Identifying Ideal Lattices

Jintai Ding[1] and Richard Lindner[2]

[1] University of Cincinnati, Department of Mathematical Sciences
PO Box 210025, Cincinnati, OH 45221-0025, USA
jintai.ding@uc.edu

[2] Technische Universität Darmstadt, Department of Computer Science
Hochschulstraße 10, 64289 Darmstadt, Germany
rlindner@cdc.informatik.tu-darmstadt.de

Abstract. Micciancio defined a generalization of cyclic lattices, called ideal lattices. These lattices can be used in cryptosystems to decrease the number of parameters necessary to describe a lattice by a square root, making them more efficient. He proves that the computational intractability of classic lattice problems for these lattices gives rise to provably secure one-way and collision-resistant hash functions. This provable security relies on the assumption that reducing bases of ideal lattices is similar to reducing bases of random lattices. We give an indication that lattice problems in ideal lattices do not represent the general case by providing a distinguisher, which decides in time $\mathcal{O}(n^4)$ whether a given basis of rank n spans an ideal lattice or not. Using this algorithm we perform a statistical analysis for several dimensions and show that randomly generated lattices are practically never ideal.

Keywords: decision problems, lattices, complexity, NTRU.

1 Introduction

Integer lattices are an important part of modern cryptological research (for example [6,5,4,7]). In order to deploy lattices in cryptographic systems, the number of parameters used to describe the lattice should be as small as possible. The most common way to realize this is to use ideal lattices. Ideal lattices are a new concept, first mentioned by Micciancio [3], but similar lattice classes have been used for a long time. For example cyclic lattices, a special case of ideal lattices, are used in NTRUEncrpyt and NTRUSign [2,1].

The concept of ideal lattices is new and no fundamental study has been made so far. It is unknown how many ideal lattices there are amongst all lattices. And more importantly, it is unclear if there are any computational problems which are known to be hard for random lattices and are still hard for random ideal lattices. Micciancio shows that, should the problem of finding short vectors in ideal lattices be as hard as the general case, then a certain class of hash functions is provably one-way and collision-resistant.

Here we give evidence that distinguishing ideal lattices from general ones can be done in polynomial time and show that in practice randomly chosen lattices are never ideal. These results give more insight into the structure of ideal lattices and their usefulness for cryptographic protocols.

1.1 Roadmap

We first explain how ideal lattices are related to general ones. In section 2, we present an efficient algorithm to decide whether or not a given lattice basis spans an ideal lattice or not. In section 3 we make the decision problem more complex by distinguishing between lattices whose isomorphism class contains an ideal lattice and lattices who are not isomorphic to an ideal lattice. Here we show that for dimension 2 there are infinitely many lattices whose isomorphism class does not contain an ideal lattice. Finally in section 4 we give the results from a statistical experiment to determine how big the percentage of ideal lattices is among general ones in some fixed dimensions.

1.2 Notation

A boldface letter $\mathbf{v}$ represents a vector in column format. The i-th element of a columnvector $\mathbf{v}$ is denoted $\mathbf{v}_i$.

The n-dimensional identity matrix is denoted I_n. For a given matrix M, the element in column i and row j is $M_{(i,j)}$, whereas $M_{(i,\cdot)}$ refers to the i-th column and analogously $M_{(\cdot,j)}$ denotes the j-th row of M.

We denote the ring of matrices with n columns, m rows, and elements from a given ground ring R simply as $R^{(n,m)}$.

When we say a lattice L is spanned by a basis B, where B is an $n \times m$-matrix, we mean that L is the $\mathbb{Z}$-span of the vectors $B_{(i,\cdot)}$, for $i = 1, \dots, m$. Many integer bases span the same lattice, however for full-rank lattices there is always a unique basis in Hermite Normal Form. This form can efficiently be calculated from any other basis by using Euclids Algorithm on each row (see section 2.5, [9]).

Definition 1 (HNF). *An invertible matrix $H \in \mathbb{Z}^{(n,n)}$ is in* Hermite Normal Form *if and only if*

i. H is upper triangular,
ii. the diagonal entries are positive,
iii. the off diagonal entries are non-negative and smaller than the diagonal entry in their row.

