PAPER *Special Section on Discrete Mathematics and Its Applications*

Explicit Relation between Low-Dimensional LLL-Reduced Bases and Shortest Vectors

Kotaro MATSUDA[†a)], **Atsushi TAKAYASU**[†,††b)], ***Nonmembers*****, *and*** **Tsuyoshi TAKAGI**[†c)], ***Member***

SUMMARY The *Shortest Vector Problem* (SVP) is one of the most important lattice problems in computer science and cryptography. The *LLL lattice basis reduction algorithm* runs in polynomial time and can compute an *LLL-reduced basis* that provably contains an approximate solution to the SVP. On the other hand, the LLL algorithm in practice tends to solve low-dimensional exact SVPs with high probability, i.e., > 99.9%. Filling this theoretical-practical gap would lead to an understanding of the computational hardness of the SVP. In this paper, we try to fill the gap in 3, 4 and 5 dimensions and obtain two results. First, we prove that given a 3, 4 or 5-dimensional LLL-reduced basis, the shortest vector is one of the basis vectors or it is a limited integer linear combination of the basis vectors. In particular, we construct explicit representations of the shortest vector by using the LLL-reduced basis. Our analysis yields a necessary and sufficient condition for checking whether the output of the LLL algorithm contains the shortest vector or not. Second, we estimate the failure probability that a 3-dimensional random LLL-reduced basis does not contain the shortest vector. The upper bound seems rather tight by comparison with a Monte Carlo simulation.

key words: *lattice, shortest vector problem, LLL algorithm, lattice-based cryptography*

1. Introduction

1.1 Background

Public key cryptography is a fundamental technique for ensuring security in today's information society. The RSA cryptosystem [37] and elliptic curve cryptosystem [19], [29] are widely used, as exemplified by the SSL/TLS protocol. Since the level of security relates to the hardness of the integer factorization and discrete logarithm problems that are believed to be computationally hard, the schemes are believed to be currently secure. However, due to Shor's breakthrough work [42], these schemes can be broken in polynomial time by using a quantum algorithm. Therefore, constructing alternative cryptosystems that are secure in the post-quantum era has become the main stream of cryptography research. *Lattice-based cryptography* is one of the most promising candidates to resolve this issue. Its security relates to the hardness of the shortest vector problem (SVP). Given a lattice basis, the goal of SVP is to find the shortest non-zero lattice vector. SVP is NP-hard under randomized reductions [1] and is believed to be computationally hard even against quantum adversaries.

Although several lattice-based schemes, e.g., [15], [16], [36], have been proposed thus far, this does not suggest that they can be efficiently and securely used in practice. More concretely, we do not know the most suitable lattice dimensions for the best efficiency/security trade-off. To find them, we should examine the behavior of *lattice basis reduction algorithms* that are frequently used to estimate the hardness of SVPs. There are two types of SVP algorithm; one for solving exact SVPs, the other for solving α-SVPs. Given a lattice basis, the goal of an α-SVP for $\alpha > 1$ is to find a lattice vector whose norm is at most α times more than that of the shortest non-zero vector. In the context of the security of lattice-based cryptography, we want to estimate the running times of α-SVPs for a small constant α, e.g., $\alpha = 1.05$. In this paper, we focus on the *LLL algorithm* [23]. The LLL algorithm runs in polynomial time, but solves the α-SVP for only large α that is exponential in the lattice dimensions. There are several (super-)exponential time algorithms for solving exact SVPs, e.g., enumeration [10], [20], sieve algorithms [2], [27], random sampling reductions [40], Voronoi cell computations [26], and so on, and all of them utilize the LLL algorithm as preprocessing. In addition, several reduction algorithms e.g., BKZ reduction [38], [40], transference reduction [12], slide reduction [13], and so on, have been proposed for solving α-SVPs for smaller α than the LLL algorithm. All the algorithms are generalizations of the LLL algorithm and utilize it as a subroutine. Therefore, the LLL algorithm is a fundamental tool for solving (α-)SVPs and understanding the behavior of the LLL algorithm should be a crucial goal in the study of (α-)SVP algorithms.

The main stream of SVP is widely studied by many researchers especially in cryptography community. There are mainly two directions for studying the hardness of SVP, i.e., (1) *practical* analysis based on several heuristics, (2) *theoretical* analysis based on as strict discussion as possible. The first approach (1) is the current main stream of this research area and has recently provided several fantastic results. Indeed, based on several heuristics such as the Gaussian heuristic, the geometric series assumption [39], and the randomness assumption [5], [11], [43], several faster SVP algorithms have been proposed. To solve the exact SVP, faster variants of enumeration [14], sieve algorithms [7], [9], [21], [22], [34], and random sampling re-

Manuscript received October 1, 2018.
Manuscript revised January 22, 2019.

[†]The authors are with the Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, 113-8654 Japan.

[††]The author is with National Institute of Advanced Industrial Science and Technology, Tokyo, 135-0064 Japan.

a) E-mail: kotaro_matsuda@mist.i.u-tokyo.ac.jp
b) E-mail: takayasu@mist.i.u-tokyo.ac.jp
c) E-mail: takagi@mist.i.u-tokyo.ac.jp

DOI: 10.1587/transfun.E102.A.1091

ductions [5], [11], [24], [44] have been proposed. Similarly, faster variants of the LLL [30], [32], [35] and the BKZ [6], [8], [17], [28], [45] have been proposed.

What we study in this paper is differs from these works since we focus on the second approach (2). Since several substantial results have recently been proposed in the first approach (1), many readers tend to forget importance of the other approach (2). However, the second approach (2) is an arguably essential research topic for studying the hardness of SVP. In particular, we study theoretical behaviors of the LLL reduction in low dimensions. One may feel that LLL in low dimensions looks a weak target since we finally want to know practical behaviors of LLL in high dimensions or possibly BKZ-reduced bases. However, it is a much harder problem than one may expect. Indeed, as we will claim below there still exists fundamental problem regarding a behavior of LLL even in low dimensions. Furthermore, all papers which try to analyze high dimensional LLL-reduced bases or BKZ-reduced bases rely on experimental analysis or several heuristics. Therefore, low-dimensional LLL-reduced bases have to be a good target to put the research direction forward.

As we claimed above, the LLL algorithm has been proven to solve an α-SVP of exponentially large α. However, it is actually much more effective in practice; it can solve exact SVPs with high probability in low dimensions. Alsayigh et al. [4] found special classes of 3-dimensional lattice bases in which the LLL algorithm always/never solves the exact SVP. Moreover, low-dimensional SVPs have been studied by Semaév [41] and Nguyen and Stehlé [33]; they constructed efficient lattice reduction algorithms specific to 3 or 4 dimensions, but they did not analyze the relation to the LLL algorithm. Our motivation is rather similar to Alsayigh et al.'s work [4]. Inspired by it, we decided to study the relationship between outputs of the LLL algorithm and shortest vectors in low dimensions.

1.2 Our Contributions

In this paper, we show an explicit relation between LLL-reduced bases and the shortest vectors in three, four and five dimensions. We prove that at least one of a few fixed linear integer combinations of the LLL-reduced basis vectors is the shortest non-zero vector in the lattice if the LLL-reduced basis does not contain the shortest non-zero vector in three, four and five dimensions. From this, we obtain a necessary and sufficient condition that an LLL-reduced basis does not contain the shortest vector. For example, if a 3-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ does not contain the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$, then either $\boldsymbol{b}_2 \pm \boldsymbol{b}_3$ or $\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3$ is the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$. Thus, we can easily find one of the shortest non-zero vectors in the lattice by changing the LLL algorithm slightly. Moreover, by using this condition, we estimate the failure probability that a random LLL-reduced basis does not contain the shortest vector in three dimensions. To be more precise, we consider 6-dimensional space where each point is corresponded to a 3-dimensional basis, and then we estimate the ratio of the volume of the region corresponded to LLL-reduced bases not containing the shortest vector over that of the region corresponded to LLL-reduced bases. We calculate its upper bound by numerical integration. We also show that the upper bound we obtain is about twice the value obtained in a Monte Carlo simulation.

1.3 Organization

In Sect. 2, we recall the basic notions of lattices, SVP, and LLL algorithm. In Sect. 3, we show the explicit relation between LLL-reduced bases and the shortest vectors in three, four and five dimensions. In Sect. 4, we estimate the failure probability that a 3-dimensional random LLL-reduced basis does not contain the shortest vector. In addition, we compare the upper bound with the value obtained by the Monte Carlo method.

2. Preliminaries

In this section, we recall the basic definitions of lattices and the (α-)shortest vector problem (SVP). Then, we explain the LLL algorithm and its behavior in low dimensions.

2.1 Notation

Let $\mathbb{R}$ and $\mathbb{Z}$ denote a set of real numbers and integers, respectively. Let a lowercase bold letter $\boldsymbol{b}$ denote a vector whose transpose is denoted by $\boldsymbol{b}^\top$. The Euclidean norm of a vector $\boldsymbol{b}$ is denoted by $\|\boldsymbol{b}\|$. The inner product of $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ is denoted by $\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle$. Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ be a set of linearly independent vectors. The Gram-Schmidt orthogonal basis $(\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*)$ is defined as follows: $\boldsymbol{b}_1^* = \boldsymbol{b}_1$ and $\boldsymbol{b}_i^* = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \boldsymbol{b}_j^*$ for $2 \le i \le n$, where $\mu_{ij} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{\|\boldsymbol{b}_j^*\|^2}$ are called Gram-Schmidt orthogonal coefficients. We will sometimes write μ_{ij} as $\mu_{i,j}$ in this paper.

