Efficient Estimation of Number of Short Lattice Vectors in Search Space under Randomness Assumption

Yoshitatsu Matsuda
matsuda@st.seikei.ac.jp
Seikei University
Musashino-shi, Tokyo, Japan

Tadanori Teruya
tadanori.teruya@aist.go.jp
National Institute of Advanced
Industrial Science and Technology
Koto-ku, Tokyo, Japan

Kenji Kashiwabara
kashiwa@idea.c.u-tokyo.ac.jp
The University of Tokyo
Meguro-ku, Tokyo, Japan

ABSTRACT

Lattice basis reduction algorithms are widely-used heuristic methods for solving the Shortest Vector Problem (SVP) on lattices. Recently, the sampling reduction approach has achieved high performance solving the SVP on high-dimensional lattices. It repeats a generation process of short lattice vectors and a lattice basis reduction algorithm alternately. In the generation process, it generates a lot of lattice vectors in a search space based on a current lattice basis and selects short lattice vectors from them. Therefore, it is quite important for investigating and accelerating the sampling reduction to estimate the number of short lattice vectors in a search space. In this paper, we propose a new method for estimating the number of short lattice vectors by the Gram-Charlier A series under the randomness assumption. The Gram-Charlier A series is a basic asymptotic expansion of any probability distribution by utilizing the higher order cumulants such as the skewness and the kurtosis. The proposed method uses a “parametric” model, which gives a calculable and continuous function of the number of short lattice vectors. The proposed method is much more efficient than the previous methods using the non-parametric estimation. Moreover, its convergence speed can be evaluated theoretically. This is expected to enable us to investigate lattice basis reduction algorithms intensively in various situations and clarify their properties. Numerical experiments verified that this method can estimate the number of short lattice vectors of an actual lattice basis quite accurately.

CCS CONCEPTS

• **Security and privacy** → **Cryptography; Public key (asymmetric) techniques.**

KEYWORDS

public-key cryptography, lattice techniques, probability theory

ACM Reference Format:

Yoshitatsu Matsuda, Tadanori Teruya, and Kenji Kashiwabara. 2019. Efficient Estimation of Number of Short Lattice Vectors in Search Space under Randomness Assumption. In *The 6th ACM ASIA Public-Key Cryptography*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

APKC '19, July 8, 2019, Auckland, New Zealand

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6784-4/19/07...\$15.00

<https://doi.org/10.1145/3327958.3329543>

Workshop (APKC '19), July 8, 2019, Auckland, New Zealand. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3327958.3329543>

1 INTRODUCTION

Recently, post-quantum cryptography has drawn a great deal of attention, where lattice-based cryptography is known to be a promising approach [11]. Lattice-based cryptography is essentially based on the difficulty of the shortest vector problem (SVP). The SVP is the problem of finding the shortest non-zero lattice vector of a given lattice basis. It is formalized to the minimization problem of the Euclidean norm (namely, the length) $\ell = \left\| \sum_{i=1}^n a_i \vec{b}_i \right\|$ with respect to non-zero $\vec{a} = (a_i) \in \mathbb{Z}^n$, where $\{\vec{b}_1, \dots, \vec{b}_n\}$ ($\vec{b}_i \in \mathbb{R}^m$) is a basis vector of the lattice, where a full-rank integral lattice ($n = m$ and $\vec{b}_i \in \mathbb{Z}^m$) is usually assumed.

The practical difficulty of the SVP is not known. Therefore, many algorithms have been proposed for solving the SVP as efficiently as possible. Some algorithms can find the exact shortest lattice vector in a low-dimensional lattice, for example, enumeration [12] and sieving [2]. However, the exact SVP is known to be an intractable problem in a high-dimensional lattice. Therefore, an approximate version of the SVP (often called Hermite-SVP) is widely used in practice, where not the exact shortest but very short lattice vectors are sought. In other words, we search for $\vec{a}$ satisfying $\left\| \sum_{i=1}^n a_i \vec{b}_i \right\| < (1 + \epsilon) \hat{\ell}$, where $\hat{\ell}$ is an estimation of the exact minimum and ϵ is a small threshold. Many algorithms have been proposed for finding an approximate short lattice vector, for example, the Lenstra-Lenstra-Lovász algorithm (LLL) [13], the block Korkine-Zolotarev algorithm (BKZ) [18], random sampling reduction (RSR) [17], a sieving-type algorithm [7], and so on.

Currently, many state of the art algorithms compete with each other for solving Hermite-SVP efficiently in high-dimensional sample lattices from TU Darmstadt SVP challenge [16], for example, Teruya et al. [19], Aono and Nguyen [3], Kashiwabara and Fukase [9], and so on. These algorithms can be regarded as variants of the (random) sampling reduction. Generally speaking, they try to find relatively short lattice vectors in a search space. Then, they try to find very short lattice vector by repeating this search process incrementally. Therefore, it is quite important for evaluating and improving these algorithms to estimate the number of short lattice vectors in a given search space. Thus, many estimation methods have been previously proposed [3, 8–10]. The geometric description inspired by the Gaussian heuristic is a widely-used principle for estimating the number of short lattice vectors by using the volume of the intersection between the lattice and a ball [8]. However,

it is intractable in practice if the dimension n of lattice is large. Though some more efficient algorithms estimating the intersection have been proposed recently [3, 10], they are nevertheless time-consuming. We refer to these methods using the geometric description as the “non-parametric” approach in this paper. On the other hand, the “parametric” approach is proposed in [9], where the probability distribution of the lengths of lattice vectors is approximated as a normal distribution with only two parameters (the mean and the variance) under the randomness assumption and the central limit theorem. Though this approach is simple and quite efficient, it gives a rough estimate especially for short lengths as is pointed out in [3].

Our Contribution. In this paper, we propose a novel method based on the parametric approach by extending the normal approximation in order to estimate the number of short lattice vectors in a given search space. The key feature of the proposed method is that the probability distribution of the lengths is approximated by the Gram-Charlier A series, which is a basic asymptotic expansion of any probability distribution by utilizing the higher order cumulants (such as the skewness and the kurtosis). This method is essentially based only on the randomness assumption. This method is quite efficient especially for a class of search spaces (that we call product-type search space) which includes both a singleton with a natural number representation and the RSR-type search space. In addition, its convergence speed is theoretically guaranteed to be high. Numerical experiments in the RSR-type search space verified that the proposed method is much more efficient than the non-parametric approach and can estimate the number of short lattice vectors much more accurately than the normal approximation.

Road Map. This paper is organized as follows. Section 2 gives the preliminaries such as the basic concepts of the SVP on lattices and the introduction of the Gram-Charlier A series. Section 3 describes the related work about both the previous non-parametric and parametric approaches for estimating the number of short lattice vectors. Section 4 explains our proposed method using the Gram-Charlier A series and its convergence speed. In Section 5, the numerical experiments in the RSR-type search space verify the efficiency and accuracy of our proposed method. Lastly, this paper is concluded in Section 6.

