

Voronoi-cella számítás elméletben és gyakorlatban

Fazekas Péter László

Témavezető: Dr. Grolmusz Vince

1. Bevezető

Georges Voronoi a „Deuxième Mémoire sur les paralléloèdres primitifs” [12] című munkájában olyan politópokat vizsgált, amelyek eltoltjaiból \mathbb{R}^n egy lap-illeszkedő parkettázását kapjuk. Az ilyen politópokat paralelohedrának nevezte el. Belátta, hogy minden primitív paralelohedra affin ekvivalens egy rács Voronoi-cellájával, és megfogalmazta a sejtését miszerint ez tetszőleges paralelohedrára igaz. A rácsok Dirichlet-tartománya azóta a Voronoi-cella elnevezést vette át.

A kutatás eredménye, hogy bemutatjuk Voronoi elméletének egy alkalmazását. Voronoi a kvadrátikus formák nyelvén beszél, míg az alkalmazások szempontjából érdekesebb az elméletet a rácsok nyelvén megfogalmazni. John Conway és Neil Sloane egy hat részes cikksorozatot készített többek között abból a célból, hogy szisztematizálják az alacsony dimenziós rácsokra bevezetett jelöléseket, amelyek a szakirodalom különböző területein előfordulnak. Ezen cikksorozat 6. részében [9] összefoglalják Voronoi elméletének alapjait, azt a rácsok nyelvén bemutatva. A 3. fejezetben az ő szisztematikájukat követem, viszont az itt található bizonyítások az önálló munkám eredményei.

Az alkalmazás a modern kriptográfia területén merül fel. Itt központi szerepet játszanak bizonyos rácsokon adott algoritmikus problémák. Fontos, hogy ezen problémák bonyolultságát minél pontosabban megértsük, ugyanis modern kriptográfiai rendszerek biztonsága múlik rajtuk [11], [2]. Bemutatom Miccancio és Voulgaris algoritmusát [13], amely alapját a Voronoi-cellák elmélete nyújtja. Ezen algoritmus volt az első amely szimpla exponenciális időben megoldást adott az említett problémák megoldására. Ezen algoritmus jelenleg az egyetlen ismert determinisztikus algoritmus amelyik bizonyítottan ilyen jól teljesít, és vele kapcsolatban még számos megoldatlan kérdés merül fel, ami további jövőbeli kutatásnak ad okot.

2. Alap fogalmak

Legyen \mathbb{R}^n az Euklideszi vektortér a szokásos skaláris szorzással. Az \mathbb{R}^n egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisának egész együtthatós lineáris kombinációi által alkotott L halmazt *rácsnak* hívjuk. Ilyenkor a bázisvektorokat az L rács bázisának, az L rácsot pedig a $\mathbf{b}_1, \dots, \mathbf{b}_n$ vektorok által generált n dimenziós rácsnak nevezzük. Ha ki akarjuk emelni a bázisvektorokat, akkor erre az $L(\mathbf{b}_1, \dots, \mathbf{b}_n)$ jelölést használjuk. Például \mathbb{Z}^n a szokásos bázis által generált, n dimenziós rács. Az n dimenziós rácsok halmazát jelölje \mathcal{L}_n . Az n dimenziós rácsok pontosan \mathbb{R}^n olyan diszkrét additív részcsoportjai, amelyek nem esnek bele \mathbb{R}^n egy valódi alterébe ([6] 18. oldal).

A diszkrét tulajdonság következménye, hogy minden L rácsban található olyan nem $\mathbf{0}$ vektort, amely hossza minimális. Ezen vektor hosszát $\lambda_1(L)$ jelöli és a rács első minimumának hívjuk. Egy n dimenziós rácsnak definiálhatjuk n különböző minimumát. A

$$\lambda_i(L) \stackrel{\text{def}}{=} \inf\{r \in \mathbb{R} \mid \exists \mathbf{l}_1, \dots, \mathbf{l}_i \in L \text{ lineárisan független vektorok, hogy } \forall i: \|\mathbf{l}_i\| \leq r\}$$

valós számot a rács i . minimumának hívjuk. Ekkor meggondolható, hogy $\lambda_1(L) \leq \lambda_2(L) \leq \dots \leq \lambda_n(L)$ és adott rácsnak mindig vannak olyan független $\mathbf{l}_1, \dots, \mathbf{l}_n$ vektorai amelyekre

$$\|\mathbf{l}_1\| = \lambda_1(L), \dots, \|\mathbf{l}_n\| = \lambda_n(L)$$

teljesül.

Egy rács *determinánsa* vagy *térfogata*, az a rács egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisa által kifeszített fundamentális paralelepipedon

$$P = \{x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n \mid \forall i: x_i \in [-1/2, 1/2]\}$$

térfogata. Egy L rács térfogatát jelölje vol L . Ha $\mathbf{b}_1, \dots, \mathbf{b}_n$ az L rács egy bázisa, $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ pedig ezen bázis Gram-Schmidt ortogonalizáltja, akkor

$$\text{vol } L = \|\mathbf{b}_1^*\| \cdot \dots \cdot \|\mathbf{b}_n^*\|.$$

Legyen adott egy L rács. Ha L nem 1 dimenziós, akkor végtelen sok különböző bázisa van. A rács azon bázisait szeretjük jobban, amely vektorai közel merőlegesek egymásra. Egy ilyen bázist *redukált* bázisnak hívunk. A redukáltság számos különböző fogalma ismert. Mi a dolgozat során kettőt fogunk használni.

