Malaysian Journal of Mathematical Sciences 18(2): 287–300 (2024)
https://doi.org/10.47836/mjms.18.2.05

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

On the Properties of Reduced Basis Related to Lattice-Reduced Algorithm

Salleh, N.*[1] and Kamarulhaili, H.[1]

[1]*School of Mathematical Sciences, Universiti Sains Malaysia, Malaysia*

E-mail: mymy_nsbs@yahoo.com.my
**Corresponding author*

Received: 5 December 2023
Accepted: 4 February 2024

Abstract

The concept of the Shortest Vector Problem (SVP) has surprisingly been used widely in many applications of lattice-based cryptography, notably in public-key cryptanalysis. One of the applications is to develop a well-known algorithm of lattice reduction, namely the LLL (Lenstra-Lenstra-Lovasz) algorithm. The LLL algorithm is known to be able to reduce the basis of a lattice to a minimum set of vectors, which is called the LLL-reduced basis. In this paper, we investigate the properties of the LLL-reduced basis for some different factor δ values. By changing and adjusting the value of factor δ, the proposed value of factor δ in the LLL-reduced basis produces some interesting properties. We also looked into the relationship between the initial vector and the factor δ in the LLL-reduced basis and developed some related properties.

Keywords: lattice-based cryptography; LLL algorithm; reduced basis.

1 Introduction

The lattice problem is a fundamental problem in mathematics and computer science that has been studied for centuries, and this is likely to remain so in the future. The lattice problem involves arranging points on a lattice, which is a two-dimensional grid, such that no points are the same distance apart. By studying lattices, several important problems in the field of cryptography [4] that are considered difficult problems have been solved. An example of a lattice problem that can considered difficult is SVP (Shortest Vector Problem), a lattice problem of finding the shortest vector in l_2 norm (or generally in a lattice) because the exact shortest lattice basis is known quite hard to solve. That is why van Emde [13] conjectured that SVP is NP-hard in the l_2 norm and SVP is also known to be NP-hard in l_∞ norm. For a quite long time, this conjecture remained an open problem, then it was solved by Ajtai [1]. Later, Ajtai's result is improved by Cai and Nerurkar [3] by showing that the approximation factor is within a factor $(1 + 1/n^\varepsilon)$ (for any $\varepsilon > 0$) in l_2 norm, where the proof also works for l_p norm. After that, Micciancio [10] raised the hardness approximation factor further in l_p norm within any constant factor less than $\sqrt[p]{2}$. This factor $\sqrt[p]{2}$ is known as the best result between the hardness approximation factor of $\sqrt{2}$ and the approximation factor of exponential obtained in [2, 7, 12].

Remarkably, SVP has utilized the result of Minkowski's theorem [5, Theorem 16.2.9] to find the shortest possible set of vectors that can span the lattice. However, the theorem of Minkowski only proved the existence of a shortest nonzero vector, yet it cannot find such a vector. For this reason, an approximation algorithm is required to solve the problem. Thus, it is found that the LLL (Lenstra-Lenstra-Lovasz) algorithm [7] can solve SVP but only in small dimensions. While in large dimensions, unfortunately, the LLL algorithm does not perform well in solving SVP. The LLL algorithm is known for its practicality in finding a basis that is reduced in a specific way with properties such as shorter and have a smaller coefficient than the original basis. These reduced bases, which are called the LLL-reduced bases are easier to work with and analyzed. This makes them particularly useful for solving problems in both number theory and cryptography. In particular, precise LLL-reduced bases have been used to improve the security of certain cryptographic systems, such as the GGH cryptosystem [8]. They have also been used to build efficient attacks using the lattice problem to upgrade the security of the GGH cryptosystem [9].

Notably, how well the LLL-reduced bases relatively depends on the value of factor δ in the Lovász condition with the value of factor δ is restricted in the interval $(1/4, 1)$. Intuitively, Lenstra et al. [7] has chosen a certain value δ equal to $3/4$ in the construction of the LLL algorithm, and that value is considered to be the best value for the factor δ in the LLL-reduced basis so far. This work investigates the properties of the LLL-reduced basis with improved values of factor δ. By studying the existing value of factor δ in the LLL-reduced basis, this paper identifies some values of factor δ that is greater than the value δ equal to $3/4$ and then establishes the properties of the LLL-reduced basis that are associated with the proposed δ values. This paper also establishes the properties of the LLL-reduced basis with all values of factor δ in the interval $1/4$ to 1. In addition, this work has constituted the relationship between the initial lattice vector and the factor δ in the LLL-reduced basis. Thus, this paper is organized as follows: Section 2 gives the preliminaries of the lattice basis and some existing results related to the lattice basis. Section 3 provides the properties of the LLL-reduced basis by taking into account the new values of factor δ. Finally, Section 4 presents the conclusion.

2 Preliminaries

This section gives the preliminaries on the lattices, Gram-Schmidt orthogonalization method together with some existing results related to the Gram-Schmidt orthogonal basis, and LLL-reduced basis that are required in the next section.

2.1 Lattices

Let n and m be a positive integer, a lattice is a set of linear combination of vectors in $\mathbb{R}^m$ $(m \geq n)$ that is defined by

$$\mathcal{L}(\vec{b_1}, \ldots, \vec{b_n}) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\},$$

which is generated by a lattice basis $\vec{b_1}, \ldots, \vec{b_n}$. A lattice $\mathcal{L}$ is called a full rank lattice when $m = n$, where n is the lattice rank and m is the lattice dimension (refer [5, Definition 16.1.1]). A lattice $\mathcal{L}$ with dimension $m \geq 2$ always has a basis where such a lattice basis is generally not unique.