2 PRELIMINARIES

2.1 Basic Concepts of the Shortest Vector Problem on Lattices

Here, the preliminary notations and definitions about SVP are introduced. A full-rank integral lattice basis is given as an $n \times n$ matrix $B = (\vec{b}_1, \dots, \vec{b}_n)$, where each $\vec{b}_i = (b_{ij}) \in \mathbb{Z}^n$ is a basis vector. The lattice $L(B)$ is the additive group consisting of $\sum_{i=1}^n a_i \vec{b}_i$ for $a_i \in \mathbb{Z}$. The Euclidean inner product of $\vec{x}$ and $\vec{y}$ is denoted by $\langle \vec{x}, \vec{y} \rangle = \vec{x}^T \vec{y}$. The Euclidean norm (length) of $\vec{x}$ is defined as $\|\vec{x}\| = \sqrt{\langle \vec{x}, \vec{x} \rangle}$. $\vec{b}_i$ can be orthogonalized to $\vec{b}_i^* = (b_{ij}^*)$ by the following Gram-Schmidt process:

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \eta_{ji} \vec{b}_j^* \text{ and } \eta_{ji} = \frac{\langle \vec{b}_j^*, \vec{b}_i \rangle}{\|\vec{b}_j^*\|^2}. \quad (1)$$

Then, $\langle \vec{b}_i^*, \vec{b}_j^* \rangle = 0$ holds for $i \neq j$. Note that $\|\vec{b}_i^*\|$ is not constrained to be 1. B provides the fundamental parallelepiped $\{\sum_{i=1}^n t_i \vec{b}_i : t_i \in [0, 1)\}$, the volume of which is independent of the choice of the basis for the same lattice. This volume is called the determinant (or co-volume) of $L(B)$. Note that the determinant is equal to $\prod_{i=1}^n \|\vec{b}_i^*\|$.

A lattice vector $\sum_{i=1}^n a_i \vec{b}_i$ ($a_i \in \mathbb{Z}$) is given as $\sum_{i=1}^n \zeta_i \vec{b}_i^*$. The squared length of the lattice vector (denoted by ℓ^2) is given as

$$\ell^2 \left(\sum_{i=1}^n a_i \vec{b}_i \right) = \left\| \sum_{i=1}^n \zeta_i \vec{b}_i^* \right\|^2 = \sum_{i=1}^n \zeta_i^2 \|\vec{b}_i^*\|^2. \quad (2)$$

Because each $\zeta_i \in \mathbb{R}$ is given as the sum of a residual $\bar{\zeta}_i$ ($-\frac{1}{2} \leq \bar{\zeta}_i < \frac{1}{2}$) and an integer, ζ_i is uniquely determined by a natural number d_i satisfying

$$-\frac{d_i + 1}{2} \leq \zeta_i < -\frac{d_i}{2} \text{ or } \frac{d_i}{2} \leq \zeta_i < \frac{d_i + 1}{2}, \quad (3)$$

where the natural numbers begin with 0 (namely, $d_i = 0$ is allowed). The sequence $\vec{d} = (d_1, \dots, d_n)$ is called the natural number representation. It was shown in [9] that any vector in the lattice is uniquely determined by $\vec{d}$ and $B^* = (\vec{b}_1^*, \dots, \vec{b}_n^*)$. In other words, there is a one-to-one correspondence between a natural number representation and a lattice vector. Therefore, any search space of the lattice vectors can be defined as a set of natural number representations (denoted by Υ). A simple search space is used in RSR [17] and its extension [4, 14], where Υ is defined as an n -ary Cartesian product: $\Upsilon = v_1 \times v_2 \times \dots \times v_n$. Each v_i is a set of natural numbers under a maximum T_i : $\{0, 1, \dots, T_i\}$. The original RSR sets T_i to 1 for relatively large i and to 0 otherwise. We call it the RSR-type search space. A more general class of the search space can be introduced by defining each v_i as any non-empty set of natural numbers. We call the class the product-type search space. Note that the product-type search space includes any RSR-type search space and any singleton with a natural number representation.

The randomness assumption is defined as follows.

ASSUMPTION 1 (RANDOMNESS ASSUMPTION). Every residual $\bar{\zeta}_i$ is uniformly distributed in $[-\frac{1}{2}, \frac{1}{2})$ and is mutually independent of each other.

Though there are several different definitions of the randomness assumption, we employ the one above based on Schnorr's assertion [17]. The randomness assumption can not hold rigorously for actual lattices. However, it is quite useful for investigating and predicting the behavior of some algorithms for solving SVP. In addition, Ludwig [14] has observed experimentally that it holds approximately in some cases.

By assuming that the volume of $L(B)$ is approximately equal to the volume of a ball with the radius of the shortest lattice vector length, the length of the shortest lattice vector is estimated as

$$\ell_{\text{GH}} = \frac{\left(\Gamma\left(\frac{n}{2} + 1\right) \prod_{i=1}^n \|\vec{b}_i^*\| \right)^{\frac{1}{n}}}{\sqrt{\pi}}, \quad (4)$$

where Γ is the gamma function occurring in the calculation of the volume of an n -dimensional ball [11]. This approximation is called the Gaussian heuristic. Though the original shortest vector problem

(SVP) is to find the shortest non-zero lattice vector, it is generally too difficult to solve. In a similar way as in TU Darmstadt SVP challenge [16], we define the SVP as finding an extremely short lattice vector whose length is less than $(1 + \epsilon) \ell_{\text{GH}}$ where ϵ is a small positive constant ($\epsilon = 0.05$ in TU Darmstadt SVP challenge).

2.2 Gram-Charlier A Series

In this paper, we employ a classical statistical technique named the Gram-Charlier A series [6, 21] for estimating the number of short lattice vectors. Here, we explain this technique in brief.

2.2.1 Overview. Let $P(x)$ be a probability distribution function satisfying $P(x) \geq 0$ and $\int_{-\infty}^{\infty} P(x) dx = 1$. The Gram-Charlier A series is a well-known series expansion of $P(x)$ [6]. We assume that the random variable x is normalized. In other words, its mean μ and its variance σ^2 are 0 and 1, respectively. This assumption does not lose the generality because the variable of $P(x)$ is easily transformed by

$$\tilde{P}(z) = \frac{P\left(x = \frac{z - \mu_z}{\sigma_z}\right)}{\sigma_z}, \quad (5)$$

where μ_z and σ_z are the mean and the standard deviation over $\tilde{P}(z)$, respectively. Then, the Gram-Charlier A series of $P(x)$ is given as

$$P(x) = \left(1 + \sum_{r=3}^{\infty} c_r H_r(x)\right) \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}, \quad (6)$$

where $H_r(x)$ is the r -th degree Hermite polynomial defined as

$$He_r(x) e^{-\frac{x^2}{2}} = (-1)^r \frac{d^r}{dx^r} e^{-\frac{x^2}{2}}. \quad (7)$$

c_r is the r -th coefficient depending on the r -th and lower order cumulants (the details are described below). The series is guaranteed to converge if $P(x)$ decreases faster than $e^{-\frac{x^2}{4}}$ [5, 21].

