Upper bounds for failure probabilities of reductions from low density subset sum problems to lattice problems on linearly independent vectors

Shoichi Kamada*

University of Tsukuba
kamada.shoichi.ft@u.tsukuba.ac.jp

August 11, 2026

Abstract

As a new lattice problem, we introduce l-Shortest Independent Vectors Problem (l-SIVP for short), where l is a positive integer no greater than the rank of a lattice. In the case where $l = 1$, l-SIVP means SVP, and in the case where l is the rank of a lattice, l-SIVP means SIVP. We estimate upper bounds on the failure probabilities of the reductions from the subset sum problems to the l-SIVPs in terms of Ehrhart theory. Especially, in the case of $l = 1$, our upper bound is tighter than the previous result given by Coster et al. We give some considerations for dominating terms of our upper bounds of failure probabilities when l is general.

1 Introduction

First, we define the subset sum problem.

Definition 1.1 (Subset sum problem)**.** *Given a tuple* $(a_1, \ldots, a_n) \in \mathbb{Z}_{>0}^n$ *and an integer* $C \in \mathbb{Z}$*, find a tuple* $(x_1, \ldots, x_n) \in \{0, 1\}^n$ *such that*

$$x_1 a_1 + \cdots + x_n a_n = C.$$

The main theme in this paper is to give and investigate upper bounds for failure probability of reductions from subset sum problems to some lattice problems. To deal with these failure probabilities, it is necessary to assume that $a_1, \ldots, a_n$ are independent random variables. In several literatures [10, 3, 9], the following condition, which we call the (n, N)-type 1, is assumed for independent random variables $a_1, \ldots, a_n$.

(n, N)**-type** 1: $a_1, \ldots, a_n$ are uniformly distributed in the set $\{1, \ldots, N\}$.

Under the condition (n, N)-type 1, the asymptotic behaviors of the failure probabilities depend on the density, denoted by $d^\circ = d^\circ(\{a_1, \ldots, a_n\})$, which is defined by

$$d^\circ := \frac{n}{\log_2 N}. \tag{1.1}$$

(The meaning of "$\circ$" will become clear later.) For example, Coster et al [3] gave an upper bound for the failure probability of a reduction from the subset sum problem to the shortest vector problem (SVP) and showed that if $d^\circ < 0.9408...$, then the failure probability goes to 0 as $n \to \infty$. Currently, it is not known

*This work was supported by JST CREST Grant Number JPMJCR2113, Japan.

whether the value 0.9408... can be replaced by another larger value or not. Moreover, it had also never been known whether one can give a tighter upper bound for the failure probability of a reduction to SVP or not. A part of our results is to give a tighter upper bound for this failure probability.

In our approach to failure probabilities of reductions from subset sum problems to some lattice problems, Ehrhart theory is a useful tool. For convenience, we use not only the $(n.N)$-type 1, but also the following (n, N)-type 2.

(n, N)-type 2: $a_1, \ldots, a_n$ are uniformly distributed in the set $\{0, 1, \ldots, N\}$.

Under the condition (n, N)-type 2, the density, denoted by $d = d(\{a_1, \ldots, a_n\})$, is defined by

$$d := \frac{n}{\log_2(N+1)}. \tag{1.2}$$

In terms of Ehrhart theory, $(n, N+1)$-type 2 will be able to be transformed to (n, N)-type 1, and vice versa. Indeed, we will consider

$$(N+1)[0,1] \cap \mathbb{Z} = \{0, 1, \ldots, N+1\} \quad \text{and} \quad (N+1)[0,1]^\circ \cap \mathbb{Z} = \{1, \ldots, N\},$$

where $(N+1)A$ is the set $\{(N+1)a \colon a \in A\}$ for a subset $A \subseteq \mathbb{R}$ and $[0,1]^\circ$ is the (relative) interior of $[0,1]$, which is equal to $(0,1)$. Taking into account the Ehrhart-Macdonald reciprocity [11, 4], it will be natural to consider both the (n, N)-type 1 and the (n, N)-type 2.

Contribution We introduce a new lattice problem, the l-shortest independent vectors problem (l-SIVP), where l is a positive integer no greater than the rank of a lattice. Note that in the case where $l = 1$, l-SIVP means the shortest vector problem (SVP), and in the case where l is the rank of a lattice, l-SIVP means the shortest independent vectors problem (SIVP). First, we review and confirm that if the density defined in (1.1) or (1.2) is less than 0.9408..., then in both cases of (n, N)-type 1 and (n, N)-type 2, the failure probabilities of reductions from the subset sum problems to SVPs goes to 0 as $n \to \infty$. Next, we establish the upper bounds for the two types of failure probabilities in terms of Ehrhart theory. Finally, we investigate how effect the leading coefficients of Ehrhart quasipolynomials appeared in upper bounds for failure probabilities give.

Significance of our work Our work is motivated in the context of knapsack cryptography. So, our work will provide information for creating secure cryptographic protocols based on the hardness of the subset sum problem. On the other hand, recently, ChatGPT generated a puzzle, called sumplete [13]. In [8], the NP-completeness of the sumplete was shown and a physical zero-knowledge proof protocol based on the sumplete was proposed. Note that any instance of the sumplete consists of several instances of the subset sum problem. Hence, the security of cryptographic protocols based on the hardness of the sumplete depends also on the hardness of the subset sum problem. So, Our work is important to know some practical hardness of the sumplete for cryptographic protocols.

Organization In Section 2, we give terminologies and facts in lattice theory and Ehrhart theory. In Section 3, we review the failure probabilities of reductions from the subset sum problems to SVPs. In Section 4, we estimate upper bounds for the failure probabilities of reductions from the subset sum problems to l-SIVPs in terms of Ehrhart theory, and we give parts of dominant terms of the obtained upper bounds.

2 Preliminaries

A lattice Λ is a discrete subgroup of $\mathbb{R}^n$. A basis of a lattice Λ is a set of linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \Lambda$ over $\mathbb{Z}$ such that $\Lambda = \{\alpha_1 \boldsymbol{v}_1 + \cdots + \alpha_m \boldsymbol{v}_m \colon \alpha_i \in \mathbb{Z}\}$. The rank of a lattice Λ is the cardinality of a basis of Λ, denoted by $\mathrm{rank}(\Lambda)$. An element in a lattice is called a lattice point or a lattice vector. When we deal with lattice problems introduced in Subsection 2.1, we suppose that lattice points have real coordinates. When we deal with Ehrhart theory introduced in Subsection 2.2, we suppose that lattice points have integer coordinates.

