# Lattices and LLL

Lecturer: Santosh Vempala  Scribe: Digvijay Boob

## 1 Lattice

A lattice can be defined in following two ways:

**Definition 1.1 (Lattice).** *A lattice $L \subseteq R^n$ is a discrete additive set. A set $L$ is*

- ***discrete*** *if $\forall x \in L, \exists\ \delta > 0$ such that $B(x, \delta) \cap L = \{x\}$;*
- ***additive*** *if $x, y \in L \Rightarrow x + y, x - y \in L$;*

**Definition 1.2 (Lattice).** *A lattice is the set of all integer linear combinations of set of vectors.*

**Definition 1.3 (Basis of Lattice).** *A **basis** for $L$ is a list $B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \in \mathbb{R}^{n \times n}$ of linearly independent vectors such that $L = L(B) = \{x.B | x \in \mathbb{Z}^n\}$. Typically, $B \in Q^{n \times n}$ or even $\mathbb{Z}^{n \times n}$. (We can define m-dimensional $L \subseteq R^n$ for $m < n$, but we can reduce this to the full-dimensional case).*

For rest of the discussion, $K$ is a centrally symmetric convex set.

**Theorem 1.1.** *$vol(K) \geq 2^n \Rightarrow K$ contains an integer point*

**Proof.** Let $tK := \{tX : X \in K\}$. At every $y \in \mathbb{Z}^n$, we place a copy of $\frac{1}{2}K$. Notice that $vol(\frac{1}{2}K) \geq 1$. Since this is standard integer lattice

$$\exists y_1, y_2 \in \mathbb{Z}^n \text{ s.t. } \{y_1 + \tfrac{1}{2}K\} \cap \{y_2 + \tfrac{1}{2}K\} \neq \phi$$

This is because maximum volume you can pack around every integer point without having an intersection is exactly a unit hypercube centred at that integer point.

$$\{y_1 + \frac{1}{2}K\} \cap \{y_2 + \frac{1}{2}K\} \neq \phi \Rightarrow \{\frac{1}{2}K\} \cap \{y_2 - y_1 + \frac{1}{2}K\} \neq \phi$$

Let $z := y_2 - y_1$ and $w \in \{\frac{1}{2}K\} \cap \{z + \frac{1}{2}K\}$, then we have $w \in \frac{1}{2}K$ as well as $w - z \in \frac{1}{2}K$ but since $K$ is centrally symmetric we have $z - w \in \frac{1}{2}K$. By convexity of set $K$, we get $\frac{1}{2}w + \frac{1}{2}(z - w) = \frac{1}{2}z \in \frac{1}{2}K \Rightarrow z \in K$ but notice that $z$ is an integral point. □

**Definition 1.4.** $\Lambda_1(K) := \{t : tK$ *contains a non-zero integral point*$\}$

**Theorem 1.2.** $\Lambda_1(K) \leq 2vol(K)^{-\frac{1}{n}}$

**Proof.** Let $tK$ contains a non-zero integral point. Then $vol(tK) = t^n vol(K)$. Using Theorem 1.1, we get that

$$t^n vol(K) = 2^n \Rightarrow t = 2vol(K)^{-\frac{1}{n}}$$

So we get $\Lambda_1(K) \leq 2vol(K)^{-\frac{1}{n}}$ □

We can think of $\Lambda$ as distance measure defined on centrally symmetric convex body, $K$. Value $\Lambda$ signifies the minimum dilation of $K$ is required to the given point whose distance measure is under consideration. A specific case is when $K$ is a unit ball, distance measure in that case is 2-norm.

**Definition 1.5.** $\Lambda_i(K) := \{t : tK \textit{ contains } i \textit{ linearly independent integral points}\}$

**Theorem 1.3.** $\Lambda_1(K) \dots \Lambda_n(K) \leq \frac{2^n}{vol(K)}$

Let $\mathcal{L}(b_1, \dots, b_n) = A\mathbb{Z}^n$, $A$ is linear transformation mapping standard integer lattice to lattice formed by basis $(b_1, \dots, b_n)$. So $rank(A) = n$.

