Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

A Study on Some Approximations on the Average Number of the LLL Bases in Higher Dimensions

Jaewon Jung[1], **Kyunghwan Song**[2*]

[1] Department of Mathematics, Korea University, Seoul, Republic of Korea
[2] Department of Mathematics, Jeju National University, Jeju, Republic of Korea
E-mail: khsong@jejunu.ac.kr

Received: 2 December 2024; **Revised:** 17 March 2025; **Accepted:** 2 April 2025

Abstract: The Lenstra-Lenstra-Lovász (LLL) algorithm, known as one of the main algorithms to decrypt the ciphertext encrypted by Lattice-based cryptography, outputs short basis vectors for n dimensional vectors represented by $n \times n$ matrix. One of the indicators that determine the quality of this LLL algorithm is the average number of the LLL bases, and there is a result related to the average number of the $(\delta,\ \eta)$-LLL bases in dimension n in theoretical sense but the formula seems to be complicated and computing in high dimension takes a long time. In practical sense, we suggest some approximations which can be computed by just storing some constants and computing relatively simple exponential functions. To obtain the approximated results, we first express the existing results in a slightly simpler form, execute individual approximation for the part that takes a long time to calculate, and then combine the results. By finding the approximated value of the average number much faster, it helps to discuss the quality of the LLL algorithm for dimension n faster. Furthermore, in this process, we find a more precise upper bound of the average number of the $(\delta,\ \eta)$-LLL bases in higher dimensions.

***Keywords*:** shortest vector, LLL-reduction algorithm, Riemann-zeta function, Gamma function

MSC: 11H06, 11Y35, 26D07

1. Introduction

Lattice-based cryptography is a cryptographic system that are based on the hardness of lattice based problems, which is firstly introduced by Ajtai [1] and it is is a promising post-quantum cryptography family. Surely, it has the role of classical cryptography scheme, for example, key exchange and digital signature [2]. Furthermore it has various promising applications such as IoT [3] and Medical data anlytics [4]. We need some mathematical backgrounds related to linear algebra to know the process of Lattice-based cryptography. Firstly, we introduce the definition of the span of a subset of a vector space.

Definition 1 Let $S = \{\mathbf{v}_1,\ \mathbf{v}_2,\ \dots,\ \mathbf{v}_n\}$ be a subset of a vector space V. Then the span of S is the set of all linear combinations of the vectors in S and denoted by span $(S) = \{\sum_{i=1}^{n} a_i\mathbf{v}_i : a_1,\ \dots,\ a_n \in \mathbb{R}\}$.

Lattice is a set of points, which is called lattice points in n-dimensional space. In general, we can say the definition of lattice using linearly independent vectors.

DOI: https://doi.org/10.37256/cm.6320256180

Definition 2 Let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \in \mathbb{R}^m$ be a set of linearly independent vectors. The lattice L generated by S is the set of linear combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ with coefficients in $\mathbb{Z}$. That is,

$$L = \left\{ \sum_{i=1}^{n} a_i \mathbf{v}_i : a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

In this case, we say that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis for L and the dimension of L is n.

Related to the definition of lattice, there is one of the well-known problem which is called the Shortest Vector Problem (SVP). If someone finds a sufficiently short vector in a lattice, the vector is a strong candidate of the private key in a lattice-based cryptography [5].

Problem 3 The Shortest Vector Problem (SVP): Find a shortest nonzero vector in a lattice L, i.e., find a nonzero vector $\mathbf{v} \in L$ that minimizes the Euclidean norm $||\mathbf{v}||$.

Lenstra-Lenstra-Lovász (LLL) algorithm [6] computes a reduced bases in a polynomial time to give a set of sufficiently short vectors for any given lattice basis. We call this basis a LLL-reduced basis and there are many variations of LLL algorithm.

The LLL algorithm, its variations, and applications are one of the widely studied topics. For example, the LLL algorithm is introduced as a reduction algorithm for binary codes [7], an algorithm to complete half-Hadamard matrices [8]. Also the LLL algorithm is used to make a storage efficient algorothm for hermite normal form [9], to set the elliptic curve cryptosystem with bitcoin curves [10]. Furthoermore, the study for improving the efficiency of the LLL algorithm is still ongoing such as [11, 12].

This paper is organized as follows: In Section 2, the definition and properties of LLL-reduced bases is presented. And then we introduce a theoretical result of the average number of the LLL bases in fixed dimension n. In Section 3, we analyze the bounds of the average number of the LLL-bases in fixed dimension n for sufficiently large dimension n. And the last section we give two approximations of the average number of the LLL-bases in fixed dimension n.

Note that we put the draft on Arxiv [13].

2. Preliminaries

Notation 4 For convenience, we use the following notation

$$span_{\mathbb{Z}}(S) = \left\{ \sum_{i=1}^{n} a_i \mathbf{v}_i : a_1, \ldots, a_n \in \mathbb{Z} \right\},$$

for $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$.

To construct the definition of LLL basis, we have to see the definition of the component, which is related to the span of preceding independent vectors.

Definition 5 [14] Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for $\mathbb{R}^n$. $\mathbf{v}_i^*$ is the component of $\mathbf{v}_i$ that is orthogonal to span$(\mathbf{v}_1, \ldots, \mathbf{v}_n)$, and $\mu_{i,\, j} =< \mathbf{v}_i, \dfrac{\mathbf{v}_j^*}{||\mathbf{v}_j^*||^2} >$, $\mathbf{v}_1^* = \mathbf{v}_1$ and we obtain $\mathbf{v}_i^*$ for $i = 2, \ldots, n$ using Gram-Schmidt Orthogonalization as follows:

$$\mathbf{v}_i^* = \mathbf{v}_i - \sum_{j=1}^{i-1} \mu_{i,\, j} \mathbf{v}_j^*.$$

Now, we are ready to see the definition of the (δ, η)-LLL basis.

Definition 6 [14] Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for $\mathbb{R}^n$, and take two parameters $\frac{1}{2} < \delta < 1$, $\frac{1}{2} < \eta < \delta$. In practice, one often takes δ and η arbitrarily close to, but not equal to, 1 and $\frac{1}{2}$ respectively. Then a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a (δ, η)-LLL basis if

1. $|\mu_{i,\, j}| \leq \eta$ for all $j < i$.
2. $\delta||\mathbf{v}_i^*|| \leq ||\mathbf{v}_{i+1}^* + \mu_{i+1,\, i}\mathbf{v}_i^*||$ for all $i = 1, \ldots, n-1$ (the Lov*á*sz condition).

