A new transference theorem and applications to Ajtai's connection factor

Jin-Yi Cai*

Abstract

We prove a new transference theorem in the geometry of numbers, giving optimal bounds relating the successive minima of a lattice with the minimal length of generating vectors of its dual. It generalizes the transference theorem due to Banaszczyk. We also prove a stronger bound for the special class of lattices possessing n^{ϵ}-unique shortest lattice vectors. The theorems imply consequent improvement of the Ajtai connection factors in the connection of average-case to worst-case complexity of the shortest lattice vector problem. Our proofs are non-constructive, based on methods from harmonic analysis.

1 Introduction

A lattice in $\mathbf{R}^n$ is the set of all integral linear combinations of a fixed set of linearly independent vectors over $\mathbf{R}$. Such a generating set of vectors is called a basis of the lattice. Alternatively a lattice can be defined as a discrete additive subgroup Γ of $\mathbf{R}^n$. In particular, this implies that for any discrete additive subgroup Γ one can always find a basis in the above sense. The basis of a lattice is not unique, and are related to each other by unimodular transformations. The characterization and the complexity of finding a good basis that consists of short vectors is a central problem in the study of geometry of numbers.

The rank or the dimension of a lattice L, denoted by $\dim L$, is the dimension of the linear subspace it spans. The length of the shortest non-zero lattice vector is denoted by $\lambda_1(L)$. More generally, Minkowski's *successive minima* $\lambda_i(L)$ are defined as follows: for $1 \le i \le \dim L$, $\lambda_i(L) = \min_{v_1,\ldots,v_i \in L} \max_{1\le j\le i} ||v_j||$, where the sequence of vectors $v_1, \ldots, v_i \in L$ ranges over all i linearly independent lattice vectors. It is perhaps the first indication of the intricacies of higher dimensional lattices that, except for dimensions up to 3, the shortest vectors represented by the successive minima *do not* necessarily form a basis of the lattice [19]. Define $g(L)$ to be the minimum r such that a ball $B(0;r)$ centered at 0 with radius r contains a set of lattice vectors generating L. More generally, we say a sublattice $L' \subset L$ is a *saturated sublattice* if $L' = L \cap \Pi$, where Π is the linear subspace of $\mathbf{R}^n$ spanned by L'. Then we define $g_i(L)$ to be the minimum r such that the sublattice generated by $L \cap B(0;r)$ contains an i-dimensional saturated sublattice L', where $1 \le i \le \dim L$. Clearly for $d = \dim L$, $g(L) = g_d(L)$ and $\lambda_i(L) \le g_i(L)$, $1 \le i \le d$.

*Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Email: `cai@cs.buffalo.edu`. Research supported in part by NSF grant CCR-9634665, and by an Alfred P. Sloan Fellowship.

The dual lattice L^* of a lattice L of dimension n in $\mathbf{R}^n$ is defined as those vectors u, such that $\langle u, v \rangle \in \mathbf{Z}$, for all $v \in L$. It consists of all integral linear combinations of the dual basis vectors $b_1^*, \ldots, b_n^*$, where $\langle b_i^*, b_j \rangle = \delta_{ij}$. In particular $\det(L^*) = 1/\det(L)$, and $L^{**} = L$. For a lattice with dimension less than n, its dual is defined within its own linear span. There is a long history in geometry of numbers to study relationships between various quantities such as the successive minima associated with the primal and dual lattices, L and L^*. Such theorems are called transference theorems. Our main theorem in this paper is the following upper bound

$$g_i(L) \cdot \lambda_{n-i+1}(L^*) \leq Cn, \tag{1}$$

for some universal constant C, and for all i, $1 \leq i \leq n$. This is an improvement of currently the best transference theorem of this type due to Banaszczyk [6], who showed that $\lambda_i(L)\lambda_{n-i+1}(L^*) \leq C'n$, for some universal constant C'. The estimate for this latter product has a long history: Mahler [25] proved that the upper bound $(n!)^2$ holds for all lattices. This was improved by Cassels [10] to $n!$. The first polynomial upper bound was obtained by Lagarias, Lenstra and Schnorr [21] where a bound of $n^2/6$ was shown for all $n \geq 7$. The Banaszczyk bound is optimal up to a constant, for Conway and Thompson (see [26]) showed that there exists a self-dual lattice family $\{L_n\}$ with $\lambda_1(L_n) = \Omega(\sqrt{n})$. Since $g_i(L) \geq \lambda_i(L)$ for all i and for all L, our bound (1) is also optimal up to a constant. For a number of other related results see [5, 17, 6, 7].

We also prove a stronger bound for a special class of lattices where each lattice possesses an n^ϵ-unique shortest vector. This class of lattices plays an important role in the recent breakthrough by Ajtai [1] on the connection between the average-case and the worst-case complexity of the shortest lattice vector problem, and the Ajtai-Dwork public-key cryptosystem [3]. The transference theorems yield a consequent improvement of the Ajtai connection factors in [1].

The motivation for our investigation stems primarily from computational complexity. Recently Ajtai [1] established the first explicit connection between, in a certain technical sense, the worst-case and the average-case complexity of the problem of finding the shortest lattice vector or approximating its length. Moreover, Ajtai [2] proved that it is NP-hard to find the shortest lattice vector in Euclidean norm, as well as approximating the shortest vector length up to a factor of $1 + \frac{1}{2^{n^k}}$. The Ajtai connection [1] of worst-case to average-case complexity for lattice problems has been improved by Cai and Nerurkar [8]. In a forthcoming paper [9], Cai and Nerurkar also improve the NP-hardness result of Ajtai [2] to show that the problem of approximating the shortest vector length up to a factor of $1 + \frac{1}{n^\varepsilon}$, for any $\varepsilon > 0$, is also NP-hard. This improvement also works for all l_p-norms, for $1 \leq p < \infty$. Prior to that, it was known that the shortest lattice vector problem is NP-hard for the l_∞-norm, and the nearest lattice vector problem is NP-hard under all l_p-norms, $p \geq 1$ [20, 29]. Even finding an approximate solution to within any constant factor for the nearest vector problem for any l_p-norm is NP-hard [4]. On the other hand, Lagarias, Lenstra and Schnorr [21] showed, as a consequence of their *transference theorem*, that the approximation problem (in l_2-norm) within a factor of $O(n)$ *cannot* be NP-hard, unless NP = coNP. Goldreich and Goldwasser showed that approximating the shortest lattice vector within a factor of $O(\sqrt{n/\log n})$ is not NP-hard assuming the polynomial time hierarchy does not collapse [11]. Cai showed that finding an $n^{1/4}$-unique shortest lattice vector is not NP-hard unless the polynomial time hierarchy collapses[7].

The recent breakthrough by Ajtai [1, 2] has its motivations from cryptography. It is well known that the security of a cryptographic protocol depends on the intractability of some computational problem *on the average*. Unfortunately as yet we cannot prove any problem in NP intractable, even for the worst case. (This is the NP $\neq$ P question!) For lack of absolute lower bound, one usually takes NP-hardness as "proof" of intractability. However applications to cryptography demand intractability not only in the worst-case but *on the average* as well. Ajtai's paper [1] provided the only known provable connection of worst-case and average-case complexity of a problem in NP believed to be intractable. Building on the Ajtai connection, Ajtai and Dwork [3] have proposed a public-key cryptosystem with *provable* security guarantees based on only the worst-case hardness assumption for an approximate version of the shortest lattice vector problem. More precisely, they defined the notion of an n^c-unique shortest lattice vector, and showed that for a certain c, if finding the shortest lattice vector in a lattice with an n^c-unique shortest vector is hard in the worst case, then their public-key cryptosystem is provably secure. This is the first public-key cryptosystem with such provable security guarantees. Another public-key system based on lattice problems was proposed by Goldreich, Goldwasser and Halevi in [13]. Consequently there is considerable interest recently in the structural and computational properties of these lattices.

Finally we point out that although our work is mostly motivated by computational complexity considerations, our proofs are non-constructive. We build on the work of Banaszczyk [6], using methods from harmonic analysis.

