Getting Started with Lattices

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

July, 2025

1 Introduction

Security of any cryptographic protocol relies on a computationally hard mathematical problem that is infeasible to solve by any existing computer. For many of the problems used in cryptography, no proof of a known computational algorithm exists that ensures solving the problem efficiently and exactly. Lattices have been used in cryptography to serve the same purpose, i.e a computationally hard-to-solve problem used to keep things secure. The purpose of introducing lattices in cryptography was primarily to demonstrate/exploit weaknesses in cryptosystems. Later on, it turned out to be useful for developing alternative forms of public-key cryptography. As of now, when the world approaches the era of Quantum Computers, where the widely used cryptosystems are under threat, the hope comes in the form of lattices, which were previously kept as an alternative. The domain lattice-based cryptography has sped up, and frequently, research articles on lattice-based cryptography are published. Lattice problems look to be good candidates that would be resistant to quantum computer attacks. In this article, we will jump into lattices and see their mathematics.

2 Lattices

Vaguely, a lattice is a collection of evenly spaced points in space, often in a grid-like pattern. The illustrations below show some lattice structure in $\mathbb{R}^2$. Moreover, the points here are the elements of the lattice. In the notion of distance, they are equally spaced.
It is a set of points in $\mathbb{R}^n$ with periodic structure. We are now going to formally define a lattice in mathematical terms.

Definition 2.1. *A lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^m$.*

Definition 2.2. *Let B be any real $m \times n$ square matrix over the real field. The set of vectors from $\mathbb{R}^m$ that can be written as $\mathbf{v} = B\mathbf{a}$ where $\mathbf{a}$ is a vector of integers and of dimension m, is called a lattice and we denoted by $\mathcal{L}$(sometimes we will use Λ, Γ).*

$$\mathcal{L} := \left\{ \mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{b_i} | \mathbf{a_i} \in \mathbb{Z} \right\}$$

where $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ are linearly independent vectors in $\mathbb{R}^m$. Here, n is called the rank of the lattice and m is called the dimension of lattice. Each $\mathbf{b_i}$ can be looked up as columns of the matrix B, which has components b_{ij}.

More concisely, we can express it as

$$\mathcal{L} = \{\mathbf{v} = B\mathbf{a} \mid \mathbf{a} \in \mathbb{Z}^n\}$$

and then we say B is the generator matrix for the lattice.

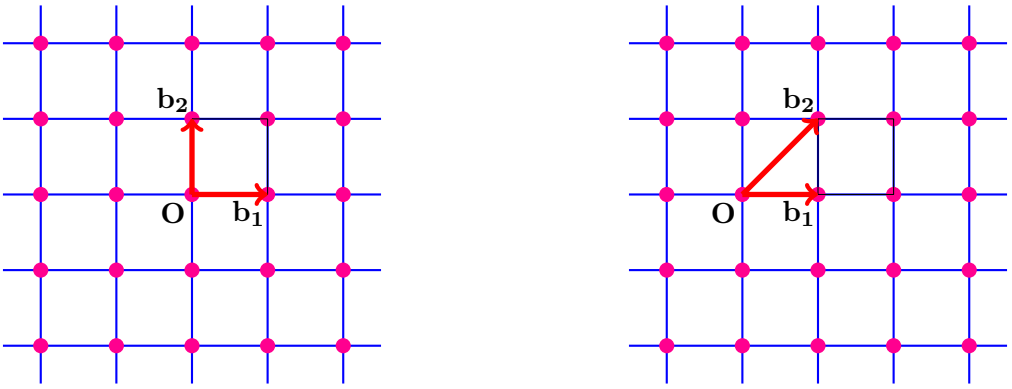


Figure 1: Lattice

3 Examples

Example 3.1. *$\mathcal{L}_1 = \mathbb{Z}^2$ is a lattice of dimension 2.*

$B = \{(1,0),(0,1)\} = \{\mathbf{b_1}, \mathbf{b_2}\}$ is a basis for $\mathbb{Z}^2$.

$$\mathcal{L}_1 = \{\alpha_1\mathbf{b_1} + \alpha_2\mathbf{b_2} | \alpha_1, \alpha_2 \in \mathbb{Z}\}$$