2.1 Lattice problems

Let $\|\cdot\|_2$ denote the ℓ_2-norm and let $B_n(\boldsymbol{v}, r)$ denote the n-dimensional open ℓ_2-ball centered at $\boldsymbol{v} \in \mathbb{R}^n$ with radius r, i.e.,

$$B_n(\boldsymbol{v}, r) := \{\boldsymbol{y} \in \mathbb{R}^n \colon \|\boldsymbol{y} - \boldsymbol{v}\|_2 < r\}.$$

For a subset $S \subseteq \mathbb{R}^n$, let $\mathrm{span}(S)$ denote the linear hull of S, i.e.,

$$\mathrm{span}(S) := \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{v}_i \colon m \in \mathbb{Z}_{>0},\, \alpha_i \in \mathbb{R},\, \boldsymbol{v}_i \in S \right\}$$

For a lattice $\Lambda \subseteq \mathbb{R}^n$, let $\lambda_i(\Lambda)$ denote the i-th successive minimum of Λ, i.e.,

$$\lambda_i(\Lambda) := \inf\{r \colon \dim(\mathrm{span}(\Lambda \cap B_n(\boldsymbol{0}, r))) \geq i\}.$$

Then we define the γ-approximate Shortest Vector Problem SVP_γ.

Definition 2.1 (SVP_γ)**.** *Given a basis of a lattice Λ, find a nonzero vector $\boldsymbol{v} \in \Lambda \setminus \{\boldsymbol{0}\}$ such that $\|\boldsymbol{v}\|_2 \leq \gamma\lambda_1(\Lambda)$.*

Here, we introduce a new lattice problem l-SIVP_γ, which is short for the γ-approximate l-Shortest Independent Vectors Problem.

Definition 2.2 (l-SIVP_γ)**.** *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and let l be an integer with $1 \leq l \leq \mathrm{rank}(\Lambda)$. Then given a basis of a lattice Λ, find l linearly independent lattice vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l \in \Lambda$ which satisfy $0 < \|\boldsymbol{v}_i\|_2 \leq \gamma\lambda_l(\Lambda)$.*

Note that 1-SIVP_γ means SVP_γ and $\mathrm{rank}(\Lambda)$-SIVP_γ means SIVP_γ, which is short for the γ-approximate shortest independent vectors problem. In what follows, we abbreviate SVP_γ and l-SIVP_γ as SVP and l-SIVP, respectively.

2.2 Ehrhart theory

Here, we introduce the Ehrhart theory. The terminology and facts used in this section follow [7, 1]. For a subset $S \subseteq \mathbb{R}^n$, let $\mathrm{conv}(S)$ denote the convex hull of S, i.e.,

$$\mathrm{conv}(S) := \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{v}_i \colon m \in \mathbb{Z}_{>0},\, \alpha_i \in \mathbb{R}_{\geq 0},\, \sum_{i=1}^{m} \alpha_i = 1,\, \boldsymbol{v}_i \in S \right\}$$

For a subset $S \subseteq \mathbb{R}^n$, let $\mathrm{aff}(S)$ denote the affine hull of S, i.e.,

$$\mathrm{aff}(S) := \left\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{v}_i \colon m \in \mathbb{Z}_{>0},\, \alpha_i \in \mathbb{R},\, \sum_{i=1}^{m} \alpha_i = 1,\, \boldsymbol{v}_i \in S \right\}$$

For a subset $P \subseteq \mathbb{R}^n$ and a positive integer N, let NP denote the set

$$\{(N\xi_1, \ldots, N\xi_n) \colon (\xi_1, \ldots, \xi_n) \in P\}.$$

We say that a subset $P \subseteq \mathbb{R}^n$ is a polytope if it is a convex hull of finitely many points in $\mathbb{R}^n$, i.e. $P = \mathrm{conv}(\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m'}\})$ for $m' \in \mathbb{Z}_{>0}$ and $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m'} \in \mathbb{R}^n$. A (real) hyperplane $H \subseteq \mathbb{R}^n$ is the set $\{(\xi_1, \ldots, \xi_n) \in \mathbb{R}^n \colon w_1\xi_1 + \cdots + w_n\xi_n = \eta\}$ for $w_1, \ldots, w_n, \eta \in \mathbb{R}$. We say that $H = \{(\xi_1, \ldots, \xi_n) \in \mathbb{R}^n \colon w_1\xi_1 + \cdots + w_n\xi_n = \eta\}$ is a supporting hyperplane of a polytope P if we have

$$P \subseteq \{(\xi_1, \ldots, \xi_n) \in \mathbb{R}^n \colon w_1\xi_1 + \cdots + w_n\xi_n \leq \eta\}$$

or

$$P \subseteq \{(\xi_1, \dots, \xi_n) \in \mathbb{R}^n \colon w_1\xi_1 + \cdots + w_n\xi_n \geq \eta\}.$$

A face of a polytope $P \subseteq \mathbb{R}^n$ is a set of the form $P \cap H$ for some supporting hyperplane $H \subseteq \mathbb{R}^n$. In particular, a 0-dimensional face is called a vertex. Note that a polytope P itself is a face. We say that a polytope $P \subseteq \mathbb{R}^n$ is integral if all vertices are in $\mathbb{Z}^n$, and a polytope P is rational if all vertices are in $\mathbb{Q}^n$. Clearly, if a polytope P is integral, then P is rational. For a subset $P \subseteq \mathbb{R}^n$, the relative interior of P, denoted by P° is the set

$$\{\boldsymbol{v} \in P \colon \text{there exists } \varepsilon > 0 \text{ such that } B_n(\boldsymbol{v}, \varepsilon) \cap \mathrm{aff}(P) \subseteq P\}.$$

For a rational polytope $P \subseteq \mathbb{R}^n$ and a positive integer N, we define

$$\mathrm{ehr}(P, N) := |NP \cap \mathbb{Z}^n| \quad \text{and} \quad \mathrm{ehr}(P^\circ, N) := |NP^\circ \cap \mathbb{Z}^n|.$$

In [5], Ehrhart proved the following theorem.

Theorem 2.3 (Ehrhart's theorem [5])**.** *Let $P \subseteq \mathbb{R}^n$ be an m-dimensional polytope. If P is rational, then* $\mathrm{ehr}(P, N)$ *is a quasipolynomial in N of degree m, i.e.,* $\mathrm{ehr}(P, N)$ *is of the form $\sum_{i=0}^{m} e_i(P, N)N^i$ where $c_i(P, N)$ is a periodic function on N. If P is integral, then* $\mathrm{ehr}(P, N)$ *is a polynomial in N of degree m.*

With Theorem 2.3, we say that $\mathrm{ehr}(P, N)$ is the Ehrhart quasipolynomial if P is rational, and it is the Ehrhart polynomial if P is integral.