2.2 Lattices

A lattice is an additive discrete subgroup of $\mathbb{R}^m$. Let $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) \in \mathbb{R}^{n \times m}$ be a set of linearly independent vectors. A lattice spanned by a basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ is defined as $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \{\sum_{i=1}^n x_i \boldsymbol{b}_i | x_i \in \mathbb{Z}\}$. For simplicity throughout the paper, we will study only full-rank lattices, i.e., $n = m$.

Let $\lambda_1(L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n))$ denote the Euclidean norm of the shortest non-zero vector in $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$. We define the *SVP* as follows.

Definition 1 (SVP): Given a basis $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, the goal of the SVP is to find a vector $\boldsymbol{b}'$ in a lattice $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ such that $\|\boldsymbol{b}'\| = \lambda_1(L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n))$ holds.

Ajtai proved that the SVP is NP-hard under randomized reduction [1].

There is also an approximate version parameterized by $\alpha > 1$.

Definition 2 (α-SVP): Given a basis $(\boldsymbol{b}_1, ..., \boldsymbol{b}_n)$ and a real number $\alpha > 1$, the goal of the α-SVP is to find a vector $\boldsymbol{b}'$ in a lattice $L(\boldsymbol{b}_1, ..., \boldsymbol{b}_n)$ such that $\|\boldsymbol{b}'\| \leq \alpha\lambda_1(L(\boldsymbol{b}_1, ..., \boldsymbol{b}_n))$ holds.

Khot proved that the α-SVP is NP-hard if α is a constant under randomized reductions [18].

2.3 LLL Algorithm

Here, we recall the *LLL algorithm*, which is a fundamental tool for solving the (α-)SVP.

Lattices do not have unique bases. There exist infinitely many bases for the same lattice under unimodular transformations. Given a lattice basis, the LLL algorithm outputs an *LLL-reduced basis* defined as follows.

Definition 3 (LLL-reduced Basis): Let δ be a real number with $\delta \in (1/4, 1]$. If a basis $(\boldsymbol{b}_1, ..., \boldsymbol{b}_n) \in \mathbb{R}^{n \times n}$ satisfies the following two conditions, it is called an LLL-reduced basis with a Lovász factor δ:

- Size reduction: $|\mu_{ij}| \leq 1/2$ holds for all i, j with $1 \leq j < i \leq n$,
- Lovász condition: $\|\boldsymbol{b}_i^* + \mu_{i,i-1}\boldsymbol{b}_{i-1}^*\|^2 \geq \delta\|\boldsymbol{b}_{i-1}^*\|^2$ hold for all i with $2 \leq i \leq n$.

The LLL algorithm runs in $\mathrm{O}(n^6 \log^3(\max(\|\boldsymbol{b}_1\|, ..., \|\boldsymbol{b}_n\|)))$ time for $\delta < 1$ (it has been proven for $\delta = 1$ in a fixed number of dimensions that it runs in polynomial time of input size [3]) and outputs LLL-reduced bases. In using the LLL algorithm, δ is usually strictly smaller than 1. In this paper, we also consider the case of $\delta = 1$, which is called "ideal" or "optimal". The first vector $\boldsymbol{b}_1$ of an LLL-reduced basis is a solution of an α-SVP for $\alpha = \left(\frac{4}{4\delta-1}\right)^{\frac{n-1}{2}}$, i.e., $\|\boldsymbol{b}_1\| \leq \left(\frac{4}{4\delta-1}\right)^{\frac{n-1}{2}} \lambda_1(L(\boldsymbol{B}))$ holds. Hence, a smaller Lovász factor enables us to solve α-SVP for a larger α. In the special case $n = 2$, LLL for $\delta = 1$ is the same as the Lagrange-Gauss reduction algorithm (see e.g. [31]). Hence, LLL runs in polynomial time and outputs the shortest vectors. It is well known that LLL outputs much shorter vectors in practice. Specifically, in three to ten dimensions, it can solve an SVP with a probability of more than 99.9% by taking a factor δ close to 1 ($\delta > 0.999$) [4].

In this paper, we say that a basis $(\boldsymbol{b}_1, .., \boldsymbol{b}_n)$ does not contain the shortest non-zero vector if $\|\boldsymbol{b}_i\| \neq \lambda_1(L(\boldsymbol{b}_1, ..., \boldsymbol{b}_n))$ holds for $1 \leq i \leq n$. In addition, we say the failure condition is when an LLL-reduced basis does not contain the shortest non-zero vector.

3. Failure Condition of LLL-Reduced Bases

Here, we discuss the necessary and sufficient condition that an LLL-reduced basis does not contain the shortest vector. Indeed, we show how the shortest vector can be represented by an integer linear combination of an LLL-reduced basis vectors.

3.1 Case of Three Dimensions and $\delta = 1$

First, we discuss the case of $n = 3$ dimensions and a Lovász factor $\delta = 1$ in Definition 3. In this case, we can prove the following theorem.

Theorem 1: Suppose a 3-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ for a Lovász factor $\delta = 1$ does not contain the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$. If $\boldsymbol{b}' = \sum_{i=1}^3 x_i\boldsymbol{b}_i$ for some integers x_1, x_2, x_3 is the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$, then $(|x_1|, |x_2|, |x_3|) = (1, 1, 1)$ or $(0, 1, 1)$ holds. In addition, there exist LLL-reduced bases $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ such that $\boldsymbol{b}' = \sum_{i=1}^3 x_i\boldsymbol{b}_i$ is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ for each $(|x_1|, |x_2|, |x_3|) = (1, 1, 1)$ or $(0, 1, 1)$.

Proof 1: The Gram-Schmidt orthogonal basis $(\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \boldsymbol{b}_3^*)$ satisfies $\boldsymbol{b}_1 = \boldsymbol{b}_1^*, \boldsymbol{b}_2 = \mu_{21}\boldsymbol{b}_1^* + \boldsymbol{b}_2^*, \boldsymbol{b}_3 = \mu_{31}\boldsymbol{b}_1^* + \mu_{32}\boldsymbol{b}_2^* + \boldsymbol{b}_3^*$. Hence, $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ can be represented as linear combinations of orthogonal basis vectors $\left(\frac{\boldsymbol{b}_1^*}{\|\boldsymbol{b}_1^*\|}, \frac{\boldsymbol{b}_2^*}{\|\boldsymbol{b}_2^*\|}, \frac{\boldsymbol{b}_3^*}{\|\boldsymbol{b}_3^*\|}\right)$ as follows:

$$\begin{pmatrix} \boldsymbol{b}_1^\top \\ \boldsymbol{b}_2^\top \\ \boldsymbol{b}_3^\top \end{pmatrix} = \begin{pmatrix} \|\boldsymbol{b}_1^*\| & 0 & 0 \\ \mu_{21}\|\boldsymbol{b}_1^*\| & \|\boldsymbol{b}_2^*\| & 0 \\ \mu_{31}\|\boldsymbol{b}_1^*\| & \mu_{32}\|\boldsymbol{b}_2^*\| & \|\boldsymbol{b}_3^*\| \end{pmatrix} \begin{pmatrix} \frac{1}{\|\boldsymbol{b}_1^*\|}\boldsymbol{b}_1^{*\top} \\ \frac{1}{\|\boldsymbol{b}_2^*\|}\boldsymbol{b}_2^{*\top} \\ \frac{1}{\|\boldsymbol{b}_3^*\|}\boldsymbol{b}_3^{*\top} \end{pmatrix}. \tag{1}$$

Since $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is LLL-reduced, we have the following inequalities:

$$\|\boldsymbol{b}_2^*\|^2 \geq (1 - \mu_{21}^2)\|\boldsymbol{b}_1^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_1^*\|^2, \tag{2}$$

$$\|\boldsymbol{b}_3^*\|^2 \geq (1 - \mu_{32}^2)\|\boldsymbol{b}_2^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_2^*\|^2 \geq \frac{9}{16}\|\boldsymbol{b}_1^*\|^2. \tag{3}$$

If x_3 satisfies $|x_3| \geq 2$, the vector $\boldsymbol{b}' = \sum_{i=1}^3 x_i\boldsymbol{b}_i$ fulfills the following inequality:

$$\|\boldsymbol{b}'\|^2 \geq (2\|\boldsymbol{b}_3^*\|)^2 = 4\|\boldsymbol{b}_3^*\|^2 \geq \frac{9}{4}\|\boldsymbol{b}_1^*\|^2 > \|\boldsymbol{b}_1\|^2. \tag{4}$$

Therefore, if $\boldsymbol{b}'$ is the shortest non-zero vector, $|x_3| \leq 1$ holds.

If $x_3 = 0$ holds, $\boldsymbol{b}'$ is in $L(\boldsymbol{b}_1, \boldsymbol{b}_2)$. The 2-dimensional LLL algorithm for $\delta = 1$ is equivalent to the Lagrange-Gauss reduction algorithm. Therefore, $\|\boldsymbol{b}_1\| = \lambda_1(L(\boldsymbol{b}_1, \boldsymbol{b}_2))$ or $\|\boldsymbol{b}_2\| = \lambda_1(L(\boldsymbol{b}_1, \boldsymbol{b}_2))$. Consequently, if the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ does not contain the shortest non-zero vector and $\boldsymbol{b}'$ is the shortest vector, $|x_3| = 1$.

Next, if x_2 satisfies $|x_2| \geq 2$,

$$\begin{aligned} \|\boldsymbol{b}'\|^2 &\geq |x_3|^2\|\boldsymbol{b}_3^*\|^2 + (x_3\mu_{32} + x_2)^2\|\boldsymbol{b}_2^*\|^2 \\ &\geq \frac{9}{4}\|\boldsymbol{b}_2^*\|^2 \geq \frac{27}{16}\|\boldsymbol{b}_1^*\|^2 > \|\boldsymbol{b}_1\|^2 \end{aligned}$$

holds in accordance with the size reduction, equations (1), (3) and $|x_3| = 1$. This contradicts the shortest property of $\boldsymbol{b}'$ and thus $|x_2| \leq 1$ holds.

