}{\|\mathbf{b}^*_{i+1}\|} \leq \frac{1}{\sqrt{1 - r_i^2/\|\mathbf{b}_i\|^2}},$$

ahol az egyenlőtlenség éles.

Amennyiben $r_i \geq \|\mathbf{b}_i\|$ akkor $\|\mathbf{b}_{i+1}\|/\|\mathbf{b}^*_{i+1}\|$ értéke tetszőlegesen nagy lehet.

Bizonyítás. Először vizsgáljuk a $r_i < \|\mathbf{b}_{i+1}\|$ esetet. Mivel a bázisunk LG redukált így

$$\mathbf{b}_{i+1} \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i).$$

(2.2.2)-nél láthattuk, hogy $\|\mathbf{b}_{i+1}\|/\|\mathbf{b}^*_{i+1}\| = 1/\sin\alpha_i$, ahol α_{i+1} a $\mathbf{b}_{i+1}$ vektor és $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i]$ altér által bezárt szög. Ezek szerint

$$\frac{\|\mathbf{b}_{i+1}\|}{\|\mathbf{b}^*_{i+1}\|} = \frac{1}{\sin\alpha_{i+1}} = \frac{1}{\sqrt{1-\cos^2\alpha_{i+1}}} = \frac{1}{\sqrt{1 - \|\mathrm{proj}_i(\mathbf{b}_{i+1})\|^2/\|\mathbf{b}_{i+1}\|^2}} \leq \frac{1}{\sqrt{1 - r_i^2/\|\mathbf{b}_i\|^2}}. \tag{3.13}$$

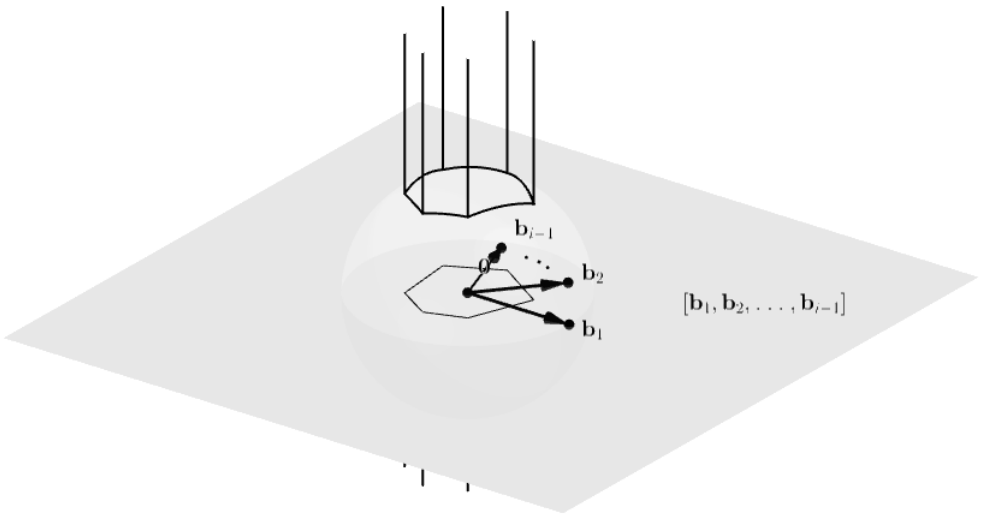
Amennyiben $\|\mathrm{proj}_i(\mathbf{b}_{i+1})\| = r_i$ és $\|\mathbf{b}_i\| = \|\mathbf{b}_{i+1}\|$ akkor az egyenlőtlenség egyenlőséggel teljesül.

Most vizsgáljuk meg, hogy mi a helyzet abban az esetben amikor $r_i \geq \|\mathbf{b}_i\|$. Tegyük fel, hogy adottak a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i \in \mathbb{R}^n$ LG redukált vektorok ($i < n$), és az ő erős redukciós tartományuk r_i sugarára $r_i \geq \|\mathbf{b}_i\|$ teljesül. Legyen $\mathbf{b}^*$ olyan 1 hosszú vektor amely merőleges a $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i]$ altérre, és legyen $\mathbf{b} \in \mathrm{E}_a(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i)$ olyan, hogy $\|\mathbf{b}\| = r_i$.

Legyen $\varepsilon > 0$ valós szám, és $\mathbf{b}_{i+1} = \mathbf{b} + \varepsilon \mathbf{b}^*$. Nyilván $\mathbf{b}_{i+1} \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i)$, és mivel $\|\mathbf{b}_i\| \leq r_i$ így $\|\mathbf{b}_i\| < \|\mathbf{b}_{i+1}\|$, tehát a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i+1}$ vektorok LG redukáltak. Mivel

$$\frac{\|\mathbf{b}_{i+1}\|^2}{\|\mathbf{b}_{i+1}^*\|^2} = \frac{\|\mathbf{b}\|^2 + \varepsilon^2 \|\mathbf{b}^*\|^2}{\varepsilon^2 \|\mathbf{b}^*\|^2} = \frac{\|\mathbf{b}\|^2}{\varepsilon^2} + 1,$$

így ε értékét elég kicsinek választva $\|\mathbf{b}_{i+1}\| / \|\mathbf{b}_{i+1}^*\|$ értéke tetszőlegesen nagy lehet. Ezzel az állítást beláttuk. □



3.4. ábra. Az LG redukáltság tartománya az első $i-1$ bázisvektor szerint a $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i]$ altérben.