For an m-dimensional rational polytope P and a positive integer N, we write an Ehrhart quasipolynomial as

$$\mathrm{ehr}(P, N) = \sum_{i=0}^{m} e_i(P, N)N^i.$$

The following theorem clarifies the relationship between $\mathrm{ehr}(P, N)$ and $\mathrm{ehr}(P^\circ, N)$.

Theorem 2.4 (Ehrhart-Macdonald reciprocity [11, 4])**.** *For an m-dimensional rational polytope $P \subseteq \mathbb{R}^n$ and a positive integer N, it holds that*

$$\mathrm{ehr}(P, -N) = (-1)^m \mathrm{ehr}(P^\circ, N).$$

In [12], McMullen introduced the i-index of a rational polytope P. The i-index $\mathrm{ind}_i(P)$ is defined as the smallest positive integer s such that for each i-dimensional face F in P, $\mathrm{aff}(sF)$ contains points in $\mathbb{Z}^n$. The following theorem [12, Theorem 4] due to McMullen is useful to determine whether the coefficients of an Ehrhart quasipolynomial are constant or not.

Theorem 2.5 (McMullen's theorem)**.** *For an m-dimensional rational polytope P, let*

$$\mathrm{ehr}(P, N) = \sum_{i=0}^{m} e_i(P, N)N^i$$

be the Ehrhart quasipolynomial of P. Then the i-index $\mathrm{ind}_i(P)$ *is the period of $e_i(P, N)$ as a function of N.*

For a unimodular matrix $\boldsymbol{U} \in \mathbb{Z}^{n \times n}$ and a vector $\boldsymbol{v} \in \mathbb{Z}^n$, a unimodular transformation is defined as a transformation $\mathbb{R}^n \to \mathbb{R}^n$; $\boldsymbol{\xi} \mapsto \boldsymbol{\xi}\boldsymbol{U} + \boldsymbol{v}$. We say that a polytope $P \subseteq \mathbb{R}^n$ is unimodularly equivalent to a polytope $Q \subseteq \mathbb{R}^n$ if there exists a unimodular transformation $\psi \colon \mathbb{R}^n \to \mathbb{R}^n$ such that $P = \psi(Q)$.

Proposition 2.6. *Let $P \subset \mathbb{R}^n$ be an m-dimensional rational polytope, Assume that the set* $\mathrm{aff}(P)$ *has points in $\mathbb{Z}^n$. Then P is unimodularly equivalent to some rational polytope $Q \subseteq \mathbb{R}^m \times \{\boldsymbol{0}\} \subseteq \mathbb{R}^n$.*

Proof. Assume that $\boldsymbol{u}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_m \in \mathrm{aff}(P) \cap \mathbb{Z}^n$ are affine independent over $\mathbb{R}$ and they satisfies

$$\mathrm{aff}(P) = \boldsymbol{u} + \mathrm{span}(\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}).$$

Moreover, assume that $\boldsymbol{u} \in P \cap \mathbb{Z}^n$. Here, we determine $\boldsymbol{U}$ and $\boldsymbol{v}$ in the unimodular transformation $\boldsymbol{\xi} \mapsto \boldsymbol{\xi}\boldsymbol{U} + \boldsymbol{v}$. We write any vector $\boldsymbol{\eta} \in P$ as $\boldsymbol{\xi}\boldsymbol{U} + \boldsymbol{v}$ for some $\boldsymbol{\xi}$. Then we have $\boldsymbol{\xi} = (\boldsymbol{\eta} - \boldsymbol{v})\boldsymbol{U}^{-1}$. On the other hand, $\boldsymbol{\eta}$ can be written as $\boldsymbol{u} + \sum_{i=1}^{m} \alpha_i \boldsymbol{u}_i$ for some $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$.

As one of choices, we choose $\boldsymbol{v} := \boldsymbol{u}$. Here, we construct a unimodular matrix $\boldsymbol{U}' = \boldsymbol{U}^{-1}$. We may perform a row reduction for a matrix $({}^t\boldsymbol{u}_1, \ldots, {}^t\boldsymbol{u}_m | \boldsymbol{I}_n)$, where $\boldsymbol{I}_n$ is the identity matrix of size n. After a row reduction, we have a matrix $(\boldsymbol{E}|{}^t\boldsymbol{U}')$, where $\boldsymbol{E}$ is a row echelon form whose last $n - m$ rows are zero. Hence, the proof of the proposition is complete. □

Proposition 2.7. *For unimodularly equivalent rational polytopes $P, Q \subseteq \mathbb{R}^n$, the Ehrhart quasipolynomial of P and that of Q are the same.*

For an m-dimensional polytope $P \subseteq \mathbb{R}^n$ that is integral or rational with $\mathrm{ind}_m(P) = 1$, a relative volume $\mathrm{relvol}(P)$ is defined as a quantity

$$\frac{\mathrm{vol}_m(P)}{\det(\mathrm{aff}(P) \cap \mathbb{Z}^n)},$$

where $\mathrm{vol}_m(P)$ is the m-dimensional volume of P, and $\det(\mathrm{aff}(P) \cap \mathbb{Z}^n)$ is the determinant of the lattice $\mathrm{aff}(P) \cap \mathbb{Z}^n$, which is defined as the m-dimensional volume of a fundamental parallelotope of $\mathrm{aff}(P) \cap \mathbb{Z}^n$.

Proposition 2.8 ([1, 12])**.** *Let $P \subseteq \mathbb{R}^n$ be an m-dimensional polytope that is integral or rational with $\mathrm{ind}_m(P) = 1$. Then the leading coefficient of the Ehrhart (quasi)polynomial is a constant that is equal to $\mathrm{relvol}(P)$.*

3 Failure probabilities of reductions to SVPs

Assume that a solution $\boldsymbol{x} := (x_1, \ldots, x_n) \in \{0, 1\}^n$ to the subset sum problem is fixed for every n, and $a_1, \ldots, a_n$ are independent random variables that satisfy the (n, N)-type 1 or the (n, N)-type 2.

For a tuple $\boldsymbol{a} := (a_1, \ldots, a_n)$ and $C_{\boldsymbol{a}} := x_1 a_1 + \cdots + x_n a_n$, let $L(\boldsymbol{a}, C_{\boldsymbol{a}})$ denote a lattice spanned by rows of the matrix

$$\boldsymbol{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 & na_1 \\ 0 & 1 & \cdots & 0 & na_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & na_n \\ \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & nC_{\boldsymbol{a}} \end{pmatrix}.$$

We define a vector $\hat{\boldsymbol{x}}$ as $(x_1 - 1/2, \ldots, x_n - 1/2, 0)$. It is clear that $\hat{\boldsymbol{x}} \in L(\boldsymbol{a}, C_{\boldsymbol{a}})$.