2.2.2 Cumulants. Here, we explain the cumulants, which are the most important statistics for the Gram-Charlier A series. The r -th order cumulants of $P(x)$ (denoted by κ_r) are calculated recursively by

$$\kappa_r = \mu_r - \sum_{m=1}^{r-1} \binom{r-1}{m-1} \kappa_m \mu_{r-m}, \quad (8)$$

where μ_r is the r -th order moment of $P(x)$ given as

$$\mu_r = \int_{-\infty}^{\infty} x^r P(x) dx. \quad (9)$$

Then, $\kappa_1 = \mu_1$ and $\kappa_2 = \mu_2 - \mu_1^2 = \sigma^2$ are the mean and the variance, respectively. κ_3 and κ_4 are often called the skewness and the kurtosis, respectively. The cumulants are the important statistics characterizing any probability distribution and have various good mathematical properties. In this paper, we utilize the homogeneity and the additivity in the following. Let $\kappa_r(x)$ be the r -th order cumulant of a random variable x . Then, the following equation holds:

$$\kappa_r(ax) = a^r \kappa_r(x), \quad (10)$$

where a is an arbitrary constant. This property is called the homogeneity. If x and y are statistically independent random variables, the following equation holds:

$$\kappa_r(x + y) = \kappa_r(x) + \kappa_r(y). \quad (11)$$

This property is called the additivity. In addition, the following important property holds for any normal distribution: $\kappa_r = 0$ for $r \geq 3$.

2.2.3 Coefficients. Though the coefficients of the Gram-Charlier A series of the normalized distribution of x are given as complicated combinations of the cumulants, it has been known that they are simply described by the Bell polynomials [22]:

$$c_r = \frac{B_r(0, 0, \kappa_3, \kappa_4, \dots, \kappa_r)}{r! \sqrt{\kappa_2^r}}, \quad (12)$$

where κ_r is the r -th order cumulant of the non-normalized (original) distribution of z . B_r is the r -th complete exponential Bell polynomial, which can be calculated recursively by

$$B_{r+1}(u_1, u_2, \dots, u_{r+1}) = \sum_{i=0}^r \binom{r}{i} B_{r-i}(u_1, \dots, u_{r-i}) u_{i+1} \quad (13)$$

with $B_0 = 1$. Therefore, the calculation of c_r is of the order of r^2 .

There is another formulation of c_r . The Hermite polynomials have the following orthogonality property:

$$\int_{-\infty}^{\infty} He_p(x) He_q(x) e^{-\frac{x^2}{2}} dx = \sqrt{2\pi} p! \delta_{pq}, \quad (14)$$

where δ_{pq} is 1 if $p = q$ and 0 otherwise. Using the expectation of $He_r(x)$ ($r \geq 3$) over $P(x)$, c_r is given as

$$c_r = \frac{\int_{-\infty}^{\infty} He_r(x) P(x) dx}{r!}. \quad (15)$$

This formulation plays an important role for analyzing the convergence speed.

2.2.4 Cumulative Distribution Function. The cumulative distribution function of $P(x)$ is defined as

$$F(x) = \int_{-\infty}^x P(u) du. \quad (16)$$

The integration of the $He_r(x) e^{-\frac{x^2}{2}}$ is given as

$$\begin{aligned} \int_{-\infty}^x He_r(u) e^{-\frac{u^2}{2}} du &= - \int_{-\infty}^x \frac{dHe_{r-1}(u) e^{-\frac{u^2}{2}}}{du} du \\ &= -He_{r-1}(x) e^{-\frac{x^2}{2}}. \end{aligned} \quad (17)$$

Therefore, the Gram-Charlier A series of $F(x)$ is given as

$$F(x) = \int_{-\infty}^x \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}} du - \left(\sum_{r=3}^{\infty} c_r He_{r-1}(x) \right) \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}, \quad (18)$$

where the first term of the right side is a sort of the Gaussian error function. The Gaussian error function is known to be easily calculated numerically. A general cumulative distribution function $\tilde{F}(z)$ with non-normalized z is given as

$$\tilde{F}(z) = F\left(\frac{z - \mu_z}{\sigma_z}\right). \quad (19)$$

3 RELATED WORKS

In order to investigate the sampling reduction algorithms, it is important to estimate accurately the number of short vectors in a given search space. Here, we explain the two previous approaches: the non-parametric approach using the geometric description and the parametric one using the normal approximation.

3.1 Non-parametric Approach

The geometric description inspired by the Gaussian heuristic assumes that the number of short lattice vectors is proportional to the volume of the intersection between the search space covered by all the possible lattice vectors and a ball with a small radius R , where R corresponds to a given short length. This technique gives an accurate non-parametric estimation. However, it was generally intractable to count the actual intersection because there are quite a lot of lattice vectors in a search space. Recently, some state of the art methods were proposed for estimating the intersection in practice by dividing the lattice space into small partitions such as cylinders [10] and boxes [3] and utilizing various techniques for acceleration. Nevertheless, they are still time-consuming because their complexity depends on a large number of lattice vectors and small partitions. Even the most efficient algorithm [3] needs about two seconds to estimate the number of short lattice vectors for a single natural number representation in the search space. Moreover, it is difficult to investigate their estimation analytically because it is non-parametric and point-wise.

3.2 Parametric Approach

The normal approximation is a parametric approach under the randomness assumption and the central limit theorem [9]. It approximates the probability distribution of the squared length ℓ^2 of the lattice vectors as a normal distribution whose parameters are only the mean and the variance. The mean of ℓ^2 for a generated lattice vector is given as the first order moment of ℓ^2 :

$$E(\ell^2) = \sum_{i=1}^n E(\zeta_i^2) \|\vec{b}_i^*\|^2, \quad (20)$$

where $E()$ is the expectation operator over all the possible bases. ζ_i is the sum of $\tilde{\zeta}_i$ (a uniformly distributed random variable in $[-\frac{1}{2}, \frac{1}{2})$) and $\frac{\pm d_i}{2}$ (a half integer). Fukase and Kashiwabara calculated $E(\ell^2)$ analytically by assuming that every d_i is equal to 0 [9]. The distribution of $\tilde{\zeta}_i$ is formally given by

$$P_{\tilde{\zeta}}(x) = \begin{cases} 1 & -\frac{1}{2} \leq x < \frac{1}{2}, \\ 0 & \text{otherwise.} \end{cases} \quad (21)$$

Then, the mean $\mu = E(\ell^2)$ is given as

$$\mu = \sum_{i=1}^n \|\vec{b}_i^*\|^2 \int_{-\frac{1}{2}}^{\frac{1}{2}} x^2 dx = \frac{\sum_{i=1}^n \|\vec{b}_i^*\|^2}{12}. \quad (22)$$

Similarly, the second order moment $E(\ell^4)$ is given as

$$E(\ell^4) = \sum_{i=1}^n E(\zeta_i^4) \|\vec{b}_i^*\|^4 + \sum_{i=1}^n E(\zeta_i^2) \|\vec{b}_i^*\|^2 \sum_{j=1, j \neq i}^n E(\zeta_j^2) \|\vec{b}_j^*\|^2, \quad (23)$$

where we utilize the statistical independence between ζ_i and ζ_j ($i \neq j$) under the randomness assumption. Then, the variance $\sigma^2 = E(\ell^4) - \mu^2$ is given as

$$\sigma^2 = \sum_{i=1}^n E(\zeta_i^4) \|\vec{b}_i^*\|^4 - \frac{\sum_{i=1}^n \|\vec{b}_i^*\|^4}{144} = \frac{\sum_{i=1}^n \|\vec{b}_i^*\|^4}{180}. \quad (24)$$

μ and σ^2 determine the simple normal distribution function which can be investigated both numerically and analytically [9]. However, a serious weakness of this approximation is that the estimation is different from the actual distribution especially when the lengths of lattice vectors are short as is pointed out in [3]. In other words, the normal approximation is too rough to accurately estimate the number of short lattice vectors. In addition, it does not consider a search space including multiple lattice vectors because every d_i is set to 0.

