Hindawi
Journal of Mathematics
Volume 2024, Article ID 7777881, 6 pages
https://doi.org/10.1155/2024/7777881

Research Article

The Second and Fourth Moments of Discrete Gaussian Distributions over Lattices

Wei Zhao[1] **and Guoyou Qian**[2]

[1]*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*
[2]*Mathematical College, Sichuan University, Chengdu 610064, China*

Correspondence should be addressed to Guoyou Qian; qiangy1230@163.com

Received 17 October 2023; Revised 29 March 2024; Accepted 3 May 2024; Published 20 May 2024

Academic Editor: Antonio Di Crescenzo

Let Λ be an n-dimensional lattice. For any n-dimensional vector $\mathbf{c}$ and positive real number s, let $D_{s,\mathbf{c}}$ and $D_{\Lambda,s,\mathbf{c}}$ denote the continuous Gaussian distribution and the discrete Gaussian distribution over Λ, respectively. In this paper, we establish the exact relationship between the second and fourth moments centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and those of the continuous Gaussian distribution $D_{s,\mathbf{c}}$, respectively. This provides a quantization form of the result obtained by Micciancio and Regev on the second and fourth moments of discrete Gaussian distribution. Using the relationship, we also derive an uncertainty principle for Gaussian functions, which extend the result of Zheng, Zhao, and Xu. Our proof is based on combination of the idea of Micciancio and Regev and the idea of Zheng, Zhao, and Xu, where the main tool is high-dimensional Fourier transform.

1. Introduction

An n-dimensional *lattice* $\Lambda \subseteq \mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$. The *dual lattice* $\widehat{\Lambda}$ of Λ is defined to be

$$\widehat{\Lambda} = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\}, \tag{1}$$

where $\langle \mathbf{x}, \mathbf{y} \rangle$ denotes the canonical inner product of $\mathbf{x}$ and $\mathbf{y}$ (see, for example, [1, 2]). Given parameters $s > 0$ and $\mathbf{c} \in \mathbb{R}^n$, let $\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi \|(\mathbf{x}-\mathbf{c})/s\|^2}$ with $\mathbf{x}$ being any n-dimensional vector. As in [3, 4], the probability density function of the continuous Gaussian distribution around $\mathbf{c}$ with parameter s is defined by $D_{s,\mathbf{c}}(\mathbf{x}) = \rho_{s,\mathbf{c}}(\mathbf{x})/s^n$ for any $\mathbf{x} \in \mathbb{R}^n$. By direct calculation, one can obtain that the second and fourth central moments of the random variable subject to $D_{s,\mathbf{c}}$ are $(ns^2/2\pi)$ and $(3ns^4/4\pi^2)$, respectively. The discrete Gaussian distribution over Λ is defined for any $\mathbf{x} \in \Lambda$ by

$$D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}, \tag{2}$$

where $\rho_{s,\mathbf{c}}(S) = \sum_{\mathbf{x} \in S} \rho_{s,\mathbf{c}}(\mathbf{x})$ for any countable subset $S \subseteq \mathbb{R}^n$ (see [3–5] for a more in-depth discussion on $D_{\Lambda,s,\mathbf{c}}$).

In [6], Banaszczyk initiated the study of discrete Gaussian distributions and established several measure inequalities to prove transference theorems for lattices. In [7, 8], Banaszczyk obtained more measure inequalities for convex bodies, which are very useful in the study of lattice-based cryptography. In [3, 4], Micciancio and Regev introduced an important lattice parameter named as *smoothing parameter*, which is defined for any $\epsilon > 0$ and any lattice Λ by

$$\eta_\epsilon(\Lambda) = \min\{s > 0 : \rho_{1/s}(\widehat{\Lambda}) \leqslant 1 + \epsilon\}. \tag{3}$$

Subsequently, Micciancio and Regev [3, 4] proved that $D_{\Lambda,s,\mathbf{c}}$ has very good statistical properties if s is large enough relatively to $\eta_\epsilon(\Lambda)$. For more detailed background information and development on the study of smoothing parameter and discrete Gaussian distribution, we refer readers to the important papers [3, 4, 9–16].

