PEOPLE's DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf university of Msila
Faculty of Mathematics and computer sciences
Department of Mathematics

Master memory

Field : Mathematics and computer sciences.
Branch : Mathematics.
Option : Algebra and Discrete Mathematics.

Theme

Lattices in Euclidean Space: Problems and Applications.

Prsented by:
Ms. Farida DAIF.

The jury composed of :

GHADBANE Naser	MC,	University of M'sila	**President.**
MIHOUBI Douadi	prof,	University of M'sila	**Supervisor.**
HEBOUB Lakhdar	MAC,	University of M'sila	**Examiner.**

University year 2019/2020.

Lattices in Euclidean Space: Problems and Applications.

Daif Farida

October 13, 2020

.

Acknowledgements

In the beginning, we must praise and thank ***"Allah"****, without whom we would not have completed this memory. Praise be to* ***"Allah"*** *who helped us achieve our goal today despite all the difficulties we faced.*

I would like to express my thanks and gratitude to the jury , my distinguished professors, headed by the supervising professor, ***Mihoubi Douadi****, for devoting their time and their effort to read and examine my work.*

I wish also to express my profound appreciation to everyone who supported and encouraged us to reach this day from the teachers, Colleagues and professors, especially my professor ***Amroune.N*** *I am grateful to him for all the assistance and support. My sincere thanks to my dear sisters* ***Abir, Selsebile, Ibtisem, Meriam, Fatima and Djamila****, especially th doctorate student* ***Koraiche.S*** *for all the helpes. You were the best supportive of me and I am deeply grateful for you.*

At last, I would like to thank my family who provided us with all kinds of support and patience with us and believed in us to achieve this dream.

Contents

List of Figures

List of Algorithms

Introduction

The mathematical modern asymetric cryptosystems are based on the notion of **one-way function**, which is given the plaintext x it is easy to compute the ciphertext $y = f(x)$, but given the ciphertext y it is very hard to compute x such that $y = f(x)$. An example of a **trapdoor one-way function**:

Fix a prime p. Let a and B be nonzero integers $mod(p)$ and suppose $B \equiv a^x mod(p)$ The problem of finding x is called the **discrete logarithm** problem[17].

The **RSA** problem given e and N such that $\gcd(e, (p-1)(q-1)) = 1$ and a value y, to find x such that

$$F(x) = x^e \equiv y \; mod(N).$$

This is similar to the problem of inverting the one-way function. However it is more than that. The function $F(x)$ in the **RSA** problem has an extra property: there exists a value d which allows one to efficiently invert the function. The value d is called the **trapdoor**, and such functions are called **trapdoor one-way functions**.
In the **RSA** algorithm, we saw how the difficulty of factoring yields useful cryptosystems[13].

One of the main problems on discrete algorithms is Lattice problems such as **SVP** and **CVP**, those problems difficult to tackle. This remarkable property is what makes lattice-based cryptographic constructions so attractive. Lattice problems are used as the foundation for building lattice based cryptosystems. Lattice-based cryptosystems usually enjoy strong security guarantees, which means that breaking their security is proved at least as hard as solving some lattice problems in any of its instances, also the worst ones.

In this memory, we interested to define the lattices and his problems and finally we review some protocols based on lattice in three chapters:
In **Chapter one:** we recall some of the important concepts in lineare algebra ase the basis, the Euclidean space and we define the word lattices and some the moste nessery problems in lattices **SV problem** and **CV problem**.

In **the second chapter:** an review of the best algorithems used to redused the lattices basis as the **LLL** algorithem, and **Babai's** to solve those problems.

Finally, in **the laste chpter:** a review of some lattices-dependent protocols as **GGH**, **NTRU**, and the effect of lattices on the efficiencies of those cryptosystems, and methods of attacking them by means of reduction algorithms, and the effect of lattices on the **RSA** cryptosystem.

Chapter 1

Elementary concept

Lattices are regular arrangements of points in Euclidean space. The theory of lattices may be described as discrete linear algebra. In this chapter we begin with a review of elementary linear algebra, which we will use during research, and definition of what lattices are, and the most important characteristics that this type of space possesses, and some of the most important concepts that must be known to study lattices. We are also in the last section for this chapter, we show the most important problems presented by lattices, and some difficult problems to solve.
Basic references for this chapter are [6, 1, 9].

Euclidean space $\mathbb{R}^n$

The Euclidean space $\mathbb{R}^n$ consists of all column vectors X with n components.

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

1.1 Vector space

The vector space $\mathbb{R}^n$ consists of all n-tuples of elements from $\mathbb{R}$ with the familiar operations of vector addition and scalar multiplication defined by:

$$X + Y = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix};$$

$$aX = a \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{pmatrix}.$$

for any $X, Y \in \mathbb{R}^n$ and $a \in \mathbb{R}$.
We use dot notation for the scalar product of vectors.

$$X.Y^t = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} . (y_1, y_2, \cdots, y_n) = x_1.y_1 + x_2.y_2 + \cdots + x_n.y_n = \sum_{i=1}^{n} x_i y_i.$$

Length: The length $\| X \|$ of a vector X is the squert root of $X.X^t$:

$$length(X) = \| X \| = \sqrt{X.X^t}.$$

Exemple 1.1.1 *Let $X = (3, 2, 4)^t$ and Let $Y = (5, 8, 6)^t$*

The scalar product of vectors

$$X.Y^t = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} . (5, 8, 6) = 3.5 + 2.8 + 4.6 = 55.$$

The length of the vector X

$$\| X \| = \left(\begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} . \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix}^t \right)^{1/2} = \sqrt{3^2 + 2^2 + 4^2} = \sqrt{29} \approx 5.385.$$

1.1.1 Subspace

A subspace of a vector space is a set of a vectors (including 0) that satisfies two requirements: If X and Y are vectors in the subspace and a is any scaler,

1. $X + Y$ is in the subspace.
2. aX is in the subspace.

1.1.2 Basis of a Vector Space

Definition 1.1.1 ***Linear independence:*** *The vectors $X_1, X_2, \cdots, X_n \in \mathbb{R}^n$ are **linearly independent** if the equation*

$$a_1 X_1 + a_2 X_2 + \cdots + a_n X_n = 0 \qquad (a_1, a_2, \cdots, a_n \in \mathbb{R}).$$

has only the trivial solution $a_i = 0$ for $i = 1, 2, \cdots, n$.

Exemple 1.1.2 *Let $A = \{\boldsymbol{u}, \boldsymbol{v}\}$ $\boldsymbol{u} = (1, 0)$ et $\boldsymbol{v} = (1, 1)$ we show that they are linearly independent. Suppose there are two real numbers λ, μ, such that: $\lambda.\boldsymbol{u} + \mu.\boldsymbol{v} = 0$. It means that $\lambda(1, 0) + \mu(1, 1) = (0, 0)$. If we develop, we find*

$$\lambda(1, 0) + \mu(1, 1) = (\lambda + \mu, \mu) = (0, 0).$$

We therefore conclude that necessarily $\lambda = \mu = 0$, and therefore that the vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ are linearly independent.

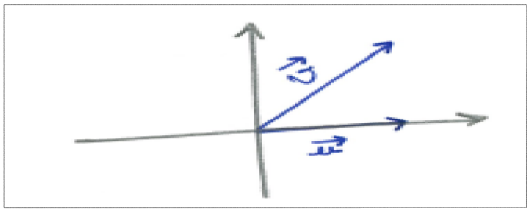

Figure 1.1: A linearly independent vectors.

Definition 1.1.2 ***Orthogonal projection:***
*Given vectors $X, Y \in \mathbb{R}^n$ with $Y \neq 0$, we can express X as a sum of two vectors, **X = u + v**, where **u** is parallel to Y and **v** is orthogonal to Y*

$$u = (\frac{XY}{YY})Y,\ v = X - (\frac{XY}{YY})Y.$$

*We call **u** the **orthogonal projection** of X onto Y*

Vectors that Span a Subspace

A set of vectors **span** a space if their linear combinations fill the space.

Definition 1.1.3 *A **basis** for a vector space is a sequence of vectors with tow propreties:*
The basis vectors are linearly independent and they spane the space

Orthogonal basis

To start, we should define the orthogonality. Two vectors are orthogonal when their dot product is zero:

$$X.Y = 0 \text{ or } X^t.Y = 0.$$

The orthogonal part of X over Y, denoted $\tilde{X}$ is the following vector:

$$\tilde{X} = X - \text{projection}(X \text{ onto } Y).$$

Definition 1.1.4 *Suppose we have a basis $B = \{b_1, b_2, \cdots, b_n\}$ for some space $\mathbb{R}^n$. We will say that this basis is orthogonal if we take any b_i, b_j with $i \neq j$ then b_i and b_j are orthogonal i.e, their dot product is 0.*

1.2 Lattice

Lattice is a discrete additive subgroup of $\mathbb{R}^n$[2], i.e, it is a subset $L \subset \mathbb{R}^n$ satisfying the following properties:
(subgroup) L is closed under addition and subtraction,
(discrete) if and only if each of its points is isolated.
In this section, we review the research topic, we start by defining lattices, and some of their distinctive characteristics, and then we know the most important problems in lattices.

Definition 1.2.1 *Let $X_1, X_2, \cdots, X_n \in \mathbb{R}^n$ be a linearly independent vectors. We say a lattice L with dimension n **generated** or **spaned** by The basis vectors $X_1, X_2, \cdots, X_n$ the set of all linear combinations of the vectors with integral coefficients:*

$$L = \mathbb{Z}X_1 + \mathbb{Z}X_2 + \cdots + \mathbb{Z}X_n = \left\{ \sum_{i=1}^{n} a_i X_i \,|a_1, a_2, \cdots, a_n \in \mathbb{Z} \right\}.$$

The prime example for the concept of lattice is $\mathbb{Z}^n$, the set of points in the n-dimensional real linear space $\mathbb{R}^n$ with all coordinates being integers.

For $i = 1, 2, \cdots, n$ we write $X_i = (x_1, x_2, \cdots, x_n)$ and form the $n \times n$ matrix $X = (x_{ij})$. The determinant of the lattice L with basis $X_1, X_2, \cdots, X_n$ is

$$\det(L) = |\det(X)|.$$

For the m-demontional lattices $m \leq n$ spanned by $X_1, X_2, \cdots, X_m$ in n-dimensional Euclidean space $X_i = (x_1, x_2, \cdots, x_n)$ is defined to be

$$L = \mathbb{Z}X_1 + \mathbb{Z}X_2 + \cdots + \mathbb{Z}X_m = \left\{ \sum_{i=1}^{m} a_i X_i \,|a_1, a_2, \cdots, a_m \in \mathbb{Z} \right\}.$$

We write $X = (x_{ij})$ the $m \times n$ matrix. We call The **Gram matrix** of the lattice L the $m \times m$ matrix sutch that: $\Delta(L) = (x_i . x_j) = XX^t$. The determinant of the Gram matrix is always positive. And we define the **determinant** of the lattice L to be its square root:

$$\det(L) = \sqrt{\det(XX^t)}.$$

The lattice **rank** is n and the lattice **dimension** is m. If $n = m$ then L is said to be a **full rank**

Exemple 1.2.1 *Consider the 3-dimensional lattice L in 4-dimensional Euclidean space spanned by the rows of this matrix:*

$$\begin{pmatrix} 5 & -2 & 3 & 4 \\ 6 & 8 & 7 & 1 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

We compute the Gram matrix:

$$\Delta(L) = XX^t = \begin{pmatrix} 5 & -2 & 3 & 4 \\ 6 & 8 & 7 & 1 \\ 3 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 5 & 6 & 3 \\ -2 & 8 & 4 \\ 3 & 7 & 2 \\ 4 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 68 & 41 & 17 \\ 41 & 150 & 65 \\ 17 & 65 & 30 \end{pmatrix}.$$

So the determinent of lattice L:

$$\det(L) = \sqrt{\det(\Delta(L))} = \sqrt{15530}.$$

Lemma: 1.2.1 *Let L be a lattice in $\mathbb{R}^n$, and let $X_1, X_2, \cdots, X_m$, and $Y_1, Y_2, \cdots, Y_m$ are linearly independent vectors. Let X (respectively Y) be the $n \times m$ matrix with x_i (respectively y_i) in row i for $i = 1, 2, \cdots, m$. X, Y be tow basis generate the same lattice L, if and only if $Y = CX$ for some $m \times m$ matrix C with integer entries and determinant ± 1.*

Proof. Every Y_i belongs to the lattice with basis $X_1, X_2, \cdots, X_m$, and every X_i belongs to the lattice with basis $Y_1, Y_2, \cdots, Y_m$. It follows that

$$X_i = \sum_{i=1}^{m} b_{ij} Y_j \qquad Y_i = \sum_{i=1}^{m} c_{ij} X_i \qquad (i = 1, 2, \cdots, m),$$

Where $B = (b_{ij})$ and $C = (c_{ij})$ are $m \times m$ matrices with integer entries. Writing these two equations in matrix form gives $X = BY$ and $Y = CX$, and hence $X = BCX$ and $Y = CBY$. Since both $X_1, X_2, \cdots, X_m$ and $Y_1, Y_2, \cdots, Y_m$ are bases of $\mathbb{R}^n$, the corresponding matrices X and Y are invertible, and can be canceled from the equations. Therefore $BC = I$ and $CB = I$, and so $\det(B).\det(C) = 1$. Since B and C have integer entries, it follows that either $\det(B) = \det(C) = 1$ or $\det(B) = \det(C) = -1$.

