A relation of primal-dual lattices and the complexity of shortest lattice vector problem

Jin-Yi Cai*

Abstract

We give a simplified proof of a theorem of Lagarias, Lenstra and Schnorr [17] that the problem of approximating the length of the shortest lattice vector within a factor of Cn, for an appropriate constant C, cannot be NP-hard, unless NP = coNP. We also prove that the problem of findng a $n^{1/4}$-unique shortest lattice vector is not NP-hard under polynomial time many-one reductions, unless the polynomial time hierarchy collapses.

1 Introduction

A discrete additive subgroup of $\mathbf{R}^n$ is called a lattice. Recently in a beautiful paper Ajtai [1] established the first explicit connection between, in a certain technical sense, the worst-case and the average-case complexity of the shortest lattice vector problem. This is the problem of finding or approximating the shortest lattice vector or its length. In a tour de force, Ajtai [2] further established the NP-hardness of the problem of finding the shortest lattice vector (in Euclidean norm, or l_2-norm), as well as the problem of approximating the shortest vector length up to a factor of $1 + \frac{1}{2^{n^k}}$. Here k is a sufficiently large but fixed constant, and n is the dimension of the lattice or the size of the problem. The Ajtai connection [1] of worst-case to average-case complexity for lattice problems has been improved by Cai and Nerurkar [7]. In a forthcoming paper [8], 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, $p \geq 1$ [16, 24]. Even finding an approximate solution to within any constant factor for the nearest vector problem for any l_p-norm is NP-hard [4]. In the other direction, Lagarias, Lenstra and Schnorr [17] showed that the approximation problem (in l_2-norm) within a factor of $O(n)$ *cannot* be NP-hard, unless NP = coNP. Our first result is to present a simplified proof of this theorem using a generalization of an idea of Ajtai [1].

The recent breakthrough by Ajtai [1, 2] has its motivations from cryptography, and the connection between average-case and worst-case complexity in general. It has been realized for some time that the security of a cryptographic protocol depends on the intractability of certain computational problem *on the average*. Unfortunately as yet we have no such proofs

*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 grants CCR-9634665, and by an Alfred P. Sloan Fellowship.

for any problem in NP. The next best thing to an absolute lower bound would be a proof of NP-hardness for breaking the protocol. To this end, 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 a n^c-unique shortest lattice vector, and showed that for a certain c, if finding the shortest lattice vector in a lattice with a 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. Hence there is considerable interest recently in the determination of the exact complexity for a variety of problems related to the shortest vector problem. In particular one would like to narrow the gap between those cases where NP-hardness can be proved and those where it is probably not NP-hard. Goldreich and Goldwasser have obtained the following result: Approximating the shortest lattice vector within a factor of $O(\sqrt{n/\log n})$ is not NP-hard under polynomial time many-one reductions, assuming the polynomial time hierarchy does not collapse [9]. We adapt their proof to show that the problem of finding a $n^{1/4}$-unique shortest lattice vector is not NP-hard under polynomial time many-one reductions, unless the polynomial time hierarchy collapses.

2 Preliminaries

A lattice L (of full rank) in $\mathbf{R}^n$ is the set of all integral linear combinations of a set of n linearly independent vectors in $\mathbf{R}^n$. Such a linearly independent set of generating vectors is called a basis for L. Basis vectors for a lattice are not unique, but related by unimodular transformations.

The dimension of a lattice L, denoted $\dim L$, is the number of vectors in a basis. We denote the length (Euclidean norm) of a vector v by $||v||$. The inner product is denoted by $\langle u, v\rangle$, and $||v||^2 = \langle v, v\rangle$.

A fundamental theorem of Minkowski is the following:

Theorem 2.1 (Minkowski) *There is a universal constant γ, such that for any lattice L of dimension n, $\exists v \in L$, $v \neq 0$, such that*

$$||v|| \leq \gamma\sqrt{n}\det(L)^{1/n}.$$

The determinant $\det(L)$ of a lattice is the volume of the n-dimensional fundamental parallelepiped, and the absolute constant γ is known as Hermite's constant. (Some authors define the least upper bound for $||v||/\det(L)^{1/n}$ or its square $||v||^2/\det(L)^{2/n}$ as Hermite's constant γ_n, then γ_n is bounded above by $\gamma\sqrt{n}$ or $\gamma^2 n$, respectively, for all lattices of dimension n, where γ is some universal constant.) We denote $\mathrm{unit}(L) = \det(L)^{1/\dim(L)}$. We denote by $\lambda_1(L)$ the length of the shortest non-zero lattice vector of L. Then Minkowski's Theorem can also be stated as $\lambda_1(L) \leq \gamma\sqrt{n} \cdot \mathrm{unit}(L)$.