In [3], it was considered that

$$\left| \sum_{i=1}^{n} (1 - 2x_i) a_i \right| \geq \frac{1}{2} \max_i a_i, \tag{3.1}$$

and it was shown that any instance of the subset sum problem is reducible to (3.1).

We consider the existence of a vector $\hat{\boldsymbol{y}}$ that satisfies

$$\begin{cases} \hat{\boldsymbol{y}} \in L(\boldsymbol{a}, C_{\boldsymbol{a}}), \\ \|\hat{\boldsymbol{y}}\|_2^2 \leq \|\hat{\boldsymbol{x}}\|_2^2 = \dfrac{n}{4}, \\ \hat{\boldsymbol{y}} \notin \{\boldsymbol{0}, \hat{\boldsymbol{x}}, -\hat{\boldsymbol{x}}\}. \end{cases} \tag{3.2}$$

Two types of failure probabilities of reductions from subset sum problems to SVPs are defined as follows.

$$p_1^\circ(n,N) := \Pr(\text{For an } (n,N)\text{-type 1 tuple } \boldsymbol{a},\ \exists \hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l \text{ that satisfy (3.2) and } \boldsymbol{a} \text{ satisfies (3.1)}),$$
$$p_1(n,N) := \Pr(\text{For an } (n,N)\text{-type 2 tuple } \boldsymbol{a},\ \exists \hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l \text{ that satisfy (3.2) and } \boldsymbol{a} \text{ satisfies (3.1)}),$$

where the probability spaces for the probabilities $p_l^\circ(n,N)$ and $p_l(n,N)$ are with respect to $\boldsymbol{a}$.

For positive integers n and k, we define a number $M(n,k)$ as

$$|\{\boldsymbol{y} \in \mathbb{Z}^n \colon \|\boldsymbol{y}\|_2^2 \le k\}|.$$

Proposition 3.1 (Coster et al. [3]). *It holds that*

$$p_1^\circ(n,N) \le (4n\sqrt{n}+1)M\left(n,\frac{n}{4}\right)\frac{1}{N}.$$

In [3], Coster et al. gave the following upper bound for $M(n,n/4)$.

$$M\left(n,\frac{n}{4}\right) \le 2^{\frac{n}{0.9408\dots}}.$$

From this, the following theorem was obtained in [3].

Theorem 3.2 (Coster et al., 1992 [3]). *If $d^\circ < 0.9408...$, then $p_1^\circ(n,N) \to 0$ as $n \to \infty$.*

From the point of view of computational theory or cryptography, Theorem 3.2 can be rewritten as follows.

Theorem 3.2′ (Coster et al., 1992 [3]). *If $d^\circ < 0.9408...$, then a random instance of the subset sum problem with respect to (n,N)-type 1 can be solved almost always in polynomial time with a single call to the SVP oracle.*

When the densities d° in the above theorems are replaced by d, the same claims hold, i.e., the following theorems hold.

Theorem 3.3. *If $d < 0.9408...$, then $p_1(n,N) \to 0$ as $n \to \infty$.*

Theorem 3.3′. *If $d < 0.9408...$, then a random instance of the subset sum problem with respect to (n,N)-type 2 can be solved almost always in polynomial time with a single call to the SVP oracle.*

4 Failure probabilities of reductions to l-SIVP

We consider the existence of vectors $\hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l$ that satisfy

$$\begin{cases} \hat{\boldsymbol{y}}_i \in L(\boldsymbol{a}, C_{\boldsymbol{a}}), \\ \|\hat{\boldsymbol{y}}_i\|_2^2 \le \|\hat{\boldsymbol{x}}\|_2^2 = \dfrac{n}{4}, \\ \hat{\boldsymbol{y}}_i \notin \{\boldsymbol{0}, \hat{\boldsymbol{x}}, -\hat{\boldsymbol{x}}\}, \\ \hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l \text{ are linearly independent over } \mathbb{Q}. \end{cases} \tag{4.1}$$

Two types of failure probabilities of reductions from subset sum problems to l-SIVPs are defined as follows.

$$p_l^\circ(n,N) := \Pr(\text{For an } (n,N)\text{-type 1 tuple } \boldsymbol{a},\ \exists \hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l \text{ that satisfy (4.1) and } \boldsymbol{a} \text{ satisfies (3.1)}),$$
$$p_l(n,N) := \Pr(\text{For an } (n,N)\text{-type 2 tuple } \boldsymbol{a},\ \exists \hat{\boldsymbol{y}}_1,\dots,\hat{\boldsymbol{y}}_l \text{ that satisfy (4.1) and } \boldsymbol{a} \text{ satisfies (3.1)}),$$

where the probability spaces for the probabilities $p_l^\circ(n,N)$ and $p_l(n,N)$ are with respect to $\boldsymbol{a}$.

Since we describe upper bounds for the failure probabilities in terms of Ehrhart theory, we define a kind of polytope. For a matrix $\boldsymbol{W} \in \mathbb{Z}^{l\times n}$, let $H_{\boldsymbol{W}}$ denote the set defined by

$$H_{\boldsymbol{W}} := \{\boldsymbol{\xi} \in \mathbb{R}^n \colon \boldsymbol{\xi}\, {}^t\boldsymbol{W} = \boldsymbol{0}\}.$$

Let $Q_n = [0,1]^n$. Then we define a polytope $P_{\boldsymbol{W}} \subseteq \mathbb{R}^n$ as

$$H_{\boldsymbol{W}} \cap Q_n.$$

Note that the dimension of $P_{\boldsymbol{W}}$ is less than n when a matrix $\boldsymbol{W}$ is not zero.

For a vector $\hat{\boldsymbol{c}}_i = (c_{i,1}, \dots, c_{i,n}, c_{i,n+1}) \in \mathbb{Z}^{n+1}$, we define

$$\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i} := \hat{\boldsymbol{c}}_i \boldsymbol{B} \in L(\boldsymbol{a}, C_{\boldsymbol{a}}), \tag{4.2}$$

$$\boldsymbol{w}_{\hat{\boldsymbol{c}}_i} := (c_{i,1} + c_{i,n+1}x_1, \dots, c_{i,n} + c_{i,n+1}x_n) \in \mathbb{Z}^n. \tag{4.3}$$

If $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l}$ satisfies (4.1), then we have

$$\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i} = \left(c_{i,1} + \frac{c_{i,n+1}}{2}, \cdots, c_{i,n} + \frac{c_{i,n+1}}{2}, 0\right), \tag{4.4}$$

$$\sum_{j=1}^{n} c_{i,j}a_j + c_{i,n+1}C_{\boldsymbol{a}} = \sum_{j=1}^{n}(c_{i,j} + c_{i,n+1}x_j)a_j = 0. \tag{4.5}$$

