

Improved hardness results for unique shortest vector problem

Divesh Aggarwal and Chandan Dubey

Institute for Theoretical Computer Science

ETH Zurich

divesha@inf.ethz.ch

chandan.dubey@inf.ethz.ch

Abstract. We give several improvements on the known hardness of the unique shortest vector problem.

- We give a deterministic reduction from the shortest vector problem to the unique shortest vector problem. As a byproduct, we get deterministic NP-hardness for unique shortest vector problem in the ℓ_∞ norm.
- We give a randomized reduction from SAT to $\text{uSVP}_{1+1/\text{poly}(n)}$. This shows that $\text{uSVP}_{1+1/\text{poly}(n)}$ is NP-hard under randomized reductions.
- We show that if $\text{GapSVP}_\gamma \in \text{co-NP}$ (or co-AM) then $\text{uSVP}_{\sqrt{\gamma}} \in \text{co-NP}$ (co-AM respectively). This simplifies previously known $\text{uSVP}_{n^{1/4}} \in \text{co-AM}$ proof by Cai [10] to $\text{uSVP}_{(n/\log n)^{1/4}} \in \text{co-AM}$, and additionally generalizes it to $\text{uSVP}_{n^{1/4}} \in \text{co-NP}$.
- We give a deterministic reduction from search- uSVP_γ to the decision- $\text{uSVP}_{\gamma/2}$. We also show that the decision- uSVP is NP-hard for randomized reductions, which does not follow from Kumar-Sivakumar [21].

1 Introduction

A *lattice* is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$ in \mathbb{R}^m . These vectors are referred to as a *basis* of the lattice and n is the *rank* of the lattice. The *successive minima* $\lambda_i(\mathbb{L})$ (where $i = 1, \dots, n$) for the lattice \mathbb{L} are among the most fundamental parameters associated to a lattice. The $\lambda_i(\mathbb{L})$ is defined as the smallest value such that a sphere of radius $\lambda_i(\mathbb{L})$ centered around the origin contains at least i linearly independent lattice vectors. Lattices have been investigated by computer scientists for a few decades after the discovery of the LLL algorithm [22]. More recently, Ajtai [2] showed that lattice problems have a very desirable property for cryptography i.e., they exhibit a worst-case to average-case reduction. This property immediately 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.

We now describe some of the most fundamental and widely studied lattice problems. Given a lattice \mathbb{L} , the γ -approximate shortest vector problem (SVP_γ) is the problem of finding a non-zero lattice vector of length at most $\gamma\lambda_1(\mathbb{L})$. Let the minimum distance of a point $\mathbf{t} \in \mathbb{R}^m$ from a vector of the lattice \mathbb{L} be denoted by $\mathbf{d}(\mathbf{t}, \mathbb{L})$. Given a lattice \mathbb{L} and a point $\mathbf{t} \in \mathbb{R}^m$, the γ -approximate closest vector problem or CVP_γ , is the problem of finding a $\mathbf{v} \in \mathbb{L}$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \gamma\mathbf{d}(\mathbf{t}, \mathbb{L})$.

Besides the search version just described, CVP and SVP also have a decision version. The problem GapCVP_γ is the problem of deciding if, given $(\mathbf{B}, \mathbf{t}, d \in \mathbb{R})$, $\mathbf{d}(\mathbf{t}, \mathbb{L}(\mathbf{B})) \leq d$ or $\mathbf{d}(\mathbf{t}, \mathbb{L}(\mathbf{B})) > \gamma d$. Similarly, the problem GapSVP_γ is the problem of deciding if, given $(\mathbf{B}, d \in \mathbb{R})$, $\lambda_1(\mathbb{L}(\mathbf{B})) \leq d$ or $\lambda_1(\mathbb{L}(\mathbf{B})) > \gamma d$.

The two problems CVP and SVP are quite well studied. We know that they can be solved exactly in deterministic $2^{O(n)}$ time [27,5]. They can be approximated within a factor of $2^{n(\log \log n)^2 / \log n}$, in polynomial time, using LLL [22] and subsequent improvements by Schnorr [30] (for details, see the book by Micciancio and Goldwasser [16]). On the other hand, it is known that there exists $c > 0$, such that no polynomial time algorithm can approximate these problems within a factor of $n^{c/\log \log n}$, unless $\mathbf{P} = \mathbf{NP}$ or another unlikely scenario is true [12,17,8]. It is also known that both these problems cannot be NP-hard for a factor of $\sqrt{n/\log n}$ or the polynomial hierarchy will collapse.

A variant of SVP that has been especially relevant in cryptography is the unique shortest vector problem (uSVP). The problem uSVP_γ is the problem of finding the shortest non-zero vector of the lattice, given the promise that $\lambda_2(\mathbb{L}) \geq \gamma\lambda_1(\mathbb{L})$. The security of the first public key cryptosystem by Ajtai-Dwork [1] was based on the worst-case hardness of $\text{uSVP}_{O(n^8)}$. In a series of papers [14,29], the uniqueness factor was reduced to $O(n^{1.5})$.

In contrast to CVP and SVP , much less is known about the hardness of uSVP . The current NP-hardness result known for uSVP_γ is for $\gamma < 1 + 2^{-n^c}$, which is shown by a randomized reduction from SVP [21]. In [23], it was shown that there is a reduction from uSVP_γ to GapSVP_γ and also a reduction from GapSVP_γ to $\text{uSVP}_{\frac{\gamma}{2\sqrt{n/\log n}}}$. From the first reduction, we can conclude that $\text{uSVP}_\gamma \in \text{co-NP}$ if $\text{GapSVP}_\gamma \in \text{co-NP}$ which, using the result of [6] implies that $\text{uSVP}_{\sqrt{n}} \in \text{co-NP}$. It is already known from Cai [10] that $\text{uSVP}_{n^{1/4}} \in \text{co-AM}$. A discussion of the proofs and the simplification can be found in Section 5.

Contributions of this paper. In Section 3.1, we give a deterministic polynomial time reduction from SVP to uSVP achieving similar bounds as [21] for the ℓ_2 norm. This implies, unlike [21], that deterministic NP-hardness of SVP implies deterministic NP-hardness of uSVP . Also, this result shows that the decision problem duSVP is also NP-hard under randomized reductions. In Section 3.2, we show that a similar idea gets us NP-hardness proof for uSVP in ℓ_∞ norm. In Section 4, we show that $\text{uSVP}_{1+1/\text{poly}(n)}$ is hard by giving a randomized reduction of the SVP instance created by Khot [20] to $\text{uSVP}_{1+1/\text{poly}(n)}$. In Section 5, we show $\text{uSVP}_{c(n)^{1/4}} \in \text{co-NP}$ for some $c > 0$, which implies that uSVP_γ cannot be NP-hard for $\gamma \geq cn^{1/4}$ unless $\mathbf{NP} = \text{co-NP}$. In Section 6, we give a search to decision reduction for the unique shortest vector problem, i.e., a reduction from uSVP_γ to $\text{duSVP}_{\gamma/2}$. The definition of duSVP is implicit in Cai [10]. A comparison of some of our results with previously known results has been depicted in Figures 1 and 2.