We denote the n-dimensional general linear group of all invertible matricies over a ring R as $\mathrm{GL}_n(R)$. The n-dimensional orthogonal group of length preserving transformations is $\mathrm{O}_n(R)$, and the special orthogonal group, where all transformations have determinant 1 is $\mathrm{SO}_n(R)$. Their general relationship is

$$\mathrm{SO}_n(R) \lhd \mathrm{O}_n(R) < \mathrm{GL}_n(R),$$

where $\lhd$ stands for normal subgroup and $<$ for subgroup.

2 Identifying ideal lattices

2.1 Ideal lattices

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

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

And let the ring of all integer polynomials modulo q be

$$R_q := \mathbb{Z}[X]/q(X)\mathbb{Z}[X].$$

As a $\mathbb{Z}$-module, R_q is isomorphic to $\mathbb{Z}^n$ regardless of the choice of q. The isomorphism is given by Φ_q

$$\begin{array}{rcl} \Phi_q \ : & \mathbb{Z}^n & \longrightarrow \qquad R_q \\ : & (v_0, \ldots, v_{n-1}) & \longmapsto v_0 + v_1X + \cdots + v_{n-1}X^{n-1} + q(X)\mathbb{Z}[X]. \end{array}$$

This means we have many different ring-multiplications on $\mathbb{Z}^n$, depending on which polynomial q we pick in this isomorphism.

Definition 2 (Ideal lattice). *Let L be a sublattice of $\mathbb{Z}^n$. If there exists a monic polynomial $q \in \mathbb{Z}[X]$ of degree n, such that $\Phi_q(L)$ is an ideal in R_q, we call L an ideal lattice.*

To be more explicit we can say a lattice L is ideal with respect to a vector $\mathbf{q}$*, this means for the polynomial $q(X) = \sum_{i=1}^{n} \mathbf{q}_i X^{i-1} + X^n$ the image $\Phi_q(L)$ is an ideal in R_q.*

Conversely if I is an ideal in R_q, then the inverse images $\Phi_q^{-1}(I)$ is always an ideal sublattice of $\mathbb{Z}^n$. A lattice which is ideal with respect to the rotation polynomial $q(X) = X^n - 1$ is called cyclic.

2.2 Identification

When we are given a basis B for a sublattice of $\mathbb{Z}^n$, and we want to know whether it spans an ideal lattice with respect to some polynomial q or not.

Lemma 1. *Let $B \in \mathbb{Z}^{(m,n)}$ be a basis of the lattice L. Then L is ideal if and only if there exists an integral transformation $T \in \mathbb{Z}^{(m,m)}$ and a tuple $(q_0, \ldots, q_{n-1}) \in \mathbb{Z}^n$ such that*

$$\underbrace{\begin{pmatrix} 0 \cdots 0 & -q_0 \\ & -q_1 \\ I_{n-1} & \vdots \\ & -q_{n-1} \end{pmatrix}}_{=:Q} B = BT.$$

Proof. Before we start with the actual proof, we use the isomorphism Φ_q to transfer the multiplication with X in R_q to a mapping on $\mathbb{Z}^n$. This mapping will be linear, because for any $v, w \in \mathbb{Z}^n$

$$\Phi_q^{-1}(\Phi_q(v+w)X) = \Phi_q^{-1}(\Phi_q(v)X) + \Phi_q^{-1}(\Phi_q(w)X).$$

So the mapping can be written as a matrix, which we define to be Q

The lattice L is ideal, if $I := \Phi_q(L)$ is an ideal in R_q with respect to some monic polynomial q of degree n. Since L is a lattice, I will be an ideal exactly if it is closed under multiplications by X in R_q. This in turn is equivalent to $L = \mathrm{span}(B)$ being closed under the mapping Q we defined above. Which is the same as saying there exists a transformation $T \in \mathbb{Z}^{(m,m)}$ such that $QB = BT$. $\square$

Note that using lemma 1 we can decide whether a lattice L is ideal or not, regardless of the basis we use to describe L. Also the polynomial q, and the associated factor ring R_q, in which the image of a given lattice is an ideal, need not be unique. For example if we pick an arbitrary monic polynomial q then the image under Φ_q of the lattice $\mathbb{Z}^n$ will always be the whole ring R_q, which is of course an ideal in its self. So this lattice is ideal with respect to all choices of q. In terms of our equation $QB = BT$, this means that no matter how we fill the rightmost column of the matrix Q, we can always find a integer transformation T that will make the equation hold.

2.3 Algorithm

For the algorithm, we will only consider the case where L has full rank, i.e. the basis consists of n linear independent vectors. This is not a fundamental restriction, because Lyubashevsky and Micciancio have shown that if a lattice is ideal with respect to an irreducible monic polynomial, then it has full rank [3, Lemma 3.2].