Első 4 dimenzióban ezt felhasználhatjuk a következő tétel bizonyítására:

3.20. Tétel. *Legyen L egy k dimenziós rács, és $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ ennek egy bázisa. $1 \leq k \leq 4$ esetén a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis pontosan akkor LG redukált, ha*

$$\|\mathbf{b}_1\| = \lambda_1(L),\ \|\mathbf{b}_2\| = \lambda_2(L),\ \ldots\ \|\mathbf{b}_k\| = \lambda_k(L)$$

teljesül.

Bizonyítás. ($\Rightarrow$) Tegyük fel, hogy a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$ bázis LG redukált. Legyen a bázis Gram-Schmidt ortogonalizáltja $\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*$. Jelölje r_i a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i$ vektorok erős redukciós tartományának sugarát ($1 \leq i \leq k$). Ekkor a 3.18. és 3.19. tételek szerint

$$\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|} \leq \frac{1}{\sqrt{1 - r_{i-1}^2 / \|\mathbf{b}_{i-1}\|^2}} \leq \frac{1}{\sqrt{1 - (i-1)/4}} \leq 2$$

tehát

$$\|\mathbf{b}_i\| \leq 2\|\mathbf{b}_i^*\|. \tag{3.14}$$

Legyen $1 < i \leq k$ index. Legyenek $s_1, s_2, \ldots, s_i$ egész számok úgy, hogy $s_i \neq 0$. Ha $s_i = \pm 1$ akkor az erős redukáltság miatt, ha pedig $1 < |s_i|$ akkor (3.14) miatt

$$\|\mathbf{b}_i\| \leq \|s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \ldots + s_i\mathbf{b}_i\|.$$

Ezek szerint az összes $\mathbf{b}_i$ vektornál rövidebb rácsvektor a $[\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}]$ altérbe esik, így $\|\mathbf{b}_1\|$, $\|\mathbf{b}_2\|$, … $\|\mathbf{b}_k\|$ tényleg a szukcesszív minimumok.

($\Leftarrow$) Tegyük fel, hogy

$$\|\mathbf{b}_1\| = \lambda_1(L),\ \|\mathbf{b}_2\| = \lambda_2(L),\ \ldots\ \|\mathbf{b}_n\| = \lambda_n(L).$$

Ekkor $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_n\|$.

Feltételezzük indirekt, hogy a bázis nem LG redukált. Ekkor a bázis nem lehet erősen redukált, így létezik olyan i index, hogy $\|\mathbf{b}_i\| > \|\mathbf{r}_i\|$ ahol $\mathbf{r}_i$ a $\mathbf{b}_i$ vektor erősen redukáltja. Legyen m minimális index amire $\|\mathbf{b}_m\| > \|\mathbf{r}_i\|$. Ekkor a

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{m-1}, \mathbf{r}_i$$

vektorok lineárisan függetlenek, továbbá $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_{m-1}\| \leq \|\mathbf{r}_i\|$, tehát az m. szukcesszív minimum definíciója szerint $\lambda_m(L) \leq \|\mathbf{r}_i\| < \|\mathbf{b}_m\|$. Így ellentmondásra jutottunk. □

Ez és a 3.1. állítás alapján láthatjuk, hogy az 3.1. algoritmus az első 4 dimenzióban megtalálja egy rács azon bázisát, amely ortogonalitási defektusa minimális. Reális elvárás, hogy az algoritmus elvezessen minket a δ_3 és δ_4 értékek meghatározásához.

Legyenek $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-1}$ a szokásos ortonormált bázis első $n-1$ vektora $\mathbb{R}^n$-ben, azaz legyen

$$\begin{aligned}
\mathbf{b}_1 &= (1,0,0,\ldots,0,0)\\
\mathbf{b}_2 &= (0,1,0,\ldots,0,0)\\
&\ldots\\
\mathbf{b}_{n-1} &= (0,0,0,\ldots,1,0).
\end{aligned}$$

Ezek nyilván LG redukáltak. Válasszuk meg ezekhez most a $\mathbf{b}_n \in \mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-1})$ vektort úgy, hogy a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ olyan LG redukált bázis legyen, amely ortogonalitási defektusa a lehető legnagyobb. Ez a 3.19. tétel szerint csak $n \leq 4$ esetén tehető meg, ugyanis, különben az $\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-1})$ erős redukciós tartomány r_e sugara nagyobb lenne mint 1, tehát ekkor $\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \|\mathbf{b}_n\|/\|\mathbf{b}_n^*\|$ értéke tetszőlegesen nagy lehet.