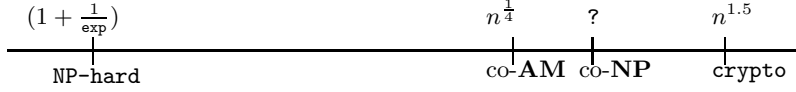


Fig. 1. Before this paper

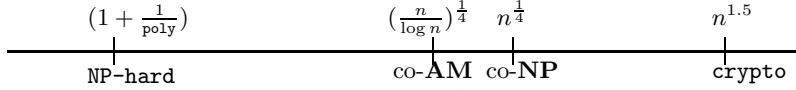


Fig. 2. After this paper

2 Preliminaries

2.1 Notation

A lattice basis is a set of linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$. It is sometimes convenient to think of the basis as an $m \times n$ matrix \mathbf{B} , whose n columns are the vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$. The lattice generated by the basis \mathbf{B} will be written as $\mathbb{L}(\mathbf{B})$ and is defined as $\mathbb{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$. A vector $\mathbf{v} \in \mathbb{L}$ is called a primitive vector of the lattice \mathbb{L} if it is not an integer multiple of another lattice vector except $\pm\mathbf{v}$. We will assume that the lattice is over rationals, i.e., $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{Q}^m$, and the entries are represented by the pair of numerator and denominator.

A *shortest vector* of a lattice is a non-zero vector in the lattice whose ℓ_2 norm is minimal. The length of the shortest vector is $\lambda_1(\mathbb{L}(\mathbf{B}))$, where λ_1 is as defined in the introduction. For a vector $\mathbf{t} \in \mathbb{R}^m$, let $d(\mathbf{t}, \mathbb{L}(\mathbf{B}))$ denote the distance of \mathbf{t} to the closest lattice point in $\mathbb{L}(\mathbf{B})$.

For any lattice \mathbb{L} , and any vector $\mathbf{v} \in \mathbb{L}$, we denote by $\mathbb{L}_{\perp\mathbf{v}}$ the lattice obtained by projecting \mathbb{L} to the space orthogonal to \mathbf{v} .

For an integer $k \in \mathbb{Z}^+$ we use $[k]$ to denote the set $\{1, \dots, k\}$.

2.2 Lattice Problems

In this paper we are concerned with the shortest vector problem and the unique shortest vector problem. The search and decision versions of the shortest vector problem are defined below.

GapSVP $_\gamma$: Given a lattice basis \mathbf{B} and an integer d , say “YES” if $\lambda_1(\mathbb{L}(\mathbf{B})) \leq d$ and “NO” if $\lambda_1(\mathbb{L}(\mathbf{B})) > \gamma d$.

SVP $_\gamma$: Given a lattice basis \mathbf{B} , find a non-zero vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v}\| \leq \gamma \lambda_1(\mathbb{L}(\mathbf{B}))$.

We now formally define the search and decision unique shortest vector problem. The definition of the decision version of **uSVP** is implicit in Cai [10], although, to our knowledge, it has not been explicitly defined anywhere in the literature.

uSVP $_\gamma$: Given a lattice basis \mathbf{B} such that $\lambda_2(\mathbb{L}(\mathbf{B})) \geq \gamma \lambda_1(\mathbb{L}(\mathbf{B}))$, find a vector $\mathbf{v} \in \mathbb{L}(\mathbf{B})$ such that $\|\mathbf{v}\| = \lambda_1(\mathbb{L}(\mathbf{B}))$.

duSVP $_\gamma$: Given a lattice basis \mathbf{B} and an integer d , such that $\lambda_2(\mathbb{L}(\mathbf{B})) \geq \gamma \lambda_1(\mathbb{L}(\mathbf{B}))$, say “YES” if $\lambda_1(\mathbb{L}(\mathbf{B})) \leq d$ and “NO” if $\lambda_1(\mathbb{L}(\mathbf{B})) > d$.

2.3 Defining co-AM and co-NP

The definitions of this section have been adapted from [13].

Definition 1. A promise problem $\Pi = (\Pi_{\text{YES}}, \Pi_{\text{NO}})$ is said to be in **co-NP** if there exists a polynomial-time recognizable (witness) verification predicate V such that

- For every $x \in \Pi_{\text{NO}}$, there exists $w \in \{0, 1\}^*$ such that $V(x, w) = 1$.
- For every $x \in \Pi_{\text{YES}}$ and every $w \in \{0, 1\}^*$, $V(x, w) = 0$.

Definition 2. A promise problem $\Pi = (\Pi_{\text{YES}}, \Pi_{\text{NO}})$ is said to be in **co-AM** if there exists a polynomial-time recognizable verification predicate V and polynomials p, q such that for every $x \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$ with $|x| = n$, and y chosen uniformly at random from $\{0, 1\}^{p(n)}$,

- If $x \in \Pi_{\text{NO}}$, then there exists $w \in \{0, 1\}^{q(n)}$, such that $\Pr(V(x, y, w) = 1) \geq \frac{2}{3}$.
- If $x \in \Pi_{\text{YES}}$, then for all $w \in \{0, 1\}^{q(n)}$, $\Pr(V(x, y, w) = 1) \leq \frac{1}{3}$.

3 A deterministic polynomial time reduction from SVP to uSVP

Let us suppose that $\mathbf{B} = [\mathbf{b}_1 \ \mathbf{b}_2 \ \dots \ \mathbf{b}_n]$ is the input lattice. The Gram Schmidt orthogonalization of \mathbf{B} , denoted as $\{\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_n\}$, is defined as

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{\mathbf{b}}_j, \text{ where } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \tilde{\mathbf{b}}_j \rangle}{\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle}.$$

Definition 3. A basis $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ is a δ -LLL reduced basis [22] if the following holds:

- $\forall 1 \leq j < i \leq n, |\mu_{i,j}| \leq \frac{1}{2}$,
- $\forall 1 \leq i < n, \delta \|\tilde{\mathbf{b}}_i\|^2 \leq \|\mu_{i+1,i} \tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$.

We choose $\delta = \frac{3}{4}$ and then, from the above definition, for a δ -LLL reduced basis, $\forall 1 \leq i < n, \|\tilde{\mathbf{b}}_i\| \leq \sqrt{2} \|\tilde{\mathbf{b}}_{i+1}\|$. This implies that

$$\|\tilde{\mathbf{b}}_1\| \leq 2^{(i-1)/2} \|\tilde{\mathbf{b}}_i\|.$$

Since there is an efficient algorithm [22] to compute an LLL-reduced basis, we assume, unless otherwise stated, that the given basis is always LLL-reduced and hence satisfies the above mentioned properties.