In the seminal work [3, 4], Micciancio and Regev proved that vectors distributed according to $D_{\Lambda,s,\mathbf{c}}$ have the mean value very close to $\mathbf{c}$, and expected squared distance from $\mathbf{c}$ very close to $(ns^2/2\pi)$, and the fourth moments centered around $\mathbf{c}$ very close to $(3ns^4/4\pi^2)$ provided that s is larger than $2\eta_\epsilon(\Lambda)$.

Theorem 1. *For any n-dimensional lattice Λ, vector $\mathbf{c} \in \mathbb{R}^n$, and positive reals $\epsilon \in (0,1)$, $s \geqslant 2\eta_\epsilon(\Lambda)$, we have*

$$\left\|\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,s,\mathbf{c}}}[\boldsymbol{\xi}-\mathbf{c}]\right\|^2 \leqslant \left(\frac{\epsilon}{1-\epsilon}\right)^2 s^2 n, \tag{4}$$

$$\left|\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,s,\mathbf{c}}}\left[\|\boldsymbol{\xi}-\mathbf{c}\|^2\right] - \frac{ns^2}{2\pi}\right| \leqslant \frac{\epsilon}{1-\epsilon} s^2 n, \tag{5}$$

$$\left|\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,s,\mathbf{c}}}\left[\|\boldsymbol{\xi}-\mathbf{c}\|^4\right] - \frac{3ns^4}{4\pi^2}\right| \leqslant \frac{\epsilon}{1-\epsilon} s^4 n. \tag{6}$$

Proof. Inequality (4) is the first result of Lemma 4.3 in [4]. Inequalities (5) and (6) can be derived directly from Lemma 4.2 in [3, 4]. □

In this paper, we mainly focus on the statistical properties of discrete Gaussian distributions. Our motivation is to provide a quantization form of the result obtained by Micciancio and Regev [3, 4] on the second and fourth moments of discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$. In particular, we shall establish the exact relationship between the second and fourth moments centered around $\mathbf{c}$ of discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and the second and fourth moments centered around $\mathbf{c}$ of the continuous Gaussian distribution $D_{s,\mathbf{c}}$. Using the relationship, we can also derive an uncertainty principle for Gaussian functions $\rho_{s,\mathbf{c}}$ on lattices. As in [1, 5], for a complex function f on $\mathbb{R}^n$, the Fourier transform of f is defined by $\widehat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i\langle \mathbf{x},\mathbf{y}\rangle} d\mathbf{x}$. Uncertainty principle plays an important role in harmonic analysis, quantum mechanics, and time–frequency analysis. The classical n-dimensional Heisenberg uncertainty principle for continuous Fourier transform with respect to a rapidly decreasing function $f\colon \mathbb{R}^n \longrightarrow \mathbb{C}$ can be stated as the following inequality (see [17, 18]):

$$\int_{\mathbb{R}^n} \|\mathbf{x}\|^2 \frac{|f(\mathbf{x})|^2}{\int_{\mathbb{R}^n} |f(\mathbf{t})|^2 d\mathbf{t}} d\mathbf{x} \int_{\mathbb{R}^n} \|\mathbf{y}\|^2 \frac{|\widehat{f}(\mathbf{y})|^2}{\int_{\mathbb{R}^n} |f(\mathbf{t})|^2 d\mathbf{t}} d\mathbf{y} \geqslant \frac{n^2}{16\pi^2}. \tag{7}$$

The uncertainty principle tells us that the quantities $\int_{\mathbb{R}^n} \|\mathbf{x}\|^2 |f(\mathbf{x})|^2 / \int_{\mathbb{R}^n} |f(\mathbf{t})|^2 d\mathbf{t}\, d\mathbf{x}$ and $\int_{\mathbb{R}^n} \|\mathbf{y}\|^2 |\widehat{f}(\mathbf{y})|^2 / \int_{\mathbb{R}^n} |f(\mathbf{t})|^2 d\mathbf{t}\, d\mathbf{y}$ both cannot be too small. That is, a function f and its Fourier transform $\widehat{f}$ both cannot be essentially localized.

