J. Korean Math. Soc. **59** (2022), No. 6, pp. 1047–1065
https://doi.org/10.4134/JKMS.j210496
pISSN: 0304-9914 / eISSN: 2234-3008

ON PAIRWISE GAUSSIAN BASES AND LLL ALGORITHM FOR THREE DIMENSIONAL LATTICES

Kitae Kim, Hyang-Sook Lee, Seongan Lim, Jeongeun Park, and Ikkwon Yie

Abstract. For two dimensional lattices, a Gaussian basis achieves all two successive minima. For dimension larger than two, constructing a pairwise Gaussian basis is useful to compute short vectors of the lattice. For three dimensional lattices, Semaev showed that one can convert a pairwise Gaussian basis to a basis achieving all three successive minima by one simple reduction. A pairwise Gaussian basis can be obtained from a given basis by executing Gauss algorithm for each pair of basis vectors repeatedly until it returns a pairwise Gaussian basis. In this article, we prove a necessary and sufficient condition for a pairwise Gaussian basis to achieve the first k successive minima for three dimensional lattices for each $k \in \{1, 2, 3\}$ by modifying Semaev's condition. Our condition directly checks whether a pairwise Gaussian basis contains the first k shortest independent vectors for three dimensional lattices. LLL is the most basic lattice basis reduction algorithm and we study how to use LLL to compute a pairwise Gaussian basis. For $\delta \geq 0.9$, we prove that LLL(δ) with an additional simple reduction turns any basis for a three dimensional lattice into a pairwise SV-reduced basis. By using this, we convert an LLL reduced basis to a pairwise Gaussian basis in a few simple reductions. Our result suggests that the LLL algorithm is quite effective to compute a basis with all three successive minima for three dimensional lattices.

1. Introduction

A lattice L in the Euclidean space $\mathbb{R}^m$ is a discrete subgroup of $\mathbb{R}^m$. It is usually represented by a basis which is a set of linearly independent vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset \mathbb{R}^m$, $n \leq m$. Since a lattice is a discrete space, there is a shortest non-zero vector measured by the Euclidean norm. The algorithms BKZ [3] and LLL [7] compute bases with relatively short vectors in a polynomial time in n and $\log_2 B$, where B is the maximum norm of the vectors in the input basis.

The problem of finding a shortest nonzero vector is called the shortest vector problem (SVP). SVP is a very interesting computational problem of lattices

Received August 13, 2021; Accepted July 28, 2022.
2020 *Mathematics Subject Classification.* Primary 58B34, 58J42, 81T75.
Key words and phrases. Lattice, pairwise-Gaussian basis, lattice basis reduction, LLL.

since the security of lattice based cryptography relies on the hardness of it. Ajtai proved that the SVP is an NP-hard problem under randomized reductions [1]. We say that a basis is SV-reduced if the basis contains a shortest nonzero vector of the lattice.

For two dimensional lattices, the problem of computing a SV-reduced basis is completely solved by Gauss algorithm, whose output we call the Gaussian basis. The pairwise Gaussian property played an important role in finding shortest vector of lattices (e.g. Gauss Sieve) [8]. Currently, the only known method of constructing a pairwise Gaussian basis is to run Gauss algorithm for each pair of basis vectors repeatedly until it returns a pairwise Gaussian basis. In practice, it is known that it only requires a small number of calls for Gauss algorithm to get a pairwise Gaussian for any dimension.

For three dimensional lattices, Semaev proved that if a pairwise Gaussian basis satisfies a certain condition, then the basis achieves all three successive minima of the lattice [11]. In [11], Semaev presented an algorithm to compute a basis with three successive minima directly in $O((\log_2 B)^2)$ bit operations. Semaev also shows that repeating Gauss algorithm naively gives a pairwise Gaussian basis in $O((\log_2 B)^3)$ bit operations.

In this article, we study pairwise Gaussian bases for three dimensional lattices. We note that the condition given by Semaev is for a basis to achieve all three successive minima and we observe that Semaev's condition can be refined for each successive minimum. From this observation, we present a necessary and sufficient condition for a pairwise Gaussian basis to achieve the first k successive minima for three dimensional lattices for each $k \in \{1, 2, 3\}$. Our condition checks whether a pairwise Gaussian basis contains a shortest nonzero vector, or first two independent shortest vectors, or all three independent shortest vectors for a three dimensional lattice. We also show how to use the LLL algorithm to compute a pairwise Gaussian basis. Since the proven complexity of LLL algorithm is known to be $O((\log_2 B)^3)$ bit operations, the asymptotic complexity is not improved from repeating Gauss algorithm. However, considering the fact that LLL algorithm works better in practice than the proven complexity, constructing an LLL-based make-pairwise-Gaussian algorithm is interesting. We first present an algorithm, LLLG(δ), which outputs a pairwise Gaussian basis with 99% probability according to experimental results (by Python software) for $\delta \geq 0.92$. We prove that the output of LLLG(δ) algorithm is a pairwise SV-reduced basis if $\delta \geq 0.9$. This fact allows us to present Algorithm 6, which computes a pairwise Gaussian basis using LLL with additional simple reductions. And our Algorithm 6 together with Algorithm 3 can be used to compute a basis that achieves the first k successive minima for any $k \leq 3$ efficiently in three dimensional lattices. According to [9], computing a good color transform matrix requires to compute a SV-reduced basis in a three dimensional lattice. And our LLL-based reduction algorithm can be directly applied to this case.

The rest of the article is organized as follows. In Section 2, we review some basics of lattice, Gaussian bases, pairwise Gaussian bases and the lattice basis

reduction algorithm LLL. In Section 3, we present our main results. We prove a necessary and sufficient condition for a pairwise Gaussian basis to achieve the first k successive minima for three dimensional lattices for each $k \in \{1, 2, 3\}$. We prove that three dimensional LLL(δ) algorithm outputs pairwise SV-reduced in one simple reduction and, by using this, we present how to convert an LLL reduced basis to a pairwise Gaussian basis efficiently in a few simple reduction in Algorithm 6. In Subsection 3.3, we present our experimental results by using Python. And the conclusion is in Section 4.

2. Preliminaries

In this section, we review some basic concepts on lattices and the notions used throughout this paper. We use column representation of vectors and define the length of a vector $\mathbf{v} \in \mathbb{R}^m$ as the standard Euclidean norm $\|\mathbf{v}\| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$. We denote by $\lceil x \rfloor$ the nearest integer of $x \in \mathbb{R}$. The sign function $\mathrm{sign}(x)$ denotes the sign of a real number x (i.e., $x = \mathrm{sign}(x) \cdot |x|$). We denote $\log_2$ as log.

Definition 2.1 (Lattice)**.** Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$ be a set of linearly independent vectors, where $n \leq m$. The lattice L generated by $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is the set of linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ with coefficients in $\mathbb{Z}$,

$$L = \{a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n : a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

A basis for L is any set of independent vectors that generates L. The dimension of L is the number of vectors in a basis for L. We denote a basis as $(\mathbf{v}_1, \ldots, \mathbf{v}_n)_{\leq}$ if $\|\mathbf{v}_i\| \leq \|\mathbf{v}_{i+1}\|$ for all $i = 1, \ldots, n-1$.

There are two types of geometric invariants for lattices. One is the determinant $\det(L)$ of the lattice L, which is defined as the volume of the n-dimensional fundamental parallelepiped spanned by any basis of the lattice. The determinant $\det(L)$ is easy to compute from any basis. The other is the first minimum $\lambda_1(L)$ of the lattice L, which is the size (Euclidean norm) of a shortest nonzero vector of the lattice. The first minimum of a lattice is extremely hard to compute in general and the security of lattice based cryptography relies on its hardness.

A common strategy for computing shortest vectors of lattices is developing practical algorithms for computing a basis with relatively short vectors and developing algorithm for computing nonzero shortest vectors from the basis.