**Definition 1.6.** $\Lambda_1(\mathcal{L}, K) := min\{t : tK \cap \mathcal{L} \setminus \{0\} \neq \phi\}$

Notice that $\Lambda_1(\mathcal{L}, B^n)$ = Shortest nonzero vector in $\mathcal{L}$ (SVP), where $B^n$ is n-dimensional euclidean ball.

**Theorem 1.4 (Minkowski's first theorem).** $\Lambda_1(\mathcal{L}, K) \leq 2\left(\frac{det(A)}{vol(K)}\right)^{\frac{1}{n}}$

**Proof.** Notice that since $A$ is invertible matrix, we have that

$$\begin{aligned} \mathcal{L} \cap tK \neq \phi &\Leftrightarrow A^{-1}\mathcal{L} \cap tA^{-1}K \neq \phi \\ &\Leftrightarrow \mathbb{Z}^n \cap tA^{-1}K \neq \phi \end{aligned}$$

$vol(A^{-1}K) = \frac{vol(K)}{det(A)}$
Now applying theorem 1.2, we get minimum value of $t$ is $\Lambda_1(A^{-1}K) \Rightarrow \Lambda_1(\mathcal{L}, K) \leq 2\left(\frac{det(A)}{vol(K)}\right)^{\frac{1}{n}}$ □

**Theorem 1.5 (Minkowski's second theorem).** $\Lambda_1(\mathcal{L}, K) \dots \Lambda_n(\mathcal{L}, K) \leq \frac{2^n det(A)}{vol(K)}$

**Proof.** Using the same argument as in the previous proof, we replace $vol(K)$ in theorem 1.3 by $\frac{vol(K)}{det(A)}$ to get the required result. □

**Claim 1.6.** *If columns of matrix $B$ are basis of full dimensional lattice $\mathcal{L}(B)$ then $\forall$ $U$ unimodular, $\mathcal{L}(BU) = \mathcal{L}(B)$*

**Proof.** Since U is unimodular matrix, columns of $BU$ are formed by elementary (unimodular) columns transformation of columns of $B$. So any lattice point in $\mathcal{L}(BU)$ can be written as integral combination of columns of $B$. So we get $\mathcal{L}(BU) \subseteq \mathcal{L}(B)$.
Now $B = (BU)U^{-1}$. Clearly $U^{-1}$ is integral matrix as all entries of $adj(U)$ are integral and $|det(U)| = 1$. So we get columns of $B$ are elementary columns operations on columns of $BU$. so every point in $B$ can be written as integral combination of columns in $BU \Rightarrow \mathcal{L}(B) \subseteq \mathcal{L}(BU)$ □

# 2 Diophantine Approximations

**Theorem 2.1 (Dirichlet's Approximation theorem).** *Given real numbers $\alpha_1, \ldots, \alpha_n$ and $\epsilon > 0$, there are $p_1, \ldots, p_n, Q \in \mathbb{Z}$ and $Q \leq \epsilon^{-n}$ s.t. $|p_i - \alpha_i q| \leq \epsilon$ and $|q| \leq Q$*

**Proof.** We have that
$-\epsilon \leq p_i - \alpha_i q \leq \epsilon, \forall\ i = 1, \ldots, n$ and $\frac{\epsilon}{Q}|q| \leq \epsilon$
We can write this in matrix form as

$$\epsilon e \leq \begin{bmatrix} I & -\alpha \\ \mathbf{0} & \epsilon/Q \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} \leq \epsilon e$$

where $\alpha = [\alpha_1, \ldots, \alpha_n]^T$ and $e$ is vector of all 1. Lets call the matrix in the above eq as A. So we get that $\mathcal{K} := \|Ax\|_\infty \leq \epsilon$ must have at least one integer solution. Clearly $\mathcal{K}$ is centrally symmetric convex set. So from Minkowski's first theorem, we get that $vol(\mathcal{K}) \geq 2^{n+1}$ for it to have an integer solution. So we get that $vol(\mathcal{K}) = \frac{(2\epsilon)^{n+1}}{|det(A)|} \geq 2^{n+1}$ But $|det(A)| = \epsilon/Q$ So the least value of Q we need to get an integral solution is $\epsilon^{-n}$. □

# 3 Gauss's 2D basis reduction algorithm

**Input:** $b_1, b_2$. Without loss of generality, $\|b_2\| \geq \|b_1\|$

1. Find $m \in \mathbb{Z}$ s.t. $\|b_2 - mb_1\|$ is minimised. ($m$ is closest integer to $\frac{b_2.b_1}{\|b_1\|}$). Let $b_2' = b_2 - mb_1$
2. If $\|b_2'\| \geq (1-\epsilon)\|b_1\|$ then STOP. Else swap between $b_1, b_2'$ and repeat.

