On Promise Problem of the Generalized Shortest Vector Problem

Wenwen Wang[1,2,3] and Kewei Lv[1,2](✉)

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
Beijing 100093, China
{wangwenwen,lvkewei}@iie.ac.cn
[2] Data Assurance Communication Security Research Center,
Chinese Academy of Sciences, Beijing 100093, China
[3] University of Chinese Academy Sciences, Beijing 100049, China

Abstract. In 2009, Blömer and Naewe proposed the Generalized Shortest Vector Problem (GSVP). We initiate the study of the promise problem (GAPSAM) for GSVP. It is a promise problem associated with estimating the subspace avoiding minimum. We show GAPSAM$_{c\cdot n}$ lies in *coNP*, where c is a constant. Furthermore, we study relationships between GAPSAM of a lattice and the nth successive minimum, the shortest basis, and the shortest vector in the dual of the saturated sublattice, and obtain new transference theorems for GAPSAM. Then, using the new transference theorems, we give various deterministic polynomial time reductions among the promise problems for some lattice problems. We also show GAPSAM$_\gamma$ can be reduced to the promise problem associated to the Closest Vector Problem (GAPCVP$_\gamma$) under a deterministic polynomial time rank-preserving reduction.

Keywords: The generalized shortest vector problem · The saturated sublattice · Transference theorems · Polynomial time reduction

1 Introduction

A lattice is the set of all integer combinations of n linearly independent vectors in $\mathbb{R}^m$, where n is the rank of the lattice, m is the dimension of the lattice, and the n linearly independent vectors are called a lattice basis. Let $B = [\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n]$ be a basis of the lattice $\boldsymbol{L}$. The ith successive minimum $\lambda_i(\boldsymbol{L})$ of the lattice $\boldsymbol{L}$ is the least number r such that the sphere centered at the origin with radius r contains i linearly independent lattice vectors. The length of a basis $\boldsymbol{B}$ is $g(\boldsymbol{B})$, that is, $g(\boldsymbol{B}) = \max_i \|\boldsymbol{b}_i\|$, and $g(\boldsymbol{L})$ is the minimum value of $g(\boldsymbol{B})$ over all bases $\boldsymbol{B}$ of $\boldsymbol{L}$. Some important lattice problems are defined below, where $\gamma \geq 1$ is a function of rank:

SVP (Shortest Vector Problem): Given a lattice $\boldsymbol{L}$, find approximate nonzero lattice vector $\boldsymbol{v}$ such that $\|\boldsymbol{v}\| \leq \gamma \cdot \lambda_1(\boldsymbol{L})$.

S. Qing et al. (Eds.): ICICS 2015, LNCS 9543, pp. 37–49, 2016.
DOI: 10.1007/978-3-319-29814-6_4

CVP (Closest Vector Problem): Given a lattice $\boldsymbol{L}$ and a target vector $\boldsymbol{t}$, find a lattice point $\boldsymbol{v}$ such that $dist(\boldsymbol{v}, \boldsymbol{t}) \leq \gamma \cdot dist(\boldsymbol{L}, \boldsymbol{t})$.

SIVP (Shortest Independent Vector Problem): Given a lattice $\boldsymbol{L}$ of rank n, find n linearly independent lattice vector $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n$ such that $\|\boldsymbol{s}_i\| \leq \gamma \cdot \lambda_n(\boldsymbol{L}), i = 1, 2, \ldots, n$.

SBP (Shortest Basis Problem): Given a lattice $\boldsymbol{L}$, $\boldsymbol{L}$ is generated by basis $\boldsymbol{B}$, find an equivalent basis $\boldsymbol{B}'$ such that $g(\mathcal{L}(\boldsymbol{B}')) \leq \gamma \cdot g(\boldsymbol{L})$.

These lattice problems have been widely studied, and it is known that all of these problems are NP-hard [1,7,13,14]. Aharonov and Regev [3] showed that approximating SVP and CVP lie in $NP \cap coNP$ within a factor of $\sqrt{n}$. Goldreich and Goldwasser [11] showed that approximating SVP and CVP lie in $NP \cap coAM$ within a factor of $\sqrt{n/O(\log n)}$. Boppana et al. [8] found that approximating SVP and CVP within a factor of $\sqrt{n/O(\log n)}$ is not NP-hard unless the polynomial hierarchy collapses. Ajtai, Kumar and Sivakumar [2] proposed a sieve method for computing SVP under a randomized $2^{O(n)}$ time algorithm. Blömer and Seifert [7] proved that approximating SIVP and SBP within any constant factor are NP-hard and within a factor of $O(n/\sqrt{\log n})$ are $NP \cap coAM$. Guruswami et al. [12] proved that SIVP lies in $coAM$ within an improved approximation factor of $O(\sqrt{n/\log n})$ and is in $coNP$ within an approximation factor of $O(\sqrt{n})$. Blömer and Naewe [5] proposed the Generalized Shortest Vector Problem (GSVP) and gave polynomial-time reductions from SVP, CVP, SIVP, and SMP (Successive Minima Problem) to GSVP. They also proved that there exists a randomized algorithm in single-exponential time which approximates the GSVP within a factor of $1 + \epsilon$, where $0 < \epsilon \leq 2$, with success probability $1 - 2^{-\Omega(n)}$ for all ℓ_p norms. This result implies that in single-exponential time there exists an approximation algorithm for all above-mentioned lattice problems for all ℓ_p norms for $1 \leq p \leq \infty$. Micciancio [16] gave efficient reductions among approximation problems and showed that several lattice problems that are equivalent under polynomial-time rank-preserving reductions.