2.1. Definíció. Azt mondjuk, hogy az n dimenziós L rács egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisa *Lagrange-Gauss redukált* vagy röviden *LG-redukált*, ha

$$\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \dots \leq \|\mathbf{b}_n\|$$

és tetszőleges i index és $s_1, \dots, s_{i-1} \in \mathbb{Z}$ számok esetén

$$\|\mathbf{b}_i\| \leq \|\mathbf{b}_i - s_1 \mathbf{b}_1 - \dots - s_{i-1} \mathbf{b}_{i-1}\|.$$

LG-redukált bázis első 4 dimenzióban polinomiális időben található és a bázis vektorainak hossza rendre az általuk kifeszített rács minimumai [10]. Ennek következményeként a következőt kapjuk:

2.2. Állítás. Legyen adott egy n dimenziós L rács, és ennek egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ LG-redukált bázisa. Ekkor tetszőleges $i < j$ esetén

$$|\mathbf{b}_i \cdot \mathbf{b}_j| \leq \mathbf{b}_j^2 / 2$$

teljesül. $n \leq 4$ esetén emellett még a

$$|\mathbf{b}_i \cdot \mathbf{b}_j| \leq \mathbf{b}_i^2 / 2$$

egyenlőtlenség is fennáll.

Bizonyítás. A $|\mathbf{b}_i \cdot \mathbf{b}_j| \leq \mathbf{b}_j^2/2$ egyenlőtlenség azt jelenti, hogy \mathbf{b}_i a $[\mathbf{0}, \mathbf{b}_j]$ és $[\mathbf{0}, -\mathbf{b}_j]$ szakaszok felezőhipersíkjai által határolt sávba esik. Ha az egyenlőtlenség nem állna fent, akkor vagy $\|\mathbf{b}_i - \mathbf{b}_j\| \leq \|\mathbf{b}_i\|$ vagy $\|\mathbf{b}_i + \mathbf{b}_j\| \leq \|\mathbf{b}_i\|$ teljesülne, ami ellentmondana az LG-redukáltság definíciójának. A második egyenlőtlenség ugyanígy látszik, csak ott a rács minimumainak definíciója szerint jutunk ellentmondásra. \square

A redukáltság egy fontos fogalmát Lovász László, H. Lenstra és A. Lenstra találta ki. Legyen $\mathbf{b}_1, \dots, \mathbf{b}_n$ egy bázis, és legyen $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ ezen bázis Gramm-Schmidt ortogonalizáltja. Legyen \mathbf{b}'_i a \mathbf{b}_i vektor $\mathbf{b}_1, \dots, \mathbf{b}_{i-2}$ vektorok által kifeszített altérre merőleges komponense, ahol $i \geq 2$.

2.3. Definíció. Azt mondjuk, hogy egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázis LLL-redukált, ha tetszőleges $j < i$ indexek esetén

$$|\mathbf{b}_i \cdot \mathbf{b}_j^*| \leq (\mathbf{b}_j^*)^2/2$$

és tetszőleges $2 \leq i$ index esetén

$$\|\mathbf{b}_{i-1}^*\| \leq (2/\sqrt{3})\|\mathbf{b}'_i\|$$

teljesül.

Az LLL-redukáltság fogalma azért kulcsfontosságú, mivel LLL-redukált bázis polinomiális időben található ([7] 21. oldal). Használni fogjuk, hogy LLL-redukált bázisokra igaz a következő [8]:

2.4. Állítás. Legyen $\mathbf{b}_1, \dots, \mathbf{b}_n$ egy LLL-redukált bázis. Legyen $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ ezen bázis Gramm-Schmidt ortogonalizáltja. Ekkor tetszőleges i index esetén

$$\frac{1}{2} \sqrt{\|\mathbf{b}_1^*\|^2 + \dots + \|\mathbf{b}_i^*\|^2} \leq 2^{i/2-1} \|\mathbf{b}_i^*\|.$$

3. Voronoi cella meghatározása 2 és 3 dimenzióban

Egy $L \in \mathcal{L}_n$ rács Voronoi-cellája \mathbb{R}^n azon pontjaiból áll, melyek legalább olyan közel vannak az origóhoz, mint bármely másik rácsponthoz. Az L rács Voronoi-celláját jelölje $\text{vor}L$.

Adott $\mathbf{0} \neq \mathbf{v} \in \mathbb{R}^n$ esetén a $\mathbf{0}$ és \mathbf{v} felezőhipersíkja által határolt $\mathbf{0}$ fele néző féltérrel jelölje $H_{\mathbf{v}}$ ($H_{\mathbf{v}} = \{\mathbf{u} \in \mathbb{R}^n \mid \mathbf{v} \cdot \mathbf{u} \leq \mathbf{v}^2/2\}$). Ekkor

$$\text{vor}L = \bigcap_{\mathbf{l} \in L} H_{\mathbf{l}}. \quad (3.1)$$

Igazából $\text{vor}L$ előáll véges sok féltér metszeteként is. Elég azon \mathbf{l} rácspontokhoz tartozó $H_{\mathbf{l}}$ féltéreket venni, ahol $\text{vor}L$ metszete a féltérrel határoló hipersíkkal $n - 1$ dimenziós. Az ilyen vektorokat *szigorú Voronoi-vektoroknak* hívjuk. Ha a hipersík metszete nem feltétlen $n - 1$ dimenziós, viszont nem üres, akkor az \mathbf{l} rácsvektort *Voronoi-vektornak* hívjuk. Nyilván ha \mathbf{l} szigorú Voronoi-vektor akkor $-\mathbf{l}$ is az. Ezek szerint a Voronoi-Cella egy origó szimmetrikus politóp. Rácsvektorokkal való eltoltjai \mathbb{R}^n egy lap-illeszkedő parkettázását adják.