Exemple 1.2.2 *The lattice generated by* $(1,0)^t$ *and* $(0,1)^t$ *is* $\mathbb{Z}^2$*, the lattice of all integers points. This basis is not unique: for example,* $(1,1)^t$ *and* $(-1,0)^t$ *also generate* $\mathbb{Z}^2$
see Figure 1.2

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \quad \det(C) = 1$$

$$Y = CX = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

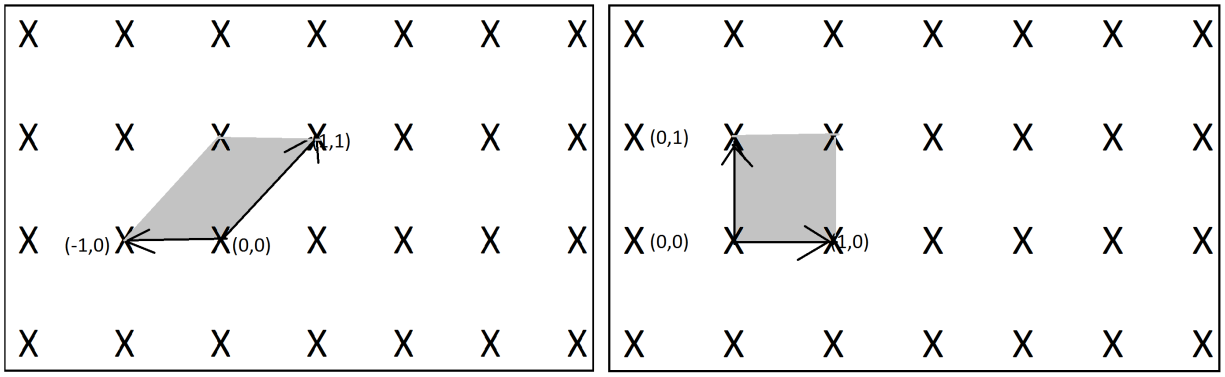

Figure 1.2: Two different basis generate $\mathbb{Z}^2$.

Corollary : 1.2.1 *The determinant of a lattice does not depend on the basis.*

Proof: Suppose the lattice $L \in \mathbb{R}^n$ has two bases $X_1, X_2, \cdots, X_n$ and $Y_1, Y_2, \cdots, Y_n$. $Y_i \in L$. So befor (Lemma 1.2) $Y = CX$, then we have

$$|\det(Y)| = |\det(CX)| = |\det(C)\det(X)| = |\pm\det(X)| = |\det(X)|.$$

Since the two bases are arbitrary, this completes the proof.

Definition 1.2.2 *An* $n \times n$ *matrix with integer entries and determinant* ± 1 *will be called* ***unimodular****.*

Definition 1.2.3 *A unimodular row operation on a matrix is one of the following elementary row operations:*
Multiply any row by -1*;*
Interchange any two rows;
Add an integral multiple of any row to any other row.
If we apply unimodular row operations to the matrix X *whose rows contain a basis of the lattice* L*, then we obtain another basis of the same lattice.*

Definition 1.2.4 ***Sublattice:***
Let $L \in \mathbb{R}^n$ *be the lattice with basis* $X_1, X_2, \cdots, X_n$*. Suppose that* $Y_1, Y_2, \cdots, Y_n \in L$ *are linearly independent,* $X = (x_{ij})$ *and* $Y = (y_{ij})$ *we call a sublattice of* L *every lattice (we denote it* M *) generated by* $Y_1, Y_2, \cdots, Y_n$*. And write* $M \subseteq L$*.*
Each basis vector Y_i *for the sublattice* M *belongs to the lattice* L

$$Y_i = \sum_{i=1}^{n} c_{ij} X_i, \qquad \text{where } c_{ij} \in \mathbb{Z} \text{ for all } i, j = 1, 2, \cdots, n.$$

So as a matrix equation, this says that $Y = CX$*, where* $C = (c_{ij})$ *is the non-singular* $n \times n$ *matrix of integer coefficients.*

Definition 1.2.5 *Let L be an m-dimensional lattice in $\mathbb{R}^n$, shortest nonzero vector in a lattice L, which we denote by*

$$\wedge_1(L) = \min_{X \in L,\ X \neq 0} (\| X \|).$$

In geniral the i-th successive minimum of the lattice, denoted $\wedge_i(L)$, is the smallest real number $(r \neq 0)$ such that there exist i linearly independent vectors $X_1, X_2, \cdots, X_i \in L$ such that:

$$\| X_1 \|, \| X_2 \|, \cdots, \| X_i \| \leq r.$$

This quantity can be expressed more concisely by the equation

$$\wedge_i(L) = \min_{X_1, X_2, \cdots, X_i \in L} \max(\| X_1 \|, \| X_2 \|, \cdots, \| X_i \|) \ (r \neq 0).$$

Where the minimum is over all sets of i linearly independent vectors in L. It is easy to see that the successive minima are weakly increasing:

$$\wedge_1(L) \leq \wedge_2(L) \leq \cdots \leq \wedge_m(L).$$

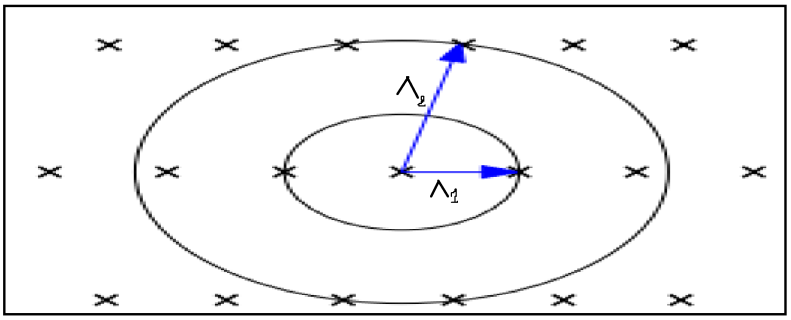

Figure 1.3: Successive minima in $L \in \mathbb{R}^2$.

Definition 1.2.6 [7] *Let L be a lattice of dimension n and let $X_1, X_2, \cdots, X_n$ be a basis for L. The fundamental domain (or fundamental parallelepiped) for L corresponding to this basis is the set*

$$\mathcal{F}(X_1, X_2, \cdots, X_n) = \{t_1 X_1 + t_2 X_2 + \cdots + t_n X_n \quad : 0 \leq t_i < 1\}.$$

Exemple 1.2.3 *The shaded area in Figure 1.4 illustrates a fundamental domain in dimension 2.*

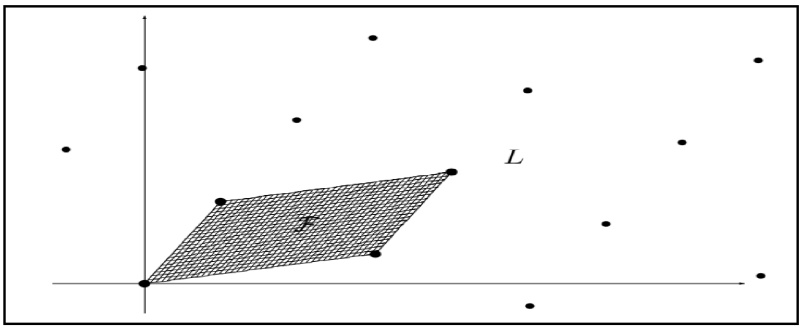

Figure 1.4: Fundamental domainin $L \in \mathbb{R}^2$.

Proposition: 1.2.1 *Let $L \subset \mathbb{R}^n$ be a lattice of dimension n and let $\mathcal{F}$ be a fundamental domain for L. Then very vector $Y \in \mathbb{R}^n$ can be written in the form $Y = t + X$ for a unique $t \in \mathcal{F}$ and a unique $X \in L$. Equivalently, the union of the translated fundamental domains*

$$\mathcal{F} + X = \{t + X : t \in \mathcal{F}\}.$$

as X ranges over the vectors in the lattice L exactly covers $\mathbb{R}^n$.

In Exemple 1.2.3 Translations of $\mathcal{F}$ by vectors in L exactly covers $\mathbb{R}^2$.

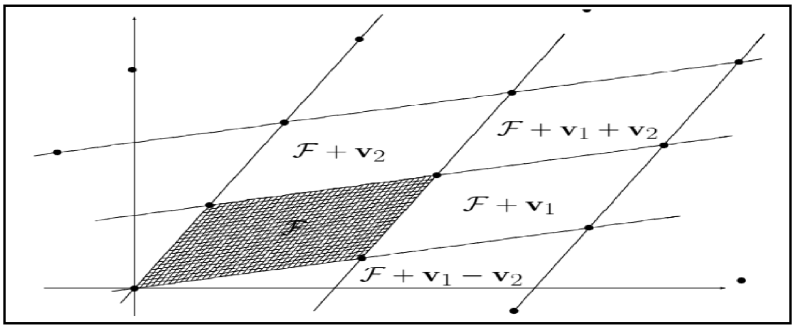

Figure 1.5: Translated fundamental domains($\mathbb{R}^2$).

Remark: 1.1 *The determinant of a lattice L is the volume of the parallelepiped (fundamental domains) in $\mathbb{R}^n$ whose edges are the lattice basis vectors. all fundamental domains have the same volume.*

1.3 Lattice problems

There are several natural computational problems relating to lattices. We start by listing some problems that can be efficiently solved using linear algebra.

Problem: 1.1 ***(Lattice basis:)*** *Given a set of vectors $X_1, X_2, \cdots, X_n$ in $\mathbb{R}^n$ (possibly linearly dependent) find a basis for the lattice generated by them.*
Simply any unimodular row operations to the matrix X whose rows contain a basis of the lattice L, then we obtain another basis of the same lattice. equivalently, left multiplication of the matrix X by an integer matrix C with determinant ± 1.

Exemple 1.3.1 *The rows X_1, X_2, X_3, X_4 of the following 4×4 matrix X form a basis of a lattice L in $\mathbb{R}^4$:*

$$X = \begin{pmatrix} -2 & 7 & 7 & -5 \\ 3 & -2 & 6 & -1 \\ 2 & -8 & -9 & -7 \\ 8 & -9 & 6 & -4 \end{pmatrix}, \quad \det(X) = 632.$$

We can find another basis of the same lattice using a unimodular matrix C:

$$C = \begin{pmatrix} -13071 & -5406 & -9282 & -2303 \\ -20726 & -8571 & -14772 & -3651 \\ -2867 & -1186 & -2043 & -505 \\ -14338 & -5936 & -10216 & -2525 \end{pmatrix}, \quad \det(C) = -1.$$

The rows Y_1, Y_2, Y_3, Y_4 of the matrix $Y = CX$ form another basis of L:

$$Y = CX = \begin{pmatrix} -27064 & 14298 & -54213 & 144947 \\ -43013 & 23095 & -85466 & 230209 \\ -5950 & 3192 & -11828 & 31842 \\ -29764 & 15959 & -59188 & 159238 \end{pmatrix}, \quad \det(Y) = -632.$$

Problem: 1.2 ***(Membership:)*** *Given a lattice basis $X \in \mathbb{R}^m$ and a vector $Y \in \mathbb{R}^{m \times n}$ decide if $Y \in L(X)$.*
The equation $XU = Y$ can be seen as a system of m linear equations in n variables. We can therefore solve it efficiently by Gaussian elimination.

Problem: 1.3 ***(Equivalence:)*** *Given $X, Y \in \mathbb{R}^{m\times n}$two bases. Decide if these two bases spawn the same $(L(X) = L(Y))$.*
It is enough to calculate the passage matrix C and to check if it is unimodular.

1.4 Hard lattice problems

1.4.1 The Shortest Vector Problem (SVP)

[15] We recall the first successive minimum of the lattice L, which is the length of the shortest nonzero lattice vector. The first obvious problem in lattice theory is to find a nonzero lattice vector that reaches this minimum. Note that it is never unique, as $\| (-X) \| = \| X \|$ for all lattice vectors $X \in L$ (there may be other lattice points with the same norm).

Shortest Vector Problem:

[14] Given a basis of L, find $Y \in L$ such that $\| Y \| = \wedge_1(L)$.

1.4.2 The Closest Vector Problem (CVP)

The second obvious problem in lattice theory is to find, for a given target point $W \in \mathbb{R}^m$, a lattice point that is closest to W. Note that it may not be unique, but in many cases it will. It makes sense to assume that: $W \notin L$.

Closest Vector Problem:

Let $d(W, L)$ denote the distance of $W \in \mathbb{R}^m$ to the closest lattice point.
Given a basis of L and a target $W \in \mathbb{R}^m$, find $X \in L$ such that $\| W - X \| = d(W, L)$.

SVP and **CVP** problems are difficult to be resolved exactly, so we present some problems that are approximate and less difficult.

The approximate SVP problem:

Lat a lattice L and an approximation factor $\alpha \in \mathbb{R}^+$.
Given a basis matrix X for L, compute a non-zero vector $Y \in L$ such that $\| Y \| \leq \alpha \wedge_1$ ($\wedge_1$ is the first minimum).

The approximate CVP problem:

Lat a lattice L and an approximation factor $\alpha \geq 0$.
Given a basis of L, a target $W \in \mathbb{R}^m$, for all $Y \in L$, find $X \in L$ such that:

$$\| W - X \| \leq \alpha \| W - Y \| .$$

Exemple 1.4.1 *Let $L \subset \mathbb{R}^2$ be the lattice with basis matrix:*

$$X = \begin{pmatrix} 1001 & 0 \\ 0 & 2008 \end{pmatrix}.$$

Then every lattice vector is of the form ***(1001a, 2008b)*** *where* ***a, b*** $\in \mathbb{Z}$*.Hence* ***the shortest non-zero vectors*** *are clearly* ***(1001, 0)*** *and* ***(-1001, 0)****.Similarly,* ***the closest vector*** *to* ***W= (2974, 4098)*** *is clearly* ***(3003, 4016)****.*

This example so easy the reason is that the basis vectors are orthogonal. Even in large dimensions, the **SVP** and **CVP** problems are easy if one has an orthogonal basis for a lattice. When given a basis that is not orthogonal, it is difficult to find combination of the basis vectors that gives a vector strictly shorter than the shortest basis vector, especially in large dimensions Similarly for the closest vector. So the orthogonal basis facilitates the solution of those problems.

Chapter 2

Lattices reduction

A lattice has an infinity of basis, which are all equivalent, and some of these basis have more interesting properties. The main of reduction is to find in one "reasonable" time a basis with "nearly good" Euclidean properties, formed by vectors nearly orthogonal, and sufficient to give approximations for the minima successive. But, as we have already seen, in the cas that lattices have a larger dimension, it is difficult to find a good basis. In this chapter we present some principal reduction algorithms.
The main reductions are: Harmet, Korkine and Zolotarev reduction, Lenstra, Lenstra and Lovász (LLL) reduction and BKZ block reduction.