Finally we prove $|x_1| \leq 1$. From $\boldsymbol{b}' = \sum_{i=1}^{3} x_i \boldsymbol{b}_i$, we have the equality $\|\boldsymbol{b}'\|^2 = (x_1 + \mu_{21}x_2 + \mu_{31}x_3)^2\|\boldsymbol{b}_1^*\|^2 + (x_2 + \mu_{32}x_3)^2\|\boldsymbol{b}_2^*\|^2 + x_3^2\|\boldsymbol{b}_3^*\|^2$. From $|x_2| \leq 1$, $|x_3| \leq 1$ and the size reduction, $|\mu_{21}x_2 + \mu_{31}x_3| \leq 1$ holds. Therefore, if $\boldsymbol{b}'$ is the shortest non-zero vector, $|x_1| \leq 1$.

Moreover, if $(|x_1|, |x_2|, |x_3|) = (1, 0, 1)$, $\|\boldsymbol{b}'\| \geq \|\boldsymbol{b}_3\|$ holds by the size reduction. From the above, if $\boldsymbol{b}' = \sum_{i=1}^{3} x_i \boldsymbol{b}_i$ is the shortest vector, $(|x_1|, |x_2|, |x_3|) = (1, 1, 1)$ or $(0, 1, 1)$ holds. This means we find LLL-reduced bases that do not contain the shortest vector for each occasion (this is shown in Appendix A). □

This theorem leads to the following corollary.

Corollary 1: For a Lovász factor $\delta = 1$, the following is a necessary and sufficient condition that an LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ does not contain the shortest vector: One of the vectors $\boldsymbol{b}_2 \pm \boldsymbol{b}_3$ or $\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3$ (the signs are exclusively alternating) is shorter than $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, and $\boldsymbol{b}_3$.

From this corollary, we can obtain one of the shortest non-zero vectors using the output of the LLL algorithm and comparing the norm of $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$ with those of linear combinations $\boldsymbol{b}_2 \pm \boldsymbol{b}_3$ and $\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3$. We note that the result is derived for analyzing *theoretical* behaviors of LLL-reduced bases. Specifically, even when we obtain analogous results for high dimensions, they do not seem useful to speed-up practical enumeration. In particular, although we do not use any heuristics during the analysis, practical enumeration based on several heuristics has to be faster than the above analysis.

The representation of the shortest vectors by limited number of integer linear combinations may look similar to natural number representation/tag in the context of enumeration and random sampling reduction [5], [11], [24], [44]. However, unfortunately we cannot find close relation with these notions. Furthermore, unlike ours the researches [5], [11], [24], [44] are heavily based on several heuristics, e.g., randomness assumption [43].

3.2 Case of Three Dimensions and $\delta < 1$

Next, we extend Theorem 1 to the case of a Lovász factor $\delta < 1$. Note that the LLL algorithm often uses $\frac{3}{4} \leq \delta$, but we prove the following theorem for the case of $\frac{7}{12} \leq \delta \leq 1$.

Theorem 2: Theorem 1 holds for a Lovász factor $\frac{7}{12} \leq \delta \leq 1$.

Proof 2: From the size reduction, the Lovász condition and $\frac{7}{12} \leq \delta \leq 1$, we have

$$\|\boldsymbol{b}_2^*\|^2 \geq \left(\delta - \frac{1}{4}\right)\|\boldsymbol{b}_1^*\|^2 \geq \frac{1}{3}\|\boldsymbol{b}_1^*\|^2 \text{ and}$$
$$\|\boldsymbol{b}_3^*\|^2 \geq \left(\delta - \frac{1}{4}\right)\|\boldsymbol{b}_2^*\|^2 \geq \frac{1}{3}\|\boldsymbol{b}_2^*\|^2.$$

Suppose $x_3 \geq 2$, then we obtain the following inequality:

$$\begin{aligned}\|\boldsymbol{b}'\|^2 &\geq 4\|\boldsymbol{b}_3^*\|^2 \geq \|\boldsymbol{b}_3^*\|^2 + \|\boldsymbol{b}_2^*\|^2 \\ &\geq \|\boldsymbol{b}_3^*\|^2 + \frac{1}{4}\|\boldsymbol{b}_2^*\|^2 + \frac{1}{4}\|\boldsymbol{b}_1^*\|^2 \geq \|\boldsymbol{b}_3\|^2.\end{aligned}$$

This implies $|x_3| \leq 1$.

Now, let us prove $x_3 \neq 0$. $\|\boldsymbol{b}'\|^2 \geq 4\|\boldsymbol{b}_2^*\|^2 \geq \frac{4}{3}\|\boldsymbol{b}_1^*\|^2 > \|\boldsymbol{b}_1\|^2$ holds for $x_3 = 0$ and $|x_2| \geq 2$. $\|\boldsymbol{b}'\|^2 \geq \|\boldsymbol{b}_2^*\|^2 + (x_1 + \mu_{12})^2\|\boldsymbol{b}_1^*\|^2 \geq \|\boldsymbol{b}_2\|^2$ holds for $x_3 = 0$ and $|x_2| = 1$. $\|\boldsymbol{b}'\| \geq \|\boldsymbol{b}_1\|$ holds for $x_3 = 0$ and $x_2 = 0$. This contradicts the shortest property of $\boldsymbol{b}'$. Therefore $x_3 \neq 0$, *i.e.*, $|x_3| = 1$.

If $|x_2| \geq 2$,

$$\begin{aligned}\|\boldsymbol{b}'\|^2 &\geq \frac{9}{4}\|\boldsymbol{b}_2^*\|^2 + \|\boldsymbol{b}_3^*\|^2 \\ &\geq \frac{2}{3}\|\boldsymbol{b}_1^*\|^2 + \frac{1}{4}\|\boldsymbol{b}_2^*\|^2 + \|\boldsymbol{b}_3^*\|^2 > \|\boldsymbol{b}_3\|^2\end{aligned}$$

holds by the size reduction and $\|\boldsymbol{b}_2^*\| \geq \frac{1}{3}\|\boldsymbol{b}_1^*\|$. Therefore $|x_2| \leq 1$ holds. A discussion similar to the proof in the case of $\delta = 1$ leads to $|x_1| \leq 1$.

Thus, Theorem 2 is proved. □

A corollary similar to Corollary 1 holds for $\frac{7}{12} \leq \delta \leq 1$.

3.3 Case of Four and Five Dimensions and $\delta = 1$

An ideal goal of our approach has to be an extension for the asymptotic case. However, to avoid using any heuristics, the computations during the analyses take huge amount of times. For example, we list all the possible linear combinations to find the shortest vector and the listing is at least harder than solving SVP. Therefore, providing the analogous analysis in high dimensions without any heuristics has to be an intractable problem. In this paper, to observe analogous behaviors for higher dimensions, we prove theorems in the case of $n = 4$ or 5 dimensions and a Lovász factor $\delta = 1$. The proofs are similar to that of Theorem 1 (Summaries are in Appendix B).

Theorem 3: Suppose a 4-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ for a Lovász factor $\delta = 1$ does not contain the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$. Then one of the vectors $\sum_{i=1}^{4} x_i \boldsymbol{b}_i$ satisfying $(|x_1|, |x_2|, |x_3|, |x_4|) = (0, 1, 1, 0), (1, 1, 1, 0), (0, 0, 1, 1), (1, 0, 1, 1), (0, 1, 0, 1), (1, 1, 0, 1), (0, 1, 1, 1)$ or $(1, 1, 1, 1)$ is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$. In addition, there exist LLL-reduced bases $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ such that $\boldsymbol{b}' = \sum_{i=1}^{4} x_i \boldsymbol{b}_i$ for each $(|x_1|, |x_2|, |x_3|, |x_4|)$ of the above equation is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$.

Theorem 4: Suppose a 5-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$ for a Lovász factor $\delta = 1$ does not contain the shortest non-zero vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$. Then one of the vectors $\sum_{i=1}^{5} x_i \boldsymbol{b}_i$ satisfying $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) =$
$(0, 1, 1, 0, 0), (1, 1, 1, 0, 0), (0, 0, 1, 1, 0), (1, 0, 1, 1, 0),$
$(0, 1, 0, 1, 0), (1, 1, 0, 1, 0), (0, 1, 1, 1, 0), (1, 1, 1, 1, 0),$
$(0, 1, 0, 0, 1), (0, 0, 1, 0, 1), (0, 0, 0, 1, 1), (1, 1, 0, 0, 1),$
$(1, 0, 1, 0, 1), (1, 0, 0, 1, 1), (0, 1, 1, 0, 1), (0, 1, 0, 1, 1),$

$(0,0,1,1,1), (1,1,1,0,1), (1,1,0,1,1), (1,0,1,1,1),$
$(0,1,1,1,1), (1,1,1,1,1), (2,1,1,1,1), (0,2,1,1,1),$
$(1,2,1,1,1)$ or $(2,2,1,1,1)$ is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$. In addition, there exist LLL-reduced bases $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$ for each $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|)$ of the above equation such that $\boldsymbol{b}' = \sum_{i=1}^{5} x_i \boldsymbol{b}_i$ is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$.

From these theorems, we can easily find one of the shortest non-zero vectors in a four or five-dimensional lattice by changing the LLL algorithm slightly. Namely, if a 4 or 5-dimensional LLL-reduced basis does not contain the shortest non-zero vector in the lattice, then one of the vectors appearing in Theorems 3 and 4 is the shortest non-zero vector.