4 METHOD

Here, we explain a new method for estimating the number of short lattice vectors in a search space by utilizing the Gram-Charlier A series.

4.1 Overview

Under the randomness assumption, the squared lengths of the lattice vectors in a search space Υ is given as a random variable z with a probability distribution. Let $P(z|\Upsilon)$ and $F(z|\Upsilon)$ be the conditional probability distribution of a squared length z given Υ and its cumulative distribution, respectively. Then, the expectation of the number of lattice vectors below a given squared length $z = \ell^2$ in Υ is given as

$$N(\ell^2) = \tilde{F}(\ell^2|\Upsilon) \# \Upsilon, \quad (25)$$

where $\# \Upsilon$ is the cardinality (the number of members) of Υ . By estimating up to the Q -th order cumulants of $P(z|\Upsilon)$, the Q -th order expansion of the Gram-Charlier A series of $\tilde{F}(z|\Upsilon)$ (denoted by $\tilde{F}_Q(z|\Upsilon)$) is determined uniquely. z is given as $\ell^2 = \sum_i \zeta_i^2 \|\vec{b}_i^*\|^2$ of Eq. (2). Now, Υ is assumed to a product-type search space $\Upsilon = \prod_i v_i$. Then, $\# \Upsilon$ is given as $\prod_i \# v_i$. In addition, in the similar way as in [4, 14, 17], each ζ_i is given as an independently and uniformly distributed random variable under the randomness assumption. The distribution of ζ_i is formally given by

$$P_{\zeta_i}(x) = \begin{cases} \frac{1}{\# v_i} & \exists p \in v_i \left(-\frac{p+1}{2} \leq x < -\frac{p}{2} \vee \frac{p}{2} \leq x < \frac{p+1}{2} \right), \\ 0 & \text{otherwise.} \end{cases} \quad (26)$$

Thus, the r -th order moment of ζ_i^2 (denoted by μ_{ir}) is given as

$$\mu_{ir} = \int_{-\infty}^{\infty} x^{2r} P_{\zeta_i}(x) dx = \frac{\sum_{p \in v_i} \alpha_{pr}}{\# v_i}, \quad (27)$$

where each α_{pr} is a constant given as

$$\alpha_{pr} = \frac{\left((p+1)^{2r+1} - p^{2r+1} \right)}{(2r+1) 2^{2r}}. \quad (28)$$

Though it is hard to give a closed form of the r -th cumulant of ζ_i^2 (denoted by κ_{ir}), each κ_{ir} is calculated recursively by Eq. (8). Note that κ_{ir} can take the rigorously accurate value by rational

number arithmetic. Using the homogeneity and the additivity of the cumulants of independent variables, the r -th order cumulants of ℓ^2 (denoted by κ_r) is given as

$$\kappa_r = \sum_{i=1}^n \kappa_{ir} \rho_i^r, \quad (29)$$

where ρ_i is given as

$$\rho_i = \left\| \vec{b}_i^* \right\|^2 = \sum_{j=1}^n \left(b_{ij}^* \right)^2. \quad (30)$$

We call $\boldsymbol{\rho} = (\rho_i)$ the shape of $\mathbf{B}^*$. Then, the coefficients of the Gram-Charlier A series (c_r) can be calculated recursively by Eqs. (12) and (13). Thus, the form of $\tilde{F}_Q(z|\Upsilon, \boldsymbol{\rho})$ is given as

$$\tilde{F}_Q(z|\Upsilon, \boldsymbol{\rho}) = \int_{-\infty}^{\frac{z-\kappa_1}{\sqrt{\kappa_2}}} \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}} du - \left(\sum_{r=3}^Q c_r \text{He}_{r-1} \left(\frac{z-\kappa_1}{\sqrt{\kappa_2}} \right) \right) \frac{e^{-\frac{\left(\frac{z-\kappa_1}{\sqrt{\kappa_2}}\right)^2}}}{\sqrt{2\pi}}. \quad (31)$$

Finally, $N(\ell^2)$ is approximately estimated by

$$N(\ell^2) \simeq \tilde{F}_Q(\ell^2|\Upsilon, \boldsymbol{\rho}) \prod_{i=1}^n \#v_i, \quad (32)$$

which is a function of ℓ^2 . The form of the function depends on only the search space Υ and the shape of the current lattice basis $\boldsymbol{\rho}$.

In this paper, we focus on only the product-type search spaces. However, any non-product-type search space can be managed by the proposed method when it is divided into several product-type search spaces. By noting that a singleton is a product-type search space, $N(\ell^2)$ can be always estimated by dividing any given search space into singletons:

$$N(\ell^2) \simeq \sum_{\vec{d} \in \Upsilon} F_Q(\ell^2|\{\vec{d}\}, \boldsymbol{\rho}). \quad (33)$$

4.2 Algorithmic Description

The algorithmic description of the above estimation process in a product-type search space is given here.

First, up-to the Q -th order cumulants κ_{ir} of each index i are calculated by Algorithm 1. Each κ_{ir} depends on only v_i . Therefore, if v_i is limited to only a few types of sets (for example, an RSR-type search space with a small T_i), they can be calculated as constants in advance. Our workstation took less than one minute to pre-calculate every κ_{ir} by rational number arithmetic when the maximum of T_i and Q were set to 10 and 200, respectively.

Second, the Q -th degree approximation of $N(z)$ (denoted by $N_Q(z)$) is given by Algorithm 2. $N_Q(z)$ can be calculated easily for any value of z because it is a parametric continuous function. The time complexity is $O(n^2 + nQ + Q^2)$, which consists of the calculations of every ρ_i ($O(n^2)$), every κ_r ($O(nQ)$), and every B_r ($O(Q^2)$). If Q is not much larger than n , the complexity is $O(n^2)$. As the complexity of the orthogonalization of $\mathbf{B}$ is higher than $O(n^2)$, the complexity of Algorithm 2 is so low that it is negligible.

Algorithm 1 Calculation of the cumulants for every index in a product-type sample space.

Require: $\Upsilon = \prod_i v_i$ (a product-type search space) and Q (the maximum degree of approximation).

```

for  $i = 1$  to  $n$  do
  for  $r = 1$  to  $Q$  do
     $\mu_{ir} \leftarrow \sum_{p \in v_i} \frac{\left( (p+1)^{2r+1} - p^{2r+1} \right)}{\#v_i(2r+1)2^{2r}}.$ 
     $\kappa_{ir} \leftarrow \mu_{ir} - \sum_{m=1}^{r-1} \binom{r-1}{m-1} \kappa_{im} \mu_{i(r-m)}.$ 
  end for
end for
return  $(\kappa_{ir}).$ 

```

Algorithm 2 Construction of a function estimating the number of lattice vectors below a given squared length.

