Discrete Gaussian Measures and New Bounds of the Smoothing Parameter for Lattices

Zhongxiang Zheng[*], Guangwu Xu[†‡], and Chunhuan Zhao [§]

Abstract

In this paper, we start with a discussion of discrete Gaussian measures on lattices. Several results of Banaszczyk are analyzed, different approaches are suggested. In the second part of the paper we prove two new bounds for the smoothing parameter of lattices. Under the natural assumption that ε is suitably small, we obtain two estimations of the smoothing parameter:

1. $$\eta_\varepsilon(\mathbb{Z}) \leq \sqrt{\frac{\ln\left(\frac{\varepsilon}{44}+\frac{2}{\varepsilon}\right)}{\pi}}.$$

2. For a lattice $\mathcal{L} \subset \mathbb{R}^n$ of dimension n,
$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(n-1+\frac{2n}{\varepsilon}\right)}{\pi}}\tilde{bl}(\mathcal{L}).$$

1 Introduction

An n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors (a basis) $\mathbf{b_1}, \ldots, \mathbf{b_n}$. This basis is also denoted by the matrix $\mathbf{B}$ whose columns are $\mathbf{b}_1, \ldots, \mathbf{b}_n$ and the lattice $\mathcal{L}$ is sometimes written in a more explicit manner:

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

The lattice $\mathcal{L}$, as a $\mathbb{Z}$-module, has a dual lattice (module) $\hat{\mathcal{L}} = \mathrm{Hom}(\mathcal{L}, \mathbb{Z})$ which can be realized precisely by the following set:

$$\hat{\mathcal{L}} = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z},\ \forall \mathbf{x} \in \mathcal{L}\}.$$

[*] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China;

[†] Department of EE & CS, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA; e-mail: gxu4uwm@uwm.edu.

[‡] Corresponding author.

[§] Institute for Advanced Study, Tsinghua University, Beijing 100084, China;

Computationally infeasible problems like Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) and their variants in high dimensional lattices are good bases for setting up cryptosystems using lattices. Lattice-based cryptography is also believed to resist quantum computer attacks. In introducing random noises in lattice-based cryptosystems, discrete Gaussian distribution is one of the most important choices. Given parameters $s > 0$ and $\mathbf{c} \in \mathbb{R}^n$, the discrete Gaussian measure assigns a lattice vector $\mathbf{v} \in \mathcal{L}$ the probability value $\frac{\rho_{s,\mathbf{c}}(\mathbf{v})}{\rho_{s,\mathbf{c}}(\mathcal{L})}$ where $\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{s^2}}$ and $\rho_{s,\mathbf{c}}(S) = \sum_{\mathbf{x}\in S}\rho_{s,\mathbf{c}}(\mathbf{x})$ for any countable set S. In the study of lattices, dual lattices, and the Gaussian function ρ_s, Fourier analysis has a great role to play. One of the useful tools is the classical Poisson formula which gives

$$\rho_{s,\mathbf{c}}(\mathcal{L}) = \frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}} e^{-2\pi i\langle\mathbf{y},\mathbf{c}\rangle}\rho_{\frac{1}{s}}(\mathbf{y}).$$

A study of discrete Gaussian measures on lattices was initiated by Banaszczyk. In his seminal work [1, 2], several measure inequalities were proved and new transference theorems were discovered. His results have been playing important roles in lattice-based cryptography. In the first part of this paper, we shall discuss some measure inequalities from [1, 2] by stating improvements and proposing different proofs. We also establish a relation between the second moments of $\rho_{s,\mathbf{c}}(\mathcal{L})$ and $\rho_{\frac{1}{s},\mathbf{0}}(\hat{\mathcal{L}})$.

In [9], Micciancio and Regev introduced a new numerical parameter for lattices that is related to discrete Gaussian measures –the smoothing parameter. For an n-dimensional lattice $\mathcal{L}$, the smoothing parameter is defined with respect to an $\varepsilon > 0$ and given by

$$\eta_\varepsilon(\mathcal{L}) = \min\{s : \rho_{\frac{1}{s}}(\hat{\mathcal{L}}) \leq 1 + \varepsilon\}.$$

Using the Poisson formula, it has been proved in [9] that the distribution defined on $\mathbb{R}^n/\mathcal{L}$ whose density function is $d(\mathbf{x}) = \frac{1}{s^n}\rho_s(\mathcal{L} + (\mathbf{x} - \mathbf{c}))$ is statistically close to the uniform distribution on $\mathbb{R}^n/\mathcal{L}$, if $s \geq \eta_\varepsilon(\mathcal{L})$.