4. Estimating the Failure Probability in Three Dimensions

In this section, we estimate the failure probability that a 3-dimensional random LLL-reduced basis does not contain the shortest vector. We consider six-dimensional space parameterized by six variables $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$. In the space, each point is correspond one-to-one with a basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ since $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is determined by $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$. We estimate the ratio of the volume of the region corresponded to LLL-reduced bases not containing the shortest vector over that of the region corresponded to LLL-reduced bases. We obtain its upper bound by numerical integration and compare it with the value obtained by the Monte Carlo method.

4.1 Projection Region

Here, in order to estimate the failure probability by integration, we first describe the condition for an LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ by projecting $\boldsymbol{b}_3$ on the plane H spanned by $(\boldsymbol{b}_1, \boldsymbol{b}_2)$. For a fixed $(\boldsymbol{b}_1, \boldsymbol{b}_2)$ satisfying $\|\boldsymbol{b}_2\|^2 \geq \delta\|\boldsymbol{b}_1\|^2$, the blue rectangular region in Fig. 1 shows the condition for the possible projection of $\boldsymbol{b}_3$ on H such that $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is LLL-reduced. For simplicity we show the region that satisfies $\mu_{21} \geq 0$ and $\mu_{32} \geq 0$. The width of the rectangle is determined by the size reduction of $|\mu_{31}| \leq \frac{1}{2}$ appearing in the LLL-reduced basis. The heights of the upper and lower parts of the rectangle are decided by the size reduction $|\mu_{32}| \leq \frac{1}{2}$, and the Lovász condition, $\|\boldsymbol{b}_3^*\|^2 + \mu_{32}^2\|\boldsymbol{b}_2^*\|^2 \geq \delta\|\boldsymbol{b}_2^*\|$, respectively.

Next, we explain the condition for an LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ not containing the shortest vector. By Theorem 2, if a 3-dimensional LLL-reduced basis does not contain the shortest vector, $\boldsymbol{b}_2 \pm \boldsymbol{b}_3$ or $\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3$ (the signs are exclusively alternating) is the shortest vector. Therefore, $\|\boldsymbol{b}_2 \pm \boldsymbol{b}_3\| < \min(\|\boldsymbol{b}_1\|, \|\boldsymbol{b}_2\|, \|\boldsymbol{b}_3\|)$ or $\|\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3\| < \min(\|\boldsymbol{b}_1\|, \|\boldsymbol{b}_2\|, \|\boldsymbol{b}_3\|)$ holds in this case. Thus, for fixed $\boldsymbol{b}_1, \boldsymbol{b}_2$ and $\boldsymbol{b}_3^*$, the region of the projection of $\boldsymbol{b}_3$ onto H is the red region in Fig. 2 if the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ does not contain the shortest vector.

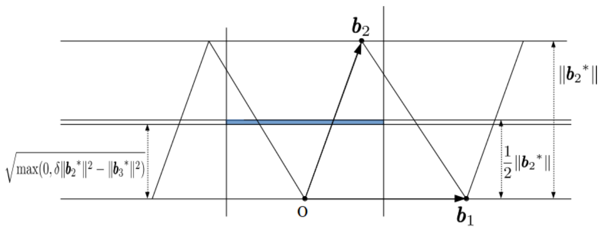

$\boldsymbol{b}_2$
$\|\boldsymbol{b}_2{}^*\|$
$\sqrt{\max(0, \delta\|\boldsymbol{b}_2{}^*\|^2 - \|\boldsymbol{b}_3{}^*\|^2)}$
$\frac{1}{2}\|\boldsymbol{b}_2{}^*\|$
O
$\boldsymbol{b}_1$

Fig. 1 Region of the projection of $\boldsymbol{b}_3$ onto a plane $H = \text{span}(\boldsymbol{b}_1, \boldsymbol{b}_2)$ (blue region : $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is an LLL-reduced basis).

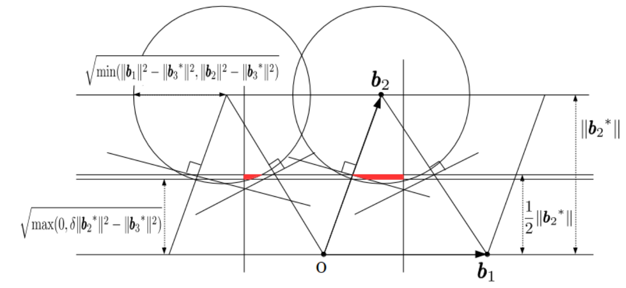

$\sqrt{\min(\|\boldsymbol{b}_1\|^2 - \|\boldsymbol{b}_3{}^*\|^2, \|\boldsymbol{b}_2\|^2 - \|\boldsymbol{b}_3{}^*\|^2)}$
$\boldsymbol{b}_2$
$\|\boldsymbol{b}_2{}^*\|$
$\sqrt{\max(0, \delta\|\boldsymbol{b}_2{}^*\|^2 - \|\boldsymbol{b}_3{}^*\|^2)}$
$\frac{1}{2}\|\boldsymbol{b}_2{}^*\|$
O
$\boldsymbol{b}_1$

Fig. 2 Region of the projection of $\boldsymbol{b}_3$ onto a plane $H = \text{span}(\boldsymbol{b}_1, \boldsymbol{b}_2)$ (red region : $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is an LLL-reduced basis not containing the shortest vector).

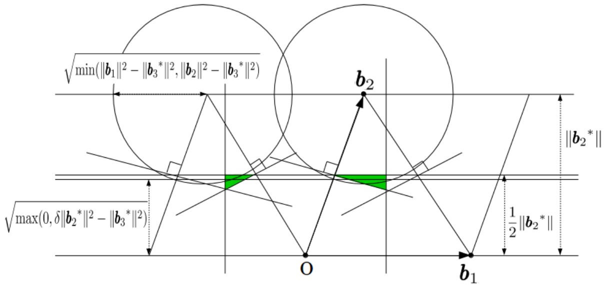

$\sqrt{\min(\|\boldsymbol{b}_1\|^2 - \|\boldsymbol{b}_3{}^*\|^2, \|\boldsymbol{b}_2\|^2 - \|\boldsymbol{b}_3{}^*\|^2)}$
$\boldsymbol{b}_2$
$\|\boldsymbol{b}_2{}^*\|$
$\sqrt{\max(0, \delta\|\boldsymbol{b}_2{}^*\|^2 - \|\boldsymbol{b}_3{}^*\|^2)}$
$\frac{1}{2}\|\boldsymbol{b}_2{}^*\|$
O
$\boldsymbol{b}_1$

Fig. 3 Region of the projection of $\boldsymbol{b}_3$ onto a plane $H = \text{span}(\boldsymbol{b}_1, \boldsymbol{b}_2)$.

4.2 Upper Bound of the Failure Probability in Three Dimensions

In three dimensions, we estimate the failure probability that a 3-dimensional random LLL-reduced basis does not contain the shortest vector. This failure probability can be calculated as the ratio of the volume of the red region in Fig. 2 over that of the blue region in Fig. 1. However, the calculation of the volume of the red region is relatively hard, and thus we evaluate the volume of the green region in Fig. 3, which contains the red region. To calculate the volumes of the blue and green regions, we use numerical integration over six variables $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$. In particular, the calculation can be used to estimate the volume of the hypersurface in six-dimensional space parameterized by the above variables.

Here, we prove the following theorem for estimating the upper bound of the failure probability.

Theorem 5: Let S be six dimensional space $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$. Let $D \subset S$ be the region corresponded LLL-reduced bases $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$. Let $E \subset S$ be the region corresponded LLL-reduced bases $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ not containing the shortest vector in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$. Let P be the failure probability calculated as the ratio of the volume of E over that of D. Then $P < 2.94 \times 10^{-4}$ holds by taking Lovász factor $\delta = 1$.

If we fix $\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|$, and $\mu_{21}\|\boldsymbol{b}_1^*\|$, the region D and E is shown as the blue region in Fig. 1 and the red one in Fig. 2, respectively. Therefore, we try to integrate their volume.

Proof 3: If the value $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\|$ is fixed, the ratio of volume of the region E over that of the region D is constant independently of the value $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\|$. Therefore, we estimate P under the scaling $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$. Let V be the volume of the region D under $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$. Since the green region in Fig. 3 contains the red region in Fig. 2 corresponding to E in Theorem 5, the failure probability P is less than U/V where U is the volume of the green region in Fig. 3 under $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$. We can calculate U and V by using numerical integration over six variables $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$ under the scaling $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$.

First, we discuss the possible ranges of the six variables $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \|\boldsymbol{b}_3^*\|, \mu_{21}\|\boldsymbol{b}_1^*\|, \mu_{31}\|\boldsymbol{b}_1^*\|, \mu_{32}\|\boldsymbol{b}_2^*\|)$. We may assume $\mu_{21} \geq 0$ by symmetry of the conditions for an LLL-reduced basis. From the size reduction and the Lovász condition of the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$, we have

$$0 \leq \|\boldsymbol{b}_1^*\| \leq \frac{\|\boldsymbol{b}_2^*\|}{\sqrt{\delta - \frac{1}{4}}},$$

$$0 \leq \|\boldsymbol{b}_2^*\| \leq \frac{\|\boldsymbol{b}_3^*\|}{\sqrt{\delta - \frac{1}{4}}} = \frac{1}{\sqrt{\delta - \frac{1}{4}}\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|}.$$

Therefore,

$$0 \leq \|\boldsymbol{b}_1^*\| \leq \min\left(\frac{\|\boldsymbol{b}_2^*\|}{\sqrt{\delta - \frac{1}{4}}}, \frac{1}{\sqrt{\delta - \frac{1}{4}}\|\boldsymbol{b}_2^*\|^2}\right) \tag{5}$$

holds. In addition, from the size reduction and the Lovász condition, $0 \leq \mu_{21}\|\boldsymbol{b}_1^*\| \leq \frac{1}{2}\|\boldsymbol{b}_1^*\|$ and $\mu_{21}^2\|\boldsymbol{b}_1^*\|^2 + \|\boldsymbol{b}_2^*\|^2 \leq \delta\|\boldsymbol{b}_1^*\|^2$. Thus,

$$\sqrt{\max(0, \delta\|\boldsymbol{b}_1^*\|^2 - \|\boldsymbol{b}_2^*\|^2)} \leq \mu_{21}\|\boldsymbol{b}_1^*\| \leq \frac{\|\boldsymbol{b}_1^*\|}{2}. \tag{6}$$

Therefore, the area of the blue domain in Fig. 1 is $\|\boldsymbol{b}_1^*\|(\frac{\|\boldsymbol{b}_1^*\|}{2} - \sqrt{\max(0, \delta\|\boldsymbol{b}_1^*\|^2 - \|\boldsymbol{b}_2^*\|^2)})$.