In [14], the average number of the (δ, η)-LLL bases is evaluated and this is directly related to the probability to find a shortest vector in a fixed lattice whose dimension is n. Note that $SL(n, \mathbb{R})/SL(n, \mathbb{Z})$ represents n-dimensional lattices of covolume 1 and the average is taken with respect to the measure derived from Haar measure on $SL(n, \mathbb{R})$. See [14] for detailed information.

Theorem 7 [14] The average number of the (δ, η)-LLL bases in dimension n is

$$2 \cdot (2\eta)^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{S_i(1)}{\zeta(i)} \cdot \frac{1}{n} \prod_{i=1}^{n-1} \frac{1}{i(n-i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx, \tag{1}$$

where $\zeta(i)$ is the Riemann-zeta function and $S_i(x)$ is the surface area of a sphere in $\mathbb{R}^i$ of radius x.

We give some approximations of (1) using relatively simple formula in the next section. Note that the study on the approximation using linear regression without the proof is in [15].

3. Main results

Since $S_i(1) = \dfrac{2\pi^{\frac{i}{2}}}{\Gamma\left(\frac{i}{2}\right)}$, we have the following equations.

$$2 \cdot (2\eta)^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{S_i(1)}{\zeta(i)} \cdot \frac{1}{n} \prod_{i=1}^{n-1} \frac{1}{i(n-i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx$$

$$= 2^{\frac{n^2-3n+4}{2}} \eta^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{\dfrac{2\pi^{\frac{i}{2}}}{\Gamma\left(\frac{i}{2}\right)}}{\zeta(i)} \cdot \frac{1}{n} \prod_{i=1}^{n-1} \frac{1}{i(n-i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx$$

$$= 2^{\frac{n^2-3n+4}{2}} \eta^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{1}{\frac{1}{2} i(i-1)\pi^{-\frac{i}{2}} \Gamma\left(\frac{i}{2}\right) \zeta(i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx.$$

Therefore Equation (1) is equal to

$$2^{\frac{n^2-3n+4}{2}} \eta^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{1}{\xi(i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx, \tag{2}$$

where $\xi(i) = \frac{1}{2}i(i-1)\pi^{-i/2}\Gamma\left(\frac{i}{2}\right)\zeta(i)$, which is called the Riemann-Xi function. Therefore, finding upper and lower bound of the product of the Riemann-Xi functions and that of the product of the integration part of the equation (2) are critical parts of finding the approximation of the average number of the LLL bases in sufficiently large dimension n. We treat these two parts in the following sections and then summarize them to find upper and lower bound of (2).

3.1 *The bound of the product of the Riemann-Xi functions*

Because the Riemann-Xi function is defined by $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, firstly we have to find the bounds of $\Gamma\left(\frac{s}{2}\right)$ and $\zeta(s)$. Immediately, we have

$$\sqrt{\pi}\left(\frac{s-2}{2e}\right)^{(s-2)/2}(s-2)^{1/2} < \Gamma(\frac{s}{2}) < \sqrt{\pi}\left(\frac{s-2}{2e}\right)^{(s-2)/2}(s-1)^{1/2}$$

using Lemma 1.9 in [16]. Also, we can check that

$$1 < \zeta(s) < 1 + \frac{1}{s-1},$$

using the integral test. Therefore we get

$$\frac{1}{2}s(s-1)\pi^{-s/2}\sqrt{\pi}\left(\frac{s-2}{2e}\right)^{(s-2)/2}(s-2)^{1/2} \tag{3}$$

$$<\xi(s)$$

$$<\frac{1}{2}s(s-1)\pi^{-s/2}\sqrt{\pi}\left(\frac{s-2}{2e}\right)^{(s-2)/2}(s-1)^{1/2}\left(1+\frac{1}{s-1}\right). \tag{4}$$

The left side of this inequality (3) is greater than

$$\frac{1}{2}(s-2)^2\pi^{-s/2}\sqrt{\pi}\left(\frac{s-2}{2e}\right)^{(s-2)/2}(s-2)^{1/2}$$

$$=\frac{1}{2\sqrt{\pi}}(s-2)^{(s+3)/2}\cdot\left(\frac{1}{2\pi e}\right)^{(s-2)/2}, \tag{5}$$

and the right side of this inequality (4) is less than

$$\frac{1}{2}(s-1)^2\pi^{-(s-1)/2}\left(\frac{s-1}{2e}\right)^{(s-2)/2}(s-1)^{1/2} = \frac{1}{2\sqrt{\pi}}(s-1)^{(s+3)/2}\cdot\left(\frac{1}{2\pi e}\right)^{(s-2)/2}, \tag{6}$$

for $s \geq 6$. From (5) and (6), we have

$$\prod_{s=6}^{n}\left(2\sqrt{\pi}(s-1)^{-(s+3)/2}\cdot(2\pi e)^{(s-2)/2}\right)$$

$$=\left(2\sqrt{\pi}\right)^{(n-5)}(2\pi e)^{(n^2-3n-10)/4}\cdot\prod_{s=6}^{n}(s-1)^{-(s+3)/2}<\prod_{s=6}^{n}\frac{1}{\xi(s)}$$

$$<\prod_{s=6}^{n}\left(2\sqrt{\pi}(s-2)^{-(s+3)/2}\cdot(2\pi e)^{(s-2)/2}\right)=\left(2\sqrt{\pi}\right)^{(n-5)}(2\pi e)^{(n^2-3n-10)/4}\cdot\prod_{s=6}^{n}(s-2)^{-(s+3)/2},$$

and we can simplify the product part as follows:

$$\prod_{s=6}^{n}(s-1)^{-(s+3)/2}$$

$$=\exp\left(\sum_{s=6}^{n}\left(-\frac{s+3}{2}\right)\ln(s-1)\right)$$

$$=\exp\left(-\frac{1}{2}\sum_{s=6}^{n}(s-1)\ln(s-1)-2\sum_{s=6}^{n}\ln(s-1)\right)$$