2.2 Gram-schmidt orthogonalization

Through the Gram-Schmidt process, any basis in the vector space $V = span(\vec{b_1}, \ldots, \vec{b_n})$ can be converted into a Gram-Schmidt orthogonal basis $\vec{b_1^*}, \ldots, \vec{b_n^*}$. Noting that, the produced Gram-Schmidt orthogonal basis $\vec{b_i^*}$ is the component of $\vec{b_i}$ orthogonal to $span(\vec{b_1}, \ldots, \vec{b_n})$ that is defined by the following formula [5, Appendix A.10.2]

$$\vec{b_i^*} = \vec{b_i} - \sum_{j=1}^{i-1} u_{i,j} \vec{b_j^*}, \text{ where } u_{i,j} = \frac{\langle \vec{b_i} \ , \ \vec{b_j^*} \rangle}{\langle \vec{b_j^*} \ , \ \vec{b_j^*} \rangle} \tag{1}$$

for $1 \leq j < i \leq n$ with setting $\vec{b_1^*} = \vec{b_1}$. In specific, the number of the Gram-Schmidt orthogonal basis $\vec{b_i^*}$ matches the number of basis vector $\vec{b_i}$ together with the additional terms. Those additional terms are parts of the basic vector $\vec{b_i}$ that are not orthogonal. The Gram-Schmidt orthogonal vector $\vec{b_i^*}$ satisfies some properties as in the following lemmas.

Lemma 2.1. [5, *Lemma 17.2.2*] *Let* $\{\vec{b_1}, \ldots, \vec{b_n}\}$ *be linearly independent in* $\mathbb{R}^m$ *and let* $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ *be the Gram-Schmidt orthogonalization. Then,*

1. $\|\vec{b_i^*}\| \leq \|\vec{b_i}\|$ *for* $1 \leq i \leq n$.
2. $\langle \vec{b_i} \ , \ \vec{b_i^*} \rangle = \langle \vec{b_i^*} \ , \ \vec{b_i^*} \rangle$ *for* $1 \leq i \leq n$.
3. *Denote the closest integer to* $u_{k,j}$ *by* $\lfloor u_{k,j} \rceil$. *If* $\vec{b_k'} = \vec{b_k} - \lfloor u_{k,j} \rceil \vec{b_j}$ *for* $1 \leq k \leq n$ *and* $1 \leq j < k$ *and if* $u'_{k,j} = \langle \vec{b_i^*} \ , \ \vec{b_i^*} \rangle$, *then* $\lfloor u'_{k,j} \rceil \leq 1/2$.

Lemma 2.2. [6, *Proposition 7.68*] *Let* $\{\vec{b_1}, \ldots, \vec{b_n}\}$ *be a basis for a lattice* $\mathcal{L}$ *and let* $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ *be the associated Gram-Schmidt orthogonal basis. Then,* $\det(\mathcal{L}) = \prod_{i=1}^{n} \|\vec{b_i^*}\|$.

Lemma 2.3. [11, *Lemma 7*] *If* $\{\vec{b_1}, \ldots, \vec{b_n}\}$ *is a basis of a lattice* $\mathcal{L}$, *then its Gram-Schmidt orthogonal basis* $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ *satisfies* $\min_{j \leq i \leq n} \|\vec{b_i^*}\| \leq \lambda_j$ *for all* $1 \leq j \leq n$.

2.3 LLL-reduced basis

Some of the lattice bases may be short or nearly orthogonal, and those lattice bases are called reduced lattice bases. Remarkably, the Gram-Schmidt orthogonal vector $\vec{b_i^*}$ may become an LLL-reduced basis. By definition, the LLL-reduced basis with factor δ is said to satisfy the following conditions:

1. $|u_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$, (Size reduced condition)
2. $\|\vec{b_i^*}\|^2 \geq (\delta - u_{i,j}^2)\|\vec{b_j^*}\|^2$ for $1/4 < \delta < 1$, and $1 \leq j < i \leq n$, (Lovász condition)

where $u_{i,j} = \langle \vec{b_i}\ ,\ \vec{b_j^*} \rangle / \langle \vec{b_j^*}\ ,\ \vec{b_j^*} \rangle$ and $\|\vec{b_i^*}\|^2 = \langle \vec{b_i^*}\ ,\ \vec{b_i^*} \rangle$ (refer [5, Definition 17.2.4]). If the coefficient $u_{i,j}$ is equal to 0 for all i and j, then the basis becomes orthogonal. Indeed, the results obtained in the following section has indicated that the LLL-reduced basis with the new adjusted values of factor δ is seen to be stronger, in terms of the upper bounds obtained.

3 Properties Related to δ-LLL-Reduced Basis

This section is the culmination of results obtained in this work. Properties related to LLL-reduced basis with factor δ are discussed in this section taking into consideration the new adjusted values of factor δ. More new results on relationship between the initial vector and the factor δ in LLL-reduced basis are also presented here.

For convenience, the term δ-LLL-reduced basis is used to represent the term LLL-reduced basis with factor δ. In the interval $(1/4, 1)$, the value δ equal to $3/4$ is traditionally chosen to be the best value of factor δ in δ-LLL-reduced basis and its properties as in [5, Lemma 17.2.8]. The reason is that the value δ equal to $3/4$ yields the smallest integer value for the term α, that is, $\alpha = 2$, where the term α is defined as follows.

Definition 3.1. *Let* $1/4 < \delta < 1$ *and set* $\alpha = (\delta - 1/4)^{-1}$, *then the orthogonal lattice vectors* $\vec{b_1^*}, \ldots, \vec{b_n^*}$ *is said to be reduced with respect to* α *when* $\|\vec{b_j^*}\|^2 \leq \alpha \|\vec{b_i^*}\|^2$ *for* $4/3 < \alpha < \infty$ *and* $1 \leq j < i \leq n$.

Instead of value δ equal to $3/4$, Galbraith [5] established the properties of an LLL-reduced basis using the value δ equal to 0.957 [5, Lemma 17.2.9] and shown that the value has a stronger δ-LLL-reduced basis than a $3/4$-LLL-reduced basis. Motivated by this result, it is possible to find another value for the factor δ in the interval between $3/4$ and 1 that will have a stronger δ-LLL-reduced basis than the $3/4$-LLL-reduced basis. Thus, the proposed value δ will be in the interval (3/4,1) that is divided into two different intervals such as the interval between $3/4$ and 0.957, and the interval between 0.957 and 1.