2.1 Small dimensional lattice reduction algorithms

2.1.1 Two-dimensional lattices

Let X and Y form a basis of $\mathbb{R}^2$. The lattice $L \subset \mathbb{R}^2$ generated by X and Y is the set of all integral linear combinations of X and Y:

$$L = \{aX + bY \mid a, b \in \mathbb{Z}\}.$$

A basic problem is to find a shortest (nonzero) vector in this lattice, such that for all $w \in L,\ w \neq 0$. $\wedge_1$ for which $\wedge_1 \leq \| w \|$.
This is achieved by the **Gaussian algorithm**. In fact this algorithm finds a minimal basis of a two-dimensional lattice.

Definition 2.1.1 [9] *We say that a basis $X,\ Y$ of a lattice L in $\mathbb{R}^2$ is **minimal** if X is a shortest nonzero vector in L and Y is a shortest vector in L which is not a multiple of X.*

The Gaussian algorithm

The Gaussian algorithm used to compute the minimal basis $V_1,\ V_2$ of the lattice L. is based on compare the length of basis vectors.

First, put $V_1 = X,\ V_2 = Y$;

Calculate the nearest integer m to the orthogonal projection coefficient $\lambda = \dfrac{V_1.V_2}{V_1.V_1}$ instead of λ itself, because the vector V_2 must remain in the lattice L. The integer is $m = \left\lceil \dfrac{V_1.V_2}{V_1.V_1} \right\rfloor$ and change V_2 to becoms: $V_2 = V_2 + mV_1$.

If $\| V_2 \| < \| V_1 \|$, we interchange the vectors, and repeat the same steps. If $\| V_2 \| \geq \| V_1 \|$ and $|m| \leq 1$ terminate with this minimal basis. Therefore V_2 is a shortest vector in L linearly independent of V_1.

Algorithm 1 The Gaussian algorithm.

- **Input:** A basis $X,\ Y$ of a lattice L in $\mathbb{R}^2$ such that $\| X \| \leq \| Y \|$.
- **Output:** A minimal basis $V_1,\ V_2$ of the lattice L.

i) Set $V_1 \longleftarrow X$ and $V_2 \longleftarrow Y$. Set $finished \longleftarrow false$.

ii) While not finished do:

a) Set $m \longleftarrow \left\lceil \frac{V_1.V_2}{V_1.V_1} \right\rfloor$.

b) Set $V_2 \longleftarrow V_2 - mV_1$.

c) If $\| V_1 \| \leq \| V_2 \|$ then:

1) set finished $\longleftarrow$ true.
else

2) set $u \longleftarrow V_1,\ V_1 \longleftarrow V_2,\ V_2 \longleftarrow u$ (interchange V_1 and V_2).

iii) Return V_1 and V_2.

The next lemma shows that the new second vector V_2 is **nearly orthogonal** to the old first vector V_1.

Lemma: 2.1.1 *After the calculating of the new vector V_2 (step $(ii))(b))$ of **Algorithm** 1) we have:*

$$\| V_2.V_1 \| \leq \frac{1}{2} \| V_1 \|^2 .$$

Proof: From the definition we have:

$m = \left\lceil \frac{V_1.V_2}{V_1.V_1} \right\rfloor$, which implies that $\frac{V_1.V_2}{V_1.V_1} - \frac{1}{2} < \frac{V_1.V_2}{V_1.V_1} \leq \frac{V_1.V_2}{V_1.V_1} + \frac{1}{2}$.

Multiplying this inequality by $(V_1.V_1)$ and subtracting $m(V_1.V_1)$ from all parts gives

$-\frac{1}{2}(V_1.V_1) < V_2.V_1 - m(V_1.V_1) \leq \frac{1}{2}(V_1.V_1)$, and this implies that $\| (V_2 - mV_1).V_1 \| \leq \frac{1}{2} \| V_1 \|^2$.

Properties 2.1.1 *:*

*Let $X,\ Y$ a basis vectors of a lattice L in $\mathbb{R}^2$. We have frome (step $(ii))(b))$ of **Algorithm** 1) $V_1' = V_1,\ \ V_2' = V_2 - mV_1$, where $V_1',\ V_2'$ are the new vectors. So we can express (step $(ii))(b))$ of **Algorithm** 1) as matrix equation $V.C = V'$ such that:*

$$V = \begin{pmatrix} V_1 \\ V_2 \end{pmatrix},\ C = \begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix},\ V' = \begin{pmatrix} V_1' \\ V_2' \end{pmatrix}.$$

*The matrix **C** is **unimodular** $(\det(C) = 1)$. So step (ii)) preserves the property that V_1, V_2 is a basis of the lattice L.*

The Gaussian algorithm can be applied to any two linearly independent vectors $V_1,\ V_2$ in the Euclidean vector space $\mathbb{R}^n$ for any $n \geq 2$. The vectors $V_1,\ V_2$ span a subspace of $\mathbb{R}^n$ linearly isomorphic to $\mathbb{R}^2$, and generate a two-dimensional lattice L in $\mathbb{R}^2$ (as before, this is the set of all integral linear combinations of $V_1,\ V_2$).

Theorem: 2.1.1 *The Gaussian algorithm terminates, and upon termination V_1 is a shortest nonzero vector in the lattice, and V_2 is a shortest vector in the lattice which is not a multiple of V_1.*

Proof: Let $V_1,\ V_2$ a basis of the lattice L and let u be any nonzero vector in L, so that $u = aV_1 + bV_2$, for non zero $a, b \in \mathbb{Z}$.

$$\| u \|^2 = (aV_1 + bV_2).(aV_1 + bV_2). \tag{2.1}$$
$$= a^2 \| V_1 \|^2 + 2ab(V_1.V_2) + b^2 \| V_2 \|^2 . \tag{2.2}$$
$$\geq a^2 \| V_1 \|^2 - |ab| \| V_1 \|^2 + b^2 \| V_2 \|^2 . \tag{2.3}$$
$$\geq a^2 \| V_1 \|^2 - |ab| \| V_1 \|^2 + b^2 \| V_1 \|^2 . \tag{2.4}$$
$$= (a^2 - |ab| + b^2) \| V_1 \|^2, \ \ (\| V_1 \| \leq \| V_2 \|). \tag{2.5}$$

$a, b \neq 0$, we have $a^2b^2 < (a^2 + b^2)^2$ and hence $|ab| < a^2 + b^2$.Therefore $\| u \|^2 \geq \| V_1 \|^2$, and so $\mathbf{V}_1$ is a **shortest vector** in L.
Now suppose that $u = aV_1 + bV_2$ is linearly independent of V_1 equivalently that $b \neq 0$. We have

$$\| u \|^2 \geq a^2 \| V_1 \|^2 - |ab| \| V_1 \|^2 + b^2 \| V_2 \|^2 . \tag{2.6}$$
$$= a^2 \| V_1 \|^2 - |ab| \| V_1 \|^2 + \frac{1}{4}b^2 \| V_2 \|^2 + \frac{3}{4}b^2 \| V_2 \|^2 . \tag{2.7}$$
$$\geq a^2 \| V_1 \|^2 - |ab| \| V_1 \|^2 + \frac{1}{4}b^2 \| V_1 \|^2 + \frac{3}{4}b^2 \| V_2 \|^2, \ \ (\| V_1 \| \leq \| V_2 \|). \tag{2.8}$$
$$= (|a| - \frac{1}{2}|b|)^2 \| V_1 \|^2 + \frac{3}{4}b^2 \| V_2 \|^2 . \tag{2.9}$$

Hence $\| u \|^2 \geq \| V_2 \|^2$ if $|b| \neq 1$. If $b = \pm 1$ then we have

$$\| u \|^2 \geq a^2 \| V_1 \|^2 - |a| \| V_1 \|^2 + \| V_2 \|^2 = |a|(|a| - 1) \| V_1 \|^2 + \| V_2 \|^2 . \tag{2.10}$$

Since $a \in \mathbb{Z}$ we have $|a|(|a| - 1) = 0$ for $|a| \leq 1$ and $|a|(|a| - 1) > 0$ for $|a| \geq 2$, and so it follows that $\| u \|^2 \geq \| V_2 \|^2$ in this case also. Therefore V_2 is a shortest vector in L linearly independent of V_1.

Exemple 2.1.1 *Let $V_1 = (736, 849)$ and $V_2 = (157, 143)$ be a basis vectors of lattice $L \in \mathbb{R}^2$*

We first compute $\| V_1 \|^2 = 1262497$ and $\| V_2 \|^2 = 45098$. Since V_2 is shorter than V_1, we swap them, so

$$V_1 = (157, 143) \text{ and } V_2 = (736, 849).$$

Next we compute : $m = \left\lceil \frac{V_1.V_2}{\| V_1 \|^2} \right\rfloor = \lceil 5.25 \rfloor = 5,$

We subtract m multiple of V_1 from V_2 and we replace V_2 with.

$$V_2 = V_2 - mV_1 = (-49, 134).$$

This new vector has norm $\| V_2 \|^2 = 20357$, which is smaller than $\| V_1 \|^2 = 45098$, so we swap again :

$$V_1 = (-49, 134) \text{ and } V_2 = (157, 143).$$

We repeat the process with $m = \left\lceil \frac{V_1.V_2}{\| V_1 \|^2} \right\rfloor = \lceil 0.56 \rfloor = 1$, *which gives the new vector*

$$V_2 = V_2 - mV_1 = (206, 9).$$

having norm $\| V_2 \|^2 = 42517$, we compute again $m = \left\lceil \frac{V_1.V_2}{\| V_1 \|^2} \right\rfloor = \lceil 0.44 \rfloor = 0,$

*The final basis is quite small, and $V_1 = (-49, 134)$ is a solution to **SVP** for the lattice L.*

2.1.2 Three-dimentional lattices

Definition 2.1.2 *A 3-dimentional lattice in $\mathbb{R}^n$ generated by $b_1,\ b_2,\ b_3$ is the set of all integral linear combinations of $b_1,\ b_2,\ b_3$:*

$$L = \{a_1b_1 + a_2b_2 + a_3b_3 \mid a_1, a_2, a_3 \in \mathbb{Z}\}.$$

Let L be a 3-dimentional lattice in $\mathbb{R}^n$, and let $b_1,\ b_2,\ b_3$ be a basis of L

Definition 2.1.3 [8] *We say that a basis $b_1,\ b_2,\ b_3$ of a 3dimensional lattice L in $\mathbb{R}^n$, $n \geq 3$, is reduced if its vectors satisfy*

1. $\| b_1 \| \leq \| b_2 \| \leq \| b_3 \|$;
2. $\| b_2 + x_1b_1 \| \geq \| b_3 \|$ *and* $\| b_3 + x_2b_2 + x_1b_1 \| \geq \| b_3 \|$ *for all integers x_1, x_2.*

Algorithm for Reducing

Algorithm 2 3-dimentional lattices reducing algorithm.

- **Input:**Basis vectors b_1, b_2, b_3 of a 3-dimensional lattice in $R^n,\ n \geq 3$, ordered such that $\| b_1 \| \leq \| b_2 \| \leq \| b_3 \|$.
- **Output:** A reduced basis b_1, b_2, b_3 of this lattice.

i) ste (reduce the pair b_1, b_2) Evaluate $a, b = G(b_1, b_2)$, replace $b_1,\ b_2 \longleftarrow a, b$.

ii) ste (find a minimum of $\| \ b_3 + x_2b_2 + x_1b_1 \ \|$) Compute integers x_1, x_2 such that $\| b_3 + x_2b_2 + x_1b_1 \|$ is minimal. We have $\| x_2 - y_2 \| \leq 1$ and $\| x_1 - y_1 \| \leq 1$, where

$$y_1 = -\frac{\frac{(b_2,b_3)}{\| b_2 \|^2} - \frac{(b_1,b_2)}{\| b_2 \|^2}\cdot\frac{(b_1,b_3)}{\| b_1 \|^2}}{1 - \frac{(b_1,b_2)}{\| b_1 \|^2}\cdot\frac{(b_1,b_2)}{\| b_2 \|^2}},\ y_2 = -\frac{\frac{(b_1,b_3)}{\| b_1 \|^2} - \frac{(b_1,b_2)}{\| b_1 \|^2}\cdot\frac{(b_2,b_3)}{\| b_1 \|^2}}{1 - \frac{(b_1,b_2)}{\| b_1 \|^2}\cdot\frac{(b_1,b_2)}{\| b_2 \|^2}}.$$

iii) ste (replace $b_3 \longleftarrow a$) If $\| \ a \ \| \geq \| \ b3 \ \|$, then terminate, else replace $b_3 \longleftarrow a$. Order b_1, b_2, b_3 such that $\| b_1 \| \leq \| b_2 \| \leq \| b_3 \|$ and go to Step 1.

Remark: 2.1 *We suppose that the basis b1, b2, b3 is defined also by numbers*

$$|b_1|^2, |b_2|^2, |b_3|^2, (b_1, b_2), (b_1, b_3), (b_2, b_3).$$

We change the numbers in each step when changing the basis.

2.2 High dimensional lattice reduction algorithms

2.2.1 Gram-Schmidt Orthogonalization

Gram-Schmidt orthogonalization is a basic procedure in linear algebra that takes any set of n linearly independent vectors, and creates a set of n orthogonal vectors. It works by projecting each vector on the space orthogonal to the span of the previous vectors.

Definition 2.2.1 *Let $X_1, X_2, \cdots, X_n$ be a basis of $\mathbb{R}^n$. The Gram-Schmidt orthogonalization of $X_1, X_2, \cdots, X_n$ is the following basis $\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_n$*

$X_1 = \tilde{X}_1$,

$\tilde{X}_i = X_i - \sum_{j=1}^{i-1} \mu_{ij}\tilde{X}_j,\ (2 \leq i \leq n),\ \mu_{ij} = \dfrac{X_i \cdot \tilde{X}_j}{\tilde{X}_j \cdot \tilde{X}_j},\ (1 \leq j < i \leq n).$

We write $X_i = (x_{i1}, \cdots, x_{in})$ and form the matrix $X = (x_{ij})$, and similarly $\tilde{X} = (\tilde{x}_{ij})$. Then can be written as the matrix equation:

$$X = M\tilde{X},\ \ M = (\mu_{ij}).$$

The matrix M is lower triangular with $\mu_{ii} = 1$ for all i,

$$M = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ \mu_{2,1} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \cdots & 1 \end{pmatrix},$$

so it is invertible, and hence we also have $\tilde{X} = M^{-1}X$.