There is a second Minkowski theorem dealing with the geometric mean of the so-called *successive minima* $\sqrt[n]{\prod_{i=1}^{n} \lambda_i}$ in place of λ_1. Here $\lambda_i(L)$ is defined as $\lambda_i(L) = \min_{v_1,\ldots,v_i \in L} \max_{1\leq j\leq i} ||v_j||$, where the sequence of vectors $v_1, \ldots, v_i \in L$ ranges over all i linearly independent lattice vectors.

Theorem 2.2 (Minkowski) *For any lattice L of dimension n,*

$$\left(\prod_{i=1}^{n} \lambda_i(L)\right)^{1/n} \leq \gamma\sqrt{n}\det(L)^{1/n}.$$

If $v_1, \ldots, v_k$ are vectors in $\mathbf{R}^n$, such that the linear span of $\{v_1, \ldots, v_k\}$ intersects L in a sublattice of dimension k, then we can obtain a *quotient* lattice, denoted by $L/L(v_1, \ldots, v_k)$, by orthogonally projecting L to the orthogonal complement of the span of $\{v_1, \ldots, v_k\}$. Note that $v_1, \ldots, v_k$ need not be lattice vectors.

Given a lattice L, the basis length $\mathrm{bl}(L)$ is the minimum over all basis vectors $\{b_1, b_2, \ldots, b_n\}$ of the maximum length $||b_i||$. Call a sequence of n *non-zero* vectors $\langle b_1, b_2, \ldots, b_n\rangle$ an admissible sequence for L, if $b_1 \in L$, $b_2 \in L_1 = L/L(b_1)$, etc. In general $L_0 = L$, $b_1 \in L_0$, and $L_k = L_{k-1}/L_{k-1}(b_k)$, $b_{k+1} \in L_k$, for $1 \leq k \leq n-1$. It is easy to see that $L_k = L/L(b_1, \ldots, b_k)$. We define $\widetilde{bl}(L)$ to be the minimum over all admissible sequences $\langle b_1, b_2, \ldots, b_n\rangle$ for L of the maximum length $||b_i||$.

The dual lattice L^* of a lattice 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 $\mathrm{unit}(L^*) \cdot \mathrm{unit}(L) = 1$, and $L^{**} = L$.

A lattice L is said to have a n^c-unique shortest lattice vector, if there is a non-zero vector $v \in L$, such that, if $||u|| \leq n^c||v||$ for any lattice vector $u \in L$, then there is an integer k such that $u = kv$. Clearly such a vector v is unique up to sign $\pm v$.

Lagarias, Lenstra and Schnorr [17] proved the following theorem:

Theorem 2.3 (Lagarias, Lenstra and Schnorr) *The problem of approximating the length of the shortest lattice vector within a factor of Cn, for an appropriate constant C, cannot be NP-hard, unless NP = coNP.*

Their result is based on the following type of inequalities called transference theorems:

Theorem 2.4 (Lagarias, Lenstra and Schnorr) *For any lattice L of dimension n,*

$$1 \leq \lambda_i(L)\lambda_{n-i+1}(L^*) \leq \frac{1}{6}n^2,$$

for all $1 \leq i \leq n$ and all $n \geq 7$.

For related results see [5, 15]. The proof in [17] uses Korkin-Zolotarev basis of a lattice. Their transference theorem has been improved by Banaszczyk [6], where the factor n^2 has been replaced by n.

Theorem 2.5 (Banaszczyk) *For any lattice L of dimension n,*

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

for some universal constant C, and for all $1 \leq i \leq n$ and all n.

Banaszczyk's proof is non-elementary, based on harmonic analysis. This bound of Cn is essentially optimal up to the constant C, since a construction by Conway and Thompson (see [21]) shows that there exists a self-dual lattice family $\{L_n\}$ with $\lambda_1(L_n) = \Omega(\sqrt{n})$.

3 A product relation

Theorem 2.3 follows easily from Banaszczyk's inequality (Theorem 2.5). Even though Banaszczyk's inequality is stronger than that of Theorem 2.4, the bound to non-NP-hardness for approximability of shortest lattice problem remains $O(n)$.

