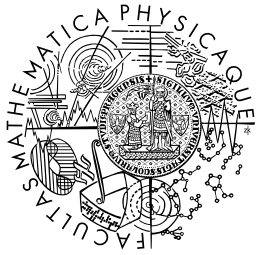

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Sára Vyhnalová

Ideal lattices in cryptography

Department of Algebra

Supervisor of the master thesis: Mgr. Vítězslav Kala, Ph.D.

Study programme: Mathematics

Study branch: Mathematics for Information Technologies

Prague 2021

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Author's signature

I would like to thank my consultant Pavlo Yatsyna, Ph.D. for his helpfulness to answer questions, his patience and valuable advice. I would also like to thank my supervisor Mgr. Vítězslav Kala, Ph.D. for good ideas and important remarks and my family, who has supported me throughout the studies.

Title: Ideal lattices in cryptography

Author: Sára Vyhnalová

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., consultant Pavlo Yatsyna, Ph.D., Department of Algebra

Abstract: The thesis is focused on the theory of special lattices that are important in cryptography, namely ideal, cyclic and NTRU lattices. Specifically, we expand and generalise the work of Ding and Lindner on Identifying Ideal Lattices. The algorithm for identifying ideal lattices is included, along with illustrative examples and more detailed proofs of propositions on which the algorithm is based. In the section about Lattice Isomorphism there is also included a generalised theorem from the paper. We extend the result of identifying the NTRU lattices and supplement it with several examples. The thesis also contains Chapter Applications in Cryptography where we describe a cryptographic hash function based on ideal lattices. And finally, we provide a brief overview of the cryptographic algorithms using NTRU lattices.

Keywords: ideal lattice, cyclic lattice, NTRU lattice

Contents

Introduction

Lattice-based cryptography has recently become a common topic in modern cryptography. More and more experts are talking about a possible step in the development of quantum computers. If they were constructed, they would pose a real threat to contemporary popular algorithms in Asymmetric Cryptography such as widely used RSA. In the cryptographic world, there is an effort to respond to this threat in a timely manner.

Concretely, in 2017, the American National Institute of Standards and Technologies (NIST) launched an activity called Post Quantum Cryptography Standardization. The aim is to select the most suitable ones from the list of candidates such that they would also be resistant to cryptanalysis using a quantum computer. This process is divided into two categories:

- Public-key Encryption and Key Encapsulation Mechanisms (KEMs)
- Digital Signature algorithms.

NIST plans to choose approximately 2 algorithms in each category. In the end, there will be a standard issued, according to which the chosen algorithms will be used in practice. The standardization influences also the European legislative because European standards stem from NIST's standards.

The interesting aspect is that algorithms based on lattices have represented a large proportion of the candidates for post-quantum algorithms since the beginning of the standardization process. Moreover, lattice-based algorithms such as NTRU Cryptosystem, Crystals-Dilithium Signature Scheme and many others have become the Third Round Finalists, which started July 22, 2020.

The huge disadvantage of multiple post-quantum algorithms is their noneffi-ciency such as large keys, long signatures, a large amount of parameters. In the field of cryptography on lattices, efforts are being made to refine the number of parameters. One way of doing this is by using structured lattices, such as ideal lattices or NTRU lattices. In numerous sources these types of lattices are not mentioned at all, or only marginally, and are often not properly formalised.

The goal of this thesis is to formalise the theory of the above mentioned special types of lattices, to highlight and generalise the interesting properties and to extend some of the claims about ideal lattices to NTRU lattices.

In the first chapter, we recall some definitions and important propositions from the various subjects and we pay most attention to the definition of a lattice in general.

In the very beginning of the second chapter, we introduce the topic of ideal lattices. We will see that the concept of ideal lattices is really related to the concept of ideal as it has been understood in the course of Algebra. We also define a special case of ideal lattices, namely the cyclic lattice.

In Chapters 2 and 3, we rely in particular on the paper from authors Jintai Ding, University of Cincinnati, USA and Richard Lindner, Technische Universität Darmstadt, Germany [Ding and Lindner, 2007]. The original result of this article is an algorithm that for a given basis decides whether the corresponding lattice is ideal or not. The construction of the algorithm requires important propositions, which we have included in our work. Proofs are written with precision and clarity

of the steps that were skipped in the article. Chapter 2 contains also several propositions that we have written down and proved by ourselves since they have shown to be useful. In the third chapter, in addition to the mentioned algorithm and the detailed proof of its correctness, we also give our own examples in which we deal with the particular structure of the basis.

Another interesting result of the paper [Ding and Lindner, 2007] is the generalisation of identifying ideal lattices to isomorphism classes and the theorem about an infinite number of lattices in dimension 2, which does not contain any ideal lattice in their isomorphism class. We have generalised this theorem to another basis form in dimension 2.

Chapter 4 is entitled NTRU lattices. It is based on our thoughts inspired by [Ding and Lindner, 2007, Section 2.7]. We will look at extending the definition of an NTRU lattice to a more general form than that given in [Coppersmith and Shamir, 1997]. To a certain extent, for NTRU lattices we offer an analogous proposition to the one from the second chapter which was important for the algorithm for Identifying ideal lattices.

In the last chapter, we give the applications of structured lattices in cryptography, namely the design of a hash function based on ideal lattices and briefly, we also introduce applications of the NTRU lattices. As a reference we use [Micciancio and Regev, 2008].

1. Preliminaries

1.1 Matrix notation

Firstly, let us introduce the basic notation that is used throughout the thesis.

The symbol $\mathbb{Z}^{n\times m}$ stands for the set of all matrices with integer coefficients consisting of n rows and m columns and $\mathbb{Z}^n$ is the set of all vectors with n integer elements. Analogously $\mathbb{R}^{n\times m}$ stands for $n \times m$ matrices with real coefficients.

Matrices and vectors are denoted by bold letters, for example a matrix $\mathbf{C} \in \mathbb{Z}^{n\times m}$ or a vector $\mathbf{v} \in \mathbb{Z}^n$. By vector $\mathbf{v}$ we mean a column vector (a row vector is written with the transposition sign as $\mathbf{v}^\top$).

Entries in a matrix are written in normal letters, not in bold, although the matrix itself is denoted by a bold letter. For instance $\mathbf{C} \in \mathbb{Z}^{n\times m}$ would be denoted:

$$\mathbf{C} = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1m} \\ C_{21} & C_{22} & \cdots & C_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nm} \end{pmatrix}.$$

We also introduce the symbol $\mathbf{C}_{i,\cdot}$ (in bold) denoting the i-th row, analogously $\mathbf{C}_{\cdot,j}$ for the j-th column.

Symbol $\mathbf{I}_n$ denotes $n \times n$ identity matrix

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

When all of the entries in an $n \times m$ matrix are zeros, it can be simplified by the following notation:

$$\left(\quad \mathbf{0}_{n\times m} \quad \right)$$

or we can rewrite matrix $\mathbf{C}$ mentioned above in this section by bypassing writing precise entries in the following manner:

$$\left(\quad \mathbf{C}_{n\times m} \quad \right) \text{ or } \left(\quad \mathbf{C} \quad \right).$$

Sometimes when the structure of a matrix is important, we give an indication of it. For example, we emphasize division into columns (for instance $\mathbf{b}_1, \mathbf{b}_2, \ldots \mathbf{b}_m \in \mathbb{R}^n$):

$$\left(\begin{array}{c|c|c|c} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_m \end{array} \right),$$

or into rows:

$$\left(\begin{array}{c} \mathbf{B}_{1,\cdot} \\ \hline \mathbf{B}_{2,\cdot} \\ \hline \vdots \\ \hline \mathbf{B}_{n,\cdot} \end{array}\right),$$

or we highlight boundaries between blocks or parts of the matrix:

$$\left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right).$$

Another important type of matrices are triangular matrices. A square matrix is called upper triangular if all of the entries below the main diagonal are zero. For simplification, we will use the notation with big zero:

$$\begin{pmatrix} B_{11} & B_{12} & B_{13} & \dots & B_{1n} \\ & B_{22} & B_{23} & \dots & B_{2n} \\ & & \ddots & & \vdots \\ & \mathbf{0} & & \ddots & \vdots \\ & & & & B_{nn} \end{pmatrix}.$$

By $GL_n(\mathbb{Z})$ we mean the group of all invertible matrices over $\mathbb{Z}$. These are square matrices with integer coefficients whose determinant is an invertible element in $\mathbb{Z}$ (only 1 and -1 are invertible elements in $\mathbb{Z}$).

Symbol $\mathrm{span}_{\mathbb{Z}}(\mathbf{b}_1, \dots, \mathbf{b}_m)$ stands for the set of all integer combinations of vectors $\mathbf{b}_1, \dots, \mathbf{b}_m \in \mathbb{R}^n$ or if we denote $\mathbf{B} = (\mathbf{b}_1 | \dots | \mathbf{b}_m)$, we can also write $\mathrm{span}_{\mathbb{Z}}(\mathbf{B})$.

1.2 Review

Let us mention some mathematical concepts and basic propositions that will be essential for this thesis.

1.2.1 Congruences for matrices

In the chapter about ideal lattices, to be more precise in Section 3.1, we will look at the entries in one matrix and check whether they are congruent to the entries on the same positions in another matrix modulo an integer number. The following definitions generalise the concept of congruences to integer matrices.

Definition 1 (Divisibility for matrices)**.** *Let $c \in \mathbb{Z}$ and $\mathbf{A} \in \mathbb{Z}^{n \times m}$. We say that number c divides matrix $\mathbf{A}$ (denoting by $c \mid \mathbf{A}$) if there exists a matrix $\mathbf{Z} \in \mathbb{Z}^{n \times m}$ such that $\mathbf{A} = c\mathbf{Z}$.*

Remark. Divisibility $c \mid \mathbf{A}$ is equivalent to the fact that each entry of matrix $\mathbf{A}$ is divisible by c.

We will also use notation $\mathbf{A} \mod d$, which means that in matrix $\mathbf{A}$, the operation of modulo is applied to each entry.

Definition 2 (Congruence relation for matrices)**.** *Let $c \in \mathbb{Z}$ and $\mathbf{A}, \mathbf{B} \in \mathbb{Z}^{n\times m}$. $\mathbf{A}$ is congruent to $\mathbf{B}$ modulo c (we write $\mathbf{A} \equiv \mathbf{B} \mod c$) if $c \mid (\mathbf{A} - \mathbf{B})$.*

Remark. Divisibility and congruences for vectors can be defined analogously or can be viewed as special cases of these definitions where vectors are considered to be matrices from $\mathbb{Z}^{n\times 1}$.

Let us firstly remind Chinese Remainder Theorem from the course of Algebra and afterwards, we will connect it with vector congruences.

Theorem 3 (Chinese Remainder Theorem (**CRT**))**.** *Let $k \in \mathbb{N}$, $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ and $m_1, m_2, \ldots, m_k \in \mathbb{N}$ be pairwise coprime. If we denote by M the product $M = \prod_{i=1}^{n} m_i$, then system*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

has a unique solution $x \in \{0, 1, \ldots, M-1\}$.

Proof. This theorem and the proof can be found in [Stanovský, Section 4.5]. □

Remark. If we wanted to calculate the solution for the system of congruences where there was an unknown vector $\mathbf{x}$ instead of one-dimensional variable x and where $\mathbf{a}_i \in \mathbb{Z}^n$:

$$\begin{aligned} \mathbf{x} &\equiv \mathbf{a}_1 \mod m_1 \\ \mathbf{x} &\equiv \mathbf{a}_2 \mod m_2 \\ &\vdots \\ \mathbf{x} &\equiv \mathbf{a}_k \mod m_k, \end{aligned}$$

we could use Theorem 3 repeatedly n times to get a unique solution for each entry and thus we would get a unique vector solution with entries smaller than product $M = m_1 m_2 \cdots m_k$.

1.2.2 Adjugate matrices

In many calculations in the thesis, we will work with the adjugate matrix whose definition is closely related to the cofactor matrix. These concepts refer to square matrices.

Definition 4 (Cofactor and adjugate matrix)**.** *(1) Let $\mathbf{A}$ be an $n \times n$ matrix. By $\mathbf{M}_{ij}$ we mean a matrix of order $n-1$ obtained from $\mathbf{A}$ by deleting the i-th row and the j-th column.*

(2) The cofactor matrix *of $\mathbf{A}$ is a matrix:*

$$\mathbf{C} = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{pmatrix}$$

where $C_{ij} = (-1)^{i+j} \det(\mathbf{M}_{ij})$.

(3) The adjugate matrix of $\mathbf{A}$ *is the transpose of the cofactor matrix* $\mathbf{C}$ *of* $\mathbf{A}$*:*

$$\operatorname{adj}(\mathbf{A}) = \mathbf{C}^{\mathsf{T}}.$$

Remark. This basic property adjugate matrices have (see for example page 22 in [Horn and Johnson, 2013]):

$$\operatorname{adj}(\mathbf{A})\mathbf{A} = \mathbf{A}\operatorname{adj}(\mathbf{A}) = \det(\mathbf{A})\mathbf{I_n}.$$

This means that $\mathbf{A}$ and $\operatorname{adj}(\mathbf{A})$ are invertible if and only if the determinant of $\mathbf{A}$ is an invertible element.

1.2.3 Hermite Normal Form

Another important and often used concept in this thesis is Hermite Normal Form (for abbreviation we will use **HNF**). The structure of a matrix in **HNF** can simplify many calculations.

Definition 5 (**HNF**)**.** *Matrix* $\mathbf{H} \in \mathbb{Z}^{n\times n}$ *with non-zero determinant is in* Hermite Normal Form *if and only if the following hold*

i. $\mathbf{H}$ *is upper triangular,*

ii. the diagonal entries of $\mathbf{H}$ *are positive,*

iii. the off-diagonal entries are non-negative and strictly smaller than the diagonal entry in their row.

Theorem 6 (Existence of **HNF**)**.** *Let* $\widetilde{\mathbf{B}}$ *be an* $n \times n$ *matrix with coefficients in* $\mathbb{Z}$*. Then there exists a unique* $n \times n$ *matrix* $\mathbf{B}$ *in* ***HNF*** *of the form* $\mathbf{B} = \widetilde{\mathbf{B}}\mathbf{U}$ *where* $\mathbf{U} \in GL_n(\mathbb{Z})$*.*

Proof. This theorem is proved in [Cohen, 2013, Theorem 2.4.3] by providing an algorithm for finding such a matrix $\mathbf{U}$. □

1.3 Lattices

Here we sum up basic concepts related to lattices from the course of Computer Algebra 2.

Definition 7 (Lattice in $\mathbb{R}^n$)**.** *Let* $m \leq n$ *and* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m \in \mathbb{R}^n$ *be linearly independent vectors.* A lattice in $\mathbb{R}^n$ *is the set of all integer combinations of vectors* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$ *denoted:*

$$L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m) = \{\sum_{i=1}^{m} x_i\mathbf{b}_i \mid x_i \in \mathbb{Z}\}.$$

Remark. Straightforwardly from the definition it follows that lattices are closed under addition. Further, if $a \in L$ then also $-a \in L$. These facts we will implicitly use throughout the text.

Notation of the following definitions and remarks in this section is related to Definition 7.