Properties 2.2.1 *The vectors of **GSO** basis verify:*

1. $\tilde{X}_i \cdot \tilde{X}_j = 0$ *for* $1 \leq i < j \leq n$.

   For $j = 2$ we have $\tilde{X}_1.\tilde{X}_2 = \tilde{X}_1.(X_2 - \mu_{1,1}\tilde{X}_1) = \tilde{X}_1.X_2 - \dfrac{\tilde{X}_1.X_2}{\tilde{X}_1.\tilde{X}_1}\tilde{X}_1.\tilde{X}_1 = 0$, *suppose that it is achieved for j, and we show for $j+1$.*

   $$\tilde{X}_i.\tilde{X}_{j+1} = \tilde{X}_i.(X_{j+1} - \sum_{k=1}^{j} \mu_{j+1,k}\tilde{X}_k) = \tilde{X}_i.X_{j+1} - \sum_{k=1}^{j} \mu_{j+1,k}\tilde{X}_k.\tilde{X}_i;$$

   we have $\tilde{X}_i.\tilde{X}_j = 0$, so we get

   $$\tilde{X}_i.\tilde{X}_{j+1} = \tilde{X}_i.X_{j+1} - \mu_{j+1,i}\tilde{X}_i.\tilde{X}_i = \tilde{X}_i.X_{j+1} - \frac{\tilde{X}_i.X_{j+1}}{\tilde{X}_i.\tilde{X}_i}.\tilde{X}_i.\tilde{X}_i = 0.$$

2. *span* $(\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k)$ = *span* $(X_1, X_2, \cdots, X_n)$ *for* $1 \leq k \leq n$.

   We have

   $$\tilde{X}_i = X_i - \sum_{j=1}^{i-1} \mu_{ij}\tilde{X}_j,\ \textit{so}\ X_i = \tilde{X}_i + \sum_{j=1}^{i-1} \mu_{ij}\tilde{X}_j = \sum_{j=1}^{i} \mu_{ij}\tilde{X}_j.$$

   Then we have: $X_i \in$ span $(\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k)$ for $1 \leq i \leq k$, and hence:

   $$\textit{span}\ (X_1, X_2, \cdots, X_k) \subseteq \textit{span}\ (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k).$$

   Conversely, for $k = 1$ we have $\tilde{X}_1 = X_1$ and so the claim is obvious. Assume that the claim holds for some $k \geq 1$.

   $$\tilde{X}_{k+1} = X_{k+1} - \sum_{j=1}^{k} \mu_{k+1,j}\tilde{X}_j = X_{k+1} + Y,\ \ Y \in \textit{span}\ (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k).$$

   By hypothesis we have: span $(\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k) \subseteq$ span $(X_1, X_2, \cdots, X_k)$, and so the last equation implies $\tilde{X}_{k+1} \in$ span $(X_1, X_2, \cdots, X_{k+1})$. So

   $$\textit{span}\ (\tilde{X}_1, \tilde{X}_2, \cdots, \tilde{X}_k) \subseteq \textit{span}\ (X_1, X_2, \cdots, X_k).$$

3. $\| \tilde{X}_k \| \leq \| X_k \|$ *for* $1 \leq k \leq n$.

   We see above:

$$X_k = \tilde{X}_k + \sum_{j=1}^{i-1} \mu_{kj} \tilde{X}_j \ \textit{implies} \ \ \| X_k \|^2 = \| \tilde{X}_k \|^2 + \sum_{j=1}^{i-1} \mu_{kj}^2 \| \tilde{X}_j \|^2 .$$

4. $\det(\tilde{X}) = \det(X)$.
   We have $X = M\tilde{X}$ *where* $M = (\mu_{ij})$ *is a lower triangular matrix with* $\mu_{ii} = 1$ *for* $1 \leq i \leq n$. *Hence* $\det(M) = 1$ *and therefore* $\det(X) = \det(M)\det(\tilde{X}) = \det(\tilde{X})$.

Definition 2.2.2 *Let* $X_1, \cdots, X_n$ *be a basis of* $\mathbb{R}^n$, *and let* X *be the* $n \times n$ *matrix. For* $1 \leq k \leq n$, *let* X_k *be the* $k \times n$ *matrix consisting of the first* k *rows The* ***k-th Gram matrix*** *of this basis is the* $k \times k$ *symmetric matrix*

$$G_k = X_k X_k^t.$$

The k-th Gram determinant of this basis is $d_k = \det(G_k)$

Proposition: 2.2.1 *Let* $X_1, \cdots, X_n$ *be a basis of* $\mathbb{R}^n$, *and let* $\tilde{X}_1, \cdots, \tilde{X}_n$ *be its Gram-Schmidt orthogonalization. For*$1 \leq k \leq n$ *the k-th Gram determinant of the basis is the product of the square-lengths of the* ***GSO*** *vectors:*

$$d_k = \prod_{i=1}^{k} \| \tilde{X}_i \|^2 .$$

So for a lattice L of n-dmontional we have:

$$\det L^2 = \det G(L) = \prod_{i=1}^{n} \| \tilde{X}_i \|^2 .$$

In another meaning

$$\det L = \prod_{i=1}^{n} \| \tilde{X}_i \| .$$

Proposition: 2.2.2 *Let L be the lattice generated by* $X_1, \cdots, X_n$, *and let* $\tilde{X}_1, \cdots, \tilde{X}_n$ *be its Gram-Schmidt orthogonalization. For any nonzero* $Y \in L$ *we have*

$$\| y \| \geq \min \left\{ \| \tilde{X}_1 \|, \cdots, \| \tilde{X}_n \| \right\}.$$

Proof: Let $(Y \neq 0) \in L$. Y is a linear combination of the basis vectors

$$Y = \sum_{i=1}^{n} a_i X_i \mid a_i \in \mathbb{Z}, 1 \leq i \leq n. \tag{2.11}$$

We can express $X_1, \cdots, X_n$ in terms of $\tilde{X}_1, \cdots, \tilde{X}_n$.

$$Y = \sum_{i=1}^{k} a_i \sum_{j=1}^{i} \mu_{ij} \tilde{X}_j = \sum_{i=1}^{k} \sum_{j=1}^{i} a_i \mu_{ij} \tilde{X}_j. \tag{2.12}$$

using $\mu_{kk} = 1$, we obtain

$$Y = \sum_{i=1}^{k} (\sum_{j=i}^{k} a_i \mu_{ij}) \tilde{X}_j = a_k \tilde{X}_k + \sum_{i=1}^{k-1} (a_i \mu_{ij}) \tilde{X}_j. \tag{2.13}$$

Since $\tilde{X}_1, \cdots, \tilde{X}_n$ are orthogonal, a_k is a nonzero integer, we have $a_k^2 \geq 1$, and so

$$\| Y \|^2 \geq (\| \tilde{X}_k \|^2 + \sum_{i=1}^{k-1} (a_i \mu_{ij})^2 \| \tilde{X}_j \|^2) \geq 0. \tag{2.14}$$

$\| Y \|^2 \geq \| \tilde{X}_k \|^2 \geq \min \left\{ \| \tilde{X}_1 \|^2, \cdots, \| \tilde{X}_n \|^2 \right\}$, implies $\| Y \| \geq \| \tilde{X}_k \| \geq \min \left\{ \| \tilde{X}_1 \|, \cdots, \| \tilde{X}_n \| \right\}$.

Exemple 2.2.1 *Lat the 2-dimontional lattice in Figure 2.1*

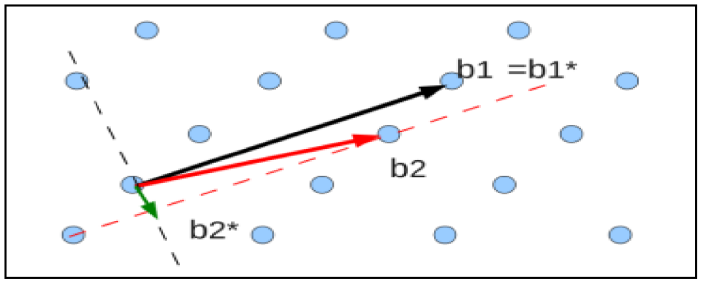

Figure 2.1: Present an orthogonal lattice basis of Gram-Schmidt in $\mathbb{R}^2$.

The vectors of $B^\star$ are orthogonal vectors, and for $i = 1, \cdots, n$, the vectors $(b_1^\star, \cdots, b_i^\star)$ generate the same vector space as the vectors $(b_1, \cdots, b_i)$. But, $B^\star$ is generally not a basis of the lattice.

For the lattice given in Figure 2.1 generated by the vectors (b_1, b_2), the orthogonal basis $(b_1^\star, b_2^\star)$ is not a basis of the lattice. In furthermore, the Gram-Schmidt orthogonalization depends on the order of the vectors of basis B.

Theorem: 2.2.1 ***(Minkowski's first theorem)*** *Let L be a lattice of rank n in $\mathbb{R}^n$. Then*

$$\wedge_1(L) \leq \sqrt{n} \det(L)^{1/n}.$$

Definition 2.2.3 ***(Hermite's lattice constant)****, is the supremum of the following quantities as L ranges over all m-dimensional lattices:*

$$\gamma_m = \frac{\wedge_1^2(L)}{\det(L)^{2/m}}.$$

Definition 2.2.4 ***(Orthogonality defect and basis length defect)****. Let $X = (X_1, \cdots, X_n)$ be a basis of the lattice L. The quality of a basis can be measured by the three parameters defined as follows: (The followin parameters, the orthogonality defect $\delta(X)$, length defects $\lambda_i(X)$ and Hermit defect $\gamma(X)$, measure the quality of the basis.)*

$$\delta(X) = \prod_{i=1}^{n} \frac{\| X_i \|}{\| \tilde{X}_i \|}, \qquad \lambda_i(X) = \frac{\| X_i \|}{\wedge_i(L)}, \qquad \gamma_m = \frac{\wedge_1^2(L)}{\det(L)^{2/m}}.$$

The orthogonality defect is always greater than 1, and equals 1 if and only if the basis is orthogonal. The basis will be almost orthogonal if $\delta(X)$ is close to 1. A basis will be almost minimal if all its defects of length $\lambda_i(X)$ are close to 1.

Proposition: 2.2.3 *We have*

$$1 \leq \frac{\delta(X)}{\prod_{i=1}^{n} \lambda_i(X)} \leq \gamma_m^m.$$

2.2.2 Hermite-Korkine-Zolotarev reduction (HKZ)

A basis $X_1, \cdots, X_n$ of a lattice L is said to be HKZ-reduced if the following conditions are verify

1. $\| \mu_{ij} \| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$.
2. The vector X_1 is a shortest vector of the lattice L.
3. the basis $(\tilde{X}_2, \cdots, \tilde{X}_n)$ is Korkine-Zolotarev reduced (this is the orthogonal projection of the basis of L onto the orthogonal complement of X_1).

An HKZ-reduced basis provides a good approximation of the successive minima. Since we know the following inequality for length defects:

$$\frac{4}{i+3} \leq \lambda_i(X) = \frac{\| X_i \|}{\wedge_i(L)} \leq \frac{i+3}{4}, \qquad \text{for} 1 < i \leq n.$$

2.2.3 BKZ Block reduction

A type of reduction, called by **blocks**, which is an intermediate reduction between the **LLL** reduction and the **HKZ** reduction. Block size β is fixed in the algorithm, but can vary, and depending on the choice of block size, we find the notion of **LLL**-reduction for $\beta = 2$ or that of **HKZ** for $\beta = n$.

The **block Korkine–Zolotarev** replaces the swap step in the standard **LLL** algorithm by a block reduction step. One way to view the swap and size reduction process in **LLL** is **Gaussian** lattice reduction on the 2-dimensional lattice spanned by X_{k-1} and X_k. In **BKZ-LLL**, one works instead with a block of vectors of length β, say

$$X_k, X_{k+1}, \cdots, X_{k+\beta-1},$$

and one replaces the vectors in this block with a **HKZ**-reduced basis spanning the same sub-lattice.

A notion of reduction operates a compromise between the quality of the reduction and the complexity to obtain it. For example, the reduction within the meaning of **Korkine** and **Zolotarev** produces a base whose quality is much higher to that produced by the reduction within the meaning of **LLL**, if β is large, there is an obvious disadvantage in that it takes a long time to compute a **HKZ**-reduced basis.

Theorem: 2.2.2 [7] *If the **BKZ** algorithm is run on a lattice L of dimension n using blocks of size β, then the algorithm is guaranteed to terminate in no more than $O(\beta^{c\beta} n^d)$ steps, where c and d are small constants.*

2.3 The LLL Algorithm

Definition 2.3.1 [9] *The reduction parameter is a real number α such that*

$$\frac{1}{4} < \alpha < 1.$$

The standard value of the parameter is: $\alpha = \frac{3}{4}$.

Let $X_1, \cdots, X_n$ *be an ordered basis of the lattice L in* $\mathbb{R}^n$*, and let*$\tilde{X}_1, \cdots, \tilde{X}_n$ *be its Gram-Schmidt orthogonalization. The basis* $X_1, \cdots, X_n$ *is called* α***-reduced*** *(or LLL-reduced with parameter* α*) if it satisfies*

1. $\| \mu_{ij} \| \leq \frac{1}{2}$ *for* $1 \leq j < i \leq n$.
2. $\| \tilde{X}_i + \mu_{i,i-1}\tilde{X}_{i-1} \|^2 \geq \alpha \| \tilde{X}_{i-1} \|^2$ *for* $2 \leq i \leq n$.

