The Search Successive Minima Problem Is Equivalent to Its Optimization Version

Haoyu Li[1,2,3] and Yanbin Pan[1,2(✉)]

[1] Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
panyanbin@amss.ac.cn
[2] Science and Technology on Communication Security Laboratory, Chengdu 610041, China
[3] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
lihaoyu14@mails.ucas.ac.cn

Abstract. The shortest vector problem (SVP) and the shortest independent vectors problem (SIVP) are two famous problems in lattices, which are usually used to evaluate the hardness of some computational problems related to lattices. It is well known that the search-SVP is equivalent to its optimization version. However, it seems very difficult to prove the equivalence between search-SIVP and optimization-SIVP. In this paper, we revisit the Successive Minima Problem (SMP), which is proved the equivalence relation with SIVP. Naturally we will consider its optimization version as to find all successive minima of a given lattice, and finally we will prove that it is equivalent to its search version.

Keywords: Lattice · Successive minima · SMP · SVP · SIVP

1 Introduction

Since Ajtai's seminal work [1] in 1996, lattice-based cryptosystems become more and more popular due to their potential ability to resist the quantum computer attack and successful applications in constructing important cryptographic primitives: such as the hash functions [1,19,20,23], the digital signature schemes [4,9,13], the encryption schemes [3,11,14,25], and the fully homomorphic encryption schemes [7,10].

Another attractive feature of lattice-based cryptosystems is their average-case security can be based on the worst-case hardness of some lattice problems,

This work was supported in part by the NNSF of China (No. 61572490, and No. 11471314), the National Center for Mathematics and Interdisciplinary Sciences, CAS, and Science and Technology on Communication Security Laboratory (No. 9140C110301150C11051).

© Springer International Publishing AG, part of Springer Nature 2018
B. B. Kang and T. Kim (Eds.): WISA 2017, LNCS 10763, pp. 39–50, 2018.
https://doi.org/10.1007/978-3-319-93563-8_4

which are typically some approximation variants of the shortest vector problem (SVP) and the shortest independent vectors problem (SIVP).

SVP refers to the problem of finding a shortest non-zero vector in a given lattice, and its hardness has been studied widely [2,6,8,12]. Interestingly, there are three variants of SVP: search-SVP, optimization-SVP, and decisional-SVP, which aim to find a shortest nonzero vector, find the length of the shortest vector, and decide whether the shortest vector is shorter than some given number respectively. It is well known that the three variants of SVP are equivalent to each other (see [22]). In fact, it is obvious that if we could solve search-SVP then we can solve the other two problems. Moreover, it is easy to show the equivalence between decisional-SVP and optimization-SVP. However, reducing search-SVP to optimization-SVP is not an easy task.

The first efficient reduction from search-SVP to optimization-SVP was presented by Kannan [18] in 1987. However, the reduction is not rank-preserving, since it needs the optimization-SVP oracle to deal with some lower rank lattices, besides the lattices with the same rank as the original lattice. Moreover, the reduction invokes the optimization-SVP oracle for polynomial times. In 2013, Hu and Pan [16] revisited the reduction and presented a rank-preserving reduction which can solve search-SVP with only one call to the optimization-SVP oracle.

When considering the relations between search-SIVP and optimization-SIVP, it becomes a bit more complicated. Search-SIVP refers to the question of finding n linearly independent vectors in a given n-rank lattice $\mathcal{L}$ such that the maximal length of the vectors is as small as possible. In fact, denote by $\lambda_i(\mathcal{L})(1 \leq i \leq n)$ the successive minima, that is, the minimum length of a set of i linearly independent vectors in $\mathcal{L}$, where the length of a set is defined as the length of the longest vector in it. Then the target of search-SIVP is to find n linearly independent vectors with length at most $\lambda_n(\mathcal{L})$, whereas optimization-SIVP should be defined as the problem to find λ_n. It is obvious that optimization-SIVP can be reduced to its search version. However, it seems hard to give a reduction from the search version to the optimization version since λ_n is only an upper bound of the length of these independent vectors.

In this paper, we consider a lattice problem called the successive minima problem (SMP), which is introduced in [5]. In fact, the original SMP in [5] which aims to find n linearly independent vectors achieving the successive minima respectively is a search version of this problem. We will naturally consider its optimization version as to find all the values of successive minima. Therefore, the relation between these two variants will be considered. Obviously, a reduction from optimization-SMP to its search version is trivial, but the inverse reduction seems difficult.