The LLL-reduced basis is the basic notion of a relatively good basis which can be computed efficiently for a general lattice [7]. In [7], Lenstra, Lenstra, Lovász presented the LLL algorithm that turns any basis into an LLL-reduced basis efficiently. The notion of LLL-reduced basis involves with Gram-Schmidt Orthogonalization (GSO) for vectors, which is explained as follows:

Definition 2.2 (GSO)**.** Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of a lattice L. The Gram-Schmidt Orthogonalization (GSO) of $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ is $(\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*)$, computed as

follows:

$$\mathbf{v}_1^* = \mathbf{v}_1,$$
$$\mathbf{v}_i^* = \mathbf{v}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{v}_j^* \quad (2 \le i \le n) \text{ where } \mu_{i,j} = \frac{\mathbf{v}_i \cdot \mathbf{v}_j^*}{\mathbf{v}_j^* \cdot \mathbf{v}_j^*}.$$

The definition of the LLL-reduced basis has a parameter $\delta \in (\frac{1}{4}, 1]$.

Definition 2.3 (LLL(δ)-reduced basis)**.** A basis $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ for an n-dimensional lattice, with its GSO $(\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*)$, is LLL($\delta$)-reduced if it satisfies the following conditions:

- (Size reduction) $|\mu_{i,j}| = \frac{|\mathbf{v}_i \cdot \mathbf{v}_j^*|}{\mathbf{v}_j^* \cdot \mathbf{v}_j^*} \le \frac{1}{2}$ for all $1 \le j < i \le n$.
- (Lovász condition) $\|\mathbf{v}_i^*\|^2 \ge (\delta - \mu_{i,i-1}^2)\|\mathbf{v}_{i-1}^*\|^2$ for all $1 < i \le n$.

The quality of LLL(δ)-reduced basis is proven as follows:

Theorem 2.4 ([5])**.** *Every LLL(δ)-reduced basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ of a lattice L has the following properties*;

$$\prod_{i=1}^{n} \|\mathbf{v}_i\| \le \alpha^{\frac{n(n-1)}{4}} \det(L) \text{ and } \min_{1 \le i \le n} \{\|\mathbf{v}_i\|\} \le \alpha^{\frac{(n-1)}{2}} \cdot \lambda_1(L)$$

with $\alpha = \frac{1}{\delta - \frac{1}{4}}$ for $\delta \in (\frac{1}{4}, 1]$.

In particular, the size of a shortest vector in any LLL(δ)-reduced basis for three dimensional lattices is estimated as follows:

Corollary 2.5 ([5])**.** *Every LLL(δ)-reduced basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of a lattice L satisfies the followings*:

$$\prod_{i=1}^{3} \|\mathbf{v}_i\| \le \alpha^{\frac{3}{2}} \det(L) \text{ and } \min_{1 \le i \le 3} \{\|\mathbf{v}_i\|\} \le \alpha \cdot \lambda_1(L).$$

From Corollary 2.5, we see that every LLL(1)-reduced basis for three dimensional lattices contains a vector whose Euclidean norm is very close to the first minimum, but it is not easy to convince whether it contains a shortest non-zero vector of the lattice.

We recall the definition of the successive minimum, which is a generalized notion of the first minimum.

Definition 2.6 (Successive minimum)**.** The i-th successive minimum $\lambda_i(L)$ of a lattice L is the smallest real number r such that there are i linearly independent vectors in L of length at most r;

$$\lambda_i(L) = \inf\left\{r \mid \dim(\mathsf{span}(L \cap \bar{\mathbf{B}}(\mathbf{0}, r))) \ge i\right\},$$

where $\bar{\mathbf{B}}(\mathbf{0}, r) = \{\mathbf{x} \in \mathbb{R}^m \mid \|\mathbf{x}\| \le r\}$ is the closed ball of radius r around $\mathbf{0}$. We say that a basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)_{\le}$ of L achieves the first minimum or SV-reduced if $\|\mathbf{v}_1\| = \lambda_1(L)$.

It is known that there is a lattice L with no basis of L achieves all the successive minima of L if the dimension is larger than four. The Minkowski reduced basis is known to achieve all the successive minima up to dimension four and the definition of the Minkowski reduced basis is given as follows.

Definition 2.7 (Minkowski reduced basis [10])**.** An ordered basis $(\mathbf{v}_1, \ldots, \mathbf{v}_n)_{\leq}$ of a lattice L is Minkowski-reduced if and only if for all $1 \leq i \leq n$, the vector $\mathbf{v}_i$ has minimal norm among all lattice vectors $\mathbf{v}_i$ such that $(\mathbf{v}_1, \ldots, \mathbf{v}_i)_{\leq}$ can be extended to a basis of L.

The Gauss algorithm, Algorithm 1, computes a Minkowski reduced basis for two dimensional lattices.

Algorithm 1 Gauss algorithm [4]

Input: A basis $\{\mathbf{x}, \mathbf{y}\}$ of a lattice L in $\mathbb{Z}^2$ s.t. $\|\mathbf{x}\| \leq \|\mathbf{y}\|$
Output: A Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2)_{\leq}$ of the lattice L

Set $\mathbf{v}_1 \leftarrow \mathbf{x}$ and $\mathbf{v}_2 \leftarrow \mathbf{y}$
$\mathbf{v}_2 \leftarrow \mathbf{v}_2 - \lceil \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\mathbf{v}_1 \cdot \mathbf{v}_1} \rfloor \mathbf{v}_1$
while $\|\mathbf{v}_2\| < \|\mathbf{v}_1\|$ **do**
    Swap $\mathbf{v}_1$ and $\mathbf{v}_2$
    $\mathbf{v}_2 \leftarrow \mathbf{v}_2 - \lceil \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\mathbf{v}_1 \cdot \mathbf{v}_1} \rfloor \mathbf{v}_1$
end while
return $(\mathbf{v}_1, \mathbf{v}_2)$

We define the Gaussian basis as follows so that the output of Gauss algorithm is Gaussian. Note that the notion of Gaussian basis is equivalent to the two dimensional Minkowski-reduced basis.

Definition 2.8 (Gaussian Basis)**.** A basis $\{\mathbf{v}, \mathbf{w}\}$ is Gaussian if

$$|\mathbf{v} \cdot \mathbf{w}| \leq \frac{1}{2} \min\left(\|\mathbf{v}\|^2, \|\mathbf{w}\|^2\right), \text{ equivalently, } \|\mathbf{v} \pm \mathbf{w}\|^2 \geq \max\left(\|\mathbf{v}\|^2, \|\mathbf{w}\|^2\right).$$

Lemma 2.9 ([2])**.** *Let $B = \{\mathbf{v}, \mathbf{w}\}$ be a basis for a lattice L. Then B is Gaussian if and only if $\lambda_1(L) = \min\left(\|\mathbf{v}\|, \|\mathbf{w}\|\right)$ and $\lambda_2(L) = \max\left(\|\mathbf{v}\|, \|\mathbf{w}\|\right)$.*

For higher dimension, we define pairwise SV-reducedness and pairwise Gaussian as follows.

Definition 2.10 (Pairwise SV-reduced)**.** A basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ for a lattice L is pairwise SV-reduced if $\lambda_1(\mathbf{v}_i, \mathbf{v}_j) = \min\left(\|\mathbf{v}_i\|, \|\mathbf{v}_j\|\right)$ for $i, j = 1, \ldots, n$ with $i \neq j$.

Definition 2.11 (Pairwise Gaussian)**.** A basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ for a lattice L is pairwise Gaussian if any pair $\{\mathbf{v}_i, \mathbf{v}_j\}$ is Gaussian, that is,

$$|\mathbf{v}_i \cdot \mathbf{v}_j| \leq \frac{1}{2} \min\left(\|\mathbf{v}_i\|^2, \|\mathbf{v}_j\|^2\right) \text{ for all } i, j = 1, \ldots, n \text{ with } i \neq j.$$

From the definition, any pairwise Gaussian basis is a pairwise SV-reduced basis.