The first non-trivial upper bound for $\eta_\varepsilon(\mathcal{L})$ was established by Micciancio and Regev in [9], denoting $\lambda_i(\mathcal{L})$ to be the ith successive minimum, they proved that

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}\lambda_n(\mathcal{L}). \tag{1}$$

A bound for $\eta_\varepsilon(\mathcal{L})$ in terms of dual minimum distance in ℓ^∞-norm was given by Peikert in [11]:

$$\eta_\varepsilon(\mathcal{L}) \leq \frac{\sqrt{\frac{\ln(2n(1+\frac{1}{\varepsilon}))}{\pi}}}{\lambda_1^\infty(\hat{\mathcal{L}})}. \tag{2}$$

Let $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n)$ be a basis of $\mathcal{L}$ such that $\max_j \|\mathbf{b}_j^*\|$ is smallest (such an quantity is usually written as $\tilde{bl}(\mathcal{L})$), where $\{\mathbf{b}_1^*, \mathbf{b}_2^*, \cdots, \mathbf{b}_n^*\}$ is its Gram-Schmidt orthogonal basis. It is known that (lemma 7.1 of [8]) there is a basis $\mathbf{B}$ of $\mathcal{L}$ such that $\max_j \|\mathbf{b}_j^*\| \leq \lambda_n(\mathcal{L})$. Gentry, Peikert, and Vaikuntanathan obtained the first portion following relation in [7]

$$\frac{1}{\lambda_1^\infty(\hat{\mathcal{L}})} \leq \tilde{bl}(\mathcal{L}) \leq \lambda_n(\mathcal{L}).$$

As a result, they gave a new bound on the smoothing parameter relative to the lattice quantity $\tilde{bl}(\mathcal{L})$:

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(2n(1+\frac{1}{\varepsilon})\right)}{\pi}}\tilde{bl}(\mathcal{L}). \tag{3}$$

These mean that the bound (2) is the best one and (3) implies (1).

In a recent work [5], Chung, Dadush, Liu and Peikert initiated a study of the complexity of approximating the smoothing parameter to within a factor. They provided two novel and nearly tight characterizations of the magnitude of discrete Gaussian sums over lattices.

In the second part of the paper, we work on improving the current bounds for smoothing parameter directly. The goal is to getting closer to the exact value of the smoothing parameter of a lattice. Under some natural conditions we obtain two better bounds. The first one is for the case of $\mathcal{L} = \mathbb{Z}$. Given $\varepsilon \leq \rho_{1,\mathbf{0}}(\mathbb{Z}) - 1$, we have

$$\eta_\varepsilon(\mathbb{Z}) \leq \sqrt{\frac{\ln\left(\frac{\varepsilon}{44}+\frac{2}{\varepsilon}\right)}{\pi}}.$$

Our second result in the second part of the paper is to improve (3) for general n-dimensional lattice ($n \geq 2$) by proving

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(n-1+\frac{2n}{\varepsilon}\right)}{\pi}}\tilde{bl}(\mathcal{L}).$$

The paper is organized as follows. We introduce some background materials and discuss several important results of Banaszczyk in section 2. Section 3 is devoted to new upper bounds of smoothing parameter of lattices. The last section is the conclusion.

2 Fourier Transform and Discrete Gaussian Measures on Lattices

Recall that we used the Gaussian function $\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{s^2}}$ to define discrete Gaussian measure over a lattice $\mathcal{L}$. For any countable set $S \subset \mathbb{R}^n$, we denote $\rho_{s,\mathbf{c}}(S) = \sum_{\mathbf{x}\in S}\rho_{s,\mathbf{c}}(\mathbf{x})$.

For any vector $\mathbf{c} \in \mathbb{R}^n$, real $s > 0$, a discrete Gaussian distribution over $\mathcal{L}$ is defined as:

$$\forall \mathbf{x} \in \mathcal{L}, \quad D_{s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(L)}.$$

When $s = 1$ and/or $\mathbf{c} = \mathbf{0}$, the corresponding subscripts for $D_{s,\mathbf{c}}$ and $\rho_{s,\mathbf{c}}$ are omitted.

The Fourier transform of a rapidly decreasing smooth function $f : \mathbb{R}^n \to \mathbb{C}$ [1] is defined to be

$$\hat{f}(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) e^{-2\pi i \langle \mathbf{x}, \mathbf{y} \rangle} d\mathbf{x}.$$

Several relevant properties of the Fourier transform include

1. If $f(\mathbf{x}) = g(\mathbf{x} + \mathbf{v})$ for some function g and vector $\mathbf{v}$, then $\hat{f}(\mathbf{y}) = e^{2\pi i \langle \mathbf{y}, \mathbf{v} \rangle} \hat{g}(\mathbf{y})$.
2. If $f(\mathbf{x}) = e^{2\pi i \langle \mathbf{x}, \mathbf{v} \rangle} g(\mathbf{x})$ for some function g and vector $\mathbf{v}$, then $\hat{f}(\mathbf{y}) = \hat{g}(\mathbf{y} - \mathbf{v})$.
3. For the Gaussian function ρ, we have $\hat{\rho}(\mathbf{y}) = \rho(\mathbf{y}), \hat{\rho}_s(\mathbf{y}) = s^n \rho_{\frac{1}{s}}(\mathbf{y})$.
4. For any vector $\mathbf{v} \in \mathbb{R}^n$, $\rho(\mathcal{L} + \mathbf{v}) \leq \rho(\mathcal{L})$.