By perturbing the original lattice basis carefully as in [16], we can transform it to another basis of a new lattice, and we consider the relation between this pair of lattice bases. Then we find that the components of all successive minimal vectors do not change. Moreover, the successive minima of the new lattice are all different, which lead to an algorithm to recover all components for successive

minimal vectors of the original lattice. Similar to [16], the reduction from search-SMP to optimization-SMP is also rank-preserving. But by using some results of matrix analysis, we find that our reduction holds for every lattice, no matter whether it is full-rank or not.

Roadmap. The remainder of the paper is organized as follows. In Sect. 2, we give some preliminaries needed. In Sect. 3, we describe the reduction from search successively minimal vectors to its optimization version. Finally, we give a short conclusion in Sect. 4.

2 Preliminaries

We denote by $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Z}^+$, and $\mathbb{R}^+$ the integer ring, the real field, the complex field, the set of positive integers, and the set of positive real numbers respectively.

For any vector $v = (v_1, v_2, \cdots, v_m)^T \in \mathbb{R}^m$ and $m \in \mathbb{Z}^+$, we denote by $\|v\| = \sqrt{\sum_{i=1}^{m} v_i^2}$ its length.

2.1 Lattice and the Successively Minima Problem

Given a matrix $B = (b_{ij}) \in \mathbb{R}^{m \times n}$ with rank n, the lattice $\mathcal{L}(B)$ spanned by the columns of B is

$$\mathcal{L}(B) = \{Bx = \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z}\},$$

where b_i is the ith column of B. We call m, n the dimension and the rank of $\mathcal{L}(B)$ respectively. The determinant of $\mathcal{L}(B)$, say $\det(\mathcal{L}(B))$, is defined as $\sqrt{\det(B^T B)}$. It is easy to see when B is full-rank ($n = m$), its determinant becomes $|\det(B)|$.

Definition 1 (Successive Minima). *For a n-rank lattice $\mathcal{L}(B)$ with $B \in \mathbb{R}^{m \times n}$, and $i \in \{1, 2, \cdots, n\}$, we define the ith successive minimum as*

$$\lambda_i(\mathcal{L}(B)) = \inf \left\{ r \in \mathbb{R}^+ | \dim(span(\overline{B(0,r)} \bigcap \mathcal{L}(B))) \geq i \right\},$$

where $\overline{B(0,r)}$ is the closed ball centered at 0 with radius $r \in \mathbb{R}^+$, i.e., $\overline{B(0,r)} = \{x \in \mathbb{R}^m | \|x\| \leq r\}$.

Simply speaking, $\lambda_i(\mathcal{L}(B))$ means the infimum of the maximal length of i linearly independent vectors in $\mathcal{L}(B)$.

It is well-known that the successive minima can be achieved, that is, there exist n linearly independent lattice vectors $v_1, v_2, \cdots, v_n \in \mathcal{L}(B)$ such that $\|v_i\| = \lambda_i(\mathcal{L}(B))$. Therefore, we can define

Definition 2 (Successively Minimal Vectors). *Given a lattice basis $B \in \mathbb{R}^{m \times n}$ with rank n, any n linearly independent lattice vectors $v_1, v_2, \cdots, v_n \in \mathcal{L}(B)$ satisfying $\|v_i\| = \lambda_i(\mathcal{L}(B))$ are called the successively minimal vectors of $\mathcal{L}(B)$.*

In [5,21], the Successive Minima Problem is defined as below:

Definition 3 (SMP$_\gamma$). *Given a lattice $\mathcal{L}(B)$ and a constant $\gamma \geq 1$, output n linearly independent vectors $v_1, v_2, \ldots, v_n$ in $\mathcal{L}(B)$ such that $\|v_i\| \leq \gamma \lambda_i(\mathcal{L}(B))$.*

When $\gamma = 1$, it becomes Search-SMP:

Definition 4 (Search-SMP). *Given a lattice $\mathcal{L}(B)$, find a set of the successively minimal vectors in $\mathcal{L}(B)$.*

It is proved that SMP is equivalent to SIVP and the closest vector problem (CVP) in [21]. We can define its optimization version similar to SVP as following:

Definition 5 (Optimization-SMP). *Given a lattice $\mathcal{L}(B)$, find the successive minima of $\mathcal{L}(B)$.*

2.2 Linear Algebra

For a matrix $A \in \mathbb{C}^{m \times n}$, we denote by A^* its conjugate transpose and A^T its transpose. The singular values of A is defined to be the nonnegative square root of the eigenvalues of A^*A.

