Into Minkowski Realm

Debadatta Kar
Cryptography Research Lab
Indian Institute of Science Education and Research Bhopal

July 10, 2025

Lecture 2

1 Introduction

The ambient space $\mathbb{R}^n$, which is a vector space, is where the additive subgroup named lattice stays. Any vector in the lattice is a vector in the space $\mathbb{R}^n$. However, when we take any vector in $\mathbb{R}^n$, it may be or may not be in the lattice $\mathcal{L}$. We are equipped with some strong mathematical tools that help us to cleverly look at some problems.

2 Successive Minima

A general question to ask in lattice is, what is the shortest of all the vectors in the lattice? Such a vector is called the short vector. This notion of shortness comes from the length of the vector. The shortest vector need not be unique. There can be exponentially many short vectors.
The space $\mathbb{R}^m$ and $\mathcal{L}$ are equipped with the following norms, and the Euclidean norm is what we will be using most of the time.

- l_2 or Euclidean norm
$$||x||_2 = \sqrt{\sum_{i=1}^{n} x_i^2}$$
- l_1 norm
$$||x||_1 = \sum_{i=1}^{n} |x_i|$$
- l_∞ norm
$$||x||_\infty = \max_{1 \le i \le n} \{|x_i|\}$$

The shortest non-zero vector in the lattice is called the first successive minima and often denoted as $\lambda_1(\mathcal{L})$. Now, a natural question is to ask, what is the length of this short vector? can we find a region where this vector can be trapped inside? Or can we say that the vector cannot be smaller than some length l? These questions bring us to the theorems stated as Minkowski's theorem.
Before that, lets see a bound for the λ_1

Theorem 2.1. *Let B be a rank-n lattice basis, and B^* be its Gram-Schmidt orthogonalisation, then*
$$\lambda_1(B) \ge \min_{1 \le i \le n} \{||b_j^*||\}$$

Proof. Let $x \in \mathbb{Z}^n$ be any non-zero integer vector.
By definition of lattice, we have $Bx \in \mathcal{L}$
If B is the lattice basis then consider the Gram-Schmidt orthonormal basis B^*
Now compute, $|\langle Bx, b_j^* \rangle| = |\langle \sum_{i=1}^n x_i b_i, b_i^* \rangle| = |\sum_{i=1}^n x_i \langle b_i, b_i^* \rangle|$.
Now, the vectors from the Gram-Schmidt process give us the relation $\langle b_i, b_j^* \rangle = 0 \ \forall i < j$. Moreover, let's take the scenario where i denotes the maximum index for which x_i is non-zero. This is a general case that will give us
$|\langle Bx, b_j^* \rangle| = |x_j| ||b_j^*||^2$
Applying Cauchy schwartz we will obtain

$$||Bx|| \cdot ||b_j^*|| \geq |x_j| ||b_j^*||^2$$

Further implications gives,

$$||Bx|| \geq |x_j| ||b_j^*|| \geq \min_{1 \leq i \leq n} \{||b_j^*||\}$$

Finally, we obtain,

$$\lambda_1(B) \geq \min_{1 \leq i \leq n} \{||b_j^*||\} \tag{1}$$

This gives us the lower bound for the short vector λ_1 of the lattice $\mathcal{L}$. □

We can also talk about second minima, third minima and so on. It can be defined as

$$\lambda_i = inf \{t | B(0,r) \cap \mathcal{L} \text{ contaions atleast } i \text{ linearly independent short vectors}\}$$

3 Into Minkowski's Realm

The general intuition about the density of lattice points is that

$$\det(\mathcal{L}) \propto \frac{1}{\text{density}}$$

So we should be able to find a bound for λ_1 in terms of $\det(\mathcal{L})$. This is trivial that $\lambda_1 \leq \det(\mathcal{L})$. That looks nice until we scale the lattice vectors by a factor k. That is $\mathcal{L}' = k\mathcal{L}$.
This gives

$$\det(\mathcal{L}') = k^n \det(\mathcal{L})$$

Which gives an exponential bound that we are trying to avoid.
To solve this problem, Minkowski's theorem comes into the picture. We will now state and prove the theorems given by Minkowski.