Being pairwise Gaussian does not guarantee a basis to achieve the first minimum of the lattice, even in three dimensional lattices [11]. For a three dimensional pairwise Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)_{\leq}$ with $\epsilon_{i,j} = sign(\mathbf{v}_i \cdot \mathbf{v}_j)$, the value $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3}$ takes important role for the quality of the basis. If $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} \neq -1$, by changing the signs of the vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$, we get

$$\mathbf{v}_1 \cdot \mathbf{v}_2 \geq 0,\ \mathbf{v}_1 \cdot \mathbf{v}_3 \geq 0, \text{ and } \mathbf{v}_2 \cdot \mathbf{v}_3 \geq 0.$$

This fact assures that $\|\mathbf{v}_3\| \leq \|x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \mathbf{v}_3\|$ for all $x_i \in \mathbb{Z}$. Starting with this, Semaev proved that for a pairwise Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)_{\leq}$ with $\epsilon_{i,j} = sign(\mathbf{v}_i \cdot \mathbf{v}_j)$,

$$\|\mathbf{v}_3\| \leq \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\| \text{ for } \epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$$

if and only if the basis is a Minkowski-reduced basis in [11]. Since a Minkowski-reduced basis is known to achieve all the successive minima for three dimensional, Semaev's condition is a necessary and sufficient condition for a pairwise Gaussian basis to achieve all three successive minima, that is, $\|\mathbf{v}_1\| = \lambda_1(L)$, $\|\mathbf{v}_2\| = \lambda_2(L)$ and $\|\mathbf{v}_3\| = \lambda_3(L)$. By using this, Semaev presented how to compute a basis with all the successive minima for three dimensional lattices from a pairwise Gaussian basis which can be describe in Algorithm 2.

Algorithm 2 Computing a basis with all three successive minima from a pairwise Gaussian basis [11]

Input: A pairwise Gaussian basis $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of a lattice L
Output: A basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ of L with $\lambda_i(L) = \|\mathbf{v}_i\|$ for $i = 1, 2, 3$

1: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow Ordering(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$
2: **if** $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$ and $\|\mathbf{v}_3\| > \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\|$ **do**
3: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{w}, \mathbf{v}_1, \mathbf{v}_2)$ where $\mathbf{w} = \mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3$
4: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow Ordering(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$
5: **end if**
6: **Return** $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$

Considering that a naive approach of computing a pairwise Gaussian basis is somewhat inefficient, Semaev also presented an algorithm that computes a basis with all the successive minima for three dimensional lattices.

3. Main results

In this paper, we present a refined version of the result of Semaev for a pairwise Gaussian basis for three dimensional lattices by focusing on the individual minimum. With this refinement, we can directly check if a given pairwise Gaussian basis achieves the first minimum, or the first and second minimum or all three successive minima. We also present how to use LLL algorithm to

compute a pairwise Gaussian algorithm. Therefore, our result shows how to compute a basis with all three successive minima by using LLL.

3.1. A refined condition to achieve successive minimum

Semaev presented the following necessary and sufficient condition for a pairwise Gaussian basis to achieve all three successive minima: for a pairwise Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)_{\leq}$ with $\epsilon_{i,j} = sign(\mathbf{v}_i \cdot \mathbf{v}_j)$,

$$\|\mathbf{v}_3\| \leq \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\| \text{ for } \epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$$

if and only if

$$\|\mathbf{v}_1\| = \lambda_1(L), \|\mathbf{v}_2\| = \lambda_2(L) \text{ and } \|\mathbf{v}_3\| = \lambda_3(L).$$

From Semaev's condition, we see that if $\|\mathbf{v}_3\| > \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\|$ for $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$, it does not achieve all three successive minima. In this case, it is interesting to know whether the basis is $\|\mathbf{v}_1\| = \lambda_1(L)$ or $\|\mathbf{v}_2\| = \lambda_2(L)$. The Algorithm 2 from [11] also tells that if $\|\mathbf{v}_3\| > \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\|$ for $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$, then the basis $(\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3)_{\leq} \leftarrow Ordering(\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3, \mathbf{v}_1, \mathbf{v}_2)$ achieves all three successive minima of the lattice. Therefore, we have four cases for $\mathbf{w} = \mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3$ with $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$:

- If $\|\mathbf{w}\| \geq \|\mathbf{v}_3\|$, then $\lambda_i(L) = \|\mathbf{v}_i\|$ for all $i = 1, 2, 3$.
- If $\|\mathbf{v}_3\| > \|\mathbf{w}\| \geq \|\mathbf{v}_2\|$, then $\lambda_i(L) = \|\mathbf{v}_i\|$ for $i = 1, 2$ and $\lambda_3(L) = \|\mathbf{w}\|$.
- If $\|\mathbf{v}_2\| > \|\mathbf{w}\| \geq \|\mathbf{v}_1\|$, then $\lambda_1(L) = \|\mathbf{v}_1\|$, $\lambda_2(L) = \|\mathbf{w}\|$, and $\lambda_3(L) = \|\mathbf{v}_2\|$.
- If $\|\mathbf{v}_1\| > \|\mathbf{w}\|$, then $\lambda_1(L) = \|\mathbf{w}\| < \|\mathbf{v}_1\| = \lambda_2(L)$ and $\lambda_3(L) = \|\mathbf{v}_2\|$. In this case, the basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)_{\leq}$ does not achieve the first minimum.

Therefore, we have the following refined version of Semaev's results on necessary and sufficient condition for a pairwise Gaussian basis in terms of successive minimum of the lattice.

Theorem 3.1. *Let $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)_{\leq}$ be a pairwise Gaussian basis of a lattice L and let $\epsilon_{i,j} = sign(\mathbf{v}_i \cdot \mathbf{v}_j)$. For each $k = 1, 2, 3$, the following holds.*

A necessary and sufficient condition for $\lambda_i(L) = \|\mathbf{v}_i\|$ for all $i \leq k$ is

$$\|\mathbf{v}_k\| \leq \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\| \text{ for } \epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1.$$

With this refinement, we can directly check if a given pairwise Gaussian basis achieves the first minimum, or the first and second minimum or all three successive minima. We can modify Algorithm 2 to output a SV-reduced basis (by specifying $k = 1$ at input), to achieve the first two successive minima (by specifying $k = 2$ at input), or all three successive minima (by specifying $k = 3$ at input).

We note that, for $k = 1$, Algorithm 3 outputs the input if the input basis is SV-reduced and it outputs a basis with all three successive minima if the input basis is not SV-reduced.

Example 3.2 shows that the given basis does not achieve all three minima but it achieves the first minimum or second minimum.

Algorithm 3 Reduction algorithm for a pairwise Gaussian basis

Input: A pairwise Gaussian basis $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of a lattice L and $k \in \{1, 2, 3\}$
Output: A basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ of L with $\lambda_i(L) = \|\mathbf{v}_i\|$ for $i \leq k$

1: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow Ordering(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$
2: **if** $\epsilon_{1,2} \cdot \epsilon_{1,3} \cdot \epsilon_{2,3} = -1$ and $\|\mathbf{v}_k\| > \|\mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3\|$ **do**
3: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{w}, \mathbf{v}_1, \mathbf{v}_2)$ where $\mathbf{w} = \mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3$
4: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow Ordering(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$
5: **end if**
6: **Return** $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$

Example 3.2. Let L be a lattice with the basis $B = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, where $\mathbf{v}_i$ is the i-th column vector of the following matrix:

$$\begin{bmatrix} 0 & 1 & 4 \\ -4 & 1 & -2 \\ 1 & -4 & 0 \end{bmatrix}$$

This basis B is pairwise Gaussian and

$$\|\mathbf{v}_1\|^2 = 17, \|\mathbf{v}_2\|^2 = 18, \|\mathbf{v}_3\|^2 = 20, \mathbf{v}_1 \cdot \mathbf{v}_2 = -8, \mathbf{v}_1 \cdot \mathbf{v}_3 = 8, \mathbf{v}_2 \cdot \mathbf{v}_3 = 2.$$

For $\mathbf{w} = \mathbf{v}_1 + \mathbf{v}_2 - \mathbf{v}_3 = (-3, -1, -3)$, we have

$$\|\mathbf{v}_1\| < \|\mathbf{w}\| = \sqrt{19} < \|\mathbf{v}_3\|.$$

Semaev's condition says that the basis B does not achieve all three successive minima. By Theorem 3.1, we see that the basis B achieves the first minimum and the second minimum of the lattice L. In fact, the basis $B' = (\mathbf{v}'_1, \mathbf{v}'_2, \mathbf{v}'_3)_{\leq}$ with

$$\begin{bmatrix} \mathbf{v}'_1 & \mathbf{v}'_2 & \mathbf{v}'_3 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{w} \end{bmatrix} = \begin{bmatrix} 0 & 1 & -3 \\ -4 & 1 & -1 \\ 1 & -4 & -3 \end{bmatrix}$$

achieves all three successive minima of the lattice L.

