New Transference Theorems on Lattices Possessing n^{ϵ}-unique Shortest Vectors

Wei Wei[1], Chengliang Tian[2] and Xiaoyun Wang[3]

[1] Institute for Advanced Study
Tsinghua University Beijing, 100084, P.R. China.
Email: wei-wei08@mails.tsinghua.edu.cn
[2] Key Lab of Cryptologic Technology and Information Security
Shandong University Jinan, 250100, P.R. China.
Email: chengliangtian@mail.sdu.edu.cn
[3] Institute for Advanced Study
Tsinghua University Beijing, 100084, P.R. China.
Email: xiaoyunwang@mail.tsinghua.edu.cn

Abstract. We prove three optimal transference theorems on lattices possessing n^{ϵ}-unique shortest vectors which relate to the successive minima, the covering radius and the minimal length of generating vectors respectively. The theorems result in reductions between $\mathrm{GapSVP}_{\gamma'}$ and $\mathrm{GapSIVP}_{\gamma}$ for this class of lattices. Furthermore, we prove a new transference theorem giving an optimal lower bound relating the successive minima of a lattice with its dual. As an application, we compare the respective advantages of current upper bounds on the smoothing parameter of discrete Gaussian measures over lattices and show a more appropriate bound for lattices whose duals possess $\sqrt{n}$-unique shortest vectors.

Key words: Transference theorem, Reduction, Gaussian measures, Smoothing parameter

1 Introduction

Transference theorems are classical problems in the geometry of numbers [12, 22]. Usually, they reflect relationships of the successive minima associated with the primal and dual lattices. Moreover, transference theorems relating to other quantities such as the covering radius and the minimal length of generating vectors are considered as well. There are some important applications to computational complexity theory and lattice-based cryptography. Transference theorems are applied to improve the connection factor in the worst-case to average-case reductions [10, 23] which were first proposed by Ajtai [2] and have been outperformed by [14]. They also play a significant role in the dimension preserving reduction from CVP (closest vector problem) to SIVP (shortest independent vectors problem) [24]. As a consequence of transference theorems, the references [9, 18] showed that the approximating problems including SVP (shortest vector problem), SIVP and SBP (shortest basis problem) within a factor of $O(n)$ can not be NP-hard under Karp-reductions unless NP=coNP, and the factor has been improved to $O(\sqrt{n})$ by [1] for SVP. Besides, they are also used to bound the operation numbers in each recursive step in the computation of CVP [8].

An n-dimensional lattice $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \text{ for } 1 \leq i \leq n\}$ is a discrete additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^n$.[4] The sequence of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a lattice basis and it is represented conveniently as a matrix $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ with the basis vectors as columns. The family of all n-dimensional lattices in $\mathbb{R}^n$ is denoted $\mathcal{L}_n$. The determinant $\det(L)$ is the volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$, where $\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : 0 \leq x_i < 1\}$. The dual lattice of L is defined to

[4] In fact, this is the definition of *full-rank* lattice, which is the case we consider in this paper.

be $L^* = \{\mathbf{x} \in \mathrm{span}(L) : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for each } \mathbf{y} \in L\}$, where $\langle \mathbf{x}, \mathbf{y} \rangle$ is the canonical inner product in $\mathbb{R}^n$.

For any lattice $L \in \mathcal{L}_n$ and any $\mathbf{0}$-symmetric convex body U, define the ith successive minimum of L with respect to U as $\lambda_i(L, U) = \min\{r > 0 : \dim(\mathrm{span}(L \cap rU)) \geq i\}$ for $1 \leq i \leq n$. In this paper we mainly concern the case $U = \mathcal{B}_p^n$ and write $\lambda_i^{(p)}(L)$ instead of $\lambda_i(L, \mathcal{B}_p^n)$ for simplicity, where $\mathcal{B}_p^n$ is the closed unit ball of $\mathbb{R}^n$ in l_p norm for $p \in [1, \infty]$. Specially, we regard p as 2 when omitted. We define that L possesses an n^ϵ-unique shortest vector, if $\lambda_2(L) > n^\epsilon \lambda_1(L)$. The covering radius of L with respect to U is defined as $\mu(L, U) = \min\{r > 0 : L + rU = \mathbb{R}^n\}$. A deep hole is a point $\mathbf{t} \in \mathrm{span}(\mathbf{B})$ at distance $d_U(\mathbf{t}, L) = \mu(L, U)$, where $d_U(\mathbf{t}, L) = \inf_{\mathbf{v} \in L} \|\mathbf{t} - \mathbf{v}\|_U = \inf_{\mathbf{v} \in L} \inf\{r \geq 0 : \mathbf{t} - \mathbf{v} \in rU\}$. The usual definition of the covering radius, denoted $\mu(L)$, regards U as $\mathcal{B}_2^n$ which is also the case considered in this paper. One more quantity $w_L(U) = \min_{\mathbf{v} \in L^* \setminus \{\mathbf{0}\}} (\max_{\mathbf{u} \in U} \langle \mathbf{u}, \mathbf{v} \rangle - \min_{\mathbf{u} \in U} \langle \mathbf{u}, \mathbf{v} \rangle)$ is called the lattice width of U. It's clear that $w_L(\mathcal{B}_2^n) = 2\lambda_1(L^*)$. The upper bound on $\mu(L, U) \cdot w_L(U)$ is investigated in the flatness theorem [7] which is a classical problem in the geometry of numbers and also has important applications to integer programming [13,17]. Another lattice quantity $g(L)$ is the minimal length of generating vectors which is defined as the minimum r such that the ball $r\mathcal{B}_2^n$ contains a set of basis of L. More generally, define $g_i(L)$ to be the minimum r such that the sublattice generated by $L \cap r\mathcal{B}_2^n$ contains an i-dimensional sublattice L' satisfying $L' = L \cap \mathrm{span}(L')$ for $1 \leq i \leq n$. Obviously, $g_i(L) \geq \lambda_i(L)$ and $g_n(L) = g(L)$.

For any n-dimensional lattice L, determining the upper bound on $\max_{1 \leq i \leq n} \lambda_i(L)\lambda_{n-i+1}(L^*)$ known as the transference theorem has experienced a long process from the initial superexponential results to polynomial bound. Lagarias et al. [18] gave the first polynomial bound of $n^2/6$ for $n \geq 7$ using the Korkin-Zolotarev reduced basis. Based on Gaussian measures and their Fourier transforms, Banaszczyk [4] proved the optimal bound $\max_{1 \leq i \leq n} \lambda_i(L)\lambda_{n-i+1}(L^*) \leq n$ for any positive integer n. In the same reference, a transference theorem relating the successive minimum of a lattice with the covering radius of its dual was given which is $\lambda_1(L^*)\mu(L) \leq n/2$ for all positive integer n. In a subsequent work [10], Cai generalized the transference theorem and proved $\max_{1 \leq i \leq n} \lambda_i(L^*)g_{n-i+1}(L) \leq cn$ for some constant c. Meanwhile, in order to improve Ajtai's connection factor in the worst-case to average-case reduction, Cai proved an upper bound $O(n^{1-\epsilon})$ on $\lambda_1(L^*)g(L)$ for lattices possessing n^ϵ-unique shortest vectors when $0 < \epsilon \leq 1/2$. It yields a stronger upper bound on $\lambda_1(L^*)\lambda_n(L)$ consequently. However, our observations reveal that transference theorems on lattices possessing n^ϵ-unique shortest vectors don't reach the optimal bounds.

Since the cryptographic lattices often possess gaps between λ_1 and λ_2, it's of more practical significance to study transference theorems on lattices with gaps especially possessing n^ϵ-unique shortest vectors. In [3], Ajtai and Dwork constructed the first provable lattice-based cryptosystem whose security is based on the worst-case hardness of uSVP$_\gamma$ (SVP for lattices with $\lambda_2 > \gamma\lambda_1$). Additionally, for the LWE-based cryptosystem [28], the gap between λ_1 and λ_2 in the embedding lattice is discussed in [20] as well. Moreover, uSVP$_\gamma$ as an increasingly concerned problem used in lattice-based cryptography, its hardness, polynomial time algorithm for $\gamma = O(2^{n/4})$ and the relevant embedding technique are investigated in [19, 21]. The NTRU cryptosystem is the most efficient lattice-based encryption scheme up until now and the reference [16] pointed out that there is a gap between λ_N and λ_{N+1} in NTRU lattice of dimension $2N$. Therefore, it's deserved to study transference theorems on lattices with gaps.