From the above discussion, V can be calculated by integration, as follows:

$$V = \int_0^\infty \Bigg(\int_0^{\min\left(\frac{y}{\sqrt{\delta - \frac{1}{4}}}, \frac{1}{\sqrt{\delta - \frac{1}{4}} y^2}\right)} x \left(\frac{x}{2} - \sqrt{\max(0, \delta x^2 - y^2)}\right) \cdot \left(\frac{y}{2} - \sqrt{\max\left(0, \delta y^2 - \left(\frac{1}{xy}\right)^2\right)}\right) \frac{\sqrt{x^4 y^4 + x^2 + y^2}}{x^2 y^2} \mathrm{d}x \Bigg) \mathrm{d}y,$$

where $x = \|\boldsymbol{b}_1^*\|, y = \|\boldsymbol{b}_2^*\|$. (Note that $\frac{\sqrt{x^4y^4+x^2+y^2}}{x^2y^2}$ is the Jacobian under $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$.)

Next, we evaluate the upper bound of U. If $\boldsymbol{b}_1, \boldsymbol{b}_2$ and $\boldsymbol{b}_3^*$ are fixed, the area of the green region in Fig. 2 is $\frac{\|\boldsymbol{b}_1^*\|}{4} \cdot \frac{\mu_{12}\|\boldsymbol{b}_1^*\|}{\|\boldsymbol{b}_2^*\|} \cdot \left(\frac{\|\boldsymbol{b}_1^*\|}{2} - \frac{\mu_{12}\|\boldsymbol{b}_1^*\|}{2}\right)$. When the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ does not contain the shortest vector, $\lambda_1(L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3))^2 \geq \|\boldsymbol{b}_3^*\|^2 + \frac{1}{4}\|\boldsymbol{b}_2^*\|^2$ holds by Theorem 1. Therefore, from $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$ and $\|\boldsymbol{b}_1\| \geq \lambda_1(L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3))$, we have

$$\|\boldsymbol{b}_1\|^2 \geq \left(\frac{1}{\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|}\right)^2 + \frac{1}{4}\|\boldsymbol{b}_2^*\|^2.$$

This inequality implies

$$\|\boldsymbol{b}_1^*\| \geq \sqrt{\frac{\|\boldsymbol{b}_2^*\|^3 + \sqrt{\|\boldsymbol{b}_2^*\|^6 + 64}}{8\|\boldsymbol{b}_2^*\|}}. \tag{7}$$

From (5) and (7), if $\|\boldsymbol{b}_2^*\| \leq 1$ holds, $\left(\frac{(\delta - \frac{1}{4})^2}{1 - \frac{1}{4}(\delta - \frac{1}{4})}\right)^{\frac{1}{6}} \leq \|\boldsymbol{b}_2^*\| \leq 1$, otherwise $1 \leq \|\boldsymbol{b}_2^*\| \leq \left(\frac{1}{\delta(\delta - \frac{1}{4})}\right)^{\frac{1}{6}}$ holds.

From the above discussion, U can be estimated as follows:

$$\begin{aligned}
U = &\int_{\left(\frac{(\delta-\frac{1}{4})^2}{1-\frac{1}{4}(\delta-\frac{1}{4})}\right)^{\frac{1}{6}}}^{1} \left(\int_{\sqrt{\frac{y^3+\sqrt{y^6+64}}{8y}}}^{\frac{y}{\sqrt{\delta-\frac{1}{4}}}} \frac{x}{4} \left(\int_0^{\frac{x}{2}} \frac{t}{y}\left(\frac{x}{2} - \frac{t}{2}\right) \mathrm{d}t \right) \frac{\sqrt{x^4 y^4 + x^2 + y^2}}{x^2 y^2} \mathrm{d}x \right) \mathrm{d}y \\
&+ \int_1^{\left(\frac{1}{\delta(\delta-\frac{1}{4})}\right)^{\frac{1}{6}}} \left(\int_{\sqrt{\frac{y^3+\sqrt{y^6+64}}{8y}}}^{\frac{1}{\sqrt{\delta-\frac{1}{4}}y^2}} \frac{x}{4} \left(\int_0^{\frac{x}{2}} \frac{t}{y}\left(\frac{x}{2} - \frac{t}{2}\right) \mathrm{d}t \right) \frac{\sqrt{x^4 y^4 + x^2 + y^2}}{x^2 y^2} \mathrm{d}x \right) \mathrm{d}y \\
= &\int_{\left(\frac{(\delta-\frac{1}{4})^2}{1-\frac{1}{4}(\delta-\frac{1}{4})}\right)^{\frac{1}{6}}}^{1} \left(\int_{\sqrt{\frac{y^3+\sqrt{y^6+64}}{8y}}}^{\frac{y}{\sqrt{\delta-\frac{1}{4}}}} \frac{x^3\sqrt{x^4 y^4 + x^2 + y^2}}{96 y^3} \mathrm{d}x \right) \mathrm{d}y \\
&+ \int_1^{\left(\frac{1}{\delta(\delta-\frac{1}{4})}\right)^{\frac{1}{6}}} \left(\int_{\sqrt{\frac{y^3+\sqrt{y^6+64}}{8y}}}^{\frac{1}{\sqrt{\delta-\frac{1}{4}}y^2}} \frac{x^3\sqrt{x^4 y^4 + x^2 + y^2}}{96 y^3} \mathrm{d}x \right) \mathrm{d}y,
\end{aligned}$$

where $x = \|\boldsymbol{b}_1^*\|, y = \|\boldsymbol{b}_2^*\|$ and $t = \mu_{21}\|\boldsymbol{b}_1^*\|$. By taking $\delta = 1$, we can calculate V and U by numerical integration to be $V \fallingdotseq 0.439$ and $U \fallingdotseq 0.000129$. Therefore, the probability

P satisfies

$$P < \frac{U}{V} \fallingdotseq \frac{0.000129}{0.439} \fallingdotseq 2.94 \times 10^{-4}.$$

□

According to this proof, we have theoretically obtained that a random LLL-reduced basis contains the shortest vector with high probability, *i.e.* more than 99.9%, by taking a factor δ close to 1.

4.3 Monte Carlo Simulation

We estimate the failure probability P in Theorem 5 by using a Monte Carlo simulation. Under $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$, the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is represented as follows:

$$\boldsymbol{b}_1 = \begin{pmatrix} \|\boldsymbol{b}_1^*\| \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{b}_2 = \begin{pmatrix} \mu_{21}\|\boldsymbol{b}_1^*\| \\ \|\boldsymbol{b}_2^*\| \\ 0 \end{pmatrix}, \quad \boldsymbol{b}_3 = \begin{pmatrix} \mu_{31}\|\boldsymbol{b}_1^*\| \\ \mu_{32}\|\boldsymbol{b}_2^*\| \\ \frac{1}{\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|} \end{pmatrix}.$$

Since it is too difficult to sample an LLL-reduced basis uniformly at random, we use the sampling which is not uniformly at random in reality. Therefore, we merely calculate the approximate value of the failure probability by Monte Carlo simulation. In our experiment, in order to sample LLL-reduced bases as uniformly random as possible under $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$, we first sample lattice bases as uniformly random as possible so that the sampling domain contains almost all LLL-reduced bases. Then we check whether the sampled bases are LLL-reduced or not. Finally we check whether the sampled LLL-reduced bases contain the shortest vector or not. For the purpose, we first sample $\|\boldsymbol{b}_1^*\|$ in a range $[0.0, 1.3]$, $\|\boldsymbol{b}_2^*\|$ in $[0.0, 10.0]$, $\mu_{21}\|\boldsymbol{b}_1^*\|$ and $\mu_{31}\|\boldsymbol{b}_1^*\|$ in $[-0.65, 0.65]$, and $\mu_{32}\|\boldsymbol{b}_2^*\|$ in $[-5.0, 5.0]$ by using Mersenne twister [25]. We set the upper bounds of $\mu_{21}\|\boldsymbol{b}_1^*\|$, $\mu_{31}\|\boldsymbol{b}_1^*\|$, and $\mu_{32}\|\boldsymbol{b}_2^*\|$ due to the size reduction $|\mu_{21}| \leq \frac{1}{2}$, $|\mu_{31}| \leq \frac{1}{2}$, and $|\mu_{32}| \leq \frac{1}{2}$. The range of $\|\boldsymbol{b}_1^*\|$ is adequate because $\|\boldsymbol{b}_1^*\| \leq \frac{2}{\sqrt{3}} < 1.3$ if $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ is LLL-reduced and $\|\boldsymbol{b}_1^*\|\|\boldsymbol{b}_2^*\|\|\boldsymbol{b}_3^*\| = 1$. Although $\|\boldsymbol{b}_2^*\|$ is not bounded above by a constant which is independent of $\|\boldsymbol{b}_1^*\|$, we need to bound the range of $\|\boldsymbol{b}_2^*\|$ to demonstrate our experiment. To be precise, we also tried the experiment with a larger bound of $\|\boldsymbol{b}_2^*\|$; however, in this case sampled lattice bases are not LLL-reduced with high probability. In our experiment with the upper bound $\|\boldsymbol{b}_2^*\| \leq 10.0$, we sampled 76,429,270,520 bases and there were 60,000,000 LLL-reduced bases, of which 8,736 contained no shortest vector. This approximate failure probability is $\frac{8{,}736}{60{,}000{,}000} \simeq 1.46 \times 10^{-4}$. In addition, in the case the upper bound of $\|\boldsymbol{b}_2^*\| \leq 40.0$, we sampled 12,236,665,172 bases and there were 600,000 LLL-reduced bases, of which 77 contained no shortest vector. This approximate failure probability is $\frac{77}{600{,}000} \simeq 1.28 \times 10^{-4}$. The approximate failure probabilities in both experiments are almost the same. Therefore, we consider 10.0 is sufficient for the upper bound of $\|\boldsymbol{b}_2^*\|$ and we used 10.0 as the upper bound. From above, the approximate value of P is $\frac{8{,}736}{60{,}000{,}000} \simeq 1.46 \times 10^{-4}$. The upper bound of P in Theorem 5 is of the same magnitude as the above value. More precisely, the upper bound of the failure probability in Theorem 5 is about twice as large as the value obtained by Monte Carlo simulation.