Lemma 1. For an LLL reduced basis \mathbf{B} , if $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$ is a shortest vector, then $|\alpha_i| < 2^{3n/2}$ for all $i \in [n]$.

Proof. We show by induction that for $0 \leq i \leq n-1, |\alpha_{n-i}| \leq 2^{n/2+i}$. Since \mathbf{u} is the shortest vector of $\mathcal{L}(\mathbf{B})$, $\|\mathbf{u}\| \leq \|\mathbf{b}_1\|$. Also, since the projection of \mathbf{u} in the direction of $\tilde{\mathbf{b}}_n$ is $\alpha_n \tilde{\mathbf{b}}_n$,

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

This implies that $|\alpha_n| \leq 2^{(n-1)/2}$.

Now assume that $|\alpha_{n-i}| \leq 2^{n/2+i}$ for $0 \leq i < k$. Then, using the fact that $\|\mathbf{u}\| \leq \|\mathbf{b}_1\|$ and that the projection of \mathbf{u} in the direction of $\tilde{\mathbf{b}}_{n-k}$ is $\left(\alpha_{n-k} + \left(\sum_{j=n-k+1}^n \mu_{j,n-k} \alpha_j \right) \right) \tilde{\mathbf{b}}_{n-k}$, we get that

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

Therefore,

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

□

3.1 Deterministic reduction from SVP to uSVP

Given an instance of $\text{SVP}(\mathbf{B}, d)$, we define a new lattice $\mathbb{L}(\mathbf{B}')$ as follows.

$$\begin{pmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \dots & \mathbf{b}_n \\ \frac{1}{2^{2n^2}} & 0 & \dots & 0 \\ 0 & \frac{2^{2n}}{2^{2n^2}} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \frac{2^{2n^2-2n}}{2^{2n^2}} \end{pmatrix}$$

So, $(\mathbf{b}'_i)^T = [\mathbf{b}_i^T \ 0 \ \dots \ 0 \ \dots \ 0 \ \frac{2^{2(i-1)n}}{2^{2n^2}} \ 0 \ \dots \ 0]$, where the $(m+i)$ 'th entry is non-zero. For a vector $\mathbf{v} = \sum_i^n \alpha_i \mathbf{b}_i \in \mathbb{L}(\mathbf{B})$, we call $\mathbf{v}' = \sum_i^n \alpha_i \mathbf{b}'_i$ as the corresponding vector.

Lemma 2. *For the new basis \mathbf{B}' , $\lambda_1^2(\mathbb{L}(\mathbf{B})) \leq \lambda_1^2(\mathbb{L}(\mathbf{B}')) \leq \lambda_1^2(\mathbb{L}(\mathbf{B})) + 2^{-n/2}$.*

Proof. The first inequality follows from the fact that the length of the vectors can't get shorter in $\mathbb{L}(\mathbf{B}')$. For the second inequality, let \mathbf{v} be a shortest vector in $\mathbb{L} = \mathbb{L}(\mathbf{B})$ such that $\mathbf{v} = \sum_i^n \alpha_i \mathbf{b}_i$. Then from Lemma 1, $|\alpha_i| < 2^{3n/2}$, and hence

$$\begin{aligned}
\left\| \sum_{i=1}^n \alpha_i \mathbf{b}'_i \right\|^2 &< \lambda_1^2(\mathbb{L}) + \sum_{i=0}^{n-1} \alpha_{i+1}^2 \frac{2^{4in}}{2^{4n^2}} \\
&< \lambda_1^2(\mathbb{L}) + 2^{3n} \frac{2^{4n^2} - 1}{(2^{4n} - 1)2^{4n^2}} \\
&< \lambda_1^2(\mathbb{L}) + 2^{-n/2} .
\end{aligned}$$

□

Lemma 3. *Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{L}(\mathbf{B})$ be two distinct vectors such that $\|\mathbf{v}_1\| = \|\mathbf{v}_2\| = \lambda_1(\mathbb{L}(\mathbf{B}))$ and let $\mathbf{v}'_1, \mathbf{v}'_2 \in \mathbb{L}(\mathbf{B}')$ be the corresponding vectors. Then, $|\|\mathbf{v}'_1\|^2 - \|\mathbf{v}'_2\|^2| > 2^{-4n^2}$*

Proof. Let $\mathbf{v}_1 = \sum_{i=1}^n \alpha_i \mathbf{b}_i$ and $\mathbf{v}_2 = \sum_{i=1}^n \beta_i \mathbf{b}_i$. Let $j \in [n]$ be the largest number such that $\alpha_j \neq \beta_j$. Then,

$$\begin{aligned}
\|\mathbf{v}'_1\|^2 - \|\mathbf{v}'_2\|^2 &= \left| \sum_{i=1}^n (\alpha_i^2 - \beta_i^2) \left(\frac{2^{2(i-1)n}}{2^{2n^2}} \right)^2 \right| \\
&> |(\alpha_j^2 - \beta_j^2) \cdot \frac{2^{4(j-1)n}}{2^{4n^2}} + \sum_{i=1}^{j-1} (\alpha_i^2 - \beta_i^2) \cdot \frac{2^{4(i-1)n}}{2^{4n^2}}| \\
&> \frac{2^{4(j-1)n}}{2^{4n^2}} - 2^{3n} \sum_{i=1}^{j-1} \frac{2^{4(i-1)n}}{2^{4n^2}} \\
&= \frac{2^{4(j-1)n}}{2^{4n^2}} - 2^{3n} \frac{2^{4(j-1)n} - 1}{2^{4n^2}(2^{4n} - 1)} \\
&> \frac{1}{2^{4n^2}}.
\end{aligned}$$

□

Lemma 4. *Let $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2$ be vectors in an integer lattice $\mathbb{L} = \mathbb{L}(\mathbf{B})$.*

- If $\|\mathbf{v}_1\| > \|\mathbf{v}_2\|$, then $\|\mathbf{v}_1\|^2 - \|\mathbf{v}_2\|^2 \geq 1$.
- If $\|\mathbf{v}\| > \lambda_1(\mathbb{L})$, then if $\mathbf{v}' \in \mathbb{L}(\mathbf{B}')$ is the corresponding vector, then $\|\mathbf{v}'\|^2 > \lambda_1^2(\mathbf{B}) + 1$.

Proof. The first item follows from the fact that for integer lattices the ℓ_2^2 norm of a vector is also an integer. The second item follows from the fact that \mathbf{v} is not the shortest vector in $\mathbb{L}(\mathbf{B})$ and $\|\mathbf{v}'\|^2 > \|\mathbf{v}\|^2$. □

Without loss of generality, we can assume $\mathbb{L}(\mathbf{B})$ to be an integer lattice, and hence, using the above lemma, we get the following result.