Using the singular values or the eigenvalues of matrices, we can obtain the following Lemma stated in [15]:

Lemma 1 (Rayleigh quotient). *Let $A \in \mathbb{C}^{m \times n}$ and $0 \leq \mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$ be all eigenvalues of A^*A, then for any $x = (x_i) \in \mathbb{C}^n \backslash \{0\}$, we have*

$$\mu_1 \leq \frac{x^* A^* A x}{x^* x} \leq \mu_n.$$

We present a lower bound for the smallest singular value of a matrix in the following lemma, whose proof can be found in [24].

Lemma 2. *Given a matrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ with $\det(A) \neq 0$, we let $0 \leq \sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_n$ be all singular values of A, then the smallest singular value σ_1 satisfies the inequality:*

$$\sigma_1 \geq \left(\frac{n-1}{\|A\|_F^2}\right)^{\frac{n-1}{2}} |\det(A)|,$$

where $\|A\|_F = \left(\sum_{i,j=1}^{n} |a_{ij}|^2\right)^{\frac{1}{2}}$ is the Frobenius norm of A.

Finally, we give a lemma to illustrate the perturbation bound for the determinant of a matrix [17]:

Lemma 3. *Let $B, C \in \mathbb{C}^{n \times n}$, then*

$$|\det(B + C) - \det(B)| \leq n \|C\|_F \max\{\|B\|_F, \|B + C\|_F\}^{n-1}.$$

3 The Search-SMP Is Equivalent to Optimization-SMP

It is obvious that if we could solve search-SMP, then we can solve optimization-SMP easily. To show the equivalence between the two problems, what we really need is a reduction from search-SMP to its optimization version.

In this section, we give such a reduction, which consists of three main steps. Suppose we want to find the successively minimal vectors in a given lattice $\mathcal{L}(B)$, we first construct a new lattice basis B_ϵ by perturbing the original basis B. By the optimization-SMP oracle, we can then get the successive minima of $\mathcal{L}(B_\epsilon)$. In fact, using the successive minima, we can efficiently recover the coefficients of the successively minimal vectors under the basis B_ϵ. With the recovered coefficients, we can get the successively minimal vectors in $\mathcal{L}(B)$ finally.

First we present a lemma to show that the coefficients of the successively minimal vectors under the basis can be well bounded.

Lemma 4. *Given a lattice basis $B = (b_{ij}) \in \mathbb{Z}^{m\times n}$ with rank n, let $M = \max\{|b_{ij}|\}$. For any $x = (x_i) \in \mathbb{Z}^n$ such that $\|Bx\| \le \lambda_n(\mathcal{L}(B))$, we have*

$$x_i^2 \le 2^{\frac{n+1}{2}} n^{\frac{n-1}{2}} (mM^2)^n.$$

Proof. Note that when $n = 1$, the result is trivial, so we assume $n \ge 2$.

It is easy to check that $\lambda_i(\mathcal{L}(B))^2 \le \max\{\|b_i\|^2\} \le mM^2$, so for any $x = (x_i) \in \mathbb{Z}^n$ such that $\|Bx\| \le \lambda_n(\mathcal{L}(B))$, we have

$$\|Bx\|^2 \le mM^2.$$

Considering the Gram matrix $A = B^TB$, that is,

$$A = \begin{pmatrix} b_{11}^2 + b_{21}^2 + \cdots + b_{m1}^2 & \cdots & b_{11}b_{1n} + b_{21}b_{2n} + \cdots + b_{m1}b_{mn} \\ \vdots & \ddots & \vdots \\ b_{1n}b_{11} + b_{2n}b_{21} + \cdots + b_{mn}b_{m1} & \cdots & b_{1n}^2 + b_{2n}^2 + \cdots + b_{mn}^2 \end{pmatrix},$$

by Lemma 1, we know that

$$0 < \mu_1(A) = \mu_1(B^TB) \le \frac{x^TB^TBx}{x^Tx} = \frac{\|Bx\|^2}{\|x\|^2}.$$