For the description of the algorithm, we will use the following matrix M and function F:

$$M := \begin{pmatrix} 0 \cdots & 0 \\ & \vdots \\ I_{n-1} & \\ & 0 \end{pmatrix}, \qquad \begin{aligned} F \ &: \mathbb{Z}^n \longrightarrow \mathbb{Z}^{(n,n)} \\ &: \mathbf{v} \longmapsto \begin{pmatrix} \mathbf{0} \cdots \mathbf{0}\ \mathbf{v} \end{pmatrix}. \end{aligned}$$

We will use this to rewrite the matrix $Q = M - F(\mathbf{q})$.

Algorithm 1: Identifying ideal lattices with full rank bases

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

1 Transform B into HNF
2 Calculate $A = \text{adj}(B)$, $d = \det(B)$, and $z = B_{(n,n)}$
3 Calculate the product $P = AMB \bmod d$
4 **if** *only the last column of* P *is non-zero* **then**
5 | set $\mathbf{c} = P_{(\cdot,n)}$ to equal this column
6 **else return false**
7 **if** $z \mid \mathbf{c}_i$ *for* $i = 1, \ldots, n$ **then**
8 | use CRT to find $\mathbf{q}^* \equiv \mathbf{c}/z \bmod d/z$ and $\mathbf{q}^* \equiv \mathbf{0} \bmod z$
9 **else return false**
10 **if** $B\mathbf{q}^* \equiv \mathbf{0} \pmod{d/z}$ **then**
11 | **return true**, $\mathbf{q} = B\mathbf{q}^*/d$
12 **else return false**

For an efficient way to transform B into Hermite Normal Form, we refer to [9].

Using the upper triangular form of B, it is easy to calculate $\det(B) = \prod_{i=1}^{n} B_{(i,i)}$. We may also calculate the characteristic polynomial of B, which is $p(X) = \prod_{i=1}^{n}(X - B_{(i,i)})$. Since the determinant is the constant term of this polynomial, we may define another polynomial $q(X) = (\det(B) - p(X))/X$. Since p annihilates B, the adjugate of B is given by this polynomial q evaluated at B.

2.4 Correctness

Theorem 1. *Algorithm 1 is correct.*

Proof. We show the correctness of the algorithm by showing that whenever the algorithm terminates the result is correct. We will rely heavily on lemma 1, which is an equivalent formulation of L being ideal in terms of a basis B. It states that if there are $\mathbf{q} \in \mathbb{Z}^n, T \in \mathbb{Z}^{(n,n)}$ such that

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

then the lattice L spanned by B is ideal. In the case of full-rank B, this is equivalent to demanding the existence of $\mathbf{q} \in \mathbb{Z}^n$ such that

$$AMB \equiv AF(\mathbf{q})B \pmod{d}.$$

The second statement is easier to check since we do not have to look for the transformation matrix T. Indeed using the upper triangular form of B and that $z = B_{(n,n)}$ this statement simplifies to:

$$AMB \equiv zF(A\mathbf{q}) \pmod{d}. \tag{1}$$

If the algorithm terminates with false in line **6**, then equation (1) cannot be satisfied, because P is the LHS of this equation and should have the same form as the RHS, i.e. a matrix with only one non-zero vector.

For the same reason any element of the non-zero vector, called $\mathbf{c}$ needs to be divisible by z, because the RHS shows a scalar z times the a vector $A\mathbf{q}$ in the last column. Here we use the fact that z is a factor in d, otherwise we might not find this factor modulo d. If this condition is not satisfied the algorithm terminates with false in line **9**.

To show that our final termination with false is correct, consider the case that $B\mathbf{q}^* \not\equiv \mathbf{0} \bmod d/z$. Since we chose $\mathbf{q}^*$ to be congruent to 0 modulo z, this implies

$$B\mathbf{q}^* \not\equiv \mathbf{0} \bmod d. \tag{2}$$

Again by equation (1) we know that $\mathbf{q}^*$ should be congruent to $A\mathbf{q}$ for which equation (2) cannot hold.