Example 3.2. *$\mathcal{L}_2 = 2\mathbb{Z}^2$ is a lattice of dimension 2, and it is a sub-lattice of $\mathcal{L}_1$.*

A lattice can have multiple bases.
$B' = \{(2,0),(0,2)\} = \{\mathbf{b'_1}, \mathbf{b'_2}\}$ is a basis for $2\mathbb{Z}^2$.
$C' = \{(-2,0),(0,2)\} = \{\mathbf{c'_1}, \mathbf{c'_2}\}$ is also a basis for $2\mathbb{Z}^2$.
Moreover, two different bases can either generate the same lattice or different lattices. Sometimes, two different bases generate lattices such that one is contained in another, in such case we would say that the one that is contained in the other is a sub-lattice.
Observe that B' is not a basis for Λ_1. Also Λ_2 is a sublattice of Λ.

4 More on Lattices

- 0 is an element of the lattice, we also call it the origin of the lattice.
- All elements of the lattice are generated by the linear combination of basis vectors, where the coefficients are taken from $\mathbb{Z}$
- We can think of it as a subset of $\mathbb{R}^m$ with each point placed in an even setup of distance.
- The basis set of a lattice need not be unique!!

Some quick remarks about lattices and bases.

- A lattice is of full rank if the generator matrix B is of full rank($m = n$).
- Every non-singular matrix (square matrix having determinant non-zero) corresponds to some lattice of full rank

Definition 4.1. *A matrix $U \in \mathbb{Z}^{n\times n}$ is called unimodular if* $\det(A) = \pm 1$

For example $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ is unimodular.

Lemma 4.2. *If U is unimodular so is U^{-1} and in particular $U^{-1} \in \mathbb{Z}^{n\times n}$*

Theorem 4.3. *Two bases B_1 and B_2 generate the same lattice Λ iff they are related by $B_2 = B_1 A$, where A is an unimodular matrix.*

Proof. Assume that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. For each column b_i of B_2 we have $b_i \in \mathcal{L}(B_1)$. This implies the existence of an integer matrix U such that $B_2 = B_1 U$. Similarly, $B_1 = B_2 V$ for some integer matrix V.
Hence,

$$B_2 = B_1 U = B_2 V U$$

And now,

$$B_2^T B_2 = (B_2 V U)^T B_2 V U = (VU)^T B_2^T B_2 V U$$

Now, on computing the determinant, we get,

$$\det(B_2^T B_2) = \det((VU)^T B_2^T B_2 VU)$$

Using the properties of the determinant, we get,

$$\det(B_2)^2 = \det(VU)^2 \det(B_2)^2$$

This gives that,

$$\det(V)^2 \det(U)^2 = 1$$

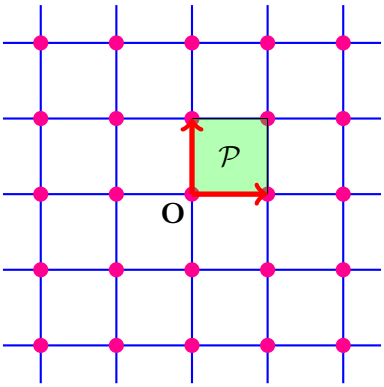
Here, both the determinant values are integer type. So, the only possibility is $\det(U) = \pm 1$ and $\det(V) = \pm 1$

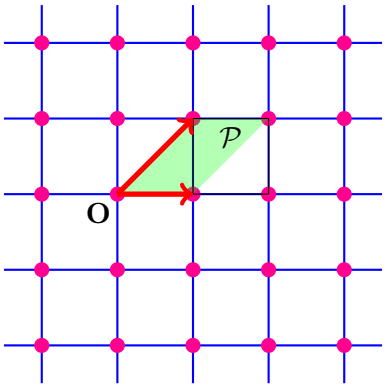
□

Definition 4.4. **(Fundamental Parallelepiped)** *For any lattice basis B we define*

$$\mathcal{P}(B) = \{B\mathbf{x} | \mathbf{x} \in \mathbb{R}^n, \forall i : 0 \leq x_i < 1\}$$

as the fundamental parallelepiped.





