

Algorithms for the Shortest Vector Problem in 2-dimensional Lattices, Revisited

Lihao Zhao, Chengliang Tian, Jingguo Bi, Guangwu Xu, Jia Yu

Abstract

Efficiently solving the Shortest Vector Problem (SVP) in two-dimensional lattices holds practical significance in cryptography and computational geometry. While simpler than its high-dimensional counterpart, two-dimensional SVP motivates scalable solutions for high-dimensional lattices and benefits applications like sequence cipher cryptanalysis involving large integers. In this work, we first propose a novel definition of reduced bases and develop an efficient adaptive lattice reduction algorithm **CrossEuc** that strategically applies the Euclidean algorithm across dimensions. Building on this framework, we introduce **HVec**, a vectorized generalization of the Half-GCD (HGCD) algorithm originally defined for integers, which can efficiently halve the bit-length of two vectors and may have independent interest. By iteratively invoking **HVec**, our optimized algorithm **HVecSBP** achieves a reduced basis in $O(\log nM(n))$ time for arbitrary input bases with bit-length n , where $M(n)$ denotes the cost of multiplying two n -bit integers. Compared to existing algorithms, our design is applicable to general forms of input lattices, eliminating the cost of pre-converting input bases to Hermite Normal Form (HNF). The comprehensive experimental results demonstrate that for the input lattice bases in HNF, the optimized algorithm **HVecSBP** achieves at least a $13.5\times$ efficiency improvement compared to existing methods. For general-form input lattice bases, converting them to HNF before applying **HVecSBP** offers only marginal advantages in extreme cases where the two basis vectors are nearly degenerate (e.g., collapsing into integer-like scalars). However, as the linear dependency between input basis vectors decreases, directly employing **HVecSBP** yields increasingly significant efficiency gains, outperforming hybrid approaches that rely on prior **HNF** conversion.

Index Terms

Lattices, Half-GCD, Shortest Vector Problem (SVP), Hermite Normal Form (HNF), Lattice Basis Reduction

I. INTRODUCTION

A lattice is a classic object of study in the geometry of numbers, originating from research on sphere packing and covering problems in the 17th century. Around 1840, Gauss introduced the concept of a lattice and determined the maximum density of sphere packing in three-dimensional space. In the past thirty years, lattice theory has demonstrated its powerful applications in coding theory and cryptography, particularly through lattice-based cryptography. The application of lattice theory in these domains underscores its importance in tackling contemporary challenges in data security and communication. Its role in developing cryptographic methods that are resistant to both classical and quantum attacks highlights its value in securing digital information.

In general, a lattice is a set of discrete points in n -dimensional real space that has a periodic structure. Specifically, for d linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_d$ in the m -dimensional real space \mathbb{R}^m , a lattice \mathcal{L}

$$\mathcal{L} = L(\mathbf{B}) = \left\{ \sum_{i=1}^d z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}.$$

is the set of all integer linear combinations of these vectors, where d is called the dimension of the lattice and the set of d vectors $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_d]$ is called a basis of the lattice. The k -th successive minimum of a lattice is defined as

$$\lambda_k(\mathcal{L}) = \inf\{r > 0 : \dim(\text{span}(\mathcal{B}(\mathbf{o}, r) \cap \mathcal{L})) \geq k\},$$

which $\mathcal{B}(\mathbf{o}, r)$ represents the open ball of radius r centered at the origin. In particular, $\lambda_1(L)$ denotes the length of the shortest non-zero vector in the lattice.

One of the most fundamental computational problems in lattice theory, known as the Shortest Vector Problem (SVP), is to find the shortest vector in a lattice. For a given lattice \mathcal{L} , this involves identifying a non-zero lattice vector \mathbf{v} such that

This research is supported by Natural Science Foundation of Shandong Province (No. ZR2022MF250), National Natural Science Foundation of China (No. 61702294, 12271306), National Key Research and Development Program of China (No. 2024YFB4504700, 2022YFB2702804), and the Youth Science and Technology Innovation Talent Support Program Project of Beijing University of Posts and Telecommunications (No. 2023ZCJH10). (*Corresponding author: C. Tian*)

L. Zhao, C. Tian and J. Yu are with the College of Computer Science and Technology, Qingdao University, Qingdao 266071, China. E-mail: zlh_qdu@163.com; tianchengliang@qdu.edu.cn; qduyujia@163.com.

