New Variants of Lattice Problems and Their NP-Hardness

Wulu Li

School of Mathematical Science
Peking University
Beijing, China
liwulu@pku.edu.cn

Abstract. We introduce some new variants of lattice problems: Quadrant-SVP, Quadrant-CVP and Quadrant-GapCVP'. All of them are NP-hard under deterministic reductions from subset sum problem. These new type of lattice problems have potential in construction of cryptosystems. Moreover, these new variant problems have reductions with standard SVP (shortest vector problem) and CVP (closest vector problem), this feature gives new way to study the complexity of SVP and CVP, especially for the proof of NP-hardness of SVP under deterministic reductions, which is an open problem up to now.

Keywords: lattice, complexity, NP-hard, deterministic reduction.

1 Introduction

Lattice has been widely studied in cryptography in these years, for its problems enjoy very strong security proofs based on worst-case hardness, and they have potential against quantum attack.

A lattice $\mathcal{L}$ is a discrete subgroup of the Euclidean space $\mathbb{R}^m$, and it is generated by linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n$, namely:

$$\mathcal{L} = \{\sum_{i=1}^{n} x_i \mathbf{b}_i | x_i \in \mathbb{Z}, \mathbf{b}_i \in \mathbb{R}^m\}.$$

Denoted by $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n)$, m, n are called the dimension and the rank of it. Usually, we consider lattices with rational generating vectors, and it is called the rational lattices.

Lattice was first studied as a part of geometry of numbers, and was developed Gauss, Hermite, Zolotarev, Dirichlet, Minkowski [18] and Voronoi [22]. There are mainly two classical problems over lattices: SVP and CVP.

SVP (shortest vector problem): given lattice and norm (such as ℓ_2 norm, etc), find the shortest nonzero vector in it;

CVP (closest vector problem): given lattice, norm and a target vector $\mathbf{t} \in \mathbb{R}^m$, find the closest lattice vector from $\mathbf{t}$.

X. Huang and J. Zhou (Eds.): ISPEC 2014, LNCS 8434, pp. 511–523, 2014.

Since the historic work introduced by Lenstra *et.al* [13]: the LLL algorithm, which is the first algorithm for approximate SVP with factor $\phi = O((2/\sqrt{3})^n)$. In 1986, algorithm for approximate CVP was introduced by Babai [4], using the LLL method; Schnorr [20] improved the LLL algorithm and decreased the approximate factor to $(1+\epsilon)^n$; in 2001, Ajtai, Kumar and Sivakumar [3] proposed a new sieve method for solving SVP; Blömer [5] improved the AKS algorithm for solving GSVP and CVP; recently a new algorithm for SVP based on voronoi cell was introduced by Micciancio [17], with single exponential running time.

There are a variety of cryptosystems building on lattice assumptions. In 1996, the Ajtai-Dwork [2] public-key cryptosystem was proposed, the security is based on the worst-case hardness of unique-SVP, it was the first lattice based public-key cryptosystem with provable security; GGH [10] was proposed by Goldreich, Goldwasser and Halevi in 1996; in 1997, Hoffstein, Pipher and Silverman introduced NTRU [11], it is the most efficient lattice based cryptosystem; Oded Regev [19] proposed LWE and cryptosystem built from it, its security was based on the hardness of worst-case hardness of CVP; in 2009, Gentry [8] proposed the first fully-homomorphic encryption scheme based on lattice.

1.1 NP-Hardness Result of SVP and CVP

The complexity of lattice problems has been studied since 1980s. In 1981, van Emde Boas [21] proved the NP-hardness of CVP in ℓ_p norm and NP-hardness of SVP in ℓ_∞ norm, also he conjectured the NP-hardness of SVP in ℓ_p norm; in 1996, Ajtai [1] proved that SVP in ℓ_2 norm is NP-hard, under randomized reduction; Cai [6] improved Ajtai's work, showed approximating SVP in ℓ_p norm within factor $O(1+1/n^\epsilon)$ is NP-hard, his result also based on randomized reduction; Micciancio [14]proved approximating SVP in ℓ_p norm within factor $\sqrt[p]{2}$ is NP-hard under randomized reduction; Knot [12] proved that under assumption "NP≠RTIME", approximate SVP within factor $\gamma(n) = 2^{\log^{1/2-\epsilon}(n)}$ is NP-hard; a recent work by Micciancio [15] improved Knot's result, showed NP-harness of approximating SVP within constant factor under RUR-reduction. But there are no deterministic reductions to prove the NP-hardness of SVP up to now.

On the other side, Goldreich and Goldwasser [9] showed that under approximate factor $\gamma = \sqrt{n/O(\log n)}$, if approximating SVP is NP-hard, then coNP⊆AM, which is thought to be impossible in complexity theory, so proving the hardness of SVP from constant factor c to $\sqrt{n/O(\log n)}$ is still an open problem.