Together with $\|Bx\|^2 \le mM^2$, we have

$$\|x\|^2 \le \frac{mM^2}{\mu_1(A)}.$$

So for each $i (1 \le i \le n)$, we have

$$|x_i| \le \frac{\sqrt{m}M}{\sqrt{\mu_1(A)}}. \tag{1}$$

Note that the singular values of $A = B^T B$ are in fact their eigenvalues. By the lower bound of the smallest singular value in Lemma 2, we know

$$\mu_1(A) \geq (\frac{n-1}{\|A\|_F^2})^{\frac{n-1}{2}} |\det(A)|. \tag{2}$$

Since the entries of B are integers, then

$$|\det(A)| \geq 1 > \frac{1}{2}.$$

Notice that the absolute values of entries of B are bounded by M, then the absolute values of entries of A are bounded by mM^2, which implies that

$$\|A\|_F^2 \leq n^2(mM^2)^2 = (nmM^2)^2.$$

Since $n \geq 2$, we have $n - 1 \geq \frac{n}{2}$. Hence, we have:

$$\mu_1 \geq \frac{1}{2}(\frac{1}{2nm^2M^4})^{\frac{n-1}{2}}$$

By (1),

$$x_i^2 \leq 2mM^2(2nm^2M^4)^{\frac{n-1}{2}} = 2^{\frac{n+1}{2}} n^{\frac{n-1}{2}} (mM^2)^n.$$

Remark 1. We can also use $B^T Bx$ to evaluate the upper bound of each component of x by the Cramer's Rule and Hadamard inequality, and the upper bound will be $n^{n/2}m^{n+1/2}M^{2n}$. This bound is not so tight as in Lemma 4.

In the following, we describe our reduction in detail.

Theorem 1. *Given an oracle $\mathcal{O}$ that can solve the optimization SMP for any lattice $\mathcal{L}(B')$ with basis $B' \in \mathbb{Z}^{m\times n}$, there is a deterministic polynomial time algorithm that can solve the search SMP for $\mathcal{L}(B)$ with the input basis $B \in \mathbb{Z}^{m\times n}$.*

Proof. We will complete the proof in the following 4 steps:

(1) First we construct a matrix $B_\epsilon \in \mathbb{Z}^{m\times n}$:

$$B_\epsilon = \epsilon_{n+1}B + \begin{pmatrix} \epsilon_1 & \epsilon_2 & \dots & \epsilon_n \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

where ϵ_i's are determined as below.

Let $M_1 = 2^{\frac{n+1}{4}} n^{\frac{n-1}{4}} m^{\frac{n}{2}} (M+1)^n$ and $M_2 = \sqrt{m}(M+1)$ where $M = \max\{|b_{ij}|\}$, then we choose

$$p = 2\max\{M_2^2, 2M_1M_2, 2M_1^2\} + 1.$$

Note that $\log p = \text{poly}(n, m, \log M)$, where $\text{poly}(n, m, \log M)$ stands for a polynomial of n, m and $\log M$.

Then we choose $n+1$ positive integers $a_1 < a_2 < \cdots < a_n < a_{n+1}$ such that all $a_i + a_j (1 \le i \le j \le n+1)$'s are distinct and a_{n+1} is bounded by $\mathrm{poly}(n)$. As in Lemma 1 of [16], we can first choose

$$a_i = i^2 + (2(n+1)^2)i + 4(n+1)^4,$$

for $i = 1, 2, \cdots, n$. Then we let

$$a_{n+1} = 3a_n.$$

By Lemma 1 in [16], all $a_i + a_j (1 \le i \le j \le n)$'s are distinct. Together with the fact that $a_{n+1} > 2a_n$, it is easy to see that $a_i + a_j (1 \le i \le j \le n+1)$'s are distinct and a_{n+1} is bounded by $\mathrm{poly}(n)$. Finally we let

$$\epsilon_i = p^{a_i}.$$

Notice that for every entry $b_{\epsilon ij}$ in B_ϵ, $\log |b_{\epsilon ij}| = \mathrm{poly}(n, m, \log M)$. Hence B_ϵ can be constructed efficiently.