**Lemma 3.1.** *At the end of this algorithm, we have $\|b_2^*\| \geq \sqrt{\left((1-\epsilon)^2 - \frac{1}{4}\right)}\|b_1^*\|$*

**Proof.** When we stop the angle between $b_1$ and $b_2$ must be $\geq \frac{\pi}{3}$ otherwise we can do the reduction once more which will reduce the length of longer vector. So we have that

$$\|b_2\| \geq (1-\epsilon)\|b_1\| \text{ and } |b_2.b_1| \leq \frac{b_1.b_1}{2}$$

$$\Rightarrow \|b_2^*\| \geq \sqrt{\left((1-\epsilon)^2 - \frac{1}{4}\right)}\|b_1^*\|$$

□

Since, in every iteration the length of shortest vector is reduced by a constant factor of $(1-\epsilon)$. So number of iterations is $O(\frac{1}{\epsilon}\log(\|b_1\|)$ where $\|b_1\|$ is the length of initial vector.

# 4 LLL

In LLL algorithm, we use Gauss' 2-D algorithm along with the property that $\|b^*_{i+1}\| \geq \delta\|b^*_i\|$. The algorithm is as follows:

1. Compute $b^*_1, \ldots, b^*_n$
2. If there is an $i$ s.t. $\|b^*_{i+1}\| < \delta\|b_i\|$, define $x, y$ as projections of these vectors to space orthogonal to $V_{i-1} = span\{b_1, \ldots, b_{i-1}\}$. Apply Gauss' 2D-algorithm with parameter $\epsilon$ to $x$ and $y$ to get vector $u$ and $v$. Let $U$ be the unimodular matrix obtained in this basis reduction using elementary operation i.e.

$$U \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$$

3. set

$$\begin{bmatrix} b_i \\ b_{i+1} \end{bmatrix} = U \begin{bmatrix} b_i \\ b_{i+1} \end{bmatrix}$$

4. Repeat 1,2,3 as long as possible.

**Theorem 4.1 (LLL [1]).** *The basis reduction procedure applied with parameters $\delta \in \left(0, \frac{\sqrt{3}}{2}\right)$ and $\epsilon$ s.t. $\delta^2 < (1-\epsilon)^2 - \frac{1}{4}$, to a given starting basis of any lattice, $L$, results in a basis $b_1, \ldots, b_n$ s.t.*

1. $\|b_1\| \leq \delta^{-n}\Lambda_1(L)$
2. $\|b_1\|\|b_2\| \ldots \|b_n\| \leq \delta^{-n^2}\|b^*_1\|\|b^*_2\| \ldots \|b^*_n\|$

**Proof.** We know that at the end of the algorithm, $\|b^*_{i+1}\| \geq \delta\|b^*_i\|, \forall\ i = 1, \ldots, n-1$. So we get that $\|b^*_j\| \geq \delta^{j-1}\|b_1\|$. Let v be the shortest vector in L. Then $v = \sum_{i=1}^{n} \lambda_i b^*_i$. So

$\Lambda_1 = \|v\| \geq \sum_{i=1}^{n} |\lambda_i$

$|b^*_i\| \geq \|b^*_n\| \geq \delta^{n-1}\|b^*_1\|$. So we get $\|b^*_1\| \leq \frac{1}{\delta^n}\Lambda_1$