We will give a self-contained elementary proof of Theorem 2.3. The inequalities we prove are not as strong as Banaszczyk's inequality, but the proofs are much simpler, and yields the same bound $O(n)$ for non-NP-hardness. We first prove a lemma, which is modeled after a lemma of Ajtai [1]. The lemma is proved using Minkowski's First Theorem on shortest lattice vectors.

Lemma 3.1 *For any lattice L of dimension n, and for any threshold $t > 0$, there exist an admissible sequence of vectors for L, $\langle b_1, b_2, \ldots, b_n \rangle$, and an integer k, $0 \leq k \leq n$, such that,*

- *If $k > 0$, then $||b_1||, \ldots, ||b_k|| \leq \gamma\sqrt{n}t$.*
- *If $k < n$, then $\mathrm{unit}(L/L(b_1, \ldots, b_k)) > t$.*

Remark: The conditions $k > 0$ and $k < n$ can be omitted in the statements if we understand that the statements are vacuously true for the cases where $k = 0$ or $k = n$ respectively.

Proof: The lemma is trivially true for $n = 1$. We suppose $n > 1$, and prove by induction.

If $\mathrm{unit}(L) > t$, then the lemma is trivially true by taking $k = 0$, and any admissible sequence $\langle b_1, b_2, \ldots, b_n \rangle$.

Now suppose $\mathrm{unit}(L) \leq t$. Then by Minkowski's Theorem, there exists a non-zero vector $b_1 \in L$, such that $||b_1|| \leq \gamma\sqrt{n}t$. Consider $L_1 = L/L(b_1)$. By induction, for L_1 of dimension $n-1$, there exist an admissible sequence $\langle b_2, \ldots, b_n \rangle$ for L_1 and an integer k, $1 \leq k \leq n$, such that

- If $k > 1$, then $||b_2||, \ldots, ||b_k|| \leq \gamma\sqrt{n-1}t$.
- If $k < n$, then $\mathrm{unit}(L_1/L(b_2, \ldots, b_k)) > t$.

However, note that, $\langle b_1, b_2, \ldots, b_n \rangle$ is an admissible sequence for L, and $L_1/L(b_2, \ldots, b_k) = L/L(b_1, b_2, \ldots, b_k)$, the lemma follows. □

Theorem 3.1

$$1 \leq \lambda_1(L^*) \cdot \widetilde{bl}(L) \leq \gamma^2 n.$$

Proof: We first show that the product is at least 1.

Let $v \in L^*$ be an arbitrary non-zero vector in the dual lattice. Let $\langle b_1, b_2, \ldots, b_n \rangle$ be an admissible sequence of vectors of L, with $\max_{1 \leq i \leq n} ||b_i|| = \widetilde{bl}(L)$. Since $b_1, b_2, \ldots, b_n$ are n linearly independent vectors, there exists some i, such that $\langle v, b_i \rangle \neq 0$. Let $i \geq 1$ be the least such index. Hence, for all j, $1 \leq j < i$, $\langle v, b_j \rangle = 0$, and $\langle v, b_i \rangle \neq 0$. (If $i = 1$ then the first statement is vacuous.) We want to show that

$$||v|| \cdot \max_{1 \leq i \leq n} ||b_i|| = ||v|| \cdot \widetilde{bl}(L) \geq 1.$$

Suppose $i = 1$. Then since $b_1 \in L$, $\langle v, b_1 \rangle$ is a non-zero integer, $|\langle v, b_1 \rangle| \geq 1$. Hence $1 \leq ||v|| \cdot ||b_1|| \leq ||v|| \cdot \max_{1 \leq i \leq n} ||b_i||$, by Cauchy-Schwarz.

Now suppose $i > 1$. By the definition of admissible sequence, there exist real numbers $\alpha_1, \ldots, \alpha_{i-1}$, such that $b_i + \sum_{j=1}^{i-1} \alpha_j b_j \in L$. Recall that $\langle v, b_j \rangle = 0$, for all $1 \leq j < i$, and $\langle v, b_i + \sum_{j=1}^{i-1} \alpha_j b_j \rangle$ is an integer, and $\langle v, b_i \rangle \neq 0$, we obtain $\langle v, b_i \rangle = \langle v, b_i + \sum_{j=1}^{i-1} \alpha_j b_j \rangle$ is a non-zero integer, and thus is of absolute value at least 1. Therefore, $1 \leq |\langle v, b_i \rangle| \leq ||v|| \cdot ||b_i|| \leq ||v|| \cdot \max_{1 \leq i \leq n} ||b_i||$, again by Cauchy-Schwarz.