The celebrated Donoho–Stark uncertainty principle on the cyclic group Z_N [19] states that, for a function $f \in \ell^2(Z_N)\backslash\{0\}$,

$$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})| \geqslant |G|, \tag{8}$$

where $\mathrm{supp}(f) = \{j \in Z_N\colon f(j) \neq 0\}$ and $|S|$ denotes the cardinality of a set S. If the group becomes $G = \mathbb{Z}/p\mathbb{Z}$ for some prime p, Tao [20] then improved the above estimate as

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\widehat{f})| \geqslant |G| + 1. \tag{9}$$

For simplicity, we write $\rho_{s,\mathbf{0}}(\mathbf{x})$ by $\rho_s(\mathbf{x})$ for any $s > 0$. Motivated by the technique developed by Banaszczyk in [6], Zheng et al. proved the following simple form of uncertainty principle for Gaussian functions ρ_s on lattices by using Fourier analysis in their important work [16].

Theorem 2. *Let Λ be an n-dimensional lattice and $s > 0$. We have*

$$\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}\|^2 \frac{\rho_s(\mathbf{x})}{\rho_s(\Lambda)} + s^4 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{\widehat{\rho_s}(\mathbf{y})}{\widehat{\rho_s}(\widehat{\Lambda})} = \frac{ns^2}{2\pi}. \tag{10}$$

Notice that the quantity $(ns^2/2\pi)$ in Theorem 2 is just the second moment of the continuous Gaussian distribution $D_{s,\mathbf{0}}$. That is, Theorem 2 gives the exact difference between the second moment of $D_{\Lambda,s,\mathbf{0}}$ and the second moment of $D_{s,\mathbf{0}}$. In addition, Theorem 2 also establishes the precise relationship between the second moment of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{0}}$ over the lattice Λ and the second moment of discrete Gaussian distribution $D_{\widehat{\Lambda},1/s,\mathbf{0}}$ over the dual lattice $\widehat{\Lambda}$ of Λ since $\widehat{\rho_s}(\mathbf{x}) = s^n \rho_{1/s}(\mathbf{x})$. Naturally, one expects to determine the exact differences between the second and fourth moments centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and those of the continuous Gaussian distribution $D_{s,\mathbf{c}}$ and to establish an uncertainty principle for general Gaussian functions $\rho_{s,\mathbf{c}}$ on lattices. Combining the idea of the proof of Lemma 4.2 in [3, 4] by Micciancio and Regev with the technique developed by Zheng et al. in [16], we prove two equalities connecting the second and fourth moments centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and the second and fourth moments centered around $\mathbf{c}$ of the continuous Gaussian distribution $D_{s,\mathbf{c}}$, respectively. Our main tool is high-dimensional Fourier transform. In addition, we establish an uncertainty principle for Gaussian functions $\rho_{s,\mathbf{c}}$ on lattices. We are now in a position to state our main result.

Theorem 3. *For any n-dimensional lattice Λ, vector $\mathbf{c} \in \mathbb{R}^n$, and real $s > 0$, we have*

$$\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}-\mathbf{c}\|^2 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} + s^4 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} = \frac{ns^2}{2\pi}, \tag{11}$$

and

$$\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}-\mathbf{c}\|^4 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} + \frac{3s^6}{\pi} \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} - s^8 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^4 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} = \frac{3ns^4}{4\pi^2}. \tag{12}$$

