Necessary and sufficient conditions for shortest vectors in lattices of dimension 2 and 3

Youngin Cho*, **Boyun Choi***, **Hyemin Gu***, **Hyang-sook Lee, Jeong-eun Park***

Department of Mathematics Ewha Womans University

Contact Information:
Department of Mathematics
Ewha Womans University

younginewha94@gmail.com, choiboyun1203@gmail.com, nicolegu6616@naver.com, hsl@ewha.ac.kr, jungeun7430@naver.com

Introduction

A lattice in the Euclidean space is an important issue for cryptography these days. Finding **a nonzero shortest vector** of a given lattice(SVP) is one of the hard problems in a lattice in the Euclidean space. Also the cryptography schemes based on these lattice hard problems receive the attention as alternatives for the coming period of developing quantum computers. The higher the dimension of a lattice , the more difficult solving SVP. So we start with low dimensional lattices to try to find a pattern of a shortest vector in higher dimensional lattices. In low dimensions, gaussian property of basis vectors is a key factor to be a shortest vector of a lattice among basis vectors of the lattice. We suggest necessary and sufficient conditions for a shortest vector in lattices of dimension 2,3 and introduce an algorithm giving a pairwise gaussian basis as an output of a 3 dimensional lattice.

Flow Outline

Lattice of dimension 2

(Known)
A neccessary and sufficient condition for a shortest vector in a lattice in dimension 2:
Gaussian basis
by Gaussian algorithm

Lattice of dimension 3

A necessary condition to have pairwise Gaussian basis vectors

An algorithm to produce a pairwise Gaussian basis

A neccessary condition for the shortest basis vector to be shortest in a lattice: pairwise Gaussian & another property

Main Theorem:
A necessary and sufficient condition for a shortest vector in a lattice in dimension 3

Preliminaries

Definition 1

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}$ be a set of linearly independent vectors. 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.

Notation 1

We call $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for a lattice L and $\mathcal{B}^* = \{\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*\}$ be **the corresponding Gram-Schmidt orthogonal basis** with $\mathcal{B}$. Let $F^* = F(\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*)$ be the analogous matrix whose rows are the vectors $\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*$. Then F and F^* are related by

$$MF^* = F$$

where M is the change of basis matrix

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

Notation 2

$\|\cdot\|$ refers to Euclidean norm.

Definition 2

An ordered basis $(\mathbf{v}_1, \mathbf{v}_2)_\leq$ of a lattice L in $\mathbb{R}^n$ is called **Gaussian** if $|\mathbf{v}_2 \cdot \mathbf{v}_1| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$.

Definition 3

[2],[4]
The basis $\mathcal{B}$ is said to be **LLL reduced** if it satisfies the following two conditions:
(**Size condition**) $|\mu_{i,j}| = \frac{|\mathbf{v}_i \cdot \mathbf{v}_j^*|}{\|\mathbf{v}_j^*\|^2} \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$.
(**Lovász condition**) $\|\mathbf{v}_i^* + \mu_{i,i-1}^2\mathbf{v}_{i-1}^*\|^2 \geq \alpha\|\mathbf{v}_{i-1}^*\|^2$ for all $1 < i \leq n$, where $\frac{1}{4} < \alpha \leq 1$.
An LLL reduced basis is a good basis and it is possible to compute an LLL reduced basis in polynomial time.

Lemmas

Lattices of dimension 2

[1],[5]
Consider a lattice L in dimension 2.

1. For a basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ of L such that $|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$ (**Gaussian**), $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$ if and only if $\mathbf{v}_1$ is a shortest vector in L
2. For any basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ of L, there exists an algorithm to make a basis such that $|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$
$\Rightarrow$ Gaussian Algorithm
3. For any basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ of L,
$|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \frac{1}{2}\|\mathbf{v}_1\|^2$ and $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$ if and only if $\mathbf{v}_1$ is a shortest vector in L

Lattices of dimension 3

Consider a lattice L in dimension 3.

1. For any basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of L such that $|\mathbf{v}_i \cdot \mathbf{v}_j| \leq \frac{1}{2}\|\mathbf{v}_i\|^2$ for $i < j$ (**Pairwise Gaussian**),
$\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\| \leq \|\mathbf{v}_3\|$ (We call it "ordered") and
$|\mathbf{v}_1 \cdot (\epsilon_2\mathbf{v}_2 + \epsilon_3\mathbf{v}_3)| \leq \frac{1}{2}\|\epsilon_2\mathbf{v}_2 + \epsilon_3\mathbf{v}_3\|^2$ for all $\epsilon_i \in \{0, \pm1\}$ (i = 2, 3)
if and only if $\mathbf{v}_1$ is a shortest vector in L.
(Proof is similar to [3].)
2. For any basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of L, there exists an algorithm to make a basis such that $|\mathbf{v}_i \cdot \mathbf{v}_j| \leq \frac{1}{2}\|\mathbf{v}_i\|^2$ for $i < j \Rightarrow$ We introduce the algorithm.