The last component in $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i}$ follows from the first condition of (4.1). For a matrix $\hat{\boldsymbol{C}} = {}^t({}^t\hat{\boldsymbol{c}}_1, \dots, {}^t\hat{\boldsymbol{c}}_l) = (c_{i,j}) \in \mathbb{Z}^{l\times(n+1)}$, let $\boldsymbol{W}_{\hat{\boldsymbol{C}}}$ denote a matrix ${}^t({}^t\boldsymbol{w}_{\hat{\boldsymbol{c}}_1}, \dots, {}^t\boldsymbol{w}_{\hat{\boldsymbol{c}}_l})$. For a matrix $\boldsymbol{W}_{\hat{\boldsymbol{C}}}$, we write (4.5) in the following form.

$$\boldsymbol{a}\, {}^t\boldsymbol{W}_{\hat{\boldsymbol{C}}} = \boldsymbol{0}. \tag{4.6}$$

As a similar condition to (4.1), we consider the following condition for $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l}$ ($\hat{\boldsymbol{c}}_i \in \mathbb{Z}^{n+1}$).

$$\begin{cases} \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i} = \left(c_{i,1} + \frac{c_{i,n+1}}{2}, \dots, c_{i,n} + \frac{c_{i,n+1}}{2}, 0\right), \\ \|\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i}\|_2^2 \le \|\hat{\boldsymbol{x}}\|_2^2 = \dfrac{n}{4}, \\ \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_i} \notin \{\boldsymbol{0}, \hat{\boldsymbol{x}}, -\hat{\boldsymbol{x}}\}, \\ \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l} \text{ are linearly independent over } \mathbb{Q}. \end{cases} \tag{4.7}$$

Note that a tuple $\boldsymbol{a} = (a_1, \dots, a_n)$ of independent random variables does not appear in (4.7). This is a significant difference from (4.1).

Under (3.1), we have

$$|c_{i,n+1}| \le 2n\sqrt{n}. \tag{4.8}$$

(See [3].)

Now we state our main theorem.

Theorem 4.1. *We have*

$$p_l^{\circ}(n,N) \le \frac{1}{N^n}\sum_{\hat{\boldsymbol{C}}} \mathrm{ehr}(P^{\circ}_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N+1) \quad \textit{and} \quad p_l(n,N) \le \frac{1}{(N+1)^n}\sum_{\hat{\boldsymbol{C}}} \mathrm{ehr}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N),$$

where the summations take over all matrices $\hat{\boldsymbol{C}} = {}^t({}^t\hat{\boldsymbol{c}}_1, \dots, {}^t\hat{\boldsymbol{c}}_l) = (c_{i,j}) \in \mathbb{Z}^{l\times(n+1)}$ *such that* $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l}$ *satisfies* (4.7) *and* $|c_{i,n+1}| \le 2n\sqrt{n}$.

By the way, the number of terms in each sum in Theorem 4.1 is at most $(1 + 4n\sqrt{n})^l M\left(n, \frac{n}{4}\right)^l$.

Proof of Theorem 4.1. Clearly, (4.1) for $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l}$ implies (4.6) and (4.7), and (3.1) implies (4.8). So, we have the following upper bound for $p_l^\circ(n, N)$.

$$\begin{aligned} p_l^\circ(n,N) &\le \Pr\left(\bigcup_{\hat{\boldsymbol{C}}} \{\boldsymbol{a} \text{ of } (n,N)\text{-type 1 satisfies } \boldsymbol{a}\,{}^t\boldsymbol{W}_{\hat{C}} = \boldsymbol{0}\}\right) \\ &\le \sum_{\hat{\boldsymbol{C}}} \Pr\left(\boldsymbol{a} \text{ of } (n,N)\text{-type 1 satisfies } \boldsymbol{a}\,{}^t\boldsymbol{W}_{\hat{C}} = \boldsymbol{0}\right), \end{aligned} \tag{4.9}$$

where the union and the summation take over all matrices $\hat{\boldsymbol{C}} = {}^t({}^t\hat{\boldsymbol{c}}_1, \dots, {}^t\hat{\boldsymbol{c}}_l) = (c_{i,j}) \in \mathbb{Z}^{l\times(n+1)}$ such that $\hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_1}, \dots, \hat{\boldsymbol{y}}_{\hat{\boldsymbol{c}}_l}$ satisfies (4.7) and $|c_{i,n+1}| \le 2n\sqrt{n}$. Similarly we have for $p_l(n, N)$.

$$p_l(n,N) \le \sum_{\hat{\boldsymbol{C}}} \Pr(\boldsymbol{a} \text{ of } (n,N)\text{-type 2 satisfies } \boldsymbol{a}\,{}^t\boldsymbol{W}_{\hat{C}} = \boldsymbol{0}). \tag{4.10}$$

Each term in (4.9) can be written as

$$\frac{|\{\boldsymbol{a} \in \{1,\dots,N\}^n \colon \boldsymbol{a}\,{}^t\boldsymbol{W}_{\hat{\boldsymbol{C}}} = \boldsymbol{0}\}|}{N^n} = \frac{|(N+1)P^\circ_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}} \cap \mathbb{Z}^n|}{N^n}.$$

The numerator in the last expression is $\mathrm{ehr}(P^\circ_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N+1)$. On the other hand, each term in (4.10) can be written as

$$\frac{|\{\boldsymbol{a} \in \{0,1,\dots,N\}^n \colon \boldsymbol{a}\,{}^t\boldsymbol{W}_{\hat{\boldsymbol{C}}} = \boldsymbol{0}\}|}{(N+1)^n} = \frac{|NP_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}} \cap \mathbb{Z}^n|}{(N+1)^n},$$

The numerator in the last expression is $\mathrm{ehr}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N)$. Therefore, we complete the proof. □

We give another form of Theorem 4.1 in Theorem 4.1′. For a matrix $\boldsymbol{W} \in \mathbb{R}^{l'\times n'}$ with $\operatorname{rank}\boldsymbol{W} = l'$, we define a function $f_{\boldsymbol{W}} \colon \mathbb{R}^{l'} \to \mathbb{R}$ as

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) := \mathrm{vol}_{n'-l'}\left((H_{\boldsymbol{W}} + \boldsymbol{\eta}\boldsymbol{W}) \cap Q_{n'}\right), \tag{4.11}$$

where $\mathrm{vol}_{n'-l'}$ is the $(n'-l')$-dimensional volume in $\mathbb{R}^{n'}$. Rigorously speaking, the measure $\mathrm{vol}_{n'-l'}$ in (4.11) is written as the Hausdorff measure $\mathcal{H}^{n'-l'}$, i.e.,