Condition 2 is called the **exchange condition** (Lovás condition). Since $\tilde{X}_1, \cdots, \tilde{X}_n$ are orthogonal, condition 2 can be written as

$$2.^* \ \| \tilde{X}_i \|^2 \geq (\alpha - \mu_{i,i-1}^2) \| \tilde{X}_{i-1} \|^2 \ \text{ for } 2 \leq i \leq n.$$

Condition 1 says that each basis vector X_i is **almost orthogonal** to the span of the previous vectors. Is called the **(Size Condition)**.
Conditions 2 and 2^* say that exchanging X_{i-1} and X_i and then recomputing the **GSO** can produce a new shorter vector

$$\tilde{X}_{i-1}^* = \tilde{X}_i + \mu_{i,i-1}\tilde{X}_{i-1}.$$

Definition 2.3.2 [9] *The auxiliary parameter* β *define as follows:*

$$\beta = \frac{4}{4\alpha - 1}, \ \ implies \ \ \frac{1}{\beta} = \alpha - \frac{1}{4}$$

For the standard value $\alpha = \frac{3}{4}$ *we obtain* $\beta = 2$.

Theorem: 2.3.1 [7] *Let L be n-dimension lattice, for* $\beta = 2$*. Any LLL reduced basis* $X_1, \cdots, X_n$ *for L has the following properties:*

1. $\| x_j \|^2 \leq 2^{i-j} \| \tilde{X}_i \|^2$ *for*$1 \leq j \leq i \leq n$,
2. $\det(L) \leq \prod_{i=1}^n \| X_n \| \leq 2^{n(n-1)/4} \det(L)$,
3. $\| X_1 \| \leq 2^{(n-1)/4}(\det(L)^{1/n})$.

Proof: For $\alpha = \frac{3}{4}, \beta = 2$ The Lovász condition and the fact that $|\mu_{i,i-1}| \leq \frac{1}{2}$ imply that

$$\| \tilde{X}_i \|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2) \| \tilde{X}_{i-1} \|^2 \geq (\frac{3}{4} - \frac{1}{4}) \| \tilde{X}_{i-1} \|^2 = \frac{1}{2} \| \tilde{X}_{i-1} \|^2 . \tag{2.15}$$

So it gives $\| \tilde{X}_{i-1} \|^2 \leq 2 \| \tilde{X}_i \|^2$ implies that $\| \tilde{X}_j \|^2 \leq 2^{i-j} \| \tilde{X}_i \|^2$, $(1 \leq j \leq i \leq n)$.

We now compute

$$\| X_i \|^2 = \| \tilde{X}_i + \sum_{j=0}^{i-1} \mu_{i,j}\tilde{X}_j \|^2 \tag{2.16}$$

$$= \| \tilde{X}_i \|^2 + \sum_{j=0}^{i-1} \mu_{i,j}^2 \| \tilde{X}_j \|^2 \tag{2.17}$$

$$\leq \| \tilde{X}_i \|^2 + \sum_{j=0}^{i-1} \frac{1}{4} 2^{i-j} \| \tilde{X}_i \|^2 \tag{2.18}$$

$$\leq (1 + \sum_{j=0}^{i-1} \frac{1}{4} 2^{i-j}) \| \tilde{X}_i \|^2 \tag{2.19}$$

Using the summation formula for a geometric sequence, we obtain

$1 + \sum_{j=0}^{i-1} \frac{1}{4} 2^{i-j} = 1 + \frac{1}{4} \frac{2^i - 2}{2 - 1} \leq 2^{i-1}$. We now have $\| X_i \|^2 \leq 2^{i-1} \| \tilde{X}_i \|^2$

$$\det(L) = \| \tilde{X}_1 \| \cdots \| \tilde{X}_n \| \leq \| X_1 \| \cdots \| X_n \| \tag{2.20}$$

$$\| X_1 \|^2 \cdots \| X_n \|^2 \leq 2^0 \| \tilde{X}_1 \|^2 \cdots 2^{n-1} \| \tilde{X}_n \|^2 = 2^{n(n-1)/2} \| \tilde{X}_1 \|^2 \cdots \| \tilde{X}_n \|^2 \tag{2.21}$$

and therefore

$$\prod_{i=1}^{n} \| X_i \|^2 \leq 2^{n(n-1)/2} \prod_{i=1}^{n} \| \tilde{X}_i \|^2, \text{ implies } \prod_{i=1}^{n} \| X_i \| \leq 2^{n(n-1)/4} \prod_{i=1}^{n} \| \tilde{X}_i \|, \tag{2.22}$$

Then $\det(L) \leq \prod_{i=1}^{n} \| X_n \| \leq 2^{n(n-1)/4} \det(L)$.

We have also frome above $\| X_1 \|^2 \leq 2^{i-1} \| \tilde{X}_i \|^2$, so $\| X_1 \|^{2n} \leq 2^{n(n-1)/2} \det(L)^2$.

Now taking $2n$-th roots we find

$$\| X_1 \| \leq 2^{(n-1)/4} \det(L)^{1/n}. \tag{2.23}$$

This completes the proof.

The LLL algorithm

Algorithm 3 The LLL algorithm.

- **Input:**A basis $X_1, \cdots, X_n$ for a lattice L
- **Output:**A LLL reduced basis $X_1, \cdots, X_n$.

i) Set $k = 2$
ii) Set $\tilde{X}_1 = X_1$
iii) Loop while $k \leq n$
iv) Loop $j = 1, 2, 3, \cdots, k-1$
v) Set $X_k = X_k - \lceil \mu_{k,j} \rfloor \tilde{X}_j$ [Size Reduction]
vi) End j Loop
vii) If $\| \tilde{X}_k \|^2 \geq (\frac{3}{4} - \mu^2_{k,k-1}) \| \tilde{X}_{k-1} \|^2$ [Lov'asz Condition]
viii) Else
ix) Swap X_{k-1} and X_k [Swap Step]
x) Set $k = \max(k-1, 2)$
xi) End If
xii) End k Loop

Note: At each step, $\tilde{X}_1, \cdots, \tilde{X}_k$ is the orthogonal set of vectors obtained by applying **Gram–Schmidt** to the current values of $X_1, \cdots, X_n$, and $\mu_{i,j} = (\tilde{X}_i . \tilde{X}_j) / \| \tilde{X}_j \|^2$.

The LLL algorithm (**Algorithm**3) works as follows:
Given a basis $X_1, X_2, \cdots, X_n$, it is easy to form a New basis that satisfies the **Size Condition**. Roughly speaking, we do this by subtracting from X_k appropriate integer multiples of the previous vectors $X_1, X_2, \cdots, X_{k-1}$ so as to make X_k smaller.
In the LLL algorithm, we do this in stages, rather than all at once, and we see that the size reduction condition depends on the ordering of the vectors. After doing size reduction, we check to see whether the **Lovász condition** is satisfied. If it is, then we have a (nearly) optimal ordering of the vectors. If not, then we reorder the vectors and do further size reduction.

The goal of LLL is to produce a list of short vectors in increasing order of length. For each $1 \leq i \leq n$, let L_i denote the lattice spanned by $X_1, X_2, \cdots, X_i$. Note that as LLL progresses, the sublattices L_i change due to the swap step; only L_n remains the same, since it is the entire lattice. What LLL attempts to do is to find an ordering of the basis vectors (combined with size reductions whenever possible) that minimizes the determinants $\det(L_i)$ i.e, LLL attempts to minimize the volumes of the fundamental domains of the sublattices $L_1, \cdots, L_n$.

Algorithm parameters

1. **Output Parameters**

   The geometry of the output basis is described with three main parameters , the orthogonality defect $\delta(X)$, length defects $\lambda_i(X)$ and Hermit defect $\gamma(X)$, They satisfy the following features, which are expressed as a function of $s = 2\alpha\sqrt{4-\alpha^2}$

$$\delta(X) = \prod_{i=1}^{n} \frac{\| X_i \|}{\| \tilde{X}_i \|} \leq s^{m(m-1)/2}, \quad \lambda_i(X) = \frac{\| X_i \|}{\wedge_i(L)} \leq s^{m-1}, \quad \gamma_m = \frac{\wedge_1^2(L)}{\det(L)^{2/m}} \leq s^{m-1}.$$

This proves that the output satisfies good Euclidean properties. In particular, the length of the first vector of $\tilde{X}$ is an approximation of the first minimum $\wedge_1(L)$ to a factor that exponentially depends on dimension m.

2. **The number of iterations**

On a base X of a lattice $L \in \mathbb{R}^n$ of dimension m, the number of iterations K of the LLL (α) algorithm checks the following inequalities:

$$K \leq (m-1) + m(m-1)\log_t \frac{A}{a},$$

with $A = \left\{\max \parallel \tilde{X}_i \parallel\right\}, \quad a = \left\{\min \parallel \tilde{X}_i \parallel\right\}, \ 1 \leq i \leq m, \quad \tilde{X}_i \in \tilde{X}$ the GSO basis.

Theorem: 2.3.2 [7] *The algorithm LLL terminates in a finite number of steps and returns an LLL reduced basis for L.*
Let $B = \max \parallel X_i \parallel$. Then the algorithm executes the main k loop (Steps (iii))–(xii))) no more than $O(n^2 logn + n^2 logB)$ times. In particular, the LLL algorithm is a polynomial time algorithm.

Exemple 2.3.1 *Using LLL to find a nearest orthogonal basis for the lattice $L \in \mathbb{R}^3$ spanned by $X_1 = (13, 21, 8),\ X_2 = (48, 17, 5)$ and $X_3 = (34, 3, 3)$*

*We ferstly combut the **GS** basis :*
we take $\tilde{X}_1 = X_1$

$$\tilde{X}_2 = X_2 - \mu_{2,1}X_1, \qquad \mu_{2,1} = \frac{X_2 \cdot \tilde{X}_1}{\tilde{X}_1 \cdot \tilde{X}_1},$$

$$\tilde{X}_2 = (48, 17, 5) - \frac{(48, 17, 5)(13, 21, 8)}{(13, 21, 8)(13, 21, 8)}(13, 21, 8) \approx (28.37, -14.71, -7.08).$$

Now use X_1 to reduce X_2:

$$X_2 = (48, 17, 5) - \left\lceil \frac{(48, 17, 5)(13, 21, 8)}{(13, 21, 8)(13, 21, 8)} \right\rfloor (13, 21, 8) = (35, -4, -3).$$

This is our new X_2
check lovàsz condition:

$$\parallel \tilde{X}_1 \parallel^2 = 674 \qquad \parallel \tilde{X}_2 \parallel^2 \approx 1071.37 \qquad \mu_{2,1} = \frac{(35, -4, -3)(13, 21, 8)}{(13, 21, 8)(13, 21, 8)} \approx 0.54.$$

So $(\frac{3}{4} - \mu_{2,1}^2) \approx 0.46, \qquad \parallel \tilde{X}_2 \parallel^2 \geq (\frac{3}{4} - \mu_{2,1}^2) \parallel \tilde{X}_1 \parallel^2 .$

So we can move to the next vector X_3

*We must recompute the **GS** basis. We take $\tilde{X}_1 = X_1$, and must find $\tilde{X}_2$ and $\tilde{X}_3$*

$$\tilde{X}_2 = (28.37, -14.71, -7.08).$$

$\tilde{X}_3 = X_3 - \mu_{3,1}\tilde{X}_1 - \mu_{3,2}\tilde{X}_1$, *where* $\mu_{3,1} = \dfrac{X_3 \cdot \tilde{X}_1}{\tilde{X}_1 \cdot \tilde{X}_1}$, *and* $\mu_{3,2} = \dfrac{X_3 \cdot \tilde{X}_2}{\tilde{X}_2 \cdot \tilde{X}_2}$,

$$\tilde{X}_3 = (1.1, -0.44, 2.99).$$

Now use X_1 to reduce X_3

$$X_3 = X_3 - \left\lceil \frac{X_3.\tilde{X}_1}{\tilde{X}_1.\tilde{X}_1} \right\rfloor X_1 = (34,3,3) - \left\lceil \frac{(34,3,3).(13,21,8)}{(13,21,8).(13,21,8)} \right\rfloor (13,21,8) = (21,-18,-5).$$

Then use X_2 to reduce the new X_3

$$X_3 = (21,-18,-5) - \left\lceil \frac{(21,-18,-5).(28.37,-14.71,-7.08)}{(28.37,-14.71,-7.08).(28.37,-14.71,-7.08)} \right\rfloor (35,-4,-3)$$

$$= (-14,-14,-2).$$

check lovàsz condition:

$$\| \tilde{X}_2 \|^2 \approx 1071.37, \qquad \| \tilde{X}_3 \|^2 = 10.34$$

$$\mu_{3,2} = \frac{(-14,-14,-2)(28.37,-14.71,-7.08)}{(28.37,-14.71,-7.08)(28.37,-14.71,-7.08)} \approx -0.17$$

So $(\frac{3}{4} - \mu_{3,2}^2) \approx 0.72, \qquad \| \tilde{X}_3 \|^2 \not\geq (\frac{3}{4} - \mu_{3,2}^2) \| \tilde{X}_2 \|^2.$

We swap X_3 and X_2, we have now : $X_2 = (-14,-14,-2), \qquad X_3 = (35,-4,-3).$

*We try now to reduce X_2. Apply **GS** basis:*

take $\tilde{X}_1 = X_1$ and we find: $\tilde{X}_2 \approx (-4.51, 1.33, 3.84),$

use X_1 to reduce X_2:

$$X_2 = (-14,-14,-2) - \left\lceil \frac{(-14,-14,-2).(13,21,8)}{(13,21,8).(13,21,8)} \right\rfloor (13,21,8) = (-1,7,6).$$

Checking the lovàsz condition:

$$\| \tilde{X}_1 \|^2 = 674, \qquad \| \tilde{X}_2 \|^2 \approx 36.85.$$

$$\mu_{2,1} = \frac{(-14,-14,-2)(13,21,8)}{(13,21,8)(13,21,8)} \approx -0.73$$

Since $(\frac{3}{4} - \mu_{2,1}^2) \approx 0.21, \qquad \| \tilde{X}_2 \|^2 \not\geq (\frac{3}{4} - \mu_{2,1}^2) \| \tilde{X}_1 \|^2.$