3.1 A factor δ in the interval between $3/4$ and 0.957

For the interval between $3/4$ and 0.957, the value δ equal to 0.935 is chosen because this value is the closest value to 0.957 that has the strongest LLL-reduced basis compared to $3/4$-LLL-reduced basis even though weaker than 0.957-LLL-reduced basis. Thus, the 0.935-LLL-reduced basis has the properties described as follows.

Proposition 3.1. *Let $\{\vec{b_1}, \ldots, \vec{b_n}\}$ be linearly independent in $\mathcal{L} \subset \mathbb{R}^m$ and let $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ be an LLL-reduced basis with $\delta = 1/4+1/\sqrt[11]{64} \approx 0.935$. Notably, $\|\vec{b^*}\|^2 = \langle \vec{b^*} \ , \ \vec{b^*} \rangle$. Then, the following conditions hold:*

1. $\|\vec{b_j^*}\|^2 \leq 2^{6(i-j)/11}\|\vec{b_i^*}\|^2$ *for* $1 \leq j \leq i \leq n$.
2. $\|\vec{b_i^*}\|^2 \leq \|\vec{b_i}\|^2 \leq (\frac{1}{4} + 2^{6(i-1)/11})\|\vec{b_i^*}\|^2$ *for* $1 \leq i \leq n$.
3. $\|\vec{b_j}\| \leq 2^{3i/11}\|\vec{b_i^*}\|$ *for* $1 \leq j \leq i \leq n$.

Proof.

1. Use the value $\delta = 1/4+1/\sqrt[11]{64} \approx 0.935$ in the Definition 3.1 yields $\alpha = 200/137$ and satisfies $\|\vec{b_j^*}\|^2 \leq (200/137)\|\vec{b_i^*}\|^2$. Since $200/137 = 1.459854015 \approx 2^{6/11} = 1.459480106$, then the inequality is equivalent to $\|\vec{b_j^*}\|^2 \leq (2^{6/11})\|\vec{b_i^*}\|^2$. Thus, part 1 follows from the mathematical induction.
2. By Equation (1), let

$$\begin{aligned}\|\vec{b_i}\|^2 = \langle \vec{b_i} \ , \ \vec{b_i} \rangle &= \langle \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*} \ , \ \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*} \rangle \\ &= \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} u_{i,j}^2\|\vec{b_j^*}\|^2 \\ &\leq \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1}(1/4)\|\vec{b_j^*}\|^2,\end{aligned}$$

due to the size-reduced condition applied to the last inequality. Then, using part 1 to the last inequality gives

$$\|\vec{b_i}\|^2 \leq \|\vec{b_i^*}\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{6(i-j)/11}\|\vec{b_i^*}\|^2 = \left(1 + \frac{1}{4}\sum_{j=1}^{i-1}(2^{6/11})^{i-j}\right)\|\vec{b_i^*}\|^2.$$

Note that the term

$$\sum_{j=1}^{i-1}(2^{6/11})^{i-j} = 2^{6i/11}\sum_{j=1}^{i-1}(2^{-6/11})^{j} = 2^{6i/11}\sum_{j=2}^{i}(2^{-6/11})^{j-1}.$$

Using the formula of the geometric series for finite sum to the equation above yields

$$2^{6i/11}\sum_{j=2}^{i}(2^{-6/11})^{j-1} = 2^{6i/11}\left(\frac{(2^{-6/11})^1 - (2^{-6/11})^i}{1-(2^{-6/11})}\right) = \frac{2^{6i/11} - 2^{6/11}}{2^{6/11}-1}.$$

Thus,

$$\begin{aligned}\|\vec{b_i}\|^2 &\leq \left(1+\frac{1}{4}\left(\frac{2^{6i/11}-2^{6/11}}{2^{6/11}-1}\right)\right)\|\vec{b_i^*}\|^2\\ &= \left(\frac{2^{6/11}-1-2^{-16/11}}{2^{6/11}-1}+\frac{2^{6(i-1)/11}}{(2^{6/11}-1)2^{16/11}}\right)\|\vec{b_i^*}\|^2\\ &= \frac{1}{(2^{6/11}-1)2^{16/11}}\left(2^{22/11}-2^{16/11}-1+2^{6(i-1)/11}\right)\|\vec{b_i^*}\|^2\\ &\leq \left(2^2-2^{16/11}-1+2^{6(i-1)/11}\right)\|\vec{b_i^*}\|^2\\ &= \left(0.259+2^{6(i-1)/11}\right)\|\vec{b_i^*}\|^2.\end{aligned}$$

Rewriting this in a fractional term gives $\|\vec{b_i}\|^2 \leq \left(1/4+2^{6(i-1)/11}\right)\|\vec{b_i^*}\|^2$. Therefore, part 2 is obtained after applying Lemma 2.1 (part 1) to the latter inequality.

3. Consider a part of the last inequality from the part 2, that is $1/4+2^{6(j-1)/11}$, yields

$$\frac{1}{4}+2^{6(j-1)/11} \leq 2^{6j/11},$$

since $j \geq 1$. Then, the part 2 becomes $\|\vec{b_j}\|^2 \leq 2^{6j/11}\|\vec{b_j^*}\|^2$. After that, applying part 1 to the latter inequality gives

$$\|\vec{b_j}\|^2 \leq 2^{6j/11}\left(2^{6(i-j)/11}\|\vec{b_i^*}\|^2\right) = 2^{6i/11}\|\vec{b_i^*}\|^2.$$

Then, taking the square root of the above inequality yields part 3.