2 Preliminaries

The main tools of our proof are Gaussian-like measures on a lattice, and their Fourier transforms. For a given lattice L of dimension n in $\mathbf{R}^n$, $v \in L$, we define

$$\sigma_L(\{v\}) = \frac{e^{-\pi||v||^2}}{\sum_{x \in L} e^{-\pi||x||^2}}. \tag{2}$$

The Fourier transform of σ_L is

$$\widehat{\sigma_L}(u) = \int_{x \in \mathbf{R}^n} e^{2\pi i \langle u,x \rangle} d\sigma_L = \sum_{v \in L} e^{2\pi i \langle u,v \rangle} \sigma_L(\{v\}), \tag{3}$$

where $u \in \mathbf{R}^n$. Note that σ_L is an even function, so that

$$\begin{aligned} \widehat{\sigma_L}(u) &= \sum_{v \in L} \sigma_L(\{v\}) \cos(2\pi \langle u,v \rangle) & (4) \\ &= \frac{\sum_{v \in L} e^{-\pi||v||^2} \cos(2\pi \langle u,v \rangle)}{\sum_{x \in L} e^{-\pi||x||^2}}. & (5) \end{aligned}$$

Define

$$\tau_L(u) = \frac{\sum_{y \in L+u} e^{-\pi||y||^2}}{\sum_{x \in L} e^{-\pi||x||^2}}. \tag{6}$$

Then the following identities hold

Lemma 2.1

$$\widehat{\sigma_L}(u) = \tau_{L^*}(u), \tag{7}$$

where L^* is the dual lattice of L. By duality

$$\widehat{\sigma_{L^*}}(u) = \tau_L(u). \tag{8}$$

The proof of Lemma 2.1 uses Poisson summation formula, see [18, 6]. The following lemma is proved in [6] (Lemma 1.5) and is crucial to our proof (in the following $\backslash$ denotes set difference):

Lemma 2.2 *For each $c \geq 1/\sqrt{2\pi}$,*

$$\sigma_L(L \backslash B(0; c\sqrt{n})) = \frac{\sum_{v \in L \backslash B(0;c\sqrt{n})} e^{-\pi||v||^2}}{\sum_{x \in L} e^{-\pi||x||^2}} < \left(c\sqrt{2\pi e}e^{-\pi c^2}\right)^n; \tag{9}$$

and for all $u \in \mathbf{R}^n$,

$$\frac{\sum_{v \in (L+u) \backslash B(0;c\sqrt{n})} e^{-\pi||v||^2}}{\sum_{x \in L} e^{-\pi||x||^2}} < 2\left(c\sqrt{2\pi e}e^{-\pi c^2}\right)^n. \tag{10}$$

3 The First Inequality

For simplicity we first present an inequality relating the minimal length $g(L)$ of a generating set of lattice vectors for L, with the shortest lattice vector length $\lambda_1(L^*)$ of its dual L^*. In this simpler setting, the main idea of the proof can be seen more transparently without unnecessary complications. In the next section a general version of this inequality will be proved relating $g_i(L)$ and $\lambda_{n-i+1}(L^*)$, of which the inequality in this section is a special case.

Theorem 3.1 *For every lattice L of dimension n, and for every constant $c > 3/2\pi$,*

$$g(L)\lambda_1(L^*) \leq cn,$$

for all sufficiently large n.

We prove by contradiction. Suppose $g(L)\lambda_1(L^*) > cn$. Let c_1 and c_2 be two constants, such that $c_1c_2 = c$ and $c_1 > 1/\sqrt{2\pi}$ and $c_2 > 3/\sqrt{2\pi}$. By substituting L with sL for a suitable scaling factor s, we may assume that

$$g(L) > c_1\sqrt{n}$$

and

$$\lambda_1(L^*) > c_2\sqrt{n}.$$

Let L' be the sublattice of L generated by the intersection $L \cap B(0; c_1\sqrt{n})$, where $B(0; c_1\sqrt{n})$ is the n-dimensional ball of radius $c_1\sqrt{n}$ centered at 0. Then L' is a proper sublattice of L. If $\dim L' < n$, then let P be the linear span of L', and let $b_1, \ldots, b_i$ be a lattice basis of $L \cap P$, where $i = \dim L' < n$. This can be extended to a lattice basis $b_1, \ldots, b_i, \ldots, b_n$ for L and we may replace L' by the sublattice generated by $b_1, \ldots, b_i, \ldots, 2b_n$, say. Thus without loss of generality we may assume L' is of dimension n. The important point is that we have a proper sublattice $L' \subset L$, which is of dimension n and contains $L \cap B(0; c_1\sqrt{n})$.

For any fixed $u \in \mathbf{R}^n$,

$$\begin{aligned}
\widehat{\sigma_L}(u) &= \sum_{v\in L} \sigma_L(\{v\}) \cos(2\pi\langle u, v\rangle) \\
&= \sum_{v\in L'} \sigma_{L'}(\{v\}) \cos(2\pi\langle u, v\rangle) + \sum_{v\in L'} (\sigma_L(\{v\}) - \sigma_{L'}(\{v\})) \cos(2\pi\langle u, v\rangle) \\
&\quad + \sum_{v\in L\setminus L'} \sigma_L(\{v\}) \cos(2\pi\langle u, v\rangle) \\
&= \widehat{\sigma_{L'}}(u) + A + B, \qquad \text{say.}
\end{aligned}$$

Since $L \cap B(0; c_1\sqrt{n}) \subset L'$, the last term

$$\begin{aligned}
|B| &\leq \sum_{v\in L\setminus B(0;c_1\sqrt{n})} \sigma_L(\{v\}) \\
&= \sigma_L(L\setminus B(0; c_1\sqrt{n})) \\
&< \left(c_1\sqrt{2\pi e}e^{-\pi c_1^2}\right)^n,
\end{aligned}$$

by Lemma 2.2 inequality (9). Denote the last term by ϵ_1^n, say.

For the other error term A, we note that $\sigma_L(\{v\}) < \sigma_{L'}(\{v\})$, so that

$$\begin{aligned}
|A| &\leq \sum_{v\in L'} |\sigma_L(\{v\}) - \sigma_{L'}(\{v\})| \\
&= \sum_{v\in L'} [\sigma_{L'}(\{v\}) - \sigma_L(\{v\})] \\
&= \sum_{v\in L'} e^{-\pi||v||^2} \left[\frac{1}{\sum_{x\in L'} e^{-\pi||x||^2}} - \frac{1}{\sum_{x\in L} e^{-\pi||x||^2}}\right] \\
&= \sum_{v\in L'} e^{-\pi||v||^2} \frac{\sum_{z\in L\setminus L'} e^{-\pi||z||^2}}{\sum_{x\in L'} e^{-\pi||x||^2} \cdot \sum_{y\in L} e^{-\pi||y||^2}} \\
&= \frac{\sum_{z\in L\setminus L'} e^{-\pi||z||^2}}{\sum_{y\in L} e^{-\pi||y||^2}} \\
&= \sum_{z\in L\setminus L'} \sigma_L(\{z\}).
\end{aligned}$$

But we have already seen that

$$\sum_{z\in L\setminus L'} \sigma_L(\{z\}) \leq \sum_{v\in L\setminus B(0;c_1\sqrt{n})} \sigma_L(\{v\}) < \epsilon_1^n.$$

Hence

$$\widehat{\sigma_L}(u) > \widehat{\sigma_{L'}}(u) - 2\epsilon_1^n. \tag{11}$$

Our next task is to show that we can choose an appropriate u so that $\widehat{\sigma_L}(u)$ is small yet $\widehat{\sigma_{L'}}(u)$ is large. By Lemma 2.1, we have $\widehat{\sigma_L}(u) = \tau_{L^*}(u)$, and $\widehat{\sigma_{L'}}(u) = \tau_{L'^*}(u)$. Thus we only need to choose a u such that $\tau_{L^*}(u)$ is small and $\tau_{L'^*}(u)$ is large.

We need the following lemma.

Lemma 3.1 *Suppose L_1 is a proper sublattice of L_2, then there exists a $p \in L_2$, such that*

$$\min_{q \in L_1} ||p - q|| \geq \frac{\lambda_1(L_1)}{3}.$$

(Since a lattice is a discrete subset of $\mathbf{R}^n$, the above minimum over q clearly exists.)

Proof: Suppose such a p does not exist. Then for all $p \in L_2$,

$$\min_{q \in L_1} ||p - q|| < \frac{\lambda_1(L_1)}{3}.$$

Take any $p \in L_2 \backslash L_1$. Then there exists a $q \in L_1$, such that $||p - q|| < \lambda_1(L_1)/3$. Let $u = p - q$, then $u \in L_2 \backslash L_1$, in particular $u \neq 0$.