Actually, the NP-hardness under randomized reductions is not a standard complexity result, how to find a deterministic reduction to prove the NP-hardness of lattice problem is also an open problem. In this paper, we focus on variants of lattice problems and prove their NP-hardness under deterministic reductions.

1.2 Our Results and Open Problems

We introduce 3 new variants of lattice problem: Quadrant-SVP, Quadrant-CVP and Quadrant-CVP', all these problems have NP-hardness under deterministic

reductions. The Quadrant-SVP, defined similar to SVP, is to find the shortest nonzero lattice vector in given subset of $\mathbb{R}^n$, usually we call the subset "quadrant" of Euclid space, in this paper, we use quadrant $Q_1 = \{\mathbf{x} = (x_1, \cdots, x_m) | \forall i \in [m],\ x_i \geq 0\}$.

(Quadrant-SVP) Given lattice $\mathcal{L}$ in $\mathbb{R}^m$, ℓ_p norm and Q_1, find the shortest nonzero vector in $\mathcal{L} \cap Q_1$.

(Quadrant-CVP) Given lattice $\mathcal{L}$ in $\mathbb{R}^m$, ℓ_p norm and a target vector $\mathbf{t} \in \mathbb{R}^m$, find a lattice vector $\mathbf{v}$ such that $||\mathbf{v} - \mathbf{t}|| = min\{||\mathbf{x} - \mathbf{t}|| | \mathbf{x} \in \mathcal{L}, \mathbf{x} - \mathbf{t} \in Q_1\}$.

The main result of this paper is contained in the following theorem:

Theorem 1. *For any given lattice $\mathcal{L}$ and ℓ_p norm, there exist no polynomial time algorithms to solve Quadrant-SVP, Quadrant-CVP and Quadrant-CVP', unless P=NP.*

We give the first construction of Quadrant lattice problems and prove their NP-hardness, which is the main contribution of this paper. Besides, we give a deterministic reduction from Quadrant-CVP' to CVP, the result can be seen as a new proof of NP-hardness of CVP, this Quadrant method can be used in studying the complexity of SVP and CVP.

By proving the NP-hardness of Quadrant-SVP, we get closer to prove the NP-hardness of SVP under deterministic reduction, which is still an open problem; on the other hand, how to prove the NP-hardness of Quadrant lattice problems with larger approximate factor is also an open problem.

1.3 Organization

In section 2 we give readers some preliminaries; in section 3 we give the definition of Quadrant lattice problems and prove their NP-hardness; in section 4 we discuss the approximate variants of Quadrant lattice problems and prove their NP-hardness; in section 5 we give the conclusion.

2 Preliminaries

2.1 Lattice

Lattice is a subgroup of Euclidian space $\mathbb{R}^m$, it is generated by n independent vectors, namely:

$$\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i | \mathbf{x} = (x_1, \cdots, x_m) \in \mathbb{Z}^m\}$$

Where m is the dimension of $\mathcal{L}$, n is its rank, the vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ is the basis of $\mathcal{L}$.

The Gram-Schmidt orthogonalization of a basis $\mathbf{B}$ is the sequence of orthogonal vectors $\widetilde{\mathbf{b}_1}, \ldots, \widetilde{\mathbf{b}_n}$, where $\widetilde{\mathbf{b}_i}$ is the component of $\mathbf{b}_i$ orthogonal to

$span(\mathbf{b}_1, \cdots, \mathbf{b}_{i-1})$, clearly, $||\widetilde{\mathbf{b}_i}|| \leq ||\mathbf{b}_i||$, where $||\cdot||$ denotes the Euclidian norm in $\mathbb{R}^m$, namely, the ℓ_p norm.

The ith successive minimum λ_i is defined as the smallest r that $\mathbf{b}_r$ contains at least i independent vectors in $\mathbb{R}^m$ (λ_i can be defined in different norms, such as ℓ_p), λ_1 is the length of the shortest vector in $\mathcal{L}$. For a linearly independent vector set $\mathbf{S} \subset \mathcal{L}$, where $\mathbf{S} = \{\mathbf{s}_1 \dots \mathbf{s}_r\}$, we denote r as the rank of $\mathbf{S}$ and denote $||\mathbf{S}||$ as the longest norm of $\mathbf{s}_1 \dots \mathbf{s}_r$, namely:

$$||\mathbf{S}|| = \max_i \{||\mathbf{s}_1|| \dots ||\mathbf{s}_r||\}.$$

If the $\mathbf{S}$ has rank n, we call $\mathbf{S}$ a full rank independent vector set. So λ_n is the norm of shortest full rank independent vector set.