Amennyiben $n \leq 4$, akkor válasszuk meg a $\mathbf{b}_n$ vektort úgy, hogy $\|\mathrm{proj}_{n-1}(\mathbf{b}_n)\| = r_e$ és $\|\mathbf{b}_{n-1}\| = \|\mathbf{b}_n\|$ teljesüljön. Az így kapott $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ vektorok által genertált rácsot jelölje L. Ekkor a 3.18. és 3.18. tételek szerint

$$\delta(L) = \delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \frac{\|\mathbf{b}_n\|}{\|\mathbf{b}_n^*\|} = \frac{1}{\sqrt{1 - r_e^2/\|\mathbf{b}_{n-1}\|^2}} = \frac{1}{\sqrt{1-(n-1)/4}}.$$

$n = 2$ esetén L a korábban (2.2.4)-nél definiált A_2 rács, és ahogy azt már korábban is láttuk, ekkor

$$\delta(L) = \delta(\mathbf{b}_1, \mathbf{b}_2) = \frac{2}{\sqrt{3}}. \tag{3.15}$$

$n = 3$ esetén

$$\delta(L) = \delta(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) = \sqrt{2}, \tag{3.16}$$

$n = 4$ esetén pedig

$$\delta(L) = \delta(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4) = 2. \tag{3.17}$$

Mint azt hamarosan látni fogjuk, ezek az értékek rendre a $\delta_2, \delta_3, \delta_4$ konstansok.

Ahhoz, hogy ezt megmutassuk, először a 3.18. tétel felső becslésénél egy jobb becslést adunk a 2 és 3 dimenziós rácsok erős redukciós tartományának sugarára. Ehhez először jobban megismerkedünk az ilyen rácsok Voronoi cellájával.

3.21. Tétel. *Legyen adott egy 2 dimenziós $L \subset \mathbb{R}^n$ rács. Legyen $\mathbf{u}, \mathbf{v}$ ennek egy LG-redukált bázisa. Ekkor a rács Voronoi-releváns vektorait a következő módon adhatjuk meg:*

1. *Ha $\mathbf{u}$ és $\mathbf{v}$ merőlegesek egymásra, akkor a rács Voronoi-releváns vektorai*

$$\pm\mathbf{u},\ \pm\mathbf{v}.$$

2. *Ha $\arg(\mathbf{u}, \mathbf{v}) \in [\pi/3, \pi/2[$, akkor a rács Voronoi-releváns vektorai*

$$\pm\mathbf{u},\ \pm\mathbf{v},\ \mathbf{v}-\mathbf{u},\ \mathbf{u}-\mathbf{v}.$$

3. *Ha $\arg(\mathbf{u}, \mathbf{v}) \in]\pi/2, 2\pi/3]$, akkor a rács Voronoi-releváns vektorai*

$$\pm\mathbf{u},\ \pm\mathbf{v},\ -\mathbf{v}-\mathbf{u},\ \mathbf{u}+\mathbf{v}.$$

Bizonyítás. Az első eset nyilvánvaló, a 3. eset pedig azonnal következik a 2. esetből, ugyanis, ekkor $\mathbf{u}, -\mathbf{v}$ is egy LG-redukált bázisa az L rácsnak, és $\arg(\mathbf{u}, -\mathbf{v}) \in [\pi/3, \pi/2[$.

Vizsgáljuk tehát a 2. esetet. Korábban (1.4.5)-nél láttuk, hogy

$$\operatorname{vor} L = \bigcap_{\mathbf{b} \in L \setminus \{\mathbf{0}\}} \{\mathbf{v} \in [L] \mid \mathbf{v} \cdot \mathbf{b} \leq \mathbf{b}^2/2\},$$

azaz a L rács előáll

$$\{\mathbf{v} \in [L] \mid \mathbf{v} \cdot \mathbf{b} \leq \mathbf{b}^2/2\}$$

alakú félsíkok metszeteként, ahol $\mathbf{b}$ rácspont. Amit be szeretnénk látni, hogy $\operatorname{vor} L$ pontosan az