Definition 8 (Rank and Dimension of the Lattice)**.** *The integer n is called the* dimension *and m is called the* rank *of the lattice.*

Definition 9 (Full-rank Lattice)**.** *Lattices such that $m = n$ are called* full-rank lattices*.*

Definition 10 (Lattice Basis)**.** *The sequence of vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$ from Definition 7 is called a* lattice basis *and it is conveniently represented as a matrix*

$$\mathbf{B} = \left(\begin{array}{c|c|c|c} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_m \end{array} \right) \in \mathbb{R}^{n \times m}.$$

Remark. Using matrix notation from Definition 10 we can rewrite Definition 7 into the following form:

$$L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m) = L(\mathbf{B}) = \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^m\}.$$

For simplification, especially when it is not important to specify the basis, we will often use simply L for denoting the lattice instead of $L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m)$. Implicitly we assume that lattice L has its basis which consists of vectors from $\mathbb{R}^n$ (as mentioned above, n is called the dimension of lattice L).

Since a given basis determines the lattice, in many cases we can work with the basis instead of the whole lattice, for example we use this fact in Section about the lattice isomorphism (Section 3.3).

Definition 11 (Sublattice)**.** *Let L be a lattice. We say that K is a sublattice of L if $K \subseteq L$ and K is a lattice itself.*

The following theorem and its corollary say that the lattice with basis $\mathbf{B}$ is identical to the lattice whose basis is $\mathbf{B}$ in **HNF**. This fact will be helpful for the algorithm in Section 3.1.

Theorem 12. *Let $\mathbf{B}$ and $\mathbf{C}$ be $n \times n$ matrices. Then $L(\mathbf{B}) = L(\mathbf{C})$ if and only if there exists a matrix $\mathbf{U} \in GL_n(\mathbb{Z})$ such that $\mathbf{B} = \mathbf{CU}$.*

Proof. For the proof, see [Micciancio, 2012, Theorem 4]. □

Corollary 13. *Let $\widetilde{\mathbf{B}} \in \mathbb{Z}^{n \times n}$ and $\mathbf{B}$ be the corresponding matrix in **HNF**. Then $L(\widetilde{\mathbf{B}}) = L(\mathbf{B})$.*

Proof. Since $\mathbf{B} = \widetilde{\mathbf{B}}\mathbf{U}$ for some $\mathbf{U} \in GL_n(\mathbb{Z})$ according to Theorem 6, we can apply Theorem 12 to get $L(\widetilde{\mathbf{B}}) = L(\mathbf{B})$. □

2. Ideal lattices

This chapter is based on [Ding and Lindner, 2007, Pages 3 and 4]. As in the paper, we also begin with the definition of an ideal lattice and continue with the key theorem that results in the algorithm for identifying ideal lattices.

Proofs from the article are described here in more detail. Besides, we offer several propositions which we came across. We have formulated and proved them (for instance, Proposition 20 or Lemma 21).

2.1 Definition and basic properties

Ideal lattices, as the name indicates, are really linked to the notion of an ideal from the basic course of Algebra. Firstly, we need to introduce the ring of polynomials and the isomorphism used in our definition. Secondly, we will move on to the definition of an ideal lattice itself.

2.1.1 Isomorphism $\Phi_{\mathbf{q}}$ and Ring $R_{\mathbf{q}}$

Let $\mathbf{q}(x) \in \mathbb{Z}[x]$ be a *monic* polynomial of degree n:

$$\mathbf{q}(x) = q_0 + \cdots + q_{n-1}x^{n-1} + x^n.$$

And let the ring of all integer polynomials modulo $\mathbf{q}$ be

$$R_{\mathbf{q}} := \mathbb{Z}[x]/\mathbf{q}(x)\mathbb{Z}[x].$$

There are two points of view:

- In the additive view: As a $\mathbb{Z}$-module, $R_{\mathbf{q}}$ is isomorphic to $\mathbb{Z}^n$ regardless of the choice of $\mathbf{q}$. The isomorphism is given by

$$\begin{array}{rccc} \Phi_{\mathbf{q}} : & \mathbb{Z}^n & \longrightarrow & R_{\mathbf{q}} \\ & (v_0, \ldots, v_{n-1})^\top & \longmapsto & v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x]. \end{array}$$

- In the multiplicative view: Component-wise multiplication is not preserved in general. We define the multiplication on $\mathbb{Z}^n$, depending on polynomial $\mathbf{q}$ picked in this isomorphism.

Remark. In the following text, by $\Phi_{\mathbf{q}}$ and $R_{\mathbf{q}}$ we always mean the isomorphism and the ring defined above.

2.1.2 Ideal lattices

Definition 14 (Ideal lattice)**.** *Let L be a sublattice of $\mathbb{Z}^n$. If there exists a monic polynomial of degree n*

$$\mathbf{q}(x) = \sum_{i=0}^{n-1} q_i x^i + x^n \in \mathbb{Z}[x],$$

such that $\Phi_{\mathbf{q}}(L)$ is an ideal in $R_{\mathbf{q}}$, we call L an ideal lattice with respect to $\mathbf{q}(x)$.

Remark. Using the notation from the definition above, we can also say that L is an ideal lattice with respect to vector $\mathbf{q} = (q_0, q_1, \ldots, q_{n-1})^\top$. Even if it is not necessary to specify polynomial $\mathbf{q}$, we simply call L an ideal lattice.

Observation 15. *If I is an ideal in $R_\mathbf{q}$, then the inverse image $\Phi_\mathbf{q}^{-1}(I)$ is always an ideal sublattice of $\mathbb{Z}^n$.*

Proof. a) $\Phi_\mathbf{q}^{-1}(I)$ is closed under addition because an ideal in $R_\mathbf{q}$ is closed under addition so it is an additive subgroup of $\mathbb{Z}^n$ hence $\Phi_\mathbf{q}^{-1}(I)$ is a sublattice of $\mathbb{Z}^n$ and

b) $\Phi_\mathbf{q}(\Phi_\mathbf{q}^{-1}(I)) = I$ is an ideal implies $\Phi_\mathbf{q}^{-1}(I)$ is an ideal lattice. □

Definition 16 (Cyclic lattice)**.** *A lattice which is ideal with respect to the rotation polynomial $\mathbf{q}(x) = x^n - 1$ is called* cyclic.

2.2 Identifying ideal lattices

As mentioned in the very beginning of this chapter, the thesis also includes an interesting result, originally proposed in [Ding and Lindner, 2007]. It is an algorithm that determines for a given basis whether the corresponding lattice is ideal or not. But firstly, we need to formulate and prove the key theorem on which the algorithm is based.

2.2.1 Notation

In the next chapter we will use the following notation.

Let $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$. By $\mathbf{Q}$ we will denote matrix:

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & -q_0 \\ \hline & & & -q_1 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & -q_{n-1} \end{array}\right).$$

Matrix $\mathbf{Q}$ can be written as $\mathbf{Q} = \mathbf{M} - F(\mathbf{q})$ where $\mathbf{M}$ and F are defined as follows:

$$\mathbf{M} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right) \quad \text{and} \quad F : \begin{array}{ccc} \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^{n\times n} \\ (v_0, \ldots, v_{n-1})^\top & \longmapsto & \begin{pmatrix} 0 & 0 & \cdots & v_0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & v_{n-2} \\ 0 & \cdots & 0 & v_{n-1} \end{pmatrix} \end{array}.$$

Remark. Matrix $\mathbf{M}$ and mapping F are dependent on the dimension n (as $\mathbf{M}_n$ or F_n) but since it is usually possible to deduce n from the context, for simplification we will omit indices.

Adjugate matrices will be often used in this chapter. For the definition of an adjugate matrix, see section 1.2.2.

2.2.2 Function F and matrix multiplication

We will use the following two simple facts in several other proofs. In the paper [Ding and Lindner, 2007], there are these facts used implicitly. For clarity, we have written them down as small observations.

Observation 17. *Let* $\mathbf{A}$ *be an* $n \times n$ *matrix and* $\mathbf{q}$ *be a vector of length* n*. Then* $\mathbf{A}F(\mathbf{q}) = F(\mathbf{Aq})$.

Proof. Straightforwardly from matrix-vector multiplication, we get:

$$\mathbf{A}F(\mathbf{q}) = \left(\begin{array}{c} \\ \mathbf{A}_{n\times n} \\ \\ \end{array}\right)\left(\begin{array}{c|c} & \\ \mathbf{0}_{n\times(n-1)} & \mathbf{q} \\ & \end{array}\right) =$$

$$= \left(\begin{array}{c|c} & \\ \mathbf{0}_{n\times(n-1)} & \mathbf{Aq} \\ & \end{array}\right) = F(\mathbf{Aq}).$$

□

Observation 18. *Let* $\mathbf{B}$ *be an* $n \times n$ *upper triangular matrix and* $\mathbf{q}$ *be a vector of length* n*. Then*

$$F(\mathbf{q})\mathbf{B} = B_{nn}F(\mathbf{q}) \tag{2.1}$$
$$= \mathbf{q} \cdot \mathbf{B}_{n,\cdot} \tag{2.2}$$

Proof. Let us start with equation (2.1). Straightforwardly from matrix-vector multiplication, we get:

$$F(\mathbf{q})\mathbf{B} = \left(\begin{array}{c|c} & \\ \mathbf{0}_{n\times(n-1)} & \mathbf{q} \\ & \end{array}\right)\begin{pmatrix} B_{11} & B_{12} & B_{13} & \dots & B_{1n} \\ & B_{22} & B_{23} & \dots & B_{2n} \\ & & \ddots & & \vdots \\ & \mathbf{0} & & \ddots & B_{(n-1)n} \\ & & & & B_{nn} \end{pmatrix} =$$

$$= \left(\begin{array}{c|c} & \\ \mathbf{0}_{n\times(n-1)} & B_{nn}\mathbf{q} \\ & \end{array}\right) = B_{nn}\left(\begin{array}{c|c} & \\ \mathbf{0}_{n\times(n-1)} & \mathbf{q} \\ & \end{array}\right) =$$

$$= B_{nn}F(\mathbf{q}).$$

Matrix $B_{nn}F(\mathbf{q})$ can be written using vector multiplication as $\mathbf{q} \cdot \mathbf{B}_{n,\cdot}$, where $\mathbf{B}_{n,\cdot}$ contains only zeros except for diagonal entry B_{nn}, which is exactly equation (2.2). □

2.2.3 Key Theorem

The aim of the following section is to replace the very brief proof of Lemma 1 from the article [Ding and Lindner, 2007] by a more detailed one, where we include explanations of particular steps. In our text, we refer to it as to the key theorem.

Theorem 19 (Identifying Ideal Lattices)**.** *Let $\mathbf{B} \in \mathbb{Z}^{n\times m}$ be a basis of lattice L. Then L is an ideal lattice if and only if there exist $\mathbf{T} \in \mathbb{Z}^{m\times m}$ and $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that*

$$\underbrace{\left(\begin{array}{c|c} 0 \;\cdots\; 0 & -q_0 \\ \hline & -q_1 \\ \mathbf{I}_{n-1} & \vdots \\ & -q_{n-1} \end{array}\right)}_{=\mathbf{Q}} \cdot \mathbf{B} = \mathbf{B}\mathbf{T}. \tag{2.3}$$

Proof. The proof will be achieved by proving several claims. We will show three equivalences that we will use subsequently and from this by transitivity the theorem will follow.

In the following claims let us consider polynomial $\mathbf{q}(x) = q_0 + \cdots + q_{n-1}x^{n-1} + x^n$ and corresponding $R_\mathbf{q}$.

Claim 1. *L is an ideal lattice (with respect to $\mathbf{q}$) if and only if $\Phi_\mathbf{q}(L)$ is closed under multiplication by x in $R_\mathbf{q}$.*

Proof. The fact that L is an ideal lattice means, according to the definition, that $I := \Phi_\mathbf{q}(L)$ is an ideal in $R_\mathbf{q}$ with respect to some monic polynomial $\mathbf{q}$ of degree n.

The definition of an ideal of a ring contains three items: $\Phi_\mathbf{q}(L) \subseteq R_\mathbf{q}$ is ideal if it is

(i) $\forall a, b \in \Phi_\mathbf{q}(L) : a + b \in \Phi_\mathbf{q}(L)$

(ii) $\forall a \in \Phi_\mathbf{q}(L) : -a \in \Phi_\mathbf{q}(L)$

(iii) $\forall a \in \Phi_\mathbf{q}(L), r \in R_\mathbf{q} : ar \in \Phi_\mathbf{q}(L)$.

Firstly, we will show that items (i) and (ii) hold anytime we have lattice L. Secondly, we will prove that point (iii) holds if and only if $\Phi_\mathbf{q}(L)$ is closed under multiplication by x.

(i) Let us take $a, b \in \Phi_\mathbf{q}(L) \subseteq R_\mathbf{q} = \mathbb{Z}[x]/\mathbf{q}(x)\mathbb{Z}[x]$,

$$\begin{aligned} a &= a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x], \\ b &= b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x], \end{aligned}$$

where $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in \mathbb{Z}$.
We want to show that also $a + b \in \Phi_\mathbf{q}(L)$. L is closed under addition, so

$$\Phi_\mathbf{q}^{-1}(a) + \Phi_\mathbf{q}^{-1}(b) = (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})^\top \in L$$

and $\Phi_{\mathbf{q}}$ is an isomorphism (we can use the linearity), so

$$\Phi_{\mathbf{q}}(\Phi_{\mathbf{q}}^{-1}(a) + \Phi_{\mathbf{q}}^{-1}(b)) = \Phi_{\mathbf{q}}(\Phi_{\mathbf{q}}^{-1}(a)) + \Phi_{\mathbf{q}}(\Phi_{\mathbf{q}}^{-1}(b)) = a + b \in \Phi_{\mathbf{q}}(L).$$

(ii) Now we consider an arbitrary

$$a = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x] \in \Phi_{\mathbf{q}}(L).$$

By lattice properties if $(a_0, a_1, \ldots, a_{n-1})^\top \in L$ then also $(-a_0, -a_1, \ldots, -a_{n-1})^\top \in L$. Therefore we can apply mapping $\Phi_{\mathbf{q}}$ to get

$$\begin{aligned}\Phi_{\mathbf{q}}(-a_0, -a_1, \ldots, -a_{n-1})^\top &= -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x] \\ &= -a \in \Phi_{\mathbf{q}}(L).\end{aligned}$$

(iii) We will show that

$$\begin{aligned}&\forall a \in \Phi_{\mathbf{q}}(L), r \in R_{\mathbf{q}} : ar \in \Phi_{\mathbf{q}}(L) \text{ holds} \\ &\qquad\qquad \iff \Phi_{\mathbf{q}}(L) \text{ is closed under multiplication by } x.\end{aligned}$$

"$\Rightarrow$" By setting $r = x$.
"$\Leftarrow$" Let us take an arbitrary $a \in \Phi_{\mathbf{q}}(L)$. We want to prove that

$$a \cdot (r_0 + r_1 x + \ldots + r_{n-1}x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x]) \in \Phi_{\mathbf{q}}(L),$$

where $r_0, \ldots, r_{n-1} \in \mathbb{Z}$. By assumption $x \cdot a \in \Phi_{\mathbf{q}}(L)$ and using item (i) above we know also $\Phi_{\mathbf{q}}(L)$ is closed under addition, so

$$\underbrace{(xa + xa + \cdots + xa)}_{r_1} = r_1 xa \in \Phi_{\mathbf{q}}(L).$$

Similarly we get $r_2 xa, \ldots, r_{n-1}xa \in \Phi_{\mathbf{q}}(L)$.

