Good basis vs bad basis: On the ability of Babai’s Round-off Method for solving the Closest Vector Problem

A Mandangan1,2, H Kamarulhaili1 and M A Asbullah3

1School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Penang, Gelugor, Pulau Pinang, Malaysia
2Mathematics, Real Time Graphics and Visualization Laboratory, Faculty of Sciences & Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia
3Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Sciences, Universiti Putra Malaysia, 43400 UPM Serdang, Serdang, Selangor, Malaysia
3Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Serdang, Selangor, Malaysia

Email: 1arifmandangan@student.usm.my, 3ma_asyraf@upm.edu.my

Abstract. A lattice basis is consisting of linearly independent basis vectors that span the lattice. A lattice in dimension of 2 and above have infinitely many bases. These bases have different quality in terms of the length (norm) and orthogonality of basis vectors. A lattice basis with reasonably short and orthogonal basis vectors is normally referred to as a ‘good basis’. On the contrary, a lattice basis with long and non-orthogonal basis vectors is normally referred to as a ‘bad basis’. The most establish hard problems in lattice are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). The solutions of these NP-hard problems can be categorized as exact and approximation solutions. Since the hardness of these problems significantly grows once the lattice dimension increases, approximation methods for solving these problems are preferable in practice. Babai’s Round-off Method is an approximation method for solving the CVP. Executing this method by using different bases of the same lattice return outputs with different distance to the target vector. When the method is executed using a good basis, it works effectively for returning a lattice vector that is located close to the target vector. On the contrary, the method works ineffectively when it is executed using a bad basis where the returned lattice vector is located far from the target vector. In this study, we investigated the reasons behind this occurrence. For that purpose, we solved a CVP instance by executing the Babai’s Round-off Method using a good basis and a bad basis. As a result, we discovered how the norms and orthogonality of basis vectors play their role for influencing the quality of the output returned by the method.
1. Introduction

As opposed to the widely used RSA [1] cryptosystem and several other factoring-based cryptosystems such as [2, 3, 4] that still withstands 40 years of cryptanalysis [5, 6, 7], however in the era of quantum computing, such factoring-based problem is completely insecure. One of the most promising candidates to be the alternative to replace the current existing source of mathematical security is any cryptosystem that were designed based on lattice problems. Lattice problems are mostly related to length (norm) and distance minimization involving lattice vectors. For instance, the classical Closest Vector Problem (CVP) and the Shortest Vector Problem (SVP). The CVP is proven to be NP-hard [8] and the SVP is NP-hard under randomized reduction [9]. Solving these problems in low-dimensional lattice may result the exact solution and this solution can be found in reasonable amount of time. As the lattice dimension increases, the difficulty for solving these problems significantly grows as well. In large-dimensional lattice, the effort to solve these problems for their exact solutions becomes tougher and it could be impractical to be done. That is why approximation methods are preferable in practice especially when we are dealing with large-dimensional lattice.

There are several methods have been proposed to approximate the CVP. In 1986, Babai proposed two approximation methods known as Nearest Plane Method and Round-off Method [10]. Let \( n \in \mathbb{N} \) representing a lattice dimension. When these methods are executed by using Lovász-reduced basis, both methods work nicely and able to return a lattice vector that is located close to a given target vector \( \vec{t} \in \mathbb{R}^n \) within a factor of \( c^n \), for a constant \( c \in \mathbb{R} \). Later in 2000, Klein proposed a heuristic technique to approximate the CVP in special occasion when the target vector is located unusually close to the closest lattice vector [11]. Just like the Babai’s methods, the ability of Klein’s proposal also relies heavily on the quality of the used lattice basis. In 2014, a new approach to solve the CVP using Residue Number System (RNS) has been introduced [12]. In this proposal, the Babai’s Round-off Method is being implemented in RNS. Lately in 2017, an arithmetical improvement on the Babai’s Round-off Method by combining the RNS approach with the use of lattices of Optimal Hermite Normal Form (OHNF) has been proposed [13]. Although the Babai’s Nearest Plane Method has better accuracy than the Babai’s Round-off Method, the simplicity of the Babai’s Round-off Method allows it to offer better efficiency and makes it preferable in practice. In this study, we focus mainly on the CVP and the Babai’s Round-off Method.

A lattice may have infinitely many bases with different quality in terms of the norm and orthogonality of vectors in those bases. The vectors in a basis are called basis vectors. A lattice basis with shorter and more-orthogonal basis vectors is normally referred to as a ‘good basis’ while a lattice basis with longer and less orthogonal basis vectors is normally addressed as a ‘bad basis’. Executing the Babai’s Round-off Method by using different bases of the same lattice return outputs with different quality in terms of the distance between the returned vector with the target vector. If the method is executed using a good basis, the method works nicely for solving the CVP where the returned lattice vector is located closer to the target vector compared to the lattice vector that is returned by the method when it is executed using a bad basis. In this paper, we investigated the reasons why the effectivity of the Babai’s Round-off Method differs when it is executed using lattice bases with different quality in terms of the norm and orthogonality of basis vectors in those bases. From that, we discovered how the norms and orthogonality of basis vectors influencing the quality of the output given by the Babai’s Round-off Method.