The following classical Poisson summation formula has been a useful tool in the theory of lattice. The proof of this formula can be found in [14].

Lemma 1. *For a rapidly decreasing smooth function f and an n-dimensional lattice $\mathcal{L} = \mathcal{L}(\mathbf{B}) \subset \mathbb{R}^n$,*

$$\sum_{\mathbf{x} \in \mathcal{L}} f(\mathbf{x}) = \frac{1}{\mathrm{vol}(\mathbb{R}^n / \mathcal{L})} \sum_{\mathbf{y} \in \hat{\mathcal{L}}} \hat{f}(\mathbf{y}),$$

where $\mathrm{vol}(\mathbb{R}^n / \mathcal{L}) = |\det(\mathbf{B})|$ *is the volume of the fundamental parallelepiped of $\mathcal{L}$.*

In the rest part of this section, we discuss some results of Banaszczyk [1, 2]. The next two lemmas have been widely used.

Lemma 2 ([1], Lemma 1.5)**.** *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Then for any $c > \frac{1}{\sqrt{2\pi}}$,*

$$\frac{\rho\big(\mathcal{L} \setminus \mathcal{B}(0, c\sqrt{n})\big)}{\rho(\mathcal{L})} < \big(c\sqrt{2\pi e}\ e^{-\pi c^2}\big)^n. \tag{4}$$

Furthermore, for $\mathbf{v} \in \mathbb{R}^n$,

$$\frac{\rho\big((\mathcal{L} + \mathbf{v}) \setminus \mathcal{B}(0, c\sqrt{n})\big)}{\rho(\mathcal{L})} < 2\big(c\sqrt{2\pi e}\ e^{-\pi c^2}\big)^n. \tag{5}$$

Here $\mathcal{B}(\mathbf{c}, r)$ denotes the ball in $\mathbb{R}^n$ centered at $\mathbf{c}$ and with radius r.

[1] This means that f and all its (partial) derivatives $D^\beta f$ are rapidly decreasing in the sense that $\sup_{\mathbf{x} \in \mathbb{R}^n} |\mathbf{x}^\alpha D^\beta f(\mathbf{x})| < \infty$ for every $\alpha, \beta \in \mathbb{N}^n$. Such a function is said to be in the Schwartz space.

Lemma 3 ([2], Lemma 2.4). *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $\mathbf{u} \in \mathbb{R}^n$ a vector. For any $t \geq 0$, we have*

$$\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ |x_k|\geq t}} \rho(\mathbf{x}) \leq 2e^{-\pi t^2}\rho(\mathcal{L}). \tag{6}$$

The result of this lemma implies

$$\rho\big((\mathcal{L}+\mathbf{u}) \setminus t\mathcal{B}^{(\infty)}\big) < 2ne^{-\pi t^2}\rho(\mathcal{L}).$$

where $\mathcal{B}^{(\infty)}$ is the unit ball of $\mathbb{R}^n$ (centered at the origin) in ℓ_∞ norm. This fact was used in [11] to prove the bound (2).

These lemmas were used to prove transference theorem for lattices [1, 2, 4]. Now they are playing a significant role in applying Gaussian measures in lattice-based cryptography.

It is remarked that in [17], Tian, Liu, and Xu presented an improvement of lemma 2 with a transparent proof. Their result states

Lemma 4 ([17], Theorem 3.1). *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Then for any $c > \frac{1}{\sqrt{2\pi}}$ and $\mathbf{v} \in \mathbb{R}^n$,*

$$\frac{\rho\big((\mathcal{L}+\mathbf{v}) \setminus \mathcal{B}(0, c\sqrt{n})\big)}{\rho(\mathcal{L})} < \big(c\sqrt{2\pi e}\ e^{-\pi c^2}\big)^n. \tag{7}$$

It is seen that the factor 2 is removed from (5).

Next, we would like to describe a proof of lemma 3 that is different from the original one given in [2]. We believe that this proof reveals some information that might be useful in improving the estimation for certain well structured lattices.

Proof of lemma 3

$$\begin{aligned}
\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ |x_k|\geq t}} e^{-\pi\|\mathbf{x}\|^2} &= e^{-\pi t^2}\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ |x_k|\geq t}} e^{-\pi(\|\mathbf{x}\|^2-t^2)} = e^{-\pi t^2}\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ |x_k|\geq t}} e^{-\pi((x_k^2-t^2)+\sum_{j\neq k} x_j^2)} \\
&= e^{-\pi t^2}\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ |x_k|\geq t}} e^{-2\pi t(|x_k|-t)}e^{-\pi((|x_k|-t)^2+\sum_{j\neq k} x_j^2)} \leq e^{-\pi t^2}\sum_{\substack{\mathbf{x}\in L+\mathbf{u}\\ |x_k|\geq t}} e^{-\pi((|x_k|-t)^2+\sum_{j\neq k} x_j^2)} \\
&= e^{-\pi t^2}\left(\sum_{\substack{\mathbf{x}\in\mathcal{L}+\mathbf{u}\\ x_k\geq t}} e^{-\pi((x_k-t)^2+\sum_{j\neq k} x_j^2)} + \sum_{\substack{\mathbf{x}\in L+\mathbf{u}\\ x_k\leq -t}} e^{-\pi((x_k+t)^2+\sum_{j\neq k} x_j^2)}\right) \\
&\leq e^{-\pi t^2}\left(\rho(\mathcal{L}+(\mathbf{u}-t\mathbf{e}_k)) + \rho(\mathcal{L}+(\mathbf{u}+t\mathbf{e}_k))\right) \leq 2e^{-\pi t^2}\rho(\mathcal{L}),
\end{aligned}$$