By using $x\Phi_{\mathbf{q}}(L) \subseteq \Phi_{\mathbf{q}}(L)$ iteratively:

$$r_2 x^2 a \in \Phi_{\mathbf{q}}(L), \ldots, r_{n-1}x^{n-1}a \in \Phi_{\mathbf{q}}(L)$$

and finally by using addition:

$$r_1 xa + r_2 x^2 a + \ldots + r_{n-1}x^{n-1}a \in \Phi_{\mathbf{q}}(L).$$

The equivalence is now complete.

$\triangle$

Claim 2. $\Phi_{\mathbf{q}}(L)$ is closed under multiplication by polynomial x in $R_{\mathbf{q}} \iff L = \text{span}_{\mathbb{Z}}(\mathbf{B})$ is closed under multiplication by $\mathbf{Q}$, where

$$\mathbf{Q} = \left(\begin{array}{c|c} 0 \;\cdots\; 0 & -q_0 \\ \hline & -q_1 \\ \mathbf{I}_{n-1} & \vdots \\ & -q_{n-1} \end{array}\right).$$

Proof.

Multiplication by polynomial x can be expressed as

$$\underbrace{(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})}_{=:\mathbf{a}(x)} \cdot x = a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n,$$

where $\mathbf{a}(x)$ is an arbitrary polynomial of a degree less than n.

In $R_{\mathbf{q}}$ this equality holds:

$$\mathbf{q}(x) = q_0 + \cdots + q_{n-1}x^{n-1} + x^n = 0$$

and

$$x^n = -q_0 - q_1 x - \cdots - q_{n-1}x^{n-1}.$$

Therefore

$$\begin{aligned}
&\mathbf{a}(x) \cdot x + \mathbf{q}(x)\mathbb{Z}[x] = \\
&= a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}(-q_0 - q_1 x - \cdots - q_{n-1}x^{n-1}) + \mathbf{q}(x)\mathbb{Z}[x] \\
&= -a_{n-1}q_0 + (a_0 - q_1 a_{n-1})x + \cdots + (a_{n-2} - q_{n-1}a_{n-1})x^{n-1} + \mathbf{q}(x)\mathbb{Z}[x].
\end{aligned}$$

Now we apply mapping $\Phi_{\mathbf{q}}^{-1}$.

$$\Phi_{\mathbf{q}}^{-1}\left(\mathbf{a}(x) \cdot x + \mathbf{q}(x)\mathbb{Z}[x]\right) = (-a_{n-1}q_0, a_0 - q_1 a_{n-1}, \ldots, a_{n-2} - q_{n-1}a_{n-1})^\top.$$

We can observe (it comes from matrix-vector multiplication) that this equality holds:

$$\left(\begin{array}{c|c} \begin{matrix} 0 & \cdots & 0 \end{matrix} & \begin{matrix} -q_0 \\ -q_1 \\ \vdots \\ -q_{n-1} \end{matrix} \\ \hline \mathbf{I}_{n-1} & \end{array}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} -q_0 \cdot a_{n-1} \\ a_0 - q_1 \cdot a_{n-1} \\ \vdots \\ a_{n-2} - q_{n-1} \cdot a_{n-1} \end{pmatrix},$$

which is exactly

$$\mathbf{Q} \cdot \Phi_{\mathbf{q}}^{-1}\left(\mathbf{a}(x) + \mathbf{q}(x)\mathbb{Z}[x]\right) = \Phi_{\mathbf{q}}^{-1}\left(\mathbf{a}(x) \cdot x + \mathbf{q}(x)\mathbb{Z}[x]\right).$$

Thus, for every $\mathbf{a}(x) + \mathbf{q}(x)\mathbb{Z}[x] \in \Phi_{\mathbf{q}}(L)$:

$$\mathbf{a}(x) \cdot x + \mathbf{q}(x)\mathbb{Z}[x] \in \Phi_{\mathbf{q}}(L) \iff \mathbf{Q}(\Phi_{\mathbf{q}}^{-1}\left(\mathbf{a}(x) + \mathbf{q}(x)\mathbb{Z}[x]\right)) \in L = \mathrm{span}_{\mathbb{Z}}(\mathbf{B}).$$

We have just proved that $\Phi_{\mathbf{q}}(L)$ is closed under multiplication by x in $R_{\mathbf{q}}$ if and only if $L = \mathrm{span}_{\mathbb{Z}}(\mathbf{B})$ is closed under multiplication by $\mathbf{Q}$.

△

Claim 3. $L = \mathrm{span}_{\mathbb{Z}}(\mathbf{B})$ is closed under multiplication by $\mathbf{Q}$ if and only if there exists a matrix $\mathbf{T} \in \mathbb{Z}^{m \times m}$ such that $\mathbf{QB} = \mathbf{BT}$.

Proof. Let us denote the columns in matrix $\mathbf{B}$ as

$$\mathbf{B} = \left(\begin{array}{c|c|c|c} & & & \\ \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_m \\ & & & \end{array}\right).$$

"$\Leftarrow$" If $\mathbf{QB} = \mathbf{BT}$ for an integer transformation $\mathbf{T}$, it means that every column of $\mathbf{QB}$ is included in L (it is an integer combination of $\mathbf{b}_1, \ldots, \mathbf{b}_m$.) If product $\mathbf{Qb}_i$ is contained in L and since L is closed under addition, then also $\mathrm{span}_{\mathbb{Z}}(\mathbf{B})$ is closed under multiplication by $\mathbf{Q}$.

"$\Rightarrow$" L is closed under multiplication by $\mathbf{Q}$, so

$$\mathbf{Qb}_1, \ldots, \mathbf{Qb}_m \in L = \mathrm{span}_{\mathbb{Z}}(\mathbf{B}).$$

The fact that $\mathbf{Qb}_1 \in \mathrm{span}_{\mathbb{Z}}(\mathbf{B})$ means that $\mathbf{Qb}_1$ can be written in the following form:

$$\mathbf{Qb}_1 = z_1^{(1)}\mathbf{b}_1 + z_2^{(1)}\mathbf{b}_2 + \ldots + z_m^{(1)}\mathbf{b}_m$$

for some $z_1^{(1)}, z_2^{(1)}, \ldots, z_m^{(1)} \in \mathbb{Z}$.
Similarly

$$\mathbf{Qb}_2 \in \mathrm{span}_{\mathbb{Z}}(\mathbf{B}) \iff \mathbf{Qb}_2 = z_1^{(2)}\mathbf{b}_1 + z_2^{(2)}\mathbf{b}_2 + \ldots + z_m^{(2)}\mathbf{b}_m$$

for some $z_1^{(2)}, z_2^{(2)}, \ldots, z_m^{(2)} \in \mathbb{Z}$ and so on.

Therefore we can write:

$$\mathbf{QB} = \left(\begin{array}{c|c|c|c} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_m \end{array}\right) \underbrace{\begin{pmatrix} z_1^{(1)} & z_2^{(1)} & \cdots & z_m^{(1)} \\ z_1^{(2)} & z_2^{(2)} & \cdots & z_m^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{(m)} & z_2^{(m)} & \cdots & z_m^{(m)} \end{pmatrix}}_{=:\mathbf{T}}.$$

So we have found an integer transformation $\mathbf{T}$ such that $\mathbf{QB} = \mathbf{BT}$.

△

By using successively observations above, we get: L is an ideal lattice (with respect to $\mathbf{q}$) if and only if there exists a matrix $\mathbf{T} \in \mathbb{Z}^{m\times m}$ such that $\mathbf{QB} = \mathbf{BT}$.

This fact can be described in other words as: L is an ideal lattice $\iff \exists \mathbf{T} \in \mathbb{Z}^{m\times m}$ and $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that

$$\underbrace{\left(\begin{array}{ccc|c} 0 & \cdots & 0 & -q_0 \\ & & & -q_1 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & -q_{n-1} \end{array}\right)}_{=:\mathbf{Q}} \cdot \mathbf{B} = \mathbf{BT}.$$

□

Remark. It follows from the proof that if we have L with basis $\mathbf{B}$ satisfying the following: there exists $\mathbf{T} \in \mathbb{Z}^{m\times m}$ and $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that $\mathbf{QB} = \mathbf{BT}$, then L is ideal with respect to $\mathbf{q}(x) = \sum_{i=0}^{n-1} q_i x^i + x^n$.

2.2.4 Equivalent formulations of Theorem 19 for full-rank lattices

In this section we discuss the full-rank lattices which are those whose dimension and rank are both equal to $n \in \mathbb{N}$ (see Definition 9). Here we use notation from section 2.2.1.

The following Proposition 20 was created by gathering facts used throughout the paper [Ding and Lindner, 2007]. We decided to write these spread facts clearly and prove them carefully.

Proposition 20 (Equivalent conditions for Ideal Lattices)**.** *Let L be a sublattice of $\mathbb{Z}^n$ and $\mathbf{B} \in \mathbb{Z}^{n\times n}$ its basis.*

Then the following points are equivalent:

(i) *L is an ideal lattice.*

(ii) *There exist $\mathbf{T} \in \mathbb{Z}^{n\times n}$ and $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that $\mathbf{QB} = \mathbf{BT}$.*

(iii) *There exist $\mathbf{T} \in \mathbb{Z}^{n\times n}$ and $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that $\mathbf{MB} - F(\mathbf{q})\mathbf{B} = \mathbf{BT}$.*

(iv) *There exists $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that $\mathbf{AMB} \equiv \mathbf{A}F(\mathbf{q})\mathbf{B} \mod d$.*

Moreover if $\mathbf{B}$ is an upper triangular matrix, all the items are equivalent also with:

(v) *There exists $(q_0, \ldots, q_{n-1})^\top \in \mathbb{Z}^n$ such that $\mathbf{AMB} \equiv B_{nn}F(\mathbf{Aq}) \mod d$.*

Proof. We will prove the equivalences between pairs of items and by the transitivity we will get that all the items will be mutually equivalent.

(i) $\Leftrightarrow$ (ii) It has been already proven in Theorem 19 for $m = n$.

(ii) $\Leftrightarrow$ (iii) We can equivalently rewrite equality $\mathbf{QB} = \mathbf{BT}$ for some $\mathbf{T} \in \mathbb{Z}^{n\times n}$ stated in Theorem 19 (using Notation in section 2.2.1) into

$$\mathbf{QB} = (\mathbf{M} - F(\mathbf{q}))\mathbf{B} = \mathbf{MB} - F(\mathbf{q})\mathbf{B} = \mathbf{BT}.$$

(iii) $\Leftrightarrow$ (iv) Firstly "$\Rightarrow$", let us take $\mathbf{A} = \mathrm{adj}(\mathbf{B})$ and multiply the equality from (iii) by $\mathbf{A}$. We get:

$$\mathbf{AMB} - \mathbf{A}F(\mathbf{q})\mathbf{B} = \mathbf{ABT}.$$

Since $\mathbf{A}$ is an adjugate matrix of $\mathbf{B}$, property $\mathbf{AB} = d\mathbf{I}_n$ holds where $d = \det(\mathbf{B})$ (see the remark in Section 1.2.2). We can write:

$$\mathbf{AMB} - \mathbf{A}F(\mathbf{q})\mathbf{B} = d\mathbf{T}.$$

It means that $\mathbf{AMB}$ is necessarily congruent to $\mathbf{A}F(\mathbf{q})\mathbf{B} \mod d$ (see Definition 2):

$$\mathbf{AMB} \equiv \mathbf{A}F(\mathbf{q})\mathbf{B} \mod d.$$

Also the opposite implication: congruence $\mathbf{AMB} \equiv \mathbf{A}F(\mathbf{q})\mathbf{B} \mod d$ implies by definition the existence of some $\mathbf{T} \in \mathbb{Z}^{n\times n}$ such that $\mathbf{AMB} - \mathbf{A}F(\mathbf{q})\mathbf{B} = d\mathbf{T}$.

(iv) $\Leftrightarrow$ (v) Since $\mathbf{B}$ is in the upper triangular form we have (by firstly applying Observation 17 to the right-hand side to get there $F(\mathbf{Aq})\mathbf{B}$ and afterwards applying Observation 18):

$$\mathbf{AMB} \equiv B_{nn}F(\mathbf{Aq}) \mod d.$$

□

2.2.5 Necessary condition for ideal lattices

The following lemma is one of our results. It has come out that this is very helpful in specific examples, where we want to show that a certain lattice is not ideal (we use it, for instance, in the proof of Proposition 32).

Lemma 21. *Let L be a sublattice of $\mathbb{Z}^n$ and $\mathbf{B} \in \mathbb{Z}^{n\times n}$ its basis (not necessarily in **HNF**). If L is an ideal lattice, then every row of $\mathbf{AMB} \mod d$ is an integer multiple of the last row of matrix $\mathbf{B}$ modulo d.*

Proof. If L is an ideal lattice, we get (using points (i) and (iv) from Proposition 20):

$$\mathbf{AMB} \equiv \mathbf{A}F(\mathbf{q})\mathbf{B} \mod d.$$

According to Observation 17 the right-hand side can be rewritten into $F(\mathbf{Aq})\mathbf{B}$. Thus if we denote the rows in $\mathbf{B}$ and elements in vector $\mathbf{Aq}$:

$$\mathbf{B} = \left(\begin{array}{c} \mathbf{B}_{1,\cdot} \\ \hline \mathbf{B}_{2,\cdot} \\ \hline \vdots \\ \hline \mathbf{B}_{n,\cdot} \end{array}\right) \text{ and } \mathbf{Aq} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix},$$

we get:

$$F(\mathbf{Aq})\mathbf{B} = \left(\begin{array}{c|c} \mathbf{0}_{n\times(n-1)} & \begin{array}{c} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{array} \end{array}\right) \left(\begin{array}{c} \mathbf{B}_{1,\cdot} \\ \hline \mathbf{B}_{2,\cdot} \\ \hline \vdots \\ \hline \mathbf{B}_{n,\cdot} \end{array}\right) = \left(\begin{array}{c} a_0\mathbf{B}_{n,\cdot} \\ \hline a_1\mathbf{B}_{n,\cdot} \\ \hline \vdots \\ \hline a_{n-1}\mathbf{B}_{n,\cdot} \end{array}\right).$$

We see that each row in $F(\mathbf{Aq})\mathbf{B}$ is a multiple of $\mathbf{B}_{n,\cdot}$ which is the last row of $\mathbf{B}$. Since $\mathbf{AMB} \mod d$ is congruent to this, each row in matrix $\mathbf{AMB} \mod d$ is a multiple of $\mathbf{B}_{n,\cdot} \mod d$. □

2.2.6 Full-rank lattices

Usually when doing research on lattices, people focus on the full-rank lattices. In the algorithm (see Section 3.1) we will also focus on the full-rank basis only. This is not a fundamental restriction, because of the following proposition: (the proof stems from [Micciancio and Lyubashevsky, 2005, Lemma 3.2])

Proposition 22. *Let $\mathbf{f} \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n. Every ideal $I \neq \{\mathbf{0}\}$ of ring $\mathbb{Z}[x]/(\mathbf{f})$ is isomorphic to a full-rank lattice in $\mathbb{Z}^n$.*

Proof. Since $\mathbb{Z}[x]/(\mathbf{f})$ is a noetherian ring, each ideal is finally generated $I = \langle \mathbf{g}_1, \ldots, \mathbf{g}_m \rangle$. We can assume without loss on generality that they have degree less than n. Moreover one of $\mathbf{g}_i$ has to be nonzero, because $I \neq \{\mathbf{0}\}$, and without loss of generality we can assume it is $\mathbf{g}_1$. We will show that

$$\{\mathbf{g}_1, \mathbf{g}_1 x, \mathbf{g}_1 x^2, \ldots, \mathbf{g}_1 x^{n-1}\}$$

is a linearly independent set over $\mathbb{Z}$. This means that vectors

$$\Phi_{\mathbf{f}}^{-1}(\mathbf{g}_1), \Phi_{\mathbf{f}}^{-1}(\mathbf{g}_1 x), \Phi_{\mathbf{f}}^{-1}(\mathbf{g}_1 x^2), \ldots, \Phi_{\mathbf{f}}^{-1}(\mathbf{g}_1 x^{n-1})$$

are also linearly independent over $\mathbb{Z}$ (using the notation from Section 2.1.1), so lattice L containing them must have rank n.