Consider the following set of lattice points in L_2: $\{ku | k \in \mathbf{Z} \text{ and } k \geq 1\}$. By assumption, each ku is associated with a point in L_1, with distance less than $\lambda_1(L_1)/3$. By definition, u is associated to 0. But for k large, clearly ku cannot be associated to 0. This is certainly true when $k \geq \lambda_1(L_1)/(3||u||)$. Let k_0 be the first k such that ku is associated to a $z \in L_1$, where $z \neq 0$. Then $k_0 > 1$. It follows that

$$||z|| = ||z - 0|| = ||(z - k_0 u) + u + ((k_0 - 1)u - 0)|| < \lambda_1(L_1),$$

a contradiction. The Lemma is proved. $\square$

Now we note that since L' is a full ranked proper sublattice of L, L^* is a proper sublattice of L'^*. That it is proper follows from the identity of index

$$\det(L'^*)/\det(L^*) = \det(L)/\det(L') > 1.$$

By Lemma 3.1, take a $u \in L'^*$, such that $\min_{q \in L^*} ||u - q|| \geq \frac{\lambda_1(L^*)}{3}$. Then since $u \in L'^*$, we have $L'^* + u = L'^*$, and

$$\tau_{L'^*}(u) = \frac{\sum_{x \in L'^* + u} e^{-\pi ||x||^2}}{\sum_{x \in L'^*} e^{-\pi ||x||^2}} = 1.$$

On the other hand, since

$$\min_{q \in L^*} ||u - q|| \geq \frac{\lambda_1(L^*)}{3} > \frac{c_2}{3}\sqrt{n},$$

we note that no point in $L^* + u$ is within $\frac{c_2}{3}\sqrt{n}$ in norm, and so

$$\tau_{L^*}(u) \quad = \quad \frac{\sum_{x \in L^* + u} e^{-\pi ||x||^2}}{\sum_{x \in L^*} e^{-\pi ||x||^2}}$$

$$\begin{aligned}
&= \frac{\sum_{v \in (L^*+u) \setminus B(0; c_2\sqrt{n}/3)} e^{-\pi ||v||^2}}{\sum_{x \in L^*} e^{-\pi ||x||^2}} \\
&< 2\left(\frac{c_2}{3}\sqrt{2\pi e} e^{-\pi \left(\frac{c_2}{3}\right)^2}\right)^n \\
&= 2\epsilon_2^n,
\end{aligned}$$

by Lemma 2.2 inequality (10). Since both c_1 and $c_2/3 > 1/\sqrt{2\pi}$, we have both ϵ_1 and $\epsilon_2 < 1$ by elementary estimate. Thus it follows from (11) that

$$2\epsilon_2^n > 1 - 2\epsilon_1^n,$$

which is a contradiction for large n. The proof of Theorem 3.1 is complete.

4 The General Inequality

We now prove a general inequality which relates the quantities $g_i(L)$ and $\lambda_{n-i+1}(L^*)$. This theorem generalizes the result of the last section as well as the transference theorem of Banaszczyk [6].

Theorem 4.1 *For every constant $c > 3/2\pi$, there exists an n_0, such that*

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

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

We prove Theorem 4.1 by contradiction. The main idea will be similar to the proof in the last section, relying on a double estimate for the Fourier transforms of Gaussian-like measures on the lattice and a proper sublattice. But the details are more involved.

Suppose the inequality does not hold. Choose c_1 and c_2 as before. By a suitable scaling factor, we may assume that both

$$g_{n-i+1}(L) > c_1\sqrt{n},$$

and

$$\lambda_i(L^*) > c_2\sqrt{n}.$$

Let $u_1, \ldots, u_{i-1}$ be a set of linearly independent lattice vectors in L^* attaining the successive minima $\lambda_1(L^*), \ldots, \lambda_{i-1}(L^*)$, respectively. Let S be the linear subspace of $\mathbf{R}^n$ spanned by $u_1, \ldots, u_{i-1}$. Thus $\dim S = i - 1$ and there are no vectors in $L^* \setminus S$ with norm less than $\lambda_i(L^*)$. For suppose there were some $u \in L^* \setminus S$, $||u|| < \lambda_i(L^*)$. Let $j = \min\{k \mid ||u|| < \lambda_k(L^*)\}$. Then $1 \leq j \leq i$. Let $C = \{u_1, \ldots, u_{j-1}, u\}$. It is clear that C is a set of j linearly independent vectors in L^*, with $\max\{||x|| \mid x \in C\} = ||u|| < \lambda_j(L^*)$. A contradiction. In particular there are no vectors in $L^* \setminus S$ with norm less than or equal to $c_2\sqrt{n}$.

$L^* \cap S$ is a lattice of dimension $i - 1$. Let $v_1^*, \ldots, v_{i-1}^*$ be a basis of $L^* \cap S$, and this can be extended to a basis $v_1^*, \ldots, v_{i-1}^*, v_i^*, \ldots, v_n^*$ for the lattice L^*. Let $v_1, \ldots, v_n$ be its dual basis for L. We note that $v_1^*, \ldots, v_{i-1}^*$ is also a vector space basis for S, while $v_i, \ldots, v_n$ is a vector space basis for $S^\perp$ as well as a lattice basis for the sublattice $L \cap S^\perp$ of L.

We now define two projections from $\mathbf{R}^n$ to $S^\perp$:

$$\pi \quad : \quad \mathbf{R}^n \longrightarrow S^\perp \tag{12}$$

$$\sum_{j=1}^{i-1} x_j v_j^* + \sum_{j=i}^{n} x_j v_j \mapsto \sum_{j=i}^{n} x_j v_j, \tag{13}$$

is the orthogonal projection onto $S^\perp$, and

$$\varphi \quad : \quad \mathbf{R}^n \longrightarrow S^\perp \tag{14}$$

$$\sum_{j=1}^{n} x_j v_j \mapsto \sum_{j=i}^{n} x_j v_j, \tag{15}$$

is the projection "modulo $v_1, \ldots, v_{i-1}$ in terms of the basis $v_1, \ldots, v_n$". We note that both projections are well defined, and

$$\varphi(L) = L \cap S^\perp = \{\sum_{j=i}^{n} x_j v_j \mid x_j \in \mathbf{Z}\}.$$

We need several technical lemmas.

Lemma 4.1

$$\pi(L^*) = (L \cap S^\perp)^*.$$

Proof: We have noted already that $L \cap S^\perp$ is a sublattice of L of dimension $n - i + 1$ with lattice basis $v_i, \ldots, v_n$. Thus its dual lattice $(L \cap S^\perp)^*$ is also an $(n-i+1)$-dimensional lattice in the space $S^\perp$.

For every $v \in \pi(L^*)$, there exists a $v' \in L^*$, such that $v = \pi(v')$, i.e., $v - v' \in S$. Hence, for all $x \in S^\perp$,

$$\langle v, x \rangle = \langle v', x \rangle.$$

In particular, for all $x \in L \cap S^\perp$, $\langle v, x \rangle$ is an integer. Thus, $v \in (L \cap S^\perp)^*$.

Conversely, for every $v \in (L \cap S^\perp)^*$, let

$$v' = v - \sum_{j=1}^{i-1} \langle v, v_j \rangle v_j^*.$$

We claim that $\pi(v') = v$, and $v' \in L^*$, thus $v \in \pi(L^*)$. It is clear that $\pi(v') = v$, since $\sum_{j=1}^{i-1} \langle v, v_j \rangle v_j^* \in S$. It is also clear that for each basis vector v_j of L, if $j \leq i-1$ then $\langle v', v_j \rangle = 0$, and if $j \geq i$ then $\langle v', v_j \rangle = \langle v, v_j \rangle \in \mathbf{Z}$, since $v_j \in L \cap S^\perp$ for $j \geq i$. □

Let L' be the sublattice of L generated by all lattice vectors of L with length at most $c_1\sqrt{n}$, namely $L \cap B(0; c_1\sqrt{n})$. As $g_{n-i+1}(L) > c_1\sqrt{n}$, L' does not contain any $(n-i+1)$-dimensional saturated sublattice of L.

Lemma 4.2 *$\varphi(L')$ is a proper sublattice of $L \cap S^{\perp}$.*

Proof: Clearly $\varphi(L') \subseteq \varphi(L) = L \cap S^{\perp}$. To show that it is a proper sublattice let's assume $\varphi(L') = L \cap S^{\perp}$. Then $v_i, \ldots, v_n \in \varphi(L')$. It follows that there are vectors $w_i, \ldots, w_n \in L'$, $v_j = \varphi(w_j)$, $j = i, \ldots, n$. Thus, each $w_j = v_j + \sum_{k=1}^{i-1} x_{jk} v_k$ for some integers x_{jk}, $j = i, \ldots, n$ and $k = 1, \ldots, i-1$.