Example 3.3 shows that the output of LLL(1) does not necessarily contain a shortest non-zero vector of the lattice even in three dimensional lattices.

Example 3.3. Let L be a lattice with the LLL(1)-reduced basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$, where $\mathbf{v}_i$ is the i-th column vector of the following matrix:

$$\begin{bmatrix} -27 & 38 & 19 \\ -84 & -46 & -63 \\ 16 & 72 & -68 \end{bmatrix}$$

Now we explain how to check the basis given in Example 3.3 does not contain a shortest non-zero vector of the lattice and how to get a basis that contains a shortest non-zero vector of the lattice.

This basis is pairwise Gaussian since

$$\|\mathbf{v}_1\|^2 = 8041 \leq \|\mathbf{v}_2\|^2 = 8744 \leq \|\mathbf{v}_3\|^2 = 8954$$

and

$$\frac{|\mathbf{v}_1 \cdot \mathbf{v}_2|}{\|\mathbf{v}_1\|^2} = 0.49,\ \frac{|\mathbf{v}_1 \cdot \mathbf{v}_3|}{\|\mathbf{v}_1\|^2} = 0.45,\ \frac{|\mathbf{v}_2 \cdot \mathbf{v}_3|}{\|\mathbf{v}_2\|^2} = 0.14.$$

By Theorem 3.1, we see that the basis does not achieve the first minimum. More precisely,

$$\mathbf{w} = \mathbf{v}_1 - \epsilon_{1,2}\mathbf{v}_2 - \epsilon_{1,3}\mathbf{v}_3 = \mathbf{v}_1 - \mathbf{v}_2 - \mathbf{v}_3 = (-84, 25, 12),$$

and $\|\mathbf{w}\|^2 = 7825 < 8041 = \|\mathbf{v}_1\|^2$.

By Algorithm 3 on input $k = 1$, we update the basis into

$$\begin{bmatrix}\mathbf{w} & \mathbf{v}_1 & \mathbf{v}_2\end{bmatrix} = \begin{bmatrix}-84 & -27 & 38 \\ 25 & -84 & -46 \\ 12 & 16 & 72\end{bmatrix}.$$

We see that the basis $(\mathbf{w}, \mathbf{v}_1, \mathbf{v}_2)_{\leq}$ is pairwise Gaussian and it satisfies the necessary and sufficient condition of Theorem 3.1 since

$$\mathbf{w} \cdot \mathbf{v}_1 = 360 < \frac{\|\mathbf{w}\|^2}{2}, \mathbf{w} \cdot \mathbf{v}_2 = 2906 < \frac{\|\mathbf{w}\|^2}{2} \text{ and } \mathbf{v}_1 \cdot \mathbf{v}_2 = 3990 < \frac{\|\mathbf{v}_1\|^2}{2}.$$

Therefore, $\mathbf{w}$ is a shortest non-zero vector of the lattice and the basis $(\mathbf{w}, \mathbf{v}_1, \mathbf{v}_2)$ achieves all three successive minima.

In the following section, we will show how to use LLL algorithm to compute a pairwise Gaussian algorithm. Therefore, it shows how to compute a basis with all three successive minima by using LLL.

3.2. Make-pairwise-Gaussian algorithms

3.2.1. *A make-pairwise-Gaussian algorithm by repeated Gauss.* In [11], Semaev showed that using the Gauss algorithm pairwise repeatedly until it gives a pairwise Gaussian basis takes $O(\log^3 B)$ bit operations, where B is the maximum Euclidean norm of the vectors in the input basis. There is no explicit way of how to repeat the Gauss algorithm until it gives a pairwise Gaussian, since the number of repeat is not large in practice. In Algorithm 4, we present a simple process of using Gauss algorithm repeatedly to get a pairwise Gaussian basis. At each while loop of Algorithm 4, we separate two cases. If $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is not pairwise SV-reduced, it runs Lines 5 to 10. If $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is pairwise SV-reduced but not pairwise Gaussian, then it runs Lines 11 and 12.

From our experiments with 100,000 uniform randomly chosen input $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ for $\mathbf{u}_i \in \mathbb{Z}^m$ with $\|\mathbf{u}_i\|_\infty \leq 2^{10}$, the maximum of while loop count for Algorithm 4 for $m = 3$ was 11, which occurs twice. We note that the experiments with randomly chosen three vectors do not cover the extremely bad cases. Considering possible bad cases, we also test for 100,000 randomly chosen input $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of Hermite normal form, which is considered bad enough not to give any information on short vectors of the lattice. In the experiments with input basis of Hermite normal form, the maximal while loop count of Algorithm 4 for $m = 3$ was 12. We note that if the intermediate input $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is pairwise SV-reduced, then the computations of Lines 5-10 are not necessary

Algorithm 4 Make-Pairwise-Gaussian Algorithm by Repeated Gauss

Input: A basis $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of a lattice $L \subset \mathbb{Z}^m$
Output: A pairwise Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ of L

1: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$
2: **while** $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is not pairwise Gaussian **do**
3: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow \text{Ordering}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$
4: $(\mathbf{v}_1', \mathbf{v}_2') \leftarrow \text{Gauss}(\mathbf{v}_1, \mathbf{v}_2)$; $(\mathbf{v}_1'', \mathbf{v}_3') \leftarrow \text{Gauss}(\mathbf{v}_1, \mathbf{v}_3)$; $(\mathbf{v}_2'', \mathbf{v}_3'') \leftarrow \text{Gauss}(\mathbf{v}_2, \mathbf{v}_3)$
5: **if** $\mathbf{v}_1 \neq \mathbf{v}_1'$ **then**
6: $(\mathbf{v}_1, \mathbf{v}_2) \leftarrow (\mathbf{v}_1', \mathbf{v}_2')$
7: **else if** $\mathbf{v}_1 \neq \mathbf{v}_1''$ **then**
8: $(\mathbf{v}_1, \mathbf{v}_3) \leftarrow (\mathbf{v}_1'', \mathbf{v}_3')$
9: **else if** $\mathbf{v}_2 \neq \mathbf{v}_2''$ **then**
10: $(\mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{v}_2'', \mathbf{v}_3'')$
11: **else**
12: $(\mathbf{v}_2, \mathbf{v}_3) \leftarrow \text{Gauss}(\mathbf{v}_2', \mathbf{v}_3')$
13: **end if**
14: **end while**
15: **Return** $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$

in that iteration, and thus the intermediate computation can be more simplified if one can make the intermediate input as pairwise SV-reduce. In the following section, we investigate the effect of using LLL with respect to this issue of Algorithm 4 and present Algorithm 6.

3.2.2. *A make-pairwise-Gaussian algorithm using LLL.* In this section, we present algorithms of computing pairwise Gaussian basis using LLL for three dimension lattice. First, we prove a special property of LLL algorithm with respect to pairwise Gaussian basis. And then we present a make-pairwise-Gaussian algorithm using LLL. By using LLL, we made the intermediate input to be pairwise SV-reduced and thus using LLL removes the computations of Lines 5-10 of Algorithm 4 in each iteration. Experimentally, we show that using LLL makes the while loop count one in Algorithm 4, which will be explained in Section 3.3.

We prove a fact on the sizes of basis vectors under certain conditions which will be useful to prove the complexity of our proposed make-pairwise-Gaussian algorithm using LLL. In fact, one sees Lemma 3.4 is a consequence of Theorem 3.2 from [6], but we present a direct proof here for self containment.