□

3.2 A factor δ in the interval between 0.957 and 1

For the interval 0.957 and 1, the value δ equal to 0.993 is chosen because this value is the closest value to 1 that has a stronger LLL-reduced basis than 0.957-LLL-reduced basis. Here are the properties of the 0.993-LLL-reduced basis.

Proposition 3.2. *Let $\{\vec{b_1},\ldots,\vec{b_n}\}$ be linearly independent in $\mathcal{L} \subset \mathbb{R}^m$ and let $\{\vec{b_1^*},\ldots,\vec{b_n^*}\}$ be an δ-LLL-reduced basis with $\delta = 1/4+1/\sqrt[7]{8} \approx 0.993$. Notably, $\|\vec{b^*}\|^2 = \langle \vec{b^*}\ ,\ \vec{b^*}\rangle$. Then, the following conditions hold:*

1. $\|\vec{b_j^*}\|^2 \leq 2^{3(i-j)/7}\|\vec{b_i^*}\|^2$ *for* $1 \leq j \leq i \leq n$.
2. $\|\vec{b_i^*}\|^2 \leq \|\vec{b_i}\|^2 \leq (\frac{1}{36}+2^{3(i-1)/7})\|\vec{b_i^*}\|^2$ *for* $1 \leq i \leq n$.
3. $\|\vec{b_j}\| \leq 2^{3i/14}\|\vec{b_i^*}\|$ *for* $1 \leq j \leq i \leq n$.

Proof. The proof followed a similar argument as Proposition 3.1.

1. Use the value $\delta = 1/4+1/\sqrt[7]{8} \approx 0.993$ in the Definition 3.1 yields $\alpha = 1000/743$ and satisfies $\|\vec{b_j^*}\|^2 \leq (1000/743)\|\vec{b_i^*}\|^2$. Since $1000/743 = 1.34589502 \approx 2^{3/7} = 1.345900193$, then the inequality is equivalent to $\|\vec{b_j^*}\|^2 \leq (2^{3/7})\|\vec{b_i^*}\|^2$. Thus, part 1 follows from the mathematical induction.

2. By Equation (1), let

$$\begin{aligned}\|\vec{b_i}\|^2 = \langle \vec{b_i}\ ,\ \vec{b_i}\rangle &= \langle \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*}\ ,\ \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*}\rangle \\ &= \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} u_{i,j}^2 \|\vec{b_j^*}\|^2 \\ &\leq \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} (1/4)\|\vec{b_j^*}\|^2,\end{aligned}$$

due to the size-reduced condition applied to the last inequality. Then, using part 1 to the last inequality gives

$$\|\vec{b_i}\|^2 \leq \|\vec{b_i^*}\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{3(i-j)/7}\|\vec{b_i^*}\|^2 = \left(1 + \frac{1}{4}\sum_{j=1}^{i-1}(2^{3/7})^{i-j}\right)\|\vec{b_i^*}\|^2.$$

Note that the term

$$\sum_{j=1}^{i-1}(2^{3/7})^{i-j} = 2^{3i/7}\sum_{j=1}^{i-1}(2^{-3/7})^{j} = 2^{3i/7}\sum_{j=2}^{i}(2^{-3/7})^{j-1}.$$

Using the formula of the geometric series for finite sum to the inequality above yields

$$2^{3i/7}\sum_{j=2}^{i}(2^{-3/7})^{j-1} = 2^{3i/7}\left(\frac{(2^{-3/7})^1 - (2^{-3/7})^i}{1-(2^{-3/7})}\right) = \frac{2^{3i/7} - 2^{3/7}}{2^{3/7}-1}.$$

Thus,

$$\begin{aligned}\|\vec{b_i}\|^2 &\leq \left(1 + \frac{1}{4}\left(\frac{2^{3i/7} - 2^{3/7}}{2^{3/7}-1}\right)\right)\|\vec{b_i^*}\|^2 \\ &= \left(\frac{2^{3/7} - 1 - 2^{-11/7}}{2^{3/7}-1} + \frac{2^{3(i-1)/7}}{(2^{3/7}-1)2^{11/7}}\right)\|\vec{b_i^*}\|^2 \\ &= \frac{1}{(2^{3/7}-1)2^{11/7}}\left(2^{14/7} - 2^{11/7} - 1 + 2^{3(i-1)/7}\right)\|\vec{b_i^*}\|^2 \\ &\leq \left(2^2 - 2^{11/7} - 1 + 2^{3(i-1)/7}\right)\|\vec{b_i^*}\|^2 \\ &= \left(0.028 + 2^{3(i-1)/7}\right)\|\vec{b_i^*}\|^2.\end{aligned}$$

Rewriting this in a fractional term gives $\|\vec{b_i}\|^2 \leq \left(1/36 + 2^{3(i-1)/7}\right)\|\vec{b_i^*}\|^2$. Therefore, part 2 is obtained after applying Lemma 2.1 (part 1) to the latter inequality.

3. Consider a part of the last inequality from the part 2, that is $1/36 + 2^{3(j-1)/7}$, yields

$$\frac{1}{36} + 2^{3(j-1)/7} \leq 2^{3j/7},$$

since $j \geq 1$. Then, part 2 becomes $\|\vec{b_j}\|^2 \leq 2^{3j/7}\|\vec{b_j^*}\|^2$. After that, applying part 1 to the latter inequality gives

$$\|\vec{b_j}\|^2 \leq 2^{3j/7}\left(2^{3(i-j)/7}\|\vec{b_i^*}\|^2\right) = 2^{3i/7}\|\vec{b_i^*}\|^2.$$

Then, the square root of the above inequality complete the proof of part 3.

□

3.2.1 A factor δ in the interval between $1/4$ and 1

From the existing and the proposed results, it was found that the properties of the δ-LLL-reduced basis can be generalized to all values of factor δ in the interval $(1/4, 1)$. Thus, the properties of the δ-LLL-reduced basis in the interval $(1/4, 1)$ is established as the following theorem.