Transference theorems reflect relationships between the successive minima of a lattice and its dual lattice. As a consequence of transference theorems, it was shown in [15] that, under Karp reduction, $\text{SVP}_{O(n)}$ can not be NP-hard unless $NP = coNP$. Banaszczyk [4] proved that the following inequality: for a lattice $\boldsymbol{L}$ of rank n with dual lattice $\boldsymbol{L}^*$, $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}^*) \leq n$. Cai [9,10] generalized the transference theorems of Banaszcyk to obtain the following bounds relating the successive minima of a lattice with the minimum length of generating vectors of its dual: for a lattice $\boldsymbol{L}$ of rank n with dual lattice $\boldsymbol{L}^*$, $1 \leq \lambda_{n-i+1}(\boldsymbol{L}) \cdot g_i(\boldsymbol{L}^*) \leq C \cdot n$ for all $1 \leq i \leq n$ and some universal constant C. The lattice quantity $g_i(\boldsymbol{L})$ is defined as follows. First, $g(\boldsymbol{L})$ is the minimum value r such that the ball $\mathcal{B}(0, r)$ centered at 0 with radius r contains a set of linearly independent lattice vectors that generate the lattice $\boldsymbol{L}$. Define a saturated sublattice $\boldsymbol{L}'$ such that a sublattice $\boldsymbol{L}' \subset \boldsymbol{L}$ satisfies $\boldsymbol{L}' = \boldsymbol{L} \cap span(\boldsymbol{L}')$ [10]. Then, $g_i(\boldsymbol{L})$ is the minimum value r such that the sublattice generated by $\boldsymbol{L} \cap \mathcal{B}(0, r)$ contains an i dimensional saturated sublattice $\boldsymbol{L}'$ for $1 \leq i \leq dim(\boldsymbol{L})$.

From [10], $\lambda_i(\boldsymbol{L}) \cdot g_{n-i+1}(\boldsymbol{L}^*) \leq C \cdot n$ and $g_n(\boldsymbol{L}) = g(\boldsymbol{L})$ for all $1 \leq i \leq n$, the proof used the discrete Fourier transform and discrete potential functions.

Our Contributions. The first contribution is to present the promise problem GAPSAM associated with GSVP and construct new transference theorems for GAPSAM using the algorithm from [16] and properties of subspace. We obtain the following inequalities:

$$1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n, \tag{1}$$

$$1 \leq \lambda_M(\boldsymbol{L}) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n, \tag{2}$$

where n is the rank $\boldsymbol{L}_1$ and $\boldsymbol{L}_1^*$ is the dual of $\boldsymbol{L}_1$, c and d are constants. The subspace avoiding minimum $\lambda_M(\boldsymbol{L})$ of a lattice $\boldsymbol{L}$ with respect to some subspace $\boldsymbol{M} \subset span(\boldsymbol{L})$ is the smallest real number r such that there exists a vector in $\boldsymbol{L} \backslash \boldsymbol{M}$ of length at most r.

By Regev's result [17], we also prove that for a lattice $\boldsymbol{L}$ of rank l and a subspace $\boldsymbol{M} \subset span(\boldsymbol{L})$,

$$1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq n, \tag{3}$$

where $\boldsymbol{L}_1^*$ is the dual of a saturated rank n sublattice $\boldsymbol{L}_1$ of $\boldsymbol{L}$.

The inequality (2) is similar to Cai's, but our proof is simper. In [9,10], Cai presented the inequality $1 \leq \lambda_1(\boldsymbol{L}) \cdot g(\boldsymbol{L}^*) \leq C \cdot n$, which reflects the relationship between the shortest lattice vector of $\boldsymbol{L}$ and the shortest basis of the dual lattice $\boldsymbol{L}^*$. Our result, $1 \leq \lambda_M(\boldsymbol{L}) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n$, associates the minimum length of lattice vectors in $\boldsymbol{L} \backslash \boldsymbol{M}$ to the shortest basis of dual saturated sublattice $\boldsymbol{L}_1$ generated by intersecting $\boldsymbol{L}$ with a subspace $\boldsymbol{V} \subset span(\boldsymbol{L})$, where $\boldsymbol{V} \oplus \boldsymbol{M} = span(\boldsymbol{L})$.

By these results, we prove that GAPSAM_{cn} is in $coNP$, where c is a constant. We also give polynomial reductions between GAPSVP, GAPSIVP, and GAPSBP and GAPSAM. We also obtain the following inequalities: $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n$; $1 \leq \lambda_1(\boldsymbol{L}) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n$; $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq n$, where $\boldsymbol{L}_1^*$ is the dual of a saturated rank n sublattice $\boldsymbol{L}_1$ of $\boldsymbol{L}$. These inequalities show the relationships between the lattice and the dual of the saturated sublattice.

The second contribution is that for any $\gamma \geq 1$, we give a deterministic polynomial time rank-preserving reduction from GAPSAM_γ to GAPCVP_γ.

Micciancio [16] considered SVP$'$ as a variant of SVP which is a new less standard problem on lattices. The problem SVP$'$ is to minimize the norm $\|\boldsymbol{Bx}\|$ where $x = (x_1, \ldots, x_i, \ldots, x_n)$ and $x_i \neq 0$ for some i. Here, we propose the promise version GAPSVP$'$ for SVP$'$ and show that there exist rank and approximation preserving reductions from GAPSAM_γ to GAPSVP'_γ and GAPSVP'_γ to GAPCVP_γ. Hence, GAPSAM_γ can be reduced to GAPCVP_γ under deterministic polynomial time rank-preserving reduction.

Organization. The paper is organized as follows. In Sect. 2, we introduce basic notations for lattices and some promise versions of lattice problems. In Sect. 3, we first study of the promise problem GAPSAM for GSVP. Then, we present variants of transference theorems for GAPSAM. From these relationships, we give polynomial time reductions from GAPSAM to other lattice problems. In Sect. 4, we show that GAPSAM$_\gamma$ can be reduced to GAPCVP$_\gamma$.

2 Preliminaries

Let $\mathbb{R}^m$ be an m-dimensional Euclidean space. For every vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{R}^m$, the ℓ_2-norm of $\boldsymbol{x}$ is defined as $\|\boldsymbol{x}\|_2 = \sqrt{\sum_{i=1}^m x_i^2}$. The scalar product of two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_i x_i y_i$. dist($\boldsymbol{x}$,$\boldsymbol{L}$) is the minimum Euclidean distance from $\boldsymbol{x} \in \mathbb{R}^m$ to any vector in $\boldsymbol{L}$. All definitions and results in this paper are based on the ℓ_2 norm.