We swap X_3 and X_2 . We have now : $X_1 = (-1,7,6), \qquad X_2 = (13,21,8).$

*Start again. Finding **GS** basis*

take $\tilde{X}_1 = X_1 = (-1,7,6)$ and we find: $\tilde{X}_2 \approx (15.12, 6.16, -4.72),$

use X_1 to reduce X_2:

$$X_2 = (13,21,8) - \left\lceil \frac{(13,21,8).(-1,7,6)}{(-1,7,6).(-1,7,6)} \right\rfloor (-1,7,6) = (15,7,-4).$$

Checking the lovàsz condition:

$$\| \tilde{X}_1 \|^2 = 86, \qquad \| \tilde{X}_2 \|^2 \approx 288.84, \qquad \mu_{2,1} \approx 2.12.$$

Since $(\frac{3}{4} - \mu_{2,1}^2) \approx -1.37, \qquad \| \tilde{X}_2 \|^2 \geq (\frac{3}{4} - \mu_{2,1}^2) \| \tilde{X}_1 \|^2$
we keep them and use to reduce X_3
***GS** basis:* $\tilde{X}_1 = (-1, 7, 6), \qquad \tilde{X}_2 = (15.12, 6.16, -4.72), \qquad \tilde{X}_3 = (9.87, -7.28, 10.19).$

Reduce X_3 *by* X_1*:*

$$X_3 = (35, -4, -3) - \left\lceil \frac{(35, -4, -3).(-1, 7, 6)}{(-1, 7, 6).(-1, 7, 6)} \right\rfloor (-1, 7, 6) = (34, 3, 3).$$

Reduce X_3 *by* X_1*:*

$$X_3 = (34, 3, 3) - \left\lceil \frac{(34, 3, 3).(15.12, 6.16, -4.72)}{(15.12, 6.16, -4.72).(15.12, 6.16, -4.72)} \right\rfloor (15, 7, -4) = (4, -11, 15).$$

Checking the lovàsz condition:

$$\| \tilde{X}_2 \|^2 = 288.84, \qquad \| \tilde{X}_3 \|^2 \approx 254.25, \qquad \mu_{2,1} \approx -0.27.$$

Since $(\frac{3}{4} - \mu_{2,1}^2) \approx 0.68, \qquad \| \tilde{X}_3 \|^2 \geq (\frac{3}{4} - \mu_{2,1}^2) \| \tilde{X}_2 \|^2.$

We see that X_3 *and* X_2 *satisfy the lovàsz condition.*

So $X_1 = (-1, 7, 6),\ X_2 = (15, 7, -4)$ *and* $X_3 = (4, -11, 15)$ *form areasonably orthogonal basis for the lattice* L*.*

2.3.1 Using LLL to solve SVP and CVP

We explained that if a lattice L has an orthogonal basis, then it is very easy to solve both SVP and CVP. The LLL algorithm does not return an orthogonal basis, but it does produce a basis reasonably orthogonal to one another. Thus we can use the LLL to solves CVP and SVP.

Babai's algorithm

If a lattice $L \subset \mathbb{R}^n$ has a basis $X_1, \cdots, X_n$ consisting of vectors that are pairwise orthogonal, then it is easy to solve both SVP and CVP. Thus to solve SVP, we observe that the length of any vector in L is given by the formula

$$\| a_1 X_1 + \cdots + a_n X_n \|^2 = a_1^2 \| X_1 \|^2 + \cdots + a_n^2 \| X_n \|^2 . \tag{2.24}$$

Since $a_1, \cdots, a_n \in \mathbb{Z}$, suppose that we want to find the vector in L that is closest to a given vector $W \in \mathbb{R}^n$.

$$W = t_1 X_1 + \cdots + t_n X_n \text{ with } t_1, \cdots, t_n \in \mathbb{R}. \tag{2.25}$$

Then for $X = a_1 X_1 + \cdots + a_n X_n \in L$, we have

$$\| X - W \|^2 = (a_1 - t_1)^2 \| X_1 \|^2 + \cdots + (a_n - t_n)^2 \| X_n \|^2 . \tag{2.26}$$

The a_i are required to be integers, so (2.26) is minimized if we take each a_i to be the integer closest to the corresponding t_i. So for any vector $Y \in L \| X - W \| \leq \| Y - W \|$, so X is the closest vector of W.

If the vectors in the basis are nearests orthogonal, then we may successful in solving **CVP**, but if the basis vectors are not orthogonal or nearests to be, then the algorithm does not work well.

A basis $X_1, \cdots, X_n$ for L determines a fundamental domain $\mathcal{F}$, the translates of $\mathcal{F}$ by the elements of L fill up the entire space $\mathbb{R}^n$, so any $W \in \mathbb{R}^n$ is in a unique translate $\mathcal{F} + X$ of $\mathcal{F}$ by an element $X \in L$. We take the vertex of the parallelepiped $L + X$ that is closest to W as our hypothetical solution to **CVP**. This procedure is illustrated in Figure 2.2. It is easy to find the closest vertex.

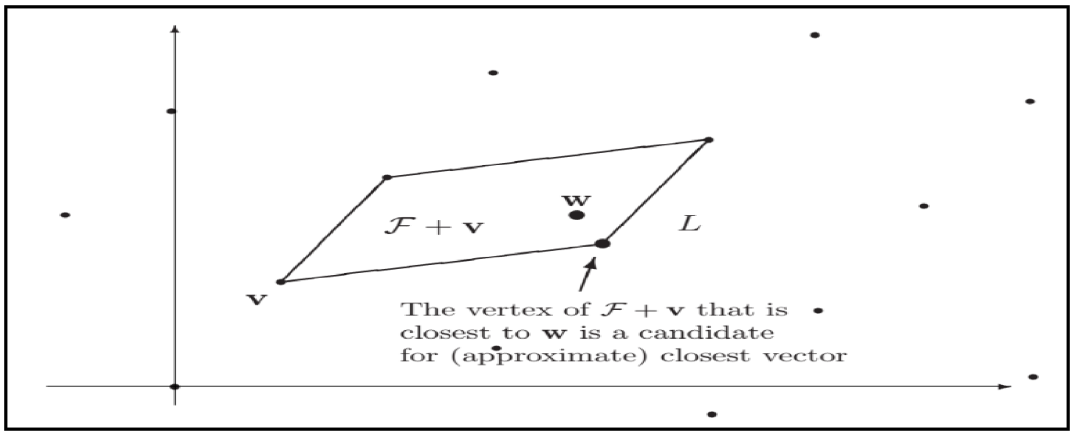

Figure 2.2: Using a given fundamental domain to try to solve CVP.

Theorem: 2.3.3 [14] *Suppose that the basis $X_1, \cdots, X_n$ of the lattice $L \subset \mathbb{R}^n$ is LLL-reduced with standard reduction parameter $\alpha = \frac{3}{4}$. Let $W \in \mathbb{R}^n$ be an arbitrary vector. Then the lattice vector $X \in L$ produced by the nearest plane algorithm on input W satisfies*

$$\| X - W \| \leq 2^{\frac{n}{2}} \min_{Y \in L} \| Y - W \| .$$

Algorithm 4 Babai's Algorithm.

- **Input:**A basis $X_1, \cdots, X_n \in \mathbb{R}^n$ for a lattice L and the target vector $W \in \mathbb{R}^m$.
- **Output:** A vector $X \in L$ such that $\| X - W \| \leq 2^{\frac{n}{2}} \min_{Y \in L} \| Y - W \|$.
  - Run α-LLL on $X_1, \cdots, X_n$ with $\alpha = \frac{3}{4}$.
  - $X \longleftarrow W$.

for $j = n$ to 1 **do**

$X \longleftarrow X - \mu_j X_j$ where $\mu_j = \dfrac{X.\tilde{X}_j}{\tilde{X}_j.\tilde{X}_j}$

Output $W - X$.

An alternative to the nearest plane method is the **rounding technique**. This is simpler to compute in practice, since it does not require the computation of a Gram-Schmidt basis, but harder to analyse in theory. This method is not guaranteed to solve CVP.

Let $X_1, \cdots, X_n$ be a basis for a full rank lattice in $\mathbb{R}^n$. Given a target $W \in \mathbb{R}^n$ we can write

$$W = \sum_{i=1}^{n} t_i X_i$$

with $t_i \in \mathbb{R}$. One computes the coefficients t_i by solving the system of linear equations. The rounding technique is simply to set

$$X = \sum_{i=1}^{n} \lceil t_i \rfloor X_i$$

where $\lceil t_i \rfloor$ means take the closest integer to the real number t. This procedure can be performed using any basis for the lattice. Babai has proved that $\| X - W \|$ is within an exponential factor of the minimal value if the basis is LLL-reduced. The method trivially generalises to non-full-rank lattices as long as W lies in the R-span of the basis. The method trivially generalises to non-full-rank lattices as long as W lies in the $\mathbb{R}$-span of the basis.

Theorem: 2.3.4 [15] *Let $X_1, \cdots, X_n$ be an LLL-reduced basis (with factor $\alpha = \frac{3}{4}$) for a lattice$L \subseteq \mathbb{R}^n$. Then the output X of the Babai rounding method on input $W \in \mathbb{R}^n$ satisfies*

$$\| X - W \| \leq (1 + 2n(9/2)^{n/2}) \| Y - W \| .$$

for all $Y \in L$.

Exemple 2.3.2 *Let use the same lattice reduced in th Exemple (2.3.1), we try to find a closest vector for $W = (2, 76, 62) \in \mathbb{R}^3$. We tacke the reduced basis of the lattice L*
We solve the equation:

$$W = a_1 X_1 + a_2 X_2 + a_3 X_3$$
$$= a_1(-1, 7, 6) + a_2(15, 7, -4) + a_3(4, -11, 15)$$

which corresponds to the system:

$$\begin{cases} -a_1 + 15a_2 + 4a_3 = 2; \\ 7a_1 + 7a_2 - 11a_3 = 76; \\ 6a_1 - 4a_2 + 15a_3 = 62. \end{cases}$$

We used Cramer's method to solved the system. We find

$$a_1 = \frac{-30160}{-2906} \approx 10.37;\ a_2 = \frac{-2296}{-2906} \approx 0.79 \text{ and } a_3 = \frac{-548}{-2906} \approx 0.22.$$

We take the nearest integer

$$a_1 = 10; \quad a_2 = 1; \quad a_3 = 0.$$

Then:

$$10(-1, 7, 6) + 1(15, 7, -4) + 0(4, -11, 15) = (5, 77, 56).$$

is a vector close to $W = (2, 76, 62)$.

LLL as an Approximation to SVP

The LLL algorithm is an approximation algorithm for the problem SVP. Even if the first vector returned by LLL is not necessarily a shorter vector of the lattice, we know that its norm can be compared to the first minimum, with however an exponential factor in the dimension n.

Theorem: 2.3.5 [14] *Let $X_1, \cdots, X_n$ LLL-reduced lattice basis. Further, in that case*

$$\min \| Y \| \geq 2^{n-1/2} \| X_1 \| .$$

where Y is a linear combination of lattice basis vector ($Y \in L - \{0\}$)

Proof: let $X_1, \cdots, X_n$ LLL-reduced lattice basis. $\tilde{X}_1, \cdots, \tilde{X}_n$ be it's **GS** basis, we have the following results .

1. For any k, $\| \tilde{X}_k \|^2 \geq \frac{1}{2} \| \tilde{X}_{k-1} \|^2$.
2. More generally $\| \tilde{X}_k \|^2 \geq \frac{1}{2^{k-1}} \| \tilde{X}_1 \|^2$.
3. For any lattice vector X_i we have $\| X_k \|^2 < 2^{k-1} \| \tilde{X}_k \|^2$.

Consider any vector Y in the lattice where

$$Y = \sum_{i=1}^{n} a_i X_i, \;\; a_i \in \mathbb{Z}, \;\; 1 \leq i \leq n \tag{2.27}$$

since the **GS** basis is a lattice basis, we must be able to express Y as linear combination of the **GS** vectors

$$Y = \sum_{i=1}^{n} \mu_i \tilde{X}_i, \;\; \mu_i \in R, \;\; 1 \leq i \leq n. \tag{2.28}$$

We want to find relationship between a_i and μ_i
since we have:

$$\sum_{i=1}^{n} a_i X_i = \sum_{i=1}^{n} \mu_i \tilde{X}_i. \tag{2.29}$$

meanwhile from: $\tilde{X}_i = X_i - \sum_{i=1}^{n} \mu_{ij} \tilde{X}_j$

from the dot product with $\tilde{X}_k$ we obtain

$$\tilde{X}_i . \tilde{X}_k = X_i . \tilde{X}_k - \sum_{i=1}^{n} \mu_{ij} \tilde{X}_j . \tilde{X}_k = X_i . \tilde{X}_k. \;\; implies \;\; X_i = \tilde{X}_i. \tag{2.30}$$

consequently, if $i \neq k$ then $X_i \tilde{X}_k = 0$ while $k = i \; \tilde{X}_i \tilde{X}_k = \| \tilde{X}_k \|^2$.

From(2.29) and from the dot product in (2.30). The dot product will all be zero, execept for the dot product will the $k - th$ basis vector giving us

$$a_k X_k . \tilde{X}_k = b_k \tilde{X}_k . \tilde{X}_k, \tag{2.31}$$

$$a_k \tilde{X}_k . \tilde{X}_k = b_k \tilde{X}_k . \tilde{X}_k. \tag{2.32}$$

consequently, $\mu_k = a_k$.

