Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 76 (2013)

Improved hardness results for unique shortest vector problem

Divesh Aggarwal* Chandan Dubey†

Abstract

The unique shortest vector problem on a rational lattice is the problem of finding the shortest non-zero vector under the promise that it is unique (up to multiplication by -1). We give several incremental improvements on the known hardness of the unique shortest vector problem (uSVP) using standard techniques. This includes a deterministic reduction from the shortest vector problem to the uSVP, the NP-hardness of uSVP on $\left(1+\frac{1}{\mathrm{poly}(n)}\right)$-unique lattices, and a proof that the decision version of uSVP defined by Cai [Cai98] is in co-NP for $n^{1/4}$-unique lattices.

1 Introduction

Despite its simple grid like structure, lattices have wide and varied applications in many areas of mathematics and after the discovery of LLL algorithm [LLL82] also in computer science. The scope of the application was furthered by the breakthrough result of Ajtai [Ajt04], who showed that lattice problems have a very desirable property for cryptography: a worst case to average case reduction. This property yields one-way functions and collision resistant hash functions, based on the *worst case* hardness of lattice problems. This is in a stark contrast to the traditional number theoretic constructions which are based on the average-case hardness e.g., factoring, discrete logarithms.

A *lattice* L is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$. These vectors are referred to as a *basis* of the lattice and n is called the *rank* of the lattice. The *successive minima* $\lambda_i(\mathrm{L})$ (where $i = 1, \ldots, n$) of the lattice L are among the most fundamental parameters associated to a lattice. The $\lambda_i(\mathrm{L})$ is defined as the smallest value such that a sphere of radius $\lambda_i(\mathrm{L})$ centered around the origin contains at least i linearly independent lattice vectors.

The shortest vector problem (SVP) is arguably the most important problem on rational lattices. Given a lattice L, the problem asks for a shortest non-zero vector of length $\lambda_1(\mathrm{L})$. A generalization of the decision version of the SVP leads to the GapSVP problem. The GapSVP_γ can be seen as a promise problem, which given a lattice L and an integer d, asks to distinguish between the case $\lambda_1(\mathrm{L}) \leq d$ and $\lambda_1(\mathrm{L}) > \gamma d$.

A lattice L is called γ unique if $\lambda_2(\mathrm{L}) > \gamma\lambda_1(\mathrm{L})$. In this work, we will be concerned with the unique shortest vector problem (uSVP for short). For a parameter γ, the uSVP_γ is defined as follows. Given a γ-unique lattice L; find the shortest non-zero vector in L. Notice that for uSVP, γ can be interpreted both as a uniqueness factor, and approximation factor. The two resulting problems are equivalent. This justifies the uSVP_γ notation. The security of the first

*Department of Computer Science, EPFL.
†Department of Computer Science, ETH Zurich.

ISSN 1433-8092

lattice based public-key cryptosystem by Ajtai-Dwork [AD97] was based on the worst-case hardness of $\text{uSVP}_{O(n^8)}$. In a series of papers [GGH97, Reg04], the uniqueness factor was reduced to $O(n^{1.5})$.

Our understanding of the hardness of uSVP is far from satisfactory. The uSVP problem was proved equivalent to the GapSVP problem upto an approximation factor of $\sqrt{n}$ [LM09]. Unfortunately, the reduction from GapSVP to uSVP does not imply hardness because of a loss of $\sqrt{n}$ factor [LM09]. Kumar-Sivakumar [KS01], via a randomized reduction from SVP, show that uSVP_γ is NP-hard for $\gamma = 1 + 2^{-n^c}$, for some constant c. We improve this result by giving a deterministic reduction from SVP to uSVP. We also give a randomized reduction which shows that uSVP is NP-hard for $\gamma = 1 + 1/\operatorname{poly}(n)$ under randomized reductions.

There are two versions of the decision uSVP in the literature: one given by Cai [Cai98] (denoted, duSVP) and another by Regev [Reg04] (denoted, duSVP'). Unlike the duSVP' defined by Regev, a search to decision reduction is not known for the duSVP. Cai also shows that duSVP is in co-AM for $n^{1/4}$-unique lattices. We give three results here, all concerning duSVP.

(i). We show that the search uSVP_γ can be solved in polynomial time given an oracle for the $\text{duSVP}_{\gamma/2}$.

(ii). The duSVP problem is in co-AM on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices and is in co-NP for $n^{1/4}$-unique lattices.

(iii). The duSVP problem is NP-hard on $(1 + 2^{-n^c})$-unique lattices, for some constant c.

It is unlikely that GapSVP_γ is NP-hard for $\gamma = \left(\frac{n}{\log n}\right)^{1/2}$, as otherwise the polynomial hierarchy collapses [GG00, CN00]. The same conclusion does not follows from item (ii) in case of duSVP. The decision uSVP is a promise problem (as opposed to a *total* problem) and, unlike GapSVP, we do not know how to handle the queries which do not satisfy the promise.

The results on duSVP can be interpreted as follows. Item (i)+(iii) indicate that duSVP is likely to be a difficult problem, especially if we assume that uSVP is a hard problem. On the other hand, item (ii) points out that duSVP perhaps is not so hard on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices. Showing that the polynomial hierarchy collapses if duSVP is NP-hard on $\left(\frac{n}{\log n}\right)^{1/4}$-unique lattices is an open problem.

2 Preliminaries

For a positive integer k we use the notation $[k]$ to denote the set $\{1, \ldots, k\}$.