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \mathcal{H}^{n'-l'}\left((H_{\boldsymbol{W}} + \boldsymbol{\eta}\boldsymbol{W}) \cap Q_{n'}\right), \tag{4.12}$$

where for any positive integer n'', $\mathcal{H}^{n''}$ is the Hausdorff measure in $\mathbb{R}^{n'}$ scaled so that $\mathcal{H}^{n'} = \mathcal{L}^{n'}$ in $\mathbb{R}^{n'}$ for the n'-dimensional Lebesgue measure $\mathcal{L}^{n'}$. Note that $f_{\boldsymbol{W}}(\boldsymbol{0}) = \mathrm{vol}_{n'-l'}(P_{\boldsymbol{W}}) = \mathcal{H}^{n'-l'}(P_{\boldsymbol{W}})$ and the dimension of $(H_{\boldsymbol{W}} + \boldsymbol{\eta}\boldsymbol{W}) \cap Q_{n'}$, which depends on $\boldsymbol{\eta}$, is not necessarily equal to $n'-l'$ (the case where $\boldsymbol{\eta} = \boldsymbol{0}$ is not exceptional). For a matrix $\boldsymbol{W} \in \mathbb{R}^{l'\times n'}$ with $\operatorname{rank}(\boldsymbol{W}) = l'$, we define a linear mapping $\varphi_{\boldsymbol{W}} \colon \mathbb{R}^{n'} \to \mathbb{R}^{l'}$ as $\varphi_{\boldsymbol{W}}(\boldsymbol{\xi}) := \boldsymbol{\xi}\,{}^t\boldsymbol{W}$. Let $X_1, \dots, X_{n'}$ denote independent random variables, each uniformly distributed in $[0, 1]$, and let $\rho_{\boldsymbol{W}}(\boldsymbol{\eta})$ denote the probability density function of $\varphi_{\boldsymbol{W}}(X_1, \dots, X_{n'})$.

The following lemma clarifies the relationship between $f_{\boldsymbol{W}}(\boldsymbol{\eta})$ and $\rho_{\boldsymbol{W}}(\boldsymbol{\eta})$.

Lemma 4.2. *For a matrix $\boldsymbol{W} \in \mathbb{R}^{l'\times n'}$ with $\operatorname{rank}(\boldsymbol{W}) = l'$, we have*

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \sqrt{\det(\boldsymbol{W}\,{}^t\boldsymbol{W})}\rho_{\boldsymbol{W}}(\boldsymbol{\eta}\boldsymbol{W}\,{}^t\boldsymbol{W}).$$

The following lemma [6, Theorem 3.11], called the coarea formula, is useful to prove Lemma 4.2.

Lemma 4.3 (Coarea formula [6]). *For positive integers n' and l' with $n' \geq l'$, let $\varphi\colon \mathbb{R}^{n'} \to \mathbb{R}^{l'}; \boldsymbol{\xi} = (\xi_1, \ldots, \xi_{n'}) \mapsto (\varphi_1(\boldsymbol{\xi}), \ldots, \varphi_{l'}(\boldsymbol{\xi}))$ be a Lipschitz continuous mapping. Then for $\mathcal{L}^n$-integrable function $\psi\colon \mathbb{R}^{n'} \to \mathbb{R}$, it holds that*

$$\int_{\mathbb{R}^{n'}} \psi(\boldsymbol{\xi}) J(f)(\boldsymbol{\xi}) d\boldsymbol{\xi} = \int_{\mathbb{R}^{l'}} \left(\int_{\varphi^{-1}(\boldsymbol{\eta})} \psi(\boldsymbol{\xi}) d\mathcal{H}^{n'-l'}(\boldsymbol{\xi}) \right) d\boldsymbol{\eta},$$

where $J(f)$ is the Jacobian of f, i.e., $J(f)$ is defined as the square root of the absolute value of the determinant of the gram matrix of the matrix $\left(\frac{\partial \varphi_i(\boldsymbol{\xi})}{\partial x i_j} \right)$.

Proof of Lemma 4.2. Let $f_{\boldsymbol{W}}(\boldsymbol{\eta})$ be given in (4.12). Using a mapping $\varphi_{\boldsymbol{W}}$, we can write

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \mathcal{H}^{n'-l'} \left(\varphi_{\boldsymbol{W}}^{-1}(\boldsymbol{\eta} \boldsymbol{W}^{\,t}\boldsymbol{W}) \cap Q_{n'} \right).$$

Put $\boldsymbol{\eta}' = (\eta'_1, \ldots, \eta'_{l'})$ and

$$I = \frac{1}{\Delta\eta_1 \cdots \Delta\eta_{l'}} \int_{\eta_1}^{\eta_1 + \Delta\eta_1} \cdots \int_{\eta_{l'}}^{\eta_{l'} + \Delta\eta_{l'}} f_{\boldsymbol{W}}(\boldsymbol{\eta}') d\eta'_1 \cdots d\eta'_{l'}.$$

Clearly, we have

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \lim_{\Delta\eta_1 \to 0} \cdots \lim_{\Delta\eta_l \to 0} I.$$

Changing a variable $\boldsymbol{\eta}'$ to $\boldsymbol{\eta}''$ with $\boldsymbol{\eta}'' = \boldsymbol{\eta}' \boldsymbol{W}^{\,t}\boldsymbol{W}$, we have

$$I = \frac{1}{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})} \frac{1}{\Delta\eta_1 \cdots \Delta\eta_l} \int_{D_{\boldsymbol{\eta}''}} \mathcal{H}^{n-l} \left(\varphi_{\boldsymbol{W}}^{-1}(\boldsymbol{\eta}'') \cap Q_{n'} \right) d\boldsymbol{\eta}'',$$

where $D_{\boldsymbol{\eta}''} := \{\boldsymbol{\eta}'' \in \mathbb{R}^{l'} : \boldsymbol{\eta}'' = \boldsymbol{\eta}' \boldsymbol{W}^{\,t}\boldsymbol{W} \text{ and } \eta_i \leq \eta'_i \leq \eta_i + \Delta\eta_i\}$. For a set $S \subseteq \mathbb{R}^{n'}$, let 1_S denote the indicator function of S. Applying Lemma 4.3 with $\varphi = \varphi_{\boldsymbol{W}}$ and $\psi = 1_{\varphi^{-1}(D_{\boldsymbol{\eta}''}) \cap Q_{n'}}$, we have

$$\sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})} \mathcal{L}^n \left(\varphi_{\boldsymbol{W}}^{-1}(D_{\boldsymbol{\eta}''}) \cap Q_{n'} \right) = \int_{D_{\boldsymbol{\eta}''}} \mathcal{H}^{n'-l'}(\varphi_{\boldsymbol{W}}^{-1}(\boldsymbol{\eta}'') \cap Q_{n'}) d\boldsymbol{\eta}''.$$