We show next that

$$\lambda_1(L^*) \cdot \widetilde{bl}(L) \leq \gamma^2 n,$$

where γ is Hermite's constant.

Take t to be an arbitrary real number less than $\frac{1}{\gamma\sqrt{n}} \widetilde{bl}(L)$. Then the integer k from Lemma 3.1 must be less than n, lest there be an admissible sequence for L with $\max_{1 \leq i \leq n} ||b_i|| < \widetilde{bl}(L)$. Hence, the second clause in the lemma holds with some $k < n$, so that the quotient lattice $L/L(b_1, \ldots, b_k)$ is of dimension at least 1. Note that the dual lattice $(L/L(b_1, \ldots, b_k))^*$ within the $(n-k)$-dimensional linear span of $L/L(b_1, \ldots, b_k)$ is a sublattice of L^*. By the lemma, $\mathrm{unit}(L/L(b_1, \ldots, b_k)) > t$, thus $\mathrm{unit}\left((L/L(b_1, \ldots, b_k))^*\right) < 1/t$. By Minkowski's Theorem again, there exists a non-zero vector of $(L/L(b_1, \ldots, b_k))^*$, hence of L^*, whose length is less than $\gamma\sqrt{n-k} \cdot 1/t \leq \gamma\sqrt{n}/t$. Since $t < \frac{1}{\gamma\sqrt{n}} \widetilde{bl}(L)$ is arbitrary, the shortest non-zero lattice vector of L^* must have length at most $\gamma^2 n / \widetilde{bl}(L)$, i.e.,

$$\lambda_1(L^*) \cdot \widetilde{bl}(L) \leq \gamma^2 n. \qquad \square$$

Note that $L^{**} = L$, we can apply this theorem to the dual lattice L^*, and obtain

Corollary 3.1

$$1 \leq \lambda_1(L) \cdot \widetilde{bl}(L^*) \leq \gamma^2 n.$$

The same idea can give a similar bound relating the shortest vector length $\lambda_1(L)$ with the basis length $\mathrm{bl}(L^*)$ of the dual. Stronger bounds are found in [6].

Theorem 3.2

$$1 \leq \lambda_1(L^*) \cdot \mathrm{bl}(L) \leq C n^{1.5},$$

where C is an absolute constant.

The lower bound $1 \leq \lambda_1(L^*) \cdot \mathrm{bl}(L)$ is known (see e.g. [1]) and is relatively easy; we repeat it here: Let $v \in L^*$, $v \neq 0$, and $||v|| = \lambda_1(L^*)$. Then for any basis $b_1, \ldots, b_n$ of L, there must be some i, such that $\langle v, b_i \rangle \neq 0$. Being integral, $|\langle v, b_i \rangle| \geq 1$. The lower bound then follows from the Cauchy-Schwarz inequality.

For the upper bound, we need a similar lemma.

Lemma 3.2 *For any lattice L of dimension n, and for any threshold $t > 0$, there exist a basis of L, $\{b_1, b_2, \ldots, b_n\}$, and an integer k, $0 \leq k \leq n$, such that,*

- *If $k > 0$, then $||b_1||, \ldots, ||b_k|| \leq cnt$, for some absolute constant c.*
- *If $k < n$, then $\mathrm{unit}(L/L(b_1, \ldots, b_k)) > t$.*

Proof: (of Lemma 3.2) By induction. $n = 1$ is a direct consequence of Minkowski's Theorem.

Suppose $n > 1$. If $\text{unit}(L) > t$, then the lemma is trivially true by taking $k = 0$, and any basis of L.

Next we assume $\text{unit}(L) \le t$. Then by Minkowski's Theorem, there exists a non-zero vector $b_1 \in L$, such that $||b_1|| \le \gamma\sqrt{n}t$. We may assume that b_1 is a primitive vector, i.e., it is not an integral multiple of other lattice vectors (other than $\pm b_1$). Let $L' = L/L(b_1)$. By induction, for L' of dimension $n-1$, there exist a basis $\{b'_2, \ldots, b'_n\}$ for L' and an integer k, $1 \le k \le n$, such that

- If $k > 1$, then $||b'_2||, \ldots, ||b'_k|| \le c(n-1)t$.
- If $k < n$, then $\text{unit}(L'/L(b'_2, \ldots, b'_k)) > t$.