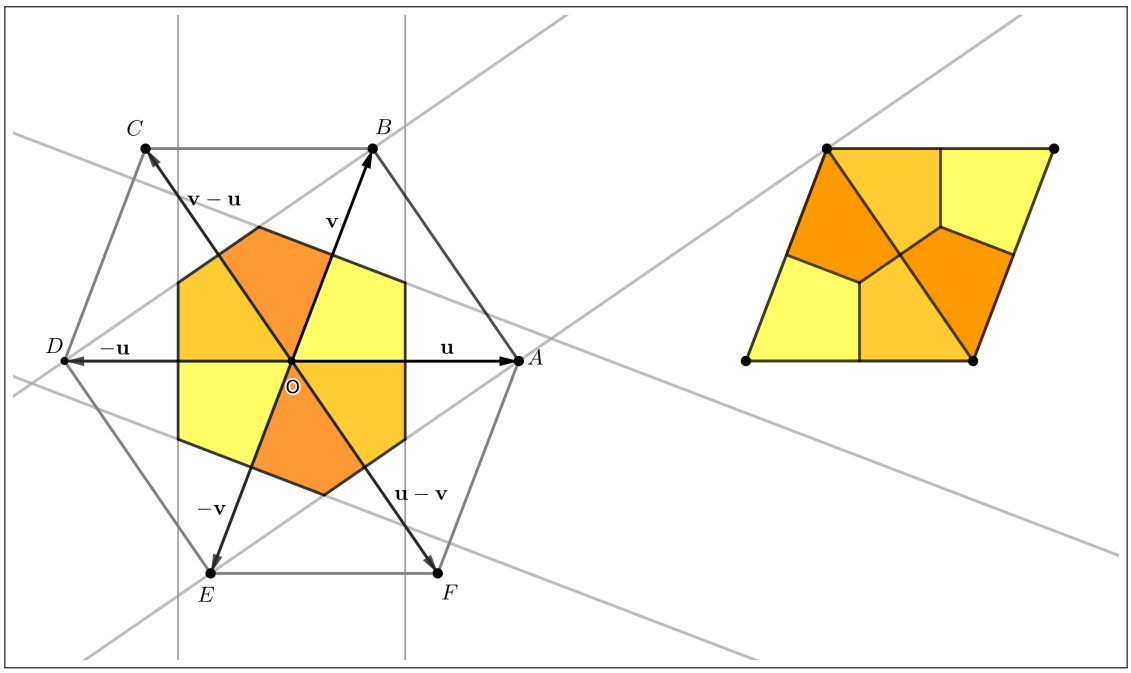
$$\pm\mathbf{u},\ \pm\mathbf{v},\ \mathbf{v}-\mathbf{u},\ \mathbf{u}-\mathbf{v}$$

vektorokhoz tartozó félterek metszete. Legyen ezen félterek metszete P. Megmutatjuk, hogy P átdarabolható az $\mathbf{u}$ és $\mathbf{v}$ vektorok által kifeszített paralelogrammába, tehát P térfogata a rács térfogata. Ez csak akkor lehetséges, ha P a rács Voronoi cellája.

Az átdarabolás a 3.5. ábrán látható. Az átdarabolás azért működik, mivel az OAB, OBC, OCD, ODE, OEF és OFA háromszögek egybevágóak, amelyek köréírható köreinek középpontjai a Voronoi cella egy-egy csúcsa.

Mivel a voronoi cellát határoló oldalak pont ezen háromszögek megfelelő oldalfelező merőlegesei, így az ábrán látható módon a Voronoi cella ténylegesen átdarabolható a rács egy fundamentális paralelogrammájába.

Az ábrából az is látszik, hogy bármely vektorhoz tartozó félsíkot elhagyva, a maradék félsíkok metszete a Voronoi cellánál bővebb halmazt alkot, így a tételt beláttuk.



3.5. ábra. Voronoi cella átdarabolása a síkon

□

3.22. Tétel. *Legyen $L \subset \mathbb{R}^n$ egy két dimenziós rács, $\mathbf{u},\mathbf{v}$ ennek egy LG redukált bázisa, és r_e pedig a* $\mathrm{E}(\mathbf{u},\mathbf{v})$ *erős redukciós tartomány sugara. Ekkor*

$$\frac{r_e}{\|\mathbf{v}\|} \leq \sqrt{1-\frac{\delta(\mathbf{u},\mathbf{v})^2}{2}}.$$

Bizonyítás. Elég az állítást abban az esetben bebizonyítani, ha $L \subset \mathbb{R}^2$, $\mathbf{u} = (1,0)$, és az $\mathbf{u},\mathbf{v}$ LG redukált vektorok által bezárt α szög a $[\pi/3,\pi/2]$ szögtartományba esik. Ezek mellett feltehető még, hogy a $\mathbf{v}$ vektor a felső félsíkba esik.

Legyen tehát $\mathbf{u} = (1,0)$ és legyen

$$T = \{\mathbf{v} \in \mathrm{E}(\mathbf{u}) \mid \mathbf{v} = (v_1,v_2) \text{ ahol } v_2 \geq 0,\ \arg(\mathbf{u},\mathbf{v}) \in [\pi/3,\pi/2], \|\mathbf{u}\| \leq \|\mathbf{v}\|\}. \tag{3.18}$$

Jelölje $\mathbf{x} \in T$ esetén $r(\mathbf{x})$ az $\mathbf{u},\mathbf{x}$ vektorok által generált rács Voronoi cellájának sugarát. Ez a sugár pont a 3.5. ábrán látható *OAB* háromszög köréírható körének sugara, azaz azon szakasz hossza amely az $\mathbf{u}$ és $\mathbf{x}$ vektorok felezőmerőlegeseinek metszéspontját összeköti $\mathbf{0}$-val.