2. Mathematical Preliminaries

Throughout this paper, we consider all vectors as column vectors. For instance, let \( n \in \mathbb{N} \) and \( \vec{v} \in \mathbb{R}^n \) is a column vector with \( n \) entries \( v_i \in \mathbb{R} \) for all \( i = 1, \ldots, n \). The vector \( \vec{v} \) can be converted into an integer vector \( \lfloor \vec{v} \rfloor \in \mathbb{Z}^n \) by rounding each entry of the vector \( \vec{v} \) as \( v_i \in \mathbb{Z}^n \) such that \( |v_i - \lfloor v_i \rfloor| < \frac{1}{2} \) for all \( i = 1, \ldots, n \). All matrices are denoted using capital letters. For instance, let \( m, n \in \mathbb{N} \) and \( G \in \mathbb{R}^{m \times n} \) is an \( m \times n \)-matrix with entries \( g_{ij} \in \mathbb{R} \) for all \( i = 1, \ldots, m \) and \( j = 1, \ldots, n \). The set of vectors \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^m \) can be represented in a matrix form as the following:
\[ G = [\vec{g}_1 \ \vec{g}_2 \ \ldots \ \vec{g}_n] = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{m,1} & g_{m,2} & \cdots & g_{m,n} \end{bmatrix} \]  

where each vector \( \vec{g}_j \in \mathbb{R}^m \) for all \( j = 1, \ldots, n \), becomes the column of the matrix \( G \).

**Definition 1:** [9] For \( m, n \in \mathbb{N} \), let \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^m \). A linear combination of the vectors \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \) is any vector \( \vec{v} \in \mathbb{R}^m \) of the form \( \vec{v} = \sum_{i=1}^{n} \alpha_i \vec{g}_i \) where \( \alpha_i \in \mathbb{R} \) for all \( i = 1, \ldots, n \).

**Definition 2:** [9] For \( m, n \in \mathbb{N} \), let \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^m \). The set \( \{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n\} \) is linearly independent if the only way to get \( \alpha_1 \vec{g}_1 + \alpha_2 \vec{g}_2 + \cdots + \alpha_n \vec{g}_n = \vec{0} \) is to have \( \alpha_i = 0 \), for all \( i = 1, \ldots, n \). Otherwise, the set is linearly dependent.

The space \( \mathbb{R}^m \) contains all vectors \( \vec{v} \in \mathbb{R}^m \). A lattice \( L \) is a subset of the space \( \mathbb{R}^m \). When the lattice \( L \) is spanned by the linearly independent set \( \{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n\} \), then each vector in the lattice \( L \) can be represented as a linear combination of the vectors \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \) where the scalars are restricted to be integers only. A lattice can be defined as the following:

**Definition 3:** [13] For \( m, n \in \mathbb{N} \) with \( n \leq m \), let \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^m \) where the set \( \{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n\} \) is linearly independent. The set of all linear combinations of the vectors \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \) with integer scalars is called a lattice. It is denoted as

\[ L(\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n) = \left\{ \sum_{i=1}^{n} a_i \vec{g}_i \bigg| a_i \in \mathbb{Z}, \forall i = 1, \ldots, n \right\}. \]

Since the set \( \{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n\} \) can be represented as a matrix \( G \) as shown in the equation (1), then the lattice \( L(\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n) \) can be simply denoted as \( L(G) = G\vec{a} \) where \( \vec{a} \in \mathbb{Z}^n \) is a vector of integer scalars. The linearly independent set \( \{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n\} \) that span the lattice \( L(G) \) is called a basis for the lattice \( L(G) \). The vectors \( \vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \) are called the basis vectors. The rank of the lattice \( L(G) \) is \( m \), denoted as \( \text{rank}(L(G)) = m \) while the dimension of the lattice \( L(G) \) is \( n \), denoted as \( \text{dim}(L(G)) = n \).

Any lattice with equal rank and dimension is referred to as a full-rank lattice. For instance, let \( \vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n \) where the set \( \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\} \) is linearly independent and it can be represented as the square matrix \( B \in \mathbb{R}^{n \times n} \). Thus, the lattice \( L(B) \subset \mathbb{R}^n \) that is spanned by the basis \( B \) is a full rank lattice with \( \text{rank}(L(B)) = \text{dim}(L(B)) = n \). According to the following theorem, the matrix \( B \) is a nonsingular matrix with \( \text{det}(B) \neq 0 \).