Now $\{b'_2, \ldots, b'_n\}$ can be lifted to a set of lattice vectors $\{b_2, \ldots, b_n\}$ of L, together with b_1, forms a basis of L. In fact, each $b_i = b'_i + \alpha_i b_1$, for some $|\alpha_i| \le 1/2$, and by being orthogonal,

$$||b_i||^2 \le ||b'_i||^2 + ||b_1||^2/4 \le c^2(n-1)^2t^2 + \gamma^2 nt^2/4.$$

It follows that $||b_i|| \le cnt$, for $i \le k$, if we take $c = \gamma$, say. (c can be taken to be any constant slightly bigger than $\gamma/(2\sqrt{2})$.) Finally we note that

$$L'/L(b'_2, \ldots, b'_k) = L/L(b_1, b_2, \ldots, b_k).$$

The lemma is proved. $\square$

Returning to the proof of Theorem 3.2, we take the threshold t to be slightly less than $\text{bl}(L)/cn$. Then the integer k from Lemma 3.2 must be less than n, lest there be a basis of L with $\max_{1 \le i \le n} ||b_i|| < \text{bl}(L)$. Thus we have a quotient lattice $L/L(b_1, \ldots, b_k)$ of dimension at least 1, with $\text{unit}(L/L(b_1, \ldots, b_k)) > t$. Again the dual lattice $(L/L(b_1, \ldots, b_k))^*$ within the $(n-k)$-dimensional linear span of $L/L(b_1, \ldots, b_k)$ is a sublattice of L^*. Thus $\text{unit}\left((L/L(b_1, \ldots, b_k))^*\right) < 1/t$. By Minkowski's Theorem again, there exists a non-zero vector of $(L/L(b_1, \ldots, b_k))^*$, hence of L^*, whose length is less than $\gamma\sqrt{n-k} \cdot 1/t \le \gamma\sqrt{n}/t$.

Since t can be chosen arbitrarily close to $\text{bl}(L)/cn$, the shortest non-zero lattice vector of L^* must have length at most $c\gamma n^{1.5}/\text{bl}(L)$, i.e.,

$$\lambda_1(L^*) \cdot \text{bl}(L) \le Cn^{1.5},$$

for some absolute constant C. $\square$

4 The complexity of approximate shortest lattice vector

We show next that Theorem 2.3 follows immediately from Theorem 3.1.

Theorem 4.1 *If the problem of finding the length of the shortest lattice vector for a lattice of dimension n, within a factor of $\gamma^2 n$, is NP-hard under polynomial-time Turing reductions, then NP = coNP.*

Proof: Suppose there is a polynomial-time Turing machine M reducing SAT to the problem of finding the length of the shortest lattice vector for a lattice of dimension n, within a factor of $\gamma^2 n$. The precise meaning of this reduction is in terms of the notion of a promise problem [23], where every oracle query by M consists of a lattice L and a threshold t, with the property that either the shortest lattice vector of L has length $\leq t$ (in which case the oracle answer is "yes"), or the length is $> (\gamma^2 \dim L)t$ (in which case the oracle answer is "no"). The lattice L is presented to the oracle in terms of a basis. The dimension as well as the bit-length of the basis vectors of L are bounded by a fixed polynomial of the input length to M, and each oracle query counts as one step by M.

We now describe an NP∩coNP algorithm to solve SAT. Thus NP⊆ NP∩coNP, and so NP = coNP. Upon any input boolean formula to M, we simulate M, where we handle each query as follows. Suppose L and a threshold t are presented. First let's suppose $\lambda_1(L) \leq t$, then we can guess a short non-zero vector of L, and verify that its length is at most t. It is not difficult to see that the bit-length of such a shortest vector in terms of the given basis vectors is polynomially bounded.