A lattice basis is a set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$. It is sometimes convenient to think of the basis as an $m \times n$ matrix $\mathbf{B}$, whose n columns are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The lattice generated by the basis $\mathbf{B}$ will be written as $\mathrm{L}(\mathbf{B})$ and is defined as $\mathrm{L}(\mathbf{B}) = \{\mathbf{Bx} | \mathbf{x} \in \mathbb{Z}^n\}$. A vector $\mathbf{v} \in \mathrm{L}$ is called a primitive vector of the lattice L if it is not an integer multiple of another lattice vector except $\pm\mathbf{v}$. We will assume that the lattice is over integers, i.e., $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$. The restriction to integers instead of arbitrary real vectors is important for making the input representable in a finite number of bits.

The *successive minima* $\lambda_i(\mathrm{L})$ (where $i = 1, \ldots, n$) of the lattice L is defined as the smallest value such that a sphere of radius $\lambda_i(\mathrm{L})$ centered around the origin contains at least i linearly

independent lattice vectors. A lattice L is called γ-unique if $\lambda_2(\mathrm{L}) > \gamma\lambda_1(\mathrm{L})$. In this paper we are concerned with the following variants of the unique shortest vector problem.

uSVP$_\gamma$: Given a γ-unique lattice basis $\mathbf{B}$, find a vector $\mathbf{v} \in \mathrm{L}(\mathbf{B})$ such that $\|\mathbf{v}\| = \lambda_1(\mathrm{L}(\mathbf{B}))$.

duSVP$_\gamma$: Given a γ-unique lattice basis $\mathbf{B}$, and an integer d, say "YES" if $d \leq \lambda_1(\mathbf{B})$ and "NO" otherwise.

duSVP$'_\gamma$: Given a γ-unique lattice basis $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n]$, a prime $p > 2$ and an integer d, say "YES" if p divides the coefficient of $\mathbf{b}_1$ in the shortest vector of the lattice $\mathrm{L}(\mathbf{B})$ and say "NO" otherwise.

There are two decision variants of the uSVP problem. Chronologically, the first one i.e., duSVP was defined implicitly in [Cai98] and explicitly in [CN00]. The second one i.e., duSVP$'$, is given in [Reg04] and has the desirable property that uSVP$_\gamma$ can be solved using an oracle that solves duSVP$'_\gamma$.

We now prove a few useful results on lattices. The following lemma is taken from [KS01]. A proof is provided for completeness.

Lemma 1. *Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of a lattice* L. *For any two vectors $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i, \mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i \in \mathrm{L}$ such that $\mathbf{u} \neq \pm\mathbf{v}$ and $\|\mathbf{u}\| = \|\mathbf{v}\| = \lambda_1(\mathrm{L})$, there exists $j \in [n]$ such that $\alpha_j \not\equiv \beta_j \pmod 2$.*

Proof. For the sake of contradiction, assume that there exists a lattice vector $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i$ and a lattice vector $\mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i$ such that $\|\mathbf{u}\| = \|\mathbf{v}\| = \lambda_1(\mathrm{L})$ and $\alpha_j \equiv \beta_j \pmod 2$ for all $j \in [n]$. But then, $\frac{\mathbf{u}+\mathbf{v}}{2} \in \mathrm{L}$ and $\frac{\mathbf{u}-\mathbf{v}}{2} \in \mathrm{L}$. Since $\mathbf{u} \neq \pm\mathbf{v}$, both these vectors are non-zero. Also,

$$\left\|\frac{\mathbf{u}+\mathbf{v}}{2}\right\|^2 + \left\|\frac{\mathbf{u}-\mathbf{v}}{2}\right\|^2 = \frac{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2}{2} = (\lambda_1(\mathrm{L}))^2 \ .$$

But this implies that $0 < \|\frac{\mathbf{u}+\mathbf{v}}{2}\|, \|\frac{\mathbf{u}-\mathbf{v}}{2}\| < \lambda_1(\mathrm{L})$, a contradiction. □

We next define the LLL reduced basis [LLL82].

Definition 1. *Given a basis $\mathbf{B} = [\mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_n]$, the Gram-Schmidt orthogonalization of $\mathbf{B}$ is defined by $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\tilde{\mathbf{b}}_j$, where $\mu_{ij} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle}$.*

Note that the Gram-Schmidt orthogonal basis satisfies $\langle \tilde{\mathbf{b}}_i, \tilde{\mathbf{b}}_j \rangle = 0$, for all $i \neq j$.

Definition 2. *A basis $\mathbf{B} = [\mathbf{b}_1\ \ldots\ \mathbf{b}_n]$ with Gram-Schmidt orthogonal basis $[\tilde{\mathbf{b}}_1\ \ldots\ \tilde{\mathbf{b}}_n]$ is LLL reduced if for all $1 \leq i < n$, $\|\tilde{\mathbf{b}}_i\|^2 \leq 2\|\tilde{\mathbf{b}}_{i+1}\|^2$ and for all $1 \leq j < i \leq n$, $\mu_{ij} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle} \leq \frac{1}{2}$.*

The LLL reduced basis property can be interpreted as "$\tilde{\mathbf{b}}_{i+1}$ is not much shorter than $\tilde{\mathbf{b}}_i$". It is possible to LLL reduce any basis in polynomial time [LLL82].