Obviously, when $\mathbf{c} = \mathbf{0}$, equality (11) in Theorem 3 becomes Zheng-Zhao-Xu Theorem (see Theorem 1 of [16]). But we cannot call (11) the uncertainty principle since $\widehat{\rho_{s,\mathbf{c}}}(\mathbf{x}) = s^n \rho_{1/s}(\mathbf{x}) e^{-2\pi i \langle \mathbf{x},\mathbf{c}\rangle}$ may take complex values. Let $\Re e(\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y}))$ denote the real part of $\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})$. With the help of the facts that $|\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})| \geqslant \Re e(\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y}))$ and $\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda}) = \det(\Lambda)\rho_{s,\mathbf{c}}(\Lambda) > 0$, one can easily deduce the following result by (11), which can be called the uncertainty principle for Gaussian functions over lattices. This extends the uncertainty principle obtained by Zheng et al. in [16] from the Gaussian function $\rho_{s,\mathbf{0}}$ to the general Gaussian function $\rho_{s,\mathbf{c}}$.

Theorem 4. *For any n-dimensional lattice Λ, vector $\mathbf{c} \in \mathbb{R}^n$, and real $s > 0$, we have*

$$\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x} - \mathbf{c}\|^2 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} + s^4 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{|\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})|}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \geqslant \frac{ns^2}{2\pi}. \tag{13}$$

Equality (11) in Theorem 3 implies that the exact difference between the second moment centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and the second moment centered around $\mathbf{c}$ of the continuous Gaussian distribution $D_{s,\mathbf{c}}$ is just equal to $s^4 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 (\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})/\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda}))$. Equality (12) in Theorem 3 implies that the exact difference between the fourth moment centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and the fourth moment centered around $\mathbf{c}$ of the continuous Gaussian distribution $D_{s,\mathbf{c}}$ is just equal to $3s^6/\pi \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 (\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})/\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})) - s^8 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^4 (\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})/\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda}))$. Theorem 4 implies that the second moment $\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x} - \mathbf{c}\|^2 (\rho_{s,\mathbf{c}}(\mathbf{x})/\rho_{s,\mathbf{c}}(\Lambda))$ centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and the sum $\sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 (|\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})|/\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda}))$ involving the Fourier transform $\widehat{\rho_{s,\mathbf{c}}}$ of $\rho_{s,\mathbf{c}}$ both cannot be too small. We shall prove Theorem 3 and provide an interesting corollary in Section 2.

2. Proof of Theorem 4

In the following, n is a fixed positive integer. We first give the following useful properties of high-dimensional Fourier transform.

Lemma 5 (see Lemmas 1.1.2 and 1.2.1 of [5]). *Suppose that $f(\mathbf{x})$ and $g(\mathbf{x})$ are two complex functions defined on $\mathbb{R}^n$. We have the following:*

(i) If $f(\mathbf{x}) = g(\mathbf{x}) e^{2\pi i \langle \mathbf{x},\mathbf{v}\rangle}$ for some $\mathbf{v} \in \mathbb{R}^n$, then

$$\widehat{f}(\mathbf{x}) = \widehat{g}(\mathbf{x} - \mathbf{v}). \tag{14}$$

(ii) For any vectors $\mathbf{c}, \mathbf{x}$, and $s > 0$, we have

$$\widehat{\rho_{s,\mathbf{c}}}(\mathbf{x}) = s^n \rho_{1/s}(\mathbf{x}) e^{-2\pi i \langle \mathbf{x},\mathbf{c}\rangle}. \tag{15}$$

For the purpose of establishing the relationship between the second and fourth moments centered around $\mathbf{c}$ of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ and those of the continuous Gaussian distribution $D_{s,\mathbf{c}}$, we need the following Poisson summation formula which has been widely used in the theory of lattices.