Now suppose $\lambda_1(L) > t$, then by hypothesis $\lambda_1(L) > (\gamma^2 \dim L)t$. Apply Corollary 3.1 to the lattice L^*, we have $1 \leq \lambda_1(L) \cdot \widetilde{bl}(L^*) \leq \gamma^2 \dim L$. It follows that $\widetilde{bl}(L^*) < 1/t$. Moreover, $\widetilde{bl}(L^*) < 1/t$ implies that $\lambda_1(L) \geq \frac{1}{\widetilde{bl}(L^*)} > t$. Thus, we simply guess an admissible sequence $\langle \delta_1, \ldots, \delta_{\dim L^*} \rangle$ of vectors for the dual lattice L^*, and verify that $\max_i ||\delta_i|| < 1/t$. Again it is not difficult to see that one can first compute a dual basis from the basis given for L, and verify all the necessary requirements in polynomial time. In particular, the bit-length of such a guess is polynomially bounded. □

As mentioned earlier, much of the recent interest in the complexity of problems related to shortest lattice vectors stems from the great advances made by Ajtai [1], and Ajtai and Dwork [3]. In particular, the Ajtai-Dwork public-key cryptosystem is provably secure assuming only the worst case intractability of the following problem: Given a n-dimensional lattice L with a n^c-unique shortest vector, for some large constant c, find its shortest vector.

Ajtai [2] has shown more recently that the shortest lattice vector problem is NP-hard under randomized polynomial time reductions. In view of applications to cryptographic security, hardness for approximate versions of the shortest lattice vector problem are also important. To this end, Ajtai [2] showed that for a sufficiently large but fixed k, to approximate the length of the shortest lattice vector within a factor of $1 + \frac{1}{2^{n^k}}$ remains NP-hard under randomized polynomial time reductions. More precisely, this means that there is a probabilistic polynomial time reduction σ with the following property: Given an arbitrary boolean formula Φ, $\sigma(\Phi)$ is a lattice L with a threshold t, such that, if Φ is satisfiable $\Phi \in$ SAT, then with high probability $\lambda_1(L) \leq t$, and if Φ is not satisfiable $\Phi \notin$ SAT, then $\lambda_1(L) > \left(1 + \frac{1}{2^{n^k}}\right) t$. Furthermore, given any approximate short vector $v \in L$, with $0 < ||v|| \leq \left(1 + \frac{1}{2^{n^k}}\right) t$, a satisfying assignment to Φ can be easily constructed from v. This approximation factor has been improved by Cai and Nerurkar [8] to $1 + \frac{1}{n^\varepsilon}$, for any $\varepsilon > 0$.

The results discussed in this paper belong to the other direction, namely certain approximate shortest lattice vector problems are not NP-hard under some standard complexity assumptions. Going beyond the factor n, Goldreich and Goldwasser [9] have shown that approximating the shortest lattice vector within a factor of $O(\sqrt{n/\log n})$ is not NP-hard under polynomial time many-one reductions, assuming the polynomial time hierarchy does not collapse. This is a stronger result of non-NP-hardness, assuming a stronger complexity assumption. More precisely they showed that there is a (bounded round) interactive proof system (AM) for the assertion that $\lambda_1(L) > t \cdot \sqrt{n/\log n}$, *assuming* that the lattice L satisfies the promise that either $\lambda_1(L) \le t$ or $\lambda_1(L) > t \cdot \sqrt{n/\log n}$. The main consequence of the interactive proof is that unless the polynomial time hierarchy collapses, the following reduction $\sigma(\Phi) = (L, t)$ does not exist in polynomial time: Given an instance Φ for SAT, if $\Phi \in$ SAT, then $\lambda_1(L) \le t$, and if $\Phi \notin$ SAT, then $\lambda_1(L) > t \cdot \sqrt{n/\log n}$.

The basic idea of the IP protocol of [9] is rather simple and beautiful that we describe it informally: Suppose L satisfies the promise of either $\lambda_1(L) \le t$ or $\lambda_1(L) > t \cdot \sqrt{n/\log n}$, and the prover claims that $\lambda_1(L) > t \cdot \sqrt{n/\log n}$. Imagine we surround each lattice point $p \in L$ a ball $B_p(r)$ centered at p with radius $r = t \cdot \sqrt{n/\log n}/2$. If the prover P is honest, then all such balls are disjoint. Now the verifier randomly picks a lattice point p in secret, and randomly picks a point z in $B_p(r)$. The verifier presents z to the prover, who should respond with p, the center of the ball from which z was chosen. It is clear that for an honest prover P with unlimited computing power, since all the balls $B_p(r)$ are disjoint, he has no difficulty meeting his obligation. However, suppose the prover P' is dishonest, so that in fact $\lambda_1(L) \le t$. Then for any lattice point p picked by the verifier, there is at least one nearby lattice point p' with $||p - p'|| \le t$. Then $B_p(r)$ and $B_{p'}(r)$ would have a large intersection. This follows from the fact that the radius is almost $n^{1/2}$ times the distance of their respective centers. It follows that there is a significant probability that a dishonest prover will be caught, since in case a point $z \in B_p(r) \cap B_{p'}(r)$ is chosen, the verifier could equally have chosen p or p'.