3 Deterministic reductions

In this section, we give two deterministic reductions. The first is a way to make any lattice unique while the second is to solve uSVP using a duSVP oracle. We first give an overview of the techniques used in each reduction.

In the first reduction, we transform a lattice into a unique lattice. The idea is to introduce errors in the basis such that shortest vectors of the same length map to vectors of different lengths in the lattice with errors. A similar idea was used by Kannan [Kan87] to reduce the search SVP to decision SVP for the exact case. Kannan's idea was to scale the co-ordinate system, each with a different multiple, such that the co-ordinate of a shortest vector can be recovered from its length. The downside of Kannan's reduction is that it needs to call the decision SVP oracle polynomially many times to recover the signs of the shortest vector entries. Hu-Pan [HP14] fixed this problem by using a combination of scaling and then introducing appropriate additive errors in the first co-ordinate of the basis vectors. For appropriately chosen $\epsilon_1, \cdots, \epsilon_{n+1}$, the transformation of Hu-Pan can be described as follows.

$$\mathbf{B} \to \epsilon_{n+1}\mathbf{B} + \begin{pmatrix} \epsilon_1 & \epsilon_2 & \dots & \epsilon_n \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Our reduction is different from theirs in the following way. Instead of scaling the original lattice, we embed it into a space with dimensions $2n$, where n is the dimension of the original lattice. At the same time, we also introduce systematic errors in a unique dimension for each basis vector. This is possible because the number of dimensions has doubled from before. Succinctly, for appropriately chosen errors $\epsilon_1, \cdots, \epsilon_n$, the transformation can be described as follows.

$$[\mathbf{b}_1, \cdots, \mathbf{b}_n] \to \begin{pmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_n \\ \epsilon_1 & 0 & \dots & 0 \\ 0 & \epsilon_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \epsilon_n \end{pmatrix}$$

The second reduction is from uSVP_γ to $\text{duSVP}_{\gamma/2}$. This reduction borrows heavily from the uSVP_γ to GapSVP_γ reduction given by Lyubashevsky-Micciancio [LM09]. Our modification is to replace the GapSVP_γ oracle by $\text{duSVP}_{\gamma/2}$ oracle as follows. For computing the unique shortest vector, we split the original lattice into three sparser lattices, all containing a vector which is two times the shortest vector. We can then replace the GapSVP_γ oracle and use the $\text{duSVP}_{\gamma/2}$ oracle to find the sub-lattice which also contains the shortest vector.

3.1 Making a lattice unique

If a basis is LLL reduced then the coefficients of the basis vectors in any shortest vector of the lattice, can be bounded by $2^{3(n-1)/2}$. This result might have been implicitly used in the literature before, but we are not aware of any explicit formalizations.

Lemma 2. *Let* $\mathbf{B} = [\mathbf{b}_1 \ \cdots \ \mathbf{b}_n]$ *be a* LLL *reduced basis and* $\mathbf{u} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$ *be a shortest vector of the lattice. Then, for all* $i \in [n]$, $|\alpha_i| \leq 2^{3(n-1)/2}$.

Proof. Let us suppose that $[\tilde{\mathbf{b}}_1 \ \cdots \ \tilde{\mathbf{b}}_n]$ be the Gram-Schmidt orthogonal basis corresponding to $\mathbf{B}$ and $\mathrm{L} = \mathrm{L}(\mathbf{B})$. For proving the lemma, it suffices to prove that for $0 \leq j < n$, $|\alpha_{n-j}| \leq 2^{(n-1)/2+j}$. We use induction on j to prove this claim.

Consider the base case of $j = 0$. From the property of the Gram-Schmidt orthogonalization, $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$ and the projection of the vector $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$ in the direction of $\tilde{\mathbf{b}}_n$ is $\alpha_n \tilde{\mathbf{b}}_n$. But then, the following inequality shows that $|\alpha_n| \leq 2^{(n-1)/2}$.

$$\|\tilde{\mathbf{b}}_1\| \geq \|\mathbf{u}\| \geq |\alpha_n| \|\tilde{\mathbf{b}}_n\| \geq 2^{-(n-1)/2} |\alpha_n| \|\tilde{\mathbf{b}}_1\|$$

By induction hypothesis, one assumes that $|\alpha_{n-s}| \leq 2^{(n-1)/2+s}$ for $0 \leq s < k$.

To complete the proof by induction, it suffices to show that $|\alpha_{n-k}| \leq 2^{(n-1)/2+k}$. By the property of Gram-Schmidt orthogonalization, the projection of $\mathbf{u}$ in the direction of $\tilde{\mathbf{b}}_{n-k}$ is

$$\left(\alpha_{n-k} + \left(\sum_{i=n-k+1}^{n} \mu_{i,n-k} \alpha_i \right) \right) \tilde{\mathbf{b}}_{n-k}, \text{ where } \mu_{i,n-k} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_{n-k} \rangle}{\langle \tilde{\mathbf{b}}_{n-k}, \tilde{\mathbf{b}}_{n-k} \rangle} \tag{1}$$