Thus, if

$$\{\mathbf{g}_1, \mathbf{g}_1 x, \mathbf{g}_1 x^2, \ldots, \mathbf{g}_1 x^{n-1}\}$$

were linearly dependent, there would exist a non-zero sequence of coefficients $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n$ such that

$$a_0\mathbf{g}_1 + a_1\mathbf{g}_1 x + a_2\mathbf{g}_1 x^2 + \ldots + a_{n-1}\mathbf{g}_1 x^{n-1} \in (\mathbf{f}).$$

This means that there would exist a polynomial $\mathbf{h} \in \mathbb{Z}[x]$ such that

$$a_0\mathbf{g}_1 + a_1\mathbf{g}_1 x + a_2\mathbf{g}_1 x^2 + \ldots + a_{n-1}\mathbf{g}_1 x^{n-1} = \mathbf{fh}.$$

The left-hand side can be written as

$$\mathbf{g}_1(a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1}x^{n-1})$$

and $\mathbf{f}$ which is irreducible (and prime) divides this product, hence then either $\mathbf{f} \mid \mathbf{g}_1$ or $\mathbf{f} \mid (a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1}x^{n-1})$. These polynomials have degrees less than n so one of them would have to be zero. □

3. Algorithm and Examples

The chapter is based on [Ding and Lindner, 2007, Section 2.3, 2.4 and 2.6] enriched by our own examples. The algorithm for identifying ideal lattices takes the most important part here. We offer the proof of its correctness in more detail using an arranged structure.

3.1 Algorithm for identifying ideal lattices

In the paper, there is the algorithm described in a very similar way except for steps that were vague. We reformulated them to make the algorithm more precise.

Algorithm 1: Identifying ideal lattices with full-rank bases

Data: A full-rank basis $\widetilde{\mathbf{B}} \in \mathbb{Z}^{n \times n}$
Result: **true** and $\mathbf{q}$, if $\mathbf{B}$ spans an ideal lattice with respect to $\mathbf{q}$, otherwise **false**

1 Transform $\widetilde{\mathbf{B}}$ into **HNF**, set the obtained matrix to $\mathbf{B}$
2 Calculate $\mathbf{A} = \mathrm{adj}(\mathbf{B}), d = \det(\mathbf{B})$, and $z = B_{nn}$
3 Calculate product $\mathbf{P} = \mathbf{AMB} \mod d$
4 **if** *the first* $n-1$ *columns of* $\mathbf{P}$ *are zero* **then**
5 | set $\mathbf{c} = \mathbf{P}_{\cdot,n}$ to equal the last column
6 **else return false**
7 **if** $z \mid \mathbf{c}_i$ *for* $i = 1, \ldots, n$ **then**
8 | use **CRT** to find $\mathbf{q}^* \equiv \frac{1}{z}\mathbf{c} \mod d/z$ and $\mathbf{q}^* \equiv \mathbf{0} \mod z$
9 **else return false**
10 **if** $\mathbf{Bq}^* \equiv \mathbf{0} \mod d/z$ **then**
11 | **return true**, $\mathbf{q} = \frac{1}{d}\mathbf{Bq}^*$
12 **else return false**

Remark. For clarification of selected steps:

- An algorithm for transformation of $\widetilde{\mathbf{B}}$ into **HNF** is provided as a part of the proof in [Cohen, 2013, Theorem 2.4.3].
- Since $\mathbf{B}$ is in **HNF**, its entries are positive so determinant d (as a product of diagonal entries) is a natural number and we can calculate modulo d.
- Abbreviation **CRT** in step 8 stands for Chinese Remainder Theorem (for understanding the way in which we use it, see Theorem 3 and the affiliated remark).

In the original paper, many steps in the proof of correctness of Algorithm 1 were unclear. We have adjusted the proof to a more readable form and added parts of explanation that were skipped in [Ding and Lindner, 2007, Section 2.4].

Theorem 23 (Correctness)**.** *Algorithm 1 is correct.*

Proof. We will show that the algorithm always gives the correct result.

Firstly, let us notice that transformation into **HNF** does not change the lattice. Thus if the algorithm examines whether $L(\mathbf{B})$ is ideal lattice, it is the same as to examine whether $L(\widetilde{\mathbf{B}})$ is ideal. This follows from Corollary 13.

Let us take $\mathbf{A} = \mathrm{adj}(\mathbf{B})$ like in Algorithm 1. Since $\mathbf{B}$ is in the upper triangular form, Proposition 20, items (i) and (v) imply that lattice L spanned by $\mathbf{B}$ is an ideal lattice if and only if there exists a vector $\mathbf{q} \in \mathbb{Z}^n$ such that

$$\mathbf{AMB} \equiv B_{nn} F(\mathbf{Aq}) \mod d.$$

So if we use notation $z = B_{nn}$ from Algorithm 1, we get that for an ideal lattice this congruence equivalently holds:

$$\mathbf{AMB} \equiv zF(\mathbf{Aq}) \mod d. \tag{3.1}$$

On the right-hand side, there is a matrix where columns 1 to $n-1$ are full of zeros. Therefore if we are calculating modulo d, only the last column of matrix $\mathbf{AMB} \mod d$ can (but it does not have to) be non-zero for an ideal lattice. It means that if the algorithm terminates in step 6, lattice L is not ideal and result "false" is correct.

If we denote the last column of $\mathbf{AMB} \mod d$ by $\mathbf{c}$, from equality (3.1) which holds for an ideal lattice, we get:

$$\mathbf{c} \equiv z\mathbf{Aq} \mod d. \tag{3.2}$$

Since z is a divisor of d (because d is the determinant of an upper triangular matrix where z is one of the diagonal entries), also

$$\mathbf{c} \equiv z\mathbf{Aq} \mod z.$$

The right-hand side is equivalent to zero modulo z, therefore z is a divisor of the left-hand side, as well. It means that all of the entries of $\mathbf{c}$ have to be divisible by $z = B_{n,n}$ for an ideal lattice. So if it is not true and the algorithm terminates on line 9, result "false" is again correct.

The last termination in the algorithm occurs in the case that

$$\mathbf{Bq}^* \not\equiv \mathbf{0} \mod d/z,$$

where $\mathbf{q}^* \equiv \frac{1}{z}\mathbf{c} \mod d/z$ and $\mathbf{q}^* \equiv \mathbf{0} \mod z$.

Claim 4.

$$\mathbf{Bq}^* \not\equiv \mathbf{0} \mod d/z \implies \mathbf{Bq}^* \not\equiv \mathbf{0} \mod d.$$

Proof. By contradiction. Let us assume

$$\mathbf{Bq}^* \equiv \mathbf{0} \mod d.$$

Since d and $\mathbf{q}^*$ are divisible by z, we can use the congruence property of division (component-wise) to get:

$$\mathbf{B}(\frac{1}{z}\mathbf{q}^*) \equiv \mathbf{0} \mod d/z,$$

Now, by the other property of congruences, we can multiply the left-hand side and right-hand side by z to get:

$$\mathbf{Bq}^* \equiv \mathbf{0} \mod d/z,$$

which leads to the contradiction to an assumption.

△

Thus we know $\mathbf{Bq}^* \not\equiv \mathbf{0} \mod d$ which will be used in further calculations.

From equation (3.2), we get for an ideal lattice:

$$\frac{1}{z}\mathbf{c} \equiv \mathbf{Aq} \mod d,$$

which implies

$$\mathbf{q}^* = \frac{1}{z}\mathbf{c} \equiv \mathbf{Aq} \mod d. \tag{3.3}$$

If we multiply this equation by $\mathbf{B}$ and use the remark in Section 1.2.2, we get:

$$\mathbf{Bq}^* \equiv \mathbf{BAq}^* \equiv d\mathbf{I}_n\mathbf{q}^* \equiv \mathbf{0} \mod d. \tag{3.4}$$

Equation (3.4) holds for an ideal lattice. So if the algorithm terminates in step 12 in the case $\mathbf{Bq}^* \not\equiv \mathbf{0} \mod d/z$, by Claim 4: $\mathbf{Bq}^* \not\equiv \mathbf{0} \mod d$ so equation (3.4) does not hold and lattice L is not ideal.

The last possible termination of the algorithm is in step 11. In the first part of this proof, we have seen that finding a solution for congruence (3.1) is equivalent to having solutions $\mathbf{q}, \mathbf{T}$ for:

$$(\mathbf{M} - F(\mathbf{q}))\mathbf{B} = \mathbf{BT},$$

which is equivalent to L being an ideal lattice according to Theorem 20. We will show that

$$\mathbf{P} = \mathbf{AMB} \equiv zF(\mathbf{Aq}) \mod d,$$

which is exactly equation (3.1). Since the algorithm terminates in step 11, it means that in the previous "if conditions" the answer was positive. By line 5 we get

$$\begin{aligned}\mathbf{P} = \mathbf{AMB} &\mod d\\ \equiv F(\mathbf{c}) &\mod d\end{aligned}$$

(in $\mathbf{P}$, there are first $n-1$ columns zero and the last column is denoted by $\mathbf{c}$).

By the positive answer of the next "if condition" (in step 8) we have $\mathbf{q}^* = \frac{1}{z}\mathbf{c} \mod \frac{d}{z}$. We can rewrite this as $\frac{d}{z}|(\mathbf{q}^* - \frac{1}{z}\mathbf{c})$. It means there exists $\mathbf{k} \in \mathbb{Z}^n$ such that $\mathbf{q}^* - \frac{1}{z}\mathbf{c} = \frac{d}{z}\mathbf{k}$. If we multiply this equality by z we have: $z\mathbf{q}^* - \mathbf{c} = d\mathbf{k}$. It means $d|(z\mathbf{q}^* - \mathbf{c})$ and

$$z\mathbf{q}^* \equiv \mathbf{c} \mod d.$$

So we can write

$$\mathbf{P} \equiv F(\mathbf{c}) \equiv F(z\mathbf{q}^*) \equiv zF(\mathbf{q}^*) \mod d.$$

Finally, we can use the property of adjugate matrices (see the remark in Section 1.2.2)

$$\mathbf{I}_n(zF(\mathbf{q}^*)) = \frac{1}{d}\mathbf{AB} \cdot z(F(\mathbf{q}^*))$$

to get:

$$\mathbf{P} \equiv zF(\mathbf{q}^*) \equiv \mathbf{I}_n(zF(\mathbf{q}^*)) \equiv \frac{1}{d}\mathbf{AB} \cdot z(F(\mathbf{q}^*)) \equiv \frac{z}{d}\mathbf{AB} \cdot F(\mathbf{q}^*) \mod d.$$

Using Observation 17 we can write

$$\mathbf{P} \equiv \frac{z}{d}\mathbf{AB} \cdot F(\mathbf{q}^*) \equiv \frac{z}{d} \cdot F(\mathbf{ABq}^*) \mod d.$$

By small arrangements

$$\mathbf{P} \equiv zF(\mathbf{A}\frac{\mathbf{Bq}^*}{d}) \mod d,$$

which is according to our definition of $\mathbf{q}$ in step 11 exactly the equivalent condition for proving L is an ideal lattice (equation (3.1)) that is

$$\mathbf{P} \equiv zF(\mathbf{Aq}) \mod d.$$

We have shown that each output of the algorithm is correct. □

3.2 Examples

The following section was created as a selection of examples that we have found interesting. The concept of circulant matrices has led us down to the consideration of the relation between the cyclic lattices and the structure of their basis. Ideas and results are included in Section 3.2.2. In the end, this section contains as well a few examples from the original paper [Ding and Lindner, 2007, Section 2.6] which we describe in more detail.

3.2.1 Applying the algorithm

In this section we introduce a special type of matrices so called circulant matrices. This is a nice model for seeing how the algorithm works.

Example. By *circulant matrix* we mean a square $n \times n$ matrix such that columns are cyclically shifted:

$$\mathbf{A} = \begin{pmatrix} a_1 & a_n & \cdots & a_2 \\ a_2 & a_1 & \cdots & a_3 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$

This structure can be obtained using multiplication by matrix

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 1 \\ \hline & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right) \text{ and } \mathbf{a} = (a_1, a_2 \ldots, a_n)^\top \in \mathbb{Z}^n$$

as

$$\mathbf{A} = (\mathbf{a}|\mathbf{Q}\mathbf{a}|\ldots|\mathbf{Q}^{n-1}\mathbf{a}).$$

Let us apply Algorithm 1 to this circulant matrix (corresponding steps in the algorithm are numbered by the same value as it is here in the example):

$$\widetilde{\mathbf{B}} = \begin{pmatrix} 5 & 7 & 3 \\ 3 & 5 & 7 \\ 7 & 3 & 5 \end{pmatrix}.$$

Algorithm 2: Example

1 Firstly, we need to transform matrix $\widetilde{\mathbf{B}}$ into **HNF**. Using the following

$$\mathbf{U} = \begin{pmatrix} 2 & 1 & 1 \\ 17 & 11 & 8 \\ -13 & -8 & -6 \end{pmatrix} \in GL_n(\mathbb{Z})$$

we get

$$\mathbf{B} = \widetilde{\mathbf{B}}\mathbf{U} = \begin{pmatrix} 90 & 58 & 43 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

2 We calculate

$$\mathbf{A} = \mathrm{adj}(\mathbf{B}) = \begin{pmatrix} 2 & -58 & -28 \\ 0 & 90 & -90 \\ 0 & 0 & 180 \end{pmatrix},$$

$d = \det(\mathbf{B}) = 180$, and $z = B_{33} = 1$.

3 Calculation of product $\mathbf{P} = \mathbf{AMB} \mod 180$, where $\mathbf{M} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$:

$$\mathbf{P} = \begin{pmatrix} -5220 & -3420 & -2522 \\ 8100 & 5040 & 3780 \\ 0 & 360 & 180 \end{pmatrix} \mod 180 = \begin{pmatrix} 0 & 0 & 178 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

4 Since the first 2 columns of $\mathbf{P}$ are zero,

5 therefore we set $\mathbf{c} = \mathbf{P}_{\cdot,3} = \begin{pmatrix} 178 \\ 0 \\ 0 \end{pmatrix}$.