Theorem 3.1. *Let $\{\vec{b_1}, \ldots, \vec{b_n}\}$ be linearly independent in $\mathcal{L} \subset \mathbb{R}^m$ and let $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ be an δ-LLL-reduced basis with $1/4 < \delta < 1$. Notably, $\|\vec{b^*}\|^2 = \langle \vec{b^*}\ ,\ \vec{b^*} \rangle$. Then, the following conditions hold:*

1. $\|\vec{b_j^*}\|^2 \leq (\delta - 1/4)^{-(i-j)} \|\vec{b_i^*}\|^2$ *for* $1 \leq j \leq i \leq n$.
2. $\|\vec{b_i^*}\|^2 \leq \|\vec{b_i}\|^2 \leq \big(4(1-\delta) + (\delta - 1/4)^{-(i-1)}\big)\|\vec{b_i^*}\|^2$ *for* $2 \leq i \leq n$.
3. $\|\vec{b_j}\| \leq (\delta - 1/4)^{-i/2} \|\vec{b_i^*}\|$ *for* $1 \leq j \leq i \leq n$.

Proof. The proof followed a similar argument as Proposition 3.1.

1. From Definition 3.1, it is known that $\|\vec{b_j^*}\|^2 \leq 1/(\delta - 1/4)\|\vec{b_i^*}\|^2$ for $1 \leq j < i \leq n$. By the mathematical induction, part 1 is obtained.
2. Since Equation (1) gives $\vec{b_i} = \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*}$, then

$$\|\vec{b_i}\|^2 = \langle \vec{b_i}\ ,\ \vec{b_i} \rangle = \langle \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*}\ ,\ \vec{b_i^*} + \sum_{j=1}^{i-1} u_{i,j}\vec{b_j^*} \rangle = \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} u_{i,j}^2 \|\vec{b_j^*}\|^2.$$

From the size reduced condition, $|u_{i,j}| \leq 1/2$, it is found that $u_{i,j}^2 \leq 1/4$. Thus, the equation above becomes $\|\vec{b_i}\|^2 \leq \|\vec{b_i^*}\|^2 + (1/4)\sum_{j=1}^{i-1} \|\vec{b_j^*}\|^2$. After that, using part 1 to the latter inequality gives

$$\begin{aligned} \|\vec{b_i}\|^2 &\leq \|\vec{b_i^*}\|^2 + \frac{1}{4}\sum_{j=1}^{i-1} \left(\delta - \frac{1}{4}\right)^{-(i-j)} \|\vec{b_i^*}\|^2 \\ &= \left(1 + \frac{1}{4}\sum_{j=1}^{i-1} \left(\delta - \frac{1}{4}\right)^{-(i-j)}\right)\|\vec{b_i^*}\|^2. \end{aligned}$$

Note that the term

$$\sum_{j=1}^{i-1} \left(\delta - \frac{1}{4}\right)^{-(i-j)} = \left(\delta - \frac{1}{4}\right)^{-i} \sum_{j=1}^{i-1} \left(\delta - \frac{1}{4}\right)^{j} = \left(\delta - \frac{1}{4}\right)^{-i} \sum_{j=2}^{i} \left(\delta - \frac{1}{4}\right)^{j-1}.$$

Using the formula of the geometric series for finite sum,

$$\sum_{k=m}^{n} r^{k-1} = \frac{r^{m-1} - r^n}{1 - r}, \qquad r \neq 1$$

to the last equation above gives

$$\begin{aligned} \left(\delta - \frac{1}{4}\right)^{-i} \sum_{j=2}^{i} \left(\delta - \frac{1}{4}\right)^{j-1} &= \left(\delta - \frac{1}{4}\right)^{-i} \left(\frac{(\delta - 1/4)^1 - (\delta - 1/4)^i}{1 - (\delta - 1/4)}\right) \\ &= \left(\frac{4}{5 - 4\delta}\right)\left(\left(\delta - \frac{1}{4}\right)^{-(i-1)} - 1\right). \end{aligned}$$

Thus,

$$\begin{aligned}\|\vec{b_i}\|^2 &\leq \left(1+\frac{1}{4}\left[\left(\frac{4}{5-4\delta}\right)\left(\left(\delta-\frac{1}{4}\right)^{-(i-1)}-1\right)\right]\right)\|\vec{b_i^*}\|^2\\ &= \left(\left(\frac{4-4\delta}{5-4\delta}\right)+\left(\frac{1}{5-4\delta}\right)\left(\delta-\frac{1}{4}\right)^{-(i-1)}\right)\|\vec{b_i^*}\|^2\\ &= \left(\frac{1}{5-4\delta}\right)\left((4-4\delta)+\left(\delta-\frac{1}{4}\right)^{-(i-1)}\right)\|\vec{b_i^*}\|^2\\ &\leq \left(4(1-\delta)+\left(\delta-\frac{1}{4}\right)^{-(i-1)}\right)\|\vec{b_i^*}\|^2.\end{aligned}$$

Squaring part 1 of Lemma 2.1 and then applying it to the latter inequality yields part 2.

3. Part 3 follows from the last inequality above for $j \geq 1$. Thus, producing the following inequality

$$4(1-\delta)+(\delta-1/4)^{-(j-1)} \leq (\delta-1/4)^{-j}.$$

This implies $\|\vec{b_j}\|^2 \leq (\delta-1/4)^{-j}\|\vec{b_j^*}\|^2$. Applying part 1 to this inequality gives

$$\|\vec{b_j}\|^2 \leq \left(\delta-\frac{1}{4}\right)^{-i}\|\vec{b_i^*}\|^2.$$

Taking the square root of the above gives the desired result.