A lattice $\boldsymbol{L}$ is the set of all linear combinations generated by n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ in $\mathbb{R}^m (m \geq n)$, that is,

$$\boldsymbol{L} = \{\sum_{i=1}^n x_i \boldsymbol{b}_i | x_i \in \mathbb{Z}, 1 \leq i \leq n\}.$$

The integer n is the rank of the lattice and m is the dimension of the lattice. The sequence of linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$ is called a basis of the lattice. We can represent $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ as a matrix $\boldsymbol{B}$ with m rows and n columns, that is, $\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n] \in \mathbb{R}^{m \times n}$. The lattice $\boldsymbol{L}$ generated by a basis $\boldsymbol{B}$ is denoted by $\boldsymbol{L} = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$. A lattice has many different bases. Two matrices $\boldsymbol{B}$ and $\boldsymbol{B}'$ are two bases of the same lattice $\mathcal{L}$ if and only if $\boldsymbol{B} = \boldsymbol{B}'U$ for some unimodular matrix U. If $\mathcal{L}(\boldsymbol{S})$ is a sublattice of $\mathcal{L}(\boldsymbol{B})$, then any lattice point from the lattice $\mathcal{L}(\boldsymbol{S})$ also belongs to $\mathcal{L}(\boldsymbol{B})$. We denote this by $\mathcal{L}(\boldsymbol{S}) \subseteq \mathcal{L}(\boldsymbol{B})$.

For a lattice $\boldsymbol{L}$, the dual lattice $\boldsymbol{L}^*$ is a set of all vectors $\boldsymbol{y} \in \mathit{span}(\boldsymbol{L})$ that satisfy $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}$ for all $\boldsymbol{x} \in \boldsymbol{L}$, that is,

$$\boldsymbol{L}^* = \{\boldsymbol{y} \in \mathit{span}(\boldsymbol{L}) : \forall \boldsymbol{x} \in \boldsymbol{L}, \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z}\}.$$

The dual lattice $\boldsymbol{L}^*$ is a lattice.

Successive minima are fundamental constants of a lattice. The first successive minimum of a lattice $\boldsymbol{L}$, denoted by $\lambda_1(\boldsymbol{L})$, is the length of the shortest non-zero lattice vector. Formally, $\lambda_1(\boldsymbol{L}) = \mathit{min}\{\|\boldsymbol{x}\| : \boldsymbol{x} \in \boldsymbol{L} \backslash \{0\}\} = \mathit{min}_{\boldsymbol{x} \neq \boldsymbol{y} \in \boldsymbol{L}} \|\boldsymbol{x} - \boldsymbol{y}\|$. The ith minimum $\lambda_i(\boldsymbol{L})$ of a lattice $\boldsymbol{L}$ is the smallest value r such that $\mathcal{B}(0, r)$ contains i linearly independent lattice vectors, that is, $\lambda_i(\boldsymbol{L}) = \mathit{min}\{r : \mathit{dim}(\boldsymbol{L} \cap \mathcal{B}(0, r)) \geq i\}$ where $\mathcal{B}(0, r)$ is an open ball of radius r centered in $\boldsymbol{0}$.

Let $g(\boldsymbol{B})$ be the maximum length of vectors $\boldsymbol{b}_i$ in the basis $\boldsymbol{B}$, that is, $g(\boldsymbol{B}) = \max\limits_i \|\boldsymbol{b}_i\|$. We define $g(\boldsymbol{L})$ as the minimum value of $g(\boldsymbol{B})$ over all bases $\boldsymbol{B}$ of $\boldsymbol{L}$, that is, $g(\boldsymbol{L}) = \min\limits_{\boldsymbol{B}} g(\boldsymbol{B})$.

The following are several important lattice problems. Here we only concentrate on promise problems for approximate lattice problems.

Definition 1 (GAPSVP$_\gamma$)**.** *$(\boldsymbol{L}, r)$ is an instance of GAPSVP$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and $r \in \mathbb{Q}$ is a rational number, such that*

- *$(\boldsymbol{L}, r)$ is a YES instance if $\lambda_1(\boldsymbol{L}) \leq r$,*
- *$(\boldsymbol{L}, r)$ is a NO instance if $\lambda_1(\boldsymbol{L}) > \gamma \cdot r$.*

Definition 2 (GAPCVP$_\gamma$)**.** *$(\boldsymbol{L}, \boldsymbol{t}, r)$ is an instance of GAPCVP$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n, $\boldsymbol{t} \in \mathbb{Z}^m$ is a vector and $r \in \mathbb{Q}$ is a rational number, such that*

- *$(\boldsymbol{L}, \boldsymbol{t}, r)$ is a YES instance if $dist(\boldsymbol{L}, \boldsymbol{t}) \leq r$,*
- *$(\boldsymbol{L}, \boldsymbol{t}, r)$ is a NO instance if $dist(\boldsymbol{L}, \boldsymbol{t}) > \gamma \cdot r$.*

Definition 3 (GAPSIVP$_\gamma$)**.** *$(\boldsymbol{L}, r)$ is an instance of GAPSIVP$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and $r \in \mathbb{Q}$ is a rational number, such that*

- *$(\boldsymbol{L}, r)$ is a YES instance if $\lambda_n(\boldsymbol{L}) \leq r$,*
- *$(\boldsymbol{L}, r)$ is a NO instance if $\lambda_n(\boldsymbol{L}) > \gamma \cdot r$.*

Definition 4 (GAPSBP$_\gamma$)**.** *$(\boldsymbol{L}, r)$ is an instance of GAPSBP$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and generated by a basis $\boldsymbol{B}$ and $r \in \mathbb{Q}$ is a rational number, such that*

- *$(\boldsymbol{L}, r)$ is a YES instance if there exists an equivalent basis $\boldsymbol{B}'$ to $\boldsymbol{B}$ such that $g(\mathcal{L}(\boldsymbol{B}')) \leq r$,*
- *$(\boldsymbol{L}, r)$ is a NO instance if for all equivalent basis $\boldsymbol{B}'$ to $\boldsymbol{B}$ has $g(\mathcal{L}(\boldsymbol{B}')) > \gamma \cdot r$.*

Definition 5 (SVP$'$ [16])**.** *Given a lattice $\boldsymbol{B} \in \mathbb{Z}^{m \times n}$ and an index $i \in \{1, \ldots, n\}$, find a lattice vector $\boldsymbol{Bx}$ with $x_i \neq 0$ such that $\|\boldsymbol{Bx}\| \leq \gamma min\{\|\boldsymbol{Bx}\| : x_i \neq 0\}$.*

We now propose the promise problem GAPSVP$'$ associated to the approximate problem SVP$'$.