7 Every number is divisible by 1,

8 hence we can use **CRT** to find $\mathbf{q}^* \equiv \mathbf{c} \mod 180$ and $\mathbf{q}^* \equiv \mathbf{0} \mod 1$. The second congruence does not add any other information since each number is congruent $0 \mod 1$. Thus we set

$$\mathbf{q}^* = \begin{pmatrix} 178 \\ 0 \\ 0 \end{pmatrix}.$$

10 The final "if condition" is also satisfied because:

$$\mathbf{Bq}^* = \begin{pmatrix} 90 & 58 & 43 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 178 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 178 \cdot 90 \\ 0 \\ 0 \end{pmatrix} \mod 180 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

11 Finally, the algorithm terminates with the answer *true* and

$\mathbf{q} = \frac{1}{180}\mathbf{Bq}^* = \begin{pmatrix} 89 \\ 0 \\ 0 \end{pmatrix}$.

3.2.2 Circulant matrices and cyclic lattices

In the previous section, using the algorithm, we have seen that the lattice with basis

$$\mathbf{B} = \begin{pmatrix} 5 & 7 & 3 \\ 3 & 5 & 7 \\ 7 & 3 & 5 \end{pmatrix}$$

is ideal with respect to polynomial $x^3 + 89$. Corresponding $\mathbf{Q}$ to this polynomial is

$$\mathbf{Q} = \begin{pmatrix} 0 & 0 & -89 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Therefore we know (using equality (2.3) in Theorem 19) that there exists an integer matrix $\mathbf{T} \in \mathbb{Z}^{n \times n}$ such that $\mathbf{QB} = \mathbf{BT}$. We can multiply the equality by $\mathbf{B}^{-1}$ to get

$$\mathbf{T} = \begin{pmatrix} -14 & -6 & -9 \\ -118 & -51 & -85 \\ 91 & 40 & 65 \end{pmatrix}.$$

However, the algorithm does not guarantee the uniqueness of polynomial $\mathbf{q}$. For instance, $\mathbf{B}$ is also ideal with respect to $x^3 - 1$. This can be seen from equality (2.3) in Theorem 19:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 7 & 3 \\ 3 & 5 & 7 \\ 7 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 7 & 3 \\ 3 & 5 & 7 \\ 7 & 3 & 5 \end{pmatrix} \mathbf{T},$$

where we set $\mathbf{T}$ to be

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The general property of $n \times n$ circulant matrices is that they are a basis of an ideal lattice with respect to polynomial $x^n - 1$. This brings us back to the definition of a cyclic lattice which is an ideal lattice with respect to polynomial $x^n - 1$. This could lead to speculations whether there is indeed a basis of this special shape for each cyclic lattice. The following calculation shows a counter-example when we have a cyclic lattice, but the basis of this form does not exist.

Example. Let us work in dimension 2, we have the polynomial $x^2 - 1$, thus:

$$\mathbf{Q} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and let us consider basis } \mathbf{B} = \begin{pmatrix} -2 & -1 \\ -2 & 1 \end{pmatrix}.$$

This $\mathbf{B}$ is a basis of an ideal lattice with respect to $x^2 - 1$ (a cyclic lattice). This can be seen using Theorem 19 for

$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ satisfying } \mathbf{QB} = \mathbf{BT}.$$

However, there is no vector $\mathbf{a} \in \mathbb{Z}^2$ such that $(\mathbf{a}|\mathbf{Qa})$ would be also a basis of lattice $L(\mathbf{B})$, which can be proved in the following way:

If there existed such a basis $\mathbf{A} = (\mathbf{a}|\mathbf{Qa})$ of lattice $L(\mathbf{B})$, matrix $\mathbf{A}$ would be of the form $\mathbf{A} = \mathbf{BU}$ for some matrix $\mathbf{U} \in GL_n(\mathbb{Z})$ (see Theorem 12).

Let us denote

$$\mathbf{U} = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \text{ and } \mathbf{A} = \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}.$$

We assume all these relations:

$$\mathbf{A} = \mathbf{BU} = (\mathbf{a}|\mathbf{Qa}) = \begin{pmatrix} v_1 & v_3 \\ v_3 & v_1 \end{pmatrix}$$

and using the following calculations:

$$\mathbf{BU} = \begin{pmatrix} -2 & -1 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} = \begin{pmatrix} -2u_1 - u_3 & -2u_2 - u_4 \\ -2u_1 + u_3 & -2u_2 + u_4 \end{pmatrix},$$

we get these equations:

$$-2u_1 - u_3 = -2u_2 + u_4$$
$$-2u_1 + u_3 = -2u_2 - u_4.$$

Straightforwardly from this system of equations we get $u_1 = u_2$ and $u_3 = u_4$. This means

$$\det \mathbf{U} = \det \begin{pmatrix} u_1 & u_1 \\ u_3 & u_3 \end{pmatrix} = -2u_1u_3.$$

Since u_1 and u_3 are integers, $\det(\mathbf{U}) = -2u_1u_3 \neq \pm 1$ and such a matrix $\mathbf{U} \notin GL_n(\mathbb{Z})$. Therefore $L(\mathbf{B})$ has no basis of the form $(\mathbf{a}|\mathbf{Qa})$ for $\mathbf{a} \in \mathbb{Z}^2$.

3.2.3 Examples from the paper

The following lemma comes from the paper [Ding and Lindner, 2007, Section 2.6]. It is a nice result that we have reformulated a little bit and added some steps to the proof.

Lemma 24. *Let $\mathbf{B} \in \mathbb{Z}^{n \times n}$ be a basis in HNF of a full-rank ideal lattice with respect to $\mathbf{q}$. Then for the first diagonal entry of $\mathbf{B}$ and for every $k \in \mathbb{Z}$ matrix*

$$\mathbf{B}' = \left(\begin{array}{c|ccc} kB_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{array} \right)$$

spans an ideal lattice of dimension $n+1$ with respect to $\mathbf{q}' = (0\ \mathbf{q})^\top$.

Proof. Since the lattice spanned by $\mathbf{B}$ is an ideal lattice, we can use Theorem 19: there exists a matrix $\mathbf{T} \in \mathbb{Z}^{n \times n}$ such that

$$\mathbf{MB} - F(\mathbf{q})\mathbf{B} = \mathbf{BT},$$

where

$$\mathbf{M} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array} \right).$$

We will use Theorem 19 to prove that the lattice spanned by $\mathbf{B}'$ is also ideal with respect to $\mathbf{q}' = (0, q_0, q_1, \ldots, q_{n-1})^\top$. Therefore we want to find $\mathbf{T}'$ such that:

$$\left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I}_n & & \vdots \\ & & & 0 \end{array}\right)\mathbf{B}' - \left(\begin{array}{c|c} & 0 \\ \mathbf{0}_{(n+1)\times n} & q_0 \\ & \vdots \\ & q_{n-1} \end{array}\right)\mathbf{B}' = \mathbf{B}'\mathbf{T}'. \tag{3.5}$$

The first term on the left-hand side of equality (3.5):

$$\left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I}_n & & \vdots \\ & & & 0 \end{array}\right)\left(\begin{array}{c|ccc} kB_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline kB_{11} & & & \\ \vdots & & \mathbf{MB} & \\ 0 & & & \end{array}\right).$$

The second term on the left-hand side of equality (3.5):

$$\left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & F(\mathbf{q}) & \\ 0 & & & \end{array}\right)\left(\begin{array}{c|ccc} kB_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & F(\mathbf{q})\mathbf{B} & \\ 0 & & & \end{array}\right).$$

Since by assumption $\mathbf{MB} - F(\mathbf{q})\mathbf{B} = \mathbf{BT}$, we can rewrite the left-hand side in equality (3.5):

$$\left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline kB_{11} & & & \\ \vdots & & \mathbf{MB} & \\ 0 & & & \end{array}\right) - \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & F(\mathbf{q})\mathbf{B} & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline kB_{11} & & & \\ \vdots & & \mathbf{BT} & \\ 0 & & & \end{array}\right).$$

Thus, if we set $\mathbf{T}'$ to:

$$\mathbf{T}' = \left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline k & & & \\ \vdots & & \mathbf{T} & \\ 0 & & & \end{array}\right),$$

equality (3.5) will be satisfied:

$$\left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline kB_{11} & & & \\ \vdots & & \mathbf{BT} & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} kB_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{array}\right)\left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline k & & & \\ \vdots & & \mathbf{T} & \\ 0 & & & \end{array}\right).$$

From this, using Theorem 19, we get that $\mathbf{B}'$ spans an ideal lattice with respect to $\mathbf{q}' = (0\ \mathbf{q})^\top$. □

Another interesting example from [Ding and Lindner, 2007] is in Section 3.3.1.

3.3 Lattice isomorphism

A part of our own contribution is the generalised Theorem 3 from [Ding and Lindner, 2007]. This theorem is based on the theory of Lattice isomorphism, so we will begin the section with the most reliable definitions and propositions.

3.3.1 Definitions and basic properties

These two matrices provide an interesting example that similarly looking matrices are one a basis of an ideal lattice, the other one not (it can be seen using Algorithm 1):

$$\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \text{ , where } k \in \mathbb{Z} \setminus \{0, \pm 1\}.$$

It happens because not all real transformations keep the ring structure. This is the motivation for the concept of Lattice isomorphism.

Definition 25 (Lattice isomorphism)**.** *Let L, M be sublattices of $\mathbb{R}^n$. We say that L* is isomorphic to *M if there exists an orthogonal transformation $\mathbf{T} \in \mathrm{O}_n(\mathbb{R})$ such that $M = \mathbf{T}L := \{\mathbf{T}l \mid l \in L\}$.*

Definition 26 (Lattice isomorphism class)**.** *Let L be a sublattice of $\mathbb{R}^n$. The isomorphism class of L is the orbit corresponding to L*

$$\mathrm{O}_n(\mathbb{R})L = \{\mathbf{T}L \mid \mathbf{T} \in \mathrm{O}_n(\mathbb{R})\}.$$

Lemma 27. *Let L, M be sublattices of $\mathbb{Q}^n$. If L has full rank and is isomorphic to M, i.e. there exists $\mathbf{T} \in \mathrm{O}_n(\mathbb{R})$ such that $M = \mathbf{T}L$, then $\mathbf{T} \in \mathrm{O}_n(\mathbb{Q})$.*

Proof. Since L is a sublattice of $\mathbb{Q}^n$ and has full rank, L has a basis $\mathbf{B}_L \in \mathbb{Q}^{n \times n}$. L is isomorphic to M, thus every point in L, basis included, is mapped into $M \subseteq \mathbb{Q}^n$.

Therefore $\mathbf{C} := \mathbf{T}\mathbf{B}_L \in \mathbb{Q}^{n \times n}$. This means T must be rational as well because B is invertible (it is a full-rank matrix over field $\mathbb{Q}$). Hence

$$\mathbf{T} = \mathbf{C}\mathbf{B}_L^{-1} \in \mathrm{O}_n(\mathbb{Q}).$$

□

Since we consider only integer matrices and $\mathbb{Z} \subset \mathbb{Q}$, Lemma 27 says that it is sufficient to study only $\mathrm{O}_n(\mathbb{Q})$ instead of $\mathrm{O}_n(\mathbb{R})$.

3.3.2 Structure of $\mathrm{O}_2(\mathbb{Q})$

Our generalised theorem is proved for dimension two. Thus from now till the end of this chapter, we consider dimension two only. Before we will provide the generalised theorem about the ideal lattices in particular isomorphism classes, we will take a look at the structure of $\mathrm{O}_2(\mathbb{Q})$.

Proposition 28. *(a) Every orthogonal transformation in $\mathbb{R}^2$ is a rotation or a reflection.*

$$\mathrm{O}_2(\mathbb{R}) = \left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \middle| \alpha \in [0, 2\pi) \right\rangle.$$

(b) *The group of orthogonal* 2×2 *matrices over* $\mathbb{Q}$ *can be written in the following way:*

$$\mathrm{O}_2(\mathbb{Q}) = \left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \Big| \alpha \in [0, 2\pi) \right\rangle \cap \mathbb{Q}^{2\times 2},$$

which can be rewritten into the form

$$\left\{ \frac{1}{c} \begin{pmatrix} b & -a \\ a & b \end{pmatrix}, \frac{1}{c} \begin{pmatrix} -b & a \\ a & b \end{pmatrix} \Big| a, b, c \in \mathbb{Z}, a^2 + b^2 = c^2 \right\}.$$

Proof. (a) This claim is included in [Barto and Tůma, Proposition 10.24].

(b) The equality

$$\mathrm{O}_2(\mathbb{Q}) = \left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \Big| \alpha \in [0, 2\pi) \right\rangle \cap \mathbb{Q}^{2\times 2}$$

follows from (a).

Now it is sufficient to show equality between two sets:

$$\left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \Big| \alpha \in [0, 2\pi) \right\rangle \cap \mathbb{Q}^{2\times 2}$$

$$= \left\{ \frac{1}{c} \begin{pmatrix} b & -a \\ a & b \end{pmatrix}, \frac{1}{c} \begin{pmatrix} -b & a \\ a & b \end{pmatrix} \Big| a, b, c \in \mathbb{Z}, a^2 + b^2 = c^2 \right\}.$$

We will provide the proof by two inclusions:

"$\subseteq$" Matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

is included in the second set because it is of the form

$$\frac{1}{c} \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$$

for $a = 0, b = 1$ and $c = 1$.

Now let us take an arbitrary matrix of the form

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

with rational coefficients and we will show this matrix is included in

$$\left\{ \frac{1}{c} \begin{pmatrix} b & -a \\ a & b \end{pmatrix}, \frac{1}{c} \begin{pmatrix} -b & a \\ a & b \end{pmatrix} \Big| a, b, c \in \mathbb{Z}, a^2 + b^2 = c^2 \right\}.$$

Because of the rational coefficients we can rewrite

$$\sin(\alpha) = \frac{z_1}{z_2} \text{ and } \cos(\alpha) = \frac{w_1}{w_2} \text{ for some } z_1, z_2, w_1, w_2 \in \mathbb{Z}.$$

Since $\sin(\alpha)^2 + \cos(\alpha)^2 = 1$ we get

$$\left(\frac{z_1}{z_2}\right)^2 + \left(\frac{w_1}{w_2}\right)^2 = 1 \text{ which gives } (z_1 w_2)^2 + (w_1 z_2)^2 = (z_2 w_2).$$

If we set $a = z_1 w_2$, $b = w_1 z_2$ and $c = z_2 w_2$, we get

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} = \begin{pmatrix} \frac{w_1}{w_2} & -\frac{z_1}{z_2} \\ \frac{z_1}{z_2} & \frac{w_1}{w_2} \end{pmatrix} = \begin{pmatrix} \frac{b}{c} & -\frac{a}{c} \\ \frac{a}{c} & \frac{b}{c} \end{pmatrix} = \frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix},$$

where $a^2 + b^2 = c^2$. Therefore, this set inclusion is complete.