Theorem 1. *Given a lattice $\mathbb{L} = \mathbb{L}(\mathbf{B})$, there is a deterministic polynomial reduction transforming it to another lattice $\mathbb{L}' = \mathbb{L}(\mathbf{B}')$ such that $\frac{\lambda_2(\mathbb{L}')}{\lambda_1(\mathbb{L}')} > \sqrt{1 + \frac{1}{c \cdot 2^{4n^2} \lambda_1^2(\mathbb{L})}}$ for some $c \leq 1/4$. In particular, **duSVP** is **NP-hard** under randomized reductions.*

Proof. From Lemma 3 and Lemma 4, we have that $\lambda_2^2(\mathbb{L}') - \lambda_1^2(\mathbb{L}') > 2^{-4n^2}$, which implies $\frac{\lambda_2(\mathbb{L}')}{\lambda_1(\mathbb{L}')} > \sqrt{1 + \frac{1}{2^{4n^2} \lambda_1^2(\mathbb{L}')}}$. From Lemma 2, $\lambda_1^2(\mathbb{L}') < \lambda_1^2(\mathbb{L}) + \frac{1}{2^{n/2}}$, and hence $\frac{\lambda_2(\mathbb{L}')}{\lambda_1(\mathbb{L}')}$ is at least $1 + \frac{c}{2^{4n^2} \lambda_1^2(\mathbb{L})}$, for some constant $c \leq \frac{1}{4}$. □

We would like to point out that we assumed in Lemma 4 that the lattice \mathbb{L} is an integer lattice. Hence, $\lambda_1(\mathbb{L})$ can be $O(2^{cn} \cdot \text{input size})$ and hence, $\frac{\lambda_2(\mathbb{L}')}{\lambda_1(\mathbb{L}')}$ can be arbitrarily close to 1. The original Kumar-Sivakumar [21] proof also suffers with the same problem. The idea there is to show that the number of lattice points in a ball centered at the origin and of radius $\sqrt{2}\lambda_1(\mathbb{L})$ is at most 2^n . Then one can create a new lattice \mathbb{L}' with a unique short vector \mathbf{v} with $\lambda_1(\mathbb{L}) \leq \|\mathbf{v}\| < \sqrt{2}\lambda_1(\mathbb{L})$. In the worst case, the ratio of $\lambda_2^2(\mathbb{L}')$ and $\lambda_1^2(\mathbb{L}')$ for the new lattice (assuming that the original lattice was integer lattice) can be as small as $\frac{2\lambda_1^2(\mathbb{L})}{2\lambda_1^2(\mathbb{L}) - 1}$, which is $(1 + \frac{1}{2\lambda_1^2(\mathbb{L})})$. As $\lambda_1(\mathbb{L})$ is $O(2^{cn} \cdot \text{input size})$, we get $(1 + 1/exp)$ hardness of **uSVP** in both cases.

3.2 Deterministic hardness of **uSVP** in ℓ_∞ norm

In this section, we show that the **uSVP** problem is **NP-hard** in the ℓ_∞ norm. For simplicity of description, we assume that all norms in this section are ℓ_∞ norms. Also, as before, the lattice \mathbb{L} is an integer lattice.

For the LLL reduced basis $\{\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_n\}$, there is a constant c such that $\|\tilde{\mathbf{b}}_1\| \leq 2^{c(i-1)} \|\tilde{\mathbf{b}}_i\|$, for all $i \in [n]$. An induction proof as in Lemma 1 gives the following corollary.

Corollary 1. *If the basis \mathbf{B} is LLL reduced then for the shortest vector $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$, one has that for all i , $|\alpha_i| < 2^{(c+1)n}$, for some constant c .*

We use the following theorem by P. van Emde Boas [7].

Theorem 2. *The problem SVP in ℓ_∞ norm is NP-hard.*

Now we prove the main result of this section.

Theorem 3. *The problem uSVP in ℓ_∞ norm is NP-hard.*

Proof. We take the instance resulting from Theorem 2 and make the shortest vector unique. Let $\eta = (c+1)n$, then for all $i \in [n]$, $|\alpha_i| < 2^\eta$. Given the basis $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$, we perturb the basis slightly in the following way. The basis vector \mathbf{b}_i gets $\frac{2^{2(i-1)\eta}}{2^{2\eta^2}}$ added to each of its entries. For the new lattice \mathbb{L}' , we have the following easy to prove observations. The theorem follows from them.

– If $\mathbf{v} = \sum_i \alpha_i \mathbf{b}_i \in \mathbb{L}$ is a shortest vector then the vector $\mathbf{v}' = \sum_i \alpha_i \mathbf{b}'_i \in \mathbb{L}'$. Also,

$$\lambda_1(\mathbb{L}') \leq \|\mathbf{v}'\| \leq \lambda_1(\mathbb{L}) + \sum_{i=1}^n \alpha_i \frac{2^{2(i-1)\eta}}{2^{2\eta^2}} = \lambda_1(\mathbb{L}) + 2^{1-\eta}.$$

- Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{L}$ and $\|\mathbf{v}_1\| > \|\mathbf{v}_2\|$, then $\|\mathbf{v}_1\| - \|\mathbf{v}_2\| \geq 1$, as \mathbb{L} is an integer lattice.
- Let $\mathbf{v} = \sum_{i \in [n]} \alpha_i \mathbf{b}_i \in \mathbb{L}$ and let $\mathbf{b}_{i,j}$ be the j 'th entry of \mathbf{b}_i . If \mathbf{v}' is the vector corresponding to \mathbf{v} in \mathbb{L}' and $\|\mathbf{v}'\| = |\sum_{i \in [n]} \alpha_i \mathbf{b}'_{i,j}|$, for some $j \in [m]$, then $\|\mathbf{v}\| = |\sum_{i \in [n]} \alpha_i \mathbf{b}_{i,j}|$ for the same j . This follows from the fact that the $\sum_{i \in [n]} \alpha_i \mathbf{b}_{i,j}$ for all j is an integer, and hence will either be equal to $\|\mathbf{v}\|$ or will be at most $\|\mathbf{v}\| - 1$.
- Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{L}$ such that $\|\mathbf{v}_1\| = \|\mathbf{v}_2\| = \lambda_1(\mathbb{L})$ then $|\|\mathbf{v}'_1\| - \|\mathbf{v}'_2\|| > |\sum_i (\alpha_i - \beta_i) \frac{2^{2(i-1)\eta}}{2^{2\eta^2}}|$. Similarly, as in Lemma 3, we get that $|\|\mathbf{v}'_1\| - \|\mathbf{v}'_2\|| > 2^{-2\eta^2}$.

□

4 Hardness of uSVP within $1 + 1/n^c$

The following is a result obtained by letting $\eta = \frac{1}{40}$, $p = 2$, and $k = 1$ in Theorem 3.1 and Theorem 5.1 of [20].