In this paper, we mainly study transference theorems on lattices possessing n^ϵ-unique shortest vectors. First we prove $\lambda_1(L^*)\mu(L) \leq 1/2 + n^{1-\epsilon}$ for all positive integer n. It yields consequently $\lambda_1(L^*)\lambda_n(L) \leq 1 + 2n^{1-\epsilon}$ which improves the result in [10] when $\epsilon \in [1/2, 3/2]$. Meanwhile, we give

a transference theorem $\lambda_1(L^*)g(L) \leq 1 + 4n^{1-\epsilon}$ for any $\epsilon > 0$. Using the improvements, for this class of lattices, there exist polynomial time reductions between $\text{GapSVP}_{\gamma'}$ and GapSIVP_{γ}.

Furthermore, we notice that nearly all transference theorems considered in current literature are about upper bounds on some quantities relating a lattice with its dual. It is obvious that $\lambda_1(L^*)\lambda_n(L) \geq 1$, but for generic l_p norm the lower bound on $\lambda_1^{(p)}(L^*)\lambda_n^{(q)}(L)$ is not clear. Our second contribution is to give a lower bound on the quantity $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n)$, where $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n) = \inf_{L\in\mathcal{L}_n} \min_{1\leq i\leq n} \lambda_i^{(p)}(L)\lambda_{n-i+1}^{(q)}(L^*)$ for any $p,\ q \in [1,\infty]$. As an application, we analyze the current upper bounds on the smoothing parameter of discrete Gaussian measures over lattices and give a more appropriate bound for lattices whose duals possess $\sqrt{n}$-unique shortest vectors.

The rest of this paper is organized as follows: Section 2 reviews basic notations and backgrounds. In Section 3 we prove the optimal transference theorems on lattices possessing n^{ϵ}-unique shortest vectors, and give the reductions between $\text{GapSVP}_{\gamma'}$ and GapSIVP_{γ} for this class of lattices. In Section 4, we show a transference theorem giving the lower bound on $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n)$ and some investigations of upper bounds on the smoothing parameter of discrete Gaussian measures over lattices. Conclusions are given in Section 5.

2 Preliminaries

2.1 Notations and Backgrounds

The real numbers and integers are denoted by $\mathbb{R}$ and $\mathbb{Z}$ respectively. Vectors are represented as bold lower-case letters, e.g. $\mathbf{x}$. For a vector $\mathbf{x}$, the ith coordinate is denoted by x_i. The inner product between $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$.

A norm $\|\cdot\|$ is a nonnegative real-valued function on $\mathbb{R}^n$ that satisfies the following: $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0$, $\|\alpha\mathbf{x}\| = |\alpha|\|\mathbf{x}\|$ for any scalar $\alpha \in \mathbb{R}$, and $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$ for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. It induces a corresponding distance function $\text{dist}(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|$. The l_p norm of $\mathbf{x}$ is $\|\mathbf{x}\|_p = (\sum_{i=1}^n |x_i|^p)^{1/p}$ for any $p \in [1,\infty)$ and the l_∞ norm is $\|\mathbf{x}\|_\infty = \max_{1\leq i\leq n} |x_i|$. We mean $p = 2$ when omitted. For any $\mathbf{x},\ \mathbf{y} \in \mathbb{R}^n$, the Hölder's inequality shows, if $1/p + 1/q = 1$, $p,\ q \in [1,\infty]$, then $\sum_{i=1}^n |x_i y_i| \leq \|\mathbf{x}\|_p \cdot \|\mathbf{y}\|_q$. We mean $1/p = 0$ ($1/q = 0$, respectively) when $p = \infty$ ($q = \infty$).

The following definition shows a straightforward way to get a basis of the dual lattice from a given primal lattice basis.

Definition 2.1. *For a basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a lattice $L \in \mathcal{L}_n$, its dual basis is defined as $\mathbf{D} = [\mathbf{d}_1, \ldots, \mathbf{d}_n]$ which satisfies $\langle \mathbf{b}_i, \mathbf{d}_j \rangle = \delta_{ij}$, where δ_{ij} $(1 \leq i, j \leq n)$ denotes the Kronecker symbol.*

For a lattice L, the Gram-Schmidt minimum is defined as,

Definition 2.2 ([14]). *For any lattice $L \in \mathcal{L}_n$, the* Gram-Schmidt minimum *is defined as*

$$\widetilde{bl}(L) = \min_{\mathbf{B}} \| \widetilde{\mathbf{B}} \| = \min_{\mathbf{B}} \max_{1\leq i\leq n} \| \widetilde{\mathbf{b}}_i \|,$$

where $\widetilde{\mathbf{B}} = [\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n]$ denotes the Gram-Schmidt orthogonalization of $\mathbf{B}$ and the minimum is taken over all bases $\mathbf{B}$ of L.

The following lemma states that a basis within a $\sqrt{n}/2$ enlargement in size can be computed in polynomial time from any set of n linearly independent lattice vectors.

Lemma 2.3 ([11]). *Let $s_1, \ldots, s_n$ be any linearly independent vectors in a lattice $L = \mathcal{L}(b_1, \ldots, b_n)$ with $\|s_i\| \leq M$. Then a basis $r_1, \ldots, r_n$ can be computed in polynomial time such that $\|\widetilde{r_i}\| \leq \|\widetilde{s_i}\|$ and $\|r_i\| \leq \max\{1, \sqrt{n}/2\}M$.*

We give precise definitions for some computational lattice problems considered in this paper, which are of great importance and widely studied.

Definition 2.4 ($\mathbf{SVP}_\gamma$). *Given an n-dimensional lattice $L \subseteq \mathbb{Z}^n$, find a nonzero vector $\mathbf{v} \in L$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(L)$.*

Definition 2.5 ($\mathbf{GapSVP}_\gamma$). *Given an n-dimensional lattice $L \subseteq \mathbb{Z}^n$ and a parameter $d > 0$. If $\lambda_1(L) \leq d$, output* Yes *instances. If $\lambda_1(L) > \gamma \cdot d$, output* NO *instances.*

Definition 2.6 ($\mathbf{SIVP}_\gamma$). *Given an n-dimensional lattice $L \subseteq \mathbb{Z}^n$, find a set of n linearly independent vector $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ in L such that $\max_{1 \leq i \leq n} \|\mathbf{v}_i\| \leq \gamma \cdot \lambda_n(L)$.*

Definition 2.7 ($\mathbf{GapSIVP}_\gamma$). *Given an n-dimensional lattice $L \subseteq \mathbb{Z}^n$ and a parameter $d > 0$. If $\lambda_n(L) \leq d$, output* Yes *instances. If $\lambda_n(L) > \gamma \cdot d$, output* NO *instances.*

2.2 Gaussian Measures and Fourier Transform

Gaussian measures over lattices and their Fourier transforms are main tools to prove the existing transference theorems [4, 5, 10]. Meanwhile, Gaussian measures are also used to construct a new technique to sample random points in worst-case to average-case reductions [14, 25, 27]. Our transference theorems also utilize Gaussian measures and their Fourier transforms, combining some new observations of geometrical properties of lattices with gaps.

For any vectors $\mathbf{c}, \mathbf{x} \in \mathbb{R}^n$ and any $s > 0$, let

$$\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\|\mathbf{x}-\mathbf{c}\|^2/s^2}$$

be a Gaussian function centered at $\mathbf{c}$ scaled by a parameter s. We assume s and $\mathbf{c}$ are taken to be 1 and $\mathbf{0}$ respectively when omitted. We write $\rho_{s,\mathbf{c}}(A) = \sum_{\mathbf{x}\in A} \rho_{s,\mathbf{c}}(\mathbf{x})$ for any countable set A.

