Contents

Chapter 1

Introduction to Lattice

Definition: Let $b_1, \dots, b_n \in \mathbb{R}^m$ be n linearly independent vectors. The **lattice** generated by these vectors is denoted as $\mathcal{L}(b_1, \dots, b_n)$ and

$$\mathcal{L}(b_1, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \,\middle|\, x_i \in \mathbb{Z} \right\}$$

If we let $B = \begin{bmatrix} b_1 & b_2 & \dots & b_n \end{bmatrix}$, then

$$\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\}$$

If $n = m$, then the lattice is said to be **full rank**. m is the dimension and n is the rank of the lattice.

– the case where $\mathcal{L}(B)$ is not a lattice.

1.1 Description of lattices

1.1.1 Algebraic description

Definition: A matrix $U \in \mathbb{Z}^{n \times n}$ is **unimodular** if $|\det U| = 1$.

Proposition 1.1. *The unimodular matrices form a group under matrix multiplication.*

Proof. Clearly, I is a unimodular matrix and is the identity element of the group. By definition, a unimodular matrix U is invertible and $|\det U^{-1}| = 1$. Also, note that

$$U^{-1} = \frac{1}{\det U} \operatorname{adj}(U)$$

where the adjugate matrix $\operatorname{adj}(U)$ is an integer matrix. Thus, $U^{-1} \in \mathbb{Z}^n$. The associativity follows from the associativity of matrix multiplication. ∎

Theorem 1.2. *Two full rank matrix $B, B' \in \mathbb{R}^n$ produce the same lattice if and only if there exists a unimodular matrix U such that $B' = BU$.*

1.1.2 Geometric description

Definition: Suppose $b_1, \ldots, b_n \in \mathbb{R}^m$ are linearly independent. The **fundamental parallelopiped** of these vectors is

$$\mathcal{P}(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \,\middle|\, x_i \in [0, 1[\right\}$$

Theorem 1.3. *Suppose Λ is a full rank n-dimensional lattice and $b_1, \ldots, b_n \in \mathbb{R}^n$ are linearly independent vectors in Λ. Then $b_1, \ldots, b_n$ are a basis for Λ if and only if*

$$\Lambda \cap \mathcal{P}(b_1, \ldots, b_n) = \{0\}$$

1.2 Determinant of lattice

Definition: Let Λ be a lattice generated basis B. The **determinant** of Λ is the volume of fundamental parallelopiped of B.

$$\det \Lambda = \operatorname{vol}(\mathcal{P}(B))$$

It can be shown that $\operatorname{vol}(\mathcal{P}(B)) = \sqrt{\det B^T B}$. To show that this definition is well-defined, we must prove that for any basis two B, B', the volumes of fundamental parallelopipeds are equal. Since, B and B' generate the same lattice, by 1.2, there exists a unimodular matrix U such that $B' = BU$.

$$\begin{aligned}
\operatorname{vol}(\mathcal{P}(B')) &= \sqrt{\det B'^T B'} \\
&= \sqrt{\det (BU)^T BU} \\
&= \sqrt{\det U^T B^T BU} \\
&= \sqrt{\det U^T \det B^T B \det U} \\
&= \sqrt{(\det U)^2 \det B^T B} \\
&= \sqrt{\det B^T B} = \operatorname{vol}(\mathcal{P}(B))
\end{aligned}$$

which was what was wanted.

Intuitively, the $\det \Lambda$ is inversely proportional to its density.

Remark 1. In mathematical analysis, the volume – or length or area – of a set is measured with *measures*. The exact definition of a measure is beyond the scope this text, however, we will almost always use the *lebesgue measure*, unless stated otherwise. Measures can be defined on any set, and hence the measure of set may not depend on a particular metric. As a result, we are able to consider the same space with the same measure under different metrics or norms without affecting the measure.

1.3 Gram-Schmidt

In Gram-Schmidt procedure, a set of linearly independent vectors $b_1, \ldots, b_n$ are transformed into a set of orthogonal vectors $b_1^*, \ldots, b_n^*$.

$$b_i^* = b_i - \sum_{j=1}^{i-1} \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^* = b_i - \sum_{j=1}^{i-1} u_{i,j} b_j^*$$

with $b_1^* = b_1$.

Proposition 1.4.

1. *For all* $i \neq j$, $\langle b_i^*, b_j^* \rangle = 0$.

2. *For all* $i > j$, $\langle b_i^*, b_j \rangle = 0$.

3. *For all* i, $\operatorname{span}\{b_1, \ldots, b_i\} = \operatorname{span}\{b_1^*, \ldots, b_i^*\}$.