**Theorem 1:** [15] A square matrix is invertible if and only if its columns are linearly independent.

From here, we limit our discussion involving only full rank lattices. For any integer matrix \( M \in \mathbb{Z}^{n \times n} \) with \( \text{det}(M) \neq 0 \), there exists \( M^{-1} \in \mathbb{Z}^{n \times n} \) such that \( MM^{-1} = I \) where \( I \in \mathbb{Z}^{n \times n} \) is an identity matrix. Although all entries of the matrix \( M \) are integers, the entries of the inverse matrix \( M^{-1} \) are not necessarily integers. However, there is a special integer matrix with property that the inverse of this matrix is guaranteed to be a matrix with integer entries. This kind of matrix is called a unimodular matrix as defined below:

**Definition 4:** [16] For \( n \in \mathbb{N} \), let \( U \in \mathbb{Z}^{n \times n} \). The square integer matrix \( U \) is called a unimodular matrix when \( \text{det}(U) = \pm 1 \).
A lattice $\mathcal{L} \subset \mathbb{R}^n$ can be spanned by more than one basis. Any two different bases for the same lattice $\mathcal{L}$ are related by a unimodular matrix as stated in the following lemma:

**Lemma 1:** [17] For $n \in \mathbb{N}$, let $G, B \in \mathbb{R}^{n \times n}$ be non-singular matrices. The matrices $G$ and $B$ generate the same lattice $\mathcal{L} \subset \mathbb{R}^n$, denoted by $L(G) = L(B) = \mathcal{L}$, if and only if these matrices are related by a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ such that $G = BU$.

When $n \geq 2$, there are infinitely many unimodular matrix $U \in \mathbb{Z}^{n \times n}$. Each unimodular matrix can be used to generate another basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$. Therefore, the lattice $\mathcal{L}$ with a dimension $n \geq 2$ has infinitely many bases [17]. Each basis for the lattice $\mathcal{L}$ containing basis vectors with different length and orthogonality compared to the basis vectors in the other basis. The length a vector can be measured as a Euclidean norm and the distance between two vectors can be measured as a Euclidean distance.

**Definition 5:** [18] For $n \in \mathbb{N}$, let $\vec{u}, \vec{v} \in \mathbb{R}^n$. The Euclidean norm of the vector $\vec{u}$ can be computed as

$$
\|\vec{u}\| = \left(\sum_{i=1}^{n} (u_i)^2\right)^{\frac{1}{2}}
$$

(3)

and the Euclidean distance between the vectors $\vec{u}$ and $\vec{v}$ can be computed as

$$
\|\vec{u} - \vec{v}\| = \left(\sum_{i=1}^{n} (u_i - v_i)^2\right)^{\frac{1}{2}}
$$

(4)

where $u_i \in \vec{u}$ and $v_i \in \vec{v}$ for all $i = 1, ..., n$.

The orthogonality of vectors is referring to the angle between the vectors. The orthogonality of the vectors $\vec{u}$ and $\vec{v}$ can be determined by using a quantity that is called dot product. Using the dot product together with the norms of vectors $\vec{u}$ and $\vec{v}$, the angle between these vectors, denoted as $\theta_{\vec{u}, \vec{v}}$, can be computed as given in the following definition:

**Definition 6:** [18] For $n \in \mathbb{N}$, suppose that $\vec{u}, \vec{v} \in \mathbb{R}^n$. The dot products of $\vec{u}$ and $\vec{v}$ can be computed as

$$
\vec{u} \cdot \vec{v} = \sum_{i=1}^{n} u_i v_i
$$

(5)

where $u_i \in \vec{u}$ and $v_i \in \vec{v}$ for all $i = 1, ..., n$. The angle between $\vec{u}$ and $\vec{v}$ can be computed as

$$
\cos \theta_{\vec{u}, \vec{v}} = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\| \|\vec{v}\|}
$$

(6)

The vectors $\vec{u}$ and $\vec{v}$ are said to be orthogonal when $\theta_{\vec{u}, \vec{v}} = 90^\circ$. If these vectors are orthogonal, then $\vec{u} \cdot \vec{v} = \|\vec{u}\| \|\vec{v}\|(\cos 90^\circ) = \|\vec{u}\| \|\vec{v}\|(0) = 0$.

On the contrary, the vectors $\vec{u}$ and $\vec{v}$ are said to be non-orthogonal when $\theta_{\vec{u}, \vec{v}} \neq 90^\circ$. This implies that, $\vec{u} \cdot \vec{v} \neq 0$. The non-orthogonality of basis vectors could be measured by using the Hadamard ratio.

**Definition 7:** [9] For $n \in \mathbb{N}$, let $\vec{b}_1, \vec{b}_2, ..., \vec{b}_n \in \mathbb{R}^n$ be the columns of the basis $B \in \mathbb{R}^{n \times n}$ for the lattice $\mathcal{L} \subset \mathbb{R}^n$. The Hadamard ratio of the basis $B$ is the quantity

$$
\mathcal{H}(B) = \left(\frac{|\text{det}(B)|}{\prod_{i=1}^{n} \|\vec{b}_i\|}\right)^{\frac{1}{n}} \in \mathbb{R}.
$$

(7)

The value of the Hadamard ratio lies in the interval $\mathcal{H}(B) \in (0, 1]$. The closer that the value of $\mathcal{H}(B)$ to 1, then the more orthogonal are the vectors in the basis $B$. On the contrary, the vectors in the basis $B$ are more non-orthogonal when the value of $\mathcal{H}(B)$ closer to 0.
3. The Babai’s Round-off Method

There are various instances of the Closest Vector Problem (CVP). The general instance of the CVP can be defined as follows:

Definition 8: [9] For \( n \in \mathbb{N} \), let \( \mathcal{L} \subset \mathbb{R}^n \) be a lattice. Given \( \bar{t} \in \mathbb{R}^n \) as a target vector. Closest Vector Problem (CVP) is a problem to find a non-zero lattice vector \( \hat{v} \in \mathcal{L} \) that minimizes the Euclidean distance \( \|\bar{t} - \hat{v}\| \).