Hence,

$$\begin{aligned} I &= \frac{1}{\sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})}} \frac{1}{\Delta\eta_1 \cdots \Delta\eta_l} \mathcal{L}^n \left(\varphi_{\boldsymbol{W}}^{-1}(D_{\boldsymbol{\eta}''}) \cap Q_{n'} \right) \\ &= \frac{1}{\sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})}} \frac{1}{\Delta\eta_1 \cdots \Delta\eta_l} \Pr\left(\varphi_{\boldsymbol{W}}(X_1, \ldots, X_n) \in D_{\boldsymbol{\eta}''} \right) \\ &= \frac{1}{\sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})}} \frac{1}{\Delta\eta_1 \cdots \Delta\eta_l} \Pr\left(\varphi_{\boldsymbol{W}}(X_1, \ldots, X_n)(\boldsymbol{W}^{\,t}\boldsymbol{W})^{-1} \in \prod_{i=1}^{l} [\eta_i + \Delta\eta_i] \right). \end{aligned}$$

Here, let $\hat{\rho}_{\boldsymbol{W}}(\boldsymbol{\eta})$ denote the probability density function of $\varphi_{\boldsymbol{W}}(X_1, \ldots, X_n)(\boldsymbol{W}^{\,t}\boldsymbol{W})^{-1}$. Then as $\Delta\eta_1 \to 0, \ldots, \Delta\eta_{l'} \to 0$, we have

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \frac{1}{\sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})}} \hat{\rho}_{\boldsymbol{W}}(\boldsymbol{\eta}).$$

Changing a variable $\boldsymbol{\eta}$ to $\boldsymbol{\eta}'$ with $\boldsymbol{\eta} = \boldsymbol{\eta}'(\boldsymbol{W}^{\,t}\boldsymbol{W})^{-1}$, $\rho_{\boldsymbol{W}}(\boldsymbol{\eta}')$ can be written as

$$\rho_{\boldsymbol{W}}(\boldsymbol{\eta}') = \hat{\rho}_{\boldsymbol{W}}(\boldsymbol{\eta}'(\boldsymbol{W}^{\,t}\boldsymbol{W})^{-1}) \frac{1}{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})}.$$

Hence, we have

$$f_{\boldsymbol{W}}(\boldsymbol{\eta}) = \sqrt{\det(\boldsymbol{W}^{\,t}\boldsymbol{W})} \rho_{\boldsymbol{W}}(\boldsymbol{\eta} \boldsymbol{W}^{\,t}\boldsymbol{W}).$$

□

Note that the probability density function $\rho_{\boldsymbol{W}}$ is a box spline. Hence, we can give an expression for $\rho_{\boldsymbol{W}}$. For details, See [2]

For a matrix $\boldsymbol{W} \in \mathbb{R}^{l\times n}$, we define a set $S(P_{\boldsymbol{W}})$ as

$$\{j \in \{1,\dots,n\} \colon \xi_j > 0 \text{ for some } (\xi_1,\dots,\xi_n) \in P_{\boldsymbol{W}}\}.$$

From the definition of $S(P_{\boldsymbol{W}})$, $j \in \{1,\dots,n\} \setminus S(P_{\boldsymbol{W}})$ if and only if $\xi_j = 0$ for any $(\xi_1,\dots,\xi_n) \in P_{\boldsymbol{W}}$. For a matrix $\boldsymbol{W}_{\hat{\boldsymbol{C}}} \in \mathbb{Z}^{l\times n}$, let $\boldsymbol{W}'_{\hat{\boldsymbol{C}}}$ denote an $l \times |S(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}})|$ matrix given by deleting columns in $\boldsymbol{W}_{\hat{\boldsymbol{C}}} \in \mathbb{Z}^{l\times n}$ corresponding to elements in $\{1,\dots,n\} \setminus S(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}})$ and let $\boldsymbol{W}''_{\hat{\boldsymbol{C}}}$ denote a matrix given by deleting rows equal to zero from the row echelon form of $\boldsymbol{W}'_{\hat{\boldsymbol{C}}}$.

Theorem 4.1 can be restated as follows.

Theorem 4.1′. *We have*

$$p_l^\circ(n,N) \le \frac{1}{N^n} \sum_{\hat{\boldsymbol{C}}} \left(g(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}) \rho_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}(\boldsymbol{0}) (N+1)^{\dim(P^\circ_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}})} + \cdots \right), \tag{4.13}$$

$$p_l(n,N) \le \frac{1}{(N+1)^n} \sum_{\hat{\boldsymbol{C}}} \left(g(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}) \rho_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}(\boldsymbol{0}) N^{\dim(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}})} + \cdots \right), \tag{4.14}$$

where "$\cdots$"'s in (4.13) *and* (4.14) *mean nonleading terms of Ehrhart quasipolynomials* $\mathrm{ehr}(P^\circ_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N+1)$ *and* $\mathrm{ehr}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N)$*, respectively, and* $g(\boldsymbol{W}''_{\hat{\boldsymbol{C}}})$ *is the greatest common divisor of determinants of all* $\mathrm{rank}(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}) \times \mathrm{rank}(\boldsymbol{W}''_{\hat{\boldsymbol{C}}})$ *submatrices of* $\boldsymbol{W}''_{\hat{\boldsymbol{C}}}$*.*

Proof of Theorem 4.1′. We only prove (4.14). Put $m = \dim(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}})$. From Proposition 2.8, the leading coefficient $e_m(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N)$ of Ehrhart quasipolynomial of $P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}$ is the relative volume $\mathrm{relvol}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}})$. Note that $m = n - \mathrm{rank}(\boldsymbol{W}_{\hat{\boldsymbol{C}}})$ does not always hold. From the definition of $\boldsymbol{W}''_{\hat{\boldsymbol{C}}} \in \mathbb{Z}^{l'\times n'}$, it holds that

$$\mathrm{vol}_m(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) = \mathrm{vol}_m(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}) \quad \text{and} \quad m = \dim(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}) = n' - \mathrm{rank}(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}) = n' - l'.$$

Applying Lemma 4.2 with $\boldsymbol{W} = \boldsymbol{W}''_{\hat{\boldsymbol{C}}}$, we have

$$\mathrm{vol}_m(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}) = f_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}(\boldsymbol{0}) = \sqrt{\det(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}\, {}^t\boldsymbol{W}''_{\hat{\boldsymbol{C}}})}\, \rho_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}(\boldsymbol{0}).$$