Azt szeretnénk belátni, hogy tetszőleges $\mathbf{x} \in T$ esetén

$$\frac{r(\mathbf{x})}{\|\mathbf{x}\|} \leq \sqrt{1-\frac{\delta(\mathbf{u},\mathbf{x})^2}{2}} \tag{3.19}$$

teljesül.

Az állítást úgy fejezzük be, hogy vesszük az

$$f(\mathbf{x}) = \frac{r(\mathbf{x})}{\|\mathbf{x}\|} \tag{3.20}$$

és a

$$g(\mathbf{x}) = \sqrt{1 - \frac{\delta(\mathbf{u},\mathbf{x})}{2}^2} \tag{3.21}$$

függvényeket majd belátjuk, hogy $\mathbf{x} \in T$ esetén

$$f(\mathbf{x}) \leq g(\mathbf{x}). \tag{3.22}$$

Egy kis számolás után kijön, hogy $\mathbf{x} = (x,y) \in T$ esetén

$$f(\mathbf{x}) = f(x,y) = \frac{1}{2}\sqrt{\frac{(x-1)^2}{y^2} + 1} \tag{3.23}$$

és

$$g(\mathbf{x}) = g(x,y) = \frac{1}{\sqrt{2}}\sqrt{1 - \frac{x^2}{y^2}}. \tag{3.24}$$

Vegyük észre, hogy y növelésével $f(x,y)$ csökken, $g(x,y)$ pedig növekszik, így (3.22)-et elég a T tartomány alsó határán megmutatni, azaz az olyan $(x,y) \in T$ pontokra amelyekre $x^2 + y^2 = 1$. Ilyen pontokra $f(x,y) \leq g(x,y)$ pontosan akkor teljesül, ha

$$f(x,y)^2 - g(x,y)^2 \leq 0$$

azaz ha

$$\frac{1}{4}\left(\frac{(x-1)^2}{y^2} + 1\right) - \frac{1}{2}\left(1 - \frac{x^2}{y^2}\right) \leq 0.$$

mivel a most vizsgált esetben $y^2 = 1 - x^2$ így ezt a következő formába írhatjuk át:

$$\frac{1}{4}\frac{x^2 - 2x + 1}{1 - x^2} + \frac{1}{4} - \frac{1}{2} + \frac{1}{2}\frac{x^2}{1 - x^2} \leq 0,$$

amiből a következőt kapjuk:

$$x(x - 1/2) \leq 0,$$

ahol $x \in [0, 1/2]$. Ez nyilvánvalóan teljesül. Ezzel az állítást beláttuk.

□

3.23. Tétel. $\delta_3 = \sqrt{2}$

Bizonyítás. Azt már láttuk, hogy létezik olyan 3 dimenziós L rács, amelyre

$$\delta(L) = \sqrt{2}$$

teljesül (lásd 3.16). Amit még be szeretnénk látni, hogy

$$\delta_3 \leq \sqrt{2}.$$

Ezt rögtön megkapjuk a 3.19. és 3.22. tételekből, ugyanis ezek szerint egy tetszőleges 3 dimenziós L rácsnak egy LG-redukált $\mathbf{u},\mathbf{v},\mathbf{w}$ bázisára

$$\frac{\|\mathbf{w}\|^2}{\|\mathbf{w}^*\|^2} \leq \frac{1}{1-r_2^2/\|\mathbf{v}\|^2} \leq \frac{1}{1-(1-\delta(\mathbf{u},\mathbf{v})^2/2)} = \frac{2}{\delta(\mathbf{u},\mathbf{v})^2},$$

azaz

$$\delta(\mathbf{u},\mathbf{v},\mathbf{w}) = \delta(\mathbf{u},\mathbf{v}) \cdot \frac{\|\mathbf{w}\|}{\|\mathbf{w}^*\|} \leq \sqrt{2},$$

teljesül, ahol $\mathbf{w}^*$ a $\mathbf{w}$ vektor $\mathbf{u}$ és $\mathbf{v}$ által kifeszített altérre merőleges komponense. □

Valószínűsíthető, hogy az előbb leírt módszert végig lehet játszani három dimenzióban, azaz gyanítjuk a következőket:

3.24. Sejtés. *Legyen $L \subset \mathbb{R}^n$ egy három dimenziós rács, $\mathbf{u},\mathbf{v},\mathbf{w}$ ennek egy LG redukált bázisa, és r_e pedig a $\mathrm{E}(\mathbf{u},\mathbf{v},\mathbf{w})$ erős redukciós tartomány sugara. Ekkor*

$$\frac{r_e}{\|\mathbf{w}\|} \leq \sqrt{1-\frac{\delta(\mathbf{u},\mathbf{v},\mathbf{w})^2}{4}}.$$

3.25. Sejtés. $\delta_4 = 2$.

A nehézség onnan adódik, hogy 3 dimenzióban a Voronoi cellák szerkezete valamivel bonyolultabb. Valószínűleg még tovább lehet menni és a 3.24. sejtéshez hasonló 4 dimenzóban is felírható.