Lemma 3.4. *Suppose that two linearly independent vectors* $(\mathbf{v}_1, \mathbf{v}_2)_{\leq}$ *satisfy that* $2|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \|\mathbf{v}_2\|^2$. *If* $\|\mathbf{v}_2\| \leq \sqrt{3}\|\mathbf{v}_1\|$, *then* $\lambda_1(L(\mathbf{v}_1, \mathbf{v}_2)) = \|\mathbf{v}_1\|$.

Proof. We want to show that, for all $a, b \in \mathbb{Z}$ with $a^2 + b^2 \neq 0$,

$$\|\mathbf{v}_1\| \leq \|a\mathbf{v}_1 + b\mathbf{v}_2\|.$$

If one of a or b is zero, clearly it holds since $\|\mathbf{v}_1\| \le \|\mathbf{v}_2\|$, and we assume that $ab \neq 0$. First, we consider $0 < |a| \le |b|$. In this case, only $2|\mathbf{v}_1 \cdot \mathbf{v}_2| \le \|\mathbf{v}_2\|^2$ is needed for $\|\mathbf{v}_1\| \le \|a\mathbf{v}_1 + b\mathbf{v}_2\|$ as in the following.

$$\begin{aligned}\|a\mathbf{v}_1 + b\mathbf{v}_2\|^2 &= a^2\|\mathbf{v}_1\|^2 + b^2\|\mathbf{v}_2\|^2 + 2ab\mathbf{v}_1 \cdot \mathbf{v}_2 \\ &\ge a^2\|\mathbf{v}_1\|^2 + b^2\|\mathbf{v}_2\|^2 - |a||b|\|\mathbf{v}_2\|^2 \ge \|\mathbf{v}_1\|^2.\end{aligned}$$

Now we consider the case $|a| > |b| = 1$.

$$\begin{aligned}\|a\mathbf{v}_1 + b\mathbf{v}_2\|^2 &= a^2\|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|^2 + 2ab\mathbf{v}_1 \cdot \mathbf{v}_2 \\ &= \|\mathbf{v}_1\|^2 + (a^2-1)\|\mathbf{v}_1\|^2 + \|\mathbf{v}_2\|^2 + 2ab\mathbf{v}_1 \cdot \mathbf{v}_2 \\ &\ge \|\mathbf{v}_1\|^2 + \frac{a^2-1}{3}\|\mathbf{v}_2\|^2 + \|\mathbf{v}_2\|^2 - |a|\|\mathbf{v}_2\|^2 \\ &= \|\mathbf{v}_1\|^2 + \frac{(|a|-2)(|a|-1)}{3}\|\mathbf{v}_2\|^2 \ge \|\mathbf{v}_1\|^2.\end{aligned}$$

Finally, we consider the case $|a| > |b| \ge 2$.

$$\begin{aligned}\|a\mathbf{v}_1 + b\mathbf{v}_2\|^2 &= a^2\|\mathbf{v}_1\|^2 + b^2\|\mathbf{v}_2\|^2 + 2ab\mathbf{v}_1 \cdot \mathbf{v}_2 \\ &\ge a^2\|\mathbf{v}_1\|^2 + b^2\|\mathbf{v}_2\|^2 - |a||b|\|\mathbf{v}_2\|^2 \\ &\ge \frac{a^2}{3}\|\mathbf{v}_2\|^2 + b^2\|\mathbf{v}_2\|^2 - |a||b|\|\mathbf{v}_2\|^2 \\ &= \frac{b^2}{4}\|\mathbf{v}_2\|^2 + \left(\frac{|a|}{\sqrt{3}} - \frac{\sqrt{3}|b|}{2}\right)^2\|\mathbf{v}_2\|^2 \\ &\ge \|\mathbf{v}_2\|^2 \ge \|\mathbf{v}_1\|^2.\end{aligned}$$

□

Now we describe Algorithm LLLG, where a simple process is added after executing LLL and prove that the output of LLLG satisfies the hypothesis of Lemma 3.4.

Algorithm 5 LLLG(δ) Algorithm

Input: A basis $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of L, LLL parameter δ
Output: A basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3')$ of L

1: $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow LLL(\delta)(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$
2: Set $\mathbf{v}_3' \leftarrow \mathbf{v}_3 - \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor \cdot \mathbf{v}_2$
3: **Return** $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3')$

Theorem 3.5. *The output* $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3')$ *of LLLG*(δ) *algorithm satisfies the following condition for* $1/4 < \delta \le 1$:

$$|\mathbf{v}_1 \cdot \mathbf{v}_2| \le \frac{1}{2}\|\mathbf{v}_1\|^2,\ |\mathbf{v}_1 \cdot \mathbf{v}_3'| \le \frac{1}{2}\|\mathbf{v}_1\|^2,\ |\mathbf{v}_2 \cdot \mathbf{v}_3'| \le \frac{1}{2}\|\mathbf{v}_2\|^2.$$

Proof. (1) Proof for $|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$: This is clear since LLLG does not change the vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ from the output of LLL in STEP 1.

(2) Proof for $|\mathbf{v}_1 \cdot \mathbf{v}_3'| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$: By the definition of LLL(δ)-reduced basis, the intermediate output $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ (of STEP 1 of LLLG) satisfies that

- $\|\mathbf{v}_i^*\|^2 \leq \|\mathbf{v}_i\|^2$ for $i = 1, 2, 3$;
- $|\mathbf{v}_2 \cdot \mathbf{v}_1| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$, $|\mathbf{v}_3 \cdot \mathbf{v}_1| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$ and $|\mathbf{v}_3 \cdot \mathbf{v}_2^*| \leq \frac{1}{2}\|\mathbf{v}_2^*\|^2$;
- $\|\mathbf{v}_2\|^2 \geq \delta\|\mathbf{v}_1\|^2$ for $\frac{1}{4} < \delta \leq 1$.

We are going to use these for this proof. Recall that $\mathbf{v}_3' = \mathbf{v}_3 - \gamma \cdot \mathbf{v}_2$, where $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor$. First we show that $\gamma \in \{-1, 0, 1\}$. From the formulation $\mathbf{v}_2^*$, we see that

$$\mathbf{v}_3 \cdot \mathbf{v}_2^* = \mathbf{v}_3 \cdot (\mathbf{v}_2 - \mu_{2,1}\mathbf{v}_1) = \mathbf{v}_3 \cdot \mathbf{v}_2 - \mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1).$$

By the fact $|\mathbf{v}_3 \cdot \mathbf{v}_2^*| \leq \frac{1}{2}\|\mathbf{v}_2^*\|^2$, we have $|\mathbf{v}_3 \cdot \mathbf{v}_2 - \mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1)| \leq \frac{1}{2}\|\mathbf{v}_2^*\|^2$, which implies that

$$-\frac{1}{2}\|\mathbf{v}_2^*\|^2 \leq \mathbf{v}_3 \cdot \mathbf{v}_2 - \mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1) \leq \frac{1}{2}\|\mathbf{v}_2^*\|^2.$$

Adding $\mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1)$ on both sides gives

$$-\frac{1}{2}\|\mathbf{v}_2^*\|^2 + \mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1) \leq \mathbf{v}_3 \cdot \mathbf{v}_2 \leq \frac{1}{2}\|\mathbf{v}_2^*\|^2 + \mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1).$$

Dividing all parts by $\|\mathbf{v}_2\|^2$ and by using the fact $\|\mathbf{v}_2^*\|^2 \leq \|\mathbf{v}_2\|^2$,

$$-\frac{1}{2} + \frac{\mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1)}{\|\mathbf{v}_2\|^2} \leq \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\|\mathbf{v}_2\|^2} \leq \frac{1}{2} + \frac{\mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1)}{\|\mathbf{v}_2\|^2}.$$