Also, by Definition 2, $|\mu_{i,n-k}| \leq 1/2$ for all $n-k+1 \leq i \leq n$ and $\|\tilde{\mathbf{b}}_1\| \leq 2^{(i-1)/2} \|\tilde{\mathbf{b}}_i\|$. Hence,

$$\begin{aligned} \|\tilde{\mathbf{b}}_1\| \geq \|\mathbf{u}\| &\overset{(1)}{\geq} \left| \left(\alpha_{n-k} + (\sum_{i=n-k+1}^{n} \mu_{i,n-k} \alpha_i) \right) \right| \|\tilde{\mathbf{b}}_{n-k}\| \\ &\overset{\text{Def. 2}}{\geq} 2^{-(n-k-1)/2} \left| \left(\alpha_{n-k} + (\sum_{i=n-k+1}^{n} \mu_{i,n-k} \alpha_i) \right) \right| \|\tilde{\mathbf{b}}_1\| \end{aligned}$$

But then,

$$\begin{aligned} |\alpha_{n-k}| &\leq 2^{(n-k-1)/2} + \sum_{i=n-k+1}^{n} |\mu_{i,n-k} \alpha_i| \overset{\text{Def. 2}}{\leq} 2^{(n-k-1)/2} + \frac{1}{2} \sum_{i=0}^{k-1} |\alpha_{n-i}| \\ &\leq 2^{(n-k-1)/2} + \frac{1}{2} \sum_{i=0}^{k-1} 2^{(n-1)/2+i} \leq 2^{(n-1)/2+k} \ . \end{aligned}$$

□

Theorem 1. *Let* L *be an integer lattice with* LLL *reduced basis* $\mathbf{B} = [\mathbf{b}_1 \ \cdots \ \mathbf{b}_n]$. *Then, the lattice spanned by the following basis is* $(1 + 2^{-n^c})$*-unique for some constant* $c > 0$.

$$\begin{pmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_n \\ \epsilon_1 & 0 & \dots & 0 \\ 0 & \epsilon_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \epsilon_n \end{pmatrix} \text{ where } \epsilon_i = \frac{2^{2(i-1)n}}{2^{2n^2}}$$

Proof. For technical convenience, we denote the transformed basis as $\tau\mathbf{B} = [\tau\mathbf{b}_1 \ \cdots \ \tau\mathbf{b}_n]$ and the new lattice by τL. If $\mathbf{v} = \sum_i \beta_i \mathbf{b}_i \in$ L then we define $\tau\mathbf{v} = \sum \beta_i \tau\mathbf{b}_i$ and by definition, $\tau\mathbf{v} \in \tau$L. By construction, $\lambda_1(\mathrm{L}) < \lambda_1(\tau\mathrm{L})$.

(a). Our first step is to show that $\lambda_1(\tau\mathrm{L}) < \lambda_1(\mathrm{L}) + 2^{-n}$. Consider the shortest vector $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i \in$ L and the corresponding transformed vector $\tau\mathbf{u} \in \tau$L. Then, the following inequality proves this claim.

$$\|\tau\mathbf{u}\|^2 = \lambda_1^2(\mathrm{L}) + \sum_{i=1}^{n} \alpha_i^2 \frac{2^{4(i-1)n}}{2^{4n^2}} \overset{\text{Lemma 2}}{\leq} \lambda_1^2(\mathrm{L}) + 2^{3(n-1)} \frac{2^{4n^2}-1}{(2^{4n}-1)2^{4n^2}} < \lambda_1^2(\mathrm{L}) + 2^{-n}$$

(b). Next, we show that if $\mathbf{u}_1 \neq \pm\mathbf{u}_2$ are two vectors of the same length $\lambda_1(\mathrm{L})$, then $\tau\mathbf{u}_1$ and $\tau\mathbf{u}_2$ have different lengths. In particular, the difference in the square-lengths of $\tau\mathbf{u}_1$ and $\tau\mathbf{u}_2$ is at least 2^{-4n^2}. Let $\mathbf{u}_1 = \sum_i x_i \mathbf{b}_i$ and $\mathbf{u}_2 = \sum_i y_i \mathbf{b}_i$. By Lemma 1, there exists an index $j \in [n]$ such that $x_j \neq \pm y_j$. Let k be the largest such index. Then,

$$\begin{aligned}
\left| \|\tau\mathbf{u}_1\|^2 - \|\tau\mathbf{u}_2\|^2 \right| &= \left| \sum_{i=1}^{n} (x_i^2 - y_i^2) \left(\frac{2^{4(i-1)n}}{2^{4n^2}} \right) \right| \\
&\overset{\text{(Lem. 2)}}{>} \frac{2^{4(k-1)n}}{2^{4n^2}} - 2^{3(n-1)} \sum_{i=1}^{k-1} \frac{2^{4(i-1)n}}{2^{4n^2}} = \frac{2^{4(k-1)n}}{2^{4n^2}} - 2^{3n-2} \frac{2^{4(k-1)n}-1}{2^{4n^2}(2^{4n}-1)} > \frac{1}{2^{4n^2}}
\end{aligned}$$

(c). Finally, if $\mathbf{v} \in$ L is such that $\|\mathbf{v}\| > \lambda_1(\mathrm{L})$, then because L is an integer lattice, $\|\mathbf{v}\| \geq \sqrt{\lambda_1(\mathrm{L})^2 + 1}$. By construction, $\|\tau\mathbf{v}\| > \|\mathbf{v}\| \geq \sqrt{\lambda_1(\mathrm{L})^2 + 1}$.