A célunk, hogy meghatározzuk egy rács Voronoi-fontos vektorait. Voronoi a következő tételt látta be:

3.1. Tétel. Legyen L egy n dimenziós rács. Ekkor egy $\mathbf{l} \in L$ pontosan akkor Voronoi-vektor ha $\mathbf{l}/2$ legrövidebb az

$$\mathbf{l}/2 + L$$

osztály vektorai között, és pontosan akkor szigorú Voronoi-vektor, ha csak a $\pm\mathbf{l}/2$ vektorok a legrövidebbek a fenti osztályban.

Bizonyítás. Adott $\mathbf{l} \in L$ esetén legyen $F_{\mathbf{l}} = \{\mathbf{v} \in \mathbb{R}^n \mid \mathbf{v} \cdot \mathbf{l} = \mathbf{l}^2/2\} \cap \text{vor}L$, a Voronoi-cella \mathbf{l} -hez tartozó lapja.

Legyen $\mathbf{l} \in L$ tetszőleges. Tegyük fel, hogy $F_{\mathbf{l}}$ nem üres, azaz $\exists \mathbf{v} \in F_{\mathbf{l}}$. Mivel a Voronoi-cella origó szimmetrikus, így ekkor $-F_{\mathbf{l}} = F_{-\mathbf{l}}$ is a Voronoi-cella egy nem üres oldala és $-\mathbf{v} \in F_{-\mathbf{l}}$. Másrészt $F_{-\mathbf{l}} + \mathbf{l} = F_{\mathbf{l}}$, így $\mathbf{l} - \mathbf{v} \in F_{\mathbf{l}}$, amely pont a \mathbf{v} pont $\mathbf{l}/2$ pontra való tükörképe. Ekkor a Voronoi-cella konvexitása miatt $\mathbf{l}/2 \in F_{\mathbf{l}}$ is teljesül, és azt is megkaptuk, hogy $F_{\mathbf{l}}$ szimmetrikus az $\mathbf{l}/2$ pontjára.

Ezek szerint egy $\mathbf{l} \in L$ vektor pontosan akkor Voronoi-vektor, ha $\mathbf{l}/2 \in \text{vor}L$ azaz $\mathbf{l}/2$ legalább olyan közel van az origóhoz, mint bármely másik rácsponthoz. Ez ekvivalens azzal, hogy $\mathbf{l}/2$ az $\mathbf{l}/2 + L$ osztály legrövidebb vektora tehát a tétel első felével elkészültünk.

Legyen \mathbf{l} egy Voronoi-vektor. Ekkor egy $\mathbf{l}/2 + \mathbf{l}' \in \mathbf{l}/2 + L$ vektor pontosan akkor minimális hosszúságú az osztály vektorai között, ha $(\mathbf{l}/2 + \mathbf{l}')^2 = (\mathbf{l}/2)^2$. Ez pontosan akkor igaz, ha vagy $\mathbf{l} \cdot \mathbf{l}' = (\mathbf{l}')^2$ vagy $-\mathbf{l} \cdot \mathbf{l}' = (\mathbf{l}')^2$. Az első eset pont azt jelenti, hogy $\mathbf{l}/2 \in F_{\mathbf{l}'}$ a második pedig, hogy $\mathbf{l}/2 \in F_{-\mathbf{l}'}$. Ha $\mathbf{l}' \neq \mathbf{l}$ és $\mathbf{l}/2 + \mathbf{l}'$ minimális az osztály vektorai között, akkor ezek szerint $\mathbf{l}/2$ a Voronoi cella legalább 2 lapjában van benne, és így $F_{\mathbf{l}}$ nem lehet $n - 1$ dimenziós. \square

Mivel $(\mathbf{l}/2)L/L$ nem 0 osztályainak száma pontosan $2^n - 1$ így azt is megkaptuk, hogy a szigorú Voronoi-vektorok száma legfeljebb $2 \cdot (2^n - 1)$.

Egy rácsról azt mondjuk, hogy (Voronoi) első típusú, ha van úgynevezett *tompa szuperbázisa*. Azt mondjuk, hogy az L rács $\mathbf{l}_0, \mathbf{l}_1, \dots, \mathbf{l}_n$ vektorai tompa szuperbázist alkotnak, ha

- $\mathbf{l}_1, \dots, \mathbf{l}_n$ a rács egy bázisát alkotják
- tetszőleges $i \neq j$ esetén \mathbf{l}_i és \mathbf{l}_j tompa szöveget zár be, azaz

$$\mathbf{l}_i \cdot \mathbf{l}_j \leq 0$$

- $\mathbf{l}_0 + \mathbf{l}_1 + \dots + \mathbf{l}_n = \mathbf{0}$.

A következő tétel alapján, az első típusú rácsok esetén a szigorú Voronoi-vektorok meghatározása nem nehéz feladat.