For any vector $\mathbf{c}$, real $s > 0$, and lattice L, define the Gaussian distribution $D_{L,s,\mathbf{c}}$ over L as

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

The Fourier transform of D_L is

$$\widehat{D_L}(\mathbf{y}) = \int_{\mathbf{x}\in\mathbb{R}^n} e^{2\pi \mathrm{i}\langle \mathbf{y},\mathbf{x}\rangle} dD_L = \sum_{\mathbf{v}\in L} e^{2\pi \mathrm{i}\langle \mathbf{y},\mathbf{v}\rangle} D_L(\mathbf{v}) = \frac{\sum_{\mathbf{v}\in L} e^{2\pi \mathrm{i}\langle \mathbf{y},\mathbf{v}\rangle} e^{-\pi\|\mathbf{v}\|^2}}{\sum_{\mathbf{v}\in L} e^{-\pi\|\mathbf{v}\|^2}},$$

where $\mathbf{y} \in \mathbb{R}^n$. As D_L is an even function, so

$$\widehat{D_L}(\mathbf{y}) = \sum_{\mathbf{v}\in L} D_L(\mathbf{v}) \cos(2\pi\langle \mathbf{y}, \mathbf{v}\rangle) = \frac{\sum_{\mathbf{v}\in L} \cos(2\pi\langle \mathbf{y}, \mathbf{v}\rangle) e^{-\pi\|\mathbf{v}\|^2}}{\sum_{\mathbf{v}\in L} e^{-\pi\|\mathbf{v}\|^2}}.$$

From the Poisson summation formula, the following equality converts the calculation of Fourier transform on the primal lattice to its dual.

Lemma 2.8 ([4]). *One has $\widehat{D_L}(\mathbf{y}) = \rho(L^* + \mathbf{y})/\rho(L^*)$, where L^* is the dual lattice of L.*

The smoothing parameter $\eta_\epsilon(L)$ is a very important lattice quantity, since it's upper bound determines good distribution properties of discrete Gaussian measures over lattices. It is also used to estimate the size of the connection factor for worst-case to average-case reductions of lattice problems. Informally, if an uniformly random lattice point is perturbed by a Gaussian of radius $s \geq \eta_\epsilon(L)$, then the resulting distribution is ϵ close to uniform distribution over the entire space. (For the detailed statement, please refer to [25].) The precise definition is the following.

Definition 2.9 ([25]). *For any lattice $L \in \mathcal{L}_n$ and real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(L)$ is the smallest $s > 0$ such that $\rho_{1/s}(L^* \backslash \{\mathbf{0}\}) \leq \epsilon$.*

2.3 Previous Work

There are a series of important results in studying transference theorems in the geometry of numbers. Banaszczyk proved the transference theorem about the successive minima of a primal lattice and its dual.

Theorem 2.10 ([4]). *Let L be an arbitrary lattice in $\mathcal{L}_n$, then for all positive integer n one has*

$$\lambda_i(L)\lambda_{n-i+1}(L^*) \leq n \quad (i = 1, \ldots, n).$$

Banaszczyk also gave a transference theorem relating the successive minimum of a lattice with the covering radius of its dual.

Theorem 2.11 ([4]). *Let L be an arbitrary lattice in $\mathcal{L}_n$, then for all positive integer n one has*

$$\lambda_1(L^*)\mu(L) \leq \frac{n}{2}.$$

Cai extended the transference theorem (Theorem 2.10) to the quantities $\lambda_i(L^*)$ and $g_{n-i+1}(L)$.

Theorem 2.12 ([10]). *For every constant $c > 3/2\pi$, there exists an n_0 such that*

$$\lambda_i(L^*)g_{n-i+1}(L) \leq cn,$$

for every lattice L of dimension $n \geq n_0$, and every $1 \leq i \leq n$.

It is also remarked that the constant c can be selected as 2 for any positive integer n. There are transference theorems on lattices possessing n^ϵ-unique shortest vectors.

Theorem 2.13 ([10]). *For every lattice L of dimension n, if L^* has an n^ϵ-unique shortest vector, $0 < \epsilon \leq 1/2$ and $c > 3/2\pi$, then*

$$\lambda_1(L^*)g(L) \leq cn^{1-\epsilon},$$

for all sufficiently large n.

Theorem 2.14 ([10]). *For every lattice L of dimension n, if L^* has an n^ϵ-unique shortest vector, then*

$$1 \leq \lambda_1(L^*)\lambda_n(L) \leq O(n^\delta),$$

where

$$\delta = \begin{cases} 1 - \epsilon & 0 < \epsilon \leq 1/2 \\ 1/2 & 1/2 < \epsilon \leq 1 \\ 3/2 - \epsilon & 1 < \epsilon \leq 3/2 \\ 0 & \epsilon > 3/2. \end{cases}$$

3 Improved Transference Theorems on Lattices Possessing n^ϵ-unique Shortest Vectors

For any lattice $L \in \mathcal{L}_n$, define that L possesses an n^ϵ-unique shortest vector if $\lambda_2(L) > n^\epsilon \lambda_1(L)$. In Section 3.1, corresponding to three different lattice quantities, we prove transference theorems on this class of lattices. Based on our results, in Section 3.2 reductions between $\text{GapSVP}_{\gamma'}$ and GapSIVP_γ for this class of lattices are presented.

3.1 The Improved Transference Theorems

On lattices possessing n^ϵ-unique shortest vectors, firstly we prove a transference theorem giving an upper bound relating the successive minimum of a lattice with the covering radius of its dual. It yields consequently a bound on $\lambda_1(L^*)\lambda_n(L)$. Secondly, we give another transference theorem about the successive minimum and the minimal length of generating vectors, which improves Cai's result.

The following measure inequality proved by Banaszczyk aimed to study transference theorems.

Lemma 3.1 ([4]). *For each $c \geq 1/\sqrt{2\pi}$ and any $\mathbf{u} \in \mathbb{R}^n$, one has*

1. $\rho(L \setminus c\sqrt{n}\mathcal{B}_2^n) < (c\sqrt{2\pi e}\ e^{-\pi c^2})^n \rho(L)$,
2. $\rho((L+\mathbf{u}) \setminus c\sqrt{n}\mathcal{B}_2^n) < 2(c\sqrt{2\pi e}\ e^{-\pi c^2})^n \rho(L)$.

Before our theorem, we also need the following lemma which reveals the relation between $\mu(L)$ and $\lambda_n(L)$ for any lattice $L \in \mathcal{L}_n$.

Lemma 3.2 ([15]). *For any lattice $L \in \mathcal{L}_n$, we have*

$$\frac{\lambda_n(L)}{2} \leq \mu(L) \leq \frac{\sqrt{n}}{2}\lambda_n(L).$$

Theorem 3.3. *Let L be any lattice in $\mathcal{L}_n$, if L^* has an n^ϵ-unique shortest vector where $\epsilon > 0$, then for any positive integer n, we have*

$$\frac{1}{2} \leq \lambda_1(L^*)\mu(L) \leq \frac{1}{2} + n^{1-\epsilon}.$$

It follows that if $\epsilon > 1$, then $\lambda_1(L^*)\mu(L)$ approximately equals $1/2$ for all sufficiently large n.

Proof. The lower bound comes from $\mu(L) \geq \lambda_n(L)/2$ (Lemma 3.2) and $\lambda_1(L^*)\lambda_n(L) \geq 1$. In order to prove $\lambda_1(L^*)\mu(L) \leq 1/2 + n^{1-\epsilon}$, suppose the contrary that there exists a lattice L with $\lambda_1(L^*) \cdot \mu(L) > 1/2 + n^{1-\epsilon}$. Without loss of generality, we assume that

$$\lambda_1(L^*) > n^{\frac{1}{2}-\epsilon}, \tag{1}$$

$$\mu(L) > n^{\frac{1}{2}} + \frac{1}{2}n^{\epsilon-\frac{1}{2}}. \tag{2}$$

If L doesn't satisfy the two inequalities, replace L by sL for a suitably chosen constant s to make the assumptions hold.

Then we get $\lambda_2(L^*) > n^{1/2}$ from assumption (1). Assumption (2) implies there exists a deep hole $\mathbf{t} \in \mathbb{R}^n$ such that $(L+\mathbf{t}) \cap (n^{1/2} + n^{\epsilon-1/2}/2)\mathcal{B}_2^n = \emptyset$. Let $\mathbf{z}$ be an n^ϵ-unique shortest vector for L^* and K be the sublattice of L^* generated by $\mathbf{z}$. Since L^* has an n^ϵ-gap between $\lambda_1(L^*)$ and $\lambda_2(L^*)$, any point lay in $L^* \cap \sqrt{n}\mathcal{B}_2^n$ belongs to K.