Together, items (a-c) imply that the lattice τL is unique. Also, from item (b), we conclude that

$$\frac{\lambda_2(\tau\mathrm{L})}{\lambda_1(\tau\mathrm{L})} > \sqrt{1 + \frac{2^{-4n^2}}{\lambda_1(\mathrm{L})^2}} \geq 1 + \frac{2^{-4n^2}}{3\lambda_1(\mathrm{L})^2}$$

The input lattice L is an integer lattice. It follows that $\lambda_1(\mathrm{L})$ is bounded by $2^{O(n)}$ times the input size. This concludes the proof of this theorem. □

The NP-hardness of duSVP under randomized reductions, is a direct corollary of Theorem 1.

Theorem 2. *The* duSVP *variant of the decision* SVP *is* NP*-hard on* $(1 + 2^{-n^c})$*-unique lattices under randomized reductions, where* c *is a constant.*

Note that there is no obvious way to conclude this NP-hardness result from Kumar-Sivakumar [KS01]. The reason for this is that in their reduction, given a lattice L, they construct a sequence of $k = \mathrm{poly}(n)$ sublattices $\mathrm{L}_1, \ldots, \mathrm{L}_k \subseteq$ L such that at least one of them (say L_i) contains a $(1+2^{-n^c})$-unique shortest vector and $\lambda_1(\mathrm{L}_i) = \lambda_1(\mathrm{L})$. Given a $(1+2^{-n^c})$-uSVP oracle, one can easily compute $\lambda_1(\mathrm{L})$ by calling the oracle on each of $\mathrm{L}_1, \ldots, \mathrm{L}_k$ and outputting the shortest of these vectors that is in L. However, given a $(1 + 2^{-n^c})$-duSVP oracle, this is not possible because the duSVP oracle might behave arbitrarily on the sublattices that do not contain a unique shortest vector, and it is impossible to predict this behavior.

3.2 Search to decision reduction

The next task is to solve the search uSVP problem using a decision uSVP oracle. The idea is to replace the GapSVP oracle by a duSVP oracle in the uSVP_γ to GapSVP_γ reduction given by Lyubashevsky-Micciancio [LM09]. The proof, given below, shows that this replacement can be done quite smoothly without any major surprises.

Theorem 3. *Let $\gamma \geq 2$ be a number. Then, there exists a deterministic* $\text{poly}(n)$ *algorithm that solves* uSVP_γ *given a* $\text{duSVP}_{\gamma/2}$ *oracle, where n is the dimension of the input lattice.*

Proof. Let L be the γ-unique lattice spanned by the input basis $\mathbf{B} = [\mathbf{b}_1 \ \cdots \ \mathbf{b}_n]$. Let $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$ be the shortest vector in L.

Sparsification. Consider the following three bases and for $i \in [3]$, define $\mathrm{L}_i = \mathrm{L}(\mathbf{B}_i)$.

$$\begin{aligned}\mathbf{B}_1 &= (2\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n)\\ \mathbf{B}_2 &= (\mathbf{b}_1, 2\mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n)\\ \mathbf{B}_3 &= (\mathbf{b}_1 + \mathbf{b}_2, 2\mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n)\end{aligned}$$

Consider the shortest vector $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$. If α_1 is even, then $\mathbf{u} \in \mathrm{L}_1$. If α_2 is even then $\mathbf{u} \in \mathrm{L}_2$. If neither is even then the following way of writing $\mathbf{u}$ implies that $\mathbf{u} \in \mathrm{L}_3$.

$$\mathbf{u} = \alpha_1(\mathbf{b}_1 + \mathbf{b}_2) + \frac{\alpha_2 - \alpha_1}{2}(2\mathbf{b}_2) + \alpha_3\mathbf{b}_3 + \cdots + \alpha_n\mathbf{b}_n$$

By construction, $2\mathbf{u}$ belongs to each of $\mathrm{L}_1 = \mathrm{L}(\mathbf{B}_1)$, $\mathrm{L}_2 = \mathrm{L}(\mathbf{B}_2)$, and $\mathrm{L}_3 = \mathrm{L}(\mathbf{B}_3)$. Also, since each of these lattices is a sub-lattice of L, for all $i \in [3]$, $\lambda_2(\mathrm{L}_i) \geq \lambda_2(\mathrm{L})$. But then, for all $i \in [3]$, $\lambda_2(\mathrm{L}_i) > \frac{\gamma}{2}\lambda_1(\mathrm{L}_i)$. Thus, the $\text{duSVP}_{\gamma/2}$ oracle can be used to find the basis $\mathbf{B}_{s\in[3]}$ such that $\mathbf{u} \in \mathrm{L}_s$. By construction, $\mathbf{B}_s$ spans a γ-unique lattice and $\det(\mathbf{B}_s) \geq 2\det(\mathbf{B})$.

Projection. One now continues the same process of sparsification i.e., splitting the lattice spanned by $\mathbf{B}_s$ into three sparser lattices. After $t > n(n + \log_2 n)$ iterations, suppose we have a basis $\mathbf{S}$ such that $\det(\mathbf{S}) \geq 2^t \det(\mathbf{B})$ and $\mathbf{u} \in \mathrm{L}(\mathbf{S})$.