Definition 6 (GAPSVP$'_\gamma$)**.** *$(\boldsymbol{L}, i, r)$ is an instance of GAPSVP$'_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and generated by a basis $\boldsymbol{B}$ and $r \in \mathbb{Q}$ is a rational number, such that*

- *$(\boldsymbol{L}, i, r)$ is a YES instance if $\lambda_1^{(i)}(\boldsymbol{L}) \leq r$, i.e. there exists a vector $\boldsymbol{x} \in \mathbb{Z}^n$ with $x_i \neq 0$ such that $\|\boldsymbol{Bx}\| \leq r$,*
- *$(\boldsymbol{L}, i, r)$ is a NO instance if $\lambda_1^{(i)}(\boldsymbol{L}) > \gamma \cdot r$, i.e. for all vectors $\boldsymbol{x} \in \mathbb{Z}^n$ with $x_i \neq 0$ such that $\|\boldsymbol{Bx}\| > \gamma \cdot r$.*

where $\lambda_1^{(i)}(\boldsymbol{L}) = \min_{\boldsymbol{x} \in \mathbb{Z}^n} \{\|\boldsymbol{Bx}\| : x_i \neq 0\}$.

The next definition is a new lattice problem proposed in [6] where reductions from SVP, CVP, SIVP, and SMP to GSVP are given.

Definition 7 (GSVP)**.** *Given a lattice $\boldsymbol{L} \subseteq \mathbb{Z}^m$ and a linear subspace $\boldsymbol{M} \subset span(\boldsymbol{L})$, the goal is to find a vector $\boldsymbol{v} \in \boldsymbol{L} \backslash \boldsymbol{M}$ such that $\|\boldsymbol{v}\| \leq \gamma \cdot dist(0, \boldsymbol{L} \backslash \boldsymbol{M})$.*

We set

$$\lambda_M(\boldsymbol{L}) = min\{r \in \mathbb{R} | \exists\ \boldsymbol{v} \in \boldsymbol{L} \backslash \boldsymbol{M}, \|\boldsymbol{v}\| \leq r\}$$

and call this the subspace avoiding minimum (SAM).

It is clear that SVP is a special case of GSVP when $\boldsymbol{M} = \{0\}$, we have $\lambda_M(\boldsymbol{L}) = \lambda_1(\boldsymbol{L})$. So, there is a trivial reduction from SVP$_\gamma$ to GSVP$_\gamma$.

3 The Transference Theorems for GAPSAM

In this section, we first propose the promise problem (GAPSAM) associated to GSVP and present new transference theorems for GAPSAM.

3.1 The Variants of Cai's Transference Theorems

Definition 8 (GAPSAM$_\gamma$)**.** $(\boldsymbol{L}, \boldsymbol{M}, r)$ *is an instance of GAPSAM$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n, $\boldsymbol{M}$ is a linear subspace of span($\boldsymbol{L}$), $r \in \mathbb{Q}$ is a rational number, such that*

- $(\boldsymbol{L}, \boldsymbol{M}, r)$ *is a YES instance if* $\lambda_M(\boldsymbol{L}) \leq r$*,*
- $(\boldsymbol{L}, \boldsymbol{M}, r)$ *is a NO instance if* $\lambda_M(\boldsymbol{L}) > \gamma \cdot r$*.*

Banaszcyk [4], Cai [10], and Regev [17] proved that the following theorem.

Theorem 1. *For any rank-n lattice $\boldsymbol{L}$, its dual lattice is $\boldsymbol{L}^*$, there exist constants c, d such that*

1. $\lambda_1(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}^*) \leq c \cdot n.$
2. $1 \leq \lambda_1(\boldsymbol{L}) \cdot g(\boldsymbol{L}^*) \leq d \cdot n.$
3. $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}^*) \leq n.$

We also need the following lemma.

Lemma 1 [16] . There is a polynomial time algorithm that on input a lattice basis $\boldsymbol{B} = [\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n] \in \mathbb{Q}^{m \times n}$ and a linear subspace $\boldsymbol{S}$, outputs a new basis $\widetilde{\boldsymbol{B}} = [\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_d]$ for $\mathcal{L}(\boldsymbol{B})$ such that $\mathcal{L}(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_d) = \boldsymbol{S} \cap \mathcal{L}(\boldsymbol{B})$, where d is the dimension of $\boldsymbol{S} \cap span(\boldsymbol{B})$.

Combining Lemma 1 with Theorem 1, we immediately obtain the following theorem about $\lambda_M(\boldsymbol{L})$. The first two parts in the following theorem are variants of Cai's result [10]. We prove this independently with a simple method.

Theorem 2. *For any rank-l lattice $\boldsymbol{L}$ and a subspace $\boldsymbol{M} \subset span(\boldsymbol{L})$, there exist constants $c > 0$, $d > 0$ such that*

1. $1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n.$
2. $1 \leq \lambda_M(\boldsymbol{L}) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n.$
3. $1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq n.$

where $\boldsymbol{L}_1^*$ is the dual of saturated sublattice $\boldsymbol{L}_1$ with rank n of $\boldsymbol{L}$.

Proof. Assume the lattice $\boldsymbol{L}$ is generated by a basis $\boldsymbol{B} \in \mathbb{Z}^{m \times l}$. Because $\boldsymbol{M}$ is a subspace of span($\boldsymbol{L}$), $rank(\boldsymbol{M}) < rank(span(\boldsymbol{L}))$. Note that, by the properties of subspaces, there must exists a subspace $\boldsymbol{V}$ such that

$$\boldsymbol{V} \oplus \boldsymbol{M} = span(\boldsymbol{L}).$$

Run the algorithm from Lemma 1 on the lattice $\boldsymbol{L}$ and the subspace $\boldsymbol{V}$ to obtain a lattice basis $\widetilde{\boldsymbol{B}} = [\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n] \in \mathbb{Z}^{m\times n}$ for $\boldsymbol{L}$, such that $\mathcal{L}(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n) = \boldsymbol{V} \cap \boldsymbol{L}$, where $n = dim(\boldsymbol{V} \cap span(\boldsymbol{L}))$.