Lemma 5. *For some fixed constants c_1, c_2 , there exists a polynomial time reduction from a SAT instance of size n to an SVP instance (\mathbf{B}, d) where \mathbf{B} is a $2N \times N$ integer matrix with $N \leq n^{c_2}$, and $d \leq n^{c_1}$ such that:*

1. *If the SAT instance is a YES instance, then with probability at least 9/10, there exists a non-zero $\mathbf{x} \in \mathbb{Z}^N$, such that $\|\mathbf{x}\| \leq d^3$ and $\|\mathbf{B}\mathbf{x}\| \leq \sqrt{\frac{7}{8}}d$.*
2. *If the SAT instance is a NO instance, then with probability at least 9/10, for any non-zero $\mathbf{x} \in \mathbb{Z}^N$, $\|\mathbf{B}\mathbf{x}\| \geq \sqrt{d}$.*

We state below lemma 4 from [21].

Lemma 6. *Let $T \neq \emptyset$ be a finite set of size at most 2^m , and let $T = T_0 \supseteq T_1 \supseteq \dots \supseteq T_{2m}$ be a sequence of subsets of T defined by a probabilistic process that satisfies the following three properties:*

1. *For all k , $0 \leq k < 2m$, and all $x \in T$, $\Pr(x \in T_{k+1} | x \in T_k) = \frac{1}{2}$.*
2. *For all $x \in T$, $0 \leq k < \ell < 2m$, $\Pr(x \in T_{\ell+1} | x \in T_\ell, x \in T_k) = \Pr(x \in T_{\ell+1} | x \in T_\ell)$.*
3. *For all k , $0 \leq k < 2m$, and all $x, y \in T_k$, $x \neq y$, the events “ $x \in T_{k+1}$ ” and “ $y \in T_{k+1}$ ” are independent.*

Then, with probability $\frac{2}{3} - 2^{-m}$, one of the T_k 's has exactly one element.

The following result is a simpler version of Corollary 3 from [21].

Lemma 7. *Given any arbitrary lattice \mathbb{L} of rank n , the number of lattice points in \mathbb{L} of length $\lambda_1(\mathbb{L})$ is at most 2^{n+1} .*

Proof. Let $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ be the basis of \mathbb{L} . We claim that for any two vectors $\mathbf{u} \neq \pm\mathbf{v} \in \mathbb{L}$ of length $\lambda_1(\mathbb{L})$, where $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i$ and $\mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i$, there exists an i such that $\alpha_i \not\equiv \beta_i \pmod{2}$. Note that this claim implies the desired result.

Assume, on the contrary, that there exist a $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{b}_i$ and $\mathbf{v} = \sum_{i=1}^n \beta_i \mathbf{b}_i$ such that $\|\mathbf{u}\| = \|\mathbf{v}\| = \lambda_1(\mathbb{L})$ and $\alpha_i \equiv \beta_i \pmod{2}$ for all i . This implies that $\frac{\mathbf{u}+\mathbf{v}}{2} \in \mathbb{L}$ and $\frac{\mathbf{u}-\mathbf{v}}{2} \in \mathbb{L}$. Also,

$$\begin{aligned} \left\| \frac{\mathbf{u} + \mathbf{v}}{2} \right\|^2 + \left\| \frac{\mathbf{u} - \mathbf{v}}{2} \right\|^2 &= \frac{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 + 2\langle \mathbf{u}, \mathbf{v} \rangle}{4} + \frac{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\langle \mathbf{u}, \mathbf{v} \rangle}{4} \\ &= \frac{\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2}{2} = (\lambda_1(\mathbb{L}))^2. \end{aligned}$$

Since, $\mathbf{u} \neq \pm\mathbf{v}$, this implies that $0 < \|\frac{\mathbf{u}+\mathbf{v}}{2}\| < \lambda_1(\mathbb{L})$ and $0 < \|\frac{\mathbf{u}-\mathbf{v}}{2}\| < \lambda_1(\mathbb{L})$, which is a contradiction. \square

We now prove the main result of this section.

Theorem 4. *For some fixed constants c_1, c_2, c , there exists a polynomial time reduction from a SAT instance of size n to a sequence of lattice basis \mathbf{B}_i , $1 \leq i \leq 2N + 2$, and d , where \mathbf{B}_i 's are $2N \times N$ integer matrices with $N \leq n^{c_2}$, and $d \leq n^{c_1}$ such that:*

1. *If the SAT instance is a YES instance, then with probability at least $1/2$, there exists an i such that $\mathbb{L}(\mathbf{B}_i)$ has a $1 + \frac{1}{N^c}$ -unique shortest vector of length at most $\sqrt{\frac{7}{8}d}$.*
2. *If the SAT instance is a NO instance, then with probability at least $9/10$, for all i , the shortest vector of $\mathbb{L}(\mathbf{B}_i)$ is of length at least \sqrt{d} .*

Proof. Given a SAT instance, consider the pair (\mathbf{B}, d) using the reduction from Lemma 5.

We generate, as in [21], a sequence of lattices $\mathbb{L}(\mathbf{B}_0), \mathbb{L}(\mathbf{B}_1), \dots, \mathbb{L}(\mathbf{B}_{2N+2})$ inductively as follows. Suppose we have generated $\mathbb{L}(\mathbf{B}) = \mathbb{L}(\mathbf{B}_0), \mathbb{L}(\mathbf{B}_1), \dots, \mathbb{L}(\mathbf{B}_k)$ for some $0 \leq k < 2N + 2$. We now show how to generate \mathbf{B}_{k+1} . Let $\mathbf{B}_k = (\mathbf{b}_1, \dots, \mathbf{b}_N)$. Pick a subset $W \subseteq [N]$ uniformly at random from all subsets of $[N]$. If W is empty, then let $\mathbf{B}_{k+1} = \mathbf{B}_k$. Otherwise, pick any i from W . For $j \notin W$, let $\mathbf{b}'_j = \mathbf{b}_j$, and for $j \in W \setminus \{i\}$, let $\mathbf{b}'_j = \mathbf{b}_j - \mathbf{b}_i$. Finally, let $\mathbf{b}'_i = 2\mathbf{b}_i$ and $\mathbf{B}_{k+1} = (\mathbf{b}'_1, \mathbf{b}'_2, \dots, \mathbf{b}'_N)$.

Note that each of the \mathbf{B}_i 's are $2N \times N$ integer matrices. Also, since $\mathbb{L}(\mathbf{B}_i) \subseteq \mathbb{L}(\mathbf{B})$ for all $0 \leq i \leq 2N + 2$, therefore, if the SAT instance is a NO instance, then, by Lemma 5, with probability $9/10$, the shortest vector of $\mathbb{L}(\mathbf{B}_i)$ is of length at least \sqrt{d} for all i .