Note that

$$\begin{aligned}
\left|\frac{\mu_{2,1}(\mathbf{v}_3 \cdot \mathbf{v}_1)}{\|\mathbf{v}_2\|^2}\right| &= \left|\frac{(\mathbf{v}_2 \cdot \mathbf{v}_1)(\mathbf{v}_3 \cdot \mathbf{v}_1)}{\|\mathbf{v}_1\|^2\|\mathbf{v}_2\|^2}\right| \\
&\leq \left|\frac{(\mathbf{v}_2 \cdot \mathbf{v}_1)(\mathbf{v}_3 \cdot \mathbf{v}_1)}{\delta\|\mathbf{v}_1\|^2\|\mathbf{v}_1\|^2}\right| \qquad (\because \delta\|\mathbf{v}_1\|^2 \leq \|\mathbf{v}_2\|^2) \\
&\leq \frac{1}{\delta} \times \frac{1}{2} \times \frac{1}{2} \qquad (\because |\mathbf{v}_2 \cdot \mathbf{v}_1|, |\mathbf{v}_3 \cdot \mathbf{v}_1| \leq \frac{1}{2}\|\mathbf{v}_1\|^2) \\
&< 1 \qquad (\because 1/4 < \delta \leq 1).
\end{aligned}$$

Therefore, we see that $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor \in \{-1, 0, 1\}$. In particular, γ is classified as in Table 1 according to the sign of $\mu_{2,1} \cdot \mu_{3,1}$. Note that if $\gamma = 1$, then $\mu_{2,1}$ and $\mu_{3,1}$ have the same sign and if $\gamma = -1$, then $\mu_{2,1}$ and $\mu_{3,1}$ have the opposite sign.

Now we prove $|\mathbf{v}_1 \cdot \mathbf{v}_3'| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$ for each $\gamma \in \{-1, 0, 1\}$.

- If $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor = 0$, i.e., $\mathbf{v}_3' = \mathbf{v}_3$, clearly we have $|\mathbf{v}_1 \cdot \mathbf{v}_3'| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$.
- If $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor = 1$, i.e., $\mathbf{v}_3' = \mathbf{v}_3 - \mathbf{v}_2$, $\mu_{2,1}$ and $\mu_{3,1}$ have the same sign from Table 1, then we have

$$|\mathbf{v}_3' \cdot \mathbf{v}_1| = |(\mathbf{v}_3 - \mathbf{v}_2) \cdot \mathbf{v}_1| = |\mathbf{v}_3 \cdot \mathbf{v}_1 - \mathbf{v}_2 \cdot \mathbf{v}_1| = |\mu_{3,1} - \mu_{2,1}|\|\mathbf{v}_1\|^2 \leq \frac{1}{2}\|\mathbf{v}_1\|^2.$$

TABLE 1. A classification of $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor$

$\mu_{2,1} \cdot \mu_{3,1}$	Range of $\frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2}$	$\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor$
non-negative	$-\frac{1}{2} < \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} < \frac{3}{2}$	0 or 1
negative	$-\frac{3}{2} < \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} < \frac{1}{2}$	-1 or 0

- If $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor = -1$, i.e., $\mathbf{v}_3' = \mathbf{v}_3 + \mathbf{v}_2$, $\mu_{2,1}$ and $\mu_{3,1}$ have the opposite sign from Table 1, then we have

$$|\mathbf{v}_3' \cdot \mathbf{v}_1| = |(\mathbf{v}_3 + \mathbf{v}_2) \cdot \mathbf{v}_1| = |\mathbf{v}_3 \cdot \mathbf{v}_1 + \mathbf{v}_2 \cdot \mathbf{v}_1| = |\mu_{3,1} + \mu_{2,1}| \|\mathbf{v}_1\|^2 \leq \frac{1}{2}\|\mathbf{v}_1\|^2.$$

(3) Proof for $|\mathbf{v}_2 \cdot \mathbf{v}_3'| \leq \frac{1}{2}\|\mathbf{v}_2\|^2$: For $\gamma = \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor$, we have $\gamma - \frac{1}{2} < \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \leq \gamma + \frac{1}{2}$. Multiplying $\mathbf{v}_2 \cdot \mathbf{v}_2$ on both sides gives

$$\gamma(\mathbf{v}_2 \cdot \mathbf{v}_2) - \frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2) < \mathbf{v}_3 \cdot \mathbf{v}_2 \leq \gamma(\mathbf{v}_2 \cdot \mathbf{v}_2) + \frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2).$$

Subtracting $\gamma(\mathbf{v}_2 \cdot \mathbf{v}_2)$ from all parts gives

$$-\frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2) < \mathbf{v}_3 \cdot \mathbf{v}_2 - \gamma(\mathbf{v}_2 \cdot \mathbf{v}_2) \leq \frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2).$$

Rewriting the middle term gives

$$-\frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2) < (\mathbf{v}_3 - \gamma\mathbf{v}_2) \cdot \mathbf{v}_2 \leq \frac{1}{2}(\mathbf{v}_2 \cdot \mathbf{v}_2)$$

and finally

$$|(\mathbf{v}_3 - \gamma\mathbf{v}_2) \cdot \mathbf{v}_2| \leq \frac{1}{2}\|\mathbf{v}_2\|^2, \text{ that is, } |\mathbf{v}_2 \cdot \mathbf{v}_3'| \leq \frac{1}{2}\|\mathbf{v}_2\|^2$$

as required. □

Note that if the output of LLLG algorithm is ordered in size, then it is pairwise Gaussian. However, not all the outputs $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3')$ of LLLG algorithm are ordered in Euclidean norms. According to our experiments, more than 99% of randomly chosen inputs, LLLG($\delta \geq 0.99$) algorithm outputs a pairwise Gaussian basis. Now we show that the output of LLLG(δ) is always pairwise SV-reduced if $\delta \geq 0.9$.

Theorem 3.6. *For $\delta \geq 0.9$, an LLL(δ)-reduced basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ and $\mathbf{v}_3' = \mathbf{v}_3 - \lceil \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rfloor \cdot \mathbf{v}_2$, the basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3')$ is pairwise SV-reduced.*

Proof. We use the notation $\mu_{i,j} = \frac{\mathbf{v}_i \cdot \mathbf{v}_j^*}{\mathbf{v}_j^* \cdot \mathbf{v}_j^*}$ for $1 \leq j < i \leq 3$, where $(\mathbf{v}_1^*, \mathbf{v}_2^*, \mathbf{v}_3^*)$ is the GSO of $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$. Since $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is LLL(δ)-reduced, $|\mu_{i,j}| \leq 1/2$. We consider three pairs separately.

Case 1: First, we show that the pair $(\mathbf{v}_1, \mathbf{v}_2)$ is SV-reduced. From Theorem 3.5, we see that

$$\frac{|\mathbf{v}_1 \cdot \mathbf{v}_2|}{\mathbf{v}_1 \cdot \mathbf{v}_1} \leq 1/2. \tag{1}$$

If $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$, then $(\mathbf{v}_1, \mathbf{v}_2)$ is Gaussian, and thus SV-reduced. Now suppose that $\|\mathbf{v}_2\| < \|\mathbf{v}_1\|$. By Lemma 3.4 and inequality (1), it is enough to show that $\|\mathbf{v}_1\|^2 \leq 3\|\mathbf{v}_2\|^2$. Since $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is LLL(δ)-reduced, the Lovász condition implies that $\|\mathbf{v}_2\|^2 = \|\mathbf{v}_2^* + \mu_{2,1}\mathbf{v}_1^*\|^2 \geq \delta\|\mathbf{v}_1\|^2$. Therefore, for $\delta \geq 0.9$, we have

$$\|\mathbf{v}_1\|^2 \leq \frac{1}{\delta}\|\mathbf{v}_2\|^2 \leq \frac{10}{9}\|\mathbf{v}_2\|^2 \leq 3\|\mathbf{v}_2\|^2.$$

Case 2: Secondly, we show that the pair $(\mathbf{v}_2, \mathbf{v}_3')$ is SV-reduced. From Theorem 3.5, we see that

$$\frac{|\mathbf{v}_2 \cdot \mathbf{v}_3'|}{\mathbf{v}_2 \cdot \mathbf{v}_2} \leq 1/2.$$