Since Y is non zero lattice vector. We have $Y = \sum_{i=1}^{n} a_i X_i$, where at least one of the $a_i's$ is non zero integer, since the same coefficients can be used to obtain Y using the **GS** basis we also have $Y = \sum_{i=1}^{n} a_i \tilde{X}_i$, consequently

$$\| Y \|^2 \geq a_k^2 \| \tilde{X}_k \|^2, \tag{2.33}$$

$$\| Y \|^2 \geq \| \tilde{X}_k \|^2 \qquad (a_k^2 \geq 1), \tag{2.34}$$

$$\| Y \|^2 \geq \frac{1}{2^{k-1}} \| \tilde{X}_1 \|^2 \qquad \text{(from (2.30) and result2)}, \tag{2.35}$$

$$\| Y \|^2 \geq \frac{1}{2^{n-1}} \| \tilde{X}_1 \|^2, \tag{2.36}$$

$$\| Y \|^2 \geq \frac{1}{2^{k-1}} \| X_1 \|^2 . \tag{2.37}$$

Thus any non zero vector in the lattice satisfy

$$\| Y \|^2 \geq \frac{1}{2^{(n-1)/2}} \| X_1 \|^2 . \tag{2.38}$$

So the shortest vector also satisfy this inequality. This means that X_1 will no more then $2^{(n-1)/2}$ times the length of the shortest vector, so the LLL-reduced basis will allow us to solve the SVP within a factor of $2^{(n-1)/2}$.

Chapter 3

Lattices and cryptography

Cryptology is defined as the science of secrecy. It is an essential science and technique in information security, it combines two main types of activity: cryptography and cipher analysis.

Encryption aims to design protocols, prove their security, or even improve their algorithm Basics. In this chapter, we are interested in applications related to cryptology. We start with a very general introduction to cryptography, security objectives, we are looking at a new type of challenging problem emerging in lattices theory that can be used as the basis for a public key cipher system.

We will see that lattices theory has cryptographic applications that go beyond just providing a new source for difficult problems. We will discuss two public key cryptosystems based on lattice. We will start with **GGH** cryptosystem, which is most concise, though it has been subject to cryptanalytic attacks. Then we will discuss **NTRU** cryptosystem, which is most practical lattice-based cryptosystem. We will also discuss the role of these lattices in cryptanalysis the **RSA** cryptosystem.

3.1 Introduction to cryptography

3.1.1 Symmetric cryptography

Symmetric cryptography or private key encryption is to use the same key for encryption and decryption the cipher, an algorithm that is used for converting the plaintext to ciphertext, operates on a key, which is essentially a specially generated number (value).

One simple example of symmetric key cryptography is the **Monoalphabetic substitution**. In this case, the relationship between a character in the plaintext and a character in the ciphertext is always one-to-one[12]. An example Monoalphabetic substitution is the shift cipher. In this approach a character in the ciphertext is substituted by another character shifted by **"n"** places. [3]Example: A is substituted by D. Key feature of this approach is that it is very simple but the code can be attacked very easily.

Another example of symmetric key cryptography is the **Polyalphabetic substitution** this is an improvement over the shift cipher. Here the relationship between a character in the plaintext and a character in the ciphertext is always one to [12].

An example of polyalphabetic substitution is the Vigenere cipher and block ciphers. In the Vigenere cipher, a particular character is substituted by different characters in the ciphertext using the correspondence $A = 0, \cdots, Z = 25$, we can associate each key K with an alphabetic string of length m, called a keyword the Vigenere cipher encrypts m alphabetic characters at a time: each plaintext element is equivalent to m alphabetic characters[4].
The block ciphers: block encryption replace a block of fixed length with a block of m^i length.
Encryption and decryption operations of a block cipher: Some operations, such as permutation and substitution, are performed on the block of bits based on a key (a secret number) to produce another block. In the decryption process, operations are performed in the reverse order based on the same key to get back the original block.

3.1.2 Asymmetric cryptography

Asymmetric protocols are based on mathematical operations (exponentiations modular, etc.) which are much more expensive in time compared to time in symmetric protocols. These protocols are more efficient compared to symmetric protocols because they are more difficult. Asymmetric encryption works with a pair of keys: a public key which is freely accessible by any entity wishing to send a message, and a second so-called key private which is kept secret. Messages are encrypted using the public key and can only be decrypted by whoever has the corresponding private key.

RSA cryptosystem

The **RSA** system was invented by Ron Rivest, Adi Shamir and Len Adleman. The RSA protocol is both the oldest asymmetric encryption protocol and one of the most used protocols in the world. Its variants are the subject of intense scientific activity, but to this day the RSA has resisted all known attacks.
The security of the RSA system is based on the difficulty of factoring a large integer N, which is the product of two prime numbers p and q.

Description:[17] Here is how the RSA algorithm works. Chooses two distinct large primes p and q and multiplies them together to form $n = pq$. And also chooses an encryption exponent e such that

$$\gcd(e, \phi(n)) = 1.$$

Where $\phi(n) = (p-1)(q-1)$.

Sends the pair (n, e) to the sender but keeps the values of p and q secret. In particular, the sender, who could possibly be an enemy, never riccds to know p and q to send her message securely. The sender writes his message as a number m. If m is larger than n, he breaks the message into block, each of which is less than n. However, for simplicity, let's assume for the moment that $m < n$. The sender computes

$$c = m^e \bmod n.$$

Since to find the message knows p and q, and therefore can find the decryption exponent d with

$$de = 1 \bmod \phi(n).$$

Then:

$$m = c^d \bmod n.$$

So we have now the system was created as follow:

Private key: (p, q, d) where p and q are primes and $de = 1 \bmod ((p-l)(q-1))$.

Public key: (n, e) $n = pq,\ \gcd(e, (p-1)(q-1)) = 1$.

Encryption: $c = m^e \bmod n$.

Decryption: $m = c^d \bmod n$.

3.2 Lattice Based Cryptography

3.2.1 GGH Public Key Cryptosystem

This cryptosystem was developed by Goldreich, Goldwasser and Halevi in 1997. The GGH cryptosystem relies on the difficulty of the closest vector problem (CVP) in a lattice[5].
The basic idea is that, one chooses a nice basis B for a full rank lattice $L \subset \mathbb{Z}^n$ and publishes a disguised basis H.
Description:[11] Let L a full rank lattice of rank n.

Private key: A good lattice basis B. Good in the sense of consisting of short(nearly orthogonal) vectors, that allows to solve certain instances of CVP efficiently.

Public key: A bad basis H for the same lattice. Bad is in sense of being worst possible basis from a cryptanalysis point of view. $H = UB$, where U is a unimodular matrix chosen appropriately.

Encryption: Encode a message $m = (m_1; m_2; \cdots; m_n) \in \mathbb{Z}^n$ to a lattice point $v = m.H$ and add a short noise vector e, i.e. the cipher text is

$$c = v + e.$$

Decryption: For description one computes

$$cB^{-1} = (m.H + e)B^{-1} = m.UBB^{-1} + eB^{-1} = mU + eB^{-1}.$$

The term eB^{-1} being small, can be removed using Babai's rounding technique. Finally compute $m = mUU^{-1}$ to get the message.

Exemple 3.2.1 *Let $L \subset \mathbb{R}^2$ be the lattice with basis matrix B*

Private key:

$$B = \begin{pmatrix} 7 & 0 \\ 0 & 3 \end{pmatrix}, \text{ and so } B^{-1} = \begin{pmatrix} \frac{1}{7} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}. \text{ Let } U = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \text{ be a unimodular matrix.}$$

Public Key:

$$H = UB = \begin{pmatrix} 14 & 9 \\ 21 & 15 \end{pmatrix}.$$

Encryption: *Let the message vector* $v = (3, -7)$. *And the error vector* $e = (1, -1)$

$$\textit{Cipher text } c = vB + e = (104, -79).$$

Decryption: $cB^{-1} = (\frac{-104}{7}, \frac{-79}{3})$. *Which is rounded to* $(-15, -26)$. *Now one can recover message as*

$$m = (-15, -26)U^{-1} = (3, -7).$$

Cryptanalysis of GGH Cryptosystem

[11]For attack the GGH cryptosystem, we simply run a lattice basis reduction algorithm (such as LLL)on the public basis matrix H, may give us a sufficiently good basis to solve required CVP efficiently.

To computing the plain text the idea is to compute $c.H^{-1} = m + e.H^{-1}$, and try to deduce possible values for some entries of $e.H^{-1}$. For example, if the i-th column of H^{-1} has particularly small norm then one can deduce that the i-th entry of $e.H^{-1}$ is always small and hence get an accurate estimate for the i-th entry of m.

Remark: 3.1 *One can use the Babai nearest plane algorithm to solve CVP with* c *as a target vector and with public basis* H.
To prevent such an attack it is necessary that the dimension of the lattice be sufficiently large.

3.2.2 NTRU Cryptosystem

The NTRU cryptosystem proposed by Hoffstein, Pipher and Silverman, it is based on truncated polynomial rings with convolution multiplication where it has its initial name from (N-th degree truncated polynomial ring), but it can also be expressed using lattices.[5]
Note: Truncated polynomial rings is the ring of polynomials with integer coefficients over the variable X modulo the polynomial $X^N - 1$.

Description:[11] The NTRU system has the three integer parameters N, p and q, where $\gcd(p, q) = 1$. Further, d_f, d_g and d_r are integer bounds for the coefficients of the polynomials f, g and r in $\mathbb{R}$

$$F(d_1, d_2) = \{h(x) \in \mathbb{R} | h \text{ has } d_1 \text{ 1's and } d_2 \text{ -1's , and the rest of the coefficients are 0 } \}.$$

$$h \in F(d_1, d_2),\ h(x) = \sum_{i=0}^{N-1} a_i x^i \ | a_i = \pm 1.$$

We can also be described as a matrix operation. For this, we first define the cyclic rotation C that sends a vector $(x_1; x_2; \cdots; x_n)^T$ to $(x_n; x_1; \cdots; x_{n-1})^T$. For an arbitrary $x \in \mathbb{R}^n$ the circulant matrix of x is defined as

$$[C^*\mathbf{x}] = [\mathbf{x}, C\mathbf{x}, \cdots, C^{n-1}\mathbf{x}] = \begin{pmatrix} x_1 & x_n & \cdots & x_2 \\ x_2 & x_1 & \cdots & x_3 \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n-1} & \cdots & x_1 \end{pmatrix}.$$

We now have the matrix operation $[C^*\mathbf{f}]\mathbf{g}$ if we consider $\mathbf{f}$ and $\mathbf{g}$ as vectors consisting of the coefficients of f and g. This operation is associative, commutative and distributive, so $(\mathbb{R}; +; *)$ forms a ring. We define the spaces $F_f,\ F_g$ and F_r as follows:

$$F_f = F(d_f, d_f - 1), \qquad F_g = F(d_g, d_g), \qquad F_r = F(d_r, d_r).$$

Key Creation: Chooses polynomials $f \in F_f$ and $g \in F_g$, f must be invertible modulo p and q, denote the inverses f_p^{-1} and f_q^{-1} respectively.

Private Key: f and g.

public key: $h \equiv p \cdot f_q^{-1} * g \bmod q$. Or in matrix notation $\mathbf{h} \equiv p \cdot [C^*\mathbf{f}]_q^{-1}\mathbf{g} \bmod q$.

Encryption: To encrypt a message $m \in \mathbb{R}_q^n$, we randomly chooses a polynomial $r \in F_r$ and computes $c \equiv h * r + m \bmod q$.

In matrix notation, $\mathbf{h} \equiv p \cdot [C^*\mathbf{h}]\mathbf{r} + \mathbf{m} \bmod q$.

Decryption: To decrypt the message c, multiply the ciphertext and the secret key to get

$$t \equiv c \cdot f \bmod q,$$

such that all values ti are bounded by $\frac{q}{-2} \leq t_i < \frac{q}{2}$. The original message can then be computed by

$$m \equiv t \cdot f_p^{-1} \bmod q.$$

Exemple 3.2.2 *[11]Let $N = 5, p = 3$ and $q = 16$, Further, the integer bounds for the coefficients of the polynomials f, g and r are $d_f = 2,\ d_g = 2$ and $d_r = 1$. We chose the polynomials*

$$f = X^2 + X - 1,\ g = -X^4 + X^2 - X + 1 \text{ as private key and } r = -X^4 + X.$$

computed the inverse of f modulo p and q we find respectively,

$f_p^{-1} = X^4 + 2X^3 + 2X^2 + 2$ *and* $f_q^{-1} = 15X^4 + 12X^3 + 3X^2 + 9X + 10$, *and the corresponding circulant matrices are*

$$[C^*\boldsymbol{f}]_p^{-1} = \begin{pmatrix} 2 & 1 & 2 & 2 & 0 \\ 0 & 2 & 1 & 2 & 2 \\ 2 & 0 & 2 & 1 & 2 \\ 2 & 2 & 0 & 2 & 1 \\ 1 & 2 & 2 & 0 & 2 \end{pmatrix}; \qquad [C^*\boldsymbol{f}]_q^{-1} = \begin{pmatrix} 10 & 15 & 12 & 3 & 9 \\ 9 & 10 & 15 & 12 & 3 \\ 3 & 9 & 10 & 15 & 12 \\ 12 & 3 & 9 & 10 & 15 \\ 15 & 12 & 3 & 9 & 10 \end{pmatrix}.$$

The public key becomes $h \equiv p \cdot f_q^{-1} * g$ mod $q = 4X^4 + 9X^3 + 8X^2 + X + 10$, so in matrix form

$$[C^*\boldsymbol{h}] = \begin{pmatrix} 10 & 4 & 9 & 8 & 1 \\ 1 & 10 & 4 & 9 & 8 \\ 8 & 1 & 10 & 4 & 9 \\ 9 & 8 & 1 & 10 & 4 \\ 4 & 9 & 8 & 1 & 10 \end{pmatrix}.$$

Let the message be the vector $m = (-1, 0, 1, 1, 0)$. The ciphertext

$$c \equiv h * r + m \text{ mod } q \equiv -X^4 + 5X^3 - 7X^2 + 2X + 2 \text{ mod } q$$

In matrix form $[C^*\boldsymbol{h}]\boldsymbol{r} + \boldsymbol{m} \equiv (2, 2, -7, 5, -1)$ mod q.

To decrypt this ciphertext we first compute the product $t \equiv [C^*\boldsymbol{f}]\boldsymbol{c} = (2, -1, 11, -10, -1)$, *then align its coefficients to values* x *between* $\frac{16}{-2} \leq t_i < \frac{16}{2}$, *which gives the vector* $t' = (2, -1, -5, 6, -1)$.