Lemma 6 (see Theorem 2.3 of [1]). *Let Λ be an n-dimensional lattice, and let $f: \mathbb{R}^n \longrightarrow \mathbb{C}$ be a function which satisfies the following conditions (V1), (V2), and (V3):*

(V1) $\int_{\mathbb{R}^n} |f(\mathbf{x})| d\mathbf{x} < \infty$

(V2) The series $\sum_{\mathbf{x}\in\Lambda} |f(\mathbf{x} + \mathbf{v})|$ converges uniformly for all $\mathbf{v}$ belonging to a compact subset of $\mathbb{R}^n$

(V3) The series $\sum_{\mathbf{y}\in\widehat{\Lambda}} \widehat{f}(\mathbf{y})$ is absolutely convergent

Then, we have

$$\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Lambda)} \sum_{\mathbf{y}\in\widehat{\Lambda}} \widehat{f}(\mathbf{y}), \tag{16}$$

where $\mathrm{vol}(\mathbb{R}^n/\Lambda)$ denotes the volume of the fundamental parallelepiped of Λ.

Let $\boldsymbol{\xi}$ be a random vector subject to the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$. From Theorem 1, we know that the mean value of the random vector $\boldsymbol{\xi}$ subject to $D_{\Lambda,s,\mathbf{c}}$ is very close to $\mathbf{c}$. However, we still cannot determine the exact value of $\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,s,\mathbf{c}}}(\boldsymbol{\xi})$ to this day. Therefore, to prove Theorem 3, we cannot estimate the second and fourth moments of the discrete Gaussian distribution $D_{\Lambda,s,\mathbf{c}}$ by direct computation such as the continuous Gaussian distribution. Inspired by the idea of Micciancio and Regev in Lemma 4.2 of [3, 4] and the idea of Zheng, Zhao, and Xu in their Theorem 1 of [16], we can now give the proof of Theorem 3 as follows.

Proof of Theorem 3. Let $\mathbf{u} \in \mathbb{R}^n$ be a unit vector. We consider the following function:

$$F(t) = \sum_{\mathbf{x}\in\Lambda} e^{2\pi i t \langle \mathbf{x}-\mathbf{c},\mathbf{u}\rangle} \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}. \tag{17}$$

Calculating the first derivative, the second derivative, and the fourth derivative of the function $F(t)$ directly, we get

$$\begin{aligned} F'(t) &= \sum_{\mathbf{x}\in\Lambda} 2\pi i \langle \mathbf{x} - \mathbf{c}, \mathbf{u}\rangle e^{2\pi i t \langle \mathbf{x}-\mathbf{c},\mathbf{u}\rangle} \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}, \\ F''(t) &= \sum_{\mathbf{x}\in\Lambda} \left(-4\pi^2\right) \langle \mathbf{x} - \mathbf{c}, \mathbf{u}\rangle^2 e^{2\pi i t \langle \mathbf{x}-\mathbf{c},\mathbf{u}\rangle} \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}, \end{aligned} \tag{18}$$

and

$$F^{(4)}(t) = \sum_{\mathbf{x}\in\Lambda} \left(16\pi^4\right) \langle \mathbf{x} - \mathbf{c}, \mathbf{u}\rangle^4 e^{2\pi i t \langle \mathbf{x}-\mathbf{c},\mathbf{u}\rangle} \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}. \tag{19}$$

Let $f(\mathbf{x}) = e^{2\pi i t \langle \mathbf{x}-\mathbf{c},\mathbf{u}\rangle} \rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-2\pi i t \langle \mathbf{c},\mathbf{u}\rangle} \rho_{s,\mathbf{c}}(\mathbf{x}) e^{2\pi i \langle \mathbf{x},t\mathbf{u}\rangle}$. It is easy to check that $f(\mathbf{x})$ satisfies the conditions (V1), (V2), and (V3) in Lemma 6. Hence, by Lemmas 5 and 6, we obtain