Let T be the linear subspace generated by $w_i, \ldots, w_n$. Clearly $w_i, \ldots, w_n$ are linearly independent, so $\dim T = n - i + 1$, and $L \cap T$ is a saturated $(n-i+1)$-dimensional sublattice of L. By the definition of L', L' does not contain $L \cap T$.

However I claim that $L' \cap T = L \cap T$. This would be a contradiction which would prove the lemma.

To show that $L' \cap T = L \cap T$, let any $u \in L \cap T$. $u \in T$ implies that there exist real numbers $r_i, \ldots, r_n$ such that $u = \sum_{j=i}^{n} r_j w_j$. $u \in L$ implies that in the above expression, when expressed in terms of $v_1, \ldots, v_n$, all coefficients in $v_1, \ldots, v_n$ are integers. In particular, the coefficients of $v_i, \ldots, v_n$, namely $r_i, \ldots, r_n$, are all integers. Thus, u belongs to the integral span of $w_i, \ldots, w_n \in L'$, and thus $u \in L'$. $\square$

We now wish to replace $\varphi(L')$ by a full ranked proper sublattice $\tilde{L}$ of $L \cap S^{\perp}$, which contains $\varphi(L')$ (if $\varphi(L')$ is not already one). If $\dim(\varphi(L')) = n - i + 1$, then $\varphi(L')$ is already full ranked, we simply let $\tilde{L} = \varphi(L')$. If however, $\dim(\varphi(L')) < n - i + 1$, then we let $\tilde{L}$ be any proper sublattice of $L \cap S^{\perp}$, which is of dimension $n - i + 1$ and contains $\varphi(L')$. This can be accomplished as follows, for example. Let $k = \dim(\varphi(L')) \le n - i$, and let $b_1, \ldots, b_k$ be a lattice basis of $L \cap \mathrm{span}(\varphi(L'))$. This can be extended to a lattice basis of $L \cap S^{\perp}$, say $b_1, \ldots, b_k, \ldots, b_{n-i+1}$. Then we may let $\tilde{L}$ be the integral span of $b_1, \ldots, b_k, \ldots, 2b_{n-i+1}$, say.

Summarizing,

Lemma 4.3 *1. $\varphi(L') \subseteq \tilde{L}$;*

2. $\dim \tilde{L} = n - i + 1$; and

3. $\tilde{L}$ is a proper sublattice of $L \cap S^{\perp}$.

Now we let

$$L'' = \tilde{L} \oplus \langle v_1 \rangle \oplus \cdots \oplus \langle v_{i-1} \rangle.$$

Lemma 4.4 *1. $L' \subseteq L''$;*

2. $\dim L'' = n$; and

3. L'' is a proper sublattice of L.

Proof: For any $v \in L'$,

$$v = \varphi(v) + \sum_{k=1}^{i-1} x_k v_k,$$

for some integers x_k. Since $\varphi(v) \in \varphi(L') \subseteq \tilde{L}$, it follows that $v \in L''$.

$\dim L'' = n$ follows directly by the definition of L'' and $\dim(\tilde{L}) = n - i + 1$.

Finally, we show that L'' is a proper sublattice of L. That L'' is a sublattice of L is trivial. Moreover, $\varphi(L'') = \tilde{L}$ is a proper sublattice of $L \cap S^{\perp} = \varphi(L)$, hence L'' is a proper sublattice of L. $\square$

Corollary 4.1 *L^* is a proper sublattice of $(L'')^*$.*

Lemma 4.5 *There exists a vector $x \in (L'')^* \backslash (L^* + S)$.*

Proof: Since $\tilde{L}$ is a proper sublattice of $L \cap S^{\perp}$ of full rank in the linear space $S^{\perp}$, $(\tilde{L})^*$ is an $(n - i + 1)$-dimensional lattice in $S^{\perp}$ properly containing $(L \cap S^{\perp})^* = \pi(L^*)$. In particular there exists a $y \in (\tilde{L})^* \backslash \pi(L^*)$. Let

$$x = y - \sum_{k=1}^{i-1} \langle y, v_k \rangle v_k^*.$$

Then $\pi(x) = y$. This implies that $x \notin L^* + S$, for otherwise, $y = \pi(x) \in \pi(L^*)$.

We show next that $x \in (L'')^*$. Since $\dim L'' = n$ all we need to show is that for every $w \in L''$, $\langle x, w \rangle \in \mathbf{Z}$. Take any $w \in L''$,

$$w = \varphi(w) + \sum_{\ell=1}^{i-1} y_\ell v_\ell,$$

for some integral y_ℓ. By the definition of L'', $\varphi(w) \in \tilde{L}$. Then it is easy to verify that

$$\langle x, w \rangle = \langle y, \varphi(w) \rangle,$$

which belongs to $\mathbf{Z}$ since $y \in (\tilde{L})^*$ and $\varphi(w) \in \tilde{L}$. $\square$

Now we come to the crucial combinatorial lemma:

Lemma 4.6 *There exists $x \in (L'')^*$, such that*

$$\min_{y \in L^*} ||x - y|| \geq \frac{\lambda_i(L^*)}{3}.$$

Proof: Suppose not. Then for every $x \in (L'')^*$, there exists a $y \in L^*$ such that

$$||x - y|| < \frac{\lambda_i(L^*)}{3}.$$

In particular we may choose our $x \in (L'')^* \backslash (L^* + S)$ by Lemma 4.5. Let $y \in L^*$ be the corresponding point in L^* as above. Denote $x - y$ by u, then we still have $u \in (L'')^* \backslash (L^* + S)$, for clearly $u \in (L'')^*$ by Corollary 4.1; and $u \notin L^* + S$, otherwise $x \in L^* + S$ as well. In particular $u \notin S$. Moreover, $||u|| < \frac{\lambda_i(L^*)}{3}$.

Consider the set of points $\{ku \mid k = 1, 2, \ldots\}$. Each ku is associated with a point in L^* of distance less than $\lambda_i(L^*)/3$. Since $u \notin S$, for sufficiently large k, the associated point of L^*

cannot be in S. Let k_0 be the first such k, then $k_0 > 1$. Let $z \in L^* \backslash S$ be the point associated with $k_0 u$ and $z' \in L^* \cap S$ be the point associated with $(k_0 - 1)u$. Then $z - z' \in L^* \backslash S$. Furthermore,

$$||z - z'|| = ||(z - k_0 u) + u + ((k_0 - 1)u - z')|| < \lambda_i(L^*).$$

This contradicts the definition of S and $\lambda_i(L^*)$. □

We are now ready to prove Theorem 4.1. We will pick u to be the x promised in Lemma 4.6. Then as before

$$\begin{aligned}
\widehat{\sigma_L}(u) &= \sum_{v \in L} \sigma_L(\{v\}) \cos(2\pi \langle u, v \rangle) \\
&= \sum_{v \in L''} \sigma_{L''}(\{v\}) \cos(2\pi \langle u, v \rangle) + \sum_{v \in L''} (\sigma_L(\{v\}) - \sigma_{L''}(\{v\})) \cos(2\pi \langle u, v \rangle) \\
&\quad + \sum_{v \in L \backslash L''} \sigma_L(\{v\}) \cos(2\pi \langle u, v \rangle) \\
&= \widehat{\sigma_{L''}}(u) + A + B, \qquad \text{say.}
\end{aligned}$$

Since $L \cap B(0; c_1\sqrt{n}) \subset L' \subseteq L''$, the last term

$$\begin{aligned}
|B| &\leq \sum_{v \in L \backslash B(0; c_1\sqrt{n})} \sigma_L(\{v\}) \\
&< \left(c_1 \sqrt{2\pi e} e^{-\pi c_1^2}\right)^n \\
&= \epsilon_1^n,
\end{aligned}$$

by Lemma 2.2 inequality (9).