Multiplying this vector by $[C^*\boldsymbol{f}]_p^{-1}$ *gives the original message*

$$m = (2, 0, 1, 1, 0) \textit{ mod } p$$

.

Cryptanalysis of NTRU Cryptosystem:
[11]The basic concept is, define a lattice $L_{h;c}$, given the public key h and the ciphertext c as follows.

$$\begin{pmatrix} I_N & 0 \\ H & I_N.qc \end{pmatrix}.$$

where $H = [C^*\mathbf{h}]$. So this is a basis for the lattice containing all the points

$$L_{h;c} = \{(u; v) \in P \times P | u * h = v \bmod q\}.$$

and additionally the point $v_c = (0; c)$. Recall that $c = r * h + m \bmod q$. Consider now the point $v_r = (r; r * h) \in L_{h;c}$. Since v_c and v_r are both in $L_{h;c}$, also $v_c - v_r = (-r; m)$ is in the lattice. Only to be an element of the lattice does not suffice to find this element in the lattice, but when we take a closer look on the norm of this vector, we see that it is at most $\sqrt{2d_r + N}$ Compared to the norm of the expected shortest vector, the desired vector is relatively small, and therefore has a good chance to be the shortest vector. This means, that we can reduce the lattice $L_{h;c}$ until we find a vector with the right amount of 1's and -1's in the first N entries. The rest of the entries will be the message with very high probability.

Exemple 3.2.3 [11]Let use the system in the **Example 3.2.2**. The first step is to construct the lattice basis B for the lattice $L_{h,c}$ with the public key $h = 4X^4 + 9X^3 + 8X^2 + X + 10$ and the ciphertext $c = -X^4 + 5X^3 - 7X^2 + 2X + 2$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10 & 4 & 9 & 8 & 1 & 16 & 0 & 0 & 0 & 0 & 2 \\ 1 & 10 & 4 & 9 & 8 & 0 & 16 & 0 & 0 & 0 & 2 \\ 8 & 1 & 10 & 4 & 9 & 0 & 0 & 16 & 0 & 0 & -7 \\ 9 & 8 & 1 & 10 & 4 & 0 & 0 & 0 & 16 & 0 & 5 \\ 4 & 9 & 8 & 1 & 10 & 0 & 0 & 0 & 0 & 16 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then we reduce this with the **LLL** algorithm, we obtain the following matrix.

$$B' = \begin{pmatrix} -1 & 0 & -1 & -2 & 0 & 3 & -1 & -2 & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 & -1 & 1 & 3 & 2 & -1 & 1 \\ -1 & 0 & -1 & 1 & 0 & 0 & 1 & -1 & 2 & -1 & -1 \\ -1 & 0 & 0 & 1 & 2 & 1 & -1 & 0 & -3 & 0 & 2 \\ -1 & 1 & 0 & -1 & 0 & -2 & -1 & -1 & 0 & 0 & -2 \\ 0 & -1 & 1 & 2 & -2 & -2 & 0 & -2 & 0 & 1 & 3 \\ 0 & 0 & -1 & -1 & 0 & 0 & 2 & 0 & -1 & 0 & 2 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 & 1 & -4 & 2 \\ 0 & 1 & 0 & 2 & -1 & 0 & 1 & 1 & -1 & 2 & 4 \\ 0 & 0 & 2 & -1 & 3 & 1 & -1 & 1 & 0 & 0 & 2 \\ 0 & 1 & 2 & 1 & -1 & -1 & 3 & 0 & -1 & -1 & -3 \end{pmatrix}.$$

Recall that $d_r = 1$, so we search for a column vector in the reduced basis whose 5 first entries contains a 1 and a -1. This holds for the 2nd and 10-nth column. By checking the next 5 entries, we see that the second vector contains the message $(-1, 0, 1, 1, 0)$.

3.2.3 An Attack on RSA

[17] A sender wants to send a message of the form $(Theanswer is ****)$. In these cases, the message is of the form $m = B + x$, where B is fixed and $|x| < Y$.

For some integer Y. We present an attack that works when the encryption exponent is small. Suppose public RSA key $(n, e) = (n, 3)$. Then the ciphertext is

$$c = (B + x)^3 \bmod n.$$

We applie the **LLL** algorithm to the lattice generated by the vectors

$$v_1 = (n, 0, 0, 0),\ v_2 = (0, nY, 0, 0),\ v_3 = (0, 0, Y^2 n, 0),\ v_4 = (a_0, a_1 Y, a_2 Y^2, Y^3)$$

This gives a new basis $u_1, \cdots, u_4$, but we need only u_1 the theorem 2.3.1 tells us that

$$\| u_1 \| \leq 2^{3/4} (\det(v_1, \cdots, v_4)^{1/4}), \tag{3.1}$$

$$= 2^{3/4} (n^3 Y^6)^{\frac{1}{4}} = 2^{3/4} n^{3/4} Y^{3/2}. \tag{3.2}$$

We can write

$$u_1 = c_1 v_1 + \cdots + c_4 v_4 = (e_0, Y e_1, Y^2 e_2, Y^3 e_3)$$

with $c_i \in \mathbb{Z}$, and with

$$\begin{aligned} e_0 &= c_1 n + c_4 a_0, \\ e_1 &= c_2 n + c_4 a_1, \\ e_3 &= c_3 n + c_4 a_2, \\ e_4 &= c_4. \end{aligned}$$

It is easy to see that ($e_i \equiv c_4 a_i \bmod n,\ 0 \leq t \leq 2$). Form the polynomial

$$g(T) = e_3 T^3 + e_2 T^2 + e_1 T + e_0$$

Then, since the integer x satisfies $f(x) \equiv 0 \bmod n$ and since the coefficients of $c_i f(T)$ and $g(T)$ are congruent mod n,

$$0 \equiv c_i f(T) \equiv g(T) \bmod n.$$

Assume now that

$$Y < 2^{-7/6} n^{1/6}. \tag{3.3}$$

Then

$$\begin{aligned} |g(x)| &= |e_3 x^3| + |e_2 x^2| + |e_1 x| + |e_0| \\ &\leq |e_3| T^3 + |e_2| T^2 + |e_1| T + |e_0| \\ &= (1,1,1,1).(g(T) = e_3 T^3, e_2 T^2, e_1 T, e_0) \\ &\leq \| \ (1,1,1,1) \ \| \ . \ \| \ (g(T) = e_3 T^3, e_2 T^2, e_1 T, e_0) \ \| \\ &= 2 \ \| \ u_1 \ \| \ . \end{aligned}$$

Since, by 3.2 and 3.3

$$\| \ u_1 \ \| \leq 2^{3/4} n^{3/4} Y^{3/2} < 2^{3/4} n^{3/4} (2^{-7/6} n^{1/6})^{3/2} = 2^{-1} n$$

we obtain $|g(x)| < n$. Since $g(x) \equiv 0 \bmod n$, we must have $g(x) = 0$. The zeros of $g(T)$ may be determined numerically, and we obtain at most three candidates for x. Each of these may be tried to see if it gives the correct ciphertext. Therefore, we can find x.

Exemple 3.2.4 [17] Let

$$n = 192784105542869748715759425891 7, p = 757285757575769 \text{ and } q = 2545724696579693,$$

one sending the message (The answer is **). where (* *) denotes a two-digit number. Therefore the message is $m = B + x$ where $B = 200805000114192305180009190000$ and $0 \leq x < 100$. Suppose the ciphertext $c = (B + x)^3 \equiv 303263084986196485594640589 32 \bmod n$. We can form the polynomial

$$f(T) = (B + T)^3 - c \equiv T^3 + a_2 T^2 + a_1 T + a_0 \bmod n,$$

where

$$\begin{aligned} a_2 &= 602415000342576915540027570000 \\ a_1 &= 112354912400424746936217146 7964 \\ a_0 &= 587324114445679876954457927616. \end{aligned}$$

Note that $a_0 \equiv B^3 - c \bmod n$. We use LLL to find a root of $f(T) \bmod n$. We let $Y = 100$ and forms the vectors

$$v_1 = (n, 0, 0, 0), \ v_2 = (0, 100n, 0, 0), \ v_3 = (0, 0, 10^4 n, 0), \ v_4 = (a_0, 100 a_1, 10^4 a_2, 10^6)$$

The LLL algorithm produces the vector

$$\begin{aligned} &308331465484476402 v_1 - 589837092377839611 v_2 + 316253828707108264 v_3 - 101207 l 602751202635 v_4 \\ &= (246073430665887186108474, -577816087453534232385300, 405848565585194400880000, \\ &\qquad -10120716027512026350000 00). \end{aligned}$$

Then $g(T) = -10120716027512026 35 T^3 + 40584856558519440088 T^2 - 57781608745353423238 53 T$
$+ 246073430665887186108474.$

The roots of $g(T)$ are computed numerically to be

$$42.000000000, -0.949612039 \pm 76.079608511 i.$$

It is easily checked that $g(42) = 0$, so the plaintext is

$$The \ answer \ is \ 42.$$

Conclusion

In this memory, we wanted to review some encryption systems that depend on lattices problems and the methods of attacking. More precisely, the role of lattices on encryption systems.
The different basis of lattices pose two main problems, **CVP** and **SVP**.

The **GGH** cryptosystem based on the difficulty of the closest **CVP** in a lattices.

The **NTRU** security and based on **CVP** and **SVP** issues in lattices.

For this, we needed to understand these Lattices, and know the most important problems on which modern cryptography are based, so it is necessary to know the best algorithm of reduction, which allows finding a nearest orthogonal basis that facilitates the solution of those problems, and then breaks the security of systems that depend on their difficulty. One of the most important of those reduction algorithms is the **LLL** algorithm, which turns out to be the most practical in terms of time and convergence of results, which is exploited to find an approximation to shortest vector, and the **Babai's** algorithm which is used to find closest vector.

Lattices reduction has an important role in breaking the security of modern cryptography. In this remark, we review one of the methods of attacking the **RSA** cryptosystem.

Bibliography

[1] B.Vallette,L'ALGÈBRE LINÉAIRE POUR TOUS, Université de Nice Sophia-Antipolis, France, 2015.

[2] D.Micciancio, CSE 206A: Lattice Algorithms and Applications 1: Introduction to Lattices, UCSD CSE,Winter 2010.

[3] D.Mihoubi, Introduction à la Cryptographie, Mohamed Boudiaf university of Msila,2019.

[4] D.R, Stinson. CRYPTOGRAPHY THEORY AND PRACTICE THIRD EDUTION, Tylor and Francis Group,New York, 2006.

[5] F.Bergami,Lattice-Based Cryptography,Universita di'Padova Universite de'Bordeaux, 2016.

[6] G.Strang, Introduction to LINEAR ALGEBRA FOURTH EDITION, Wellesley-Cambridge Press, Cambridge, 2009.

[7] J.Hoffstein, J. Pipher, J.H.Silverman, An Introduction to Mathematical Cryptography, Springer, New York, (2008) 349-422.

[8] J.H.Silverman(Ed), Cryptography and Lattices International Conference, CaLC 2001 Providence, RI, USA, March 29-30, 2001 Revised Papers, Springer, Verlag Berlin Heidelberg, (2001).

[9] M.R.Bremner, Lattice Basis Reduction, Taylor and Francis Group, Boca Raton Florida, (2012) 1-83.

[10] M.Georgieva, Analyse probabiliste de la réduction des réseaux euclidiens cryptographiques, Université de Caen Basse-Normandie, (2013) 1-66.

[11] M.Hartmann, The Ajtai-Dwork Cryptosystem and Other Cryptosystems Based on Lattices, University of Zurich UZH, 2015.

[12] Module 8 Network Security, Version2 CSE IIT, Kharagpur. *https://nptel.ac.in/content/storage2/courses/106105080/pdf/M8L1.pdf*.

[13] N.P.Smart, Cryptography Made Simple, Springer, Switzerland, (2016) 79-90.

[14] P.Q.Nguyen, B.Vallée. The LLL Algorithm Survey and Applications, Springer, Berlin Heidelberg, 2010.

[15] S.Galbraith, Mathematics of Public Key Cryptography version 2.0, Cambridge University, (2012) 353-427.

[16] T.Laarhoven, J.van de Pol, B.de Weger, Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems, (2012).

[17] W.Trappe, L.C.Washington, Second Edition Introduction to Cryptography with Coding Theory, Pearson Prentice Hall, (2006) 164-216, 376-390.

ملخص

في هذه المذكرة، ندرس الشبكات وتطبيقاتها في علم التشفير. أولاً، سوف ندرس الشبكات (القاعدة والخصائص)، وأهم المشاكل التي تطرحها قواعدها المختلفة (مشكلة أقصر شعاع في الشبكة ومشكلة أقرب شعاع لنقطة من الفضاء الاقليدي)، والخوارزميات الاختزال القاعدة. وطرق لإيجاد حلول لهذه المشاكل.
في الختام، نقترح مخططات تشفير تعتمد على مشكلات الشبكة وطرق مهاجمتها من خلال حل هذه المشكلات.

كلمات مفتاحية

مشاكل الشبكة، القاعدة الشبكة، الخوارزميات الاختزال والتشفير القائم على الشبكة.

Abstract

In this memory we will study lattices and their applications in cryptography. Firstly, we will study lattices (basis and characteristics) and the most important problems raised by their differnt basis (shortest vectore problem and closest vector problem), algorithms for reduction basis and methods for finding solutions to these problems.
In conclusion, we offer cryptosystems that depend on lattices problems and methods of attacking them by solving those problems.

Key words :

Lattice, basis, lattice problems, reduction algorithms, lattices based cryptography.

Résumé

Dans ce mémoire, nous étudions les réseaux et leurs applications en cryptographie. Dans un premier temps, nous étudierons les réseaux (base et caractéristiques) et les problèmes les plus importants posés par leur différente bases (problème de vecteur le plus court et problème de vecteur le plus proche), les algorithmes du réduction des base et les méthodes pour trouver des solutions à ces problèmes.
En conclusion, nous proposons des cryptosystèmes qui dépendent des problèmes de réseaux et des méthodes pour les attaquer en résolvant ces problèmes.

Mot-clés :

Réseau, base, problèmes de réseau, réduction algorithmes, cryptographie basée sur des réseaux.