4. *If* $B = \begin{bmatrix} b_1 & \ldots & b_n \end{bmatrix}$ *and* $B^* = \begin{bmatrix} b_1^* & \ldots & b_n^* \end{bmatrix}$, *then*

$$B = B^* \begin{bmatrix} 1 & u_{2,1} & \ldots & u_{n,1} \\ 0 & 1 & \ldots & u_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}$$

Lemma 1.5. *If we apply the Gram-Schmidt procedure to* $B \in \mathbb{R}^{m \times n}$ *and get* $B^* \in \mathbb{R}^{m \times n}$, *then*

$$\det B^T B = \prod_{i=1}^{n} \|b_i^*\|^2$$

Proof. Note that,

$$B^* \begin{bmatrix} 1 & u_{2,1} & \ldots & u_{n,1} \\ 0 & 1 & \ldots & u_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix} = \begin{bmatrix} \frac{b_1^*}{\|b_1^*\|} & \ldots & \frac{b_1^*}{\|b_n^*\|} \end{bmatrix} \begin{bmatrix} \|b_1^*\| & u_{2,1}\|b_1^*\| & \ldots & u_{n,1}\|b_1^*\| \\ 0 & \|b_2^*\| & \ldots & u_{n,2}\|b_2^*\| \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \|b_n^*\| \end{bmatrix}$$

Let $B^{*'}$ be the orthonormal Gram-Schmidt matrix as calculated above and U' its corresponding upper triangular matrix.

$$\begin{aligned} \det B^T B &= \det\big((B^* U)^T B^* U\big) \\ &= \det\Big((U')^T (B^{*'})^T B^{*'} U'\Big) \\ &= \det U' \det (B^{*'})^T B^{*'} \det U' \\ &= \prod_{i=1}^{n} \|b_i^*\|^2 \det (B^{*'})^T B^{*'} \end{aligned}$$

Behold, the columns of $B^{*'}$ are orthonormal therefore, $(B^{*'})^T B^{*'} = I_n$ and hence

$$\det B^T B = \prod_{i=1}^{n} \|b_i^*\|^2$$

which was what was wanted. ∎

1.4 Successive Minima

Let $\lambda_i(\Lambda)$ be the minimum norm of the longest vector among any set i linearly independent vectors in Λ.

$$\lambda_i(\Lambda) = \min_{\substack{\{y_1,\ldots,y_i\} \\ \text{lin indp}}} \max_{1\le j\le i} \|y_j\|$$

or equivalently

$$\lambda_i(\Lambda) = \inf\{r \mid \dim \operatorname{span}(\Lambda \cap B_r(0)) \ge i\}$$

Theorem 1.6. *Let Λ be a littice of rank n with successive minima $\lambda_1(\Lambda), \ldots, \lambda_n(\Lambda)$. There exists a set of linearly independent vectors $v_1, \ldots, v_n \in \Lambda$ such that $\|v_i\| = \lambda_i(\Lambda)$.*

1.4.1 Lower bound on λ_1

Theorem 1.7. *Let $\mathcal{L}(B)$ be a lattice, then*

$$\lambda_1(\mathcal{L}(B)) \ge \min_j \left\|b_j^*\right\|$$

and more generally

$$\lambda_i(\mathcal{L}(B)) \ge \min)j \ge i \left\|b_j^*\right\|$$

Proof. Let $x \in \mathbb{Z}^n$, we will show that $\|Bx\| \ge \min_j \left\|b_j^*\right\|$ for all $x \in \mathbb{Z}^n$. Note that, for any i we have

$$|\langle Bx, b_i^*\rangle| = \left|\sum_{j=1}^{n} x_j \langle b_j, b_i^*\rangle\right| = \left|\sum_{j=i}^{n} x_j \langle b_j, b_i^*\rangle\right|$$

Let i be the largest indext that $x_i \neq 0$. That is, for all $j > i$, $x_j = 0$. Thus

$$|\langle Bx, b_i^*\rangle| = |x_i \langle b_i, b_i^*\rangle| = |x_i| \|b_i^*\|^2 \le \|b_i^*\|^2$$

Moreover, by Cauchy-Schwarz inequality

$$|\langle Bx, b_i^*\rangle| \le \|Bx\| \|b_i^*\|$$

ans hence

$$\|Bx\| \ge \|b_i^*\| \ge \min_j \left\|b_j^*\right\|$$

which was what was wanted. ■

Corollary 1.8. *For all lattices Λ, there exists a constant $\epsilon(\Lambda) > 0$ such that for all $x, y \in \Lambda$ we have*

$$\|x - y\| \ge \epsilon(\Lambda)$$

Proof. Note that $x - y \in \Lambda$ then, let $\epsilon(\Lambda) = \lambda_1(\Lambda)$. ■