Now, consider the case when the SAT instance is a YES instance. In this case, by Lemma 5, with probability $9/10$, we have $1 \leq \lambda_1(\mathbb{L}(\mathbf{B})) \leq \sqrt{\frac{7}{8}d}$, since, \mathbf{B} is an integer matrix. The set T is a subset of $\mathbb{L}(\mathbf{B})$ defined as follows:

$$T = \{\mathbf{v} \in \mathbb{L}(\mathbf{B}) \mid \|\mathbf{v}\| = \lambda_1(\mathbb{L}(\mathbf{B}))\}.$$

Furthermore, we define the sets T_i for $1 \leq i \leq 2N + 2$ as $T_i = T \cap \mathbb{L}(\mathbf{B}_i)$. By Lemma 7, $|T| \leq 2^{N+1}$. The sets T_i , for $1 \leq i \leq 2N + 2$ satisfy the conditions of Lemma 6 for $m = N + 1$. Thus, by Lemma 6, with probability $\frac{2}{3} - 2^{-N-1}$, there exists a $0 \leq k \leq 2N + 2$ such that $|T_k| = 1$. Note that \mathbf{B}_i is an integer matrix for all i . Thus, since $|T \cap \mathbb{L}(\mathbf{B}_k)| = 1$, we see that

$$\lambda_2(\mathbb{L}(\mathbf{B}_k)) \geq \lambda_1(\mathbb{L}(\mathbf{B}_k)) + 1 \geq \lambda_1(\mathbb{L}(\mathbf{B}_k))(1 + \sqrt{\frac{8}{7d}}).$$

Thus, there exists a constant c (which can be computed in terms of c_1 and c_2) such that with probability $\frac{9}{10} \cdot (\frac{2}{3} - 2^{-N-1}) > \frac{1}{2}$, there exists a k such that $\mathbb{L}(\mathbf{B}_k)$ has a $(1 + \frac{1}{N^c})$ -unique shortest vector of length at most $\sqrt{\frac{7}{8}d}$. This concludes the proof. \square

5 From GapSVP \in co-NP (co-AM) to duSVP \in co-NP (co-AM)

We now simplify and generalize the $\text{uSVP}_{n^{1/4}} \in \text{co-AM}$ proof by Cai [10]. We first give a simplified description of Cai's proof that uses the idea of the co-AM proof of [13]. Here, one needs to give a co-AM proof that given a lattice \mathbb{L} with $n^{1/4}$ -unique shortest vector and an integer d , $\lambda_1(\mathbb{L}) > d$. The protocol is as follows. The verifier generates uniform random points $\mathbf{p}_i \in \mathbb{L}$ for $i \in \{0, 1, \dots, \log_2(\min_i \|\mathbf{b}_i\|)\}$. For each i the verifier generates a random point $\mathbf{z}_i \in B(\mathbf{p}_i, 2^{i-1}t\sqrt{\sqrt{n} - \frac{1}{4}})$. The verifier then sends these points to the prover. The prover then provides the claimed shortest vector \mathbf{v} (primitive vector) and for the correct range when $2^i t < \|\mathbf{v}\| \leq 2^{i+1}t$, the correct point $\mathbf{p}_i \pmod{\mathbf{v}}$ which is in \mathbb{L} . If $\lambda_1(\mathbb{L}) > d$ then the prover can send the correct shortest vector \mathbf{v} and for the corresponding i the balls corresponding to different choices of $\mathbf{p} \in \mathbb{L}$ are disjoint or identical depending on whether the respective centers are congruent modulo the shortest vector \mathbf{v} . So, the prover has no trouble in providing the proof when $\lambda_1(\mathbb{L}) > d$. If on the other hand $\lambda_1(\mathbb{L}) \leq d$ and $\|\mathbf{v}\| > d$, it must be a multiple of the shortest vector or much longer than $\lambda_1(\mathbb{L})$. In this case, the balls have lot of overlap and the prover will be caught with high probability.

We show that the above idea can be generalized for any co-NP or co-AM proof, i.e., we show that for any factor γ , if $\text{GapSVP}_\gamma \in \text{co-NP}$ then $\text{duSVP}_{c\sqrt{\gamma}}$ is in co-NP (and similarly for co-AM). This implies, using the result of Aharonov and Regev [6] that $\text{GapSVP}_{\sqrt{n}} \in \text{co-NP}$, that $\text{duSVP}_{\frac{cn}{4}} \in \text{co-NP}$, and any subsequent improvements in the factor for GapSVP will imply an improvement for duSVP.

Lemma 8. *Let \mathbb{L} be a lattice such that $\lambda_2(\mathbb{L}) \geq \gamma\lambda_1(\mathbb{L})$, and let \mathbf{v} be a primitive vector in \mathbb{L} . Then:*

- If $\|\mathbf{v}\| \neq \lambda_1(\mathbb{L})$, then $\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) \leq \frac{\|\mathbf{v}\|}{\gamma}$.
- If $\|\mathbf{v}\| = \lambda_1(\mathbb{L})$, then $\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) \geq \left(\sqrt{\gamma^2 - \frac{1}{4}}\right) \|\mathbf{v}\|$.

Proof. If $\|\mathbf{v}\| \neq \lambda_1(\mathbb{L})$ and \mathbf{v} is primitive, then $\|\mathbf{v}\| \geq \lambda_2(\mathbb{L}) \geq \gamma\lambda_1(\mathbb{L})$. Let \mathbf{u} be the shortest vector in \mathbb{L} . Then the projection of \mathbf{u} in the space orthogonal to \mathbf{v} (say $\mathbf{u}' \in \mathbb{L}_{\perp\mathbf{v}}$) is of length at most $\|\mathbf{u}\| = \lambda_1(\mathbb{L})$. Also, \mathbf{u} is not parallel to \mathbf{v} , and hence, $\mathbf{u}' \neq \mathbf{0}$. This implies

$$\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) \leq \lambda_1(\mathbb{L}) \leq \frac{\|\mathbf{v}\|}{\gamma}.$$

If $\|\mathbf{v}\| = \lambda_1(\mathbb{L})$, then let \mathbf{u}' be the shortest vector in $\mathbb{L}_{\perp\mathbf{v}}$. Let \mathbf{u} be the projection of $\mathbf{u} \in \mathbb{L}$ orthogonal to \mathbf{v} . Then $\mathbf{u} = \mathbf{u}' + \alpha\mathbf{v}$ for some $\alpha \in \mathbb{R}$. Since $\mathbf{u} - \lfloor\alpha\rfloor\mathbf{v} \in \mathbb{L}$ is not an integer multiple of \mathbf{v} , $\|\mathbf{u} - \lfloor\alpha\rfloor\mathbf{v}\| \geq \lambda_2(\mathbb{L}) \geq \gamma\|\mathbf{v}\|$. Thus,

$$\gamma\|\mathbf{v}\| \leq \|\mathbf{u}' + (\alpha - \lfloor\alpha\rfloor)\mathbf{v}\| \leq \sqrt{\|\mathbf{u}'\|^2 + \frac{1}{4}\|\mathbf{v}\|^2},$$

because \mathbf{u}' is orthogonal to \mathbf{v} . This implies that

$$\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) = \|\mathbf{u}'\| \geq \left(\sqrt{\gamma^2 - \frac{1}{4}}\right) \|\mathbf{v}\|.$$