It remains to show that the termination in line **11** that returns true and a vector $\mathbf{q}$ does indeed imply that equation (1) holds, which is equivalent to B spanning an ideal lattice.

$$\begin{aligned} P &\equiv F(\mathbf{c}) \pmod{d} && \text{by line } \mathbf{5} \\ &\equiv F(z\mathbf{q}^*) \pmod{d} && \text{by line } \mathbf{8} \\ &\equiv zF(A\frac{B\mathbf{q}^*}{d}) \pmod{d}. \end{aligned}$$

Which by our definition of $\mathbf{q}$ in line **11** is equation (1). □

2.5 Complexity

The complexity is governed by the calculation of the Hermite Normal Form of the full-rank input basis B. The complexity of this is given by Storjohann [9].

Theorem 2. *Given a full-rank matrix $B \in \mathbb{Z}^{(n,m)}$ with $n \leq m$, we can calculate its HNF in time $\mathcal{O}(n^3mb^2)$, where b is a bound for the entries of B.*

We will use this theorem together with the assumption that $m = \mathcal{O}(n)$ and $b = \mathcal{O}(1)$, so the number of columns is linear in the number of rows and the matrix entries do not depend on the dimension. Under these assumptions our algorithm has a running time in $\mathcal{O}(n^4)$, provided we can show that no other step in the algorithm is asymptotically slower. The only other step that could contribute to the runtime is the calculation of the adjugate matrix A. We have seen in section 2.3 that this can be realised by evaluating a polynomial of degree $n-1$ at B, so we need to take powers of B up to $n-1$. Using normal arithmetic this takes $\mathcal{O}(n^4)$ operations, so we do not increase the runtime.

2.6 Examples

Using our algorithm, we can see that many lattices are not ideal lattices. For example let $n = 2$ and $k \in \mathbb{Z} \setminus \{0, \pm 1\}$, then

$$B_1 = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \text{ is ideal, but} \qquad B_2 = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} \text{ is not.}$$

Indeed B_2 with $k = 2$ is an example given by Lyubashevsky and Micciancio in [3]. We will use this example to perform the algorithm on it and refer to the basis as B. Matrix B is already in HNF so this step is not needed. The determinant is $d = 2$ and the adjugate matrix and the product $P = AMB \bmod d$ are

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad\qquad P = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

At this point we can stop, because all but the last column of P have to be zero if B would span an ideal lattice.

Note that you can always create examples of higher dimensions in the following fashion.

Lemma 2. *Let $B \in \mathbb{Z}^{(n,n)}$ be a basis in HNF form of a full-rank ideal lattice with respect to $\mathbf{q}$, then for any k that is a multiple of the first diagonal entry*

$$B' = \begin{pmatrix} k & 0 \cdots & \\ 0 & & \\ \vdots & & B \end{pmatrix}$$

spans an ideal lattice of dimension $n+1$ with respect to $\mathbf{q}' = (0, \mathbf{q})^T$.

Proof. We use lemma 1, so we must show that if there exists a $T \in \mathbb{Z}^{(n,n)}$ such that

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

then we can find a $T' \in \mathbb{Z}^{(n+1,n+1)}$ such that

$$\begin{pmatrix} 0 \cdots & 0 \\ & \vdots \\ I_n & 0 \end{pmatrix} B' - \begin{pmatrix} \cdots & \mathbf{0} & \mathbf{q}' \end{pmatrix} B' = B'T'. \tag{3}$$

We reformulate the LHS in order to find T'.

$$\begin{pmatrix} 0 & \cdots \cdots & 0 \\ k & & \\ 0 & MB & \\ \vdots & & \end{pmatrix} - \begin{pmatrix} 0 & \cdots \cdots & 0 \\ 0 & & \\ 0 & F(\mathbf{q})B & \\ \vdots & & \end{pmatrix} = B'T' \quad \text{so for} \quad T' = \begin{pmatrix} 0 & \cdots \cdots & 0 \\ l & & \\ 0 & T & \\ \vdots & & \end{pmatrix}$$

with $l = k/B_{(1,1)}$ the matrix T' is integral and equation (3) holds. $\square$

We will make the conditions of the general 2-dimensional case explicit. Every sublattice L of $\mathbb{Z}^2$ has a basis of the form

$$B = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \qquad A = \operatorname{adj}(B) = \begin{pmatrix} b & -c \\ 0 & a \end{pmatrix}, \qquad d = \det(B) = ab.$$

Where $a, b, c \in \mathbb{Z}$. We know L is ideal if and only if the following congruence holds.

$$AMB \equiv A\mathbf{q}B_{(n,\cdot)} \pmod{d}$$
$$\begin{pmatrix} -ac & -c^2 \\ a^2 & ac \end{pmatrix} \equiv \begin{pmatrix} 0 & bq_0 - cq_1 \\ 0 & aq_1 \end{pmatrix} \pmod{ab}$$

This gives us the following set of conditions on a, b, c:

i. $a \mid b$ and $b \mid c$,
ii. $b \mid c - q_1$,
iii. $a \mid ck - q_0$, where $k = (c - q_1)/b$.