Because a deep hole still keeps its distance to the lattice unchanged after a shift of any lattice point, without loss of generality, we can assume that $0 \le \langle \mathbf{t}, \mathbf{z} \rangle < 1$. Let $\mathbf{t}' = \frac{\langle \mathbf{t}, \mathbf{z} \rangle}{\langle \mathbf{z}, \mathbf{z} \rangle} \cdot \mathbf{z}$, and $\mathbf{x} = \mathbf{t} - \mathbf{t}'$ when $\langle \mathbf{t}, \mathbf{z} \rangle \le 1/2$. (Let $\mathbf{x} = \mathbf{t} - \mathbf{t}' + \mathbf{z}/\|\mathbf{z}\|^2$ when $\langle \mathbf{t}, \mathbf{z} \rangle > 1/2$. The proof is essentially the same. So we just consider the case $\langle \mathbf{t}, \mathbf{z} \rangle \le 1/2$). Then we have $\|\mathbf{t}'\| \le n^{\epsilon - 1/2}/2$ and $\langle \mathbf{x}, \mathbf{v} \rangle = 0$ for any $\mathbf{v} \in K$.

Consider the Fourier transform of $D_{L^*}(\mathbf{v}) = \rho(\mathbf{v})/\rho(L^*)$ on the point $\mathbf{x}$, then

$$\begin{aligned}
\widehat{D_{L^*}}(\mathbf{x}) &= \sum_{\mathbf{v} \in L^*} D_{L^*}(\mathbf{v}) \cos(2\pi \langle \mathbf{x}, \mathbf{v} \rangle) \\
&= \sum_{\mathbf{v} \in K} D_{L^*}(\mathbf{v}) + \sum_{\mathbf{v} \in L^* \setminus K} D_{L^*}(\mathbf{v}) \cos(2\pi \langle \mathbf{x}, \mathbf{v} \rangle) \\
&\ge 1 - 2D_{L^*}(L^* \setminus K) \ge 1 - 2D_{L^*}\left(L^* \setminus \sqrt{n}\mathcal{B}_2^n\right) > 1 - 2c^n,
\end{aligned}$$

where the last inequality comes from Lemma 3.1 and $c = \sqrt{2\pi e}/e^{\pi} < 1$.

On the other hand, for any $\mathbf{r} \in L$ we know that,

$$\|\mathbf{r} + \mathbf{x}\| = \|\mathbf{r} + \mathbf{t} - \mathbf{t}'\| \ge \|\mathbf{r} + \mathbf{t}\| - \|\mathbf{t}'\| > n^{\frac{1}{2}} + \frac{1}{2} n^{\epsilon - \frac{1}{2}} - \frac{1}{2} n^{\epsilon - \frac{1}{2}} = n^{\frac{1}{2}}.$$

Then by Lemma 3.1, we have

$$\widehat{D_{L^*}}(\mathbf{x}) = \frac{\rho(L + \mathbf{x})}{\rho(L)} = \frac{\rho((L + \mathbf{x}) \setminus \sqrt{n}\mathcal{B}_2^n)}{\rho(L)} < 2c^n.$$

Thus we obtain the inequality

$$1 - 2c^n < 2c^n, \quad \text{where } c = \sqrt{2\pi e}/e^{\pi} < 1.$$

However this is a contradiction for any positive integer n. The proof is completed. □

Combined with Lemma 3.2 and Theorem 3.3, we give an uniform upper bound on $\lambda_1(L^*)\lambda_n(L)$ for lattices possessing n^{ϵ}-unique shortest vectors which is better than Cai's transference theorem (Theorem 2.14).

Theorem 3.4. *Let L be any lattice in $\mathcal{L}_n$, if L^* has an n^{ϵ}-unique shortest vector where $\epsilon > 0$, then for any positive integer n, we have*

$$1 \le \lambda_1(L^*)\lambda_n(L) \le 1 + 2n^{1-\epsilon}.$$

It follows that if $\epsilon > 1$, then $\lambda_1(L^*)\lambda_n(L)$ approximately equals 1 for sufficiently large n.

The next corollary is immediately from the fact $w_L(\mathcal{B}_2^n) = 2\lambda_1(L^*)$.

Corollary 3.5. *Let L be any lattice in $\mathcal{L}_n$, if L^* has an n^{ϵ}-unique shortest vector where $\epsilon > 0$, then for any positive integer n, we have*

$$2 \le w_L(\mathcal{B}_2^n)\lambda_n(L) \le 2 + 4n^{1-\epsilon}.$$

It follows that if $\epsilon > 1$, then $w_L(\mathcal{B}_2^n)\lambda_n(L)$ approximately equals 2 for all sufficiently large n.

We consider a new transference theorem relating the successive minimum of a lattice with the minimal length of generating vectors of its dual.

Theorem 3.6. *Let L be any lattice in $\mathcal{L}_n$, if L^* has an n^ϵ-unique shortest vector where $\epsilon > 0$, then for any positive integer n, we have*

$$1 \leq \lambda_1(L^*)g(L) \leq 1 + 4n^{1-\epsilon}.$$

It follows that if $\epsilon > 1$, then $\lambda_1(L^*)g(L)$ approximately equals 1 for all sufficiently large n.

Proof. Firstly, let $\mathbf{s}$ be an n^ϵ-unique shortest vector for L^*. We extend $\mathbf{s}$ to a basis $\{\mathbf{s}, \mathbf{s}_2, \ldots, \mathbf{s}_n\}$ of L^*. Denote its dual basis $\{\mathbf{d}_1, \ldots, \mathbf{d}_n\}$ which is a basis of L. Let $S^\perp$ be the hyperplane orthogonal to $\mathbf{s}$. Then $L \cap S^\perp$ is an $n-1$ dimensional sublattice of L generated by $\{\mathbf{d}_2, \ldots, \mathbf{d}_n\}$. For any nonzero vector $\mathbf{r} \in (L \cap S^\perp)^*$, let $\mathbf{r}' = \mathbf{r} - \langle \mathbf{r}, \mathbf{d}_1 \rangle \mathbf{s}$, combining the definition of dual basis it is easy to verify $\mathbf{r}' \in L^*$. Let $x = \langle \mathbf{r}, \mathbf{d}_1 \rangle - \lceil \langle \mathbf{r}, \mathbf{d}_1 \rangle \rfloor$ where $\lceil \langle \mathbf{r}, \mathbf{d}_1 \rangle \rfloor$ denotes the nearest integer to $\langle \mathbf{r}, \mathbf{d}_1 \rangle$, so we get $\mathbf{r} - x\mathbf{s} \in L^*$ which is linearly independent with $\mathbf{s}$ and $|x| \leq 1/2$. Because $\mathbf{s}$ is an n^ϵ-unique shortest vector for L^*, we have

$$\|\mathbf{r}\|^2 + \|\mathbf{s}\|^2/4 \geq \|\mathbf{r} - x\mathbf{s}\|^2 > (n^\epsilon \|\mathbf{s}\|)^2,$$

then $\|\mathbf{r}\| > \sqrt{n^{2\epsilon} - 1/4}\|\mathbf{s}\|$. Hence we get a lower bound on $\lambda_1((L \cap S^\perp)^*)$

$$\lambda_1((L \cap S^\perp)^*) \geq \sqrt{n^{2\epsilon} - 1/4}\|\mathbf{s}\|.$$

By Theorem 2.12, for the $(n-1)$-dimensional sublattice $L \cap S^\perp$, we bound $g(L \cap S^\perp)$ as

$$g(L \cap S^\perp) \leq \frac{2(n-1)}{\lambda_1((L \cap S^\perp)^*)} \leq 4n^{1-\epsilon}/\|\mathbf{s}\|,$$

for any integer n. So we have $n-1$ linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ bounded by $4n^{1-\epsilon}/\|\mathbf{s}\|$ which can generate $L \cap S^\perp$.

Secondly, we intend to extend $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ to a basis of L. Let P be a hyperplane defined as $P = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{s} \rangle = 1\}$, clearly it is the closest parallel hyperplane to $S^\perp$ which has orthogonal distance $1/\|\mathbf{s}\|$ to $S^\perp$. Because $L \cap P$ is a shift of $L \cap S^\perp$ by some lattice point in L, the covering radius of $L \cap P$ equals that of $L \cap S^\perp$. So by Lemma 2.11, we get

$$\mu(L \cap P) = \mu(L \cap S^\perp) \leq \frac{n-1}{2\lambda_1((L \cap S^\perp)^*)} \leq n^{1-\epsilon}/\|\mathbf{s}\|.$$

Consequently, we have a lattice vector $\mathbf{v}_n$ in $L \cap P$ with length bounded by $1/\|\mathbf{s}\| + n^{1-\epsilon}/\|\mathbf{s}\|$, which is linearly independent with $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$. Then we get a set of n linearly independent vectors in L with norm at most $\max\{4n^{1-\epsilon}, 1+n^{1-\epsilon}\}/\|\mathbf{s}\|$, which is obviously smaller than $(1+4n^{1-\epsilon})/\|\mathbf{s}\|$.