2.2 SVP and CVP

Lattice is attractive in cryptography for its problems including SVP (*Gap*SVP), CVP (*Gap*CVP), all of these problems achieve NP-hardness under deterministic or randomized reductions, we define these problems in the following:

Definition 2. *(SVP) For any given lattice $\mathcal{L}$ and the ℓ_p norm, the goal is to find the shortest nonzero vector $\mathbf{v} \in \mathcal{L}$. In other words, the goal of SVP is to find $\mathbf{v} \in \mathcal{L}$ such that $||\mathbf{v}|| = \lambda_1$.*

Definition 3. *(CVP) For any given lattice $\mathcal{L}$, ℓ_p norm and a target vector $\mathbf{t} \in \mathbb{R}^m$, the goal is to find $\mathbf{v} \in \mathcal{L}$ such that $||\mathbf{v} - \mathbf{t}|| = min_{\mathbf{x} \in \mathcal{L}} ||\mathbf{x} - \mathbf{t}||$.*

There are decision versions of SVP and CVP, we omit the definition for simplicity. There are also promise version of SVP and CVP, which is often used in building of cryptosystems.

Definition 4. *(GapSVP$_\gamma$) For input a lattice basis $\mathbf{B}$ and a real d, it is a **Yes** instance if $\lambda_1 \leq d$, and is a **No** instance if $\lambda_1 > \gamma d$, if $d < \lambda_1 \leq \gamma d$, then both **Yes** and **No** would be correct.*

Definition 5. *(GapCVP$_\gamma$) For input a lattice basis $\mathbf{B}$, a vector $\mathbf{t} \in \mathbb{R}^m$ and a real d, it is a **Yes** instance if dist$(\mathcal{L}, \mathbf{t}) \leq d$, and is a **No** instance if dist$(\mathcal{L}, \mathbf{t}) > \gamma d$, where "dist" is defined by arbitrary norm (ℓ_p norm in this paper) in $\mathbb{R}^m$, $d <$ dist$(\mathcal{L}, \mathbf{t}) \leq \gamma d$, then both **Yes** and **No** would be correct.*

It is obvious that when $\gamma = 1$, $GapSVP_\gamma$ and $GapCVP_\gamma$ is the decision version of SVP and CVP.

2.3 NP-Hardness of Lattice Problems

In this subsection we review the NP-hardness results of several lattice problems, both SVP (GapSVP), CVP (GapCVP) are proved to be NP-hard, we introduce some of them in the following lemmas:

Lemma 6. *([21]) CVP is NP-hard in ℓ_p norm under deterministic reduction; SVP is NP-hard in ℓ_∞ under deterministic reduction.*

Lemma 7. *([1]) SVP in ℓ_2 norm is NP-hard under randomized reduction.*

Lemma 8. *([16]) $GapCVP_\gamma$ is NP-hard in ℓ_p norm under deterministic reduction, where $\gamma = 2^{\log^{1-\epsilon}(n)}$.*

Lemma 9. *([12]) $GapSVP_\gamma$ is NP-hard in ℓ_p norm under randomized reduction, where $\gamma = 2^{\log^{1/2-\epsilon}(n)}$.*

Since there are no NP-hardness results for SVP (GapSVP) under deterministic reductions except for ℓ_p norm, the NP-hardness of Quadrant-SVP is the first deterministic NP-hardness result for SVP type problems.

2.4 Subset Sum Problem

In this paper, we use subset sum (SS) in the construction of reduction, the SS problem is widely studied in cryptography and complexity theory.

Definition 10. *(SS) The input is an integer s and a set of integer $\mathbf{A} = \{a_1, \cdots, a_n\}$, the goal is to determine whether there exists $\mathbf{x} \in \{0,1\}^n$, such that $\sum_{i=1}^{n} x_i a_i = s$.*

SS is a classic NP-complete problem [7], we will use SS in all reduction of this paper.

Theorem 11. *([7]) Subset sum problem is NP-complete.*

Proof. Omitted for brevity. □

3 NP-Hardness of Quadrant-SVP (CVP)

3.1 Definition

In this subsection we give the definition of Quadrant-SVP, Quadrant-CVP, first of all, we define the "Quadrant" we use throughout the paper:

Definition 12. *(Quadrant) A quadrant Q is a subset of $\mathbb{R}^m$, with property that $\forall \mathbf{x} = (x_1, \cdots, x_m) \in Q$, $x_i \geq 0 (or \leq 0)$ for $i = 1, \cdots, m$.*

Obviously there are 2^m Quadrants in $\mathbb{R}^m$, Q_1 denotes $\{\mathbf{x} = (x_1, \cdots, x_m) | x_i \geq 0\}$, and Q_{2^m} denotes $\{\mathbf{x} = (x_1, \cdots, x_m) | x_i \leq 0\}$.

The Quadrant-SVP, defined as solving SVP in Q_i other than $\mathbb{R}^m$.

Definition 13. *(Quadrant-SVP) For any given lattice $\mathcal{L}$ of rank n and the ℓ_p norm, the goal is to find the shortest nonzero vector $\mathbf{v} \in \mathcal{L} \cap Q_i$, if there exist no nonzero vectors in Q_i, output $\emptyset$.*

In the rest of this paper, we will use Q_1 without loss of generosity, if fact, the hardness results of Quadrant lattice problems for any Quadrant Q_i is equivalent to problems for Q_1.