where $\mathbf{e}_k$ is the kth vector of the canonical basis of $\mathbb{R}^n$. □

In the last part of this section, we will illustrate a simple form of "uncertainty principle" for the Fourier transform on lattices. The classical uncertainty principle for continuous Fourier transform is the following inequality [15] with respect to a rapidly decreasing function $\phi : \mathbb{R} \to \mathbb{C}$:

$$\int_{-\infty}^{\infty} x^2 |\phi(x)|^2 dx \int_{-\infty}^{\infty} \xi^2 |\hat{\phi}(\xi)|^2 d\xi \geq \frac{1}{16\pi^2} \int_{-\infty}^{\infty} |\phi(x)|^2 dx \int_{-\infty}^{\infty} |\hat{\phi}(\xi)|^2 d\xi$$

If the function is of the form Ae^{-Bx^2}, then the uncertainty principle takes equality.

An uncertainty principle for finite Fourier transform was proposed by Donoho and Stark in [6], they proved that for a cyclic finite group G, if $\phi : G \to \mathbb{C}$ is a function, then

$$|\mathrm{supp}(\phi)| \cdot |\mathrm{supp}(\hat{\phi})| \geq |G|,$$

where $\mathrm{supp}(h)$ of a function h is its support. If the group is $G = \mathbb{Z}/p\mathbb{Z}$ for some prime number p, the Chebotarëv theorem (see [16]) gives a stronger version of the uncertainty principle

$$|\mathrm{supp}(\phi)| + |\mathrm{supp}(\hat{\phi})| \geq |G| + 1.$$

Inspired by the idea of Banaszczyk in his lemma 1.3 of [1], we can prove a simple version of the uncertainty principle for Gaussian functions on lattices.

Proposition 1. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $s > 0$. We have*

$$\sum_{\mathbf{x} \in \mathcal{L}} \frac{\|\mathbf{x}\|^2 \rho_s(\mathbf{x})}{\rho_s(\mathcal{L})} + s^4 \sum_{\mathbf{y} \in \hat{\mathcal{L}}} \frac{\|\mathbf{y}\|^2 \rho_{\frac{1}{s}}(\mathbf{y})}{\rho_{\frac{1}{s}}(\hat{\mathcal{L}})} = \frac{ns^2}{2\pi}.$$

Proof. Let us begin with the Poisson summation formula

$$\sum_{\mathbf{x} \in \mathcal{L}} \rho_s(\mathbf{x}) = \frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})} \sum_{\mathbf{y} \in \hat{\mathcal{L}}} \rho_{\frac{1}{s}}(\mathbf{y}).$$

Write $t = s^2$ and define the function $F : \mathbb{R} \to \mathbb{R}$ as

$$F(t) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_s(\mathbf{x}) = \sum_{\mathbf{x} \in \mathcal{L}} e^{\frac{-\pi \|\mathbf{x}\|^2}{t}}.$$

The Poisson summation formula yields another representation of the function $F(t)$

$$F(t) = \frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})} \sum_{\mathbf{y} \in \hat{\mathcal{L}}} \rho_{\frac{1}{s}}(\mathbf{y}) = \frac{\sqrt{t}^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})} \sum_{\mathbf{y} \in \hat{\mathcal{L}}} e^{-\pi t \|\mathbf{y}\|^2}.$$

Differentiating both forms with respect to t, we get equalities

$$\begin{aligned} F'(t) &= \frac{\pi}{t^2}\sum_{\mathbf{x}\in\mathcal{L}}\|\mathbf{x}\|^2 e^{\frac{-\pi\|\mathbf{x}\|^2}{t}} \\ &= \frac{n\sqrt{t}^{n-2}}{2\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}} e^{-\pi t\|\mathbf{y}\|^2} - \frac{\pi\sqrt{t}^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}}\|\mathbf{y}\|^2 e^{-\pi t\|\mathbf{y}\|^2}. \end{aligned}$$

I.e.,

$$\pi\sum_{\mathbf{x}\in\mathcal{L}}\|\mathbf{x}\|^2\rho_s(\mathbf{x}) + s^4\pi\frac{s^{n+4}}{2\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}}\|\mathbf{y}\|^2\rho_{\frac{1}{s}}(\mathbf{y}) = \frac{ns^{n+2}}{2\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}}\rho_{\frac{1}{s}}(\mathbf{y}).$$

Dividing both sides by $\frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}}\rho_{\frac{1}{s}}(\mathbf{y}) = \frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\rho_{\frac{1}{s}}(\hat{\mathcal{L}}) = \rho_s(\mathcal{L})$, we get what we wanted.