Theorem 1.9. *A set $\Lambda \subset \mathbb{R}^m$ is a lattice if and only if it is a discrete additive subgroup of $\mathbb{R}^m$.*

1.5 Minkowski's Theorems

Theorem 1.10 (Blichfeld theorem). *For any Λ and for any measurable set $S \subset \operatorname{span} \Lambda$, if S has a volume $\operatorname{vol}(S) > \det \Lambda$, then there exists two distinct points $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.*

Theorem 1.11 (Convex body theorem). *For any lattice Λ of rank n and any convext set $S \subset \operatorname{span} \Lambda$ symmetric about the origin, if $\operatorname{vol}(S) > 2^n \det \Lambda$, then S contains a non-zero lattice point.*

Theorem 1.12 (Minkowski's first theorem). *For any lattice Λ,*

$$\lambda_1(\Lambda) \leq \sqrt{n}(\det \Lambda)^{\frac{1}{n}}$$

Theorem 1.13 (Minkowski's second theorem). *For any lattice Λ of rank n under the l_2 norm*

$$\left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right)^{\frac{1}{n}} \leq \sqrt{n}(\det \Lambda)^{\frac{1}{n}}$$

tightness of Minkowski's upper bounds.

1.6 Dual lattice

Definition: The **dual lattice** or **reciprocal lattice** of Λ, denoted by Λ^* is defined as

$$\Lambda^* = \{x \in \operatorname{span} \Lambda \mid \forall y \in \Lambda, \langle x, y \rangle \in \mathbb{Z}\}$$

we can find $U = \begin{bmatrix} u_1 & \dots & u_n \end{bmatrix}$ such that $Uv_i = e_i$ by setting $U = V(V^TV)^{-1}$. If $\Lambda^* = \Lambda$, the lattice is called **self-dual**.

Proposition 1.14.

1. $(k\mathbb{Z}^n)^* = \frac{1}{k}\mathbb{Z}^n$.
2. $(\Lambda^*)^* = \Lambda$.
3. *Λ^* is a lattice and has rank n.*
4. *If B is a basis for Λ, then there exists a unique D corresponding to B such that D is a basis for Λ^* and*
   - *(a)* $\operatorname{span} D = \operatorname{span} B$.
   - *(b)* $B^T D = I$.
5. $\det \Lambda^* = \frac{1}{\det \Lambda}$.

1.7 Computational problems

Definition (Shortest vector problem): Given a basis $B \in \mathbb{Z}^{m \times n}$ find a non-zero lattice vector Bx such that $\|Bx\| \leq \|By\|$ for any other vector $y \in \mathbb{Z}^n \backslash \{0\}$

1.8 Complexity theory

A Turing machine rnus in time $t(n)$ if for all string w of size $|w| = n$, the turing machine halts in at most $t(n)$ steps. If $t(n) = a + n^b$ for some constants a, b, we say that the turing machine runs in **polynomial time**. The class of decision problems that can be solved by a deterministic turing machine in polynomial time is denoted by **P**. The class of decision problems that can be solved by a non-deterministic turing machine in polynomial time is denoted by **NP**. The **NP** class can also be characterized by the class of languages L such that there exists a relation $R \subset \Sigma^* \times \Sigma^*$ such that $(x, y) \in R$ can be checked in polynomial time in $|x|$ and $x \in L$ if and only if there exists a y that $(x, y) \in R$. Then, y is called the **NP**-witness of x.

The language A reduces to B if there exists a polynomial time computable function $f : \Sigma^* \to \Sigma^*$ such that $x \in A$ if and only if $f(x) \in B$, denoted by $A \mapsto B$, and it is called the **Karp reduction**. A is **NP-hard** if for all $B \in$ **NP**, $B \mapsto A$. A is **NP-complete** if A is **NP-hard** and $A \in$ **NP**.

Similarly, for **Cook reduction**, the language A reduces to B if there exists a polynomial time turing machine with access to an oracle that solves B that solves A.

1.9 Some lattice problems

Definition (Closest vector problem): Given $B \in \mathbb{Z}^{m\times n}$ and a target vector $t \in \mathbb{Z}^m$ find $Bx \in \mathbb{Z}^m$ such that $\|Bx - t\| \leq \|By - t\|$ for all $y \in \mathbb{Z}^n \backslash \{0\}$. There other variants to this problem.

Search find $Bx \in \mathbb{Z}^m$ such that $\|Bx - t\|$ is minimized.

Optimization Find the minimum of $\|Bx - t\|$.

Decision Given a rational number $r > 0$, decide if there exists x with $\|x - t\| < r$.

Note that the decision problem reduces to optimization problem which itself reduces to search problem.

– the reation of λ_i to each other.