4. Az általános Lagrange-Gauss algoritmus elemzése

Legyen L egy n dimenziós rács. Az előző fejezetben leírt 3.1. algoritmus egy lefutása leírható az L rács bázisainak

$$B_i := \mathbf{b}_1[i], \mathbf{b}_2[i], \ldots, \mathbf{b}_k[i] \qquad i = 1,2,\ldots,N \tag{4.1}$$

és

$$C_i := \mathbf{r}_1[i], \mathbf{r}_2[i], \ldots, \mathbf{r}_k[i] \qquad i = 1,2,\ldots,N \tag{4.2}$$

sorozataival. B_i az algoritmus i. iterációjában a méret szerint növekvő sorrendbe rendezés után kapott bázis, C_i az i. iterációbeli erős redukció után kapott bázis, N pedig az algoritmus iterációinak száma. Ekkor a B_i bázis ortogonalitási defektusát az egyszerűség kedvéért

$$\delta(B_i) := \delta(\mathbf{b}_1[i], \mathbf{b}_2[i], \ldots, \mathbf{b}_k[i]) \tag{4.3}$$

módon jelöljük.

4.1. Tétel. *A 3.1. algoritmus iterációinak száma kevesebb mint*

$$\sqrt{1! \cdot 2! \cdot \ldots \cdot (k-2)!} \cdot 3^{\binom{k+1}{2}} \cdot 2^{\binom{k-1}{2}} \cdot (\delta(B_1))^k.$$

Bizonyítás. Mivel az utolsó iteráció kivételével az algoritmus minden iterációjában legalább egy bázisvektor hossza csökken, így

$$\delta(B_1) > \delta(B_2) > \ldots > \delta(B_N). \tag{4.4}$$

Bontsuk az algoritmus futását szakaszokra. Nevezzük l-szakasznak az algoritmus olyan egymás utáni lépéseit, ami alatt az első l bázisvektor változatlan marad.

Bontsuk az algoritmus futását maximális hosszúságú 1-szakaszokra, majd rekurzív minden $(l-1)$-szakaszt bontsunk fel maximális hosszúságú l-szakaszokra ($l = 1,2,\ldots,k-2$). Egy $(l-1)$-szakaszon belül az l-szakaszok száma, az a szám, ahányszor az $(l-1)$-szakasz alatt csökkent az l. bázisvektor. Megmutatjuk, hogy az ilyen csökkenések száma legfeljebb

$$\rho_l := \sqrt{(l-1)!} 2^{l-1} 3^{k-l+1} \delta(B_1), \tag{4.5}$$

azaz az algoritmus iterációinak N számára a következő felső becslés teljesül:

$$\begin{aligned} N \leq \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_{k-1} = \sqrt{1!2!\ldots(k-2)!} \cdot 3^{2+3+\ldots+k} \cdot 2^{1+2+\ldots+k-2} \cdot (\delta(B_1))^k < \\ < \sqrt{1! \cdot 2! \cdot \ldots \cdot (k-2)!} \cdot 3^{\binom{k+1}{2}} \cdot 2^{\binom{k-1}{2}} \cdot (\delta(B_1))^k \end{aligned}$$

és ezzel belátjuk az állítást is.

Ahhoz, hogy megmutassuk (4.5)-öt, vizsgáljunk meg egy konkrét $(l-1)$-szakaszt. Kezdődjön az $(l-1)$-szakasz a

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k$$

hossz szerint növekvő sorrendbe rendezett bázissal. Ekkor az $(l-1)$-szakasz alatt az l. bázisvektornak mindig az

$$\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{l-1})$$

tartományba kell esnie, így ρ_l megbecsléséhez elég megbecsülnünk, hogy hány rácspont esik a

$$\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{l-1}) \cap \mathrm{B}(\|\mathbf{b}_l\|)$$

tartományba. Ehhez hasonlóan járunk el mint a 2.10. és 2.14. tételek bizonyításánál. Legyen

$$H = \{x_1\mathbf{b}_1^* + x_2\mathbf{b}_2^* + \ldots + x_k\mathbf{b}_k^* \mid \forall i < l\colon |x_i| \le R_i/\|\mathbf{b}_i^*\|,\ \forall i \ge l\colon |x_i| \le \|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|\}.$$

Ekkor

$$\mathrm{E}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_l) \cap \mathrm{B}(\|\mathbf{b}_{l+1}\|) \subset H,$$

így elég a H-beli rácspontok számát megbecsülni. Ehhez legyen

$$H_i := ([\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{i-1}] + s_i\mathbf{b}_i + s_{i+1}\mathbf{b}_{i+1} + \ldots + s_k\mathbf{b}_k) \cap H.$$

Legyenek $s_{i+1}, s_{i+2}, \ldots, s_k$ fix egész számok úgy, hogy H_{i+1} nem üres. Nézzük meg, hogy ekkor hányféleképp választható meg s_i, hogy H_i se legyen üres. Jelölje ezt a számot ζ_i.