□

Remarks.

1. For a self-dual lattice $\mathcal{L}$, this proposition implies that the "uncertainty" $\sum_{\mathbf{x}\in\mathcal{L}}\frac{\|\mathbf{x}\|^2\rho(\mathbf{x})}{\rho(\mathcal{L})}$ can be precisely determined, i.e.,

$$\sum_{\mathbf{x}\in\mathcal{L}}\frac{\|\mathbf{x}\|^2\rho(\mathbf{x})}{\rho(\mathcal{L})} = \frac{n}{4\pi}.$$

2. A proof can also be obtained by following the nice approach from [1]. By setting a suitable function and taking second order partial derivatives, the following interesting relation may be obtained from the proof of lemma 1.3 of [1]

$$4\pi^2\sum_{\mathbf{x}\in\mathcal{L}}x_k^2\rho_s(\mathbf{x}) = \frac{s^n}{\mathrm{vol}(\mathbb{R}^n/\mathcal{L})}\sum_{\mathbf{y}\in\hat{\mathcal{L}}}\left(2\pi s^2 - 4\pi^2 s^4 y_k^2\right)\rho_{\frac{1}{s}}(\mathbf{y}).$$

3 New Bounds for the Smoothing Parameter

In this section, we shall state and prove our improvement of the upper bound of the smoothing parameter for lattices. We will first consider the one-dimensional case and then work on the general case.

3.1 Lattices of Integers

The one-dimensional case $\mathcal{L} = \mathbb{Z}$ is simpler but it is of great practical importance. For example, in discrete Gaussian sampling, one usually starts from $\mathbb{Z}$ and builds up things for higher dimensions by using tools such as convolution [10, 12, 13, 18].

Since $\mathbb{Z}$ is self-dual, so

$$\eta_\varepsilon(\mathbb{Z}) = \min\{s : \rho_{\frac{1}{s}}(\mathbb{Z}) \le 1 + \varepsilon\}.$$

Notice that $\rho_{\frac{1}{s}}(\mathbb{Z}) = 1 + 2\sum_{j=1}^{\infty} e^{-\pi s^2 j^2} > 1 + 2e^{-\pi s^2}$. This implies that for any $\varepsilon \in (0,1)$ and $s \le \sqrt{\frac{\ln \frac{2}{\varepsilon}}{\pi}}$, the inequality $\rho_{\frac{1}{s}}(\mathbb{Z}) > 1 + \varepsilon$ holds. Thus

$$\eta_\varepsilon(\mathbb{Z}) > \sqrt{\frac{\ln \frac{2}{\varepsilon}}{\pi}}.$$

One the other hand, any of the general bounds (1), (2), and (3) would give

$$\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln(2 + \frac{2}{\varepsilon})}{\pi}}.$$

Now we have the current bounds for $\eta_\varepsilon(\mathbb{Z})$:

$$\sqrt{\frac{\ln \frac{2}{\varepsilon}}{\pi}} < \eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln(2 + \frac{2}{\varepsilon})}{\pi}}. \tag{8}$$

It is an interesting question whether we can get closer to the exact value of $\eta_\varepsilon(\mathbb{Z})$. The purpose of this subsection is to improve the upper bound in (8). First, we should note that by the Poisson summation formula,

$$\rho_s(\mathbb{Z}) = s\rho_{\frac{1}{s}}(\mathbb{Z}).$$

So we may assume $s \ge 1$ and assume $\varepsilon \le \rho(\mathbb{Z}) - 1 < 0.086435$.

The next result says that we can replace the summand 2 inside the natural logarithm in the upper bound of (8) by the "infinitesimal" $\frac{\varepsilon}{44}$.

Theorem 1. *Assume that* $\varepsilon < 0.086435$*, then*

$$\eta_\varepsilon(\mathbb{Z}) \le \sqrt{\frac{\ln(\frac{\varepsilon}{44} + \frac{2}{\varepsilon})}{\pi}}. \tag{9}$$

Proof. Given $\varepsilon > 0$, consider the polynomial

$$p(x) = x^3 + 22x - 11\varepsilon.$$

Let $\alpha = \frac{44\varepsilon}{88+\varepsilon^2}$. It is easy to check that $p(\alpha) < 0$. Since $p'(x) > 0$, so $p(x)$ has only one real zero. From the fact $\lim_{x\to+\infty} p(x) = +\infty$, we see that $p(\beta) < 0$ for any $\beta \le \alpha$.