2.7 NTRU lattices

The NTRU lattice, which was discovered by Coppersmith an Shamir is not its self an ideal lattice, but its basis is composed of 4 subbases which are bases of ideal lattices with respect to the rotational polynomial $q(X) = X^N - 1$. Here N is the dimension of the subbases and half the dimension of the NTRU lattice. The matrix Q corresponding to this polynomial is the rotational matrix

$$Q = \begin{pmatrix} \cdots & 0 & 1 \\ & & 0 \\ I_{N-1} & & \vdots \end{pmatrix}$$

It can be shown analogously to lemma 1, that NTRU lattices are easily distinguishable from random lattices because of their structure. Given a basis B of even dimension $2N$, it is an NTRU-type basis if and only if a transformation $T \in \mathbb{Z}^{(2N,2N)}$ exists such that

$$\begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix} B = BT.$$

3 Extending the identification to isomorphism classes

We have seen at the end of the last section, that being an ideal lattice is a property which is not retained under certain permutations. Indeed we may surmise, that the ring structure, which ideal lattices have, is not retained under lattice isomorphisms in general. Because lattice isomorphisms just keep the group and not the ring structure.

3.1 Preliminaries

Definition 3 (Lattice isomorphism). *Let L, M be sublattices of $\mathbb{R}^n$. We say that L is isomorphic to M, if and only if there exists an orthogonal transformation $T \in \mathrm{O}_n(\mathbb{R})$, such that $M = TL$.*

Remark 1. Notice, that if L is not of full rank, say $\mathrm{rank}(L) = k < n$, then we only need to preserve the length of the vectors in L, so forcing that T must be orthognal on the whole space might seem too much. However if T is orthogonal on L, it can be expanded to an orthogonal transformation on $\mathbb{R}^n$, by using the identity on $L^\perp$.

Definition 4 (Lattice isomorphism class). *The isomorphism class of a given lattice L is the orbit of this lattice under arbitrary lattice isomorphisms*

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

Lemma 3. *Let L, M be sublattices of $\mathbb{Q}^n$. If L has full rank and is isomorphic to M, then the isomorphism is in $\mathrm{O}_n(\mathbb{Q})$.*

Proof. Since L is a sublattice of $\mathbb{Q}^n$ and has full rank, L has a basis $B_L \in \mathbb{Q}^{(n,n)}$. We know L is isomorphic to M, so the transformation $T \in \mathrm{O}_n(\mathbb{R})$ maps B_L into $M \subseteq \mathbb{Q}^n$. So $C := B_L T \in \mathbb{Q}^{(n,n)}$ is rational. But this means T must be rational as well, because B_L is invertible.

$$T = CB_L^{-1} \in \mathrm{O}_n(\mathbb{Q})$$

□

The following example shows that two sublattices of $\mathbb{Z}^n$ can be isomorphic with a proper rational transformation.

Example 1. The two lattices L and M are isomorphic with $T \notin \mathrm{O}_n(\mathbb{Z})$.

$$B_L = \begin{pmatrix} 5 & 0 \\ 0 & 10 \end{pmatrix}, \qquad B_M = \begin{pmatrix} 3 & 8 \\ 4 & 6 \end{pmatrix}, \qquad T = \frac{1}{5}\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}$$

Since we only concern ourselves with sublattices of $\mathbb{Z}^n$, it suffices to study the group $\mathrm{O}_n(\mathbb{Q})$, when we want to find the isomorphim class of a given lattice.

3.2 Orthogonal groups

The orthogonal group over the integers $\mathrm{O}_n(\mathbb{Z})$ contains only permutations of the identity matrix with possible sign changes in every column.

$$\mathrm{O}_n(\mathbb{Z}) = \left\{ \left(\pm\mathbf{e}_{(\cdot,\sigma(1))} \;\cdots\; \pm\mathbf{e}_{(\cdot,\sigma(n))} \right) \;\middle|\; \sigma \in S_n \right\}$$

Here $\mathbf{e}_{(\cdot,i)}$ is the i-th column of the identity matrix. And S_n is the group of all permutations on $\{1, \ldots, n\}$.