Definition 4.5. *Let $\Lambda = \mathcal{L}(B)$ be a lattice of rank n. Then the determinant of the lattice is defined as the volume of the fundamental parallelepiped $\mathcal{P}(B)$ of n dimensions.*

$$\det(\Lambda) = \left|\sqrt{\det(BB^T)}\right|$$

5 Gram-Schmidt Orthogonalization

The Gram-Schmidt process in itself can be covered in an article. It serves as an algorithm to construct a set of orthogonal bases from a set of linearly independent vectors in a vector space. Let $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ be n linearly independent vectors.

$$
\begin{aligned}
\mathbf{b_1^*} &= \mathbf{b_1} \\
\mathbf{b_2^*} &= \mathbf{b_2} - \mu_{2,1}\mathbf{b_1^*} \\
\mathbf{b_3^*} &= \mathbf{b_3} - \mu_{3,1}\mathbf{b_1^*} - \mu_{3,2}\mathbf{b_2^*} \\
&\vdots \\
\mathbf{b_n^*} &= \mathbf{b_n} - \mu_{n,1}\mathbf{b_1^*} - \mu_{n,2}\mathbf{b_2^*} - \cdots - \mu_{n,n-1}\mathbf{b_{n-1}^*} \\
\text{Where, } \mu_{i,j} &= \frac{\left\langle \mathbf{b_i}, \mathbf{b_j^*} \right\rangle}{\left\langle \mathbf{b_j^*}, \mathbf{b_j^*} \right\rangle}
\end{aligned}
$$

- $\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}$ are the required orthogonal vectors, which can further be divided by their corresponding lengths to get orthonormal vectors.
- The projection of a vector $\mathbf{u}$ on a vector $\mathbf{v}$ is given by

$$\text{proj}_{\mathbf{u}}(\mathbf{v}) = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} v$$

Algorithm 1: GSO

Input : $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ a set of linearly independent vectors.
Result: Orthogonal set of vectors $B^* = \{\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}\}$

Set $\mathbf{b_1^*} = \mathbf{b_1}$
for $i = 2, 3, \ldots, n$ **do**
  Compute $\mu_{i,j} = \frac{\langle \mathbf{b_i}, \mathbf{b_j^*} \rangle}{\langle \mathbf{b_j^*}, \mathbf{b_j^*} \rangle}$ for $1 \leq j \leq i-1$
  Set $\mathbf{b_i^*} = \mathbf{b_i} - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b_j^*}$
end
return $B^* = \{\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}\}$

More from Gram-Schmidt orthogonalisation.
If basis $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ be linearly independent and $\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}$ is the Gram-Schmidt orthogonal basis then

- $\left\langle \mathbf{b_i^*}, \mathbf{b_j^*} \right\rangle = 0$ whenever $i \neq j$. This is what orthogonalisation does, it helps to get a zero inner product.
- $\left\langle \mathbf{b_i}, \mathbf{b_j^*} \right\rangle = 0$ whenever $i < j$.
- We can generate orthonormal vectors by scaling the orthonormal vectors as unit vectors. More precisely $\widehat{\mathbf{b_i^*}} = \frac{\mathbf{b_i^*}}{\|\mathbf{b_i^*}\|}$.

It is convenient to view a basis matrix as a form of matrix decomposition

$$B = B^* \times U = Q \times D \times U$$

Where, Q is orthogonal matrix, D is a diagonal matrix, U is upper triangular matrix and B^* is the orthonormal basis

Result 5.1. *If $B = \{\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}\}$ is the GSO basis of the lattice basis $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ then* $\det(\mathcal{L}) = \prod_{i=1}^{n} ||\mathbf{b_i^*}||$

Proof.

$$B = \begin{bmatrix} | & | & \cdots & | \\ \mathbf{b_1} & \mathbf{b_2} & \cdots & \mathbf{b_n} \\ | & | & \cdots & | \end{bmatrix}$$

We are able to write the following

$$\begin{aligned} \mathbf{b_1} &= \mathbf{b_1^*} \\ \mathbf{b_2} &= \mathbf{b_2^*} + \mu_{2,1}\mathbf{b_1^*} \\ \mathbf{b_3} &= \mathbf{b_3^*} + \mu_{3,1}\mathbf{b_1^*} + \mu_{3,2}\mathbf{b_2^*} \\ &\vdots \\ \mathbf{b_n} &= \mathbf{b_n^*}\mu_{n,1}\mathbf{b_1^*} + \mu_{n,2}\mathbf{b_2^*} + \cdots + \mu_{n,n-1}\mathbf{b_{n-1}^*} \end{aligned}$$