$$>\exp\left(-\frac{1}{2}\int_{6}^{n+1}(s-1)\ln(s-1)ds-2\int_{6}^{n+1}\ln(s-1)ds\right)$$

$$=\exp\left(-\frac{1}{2}\left(\frac{1}{2}n^2\ln n-\frac{1}{4}n^2-\frac{25}{2}\ln 5+\frac{25}{4}\right)-2\left(n\ln n-n-5\ln 5+5\right)\right)$$

$$=\exp\left(-\frac{n(n+8)}{4}\ln n+\frac{n(n+16)}{8}+\frac{25}{4}\ln 5-\frac{25}{8}+10\ln 5-10\right)$$

$$>\exp\left(-\frac{n(n+8)}{4}\ln n+\frac{n(n+16)}{8}+13.0284\right),$$

$$
\begin{aligned}
&\prod_{s=6}^{n}(s-2)^{-(s+3)/2} \\
&=\exp\left(\sum_{s=6}^{n}\left(-\frac{s+3}{2}\right)\ln(s-2)\right) \\
&=\exp\left(-\frac{1}{2}\sum_{s=6}^{n}(s-2)\ln(s-2)-\frac{5}{2}\sum_{s=6}^{n}\ln(s-2)\right) \\
&<\exp\left(-\frac{1}{2}\int_{5}^{n}(s-2)\ln(s-2)ds-\frac{5}{2}\int_{5}^{n}\ln(s-2)ds\right) \\
&=\exp\left(-\frac{1}{2}\Big(\frac{(n-2)^2}{2}\ln n-\frac{(n-2)^2}{4}-\frac{9}{2}\ln 3+\frac{9}{4}\Big)-\frac{5}{2}\Big((n-2)\ln(n-2)-(n-2)-3\ln 3+3\Big)\right) \\
&=\exp\left(-\frac{(n+8)(n-2)}{4}\ln(n-2)+\frac{(n+18)(n-2)}{8}+\frac{9}{4}\ln 3-\frac{9}{8}+\frac{15}{2}\ln 3-\frac{15}{2}\right) \\
&<\exp\left(-\frac{(n+8)(n-2)}{4}\ln(n-2)+\frac{(n+18)(n-2)}{8}+2.08647\right).
\end{aligned}
$$

Therefore we have

$$
\begin{aligned}
&\prod_{s=2}^{5}\frac{1}{\xi(s)}\cdot\left(2\sqrt{\pi}\right)^{(n-5)}(2\pi e)^{(n^2-3n-10)/4}\cdot\exp\left(-\frac{n(n+8)}{4}\ln n+\frac{n(n+16)}{8}+13.0284\right)<\prod_{s=2}^{n}\frac{1}{\xi(s)} \\
&<\prod_{s=2}^{5}\frac{1}{\xi(s)}\cdot\left(2\sqrt{\pi}\right)^{(n-5)}(2\pi e)^{(n^2-3n-10)/4}\cdot\exp\left(-\frac{(n+8)(n-2)}{4}\ln(n-2)+\frac{(n+18)(n-2)}{8}+2.08647\right).
\end{aligned}
$$

Also, we can verify

$$
\begin{aligned}
&(2\sqrt{\pi})^{n-5}(2\pi e)^{(n^2-3n-10)/4}\cdot 2^{(n^2-3n+4)/2}\cdot\eta^{(n-1)(n-2)/2} \\
&=\exp\left(n^2\left(\frac{3}{4}\ln 2+\frac{1}{4}\ln\pi+\frac{1}{2}\ln\eta+\frac{1}{4}\right)\right. \\
&\quad\left.+n\left(-\frac{5}{4}\ln 2-\frac{1}{4}\ln\pi-\frac{3}{2}\ln\eta-\frac{3}{4}\right)+\left(-\frac{11}{2}\ln 2-5\ln\pi+\ln\eta-\frac{5}{2}\right)\right).
\end{aligned}
$$

Hence we have a simplified form of lower bound

$$\prod_{s=2}^{5}\frac{1}{\xi(s)}\cdot\exp\Bigg(-\frac{1}{4}n^2\ln n+n^2\left(\frac{3}{4}\ln 2+\frac{1}{4}\ln\pi+\frac{1}{2}\ln\eta+\frac{3}{8}\right)$$

$$-2n\ln n+n\left(-\frac{5}{4}\ln 2-\frac{1}{4}\ln\pi-\frac{3}{2}\ln\eta+\frac{5}{4}\right)+0.9924+\ln\eta\Bigg).$$

of $2^{\frac{n^2-3n+4}{2}}\eta^{\frac{(n-1)(n-2)}{2}}\prod_{s=2}^{n}\frac{1}{\xi(s)}$.

Using $\ln n-\ln(n-2)>\frac{2}{n}$, we have

$$-\frac{1}{4}n^2\ln(n-2)+\frac{1}{8}n^2-\frac{3}{2}n\ln(n-2)+2n+4\ln(n-2)-\frac{9}{2}$$

$$<-\frac{1}{4}n^2\ln n+\frac{1}{8}n^2-\frac{3}{2}n\ln n+\frac{5}{2}n+4\ln n-\frac{3}{2}.$$

Hence we have an simplified form of upper bound

$$\prod_{s=2}^{5}\frac{1}{\xi(s)}\cdot\exp\Bigg(-\frac{1}{4}n^2\ln n+n^2\left(\frac{3}{4}\ln 2+\frac{1}{4}\ln\pi+\frac{1}{2}\ln\eta+\frac{3}{8}\right)$$

$$-\frac{3}{2}n\ln n+n\left(-\frac{5}{4}\ln 2-\frac{1}{4}\ln\pi-\frac{3}{2}\ln\eta+\frac{7}{4}\right)+4\ln n-11.4495+\ln\eta\Bigg),$$

of $2^{\frac{n^2-3n+4}{2}}\eta^{\frac{(n-1)(n-2)}{2}}\prod_{s=2}^{n}\frac{1}{\xi(s)}$.