In [10], it is proven that the Babai’s Round-off Method can approximate the CVP to within a good approximation factor. A lattice basis is required to execute the method. The quality of a basis can be improved by using lattice-reduction method such as the LLL algorithm [19]. The basis that is reduced by the LLL algorithm is specifically referred to as LLL-reduced basis. The reduced basis is consisting shorter and more orthogonal basis vectors compared to its original basis. As stated in following theorem, the Babai’s Round-off Method works nicely when it is executed using a reduced-basis:

Theorem 2: [17] Let \( n \in \mathbb{N} \). If the basis \( \{\bar{b}_1, \bar{b}_2, ..., \bar{b}_n\} \) for a lattice \( \mathcal{L} \subset \mathbb{R}^n \) is LLL-reduced basis (with respect to the Euclidean norm and with factor \( \delta = 3/4 \)) then the output of the Babai’s Round-off Method on the target vector \( \bar{t} \in \mathbb{R}^n \) is a vector \( \hat{v} \in \mathcal{L} \) such that

\[
\|\bar{t} - \hat{v}\| < \left( 1 + 2n \left( \frac{9}{4} \right)^{\frac{n}{2}} \right) \|\bar{t} - \bar{w}\|
\]

for all \( \bar{w} \in \mathcal{L} \).

The algorithm of the Babai’s Round-off Method is described in the following theorem:

Theorem 3: [9] For \( n \in \mathbb{N} \), let the set \( \{\bar{b}_1, \bar{b}_2, ..., \bar{b}_n\} \) be the basis for the lattice \( \mathcal{L} \subset \mathbb{R}^n \) and let \( \bar{t} \in \mathbb{R}^n \) be a target vector. If the basis vectors \( \bar{b}_1, \bar{b}_2, ..., \bar{b}_n \) are sufficiently orthogonal to one another, the following algorithm of the Babai’s Round-off Method solves CVP:

**Input:** A basis \( \{\bar{b}_1, \bar{b}_2, ..., \bar{b}_n\} \) for a lattice \( \mathcal{L} \subset \mathbb{R}^n \) and a target vector \( \bar{t} \in \mathbb{R}^n \).

**Output:** A lattice vector \( \hat{v} \in L(B) = \mathcal{L} \).

- Represent the vector \( \bar{t} \) as a linear combination of the basis \( \{\bar{b}_1, \bar{b}_2, ..., \bar{b}_n\} \) as follows,
  \[
  \bar{t} = \beta_1 \bar{b}_1 + \beta_2 \bar{b}_2 + ... + \beta_n \bar{b}_n.
  \]
- By representing the basis \( \{\bar{b}_1, \bar{b}_2, ..., \bar{b}_n\} \) in matrix form, \( B \in \mathbb{R}^{nxn} \), we have
  \[
  \hat{t} = B \hat{\beta}
  \]
where \( \hat{\beta} \in \mathbb{R}^n \) is an unknown vector of real scalars.

- Compute the unknown vector \( \hat{\beta} \in \mathbb{R}^n \) as \( \hat{\beta} = B^{-1} \bar{t} \).

- Round each entry of the vector \( \hat{\beta} \in \mathbb{R}^n \) to the nearest integer, i.e., \( \lfloor \beta_i \rfloor \in \mathbb{Z}, \forall \ i = 1, ..., n \).

- Compute the lattice vector \( \hat{v} \in L(B) \) as follows,
  \[
  \hat{v} = \lfloor \beta_1 \bar{b}_1 \rfloor + \lfloor \beta_2 \bar{b}_2 \rfloor + ... + \lfloor \beta_n \bar{b}_n \rfloor.
  \]

In general, if the vectors in the basis are reasonably orthogonal to one another, then the algorithm solves some version of approximation CVP, but if the basis vectors are highly non-orthogonal, then the lattice vector returned by the algorithm is generally far from the closest vector to the target vector \( \bar{t} \).
4. Approximating CVP using the Babai’s Round-off Method

As stated in the Theorem 3, the Babai’s Round-off Method works nicely when the basis vectors in the basis that is used to compute the unknown vector $\beta \in \mathbb{R}^n$ are reasonably orthogonal to one another. On the contrary, the method works ineffectively when the used basis to execute the method consists of highly non-orthogonal basis vectors. To investigate the reason behind this occurrence, we define the following CVP instance:

**Definition 9:** For $n \in \mathbb{N}$, let $G, B \in \mathbb{R}^{n \times n}$ be two different non-singular matrices with linearly independent columns $\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_n \in \mathbb{R}^n$ and $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbb{R}^n$ respectively. Suppose that, $L \subset \mathbb{R}^n$ be a lattice with two different bases $G$ and $B$ such that $G = BU$, with $U \in \mathbb{Z}^{n \times n}$ is a unimodular matrix. This implies that, the bases $G$ and $B$ are spanning the same lattice $L$, i.e., $L(G) = L(B) = L$. The basis $G$ is assumed to be a ‘good basis’ with shorter and more orthogonal basis vectors compared to the basis $B$ that is assumed to be a ‘bad basis’ with longer and highly non-orthogonal basis vectors. Given the target vector $\tilde{t} \in \mathbb{R}^n$ and the lattice bases $G$ and $B$, find the lattice vector $\tilde{v} \in L$ such that the Euclidean distance $\|\tilde{t} - \tilde{v}\|$ is minimum.

The defined CVP instance can be approximated by executing the Babai’s Round-off Method using the given lattice bases $G$ and $B$ to obtain two different lattice vectors $\tilde{v}_G \in L(G) = L$ and $\tilde{v}_B \in L(B) = L$ respectively as the results. To execute the Babai’s Round-off Method in the lattice $L(G)$, denote the target vector $\tilde{t} \in \mathbb{R}^n$ as $\tilde{t}_G$ and be represented as follows,

$$\tilde{t}_G = y_1 \tilde{g}_1 + y_2 \tilde{g}_2 + \ldots + y_n \tilde{g}_n$$

$$\tilde{t}_G = \begin{bmatrix} t_{G,1} \\ t_{G,2} \\ \vdots \\ t_{G,n} \end{bmatrix} = \begin{bmatrix} g_{11} \\ g_{21} \\ \vdots \\ g_{n1} \end{bmatrix} y_1 + \begin{bmatrix} g_{12} \\ g_{22} \\ \vdots \\ g_{n2} \end{bmatrix} y_2 + \ldots + \begin{bmatrix} g_{1n} \\ g_{2n} \\ \vdots \\ g_{nn} \end{bmatrix} y_n$$

The unknown vector of real scalars $\tilde{v} \in \mathbb{R}^n$ can be computed as follow $\tilde{v} = G^{-1} \tilde{t}_G$. Then, round each entry of the vector $\tilde{v} \in \mathbb{R}^n$ to the nearest integer as $|y_i| \in \mathbb{Z}$ for all $i = 1, \ldots, n$. Finally, the lattice vector $\tilde{v}_G \in L(G) = L$ can be computed as follows,

$$\tilde{v}_G = |y_1| \tilde{g}_1 + |y_2| \tilde{g}_2 + \ldots + |y_n| \tilde{g}_n$$

$$\tilde{v}_G = \begin{bmatrix} v_{G,1} \\ v_{G,2} \\ \vdots \\ v_{G,n} \end{bmatrix} = \begin{bmatrix} g_{11} \\ g_{21} \\ \vdots \\ g_{n1} \end{bmatrix} |y_1| + \begin{bmatrix} g_{12} \\ g_{22} \\ \vdots \\ g_{n2} \end{bmatrix} |y_2| + \ldots + \begin{bmatrix} g_{1n} \\ g_{2n} \\ \vdots \\ g_{nn} \end{bmatrix} |y_n|$$

To execute the Babai’s Round-off Method in the lattice $L(B)$, denote the target vector $\tilde{t} \in \mathbb{R}^n$ as $\tilde{t}_B$ and be represented as follows,

$$\tilde{t}_B = \beta_1 \tilde{b}_1 + \beta_2 \tilde{b}_2 + \ldots + \beta_n \tilde{b}_n$$

$$\tilde{t}_B = \begin{bmatrix} t_{B,1} \\ t_{B,2} \\ \vdots \\ t_{B,n} \end{bmatrix} = \begin{bmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{bmatrix} \beta_1 + \begin{bmatrix} b_{12} \\ b_{22} \\ \vdots \\ b_{n2} \end{bmatrix} \beta_2 + \ldots + \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{nn} \end{bmatrix} \beta_n$$

$$\tilde{t}_B = B \beta$$

The unknown vector of real scalars $\tilde{\beta} \in \mathbb{R}^n$ can be computed as $\tilde{\beta} = B^{-1} \tilde{t}_B$. Then, round each entry of the vector $\tilde{\beta} \in \mathbb{R}^n$ to the nearest integer as $|\beta_i| \in \mathbb{Z}$ for all $i = 1, \ldots, n$. Finally, the lattice vector $\tilde{v}_B \in L(B) = L$ can be computed as follows,
\[
\begin{align*}
\left[ v_{B,1} \\
v_{B,2} \\
v_{B,n} \right] &= \begin{bmatrix}
\beta_1 \\
\beta_2 \\
\beta_n \\
\end{bmatrix} + \begin{bmatrix}
b_{1,1} \\
b_{2,1} \\
b_{n,1} \\
\end{bmatrix} + \cdots + \begin{bmatrix}
b_{1,n} \\
b_{2,n} \\
b_{n,n} \\
\end{bmatrix} = \beta_1 \bar{v}_1 + \beta_2 \bar{v}_2 + \cdots + \beta_n \bar{v}_n \\
\end{align*}
\]