Clearly, the two bases $\boldsymbol{B}$ and $\widetilde{\boldsymbol{B}}$ are equivalent, that is, $\widetilde{\boldsymbol{B}} = \boldsymbol{B}U$ for some unimodular matrix U. Let $\mathcal{L}(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n) = \boldsymbol{L}_1$. Using Theorem 1 for a lattice $\boldsymbol{L}_1$ of rank n, we obtain the inequality:

$$\lambda_1(\boldsymbol{L}_1) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n.$$

Furthermore, we need to prove that $1 \leq \lambda_1(\boldsymbol{L}_1) \cdot \lambda_n(\boldsymbol{L}_1^*)$. Let $v \in \boldsymbol{L}_1$ be a vector such that $\|v\| = \lambda_1(\boldsymbol{L}_1)$. By definition of $\lambda_n(\boldsymbol{L}_1^*)$, there exist n linearly independent vectors $x_1, \ldots, x_n$ in $\boldsymbol{L}_1^*$ such that $\|x_i\| \leq \lambda_n(\boldsymbol{L}_1^*)$. We clearly see that not all of them are orthogonal to v. Hence, there exists an i such that $\langle x_i, v\rangle \neq 0$. Since $x_i \in \boldsymbol{L}_1^*$ there must be $\langle x_i, v\rangle \in \mathbb{Z}$. We have $1 \leq \langle x_i, v\rangle \leq \|x_i\| \cdot \|v\| \leq \lambda_n(\boldsymbol{L}_1^*) \cdot \lambda_1(\boldsymbol{L}_1)$. Then,

$$\lambda_1(\boldsymbol{L}_1) \cdot \lambda_n(\boldsymbol{L}_1^*) \geq 1.$$

Because $\lambda_1(\boldsymbol{L}_1)$ is the shortest non-zero vector of the saturated sublattice $\boldsymbol{L}_1 \subset \boldsymbol{L}$ generated by $\boldsymbol{L} \cap \boldsymbol{V}$ and $\lambda_M(\boldsymbol{L})$ is the shortest non-zero vector of the lattice $\boldsymbol{L}\backslash\boldsymbol{M}$, we have $\lambda_M(\boldsymbol{L}) \leq \lambda_1(\boldsymbol{L}_1)$. Therefore

$$1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n.$$

The proofs of 2 and 3 similar. For the lattice $\boldsymbol{L}_1$, we have $1 \leq \lambda_1(\boldsymbol{L}_1) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n$ and $1 \leq \lambda_1(\boldsymbol{L}_1) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq d \cdot n$. Because $\lambda_M(\boldsymbol{L}) \leq \lambda_1(\boldsymbol{L}_1)$, the results follow. This completes the proof.

Since $\lambda_1(\boldsymbol{L}) \leq \lambda_M(\boldsymbol{L})$, we obtain the following corollary.

Corollary 1. *For any rank-l lattice $\boldsymbol{L}$ and a subspace $\boldsymbol{M} \subset span(\boldsymbol{L})$, there exist constants c, d such that*

1. $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_n(\boldsymbol{L}_1^*) \leq c \cdot n.$
2. $1 \leq \lambda_1(\boldsymbol{L}) \cdot g(\boldsymbol{L}_1^*) \leq d \cdot n.$
3. $1 \leq \lambda_1(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq n.$

where $\boldsymbol{L}_1^*$ is the dual of saturated sublattice $\boldsymbol{L}_1$ with rank n of $\boldsymbol{L}$.

This corollary reflects the relationships between the shortest lattice vector of $\boldsymbol{L}$ and the nth successive minimum, the shortest basis, and the first successive minimum of the dual of a saturated sublattice $\boldsymbol{L}_1$. That is, it connects the lattice with the dual lattice of a saturated sublattice.

Part 1 of Theorem 2 immediately implies reductions between GAPSIVP and GAPSAM.

Theorem 3. *There are the following cook reductions between problem GAPSIVP and GAPSAM:*

- *The problem GAPSAM$_{cn}$ can be reduced to GAPSIVP$_1$;*
- *The problem GAPSIVP$_{cn}$ can be reduced to GAPSAM$_1$,*

where c is a constant.

Proof. Let $(\boldsymbol{L}, \boldsymbol{M}, r)$ be an instance of GAPSAM$_{cn}$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank l, and let $\boldsymbol{M} \subset span(\boldsymbol{L})$ be a subspace of $\boldsymbol{L}$. Note that $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance if $\lambda_M(\boldsymbol{L}) \leq r$, whereas $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance if $\lambda_M(\boldsymbol{L}) > cnr$.

From the proof of Theorem 2, we can obtain a lattice $\boldsymbol{L}_1$ of rank n with the dual $\boldsymbol{L}_1^*$. By Theorem 2, if $\lambda_M(\boldsymbol{L}) \leq r$ then $\lambda_n(\boldsymbol{L}_1^*) \geq 1/\lambda_M(\boldsymbol{L}) > 1/r$, if $\lambda_M(\boldsymbol{L}) > cnr$ then $\lambda_n(\boldsymbol{L}_1^*) \leq cn/\lambda_M(\boldsymbol{L}) < cn/cnr < 1/r$.

The reduction calls a GAPSIVP$_1$ oracle on $(\boldsymbol{L}_1^*, 1/r)$, which allows GAPSAM$_{cn}$ to be solved. Indeed, if the GAPSIVP$_1$ oracle on $(\boldsymbol{L}_1^*, 1/r)$ answers YES, then $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance of GAPSAM$_{cn}$. On the other hand, if GAPSIVP$_1$ oracle on $(\boldsymbol{L}_1^*, 1/r)$ answers NO, then $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance of GAPSAM$_{cn}$.

The second reduction follows by a similar method.

Using Theorem 3, we can also show the non-approximability result for GAPSAM, namely that there exists a constant c such that GAPSAM$_{cn}$ $\in coNP$.

Corollary 2. *GAPSAM$_{cn}$ $\in coNP$ for some constant c.*

Proof. Assume that $(\boldsymbol{L}, \boldsymbol{M}, r)$ is an instance of GAPSAM$_{cn}$. Then $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance if $\lambda_M(\boldsymbol{L}) \leq r$, and $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance if $\lambda_M(\boldsymbol{L}) > cnr$. Hence, we need to prove that if $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance then there is no witness that the verifier accepts, and that if $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance then there is a witness that the verifier accepts.

Indeed, using Theorem 3, when $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance of GAPSAM$_{cn}$ we have $\lambda_n(\boldsymbol{L}_1^*) > 1/r$, and when $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance we have $\lambda_n(\boldsymbol{L}_1^*) \leq 1/r$.

We then obtain n vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$ non-deterministically, and check that they are linearly independent in $\boldsymbol{L}_1^*$ and that each length at most $1/r$. Hence, there exist n vectors for which we accept a NO instance of GAPSAM$_{cn}$.

3.2 Relationships Between GAPSAM and Other Lattice Problems

In this section, we give polynomial time reductions between promise problems of GAPSVP, GAPSBP and GAPSAM.