3.2. Tétel. Legyen adott egy első típusú L rács és ennek egy $\mathbf{l}_0, \mathbf{l}_1, \dots, \mathbf{l}_n$ tompa szuperbázisa. Ekkor a $2^{n+1} - 2$ részösszeg

$$\mathbf{l}_S = \sum_{i \in S} \mathbf{l}_i \quad S \subset \{0, 1, \dots, n\}$$

$0 < |S| < n$ mind Voronoi-vektort alkotnak. \mathbf{l}_S és $\mathbf{l}_{\bar{S}}$ kongruensek modulo $2L$, viszont ezeken kívül tetszőleges két ilyen vektor különböző osztályba esik.

Ezek szerint, ha találunk egy tompa szuperbázist akkor már meg tudjuk határozni egy rács Voronoi celláját. Voronoi belátta, hogy 2 és 3 dimenzióban minden rács első típusú (egy dimenzióban minden rács triviálisan ilyen). Erre adunk egy bizonyítást az LG-redukáltság segítségével.

3.3. Tétel. Minden 2 dimenziós rács első típusú.

Bizonyítás. Legyen L egy 2 dimenziós rács, és legyen \mathbf{u}, \mathbf{v} a rács egy LG-redukált bázisa. Feltehetjük, hogy $\mathbf{u} \cdot \mathbf{v} \leq 0$, ugyanis különben vehetnénk az $\mathbf{u}, -\mathbf{v}$ bázist.

Ekkor az $\mathbf{u}, \mathbf{v}, -(\mathbf{u} + \mathbf{v})$ vektorok egy tompa szuperbázist alkotnak. Ehhez csak azt kell leellenőrizni, hogy $-\mathbf{u} \cdot (\mathbf{v} + \mathbf{u}) \leq 0$ és $-\mathbf{v} \cdot (\mathbf{v} + \mathbf{u}) \leq 0$ azaz, hogy

$$0 \leq \mathbf{u}^2 + \mathbf{u} \cdot \mathbf{v}$$

és

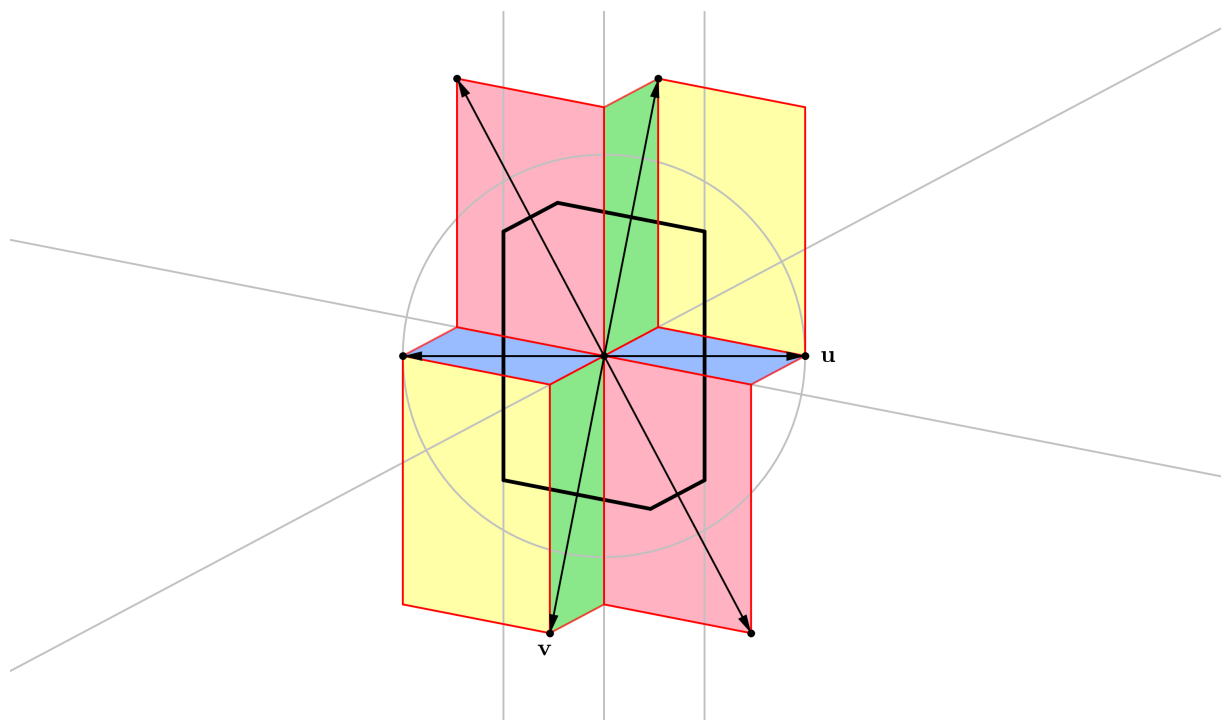
$$0 \leq \mathbf{v}^2 + \mathbf{u} \cdot \mathbf{v}$$

teljesül. Ez azonnal következik a 2.2. állításból. □

3.4. Tétel. Minden 3 dimenziós rács első típusú.

Bizonyítás. Legyen L egy 3 dimenziós rács, és legyen $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ ennek egy LG-redukált bázisa. Legyen L' az \mathbf{u} és \mathbf{v} által kifeszített 2 dimenziós rács, és legyen V ezen rács Voronoi-cellája. Legyen \mathbf{w}' a \mathbf{w} vektor \mathbf{u} és \mathbf{v} által kifeszített altérbe eső komponense. Az LG-redukáltság miatt $\mathbf{w}' \in V$ fog teljesülni.