For the other error term A, we note that $\sigma_L(\{v\}) < \sigma_{L''}(\{v\})$, so that we have as before

$$\begin{aligned}
|A| &\leq \sum_{v \in L''} |\sigma_L(\{v\}) - \sigma_{L''}(\{v\})| \\
&= \sum_{v \in L''} [\sigma_{L''}(\{v\}) - \sigma_L(\{v\})] \\
&= \sum_{v \in L''} e^{-\pi||v||^2} \left[\frac{1}{\sum_{x \in L''} e^{-\pi||x||^2}} - \frac{1}{\sum_{x \in L} e^{-\pi||x||^2}} \right] \\
&= \sum_{v \in L''} e^{-\pi||v||^2} \frac{\sum_{z \in L \backslash L''} e^{-\pi||z||^2}}{\sum_{x \in L''} e^{-\pi||x||^2} \cdot \sum_{y \in L} e^{-\pi||y||^2}} \\
&= \frac{\sum_{z \in L \backslash L''} e^{-\pi||z||^2}}{\sum_{y \in L} e^{-\pi||y||^2}} \\
&\leq \sigma_L(L \backslash B(0; c_1\sqrt{n})) \\
&< \epsilon_1^n.
\end{aligned}$$

Hence

$$\widehat{\sigma_L}(u) > \widehat{\sigma_{L''}}(u) - 2\epsilon_1^n.$$

By Lemma 2.1 $\widehat{\sigma_L}(u) = \tau_{L^*}(u)$ and $\widehat{\sigma_{L''}}(u) = \tau_{(L'')^*}(u)$. Since $u \in (L'')^*$, $(L'')^* + u = (L'')^*$ so that $\tau_{(L'')^*}(u) = 1$.

On the other hand, since

$$\min_{p \in L^*} ||u - p|| \geq \frac{\lambda_1(L^*)}{3} > \frac{c_2}{3}\sqrt{n},$$

we note that no point in $L^* + u$ is within $\frac{c_2}{3}\sqrt{n}$ in norm, and so

$$\begin{aligned}
\tau_{L^*}(u) &= \frac{\sum_{x \in L^*+u} e^{-\pi||x||^2}}{\sum_{x \in L^*} e^{-\pi||x||^2}} \\
&= \frac{\sum_{v \in (L^*+u)\setminus B(0;c_2\sqrt{n}/3)} e^{-\pi||v||^2}}{\sum_{x \in L^*} e^{-\pi||x||^2}} \\
&< 2\left(\frac{c_2}{3}\sqrt{2\pi e}e^{-\pi\left(\frac{c_2}{3}\right)^2}\right)^n \\
&= 2\epsilon_2^n,
\end{aligned}$$

by Lemma 2.2 inequality (10). Since both c_1 and $c_2/3 > 1/\sqrt{2\pi}$, both ϵ_1 and $\epsilon_2 < 1$ as before. Thus

$$2\epsilon_2^n > 1 - 2\epsilon_1^n,$$

which is a contradiction for large n. The proof of Theorem 4.1 is complete.

We remark that it is known that the product $\lambda_i(L)\lambda_{n-i+1}(L^*)$ is at least 1 for all L and all $1 \leq i \leq n$. Since $g_i(L) \geq \lambda_i(L)$, we also have $g_i(L)\lambda_{n-i+1}(L^*) \geq 1$ for all L and i, and this lower bound is easily achievable, for example by the Gaussian lattice $\mathbf{Z}^n$.

We also remark that the inequality in Theorem 4.1 can be made to hold for all n, and not just for sufficiently large n, with an appropriate constant c. For example, $c = 2$ will do, with $c_1 = \sqrt{2/3}$ and $c_2 = \sqrt{6}$.

5 n^ϵ-Unique Shortest Vector

We say that a lattice L has an n^ϵ-unique shortest vector if there exists $v \in L$, $v \neq 0$, such that for all $v' \in L$, if $||v'|| \leq n^\epsilon \cdot ||v||$, then v' is an integral multiple of v. Equivalently $\lambda_2(L)/\lambda_1(L) > n^\epsilon$. This class of lattices plays an important role in the recent work of Ajtai [1] on the connection between the average-case and the worst-case complexity of the shortest lattice vector problem, and in the Ajtai-Dwork public-key cryptosystem [3]. They showed that for a certain c, if finding the shortest lattice vector in a lattice with an n^c-unique shortest vector is hard in the worst case, then the Ajtai-Dwork public-key cryptosystem is provably secure.

Theorem 5.1 *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,*

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

for all sufficiently large n.

Proof: Choose c_1 and c_2 as before such that $c_1c_2 = c > 3/2\pi$, and $c_1, c_2/3 > 1/\sqrt{2\pi}$. By a suitable scaling factor, we may assume that both

$$g(L) > c_1\sqrt{n},$$

and

$$\lambda_1(L^*) > c_2 n^{1/2-\epsilon}.$$

By n^ϵ-uniqueness, $\lambda_2(L^*) > c_2\sqrt{n}$. Take a ball of radius $c_1\sqrt{n}$, and let L' be the sublattice generated by $L \cap B(0; c_1\sqrt{n})$. As $g(L) > c_1\sqrt{n}$, L' is a proper sublattice of L. Again we may assume without loss of generality that $\dim L' = n$. As before, for all $u \in \mathbf{R}^n$, we get

$$\widehat{\sigma_L}(u) > \widehat{\sigma_{L'}}(u) - 2\epsilon_1^n. \tag{16}$$

L^* is a proper sublattice of $(L')^*$. Therefore by Lemma 3.1 there exists $u \in (L')^* \backslash L^*$, such that

$$\min_{q \in L^*} ||u - q|| \geq \lambda_1(L^*)/3 \geq c_2 n^{1/2-\epsilon}/3.$$

If we take this u, then

$$\widehat{\sigma_{L'}}(u) = \tau_{(L')^*}(u) = 1. \tag{17}$$

We now estimate

$$\widehat{\sigma_L}(u) = \tau_{L^*}(u) = \frac{\sum_{x \in L^*+u} e^{-\pi||x||^2}}{\sum_{x \in L^*} e^{-\pi||x||^2}}.$$

The denominator is at least 1. For the numerator, we separate those terms where $||x|| \leq c_2\sqrt{n}/3$ from the rest. If there are no terms with $||x|| \leq c_2\sqrt{n}/3$ we are done since as before

$$\widehat{\sigma_L}(u) = \frac{\sum_{x \in (L^*+u) \backslash B(0, c_2\sqrt{n}/3)} e^{-\pi||x||^2}}{\sum_{x \in L^*} e^{-\pi||x||^2}} < 2\epsilon_2^n.$$

So let's assume such terms exist. Let $x_0 \in L^* + u$ be of minimum norm. Note that $||x_0|| \geq \lambda_1(L^*)/3 > c_2 n^{1/2-\epsilon}/3$.

Suppose $x, x' \in L^* + u$ and both $||x||$ and $||x'|| \leq c_2\sqrt{n}/3$. Then $x - x' \in L^*$, and $||x - x'|| \leq 2c_2\sqrt{n}/3 < \lambda_2(L^*)$. Thus $x - x'$ is an integral multiple of the shortest vector $v_1 \in L^*$ where $||v_1|| = \lambda_1(L^*)$. Thus $x \in \langle v_1 \rangle + x_0$, the one-dimensional affine sublattice of $L^* + u$. Separate the sum $\sum_{x \in L^*+u} e^{-\pi||x||^2}$ into two sums, one over the one-dimensional affine sublattice $\langle v_1 \rangle + x_0$, and a second sum over all other terms. Then the second sum is bounded by $2\epsilon_2^n$ as before, since all $||x||$ there are more than $c_2\sqrt{n}/3$.

For the first sum, take an orthogonal projection of x_0 to the linear span $\mathbf{R}v_1 + x_0$ of the one-dimensional affine sublattice $\langle v_1 \rangle + x_0$, then a simple geometric observation shows that

$$\sum_{x \in \langle v_1 \rangle + x_0} e^{-\pi||x||^2} < 2\sum_{k=0}^{\infty} e^{-\pi(1/9+k^2)c_2^2 n^{1-2\epsilon}} = e^{-\Omega(n^{1-2\epsilon})},$$

for $\epsilon < 1/2$. Thus, we derive that

$$\widehat{\sigma_L}(u) = \tau_{L^*}(u) < e^{-\Omega(n^{1-2\epsilon})} + 2\epsilon_2^n. \tag{18}$$

This is a contradiction to (16) and (17) for large n.

A more careful analysis shows that the theorem is valid even for the case $\epsilon = 1/2$. The details are given in the appendix. □

The upper bound $O(n^{1-\epsilon})$ is optimal up to a constant, for all ϵ, $0 < \epsilon \leq 1/2$. Consider the family of self-dual lattices of Conway and Thompson [26]. Let L' be such a lattice of dimension $n-1$. $L'^* = L'$ and $\lambda_1(L') = \Theta(\sqrt{n})$. Let u be a vector perpendicular to the linear span of L' with norm $||u|| = n^{-\epsilon}\lambda_1(L') = \Theta(n^{1/2-\epsilon})$. Define

$$L^* = L' \oplus \langle u \rangle.$$

Clearly $\lambda_1(L^*) = ||u||$, and u is an n^ϵ-unique shortest vector of L^*.