Ekkor $i \ge l$ esetén

$$\zeta_i \le \left\lfloor \frac{2\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|} \right\rfloor + 1 \le 3\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|},$$

$i < l$ esetén pedig a 2.13. lemmát és a 3.18. tételt felhasználva látható, hogy

$$\zeta_i \le \left\lfloor \frac{2R_i}{\|\mathbf{b}_i^*\|} \right\rfloor + 1 \le 4\frac{R_i}{\|\mathbf{b}_i^*\|} \le 2\sqrt{i}\frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_i^*\|},$$

így végül a következőt kapjuk:

$$\rho_l \le 2\sqrt{1}\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_1^*\|} \cdot 2 \cdot \sqrt{2}\frac{\|\mathbf{b}_2\|}{\|\mathbf{b}_2^*\|} \cdot \ldots \cdot 2\sqrt{l-1}\frac{\|\mathbf{b}_{l-1}\|}{\|\mathbf{b}_{l-1}^*\|} \cdot 3\frac{\|\mathbf{b}_l\|}{\|\mathbf{b}_l^*\|} \cdot 3\frac{\|\mathbf{b}_{l+1}\|}{\|\mathbf{b}_{l+1}^*\|} \cdot \ldots \cdot 3\frac{\|\mathbf{b}_k\|}{\|\mathbf{b}_k^*\|} =$$
$$= \sqrt{(l-1)!}2^{l-1}3^{k-l+1}\delta(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k) \le \sqrt{(l-1)!}2^{l-1}3^{k-l+1}\delta(B_1),$$

tehát a tételt beláttuk. □

Ahogy ezt a következő tétel mutatja, az első 4 dimenzióban ennél többet tudunk mondani. A tétel bizonyításában a [Ste08] cikk ötleteit használjuk fel.

4.2. Tétel. *A 3.1. algoritmus $2 \le k \le 4$ esetén $k\log(\max_i \|\mathbf{b}_i\|) - k\log(\lambda_1) + 1 + \mathscr{O}(1)$ iteráció alatt lefut.*

Bizonyítás. Legyen $1 < \eta$ (később pontosabban megválasztott) valós szám. Legyen m minimális, hogy az m. iterációban

$$\forall l\colon \|\mathbf{r}_l[m]\|^2 \le \eta\|\mathbf{r}_{l+1}[m]\|^2 \tag{4.6}$$

teljesül. Ekkor $0 < i < m$ esetén létezik egy olyan l index amire

$$\|\mathbf{r}_l[i]\|^2 > \eta\|\mathbf{r}_{l+1}[i]\|^2,$$

teljesül. Ekkor

$$\eta\|\mathbf{r}_{l+1}[i]\|^2 < \|\mathbf{r}_l[i]\|^2 \le \|\mathbf{b}_l[i]\|^2 \le \|\mathbf{b}_{l+1}[i]\|^2,$$

azaz

$$\|\mathbf{r}_{l+1}[i]\| < \frac{\|\mathbf{b}_{l+1}[i]\|}{\sqrt{\eta}}. \tag{4.7}$$

Mivel tetszőleges i esetén fennáll a

$$\lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_k \le \|\mathbf{b}_1[i]\| \cdot \|\mathbf{b}_2[i]\| \cdot \ldots \cdot \|\mathbf{b}_k[i]\|$$

becslés és $1 \leq i < m$ esetén (4.7) miatt

$$\|\mathbf{b}_1[i+1]\| \cdot \|\mathbf{b}_2[i+1]\| \cdot \ldots \cdot \|\mathbf{b}_k[i+1]\| < \frac{\|\mathbf{b}_1[i]\| \cdot \|\mathbf{b}_2[i]\| \cdot \ldots \cdot \|\mathbf{b}_k[i]\|}{\sqrt{\eta}},$$

így

$$m < \log\left(\frac{\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdot \ldots \cdot \|\mathbf{b}_k\|}{\lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_k}\right) + 1 \leq k \log\left(\max_i \|\mathbf{b}_i\|\right) - k \log \lambda_1 + 1. \tag{4.8}$$