5. Conclusion

We studied the explicit relation between LLL-reduced bases and the shortest vectors in three, four and five dimensions. We presented a necessary and sufficient condition that the output of the LLL algorithm does not contain the shortest vector in three dimensions for $\frac{7}{12} \leq \delta \leq 1$. From this condition, we can construct the reduction algorithm for solving SVP with probability 1 by slightly modifying the LLL algorithm (by checking a few integer linear combinations of the output). Moreover, we analyzed the probability that a basis does not contain the shortest vector in three dimensions. We proved the upper bound of the failure probability is 2.94×10^{-4} for $\delta = 1$ by evaluating the volume of space that satisfies the above necessary and sufficient conditions. In the case of four and five dimensions, we presented the necessary and sufficient conditions for $\delta = 1$ similar to the one in three dimensions.

It is interesting open problem that investigate the explicit relation of LLL-reduced bases in more than five dimensions and possibly an asymptotic case. As we claimed in Section 3.3, the extension in an asymptotic case should rely on some heuristic assumptions. If we obtain such extensions under mild assumptions, the result should be interesting. Furthermore, analogous analysis for BKZ-reduced bases is also an interesting open problem.

Acknowledgements

We would like to thank anonymous reviewers of this journal for their insightful comments to improve the paper. This work was supported by JST CREST Grant Number JPMJCR14D6, Japan.

References

[1] M. Ajtai, "The shortest vector problem in L_2 is *NP*-hard for randomized reductions (extended abstract)," Proc. STOC 1998, J.S. Vitter, ed., pp.10–19, ACM, 1998.

[2] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," Proc. STOC 2001, J.S. Vitter, P.G. Spirakis, and M. Yannakakis, eds., pp.601–610, ACM, 2001.

[3] A. Akhavi, "The optimal LLL algorithm is still polynomial in fixed dimension," Theor. Comput. Sci., vol.297, no.1-3, pp.3–23, 2003.

[4] S. Alsayigh, J. Ding, T. Takagi, and Y. Wang, "The beauty and the beasts - The hard cases in LLL reduction," Proc. IWSEC 2017, S. Obana and K. Chida, eds., LNCS 10418, pp.19–35, Springer, 2017.

[5] Y. Aono and P.Q. Nguyen, "Random sampling revisited: Lattice enumeration with discrete pruning," Proc. EUROCRYPT 2017, J. Coron and J.B. Nielsen, eds., LNCS 10211, pp.65–102, 2017.

[6] Y. Aono, Y. Wang, T. Hayashi, and T. Takagi, "Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator," Proc. EUROCRYPT 2016, M. Fischlin and J. Coron, eds., LNCS 9665, pp.789–819, Springer, 2016.

[7] A. Becker, L. Ducas, N. Gama, and T. Laarhoven, "New directions in nearest neighbor searching with applications to lattice sieving," Proc. SODA 2016, R. Krauthgamer, ed., pp.10–24, SIAM, 2016.

[8] Y. Chen and P.Q. Nguyen, "BKZ 2.0: Better lattice security estimates," Proc. ASIACRYPT 2011, D.H. Lee and X. Wang, eds., LNCS 7073, pp.1–20, Springer, 2011.

[9] L. Ducas, "Shortest vector from lattice sieving: A few dimensions for free," Proc. EUROCRYPT 2018, J.B. Nielsen and V. Rijmen, eds., LNCS 10820, pp.125–145, Springer, 2018.

[10] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," Math. Comput., vol.44, no.170, pp.463–471, April 1985.

[11] M. Fukase and K. Kashiwabara, "An accelerated algorithm for solving SVP based on statistical analysis," JIP, vol.23, no.1, pp.67–80, 2015.

[12] N. Gama, N. Howgrave-Graham, H. Koy, and P.Q. Nguyen, "Rankin's constant and blockwise lattice reduction," Proc. CRYPTO 2006, C. Dwork, ed., LNCS 4117, pp.112–130, Springer, 2006.

[13] N. Gama and P.Q. Nguyen, "Finding short lattice vectors within mordell's inequality," Proc. STOC 2008, C. Dwork, ed., pp.207–216, ACM, 2008.

[14] N. Gama, P.Q. Nguyen, and O. Regev, "Lattice enumeration using extreme pruning," Proc. EUROCRYPT 2010, H. Gilbert, ed., LNCS 6110, pp.257–278, Springer, 2010.

[15] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proc. STOC 2009, M. Mitzenmacher, ed., pp.169–178, ACM, 2009.

[16] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," Proc. STOC 2008, C. Dwork, ed., pp.197–206, ACM, 2008.

[17] G. Hanrot, X. Pujol, and D. Stehlé, "Analyzing blockwise lattice algorithms using dynamical systems," Proc. CRYPTO 2011, P. Rogaway, ed., LNCS 6841, pp.447–464, Springer, 2011.

[18] S. Khot, "Hardness of approximating the shortest vector problem in lattices," J. ACM, vol.52, no.5, pp.789–808, 2005.

[19] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol.48, no.177, pp.203–209, 1987.

[20] R. Kannan, "Improved algorithms for integer programming and related lattice problems," Proc. STOC'83. D.S. Johnson, R. Fagin, M.L. Fredman,, D. Harel, R.M. Karp, N.A. Lynch, C.H. Papadimitriou, R.L. Rivest, W.L. Ruzzo, and J.I. Seiferas, eds., pp.193–206, ACM, 1983.

[21] T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," Proc. CRYPTO 2015, R. Gennaro and M. Robshaw, eds., LNCS 9215, pp.3–22, Springer, 2015.

[22] T. Laarhoven and A. Mariano, "Progressive lattice sieving," Proc. PQCrypto 2018, T. Lange and R. Steinwandt, eds., LNCS 10786, pp.292–311, Springer, 2018.

[23] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Math. Ann., vol.261, no.4, pp.515–534, 1982.

[24] Y. Matsuda, T. Teruya, and K. Kashiwabara, "Estimation of the success probability of random sampling by the gram-charlier approximation," IACR Cryptology ePrint Archive 2018, 815, 2018.

[25] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," ACM Trans. Model. Comput. Simul., vol.8, no.1, pp.3–30, 1998.

[26] D. Micciancio and P. Voulgaris, "A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations," Proc. STOC 2010, L.J. Schulman, ed., pp.351–358, ACM, 2010.

[27] D. Micciancio and P. Voulgaris, "Faster exponential time algorithms for the shortest vector problem," Proc. SODA 2010, M. Charikar, ed., pp.1468–1480, SIAM, 2010.

[28] D. Micciancio and M. Walter, "Practical, predictable lattice basis reduction," Proc. EUROCRYPT 2016, M. Fischlin and J. Coron, eds., LNCS 9665, pp.820–849, Springer, 2016.

[29] V.S. Miller, "Use of elliptic curves in cryptography," Proc. CRYPTO'85, H.C. Williams, ed., LNCS 218, pp.417–426, Springer, 1985.

[30] A. Neumaier and D. Stehlé, "Faster LLL-type reduction of lattice bases," Proc. ISSAC 2016, S.A. Abramov, E.V. Zima, and X. Gao, eds., pp.373–380, ACM, 2016.

[31] P.Q. Nguyen, "Hermite's constant and lattice algorithms," The LLL Algorithm - Survey and Applications, P.Q. Nguyen and B. Vallée, eds., Information Security and Cryptography, pp.19–69, Springer, 2010.

[32] P.Q. Nguyen and D. Stehlé, "Floating-point LLL revisited," Proc. EUROCRYPT 2005, R. Cramer, ed., LNCS 3494, pp.215–233, Springer, 2005.

[33] P.Q. Nguyen and D. Stehlé, "Low-dimensional lattice basis reduction revisited," ACM Trans. Algorithms, vol.5, no.4, pp.46:1–46:48, 2009.

[34] P.Q. Nguyen T. Vidick, "Sieve algorithms for the shortest vector problem are practical," J. Mathematical Cryptology, vol.2, no.2., pp.181–207, 2008.

[35] A. Novocin, D. Stehlé, and G. Villard, "An LLL-reduction algorithm with quasi-linear time complexity: Extended abstract," Proc. STOC 2011, L. Fortnow and S.P. Vadhan, eds., pp.403–412, ACM, 2011.

[36] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol.56, no.6, pp.34:1–34:40, 2009.

[37] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, 1978.

[38] C. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," Theor. Comput. Sci., vol.53, no.2-3, pp.201–224, 1987.