It follows that

$$L = L^{**} = L' \oplus \langle \frac{u}{||u||^2} \rangle,$$

since u is perpendicular to the linear span of L'. Hence, L consists of parallel translations of L' with orthogonal distance $1/||u||$.

If we orthogonally project any n linearly independent lattice vectors of L to the $(n-1)$-dimensional linear span of L', we must collect among which $n-1$ linearly independent lattice vectors of L'. Thus, $\lambda_n(L) \geq \lambda_{n-1}(L') = \Theta(\sqrt{n})$. Hence

$$\lambda_n(L)\lambda_1(L^*) = \Omega(n^{1-\epsilon}).$$

It also follows that

$$g(L)\lambda_1(L^*) = \Omega(n^{1-\epsilon}).$$

Theorem 5.2 *For every lattice L of dimension n, if L^* has an n^c-unique shortest vector, then*

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

where

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

Proof: The inequality $\lambda_n(L)\lambda_1(L^*) \geq 1$ is known. The case $c \leq 1/2$ has been proved, since $g(L) \geq \lambda_n(L)$. Note that if L has an n^c-unique shortest vector then it also has an $n^{c'}$-unique shortest vector, for $c' < c$. Hence we only need to prove the case for $1 < c \leq 3/2$.

Let u be an n^c-unique shortest vector for L^*. Let S be the linear span of u and let π be the orthogonal projection to $S^\perp$. Then $\pi(L^*) = (L \cap S^\perp)^*$ by Lemma 4.1. Moreover $(L \cap S^\perp)^*$ has no "short" vectors compared to u. More precisely, if $w \in (L \cap S^\perp)^*$ is a non-zero vector, then by lifting via π^{-1} to a vector in L^*, we see that

$$||w||^2 + ||u||^2/4 > (n^c||u||)^2.$$

It follows that $\lambda_1((L \cap S^\perp)^*) = \min_{0 \neq w \in (L \cap S^\perp)^*} ||w|| \geq ||u||\sqrt{n^{2c} - 1/4}$. By Theorem 3.1,

$$\lambda_{n-1}(L \cap S^\perp) \leq O\left(\frac{n-1}{\lambda_1((L \cap S^\perp)^*)}\right) = O\left(\frac{n^{1-c}}{||u||}\right).$$

Consider the Gram-Schmidt orthogonalization of $n-1$ linearly independent lattice vectors of $L \cap S^\perp$ with norm at most $\lambda_{n-1}(L \cap S^\perp)$. They form a parallelepiped whose sides are mutually orthogonal and are at most $\lambda_{n-1}(L \cap S^\perp)$. The linear space $S^\perp$ has a "brick" tiling by the translations of this parallelepiped centered at each lattice point of $L \cap S^\perp$.

The closest parallel hyperplane H to $S^\perp$ which intersects L has orthogonal distance $1/||u||$ to $S^\perp$. Consider the "brick" tiling of this parallel plane H where each orthogonal parallelepiped is centered at a point of $L \cap H$. It follows that every point of H is within distance $\lambda_{n-1}(L \cap S^\perp) \cdot \sqrt{n-1}/2$ from a point in $L \cap H$. In particular we have a lattice vector in $L \cap H$ whose length is bounded by

$$O\left(\frac{1}{||u||} + \frac{n^{3/2-c}}{||u||}\right).$$

This vector must be linearly independent from the $n-1$ independent vectors in $L \cap S^\perp$ with norm at most $\lambda_{n-1}(L \cap S^\perp)$.

It follows that if $1 < c \le 3/2$, then $\lambda_n(L) = O(\frac{n^{3/2-c}}{||u||})$. Since $\lambda_1(L^*) = ||u||$ the theorem follows. $\square$

6 Ajtai's Connection Factor

The recent work by Ajtai [1] establishing the worst-case and the average-case complexity of shortest lattice vector problems can be improved by these transference theorems.

Let n, m, q be positive integers. Let $\mathbf{Z}_q$ be the integers mod q, and let $\mathbf{Z}_q^{n\times m}$ denote the set of $n \times m$ matrices over $\mathbf{Z}_q$. For every n, m, q, $\Omega_{n,m,q}$ denotes the uniform distribution on $\mathbf{Z}_q^{n\times m}$. For every $X \in \mathbf{Z}_q^{n\times m}$, the set $\Lambda(X) = \{y \in \mathbf{Z}^m \mid Xy \equiv 0 \bmod q\}$ defines a lattice of dimension m. $\Lambda = \Lambda_{n,m,q}$ denotes the probability space of lattices consisting of $\Lambda(X)$ by choosing X according to $\Omega_{n,m,q}$. By Minkowski's Theorem it can be proved that, $\forall c\ \exists c'$ s.t. $\forall \Lambda(X) \in \Lambda_{n,c'n,n^c}\ \exists v\ (v \in \Lambda(X)$ and $0 < \|v\| \le n)$.

Theorem 6.1 *Let $\epsilon > 0$. Assume there is a probabilistic polynomial time algorithm $\mathcal{A}$ that, with probability $1/n^{\Omega(1)}$, finds a non-zero vector of length at most n, for a uniformly chosen lattice in the class $\Lambda_{n,m,q}$, where $m = \Theta(n)$ and $q = \Theta(n^3)$. Then there is a probabilistic polynomial-time algorithm $\mathcal{B}$ that, given any integral lattice L of dimension n, with probability $1 - e^{-n}$ will*

(a) compute an estimate of $\lambda_1 = \lambda_1(L)$ up to a factor $n^{4+\epsilon}$, i.e., compute a numerical estimate $\tilde{\lambda}_1$, such that

$$\frac{\lambda_1}{n^{4+\epsilon}} \le \tilde{\lambda}_1 \le \lambda_1;$$

(b) compute an estimate of λ_1 up to a factor $n^{3+\delta+\epsilon}$, if L has an n^c-unique shortest vector, where

$$\delta = \begin{cases} 1-c & \text{if } 0 < c \le 1/2, \\ 1/2 & \text{if } 1/2 < c \le 1, \\ 3/2 - c & \text{if } 1 < c \le 3/2, \\ 0 & \text{if } c > 3/2; \end{cases}$$

(c) find the unique shortest vector if it is an $n^{4+\epsilon}$-unique shortest vector.

These exponents represent the tightness of the Ajtai connection, and are significant for any potential application to cryptography. The Ajtai connection factors given above are further improvements from the improvements presented in [8]. In the paper [1] a general polynomial factor n^c was shown for the problems of *(a), (b)* and *(c)* but no explicit values for the exponent c were given. Implicitly a factor less than n^{10}, n^{10} and n^{19} can be derived from the proofs of [1] for the problems of *(a), (b)* and *(c)* respectively.

The key step of the algorithm $\mathcal{B}$ is a probabilistic polynomial-time algorithm $\mathcal{B}'$, that uses algorithm $\mathcal{A}$ as a subroutine. Assume algorithm $\mathcal{A}$ exists. Then for any given integral lattice L of dimension n, $\mathcal{B}'$ will find a set of n linearly independent lattice vectors $v_1, v_2, \ldots, v_n$ with probability $1 - e^{-n}$, such that

$$\lambda_n(L) \leq \max_{i=1}^{n} ||v_i|| \leq n^f \lambda_n(L).$$

In [1] no explicit factor n^f was given, but a factor of n^8 can be derived from the proofs. This exponent f was improved by Cai and Nerurkar in [8] to $3 + \epsilon$, for an arbitrary small $\epsilon > 0$. This improvement was accomplished by a redesign of Ajtai's algorithm $\mathcal{B}'$ given $\mathcal{A}$. In terms of the items in Theorem 6.1 the improvement in [8] implies an Ajtai connection factor of $n^{5+\epsilon}$, $n^{5+\epsilon}$ and $n^{9+\epsilon}$ respectively.

Our current improvement in this paper is achieved by an improved analysis, rather than by any change in the algorithm design. We will start with the version of algorithm $\mathcal{B}'$ as given in [8], assuming the existence of $\mathcal{A}$. The following is an outline of the steps needed to compute the various items in Theorem 6.1. We emphasize that the only new ingredients are in the analysis, all algorithmic steps presented here other than $\mathcal{B}'$ of [8] are due to Ajtai [1].