Next, we determine the Euclidean distances \( \| \tilde{e}_G - \tilde{v}_G \| \) and \( \| \tilde{e}_B - \tilde{v}_B \| \) as the following:

\[
\| \tilde{e}_G - \tilde{v}_G \| = \left( \sum_{i=1}^{n} (t_{G,i} - v_{G,i})^2 \right)^{\frac{1}{2}}
\]

\[
\| \tilde{e}_G - \tilde{v}_G \|^2 = (t_{G,1} - v_{G,1})^2 + (t_{G,2} - v_{G,2})^2 + \cdots + (t_{G,n} - v_{G,n})^2
\]

\[
\| \tilde{e}_B - \tilde{v}_B \| = \left( \sum_{i=1}^{n} (t_{B,i} - v_{B,i})^2 \right)^{\frac{1}{2}}
\]

\[
\| \tilde{e}_B - \tilde{v}_B \|^2 = (t_{B,1} - v_{B,1})^2 + (t_{B,2} - v_{B,2})^2 + \cdots + (t_{B,n} - v_{B,n})^2
\]

For the basis vectors \( \tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_n \in \mathbb{R}^n \), we have the following distinct dot products,

\[
\begin{align*}
\tilde{g}_1 \cdot \tilde{g}_2 &= g_{1,1}g_{2,1} + g_{2,1}g_{2,2} + \cdots + g_{n,1}g_{n,2} \\
\tilde{g}_1 \cdot \tilde{g}_n &= g_{1,1}g_{1,n} + g_{2,1}g_{2,n} + \cdots + g_{n,1}g_{n,n} \\
\tilde{g}_2 \cdot \tilde{g}_n &= g_{1,2}g_{1,n} + g_{2,2}g_{2,n} + \cdots + g_{n,2}g_{n,n}
\end{align*}
\]

and the Euclidean norms of each basis vectors as follows,

\[
\begin{align*}
\| \tilde{g}_1 \|^2 &= (g_{1,1})^2 + (g_{2,1})^2 + \cdots + (g_{n,1})^2 \\
\| \tilde{g}_2 \|^2 &= (g_{1,2})^2 + (g_{2,2})^2 + \cdots + (g_{n,2})^2 \\
\| \tilde{g}_n \|^2 &= (g_{1,n})^2 + (g_{2,n})^2 + \cdots + (g_{n,n})^2
\end{align*}
\]

Therefore, the Euclidean distance \( \| \tilde{e}_G - \tilde{v}_G \|^2 \) can be simplified as follows:

\[
\| \tilde{e}_G - \tilde{v}_G \|^2 = (\gamma_1^2 + 2(-|\gamma_1|\gamma_1) + |\gamma_1|^2)\| \tilde{g}_1 \|^2 + (\gamma_2^2 + 2(-|\gamma_2|\gamma_2) + |\gamma_2|^2)\| \tilde{g}_2 \|^2 + \cdots + (\gamma_n^2 + 2(-|\gamma_n|\gamma_n) + |\gamma_n|^2)\| \tilde{g}_n \|^2
\]

\[
\begin{align*}
+ 2(\gamma_1 \gamma_2) + (-|\gamma_1| \gamma_2) + (\gamma_1 \gamma_2)|\tilde{g}_1 \cdot \tilde{g}_2) \\
+ \cdots + 2(\gamma_1 \gamma_n) + (-|\gamma_1| \gamma_n) + (\gamma_1 \gamma_n)|\tilde{g}_1 \cdot \tilde{g}_n) \\
+ 2(\gamma_2 \gamma_n) + (-|\gamma_2| \gamma_n) + (\gamma_2 \gamma_n)|\tilde{g}_2 \cdot \tilde{g}_n)
\end{align*}
\]

(18)
By applying the same way to the Euclidean distance $\| \vec{e}_B - \vec{v}_B \|^2$, it can be simplified as follows:

$$
\| \vec{e}_B - \vec{v}_B \|^2 = (\beta_1^2 + 2(-|\beta_1|\beta_2) + |\beta_2|^2)\|\vec{b}_1\|^2 + (\beta_2^2 + 2(-|\beta_2|\beta_2) + |\beta_2|^2)\|\vec{b}_2\|^2 \\
+ \cdots + (\beta_n^2 + 2(-|\beta_n|\beta_n) + |\beta_n|^2)\|\vec{b}_n\|^2 \\
+ 2(\beta_1\beta_2 - |\beta_1|\beta_2) + (\beta_1\beta_2 + |\beta_1|\beta_2)(\vec{b}_1 \cdot \vec{b}_2) \\
+ \cdots + 2(\beta_1\beta_n + (-|\beta_1|\beta_n) + |\beta_1|\beta_n)(\vec{b}_1 \cdot \vec{b}_n) \\
+ 2(\beta_2\beta_n + (-|\beta_2|\beta_n) + |\beta_2|\beta_n)(\vec{b}_2 \cdot \vec{b}_n). \\
(19)
$$