□

Theorem 5. *If $\text{GapSVP}_{\gamma\sqrt{\gamma^2 - \frac{1}{4}}} \in \text{co-NP}$, then $\text{duSVP}_\gamma \in \text{co-NP}$.*

Proof. Let (\mathbf{B}, d) be an instance of duSVP_γ . Assume a witness for recognizing $\lambda_1(\mathbb{L}(\mathbf{B})) > d$ to be a vector \mathbf{v} and a string w . The verification predicate V on input $(\mathbf{B}, d, \mathbf{v}, w)$ outputs 1 if and only if \mathbf{v} is a primitive vector of $\mathbb{L} = \mathbb{L}(\mathbf{B})$, $\|\mathbf{v}\| > d$, and the verification predicate V' for proving $\text{GapSVP}_{\gamma'} \in \text{co-NP}$, (where $\gamma' = \gamma\sqrt{\gamma^2 - \frac{1}{4}}$) on input $(\mathbf{B}', \frac{\|\mathbf{v}\|}{\gamma}, w)$ outputs 1, where \mathbf{B}' is a basis for $\mathbb{L}_{\perp\mathbf{v}}$.

CASE 1: (\mathbf{B}, d) is a “NO” instance, i.e. $\lambda_1(\mathbb{L}) > d$.

In this case, let \mathbf{v} be the shortest vector in \mathbb{L} , and w is the witness output in the proof of $\text{GapSVP}_{\gamma'} \in \text{co-NP}$ for input $(\mathbf{B}', \frac{\|\mathbf{v}\|}{\gamma})$.

Since $\lambda_1(\mathbb{L}) > d$, \mathbf{v} is a primitive vector of \mathbb{L} with length greater than d . Also, from Lemma 8, $\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) \geq \left(\sqrt{\gamma^2 - \frac{1}{4}}\right) \|\mathbf{v}\| = \gamma' \frac{\|\mathbf{v}\|}{\gamma}$.

Thus, the verification predicate V outputs 1.

CASE 2: (\mathbf{B}, d) is a “YES” instance, i.e. $\lambda_1(\mathbb{L}) \leq d$.

In this case, let us assume that there exists a witness \mathbf{v}, w such that V outputs 1.

Thus, \mathbf{v} is a primitive vector with $\|\mathbf{v}\| > d$. This implies that $\|\mathbf{v}\| \neq \lambda_1(\mathbb{L})$, and using Lemma 8, $\lambda_1(\mathbb{L}_{\perp\mathbf{v}}) \leq \frac{\|\mathbf{v}\|}{\gamma}$. Therefore, V' , and hence V , output 0, which is a contradiction. \square

This result, along with the result of [6] implies the following:

Corollary 2. *There exists $c > 0$ such that $\text{duSVP}_{cn^{1/4}} \in \text{NP} \cap \text{co-NP}$.*

Note that essentially the same idea as in Theorem 5 can be used to show that

Theorem 6. *If $\text{GapSVP}_{\gamma\sqrt{\gamma^2 - \frac{1}{4}}} \in \text{co-AM}$, then $\text{duSVP}_{\gamma} \in \text{co-AM}$.*

Thus, using the result of [13], this implies the following:

Corollary 3. *There exists $c > 0$ such that $\text{duSVP}_{c(\frac{n}{\log n})^{1/4}} \in \text{NP} \cap \text{co-AM}$.*

6 A deterministic reduction from uSVP_{γ} to $\text{duSVP}_{\gamma/2}$

The following lemma is taken from the uSVP to GapSVP reduction given in [23].

Lemma 9. *Let $\mathbb{L} = \mathbb{L}_0$ be a lattice of rank $n \geq 2$ given by its basis vectors, and let \mathbf{u} be the shortest non-zero vector of \mathbb{L} . If there exists an efficient algorithm that computes a basis for \mathbb{L}_{i+1} , a sub-lattice of \mathbb{L}_i such that $\mathbb{L}_{i+1} \neq \mathbb{L}_i$ and $\mathbf{u} \in \mathbb{L}_{i+1}$ for all $i \geq 0$, then there exists an efficient algorithm that computes a basis for a sublattice $\tilde{\mathbb{L}}$ of \mathbb{L} of rank $n - 1$ such that $\mathbf{u} \in \tilde{\mathbb{L}}$.*

Proof. Let \mathbf{B} be the given basis for \mathbb{L} , let \mathbf{S} be a basis for the sublattice \mathbb{L}_t for some $t > n(n + \log_2 n)$, and let \mathbf{D} be the dual basis of \mathbf{S} . Since \mathbb{L}_{i+1} is a sub-lattice of \mathbb{L}_i for all i , we have that $\det(\mathbf{S}) \geq 2^t \det(\mathbf{B})$, which implies $\det(\mathbf{D}) \leq 1 / (2^t \det(\mathbf{B}))$. By Minkowski’s bound [26], we have $\lambda_1(\mathbb{L}(\mathbf{D})) \leq \sqrt{n} \det(\mathbf{D})^{1/n}$, which implies that using the LLL algorithm [22], we can find a vector $\mathbf{v} \in \mathbb{L}(\mathbf{D})$ such that

$$\|\mathbf{v}\| \leq 2^n \lambda_1(\mathbb{L}(\mathbf{B})) \leq \frac{2^n \sqrt{n}}{2^{t/n} \det(\mathbf{B})^{1/n}}.$$

Also, using Minkowski’s bound, we have $\|\mathbf{u}\| \leq \sqrt{n} \det(\mathbf{B})^{1/n}$. This implies that

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\| \|\mathbf{v}\| \leq n \cdot 2^{n-t/n} < 1.$$

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

Lemma 10. *Let $\gamma \geq 2$ and \mathbb{L} be a lattice such that $\lambda_2(\mathbb{L}) \geq \gamma \lambda_1(\mathbb{L})$. Then, given any sublattice \mathbb{L}' of \mathbb{L} containing the shortest non-zero vector \mathbf{u} of \mathbb{L} and an oracle that solves $\text{duSVP}_{\gamma/2}$, there exists an algorithm that computes a sublattice $\mathbb{L}'' (\neq \mathbb{L}')$ of \mathbb{L}' such that $\mathbf{u} \in \mathbb{L}''$.*

Proof. Using the $\text{duSVP}_{\gamma/2}$ oracle, we can estimate $\|\mathbf{u}\|$ within a factor of 2 using binary search. Thus, let d be such that $d/2 < \|\mathbf{u}\| \leq d$.

Let $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$ be a basis for \mathbb{L}' and let $\mathbf{u} = \alpha_1 \mathbf{b}_1 + \dots + \alpha_n \mathbf{b}_n$ be the shortest vector of \mathbb{L} for some $\alpha_i \in \mathbb{Z}$. Note that since \mathbb{L}' is a sub-lattice of \mathbb{L} , $\lambda_2(\mathbb{L}') \geq \lambda_2(\mathbb{L})$.