Since $\ln\left(\prod_{s=2}^{5}\frac{1}{\xi(s)}\right)=1.85914510535951$, we have

Lemma 8

$$\exp\Bigg(-\frac{1}{4}n^2\ln n+n^2\left(\frac{3}{4}\ln 2+\frac{1}{4}\ln\pi+\frac{1}{2}\ln\eta+\frac{3}{8}\right)-2n\ln n+n\left(-\frac{5}{4}\ln 2-\frac{1}{4}\ln\pi-\frac{3}{2}\ln\eta+\frac{5}{4}\right)+2.8515+\ln\eta\Bigg)$$

$$<2^{\frac{n^2-3n+4}{2}}\eta^{\frac{(n-1)(n-2)}{2}}\prod_{s=2}^{n}\frac{1}{\xi(s)}<\exp\Bigg(-\frac{1}{4}n^2\ln n+n^2\left(\frac{3}{4}\ln 2+\frac{1}{4}\ln\pi+\frac{1}{2}\ln\eta+\frac{3}{8}\right)$$

$$-\frac{3}{2}n\ln n+n\left(-\frac{5}{4}\ln 2-\frac{1}{4}\ln\pi-\frac{3}{2}\ln\eta+\frac{7}{4}\right)+4\ln n-9.5903+\ln\eta\Bigg).$$

3.2 *The bound of the product of the integration part*

Let $n \geq 22$. We start with the following theorem that is used in the main computation.
Theorem 9 Let $0 < x < 1$ be a real number. Then we have

$$\prod_{k=1}^{n}(1-x^k) \geq \exp\left(\frac{x(1-x^n)}{1-x}(\ln(1-x)-1)\right). \tag{7}$$

Proof. Using Taylor series for $\ln(1-x^2)$ at $x=0$, we have

$$-\sum_{k=1}^{n}\ln(1-x^k) = \sum_{k=1}^{n}\left(\sum_{i=1}^{\infty}\frac{x^{ki}}{i}\right) = \sum_{i=1}^{\infty}\frac{1}{i}\left(\sum_{k=1}^{n}(x^i)^k\right).$$

Note that it is equal to

$$\sum_{i=1}^{\infty}\frac{1}{i}\frac{x^i\left(1-x^{in}\right)}{1-x^i} = \frac{x(1-x^n)}{1-x}\left(1+\sum_{i=2}^{\infty}\frac{x^{i-1}(1+x^n+\cdots+x^{(i-1)n})}{i\,(1+x+\cdots+x^{i-1})}\right),$$

and it is smaller than

$$\frac{x(1-x^n)}{1-x}\left(1+\sum_{i=2}^{\infty}\frac{x^{i-1}}{i-1}\right) = \frac{x(1-x^n)}{1-x}(1-\ln(1-x)).$$

It leads to the following inequality

$$\sum_{k=1}^{n}\ln(1-x^k) > \frac{x(1-x^n)}{1-x}(\ln(1-x)-1),$$

and therefore we have

$$\prod_{k=1}^{n}(1-x^k) = \exp\left(\sum_{k=1}^{n}\ln(1-x^k)\right) > \exp\left(\frac{x(1-x^n)}{1-x}(\ln(1-x)-1)\right).$$

□

Then let us apply the change of variables to the integration part as follows:

$$
\begin{aligned}
&\prod_{i=1}^{n-1}\int_{-\eta}^{\eta}\sqrt{\delta^2-x^2}^{-i(n-i)}dx\\
=&\prod_{i=1}^{n-1}\int_{-\sin^{-1}\left(\frac{\eta}{\delta}\right)}^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\delta\cos\theta)^{-i(n-i)}\delta\cos\theta d\theta(x=\delta\sin\theta)\\
=&\prod_{i=1}^{n-1}\delta^{-i(n-i)+1}\int_{-\sin^{-1}\left(\frac{\eta}{\delta}\right)}^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\cos\theta)^{-i(n-i)+1}d\theta\\
=&\prod_{i=1}^{n-1}2\delta^{-i(n-i)+1}\int_{0}^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta.
\end{aligned}
$$

For convenience, let $m=i(n-i)-1$. Since

$$
\begin{aligned}
&\int(\sec\theta)^m d\theta\\
=&\frac{\sec^{m-2}x\tan x}{m-1}+\frac{m-2}{m-1}\int(\sec\theta)^{m-2}d\theta\\
=&\frac{\sec^{m-2}x\tan x}{m-1}+\frac{m-2}{m-1}\frac{\sec^{m-4}x\tan x}{m-3}+\frac{m-2}{m-1}\frac{m-4}{m-3}\int(\sec\theta)^{m-4}d\theta\\
=&\frac{\sec^{m-2}x\tan x}{m-1}+\frac{m-2}{m-1}\frac{\sec^{m-4}x\tan x}{m-3}+\frac{m-2}{m-1}\frac{m-4}{m-3}\frac{\sec^{m-6}x\tan x}{m-5}\\
&+\frac{m-2}{m-1}\frac{m-4}{m-3}\frac{m-6}{m-5}\int(\sec\theta)^{m-6}d\theta\\
=&\cdots,
\end{aligned}
$$

we have a lower bound of $\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta$ as follows: if m is even, we have

$$\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta$$

$$> \left[\frac{\sec^{m-2} x \tan x}{m-1} + \frac{\sec^{m-4} x \tan x}{m-1} + \frac{\sec^{m-6} x \tan x}{m-1} + \cdots + \frac{\sec^{2} x \tan x}{m-1} + \frac{\tan x}{m-1}\right]_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}$$

$$= \left[\frac{\sec^{m-2} x \tan x}{m-1}\left(\frac{1-\cos^m x}{1-\cos^2 x}\right)\right]_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}$$

$$= \frac{\sec^{m-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\tan\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{m-1} \frac{1-\cos^m\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{1-\cos^2\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}$$

$$= \frac{\sec^{m-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\tan\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{m-1} \frac{1-\cos^m\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{\frac{\eta^2}{\delta^2}}$$

$$= \frac{\cos^{-m+2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\tan\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{m-1} \frac{1-\cos^m\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{\frac{\eta^2}{\delta^2}}$$

$$= \frac{\delta^2}{\eta^2(m-1)}\left(\frac{\frac{\eta}{\delta}}{\cos^{m-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)} - \frac{\eta}{\delta}\cos\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)$$

$$= \frac{\delta}{\eta(m-1)} \frac{1}{\cos^{m-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(1-\cos^m\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)$$

$$= \frac{\delta}{\eta\left(i(n-i)-2\right)} \frac{1}{\cos^{i(n-i)-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)} \cdot \left(1-\cos^{i(n-i)-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right).$$