Most belátjuk, hogy az m. iterációra az ortogonalitási defektus megfelelően kicsi lett. Az egyszerűség kedvéért a továbbiakban $\mathbf{r}_i[m]$ helyett csak simán $\mathbf{r}_i$-t írunk, továbbá az $\mathbf{r}_i$ vektor $[\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{i-1}]$-re merőleges komponensét $\mathbf{r}_i^*$-al jelöljük. Ekkor (4.6) miatt $1 \leq i < j \leq k$ esetén

$$\|\mathbf{r}_i\|^2 \leq \eta^{j-i} \|\mathbf{r}_j\|^2.$$

Mivel a $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n$ bázis erősen redukált, így $2 \leq i \leq k$ esetén a következőt kapjuk:

$$\|\mathbf{r}_i\|^2 \leq R_{i-1}^2 + \|\mathbf{r}_i^*\|^2 \leq \frac{1}{4}(\|\mathbf{r}_1\|^2 + \|\mathbf{r}_2\|^2 + \ldots + \|\mathbf{r}_{i-1}\|^2) + \|\mathbf{r}_i^*\|^2 \leq$$
$$\leq \frac{1}{4}(\eta + \eta^2 + \ldots + \eta^{i-1})\|\mathbf{r}_i\|^2 + \|\mathbf{r}_i^*\|^2.$$

Mivel az $2 \leq k \leq 4$ esetet vizsgáljuk, így $2 \leq i \leq 4$. Ebből kifolyólag η megválasztható úgy, hogy

$$\eta_i := \frac{1}{4}(\eta + \eta^2 + \ldots + \eta^{i-1}) < 1$$

teljesüljön minden $2 \leq i \leq k$ esetén ($1 < \eta < 2$). Végül η megfelelő megválasztásával azt kapjuk, hogy

$$\frac{\|\mathbf{r}_i\|}{\|\mathbf{r}_i^*\|} \leq \frac{1}{\sqrt{1-\eta_i}}, \tag{4.9}$$

tehát

$$\delta(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n) \leq \frac{1}{\sqrt{(1-\eta_2) \cdot (1-\eta_3) \ldots \cdot (1-\eta_k)}}. \tag{4.10}$$

Ezek szerint innentől a 4.1. tétel miatt az algoritmus konstans sok lépésben leáll.

Keressünk konkrét számokat a különböző esetekhez!

$k = 2$, $\eta = 2$ esetén

$$\eta_2 = 1/2$$

tehát ekkor

$$\delta(\mathbf{r}_1, \mathbf{r}_2) \leq \sqrt{2}.$$

$k = 3$, $\eta = 4/3$ esetén

$$\eta_2 = 1/3, \text{ és } \eta_3 = 7/9$$

így ekkor

$$\delta(\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3) \leq 3/\sqrt{12}.$$

$k = 4$, $\eta = 8/7$ esetén pedig

$$\eta_2 = 2/7, \ \eta_3 = 30/49, \text{ és } \eta_4 = 338/343$$

így ekkor

$$\delta(\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4) \leq \frac{343\sqrt{19}}{95}.$$

Ezzel a tételt beláttuk. □

Hivatkozások

[Bab86] L. Babai. On lovász lattice reduction and the nearest lattice point problem. In *Combinatorica 6*, page 1–13, 1986.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*, chapter 17.1. Cambridge University Press, New York, 2012.

[Gol02] Daniele Micciancio; Shafi Goldwasser. *Complexity of Lattice Problems*. Springer Science+Business Media, LLC, New York, 2002.

[Kan83] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proc. of 15th STOC*, page 193–206. ACM, 1983.

[Lek87] P. E. Gruber; C. G. Lekkerkerker. *Geometry of numbers*. Elsevier Science Publishers B.V., The Netherlands, Amsterdam, 2nd edition, 1987.

[Lov86] László Lovász. An algorithmic theory of numbers, graphs and convexity. In *CBMS-NSF Regional Conference Series in Appl. Math. Society for Industrial and Applied Mathematics*, Philadelphia, 1986.

[Ngu10] Phong Q. Nguyen. Hermite's constant and lattice algorithms. In Phong Q. Nguyen; Brigitte Vallée, editor, *The LLL Algorithm*, pages 19–71, Berlin Heidelberg, 2010. Springer-Verlag.

[SD20] Noah Stephens-Davidowitz. Complexity of lattice problems, 2020. A beszéd videófelvétele a `http://www.noahsd.com/#talks` weboldalon megtalálható. Utoljára elérve: 2024.05.13.

[Slo99] J. H. Conway; N. J. A. Sloane. *Sphere packings, Lattices and Groups*. Springer-Verlag, New York, 3rd edition, 1999.

[Ste08] Phong Q. Nguyen; Damien Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Transactions on Algorithms*, 2008.

[Ver07] Laczkovich Miklós; T. Sós Vera. *Valós Analízis II*, chapter 21. Nemzeti Tankönyvkiadó Zrt., Budapest, 2007.