Consider $\mathbf{D}$, the dual basis of $\mathbf{S}$. By definition of a dual basis $\det(\mathbf{D})\det(\mathbf{S}) = 1$ and hence, $\det(\mathbf{D}) \leq \frac{1}{2^t \det(\mathbf{B})}$. By Minkowski's bound [Min68], we have $\lambda_1(\mathrm{L}(\mathbf{D})) \leq \sqrt{n}\det(\mathbf{D})^{1/n}$. Using the LLL algorithm [LLL82], one can find a vector $\mathbf{v} \in \mathrm{L}(\mathbf{D})$ such that

$$\begin{aligned}\|\mathbf{v}\| \leq 2^n\lambda_1(\mathrm{L}(\mathbf{D})) &\leq \frac{2^n\sqrt{n}}{2^{t/n}\det(\mathbf{B})^{1/n}}, \text{ and}\\ |\langle \mathbf{u}, \mathbf{v}\rangle| \leq \|\mathbf{u}\|\|\mathbf{v}\| &\leq \sqrt{n}\det(\mathbf{B})^{1/n}\|\mathbf{v}\| \leq n \cdot 2^{n-t/n} < 1\end{aligned}$$

But $\mathbf{u} \in \mathrm{L}(\mathbf{S})$ and $\mathbf{v} \in \mathrm{L}(\mathbf{D})$, and thus $|\langle \mathbf{u}, \mathbf{v}\rangle|$ is an integer. Thus, $\langle \mathbf{u}, \mathbf{v}\rangle = 0$, i.e., $\mathbf{v}$ is perpendicular to $\mathbf{u}$. Thus, by taking the projection of $\mathrm{L}(\mathbf{S})$ perpendicular to $\mathbf{v}$, we get a lattice L' of rank $(n-1)$ such that $\mathbf{u} \in \mathrm{L}'$.

Continuing alternately with Sparsification and Projections steps, we reduce the problem to one dimension. Note that in either step we do not eliminate the shortest vector of the original lattice L i.e., $\mathbf{u}$. Thus, when the problem has been reduced to one dimension then the basis has only one vector and by the invariant, it equals $\mathbf{u}$. □

4 A co-NP reduction

In this section, we give a co-NP reduction from duSVP to GapSVP. Although not common, co-NP reductions have been used before for studying lattices [GMR05]. The result encompasses the $\text{duSVP}_{n^{1/4}} \in$ co-AM proof by Cai [Cai98].

But first, we prove the following result on γ-unique lattices. The proof of this lemma is implicit in [Cai98].

Lemma 3. *Let* L *be a* γ*-unique lattice,* $\mathbf{v}$ *be a primitive vector from* L *and* L$'$ *be the lattice obtained by projecting* L *to the space orthogonal to* $\mathbf{v}$*. Then,*

$$\begin{aligned} &\lambda_1(\mathrm{L}') \leq \frac{\|\mathbf{v}\|}{\gamma} && \text{if } \|\mathbf{v}\| \neq \lambda_1(\mathrm{L}) \\ &\lambda_1(\mathrm{L}') > \sqrt{\gamma^2 - \tfrac{1}{4}}\|\mathbf{v}\| && \text{otherwise} \end{aligned}$$

Proof. Let $\mathbf{u}$ be the shortest vector in L and $\mathbf{u}'$ be the projection of $\mathbf{u}$ in the space orthogonal to $\mathbf{v}$. By definition, $\mathbf{u}' \in \mathrm{L}'$.

Consider the case of $\|\mathbf{v}\| \neq \lambda_1(\mathrm{L})$. In this case, $\|\mathbf{v}\| \geq \lambda_2(\mathrm{L}) \geq \gamma\lambda_1(\mathrm{L})$ or $\lambda_1(\mathrm{L}) \leq \frac{\|\mathbf{v}\|}{\gamma}$. Projections do not increase the length of vectors, and hence $\lambda_1(\mathrm{L}') \leq \lambda_1(\mathrm{L}) \leq \frac{\|\mathbf{v}\|}{\gamma}$.

Otherwise, $\|\mathbf{v}\| = \lambda_1(\mathrm{L})$. In this case, assume that $\mathbf{w} \in \mathrm{L}$ is a vector such that $\mathbf{w}'$ i.e., the projection of $\mathbf{w}$ in the space orthogonal to $\mathbf{v}$, is a shortest vector in L$'$. By construction, $\mathbf{w} = \mathbf{w}' + \alpha\mathbf{v}$, for some $\alpha \in \mathbb{R}$. Note that $\mathbf{w} - \lfloor\alpha\rceil\mathbf{v} \in \mathrm{L}$ is not an integer multiple of $\mathbf{v}$ and L is γ-unique. Hence, $\|\mathbf{w} - \lfloor\alpha\rceil\mathbf{v}\| \geq \lambda_2(\mathrm{L}) > \gamma\|\mathbf{v}\|$. But then,

$$\gamma\|\mathbf{v}\| < \|\mathbf{w} - \lfloor\alpha\rceil\mathbf{v}\| \leq \|\mathbf{w}' + (\alpha - \lfloor\alpha\rceil)\mathbf{v}\| \leq \sqrt{\|\mathbf{w}'\|^2 + \frac{1}{4}\|\mathbf{v}\|^2}, \text{ and}$$

$$\lambda_1(\mathrm{L}') = \|\mathbf{w}'\| > \left(\sqrt{\gamma^2 - \frac{1}{4}}\right)\|\mathbf{v}\|$$

□

Theorem 4. *There is a* NP *reduction from* co-duSVP_γ *to* co-$\text{GapSVP}_{\gamma\sqrt{\gamma^2-\frac{1}{4}}}$.

Proof. Let $\gamma' = \gamma\sqrt{\gamma^2 - 1/4}$.