Algorithm

For any basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ of L, we produce an LLL-reduced basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ using LLL algorithm.
Note: LLL algorithm does not guarantee the orderedness of the output basis.
Then the following manipulation on the basis vector $\mathbf{v}_3$ gives a pairwise Gaussian basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3'\}$.

Algorithm 1: $LLLG$
Input: A basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ of a lattice L in $\mathbb{Z}^3$
Output: Pairwise Gaussian basis of the lattice L

```
{v1, v2, v3} ← LLL({u1, u2, u3}, 1/4 < α ≤ 1)
v3' ← v3 − ⌈(v3·v2)/||v2||²⌋ v2
return {v1, v2, v3'}
```

We call the output basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3'\}$ of $LLLG$ algorithm as **$LLLG$-reduced basis**.

Main Theorem

Let L be a lattice in $\mathbb{Z}^3$. And let $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ be a $LLLG$-reduced basis of the lattice L (i.e. $|\mathbf{v}_i \cdot \mathbf{v}_j| \leq \frac{1}{2}\|\mathbf{v}_i\|^2$ for $1 \leq i < j \leq 3$). Then

(a) $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\| \leq \|\mathbf{v}_3\|$ and
(b) $|\mathbf{v}_1 \cdot (\epsilon_2\mathbf{v}_2 + \epsilon_3\mathbf{v}_3)| \leq \frac{1}{2}\|\epsilon_2\mathbf{v}_2 + \epsilon_3\mathbf{v}_3\|^2$ where $\epsilon_i \in \{0, \pm1\}$ for i=2, 3

if and only if $\mathbf{v}_1$ is a shortest vector in L

Basis Ordering Issue

A LLL-reduced basis could be pairwise Gaussian, but not every LLL-reduced basis has this property. So we have introduced $LLLG$ algorithm. And it is proved that $LLLG$-reduced basis is pairwise Gaussian. However, ordered property is not guaranteed by the $LLLG$-reduced basis. Here is an example.
In this study, we have used $\alpha = 1$ in **Lovász condition** to make sure $\|\mathbf{v}_2\|^2 = \|\mathbf{v}_2^* + \mu_{2,1}^2\mathbf{v}_1^*\|^2 \geq \|\mathbf{v}_1\|^2$. However, $\|\mathbf{v}_3^* + \mu_{3,2}^2\mathbf{v}_2^*\|^2 \geq \|\mathbf{v}_2\|^2$ does not guarantee that $\|\mathbf{v}_3\|^2 \geq \|\mathbf{v}_2\|^2$.
So We have the case that $\|\mathbf{v}_2\| > \|\mathbf{v}_3'\| = \|\mathbf{v}_3\|$ by $LLLG$.

$$> Y := \begin{bmatrix} -79 & 48 & 47 & -764 & 667 & 0 & -55 \\ 353 & 19 & -61 & 7 & -471 & -253 & 690 \\ 167 & 13 & -44 & 719 & 217 & -368 & -118 \end{bmatrix}$$

$$Y := \begin{bmatrix} -79 & 48 & 47 & -764 & 667 & 0 & -55 \\ 353 & 19 & -61 & 7 & -471 & -253 & 690 \\ 167 & 13 & -44 & 719 & 217 & -368 & -118 \end{bmatrix}$$

$> LLLG(Y, 1)$

$$\begin{bmatrix} 167 & 13 & -44 & 719 & 217 & -368 & -118 \\ 88 & 61 & 3 & -45 & 884 & -368 & -173 \\ 353 & 19 & -61 & 7 & -471 & -253 & 690 \end{bmatrix}$$

$\frac{\mathbf{v}_2 \cdot \mathbf{v}_1}{\|\mathbf{v}_1\|^2} = -0.031757$, $\frac{\mathbf{v}_3' \cdot \mathbf{v}_1}{\|\mathbf{v}_1\|^2} = 0.44481$, $\frac{\mathbf{v}_3' \cdot \mathbf{v}_2}{\|\mathbf{v}_2\|^2} = -0.46133$.
So this basis has pairwise Gaussian property. However, the squares of norm $\|\cdot\|^2$ are 743392, 960308, 890690 respectively.(i.e. it is not ordered.)

Further Studies

We have proposed an algorithm to produce pairwise-gaussian basis vectors from any basis of a lattice. However, it is detected by the above example that $LLLG$ algorithm does not guarantee the orderedness of output basis. So far, we recommend to run the algorithm several times to receive an ordered basis as an output. And we are going to probe further to construct an improved algorithm, which guarantees ordered properties of output at once.

References

[1] M. Bremmer, *Lattice basis reduction: an introduction to the LLL algorithm and its applications*, CRC Press, 2011.

[2] J. Hoffstein, *An introduction to mathematical cryptography*, Springer, 2008.

[3] Seunghwan Chang , Taewan Kim , Hyang-sook Lee , Juhee Lee , Seongan Lim, *Minimal condition for shortest vectors in lattices*, (preprint).

[4] A. K. Lenstra, H. W. Lenstra, Jr., L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. 261, 1982, 515-534.

[5] C. R. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, 1809.