$$
\begin{aligned}
F(t) &= \frac{1}{\rho_{s,\mathbf{c}}(\Lambda)} \sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = \frac{1}{\rho_{s,\mathbf{c}}(\Lambda)} \frac{1}{\mathrm{vol}(\mathbb{R}^n/\Lambda)} \sum_{\mathbf{y}\in\widehat{\Lambda}} \widehat{f}(\mathbf{y}) \\
&= \frac{1}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \mathrm{e}^{-2\pi i t\langle \mathbf{c},\mathbf{u}\rangle} \widehat{\rho_{s,\mathbf{c}}}(\mathbf{y} - t\mathbf{u}) \\
&= \frac{1}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \mathrm{e}^{-2\pi i t\langle \mathbf{c},\mathbf{u}\rangle} s^n \rho_{1/s}(\mathbf{y} - t\mathbf{u}) \mathrm{e}^{-2\pi i\langle \mathbf{y}-t\mathbf{u},\mathbf{c}\rangle} \\
&= \frac{1}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} s^n \rho_{1/s}(\mathbf{y} - t\mathbf{u}) \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \\
&= \frac{1}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \mathrm{e}^{-\pi s^2 \|\mathbf{y}-t\mathbf{u}\|^2}.
\end{aligned}
\tag{20}
$$

Now, computing the first derivative, the second derivative, and the fourth derivative of $F(t)$ according to the above expression, we derive from $\|\mathbf{u}\| = 1$ that

$$
\begin{aligned}
F'(t) &= \frac{-2\pi s^{n+2}}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} (t - \langle \mathbf{y},\mathbf{u}\rangle) \mathrm{e}^{-\pi s^2 \|\mathbf{y}-t\mathbf{u}\|^2}, \\
F''(t) &= \frac{-2\pi s^2}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \left(1 - 2\pi s^2 (t - \langle \mathbf{y},\mathbf{u}\rangle)^2\right) s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \rho_{1/s}(\mathbf{y} - t\mathbf{u}),
\end{aligned}
\tag{21}
$$

and

$$
F^{(4)}(t) = \frac{2\pi^2 s^4}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \left[6 - 24\pi s^2 (t - \langle \mathbf{y},\mathbf{u}\rangle)^2 + 8\pi^2 s^4 (t - \langle \mathbf{y},\mathbf{u}\rangle)^4\right] s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \rho_{1/s}(\mathbf{y} - t\mathbf{u}). \tag{22}
$$

Taking $\mathbf{u}$ to be $\mathbf{e}_j$ for $1 \leqslant j \leqslant n$ in (18) and (21) successively, and then adding them up, respectively, we obtain that

$$
\begin{aligned}
&\frac{-4\pi^2}{\rho_{s,\mathbf{c}}(\Lambda)} \sum_{j=1}^{n} \sum_{\mathbf{x}\in\Lambda} \left\langle \mathbf{x} - \mathbf{c}, \mathbf{e}_j \right\rangle^2 \mathrm{e}^{2\pi i t \left\langle \mathbf{x}-\mathbf{c},\mathbf{e}_j \right\rangle} \rho_{s,\mathbf{c}}(\mathbf{x}) \\
&= \frac{-2\pi s^2}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{j=1}^{n} \sum_{\mathbf{y}\in\widehat{\Lambda}} \left(1 - 2\pi s^2 \left(t - \left\langle \mathbf{y}, \mathbf{e}_j \right\rangle\right)^2\right) s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \rho_{1/s}\left(\mathbf{y} - t\mathbf{e}_j\right).
\end{aligned}
\tag{23}
$$

Setting $t = 0$ in (23), we derive that

$$4\pi^2 \sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}-\mathbf{c}\|^2 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} = \frac{2\pi n s^2}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \rho_{1/s}(\mathbf{y}) - \frac{4\pi^2 s^4}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 s^n \mathrm{e}^{-2\pi i\langle \mathbf{y},\mathbf{c}\rangle} \rho_{1/s}(\mathbf{y}). \tag{24}$$

Now, applying Lemma 5 (ii) and dividing both sides of (24) by $4\pi^2$, we get

$$\sum_{\mathbf{x}\in\Lambda} \frac{\|\mathbf{x}-\mathbf{c}\|^2 \rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} + s^4 \sum_{\mathbf{y}\in\widehat{\Lambda}} \frac{\|\mathbf{y}\|^2 \widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} = \frac{ns^2}{2\pi}. \tag{25}$$