Now we show this sequence of n vectors can generate L. First the vector $\mathbf{s}$ partitions L into subsets $L \cap H_i$ ($i \in \mathbb{Z}$) where H_i is an $(n-1)$-dimensional hyperplane $H_i = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{s} \rangle = i\}$. Here $H_0 = S^\perp$, $H_1 = P$. For any $\mathbf{v} \in L$, there must exist a hyperplane where $\mathbf{v}$ lies and denote it by H_k. Then $\mathbf{v} - k\mathbf{v}_n \in L \cap S^\perp$ and it can be generated by $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$. So $\mathbf{v}$ can be represented by integer combinations of $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Thus the set of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis of L. Therefore $g(L) \leq (1 + 4n^{1-\epsilon})/\|\mathbf{s}\|$. We have proved that

$$\lambda_1(L^*)g(L) \leq 1 + 4n^{1-\epsilon}. \qquad \square$$

Obviously, our bound on $\lambda_1(L^*)\lambda_n(L)$ improves Cai's result for $\epsilon > 1/2$. In fact, based on our results, the instance given in [10] can illustrate that all the bounds we proved in this section are optimal up to constants for any $\epsilon > 0$. The details are included in Appendix A. We also notice that for any n-dimensional lattice L, if L^* has an n^ϵ-unique shortest vector where $\epsilon > 1$, all the quantities $g(L)$, $\lambda_n(L)$ and $2\mu(L)$ are equal to $1/\lambda_1(L^*)$ approximately.

3.2 Reductions between GapSVP$_{\gamma'}$ and GapSIVP$_{\gamma}$

The transference theorem due to Banaszczyk immediately implies a reduction from GapSVP$_{\gamma n}$ to GapSIVP$_{\gamma}$ for any factor γ. Also, Micciancio gave a polynomial time and dimension preserving reduction from SVP to SIVP for the exact ($\gamma = 1$) version [24], and announced an open problem to find polynomial time reductions between SVP$_{\gamma}$ and SIVP$_{\gamma}$ that preserve both the dimension of the lattice and the quality of approximation. As an application of the improved transference theorem in Section 3.1, we give the polynomial time reductions between GapSVP$_{\gamma'}$ and GapSIVP$_{\gamma}$ for lattices possessing n^{ϵ}-unique shortest vectors. We also indicate that the approximation factors are almost preserved if $\epsilon > 1$.

Theorem 3.7. *For any approximation factor γ, there are polynomial time reductions between GapSIVP$_{\gamma}$ and GapSVP$_{\gamma'}$ for lattices with n^{ϵ}-gaps.*
1. For any lattice $L \in \mathcal{L}_n$ which has an n^{ϵ}-unique shortest vector ($\epsilon > 0$), the problem GapSVP$_{\gamma(1+2n^{1-\epsilon})}$ can be reduced to GapSIVP$_{\gamma}$.
2. For any lattice $L \in \mathcal{L}_n$ whose dual lattice L^* has an n^{ϵ}-unique shortest vector ($\epsilon > 0$), the problem GapSIVP$_{\gamma(1+2n^{1-\epsilon})}$ can be reduced to GapSVP$_{\gamma}$.

Proof. 1. Let $(L(\mathbf{B}), d)$ be an instance of GapSVP$_{\gamma(1+2n^{1-\epsilon})}$ where the input lattice has an n^{ε}-unique shortest vector. We need to output YES if $\lambda_1(L) \leq d$ and NO if $\lambda_1(L) > \gamma(1+2n^{1-\epsilon})d$. By Theorem 3.4, if $\lambda_1(L) \leq d$, then $\lambda_n(L^*) \geq 1/d$. If $\lambda_1(B) > \gamma(1+2n^{1-\epsilon})d$, then $\lambda_n(L^*) < 1/(\gamma d)$. Thus the GapSVP$_{\gamma}$ can be solved by calling a GapSIVP$_{\gamma}$ oracle on $(L^*, 1/(\gamma d))$ such that: If the GapSIVP$_{\gamma}$ oracle on $(L^*, 1/(\gamma d))$ outputs YES, we output NO for the GapSVP$_{\gamma(1+2n^{1-\epsilon})}$. If the GapSIVP$_{\gamma}$ oracle on $(L^*, 1/(\gamma d))$ outputs NO, we output YES for the GapSVP$_{\gamma(1+2n^{1-\epsilon})}$.

The proof of 2 is essentially the same.

In particular, if $\epsilon > 1$, the approximation factors are almost preserved. □

4 Transference Theorem about Lower Bound on $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n)$

In this section, we prove a transference theorem giving a lower bound on the quantity $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n)$ where $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n) = \inf_{L\in\mathcal{L}_n} \min_{1\leq i\leq n} \lambda_i^{(p)}(L)\lambda_{n-i+1}^{(q)}(L^*)$ for any $p,\ q \in [1,\infty]$. In Section 4.2, we show some applications to upper bounds on the smoothing parameter of Gaussian measures over lattices and also give a more appropriate bound for lattices whose duals have $\sqrt{n}$-unique shortest vectors.

4.1 A Lower Bound on $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n)$

Theorem 4.1. *For any positive integer n, we have*

$$\eta(\mathcal{B}_p^n, \mathcal{B}_q^n) \geq \begin{cases} n^{1/p+1/q-1} & 1/p+1/q < 1, \quad p,\ q \in [1,\infty] \\ 1 & 1/p+1/q \geq 1, \quad p,\ q \in [1,\infty], \end{cases}$$

where $\eta(\mathcal{B}_p^n, \mathcal{B}_q^n) = \inf_{L\in\mathcal{L}_n} \min_{1\leq i\leq n} \lambda_i^{(p)}(L)\lambda_{n-i+1}^{(q)}(L^*)$ and we mean $1/p = 0$ ($1/q = 0$, respectively) when $p = \infty$ ($q = \infty$).

Proof. For any lattice $L \in \mathcal{L}_n$ and any $1 \leq i \leq n$, we prove $\lambda_i^{(p)}(L) \cdot \lambda_{n-i+1}^{(q)}(L^*)$ satisfies the inequality. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_i\} \subset L$ be i linearly independent vectors reaching the successive minima $\lambda_1^{(p)}(L), \cdots, \lambda_i^{(p)}(L)$. Take $n-i+1$ linearly independent vectors $\{\mathbf{d}_1, \ldots, \mathbf{d}_{n-i+1}\} \subset L^*$ such that

$\|\mathbf{d}_1\|_q \le \|\mathbf{d}_2\|_q \le \cdots \le \|\mathbf{d}_{n-i+1}\|_q = \lambda_{n-i+1}^{(q)}(L^*)$. Not all of them are orthogonal to every $\mathbf{v}_1, \ldots, \mathbf{v}_i$. Hence, there exist k, j such that $\langle \mathbf{d}_k, \mathbf{v}_j \rangle \neq 0$ $(1 \le k \le n-i+1, 1 \le j \le i)$. We denote $\mathbf{d}_k^{(l)}$ and $\mathbf{v}_j^{(l)}$ as the lth coordinate of $\mathbf{d}_k$ and $\mathbf{v}_j$ respectively.

Case 1: $1/p + 1/q < 1,\ p,\ q \in [1, \infty]$.

Let $1/p + 1/q = c$, where $c < 1$. By Hölder's inequality, we have

$$\|\mathbf{d}_k\|_{cq} = (\sum_{l=1}^{n} |d_k^{(l)}|^{cq})^{\frac{1}{cq}} \le ((\sum_{l=1}^{n} |d_k^{(l)}|^{cq \cdot \frac{1}{c}})^c \cdot n^{1-c})^{\frac{1}{cq}} = \|\mathbf{d}_k\|_q \cdot n^{\frac{1-c}{cq}}.$$

In the same way, we deduce $\|\mathbf{v}_j\|_{cp} \le \|\mathbf{v}_j\|_p \cdot n^{\frac{1-c}{cp}}$. Therefore

$$\begin{aligned} 1 \le |\langle \mathbf{d}_k, \mathbf{v}_j \rangle| &\le \|\mathbf{d}_k\|_{cq} \cdot \|\mathbf{v}_j\|_{cp} \le \|\mathbf{d}_k\|_q \cdot n^{\frac{1-c}{cq}} \cdot \|\mathbf{v}_j\|_p \cdot n^{\frac{1-c}{cp}} \\ &= n^{1-\frac{1}{p}-\frac{1}{q}} \|\mathbf{d}_k\|_q \|\mathbf{v}_j\|_p \le n^{1-\frac{1}{p}-\frac{1}{q}} \lambda_i^{(p)}(L) \cdot \lambda_{n-i+1}^{(q)}(L^*). \end{aligned}$$

We have shown that $\lambda_i^{(p)}(L) \cdot \lambda_{n-i+1}^{(q)}(L^*) \ge n^{\frac{1}{p}+\frac{1}{q}-1}$.