For simplicity we describe the setting in the prover-verifier language. We are given an NP proof system for co-$\text{GapSVP}_{\gamma'}$ which on input $(\mathbf{X}, t)$, where $\mathbf{X}$ is a basis and t an integer, does the following.

- If $\lambda_1(\mathbf{X}) > \gamma' t$ then there exists a witness $w = w(\mathbf{X}, t)$ such that the verifier accepts.
- If $\lambda_1(\mathbf{X}) \leq t$ then for any witness w, the verifier rejects.

Given this system, we want to design an NP proof system for co-duSVP_γ. In particular, on an input $(\mathbf{B}, d)$, where the lattice $\mathrm{L}(\mathbf{B})$ is γ-unique and d is an integer, the proof system should do the following.

- If $\lambda_1(\mathbf{B}) > d$ then there exists a witness $y = y(\mathbf{B}, d)$ such that the verifier accepts.
- If $\lambda_1(\mathbf{B}) \leq d$ then for any witness y, the verifier rejects.

We now describe how to design the NP proof system for co-duSVP$_\gamma$ given a NP proof system for co-GapSVP$_{\gamma'}$.

Let $(\mathbf{B}, d)$ be an instance of co-duSVP$_\gamma$ and $\mathrm{L} = \mathrm{L}(\mathbf{B})$. By the promise of the duSVP problem, L is γ-unique. Let the proof for co-duSVP$_\gamma$ be of the form $y = (w, \mathbf{v})$ where w is a string and $\mathbf{v} \in \mathrm{L}$. Assume that the verifier for co-duSVP$_\gamma$ accepts if and only if $\mathbf{v}$ is a primitive vector in L, $\|\mathbf{v}\| > d$, and the verifier for co-GapSVP$_{\gamma'}$ accepts the proof w for the instance $(\mathbf{B}', \frac{\|\mathbf{v}\|}{\gamma})$, where $\mathbf{B}'$ is a basis of the lattice obtained by projecting L to the space orthogonal to $\mathbf{v}$. We now show that there exists a valid witness y if $\lambda_1(\mathrm{L}) > d$ and no witness exists for $\lambda_1(\mathrm{L}) \leq d$.

- $\lambda_1(\mathrm{L}) > d$. In this case, let $\mathbf{v}$ be the shortest vector of L. Then $\mathbf{v}$ is a primitive vector of length greater than d and, by Lemma 3, $\lambda_1(\mathrm{L}') > \gamma' \frac{\|\mathbf{v}\|}{\gamma}$.
- $\lambda_1(\mathrm{L}) \leq d$. In this case, for the verifier to accept for some $y = (w, \mathbf{v})$, we have that $\|\mathbf{v}\| > d \geq \lambda_1(\mathrm{L})$, and hence by Lemma 3, $\lambda_1(\mathrm{L}') \leq \frac{\|\mathbf{v}\|}{\gamma}$. This implies that the verifier for co-GapSVP$_{\gamma'}$ rejects on input $(\mathbf{B}', \frac{\|\mathbf{v}\|}{\gamma})$ and any w.

□

The following are direct corollaries of Theorem 4.

Theorem 5. *If* GapSVP$_{\gamma\sqrt{\gamma^2-\frac{1}{4}}} \in$ co-AM*, then* duSVP$_\gamma \in$ co-AM*. In particular, there exists a constant $c > 0$ such that* duSVP$_{c(\frac{n}{\log n})^{1/4}} \in \mathrm{NP} \cap$ co-AM*.*

Proof. The proof follows from the result of [GG00], which says that GapSVP$_{\left(\frac{n}{\log n}\right)^{1/2}} \in$ co-AM. □

Theorem 6. *If* GapSVP$_{\gamma\sqrt{\gamma^2-\frac{1}{4}}} \in$ co-NP*, then* duSVP$_\gamma \in$ co-NP*. In particular, there exists a constant $c > 0$ such that* duSVP$_{cn^{1/4}} \in \mathrm{NP} \cap$ co-NP*.*

Proof. The proof follows from the result of [AR05], which says that GapSVP$_{c'n^{1/2}} \in$ co-NP for some constant c'. □

5 Improved uSVP hardness under randomized reductions

In this section, we show that the uSVP problem is NP-hard under randomized reductions on $(1 + n^{-c})$-unique lattices, where c is a constant.

The following is a result obtained by Theorem 3.1 and Theorem 5.1 of [Kho05].

Theorem 7. *The problem decision* SVP *(i.e.,* GapSVP$_1$*) is* NP*-hard under randomized reductions. The problem remains* NP*-hard when restricted to instances $(\mathbf{B}, d)$, where $\mathbf{B}$ is an n-dimensional integer lattice and d is bounded by a polynomial in n.*

We state below a result from [KS01].

Theorem 8. *Let $\mathbf{B}$ be a basis of an n-dimensional lattice $\mathrm{L} = \mathrm{L}(\mathbf{B})$. Then there exists a probabilistic polynomial time algorithm that outputs a sequence of lattice basis $\mathbf{B}_1, \ldots \mathbf{B}_{n+1}$ such that*

$$\mathrm{L} \supseteq \mathrm{L}(\mathbf{B}_1) \supseteq \cdots \supseteq \mathrm{L}(\mathbf{B}_{2n+2}) \,,$$

and with probability at least $\frac{2}{3} - 2^{-n}$, one of $\mathrm{L}(\mathbf{B}_1), \ldots, \mathrm{L}(\mathbf{B}_{2n+2})$ has exactly two vectors ($\mathbf{v}$ and $-\mathbf{v}$ for some $\mathbf{v} \in \mathrm{L}$) of length $\lambda_1(\mathrm{L})$.