Theorem 4. *There are polynomial time Karp reductions between GAPSVP and GAPSAM.*

- *GAPSVP$_n$ is reducible to GAPSAM$_1$.*
- *GAPSAM$_n$ is reducible to GAPSVP$_1$.*

Proof. Let $(\boldsymbol{L}_1^*, r)$ be an instance of GAPSVP$_n$, where $\boldsymbol{L}_1^* \subset \mathbb{Z}^m$ is a lattice. $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*$ be a basis of the lattice $\boldsymbol{L}_1^*$, and let $\boldsymbol{L}_1$ be the dual lattice of $\boldsymbol{L}_1^*$. We may assume that $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ is a basis of $\boldsymbol{L}_1$, so there must exist a lattice

$\boldsymbol{L}$ of rank l such that $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ is a basis of $\boldsymbol{L} \cap span(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, that is, $\boldsymbol{L}_1 = \boldsymbol{L} \cap span(\boldsymbol{L}_1)$. Thus L has a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_l$.

Set $\boldsymbol{V} = span(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$. Then $\boldsymbol{V}$ is a subspace of $span(\boldsymbol{L})$ and $\boldsymbol{L}_1$ is a saturated sublattice of $\boldsymbol{L}$. Define the orthogonal projection

$$\pi : span(\boldsymbol{L}) \longrightarrow span(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)^{\perp}$$

as following, for all $\boldsymbol{b} \in span(\boldsymbol{L})$,

$$\pi(\boldsymbol{b}) = \boldsymbol{b} - \sum_{i=1}^{n} \frac{\langle \boldsymbol{b}, \tilde{\boldsymbol{b}_i} \rangle}{\langle \tilde{\boldsymbol{b}_i}, \tilde{\boldsymbol{b}_i} \rangle} \tilde{\boldsymbol{b}_i}$$

where $\tilde{\boldsymbol{b}_i}$ is the Gram-Schmidt orthogonal vector of $\boldsymbol{b}_i$, $i = 1, \ldots, n$. $\pi(\boldsymbol{L})$ is a lattice of rank $l - n$ with basis $[\pi(\boldsymbol{b}_{n+1}), \ldots, \pi(\boldsymbol{b}_l)]$, where $\boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_l \in \boldsymbol{L}$. Then, we see that $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{n+1}, \ldots, \boldsymbol{b}_l$ is a basis of the lattice $\boldsymbol{L}$. In the linear span of lattice $\boldsymbol{L}$, we can find a subspace $\boldsymbol{M}$ such that $\boldsymbol{V} \oplus \boldsymbol{M} = span(\boldsymbol{L})$.

The output of the reduction is $(\boldsymbol{L}, \boldsymbol{M}, 1/r)$. We next show this reduction is correct.

Assume that $(\boldsymbol{L}_1^*, r)$ is a YES instance of GAPSVP$_n$, such that $\lambda_1(\boldsymbol{L}_1^*) \leq r$. From the Theorem 2, $1 \leq \lambda_M(\boldsymbol{L}) \cdot \lambda_1(\boldsymbol{L}_1^*) \leq n$. We have $\lambda_M(\boldsymbol{L}) \geq 1/r$. Then, $(\boldsymbol{L}, \boldsymbol{M}, 1/r)$ is a NO instance of GAPSAM$_\gamma$.

Now assume that $(\boldsymbol{L}_1^*, r)$ is a NO instance of GAPSVP$_n$, so that $\lambda_1(\boldsymbol{L}_1^*) > nr$. By Theorem 2, we have $\lambda_M(\boldsymbol{L}) < 1/r$. It follows that $(\boldsymbol{L}, \boldsymbol{M}, 1/r)$ is a YES instance of GAPSAM$_\gamma$.

The proof of the second part is similar.

Using Theorem 2, we obtain the following corollary.

Corollary 3. *There are approximate reductions between GAPSBP and GAPSAM, for some constant d.*

- *GAPSAM$_{dn}$ can be reduced to GAPSBP$_1$.*
- *GAPSBP$_{dn}$ can be reduced to GAPSAM$_1$.*

4 The Rank and Approximation Preserving Reductions

In this section, we will establish the rank and approximation preserving reduction between GAPSAM and other lattice problems.

Theorem 5. *For any approximation factor γ, there is a deterministic polynomial time rank-preserving reduction from GAPSVP$_\gamma$ to GAPSAM$_\gamma$.*

Proof. Let $(\boldsymbol{L}, r)$ be an instance of GAPSVP$_\gamma$, and define GAPSAM$_\gamma$ instance $(\boldsymbol{L}, \boldsymbol{M}, r)$, where $\boldsymbol{M} = \{0\} \subseteq span(\boldsymbol{L})$. If we computer a shortest non-zero lattice vector in $\boldsymbol{L}$, we compute a shortest lattice vector in $\boldsymbol{L} \backslash \boldsymbol{M}$, i.e., $\lambda_M(\boldsymbol{L}) = \lambda_1(\boldsymbol{L})$. So there is a trivial reduction from GAPSVP$_\gamma$ to GAPSAM$_\gamma$.

In the following, we will give a deterministic polynomial time rank-preserving reduction from GAPSAM to GAPCVP by an intermediate problem GAPSVP$'$.

Theorem 6. *For any approximation factor γ, there is a deterministic polynomial time rank-preserving reduction from GAPSAM$_\gamma$ to GAPSVP$'_\gamma$.*

Proof. Let $(\boldsymbol{L}, \boldsymbol{M}, r)$ be an instance of GAPSAM$_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and $\boldsymbol{L}$ is generated by a basis $\boldsymbol{B} = (\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$, and let $\boldsymbol{M} \subset span(\boldsymbol{L})$ be a subspace. Using the algorithm from Lemma 1, the algorithm that on input a lattice $\boldsymbol{L}$ and a subspace $\boldsymbol{M}$, outputs a new basis $\widetilde{\boldsymbol{B}} = [\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n]$ for $\boldsymbol{L}$ such that $\boldsymbol{M} \cap \boldsymbol{L} = \mathcal{L}(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_d)$, where d is the dimension of $\boldsymbol{M} \cap span(\boldsymbol{L})$, then $\boldsymbol{M} = span(\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_d)$. We have $\boldsymbol{L} = \mathcal{L}(\boldsymbol{B}) = \mathcal{L}(\widetilde{\boldsymbol{B}})$, for any lattice vector in $\boldsymbol{L}$ can be represented by the integral combinations of n linearly independent vectors $\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n$. Hence, on input an GAPSAM$_\gamma$ instance $(\boldsymbol{L}, \boldsymbol{M}, r)$, the reduction outputs the GAPSVP$'_\gamma$ instance $(\boldsymbol{L}, i, r)$ where $i \in \{d+1, \ldots, n\}$. We prove that the reduction is correct.