The Quadrant-CVP is defined as the same way:

Definition 14. *(Quadrant-CVP) Given lattice $\mathcal{L}$ in $\mathbb{R}^m$ of rank n, ℓ_p norm and a target vector $\mathbf{t} \in \mathbb{R}^m$, find a lattice vector $\mathbf{v}$ such that $||\mathbf{v} - \mathbf{t}|| = min\{|||\mathbf{x} - \mathbf{t}|||\mathbf{x} \in \mathcal{L}, \mathbf{x} - \mathbf{t} \in Q_1\}$, if there exists no vectors satisfy $\mathbf{x} - \mathbf{t} \in Q_1\}$, output $\emptyset$.*

3.2 Proof of NP-Hardness

In this subsection we prove the NP-hardness of Quadrant-SVP and Quadrant-CVP, using reductions from subset sum problem, our reduction is deterministic.

Theorem 15. *Subset sum problem can be reduced to Quadrant-SVP in polynomial time, under ℓ_p norm $(1 \leq p \leq \infty)$.*

Proof. For SS problem instance $(a_1, \cdots, a_n; s)$, choose an integer $M > 2n$, we have the following lattice basis matrix:

$$\mathbf{H} = \begin{bmatrix} Ma_1, \cdots, Ma_n & -Ms \\ -\mathbf{I}_n & \mathbf{1}_n \\ \mathbf{I}_{n+1} & \end{bmatrix}.$$

Notice that $\mathbf{I}_n$ stands for the unit matrix of dimension n, and $\mathcal{L}(\mathbf{H})$ is an integer lattice with dimension $2n + 2$. Any vector in $\mathcal{L}(\mathbf{H})$ can be written as:

$$\mathbf{Hx} = \begin{pmatrix} M(\sum_{i=1}^{n} x_i a_i - x_{n+1} s) \\ x_{n+1} - x_1 \\ \vdots \\ x_{n+1} - x_n \\ x_1 \\ \vdots \\ x_{n+1} \end{pmatrix}$$

Where $\mathbf{x} = (x_1, \cdots, x_{n+1})$. We will prove that, if we can solve Quadrant-SVP in the above lattice, we will get the solution of the SS problem. Actually, if the SS problem has a solution, then the Quadrant-SVP has a solution $\mathbf{v}$ such that $||\mathbf{v}||_{\ell_p} \leq \sqrt[p]{2n+1}$; if the SS problem has no solutions at all, then the Quadrant-SVP also has no solutions or has solution $\mathbf{v}$ such that $||\mathbf{v}||_{\ell_p} > \sqrt[p]{2n+1}$.

We will divide the proof into two parts, one for $1 \leq p < \infty$ and the other for $p = \infty$.

$(1 \leq p < \infty)$:

1. If SS problem has a solution $(x_1, \cdots, x_n) \in \{0, 1\}^n$ such that $\sum_{i=1}^{n} x_i a_i = s$, then there exists lattice vector

$$\mathbf{v} = \mathbf{H}(x_1, \cdots, x_n, 1)^T = (0, 1 - x_1, \cdots, 1 - x_n, x_1, \cdots, x_n, 1)^T.$$

Since $x_i = 0, 1$, we get $\mathbf{v} \in Q_1$ and $||\mathbf{v}||_{\ell_p} \leq \sqrt[p]{n+1}$, so there exists solution of Quadrant-SVP in $\mathcal{L}(\mathbf{H})$ with norm less than $\sqrt[p]{n+1}$.

2. If SS problem has no solutions, we prove that the Quadrant-SVP has no solutions or has solution $\mathbf{v}$ with $||\mathbf{v}||_{\ell_p} > \sqrt[p]{2n+1}$. We assume that there exists a solution of Quadrant-SVP, $\mathbf{v} \in Q_1$, that $||\mathbf{v}|| \leq \sqrt[p]{2n+1}$.
   - If $x_{n+1} \geq 2$, since $x_i \geq 0$ and $x_{n+1} - x_i \geq 0$. Among $x_1, \cdots, x_n$, we assume there are k_0 elements equal 0, k_1 elements equal 1, k_2 elements equal or bigger than 2, then $n = k_1 + k_2 + k_3$, and

$$||\mathbf{v}||_{\ell_p}^p \geq 2k_1 + 2^p + k_0 2^p + k_2 2^p$$

$$= 2(n + 2^{p-1}) + (2^p - 2)(n - k_1) \geq 2n + 2.$$

   - If $x_{n+1} = 1$, we know that for all $1 \leq i \leq n$, $x_i = 0, 1$, since the SS problem has no solutions, we get $\sum_{i=1}^{n} x_i a_i \neq s$, then $||\mathbf{v}||_{\ell_p}^p \geq M^p \geq 2^p n^p > 2n + 1$.
   - If $x_{n+1} = 0$, then for all $1 \leq i \leq n$, $x_i = 0$, we get $\mathbf{v} = \mathbf{0}$, it can not be a solution for the Quadrant-SVP problem.