J. Bi is with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China. E-mail: jguobi@bupt.edu.cn.

G. Xu is with School of Cyber Science and Technology, Shandong University (Qingdao), Qingdao 266273, China. E-mail: gxu4sdq@sdu.edu.cn.

Manuscript received October 10, 2019; revised ****, 20**.

$\|\mathbf{v}\| \leq \|\mathbf{u}\|$ holds for all non-zero vectors $\mathbf{u} \in \mathcal{L}$. The difficulty of solving this problem grows significantly with the dimension of the lattice. However, in the simplest case of two-dimensional lattices, solving the SVP—or even the Shortest Basis Problem (SBP), which seeks a basis $\mathbf{B} = [\mathbf{a} \ \mathbf{b}]$ satisfying $\|\mathbf{a}\| = \lambda_1(\mathcal{L})$ and $\|\mathbf{b}\| = \lambda_2(\mathcal{L})$ —is relatively straightforward, making it an ideal starting point for studying lattice problems. Developing fast algorithms for solving the two-dimensional SVP/SBP is of both theoretical and practical importance. From an algorithm design perspective, solving the SVP in two-dimensional lattices provides foundational insights for addressing higher-dimensional cases. For example, Lagrange’s pioneering work [5] on two-dimensional lattice reduction laid the groundwork for the celebrated LLL algorithm by A. K. Lenstra, H. W. Lenstra, and L. Lovász [6]. The LLL algorithm extends Lagrange’s approach by introducing techniques for reducing lattice bases in higher dimensions, combining ideas of approximate orthogonality and length minimization. As such, understanding and refining two-dimensional lattice reduction algorithms can directly contribute to advancements in higher-dimensional lattice computations. On the practical side, the SVP in two-dimensional lattices has direct applications in cryptanalysis. One critical indicator of the security of cryptographic random sequences is their 2-adic complexity, which measures the sequence’s resistance to linear feedback shift register attacks. Computing the 2-adic complexity involves determining the Minimal Rational Fractional Representation (MRFR) of the sequence, a problem that can be directly transformed into finding the shortest basis of a two-dimensional lattice. Specifically, given a sequence, a specialized two-dimensional lattice is constructed in Hermite Normal Form (HNF), and the shortest vector in this lattice corresponds to the MRFR. Efforts to optimize algorithms for solving the MRFR problem have shown significant progress. Arnault et al. [2] proposed a Euclidean-based algorithm in 2004, with subsequent improvements in 2008 [1], to compute the shortest basis of the lattice. However, these methods occasionally produced incorrect results in certain cases. Recently, Che et al. [3] proposed a novel and faster algorithm targeting the two-dimensional lattice shortest vector problem, significantly enhancing both the computational efficiency and reliability of solutions. Further optimization of algorithms for finding the shortest basis in two-dimensional lattices would directly accelerate the computation of 2-adic complexity, enabling faster and more accurate assessments of cryptographic random sequence security.

In summary, the above discussion highlights the two-fold significance of studying two-dimensional lattice problems: as a foundation for high-dimensional lattice theory and as a means to improve practical cryptographic applications. Therefore, continued research in this area is vital for advancing both theoretical lattice studies and practical algorithmic solutions.

A. Related works

For the SVP in two-dimensional lattices, the well-known solving algorithm is the Lagrange reduction algorithm (often referred to as the Gaussian reduction algorithm) [5, 8], which is similar to the integer Euclidean algorithm. For any two lattice basis vectors $\mathbf{a} = [a_1 \ a_2]^T$, $\mathbf{b} = [b_1 \ b_2]^T$, without loss of generality, we assume $\|\mathbf{a}\| \geq \|\mathbf{b}\|$, the core reduction step of Lagrange’s reduction algorithm uses a greedy approach to seek an integer

$$q = \left\lfloor \frac{\langle \mathbf{a}, \mathbf{b} \rangle}{\langle \mathbf{b}, \mathbf{b} \rangle} \right\rfloor$$