For notational simplicity we will assume the lattice given is $L_0 = L^*$, where $L = L_0^*$, and we will compute the shortest vector problem for the lattice L^*. With $\mathcal{B}'$ applied to L, we can compute with high probability a set of n linearly independent lattice vectors $v_1, v_2, \ldots, v_n \in L$, such that $\lambda_n(L) \leq \tilde{\lambda}_n(L) \leq n^{3+\epsilon}\lambda_n(L)$, where $\tilde{\lambda}_n(L) = \max_{i=1}^n ||v_i||$. Let $\tilde{\lambda}_1^* = 1/\tilde{\lambda}_n(L)$. By Theorem 3.1, $1 \leq \lambda_n(L)\lambda_1(L^*) \leq g(L)\lambda_1(L^*) = O(n)$. It follows that

$$\lambda_1(L^*) \geq \frac{1}{\lambda_n(L)} \geq \frac{1}{\tilde{\lambda}_n(L)} = \tilde{\lambda}_1^* \geq \frac{1}{n^{3+\epsilon}\lambda_n(L)} \geq \frac{\lambda_1(L^*)}{n^{4+\epsilon'}},$$

where, say, $\epsilon' = 2\epsilon$, which can be made arbitrary small. This proves part *(a)*.

Next we assume that L^* has an n^c-unique shortest vector u. Then Theorem 5.2 gives the improved estimate in this case. This proves part *(b)*. Now we prove part *(c)* and assume $c > 4$.

Let S be the linear span of u and let π be the orthogonal projection to $S^\perp$. We noted that $\pi(L^*) = (L \cap S^\perp)^*$, and $\lambda_1((L \cap S^\perp)^*) \geq ||u||\sqrt{n^{2c} - 1/4}$ in the proof of Theorem 5.2. The following idea to compute the unique shortest vector u is due to Ajtai [1]. We do not change any algorithmic steps, but offer a better analysis using our transference theorems. For coherence of presentation, we will outline his steps along with the better analysis.

First compute with high probability a set of n linearly independent vectors $v_1, v_2, \ldots, v_n \in L$ using algorithm $\mathcal{B}'$. For any fixed constants $a > c$ and $b \geq a + 6$, we can randomly sample n^b lattice points of L of the form $\xi = \sum_{i=1}^n c_i v_i$, where $c_i \in \mathbf{Z}$ and $|c_i| \leq n^a$. Then $||\xi|| \leq$

$n^{a+1}\tilde{\lambda}_n(L) \leq n^{a+4+\epsilon}\lambda_n(L)$. This is at most $O(n^{a+5+\epsilon}/||u||)$ by Theorem 3.1 and $\lambda_1(L^*) = ||u||$. As the closest hyperplane parallel to $S^\perp$ intersecting L has orthogonal distance $1/||u||$ to $S^\perp$, these sample points are all from at most $O(n^{a+5+\epsilon})$ many parallel hyperplanes to $S^\perp$. Since $b \geq a+6$, it follows that some pair of samples are from the same parallel hyperplane to $S^\perp$. If x and y are a pair of such samples, then $x-y$ is a lattice vector in the hyperplane $S^\perp$. Furthermore, if one repeats this process it can be shown that with high probability one can get $n-1$ linearly independent lattice vectors all belong to $S^\perp$. Provided that one can distinguish those pairs of samples x and y such that $x - y \in S^\perp$, the orthogonal direction to $S^\perp$, namely that which is parallel to u, can be computed. This vector u' can be expressed as a non-zero rational linear combination of the basis vectors, and u' is perpendicular to $S^\perp$. Thus u' must be linearly dependent on u over $\mathbf{Q}$. Multiplying with the common denominator, we get an integral combination of the basis vectors, and thus an integral multiple of the primitive vector u. By taking out the greatest common divisor of the integral coefficients in the expression, we must get u or $-u$.

Thus the key is to distinguish those pairs x and y such that $v = x - y \in S^\perp$. Take a prime $t > n^b$ and consider $w = v/t$. Consider the $\mathbf{Z}$-module L' generated by L and w. It must be a lattice. There are two cases. If $v \in L \cap S^\perp$, then $w \in S^\perp$, and $\lambda_n(L')$ will be at least $1/||u||$. If however $v \notin L \cap S^\perp$, i.e., v belongs to one of the parallel planes of $S^\perp$ other than $S^\perp$, then L' is made up of parallel translations of $L \cap S^\perp$. Moreover, the orthogonal distance of the closest pair of linear spans of these parallel translations is $1/t||u||$. Thus in this case $\lambda_n(L')$ is much smaller than $1/||u||$.

More precisely, first suppose $v \in L \cap S^\perp$. Then L' is still covered by the same set of parallel translations of $S^\perp$. The orthogonal distance of the closest pair of linear spans of these parallel translations is $1/||u||$. Thus $\lambda_n(L') \geq 1/||u||$. In particular the computed estimate $\tilde{\lambda}_n(L')$ satisfies

$$\tilde{\lambda}_n(L') \geq \lambda_n(L') \geq \frac{1}{||u||}. \tag{19}$$

Now suppose $v \notin L \cap S^\perp$. Let v belong to the kth translation of $S^\perp$, where $k \neq 0$. There are vectors $z_1, z_2 \in L$, $v = z_1 + kz_2$, where $z_1 \in L \cap S^\perp$, and $\langle z_2, u\rangle = 1$. Then $w = v/t = z_1/t + kz_2/t$, and $\langle w, u\rangle = k/t$.

Clearly $|k| < n^{a+6}$ by the estimate on the norm of the samples, hence $(t, k) = 1$. Let $\alpha, \beta \in \mathbf{Z}$, such that $\alpha t + \beta k = 1$. Then $w' = \alpha z_2 + \beta w \in L'$, and

$$\langle w', u\rangle = \alpha + \beta k/t = 1/t.$$

Thus, the orthogonal distance of $w' \in L'$ to $S^\perp$ is $1/t||u||$.

For any $z \in L'$, it is clear that $\langle tz, u\rangle \in \mathbf{Z}$, thus every point in L' has distance to $S^\perp$ an integral multiple of $1/t||u||$. Thus L' is covered by the parallel translations of $S^\perp$ with distance $1/t||u||$, and the closest parallel translation intersecting L' has distance exactly $1/t||u||$.

We claim that the following equality is a consequence of t and k being relatively prime,

$$L' \cap S^\perp = L \cap S^\perp.$$

In fact, suppose $z \in L' \cap S^\perp$. There is a basis of L which consists of a basis of $L \cap S^\perp$ together with z_2. This is true because z_2 has the closest orthogonal distance to $S^\perp$ among $L \backslash S^\perp$, by the fact that $\langle z_2, u\rangle = 1$. By the definition of L', we can write z as an integral linear combination of these vectors and w,

$$z = iw + jz_2 + z',$$

where $i, j \in \mathbf{Z}$, and z' is some vector in $L \cap S^\perp$. Taking inner product with u, we get $ik/t + j = 0$, and thus $ik + jt = 0$. Now $(t, k) = 1$ implies that $t|i$ and $k|j$, and thus $iw \in L$. Since $z_2, z' \in L$ we conclude that $z \in L$ as well. Hence $z \in L \cap S^\perp$. The claim is proved.

It follows that

$$L' = (L \cap S^\perp) \oplus \langle w'\rangle,$$

namely the set of all parallel translations of $L \cap S^\perp$ by w' with orthogonal distance $1/t||u||$.

Thus $tu \in L'^*$ and is primitive in L'^*. By Lemma 4.1, it follows that

$$\pi(L'^*) = (L' \cap S^\perp)^* = (L \cap S^\perp)^* = \pi(L^*).$$

Any vector $\tilde{u}$ of L'^* not parallel to tu must project to a non-zero vector in $\pi(L'^*) = \pi(L^*)$. However we have the estimate

$$\lambda_1(\pi(L^*)) = \lambda_1((L \cap S^\perp)^*) \geq ||u||\sqrt{n^{2c} - 1/4},$$

by the fact that L^* has an n^c-unique shortest vector. (See the proof of Theorem 5.2.) Thus $||\tilde{u}|| \geq ||u||\sqrt{n^{2c} - 1/4}$ as well. Since $a > c$, $t > n^b > n^c$, it follows that $\lambda_1(L'^*) \geq \min\{||tu||, ||u||\sqrt{n^{2c} - 1/4}\} \geq ||u||\sqrt{n^{2c} - 1/4}$.