Definition (Approximate SVP): Given a constant γ, find a non-zero vector Bx such that $\|Bx\| \leq \gamma\|By\|$ for all $y \in \mathbb{Z}^n \backslash \{0\}$.

Approximate CVP is defined similarly.

A list of polynomial time lattice problmes.

1. Membership: Given B and x, decide whether $x \in \mathcal{L}(B)$.
2. Kernel: Given $A \in \mathbb{Z}^{m\times n}$ find the a basis for $\Lambda = \{x \in \mathbb{Z}^n \mid Ax = 0\}$.
3. Kernel-mod: Given $A \in \mathbb{Z}_M^{m\times n}$ find the a basis for $\Lambda = \{x \in \mathbb{Z}^n \mid Ax = 0 \mod M\}$.
4. Basis: Given vectors $b_1, \ldots, b_n$ find a basis for the lattice generated by $b_1, \ldots, b_n$. It is done by *normal Hermitian form*, H. H is the worst basis.
5. Union: Given bases $B_1, B_2 \in \mathbb{Z}^{m\times n}$, find a basis for $\mathcal{L}(B_1) \cup \mathcal{L}(B_2)$.

6. Dual: Find a basis for the dual lattice.
7. Intersection: Given bases $B_1, B_2 \in \mathbb{Z}^{m\times n}$, find a basis for $\mathcal{L}(B_1) \cap \mathcal{L}(B_2)$.
8. Equivalence: Given bases $B_1, B_2 \in \mathbb{Z}^{m\times n}$, determine whether $\mathcal{L}(B_1) = \mathcal{L}(B_2)$.
9. Cyclic: Determine whether the lattice Λ is cyclic. The lattice Λ is cyclic if for all $x \in \Lambda$, all cyclic permutations of coordinates of x are in Λ as well.

1.10 Hardness of approximation

Definition: The promise is a pair (Π_{yes}, Π_{no}) with $\Pi_{yes}, \Pi_{no} \subset \Sigma^*$ and $\Pi_{yes} \cap \Pi_{no} = \emptyset$.

Definition: An algorithm or turing machine solves a promise (Π_{yes}, Π_{no}) if for all $w \in \Pi_{yes} \cup \Pi_{no}$, it can determine whether $w \in \Pi_{yes}$ or $w \in \Pi_{no}$.

Definition: The $GAPSVP_\gamma$ is a promise defined as follows:

$$\begin{aligned}\Pi_{yes} &= \left\{(B,r) \,\middle|\, B \text{ is a basis}, B \in \mathbb{Z}^{m\times n}, r \in \mathbb{Q},\ \text{and there exists } z \in \mathbb{Z}^n \backslash \{0\} \text{ s.t. } \|Bz\| < r\right\}\\ \Pi_{no} &= \left\{(B,r) \,\middle|\, B \text{ is a basis}, B \in \mathbb{Z}^{m\times n}, r \in \mathbb{Q},\ \text{and for all } z \in \mathbb{Z}^n \backslash \{0\} \text{ s.t. } \|Bz\| > \gamma r\right\}\end{aligned}$$

The $GAPCVP_\gamma$ is a promise defined as follows:

$$\begin{aligned}\Pi_{yes} &= \left\{(B,t,r) \,\middle|\, B \text{ is a basis}, B \in \mathbb{Z}^{m\times n}, t \in \mathbb{Z}^m, r \in \mathbb{Q}, \exists z \in \mathbb{Z}^n \backslash \{0\}, \|Bz - t\| < r\right\}\\ \Pi_{no} &= \left\{(B,t,r) \,\middle|\, B \text{ is a basis}, B \in \mathbb{Z}^{m\times n}, t \in \mathbb{Z}^m, r \in \mathbb{Q}, \forall z \in \mathbb{Z}^n \backslash \{0\}, \|Bz - t\| > \gamma r\right\}\end{aligned}$$

Theorem 1.15. *$GAPSVP_\gamma \mapsto APPROXSVP_\gamma$. $APPROXSVP_\gamma \mapsto GAPSVP_\gamma$ and*

Definition: A promise (Π_{yes}, Π_{no}) is in **NP** when there exists a relation $R \subset \Sigma^* \times \Sigma^*$ such that for all $x \in \Pi_{yes}$ there exists y such that $(x, y) \in R$ and for all $x \in \Pi_{no}$ for all y, $(x, y) \notin R$.

Definition: Suppose $f : \Sigma^* \to \Sigma^*$ is computable in polynomial time. A reduction from (Π_{yes}, Π_{no}) to (Π'_{yes}, Π'_{no}) when

$$f(\Pi_{yes}) \subset \Pi'_{yes} \text{ and } f(\Pi_{no}) \subset \Pi'_{no}$$

Definition: **NP-hard**, **NP-complete** for promises.