If $\|\mathbf{v}_2\| \leq \|\mathbf{v}_3'\|$, then $(\mathbf{v}_2, \mathbf{v}_3')$ is Gaussian, and thus SV-reduced. Now suppose that $\|\mathbf{v}_3'\| < \|\mathbf{v}_2\|$. As in Case 1, it is enough to show that $\|\mathbf{v}_2\|^2 \leq 3\|\mathbf{v}_3'\|^2$, that is, $\|\mathbf{v}_3'\|^2 \geq \frac{\|\mathbf{v}_2\|^2}{3}$. Since $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is LLL(δ)-reduced and $\mathbf{v}_1^* = \mathbf{v}_1$, the followings hold.

$$\begin{aligned}
\|\mathbf{v}_3\|^2 &= \|\mathbf{v}_3^* + \mu_{3,2}\mathbf{v}_2^* + \mu_{3,1}\mathbf{v}_1^*\|^2 = \|\mathbf{v}_3^* + \mu_{3,2}\mathbf{v}_2^*\|^2 + \mu_{3,1}^2\|\mathbf{v}_1\|^2 \\
&\geq \delta\|\mathbf{v}_2^*\|^2 + \mu_{3,1}^2\|\mathbf{v}_1\|^2 = \delta\|\mathbf{v}_2\|^2 - \delta\mu_{2,1}^2\|\mathbf{v}_1\|^2 + \mu_{3,1}^2\|\mathbf{v}_1\|^2 \\
&\geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta}{4}\|\mathbf{v}_1\|^2,
\end{aligned}$$

$$\begin{aligned}
\|\mathbf{v}_3 \pm \mathbf{v}_2\|^2 &= \|\mathbf{v}_3\|^2 + \|\mathbf{v}_2\|^2 \pm 2\mathbf{v}_2 \cdot \mathbf{v}_3 \\
&= \|\mathbf{v}_3\|^2 + \|\mathbf{v}_2\|^2 \pm 2(\mathbf{v}_2^* + \mu_{2,1}\mathbf{v}_1^*) \cdot \mathbf{v}_3 \\
&\geq \|\mathbf{v}_3\|^2 + \|\mathbf{v}_2^*\|^2 + \mu_{2,1}^2\|\mathbf{v}_1^*\|^2 - \|\mathbf{v}_2^*\|^2 - |\mu_{2,1}|\|\mathbf{v}_1^*\|^2 \\
&= \|\mathbf{v}_3\|^2 + (\mu_{2,1}^2 - |\mu_{2,1}|)\|\mathbf{v}_1\|^2 \\
&\geq \|\mathbf{v}_3\|^2 - 1/4 \cdot \|\mathbf{v}_1\|^2.
\end{aligned}$$

By the previous inequality on $\|\mathbf{v}_3\|^2$, we have

$$\begin{aligned}
\|\mathbf{v}_3 \pm \mathbf{v}_2\|^2 &\geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta}{4}\|\mathbf{v}_1^*\|^2 - 1/4 \cdot \|\mathbf{v}_1^*\|^2 \\
&= \delta\|\mathbf{v}_2\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_1\|^2.
\end{aligned}$$

We recall that $\mathbf{v}_3' \in \{\mathbf{v}_3, \mathbf{v}_3 - \mathbf{v}_2, \mathbf{v}_3 + \mathbf{v}_2\}$ from the proof of Theorem 3.5. Therefore, we have

$$\|\mathbf{v}_3'\|^2 \geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_1\|^2.$$

Now if $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$, we have, for $\delta \geq 0.9$

$$\|\mathbf{v}_3'\|^2 \geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_2\|^2 = (\delta - \frac{\delta+1}{4})\|\mathbf{v}_2\|^2$$

$$\geq \frac{17}{40}\|\mathbf{v}_2\|^2 \geq \frac{\|\mathbf{v}_2\|^2}{3} \qquad (\because \delta \geq 0.9).$$

If $\|\mathbf{v}_2\| < \|\mathbf{v}_1\|$, we use $\|\mathbf{v}_1\|^2 < \frac{1}{\delta}\|\mathbf{v}_2\|^2$ from the Lovász condition. For $\delta \geq 0.9$,

$$\|\mathbf{v}_3'\|^2 \geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta+1}{4\delta}\|\mathbf{v}_2\|^2 = (\delta - \frac{\delta+1}{4\delta})\|\mathbf{v}_2\|^2 \geq \frac{135}{360}\|\mathbf{v}_2\|^2 \geq \frac{\|\mathbf{v}_2\|^2}{3}.$$

Case 3: Finally, we show that the pair $(\mathbf{v}_1, \mathbf{v}_3')$ is SV-reduced. From Theorem 3.5, we see that

$$\frac{|\mathbf{v}_1 \cdot \mathbf{v}_3'|}{\mathbf{v}_1 \cdot \mathbf{v}_1} \leq 1/2.$$

If $\|\mathbf{v}_1\| \leq \|\mathbf{v}_3'\|$, then $(\mathbf{v}_1, \mathbf{v}_3')$ is Gaussian, and thus SV-reduced. Now suppose that $\|\mathbf{v}_3'\| < \|\mathbf{v}_1\|$. As in the previous cases, it is enough to show that $\|\mathbf{v}_3'\|^2 \geq \frac{\|\mathbf{v}_1\|^2}{3}$. From Case 2, we have

$$\|\mathbf{v}_3'\|^2 \geq \delta\|\mathbf{v}_2\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_1\|^2. \tag{2}$$

Now we want to replace the right hand side of inequality (2) in terms of $\|\mathbf{v}_1^*\|^2$. If $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$, for $\delta \geq 0.9$, inequality (2) directly yields

$$\|\mathbf{v}_3'\|^2 \geq \delta\|\mathbf{v}_1\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_1\|^2 = (\delta - \frac{\delta+1}{4})\|\mathbf{v}_1\|^2 \geq \frac{17}{40}\|\mathbf{v}_1\|^2 \geq \frac{\|\mathbf{v}_1\|^2}{3}.$$

If $\|\mathbf{v}_2\| < \|\mathbf{v}_1\|$, we use $\|\mathbf{v}_2\|^2 \geq \delta\|\mathbf{v}_1\|^2$ from the Lovász condition. For $\delta \geq 0.9$, inequality (2) gives

$$\|\mathbf{v}_3'\|^2 \geq \delta^2\|\mathbf{v}_1\|^2 - \frac{\delta+1}{4}\|\mathbf{v}_1\|^2 = (\delta^2 - \frac{\delta+1}{4})\|\mathbf{v}_1\|^2 \geq \frac{134}{400}\|\mathbf{v}_1\|^2 \geq \frac{\|\mathbf{v}_1\|^2}{3}.$$

□

Finally, we present Algorithm 6, our algorithm PG (make-pairwise-Gaussian algorithm using LLL) for three dimensional lattices.

Algorithm 6 Make-Pairwise-Gaussian Algorithm using LLL(δ) (PG)

Input: A basis $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ of a lattice L and $\delta \geq 0.9$
Output: A pairwise Gaussian basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ of L

$(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$
while $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is not pairwise Gaussian **do**
  $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow \mathrm{LLL}(\delta)(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$
  $\mathbf{v}_3 \leftarrow \mathbf{v}_3 - \lfloor \frac{\mathbf{v}_3 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2} \rceil \mathbf{v}_2$
  $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leftarrow \mathrm{Ordering}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$
  $(\mathbf{v}_2, \mathbf{v}_3) \leftarrow (\mathbf{v}_2 - \lfloor \frac{\mathbf{v}_2 \cdot \mathbf{v}_1}{\mathbf{v}_1 \cdot \mathbf{v}_1} \rceil \mathbf{v}_1, \mathbf{v}_3 - \lfloor \frac{\mathbf{v}_3 \cdot \mathbf{v}_1}{\mathbf{v}_1 \cdot \mathbf{v}_1} \rceil \mathbf{v}_1)$
  $(\mathbf{v}_2, \mathbf{v}_3) \leftarrow \mathrm{Gauss}(\mathbf{v}_2, \mathbf{v}_3)$
end while
Return $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$

The correctness of Algorithm 6 follows from the correctness of Algorithm 4 and Theorem 3.6. Since Line 3 and Line 4 of Algorithm 6 execute LLLG algorithm, the updated basis at Line 4 of Algorithm 6 is pairwise SV-reduced by Theorem 3.6. Therefore, the while loop of Algorithm 4 has been simplified in Algorithm 6. We present our experimental results of Algorithm 6 and Algorithm 4 in the following section.