The exponent $1/2$ in this interactive proof protocol comes from the well known fact that in n-dimensional space, two unit balls with center distance d have a significant intersection if $d < 1/\sqrt{n}$, and a negligible intersection if $d > 1/n^{1/2-\epsilon}$, for any $\epsilon > 0$.

In view of the particular version of the shortest vector problem upon which the Ajtai-Dwork system is based, it is interesting to consider to which extent a non-NP-hardness result can be shown for it. Define the following promise problem:

The n^c-unique shortest lattice vector problem:
Given a lattice with a n^c-unique shortest vector v, find the shortest vector $\pm v$.

Theorem 4.2 *The n^c-unique shortest lattice vector problem for $c \le 1/4$ is not NP-hard unless the polynomial time hierarchy collapses.*

Proof: Let L be a lattice with a $n^{1/4}$-unique shortest vector. We present a bounded round interactive proof system (AM) for proving that $\lambda_1(L) > t$.

Let the input size be bounded by $n^{O(1)}$. Without loss of generality let the lattice be given by its basis $L = L(b_1, b_2, \ldots, b_n)$. Let $T = \min_{1 \le k \le n} ||b_i||$, which is bounded by $2^{n^{O(1)}}$.

The interactive proof protocol is as follows:

V: For $i = 0, 1, \ldots, \lfloor \log_2 T - \log_2 t \rfloor$, and $j = 1, 2, \ldots, m = n^{O(1)}$, independently uniformly picks a lattice point p_{ij} in L (say uniformly within a large exponential sized parallelepiped), and then pick a uniformly chosen point $z_{ij} \in B_{p_{ij}}(r_i)$, where $r_i = 2^{i-1} t \sqrt{\sqrt{n} - \frac{1}{4}}$. Sends all z_{ij} to V.

P: Returns to V vectors v and $p'_1, \ldots, p'_m$.

V: Accepts if and only if $v \in L$, $||v|| > t$, v is a primitive vector in L (v is a primitive vectors iff it is not an integral multiple of another lattice vector except $\pm v$), and for the unique i such that $2^i t < ||v|| \le 2^{i+1} t$, each $z_{ij} \in B_{p'_j}(r_i)$, and finally $p'_j \equiv p_{ij} \bmod v$ for all j.

The intuitive idea is the following: The prover is supposed to return the shortest lattice vector v. Consider the orthogonal projection L' of L perpendicular to v, i.e., $L' = L/L(v)$. If v is indeed the shortest vector of L, then for the right value i, the images of the projected balls $B_{p_{ij}}(r_i)$ are either disjoint or identical, depending on whether the respective centers are congruent modulo v. And therefore an honest prover P with unlimited computing power, has no difficulty meeting his obligation. Now suppose $\lambda_1(L) \leq t$. Then since v is a primitive lattice vector with length $||v|| > t$, it must be linearly independent of the true shortest vector, and therefore $||v||$ is much longer than $\lambda_1(L)$. It follows that for the appropriate i, in the span of the orthogonal projection L' there is a lot of overlap between various projected balls $B_{p_{ij}}(r_i)$, $1 \leq j \leq m$.

Now we give more details. Suppose $\lambda_1(L) > t$. P chooses $v \in L$ with $||v|| = \lambda_1(L)$. Then

$$\lambda_1(L') > \sqrt{\sqrt{n} - \frac{1}{4}}\ \ ||v||,$$

which is approximately $n^{1/4}||v||$ for large n. This is because a non-zero vector of L' of length $\lambda_1(L')$ can be lifted to a vector in L, of length at most $\sqrt{\lambda_1(L')^2 + \frac{1}{4}||v||^2}$, and linearly independent of v. Thus $\sqrt{\lambda_1(L')^2 + \frac{1}{4}\lambda_1(L)^2} > n^{1/4}||v||$. Let i the unique value such that $2^i t < ||v|| \leq 2^{i+1}t$. Then $0 \leq i \leq \lfloor \log_2 T - \log_2 t \rfloor$. For this i, the radius r_i is less than half of $\lambda_1(L')$,