□

3.3 Relationship between the initial vector and the factor δ in LLL-reduced basis

Knowing that the Lovász condition can produce the following inequality

$$\|\vec{b_1^*}\|^2 \leq \alpha\|\vec{b_2^*}\|^2 \leq \alpha\big(\alpha\|\vec{b_3^*}\|^2\big) \leq \cdots \leq \alpha^{i-1}\|\vec{b_i^*}\|^2,$$

which can be reduced to

$$\|\vec{b_1^*}\|^2 \leq \alpha^{i-1}\|\vec{b_i^*}\|^2 \leq \alpha^{n-1}\|\vec{b_i^*}\|^2.$$

Then, take the square roots of the latter inequality gives

$$\|\vec{b_1^*}\| \leq \alpha^{(i-1)/2}\|\vec{b_i^*}\| \leq \alpha^{(n-1)/2}\min_{1\leq i\leq n}\|\vec{b_i^*}\|,$$

and apply part 1 of Lemma 2.1 to the leading term yields

$$\|\vec{b_1}\| \leq \alpha^{(i-1)/2}\|\vec{b_i^*}\| \leq \alpha^{(n-1)/2}\min_{1\leq i\leq n}\|\vec{b_i^*}\|. \tag{2}$$

Interestingly, the inequality above can give a bound for $\|\vec{b_1}\|$ that will lead to two different lengths of $\vec{b_1}$ which is related to the determinant of the lattice, $\det(\mathcal{L})$, and the successive minima, λ. Thus, these two upper bounds on $\|\vec{b_1}\|$ is represented as follows.

Proposition 3.3. *Let $\{\vec{b_1},\ldots,\vec{b_n}\}$ be linearly independent in $\mathcal{L}\subset\mathbb{R}^m$. For any $1/4<\delta<1$, the initial vector of δ-LLL-reduced basis satisfies*

$$\|\vec{b_1}\| \leq \left(\delta-\frac{1}{4}\right)^{-(n-1)/4}\big(\det(\mathcal{L})\big)^{1/n} \quad \textit{and} \quad \|\vec{b_1}\| \leq \left(\delta-\frac{1}{4}\right)^{-(n-1)/2}\lambda_1.$$

Proof. For the upper bound of $\|\vec{b_1}\|$ related to determinant of the lattice, $\det(\mathcal{L})$, multiply the leading inequality of Equation (2) over $1 \leq i \leq n$ leads to the following relation,

$$\|\vec{b_1}\|^n \leq \prod_{i=1}^{n} \alpha^{(i-1)/2} \|\vec{b_i^*}\| = \alpha^{n(n-1)/4} \prod_{i=1}^{n} \|\vec{b_i^*}\| = \alpha^{n(n-1)/4} \det(\mathcal{L}),$$

where the last inequality follows from Lemma 2.2. Next, taking the n-th root of the inequality above gives

$$\|\vec{b_1}\| \leq \alpha^{(n-1)/4} \big(\det(\mathcal{L})\big)^{1/n}.$$

From Definition 3.1, it is known that $\alpha = (\delta - 1/4)^{-1}$. By applying this to the inequality above, the desired upper bound is obtained.

For the upper bound of $\|\vec{b_1}\|$ related to successive minima, λ, use Lemma 2.3 to the last inequality of Equation (2) as follows,

$$\|\vec{b_1}\| \leq \alpha^{(n-1)/2} \min_{1 \leq i \leq n} \|\vec{b_1^*}\| \leq \alpha^{(n-1)/2} \lambda_1.$$

Similarly, applying Definition 3.1 to the last inequality yields the desired upper bound. □

Furthermore, an upper bound of $\|\vec{b_1}\|$ can lead to the following properties.

Proposition 3.4. *Let $\{\vec{b_1}, \ldots, \vec{b_n}\}$ be linearly independent in $\mathcal{L} \subset \mathbb{R}^m$. For any $1/4 < \delta < 1$, an δ-LLL-reduced basis $\{\vec{b_1^*}, \ldots, \vec{b_n^*}\}$ has the following properties:*

$$\|\vec{b_i}\| \leq \left(\delta - \frac{1}{4}\right)^{-(i-1)/2} \|\vec{b_i^*}\| \quad for \quad 1 \leq i \leq n,$$
$$\prod_{i=1}^{n} \|\vec{b_i}\| \leq \left(\delta - \frac{1}{4}\right)^{-n(n-1)/4} \det(\mathcal{L}) \quad for \quad 1 \leq i \leq n.$$

Thus, LLL-reduced basis (with a factor δ) solves apprSVP to within a factor of $(\delta - 1/4)^{-(n-1)/2}$.

Proof. To prove the first property, put the size-reduced condition into the Lovász condition as follows,

$$\|\vec{b_j^*}\|^2 \leq \left(\delta - \frac{1}{4}\right)^{-1} \|\vec{b_i^*}\|^2.$$

Apply the latter inequality repeatedly gives

$$\|\vec{b_j^*}\|^2 \leq \left(\delta - \frac{1}{4}\right)^{-(i-j)} \|\vec{b_i^*}\|^2. \tag{3}$$

Now, use Equation (1) to obtain

$$\|\vec{b_i}\|^2 = \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} u_{i,j}^2 \|\vec{b_j^*}\|^2 \leq \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} \left(\frac{1}{4}\right) \|\vec{b_j^*}\|^2,$$

due to the size-reduced condition applied to the last inequality. Next, use Equation (3) to the inequality above yields

$$\|\vec{b_i}\|^2 \leq \|\vec{b_i^*}\|^2 + \sum_{j=1}^{i-1} \left(\frac{1}{4}\right)\left(\delta - \frac{1}{4}\right)^{-(i-j)} \|\vec{b_i^*}\|^2 = \left(1 + \frac{1}{4}\sum_{j=1}^{i-1}\left(\delta - \frac{1}{4}\right)^{-(i-j)}\right)\|\vec{b_i^*}\|^2.$$