(2) Next we claim that the columns of B_ϵ are linearly independent, so B_ϵ forms a lattice basis of $\mathcal{L}(B_\epsilon)$. In fact we can prove the claim by showing that $\det(B_\epsilon^T B_\epsilon) \neq 0$. In the following, we prove that

$$|\det((\frac{1}{\epsilon_{n+1}} B_\epsilon)^T (\frac{1}{\epsilon_{n+1}} B_\epsilon))| = |\det(\frac{1}{\epsilon_{n+1}^2} B_\epsilon^T B_\epsilon)| > \frac{1}{2}.$$

Notice that the absolute values of entries of $\frac{1}{\epsilon_{n+1}} B_\epsilon$ can be bounded by $M+1$, then the absolute values of entries of $(\frac{1}{\epsilon_{n+1}} B_\epsilon)^T (\frac{1}{\epsilon_{n+1}} B_\epsilon)$ are bounded by $m(M+1)^2$. Note that

$$(\frac{1}{\epsilon_{n+1}} B_\epsilon)^T (\frac{1}{\epsilon_{n+1}} B_\epsilon) = B^T B + \frac{1}{\epsilon_{n+1}} B^T \begin{pmatrix} \epsilon_1 & \epsilon_2 & \cdots & \epsilon_n \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} + \frac{1}{\epsilon_{n+1}} \begin{pmatrix} \epsilon_1 & 0 & \cdots & 0 \\ \epsilon_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_n & 0 & \cdots & 0 \end{pmatrix} B + \frac{1}{\epsilon_{n+1}^2} \begin{pmatrix} \epsilon_1^2 & \epsilon_1\epsilon_2 & \cdots & \epsilon_1\epsilon_n \\ \epsilon_2\epsilon_1 & \epsilon_2^2 & \cdots & \epsilon_2\epsilon_n \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_n\epsilon_1 & \epsilon_n\epsilon_2 & \cdots & \epsilon_n^2 \end{pmatrix}$$

Let $A = B^T B$ and $C = (\frac{1}{\epsilon_{n+1}} B_\epsilon)^T (\frac{1}{\epsilon_{n+1}} B_\epsilon) - A$, then each entry of C can be bounded by $2M \frac{\epsilon_n}{\epsilon_{n+1}} + \frac{\epsilon_n^2}{\epsilon_{n+1}^2} \le (2M+1) \frac{\epsilon_n}{\epsilon_{n+1}} \le 2(M+1) \frac{\epsilon_n}{\epsilon_{n+1}}$, which implies

$$\|C\|_F \le 2n(M+1) \frac{\epsilon_n}{\epsilon_{n+1}}.$$

By Lemma 3, we have

$$\begin{aligned} |\det(A+C)-\det(A)| &\le n\|C\|_F \max\{\|A\|_F, \|A+C\|_F\}^{n-1} \\ &\le 2n^2(M+1)\frac{\epsilon_n}{\epsilon_{n+1}}(nm(M+1)^2)^{n-1} \\ &= 2n^{n+1}m^{n-1}(M+1)^{2n-1}\frac{\epsilon_n}{\epsilon_{n+1}}. \end{aligned}$$

By the choice of $a_n \ge n$ and $p > M_2^2$, we have

$$\begin{aligned} p^{a_{n+1}-a_n} &\ge p^{2n} \\ &> (m(M+1)^2)^{2n} \\ &\ge 4m^{2n}(M+1)^{2n} \\ &> 4m^{n-1}n^{n+1}(M+1)^{2n-1}. \end{aligned}$$

That is

$$\frac{\epsilon_n}{\epsilon_{n+1}} < \frac{1}{4n^{n+1}m^{n-1}(M+1)^{2n-1}}.$$

Then we immediately have $|\det(A+C)-\det(A)| < \frac{1}{2}$, which is in fact

$$|\det((\frac{1}{\epsilon_{n+1}}B)^T(\frac{1}{\epsilon_{n+1}}B)-\det(B^TB))| < \frac{1}{2}.$$

Note that $\det(B^TB)$ is a nonzero integer, then we finally have

$$|\det((\frac{1}{\epsilon_{n+1}}B)^T(\frac{1}{\epsilon_{n+1}}B))| > \frac{1}{2}.$$

For a vector satisfying $\|B_\epsilon x\| \le \lambda_n(\mathcal{L}(B_\epsilon))$, all the components $|x_i|$ of x can also be bounded by M_1.