Therefore

$$
\begin{aligned}
&\prod_{i=1}^{n-1}\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta\\
&>\prod_{i=1}^{n-1}\frac{\delta}{\eta\left(i(n-i)-2\right)}\frac{1}{\cos^{i(n-i)-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\cdot\left(1-\cos^{i(n-i)-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)\\
&=\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{i(n-i)-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{i(n-i)-2}\\
&>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{i(n-i)-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{i(n-i)-1}\\
&>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{in}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{in}\\
&>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\frac{1}{(n-1)!\,n^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\\
&\quad\cdot\exp\left(\frac{\cos^{n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\left(1-\cos^{(n-1)n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)}{1-\cos^{n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(\ln\left(1-\cos^{n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)-1\right)\right),
\end{aligned}
$$

by Theorem 9.

To find a lower bound when m is odd, we have to set the following lemma.

Lemma 10 Let $0<x<\frac{\sqrt{3}}{2}$ and $l\geq 19$. Then we have

$$\frac{1-x^{l-2}}{l}>\frac{1-x^{l+2}}{l+2}. \tag{8}$$

Proof. Note that Eq. (8) is equivalent to

$$(l+2)x^{l-2}-lx^{l+2}<2,$$

whose LHS is lower than $f(l)=(l+2)\left(\frac{\sqrt{3}}{2}\right)^{l-2}$. Since $f'(l)<0$ for any $l\geq 6$ and $f(19)<2$, we conclude that the inequality (8) is satisfied when $l\geq 19$. □

Then we are ready to find a lower bound of the integration part when m is odd. We start with the following inequalities and equations.

$$\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta$$

$$>\left[\frac{\sec^{m-2} x\tan x}{m-1}+\frac{\sec^{m-4} x\tan x}{m-1}+\frac{\sec^{m-6} x\tan x}{m-1}+\cdots+\frac{\sec^{3} x\tan x}{m-1}+\frac{1}{m-1}\ln\left|\sec x+\tan x\right|\right]_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}$$

$$=\left[\frac{\sec^{m-2} x\tan x}{m-1}\left(\frac{1-\cos^{m-3} x}{1-\cos^2 x}\right)+\frac{1}{m-1}\ln\left|\sec x+\tan x\right|\right]_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}$$

$$=\frac{\delta}{\eta(m-1)}\frac{1}{\cos^{m-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(1-\cos^{m-3}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)+\frac{1}{m-1}\ln\left|\sec\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)+\tan\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right|$$

$$>\frac{\delta}{\eta(m-1)}\frac{1}{\cos^{m-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(1-\cos^{m-3}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right).$$

Similar to the case when m is even, we have a lower bound

$$\prod_{i=1}^{n-1}\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta$$

$$>\prod_{i=1}^{n-1}\frac{\delta}{\eta\left(i(n-i)-2\right)}\frac{1}{\cos^{i(n-i)-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\cdot\left(1-\cos^{i(n-i)-4}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)$$

$$=\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{i(n-i)-4}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{i(n-i)-2}$$

$$>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{i(n-i)}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{i(n-i)}\text{ by Lemma 3.2}$$

$$>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\cdot\prod_{i=1}^{n-1}\frac{1-\cos^{in}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}{in}$$

$$>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\frac{1}{(n-1)!\,n^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)$$

$$\cdot \exp\left(\frac{\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\left(1-\cos^{(n-1)n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)}{1-\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(\ln\left(1-\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)-1\right)\right),$$

by Theorem 9.

Note that the formula for the lower bound is given by the same formula for both even and odd m. Therefore we have the following.

Lemma 11 Let $n \geq 22$. Then we have

$$\prod_{i=1}^{n-1}\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta$$

$$>\frac{\delta^{n-1}}{\eta^{n-1}}\cdot\frac{1}{(n-1)!\,n^{n-1}}\cdot\cos^{-\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)$$

$$\cdot \exp\left(\frac{\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\left(1-\cos^{(n-1)n}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)}{1-\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)}\left(\ln\left(1-\cos^n\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\right)-1\right)\right).$$

Because $\int(\sec\theta)^m d\theta < \dfrac{\sec^{m-2}x\tan x}{m-1}+\dfrac{m-2}{m-1}\int(\sec\theta)^m d\theta$, an upper bound is as follows:

Lemma 12

$$\prod_{i=1}^{n-1}\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta < \frac{\eta^{n-1}}{\delta^{n-1}}\sec^{\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\left(\frac{\eta}{\delta}\right)\right)\right).$$

Proof.

$$\prod_{i=1}^{n-1}\int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)}(\sec\theta)^{i(n-i)-1}d\theta$$

$$<\prod_{i=1}^{n-1}\sec^{m-2}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\tan\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)$$

$$=\tan^{n-1}\left(\sin^{-1}\left(\frac{\eta}{\delta}\right)\right)\sec^{\frac{(n-1)(n^2+n-18)}{6}}\left(\sin^{-1}\left(\left(\frac{\eta}{\delta}\right)\right)\right)$$

$$=\frac{\eta^{n-1}}{\delta^{n-1}}\sec^{\frac{(n-1)(n-3)(n+4)}{6}}\left(\sin^{-1}\left(\left(\frac{\eta}{\delta}\right)\right)\right).$$