Suppose at the end of LLL we have reduced basis $b_1, \ldots, b_n$. Component of $b_i$ in $V_{i-1} = b_i - b^*_i = \sum_{j=1}^{i-1} \alpha_j b^*_j$ where each $|\alpha_j| \leq \frac{1}{2}$ as we have a reduced basis. So $\|b_i\| \leq \|b^*_i\| + \sum_{j=1}^{i-1} |\alpha_j|.\|b^*_j\| \leq \|b^*_i\|\left(1 + \frac{1}{2}\sum_{j=1}^{i-1}\left(\frac{1}{\delta}\right)^{i-j}\right) \leq \left(\frac{1}{\delta}\right)^n \|b^*_i\|$. So we get that orthogonality defect

$$:= \frac{\prod_{i=1}^{n} \|b_i\|}{\prod_{i=1}^{n} \|b^*_i\|} \leq \delta^{-n}$$

□

**Theorem 4.2.** *Number of iteration in LLL algorithm is polynomial*

**Proof.** Suppose we have $b_i, b_{i+1}$ at the start of some iteration which are reduced into $\widehat{b}_i, \widehat{b}_{i+1}$ at the end of iteration. We know that $\|b_i^*\|.\|b_{i+1}^*\| = \|\widehat{b}_i^*\|.\|\widehat{b}_{i+1}^*\|$. Also, since it was needed to reduce this pair implies $b_{i+1}^* < \delta b_i^*$. At the end of iteration, we have output of 2-D gauss algorithm. So we know that $\|\widehat{b}_{i+1}^*\| \geq \sqrt{(1-\epsilon)^2 - \frac{1}{4}}.\|\widehat{b}_i^*\|$. So using these three inequalities we get,

$$\delta\|b_i^*\|^2 > \|b_i^*\|.\|b_{i+1}^*\| = \|\widehat{b}_i^*\|.\|\widehat{b}_{i+1}^*\| \geq \sqrt{(1-\epsilon)^2 - \frac{1}{4}}.\|\widehat{b}_i^*\|$$

$$\Rightarrow \frac{\|b_i^*\|}{\|\widehat{b}_i^*\|} > \sqrt{\frac{\sqrt{(1-\epsilon)^2 - \frac{1}{4}}}{\delta}}$$

So look at the quantity

$$\frac{\prod_{i=1}^{n} \|\widehat{b}_i^*\|^{n-i}}{\prod_{i=1}^{n} \|b_i^*\|^{n-i}} = \frac{\|\widehat{b}_i^*\|^{n-i}\|\widehat{b}_{i+1}^*\|^{n-i-1}}{\|b_i^*\|^{n-i}\|b_{i+1}^*\|^{n-i-1}} = \frac{\|\widehat{b}_i^*\|}{\|b_i^*\|} < \sqrt{\frac{\delta}{\sqrt{(1-\epsilon)^2 - \frac{1}{4}}}}$$

This is a constant fraction change in each iteration. So number of iteration is $O(\log\{\|b_1\|^{n^2}\})$
□

**Definition 4.1.** *The covering radius of a lattice $\mathcal{L}$ with respect to a convex body $\mathcal{K}$ is* $\mu(\mathcal{K}, \mathcal{L}) = min\{t : t\mathcal{K} + \mathcal{L} = \mathbb{R}^n\}$

**Definition 4.2.** *The dual of convex body $\mathcal{K} \subset \mathbb{R}^n$ is defined as*

$$\mathcal{K}^* = \{x \subset \mathbb{R}^n : x.y \leq 1, \forall\ y \in \mathcal{K}\}$$

**Definition 4.3.** *The dual lattice of $\mathcal{L}$ is*

$$\mathcal{L}^* = \{x \in span(\mathcal{L}) : x.y \in \mathbb{Z}, \forall y \in \mathcal{L}\}$$

**Theorem 4.3 (transference).** *For any lattice $\mathcal{L}$ and convex body $\mathcal{K}$ both in $\mathbb{R}^n$,*

$$\mu(\mathcal{K}, \mathcal{L})\Lambda_1((\mathcal{K} - \mathcal{K})^*, \mathcal{L}^*) \leq Cn^{4/3}\log(n)$$

**Theorem 4.4 (Integer Programming [2]).** *Integer Linear Programming can be solved in time $n^{O(n)}$ times a polynomial in the input size.*

# References


[1] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534.

[2] R. Kannan. Algorithmic geometry of numbers. *Annual reviews of computer science*, 2:231–267, 1987.