Lattices

Jiazheng Li

Organization: Tsinghua University
Contact: Foreverlasting1202@outlook.com

Contents

1 SVP, CVP, GapSVP, GapCVP 2
1.1 Introduction 2
1.2 Minkowski's Theorem 3
1.3 Lattice and Complexity Theory 4

1 SVP, CVP, GapSVP, GapCVP

1.1 Introduction

Definition 1.1.1 (Lattice)

Given k linearly independent column vector $b_1, ..., b_k \in \mathbb{R}^n$, the lattice generated by them is defined as $\mathcal{L}(b_1, ..., b_k) = \left\{\sum_{i=1}^{k} x_i b_i \mid x_i \in \mathbb{Z}\right\}$. We call $b_1, ..., b_k$ a basis of the lattice, k the rank of the lattice, and n the dimension of the lattice. In the matrix form, given a rank k matrix $B \in \mathbb{R}^{n\times k}$, the lattice of B is defined as

$$\mathcal{L}(B) = \{Bz \mid z \in \mathbb{Z}^k\}.$$

♣

Remark

Linear subspace but with integer indices.

Theorem 1.1.2

$\mathcal{L}(B_1) = \mathcal{L}(B_2)$ if $\exists\, U \in \mathbb{Z}^{k\times k}$ and $\det(U) = \pm 1$ such that $B_1 U = B_2$.

♡

Proof. Notice $U \in \mathbb{Z}^{\{k\times k\}}$ and $U^{-1} = \frac{\text{adj}(U)}{\det(U)}$, then we can prove that $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$ and $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$. □

Definition 1.1.3 (Successive Minima)

Let $\overline{B}_n(0, r)$ be the n-dimensional ball with the origin as the center, i.e.,

$$\overline{B}_n(0, r) = \{x \in \mathbb{R}^n \mid \|x\|_2 \le r\}.$$

We define the i-th successive minima of a lattice $\mathcal{L}$ to be

$$\lambda_i(\mathcal{L}) = \inf\left\{r : \dim\left(\text{span}\left(\mathcal{L} \cap \overline{B}_n(0, r)\right)\right) \ge i\right\}.$$

♣

Remark

The shortest vector under linear independence, with the note that the λ_i may be equal.

Definition 1.1.4 (Fundamental Parallelepiped)

We define the fundamental parallelepiped of a lattice $\mathcal{L}$ generated by a basis $B \in \mathbb{R}^{n\times k}$ to be

$$\mathcal{P}(B) = \left\{\sum_{i=1}^{k} c_i b_i \mid c_i \in [0, 1)\right\}.$$

♣

Definition 1.1.5 (determinant)

We define the determinant of a lattice $\mathcal{L} = \mathcal{L}(b_1, b_2, ..., b_k)$ to be

$$\det(\mathcal{L}) := \text{vol}(\mathcal{P}(B))$$

♣

We then introduce a general theorem for computing the determinant of a lattice.

Theorem 1.1.6

Given $B \in \mathbb{R}^{n\times k}$, we have

$$\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}.$$

Moreover, if $n = k$, we have $\det(\mathcal{L}(B)) = |\det(B)|$.

♡

Proof. Gram Matrix, $\text{vol}(\mathcal{P}(B)) = \sqrt{\det(G)}$, where G denote Gram Matrix and $G_{i,j} = b_i^T b_j$. □

1.2 Minkowski's Theorem

We aim to find some relationship between $\lambda_1(\mathcal{L})$ and $\det(\mathcal{L})$, since $\det(\mathcal{L})$ can be easily computed.

Theorem 1.2.1 (Minkowski's Theorem)

For any lattice $\mathcal{L}$, we have $0 < \lambda_1(\mathcal{L}) \le \sqrt{n}\sqrt[n]{\det(\mathcal{L})}$. (*For simplicity, we consider the* ***full rank*** *case.*)

♡

Remark

Let's understand this theorem. For the lower bound, we can use the lattice $\mathcal{L}\left(\begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}0\\\frac{1}{\alpha}\end{pmatrix}\right)$ when $\alpha \to \infty$ to reach it. ***For the upper bound, I have no idea now.***

Lemma 1.2.2 (Blichfeldt's Theorem)

Given any n-dimensional lattice Land for any set $S \subseteq \mathbb{R}^n$ such that $\text{vol}(S) > \det(\mathcal{L})$, there must exists $x, y \in S$ s.t. $x = y \pmod{\mathcal{L}}$ and $x - y \in \mathcal{L}$.

♡

Proof. Pigeonhole principle. Notice that there must be two points $x, y \in S$ such that $x \pmod{\mathcal{L}} = y \pmod{\mathcal{L}}$ by shifting vectors to $\mathcal{L}$. □

Definition 1.2.3 (Center-symmetric Sets and Convex Sets)

We say a set S is center-symmetric if $\forall x \in S$ we have $-x \in S$. We say S is convex if $\forall x, y \in S, \lambda \in [0, 1]$, we have $\lambda x + (1 - \lambda)y \in S$.

♣

Theorem 1.2.4

Given any n-dimensional lattice $\mathcal{L}$ for any center-symmetric convex set S such that $\mathrm{vol}(S) > 2^n \det(\mathcal{L})$, S contains a non-zero $v \in \mathcal{L}$.

Proof. Construct $2\mathcal{L}$ with $\det(2\mathcal{L}) = 2^n \det(\mathcal{L}) < \mathrm{vol}(S)$, then use Lemma 1.2.2, we can have that there must be two points $x \neq y \in S$ s.t. $x - y \in 2\mathcal{L}$. Since S is convex, $\frac{x-y}{2} \in S$ and S is center-symmetric $\Rightarrow \frac{x-y}{2} \in \mathcal{L}$. □

Proof of Theorem 1.2.1. Now, we can prove Theorem 1.2.1.

Consider a hypercube S_0 with side length $\sqrt[n]{\det(\mathcal{L})}$, and S_1 be the smallest ball containing S_0. Then

$$\forall x, y \in S_1, \|x - y\|_2 \leq \sqrt{n} \sqrt[n]{\det(L)}$$

and

$$\mathrm{vol}(S_1) > \mathrm{vol}(S_0) = \det(\mathcal{L}).$$

Since Lemma 1.2.2, we have $x, y \in S_1$ and $x - y \in \mathcal{L}$, which means there exits a vector $v \in \mathcal{L}$ and $\|v\|_2 \leq \sqrt{n} \sqrt[n]{\det(L)}$, and hence $\lambda_1(\mathcal{L}) \leq \sqrt{n} \sqrt[n]{\det(\mathcal{L})}$. □

Remark

The upper bound is not tight with some constant, since we choose a hypercube to constrict not a hyperball.

A more interesting thing is the order of upper bound can not be improved, because we can prove there exists a global constant $c \in (0, 1)$ such that for all sufficiently large n, there exists an n-dimensional lattice $\mathcal{L}_n$ such that $\lambda_1(\mathcal{L}n) \geq c\sqrt{n} \sqrt[n]{|\det(\mathcal{L}_n)|}$.

1.3 Lattice and Complexity Theory