5. Result and Discussion

If the basis $\vec{g}_1, \vec{g}_2, ..., \vec{g}_n \in \mathbb{R}^n$ are pairwise orthogonal, then the distinct dot products $\vec{g} \cdot \vec{g} = 0$ for all $i, j = 1, ..., n$ with $i \neq j$ and $i < j$. Hence, the Euclidean distance is

$$
\| \vec{e}_G - \vec{v}_G \|^2 = (\gamma_1^2 + 2(-|\gamma_1|\gamma_1) + |\gamma_1|^2)\|\vec{g}_1\|^2 + (\gamma_2^2 + 2(-|\gamma_2|\gamma_2) + |\gamma_2|^2)\|\vec{g}_2\|^2 \\
+ \cdots + (\gamma_n^2 + 2(-|\gamma_n|\gamma_n) + |\gamma_n|^2)\|\vec{g}_n\|^2 \\
$$

(20)

where $\gamma_i \in \mathbb{R}$ and $|\gamma_i| \in \mathbb{Z}$ for all $i = 1, ..., n$. In this case, the distance $\| \vec{e}_G - \vec{v}_G \|^2$ totally depends on the norms of all basis vectors $\|\vec{g}_i\|$ for all $i = 1, ..., n$. If all these norms are minimum, then the Euclidean distance $\| \vec{e}_G - \vec{v}_G \|^2$ is minimum as well. That means, the returned lattice vector $\vec{v}_G$ by the Babai’s Round-off Method is located close to the target vector $\vec{e}_G \in \mathbb{R}^n$. In this investigation, we consider this case as trivial.

Our main interest is to investigate the case when both bases $G$ and $B$ are consisting non-orthogonal basis vectors $\vec{g}_1, \vec{g}_2, ..., \vec{g}_n$ and $\vec{b}_1, \vec{b}_2, ..., \vec{b}_n$ respectively.

**Corollary 1:** Let $n \in \mathbb{N}$ and $\vec{b}_1, \vec{b}_2, ..., \vec{b}_n \in \mathbb{R}^n$. The total number of distinct dot products $\vec{b}_i \cdot \vec{b}_j$ for all $i, j = 1, ..., n$ where $i \neq j$ and $i < j$ is

$$
l = \frac{n!}{2(n-2)!} \in \mathbb{N}. \\
(21)
$$

**Proof**

Given that $\vec{b}_i, \vec{b}_j \in \mathbb{R}^n$ for all $i, j = 1, ..., n$. Note that, $\vec{b}_i \cdot \vec{b}_j = b_{i1}b_{j1} + b_{i2}b_{j2} + \cdots + b_{in}b_{jn}$ and $\vec{b}_j \cdot \vec{b}_i = b_{j1}b_{i1} + b_{j2}b_{i2} + \cdots + b_{jn}b_{in}$. Since $b_{i,j} \in \mathbb{R}$, then we have $b_{i,j}b_{j,i} = b_{j,i}b_{i,j}$ for all $i,j,s,t = 1, ..., n$. Hence,

$$
\vec{b}_i \cdot \vec{b}_j = b_{i1}b_{j1} + b_{i2}b_{j2} + \cdots + b_{in}b_{jn} = b_{j1}b_{i1} + b_{j2}b_{i2} + \cdots + b_{jn}b_{in} = \vec{b}_j \cdot \vec{b}_i \\
$$

Let $l \in \mathbb{N}$ denotes the number of distinct dot products $\vec{b}_i \cdot \vec{b}_j$ for all $i, j = 1, ..., n$ where $i \neq j$ and $i < j$. Thus, $l$ is a combination of 2 distinct vectors among all $n$ distinct vectors $\vec{b}_1, \vec{b}_2, ..., \vec{b}_n$. Therefore, $l$ can be computed using a combination formula as

$$
l = \frac{n!}{2(n-2)!} \\
$$

Denote the distinct dot products as $\vec{g}_i \cdot \vec{g}_j = \mu_k$ and $\vec{b}_i \cdot \vec{b}_j = \tau_k$ respectively where $\mu_k, \tau_k \in \mathbb{R}$ for all $k = 1, ..., l$. Hence, we have the following Euclidean distances resulted from the execution of the Babai’s Round-off Method using the bases $G$ and $B$ respectively.
and the distinct dot products and the norms of all basis vectors depend heavily on the values of the norms and distinct dot products of all basis vectors in the used lattice basis. That is why the method works effectively if the basis vectors in the lattice basis are mainly determined by the values of the norms and distinct dot products of all basis vectors in the used lattice basis. As a result, it can be observe that the Euclidean distances depend heavily on the norms of all the basis vectors and the dot products for all . The distances could be minimized when the norms and the distinct dot products of the bases and the distinct dot products of the bases are small enough. Since the basis is assumed to be a good basis with shorter and more orthogonal basis vectors compared to the bad basis that consists of longer and non-orthogonal basis vectors, the returned lattice vector is closer to the target vector compared to the lattice vector . This could be the reason why the Babai’s Round-off Method works effectively when it is executed using a good basis and it works ineffectively when it is executed using a bad basis.