For the more general group $\mathrm{O}_n(\mathbb{Q})$, there is another classification.

$$\mathrm{O}_n(\mathbb{Q}) = \left\{ \prod_{i=1}^{n} \left(I - 2u_i u_i^T \right) \;\middle|\; u_1, \ldots, u_n \in \mathbb{Q}^n \right\}.$$

So every orthogonal matrix is the product of n Householder matrices [10].

3.3 Special case $n = 2$

If we fix the dimension to be $n = 2$, then we can make the corresponding even more specific: Every $T \in \mathrm{O}_2(\mathbb{Q})$ corresponds to a possbile reflection and a rotation around the origin by some angle α. So

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

We use p_1, p_2, q_1, q_2 to identify $p_1/q_1 = \sin(\alpha)$ and $p_2/q_2 = \cos(\alpha)$. Since $\sin^2(\alpha) + \cos^2(\alpha) = 1$ we get that $(p_1q_2)^2 + (p_2q_1)^2 = (q_1q_2)^2$, so these three $a = (p_1q_2), b = (p_2q_1), c = (q_1q_2)$ must be a pythagorean triple. This tells us

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

3.4 Extending the identification

By putting together what we found in the previous sections, we show that already in dimension 2 there are infinitely many sublattices of $\mathbb{Z}^n$, whose isomorphism classes do not contain any ideal sublattices of $\mathbb{Z}^n$.

Theorem 3. *Let p_1, p_2 be different prime numbers, then the lattice spanned by*

$$B_L = \begin{pmatrix} p_1 & 0 \\ 0 & p_2 \end{pmatrix}$$

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

Proof.

$$\mathrm{O}_2(\mathbb{Q})B_L = \\ \left\{ \frac{1}{c} \begin{pmatrix} bp_1 & -ap_2 \\ ap_1 & bp_2 \end{pmatrix}, \frac{1}{c} \begin{pmatrix} -bp_1 & ap_2 \\ ap_1 & bp_2 \end{pmatrix} \mid a, b, c \in \mathbb{Z},\ a^2 + b^2 = c^2 \right\}.$$

Without loss of generality we may consider a, b, c to be given in a reduced form, such that $\gcd(a, b, c) = 1$. Because the Pythagorean equation has to hold $a^2 + b^2 = c^2$ this implies that $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

Let us first consider the matricies of the first type.

$$B_{L,1} = \frac{1}{c} \begin{pmatrix} bp_1 & -ap_2 \\ ap_1 & bp_2 \end{pmatrix}.$$

This basis has to be integral, so $bp_1/c, bp_2/c$ have to be integers. Since b and c are coprime we now know $c = \pm 1$. Again by the Pythagorean equation this means that either $a = \pm 1$ and $b = 0$, or the other way round $a = 0$ and $b = \pm 1$. There are four distinct cases $i., \ldots, iv.$ which we have to look at:

i. $a/c = 1, b/c = 0$	ii. $a/c = -1, b/c = 0$
iii. $a/c = 0, b/c = 1$	iv. $a/c = 0, b/c = -1$

Since all these cases work analogously we will show only the first.

Let us assume $a/c = 1, b/c = 0$ this leads to

$$B_{L,1} = \begin{pmatrix} 0 & -p_2 \\ p_1 & 0 \end{pmatrix} \qquad \mathrm{adj}(B_{L,1}) = \begin{pmatrix} 0 & -p_2 \\ p_1 & 0 \end{pmatrix}$$

We see that the first basis row of

$$\begin{pmatrix} 0 & -p_2 \\ p_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & -p_2 \end{pmatrix} = \begin{pmatrix} 0 & p_2^2 \\ 0 & 0 \end{pmatrix}$$

is not a multiple of the last basis row $\begin{pmatrix} p_1 & 0 \end{pmatrix}$, so the resulting lattices can never be ideal ones.