Require: $\mathbf{B}^*$ (an orthogonalized lattice basis), (κ_{ir}) (the cumulants for every index), $\#Y$, and Q .

```

for  $i = 1$  to  $n$  do
   $\rho_i \leftarrow \sum_{j=1}^n \left( b_{ij}^* \right)^2.$ 
end for
for  $r = 1$  to  $Q$  do
   $\kappa_r \leftarrow \sum_{i=1}^n \kappa_{ir} \rho_i^r.$ 
end for
 $B_0 \leftarrow 1, B_1 \leftarrow 0, B_2 \leftarrow 0.$ 
for  $r = 3$  to  $Q$  do
   $B_r \leftarrow \sum_{i=2}^{r-1} \binom{r-1}{i} B_{r-i-1} \kappa_{i+1}.$ 
   $c_r \leftarrow \frac{B_r}{r! \sqrt{\kappa_2^r}}.$ 
end for
 $F_Q(x) \leftarrow \int_{-\infty}^x \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}} du - \left( \sum_{r=3}^Q c_r \text{He}_{r-1}(x) \right) \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}.$ 
 $N_Q(z) \leftarrow \#Y F_Q \left( \frac{z-\kappa_1}{\sqrt{\kappa_2}} \right).$ 
return  $N_Q(z).$ 

```

4.3 Theoretical Evaluation of Convergence Speed

If Υ is a finite search space, the squared length ℓ^2 has finite lower and upper bounds. Therefore, a basic property of the Gram-Charlier A series [5, 21] guarantees that $N_Q(z)$ converges to the correct function if Q tends to infinity. However, this property can give no information on the convergence speed as Q tends to infinity. Here, we theoretically evaluate the convergence speed. For this purpose, a residual function of the Gram-Charlier A series is defined as

$$R_Q(x) = \sum_{r=Q+1}^{\infty} c_r \text{He}_{r-1}(x). \quad (34)$$

It is easily shown that $N_Q(z)$ is close to the true value if and only if $R_Q(x)$ is close to 0 (x is the normalized value of z). Moreover, let $\tilde{\ell}^2$ be the normalized value of the squared length ℓ^2 defined as

$$\tilde{\ell}^2 = \frac{\ell^2 - \kappa_1}{\sqrt{\kappa_2}}. \quad (35)$$

Its probability distribution is denoted by $P_{\tilde{\ell}^2}(x)$. Then, the corresponding characteristic function is given as

$$\varphi_{\tilde{\ell}^2}(\omega) = \int_{-\infty}^{\infty} P_{\tilde{\ell}^2}(x) e^{i\omega x} dx. \quad (36)$$

Now, the following two lemma holds. See Appendix A and B for their proofs.

LEMMA 4.1. *If Q is sufficiently large and $n > 1$, the following inequality holds:*

$$|R_Q(x)| \leq \frac{e^{\frac{x^2}{4}}}{\pi} \sum_{r=Q+1}^{\infty} \frac{|\varphi_{\tilde{\ell}^2}(\sqrt{r})|}{r}. \quad (37)$$

LEMMA 4.2. *If ω is sufficiently large, the following inequality holds:*

$$|\varphi_{\tilde{\ell}^2}(\omega)| \leq \frac{K_{\tilde{\ell}^2}}{|\omega|^{\frac{n}{2}}}, \quad (38)$$

where $K_{\tilde{\ell}^2}$ is a positive value determined by Υ and ρ without depending on ω .

Consequently, the following theorem is derived directly from these two lemmas:

THEOREM 4.3. *If Q is sufficiently large and $n > 1$, an upper bound of $R_Q(x)$ is given as*

$$|R_Q(x)| \leq K e^{\frac{x^2}{4}} \sum_{r=Q+1}^{\infty} r^{-\frac{n+4}{4}}, \quad (39)$$

where $K = \frac{K_{\tilde{\ell}^2}}{\pi}$ is a positive value without depending on Q and x .

This upper bound corresponds to a subsequence of the Riemann zeta function $Z\left(\frac{n+4}{4}\right)$ defined as

$$Z(s) = \sum_{i=1}^{\infty} i^{-s}. \quad (40)$$

If $s > 1$, $Z(s)$ is known to converge to a constant. Therefore, this theorem guarantees that the residual function $|R_Q(x)|$ monotonically converges to 0 as Q is larger. Moreover, the convergence speed is equivalent to that of the Riemann zeta function $Z\left(\frac{n+4}{4}\right)$. It is also worth noting that the order of the convergence speed does not depend on x . Only the initial scale is determined by $e^{\frac{x^2}{4}}$. It shows that this method is effective even for short lattice vectors with large $|x|$.

4.4 Accumulated Errors in Practical Implementation

Though the theoretical convergence speed can be evaluated, it is also important in practice to evaluate the actual errors. Here, we focus on the accumulated rounding errors in the proposed method. Since Algorithm 1 can use rational number arithmetic, there are no errors. Though ρ_i is also a rational number for an integral lattice, its expression is so complicated that it is implemented as a real number in practice. Therefore, Algorithm 2 involves rounding errors. The recursive calculation of B_r is the most dominant part accumulating the errors in Algorithm 2. Let V_r be the variance of the error on B_r . By assuming that each V_r is independent of each other and

the cumulants have the same order of errors, V_r can be roughly evaluated by a recurrence relation given as

$$V_{r+3} = \sum_{i=3}^r V_i + r - 2, \quad (41)$$

where we utilize that $B_0 = 1$, $B_1 = 1$, and $B_2 = 1$. Using the difference between V_r and V_{r-1} , this relation can be rewritten as

$$V_{r+3} = V_{r+2} + V_r + 1. \quad (42)$$

The dominant common ratio is given as the solutions of the following characteristic equation:

$$\beta^3 - \beta^2 - 1 = 0. \quad (43)$$

Though it has one real root and two complex roots, only the real root $\beta \approx 1.47 \approx \sqrt{2}$ is larger than 1. Therefore, for a given degree of approximation Q , a rough upper bound of the standard deviation of the accumulated errors is given by

$$\sqrt{V_Q} \leq 2^{\frac{Q}{4}}. \quad (44)$$

It shows that the errors are expected to cause an overflow in the standard double-precision format if $Q > 200$. As V_Q actually depends on each other, the actual value of $\sqrt{V_Q}$ often exceeds this rough upper bound. It was observed in our experiments that the estimation of the proposed method tends to be unstable in the double-precision format if $Q > 130$. Therefore, Q was set to 120 in this paper.

5 EXPERIMENTS

Here, it is numerically verified that the proposed method can estimate the actual number of short vectors accurately for several lattice bases B and search spaces α . The following four lattice bases are used:

- **B128** was originally generated in TU Darmstadt SVP challenge [16] ($n = 128$, seed = 0) and was roughly reduced by the BKZ algorithm of the fplll package [20] with block size 20.
- **B128reduced** was reduced largely from B128 by a sampling reduction algorithm.
- **B100** was generated in the same way as B128 except for $n = 100$.
- **B150** was generated in the same way as B128 except for $n = 150$.

The following two RSR-type search spaces are used:

- $\Upsilon_{2^{25}} = \{0\}^{n-26} \times \{0, 1\}^{25} \times \{1\}$.
- $\Upsilon_{2^{17}3^5} = \{0\}^{n-23} \times \{0, 1\}^{17} \times \{0, 1, 2\}^5 \times \{1\}$.