Let $s \geq \sqrt{\frac{\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon})}{\pi}}$. We have $e^{-\pi s^2} \leq \alpha$ and hence $p(e^{-\pi s^2}) < 0$. In other words, we have

$$2\left(e^{-\pi s^2} + \frac{1}{22}e^{-3\pi s^2}\right) < \varepsilon.$$

We also observe that $e^{-\pi} < \frac{1}{22} - \frac{1}{5000}$. Therefore

$$\begin{aligned}
\rho_{\frac{1}{s}}(\mathbb{Z}) &= 1 + 2(e^{-\pi s^2} + e^{-4\pi s^2} + e^{-9\pi s^2} + e^{-25\pi s^2} + e^{-36\pi s^2} + \cdots) \\
&\leq 1 + 2(e^{-\pi s^2} + e^{-\pi}e^{-3\pi s^2} + 2e^{-9\pi s^2}) \\
&\leq 1 + 2\left(e^{-\pi s^2} + \frac{1}{22}e^{-3\pi s^2} + 2e^{-9\pi s^2} - \frac{1}{5000}e^{-3\pi s^2}\right) \\
&\leq 1 + 2\left(e^{-\pi s^2} + \frac{1}{22}e^{-3\pi s^2}\right) < 1 + \varepsilon.
\end{aligned}$$

This shows that $\eta_\varepsilon(\mathbb{Z}) \leq \sqrt{\frac{\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon})}{\pi}}$. □

Remarks.

1. This bound is much more closer to the exact value of $\eta_\varepsilon(\mathbb{Z})$. Under the assumption of the theorem, we have

$$\sqrt{\frac{\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon})}{\pi}} - \sqrt{\frac{\ln\frac{2}{\varepsilon}}{\pi}} = \frac{\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon}) - \ln(\frac{2}{\varepsilon})}{\sqrt{\pi\ln(\frac{\varepsilon}{44}+\frac{2}{\varepsilon})} + \sqrt{\pi\ln\frac{2}{\varepsilon}}} < \frac{\varepsilon^2}{528}.$$

   So the new bound is within $\frac{\varepsilon^2}{528}$ of the precise value of $\eta_\varepsilon(\mathbb{Z})$.

2. Further non-essential improvement of the bound can be achieved by some careful manipulations.

3.2 General Lattices

In this subsection, we discuss the smoothing parameter for a general n-dimensional lattice with $n \geq 2$. Our aim is to prove an upper bound that is smaller than (3).

Let $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n)$ be an arbitrary basis of $\mathcal{L}$. Its Gram-Schmidt orthogonal basis $\mathbf{B}^* = (\mathbf{b}^*_\mathbf{1}, \ldots, \mathbf{b}^*_\mathbf{n})$ satisfies the relation

$$\mathbf{B} = \mathbf{B}^*\mathbf{R}$$

where $\mathbf{R} = (\mu_{ij})_{1\leq i,j\leq n} \in \mathbb{R}^{n\times n}$ is an upper triangle matrix with $\mu_{ii} = 1$ for all $i = 1, \cdots, n$.

In [7], Gentry, Peikert, and Vaikuntanathan obtained the following bound on the smoothing parameter

$$\eta_\varepsilon(\mathcal{L}) \le \sqrt{\frac{\ln\left(2n + \frac{2n}{\varepsilon}\right)}{\pi}} \max_i \|\mathbf{b}_i^*\|.$$

The main purpose of this subsection is to prove a stronger result, namely

$$\eta_\varepsilon(\mathcal{L}) \le \sqrt{\frac{\ln\left(n - 1 + \frac{2n}{\varepsilon}\right)}{\pi}} \max_i \|\mathbf{b}_i^*\|,$$

for $\varepsilon < \min\{1, 0.086435n\}$.

To this end, we first establish an inequality.

Lemma 5. *Let $c > 1$ and $0 \le x \le \frac{6nc}{n+1+2(n-2)c}(c-1)$. Then*

$$\left(1 + \frac{x}{cn}\right)^n \le 1 + x.$$

Proof.

$$\begin{aligned}
\left(1 + \frac{x}{cn}\right)^n &= 1 + \frac{x}{c} + \frac{1}{2}\frac{n-1}{n}\left(\frac{x}{c}\right)^2 + \frac{1}{6}\frac{n-1}{n}\frac{n-2}{n}\left(\frac{x}{c}\right)^3 + \frac{1}{24}\frac{n-1}{n}\frac{n-2}{n}\frac{n-3}{n}\left(\frac{x}{c}\right)^4 + \cdots \\
&\le 1 + \frac{x}{c} + \frac{n-1}{2n}\left(\frac{x}{c}\right)^2 \left(1 + \frac{n-2}{3n}\left(\frac{x}{c}\right) + \left(\frac{n-2}{3n}\left(\frac{x}{c}\right)\right)^2 + \cdots\right) \\
&\le 1 + \frac{x}{c} + \frac{n-1}{2n}\left(\frac{x}{c}\right)^2 \frac{1}{1 - \frac{(n-2)x}{3nc}} = 1 + \frac{x}{c}\left(1 + \frac{3(n-1)x}{6nc - 2(n-2)x}\right) \\
&\le 1 + x.
\end{aligned}$$

□

We shall also use the fact that for any vector $\mathbf{v} \in \mathbb{R}^n$,

$$\rho(\mathcal{L} + \mathbf{v}) \le \rho(\mathcal{L}).$$

Now let us state our main result.