Tegyük fel, hogy $\mathbf{u} \cdot \mathbf{v} \neq 0$. Ekkor a szigorú Voronoi-vektorok halmaza $B = \{\pm\mathbf{u}, \pm\mathbf{v}, \pm(\mathbf{u} + \mathbf{v})\}$. Az L' rács Voronoi celláját a 3.1. ábrán látható módon bontsuk tartományokra. Az ábrán látható piros, kék, zöld, és sárga tartományok Voronoi-cellába eső részét jelölje rendre P, K, Z és S .



3.1. ábra. Az L' rács Voronoi-cellájának felbontása

Először vizsgáljuk azt az esetet amikor $\mathbf{w}' \in P \cup K \cup Z$. Ekkor legyen $\mathbf{x}, \mathbf{y} \in B$ az a két különböző vektor amely a \mathbf{w}' -től különböző színű tartományba esik és vele tompa szöveget zár be. Ekkor a $\mathbf{x}, \mathbf{y}, \mathbf{w}, -(\mathbf{x} + \mathbf{y} + \mathbf{w})$ az L rács egy tompa superbázisa lesz. Ehhez már csak annyit kell leellenőrizni, hogy

$$-(\mathbf{x} + \mathbf{y} + \mathbf{w}) \cdot \mathbf{w} \leq 0$$

azaz, hogy

$$0 \leq \mathbf{x} \cdot \mathbf{w} + \mathbf{y} \cdot \mathbf{w} + \mathbf{w}^2.$$

Abban az esetben ha $\mathbf{x} = \pm \mathbf{u}$ és $\mathbf{y} = \pm \mathbf{v}$ a 2.2. állítás szerint azonnal elkészültünk. Vegyük észre, hogy abban az esetben ha $\mathbf{x} = \pm(\mathbf{u} + \mathbf{v})$ vagy $\mathbf{y} = \pm(\mathbf{u} + \mathbf{v})$ akkor a $\mathbf{w} \cdot \mathbf{v}$ és $\mathbf{w} \cdot \mathbf{u}$ szorzatok közül az egyik pozitív a másik pedig negatív lesz. Azon vektor amelyik nem a $\pm(\mathbf{u} + \mathbf{v})$ pedig vagy $\pm \mathbf{u}$ vagy $\pm \mathbf{v}$ lesz, így a 2.2. állítást használva ebben az esetben is elkészülünk.

Végül vizsgáljuk azt az esetet amikor $\mathbf{w}' \in S$. Feltehetjük, hogy \mathbf{w}' a sárga komponens azon paralelogrammájába esik amely egyik sarkába az \mathbf{u} vektor mutat, ugyanis különben vehetjük helyette a $-\mathbf{w}$ vektort. Ekkor az $\mathbf{u}, \mathbf{v}, \mathbf{w} - \mathbf{u}, -(\mathbf{v} + \mathbf{w})$ a rács egy tompa superbázisát fogják alkotni. Ehhez már csak azt kell megmutatni, hogy

$$-(\mathbf{w} - \mathbf{u}) \cdot (\mathbf{w} + \mathbf{v}) \leq 0$$

azaz, hogy

$$0 \leq \mathbf{w}^2 + \mathbf{v} \cdot \mathbf{w} - \mathbf{u} \cdot \mathbf{w} - \mathbf{u} \cdot \mathbf{v}$$

teljesül. Ehhez figyeljük meg, hogy $\mathbf{v} \cdot \mathbf{w} \geq 0$ tehát a 2.2. állítás szerint megint elkészültünk.

Abban az esetben amikor $\mathbf{u} \cdot \mathbf{v} = 0$ sokkal könnyebb a helyzet. Feltehető, hogy $\mathbf{w} \cdot \mathbf{u} \leq 0$ és $\mathbf{w} \cdot \mathbf{v} \leq 0$ teljesül, ugyanis ez elérhető a \mathbf{u}, \mathbf{v} vektorokat a $-\mathbf{u}, \mathbf{v}; \mathbf{u}, -\mathbf{v}; -\mathbf{u}, -\mathbf{v}$; párok valamelyikére cserélve. Ekkor az előzőekhez hasonlóan belátható, hogy az $\mathbf{u}, \mathbf{v}, \mathbf{w}, -(\mathbf{u} + \mathbf{v} + \mathbf{w})$ vektorok a rács egy tompa superbázisát alkotják. \square

Ezzel egy praktikus szempontból jól működő algoritmust is kapunk 2 és 3 dimenzióban egy rács tompa superbázisának megtalálására. Persze a Voronoi-cellát tetszőleges dimenzióban meg szeretnénk határozni.

4. Algoritmikus problémák megoldása Voronoi-cella számításal

A rácsok esetén a két legalapvetőbb algoritmikus probléma a következő:

SVP (Shortest Vector Problem): Adott egy n dimenziós L rács egy $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisa. Keressük meg azt a $\mathbf{0} \neq \mathbf{l} \in L$ vektort, melynek hossza minimális.