In the similar way as in [17], the natural number allocated to the last n -th index was always set to 1 in order to avoid the all-zero solution. $\Upsilon_{2^{25}}$ and $\Upsilon_{2^{17}3^5}$ corresponds to a standard RSR search space [17] and an extended one [4, 14], respectively. The degree of approximation Q was set to 120. Algorithm 1 were carried out in advance for $v = \{0\}, \{1\}, \{0, 1\}, \{0, 1, 2\}$ within ten seconds. The calculation time of Algorithm 2 was negligible in the total time including the orthogonalization from B to B^* .

Fig. 1 shows the results for B128 and B128reduced over $\Upsilon_{2^{25}}$. The actual number of short lattice vectors is displayed by the bumpy blue (cumulative) histogram. Note that $10^0 = 1$ in vertical axis is

the minimum of the actual number. The estimated number using the Gram-Charlier A series ($Q = 120$) is displayed by the solid green curve. The normal approximation [9] is displayed by the dashed orange curve. The number of the lattice vectors in vertical axis is displayed in log scale. The value of the squared length in horizontal axis is divided by the Gaussian heuristic ℓ_{GH}^2 . In other words, 1 in horizontal axis corresponds to the estimated minimum ℓ_{GH}^2 . Fig. 2 shows the results of the bases with B128 and B128reduced over a different sampling distributions $\Upsilon_{2^{17}3^5}$. Fig. 3 shows the results for different sizes of lattice bases (B100 and B150) over $\Upsilon_{2^{25}}$.

These results verify the accuracy of the proposed method for various lattice bases and various search spaces. In all the cases, the proposed method could estimate the actual number of short lattice vectors quite accurately. Only when the squared length is very short, it was observed that there were some fluctuations. The estimated number is the expectation so that it is essentially different from the actual one if there exist only a few satisfiable lattice vectors. Nevertheless, it seems to give a good estimation. On the other hand, the estimated number was always too large in the normal approximation.

Unfortunately, it is hard to compare the proposed method experimentally with the state of art method of the non-parametric approach in [3]. It is because the method in [3] is a complicated composition of various approximation techniques and its code has not been released publicly. Nevertheless, regarding the computation time, it is verified that the proposed method is much more efficient. As shown in Section 4.2, the time complexity of the proposed method is $O(n^2 + nQ + Q^2)$. Actually, the calculation time over any product-type search space was less than a millisecond. On the other hand, the time complexity of the method in [3] has not been clarified. In addition, it has been reported in [3] that their method needs about two seconds for a singleton search space. Regarding the accuracy of the estimation of the number of short lattice vectors, it is still unclear whether the proposed method is superior or inferior to the previous non-parametric methods. It is worth noting that the proposed method estimates the expected value of the number of short lattice vectors. On the other hand, the previous non-parametric methods try to estimate the true number. Therefore, the statistical significance will need to be discussed in order to estimate the bounds on the true number by the proposed method.

6 CONCLUSION

In this paper, we proposed a new method for estimating the number of short lattice vectors in a search space. The proposed method is based on a parametric approach using the Gram-Charlier A series. It is much more efficient than the previous non-parametric approach. In addition, an upper bound of its convergence speed is given theoretically. The numerical experiments verified that the proposed method can estimate the actual number of short lattice vectors quite accurately in various situations. Table 1 shows the qualitative comparison of the proposed parametric approach with the non-parametric approach.

We are planning to utilize the proposed method for investigating and accelerating the state of the art algorithms. The weighting of the probability in the search space may be promising [15]. One of the unsolved theoretical problems is that the proposed method

(a) B128 over $\Upsilon_{2^{25}}$.

(b) B128reduced over $\Upsilon_{2^{25}}$.

Figure 1: Actual and estimated number of short lattice vectors from the bases with $n = 128$ over $\Upsilon_{2^{25}}$: The cumulative histogram of the number of lattice vectors below a given squared length is displayed by a blue (slightly bumpy) curve. The curves of the estimated number are displayed by the normal approximation (in dashed orange) and the proposed method using the Gram-Charlier A series (in solid green). B128reduced is a reduced basis generated from B128.

heavily depends on the randomness assumption. Though the randomness assumption cannot hold rigorously [3], the experimental results of this paper verified that this assumption is quite useful for estimating the number of short lattice vectors in a search space. We are planning to investigate the randomness assumption further and discover more reasonable conditions. Moreover, we are planning to find what types of lattices can be investigated by the proposed method. In addition, there are two practical problems.

Table 1: Qualitative comparison of the proposed parametric approach with a non-parametric approach.

APPROACH	proposed parametric approach	non-parametric approach
CALCULATION TIME	quite fast	slow
ASYMPTOTIC CONVERGENCE SPEED	theoretically given	empirically given
ASSUMPTION	randomness assumption	Gaussian heuristic

(a) B128 over $\Upsilon_{2^{17}3^5}$. **(a) B100 over $\Upsilon_{2^{25}}$.** **(b) B128reduced over $\Upsilon_{2^{17}3^5}$.** **(b) B150 over $\Upsilon_{2^{25}}$.****Figure 2: Actual and estimated number of short lattice vectors from the bases with $n = 128$ over $\Upsilon_{2^{17}3^5}$.**

The first one is related to the efficient method for dividing non-product-type search space into product-type search spaces. We are planning to construct efficient divisions of the search spaces of various sampling reduction algorithms. The second practical problem is related to the high-precision calculation of the coefficients of the Gram-Charlier A series. The accumulation of errors is expected to be more serious in the future various investigations. We are planning to utilize some techniques keeping precision.

Figure 3: Actual and estimated number of short lattice vectors from the bases of a small lattice ($n = 100$) and a large one ($n = 150$).

A PROOF OF LEMMA 4.1

PROOF. First, c_r is generally given by Eq. (15). As x (denoted by $\tilde{\ell}^2$) is distributed over a limited range with lower and upper bounds, Eq. (15) can be rewritten as

$$c_r = \frac{\int_{-V}^V He_r(x) P_{\tilde{\ell}^2}(x)}{r!}, \quad (45)$$

where V is a finite constant. It is easily shown that $P_{\tilde{\ell}^2}(x)$ is bounded if $N > 1$. Therefore, $P_{\tilde{\ell}^2}(x)$ is square integrable. It is also easily shown that $He_r(x)$ is bounded (and square integrable) on $[-V, V]$. Then, the following equation holds by the Plancherel theorem:

$$c_r = \frac{\int_{-\infty}^{\infty} \overline{\varphi_{\tilde{\ell}^2}(\omega)} \phi_r(\omega) d\omega}{\sqrt{2\pi r!}}, \quad (46)$$

where $\phi_r(\omega)$ is the Fourier transform of $He_r(x)$ on $[-V, V]$ given as

$$\phi_r(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-V}^V He_r(x) e^{i\omega x} dx \quad (47)$$

and $\overline{\varphi_{\tilde{\ell}^2}(\omega)}$ is the conjugate of $\varphi_{\tilde{\ell}^2}(\omega)$ is the characteristic function of $P_{\tilde{\ell}^2}(x)$.