[39] C. Schnorr, "Lattice reduction by random sampling and birthday methods," Proc. STACS 2003, H. Alt and M. Habib, eds., LNCS 2607, pp.145–156, Springer, 2003.

[40] C. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," Math. Program., vol.66, no.1-3, pp.181–199, 1994.

[41] I.A. Semaév, "A 3-dimensional lattice reduction algorithm," Proc. CaLC 2001, J.H. Silverman, ed., LNCS 2146, pp.181–193, Springer, 2001.

[42] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol.26, no.5, pp.1484–1509, 1997.

[43] T. Teruya, "An observation on the randomness assumption over lattices," Proc. ISITA 2019, IEEE, 2018.

[44] T. Teruya, K. Kashiwabara, and G. Hanaoka, "Fast lattice basis reduction suitable for massive parallelization and its application to the shortest vector problem," Proc. PKC 2018, M. Abdalla and R. Dahab, eds., LNCS 10769, pp.437–460, Springer, 2018.

[45] J. Yamaguchi and M. Yasuda, "Explicit formula for gram-schmidt vectors in LLL with deep insertions and its applications," NuTMiC 2017, Revised Selected Papers, J. Kaczorowski, J. Pieprzyk, and J. Pomykala, eds., LNCS 10737, pp.142–160, Springer, 2017.

Appendix A: Examples of 3-Dimensional LLL-Reduced Bases Not Containing the Shortest Vector

Here, we show examples of 3-dimensional LLL-reduced bases not containing the shortest vector. If the shortest vector is $\boldsymbol{b}' = \sum_{i=1}^{3} x_i \boldsymbol{b}_i$, there are two types of LLL-reduced bases not containing the shortest vector. One satisfies $(|x_1|, |x_2|, |x_3|) = (1, 1, 1)$; the other satisfies $(|x_1|, |x_2|, |x_3|) = (0, 1, 1)$.

A.1 Example for $(|x_1|, |x_2|, |x_3|) = (0, 1, 1)$

The following LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ ensures that

$\boldsymbol{b}_2 + \boldsymbol{b}_3$ is the shortest in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$.

$$\begin{pmatrix} \boldsymbol{b}_1^\top \\ \boldsymbol{b}_2^\top \\ \boldsymbol{b}_3^\top \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 \\ -\frac{1}{3} & -\frac{\sqrt{2}}{3} & \frac{\sqrt{6}}{3} \end{pmatrix}$$

A.2 Example for $(|x_1|, |x_2|, |x_3|) = (1, 1, 1)$

The following LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$ ensures that $\boldsymbol{b}_1 + \boldsymbol{b}_2 + \boldsymbol{b}_3$ is the shortest in the lattice $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3)$.

$$\begin{pmatrix} \boldsymbol{b}_1^\top \\ \boldsymbol{b}_2^\top \\ \boldsymbol{b}_3^\top \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ -\frac{1}{2} & -\frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}$$

Appendix B: Summary of the Proofs of Theorems 3 and 4

In this section, we show the proofs of Theorems 3 and 4. The strategy is similar to Theorem 1 in three dimensions.

B.1 Proof of Theorem 3

Suppose a 4-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ does not contain the shortest non-zero vector and one of the shortest non-zero vector is $\boldsymbol{b}' = \sum_{i=1}^4 x_i \boldsymbol{b}_i$. From the size reduction, the Lovász condition, and $\lambda_1(L) < \|\boldsymbol{b}_1\|$, if $\boldsymbol{b}' = \sum_{i=1}^4 x_i \boldsymbol{b}_i$ is the shortest (non-zero), we can reduce the canditates of the possible integer coefficients (x_1, x_2, x_3, x_4). If $x_4 = 0$ holds, this case resolves itself into Theorem 1 in three dimensions. Therefore, we consider $x_4 \neq 0$.

By using the size reduction and the Lovász condition, we have

$$\begin{aligned} \|\sum_{i=1}^{4} x_i \boldsymbol{b}_i\|^2 \geq \quad & \max(0, |x_1| - \frac{1}{2}\sum_{i=2}^{4}|x_i|)^2 \|\boldsymbol{b}_1^*\|^2 \\ & + \max(0, |x_2| - \frac{1}{2}\sum_{i=3}^{4}|x_i|)^2 \|\boldsymbol{b}_2^*\|^2 \\ & + \max(0, |x_3| - \frac{1}{2}\sum_{i=4}^{4}|x_i|)^2 \|\boldsymbol{b}_3^*\|^2 \\ & + |x_4|^2 \|\boldsymbol{b}_4^*\|^2. \end{aligned}$$

In addition, $\|\boldsymbol{b}_2^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_1^*\|^2$, $\|\boldsymbol{b}_3^*\|^2 \geq \frac{9}{16}\|\boldsymbol{b}_1^*\|^2$, and $\|\boldsymbol{b}_4^*\|^2 \geq \frac{27}{64}\|\boldsymbol{b}_1^*\|^2$ hold from the size reduction and the Lovász condition. These inequalities and $\|\boldsymbol{b}'\| < \|\boldsymbol{b}_1\| = \|\boldsymbol{b}_1^*\|$ give

$$\begin{aligned} (|x_1|, |x_2|, |x_3|, |x_4|) = & (1, 0, 0, 1), (0, 0, 1, 1), (1, 0, 1, 1), \\ & (0, 1, 0, 1), (0, 1, 1, 1), (1, 1, 0, 1), \\ & (1, 1, 1, 1), (2, 1, 1, 1). \end{aligned}$$

If $(|x_1|, |x_2|, |x_3|, |x_4|) = (1, 0, 0, 1)$, $|x_1 + \mu_{41} x_4| \geq |\mu_{41} x_4|$ by size reduction. Therefore, in this case, $|x_1 \boldsymbol{b}_1 + x_4 \boldsymbol{b}_4| \geq \|\boldsymbol{b}_4\|$ holds. We can eliminate the case of $(|x_1|, |x_2|, |x_3|, |x_4|) = (1, 0, 0, 1)$.

Moreover, if $(|x_1|, |x_2|, |x_3|, |x_4|) = (2, 1, 1, 1)$ is satisfied, $|x_1 + \mu_{21}x_2 + \mu_{31}x_3 + \mu_{41}x_4| \geq \min(|1 + \mu_{21}x_2 + \mu_{31}x_3 + \mu_{41}x_4|, |-1 + \mu_{21}x_2 + \mu_{31}x_3 + \mu_{41}x_4|)$ holds by size reduction. Since $\|\sum_{i=1}^4 x_i \boldsymbol{b}_i\|^2 = (x_1 + \mu_{21}x_2 + \mu_{31}x_3 + \mu_{41}x_4)^2\|\boldsymbol{b}_1^*\|^2 + (x_2 + \mu_{32}x_3 + \mu_{42}x_4)^2\|\boldsymbol{b}_2^*\|^2 + (x_3 + \mu_{43}x_4)^2\|\boldsymbol{b}_3^*\|^2 + x_4^2\|\boldsymbol{b}_4^*\|^2$, there exists (y_1, y_2, y_3, y_4) such that $(|y_1|, |y_2|, |y_3|, |y_4|) = (1, 1, 1, 1)$ and $\|\sum_{i=1}^4 x_i \boldsymbol{b}_i\| \geq \|\sum_{i=1}^4 y_i \boldsymbol{b}_i\|$.

From the above, one of the vectors $\sum_{i=1}^4 x_i \boldsymbol{b}_i$ satisfying $(|x_1|, |x_2|, |x_3|, |x_4|) = (0, 1, 1, 0), (1, 1, 1, 0), (0, 0, 1, 1), (1, 0, 1, 1), (0, 1, 0, 1), (1, 1, 0, 1), (0, 1, 1, 1)$ or $(1, 1, 1, 1)$ is the shortest vector in $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ if the LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ does not contain the shortest vector.

In addition, we can construct an LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ such that $\sum_{i=1}^4 x_i \boldsymbol{b}_i$ is the shortest non-zero vector (x_1, x_2, x_3, x_4) satisfying the above equation (the details are available from the first author).

B.2 Proof of Theorem 4

Suppose a 5-dimensional LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$ does not contain the shortest non-zero vector, and one of the shortest non-zero vector is $\boldsymbol{b}' = \sum_{i=1}^5 x_i \boldsymbol{b}_i$. If $x_5 = 0$ holds, this case resolves itself into Theorem 3 in four dimensions. Therefore, we consider $x_5 \neq 0$. By using a similar strategy to the one taken in the proof of Theorem 3, we can reduce the canditates of the possible integer coefficients $(x_1, x_2, x_3, x_4, x_5)$ as follows:

$$\begin{aligned} & (|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = \\ & (1, 0, 0, 0, 1), (0, 1, 0, 0, 1), (0, 0, 1, 0, 1), (0, 0, 0, 1, 1), \\ & (1, 1, 0, 0, 1), (1, 0, 1, 0, 1), (1, 0, 0, 1, 1), (0, 1, 1, 0, 1), \\ & (0, 1, 0, 1, 1), (0, 0, 1, 1, 1), (1, 1, 1, 0, 1), (1, 1, 0, 1, 1), \\ & (1, 0, 1, 1, 1), (0, 1, 1, 1, 1), (1, 1, 1, 1, 1), (2, 1, 1, 1, 1), \\ & (0, 2, 1, 1, 1), (1, 2, 1, 1, 1), (2, 2, 1, 1, 1), (2, 1, 1, 0, 1), \\ & (2, 1, 0, 1, 1), (2, 0, 1, 1, 1), (3, 2, 1, 1, 1), (*, *, 2, 1, 1). \end{aligned}$$

By using a similar method as the proof of Theorem 3, we eliminate the cases of $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (1, 0, 0, 0, 1), (2, 1, 1, 0, 1), (2, 1, 0, 1, 1), (2, 0, 1, 1, 1), (3, 2, 1, 1, 1)$.