Combining Theorem 8 with Theorem 7 immediately gives the NP-hardness of uSVP.

Theorem 9. *The problem* $\text{uSVP}_{(1+\frac{1}{\text{poly}(n)})}$ *for* n*-dimensional lattices is* NP*-hard under randomized reductions.*

Proof. We give a reduction from decision SVP to $\text{uSVP}_{(1+\frac{1}{\text{poly}(n)})}$ where decision SVP is restricted to instances $(\mathbf{B}, d)$ where $\mathbf{B}$ is an n-dimensional integer lattice and d is bounded by a polynomial in n. Consider such an SVP instance. Use the algorithm in Theorem 8 to obtain a sequence of sublattices $L_1, \ldots, L_{2n+2}$, and then compute the length of the vector computed by a $\text{uSVP}_{(1+1/d)}$ oracle on each of $L_1, \ldots, L_{2n+2}$ and if the minimum of these lengths is at most d, then return YES, and NO otherwise. By Theorem 8, with probability $\frac{2}{3} - 2^{-n}$ one of them (say L_i) is such that $\lambda_1(L_i) = \lambda_1(L(\mathbf{B}))$ and

$$\lambda_2(L_i) \geq \sqrt{\lambda_1(L_i)^2 + 1} = \lambda_1(L_i)\sqrt{\left(1 + \frac{1}{\lambda_1(L_i)^2}\right)} \geq \lambda_1(L_i) \cdot \left(1 + \frac{1}{3\lambda_1(L_i)^2}\right) .$$

Thus, if the SVP instance is a YES instance, i.e., if $\lambda_1(L(\mathbf{B})) \leq d$, then, with probability $2/3 - 2^{-n}$, the $\text{uSVP}_{(1+\frac{1}{3d^2})}$ oracle computes a vector of length at most d on input L_i. On the other hand, if the SVP instance is a NO instance, then $\lambda_1(L(\mathbf{B})) > d$. This implies that the shortest vector of each of $L_1, \ldots, L_{2n+2}$ has length greater than d and hence the algorithm outputs NO with probability 1. □

6 Discussion and open problems

Many interesting problems related to uSVP and duSVP remain. The gap between the uniqueness factor $(1 + 2^{-n^c})$, for which we know that the duSVP is hard, and $(\frac{n}{\log n})^{1/4}$, for which we know that the problem is in co-**AM** is still large. It will be interesting to try to show hardness of duSVP (or even uSVP) for some constant factor.

The duSVP was not known to be **NP**-hard, as it does not follow from Kumar-Sivakumar's work [KS01]. Our deterministic reduction from `SVP` succeeds in showing the **NP**-hardness of the decision version but this hardness cannot be concluded even for a factor of $(1 + \frac{1}{\texttt{poly}})$ hardness, which remains an open problem. The search to decision equivalence of duSVP and uSVP upto a factor of 2, shows that the complexity of the two problems is not too far apart. It is interesting to try to improve the factor of 2, but this might require substantially new ideas. It is a major open question whether such a search to decision reduction is possible in the case of approximation versions of the shortest vector problem and the closest vector problem.

References

[AD97] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 284–293. ACM, 1997.

[Ajt04] Miklós Ajtai. Generating hard instances of lattice problems. In *Complexity of computations and proofs*, volume 13 of *Quad. Mat.*, pages 1–32. Dept. Math., Seconda Univ. Napoli, Caserta, 2004. Preliminary version in STOC'96.

[AR05] Dorit Aharonov and Oded Regev. Lattice problems in **NP**∩co-**NP**. *Journal of the ACM (JACM)*, 52(5):749–765, 2005.

[Cai98] Jin-Yi Cai. A relation of primal-dual lattices and the complexity of shortest lattice vector problem. *Theoretical Computer Science*, 207(1):105–116, 1998.

[CN00] Jin-Yi Cai and Ajay Nerurkar. A note on the non-np-hardness of approximate lattice problems under general cook reductions. *Information processing letters*, 76(1):61–66, 2000.

[GG00] Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences*, 60(3):540–563, 2000.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Eliminating decryption errors in the ajtai-dwork cryptosystem. In *Advances in CryptologyCRYPTO'97*, pages 105–111. Springer, 1997.

[GMR05] Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The complexity of the covering radius problem. *Computational Complexity*, 14(2):90–121, 2005.

[HP14] Gengran Hu and Yanbin Pan. Improvements on reductions among different variants of svp and cvp. In *Information Security Applications*, pages 39–51. Springer, 2014.

[Kan87] Ravi Kannan. Algorithmic geometry of numbers. *Annual review of computer science*, 2(1):231–267, 1987.

[Kho05] Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM (JACM)*, 52(5):789–808, 2005.

[KS01] S Ravi Kumar and D Sivakumar. On the unique shortest lattice vector problem. *Theoretical Computer Science*, 255(1):641–648, 2001.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LM09] Vadim Lyubashevsky and Daniele Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Advances in Cryptology-CRYPTO 2009*, pages 577–594. Springer, 2009.

[Min68] Hermann Minkowski. *Geometrie der zahlen*, volume 40. , 1968.

[Reg04] Oded Regev. New lattice-based cryptographic constructions. *Journal of the ACM (JACM)*, 51(6):899–942, 2004.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de