Theorem 2. *If $\varepsilon < \min\{1, 0.086435n\}$, then*

$$\eta_\varepsilon(L) \le \sqrt{\frac{\ln\left((n-1) + \frac{2n}{\varepsilon}\right)}{\pi}} \max_i \|\mathbf{b}_i^*\|.$$

Proof. To prove this, let $\mathbf{x} \in \mathcal{L}$. Then there are integers $x_1, \cdots, x_n$ such that

$$\begin{aligned}
\mathbf{x} &= x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n \\
&= (x_1 + \mu_{1,2}x_2 + \cdots + \mu_{1,n}x_n)\mathbf{b}_1^* + \cdots + (x_{n-1} + \mu_{n-1,n}x_n)\mathbf{b}_{n-1}^* + x_n\mathbf{b}_n^* \\
&= (x_1 + \mu(x_2, \cdots, x_n))\mathbf{b}_1^* + \cdots + (x_{n-1} + \mu(x_n))\mathbf{b}_{n-1}^* + x_n\mathbf{b}_n^*.
\end{aligned}$$

Let $s_i = \frac{s}{\|\mathbf{b}_i^*\|}$. We have

$$\rho_s(\mathbf{x}) = \rho_{s_n}(x_n)\rho_{s_{n-1}}(x_{n-1} + \mu(x_n)) \cdots \rho_{s_1}(x_1 + \mu(x_2 \cdots, x_n)).$$

Therefore

$$\begin{aligned}
\rho_s(\mathcal{L}) &= \sum_{x_1, \cdots, x_n \in \mathbb{Z}} \rho_{s_n}(x_n)\rho_{s_{n-1}}(x_{n-1} + \mu(x_n)) \cdots \rho_{s_1}(x_1 + \mu(x_2 \cdots, x_n)) \\
&= \sum_{x_2, \cdots, x_n \in \mathbb{Z}} \rho_{s_n}(x_n) \cdots \rho_{s_2}(x_2 + \mu(x_3 \cdots, x_n)) \sum_{x_1 \in \mathbb{Z}} \rho_{s_1}(x_1 + \mu(x_2 \cdots, x_n)) \\
&= \sum_{x_2, \cdots, x_n \in \mathbb{Z}} \rho_{s_n}(x_n) \cdots \rho_{s_2}(x_2 + \mu(x_3 \cdots, x_n))\rho_{s_1}(\mathbb{Z} + \mu(x_2 \cdots, x_n)) \\
&\leq \sum_{x_2, \cdots, x_n \in \mathbb{Z}} \rho_{s_n}(x_n)\rho_{s_{n-1}}(x_{n-1} + \mu(x_n)) \cdots \rho_2(x_2 + \mu(x_3 \cdots, x_n))\rho_{s_1}(\mathbb{Z}) \\
&\leq \cdots \leq \rho_{s_n}(\mathbb{Z})\rho_{s_{n-1}}(\mathbb{Z}) \cdots \rho_{s_1}(\mathbb{Z}).
\end{aligned}$$

Using Poisson summation formula, we get

$$\rho_{\frac{1}{s}}(\hat{\mathcal{L}}) \leq \rho_{\frac{1}{s_1}}(\mathbb{Z})\rho_{\frac{1}{s_2}}(\mathbb{Z}) \cdots \rho_{\frac{1}{s_n}}(\mathbb{Z}).$$

Let k_0 be such that $\|\mathbf{b}_{k_0}^*\| = \max_i \|\mathbf{b}_i^*\|$. We have

$$\rho_{\frac{1}{s}}(\hat{\mathcal{L}}) \leq \left(\rho_{\frac{\|\mathbf{b}_{k_0}^*\|}{s}}(\mathbb{Z})\right)^n.$$

Now consider the equation

$$X^2 - \left(1 + \frac{n-2}{3n}\varepsilon\right)X - \frac{n+1}{6n}\varepsilon = 0.$$

This equation has a negative root, so it must have a root $c > 1$.