Note that the term

$$\sum_{j=1}^{i-1}\left(\delta - \frac{1}{4}\right)^{-(i-j)} = \left(\delta - \frac{1}{4}\right)^{-i}\sum_{j=1}^{i-1}\left(\delta - \frac{1}{4}\right)^{j} = \left(\delta - \frac{1}{4}\right)^{-i}\sum_{j=2}^{i}\left(\delta - \frac{1}{4}\right)^{j-1}.$$

Using the formula of the geometric series for finite sum,

$$\sum_{k=m}^{n} r^{k-1} = \frac{r^{m-1} - r^n}{1-r}, \qquad r \neq 1$$

to the last equation above gives

$$\begin{aligned}\left(\delta - \frac{1}{4}\right)^{-i}\sum_{j=2}^{i}\left(\delta - \frac{1}{4}\right)^{j-1} &= \left(\delta - \frac{1}{4}\right)^{-i}\left(\frac{(\delta - 1/4)^1 - (\delta - 1/4)^i}{1 - (\delta - 1/4)}\right) \\ &= \left(\frac{4}{5-4\delta}\right)\left(\left(\delta - \frac{1}{4}\right)^{-(i-1)} - 1\right).\end{aligned}$$

Thus,

$$\begin{aligned}\|\vec{b_i}\|^2 &\leq \left(1 + \frac{1}{4}\left[\left(\frac{4}{5-4\delta}\right)\left(\left(\delta - \frac{1}{4}\right)^{-(i-1)} - 1\right)\right]\right)\|\vec{b_i^*}\|^2 \\ &= \left(\left(\frac{4-4\delta}{5-4\delta}\right) + \left(\frac{1}{5-4\delta}\right)\left(\delta - \frac{1}{4}\right)^{-(i-1)}\right)\|\vec{b_i^*}\|^2 \\ &= \left(\frac{1}{5-4\delta}\right)\left((4-4\delta) + \left(\delta - \frac{1}{4}\right)^{-(i-1)}\right)\|\vec{b_i^*}\|^2.\end{aligned}$$

Since

$$\left(\frac{1}{5-4\delta}\right)\left((4-4\delta) + \left(\delta - \frac{1}{4}\right)^{-(i-1)}\right) \leq \left(\delta - \frac{1}{4}\right)^{-(i-1)},$$

then $\|\vec{b_i}\|^2 \leq (\delta - 1/4)^{-(i-1)}\|\vec{b_i^*}\|^2$. By taking the square root of the latter inequality yields the first property.

For the second property, multiply the first property by itself n-times as

$$\prod_{i=1}^{n}\|\vec{b_i}\| \leq \prod_{i=1}^{n}\left(\delta - \frac{1}{4}\right)^{-(i-1)/2}\|\vec{b_i^*}\| = \left(\delta - \frac{1}{4}\right)^{-n(n-1)/4}\prod_{i=1}^{n}\|\vec{b_i^*}\|.$$

By applying Lemma 2.2 to the last inequality above, the second property is obtained. □

In addition, the properties from the Proposition 3.4 can be generalized to the following result.

Proposition 3.5. *Let δ-LLL-reduced basis $\{\vec{b_1}, \ldots, \vec{b_n}\}$ be in a lattice $\mathcal{L} \subset \mathbb{R}^m$. Notably, $\|\vec{b}\|$ is the Euclidean norm. For any $1/4 < \delta < 1$, the following properties hold:*

1. $\|\vec{b_j}\| \leq \left(\delta - \frac{1}{4}\right)^{-n/2} \lambda_j$ *for* $1 \leq j \leq n$.
2. $\left(\delta - \frac{1}{4}\right)^{j/2} \lambda_j \leq \|\vec{b_j}\| \leq \left(\delta - \frac{1}{4}\right)^{-n/2} \lambda_j$ *for* $1 \leq j \leq n$.
3. $\|\vec{b_j}\| \leq \left(\delta - \frac{1}{4}\right)^{-n/4} \left(\det(\mathcal{L})\right)^{1/n}$ *for* $1 \leq j \leq n$.
4. $\det(\mathcal{L}) \leq \prod_{j=1}^{n} \|\vec{b_j}\| \leq \left(\delta - \frac{1}{4}\right)^{-n(n-1)/4} \det(\mathcal{L})$ *for* $1 \leq j \leq n$.

Proof.

1. Part 3 of Theorem 3.1 implies that

$$\|\vec{b_j}\| \leq \left(\delta - \frac{1}{4}\right)^{-i/2} \|\vec{b_i^*}\| = \min_{j \leq i \leq n} \left(\delta - \frac{1}{4}\right)^{-i/2} \|\vec{b_i^*}\| \leq \left(\delta - \frac{1}{4}\right)^{-n/2} \min_{j \leq i \leq n} \|\vec{b_i^*}\|.$$

   Then, applying Lemma 2.3 to the last inequality yields part 1.

2. For the lower bound part, consider part 3 of Theorem 3.1 as follows,

$$\left(\delta - \frac{1}{4}\right)^{-i/2} \|\vec{b_i^*}\| \geq \|\vec{b_j}\| = \max_{1 \leq j \leq i} \|\vec{b_j}\| \geq \lambda_i, \quad \text{or} \quad \|\tilde{\mathrm{b}_\mathrm{i}^*}\| \geq \left(\delta - \frac{1}{4}\right)^{\mathrm{i}/2} \lambda_\mathrm{i}.$$

   Then, applying part 1 of Lemma 2.1 to the leading term of the last inequality above becomes

$$\|\vec{b_i}\| \geq \left(\delta - \frac{1}{4}\right)^{i/2} \lambda_i.$$

   Let $i = j$, then the lower bound is obtained. While the upper bound is given in part 1, thus, part 2 follows.

3. Multiply part 3 of Theorem 3.1 over n times obtaining the following inequality,

$$\|\vec{b_j}\|^n \leq \prod_{i=1}^{n} \left(\delta - \frac{1}{4}\right)^{-i/2} \|\vec{b_i^*}\| = \left(\delta - \frac{1}{4}\right)^{-n^2/4} \prod_{i=1}^{n} \|\vec{b_i^*}\| = \left(\delta - \frac{1}{4}\right)^{-n^2/4} \det(\mathcal{L}),$$

   where the last inequality followed from Lemma 2.2. Thus, taking the n-th roots of the inequality above yields part 3.