CVP (Closest Vector Problem): Adott egy n dimenziós rács $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisa, és egy tetszőleges $\mathbf{t} \in \mathbb{R}^n$ vektor. Keressük meg azt az $\mathbf{l} \in L$ rácpontot amelyre $d(\mathbf{l}, \mathbf{t})$ minimális.

Ezen problémák fontos szerepet játszanak például a kvantum utáni kriptográfia terén [11]. Mindkét probléma nehéz: CVP NP-nehéz, SVP pedig NP-nehéz randomizált visszavezetés mellett. Ezek szerint, polinomiális algoritmus találása nem remélhető, viszont jó lenne tudni, hogy mennyire jó exponenciális algoritmusokat kaphatunk.

Igazából elég a CVP-re megoldást találni, ugyanis arra SVP (és a legtöbb rácson adott algoritmikus probléma) polinomiális időben visszavezethető [2].

4.1. Micciancio és Voulgaris algoritmus

Az első szimplán exponenciális futásidejű algoritmus, ami megoldja ezen problémákat, az Micciancio és Voulgaris találmánya [13]. Ezen algoritmus azon az egyszerű megfigyelésen alapszik, hogy a CVP megoldása ekvivalens azon \mathbf{l} rácsvektor megtalálásával, amelyre

$$\mathbf{t} \in \mathbf{l} + \text{vor } L$$

azaz amelyre a \mathbf{t} vektor a Voronoi-cella \mathbf{l} rácsvektorral való eltoltjába esik. Mivel a Voronoi-cella eltoltjai a tér egy parkettázását adják, ezért ez egy jól definiált probléma. Természetesen ha \mathbf{t} kettő vagy több ilyen eltolt határán van, akkor ezen eltoltak közül bármelyiket kiválaszthatjuk.

Az algoritmus három fő elemből tevődik össze:

1. Egy bázisredukciós algoritmus, amely az L rács egy olyan $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisát találja meg, ahol egy CVP megoldása az $L_k = L(\mathbf{b}_1, \dots, \mathbf{b}_k)$ rácsban visszavezethető legfeljebb $2^{k/2}$ CVP megoldására az $L_{i-1} = L(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})$ rácsban
2. Egy n dimenziós L rács Voronoi-cellájának kiszámolása 2^n CVP megoldásával a rácsban
3. Egy algoritmus amely egy n dimenziós L rács szigorú Voronoi-vektorait megkapva megoldja a CVP algoritmust $2^{O(n)}$ időben

Az 1. pont az L rács egy LLL-redukált $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisának megtalálása. Mint azt korábban írtuk, ez polinomiális időben megtehető. A 2.4. állítás szerint ekkor a

$$K = \{x_1 \mathbf{b}_1^* + \dots + x_k \mathbf{b}_k^* \mid \forall i: -1/2 \leq x_i \leq 1/2\}$$

téglatest r testátlójának hossza legfeljebb $2^{k/2-1} \|\mathbf{b}_k^*\|$. Nem nehéz meggondolni, hogy tetszőleges $\mathbf{t} \in \mathbb{R}^k$ esetén létezik egy

$$\mathbf{l} \in (\mathbf{t} + K) \cap L$$

rácspont. Ezen rácspont távolsága \mathbf{t} -től legfeljebb a K téglatest testátlójának $r \leq 2^{k/2-1} \|\mathbf{b}_k^*\|$ hossza. Ha a \mathbf{t} vektor \mathbf{b}_k^* -val párhuzamos komponense $x\mathbf{b}_k^*$, akkor ezek szerint elég az olyan $\mathbf{b} + y\mathbf{b}_k^*$ ($\mathbf{b} \in L_{k-1}$) rácsvektorokat vizsgálni, amelyeknél $|x - y| \leq 2^{k/2-1}$. Ezt azt jelenti, hogy elég a \mathbf{t} vektorhoz legközelebb eső vektort megtalálni az olyan $y\mathbf{b}_k^* + L_{k-1}$ részrácsokban ahol $|y - x| \leq 2^{k/2-1}$. Az ilyen részrácsok száma legfeljebb $2 \cdot (2^{k/2-1} + 1) = 2^{k/2} + 2$. Adott altérben a feladat megoldható egyetlen CVP megoldásával az L_{k-1} rácsban.

A 2. pont a következő módon oldható meg: Keressük meg minden $\mathbf{0} \neq (x_1, \dots, x_n) \in \{0, 1\}^n$ esetén a $\mathbf{b} = x_1 \mathbf{b}_1 + \dots + x_n \mathbf{b}_n$ vektorhoz legközelebb eső $2\mathbf{l}$ rácspontot a $2L$ rácsban. Ekkor a $\mathbf{b} - 2\mathbf{l}$ vektor minimális hosszúságú lesz a $\mathbf{b} + 2L$ osztályban, tehát a 3.1. tétel szerint $\mathbf{b} - 2\mathbf{l}$ egy Voronoi-vektor. Ezt elvégezve kapunk olyan Voronoi-vektorokat is, amelyek nem feltétlen szigorúak, viszont ahogy azt látni fogjuk, ez nem okoz majd problémát az algoritmus futása során.