   In all of the 3 situations, we get contradiction against the fact we are assuming, then we know that the Quadrant-SVP has no solutions or has solution $\mathbf{v}$ such that $||\mathbf{v}||_{\ell_p} > \sqrt[p]{2n+1}$.

The correctness of the theorem easily followed by the above argument, when $1 \leq p < \infty$.
($p = \infty$):

1. If SS problem has a solution, use similar method, we easily get there exists solution of Quadrant-SVP in $\mathcal{L}(\mathbf{H})$ with ℓ_∞ norm less than 1.
2. If SS problem has no solutions, we get that the Quadrant-SVP has no solutions or has solution $\mathbf{v}$ with $||\mathbf{v}||_{\ell_\infty} \geq 2$.

By above argument, we can solve the SS problem by determine whether the Quadrant-SVP has a solution with norm equal or less than $\sqrt[p]{n+1}$ (or 1) when $1 \leq p < \infty$ (or $p = \infty$). □

We can easily get the NP-hardness of Quadrant-SVP under deterministic reduction:

Corollary 16. *Quadrant-SVP is NP-hard under deterministic reductions, in other words, there exist no polynomial time algorithms to solve Quadrant-SVP, unless P=NP.*

As for Quadrant-CVP, we use similar method to construct the reduction from SS problem.

Theorem 17. *Subset sum problem can be reduced to Quadrant-CVP in polynomial time, under $\ell_p (1 \leq p \leq \infty)$.*

Proof. For SS problem instance $(a_1, \cdots, a_n; s)$, choose an integer $M > 2n$, we have the following lattice basis matrix and target vector:

$$\mathbf{T} = \begin{bmatrix} Ma_1, \cdots, Ma_n \\ -\mathbf{I}_n \\ \mathbf{I}_n \end{bmatrix}, \ \mathbf{t} = (Ms, -\mathbf{1}_n, \mathbf{0}_n)^T.$$

Notice that $\mathbf{I}_n$ stands for the unit matrix of dimension n, and $\mathcal{L}(\mathbf{T})$ is an integer lattice with dimension $n+1$. For any $\mathbf{x} = (x_1, \cdots, x_n)^T$,

$$\mathbf{Tx} - \mathbf{t} = (M(\sum_{i=1}^{n} x_i a_i - s), 1 - x_1, \cdots, 1 - x_n, x_1, \cdots, x_n)^T.$$

We will also divide the proof into two parts, one for $1 \leq p < \infty$ and the other for $p = \infty$.
$(1 \leq p < \infty)$:

1. If the SS problem has a solution, say $\mathbf{x} = (x_1, \cdots, x_n)^T$, such that $\sum_{i=1}^{n} x_i a_i = s$, then there exists a lattice vector $\mathbf{v} = \mathbf{Tx}$ such that $\mathbf{v} - \mathbf{t} = (0, 1 - x_1, \cdots, 1 - x_n, x_1, \cdots, x_n)^T \in Q_1$, thus $x_i = 0, 1$, we have $||\mathbf{v} - \mathbf{t}||_{\ell_p} = \sqrt[p]{n}$, then the solution of Quadrant-CVP is within distance $\sqrt[p]{n}$ from $\mathbf{t}$.
2. If the SS problem has no solutions, we assume that there exists a solution of Quadrant-CVP, say $\mathbf{v} = \mathbf{Tx}$ such that $\mathbf{v} - \mathbf{t} \in Q_1$ and $||\mathbf{v} - \mathbf{t}||_{\ell_p} \leq \sqrt[p]{n}$, then we have $x_i = 0, 1$, and $s \neq \sum_{i=1}^{n} x_i a_i$, we have $||\mathbf{v} - \mathbf{t}||_{\ell_p}^p \geq M^p \geq (n+1)^p \geq n + 1$, which contradicts to the fact that $||\mathbf{v} - \mathbf{t}||_{\ell_p} \leq \sqrt[p]{n}$.

The correctness of the theorem followed by the above argument, when $1 \leq p < \infty$.
$(p = \infty)$:

1. If SS problem has a solution, use similar method, we easily get there exists solution $\mathbf{v}$ of Quadrant-CVP in $\mathcal{L}(\mathbf{T})$ with $||\mathbf{v} - \mathbf{t}||_{\ell_\infty} \leq 1$.
2. If SS problem has no solutions, we get that the Quadrant-CVP has no solutions or has solution $\mathbf{v}$ with $||\mathbf{v} - \mathbf{t}||_{\ell_\infty} \geq M$.