that minimizes the ℓ_2 -length of the lattice vector $\mathbf{c} = \mathbf{a} - q\mathbf{b}$ to update the lattice basis vectors with $[\mathbf{b} \ \mathbf{c}]$, if the two newly obtained \mathbf{b}, \mathbf{c} satisfy $\|\mathbf{b}\|, \|\mathbf{c}\| \leq \|\mathbf{b} \pm \mathbf{c}\|$, the algorithm terminates. Otherwise, the reduction process continues using the new vectors. This algorithm can find the shortest basis with lengths λ_1 and λ_2 in time $O(M(n)n)$, where $n = \max\{\lceil \log \|\mathbf{a}\| \rceil, \lceil \log \|\mathbf{b}\| \rceil\}$ and $M(n)$ denotes the complexity of multiplying two n -bit integers. Clearly, the choice of q is not exactly the same as that in the Euclidean algorithm of two integers. Yap [14] further studied the fully corresponding case, i.e., the algorithm gets the updated basis $[\mathbf{b} \ \mathbf{c}]$ with $\mathbf{c} = \mathbf{a} - q\mathbf{b}$ by taking

$$q = \left\lfloor \frac{\langle \mathbf{a}, \mathbf{b} \rangle}{\langle \mathbf{b}, \mathbf{b} \rangle} \right\rfloor.$$

During the process, if the update basis remains unchanged, the algorithm terminates. The author also designed a Half-Gaussian algorithm for two integer vectors, inspired by the HGCD algorithm for two integers, which improves the time complexity of lattice basis computation to $O(M(n) \log n)$. Rote’s algorithm [12] uses the lattice basis reduction method proposed by Yap [14] to solve the SVP on a two-dimensional lattice module m in $O(\log m (\log \log m)^2)$ time. Eisenbrand [4] and Che et al. [3] subsequently investigated fast algorithms for two-dimensional lattices with a known HNF basis. Specifically, when the input lattice basis satisfies $a_1 > b_1 \geq 0$, $a_2 = 0$ and $b_2 \neq 0$, it was noted that by taking

$$q = \left\lfloor \frac{a_1}{b_1} \right\rfloor$$

the shortest vector can be found more efficiently than with the Lagrange reduction algorithm. In contrast to Eisenbrand’s method [4] which addresses the standard HNF, Che et al. [3] specifically target a specialized HNF variant characterized by the constraint $b_2 = 1$. Notably, Che et al. [3] formalize an exact termination criterion for basis reduction and propose an optimized algorithm through systematic integration of the integer HGCD algorithm. Their implementation achieves a time complexity of $O(M(n) \log n)$, supported by comprehensive technical details. In comparison, Eisenbrand [4] interprets their algorithm through continued fraction theory and theoretically suggests potential optimizations via the integer HGCD algorithm to attain the same

asymptotic complexity $O(M(n) \log n)$, though without providing explicit implementation specifics. Wu and Xu [13] linked Qin Jiushao's algorithm with the solution of SVP in a special kind of two-dimensional lattices with $a_1 = 1$, $b_1 = 0$ and $\gcd(a_2, b_2) = 1$, and proposed an efficient method to solve the SVP of this kind of two-dimensional lattices with

$$q = \left\lfloor \frac{a_1 - 1}{b_1} \right\rfloor.$$

By examining each state matrix generated during the execution of the algorithm, the two vectors in the current state and their simple combinations can be utilized to extract the shortest lattice vector.

B. Motivation and Our Contribution

Existing studies reveal critical gaps in solving the SVP for two-dimensional lattices:

(1) **For HNF-form bases** $\mathbf{B} = \begin{pmatrix} a_1 & b_1 \\ 0 & b_2 \end{pmatrix}$: While prior works suggest that integer HGCD algorithms can optimize continued fraction-based methods, detailed technical analyses and implementations remain scarce. As noted in [10], “the integer HGCD algorithm is intricate, error-prone, and rarely fully detailed”, and [11] emphasizes its implementation challenges due to “numerous sub-cases and limited practical adoption.” Notably, [3] provides a concrete HGCD-based SVP solution for the special case $b_2 = 1$, but the implementation details for general b_2 is not available.