Note that the lattice $\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^n$ is defined by

$$\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^n = \{\boldsymbol{\xi} \in \mathbb{Z}^n \colon \boldsymbol{\xi}\, {}^t\boldsymbol{W}_{\hat{\boldsymbol{C}}} = \boldsymbol{0}\}.$$

Taking into account the degeneracy of $\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^n$, it is convenient to consider

$$\mathrm{aff}(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^{n'} = \{\boldsymbol{\xi}' \in \mathbb{Z}^{n'} \colon \boldsymbol{\xi}'\, {}^t\boldsymbol{W}''_{\hat{\boldsymbol{C}}} = \boldsymbol{0}\}$$

instead of $\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^n$. The determinant $\det(\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^{n+1})$ is calculated as follows.

$$\det(\mathrm{aff}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^{n+1}) = \det(\mathrm{aff}(P_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}) \cap \mathbb{Z}^{n+1}) = \frac{\sqrt{\det(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}\, {}^t\boldsymbol{W}''_{\hat{\boldsymbol{C}}})}}{g(\boldsymbol{W}''_{\hat{\boldsymbol{C}}})}.$$

Therefore, we obtain

$$e_m(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}, N) = \mathrm{relvol}(P_{\boldsymbol{W}_{\hat{\boldsymbol{C}}}}) = \gcd(\boldsymbol{W}''_{\hat{\boldsymbol{C}}}) \rho_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}(\boldsymbol{0}).$$

Remark 4.4. Probability density functions $\rho_{\boldsymbol{W}''_{\hat{\boldsymbol{C}}}}$ appeared in Theorem 4.1′ might be approximated by probability density functions of normal distributions. Our case is explained as follows. Let $X_1, X_2, \dots$ be independent random variables, each uniformly distributed in $[0,1]$, and let $w_{i,j}$ $(i = 1,\dots,l',\ j = 1,2,\dots)$ be integers.

Then $\{{}^t(w_{1,j},\dots,w_{l,j})X_j\}_{j=1}^{\infty}$ is a sequence of independent random vectors. Put $\boldsymbol{W}_n = (w_{i,j})_{1\le i\le l',\,1\le j\le n}$. Then the mean vector and the covariance matrix of a partial sum $\boldsymbol{S}_n := \sum_{j=1}^{n} {}^t(w_{1,j},\dots,w_{l,j})X_j$ are $\boldsymbol{\mu}_n := \frac{1}{2}\sum_{j=1}^{n} {}^t(w_{1,j},\dots,w_{l,j})$ and $\boldsymbol{\Sigma}_n := \frac{1}{12}\boldsymbol{W}_n\,{}^t\boldsymbol{W}_n$, respectively. Our question is whether the probability density function of $\boldsymbol{S}_n$ can be approximated by the probability density function of the normal distribution with mean vector $\boldsymbol{\mu}_n$ and covariance matrix $\boldsymbol{\Sigma}_n$. The answer is partially affirmative. That is because there is some possibility that a sufficient condition for the central limit theorem such as the multivariate Lyapunov's condition or the multivariate Lindeberg's condition does not hold for some $\{w_{i,j}\}_{1\le i\le l,\,1\le j<\infty}$. If a sufficient condition for the central limit theorem holds, then the probability density function $\rho_{\boldsymbol{W}_n}$ can be approximated as follows.

$$\rho_{\boldsymbol{W}_n}(\boldsymbol{\eta}) \approx \frac{1}{\sqrt{(2\pi)^l \det(\boldsymbol{\Sigma}_n)}} \exp\left(-\frac{1}{2}(\boldsymbol{\eta}-\boldsymbol{\mu}_n)\,\boldsymbol{\Sigma}_n^{-1}\,{}^t(\boldsymbol{\eta}-\boldsymbol{\mu}_n)\right).$$

Consider the case where $l = 1$. Then the above approximation implies

$$\rho_{\boldsymbol{w}_n}(\eta) \approx \sqrt{\frac{6}{\pi}}\frac{1}{\|\boldsymbol{w}^{(n)}\|} \exp\left(-6\frac{(\eta-\mu_n)^2}{\|\boldsymbol{w}^{(n)}\|^2}\right),$$

where $\boldsymbol{w}^{(n)} = (w_{1,1},\dots,w_{1,n})$ and $\mu_n = \sum_{j=1}^{n} w_{1,j}$.

□

References

[1] M. Beck and S. Robins. *Computing the Continuous Discretely*. Springer New York, NY, 2015.

[2] C. Boor, K. Höllig, and S. Riemenschneider. *Box Splines*. Springer New York, NY, 1993.

[3] M. Coster, A. Joux, B. Lamacchia, A. Odlyzko, C. Schnorr, and J. Stern. "Improved low-density subset sum algorithms". In: *computational complexity* 2 (1992), pp. 111–128.

[4] E. Ehrhart. "Démonstration de la loi de réciprocité du polyédre rationnel". In: *CR Acad. Sci. Paris Sér. AB* 265 (1967), A91–A94.

[5] E. Ehrhart. "Sur les polyèdres rationnels homothétiques à n dimensions". In: *CR Acad. Sci. Paris* 254 (1962), pp. 616–618.

[6] L. Evans and R. Gariepy. "Measure Theory and Fine Properties of Functions". In: Revised Edition (1st ed.) Chapman and Hall/CRC, 2015.

[7] C. Haase, B. Nill, and A. Paffenholz. "Lecture notes on lattice polytopes". In: *Fall School on Polyhedral Combinatorics* (2012).

[8] K. Hatsugai, S. Ruangwises, K. Asano, and Y. Abe. "NP-Completeness and Physical Zero-Knowledge Proofs for Sumplete, a Puzzle Generated by ChatGPT". In: *New Generation Computing* 42.3 (2024), pp. 429–448.

[9] T. Izu, J. Kogure, T. Koshiba, and T. Shimoyama. "Low-density attack revisited". In: *Designs, Codes and Cryptography* 43.1 (2007), pp. 47–59.

[10] J. Lagarias and A. Odlyzko. "Solving low-density subset sum problems". In: *Journal of the ACM* 32 (1985), pp. 229–246.

[11] I. G. MacDonald. "Polynomials Associated with Finite Gell-Complexes". In: *Journal of the London Mathematical Society* s2-4.1 (1971), pp. 181–192.

[12] P. McMullen. "Lattice invariant valuations on rational polytopes". In: *Archiv der Mathematik* 31.1 (1978), pp. 509–516.

[13] P. Penguin. *ChatGPT invented its own puzzle game*. `https://puzzledpenguin.substack.com/p/chatgpt-invented-its-own-puzzle-game`. 2023.