Case 2: $1/p + 1/q \ge 1,\ p,\ q \in [1, \infty]$.

Let $1/p + 1/q = c$, where $c \ge 1$. By Hölder's inequality, we get

$$\|\mathbf{d}_k\|_{cq} = (\sum_{l=1}^{n} |d_k^{(l)}|^{cq})^{\frac{1}{cq}} \le ((\sum_{l=1}^{n} |d_k^{(l)}|^{q})^c)^{\frac{1}{cq}} = \|\mathbf{d}_k\|_q.$$

Similarly, $\|\mathbf{v}_j\|_{cp} \le \|\mathbf{v}_j\|_p$, thus

$$1 \le |\langle \mathbf{d}_k, \mathbf{v}_j \rangle| \le \|\mathbf{d}_k\|_{cq} \cdot \|\mathbf{v}_j\|_{cp} \le \|\mathbf{d}_k\|_q \cdot \|\mathbf{v}_j\|_p \le \lambda_i^{(p)}(L) \cdot \lambda_{n-i+1}^{(q)}(L^*).$$

We complete the proof. □

We construct some concrete lattices to illustrate that the lower bound is optimal. For the case $1/p + 1/q \ge 1$, it can be easily achieved by the lattice $\mathbb{Z}^n$. While for $1/p + 1/q < 1$, for any integer n, we define an n-dimensional lattice L generated by the basis $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$ where $\mathbf{b}_1 = (-1, 1, 1, \ldots, 1)^{\mathrm{t}}$, $\mathbf{b}_i = (0, \ldots, n, \ldots, 0)^{\mathrm{t}}$ which has a single n at the ith position and 0 elsewhere for $2 \le i \le n$. Thus its dual lattice L^* has a basis $\mathbf{D} = [\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n]$ where $\mathbf{d}_1 = (-1, 0, \ldots, 0)^{\mathrm{t}}$, $\mathbf{d}_i$ has $1/n$ at the first and ith positions and 0 elsewhere for $2 \le i \le n$. It's easy to get $\lambda_1^{(p)}(L) = n^{1/p}$ and the largest l_q norm of the n independent vectors $\mathbf{d}_1 + \ldots + \mathbf{d}_n, \mathbf{d}_2, \ldots, \mathbf{d}_n$ in L^* is $n^{1/q-1}$. Then $\lambda_n^{(q)}(L^*) \le n^{1/q-1}$. Combined with $\lambda_1^{(p)}(L) \cdot \lambda_n^{(q)}(L^*) \ge n^{1/p+1/q-1}$, we obtain $\lambda_n^{(q)}(L^*) = n^{1/q-1}$, therefore $\lambda_1^{(p)}(L) \cdot \lambda_n^{(q)}(L^*) = n^{1/p+1/q-1}$.

Combined with the results of Banaszczyk, we give some refinements on relationships of some lattice quantities.

Lemma 4.2 ([5]). *A numerical constant C exists such that*

$$\sup_{L \in \mathcal{L}_n} \max_{1 \le i \le n} \lambda_i^{(p)}(L) \lambda_{n-i+1}^{(\infty)}(L^*) \le C\sqrt{p} n^{1/p} \sqrt{\log n} \quad (1 \le p < \infty).$$

Lemma 4.3 ([6]). *For any $1 \le p,\ q \le \infty$, there exists a lattice $L \in \mathcal{L}_n$ such that*

$$\lambda_1^{(p)}(L) \cdot \lambda_1^{(q)}(L^*) > [\mathrm{vol}(\mathcal{B}_p^n) \cdot \mathrm{vol}(\mathcal{B}_q^n)]^{-1/n},$$

where $\mathrm{vol}(\mathcal{B}_p^n)$ denotes the volume of the closed unit ball of $\mathbb{R}^n$ in l_p norm.

The first corollary is about the successive minima in l_∞ and l_2 norms.

Corollary 4.4. *For any lattice $L \in \mathcal{L}_n$, we have*

$$\frac{1}{\sqrt{n}} \le \lambda_1^{(\infty)}(L) \cdot \lambda_n^{(2)}(L^*) \le 4\sqrt{n \log n}.$$

Proof. The lower bound follows from Theorem 4.1. The upper bound is a result of Lemma 4.2. In fact, the constant can be easily calculated according to ([5], Lemma 1.6, 2.9, 2.10). One can refer to Appendix B for details. □

We also remark that for any integer n, there exists a lattice $L \in \mathcal{L}_n$ such that $\lambda_1^{(\infty)}(L) \cdot \lambda_n^{(2)}(L^*) > (8\pi e)^{-1/2} \cdot \sqrt{n}$. In fact, by Lemma 4.3, there exists a lattice L with

$$\lambda_1^{(\infty)}(L) \cdot \lambda_n^{(2)}(L^*) > [\mathrm{vol}(\mathcal{B}_\infty^n) \cdot \mathrm{vol}(\mathcal{B}_2^n)]^{-1/n} = [2^n \cdot \frac{\pi^{n/2}}{\Gamma(n/2+1)}]^{-1/n} \ge (8\pi e)^{-1/2} \cdot \sqrt{n},$$

where the last inequality follows from the double inequality due to Robbins [29].

Next we show the refined relationship between the Gram-Schmidt minimum of a primal lattice and the successive minimum in l_∞ norm of its dual.

Corollary 4.5. *For any lattice $L \in \mathcal{L}_n$, we have*

$$\frac{1}{\sqrt{n}} \le \widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \le 4\sqrt{n \log n}.$$

Proof. First, we prove $\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \ge 1/\sqrt{n}$. Let $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$ be a basis of L with $\max_{1 \le i \le n} \|\widetilde{\mathbf{b}_i}\| = \widetilde{bl}(L)$. For any nonzero vector $\mathbf{v} \in L^*$, not all $\mathbf{b}_i$s are orthogonal to $\mathbf{v}$. Denote k the smallest index such that $\langle \mathbf{v}, \mathbf{b}_k \rangle \neq 0$. Then

$$1 \le |\langle \mathbf{v}, \mathbf{b}_k \rangle| = |\langle \mathbf{v}, \widetilde{\mathbf{b}_k} \rangle| \le \|\mathbf{v}\| \cdot \|\widetilde{\mathbf{b}_k}\| \le \|\mathbf{v}\| \cdot \widetilde{bl}(L) \le \sqrt{n}\|\mathbf{v}\|_\infty \cdot \widetilde{bl}(L).$$

Therefore $\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \ge 1/\sqrt{n}$.

Lemma 2.3 implies that for any n linearly independent vectors $\mathbf{S} = [\mathbf{s}_1, \ldots, \mathbf{s}_n] \subset L$, one can find a basis $\mathbf{R}$ of L with $\|\widetilde{\mathbf{R}}\| \le \|\widetilde{\mathbf{S}}\|$. So $\widetilde{bl}(L) \le \lambda_n^{(2)}(L)$. Then from Corollary 1, we have $\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \le \lambda_n^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) \le 4\sqrt{n \log n}$. □

We point out that the lower bound in Corollary 4.5 is tight and the optimal upper bound is larger than $(8\pi e)^{-1/2} \cdot \sqrt{n}$. The details are included in Appendix C.

4.2 Comparison of Upper Bounds on the Smoothing Parameter

In this section, on the smoothing parameter of Gaussian measures over lattices, we compare the respective advantages of previous upper bounds relating to different lattice quantities. In addition, a more appropriate bound for a class of lattices whose duals have $\sqrt{n}$-unique shortest vectors is suggested.