(2) **For general-form bases**: Current algorithms first convert inputs to HNF via (HGCD-based) extended Euclidean algorithms. However, this conversion often inflates integer sizes, especially for short initial bases, leading to longer lattice vectors. This raises two interesting questions: (i) *Is HNF conversion necessary?* (ii) *Can direct reduction algorithms bypass this step for a faster performance?*

To address these gaps, this work investigates direct lattice reduction algorithms that eliminate HNF conversion and generalize HGCD-based optimizations to arbitrary b_2 , bridging theoretical potential with practical implementation. Concretely, our main contributions can be summarized as follows:

- 1) **Novel Definition of a Reduced Basis.** For the first time, we explicitly propose a new definition of a reduced basis that differs from the conventional Lagrange-reduced basis. This novel definition expands the theoretical framework for lattice reduction, and we rigorously prove its fundamental properties. It is expected that this lays a solid theoretical foundation for further studies in this area.
- 2) **Efficient Algorithms with Detailed Implementation and Rigorous Complexity Analysis.** Leveraging the newly defined reduced basis, we design a novel algorithm named **CrossEuc** that bypasses HNF conversion, achieving a complexity of $O(n^2)$. This approach eliminates the computational overhead associated with HNF transformation. Furthermore, we introduce a vectorized adaptation of the HGCD algorithm, termed **HVec**, which represents the first explicit extension of HGCD-like techniques to vector pairs. This innovation is of independent theoretical interest and significantly advances the efficiency of solving the SVP in two-dimensional lattices. Building on this, we present an optimized algorithm **HVecSBP** that reduces the complexity to $O(\log n \cdot M(n))$, where $M(n)$ denotes the cost of multiplying two n -bit integers.
- 3) **Comprehensive Experimental Performance Analysis.** We conduct extensive experiments comparing our methods against state-of-the-art algorithms. Results show that (1) For the input lattice basis in HNF, our algorithm **HVecSBP** is about $13\times$ faster than previous designs for the worst case. (2) For the input lattice basis in general form, compared to the previous designs without using HGCD optimization, the proposed algorithm **CrossEuc** achieves a at least $4.5\times$ efficiency improvement. Compared to the previous designs using HGCD optimization, when the input vectors are nearly degenerate (i.e., treated as integers), **HGCD-HNF-HVecSBP** method retain a slight advantage. As the linear dependency between vectors weakens, **HVecSBP** exhibits remarkably growing efficiency gains.

C. Road Map

The paper is organized as follows. Section II introduces the notations, terminologies, and the mathematical concepts and properties frequently referenced in this work. In Section III, we define our proposed reduced basis and establish its theoretical properties. Section IV presents the **CrossEuc** algorithm alongside a detailed analysis. In Section V, we propose the **HVec** algorithm, discuss its analysis, and then introduce the **HVecSBP** algorithm, which iteratively invokes **HVec** to solve the shortest basis problem in two-dimensional lattices. Section VI provides a comprehensive experimental evaluation comparing the practical performance of our improved algorithms with that of existing methods, and the paper concludes with a brief summary in the final section.

II. PRELIMINARIES

For completeness, this section introduces the necessary preliminaries for the design and analysis of our new algorithm.

A. Notations and Terminologies

Throughout this paper, \mathbb{Z} denotes the ring of integers, and \mathbb{R} represents the field of real numbers. For $x, y \in \mathbb{R}$, $\#x = \lceil \log_2(|x| + 1) \rceil$ denotes the bit size of x , while $\#(x, y) = \max\{\#x, \#y\}$ and $\underline{\#}(x, y) = \min\{\#x, \#y\}$. The round function $\lceil x \rceil$ represents the nearest integer to x , the floor function $\lfloor x \rfloor$ represents the greatest integer less than or equal to x , and the ceiling function $\lceil x \rceil$ represents the smallest integer greater than or equal to x . The "rounding towards zero" $\lfloor x \rfloor_o$ of x and the sign function $\text{sgn}(x)$ of x are defined as follows:

$$\lfloor x \rfloor_o = \begin{cases} \lfloor x \rfloor, & \text{if } x \geq 0 \\ \lceil x \rceil, & \text{else} \end{cases}, \quad \text{sgn}(x) = \begin{cases} 1, & \text{if } x \geq 0 \\ -1, & \text{else} \end{cases}.$$

We use $M(n)$ to denote the time complexity of the multiplication of two n -bit integers. Uppercase bold letters represent matrices, while lowercase bold letters represent vectors. For any two vectors $\mathbf{a} = (a_1, a_2)^T$ and $\mathbf{b} = (b_1, b_2)^T$, we define $\#(\mathbf{a}, \mathbf{b}) = \max\{\#\mathbf{a}, \#\mathbf{b}\}$ and $\underline{\#}(\mathbf{a}, \mathbf{b}) = \min\{\#\mathbf{a}, \#\mathbf{b}\}$. For a vector $\mathbf{x} = (x_1, x_2, \dots, x_m) \in \mathbb{R}^m$, its Euclidean length (ℓ_2 norm) is defined as $\|\mathbf{x}\| = \sqrt{\sum_{i=1}^m x_i^2}$, and its Minkowski length (ℓ_∞ norm) is defined as $\|\mathbf{x}\|_\infty = \max_{1 \leq i \leq m} |x_i|$.