(3) Moreover, we claim that if n linearly independent vectors $B_\epsilon x_1, B_\epsilon x_2, \cdots, B_\epsilon x_n \in \mathcal{L}(B_\epsilon)$ form a set of the successively minimal vectors in $\mathcal{L}(B_\epsilon)$ where $x_1, x_2, \cdots, x_n \in \mathbb{Z}^n$, that is, $\|B_\epsilon x_i\| = \lambda_i(\mathcal{L}(B_\epsilon)), 1 \le i \le n$, then $Bx_1, Bx_2, \cdots, Bx_n \in \mathcal{L}(B)$ also form a set of the successively minimal vectors in $\mathcal{L}(B)$.

First note that since $B_\epsilon x_1, B_\epsilon x_2, \cdots, B_\epsilon x_n \in \mathcal{L}(B_\epsilon)$ are linearly independent and B_ϵ is a basis, then $x_1, x_2, \cdots, x_n$ are linearly independent, which implies that $Bx_1, Bx_2, \cdots, Bx_n \in \mathcal{L}(B)$ are linearly independent.
Second we will prove that $\|Bx_i\| = \lambda_i(\mathcal{L}(B))$, for $1 \le i \le n$. For contradiction, let l be the smallest index such that for $1 \le i < l$, $\|Bx_i\| = \lambda_i(\mathcal{L}(B))$, whereas $\|Bx_l\| > \lambda_l(\mathcal{L}(B))$. We have

$$\|Bx_l\|^2 \ge \lambda_l(\mathcal{L}(B))^2 + 1. \tag{3}$$

By the definition of successively minimal vectors, there must exist vectors $y_i = (y_{i1}, y_{i2}, \cdots, y_{in})^T \in \mathbb{Z}^n, 1 \leq i \leq l$ such that $\|By_i\| = \lambda_i(\mathcal{L}(B))$ and $By_1, By_2, \cdots, By_l$ are linearly independent.

Considering $B_\epsilon y_i$, note that

$$\|B_\epsilon y_i\|^2 = \epsilon_{n+1}^2 \|By_i\|^2 + \sum_{j=1}^{n} y_{ij}^2 \epsilon_j^2 + \sum_{j=1}^{n} 2c(y_i) y_{ij} \epsilon_j \epsilon_{n+1} + \sum_{1 \leq j < k \leq n} 2y_{ij} y_{ik} \epsilon_j \epsilon_k, \tag{4}$$

where $c(y_i) = \sum_{j=1}^{n} b_{1j} y_{ij}$ for any $y_i \in \mathbb{Z}^n$. Since $\|By_i\| = \lambda_i(\mathcal{L}(B))$, we know that

$$\|By_i\| \leq M_2.$$

By Lemma 4, we have for $1 \leq j \leq n$

$$|y_{ij}| \leq M_1.$$

Note that $|c(y_i)| \leq \|By_i\|$, we have also

$$|c(y_i)| \leq M_2.$$

By the choice of p, we know that all coefficients $\|By_i\|^2, y_{ij}^2, 2c(y_i)y_{ij}, 2y_{ij}y_{ik}$ of $\epsilon_j \epsilon_k$ in Eq. (4) are in the interval $(-\lfloor \frac{p}{2} \rfloor, \lfloor \frac{p}{2} \rfloor)$. Since $\epsilon_j \epsilon_k$'s are different powers of p, when we take $\|B_\epsilon y_i\|^2$ as a number with base p, it is easy to check that

$$\begin{aligned} \|B_\epsilon y_i\|^2 &< \epsilon_{n+1}^2 \|By_i\|^2 + \frac{1}{2}\epsilon_{n+1}^2 \\ &\leq \epsilon_{n+1}^2 (\lambda_l(\mathcal{L}(B))^2 + \frac{1}{2}). \end{aligned}$$

However, by Eq. (3), we know that

$$\begin{aligned} \|B_\epsilon x_l\|^2 &> \epsilon_{n+1}^2 \|Bx_l\|^2 - \frac{1}{2}\epsilon_{n+1}^2 \\ &\geq \epsilon_{n+1}^2 (\lambda_l(\mathcal{L}(B))^2 + 1 - \frac{1}{2}) \\ &= \epsilon_{n+1}^2 (\lambda_l(\mathcal{L}(B))^2 + \frac{1}{2}). \end{aligned}$$