For any lattice $L \in \mathcal{L}_n$ and any $\epsilon > 0$, Micciancio and Regev proved $\eta_\epsilon(L) \le \sqrt{\ln(2n(1+1/\epsilon))/\pi} \cdot \lambda_n^{(2)}(L)$ [25] which relates the smoothing parameter with $\lambda_n^{(2)}(L)$. For the purpose of achieving worst-case to average-case reductions in l_p norms [27], Peikert gave another bound relative to the dual minimum distance in l_p norm. In particular, for l_∞ norm, it is proved that $\eta_\epsilon(L) \le$

$\sqrt{\ln(2n(1+1/\epsilon))/\pi}/\lambda_1^{(\infty)}(L^*)$. In [14] where new notion of trapdoor functions with preimage sampling was presented, Gentry et al. showed $\eta_\epsilon(L) \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi} \cdot \widetilde{bl}(L)$ where $\widetilde{bl}(L)$ denotes the Gram-Schmidt minimum of L. Using the transference theorems given in Section 4.1, we compare the three upper bounds on $\eta_\epsilon(L)$ shown in Table 1.

upper bounds on $\eta_\epsilon(L)$	$f(n) \cdot \lambda_n^{(2)}(L)$	$f(n)/\lambda_1^{(\infty)}(L^*)$	$f(n) \cdot \widetilde{bl}(L)$
$\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \geq 1$	L	S	M
$\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \leq 1$ and $\lambda_n^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) \geq 1$	L	M	S
$\lambda_n^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) \leq 1$	M	L	S

Table 1. L, M and S represent the bound is largest, middle and smallest respectively and $f(n) = \sqrt{\ln(2n(1+1/\epsilon))/\pi}$.

Case 1: $\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \geq 1$ implies $1/\lambda_1^{(\infty)}(L^*) \leq \widetilde{bl}(L) \leq \lambda_n^{(2)}(L)$. And Corollary 4.5 shows there exist lattices satisfying this inequality.

Case 2: $\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \leq 1$ and $\lambda_n^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) \geq 1$ result in $\widetilde{bl}(L) \leq 1/\lambda_1^{(\infty)}(L^*) \leq \lambda_n^{(2)}(L)$. We give an instance which satisfies this condition. Define a 3-dimensional lattice Λ generated by the basis $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3]$, where $\mathbf{b}_1 = (1, -1/2, -1)^{\mathrm{t}}$, $\mathbf{b}_2 = (0, 1, 0)^{\mathrm{t}}$ and $\mathbf{b}_3 = (0, 0, 2)^{\mathrm{t}}$. Thus its dual lattice Λ^* has a basis $\mathbf{D} = [\mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_3]$, where $\mathbf{d}_1 = (1, 0, 0)^{\mathrm{t}}$, $\mathbf{d}_2 = (1/2, 1, 0)^{\mathrm{t}}$ and $\mathbf{d}_3 = (1/2, 0, 1/2)^{\mathrm{t}}$. It is easy to verify that $\widetilde{bl}(\Lambda) \leq \sqrt{2}$, $1/\lambda_1^{(\infty)}(\Lambda^*) = 2$ and $\lambda_3^{(2)}(\Lambda) = 2$.

Case 3: $\lambda_n^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) \leq 1$ implies that $\widetilde{bl}(L) \leq \lambda_n^{(2)}(L) \leq 1/\lambda_1^{(\infty)}(L^*)$. And Corollary 4.4 shows there exist such lattices.

The following corollary shows a stronger bound on the smoothing parameter of Gaussian measures over lattices whose duals possess $\sqrt{n}$-unique shortest vectors.

Corollary 4.6. *For any lattice $L \in \mathcal{L}_n$ and any $\epsilon > 0$, if L^* has a $\sqrt{n}$-unique shortest vector, we have*

$$\eta_\epsilon(L) \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi}/\lambda_1^{(2)}(L^*).$$

Proof. Notice that the rotation of coordinate system doesn't change the smoothing parameter $\eta_\epsilon(L)$ and $\lambda_1^{(2)}(L)$ since their definitions depend on the l_2 norm of lattice vectors. Hence we rotate the coordinate system making $\lambda_1^{(\infty)}(L'^*)$ as large as possible where L' is the lattice in the new coordinate system. We know that $\lambda_1^{(\infty)}(L'^*) \leq \lambda_1^{(2)}(L'^*) = \lambda_1^{(2)}(L^*)$, but not all lattices can make $\lambda_1^{(\infty)}(L'^*)$ equal $\lambda_1^{(2)}(L^*)$ by rotations of coordinate system. However, if $\lambda_2^{(2)}(L^*) \geq \sqrt{n}\lambda_1^{(2)}(L^*)$, let $\mathbf{v} \in L^*$ with $\|\mathbf{v}\|_2 = \lambda_1^{(2)}(L^*)$, then rotate the coordinate system to keep $\mathbf{v}$ on one axis. Since $\lambda_2^{(2)}(L^*) \geq \sqrt{n}\lambda_1^{(2)}(L^*)$, there exists no lattice point in $\lambda_1^{(2)}(L^*) \cdot \mathcal{B}_\infty^n$ except $\mathbf{0}$ and $\pm\mathbf{v}$. So $\lambda_1^{(\infty)}(L'^*)$ equals $\lambda_1^{(2)}(L^*)$. Followed by $\eta_\epsilon(L') \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi}/\lambda_1^{(\infty)}(L'^*)$, we get $\eta_\epsilon(L) = \eta_\epsilon(L') \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi}/\lambda_1^{(2)}(L^*)$. □

5 Conclusion

In this paper, we prove three transference theorems on lattices possessing n^ϵ-unique shortest vectors and show reductions between $\mathrm{GapSVP}_{\gamma'}$ and $\mathrm{GapSIVP}_\gamma$ for this class of lattices. Furthermore, a transference theorem on the lower bound relating the successive minima of a lattice with its dual is presented. As applications, we compare the respective advantages of current upper bounds on smoothing parameter of Gaussian measures over lattices and show a more appropriate bound for lattices whose duals possess $\sqrt{n}$-unique shortest vectors.

References

1. D. Aharonov, O. Regev. Lattice problems in NP ∩ coNP. Journal of the ACM, 52(5): 749-765, 2005. Preliminary version in FOCS 2004.
2. M. Ajtai. Generating hard instances of lattice problems. Complexity of Computations and Proofs, Quaderni di Matematica, 13: 1-32, 2004. Preliminary version in STOC 1996.
3. M. Ajtai, C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In Proceedings of the 29th Annual ACM Symposium on Theory of Computing-STOC'97, pages 284-293, El Paso, TX, USA, May 1997.ACM.
4. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Mathematische Annalen, 296(4):625-635, 1993.
5. W. Banaszczyk. Inequalites for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. Discrete Comput.Geom. 13: 217-231, 1995.
6. W. Banaszczyk. Inequalites for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ II :Applications of K-Convexity. Discrete Comput. Geom. 16: 305-311, 1996.
7. W. Banaszczyk, A. Litvak, A. Pajor, and S. Szarek. The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces. Mathematics of Operations Research, 24(3):728 - 750, 1999.
8. J. Blömer. Closest vectors, successive minima, and dual HKZ-bases of lattices. ICALP 2000: 248-259.
9. J. Blömer, J.-P Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In Proceedings of STOC 1999, pages 711 - 720. ACM, May 1999.
10. J.-Y 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.
11. J.-Y. Cai, A. Nerurkar. An improved worst-case to average-case connection for lattice problems. Proceedings of the 38th IEEE Symposium on Foundations of Computer Science (FOCS), 1997, pp. 468 - 477.
12. J.W.S. Cassels. An introduction to the geometry of numbers. Springer, Berlin, Göttingen Heidelberg, 1959.
13. D. Dadush, C. Peikert, S. Vempala. Enumerative lattice algorithms in any norm via M-ellipsoid coverings. FOCS 2011: 580-589.
14. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the 40th ACM Symposium on Theory of Computing (STOC 2008). ACM, New York, 197 - 206.
15. V. Guruswami, D. Micciancio and O. Regev. The complexity of the covering radius problem on lattices and codes. Journal Computational Complexity archive Volume 14 Issue 2, June 2005.
16. J. Hoffstein, J. Pipher and J.H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In: ANTS 1998. LNCS, vol. 1423, pp. 267-288. Springer, Heidelberg (1998).
17. H.W. Lenstra. Integer programming with a fixed number of variables. Mathematics of Operations Research, 8(4):538 - 548, November 1983.
18. C. Lgarias, H.W. Lenstra and C.P.Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocial lattice.Combinatorica 10(4)(1990) 333-348.
19. Cong Ling, Shuiyin Liu, Laura Luzzi and Damien Stehlé. Decoding by embedding: correct decoding radius and DMT optimality. CoRR abs/1102.2936: (2011).
20. Mingjie Liu, Xiaoyun Wang, Guangwu Xu, Xuexin Zheng. Shortest Lattice Vectors in the Presence of Gaps. IACR Cryptology ePrint Archive 2011: 139 (2011).
21. V. Lyubashevsky, D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. Crypto 2009, Aug. 2009, pp. 577 - 594.
22. K. Mahler. Ein Übertragungsprinzip für konvexe Körper, Čas. Pě stování Mat. Fys. 68 (1939) 93 - 102.
23. D. Micciancio. Improved cryptographic hash functions with worst-case/average-case connection. STOC 2002: 609-618.
24. D. Micciancio. Efficient reductions among lattice problems. SODA 2008: 84-93.
25. D. Micciancio, O. Regev. Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput., 37(1): 267-302, 2007.
26. J. Milnor, D. Husemoller. Symmetric bilinear forms. Springer, Berlin, Heidelberg, New York, 1973.
27. C. Peikert. Limits on the hardness of lattice problems in l_p norms. Computational Complexity, 17(2): 300-351, 2008. Preliminary version in CCC 2007. Preliminary version in FOCS 2004.
28. O. Regev. On lattices, learing with errors, random linear codes, and cryptography. J.ACM 56(6),1-40(2009).
29. H. Robbins. A remark on Stirling's formula. Amer. Math. Monthly. 62(1955) 26-28.