4. Combining part 1 of Lemma 2.1 with the first properties of Proposition 3.4 gives

$$\vec{b_i^*}\| \leq \|\vec{b_i}\| \leq \left(\delta - \frac{1}{4}\right)^{-(i-1)/2} \|\vec{b_i^*}\|.$$

   Then, multiplying the inequality over $1 \leq i \leq n$ yields

$$\prod_{i=1}^{n} \|\vec{b_i^*}\| \leq \prod_{i=1}^{n} \|\vec{b_i}\| \leq \prod_{i=1}^{n} \left(\delta - \frac{1}{4}\right)^{-(i-1)/2} \|\vec{b_i^*}\| = \left(\delta - \frac{1}{4}\right)^{-n(n-1)/4} \prod_{i=1}^{n} \|\vec{b_i^*}\|.$$

   Next, applying Lemma 2.2 to the inequality above becomes

$$\det(\mathcal{L}) \leq \prod_{i=1}^{n} \|\vec{b_i}\| \leq \left(\delta - \frac{1}{4}\right)^{-n(n-1)/4} \det(\mathcal{L}).$$

   Thus, part 4 is obtained when letting $i = j$.

□

4 Conclusions

In this work, new values of factor δ are proposed and new properties related to the LLL-reduced basis concerning the factor δ have been established. Previous works on the LLL-reduced basis technique, including the one by Galbraith, were on wider range of interval $1/4$ to 1. Whereas, in our work this interval is narrowed down to be within $3/4$ to 1. Based on the analyses done in this work, it is found that the new proposed values of factor δ have a stronger δ-LLL-reduced basis than the $3/4$-LLL-reduced basis in terms of the upper bounds obtained, where it provides a better reduced basis. In particular, the δ-LLL-reduced basis is well defined for δ equal to 1. As the values of a factor δ approaches 1, the values of the term α get smaller than 2. A factor δ equal to $3/4$ is known as the best value of factor δ in the Lovász condition, one of the conditions for a vector to be LLL-reduced basis and is used in the existing LLL algorithm. However, according to what has been discovered in this work, it is believed that the proposed value of a factor δ equal to 0.993 will be able to replace the existing value δ equal to $3/4$ and can be used for future implementation of LLL algorithm. It is also important to note that all the properties obtained in this paper are based on theoretical aspects. Nevertheless, these properties served as a foundation and a building block for further experimental design of LLL-reduced basis, where chosing the best or optimal values of δ would rely on a practical aspect and specific purpose of the application. Therefore, it is expected that more new results are yet to emerge from this work.

Acknowledgement The authors would like to thank the Ministry of Higher Education, Malaysia for the financial support under the Fundamental Research Grant Scheme (FRGS) (reference code: FRGS/1/2020/STG06/USM/01/1).

Conflicts of Interest The authors affirm that this paper has no conflict of interest.

References

[1] M. Ajtai (1998). The shortest vector problem in L_2 is NP-hard for randomized reductions. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pp. 10–19. Association for Computing Machinery, New York. https://doi.org/10.1145/276698.276705.

[2] M. Ajtai, R. Kumar & D. Sivakumar (2001). A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, pp. 601–610. Association for Computing Machinery, New York. https://doi.org/10.1145/380752.380857.

[3] J. Y. Cai & A. Nerurkar (1998). Approximating the SVP to within a factor $(1 + 1/\dim^{\varepsilon})$ is NP-hard under randomized conditions. In *Proceedings. Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, pp. 46–55. IEEE, Buffalo, New York. https://doi.org/10.1109/CCC.1998.694590.

[4] C. Dwork (1997). Positive applications of lattices to cryptography. In *International Symposium on Mathematical Foundations of Computer Science*, pp. 44–51. Springer, Berlin, Heidelberg. https://doi.org/10.1007/bfb0029948.

[5] S. D. Galbraith (2012). *Mathematics of public key cryptography*. Cambridge University Press, New York. https://doi.org/10.1017/cbo9781139012843.

[6] J. Hoffstein, J. Pipher & J. H. Silverman (2014). An introduction to cryptography. In *An Introduction to Mathematical Cryptography*, pp. 1–59. Springer, New York. https://doi.org/10.1007/978-1-4939-1711-2_1.

[7] A. K. Lenstra, H. W. Lenstra & L. Lovász (1982). Factoring polynomials with rational coefficients. *Mathematische annalen*, *261*(4), 515–534. https://doi.org/10.1007/bf01457454.

[8] A. Mandangan, H. Kamarulhaili & M. A. Asbullah (2019). On the smallest-basis problem underlying the GGH lattice-based cryptosystem. *Malaysian Journal of Mathematical Sciences*, *13*(S), 1–11.

[9] A. Mandangan, H. Kamarulhaili & M. A. Asbullah (2023). The efficiency of embedding-based attacks on the GGH lattice-based cryptosystem. *Malaysian Journal of Mathematical Sciences*, *17*(4), 673–690. https://doi.org/10.47836/mjms.17.4.09.

[10] D. Micciancio (2001). The shortest vector in a lattice is hard to approximate to within some constant. *SIAM Journal on Computing*, *30*(6), 2008–2035. https://doi.org/10.1137/s0097539700373039.

[11] P. Q. Nguyen & B. Vallée (2010). *The LLL algorithm: Survey and applications*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02295-1.

[12] C. P. Schnorr (1987). A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, *53*(2–3), 201–224. https://doi.org/10.1016/0304-3975(87)90064-8.

[13] P. van Emde Boas (1981). *Another NP-complete problem and the complexity of computing short vectors in a lattice*. Technical Report, Department of Mathmatics, University of Amsterdam.