Note that $B_\epsilon y_1, B_\epsilon y_2, \cdots, B_\epsilon y_l$ are linearly independent, and $\lambda_l(\mathcal{L}(B_\epsilon)) = \|B_\epsilon x_l\| > \|B_\epsilon y_i\|$, $1 \leq i \leq l$, which leads to a contradiction to the definition of the successive minima. Hence, for $1 \leq i \leq n$, we have

$$\|Bx_i\| = \lambda_i(\mathcal{L}(B)).$$

(4) Finally, we recover all successively minimal vectors as following. Querying the oracle $\mathcal{O}$ with B_ϵ, we obtain $\lambda_i(\mathcal{L}(B_\epsilon)), 1 \leq i \leq n$. We next show we can efficiently find $x_i \in \mathbb{Z}^n$, such that $\|B_\epsilon x_i\| = \lambda_i(\mathcal{L}(B_\epsilon))$ by the value of $\lambda_i(\mathcal{L}(B_\epsilon))$ for $1 \leq i \leq n$.

Let $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})^T \in \mathbb{Z}^n$ satisfy

$$\lambda_i(\mathcal{L}(B_\epsilon))^2 = \|B_\epsilon x_i\|^2.$$

First note that $\log(\lambda_n(\mathcal{L}(B_\epsilon)))$ is bounded by $\mathrm{poly}(m, n, \log M)$, and by Lemma 4, we know that $\log|x_{ij}|$ can also be bounded by $\mathrm{poly}(m, n, \log M)$.

Second we expand $\|B_\epsilon x_i\|^2$ as follows:

$$\|B_\epsilon x_i\|^2 = \epsilon_{n+1}^2 \|Bx_i\|^2 + \sum_{j=1}^{n} x_{ij}^2 \epsilon_j^2 + \sum_{j=1}^{n} 2c(x_i) x_{ij} \epsilon_j \epsilon_{n+1} + \sum_{1 \leq j < k \leq n} 2x_{ij} x_{ik} \epsilon_j \epsilon_k. \quad (5)$$

Similarly, since $\|B_\epsilon x_i\| = \lambda_i(\mathcal{L}(B_\epsilon))$, we know that $\|Bx_i\| = \lambda_i(\mathcal{L}(B))$. As discussed in Step (3), all the coefficients $\|Bx_i\|^2$, x_{ij}^2, $2c(x_i)x_{ij}$, $2x_{ij}x_{ik}$ of $\epsilon_i\epsilon_j$ in Eq. (5) are in the interval $(-\lfloor \frac{p}{2} \rfloor, \lfloor \frac{p}{2} \rfloor)$. It is easy to recover all the coefficients in $\mathrm{poly}(m, n, \log M)$ time by Lemma 2 in [16]. More precisely, we can recover all x_{ij}^2 and $x_{ij}x_{il}, j \neq l$ for each x_i. In fact for x_i, let $k_i = \min\{j | x_{ij} \neq 0\}$, and we can fix x_{ik_i} positive, that is $x_{ik_i} = \sqrt{x_{ik_i}^2}$. For the remaining x_{ij}, we can recover their absolute values according to x_{ij}^2, and their signs according to the signs of $x_{ik_i}x_{ij}$. This can be done in $\mathrm{poly}(m, n, \log M)$ time.

After recovering $x_1, x_2, \cdots, x_n \in \mathbb{Z}^n$ such that $\|B_\epsilon x_i\| = \lambda_i(\mathcal{L}(B_\epsilon)), 1 \leq i \leq n$, we compute $Bx_1, Bx_2, \cdots, Bx_n \in \mathcal{L}(B)$. Then they form a set of the successively minimal vectors in $\mathcal{L}(B)$.

All the reduction above is in $\mathrm{poly}(m, n, \log M)$ time. The proof is completed. Hence, we finally have:

Corollary 1. *Search-SMP is equivalent to optimization-SMP.*

Remark 2. In our proof of the main theorem, we use the expansion of base p to recover all the successive minimal vectors. An obvious observation is that all the values $\|B_\epsilon x_i\|$ must be different since the same value must have the same expansion for base p in the interval $(-\lfloor \frac{p}{2} \rfloor, \lfloor \frac{p}{2} \rfloor)$. That is, when we add these errors to a given lattice basis B to transform it to be B_ϵ, all the successive minima $\lambda_i(\mathcal{L}(B_\epsilon))$ will be different.