Similarly, taking $\mathbf{u}$ to be $\mathbf{e}_j$ for $1 \leqslant j \leqslant n$ in (19) and (22) successively, and adding them up, respectively, we consequently obtain by setting $t = 0$ that

$$16\pi^4 \sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}-\mathbf{c}\|^4 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} = \sum_{\mathbf{y}\in\widehat{\Lambda}} \frac{\widehat{\rho_{s,\mathbf{c}}}(y)}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \left(12n\pi^2 s^4 - 48\pi^3 s^6 \|\mathbf{y}\|^2 + 16\pi^4 s^8 \|\mathbf{y}\|^4\right). \tag{26}$$

Dividing both sides of (26) by $16\pi^4$, we obtain

$$\sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}-\mathbf{c}\|^4 \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)} + \frac{3s^6}{\pi} \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} - s^8 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^4 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} = \frac{3ns^4}{4\pi^2}, \tag{27}$$

as desired. This completes the proof of Theorem 3. □

Applying the same method as in the proof of Theorem 3, we can also obtain the exact difference between the higher moments of discrete Gaussian distribution and those of continuous Gaussian distribution. But the explicit form would be more complex and the analysis will become quite cumbersome. For more general argument concerning the estimate of pth moment of discrete Gaussian distribution, the readers can refer to [13]. Applying Theorems 1 and 3, we have the following result.

Corollary 7. *Let Λ be an n-dimensional lattice and $\epsilon \in (0,1)$. Let s be a real number greater than or equal to $2\eta_\epsilon(\Lambda)$. Then, for any vector $\mathbf{c} \in \mathbb{R}^n$, we have*

$$\left| \sum_{\mathbf{y}\in\widehat{\Lambda}} \frac{\|\mathbf{y}\|^2 \widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \right| \leqslant \frac{\epsilon}{(1-\epsilon)} \cdot \frac{1}{s^2} n, \tag{28}$$

and

$$\left| \frac{3}{\pi} \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^2 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} - s^2 \sum_{\mathbf{y}\in\widehat{\Lambda}} \|\mathbf{y}\|^4 \frac{\widehat{\rho_{s,\mathbf{c}}}(\mathbf{y})}{\widehat{\rho_{s,\mathbf{c}}}(\widehat{\Lambda})} \right| \leqslant \frac{\epsilon}{1-\epsilon} \cdot \frac{1}{s^2} n. \tag{29}$$

Furthermore, if $\mathbf{c} = \mathbf{0}$ and Λ is a self-dual lattice, then

$$\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,1/s}} \left[\|\boldsymbol{\xi}\|^2\right] \leqslant \frac{\epsilon}{(1-\epsilon)} \cdot \frac{1}{s^2} n. \tag{30}$$

Proof. First, it follows immediately from Theorems 1 and 3 that inequalities (28) and (29) hold. If $\mathbf{c} = 0$ and Λ is a self-dual lattice, then $\widehat{\Lambda} = \Lambda$ and $\widehat{\rho_{s,\mathbf{c}}}(\mathbf{x}) = s^n \rho_{1/s}(\mathbf{x})$. Hence, we have

$$\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,1/s}} \left[\|\boldsymbol{\xi}\|^2\right] = \sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}\|^2 \frac{\rho_{1/s}(\mathbf{x})}{\rho_{1/s}(\Lambda)} = \sum_{\mathbf{x}\in\Lambda} \|\mathbf{x}\|^2 \frac{s^n \rho_{1/s}(\mathbf{x})}{s^n \rho_{1/s}(\Lambda)} = \sum_{\mathbf{x}\in\widehat{\Lambda}} \frac{\|\mathbf{x}\|^2 \widehat{\rho}_s(\mathbf{x})}{\widehat{\rho}_s(\widehat{\Lambda})}. \tag{31}$$

So we derive from (28) that (30) holds. The proof of Corollary 7 is completed. □

From (30), we know that $\mathrm{Exp}_{\boldsymbol{\xi}\sim D_{\Lambda,s}}[\|\boldsymbol{\xi}\|^2]$ is also very small if Λ is a self-dual lattice and $s \leqslant 1/2\eta_\epsilon(\Lambda)$.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant no. 12371333 and in part by the Stability Program of Science and Technology on Communication Security Laboratory (2022).