Next, we prove that $\sum_{i=1}^5 x_i \boldsymbol{b}_i$ is not the shortest non-zero vector if $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (*, *, 2, 1, 1)$ holds. We prove it by contradiction.

Assume that $\sum_{i=1}^5 x_i \boldsymbol{b}_i$ is the shortest non-zero vector and $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (*, *, 2, 1, 1)$ holds. From the size reduction and the Lovász condition, $\|\boldsymbol{b}_4^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_3^*\|^2 \geq \frac{27}{64}\|\boldsymbol{b}_1^*\|^2$, and $\|\boldsymbol{b}_5^*\|^2 \geq \frac{9}{16}\|\boldsymbol{b}_3^*\|^2 \geq \frac{81}{256}\|\boldsymbol{b}_1^*\|^2$ hold. Here, from the size reduction and $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (*, *, 2, 1, 1)$, $\|\sum_{i=1}^5 x_i \boldsymbol{b}_i\|^2 \geq \|\boldsymbol{b}_3^*\|^2 + \frac{1}{4}\|\boldsymbol{b}_4^*\|^2 + \|\boldsymbol{b}_5^*\|^2$ holds. Therefore, $\|\sum_{i=1}^5 x_i \boldsymbol{b}_i\|^2 \geq \frac{7}{4}\|\boldsymbol{b}_3^*\|^2 \geq \frac{63}{64}\|\boldsymbol{b}_1^*\|^2$.

Moreover, since $\sum_{i=1}^5 x_i \boldsymbol{b}_i$ is the shortest non-zero vector, $\|\sum_{i=1}^5 x_i \boldsymbol{b}_i\| < \|\boldsymbol{b}_1\|$ holds. Thus, $\frac{7}{4}\|\boldsymbol{b}_3^*\|^2 < \|\boldsymbol{b}_1^*\|^2 \Leftrightarrow \|\boldsymbol{b}_3^*\|^2 < \frac{4}{7}\|\boldsymbol{b}_1^*\|^2$. In addition, since $\|\boldsymbol{b}_3^*\|^2 \geq \frac{3}{4}\|\boldsymbol{b}_2^*\|^2$,

$\|\boldsymbol{b}_2^*\|^2 < \frac{16}{21}\|\boldsymbol{b}_1^*\|^2$ holds. Moreover, from the size reduction and the Lovász condition, $\frac{9}{16}\|\boldsymbol{b}_1^*\|^2 \leq \|\boldsymbol{b}_3^*\|^2 < \frac{4}{7}\|\boldsymbol{b}_1^*\|^2$ and $\frac{3}{4}\|\boldsymbol{b}_1^*\|^2 \leq \|\boldsymbol{b}_2^*\|^2 < \frac{16}{21}\|\boldsymbol{b}_1^*\|^2$.

Since $\|\sum_{i=1}^5 x_i\boldsymbol{b}_i\|^2 < \|\boldsymbol{b}_3\|^2 = |\mu_{31}|^2\|\boldsymbol{b}_1^*\|^2 + |\mu_{32}|^2\|\boldsymbol{b}_2^*\|^2 + \|\boldsymbol{b}_3^*\|^2$ holds, $|\mu_{31}|^2\|\boldsymbol{b}_1^*\|^2 + |\mu_{32}|^2\|\boldsymbol{b}_2^*\|^2 + \|\boldsymbol{b}_3^*\|^2 > \frac{7}{4}\|\boldsymbol{b}_3^*\|^2$. Thus, $|\mu_{31}|^2\|\boldsymbol{b}_1^*\|^2 > \frac{7}{4}\|\boldsymbol{b}_3^*\|^2 - \frac{1}{4}\|\boldsymbol{b}_2^*\|^2 > \frac{311}{1344}\|\boldsymbol{b}_1^*\|^2$ holds. From the size condition, $|\mu_{31}|^2\|\boldsymbol{b}_1^*\|^2 \leq \frac{1}{4}\|\boldsymbol{b}_1^*\|^2$ holds.

From the size reduction and the Lovász condition, we have $\|\boldsymbol{b}_1^*\|^2 - \|\boldsymbol{b}_2^*\|^2 \leq |\mu_{21}|^2\|\boldsymbol{b}_1^*\|^2 \leq \frac{1}{4}\|\boldsymbol{b}_1^*\|^2 \Leftrightarrow \frac{5}{21}\|\boldsymbol{b}_1^*\|^2 \leq |\mu_{21}|^2\|\boldsymbol{b}_1^*\|^2 \leq \frac{1}{4}\|\boldsymbol{b}_1^*\|^2$. Similarly, $\frac{5}{28}\|\boldsymbol{b}_1^*\|^2 \leq |\mu_{32}|^2\|\boldsymbol{b}_2^*\|^2 \leq \frac{4}{21}\|\boldsymbol{b}_1^*\|^2$ holds.

From the above, we have

$$\begin{aligned}
\sqrt{\frac{3}{4}}\|\boldsymbol{b}_1^*\| \leq \|\boldsymbol{b}_2^*\| &< \sqrt{\frac{16}{21}}\|\boldsymbol{b}_1^*\|,\\
\frac{3}{4}\|\boldsymbol{b}_1^*\| \leq \|\boldsymbol{b}_3^*\| &< \sqrt{\frac{4}{7}}\|\boldsymbol{b}_1^*\|,\\
\sqrt{\frac{5}{21}}\|\boldsymbol{b}_1^*\| < |\mu_{21}|\|\boldsymbol{b}_1^*\| &\leq \frac{1}{2}\|\boldsymbol{b}_1^*\|,\\
\sqrt{\frac{311}{1344}}\|\boldsymbol{b}_1^*\| < |\mu_{31}|\|\boldsymbol{b}_1^*\| &\leq \frac{1}{2}\|\boldsymbol{b}_1^*\|,\\
\sqrt{\frac{5}{28}}\|\boldsymbol{b}_1^*\| < |\mu_{32}|\|\boldsymbol{b}_2^*\| &< \sqrt{\frac{4}{21}}\|\boldsymbol{b}_1^*\|.
\end{aligned}$$

Here, a simple calculation obtains

$$\min(\|\boldsymbol{b}_1 \pm \boldsymbol{b}_2 \pm \boldsymbol{b}_3\|^2, \|\boldsymbol{b}_2 \pm \boldsymbol{b}_3\|^2) < \frac{63}{64}\|\boldsymbol{b}_1^*\|^2.$$

However, this equation contradicts that $\sum_{i=1}^5 x_i\boldsymbol{b}_i$ is the shortest since $\|\sum_{i=1}^5 x_i\boldsymbol{b}_i\|^2 \geq \frac{63}{64}\|\boldsymbol{b}_1^*\|^2$.

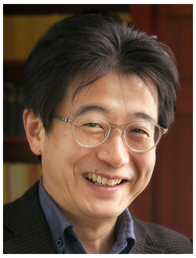
From the above, $\sum_{i=1}^5 x_i\boldsymbol{b}_i$ is not the shortest non-zero vector if $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (*, *, 2, 1, 1)$ holds.

Therefore, if $\sum_{i=1}^5 x_i\boldsymbol{b}_i$ is the shortest non-zero vector and $x_5 \neq 0$, $(x_1, x_2, x_3, x_4, x_5)$ satisfies that $(|x_1|, |x_2|, |x_3|, |x_4|, |x_5|) = (0, 1, 0, 0, 1), (0, 0, 1, 0, 1), (0, 0, 0, 1, 1), (1, 1, 0, 0, 1), (1, 0, 1, 0, 1), (1, 0, 0, 1, 1), (0, 1, 1, 0, 1), (0, 1, 0, 1, 1), (0, 0, 1, 1, 1), (1, 1, 1, 0, 1), (1, 1, 0, 1, 1), (1, 0, 1, 1, 1), (0, 1, 1, 1, 1), (1, 1, 1, 1, 1), (2, 1, 1, 1, 1), (0, 2, 1, 1, 1), (1, 2, 1, 1, 1), (2, 2, 1, 1, 1)$.

For each case, we can construct an LLL-reduced basis $(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5)$ that $\sum_{i=1}^5 x_i\boldsymbol{b}_i$ is the shortest non-zero vector (the details are available from the first author).

Kotaro Matsuda received his B.E. in mathematical engineering and information physics from the University of Tokyo in 2018. He is a master course student in the Graduate School of Information Science and Technology at the University of Tokyo. His current research interests are algorithms and data structures.

Atsushi Takayasu received his B.E. in mathematical engineering and information physics from the University of Tokyo in 2012, M.S. and Ph.D. in complexity science and engineering from the University of Tokyo in 2014 and 2017. He was a JSPS Research Fellow (DC1) during his Ph.D. course. He is currently an assistant professor in the Graduate School of Information Science and Technology at the University of Tokyo, a Collaborative Researcher in National Institute of Advanced Industrial Science and Technology. He received Best Student Paper Award in ACISP 2016. His research interest includes cryptography and information security.



Tsuyoshi Takagi received the B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He was engaged in research on network security at NTT Laboratories from 1995 to 2001. He received the Ph.D. from the Technical University of Darmstadt in 2001. He was an Assistant Professor in the Department of Science at Technical University of Darmstadt until 2005. He was a Professor at Kyushu University until 2018. He is currently a Professor in the Graduate School of Information Science and Technology at University of Tokyo. His current research interests are information security and cryptography. He received DOCOMO Mobile Science Award in 2013, IEICE Achievement Award in 2013, and JSPS Prize in 2014. Dr. Takagi was a Program Chair of the 7th International Conference on Post-Quantum Cryptography, PQCrypto 2016.