"$\supseteq$" Now we want to show that any element from set

$$\left\{ \frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix}, \frac{1}{c}\begin{pmatrix} -b & a \\ a & b \end{pmatrix} \middle| a, b, c \in \mathbb{Z}, c \neq 0, a^2 + b^2 = c^2 \right\}$$

can be found also in

$$S' := \left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \middle| \alpha \in [0, 2\pi) \right\rangle \cap \mathbb{Q}^{2\times 2}.$$

For every matrix of the first type

$$\frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix}$$

and corresponding a, b, c Pythagorean relation holds: $a^2 + b^2 = c^2$, therefore a and b are in absolute values smaller than or equal to $|c|$. It implies that $\left|\frac{a}{c}\right| \leq 1$ and $\left|\frac{b}{c}\right| \leq 1$. Since sine function maps its domain onto interval $[-1, 1]$, we can find such an angle α that $\sin(\alpha) = \frac{a}{c}$, which is a rational number. Again by Pythagorean relation $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$, we have

$$\sin(\alpha)^2 = \left(\frac{a}{c}\right)^2 = 1 - \left(\frac{b}{c}\right)^2 = 1 - \cos(\alpha)^2.$$

Therefore

$$\left(\frac{b}{c}\right)^2 = \cos(\alpha)^2.$$

Hence $\left(\frac{b}{c}\right) = \cos(\alpha)$ or $\left(\frac{b}{c}\right) = -\cos(\alpha)$. If the first case holds, matrix can be written using sine and cosine:

$$\frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix},$$

which consists of rational coefficients. If $\left(\frac{b}{c}\right) = -\cos(\alpha)$, we can use properties $\cos(\alpha) = \cos(\pi - \alpha)$ and $\sin(\alpha) = \sin(\pi - \alpha)$ and we can write

$$\frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix} = \begin{pmatrix} \cos(\alpha') & -\sin(\alpha') \\ \sin(\alpha') & \cos(\alpha') \end{pmatrix},$$

where

$$\alpha' = \begin{cases} \pi - \alpha & \text{if } \alpha \in [0, \pi] \\ \pi - \alpha + 2\pi & \text{if } \alpha \in (\pi, 2\pi). \end{cases}$$

So matrices of the first type are included in

$$\frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix} \in \left\langle \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \middle| \alpha \in [0, 2\pi) \right\rangle \cap \mathbb{Q}^{2\times 2}.$$

Now matrices of the second type:

$$\frac{1}{c}\begin{pmatrix} -b & a \\ a & b \end{pmatrix} = \frac{1}{c}\begin{pmatrix} -b & -a \\ -a & b \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

both matrices on the right-hand side are in S'. Their product is also a matrix with rational coefficients, thus also

$$\frac{1}{c}\begin{pmatrix} -b & a \\ a & b \end{pmatrix} \in S'.$$

We have proven two inclusions so the equality between the sets holds. □

3.3.3 Ideal lattices in particular lattice isomorphism classes

The current section is based on the paper [Ding and Lindner, 2007, Theorem 3]. We provide a generalisation, we extend it to composite integers. Originally, the theorem in [Ding and Lindner, 2007] was restricted to distinct primes.

Theorem 29. *Let* $z_1, z_2 \in \mathbb{Z} \setminus \{0, -1, 1\}$ *such that* $\gcd(z_1, z_2) = 1$. *Then lattice* L *with basis*

$$\mathbf{B}_L = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}$$

has no ideal sublattice of $\mathbb{Z}^2$ *in its isomorphism class.*

Proof. From Proposition 28 we know that

$$\mathrm{O}_2(\mathbb{Q}) = \left\{ \frac{1}{c}\begin{pmatrix} b & -a \\ a & b \end{pmatrix}, \frac{1}{c}\begin{pmatrix} -b & a \\ a & b \end{pmatrix} \middle| a, b, c \in \mathbb{Z}, c \neq 0, a^2 + b^2 = c^2 \right\}.$$

The isomorphism class of lattice L is determined by the basis of L, it is sufficient to consider matrices in the following forms:

$$\mathrm{O}_2(\mathbb{Q})\mathbf{B}_L = \left\{ \frac{1}{c}\begin{pmatrix} bz_1 & -az_2 \\ az_1 & bz_2 \end{pmatrix}, \frac{1}{c}\begin{pmatrix} -bz_1 & az_2 \\ az_1 & bz_2 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}, c \neq 0, a^2 + b^2 = c^2 \right\}.$$

Let us take an arbitrary matrix from $\mathrm{O}_2(\mathbb{Q})\mathbf{B}_L$ with corresponding a, b and c. Let us denote by $z = \gcd(a, b, c) \geq 1$. We can write:

$$a = z\widetilde{a},$$
$$b = z\widetilde{b},$$
$$c = z\widetilde{c},$$

where $\gcd(\widetilde{a},\widetilde{b},\widetilde{c}) = 1$. Since a, b, c are the Pythagorean triple, we can write:

$$\begin{aligned} a^2 + b^2 &= c^2, \\ z^2\widetilde{a}^2 + z^2\widetilde{b}^2 &= z^2\widetilde{c}^2, \\ \widetilde{a}^2 + \widetilde{b}^2 &= \widetilde{c}^2. \end{aligned}$$

We have equality $\widetilde{a}^2+\widetilde{b}^2 = \widetilde{c}^2$. Coprimality $\gcd(\widetilde{a},\widetilde{b},\widetilde{c}) = 1$ implies $\gcd(\widetilde{a},\widetilde{c}) = 1$. This is because of the following reasons (proof by contraposition): if $\gcd(\widetilde{a},\widetilde{c}) = z' > 1$, then $z' \mid \widetilde{c}^2 = \widetilde{a}^2 + \widetilde{b}^2$. A basic property of divisibility implies that if $z' \mid \widetilde{a}^2 + \widetilde{b}^2$ and simultaneously $z' \mid \widetilde{a}$, then also $\widetilde{b}$ is divisible by z'. Hence $\gcd(\widetilde{a},\widetilde{b},\widetilde{c}) \neq 1$.

Analogously we would get $\gcd(\widetilde{b},\widetilde{c}) = 1$.

Firstly, let us consider matrices of the first type:

$$\mathbf{B}_{L,1} = \frac{1}{c}\begin{pmatrix} bz_1 & -az_2 \\ az_1 & bz_2 \end{pmatrix}.$$

Since we are considering sublattices of $\mathbb{Z}^2$, this matrices (which span the corresponding lattices) shall have integer entries:

$$\frac{bz_1}{c} = \frac{z\widetilde{b}z_1}{z\widetilde{c}} = \frac{\widetilde{b}z_1}{\widetilde{c}} \in \mathbb{Z},$$

$$\frac{bz_2}{c} = \frac{z\widetilde{b}z_2}{z\widetilde{c}} = \frac{\widetilde{b}z_2}{\widetilde{c}} \in \mathbb{Z}.$$

We know that c cannot be equal to zero. Now we can analyse matrix entries.

If $\widetilde{b}$ is non-zero, $\widetilde{c}$ has to be equal to 1 or -1 to divide $\widetilde{b}z_1$ and $\widetilde{b}z_2$ at the same time because $\gcd(\widetilde{b},\widetilde{c}) = 1$ and z_1, z_2 have no common divisor greater than 1. If there was any prime divisor p of $\widetilde{c}$ and p divided $\widetilde{b}z_1$, then one of the following two cases should happen: p would divide $\widetilde{b}$ (which is not possible because $\gcd(\widetilde{b},\widetilde{c}) = 1$) or $p \mid z_1$ (this would be case). However, by the analogous thought p would divide z_2 as well. But z_1 and z_2 are coprime numbers thus such a prime divisor does not exist and $\widetilde{c} = 1$ or $\widetilde{c} = -1$.

If b is zero, we can use similar thoughts as before to analyse

$$\frac{az_1}{c} \text{ and } \frac{az_2}{c},$$

which leads to the same conclusion $\widetilde{c} = 1$ or $\widetilde{c} = -1$.

By using $\widetilde{a}^2 + \widetilde{b}^2 = \widetilde{c}^2$ and reasoning above we get only four distinct cases:

(1) $\frac{a}{c} = 1$ and $\frac{b}{c} = 0$,

(2) $\frac{a}{c} = -1$ and $\frac{b}{c} = 0$,

(3) $\frac{a}{c} = 0$ and $\frac{b}{c} = 1$,

(4) $\frac{a}{c} = 0$ and $\frac{b}{c} = -1$.

The first case $\frac{a}{c} = 1$ and $\frac{b}{c} = 0$. $\mathbf{B}_L^{(1)}$ is in the following form:

$$\mathbf{B}_{L,1}^{(1)} = \begin{pmatrix} 0 & -z_2 \\ z_1 & 0 \end{pmatrix}.$$

We will show (using Algorithm 1) that a lattice with the basis of this form is not ideal.

Firstly, we need to transform $\mathbf{B}_L^{(1)}$ into **HNF**. We use a unitary matrix $\mathbf{U}$ to get

$$\mathbf{B} := \mathbf{B}_{L,1}^{(1),\mathbf{HNF}} = \mathbf{B}_{L,1}^{(1)} \cdot \mathbf{U} = \begin{pmatrix} 0 & -z_2 \\ z_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} z_2 & 0 \\ 0 & z_1 \end{pmatrix}.$$

Without loss of generality we can assume that $z_1, z_2 > 0$. If z_1 or $z_2 < 0$, we would only change the corresponding signs in matrix $\mathbf{U}$ to get the positive numbers in matrix $\mathbf{B}$. (Analogous assumption we can do for all the other case.)

Let us denote by

$$\mathbf{A} := \mathrm{adj}(\mathbf{B}) = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}$$

and by $d = \det(\mathbf{B}) = z_1 z_2$.

According to the algorithm, we calculate product

$$\begin{aligned} \mathbf{P} &= \mathbf{AMB} \mod d \\ &= \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} z_2 & 0 \\ 0 & z_1 \end{pmatrix} \mod d \\ &= \begin{pmatrix} 0 & 0 \\ z_2 & 0 \end{pmatrix} \begin{pmatrix} z_2 & 0 \\ 0 & z_1 \end{pmatrix} \mod d \\ &= \begin{pmatrix} 0 & 0 \\ z_2^2 & 0 \end{pmatrix} \mod d. \end{aligned}$$

Since z_1 and z_2 are coprime numbers, moreover none of them is equal to one hence $d = z_1 z_2 \nmid z_2^2$. We see that the first column is non-zero modulo d which cannot occur when L is an ideal lattice according to step 5 in Algorithm 1. Therefore lattices with the basis of type $\mathbf{B}_L^{(1)}$ are not ideal.

If we now consider cases from (2) to (4) for a matrix of this type:

$$\mathbf{B}_{L,1} = \frac{1}{c} \begin{pmatrix} bz_1 & -az_2 \\ az_1 & bz_2 \end{pmatrix},$$

which are:

$$\mathbf{B}_{L,1}^{(2)} = \begin{pmatrix} 0 & z_2 \\ -z_1 & 0 \end{pmatrix}, \mathbf{B}_{L,1}^{(3)} = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}, \mathbf{B}_{L,1}^{(4)} = \begin{pmatrix} -z_1 & 0 \\ 0 & -z_2 \end{pmatrix},$$

we always finish the algorithm in step 5 by getting a matrix with the first column non-zero. For case (2) we get the same matrix $\mathbf{P}$ as for case (1):

$$\mathbf{P} = \begin{pmatrix} 0 & 0 \\ z_2^2 & 0 \end{pmatrix}$$

and for cases (3) and (4):

$$\mathbf{P} = \begin{pmatrix} 0 & 0 \\ z_1^2 & 0 \end{pmatrix},$$

which is again a matrix with the first column non-zero modulo d for the same reason as in case (1).

Now we consider the second type of a basis that lattices in this isomorphism class have:

$$\mathbf{B}_{L,2} = \frac{1}{c}\begin{pmatrix} -bz_1 & az_2 \\ az_1 & bz_2 \end{pmatrix}.$$

Again we have four cases (1), (2), (3) and (4) (exactly like for matrices of type $\mathbf{B}_{L,1}$ as mentioned above we get four possibilities for triples a, b, c). First case (1):

$$\mathbf{B}_{L,2}^{(1)} = \begin{pmatrix} 0 & z_2 \\ z_1 & 0 \end{pmatrix}.$$

Exactly as the case of $\mathbf{B}_{L,1}^{(1)}$, using Algorithm 1, we transform $\mathbf{B}_{L,2}^{(1)}$ into **HNF**, find the adjugate matrix and calculate

$$\mathbf{AMB} \mod d = \begin{pmatrix} 0 & 0 \\ z_2^2 & 0 \end{pmatrix}.$$

There are also other cases:

$$\mathbf{B}_{L,2}^{(2)} = \begin{pmatrix} 0 & -z_2 \\ -z_1 & 0 \end{pmatrix}, \mathbf{B}_{L,2}^{(3)} = \begin{pmatrix} -z_1 & 0 \\ 0 & z_2 \end{pmatrix}, \mathbf{B}_{L,2}^{(4)} = \begin{pmatrix} z_1 & 0 \\ 0 & -z_2 \end{pmatrix}.$$

Again, if we compute **HNF** for each of this matrices (without loss of generality $z_1, z_2 > 0$) and adjugate matrices, then we will get: For case (2) we get the same matrix $\mathbf{P}$ as for case (1)

$$\mathbf{P} = \begin{pmatrix} 0 & 0 \\ z_2^2 & 0 \end{pmatrix}$$

and for cases (3) and (4):

$$\mathbf{P} = \begin{pmatrix} 0 & 0 \\ z_1^2 & 0 \end{pmatrix}.$$

So the algorithm stops with the result that a lattice on input is not ideal. Therefore there is no ideal lattice consisting of integer coefficients in the isomorphism class given by L. □

Example. In Theorem 29 we have to take z_1 and z_2 different from 1 and -1. We could not say about the matrices of this type that in its isomorphism class there is no ideal lattice. For example the lattice with basis

$$\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}, \text{ where } k \in \mathbb{Z} \setminus \{0\}$$

is ideal itself.

4. NTRU lattices

NTRU lattices as well as ideal lattices are used in modern cryptography (see Chapter 5). As we will see, NTRU lattices are lattices with a special structure related to cyclic lattices. This chapter looks for solutions of the issues outlined in [Ding and Lindner, 2007] in section 2.7. The authors sketched that for NTRU lattices it is possible to prove a theorem similar to Theorem 19. While looking at it, we encountered certain obstacles, which we discuss in more detail in this chapter.

4.1 Notation

When talking about ideal lattices we still use notation from Section 2.2.1.

Throughout the whole chapter by matrix $\mathbf{Q}$ we mean the following:

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right).$$

Furthermore, let us introduce symbol $\circledast$ for the special type of multiplication applied on particular blocks (not usual matrix multiplication), which will be useful for the next section.