Appendix

A. An instance [10] showing the optimum of our transference theorems in Section 3.1

For any positive integer n, let Λ_1 be a self-dual $(n-1)$-dimensional lattice which means $\Lambda_1^* = \Lambda_1$ and let $\lambda_1(\Lambda_1) = c\sqrt{n}$ for some constant c. Conway and Thompson [26] showed that there exist self-dual lattices satisfying this condition. Let $\mathbf{u}$ be a vector perpendicular to the linear span of Λ_1 with norm $cn^{1/2-\epsilon}$. Define $\Lambda^* = \Lambda_1 \oplus \langle \mathbf{u} \rangle$. Then $\lambda_1(\Lambda^*) = cn^{1/2-\epsilon}$ and $\mathbf{u}$ is an n^ϵ-unique shortest vector of Λ^*. The dual of Λ^* is $\Lambda = \Lambda_1 \oplus \langle \mathbf{u}/\|\mathbf{u}\|^2 \rangle$. For any n linearly independent vectors of Λ, the orthogonal projections to $\mathrm{span}(\Lambda_1)$ are $n-1$ linearly independent vectors of Λ_1. So we get $\lambda_n(\Lambda) \geq \lambda_{n-1}(\Lambda_1) \geq \lambda_1(\Lambda_1) = c\sqrt{n}$. Therefore, $\lambda_1(\Lambda^*)\lambda_n(\Lambda) \geq c^2 n^{1-\epsilon}$. By Lemma 3.2, we have $\lambda_1(\Lambda^*)\mu(\Lambda) \geq c^2 n^{1-\epsilon}/2$. It is easy to get $\lambda_1(\Lambda^*)g(\Lambda) \geq c^2 n^{1-\epsilon}$ since $g(\Lambda) \geq \lambda_n(\Lambda)$. So the upper bounds we proved in Section 3.1 are all optimal up to constants.

B. The supplementary proof of Corollary 4.4

To calculate the constant 4 in $\lambda_1^{(\infty)}(L) \cdot \lambda_n^{(2)}(L^*) \leq 4\sqrt{n \log n}$, we first list some useful notations and results as follows.

Given a lattice $L \in \mathcal{L}_n$ and a $\mathbf{0}$-symmetric convex body U in $\mathbb{R}^n$, define $\alpha(U) = \sup_{L \in \mathcal{L}_n} \frac{\rho(L \setminus U)}{\rho(L)}$ and $\beta(U) = \sup_{L \in \mathcal{L}_n} \sup_{\mathbf{u} \in \mathbb{R}^n} \rho((L + \mathbf{u}) \setminus U)/\rho(L)$. Then for arbitrary $r > 0$, Banaszczyk proved $\beta(r\mathcal{B}_2^n) < 2n/(\pi r^2)$, and $\beta(r\mathcal{B}_\infty^n) < 2n/e^{\pi r^2}$ [5]. In the same reference, it is also proved that for any $\mathbf{0}$-symmetric convex bodies U, V in $\mathbb{R}^n$, if $2\alpha(U) + \beta(V) \leq 1 - e^{-\pi}$, then $\sup_{L \in \mathcal{L}_n} \max_{1 \leq i \leq n} \lambda_i(L, U) \cdot \lambda_{n+1-i}(L^*, V + \mathcal{B}_2^n) \leq 1$.

Let $r_1 = 2\sqrt{n}$, $r_2 = \sqrt{\log n}$, then

$$2\alpha(r_1\mathcal{B}_2^n) + \beta(r_2\mathcal{B}_\infty^n) \leq 2 \cdot \frac{2n}{\pi {r_1}^2} + \frac{2n}{e^{\pi {r_2}^2}} = \frac{1}{\pi} + \frac{2}{n^{\pi - 1}} \leq 1 - e^{-\pi}.$$

So we get

$$\sup_{L \in \mathcal{L}_n} \max_{1 \leq i \leq n} \lambda_i(L, 2\sqrt{n}\mathcal{B}_2^n) \cdot \lambda_{n+1-i}(L^*, \sqrt{\log n}\mathcal{B}_\infty^n + \mathcal{B}_2^n) \leq 1.$$

As $\lambda_{n+1-i}^{(\infty)}(L^*) = 2\sqrt{\log n}\lambda_{n+1-i}(L^*, 2\sqrt{\log n}\mathcal{B}_\infty^n) \leq 2\sqrt{\log n}\lambda_{n+1-i}(L^*, \sqrt{\log n}\mathcal{B}_\infty^n + \mathcal{B}_2^n)$, and $\lambda_i^{(2)}(L) = 2\sqrt{n}\lambda_i(L, 2\sqrt{n}\mathcal{B}_2^n)$, therefore

$$\begin{aligned}\sup_{L \in \mathcal{L}_n} \max_{1 \leq i \leq n} \lambda_i^{(2)}(L)\lambda_{n-i+1}^{(\infty)}(L^*) &\leq 2\sqrt{n} \cdot 2\sqrt{\log n}\lambda_i(L, 2\sqrt{n}\mathcal{B}_2^n) \cdot \lambda_{n+1-i}(L^*, \sqrt{\log n}\mathcal{B}_\infty^n + \mathcal{B}_2^n) \\ &\leq 4\sqrt{n \log n}.\end{aligned}$$

C. The optimum of Corollary 4.5

For the optimum of the lower bound, refer to the instance after Theorem 4.1. Let T be the lattice generated by $\mathbf{D}$, then its dual lattice $T^* = \mathcal{L}(\mathbf{B})$. It's easy to get that $\lambda_1^{(\infty)}(T^*) = 1$. Since $\widetilde{bl}(T) \leq \lambda_n^{(2)}(T) = 1/\sqrt{n}$ and $\widetilde{bl}(T) \geq (1/\sqrt{n})\lambda_1^{(\infty)}(T^*) = 1/\sqrt{n}$, we get $\widetilde{bl}(T) = 1/\sqrt{n}$. Therefore $\widetilde{bl}(T) \cdot \lambda_1^{(\infty)}(T^*) = 1/\sqrt{n}$.

Notice that $\widetilde{bl}(L) \geq \lambda_1^{(2)}(L)$, so for the upper bound, we claim by Lemma 4.3 that there exists a lattice L with

$$\begin{aligned}\widetilde{bl}(L) \cdot \lambda_1^{(\infty)}(L^*) \geq \lambda_1^{(2)}(L) \cdot \lambda_1^{(\infty)}(L^*) &> [\mathrm{vol}(B_2^n) \cdot \mathrm{vol}(B_\infty^n)]^{-1/n} \\ &= [2^n \cdot \frac{\pi^{n/2}}{\Gamma(n/2+1)}]^{-1/n} \geq (8\pi e)^{-1/2} \cdot \sqrt{n}.\end{aligned}$$