Second, we derive the asymptotic form of $\phi_r(\omega)$ for sufficiently large r . According to 13.5.16 and 13.6.18 in [1], the asymptotic form of $He_r(x)$ is known to be given as

$$He_r(x) \simeq \frac{2^{\frac{r}{2}} \Gamma\left(\frac{r+1}{2}\right) G_r(x)}{\sqrt{\pi}}, \quad (48)$$

where $G_r(x)$ is defined as

$$G_r(x) = e^{\frac{x^2}{4}} \cos\left(x\sqrt{r} - \frac{r\pi}{2}\right) = e^{\frac{x^2}{4}} \left(\frac{(-1)^r i^r e^{ix\sqrt{r}} + i^r e^{-ix\sqrt{r}}}{2} \right). \quad (49)$$

Now, we define $g_r^{\pm}(\omega)$ as

$$g_r^{\pm}(\omega) = \int_{-V}^V e^{\frac{x^2}{4}} e^{\pm ix\sqrt{r}} e^{i\omega x} dx. \quad (50)$$

Then, the following equation holds due to a basis property of the Fourier transform:

$$\int_{-\infty}^{\infty} g_r^{\pm}(\omega) d\omega = e^{\frac{x^2}{4}} e^{\pm ix\sqrt{r}}|_{x=0} = 1 \quad (51)$$

Moreover, $e^{\frac{x^2}{4}}$ is a bounded function on $[1, e^{\frac{V^2}{4}}]$ without depending r . Then, it can be shown for any $\omega \neq \pm\sqrt{r}$ that the integral of $e^{\frac{x^2}{4}} e^{\pm ix\sqrt{r}} e^{i\omega x}$ over the limited domain $[-V, V]$ is close to 0 if r is sufficiently large. Therefore, it can be shown for sufficiently large r that the following asymptotic convergence holds:

$$g_r^{\pm}(\omega) \simeq \delta(\omega \mp \sqrt{r}), \quad (52)$$

where $\delta(\omega)$ is the Dirac delta function. Then, the asymptotic form of $\phi_r(\omega)$ is given as

$$\phi_r(\omega) \simeq \frac{2^{\frac{r}{2}} \Gamma\left(\frac{r+1}{2}\right) i^r}{\sqrt{\pi}} \left(\frac{(-1)^r \delta(\omega - \sqrt{r}) + \delta(\omega + \sqrt{r})}{2} \right). \quad (53)$$

Thus, the asymptotic form of the coefficient c_r is given as

$$c_r \simeq \frac{2^{\frac{r-1}{2}} \Gamma\left(\frac{r+1}{2}\right) i^r}{\pi \Gamma(r+1)} \left(\frac{(-1)^r \overline{\varphi_{\tilde{\ell}^2}(\sqrt{r})} + \overline{\varphi_{\tilde{\ell}^2}(-\sqrt{r})}}{2} \right). \quad (54)$$

Then, the asymptotic form of $c_r He_{r-1}(x)$ is given as

$$\begin{aligned} c_r He_{r-1}(x) &\simeq \frac{2^{r-1} \Gamma\left(\frac{r+1}{2}\right) \Gamma\left(\frac{r}{2}\right) G_{r-1}(x) i^r}{\sqrt{\pi^3} \Gamma(r+1)} \left(\frac{(-1)^r \overline{\varphi_{\tilde{\ell}^2}(\sqrt{r})} + \overline{\varphi_{\tilde{\ell}^2}(-\sqrt{r})}}{2} \right) \\ &= \frac{G_{r-1}(x) i^r}{\pi r} \left(\frac{(-1)^r \overline{\varphi_{\tilde{\ell}^2}(\sqrt{r})} + \overline{\varphi_{\tilde{\ell}^2}(-\sqrt{r})}}{2} \right), \end{aligned} \quad (55)$$

where we utilize $2^{r-1} \Gamma\left(\frac{r+1}{2}\right) \Gamma\left(\frac{r}{2}\right) = \sqrt{\pi} \Gamma(r)$. Consequently, the asymptotic form of $R_Q(x)$ is given as

$$\begin{aligned} R_Q(x) &= \sum_{r=Q+1}^{\infty} \frac{e^{\frac{x^2}{4}} \cos\left(x\sqrt{r} - \frac{(r-1)\pi}{2}\right) i^r \left((-1)^r \overline{\varphi_{\tilde{\ell}^2}(\sqrt{r})} + \overline{\varphi_{\tilde{\ell}^2}(-\sqrt{r})} \right)}{2\pi r}. \end{aligned} \quad (56)$$

By using the absolute value of each term, the following inequality is derived:

$$|R_Q(x)| \leq \frac{e^{\frac{x^2}{4}}}{\pi} \sum_{r=Q+1}^{\infty} \frac{|\varphi_{\tilde{\ell}^2}(\sqrt{r})|}{r}. \quad (57)$$

□

□

B PROOF OF LEMMA 4.2

PROOF. First, an upper bound of the characteristic function of $\eta_i = \zeta_i^2$ is derived. By transforming ζ_i into η_i in $P_{\zeta_i}(x)$, the probability distribution of η_i is given as

$$P_{\eta_i}(x) = \begin{cases} \frac{1}{\#v_i \sqrt{x}} & \exists p \in v_i \left(\frac{p^2}{4} \leq x < \frac{(p+1)^2}{4} \right), \\ 0 & \text{otherwise.} \end{cases} \quad (58)$$

Then, the characteristic function of $P_{\eta_i}(x)$ is defined as

$$\varphi_{\eta_i}(\omega) = \int_{-\infty}^{\infty} P_{\eta_i}(x) e^{i\omega x} dx = \sum_{p \in v_i} \int_{\frac{p^2}{4}}^{\frac{(p+1)^2}{4}} \frac{e^{i\omega x}}{\#v_i \sqrt{x}} dx. \quad (59)$$

By substituting $\frac{t^2}{|\omega|}$ for x , the characteristic function is given as

$$\begin{aligned} \varphi_{\eta_i}(\omega) &= \sum_{p \in v_i} \frac{4}{\#v_i \sqrt{|\omega|}} \int_{\frac{\sqrt{|\omega|} p}{2}}^{\frac{\sqrt{|\omega|} (p+1)}{2}} \left(\cos t^2 + \text{sgn}(\omega) i \sin t^2 \right) dt \\ &= \sum_{p \in v_i} \frac{4}{\#v_i \sqrt{|\omega|}} \left(C\left(\frac{\sqrt{|\omega|} (p+1)}{2}\right) - C\left(\frac{\sqrt{|\omega|} p}{2}\right) \right) \\ &\quad + \sum_{p \in v_i} \frac{4 \text{sgn}(\omega) i}{\#v_i \sqrt{|\omega|}} \left(S\left(\frac{\sqrt{|\omega|} (p+1)}{2}\right) - S\left(\frac{\sqrt{|\omega|} p}{2}\right) \right), \end{aligned} \quad (60)$$

where $\text{sgn}(\omega)$ denotes the sign of ω . $C(u)$ and $S(u)$ are the Fresnel integrals defined as

$$\begin{aligned} C(u) &= \int_0^u \cos t^2 dt, \\ S(u) &= \int_0^u \sin t^2 dt. \end{aligned} \quad (61)$$

According to Section 7.3 in [1], as u tends to infinity, $C(u)$ and $S(u)$ are known to be asymptotically given as

$$\begin{aligned} C(u) &\simeq \sqrt{\frac{\pi}{2}} \left(\frac{1}{2} + \frac{\sin(u^2)}{u\sqrt{2\pi}} \right) + O\left(\frac{1}{u^3}\right), \\ S(u) &\simeq \sqrt{\frac{\pi}{2}} \left(\frac{1}{2} - \frac{\cos(u^2)}{u\sqrt{2\pi}} \right) + O\left(\frac{1}{u^3}\right). \end{aligned} \quad (62)$$