From the above discussion, we can solve the SS problem by determine whether there exists lattice vector $\mathbf{v}$ within ℓ_p (or ℓ_∞) distance $\sqrt[p]{n}$ (or 1) from $\mathbf{t}$, satisfying $\mathbf{v} - \mathbf{t} \in Q_1$. □

Notice the above reduction is deterministic, we get similar corollary:

Corollary 18. *Quadrant-CVP is NP-hard under deterministic reductions, in other words, there exist no polynomial time algorithms to solve Quadrant-CVP, unless P=NP.*

4 NP-Hardness of Promise Variants of Quadrant Lattice Problems

4.1 Definitions

There are also promise version of Quadrant lattice problem, defined similar to GapSVP and GapCVP in section 2.2, we define another 3 promise versions of Quadrant lattice problems, they are Quadrant-GapSVP, Quadrant-GapCVP, Quadrant-GapCVP'. In the rest of this paper, we use symbol $\lambda_1^{(1)}$ denotes $min_{\mathbf{0}\neq\mathbf{x}\in\mathcal{L}(\mathbf{B})\cap Q_1}\{||\mathbf{x}||_{\ell_p}\}$.

Definition 19. *(Quadrant-GapSVP$_\gamma$) For input a lattice basis* $\mathbf{B}$ *and a real* d*, it is a* ***Yes*** *instance if* $\lambda_1^{(1)} \leq d$*, and is a* ***No*** *instance if* $\lambda_1^{(1)} > \gamma d$ *or there are no nonzero lattice vectors in* Q_1*, if* $d < \lambda_1^{(1)} \leq \gamma d$*, then both* ***Yes*** *and* ***No*** *would be correct.*

We also use symbol $dist^{(1)}(\mathbf{t}, \mathcal{L})$ denotes $min_{\mathbf{v}\in\mathcal{L},\mathbf{v}-\mathbf{t}\in Q_1}\{||\mathbf{v}-\mathbf{t}||_{\ell_p}$ in the rest of this paper.

Definition 20. *(Quadrant-GapCVP$_\gamma$) For input a lattice basis* $\mathbf{B}$*, a target vector* $\mathbf{t}$ *and a real* d*, it is a* ***Yes*** *instance if* $dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq d\}$*, and a* ***No*** *instance if* $dist^{(1)}(\mathbf{t}, \mathcal{L}) > \gamma d\}$*, or there are no vectors satisfying* $\mathbf{v} - \mathbf{t} \in Q_1$*, if* $d < dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq \gamma d$*, then both* ***Yes*** *and* ***No*** *would be correct.*

4.2 NP-Hardness Proofs

Theorem 21. *The SS problem* $(a_1, \cdots, a_n; s)$ *can be reduced to Quadrant-GapSVP$_\gamma$ where* $\gamma = \sqrt[p]{2} - \epsilon$ *for* $p < \infty$ *and* $\gamma = 2 - \epsilon$ *for* $p = \infty$*, where* $\epsilon > 0$ *is a negligible constant.*

Proof. As proved in Theorem 15, we divide the proof into two parts, one for $1 \leq p < \infty$ and the other for $p = \infty$.
$(1 \leq p < \infty)$: We set $\mathcal{L}(\mathbf{H})$, $d = \sqrt[p]{n+1}$, $\gamma = \sqrt[p]{2} - \epsilon$ as the input of Quadrant-*GapSVP$_\gamma$*, where ϵ is positive small enough.

1. If the SS problem has a solution, we know from Theorem 15 that $\lambda_1^{(1)} \leq \sqrt[p]{n+1} = d$, which is not a **No** instance of Quadrant-*GapSVP$_\gamma$*;
2. If the SS problem has no solutions, we know that $\lambda_1^{(1)} \geq \sqrt[p]{2n+2} = \sqrt[p]{2}d > \gamma d$ or $\mathcal{L} \cap Q_1 = \{\mathbf{0}\}$, which is not a **Yes** instance of Quadrant-*GapSVP$_\gamma$*.

By the answer of Quadrant-*GapSVP$_\gamma$*, we can determine whether the SS problem has a solution, namely, if the output of Quadrant-*GapSVP$_\gamma$* is **Yes**, then SS has a solution; if the output of Quadrant-*GapSVP$_\gamma$* is **No**, then SS has no solutions.
$(p = \infty)$: We set $\mathcal{L}(\mathbf{H})$, $d = 1$, $\gamma = \sqrt[p]{2} - \epsilon$ as the input of Quadrant-*GapSVP$_\gamma$* as above.

1. If the SS problem has a solution, we know from Theorem 15 that $\lambda_1^{(1)} \leq 1 = d$, which is not a **No** instance of Quadrant-*GapSVP$_\gamma$*;

2. If the SS problem has no solutions, we know that $\lambda_1^{(1)} \geq 2 = 2d > \gamma d$ or $\mathcal{L} \cap Q_1 = \{\mathbf{0}\}$, which is not a **Yes** instance of Quadrant-$GapSVP_\gamma$.