In terms of matrix, we get,

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

Now the determinant,

$$\det(B) = \|\mathbf{b_1^*}\|\|\mathbf{b_2^*}\| \cdots \|\mathbf{b_n^*}\|$$

follows from the fact that $\begin{bmatrix} \frac{\mathbf{b_1^*}}{\|\mathbf{b_1^*}\|} & \frac{\mathbf{b_2^*}}{\|\mathbf{b_2^*}\|} & \cdots & \frac{\mathbf{b_n^*}}{\|\mathbf{b_n^*}\|} \end{bmatrix}$ is an orthogonal matrix, where each column is a unit vector.

□

Result 5.2. **(Pythagoras theorem)** *For an orthogonal set of vectors $\{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$*

$$\|\mathbf{b_1} + \mathbf{b_2} + \cdots + \mathbf{b_n}\|^2 = \|\mathbf{b_1}\|^2 + \mathbf{b_2}\|^2 + \cdots + \|\mathbf{b_n}\|^2$$

Result 5.3. *The GSO vector $\mathbf{b_j^*}$ corresponding to the vector $\mathbf{b_j}$ satisfy $\|\mathbf{b_j^*}\| \leq \|\mathbf{b_j}\|$*

Proof. We have,

$$\mathbf{b_j} = \mathbf{b_j^*} + \sum_{i<j} \mu_{j,i}\mathbf{b_i^*} = \mathbf{b_j^*} + \mathbf{u}$$

We have, $\mathbf{u} = \sum_{i<j} \mu_{j,i}\mathbf{b_i^*}$, which lies in the span$(\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_{j-1}^*})$
By construction $\mathbf{b_j^*}$ is orthogonal to $\mathbf{u}$ so we apply Pythagoras theorem,

$$\|\mathbf{b_j}\|^2 = \|\mathbf{b_j^*} + \mathbf{u}\|^2 = \|\mathbf{b_j^*}\|^2 + \|\mathbf{u}\|^2$$

and finally, we obtain,

$$\|\mathbf{b_j^*}\| \leq \|\mathbf{b_j}\|$$

□

Result 5.4. **(Hadamard's Inequality)** *If $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ is the basis of lattice $\mathcal{L}$ then*

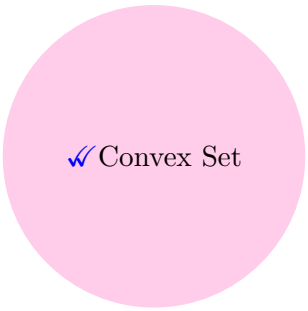
$$\det(\mathcal{L}(B)) \leq \|\mathbf{b_1}\| \times \|\mathbf{b_2}\| \times \cdots \times \|\mathbf{b_n}\|$$

Proof. We have

$$\begin{aligned} \det(\mathcal{L}(B)) &= \|\mathbf{b_1^*}\| \times \|\mathbf{b_2^*}\| \times \cdots \times \|\mathbf{b_n^*}\| \\ &\leq \|\mathbf{b_1}\| \times \|\mathbf{b_2}\| \times \cdots \times \|\mathbf{b_n}\| \qquad \text{(By previous result)} \end{aligned}$$

Apply the above result to obtain □

Definition 5.5. *A set S is called convex if $\forall\ x \neq y$ and $x, y \in S$ we have $\alpha x + (1-\alpha)y \in S$ for all $\alpha \in [0, 1]$*



Definition 5.6. *A set S is called centrally symmetric if $\forall x \in S$ we have $-x \in S$.*

In the next article, we will intensively use the definitions and results noted in this article.

References

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. ISBN: 978-1107013926. URL: `https://www.cambridge.org/core/books/mathematics-of-public-key-cryptography/DDDFA3874A53C4E6846EB3AB06161E43`.

[Reg09] Regev. *Lecture Notes on Lattices in Computer Science*. Tel Aviv University, 2009.

[Vai24] Vinod Vaikuntanathan. "Advanced Topics in Cryptography: From Lattices to Program Obfuscation". In: *MIT* (2024).