Consider three basis as follows:

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

It is easy to see that $2\mathbf{u}$ belongs to each of $\mathbb{L}(\mathbf{B}_1)$, $\mathbb{L}(\mathbf{B}_2)$, and $\mathbb{L}(\mathbf{B}_3)$. Also, since these are sub-lattices of $\mathbb{L}(\mathbf{B})$, $\lambda_2(\mathbb{L}(\mathbf{B}_i)) \geq \lambda_2(\mathbb{L}(\mathbf{B}))$. This implies that $\lambda_2(\mathbb{L}(\mathbf{B}_i)) \geq \frac{2}{\gamma} \lambda_1(\mathbb{L}(\mathbf{B}_i))$ for $i \in \{1, 2, 3\}$. Thus, using the $\text{duSVP}_{\gamma/2}$ oracle, we can check whether $\lambda_1(\mathbb{L}(\mathbf{B}_i)) \leq d$, or $\lambda_1(\mathbb{L}(\mathbf{B}_i)) > d$, and hence whether $\mathbf{u} \in \mathbb{L}(\mathbf{B}_i)$ or not.

It is sufficient to prove that $\mathbf{u} \in \mathbb{L}(\mathbf{B}_i)$ for some $i \in \{1, 2, 3\}$. If α_1 is even, then $\mathbf{u} \in \mathbb{L}(\mathbf{B}_1)$, and if α_2 is even, then $\mathbf{u} \in \mathbb{L}(\mathbf{B}_2)$. If α_1 and α_2 are both odd, then $\mathbf{u} = \alpha_1(\mathbf{b}_1 + \mathbf{b}_2) + \frac{\alpha_2 - \alpha_1}{2}(2\mathbf{b}_2) + \alpha_3 \mathbf{b}_3 + \dots + \alpha_n \mathbf{b}_n \in \mathbb{L}(\mathbf{B}_3)$. \square

Thus, given a uSVP_γ instance $\mathbb{L}(\mathbf{B})$ of rank n , using Lemma 10, we can obtain a sequence of sub-lattices (where each lattice is a strict sub-lattice of the previous one) such that each of these contains the shortest vector of $\mathbb{L}(\mathbf{B})$. Then, using Lemma 9, we obtain a basis of a sublattice of $\mathbb{L}(\mathbf{B})$ of rank $n - 1$, still containing the shortest vector of $\mathbb{L}(\mathbf{B})$. Repeating this procedure, we obtain a basis of a sublattice of $\mathbb{L}(\mathbf{B})$ of rank 1 containing the shortest vector of $\mathbb{L}(\mathbf{B})$, which will be the vector \mathbf{u} . We thus obtain the following result.

Theorem 7. *For any $\gamma \geq 2$, there exists an algorithm that solves uSVP_γ given a $\text{duSVP}_{\gamma/2}$ oracle.*

7 Discussion and open problems

Many interesting problems related to uSVP remain. The gap between the uniqueness factor $(1 + \frac{1}{\text{poly}})$, for which we know that the uSVP 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 uSVP for some constant factor.

The decision version of uSVP was not known to be NP -hard, as it does not follow from Kumar-Sivakumar's work [21]. 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 $(1 + \frac{1}{\text{poly}})$ 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

1. M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence, *STOC*, 1997.
2. M. Ajtai. Generating hard instances of lattice problems, *STOC*, 1996, 99-108.
3. M. Ajtai. The shortest vector problem in ℓ_2 is NP -hard for randomized reductions, *STOC*, 1998, 10-19.
4. Miklós Ajtai, Ravi Kumar and D. Sivakumar. Sampling Short Lattice Vectors and the Closest Lattice Vector Problem, *CCC*, 2002, pp. 53-57.
5. M. Ajtai, R. Kumar and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem, *STOC*, 1998, 266-275.
6. D. Aharonov and O. Regev. Lattice problems in $\text{NP} \cap \text{co-NP}$, *J. ACM* 52 (2005), no. 5, 749-765.
7. P. van Emde Boas. Another NP -complete partition problem and the complexity of computing short vectors in a lattice. Technical report 81-04, Mathematisch Instituut, Universiteit van Amsterdam, 1981.
8. J. Blömer and J.-P. Seifert. The complexity of computing short linearly independent vectors and short bases in a lattice, *STOC*, 1999, 711-720.

9. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296:625-635, 1993.
10. Jin-yi Cai. A Relation of Primal-Dual Lattices and the Complexity of Shortest Lattice Vector Problem. *Theor. Comput. Sci.* 207(1): 105-116 (1998).
11. I. Dinur, Approximating SVP_{∞} to within almost polynomial factors is **NP**-hard. *Theoretical Computer Science* 285 (2002) no. 1, pp. 55-71.
12. I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is **NP**-hard. *Combinatorica*, 23(2):205-243, 2003.
13. O. Goldreich, and S. Goldwasser. On the limits of non-approximability of lattice problems, *STOC*, 1998, pp. 1-9.
14. O. Goldreich, S. Goldwasser, and S. Halevi. Eliminating decryption errors in Ajtai-Dwork cryptosystem, *CRYPTO*, 1997, pp. 112-123.
15. O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2):55-61, 1999.
16. S. Goldwasser and D. Micciancio. Complexity of lattice problems, *Springer*, 2002.
17. I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors, *STOC*, 2007.
18. Ravi Kannan. Minkowski's convex body theorem and integer programming, *Math. Oper. Res.*, 12 (1987), pp. 415-440.
19. Ravi Kannan. Algorithmic geometry of numbers, *Annual Review of Computer Science* 2 (1987), 231-267.
20. S. Khot. Hardness of approximating the shortest vector problem in lattices, *JACM*, 2005, 52(5), 789-808.
21. R. Kumar and D. Sivakumar. On the unique shortest lattice vector problem, *Theoretical Computer Science* 255 (2001), no. 1-2, 641-648.
22. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovasz. Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261(1982), 513-534.
23. Vadim Lyubashevsky, Daniele Micciancio. On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem, *CRYPTO* 2009, 577-594.
24. D. Micciancio. Efficient reductions among lattice problems, *SODA*, 2008, 84-93.
25. D. Micciancio. The shortest vector problem is **NP**-hard to approximate within some constant, *SIAM journal on Computing*, 2001, 30(6), 2008-2035.
26. H. Minkowski. *Geometrie der Zahlen*, reprint 1953.
27. D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations, *STOC*, 2010, pp. 351-358.
28. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem, *STOC*, 2009.
29. O. Regev. New lattice-based cryptographic constructions, *J. ACM* 51 (2004), no. 6, 899-942.
30. C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms, *Theoretical Computer Science*, 53(2-3):201-224, 1987.