Végül a 3. pontot két lépésben oldjuk meg. Először tegyük fel, hogy $\mathbf{t} \in 2 \text{vor } L$. Legyen $G = (E, V)$ egy gráf melynek csúcsai a következő módon megadott csúcsok:

$$V = \{\mathbf{t} + \mathbf{l} \mid \mathbf{l} \in L, \mathbf{t} + \mathbf{l} \in 4 \text{vor } L\}$$

és adott $\mathbf{u}, \mathbf{v} \in V$ csúcsok esetén $uv \in E$ pontosan akkor teljesül ha $\mathbf{u} - \mathbf{v}$ egy szigorú Voronoi-vektor. Ekkor ha találunk egy $\mathbf{t} - \mathbf{l} \in \text{vor}L$ csúcsot akkor elkészültünk: \mathbf{l} egyike a \mathbf{t} csúcsához legközelebb eső rácspontoknak. Adott $\mathbf{t} + \mathbf{l}$ csúcs esetén a $\mathbf{t} + \mathbf{l} \in \text{vor}L$ tartalmazás leellenőrizhető legfeljebb $2(2^n - 1)$ skaláris szorzás elvégzésével: amit le kell ellenőrizni, hogy minden \mathbf{v} szigorú Voronoi-vektor esetén teljesül-e, hogy $(\mathbf{t} + \mathbf{l}) \cdot \mathbf{v} \leq \mathbf{v}^2/2$.

Az problémát ezek szerint megoldhatjuk mondjuk egy szélességi bejárással \mathbf{t} -ből indulva. Mivel V mérete legfeljebb 4^n , így az algoritmus tényleg $2^{O(n)}$ időben lefut. Már csak azt kell meggondolni, hogy a $\mathbf{t} \in V$ és az a $\mathbf{t} - \mathbf{l} \in V$ csúcs amelyre $\mathbf{t} - \mathbf{l} \in \text{vor}L$ ugyanabba a komponensbe esnek a G gráfban. Ehhez vegyük a $\delta \mathbf{t}$ szakaszt ahol $\delta \in [0, 1]$. Legyenek $\mathbf{v}_1, \dots, \mathbf{v}_m \in L$ vektorok, hogy $\delta \mathbf{t}$ szakasz sorban a $\mathbf{v}_i + \text{vor}L$ cellákon megy keresztül. Ekkor $\mathbf{v}_0 = \mathbf{0}$, $\mathbf{t} - \mathbf{v}_m \in \text{vor}L$ és tetszőleges i esetén megfelelő $\delta \in [0, 1]$ választással $\mathbf{v}_i - \delta \mathbf{t} \in \text{vor}L$. Mivel tetszőleges $\delta \in [0, 1]$ esetén $\delta \mathbf{t} \in 2 \text{vor}L$ így a Voronoi-cella konvexitása miatt tetszőleges i esetén megfelelő δ választással látható, hogy

$$\mathbf{t} + \mathbf{v}_i - \mathbf{v}_m = \delta \mathbf{t} + \mathbf{v}_i - \delta \mathbf{t} + \mathbf{t} - \mathbf{v}_m \in 4 \text{vor}L.$$

Az általánosság megszorítás nélkül feltehető, hogy a $\delta \mathbf{t}$ szakasz pontjai legfeljebb 2 cellába esnek bele, ugyanis ez \mathbf{t} nagyon kicsi elmozdításával elérhető lenne. Ekkor a $\mathbf{x}_i = \mathbf{t} + \mathbf{v}_i - \mathbf{v}_m$ sorban szomszédosak lesznek, így készen vagyunk.

Végül tegyük fel, hogy $\mathbf{t} \notin 2 \text{vor}L$. Legyen s minimális pozitív egész szám, hogy $\mathbf{t} \in 2^s \text{vor}L$. Legyen $\mathbf{t} = \mathbf{t}_k$. Ekkor az előző algoritmust felhasználva találhatóunk egy $\mathbf{l}_s \in 2^s L$ vektort, hogy $\mathbf{t} - \mathbf{l}_s \in 2^{s-1} \text{vor}L$. Ezt a procedúrát s -szer végrehajtva a cél vektort a rács kisebb és kisebb 2-hatványszorosába visszük és végül megtalálhatjuk azt az $\mathbf{l} \in L$ rácsvektort amelyre $\mathbf{t} - \mathbf{l} \in \text{vor}L$.

Végül csak az hiányzik, hogy az algoritmust megfelelően összerakjuk a fent leírt három összetevőből. Legyen V_k az $L_k = L(\mathbf{b}_1, \dots, \mathbf{b}_k)$ rács szigorú Voronoi-vektorainak halmaza. Az algoritmus a következő lesz:

1. Keressünk egy LLL-redukált $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázist.
2. Határozzuk meg az L_3 három dimenziós rács szigorú Voronoi-vektorait a korábban leírt LG-redukált bázist (2.1. definíció) találva.
3. Ha már meghatároztuk a V_{i-1} halmazt akkor számítsuk ki az V_i halmazt. Ezt megtehetjük 2^i CVP megoldásával. Itt minden CVP-t megoldhatunk $2^{i/2}$ CVP megoldásával az L_{i-1} rácsban, ahol a szigorú Voronoi-vektorok halmaza már ismert, így itt egy-egy CVP megoldása $2^{O(i)}$ időt vesz igénybe.

Ez így összesen nem több mint $O(1) + \sum_{i=4}^n 2^i \cdot 2^{i/2} \cdot 2^{O(i)} = 2^{O(n)}$ időt vesz igénybe. (Ez akkor igaz csak persze, ha a vektorokkal való műveleteket $O(1)$ időnek gondoljuk, viszont nagyságrendileg ugyanezt a futásidőt kapjuk különben is, mivel a vektorokkal való műveletek elvégzése a vektorok méretében polinomiális.)