4 Conclusions

In this paper, we revisit the problem SMP in lattices, and propose a rank-preserving reduction in polynomial time from search-SMP to optimization-SMP with only one call to the optimization-SMP oracle, which leads to the equivalence between search-SMP and its optimization version.

Acknowledgement. We very thank the anonymous referees for their valuable suggestions on how to improve the presentation of this paper.

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC 1996, pp. 99–108. ACM, New York (1996). https://doi.org/10.1145/237814.237838
2. Ajtai, M.: The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, STOC 1998, pp. 10–19. ACM, New York (1998). https://doi.org/10.1145/276698.276705
3. 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, STOC 1997, pp. 284–293. ACM, New York (1997). https://doi.org/10.1145/258533.258604
4. Alkim, E., Bindel, N., Buchmann, J.A., Dagdelen, Ö., Schwabe, P.: TESLA: Tightly-Secure Efficient Signatures from Standard Lattices. IACR Cryptology ePrint Archive 2015, 755 (2015). https://eprint.iacr.org/2015/755.pdf
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). https://doi.org/10.1007/978-3-540-73420-8_8
6. Boas, P.V.E.: Another NP-complete problem and the complexity of computing short vectors in lattices. Mathematics Department Report 81-04. University of Amsterdam (1981)
7. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. SIAM J. Comput. **43**(2), 831–871 (2014). https://doi.org/10.1137/120868669
8. Cai, J.Y., Nerurkar, A.: Approximating the SVP to within a factor $(1–1/\dim^{\epsilon})$ is NP-hard under randomized conditions. In: Proceedings of the Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat. No.98CB36247), pp. 46–55, June 1998
9. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_3
10. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC 2009, pp. 169–178. ACM, New York (2009). https://doi.org/10.1145/1536414.1536440
11. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 197–206. ACM, New York (2008). https://doi.org/10.1145/1374376.1374407
12. Goldreich, O., Micciancio, D., Safra, S., Seifert, J.P.: Approximating shortest lattice vectors is not harder than approximating closest lattice vectors **71**, 55–61 (1999). http://www.sciencedirect.com/science/article/pii/S0020019099000836

13. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSign: digital signatures using the NTRU lattice. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 122–140. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36563-X_9
14. 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). https://doi.org/10.1007/BFb0054868
15. Horn, R.A., Johnson, C.R.: Matrix Analysis. Cambridge University Press, Cambridge (2012)
16. Hu, G., Pan, Y.: Improvements on reductions among different variants of SVP and CVP. In: Kim, Y., Lee, H., Perrig, A. (eds.) WISA 2013. LNCS, vol. 8267, pp. 39–51. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05149-9_3
17. Ipsen, I.C.F., Rehman, R.: Perturbation bounds for determinants and characteristic polynomials. SIAM J. Matrix Anal. Appl. **30**(2), 762–776 (2008). https://doi.org/10.1137/070704770
18. Kannan, R.: Minkowski's convex body theorem and integer programming. Math. Oper. Res. **12**(3), 415–440 (1987). https://doi.org/10.1287/moor.12.3.415
19. Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_13
20. Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: a modest proposal for FFT hashing. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 54–72. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-71039-4_4
21. Micciancio, D.: Efficient reductions among lattice problems. In: Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2008, pp. 84–93. Society for Industrial and Applied Mathematics, Philadelphia (2008). http://dl.acm.org/citation.cfm?id=1347082.1347092
22. Micciancio, D., Goldwasser, S.: Complexity of Lattice Problems: A Cryptographic Perspective. The Kluwer International Series in Engineering and Computer Science, vol. 671. Kluwer Academic Publishers, Boston (2002)
23. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_8
24. Piazza, G., Politi, T.: An upper bound for the condition number of a matrix in spectral norm. J. Comput. Appl. Math. **143**(1), 141–144 (2002). http://www.sciencedirect.com/science/article/pii/S0377042702003965
25. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC 2005, pp. 84–93. ACM, New York (2005). https://doi.org/10.1145/1060590.1060603