Therefore, if $|\omega|$ is sufficiently large, $\varphi_{\eta_i}(\omega)$ is asymptotically given as

$$\varphi_{\eta_i}(\omega) \simeq \begin{cases} \frac{\sqrt{2\pi}}{\#v_i\sqrt{|\omega|}} (1 + \operatorname{sgn}(\omega) i) & 0 \in v_i, \\ O\left(\frac{1}{\#v_i|\omega|}\right) & 0 \notin v_i. \end{cases} \quad (63)$$

Then, an upper bound of $|\varphi_{\eta_i}(\omega)|$ for sufficiently large ω is given as

$$|\varphi_{\eta_i}(\omega)| \leq \frac{\sqrt{4\pi}}{\#v_i\sqrt{|\omega|}}. \quad (64)$$

Second, an upper bound of the characteristic function of $\tilde{\ell}^2$ is derived. $\tilde{\ell}^2$ is given as $(\sum_i \eta_i \rho_i - \kappa_1) / \sqrt{\kappa_2}$, where each η_i is assumed to be independent of each other. Using a basic property of the characteristic function, $\varphi_{\tilde{\ell}^2}(\omega)$ is given as

$$\varphi_{\tilde{\ell}^2}(\omega) = e^{-\frac{i\omega\kappa_1}{\sqrt{\kappa_2}}} \prod_{i=1}^n \varphi_{\eta_i}\left(\frac{\rho_i\omega}{\sqrt{\kappa_2}}\right). \quad (65)$$

Therefore, an upper bound of $|\varphi_{\tilde{\ell}^2}(\omega)|$ for sufficiently large ω is given as

$$|\varphi_{\tilde{\ell}^2}(\omega)| \leq \frac{K_{\tilde{\ell}^2}(\Upsilon, \rho)}{|\omega|^{\frac{n}{2}}}, \quad (66)$$

where $K_{\tilde{\ell}^2}(\Upsilon, \rho)$ is defined as

$$K_{\tilde{\ell}^2}(\Upsilon, \rho) = \frac{\sqrt{(4\pi\kappa_2)^n}}{\prod_{i=1}^n \rho_i \prod_{i=1}^n \#v_i}. \quad (67)$$

□

□

ACKNOWLEDGMENTS

A part of this work was supported by JST ACT-I Grant Number JPMJPR18UJ, Japan, and JSPS KAKENHI Grant Number JP18K18054, Japan.

REFERENCES

- [1] Milton Abramowitz and Irene A Stegun. 1965. *Handbook of mathematical functions with formulas, graphs, and mathematical table*. Dover New York.
- [2] Miklós Ajtai, Ravi Kumar, and 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 (STOC '01)*. ACM, New York, NY, USA, 601–610. <https://doi.org/10.1145/380752.380857>
- [3] Yoshinori Aono and Phong Q. Nguyen. 2017. Random Sampling Revisited: Lattice Enumeration with Discrete Pruning. In *EUROCRYPT (2)*. Springer, 65–102. https://doi.org/10.1007/978-3-319-56614-6_3
- [4] Johannes Buchmann and Christoph Ludwig. 2006. Practical Lattice Basis Sampling Reduction. In *Algorithmic Number Theory: 7th International Symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings*, Florian Hess, Sebastian Pauli, and Michael Pohst (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 222–237. https://doi.org/10.1007/11792086_17
- [5] Harald Cramér. 1925. On some classes of series used in mathematical statistics. In *Proceedings of the Sixth Scandinavian Congress of Mathematicians*. 399–425.
- [6] Harald Cramér. 1946. *Mathematical Methods of Statistics*. Princeton University Press.
- [7] Léo Ducas. 2018. Shortest Vector from Lattice Sieving: A Few Dimensions for Free. In *Advances in Cryptology – EUROCRYPT 2018*, Jesper Buus Nielsen and Vincent Rijmen (Eds.), Springer International Publishing, Cham, 125–145.
- [8] Ulrich Fincke and Michael Pohst. 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of computation* 44, 170 (1985), 463–471.
- [9] Masaharu Fukase and Kenji Kashiwabara. 2015. An Accelerated Algorithm for Solving SVP Based on Statistical Analysis. *JIP* 23 (2015), 67–80.
- [10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. 2010. Lattice Enumeration Using Extreme Pruning. In *Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings*, Henri Gilbert (Ed.), Springer Berlin Heidelberg, Berlin, Heidelberg, 257–278. https://doi.org/10.1007/978-3-642-13190-5_13
- [11] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. 2014. *An Introduction to Mathematical Cryptography* (2 ed.). Springer Publishing Company, Incorporated.
- [12] Ravi Kannan. 1983. Improved Algorithms for Integer Programming and Related Lattice Problems. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing (STOC '83)*. ACM, New York, NY, USA, 193–206. <https://doi.org/10.1145/800061.808749>
- [13] A. K. Lenstra, H. W. Lenstra, and L. Lovász. 1982. Factoring polynomials with rational coefficients. *Math. Ann.* 261, 4 (12 1982), 515–534. <https://doi.org/10.1007/BF01457454>
- [14] Christoph Ludwig. 2006. *Practical lattice basis sampling reduction*. Ph.D. Dissertation. Technische Universität Darmstadt.
- [15] Yoshitatsu Matsuda, Tadanori Teruya, and Kenji Kashiwabara. 2018. Estimation of the Success Probability of Random Sampling by the Gram-Charlier Approximation. *Cryptology ePrint Archive*, Report 2018/815. <https://eprint.iacr.org/2018/815>.
- [16] M Schneider and N Gama. [n. d.]. SVP challenge. Available at <https://www.latticechallenge.org/svp-challenge/>.
- [17] Claus-Peter Schnorr. 2003. Lattice Reduction by Random Sampling and Birthday Methods. In *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science, Berlin, Germany, February 27 - March 1, 2003. Proceedings (Lecture Notes in Computer Science)*, Helmut Alt and Michel Habib (Eds.), Vol. 2607. Springer, 145–156. https://doi.org/10.1007/3-540-36494-3_14
- [18] C. P. Schnorr and M. Euchner. 1994. Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. *Math. Program.* 66, 2 (Sept. 1994), 181–199. <https://doi.org/10.1007/BF01581144>
- [19] Tadanori Teruya, Kenji Kashiwabara, and Goichiro Hanaoka. 2018. Fast Lattice Basis Reduction Suitable for Massive Parallelization and Its Application to the Shortest Vector Problem. In *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25–29, 2018. Proceedings, Part I*. 437–460.
- [20] The FPLLL development team. 2016. fplll, a lattice reduction library. (2016). Available at <https://github.com/fplll/fplll>.
- [21] David L. Wallace. 1958. Asymptotic Approximations to Distributions. *Ann. Math. Statist.* 29, 3 (09 1958), 635–654. <https://doi.org/10.1214/aoms/1177706528>
- [22] Christopher S Withers and Saralees Nadarajah. 2009. Charlier and Edgeworth expansions for distributions and densities in terms of Bell polynomials. *Probability and Mathematical Statistics* 29, 2 (2009), 271–280.