For the second type isomorphic lattices we will also do the first case.

$$B_{L,2} = \frac{1}{c} \begin{pmatrix} -bp_1 & ap_2 \\ ap_1 & bp_2 \end{pmatrix} = \begin{pmatrix} 0 & p_2 \\ p_1 & 0 \end{pmatrix} \qquad \mathrm{adj}(B_{L,2}) = \begin{pmatrix} 0 & p_2 \\ p_1 & 0 \end{pmatrix}.$$

Once again the first row of

$$\begin{pmatrix} 0 & p_2 \\ p_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & p_2 \end{pmatrix} = \begin{pmatrix} 0 & p_2^2 \\ 0 & 0 \end{pmatrix}$$

is not a multiple of the last basis-row $\begin{pmatrix} p_1 & 0 \end{pmatrix}$, so we are done. □

4 Statistical analysis

We have implemented the algorithm from section 2.3 using Shoups NTL library [8]. To create random integer lattices of rank n we set a bounding-parameter b for the lattice entries and used the randomness functions provided by NTL to create n^2 random integer entries with absolute value less than b. In the rare case that the determinant of the generated basis was zero, we discarded it.

We ran our test on 1000 bases in the dimensions 2, 3, 10, and 100 using the small number-bound $b = 10$, but we never actually found an ideal lattice.

We will now justify, why ideal lattices are hard to find. The following lemma gives a condition that the randomly generated lattice bases, once they have been transformed to HNF, need to satisfy in order to be ideal.

Lemma 4. *Let B be the HNF-basis of a full-rank ideal lattice of dimension n, then the diagonal entries form a divison chain*

$$B_{(n,n)} \mid B_{(n-1,n-1)} \mid \cdots \mid B_{(1,1)}.$$

Proof. We define the function

$$\mathrm{rot}\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^n : (\mathbf{v}_1, \ldots, \mathbf{v}_n)^T \longmapsto (\mathbf{v}_n, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1})^T.$$

Let $i \in \{1, \ldots, n-1\}$, then by lemma 1 the rotation of the i-th basis vector $\mathrm{rot}(B_{(\cdot,i)})$ is in the lattice spanned by B. So there is a vector $\mathbf{t} \in \mathbb{Z}^n$ such that

$$\mathrm{rot}(B_{(\cdot,i)}) = B\mathbf{t}$$

$$\begin{pmatrix} 0 \\ * \\ B_{(i,i)} \\ 0 \end{pmatrix} = \begin{pmatrix} B_{(1,1)} & & & * & \\ & \ddots & & & \\ & & & B_{(i+1,i+1)} & \\ & 0 & & & \ddots \end{pmatrix} \begin{pmatrix} \mathbf{t}_1 \\ \vdots \\ \mathbf{t}_{i+1} \\ \vdots \end{pmatrix} . \qquad \begin{matrix} \} \, 1 \\ \} \, i-2 \\ \} \, 1 \\ \} \, n-i \end{matrix}$$

Here the rightmost numbers specify the amount of entries in each row. Since all diagonal entries of B are non-zero, the lower entries of $\mathbf{t}$ have to be $\mathbf{t}_{i+2} = \cdots = \mathbf{t}_n = 0$. This gives us $B_{(i+1,i+1)}\mathbf{t}_{i+1} = B_{(i,i)}$, so we have shown $B_{(i+1,i+1)} \mid B_{(i,i)}$. □

The likelihood that this condition is satisfied by randomly chosen bases decreases significantly with higher dimensions (or number-bounds).

References

1. J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUsign: Digital signatures using the NTRU lattice. In *Topics in Cryptology - CT-RSA 2003: The Cryptographers' Track at the RSA Conference*, volume 2612 of *Lecture Notes in Computer Science*, pages 122–140. Springer-Verlag, 2003.
2. J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: A ring-based public key cryptosystem. In *Proceedings of ANTS III*, volume 1423, pages 267–288. Springer-Verlag, 1998.
3. V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Proceedings of ICALP, Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 144–155. Springer-Verlag, 2006.
4. D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pages 356–365, 2002.
5. P. Q. Nguyen and O. Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In *Advances in Cryptology - EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 215–233. Springer-Verlag, 2006.
6. P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Cryptography and Lattices Conference*, volume 2146 of *Lecture Notes in Computer Science*, pages 146–180. Springer-Verlag, 2001.
7. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th annual ACM symposium on Theory of computing*, pages 84–93. ACM Press, 2005.
8. Victor Shoup. Number theory library (NTL) for C++. `http://www.shoup.net/ntl/`.
9. A. Storjohann. *Algorithms for matrix canonical forms.* PhD thesis, ETH Zürich, 2000.
10. F. Uhlig. Constructive ways for generating (generalized) real orthogonal matrices as products of (generalized) symmetries. *Linear Algebra and Its Applications*, 332:459–467, 2001.