Definition 30 (Symbol $\circledast$)**.** *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be two matrices from* $\mathbb{Z}^{2n\times 2n}$*, for some* $n \in \mathbb{N}$*. Let us divide both matrices into four* $n \times n$ *blocks. By symbol* $\circledast$ *we mean multiplication on blocks individually.*

$$\mathbf{A} \circledast \mathbf{B} = \left(\begin{array}{c|c} \mathbf{A_1} & \mathbf{A_2} \\ \hline \mathbf{A_3} & \mathbf{A_4} \end{array}\right) \circledast \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{A_1B_1} & \mathbf{A_2B_2} \\ \hline \mathbf{A_3B_3} & \mathbf{A_4B_4} \end{array}\right).$$

4.2 Identifying NTRU lattices

Firstly, we need to define NTRU lattices. By an NTRU lattice many references mean the lattice with a basis of the following form:

Definition 31 (NTRU lattice)**.** *Let us consider vector* $\mathbf{h} = (h_0, h_1, \ldots h_{n-1})^\top \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$*,* $\lambda, \mu \in \mathbb{Z} \setminus \{0\}$ *and* $2n \times 2n$ *matrix with the following structure:*

$$\mathbf{N} = \left(\begin{array}{c|c} \lambda\mathbf{I_n} & \mathbf{H} \\ \hline \mathbf{0} & \mu\mathbf{I_n} \end{array}\right), \text{ where } \mathbf{H} = \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-1} \\ h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}.$$

The NTRU lattice *is a lattice with such a basis* $\mathbf{N}$*. Such a basis* $\mathbf{N}$ *is called an* NTRU-type basis.

Remark. In another references, the NTRU lattice is said to be a lattice with basis $\mathbf{N}$ with blocks transposed to the lower triangular form. This description is included in the original description established in [Coppersmith and Shamir, 1997].

Let us prove that this type of lattice for $\lambda, \mu \in \mathbb{Z} \setminus \{0, \pm 1\}$ is not ideal itself. We will use our Lemma 21.

Proposition 32. *Let us consider vector* $\mathbf{h} = (h_0, h_1, \dots h_{n-1})^\top \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $\lambda, \mu \in \mathbb{Z} \setminus \{0, \pm 1\}$ *and* $2n \times 2n$ *matrix with the following structure:*

$$\mathbf{N} = \left(\begin{array}{c|c} \lambda \mathbf{I_n} & \mathbf{H} \\ \hline \mathbf{0} & \mu \mathbf{I_n} \end{array}\right), \text{ where } \mathbf{H} = \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-1} \\ h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix}.$$

Then the lattice with basis $\mathbf{N}$ *is not an ideal lattice.*

Proof. We can use Lemma 21 with notation from Algorithm 1. If we show that the condition from Lemma 21 is not satisfied, the lattice with basis $\mathbf{N}$ will not be ideal.

Let us denote by $d = \det(\mathbf{N}) = \lambda^n \mu^n$ (because $\mathbf{N}$ is an upper triangular matrix, the determinant is a product of diagonal entries), by $\mathbf{A} = \mathrm{adj}(\mathbf{N})$ and let us calculate $\mathbf{AMN} \mod d$. Firstly,

$$\mathbf{A} = \mathrm{adj}(\mathbf{N}) = \left(\begin{array}{c|c} \mu \mathbf{I_n} & -\mathbf{H} \\ \hline \mathbf{0} & \lambda \mathbf{I_n} \end{array}\right) \text{ and } \mathbf{M} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 0 \\ \hline & & & 0 \\ & \mathbf{I_{2n-1}} & & \vdots \\ & & & 0 \end{array}\right).$$

Lemma 21 says that if $\mathbf{N}$ was a basis of an ideal lattice, each row in $\mathbf{AMN} \mod d$ would be an integer multiple of $\mathbf{N}_{2n,\cdot} \mod d$. Since $\mathbf{N}$ is an upper triangular matrix, the last row of $\mathbf{N} \mod d$ has zeros at every position except for entry $N_{n,n}$. We will show that there is a non-zero entry in the left lower block of matrix $\mathbf{AMN} \mod d$ which will imply that the lattice corresponding to $\mathbf{N}$ is not an ideal lattice (according to Algorithm 1).

Let us focus on position $(n+1, n)$ in matrix $\mathbf{AMN}$, the entry on this position comes from multiplication of $n+1$-th row in matrix $\mathbf{AM}$ by the n-th column of $\mathbf{N}$:

$$(\mathbf{AMN})_{(n+1,n)} = \sum_{k=1}^{2n} \left(\sum_{r=1}^{2n} A_{(n+1)r} M_{rk} \right) N_{kn}.$$

Regarding the structure of $\mathbf{M}$:

$$M_{ij} = \begin{cases} 1 & \text{if } i = j+1 \text{ for } j = 1, 2, \dots, 2n-1 \\ 0 & \text{in all other cases.} \end{cases}$$

All the zero terms disappear, thus we can rearrange the inner sum to get:

$$(\mathbf{AMN})_{(n+1)n} = \sum_{k=1}^{2n-1} A_{(n+1)(k+1)} M_{(k+1)k} N_{kn}.$$

In the $(n+1)-th$ row of $\mathbf{A}$, there is only one non-zero entry:

$$A_{(n+1)(k+1)} = \begin{cases} \lambda & \text{if } k = n \\ 0 & \text{if } k \neq n. \end{cases}$$

This means it is sufficient to compute only the remaining term (all other summands are equal to zero)

$$(\mathbf{AMN})_{(n+1)n} = A_{(n+1)(n+1)} M_{(n+1)n} N_{nn} = \lambda \cdot 1 \cdot \lambda = \lambda^2.$$

Thus we have obtained a non-zero value (λ^2 is not zero modulo $d = \lambda^n \mu^n$) for $|\lambda|$ different from zero and one. However, for ideal lattice there should be a zero entry according to Algorithm 1. Therefore, we have proven the claim. □

It follows from the previous proposition that Theorem 19 does not hold for an NTRU lattice. In the paper [Ding and Lindner, 2007] they formulate the following proposition for NTRU lattices:

Conjecture 33. *Let $\mathbf{B} \in 2n \times 2n$ be a basis. Then B is an NTRU-type basis if and only if there exists $\mathbf{T} \in \mathbb{Z}^{2n \times 2n}$ such that*

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right) \mathbf{B} = \mathbf{BT}.$$

Since NTRU lattices are not explicitly defined in [Ding and Lindner, 2007], we are using our Definition 31. The implication from the left to the right could be easily proved by setting

$$\mathbf{T} = \left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right).$$

But when we would like to prove the opposite implication, our definition would not fulfill the theorem: if we take for instance

$$\mathbf{B} = \left(\begin{array}{c|c} \lambda \mathbf{I_n} & \mathbf{0} \\ \hline \mathbf{0} & \mu \mathbf{I_n} \end{array}\right), \text{ where } \lambda, \mu \in \mathbb{Z} \setminus \{0, \pm 1\},$$

then the basis is not in the NTRU-type form (because of the upper zero block), but equality

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right) \mathbf{B} = \mathbf{BT}$$

is satisfied for

$$\mathbf{T} = \left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right).$$

There is also another example. If we consider

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix},$$

it is not an NTRU-type basis but we can see that equality

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right)\mathbf{B} = \mathbf{BT}$$

is satisfied for

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ -2 & 0 & -1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

It is interesting that this matrix $\mathbf{B}$ is equivalent to NTRU-type basis $\mathbf{N}$ such that $\mathbf{N} = \mathbf{BU}$, where

$$\mathbf{U} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & -1 \\ 0 & -2 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

These examples show that our definition of an NTRU lattice does not satisfy Conjecture 33. In [Ding and Lindner, 2007, Section 2.7] they describe NTRU lattices in few words. We will focus on this description in the next section.

4.3 NTRU lattices (IIL) and cyclic lattices

As mentioned above, NTRU lattices are not defined in [Ding and Lindner, 2007, Section 4.7]. There is only a description which says that an NTRU lattice is not ideal itself but its basis is composed of 4 subbases which are bases of ideal lattices with respect to the rotational polynomial $\mathbf{q}(x) = x^n - 1$. We will try to do a formalised definition based on this description. We will call this lattices NTRU lattices (IIL), where IIL stands for Identifying Ideal Lattices (the name of the paper).

Definition 34 (NTRU lattice (IIL))**.** *By* the NTRU lattice (IIL) *we mean a sublattice of* $\mathbb{Z}^{2n}$ *with a basis of the form*

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right),$$

where $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ *and* $\mathbf{B}_4$ *are* $n \times n$ *blocks such that each* $\mathbf{B}_i$ *for* $i \in \{1, 2, 3, 4\}$ *is an ideal lattice with respect to* $\mathbf{q}(x) = x^n - 1$*.*

Remark. This definition does not include NTRU lattices from our first Definition 31 because $\mathbf{B}_i$ is required to be a basis, thus zero block is not accepted as not having linearly independent columns.

As we will see in the example below, Conjecture 33 cannot be satisfied neither for the NTRU lattices (IIL).

Example. Let us consider a matrix

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right).$$

We can see that this matrix is an NTRU matrix (IIL) (Definition 34 by using Theorem 19 in the following way: To prove that $\mathbf{B}$ is an NTRU-type basis we need that for each block $\mathbf{B}_i$ there exists $\mathbf{T}_i$ such that equality

$$\mathbf{Q}\mathbf{B}_i = \mathbf{B}_i\mathbf{T}_i, \text{ where } \mathbf{Q} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is satisfied. This equality holds for the choice

$$\mathbf{T}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathbf{T}_2 = \mathbf{T}_3 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \mathbf{T}_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This matrix is not invertible over $\mathbb{Z}$ because $\det(\mathbf{B}) = 2$ but it is invertible over $\mathbb{R}$ and the inverse matrix is:

$$\mathbf{B}^{-1} = \left(\begin{array}{cc|cc} -1 & 0 & 0 & 1 \\ 0 & -1/2 & 1/2 & 1/2 \\ \hline 0 & 1/2 & 1/2 & -1/2 \\ 1 & 1/2 & -1/2 & -1/2 \end{array}\right).$$

Now we can leave $\mathbf{T}$ on the left-hand side using the inverse of $\mathbf{B}$:

$$\mathbf{B}^{-1}\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right)\mathbf{B} = \mathbf{T},$$

$$\mathbf{T} = \left(\begin{array}{cc|cc} -1 & 1 & 0 & -1 \\ 1/2 & 1/2 & 1/2 & 0 \\ \hline 1/2 & 1/2 & -1/2 & 1 \\ 1/2 & -1/2 & 1/2 & 1 \end{array}\right).$$

Since $\mathbf{B}$ is an invertible matrix, the equality has exactly one solution $\mathbf{T}$ which is not an integer matrix.

We have seen that Conjecture 33 is not satisfied neither for Definition 34. We formulate and prove the idea of the conjecture in a changed format where we use block multiplication on the right-hand side, introduced in Section 4.1.

Lemma 35 (Identifying NTRU lattices (IIL))**.** *Let $\mathbf{B} \in \mathbb{Z}^{2n\times 2n}$ be a basis of a lattice of dimension $2n$ and each block in*

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right)$$

be a basis of a lattice of dimension n.

Then $\mathbf{B}$ is a basis of the NTRU lattice (IIL) if and only if there exists $\mathbf{T} \in \mathbb{Z}^{2n\times 2n}$ such that the following equality holds:

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right)\left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) \circledast \mathbf{T}. \tag{4.1}$$

Proof. Firstly, we have a common multiplication on the left-hand side of equality (4.1):

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right)\left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{QB_1} & \mathbf{QB_2} \\ \hline \mathbf{QB_3} & \mathbf{QB_4} \end{array}\right).$$

We want to prove two implications to get the equivalence:

"⇒" We have: $L(\mathbf{B})$ is an NTRU lattice (IIL) and we want to find $\mathbf{T} \in \mathbb{Z}^{2n\times 2n}$ such that equality (4.1) holds. From the NTRU lattice (IIL) definition (Definition 34):

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right),$$

where $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ and $\mathbf{B}_4$ are $n \times n$ blocks such that each $\mathbf{B}_i$ for $i \in \{1, 2, 3, 4\}$ is a basis of the ideal lattice with respect to $\mathbf{q}(x) = x^n - 1$. Using Theorem 19 and the appended remark, we get for each block $\mathbf{B}_i$:

$$\mathbf{QB}_i = \mathbf{B}_i\mathbf{T}_i \text{ for some } \mathbf{T}_i \in \mathbb{Z}^{n\times n},$$

where

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right)$$

(the last column in $\mathbf{Q}$ corresponds with $\mathbf{q}(x) = x^n - 1$).

Thus if we set

$$\mathbf{T} = \left(\begin{array}{c|c} \mathbf{T_1} & \mathbf{T_2} \\ \hline \mathbf{T_3} & \mathbf{T_4} \end{array}\right),$$

we get exactly equality (4.1):

$$\left(\begin{array}{c|c} \mathbf{QB_1} & \mathbf{QB_2} \\ \hline \mathbf{QB_3} & \mathbf{QB_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) \circledast \mathbf{T}.$$

"⇐" Now we work on the assumption

$$\left(\begin{array}{c|c} \mathbf{Q} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Q} \end{array}\right)\left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) \circledast \mathbf{T}.$$

We can divide $\mathbf{T}$ into blocks as

$$\mathbf{T} = \left(\begin{array}{c|c} \mathbf{T_1} & \mathbf{T_2} \\ \hline \mathbf{T_3} & \mathbf{T_4} \end{array}\right).$$

Therefore, we have

$$\left(\begin{array}{c|c} \mathbf{QB_1} & \mathbf{QB_2} \\ \hline \mathbf{QB_3} & \mathbf{QB_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right) \circledast \left(\begin{array}{c|c} \mathbf{T_1} & \mathbf{T_2} \\ \hline \mathbf{T_3} & \mathbf{T_4} \end{array}\right),$$

which gives

$$\left(\begin{array}{c|c} \mathbf{QB_1} & \mathbf{QB_2} \\ \hline \mathbf{QB_3} & \mathbf{QB_4} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{B_1T_1} & \mathbf{B_2T_2} \\ \hline \mathbf{B_3T_3} & \mathbf{B_4T_4} \end{array}\right).$$

For each block $i \in \{1, 2, 3, 4\}$ we have found $\mathbf{q} = (1, 0, \ldots, 0)^\top$ and $\mathbf{T}_i \in \mathbb{Z}^{n\times n}$ such that

$$\mathbf{QB}_i = \mathbf{B}_i\mathbf{T}_i.$$

Hence by Theorem 19 we know that each $\mathbf{B}_i$ generates an ideal lattice with respect to $\mathbf{q}(x) = x^n - 1$. It is exactly the definition of an NTRU lattice (IIL). □

4.4 Generalised NTRU lattices

In the previous section, we have seen that the definition of an NTRU lattice (IIL) is not compatible with Definition 31 (see the remark after Definition 34). In our point of view it is interesting to consider the generalisation of this definition to the following one, which is inspired by the description of NTRU lattices in [Ding and Lindner, 2007, Section 2.7].