Similarly, if the output of Quadrant-$GapSVP_\gamma$ is **Yes**, then SS has a solution; if the output of Quadrant-$GapSVP_\gamma$ is **No**, then SS has no solutions. □

Notice the above reduction is deterministic in polynomial time, then we easily get the NP-hardness of Quadrant-$GapSVP_\gamma$:

Corollary 22. *Quadrant-$GapSVP_\gamma$ is NP-hard under deterministic reductions, where $\gamma = \sqrt[p]{2} - \epsilon$ in $\ell_{p<\infty}$ norm and $\gamma = 2 - \epsilon$ in ℓ_∞ norm.*

The result for Quadrant-$GapCVP_\gamma$ is similar, according to Theorem 17 and Theorem 21.

Theorem 23. *The SS problem $(a_1, \cdots, a_n; s)$ can be reduced to Quadrant-$GapCVP_\gamma$ where $\gamma = poly(n)$, where $poly(n)$ denotes for any polynomial with input n.*

Proof. $(1 \leq p < \infty)$: For SS instance $(a_1, \cdots, a_n; s)$, choose $M = \gamma \sqrt[p]{n} + 1$, which is still polynomial of n, build a lattice $\mathcal{L}(\mathbf{T})$ as in Theorem 17, we set $\mathcal{L}(\mathbf{T})$, γ, $\mathbf{t}$, $d = \sqrt[p]{n}$ as the input for Quadrant-$GapCVP_\gamma$:

1. If the SS problem has a solution, we know that $dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq \sqrt[p]{n}$, which is not a **No** instance of Quadrant-$GapCVP_\gamma$;
2. If the SS problem has no solutions, we know that $dist^{(1)}(\mathbf{t}, \mathcal{L}) \geq M = \gamma \sqrt[p]{n} + 1 > \gamma d$ or $\mathcal{L} \cap Q_1 = \{\mathbf{0}\}$, which is not a **Yes** instance of Quadrant-$GapCVP_\gamma$.

We can solve the SS by solving the Quadrant-$GapCVP_\gamma$, if the output of Quadrant-$GapCVP_\gamma$ is **Yes**, then SS has a solution; if the output of Quadrant-$GapCVP_\gamma$ is **No**, then SS has no solutions.
$(1 \leq p < \infty)$: Omitted for brevity. □

Corollary 24. *Quadrant-$GapCVP_{\gamma=poly(n)}$ is NP-hard under deterministic reductions.*

4.3 Mixed Problem and Relationship with GapCVP

In this subsection we mix the original GapCVP with the Quadrant-GapCVP, propose a new type of promise problem and prove its NP-hardness under deterministic reduction, we also give reduction between the new type problem and standard GapCVP.

Definition 25. *(Quadrant-GapCVP') For input a lattice basis $\mathbf{B}$, a target vector $\mathbf{t}$ and a real d, it is a **Yes** instance if $dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq d$, and a **No** instance if $dist(\mathbf{t}, \mathcal{L}) > d$, or there are no vectors satisfying $\mathbf{v} - \mathbf{t} \in Q_1$, if $d < dist^{(1)}(\mathbf{t}, \mathcal{L})$ and $dist(\mathbf{t}, \mathcal{L}) \leq d$, then both **Yes** and **No** would be correct.*

Theorem 26. *The SS problem* $(a_1, \cdots, a_n; s)$ *can be reduced to Quadrant-GapCVP'.*

Proof. $(1 \leq p < \infty)$: For SS instance $(a_1, \cdots, a_n; s)$, choose $M = \sqrt[p]{n} + 1$, which is still polynomial of n, build a lattice $\mathcal{L}(\mathbf{T})$ as in Theorem 17, we set $\mathcal{L}(\mathbf{T})$, γ, $\mathbf{t}$, $d = \sqrt[p]{n}$ as the input for Quadrant-GapCVP':

1. If the SS problem has a solution, we know that $dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq \sqrt[p]{n}$, which is not a **No** instance of Quadrant-GapCVP';
2. If the SS problem has no solutions, we assume that $dist(\mathbf{t}, \mathcal{L}) \leq \sqrt[p]{n}$, then there exists lattice vector $\mathbf{v} = \mathbf{Tx}$ such that $\mathbf{v} - \mathbf{t} = (M(\sum_{i=1}^{n} x_i a_i - s), 1 - x_1, \cdots, 1 - x_n, x_1, \cdots, x_n)^T$ and $||\mathbf{v} - \mathbf{t}|| \leq \sqrt[p]{n}$. Since $M = \sqrt[p]{n} + 1$, we know that $\sum_{i=1}^{n} x_i a_i - s = 0$, then $\exists i$ such that $x_i \neq 0, 1$, we have $max\{|1 - x_i|, |x_i|\} \geq 2$, then $||\mathbf{v} - \mathbf{t}|| \geq \sqrt[p]{n + 2^p} > \sqrt[p]{n}$, which contradicts to the fact we are assuming, so it is not a **Yes** instance of Quadrant-GapCVP'.