References

[1] W. Ebeling, "*Lattices and codes*, A course partially based on lectures," *Adv. Lectures Math*, F. Hirzebruch, Ed., Friedr. Vieweg &Sohn, Braunschweig, Germany, 2nd edition, 2002.

[2] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Kluwer Academic Publishers, Berlin, Germany, 2002.

[3] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *45th Annual IEEE Symposium on Foundations of Computer Science*, pp. 372–381, Symposium on Foundations, Rome, Italy, 2004.

[4] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[5] Z. Zheng, K. Tian, and F. Liu, "Modern cryptography," *A Classical Introduction to Informational and Mathematical Principle*, Springer, Singapore, 2023.

[6] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Mathematische Annalen*, vol. 296, no. 1, pp. 625–635, 1993.

[7] W. Banaszczyk, "Inequalities for convex bodies and polar reciprocal lattices inR n," *Discrete and Computational Geometry*, vol. 13, no. 2, pp. 217–231, 1995.

[8] W. Banaszczyk, "*Inequalities for convex bodies and polar reciprocal lattices in RnII: application of k-convexity*," *Discrete and Computational Geometry*, vol. 16, no. 3, pp. 305–311, 1996.

[9] K. Chung, D. Dadush, F. Liu, and C. Peikert, "On the lattice smoothing parameter problem," in *Proceedings of the IEEE Conference on Computational Complexity*, pp. 230–241, Cambridge, UK, June 2013.

[10] N. Genise, D. Micciancio, C. Peikert, and M. Walter, "Improved discrete Gaussian and subgaussian analysis for lattice cryptography," *Lecture Notes in Comput. Sci*, pp. 623–651, Springer, Cham, 2020.

[11] C. Gentry, C. Peikert, and V. Vaikuntanathan, "How to use a short basis: trapdoors for hard lattices and wew cryptographic constructions," pp. 197–206, 2008, https://eprint.iacr.org/2007/432.pdf.

[12] D. Micciancio and M. Walter, "Gaussian sampling over the integers: efcient, generic, constant-time," *Proceeding CRYPTO*, vol. 12, pp. 455–485, 2017.

[13] C. Peikert, "Limits on the hardness of lattice problems in ℓ p norms," *Computational Complexity*, vol. 17, no. 2, pp. 300–351, 2008.

[14] C. Peikert, "An efficient and parallel Gaussian sampler for lattices," *Advances in Cryptology– CRYPTO 2010*, vol. 52, pp. 80–97, 2010.

[15] C. Tian, M. Liu, and G. Xu, "Measure inequalities and the transference theorem in the geometry of numbers," *Proceedings of the American Mathematical Society*, vol. 142, no. 1, pp. 47–57, 2014.

[16] Z. Zheng, C. Zhao, and G. Xu, "Discrete Gaussian measures and new bounds of the smoothing parameter for lattices," *Applicable Algebra in Engineering, Communication and Computing*, vol. 32, no. 5, pp. 637–650, 2021.

[17] G. B. Folland and A. Sitaram, "The uncertainty principle: a mathematical survey," *Journal of Fourier Analysis and Applications*, vol. 3, pp. 207–238, 1997.

[18] E. Stein and R. Shakarchi, *Fourier Analysis-An Introduction*, Princeton University Press, Princeton, NY, USA, 2003.

[19] D. Donoho and P. Stark, "Uncertainty principles and signal recovery," *SIAM Journal on Applied Mathematics*, vol. 49, no. 3, pp. 906–931, 1989.

[20] T. Tao, "An uncertainty principle for cyclic groups of prime order," *Mathematical Research Letters*, vol. 12, no. 1, pp. 121–127, 2005.