6. Conclusion

In this study, we investigated how the norms and dot products of basis vectors in a lattice basis influencing the performance of the Babai’s Round-off Method for solving the CVP. We showed that the distance between the given target vector in the CVP and the returned lattice vector by the method is mainly determined by the values of the norms and distinct dot products of all basis vectors in the used lattice basis. That is why the method performs effectively if the basis vectors in the lattice basis are reasonably orthogonal to one another and it performs ineffectively when the used basis to execute the method consists of highly non-orthogonal basis vectors. From this occurrence, it is interesting to address the following question. How orthogonal are the basis vectors to be considered as ‘reasonably’ orthogonal and how non-orthogonal are the basis vectors to be considered as ‘highly’ non-orthogonal? This study is initiated to address this question. We are optimistic that a systematic and deterministic mechanism to measure the orthogonality of a lattice basis is demanded in order to clearly classify any lattice basis as a good or bad basis.

Acknowledgement

The present research is partially supported by the Putra-Grant – GP/2017/9558800 and supported by Universiti Sains Malaysia, Universiti Malaysia Sabah and Malaysian Ministry of Education.
References

[1] Rivest R L, Shamir A and Adleman L 1978 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

[2] Mahad Z, Asbullah M A, and Ariffin M R K 2017 Efficient methods to overcome Rabin cryptosystem decryption failure. Malaysian Journal of Mathematical Sciences, 11 (S2), 9-20

[3] Asbullah M A, Ariffin M R K and Mahad Z 2018 Enhanced AAG cryptosystem: The design. Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018, 94-102

[4] Asbullah M A and Ariffin M R K 2016 Design of Rabin-like cryptosystem without decryption failure. Malaysian Journal of Mathematical Sciences, MJMS 10(S), 1-18

[5] Ghafar A H A, Ariffin M R K and Asbullah M A 2018 Extending pollard class of factorable RSA modulus. Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018, 103-118.

[6] Abubakar S I, Ariffin M R K and Asbullah M A 2018 A new simultaneous diophantine attack upon RSA moduli N = pq. Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018, 119-138.

[7] Rahman N N A, Ariffin M R K, Asbullah M A and Yunus F 2018 New vulnerability on system of Ni = p^2_iq_i using good approximation of \( \phi(N) \). Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018, 139-150.

[8] Boas P van E 1981 Another NP-complete problem and the complexity of computing short vectors in a lattice 1981 Technical Report 81-04, Mathematische Instituut, Universiy of Amsterdam. Available on-line at URL http://turing.wins.uva.nl/~peter/

[9] Hoffstein J, Pipher J and Silverman J.H 2008 Lattices and Cryptography. In S. Axler & K. A. Ribet (Eds.), An Introduction to Mathematical Cryptography Spring Street, New York: Springer Science+Business Media, LLC 349-422

[10] Babai L 1986 On Lovasz’ lattice reduction and the nearest lattice point problem Combinatorica 6(1) 1–13

[11] Klein P 2000 Finding the closest lattice vector when it’s unusually close Proceedings of the 11th Symposium on Discrete Algorithms. San Francisco, California.

[12] Bajard J, Eynard J, Merkiche N. and Plantard T 2014 Babaï round-off CVP method in RNS: Application to lattice based cryptographic protocols 2014 International Symposium on Integrated Circuits (ISIC) 440-443

[13] Martins P, Eynard J, Bajard J and Sousa L 2017 Arithmetical Improvement of the Round-off for Cryptosystems in High-Dimensional Lattices IEEE Trans. on Comp. 66(12) 2005-18

[14] Mandangan A, Kamarulhaili H, and Asbullah M A 2018 On the Underlying Hard Lattice Problems of GGH Encryption Scheme Cryptology and Information Security Conf. 2018 42

[15] Goodaire E G 2014 Matrices and Linear Equations. Linear Algebra Pure and Applies. Toh Tuck Link, Singapore, World Scientific Publishing Co. Pte. Ltd. 93-227

[16] Galbraith S D 2012 Background Mathematics. In Mathematics of Public Key Cryptography. 1st edn. New York USA: Cambridge University Press, 564-578

[17] Galbraith S D 2012 Lattices. Mathematics of Public Key Cryptography. United States of America, Cambridge University Press New York 337-46

[18] Goodaire E G 2014 Euclidean n-Space. Linear Algebra Pure and Applies. Toh Tuck Link, Singapore, World Scientific Publishing Co. Pte. Ltd. 1-83

[19] Lenstra, A K, Lenstra Jr H W and Lovász L 1982 Factoring polynomials with rational coefficients. Math. Ann., 261(4) 515–534