By Theorem 3.1 $\lambda_n(L') = O(n^{1-c}/||u||)$, and we can compute an estimate

$$\tilde{\lambda}_n(L') = O(n^{4+\epsilon-c}/||u||) < 1/||u||, \tag{20}$$

for $c > 4$ and sufficiently small ϵ. Comparing (19) and (20) we note that in this case $\tilde{\lambda}_n(L')$ is smaller than the lower bound obtained for $\tilde{\lambda}_n(L')$ in the case when the vector v belonged to the hyperplane $S^\perp$.

Hence we could distinguish the two cases with high probability and thus ultimately compute u in probabilistic polynomial time. The proof of Theorem 6.1 is complete.

Acknowledgements

I thank Ajay Nerurkar for valuable discussions and comments.

References

[1] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th Annual ACM Symposium on the Theory of Computing*, 1996. Full version available from ECCC, *Electronic Colloquium on Computational Complexity* TR96-007, at `http://www.eccc.uni-trier.de/eccc/`.

[2] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. *Electronic Colloquium on Computational Complexity*, TR97-047 at `http://www.eccc.uni-trier.de/eccc/`.

[3] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. 1996. Available from ECCC, *Electronic Colloquium on Computational Complexity* TR96-065, at `http://www.eccc.uni-trier.de/eccc/`.

[4] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. In *Proc. 34th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1993, 724-733.

[5] L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[6] W. Banaszczyk. New Bounds in Some Transference Theorems in the Geometry of Numbers. *Mathematische Annalen*, 296, pages 625–635, 1993.

[7] J-Y. Cai. A Primal-Dual Relation for Lattices and the Complexity of Shortest Lattice Vector Problem. To appear in *Theoretical Computer Science.*

[8] J-Y. Cai and A. Nerurkar. An Improved Worst-Case to Average-Case Connection for Lattice Problems. In *Proc. 38th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1997, 468–477.

[9] J-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor $\left(1+\frac{1}{\dim^{\epsilon}}\right)$ is NP-hard under randomized reductions. To appear.

[10] J. W. S. Cassels. *An Introduction to the Geometry of Numbers.* Berlin Göttingen Heidelberg: Springer 1959.

[11] O. Goldreich and S. Goldwasser. On the Limits of Non-Approximability of Lattice Problems. *Electronic Colloquium on Computational Complexity* TR97-031, at `http://www.eccc.uni-trier.de/eccc/`.

[12] O. Goldreich, S. Goldwasser, and S. Halevi. Collision-free hashing from lattice problems. 1996. Available from ECCC, *Electronic Colloquium on Computational Complexity* TR96-042, at `http://www.eccc.uni-trier.de/eccc/`.

[13] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. 1996. Available from ECCC, *Electronic Colloquium on Computational Complexity* TR96-056, at `http://www.eccc.uni-trier.de/eccc/`.

[14] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization.* Springer Verlag, 1988.

[15] P. M. Gruber. *Handbook of Convex Geometry.* Elsevier Science Publishers B.V., 1993.

[16] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers.* North-Holland, 1987.

[17] J. Håstad. Dual Vectors and Lower Bounds for the Nearest Lattice Point Problem. *Combinatorica*, Vol. 8, 1988, pages 75–81.

[18] E. Hewitt and K. A. Ross. *Abstract Harmonic Analysis*, Vol II. Berlin Göttingen Heidelberg: Springer 1970.

[19] A. Korkin and G. Zolotarev. Sur les formes quadratiques positives quaternaires. *Mathematische Annalen*, **5**, 581–583, 1872.

[20] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM Journal of Computing*, Volume 14, page 196–209, 1985.

[21] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr. Korkin-Zolotarev Bases and Successive Minima of a Lattice and its Reciprocal Lattice. *Combinatorica*, 10:(4), 1990, 333-348.

[22] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[23] H. W. Lenstra, Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8:538–548, 1983.

[24] L. Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity.* SIAM, Philadelphia, 1986.

[25] K. Mahler. Ein Übertragungsprinzip für konvexe Körper. *Čas. Pěstování Mat. Fys.* **68**, pages 93–102, 1939.

[26] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms.* Berlin Heidelberg New York: Springer 1973.

[27] C. P. Schnorr. A hierarchy of polynomial time basis reduction algorithms. *Theory of Algorithms*, pages 375–386, 1985.

[28] S. Even, A. L. Selman and Y. Yacobi. The Complexity of Promise Problems with Applications to Public-key Cryptography. *Information and Control* **61**, 159–173, 1984.

[29] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in lattices. Technical Report 81-04, Mathematics Department, University of Amsterdam, 1981.

Appendix

In this appendix we give the details for the case $\epsilon = 1/2$ in Theorem 5.1. Denote $\lambda = ||v_1|| = \lambda_1(L^*)$. Then $\lambda > c_2 > 3/\sqrt{2\pi}$. Take the orthogonal projection of the vector x_0 to the affine line, i.e., let $x_0 = y_0 + z_0$, where y_0 is perpendicular to the affine line $\mathbf{R}v_1 + x_0$, and z_0 is parallel to v_1. We may assume $\langle z_0, v_1 \rangle \geq 0$, otherwise we can replace v_1 by $-v_1$. Then $||x_0||^2 = ||y_0||^2 + ||z_0||^2$. It follows that $||y_0||, ||z_0|| \leq ||x_0||$, and since x_0 is the point of $L^* + u$ of minimum norm on the affine line, $||z_0|| \leq \lambda_1(L^*)/2$. Also $||x_0|| \geq \lambda/3$ by the choice of u in Lemma 3.1.

We split the sum

$$\sum_{k=-\infty}^{+\infty} e^{-\pi||x_0+kv_1||^2},$$

into two parts according to $k \geq 0$ and $k < 0$. For $k \geq 0$, the kth term has

$$\begin{aligned} ||x_0 + kv_1||^2 &= ||y_0||^2 + (||z_0|| + k||v_1||)^2 \\ &= ||x_0||^2 + k^2\lambda^2 + 2k||z_0||\lambda \\ &\geq \lambda^2/9 + k^2\lambda^2. \end{aligned}$$

Thus the first sum is bounded above by

$$\sum_{k=0}^{+\infty} e^{-\pi[\lambda^2/9 + k^2\lambda^2]}.$$

The leading term is $e^{-\pi\lambda^2/9} < 1/\sqrt{e}$. The successive ratio of the $(k+1)$st term over the kth term, for $k \geq 0$ is

$$e^{-\pi(2k+1)\lambda^2} \leq e^{-\pi\lambda^2} < e^{-9/2}.$$

Hence

$$\sum_{k=0}^{+\infty} e^{-\pi[\lambda^2/9 + k^2\lambda^2]} < \frac{1}{\sqrt{e}(1 - 1/e^{9/2})} \approx 0.6133443.$$

For the second part of the sum, we have

$$\begin{aligned} ||x_0 - kv_1||^2 &= ||y_0||^2 + (k||v_1|| - ||z_0||)^2 \\ &\geq (k\lambda - \lambda/2)^2 \\ &\geq \lambda^2/4 \end{aligned}$$

for $k \geq 1$. Therefore the second sum is bounded by

$$\sum_{k=1}^{+\infty} e^{-\pi[(k-1/2)\lambda]^2}.$$

The leading term is $e^{-\pi\lambda^2/4} < 1/e^{9/8}$. The successive ratio of the $(k+1)$st term over the kth term, for $k \geq 1$, is

$$e^{-\pi 2k\lambda^2} \leq e^{-2\pi\lambda^2} < e^{-9}.$$

Hence the second part of the sum is bounded by

$$\sum_{k=1}^{+\infty} e^{-\pi(k\lambda - \lambda/2)^2} < \frac{1}{e^{9/8}(1 - 1/e^9)} \approx 0.3246925.$$

It follows that

$$\sum_{k=-\infty}^{+\infty} e^{-\pi||x_0 + kv_1||^2} < 0.94.$$

We conclude that for any $c_1 > 1/\sqrt{2\pi}$ and $c_2 > 3/\sqrt{2\pi}$, there are constants $\epsilon_1 < 1$ and $\epsilon_2 < 1$, such that

$$1 - 2\epsilon_1^n = \widehat{\sigma_{L'}}(u) - 2\epsilon_1^n \leq \widehat{\sigma_L}(u) < 0.94 + 2\epsilon_2^n.$$

This is a contradiction for large n.