Thus

$$\varepsilon = \frac{6nc}{n+1+2(n-2)c}(c-1).$$

By lemma 5, we see that

$$\left(1 + \frac{\varepsilon}{cn}\right)^n \leq 1 + \varepsilon. \tag{10}$$

Note that

$$\begin{aligned}
\frac{\frac{\varepsilon}{cn}}{44}+\frac{2}{\frac{\varepsilon}{cn}} &= \frac{3(c-1)}{22(n+1+2(n-2)c)}+\frac{(n+1+2(n-2)c)}{3c}+\frac{2n}{\varepsilon} \\
&= \frac{3(c-1)}{22(n+1+2(n-2)c)}-\frac{(n+1)(c-1)}{3c}+(n-1)+\frac{2n}{\varepsilon} \\
&\leq (n-1)+\frac{2n}{\varepsilon}.
\end{aligned}$$

If $s \geq \sqrt{\frac{\ln\left((n-1)+\frac{2n}{\varepsilon}\right)}{\pi}}\|\mathbf{b}_{k_0}^*\|$, then

$$s_{k_0}=\frac{s}{\|\mathbf{b}_{k_0}^*\|} \geq \sqrt{\frac{\ln\left((n-1)+\frac{2n}{\varepsilon}\right)}{\pi}} \geq \sqrt{\frac{\ln\left(\frac{\frac{\varepsilon}{cn}}{44}+\frac{2}{\frac{\varepsilon}{cn}}\right)}{\pi}}.$$

Since $\varepsilon < 0.086435n$, so $\frac{\varepsilon}{cn} < 0.086435$. Therefore, by theorem 1, we conclude that $\rho_{\frac{\|\mathbf{b}_{k_0}^*\|}{s}}(\mathbb{Z}) \leq 1+\frac{\varepsilon}{cn}$ and hence

$$\rho_{\frac{1}{s}}(\hat{\mathcal{L}}) \leq \left(1+\frac{\varepsilon}{cn}\right)^n < 1+\varepsilon.$$

□

4 Conclusion

This paper concerns inequalities and parameter for discrete Gaussian measures on lattices. The first topic of the paper is about an analysis of several seminal results of Banaszczyk. Some different approaches are suggested, and a simple version of uncertainty principle is illustrated.

In the second part of the paper we prove two new bounds for the smoothing parameter of lattices. Under the natural assumption that $\varepsilon < \rho(\mathbb{Z}-\{0\})$, the following is proved

$$\eta_\varepsilon(\mathbb{Z}) \leq \sqrt{\frac{\ln\left(\frac{\varepsilon}{44}+\frac{2}{\varepsilon}\right)}{\pi}}.$$

This bound is much more closer to the exact value of $\eta_\varepsilon(\mathbb{Z})$ with an error at most $\frac{\varepsilon^2}{528}$. For a general lattice $\mathcal{L}$ of high dimension, we obtain that

$$\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{\ln\left(n-1+\frac{2n}{\varepsilon}\right)}{\pi}}\tilde{bl}(\mathcal{L}).$$

This improves the bound from [7].

References

[1] Wojciech Banaszczyk, New bounds in some transference theorems in the geometry of numbers, *Mathematische Annalen*, 296(4):625-635, 1993.

[2] Wojciech Banaszczyk, Inequalites for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$, *Discrete & Computational Geometry*, 13:217-231, 1995.

[3] Wojciech Banaszczyk, Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ II: Application of k-convexity, *Discrete & Computational Geometry*, 16:305–311, 1996.

[4] J. Cai, A new transference theorem in the geometry of numbers and new bounds for Ajtai's connection factor, *Discrete Applied Mathematics* 126(1):9-31, 2003.

[5] K. Chung, D. Dadush, F. Liu, and C. Peikert, On the Lattice Smoothing Parameter Problem, *IEEE Conference on Computational Complexity*, 2013, pp 230–241.

[6] D. Donoho and P. Stark, Uncertainty principles and signal recovery, *SIAM J. of Appl. Math.*, 49(1989), 906–931.

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

[8] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems: a cryptographic perspective, *Kluwer Academic Publishers*, 2002.

[9] D. Micciancio and O. Regev, Worst-case to average-case reductions based on Gaussian measures, *SIAM J. Comput.*, 37(1):267–302, 2007.

[10] D. Micciancio and M. Walter, Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time, *Proc. CRYPTO 2017*, pp 455-485, 2017.

[11] C. Peikert, Limits on the hardness of lattice problems in ℓ_p-norms, *In IEEE Conference on Computational Complexity*, pp 333-346, 2007.

[12] C Peikert, An efficient and parallel Gaussian sampler for lattices *Proc. CRYPTO 2010*, pp. 80-97, 2010.

[13] Pöppelmann T, Ducas L, Güneysu T. Enhanced lattice-based signatures on reconfigurable hardware, *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 353-370, 2014.

[14] J-P. Serre, A Course in Arithmetic, *GTM 7, Spring*, 1977.

[15] E. Stein and R. Shakarchi, Fourier Analysis–An Introduction, *Princeton University Press*, 2003.

[16] T. Tao, An uncertainty principle for cyclic groups of prime order, *http://xxx.arxiv.cornell.edu/pdf/math.CA/0308286*

[17] C. Tian, M. Liu, and G. Xu, Measure Inequalities and the Transference Theorem in the Geometry of Numbers, *Proceedings of Amer. Math. Soc.*, 142(2014) 47-57.

[18] Z. Zheng, X. Wang, G. Xu, and C. Zhao, Error Estimation of Practical Convolution Discrete Gaussian Sampling with Rejection Sampling, *https://eprint.iacr.org/2018/309*, 2018.