□

Combining Lemma 11 and 12, we have the following.
Lemma 13 Let $n \geq 22$ and $t = \sqrt{1-(\eta/\delta)^2}$. Then we have

$$\frac{\delta^{n-1}}{\eta^{n-1}} \cdot \frac{1}{(n-1)!\; n^{n-1}} \cdot t^{-\frac{(n-1)(n-3)(n+4)}{6}} \cdot \exp\left(\frac{t^n\left(1-t^{(n-1)n}\right)}{1-t^n}\left(\ln\left(1-t^n\right)-1\right)\right)$$

$$< \prod_{i=1}^{n-1} \int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta$$

$$< \frac{\eta^{n-1}}{\delta^{n-1}} \cdot t^{-\frac{(n-1)(n-3)(n+4)}{6}}.$$

Then we have a more simplified lower and upper bound of $\prod_{i=1}^{n-1} \int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta$ as follows:
Lemma 14 Let $n \geq 22$, $t = \sqrt{1-(\eta/\delta)^2}$ and $a = t^n$. Then we have

$$\frac{\delta^{n-1}}{\eta^{n-1}} \cdot \exp\left(-2(n-1)\ln n + \frac{a(1-a^{n-1})}{1-a}(\ln(1-a)-1) + \left(-\frac{n^2}{6}+3\right)\ln a\right)$$

$$< \prod_{i=1}^{n-1} \int_0^{\sin^{-1}\left(\frac{\eta}{\delta}\right)} (\sec\theta)^{i(n-i)-1} d\theta < \frac{\eta^{n-1}}{\delta^{n-1}} a^{-\frac{n^2}{6}}.$$

Proof.

$$\frac{\delta^{n-1}}{\eta^{n-1}} \cdot \frac{1}{(n-1)!\; n^{n-1}} \cdot t^{-\frac{(n-1)(n-3)(n+4)}{6}} \cdot \exp\left(\frac{t^n\left(1-t^{(n-1)n}\right)}{1-t^n}\left(\ln\left(1-t^n\right)-1\right)\right)$$

$$> \frac{\delta^{n-1}}{\eta^{n-1}} \frac{1}{(n-1)! n^{n-1}} a^{-\frac{n^2}{6}+3} \exp\left(\frac{a(1-a^{n-1})}{1-a}(\ln(1-a)-1)\right)$$

$$> \frac{\delta^{n-1}}{\eta^{n-1}} \cdot \exp\left(-2(n-1)\ln n + \frac{a(1-a^{n-1})}{1-a}(\ln(1-a)-1) + \left(-\frac{n^2}{6}+3\right)\ln a\right).$$

Also we have

$$\frac{\eta^{n-1}}{\delta^{n-1}} t^{-\frac{(n-1)(n-3)(n+4)}{6}} < \frac{\eta^{n-1}}{\delta^{n-1}} a^{-\frac{n^2}{6}}.$$

□

4. Conclusion

In this section, we summarize the previous results and give two approximations.

In the previous sections 3.1 and 3.2, we have the following simplified bound of the average number of the $(\delta,\,\eta)$-LLL bases in dimension n.

Theorem 15 Let $n \geq 22$, $t = \sqrt{1-(\eta/\delta)^2}$, and $a = t^n$. Then we have

$$\frac{\delta^{n-1}}{\eta^{n-1}} \cdot \exp\Bigg(-\frac{1}{4}n^2 \ln n + n^2 \left(\frac{3}{4}\ln 2 + \frac{1}{4}\ln \pi + \frac{1}{2}\ln \eta + \frac{3}{8} - \frac{1}{6}\ln a\right)$$

$$-4n \ln n + n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln \pi - \frac{3}{2}\ln \eta + \frac{5}{4}\right) + 2.8515 + \ln \eta + \frac{a(1-a^{n-1})}{1-a}(\ln(1-a)-1) + 3\ln a\Bigg)$$

$$< 2^{\frac{n^2-3n+4}{2}} \eta^{\frac{(n-1)(n-2)}{2}} \prod_{i=2}^{n} \frac{1}{\xi(i)} \cdot \prod_{i=1}^{n-1} \int_{-\eta}^{\eta} \sqrt{\delta^2 - x^2}^{\,-i(n-i)} dx$$

$$< \frac{\eta^{n-1}}{\delta^{n-1}} \cdot \exp\Bigg(-\frac{1}{4}n^2 \ln n + n^2 \left(\frac{3}{4}\ln 2 + \frac{1}{4}\ln \pi + \frac{1}{2}\ln \eta + \frac{3}{8} - \frac{1}{6}\ln a\right)$$

$$-\frac{3}{2}n \ln n + n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln \pi - \frac{3}{2}\ln \eta + \frac{7}{4}\right) + 4\ln n - 9.5903 + \ln \eta\Bigg).$$

Note that the upper bound of the previous theorem is a refinement of the existing result given by [14] as $O(1.02^{n^3})$. Because we are focusing on the practical case, we assume that η and δ are sufficiently close to $\frac{1}{2}$ and 1, respectively. Let $\frac{1}{2} < \eta < \frac{3}{4\sqrt{2}}$, $\frac{3}{4} < \delta < 1$ and $n \geq 22$. Then $\frac{\sqrt{2}}{2} < t < \frac{\sqrt{3}}{2}$, and therefore we have

$$\frac{\delta^{n-1}}{\eta^{n-1}} \cdot \exp\left(n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln \pi - \frac{3}{2}\ln \eta + \frac{5}{4}\right) + 2.8515 + \ln \eta + \frac{a(1-a^{n-1})}{1-a}(\ln(1-a)-1) + 3\ln a\right)$$

$$> \exp\Bigg(n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln \pi - \frac{3}{2}\ln \frac{3}{4\sqrt{2}} + \frac{5}{4}\right) + 2.8515 + \ln \frac{1}{2}$$

$$+ \frac{\left(\frac{\sqrt{3}}{2}\right)^n \left(1 - \left(\frac{\sqrt{2}}{2}\right)^{n(n-1)}\right)}{1-\left(\frac{\sqrt{3}}{2}\right)^n} \left(\ln\left(1 - \left(\frac{\sqrt{3}}{2}\right)^n\right) - 1\right) + 3\ln\left(\frac{\sqrt{2}}{2}\right)^n + (n-1)\ln\sqrt{2}\Bigg) > 0,$$

and we have

$$\frac{\eta^{n-1}}{\delta^{n-1}} \cdot \exp\left(n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln\pi - \frac{3}{2}\ln\eta + \frac{7}{4}\right) + 4\ln n - 9.5903 + \ln\eta\right)$$

$$< \exp\left(n\left(-\frac{5}{4}\ln 2 - \frac{1}{4}\ln\pi - \frac{3}{2}\ln\frac{1}{2} + \frac{7}{4}\right) + 4\ln n - 9.5903 + \ln\frac{3}{4\sqrt{2}} + (n-1)\ln\frac{\sqrt{2}}{2}\right)$$

$$< \exp\left(\frac{3}{2}n\right).$$

Combining these inequalities, we give a tight approximation as follows:

Theorem 16 (A tight version) Let $\frac{1}{2} < \eta < \frac{3}{4\sqrt{2}}$, $\frac{3}{4} < \delta < 1$, $n \geq 22$, $t = \sqrt{1-(\eta/\delta)^2}$, and $a = t^n$. Then we have

$$\exp\left(-\frac{1}{4}n^2\ln n + n^2\left(\frac{3}{4}\ln 2 + \frac{1}{4}\ln\pi + \frac{1}{2}\ln\eta + \frac{3}{8} - \frac{1}{6}\ln a\right) - 4n\ln n\right)$$

$$< 2^{\frac{n^2-3n+4}{2}}\eta^{\frac{(n-1)(n-2)}{2}}\prod_{i=2}^{n}\frac{1}{\xi(i)} \cdot \prod_{i=1}^{n-1}\int_{-\eta}^{\eta}\sqrt{\delta^2-x^2}^{-i(n-i)}dx$$

$$< \exp\left(-\frac{1}{4}n^2\ln n + n^2\left(\frac{3}{4}\ln 2 + \frac{1}{4}\ln\pi + \frac{1}{2}\ln\eta + \frac{3}{8} - \frac{1}{6}\ln a\right) - \frac{3}{2}n\ln n + \frac{3}{2}n\right).$$

$a = t^n$, or equivalently, $\ln a = n\ln t$, implies that $\exp\left(-\frac{1}{6}n^2\ln a\right) = a^{-\frac{1}{6}n^2} = t^{-\frac{1}{6}n^3}$ is the leading term of the approximation of

$$2^{\frac{n^2-3n+4}{2}}\eta^{\frac{(n-1)(n-2)}{2}}\prod_{i=2}^{n}\frac{1}{\xi(i)} \cdot \prod_{i=1}^{n-1}\int_{-\eta}^{\eta}\sqrt{\delta^2-x^2}^{-i(n-i)}dx.$$

Therefore we suggest a rough approximation as follows:

Corollary 17 (A rough version) Let $\frac{1}{2} < \eta < \frac{3}{4\sqrt{2}}$, $\frac{3}{4} < \delta < 1$, and $n \geq 22$. Then we have a rough approximation

$$\left(1-(\eta/\delta)^2\right)^{-\frac{1}{12}n^3},$$

of the average number of the $(\delta,\ \eta)$-LLL bases in dimension *n*. Immediately, the following asymptotic behavior

$$\lim_{n\to\infty}\frac{n^3\ln\left(\left(1-(\eta/\delta)^2\right)\right)}{\ln\left(2(2\eta)^{\frac{(n-1)(n-2)}{2}}\prod_{i=2}^{n}\frac{S_i(1)}{\zeta(i)} \cdot \frac{1}{n}\prod_{i=1}^{n-1}\frac{1}{i(n-i)} \cdot \prod_{i=1}^{n-1}\int_{-\eta}^{\eta}\sqrt{\delta^2-x^2}^{-i(n-i)}dx\right)} = -12,$$

holds.

Finally, we give two experimental results related to the duration of time to compute and the computed values of the average number of the (δ, η)-LLL bases in dimension n. The follwing Table 1 is the duration of time to compute the exact value and that of the approximate results for a tight approximation in Theorem 16 of the average number of the (δ, η)-LLL bases in dimension $n = 20, 40, \ldots, 160$. In this table, we use second as a unit of time and shows that the duration time to obtain the approximation values is much smaller than that of the exact value.

Table 1. Duration of time to compute a tight bound and the exact value of the average number of the (δ, η)-LLL bases in dimension n

Dimension	Duration of time (sec)		
n	Upper bound	Exact value	Lower bound
20	0.0088	44.5983	0.0002
40	0.0006	524.034	0.0002
60	0.0002	858.937	0.0001
80	0.0046	1,187.68	0.0045
100	0.0116	1,547.19	0.0118
120	0.0010	1,958.1	0.0009
140	0.0491	2,414.36	0.0487
160	0.0839	2,965.76	0.0816

Also we give computed values of the three cases, the lower, upper bound, and the exact value in Theorem 16, in Table 2. It shows that we find a right approximation of the exact value even the dimension is high.

Table 2. Computed values of a tight bound and the exact value of the average number of the (δ, η)-LLL bases in dimension n

Dimension	Computed values		
n	Upper bound	Exact value	Lower bound
20	1.4111×10^{72}	2.8791×10^{41}	1.1729×10^{-6}
40	1.9890×10^{535}	5.8551×10^{446}	1.0839×10^{349}
60	1.8770×10^{1832}	6.2983×10^{1675}	2.9125×10^{1526}
80	8.2136×10^{4428}	7.6319×10^{4197}	1.5177×10^{3996}
100	5.7482×10^{8800}	1.7127×10^{8490}	4.1244×10^{8235}
120	4.8272×10^{15428}	5.3153×10^{15034}	5.7058×10^{14726}
140	9.0743×10^{24796}	1.9539×10^{24316}	4.0847×10^{23954}
160	1.6129×10^{37392}	1.0634×10^{36822}	2.1327×10^{36406}

We use the computer with the following status-CPU: AMD R9-5900X, 3.70GHz, RAM: 32GB with Mathematica 13.1 version.

In conclusion, we find rough and tight approximations of the average number of the (δ, η)-LLL bases in dimension n when $n \geq 22$. We firstly simplify the known formula and then approximate two parts which take a long time to compute. After that, we restrict δ and η which are used in practical situation to get a better approximation. Lastly, we give two experimental results that show the approximation is right and much faster to compute. We hope that these results can be used to examine the quality of the (δ, η)-LLL bases quickly when the dimension n is greater than or equal to 22.

To help understand the overall results, the following graphs are attached. As can be seen from the graphs, computing the approximated values requires much shorter time and the calculated values are similar to the exact ones. Since the calculated values are so large that it is difficult to directly express it in a graph, the values that displayed in the graph are computed by applying the natural logarithm.