3.3. Experiments

We implement our results by using the software, Python 3.8.5 [MSC v.1916 64 bit (AMD64)] IPython 7.19.0 – An enhanced Interactive Python.

Algorithm 6 uses a subroutine LLLG. First, we examine the probability where Algorithm 5 (LLLG) outputs a pairwise Gaussian basis. In our experiments, we have tested for 100,000 randomly chosen basis $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ with $\mathbf{v}_i \in \mathbb{Z}^m$ for $\|\mathbf{v}_i\|_\infty \leq 2^{10}$ and several $3 \leq m \leq 50$. Considering that the experiments with uniformly random vectors might not cover the extremely bad cases, we have tested for randomly chosen $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ of Hermite normal form, too. Our experiments suggest that our Algorithm 5 (LLLG) outputs a pairwise Gaussian basis with high probability. Table 2 presents the experimental results on the success rate of LLLG.

TABLE 2. Success rate of LLLG to give a pairwise Gaussian basis

$(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$: a basis for a lattice $L \subset \mathbb{Z}^m$ with $\|\mathbf{v}_i\|_\infty \leq 2^{10}$								
m	3	5	10	15	20	25	40	50
($\delta = 0.90$, random input)	99.3	98.9	98.8	99.0	99.4	99.6	99.9	99.9
($\delta = 0.90$, random HNF input)	99.3	98.7	98.6	99.0	99.3	99.6	99.9	99.9
($\delta = 0.75$, random input)	95.7	93.4	93.3	95.0	96.9	98.3	99.7	99.9
($\delta = 0.75$, random HNF input)	94.9	92.3	92.1	94.5	96.7	98.1	99.7	99.9

Now we compare the efficiency Algorithm 6 which uses LLL and Algorithm 4 which is a repetition of Gauss algorithm. Considering the fact that the subroutine algorithm LLLG in Algorithm 6 repeats two dimensional projections like the Gauss algorithm, we count the number of all two dimensional projections executed in each algorithm in the comparison. In our experiment, we tested for 10,000 inputs $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \in \mathbb{Z}^{3\times 3}$ with $\|\mathbf{u}_i\|_\infty \leq 2^{30}$ which are obtained by multiplying a unimodular matrix chosen uniformly at random to a randomly chosen basis with relatively short sizes. From our experiments, the average number of two dimensional projections of Algorithm 6 is 6.6 and that of Algorithm 4 is 19.7. Figure 1 presents the number of two dimensional projections of Algorithm 6 and Algorithm 4 to return a pairwise Gaussian basis. The maximum number of two dimensional projections in Algorithm 6 is 11, and that of Algorithm 4 is 41. It is noteworthy that about 98 percent of the executions of Algorithm 4 requires at least 12 projections to return a pairwise Gaussian basis. For randomly selected inputs, both algorithms are quite efficient for computing

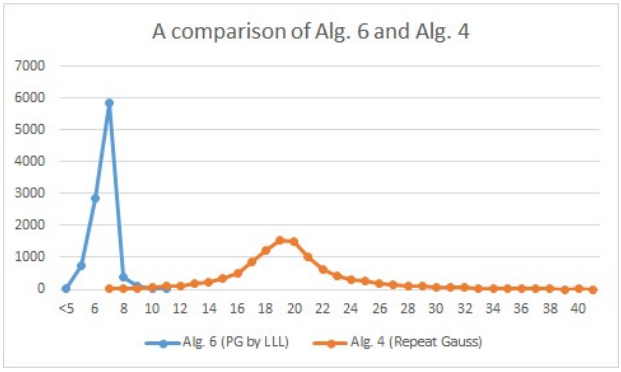

FIGURE 1. A comparison of the required number (horizontal axis) of two dimensional projections of Algorithm 6 and Algorithm 4

a pairwise Gaussian basis on average. Our experiment suggests that Algorithm 6 which uses LLL is more efficient to compute a pairwise Gaussian basis than pairwise repetitions of the Gauss algorithm in the sense that it reduces the number of two dimensional projections of Algorithm 4.

4. Conclusion

In this article, we focus on two problems for three dimensional lattices: One is on the condition for pairwise Gaussian basis to be SV-reduced and another is on constructing a pairwise Gaussian basis without using ad hoc repetition of two dimensional Gauss algorithm. We prove a necessary and sufficient condition for a pairwise Gaussian basis to achieve the first k successive minima for three dimensional lattices for each $k \in \{1, 2, 3\}$. By using this condition, we present an example of three dimensional LLL(1)-reduced basis which is not SV-reduced. We also present how to compute a pairwise Gaussian basis by using three dimensional LLL in Algorithm 6. To show the correctness of Algorithm 6, we prove that LLL(δ) with an additional simple reduction turns any basis for a three dimensional lattice into a pairwise SV-reduced basis if $\delta \geq 0.9$, which is an independently interesting result on the quality of the LLL-reduced basis for three dimensional case.

Acknowledgments. Hyang-Sook Lee was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2021R1A2C1094821) and partially supported by the Basic Science Research Program through the NRF funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177). Seongan Lim was supported by the NRF of Korea (Grant Number: 2016R1D1A1B01008562).

References

[1] M. Ajtai, *The shortest vector problem in L_2 is NP-hard for randomized reductions*, STOC 98 Proceedings of the 13th annual ACM symposium on Theory of computing , pp. 10–19, 1998.

[2] M. Bremner, *Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications*, CRC Press, 2011.

[3] Y. Chen and P. Q. Nguyen, *BKZ 2.0: better lattice security estimates*, in Advances in cryptology—ASIACRYPT 2011, 1–20, Lecture Notes in Comput. Sci., 7073, Springer, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-25385-0_1

[4] C. F. Gauss, *Disquisitiones arithmeticae*, translated and with a preface by Arthur A. Clarke, Springer-Verlag, New York, 1986.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, Undergraduate Texts in Mathematics, Springer, New York, 2008.

[6] H.-S. Lee, S. Lim, K. Song, and I. Yie, *New orthogonality criterion for shortest vector of lattices and its applications*, Discrete Appl. Math. **283** (2020), 323–335. https://doi.org/10.1016/j.dam.2020.01.023

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. https://doi.org/10.1007/BF01457454

[8] D. Micciancio and P. Voulgaris, *Faster exponential time algorithms for the shortest vector problem*, in Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, 1468–1480, SIAM, Philadelphia, PA, 2010.

[9] R. Neelamani, S. Dash, and R. G. Baraniuk, *On nearly orthogonal lattice bases and random lattices*, SIAM J. Discrete Math. **21** (2007), no. 1, 199–219. https://doi.org/10.1137/050635985

[10] P. Q. Nguyen and D. Stehlé, *Low-dimensional lattice basis reduction revisited*, ACM Trans. Algorithms **5** (2009), no. 4, Art. 46, 48 pp. https://doi.org/10.1145/1597036.1597050

[11] I. Semaev, *A 3-dimensional lattice reduction algorithm*, in Cryptography and lattices (Providence, RI, 2001), 181–193, Lecture Notes in Comput. Sci., 2146, Springer, Berlin, 2001. https://doi.org/10.1007/3-540-44670-2_13

Kitae Kim
Department of Mathematics
Inha University
Incheon 22212, Korea
Email address: ktkim@inha.ac.kr

Hyang-Sook Lee
Department of Mathematics
Ewha Womans University
Seoul 03760, Korea
Email address: hsl@ewha.ac.kr

Seongan Lim
Department of Mathematics
Inha University
Incheon 22212, Korea
Email address: seongannym@inha.ac.kr

Jeongeun Park
COSIC
KU Leuven
Belgium
Email address: jungeun7430@gmail.com

Ikkwon Yie
Department of Mathematics
Inha University
Incheon 22212, Korea
Email address: ikyie@inha.ac.kr