Theorem 3.1. *(**Blichfield**) For a full rank lattice $\mathcal{L}$ and a measurable set $S \subseteq \mathbb{R}^n$ such that $vol(S) > \det(\mathcal{L})$ there exist $x, y \in S$ such that $x - y \in \mathcal{L}$*

Proof. Let B be a basis for the lattice $\mathcal{L}$. Define a map $f : \mathbb{R}^n \to \mathcal{P}(B)$ as:

$$f\left(\sum x_i b_i\right) = \sum (x_i - \lfloor x_i \rfloor) b_i$$

Observe that

$$\sum x_i b_i - f(\sum x_i b_i) = \sum x_i b_i - (\sum (x_i - \lfloor x_i \rfloor) b_i) = \lfloor x_i \rfloor b_i \in \mathcal{L}$$

Given two points $x, y \in S$ two cases arises
case I: $f(x) = f(y)$
Now,

$$x - y = x - y - 0 = x - y - (f(x) - f(y))$$

On rearranging, we get,

$$x - y = x - y - (f(x) - f(y)) = (x - f(x)) - (y - f(y))$$

Finally,

$$x - y = (x - f(x)) - (y - f(y))$$

Both the blue and red are in lattice $\mathcal{L}$, so is their difference.
This shows $x - y \in \mathcal{L}$
case II: $f(x) \neq f(y)$
Let's for now assume this to be true for this case as well. □

Theorem 3.2. *(**Minkowski's Convex Body Theorem**) For a full rank lattice $\mathcal{L}$ and a centrally convex and symmetric set S with $Vol(S) > 2^n \det(\mathcal{L})$, S contains at least one non-zero lattice point.*

Proof. Consider a sub-region of R, name it R'
$R' = \{x | 2x \in R\}$ is obtained by shrinking R by a factor of two.
R' will inherit convexity, centrality and symmetry.
So we can apply Blichfield's lemma to obtain $x, y \in R'$ such that $x - y \in \mathcal{L}$.
Since $x, y \in R'$ we have $2x, 2y \in R$.
Also by symmetry property fo the set $-2x, -2y \in R$
Using the convexity property the convex combination $\frac{1}{2}2x + \frac{1}{2}(-2y) = x - y \in R$
Which is already a point in the lattice $\mathcal{L}$. □

Theorem 3.3. *(**Minkowski's Second Theorem**) For a full rank lattice $\mathcal{L}$*

$$\left(\prod_{i=1}^{n} \lambda_i\right)^{1/n} \leq \sqrt{n} \cdot (\det(\mathcal{L}))^{1/n}$$

Proof. Consider the open ball $S = B(0, \lambda_1)$ where $B(x, r)$ is defined as the open ball of radius r centred at x.
This ball contains a $n-$dimentional cube inside it, whose diagonal is of length $2\lambda_1$
We apply the relation $d = \sqrt{n}a$ where d, n and a are the diagonal, dimension and side of the cube and obtain $a = 2r/\sqrt{n}$

$$vol(B(0, r)) \geq a^n = \left(\frac{2\lambda_1}{\sqrt{n}}\right)^n$$

Applying the Minkowski's theorem, we get,

$$\left(\frac{2\lambda_1}{\sqrt{n}}\right)^n \leq vol(B(0, \lambda_1)) \leq 2^n \det(\mathcal{L})$$

On rearranging, we get,

$$\lambda_1(\mathcal{L}) \leq \sqrt{n} \det(\mathcal{L})^{1/n}$$

□

4 Conclusion

We explored the fascinating behaviour of the shortest non-zero vector, known as the first successive minimum $\lambda_1(\mathcal{L})$. These bounds elegantly capture the range within which the first successive minimum

$$\min_{1 \leq i \leq n} \|b_i^*\| \leq \lambda_1(\mathcal{L}) \leq \sqrt{n} \det(\mathcal{L})^{1/n}$$

References

[1] Oded Regev, *Lecture Notes on Lattices in Computer Science*, Tel Aviv University, Fall 2009.

[2] Vinod Vaikuntanathan, *Advanced Topics in Cryptography: From Lattices to Program Obfuscation*, MIT, Fall 2024.