First assume that $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a YES instance of GAPSAM$_\gamma$, $\lambda_M(\boldsymbol{L}) \leq r$, i.e., there exists a vector $\boldsymbol{x} = (x_1, \ldots, x_d, x_{d+1}, \ldots, x_n) \in \mathbb{Z}^n$ with $x_i \neq 0$, $i \in \{d+1, \ldots, n\}$ such that

$$\|\widetilde{\boldsymbol{B}}\boldsymbol{x}\| = \|x_1\tilde{\boldsymbol{b}}_1 + \ldots + x_d\tilde{\boldsymbol{b}}_d + x_{d+1}\tilde{\boldsymbol{b}}_{d+1} + \ldots + x_n\tilde{\boldsymbol{b}}_n\| \leq r.$$

For any vector $\boldsymbol{x'} = (x'_1, \ldots, x'_d, x'_{d+1}, \ldots, x'_n) \in \mathbb{Z}^n$ with $x'_i \neq 0$, $i \in \{d+1, \ldots, n\}$, we have

$$\lambda_1^{(i)}(\boldsymbol{L}) = \min_{x' \in \mathbb{Z}^n, x'_i \neq 0} \{\|\widetilde{\boldsymbol{B}}\boldsymbol{x'}\|\} \leq \|\widetilde{\boldsymbol{B}}\boldsymbol{x}\| \leq r.$$

This prove that $(\boldsymbol{L}, i, r)$ is a YES instance.

Now assume that $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance, $\lambda_M(\boldsymbol{L}) > \gamma \cdot r$, i.e., for all vectors $\boldsymbol{x} = (x_1, \ldots, x_d, x_{d+1}, \ldots, x_n) \in \mathbb{Z}^n$ with $x_i \neq 0$, $i \in \{d+1, \ldots, n\}$ such that $\|\widetilde{\boldsymbol{B}}\boldsymbol{x}\| > \gamma \cdot r$. First assume for contradiction that $(\boldsymbol{L}, i, r)$ is not a NO instance, i.e., there exists a vector $\boldsymbol{x'} = (x'_1, \ldots, x'_d, x'_{d+1}, \ldots, x'_n) \in \mathbb{Z}^n$ with $x'_i \neq 0$, $i \in \{d+1, \ldots, n\}$, hence, $\|\widetilde{\boldsymbol{B}}\boldsymbol{x'}\| \leq \gamma \cdot r$. Since $(\boldsymbol{L}, \boldsymbol{M}, r)$ is a NO instance of GAPSAM$_\gamma$, we have $\|\widetilde{\boldsymbol{B}}\boldsymbol{x'}\| > \gamma \cdot r$, contradicting the fact that $(\boldsymbol{L}, i, r)$ is not a NO instance of GAPSVP$'_\gamma$. Then, this proved that $(\boldsymbol{L}, i, r)$ is a NO instance.

Theorem 7. *For any approximation factor γ, there is a deterministic polynomial time rank-preserving reduction from GAPSVP$'_\gamma$ to GAPCVP$_\gamma$.*

Proof. Let $(\boldsymbol{L}, i, r)$ be an instance of GAPSVP$'_\gamma$, where $\boldsymbol{L} \subseteq \mathbb{Z}^m$ is a lattice of rank n and $\boldsymbol{L}$ is generated by a basis $\boldsymbol{B} = (\boldsymbol{b_1}, \ldots, \boldsymbol{b_n})$. We construct instances of GAPCVP$_\gamma$ as follows. The ides is to use the reduction from GCVP$_\gamma$ (Generalized Closest Vector Problem) to CVP$_\gamma$ of [16]. The jth instance consists of a lattice $\boldsymbol{L}^{(j)} = \mathcal{L}(\boldsymbol{B}^{(j)}) = \mathcal{L}(\boldsymbol{b_1}, \ldots, 2^{j+1}\boldsymbol{b_i}, \ldots, \boldsymbol{b_n})$ and the target vector $t^{(j)} = 2^j\boldsymbol{b_i}$, $j = 0, 1, \ldots, \lfloor \log_2 A \rfloor$(A is sufficiently large and the bound can be determined (see [16] (Theorem 3.2)). We use these instances of GAPCVP$_\gamma$

corresponding queries to the GAPCVP$_\gamma$ oracle. By call on all these instances $(\boldsymbol{L}^{(j)}, t^{(j)})$, the GAPCVP$_\gamma$ oracle return the shortest difference vectors. Since r is given in GAPSVP$'_\gamma$ instance $(\boldsymbol{L}, i, r)$, and return YES if and only if at least one of the oracle calls is answered by YES. For example, the jth call on input $(\boldsymbol{L}^{(j)}, t^{(j)})$, the shortest of the vector $\boldsymbol{B}^{(j)}\boldsymbol{x} - t^{(j)} \in \boldsymbol{L}$ is returned where $x = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in \mathbb{Z}^n$ and

$$\begin{aligned}\|\boldsymbol{B}^{(j)}\boldsymbol{x} - t^{(j)}\| &= \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + x_i \cdot 2^{j+1}\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n - 2^j\boldsymbol{b}_i\| \\ &= \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + 2^j(2x_i - 1)\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n\| \\ &\leq \gamma.\end{aligned}$$

Since $x_i \in \mathbb{Z}^n$, we have $2^j(2x_i - 1) \neq 0$. There exists a vector $\boldsymbol{x}' = (x_1, x_2, \ldots, x'_i, \ldots, x_n) \in \mathbb{Z}^n$ with $x'_i = 2^j(2x_i - 1) \neq 0$ for some $i \in \{1, \ldots, n\}$ such that $\|\boldsymbol{B}^{(j)}\boldsymbol{x} - t^{(j)}\| = \|\boldsymbol{B}\boldsymbol{x}'\| \leq r$. Then, $(\boldsymbol{L}, i, r)$ is a YES instance of GAPSVP$'_\gamma$. And selecting j is the hight power of 2 such that 2^j divides x_i. The reduction outputs the GAPCVP$_\gamma$ instance $(\boldsymbol{L}^{(j)}, t^{(j)}, r)$.