$$\lambda_1(L') > 2^i t \sqrt{\sqrt{n} - \frac{1}{4}} = 2r_i.$$

Thus the projected images of all the balls $B_p(r_i)$, for all $p \in L$ are mutually disjoint $(n-1)$-dimensional balls, except for balls with centers that differ by a multiple of v. Since the points $z_{i1}, z_{i2}, \ldots, z_{im}$ did belong to some balls $B_{p_{i1}}(r_i), B_{p_{i2}}(r_i), \ldots, B_{p_{im}}(r_i)$, the honest prover P can find some $p'_1, \ldots, p'_m \in L$, such that $z_{ij} \in B_{p'_j}(r_i)$, and $p'_j \equiv p_{ij} \bmod v$ for all j. The verifier now checks that all the requirements are satisfied. (Primitivity can be easily checked by expressing the lattice vector v in terms of any basis, and v is primitive iff the integral coefficients are relatively prime.) Hence honest provers will be accepted with probability one, and we have completeness.

To show soundness, suppose $\lambda_1(L) \leq t$. Suppose the prover P' returns v and $p'_1, \ldots, p'_m$. Without loss of generality, $v, p'_1, \ldots, p'_m \in L$, v is a primitive vector, and $||v|| > t$, and $p'_j \equiv p_{ij} \bmod v$, for otherwise it will be rejected immediately. (Note that $v \in L$ and $p'_j \equiv p_{ij} \bmod v$ implies that $p'_j \in L$, where i is the unique value as specified in the protocol.) Since v is a primitive vector with $||v|| > t \geq \lambda_1(L)$, v must be linearly independent of the true shortest vector, call it v_0. Thus by the $n^{1/4}$-uniqueness property, $||v|| > n^{1/4}\lambda_1(L)$. Hence,

$$r_i = 2^{i-1} t \sqrt{\sqrt{n} - \frac{1}{4}} \geq \sqrt{\sqrt{n} - \frac{1}{4}}\ \ ||v||/4 > n^{1/4}\sqrt{\sqrt{n} - \frac{1}{4}}\ \ \lambda_1(L)/4,$$

which is of order $\sqrt{n}\lambda_1(L)$.

For every p_{ij}, $1 \leq j \leq m$, there is at least one neighbor lattice point $\tilde{p}_{ij}$ which is at most distance $\lambda_1(L)$ away, and $p_{ij} - \tilde{p}_{ij} \equiv 0 \bmod v_0$ and hence $p_{ij} - \tilde{p}_{ij} \not\equiv 0 \bmod v$. Each such pair of balls has a substantial intersection $B_{p_{ij}}(r_i) \cap B_{\tilde{p}_{ij}}(r_i)$, since the radius is of order $\sqrt{n}\lambda_1(L)$. When the point z_{ij} is chosen to be in the intersection, $B_{p_{ij}}(r_i) \cap B_{\tilde{p}_{ij}}(r_i)$, which happens with substantial probability, p_{ij} or $\tilde{p}_{ij}$ could have been picked as the secret lattice points, with essentially equal probability (the error term is exponentially small and accounts for the boundary of the large parallelepiped). In this case, i.e., conditional to an i and $z_{ij} \in B_{p_{ij}}(r_i) \cap B_{\tilde{p}_{ij}}(r_i)$, any prover can achieve a success probability of at most $1/2 + e^{-n^c}$. We note that every try (every j) is independent, and the above estimate of $1/2 + e^{-n^c}$ is valid conditional to any other tries. Compound this by m parallel tries, and summing over all i from 0 to $\log_2 T = n^{O(1)}$, we conclude that the success probability of any prover is exponentially small, no more than $e^{-n^{c'}}$. Hence dishonest provers will be caught with probability exponentially close to one. □

Acknowledgements

We thank the anonymous referees for helpful comments. We also thank Miki Ajtai, Oded Goldreich, Shafi Goldwasser and 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 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.

[8] 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.

[9] 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/`.

[10] 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/`.

[11] 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/`.

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

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

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

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

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

[17] 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.

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

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

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

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

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

[23] 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.

[24] 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.