5. Nyitott kérdések

A cikkük végén Micciancio és Voulgaris több nyitott problémát is felsorolt. Ezek nagy része még mindig megoldatlan. Először is a fent leírt algoritmus exponenciális időben és tárban fut.

Jó lenne találni az algoritmus egy variációját amely csak polinomiális tárat használ. Christoph Hunkenschröder és társai megmutatták, hogy egy rács Voronoi-cellája mindig reprezentálható polinomiálisan sok vektort felhasználva, azonban egy ilyen reprezentációt nem sikerült a Voronoi-cella kiszámolása nélkül előállítaniuk [3]. Az eddig legjobban teljesítő polinomiális tárat használó determinisztikus algoritmus az Kannan algoritmusa. Ez $n^{O(n)}$ időben fut [4].

Az itt bemutatott algoritmus csak l_2 norma esetén működik. Adódik a kérdés, hogy lehet-e találni megoldást tetszőleges l_p norma esetén. Ennek megoldása szimpla exponenciális algoritmushoz vezetne az egész értékű programozás megoldására [5].

Az itt bemutatott algoritmus futásideje $2^{O(n)}$. Adódik a kérdés, hogy mennyire jó konstanst tudunk elérni. A CVP probléma megoldására ismert leggyorsabb algoritmus jelenleg $2^{n+o(n)}$ és ezen algoritmus véletlent használ [1]. A jelenleg ismert legjobb determinisztikus algoritmus, az amit itt bemutatunk. Az itt leírt algoritmus futásideje $4^{n+o(n)}$ -re levihető. Adódik a kérdés, hogy az algoritmus futásideje levihető-e $2^{n+o(n)}$ -re.

Egy másik nyitott kérdés, hogy az algoritmust használva megtalálható-e szimpla exponenciális időben egy rács fedési sugara, vagy ekvivalensen a Voronoi-cella azon pontja amelyik legtávolabb esik az origótól. A Voronoi-cella csúcsainak felsorolása a szigorú Voronoi-vektorok segítségével akár $n^{\Omega(n)}$ időt is igénybe vehet.

Engem még foglalkoztat néhány nyitott kérdés, amelyekkel nem találkoztam a szakirodalomban.

Van-e minden rácsnak olyan bázisa, amely szigorú Voronoi vektorokból áll?

Található-e minden $n > 1$ dimenziós rácsnak olyan $\mathbf{b}_1, \dots, \mathbf{b}_n$ bázisa, hogy minden i -re

$$\|\mathbf{b}_i\| \leq \lceil \log i \rceil \cdot \|\mathbf{b}_i^*\|$$

teljesül? 2,3 és 4 dimenzióban ez biztosan igaz, hiszen az itt bemutatott LG-redukált bázisra ez mindig teljesül. Magasabb dimenzióban ezzel a kérdéssel még senki nem foglalkozott. Egy ilyen bázis segítségével az SVP megoldható lenne $O((\log n)^n)$ időben és polinomiális tártan.

Egy kérdés amivel a szakdolgozatomban foglalkoztam, hogy meghatározom az n dimenziós merőlegességi konstans (δ_n) értékét alacsony dimenzióban. Ezen konstans értékét kiszámoltam $n = 2, 3$ esetén és érdekes módon az derült ki, hogy itt értéke megegyezik a $k = 2^{n-1}$ dimenziós Hermit konstans γ_k értékével. Azt gondolom, hogy ez az összefüggés $n = 4$ esetén is fennáll. Ennek megmutatásához elég lenne egy megfelelő felső korlátot szabni a 3 dimenziós Voronoi-cella átmérőjére [8].

Hivatkozások

- [1] D. Aggarwal and N. Stephens-Davidowitz. Just take the average! an embarrassingly simple 2^n -time algorithm for SVP (and CVP). In *SOSA*, 2018.
- [2] D. M. S. Goldwasser. *Complexity of Lattice Problems*. Springer Science+Business Media, LLC, New York, 2002.
- [3] C. Hunkenschröder, G. Reuland, and M. Schymura. On compact representations of voronoi cells of lattices. *Mathematical Programming*, 183(1):337–358, Sep 2020.

- [4] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proc. of 15th STOC*, page 193–206. ACM, 1983.
- [5] R. Kannan. Minkowski’s convex body theorem and integer programming. 6 2018.
- [6] P. E. G. C. G. Lekkerkerker. *Geometry of numbers*. Elsevier Science Publishers B.V., The Netherlands, Amsterdam, 2nd edition, 1987.
- [7] L. 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.
- [8] F. P. László. Rácsok, parkettázások, és bázisredukciós algoritmusok, 2024. Bsc thesis.
- [9] J. H. C. N. J. A. Sloane. *Sphere packings, Lattices and Groups*. Springer-Verlag, New York, 3rd edition, 1999.
- [10] P. Q. N. D. Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Transactions on Algorithms*, 2008.
- [11] N. Stephens-Davidowitz. Research statement.
<https://www.noahsd.com/NSD%20research%20statement.pdf>.
- [12] G. Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. deuxième mémoire. recherches sur les paralléloèdres primitifs. *Journal für die reine und angewandte Mathematik*, 134:198–287, 1908.
- [13] D. M. P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. *SIAM J. Comput.*, 42, 2013.