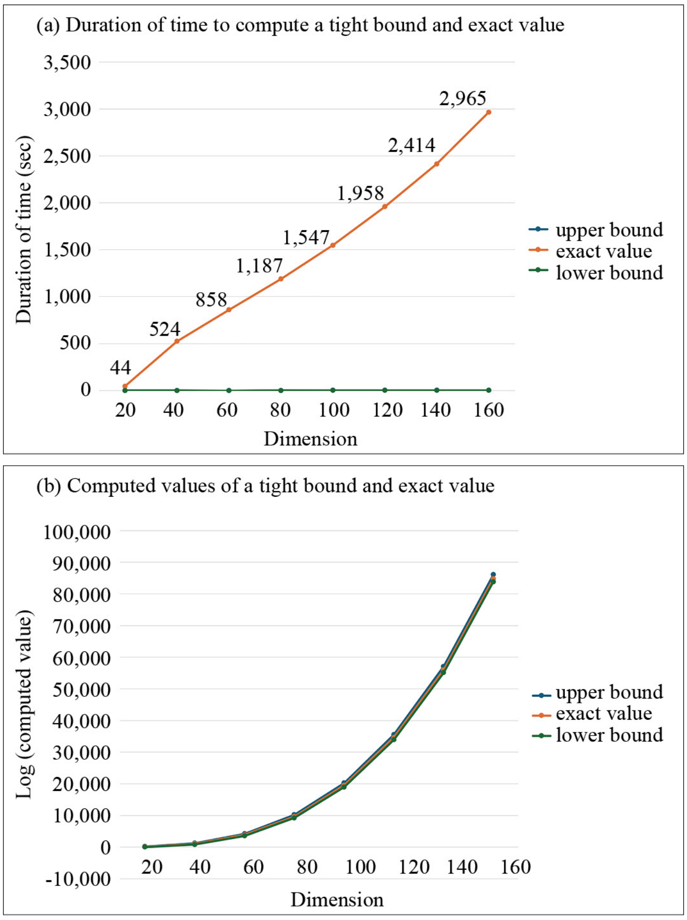

Figure 1. Graphical results for the efficiency and accuracy of the approximations of the average number of the (δ, η)-LLL bases in dimension n

From the value of the average number of the LLL bases, the average-case performance of LLL can be similar to the worst-case. Our results indicates this tendency is expected to be more severe in higher dimensions. Now, it can be said that attention should be paid to how to select the output of the LLL algorithm. But if the average number is used to establish a baseline on how much attention should be paid to the output of the LLL algorithm, we hope that it will be a way to present the criteria for how careful output selection should be when driving the LLL algorithm at higher dimensions without directly calculating the exact value.

Acknowledgement

The authors would like to thank the reviewer for his/her valuable comments for the improvement of this paper. This research was supported by the 2025 scientific promotion program funded by Jeju National University.

Conflict of interest

The authors declare no competing financial interest.

References

[1] Ajtai M. Generating hard instances of lattice problems. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. USA: Association for Computing Machinery; 1996. p.99-108.

[2] Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R. *Software and Hardware Implementation of Lattice-Cased Cryptography Schemes*. USA: Center for Embedded Cyber-Physical Systems; 2017. p.1-43.

[3] Khalid A, McCarthy S, Neill MO, Liu W. Lattice-based cryptography for IoT in a quantum world: Are we ready? In: *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*. Otranto, Italy: IEEE; 2019. p.194-199. Available from: https://doi.org/10.1109/IWASI.2019.8791343.

[4] Kocabaş O, Soyata T. Medical data analytics in the cloud using homomorphic encryption. In: *E-Health and Telemedicine: Concepts, Methodologies, Tools, and Applications*. USA: IGI Global; 2016. p.751-768.

[5] Hoffstein J, Pipher J, Silverman JH. *An Introduction to Mathematical Cryptography, Vol. 1*. New York: Springer; 2008.

[6] Lenstra AK, Lenstra HW, Lovász L. Factoring polynomials with rational coefficients. *Mathematische Annalen*. 1982; 261: 515-534. Available from: https://doi.org/10.1007/BF01457454.

[7] Debris-Alazard T, Ducas L, Van Woerden WP. An algorithmic reduction theory for binary codes: LLL and more. *IEEE Transactions on Information Theory*. 2022; 68(5): 3426-3444. Available from: https://doi.org/10.1109/TIT.2022.3143620.

[8] Goldberger A, Strassler Y. A practical algorithm for completing half-Hadamard matrices using LLL. *Journal of Algebraic Combinatorics*. 2022; 55(1): 217-244. Available from: https://doi.org/10.1007/s10801-021-01077-z.

[9] Cho GH, Lee HS, Lim S, Kim Y. Storage efficient algorithm for hermite normal form using LLL. *Linear Algebra and Its Applications*. 2021; 613: 183-200. Available from: https://doi.org/10.1016/j.laa.2020.12.022.

[10] Ulla MM, Khan MS, Sakkari DS. Implementation of elliptic curve cryptosystem with bitcoin curves on SECP256k1, NIST256p, NIST521p, and LLL. *Journal of ICT Standardization*. 2023; 11(4): 329-353. Available from: https://doi.org/10.13052/jicts2245-800X.1141.

[11] Wang Y, Takagi T. Studying lattice reduction algorithms improved by quick reordering technique. *International Journal of Information Security*. 2021; 20: 257-268. Available from: https://doi.org/10.1007/s10207-020-00501-y.

[12] Charton F, Lauter K, Li C, Tygert M. An efficient algorithm for integer lattice reduction. *arXiv:2303.02226*. 2023. Available from: https://doi.org/10.48550/arXiv.2303.02226.

[13] Jung J, Song K. A study on some approximations on the average number of the LLL bases in higher dimensions. 2022. *arXiv:2203.09406*. Available from: https://doi.org/10.48550/arXiv.2203.09406.

[14] Kim S. *On the Shape of a High-Dimensional Random Lattice*. USA: Stanford University; 2015.

[15] Song K, Seo Y. A study on the average number of LLL-based using statistical learning. *International Journal on Advanced Science, Engineering and Information Technology*. 2024; 14(3): 906-911.

[16] Batir N. Inequalities for the gamma function. *Archiv der Mathematik*. 2008; 91(6): 554-563. Available from: https://doi.org/10.1007/s00013-008-2856-9.