We want to prove that if $(\boldsymbol{L}, i, r)$ is a YES instance then $(\boldsymbol{L}^{(j)}, t^{(j)}, r)$ is a YES instance for some $j = 1, \ldots, n$, while if $(\boldsymbol{L}, i, r)$ is a NO instance then $(\boldsymbol{L}^{(j)}, t^{(j)}, r)$ is a NO instance for all $j = 1, \ldots, n$.

First assume $(\boldsymbol{L}, i, r)$ is a YES instance, $\lambda_1^{(i)}(\boldsymbol{L}) \leq r$, i.e., there exists a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in \mathbb{Z}^n$ with $x_i \neq 0$, $i \in \{1, \ldots, n\}$ such that $\|\boldsymbol{B}\boldsymbol{x}\| \leq r$. Let j be the hight power of 2 such that 2^j divides x_i. Since x_i is nonzero, we define $x_i = 2^j(2a-1)$ for some integer a. We obtain the vector $\boldsymbol{x}'$ by replacing the ith entry x_i with a, i.e., $\boldsymbol{x}' = (x_1, x_2, \ldots, a, \ldots, x_n) \in \mathbb{Z}^n$. Then,

$$\begin{aligned}dist(\boldsymbol{L}^{(j)}, t^{(j)}) &\leq \|\boldsymbol{B}^{(j)}\boldsymbol{x}' - t^{(j)}\| \\ &= \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + a \cdot 2^{j+1}\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n - 2^j\boldsymbol{b}_i\| \\ &= \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + \cdot 2^j(2a - 1)\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n\| \\ &= \|\boldsymbol{B}\boldsymbol{x}\| \leq r.\end{aligned}$$

This proves that $(\boldsymbol{L}^{(j)}, t^{(j)}, r)$ is a YES instance.

Now assume that $(\boldsymbol{L}, i, r)$ is a NO instance, $\lambda_1^{(i)}(\boldsymbol{L}) > \gamma \cdot r$, i.e., for any vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in \mathbb{Z}^n$ with $x_i \neq 0$, $i \in \{1, \ldots, n\}$ such that $\|\boldsymbol{B}\boldsymbol{x}\| > \gamma \cdot r$. For some j,

$$\begin{aligned}dist(\boldsymbol{L}^{(j)}, t^{(j)}) &= \min_{\boldsymbol{x} \in \mathbb{Z}^n} \|\boldsymbol{B}^{(j)}\boldsymbol{x} - t^{(j)}\| \\ &= \min_{\boldsymbol{x} \in \mathbb{Z}^n} \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + x_i \cdot 2^{j+1}\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n - 2^j\boldsymbol{b}_i\| \\ &= \min_{\boldsymbol{x} \in \mathbb{Z}^n} \|x_1\boldsymbol{b}_1 + x_2\boldsymbol{b}_2 + \ldots + 2^j(2x_i - 1)\boldsymbol{b}_i + \ldots + x_n\boldsymbol{b}_n\| \\ &> \gamma \cdot r.\end{aligned}$$

This proves that $(\boldsymbol{L}^{(j)}, t^{(j)}, r)$ is a NO instance.

Combining the two theorem we get the following corollary.

Corollary 4. *For any approximation factor γ, there is a deterministic polynomial time rank-preserving reduction from GAPSAM$_\gamma$ to GAPCVP$_\gamma$.*

5 Conclusions

In this paper, we propose the promise problem associated with GSVP, namely GAPSAM. We present variants of Cai's transference theorems for GAPSAM. From the relationship, we prove that GAPSAM$_{cn}$ lies in $coNP$, where c is a constant. We also give the relationships between the shortest vector of a lattice, the nth successive minima, shortest basis, and the shortest vector of the dual of a saturated sublattice. Using these new relations, we reduce some lattice problems to GAPSAM. We also reduce GAPSAM to GAPCVP under a deterministic polynomial time rank-preserving reduction.

References

1. Ajtai, M.: The shortest vector problem in l2 is NP-hard for randomized reductions. In: 30th ACM Symposium on Theory of Computing, pp. 10–19 (1998)
2. Ajtai, M., Kumar, R., Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the 33th ACM Symposium on Theory of Computing, pp. 601–610 (2001)
3. Aharonov, D., Regev, O.: Lattice problems in NP intersect coNP. J. ACM **52**(5), 749–765 (2005). Preliminary version in FOCS04
4. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. Math. Ann. **296**, 625–635 (1993)
5. Blömer, J., Naewe, S.: Sampling methods for shortest vectors, closest vectors and successive minima. Theor. Comput. Sci. **410**, 1648–1665 (2009)
6. 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)
7. Blöer, J., Seifert, J.P.: On the complexity of computing short linearly independent vectors and short bases in a lattice. In: Thirty-First Annual ACM Symposium on Theory of Computing, pp. 711–720. ACM (1999)
8. Boppana, R., Håstad, J., Zachos, S.: Does co-NP have short interactive proofs? Inf. Process. Lett. **25**, 127–132 (1987)
9. Cai, J.Y.: A New Transference Theorem and Applications to Ajtais Connection Factor, Electronic Colloquium on Computational Complexity, TR, pp. 98–05 (1998)
10. Cai, J.Y.: A new transference theorem in the geometry of numbers and new bounds for Ajtais connection factor. Discrete Appl. Math. **126**, 9–31 (2003)
11. Goldreich, O., Goldwasser, S.: On the limits of nonapproximability of lattice problems. J. Comput. Syst. Sci. **60**(3), 540–563 (2000)
12. Guruswami, V., Micciancio, D., Regev, O.: The complexity of the covering radius problem on lattices and codes. Comput. Complexity **14**(2), 90–121 (2005). Preliminary version in CCC 2004
13. Haviv, I., Regev, O.: Tensor-based hardness of the shortest vector problem to within almost polynomial factors. Theory Comput. **8**, 513–531 (2012)
14. Khot, S.: Hardness of approximating the shortest vector problem in lattices. J. ACM **52**(5), 789–808 (2005)
15. Lgarias, C., Lenstra, H., Schnorr, C.P.: Korkin-Zolotarev bases and successive minima of a lattice and its reciprocial lattice. Combinatorica **10**, 333–348 (1990)

16. Micciancio, D.: Efficient reductions among lattice problems. In: 19th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2008, pp. 84–93. Society for Industrial and Applied Mathematics (2008)
17. Regev, O.: Lecture Note on Lattices in Computer Science. Lecture 8: Dual Lattice (2004)