Definition 36 (Generalised NTRU lattice)**.** *By* the generalised NTRU lattice *we mean a sublattice of* $\mathbb{Z}^{2n}$ *with a basis of the form*

$$\mathbf{B} = \left(\begin{array}{c|c} \mathbf{B_1} & \mathbf{B_2} \\ \hline \mathbf{B_3} & \mathbf{B_4} \end{array}\right),$$

where $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3$ *and* $\mathbf{B}_4$ *are* $n \times n$ *blocks such that each* $\mathbf{B}_i$ *for* $i \in \{1, 2, 3, 4\}$ *satisfies the following:*

$$\text{There exists } \mathbf{T}_i \in \mathbb{Z}^{n \times n} \text{ such that } \mathbf{Q}\mathbf{B}_i = \mathbf{B}_i\mathbf{T}_i. \tag{4.2}$$

Such a basis $\mathbf{B}$ *is called a* (generalised) NTRU-type basis.

Remark. The description $\mathbf{B}_i$ being a basis of the ideal lattice with respect to $\mathbf{q}(x) = x^n - 1$ from Definition 34 is now replaced by existence of $\mathbf{T}_i$ such that $\mathbf{Q}\mathbf{B}_i = \mathbf{B}_i\mathbf{T}_i$. Therefore we allow some $\mathbf{B}_i$ to be a zero matrix, for example, NTRU lattices according to the original definition have basis in the upper triangular form. Thus, they also satisfy the definition of a generalised NTRU lattice.

Straightforwardly from the definition we get Lemma 35 also for the generalised NTRU lattices. Common multiplication is still not possible to achieve (see Example in Section 4.3.

5. Applications in Cryptography

Lattice-based cryptography is currently a frequently discussed topic in cryptography. Many lattice-based cryptographic constructions are rather efficient, typically quite simple to implement and they are believed to be secure against quantum computers. Quantum computers are a major threat to current widely used Public Key Cryptography based on mathematical problems such as the integer factorisation problem, the discrete logarithm problem and the elliptic-curve discrete logarithm problem. Cryptographic algorithms based on these assumptions can be efficiently broken using Shor's algorithm (see [Shor]).

Algorithms based on lattices create a large proportion of the candidates for post-quantum algorithms in the Post-Quantum Cryptography (PQC) Standardization process which is performed by American National Institute of Standards and Technologies (NIST). The Round 3 candidates were announced July 22, 2020. Lattice-based algorithms such as NTRU Cryptosystem, Crystals-Dilithium Signature Scheme and many others have become the third round finalists. The standardization influences also the European legislative because European standards stem from NIST's standards.

Another important application is the construction of hash functions derived from lattices. Their efficiency can be improved by replacing general lattices by lattices with the special structure. Here we get back to ideal and cyclic lattices which we were talking about in Chapters 2 and 3. We will provide one construction of this type in the following section as an example. Afterwards, we will briefly mention applications of NTRU lattices in Cryptography (for NTRU lattices, see Chapter 4).

After the brief Cryptographic Preliminaries section, we will get familiarised with the lattice problems which cryptographic constructions rely on. In the chapter we use information mainly from [Micciancio and Regev, 2008].

5.1 Cryptographic Preliminaries

We will use some of frequently used concepts in Cryptography. We will not work with formal definitions, for more precise formulations, see for example [Katz and Lindell, 2007]. By a *hash function* with fixed output of length n we mean a function H such that it takes as input a binary string of arbitrary length $x \in \{0,1\}^*$, and outputs a string $H(x) \in \{0,1\}^n$.

Informally, *one-way function* is a function that is easy to compute on every input, but hard to invert (given the image it is hard to find a preimage).

A hash function H is *collision-resistant* if it is hard to find two inputs a and b where $a \neq b$ but $H(a) = H(b)$.

5.2 Lattice problems

In this section, let us remind some concepts from the course of Computer Algebra.

For measuring the length of vectors in cryptography there is usually used Euclidean norm (but more generally, all the lattice problems can be defined with

respect to any norm).

Euclidean norm of a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)^\top \in \mathbb{R}^n$ is defined:

$$\|\boldsymbol{x}\|_2 := \sqrt{x_1^2 + \cdots + x_n^2}.$$

By the *shortest vector* in lattice L (denoted $\lambda(L)$) we mean

$$\lambda(L) = \min_{\mathbf{v} \in L \setminus \{\mathbf{0}\}} \|\mathbf{v}\|_2.$$

The *closest vector* to a given vector $\mathbf{w} \in \mathbb{R}^n$ (not necessarily in lattice L) is

$$\mathbf{c} = \min_{\mathbf{v} \in L} \|\mathbf{w} - \mathbf{v}\|_2 \in L.$$

These are some of the most known computational problems on lattices which we have chosen from [Micciancio and Regev, 2008, Section 2]:

- Shortest Vector Problem (SVP): Given a lattice basis $\mathbf{B}$. Find the shortest nonzero vector in $L(\mathbf{B})$.
- Closest Vector Problem (CVP): Given a lattice basis $\mathbf{B}$ and a target vector $\mathbf{w}$, find the lattice point $\mathbf{v} \in L(\mathbf{B})$ closest to $\mathbf{w}$.
- Shortest Independent Vectors Problem ($SIVP$): Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$. Find n linearly independent lattice vectors $\mathbf{s}_1, \ldots, \mathbf{s}_n$ (where $\mathbf{s}_i \in L(\mathbf{B})$ for $i = 1, 2, \ldots, n$) such that the value $\max_i ||\mathbf{s}_i||_2$ is minimal.

In Lattice-based cryptography, there are usually used approximation variants of these problems, denoted by an additional subscript. For instance, in SVP_γ (in other words also γ-approximate SVP) the problem is formulated: for given basis $\mathbf{B}$ find a vector $\mathbf{v} \in L(\mathbf{B})$ such that $\|\mathbf{v}\|_2 \leq \gamma\lambda(\mathbf{B})$.

The conjecture is that there is no polynomial-time algorithm that approximates lattice problems to within polynomial factors as for classical computers, so for quantum computers. Less formaly, it is believed that the approximation lattice problems are hard to solve within polynomial factors. The security of many lattice-based cryptographic constructions is based on this conjecture.

5.3 Efficient hash functions based on cyclic and ideal lattices

In this section we proceed from [Micciancio and Regev, 2008, Section 4] where they describe Ajtai's construction:

Algorithm 3: A hash function following Ajtai's construction

Parameters: $n, m, q, d \in \mathbb{N}$
Key: A matrix $\mathbf{A}$ chosen uniformly from $\mathbb{Z}_q^{n \times m}$
Hash function: $f_\mathbf{A} : \{0, 1, \ldots, d-1\}^m \Rightarrow \mathbb{Z}_q^n$ given by $f_\mathbf{A}(\mathbf{y}) = \mathbf{A}\mathbf{y} \mod q$.

Remark. A possible parameters choice is:

- $d = 2$,
- $q = n^2$,
- $m > n\frac{\log q}{\log d}$,

where the third item is obtained by taking bits into consideration. The function $f_{\mathbf{A}}$ maps $m \log d$ bits into $n \log q$ bits, hence to obtain a hash function that compresses the input we need to choose $m > n\frac{\log q}{\log d}$.

In the Ajtai's work, the security of a family of one-way functions constructed in such a way (later even proved a stronger property - collision resistance) is based on the worst-case hardness of n^c-approximate *SVP* for some constant $c > 0$. In other words he showed that being able to invert a function chosen from this family with non-negligible probability implies the ability to solve any instance of n^c-approximate *SVP*.

Lattice-based cryptographic functions and their efficiency can be often improved by replacing general matrices by a matrix with a special structure. For instance in Algorithm 3 there can be used

$$\mathbf{A} = (\mathbf{A}^{(1)} \mid \mathbf{A}^{(2)} \mid \dots \mathbf{A}^{(m/n)})$$

instead of a random matrix, such that each $\mathbf{A}^{(i)}$ is a circulant matrix (for the concept of circulant matrices see the example in Section 3.2.1). Thus each $\mathbf{A}^{(i)}$ has the form

$$\mathbf{A}^{(i)} = (\mathbf{a}^{(i)} | \mathbf{Q}\mathbf{a}^{(i)} | \dots | \mathbf{Q}^{n-1}\mathbf{a}^{(i)}),$$

where

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & 1 \\ \hline & & & 0 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & 0 \end{array}\right) \text{ and } \mathbf{a}^{(i)} \in \mathbb{Z}^n.$$

Or more generally we can replace matrix $\mathbf{A}$ in Algorithm 3 by

$$\mathbf{A} = (\mathbf{A}^{(1)} \mid \mathbf{A}^{(2)} \mid \dots \mathbf{A}^{(m/n)}) \text{ where } \mathbf{A}^{(i)} = (\mathbf{a}^{(i)} | \mathbf{Q}\mathbf{a}^{(i)} | \dots | \mathbf{Q}^{n-1}\mathbf{a}^{(i)})$$

for more general

$$\mathbf{Q} = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & -q_0 \\ \hline & & & -q_1 \\ & \mathbf{I}_{n-1} & & \vdots \\ & & & -q_{n-1} \end{array}\right) \text{ such that } (q_0, q_1, \dots q_{n-1})^\top, \mathbf{a}^{(i)} \in \mathbb{Z}^n.$$

We know that circulant $n \times n$ matrices having the columns linearly independent are a basis of the ideal lattice with respect to $\mathbf{q}(x) = x^n - 1$. Thus we get back to the cyclic lattices (see section 3.2.2). For more general $\mathbf{Q}$ invertible matrices of the form

$$(\mathbf{a}^{(i)} | \mathbf{Q}\mathbf{a}^{(i)} | \dots | \mathbf{Q}^{n-1}\mathbf{a}^{(i)})$$

are bases of the ideal lattices. For more details and other applications of ideal lattices see [Micciancio and Regev, 2008, Section 4].

5.4 NTRU cryptosystem

The concept of NTRU lattices (see Chapter 4, mainly Definition 31) is linked to creation of the NTRU cryptosystem [Hoffstein et al., 1998], which was originally introduced by its authors at CRYPTO'96. Since this cryptosystem is studied at the course of Algorithms on lattices, we are not going to describe it here. Operations work in ring $\mathbb{Z}[x]/(x^n - 1)$ where the addition of two polynomials is classical addition and the multiplication is supplemented by modulo $x^n - 1$.

The hardness assumption of the NTRU encryption scheme is related to the hardness of solving lattice problems over NTRU lattices of the form ($\lambda, \mu \in \mathbb{Z} \setminus \{0, \pm 1\}$)

$$\mathbf{N} = \left(\begin{array}{c|c} \lambda\mathbf{I_n} & \mathbf{H} \\ \hline \mathbf{0} & \mu\mathbf{I_n} \end{array}\right), \text{ where } \mathbf{H} = \begin{pmatrix} h_0 & h_1 & \cdots & h_{n-1} \\ h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 \end{pmatrix} \in \mathbb{Z}^{n \times n}.$$

These assumptions underlie also the NTRU-based fully-homomorphic encryption scheme [Lopez-Alt et al., 2013], the signature scheme BLISS [Ducas et al., 2013], and encryption over NTRU lattices [Ducas et al., 2014].

Conclusion

In the first chapter there are basic definitions and propositions included, with emphasis on lattices in general. In the second and the third chapter, we introduced the ideal lattices together with an algorithm for identifying ideal lattices from the paper [Ding and Lindner, 2007]. We have supplemented all the propositions by explanations of the steps which were omitted in the paper.

Our own propositions (Propositions 20 and 21) have been formulated and proved. Moreover, several examples have been added, for instance the example in Section 3.2.2 about the relation between circulant matrices and cyclic lattices. In addition, we have generalised Theorem 3 from the paper [Ding and Lindner, 2007], where we have replaced the assumption of two primes by two coprime numbers.

In Chapter 4, we have discussed the possible generalisation of the original definition of the NTRU lattice. We have managed to create a similar theorem to that which the algorithm for identifying ideal lattices was based on. The chapter is enriched with illustrative examples.

In the last chapter, we include a brief overview of the lattice problems on which the hardness of many cryptographic algorithms is based. As an example, we have provided the construction of a hash function whose efficiency has been improved using ideal or cyclic lattices. This part of the fifth chapter is based on [Micciancio and Regev, 2008]. We have also provided a brief overview of cryptographic references where NTRU lattices are used.

There are a few possible extensions of this work. In the chapters about ideal lattices, it would be useful to think about the relation between cyclic lattices and the basis structure (we have seen in the example in Section 3.2.2) that not every cyclic lattice has a basis of the form $(\mathbf{a} \mid \mathbf{Qa} \mid \ldots \mid \mathbf{Q}^{n-1}\mathbf{a})$. It could be interesting to describe in more detail for which cyclic lattices the basis of this form exists, to examine the structure of the basis of the other cyclic lattices and, finally, to extend this classification to ideal lattices in general.

It could be also an interesting question for the future research to classify all of the $\mathbf{Q}$, for which $\mathbf{QB} = \mathbf{BT}$ for some $\mathbf{T} \in \mathbb{Z}^{n\times n}$ for a fixed basis $\mathbf{B}$ of an ideal lattice (see equality (2.3) in Theorem 19).

In Chapter 4 about the NTRU lattices, there would be scope for attempting to construct an algorithm to identify NTRU lattices, similar to Algorithm 1.

The chapter on cryptographic applications could be extended providing more detailed descriptions of particular algorithms. It might also be interesting to consider in which cryptographic functions a general lattice could be replaced by a structured lattice.

Bibliography

L. Barto and J. Tůma. Lineární algebra. URL https://kam.mff.cuni.cz/~mikina/materialy/skripta_la5.pdf.

H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013. ISBN 9783662029459. URL https://books.google.cz/books?id=5TP6CAAAQBAJ.

D. Coppersmith and A. Shamir. Lattice attacks on ntru. 1997. URL https://link.springer.com/content/pdf/10.1007/3-540-69053-0_5.pdf.

J. Ding and R. Lindner. Identifying ideal lattices. 2007. URL https://eprint.iacr.org/2007/322.pdf.

L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. Lattice signatures and bimodal gaussians. Cryptology ePrint Archive, Report 2013/383, 2013. https://eprint.iacr.org/2013/383.

L. Ducas, V. Lyubashevsky, and T. Prest. Efficient identity-based encryption over ntru lattices. 2014. ISBN 978-3-662-45607-1. doi: 10.1007/978-3-662-45608-8_2.

J. Hoffstein, J. Pipher, and J. H. Silverman. Ntru: A ring-based public key cryptosystem. 1998. URL https://www.ntru.org/f/hps98.pdf.

R. A. Horn and C. R. Johnson. *Matrix analysis*. Second edition. Cambridge University Press, 2013. ISBN 978-0-521-54823-6.

J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007. ISBN 978-1-58488-551-1.

A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan. On-the fly multiparty computation on the cloud via multikey fully homomorphic encryption. 2013. URL https://eprint.iacr.org/2013/094.pdf.

D. Micciancio. 1: Introduction to lattices. 2012. URL https://cseweb.ucsd.edu/classes/wi12/cse206A-a/lec1.pdf.

D. Micciancio and V. Lyubashevsky. Generalized compact knapsacks are collision resistant. 2005. URL https://eccc.weizmann.ac.il/report/2005/142.

D. Micciancio and O. Regev. Lattice-based cryptography. 2008. URL https://cims.nyu.edu/~regev/papers/pqc.pdf.

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. URL https://arxiv.org/pdf/quant-ph/9508027.pdf.

D. Stanovský. Učební text algebra 2020/2021. URL https://www2.karlin.mff.cuni.cz/~kala/2021alg/algebra21.pdf.