So we can solve the SS by solving the Quadrant-GapCVP', if the output of Quadrant-GapCVP' is **Yes**, then SS has a solution; if the output of Quadrant-GapCVP' is **No**, then SS has no solutions.
$(1 \leq p < \infty)$: Omitted for brevity. □

Corollary 27. *Quadrant-GapCVP' is NP-hard under deterministic reductions.*

We get the NP-hardness of Quadrant-GapCVP' by reduction from SS problem, since we know the fact that GapCVP is also NP-hard under deterministic reduction, a natural question may be asked, what is the relationship between GapCVP and Quadrant-GapCVP'? Is one question harder than another? Actually, we have the following result:

Theorem 28. *There exists deterministic reduction from Quadrant-GapCVP' to* $GapCVP_{\gamma=1}$.

Proof. Given Quadrant-GapCVP' instance $(\mathcal{L}, d, \mathbf{t})$, we solve GapCVP with the same input.

1. If the $(\mathcal{L}, d, \mathbf{t})$ is not a **Yes** instance for Quadrant-GapCVP', which means $dist(\mathbf{t}, \mathcal{L}) > d$. For GapCVP, it is also not a **Yes** instance for Quadrant-GapCVP';
2. If the $(\mathcal{L}, d, \mathbf{t})$ is not a **No** instance for Quadrant-GapCVP', which means $dist^{(1)}(\mathbf{t}, \mathcal{L}) \leq d$, since $dist(\mathbf{t}, \mathcal{L}) \leq dist^{(1)}(\mathbf{t}, \mathcal{L})$, we get $dist(\mathbf{t}, \mathcal{L}) \leq d$, which is not a **No** instance for GapCVP.

The reduction easily followed by the above argument, and the reduction is deterministic. □

Form Theorem 28 we know that Quadrant-GapCVP' is easier than GapCVP, but still achieves NP-hardness. It has potential in construction of cryptosystem as GapCVP.

5 Conclusion

In this paper we study a variety of new lattice problems, they are Quadrant-SVP(CVP), Quadrant-GapSVP(CVP), Quadrant-GapCVP'. All the five problems are NP-hard under deterministic reduction, and they have reduction with the standard lattice problem. These new lattice problems are attractive for their hardness and potential in cryptography.

Although, from our point of view, there are still many open questions about the Quadrant lattice problems, such as the worst-case to average-case reduction; hardness under larger approximate factor; specific relationship with standard lattice problems.

References

1. Ajtai, M.: The shortest vector problem in l 2 is np-hard for randomized reductions. In: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, pp. 10–19. ACM (1998)
2. Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing, pp. 284–293. ACM (1997)
3. Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing, pp. 601–610. ACM (2001)
4. Babai On, L.: lovászlattice reduction and the nearest lattice point problem. Combinatorica 6(1), 1–13 (1986)
5. Blömer, J., Naewe, S.: Sampling methods for shortest vectors, closest vectors and successive minima. In: Arge, L., Cachin, C., Jurdziński, T., Tarlecki, A. (eds.) ICALP 2007. LNCS, vol. 4596, pp. 65–77. Springer, Heidelberg (2007)
6. Cai, J.-Y., Nerurkar, A.: Approximating the svp to within a factor (1+ 1/dim e) is np-hard under randomized reductions. Journal of Computer and System Sciences 59(2), 221–239 (1999)
7. Gary, M.R., Johnson, D.S.: Computers and intractability: A guide to the theory of np-completeness (1979)
8. Gentry, C.: Fully homomorphic encryption using ideal lattices (2009)
9. Goldreich, O., Goldwasser, S.: On the limits of non-approximability of lattice problems. In: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, pp. 1–9. ACM (1998)
10. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 112–131. Springer, Heidelberg (1997)
11. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
12. Khot, S.: Hardness of approximating the shortest vector problem in lattices. Journal of the ACM (JACM) 52(5), 789–808 (2005)
13. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261(4), 515–534 (1982)
14. Micciancio, D.: The shortest vector in a lattice is hard to approximate to within some constant. SIAM Journal on Computing 30(6), 2008–2035 (2001)

15. Micciancio, D.: Inapproximability of the shortest vector problem: Toward a deterministic reduction. Theory of Computing 8(1), 487–512 (2012)
16. Micciancio, D., Goldwasser, S.: Complexity of lattice problems: a cryptographic perspective, vol. 671. Springer (2002)
17. Micciancio, D., Voulgaris, P.: A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In: Proceedings of the 42nd ACM Symposium on Theory of Computing, pp. 351–358. ACM (2010)
18. Minkowski, H.: Geometrie der zahlen. BG Teubner (1910)
19. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6), 34:1–34:40 (2009)
20. Schnorr, C.-P.: A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science 53(2), 201–224 (1987)
21. van Emde-Boas, P.: Another NP-complete partition problem and the complexity of computing short vectors in a lattice, Department, Univ. (1981)
22. Voronoï, G.: Nouvelles applications des paramètres continus à la théorie des formes quadratiques. deuxième mémoire. recherches sur les parallélloèdres primitifs. Journal für die reine und angewandte Mathematik 134, 198–287 (1908)