B. Lattices and related properties

In this section, we introduce the definition of lattices and some necessary properties we used in the rest of the paper.

Definition 1 ([8]). (*Lattice*). Given linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_d \in \mathbb{R}^m$, the lattice generated by these vectors is defined as

$$\mathcal{L} = L(\mathbf{B}) = L(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_d) = \left\{ \sum_{i=1}^d z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\},$$

where d and m are called the rank and the dimension of the lattice, respectively. Specially, if $d = m$, the lattice is called full-rank.

Definition 2 ([8]). (*Determinant*). Let $\mathcal{L} = L(\mathbf{B})$ be a lattice of rank d . The determinant of \mathcal{L} , denoted $\det(\mathcal{L}) = \sqrt{|\det(\mathbf{B}^T \mathbf{B})|}$. Specially, if \mathcal{L} is full-rank, $\det(\mathcal{L}) = |\det(\mathbf{B})|$.

Definition 3 ([8]). (*Unimodular Matrix*). A matrix $\mathbf{U} \in \mathbb{Z}^{d \times d}$ is called unimodular if $\det(\mathbf{U}) = \pm 1$.

Lemma 1 ([8]). Two bases $\mathbf{B}_1, \mathbf{B}_2 \in \mathbb{R}^{m \times d}$ are equivalent if and only if $\mathbf{B}_2 = \mathbf{B}_1 \mathbf{U}$ for some unimodular matrix \mathbf{U} .

Definition 4 ([8]). (*Successive Minima*). Let \mathcal{L} be a lattice of rank d . For $k \in \{1, \dots, d\}$, the k th successive minimum is defined as

$$\lambda_k(\mathcal{L}) = \inf\{r > 0 : \dim(\text{span}(\mathcal{B}(\mathbf{o}, r) \cap \mathcal{L})) \geq k\},$$

where, for any computable norm $\|\cdot\|$, $\mathcal{B}(\mathbf{o}, r) = \{\mathbf{x} \in \mathbb{R}^m : \|\mathbf{x}\| < r\}$ represents the open ball of radius r centered at the origin.

For two-dimensional lattices, Lagrange [5] introduced the concept of a reduced basis for two-dimensional lattices. That is,

Definition 5 ([5, 8]). Let $\mathbf{B} = [\mathbf{a} \ \mathbf{b}]$ with $\mathbf{a} = (a_1 \ a_2)^T$ and $\mathbf{b} = (b_1 \ b_2)^T$ be a basis of the lattice $\mathcal{L} = L(\mathbf{B})$. The basis is called Lagrange-reduced if it satisfies the condition: $\|\mathbf{a}\|, \|\mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\|, \|\mathbf{a} - \mathbf{b}\|$. Here, $\|\cdot\|$ refers to any computable norm.

For a Lagrange-reduced basis, the following result is well-known:

Lemma 2 ([8]). If $\mathbf{B} = [\mathbf{a} \ \mathbf{b}]$ is Lagrange-reduced, then for any computable norm $\|\cdot\|$, we have $\min\{\|\mathbf{a}\|, \|\mathbf{b}\|\} = \lambda_1(\mathcal{L})$ and $\max\{\|\mathbf{a}\|, \|\mathbf{b}\|\} = \lambda_2(\mathcal{L})$.

The above property is derived from the following general fact:

Lemma 3 ([8]). For any two vectors \mathbf{x}, \mathbf{y} and any computable norm $\|\cdot\|$, if $\|\mathbf{x}\| \leq$ (resp. $<$) $\|\mathbf{x} + \mathbf{y}\|$, then $\|\mathbf{x} + \mathbf{y}\| \leq$ (resp. $<$) $\|\mathbf{x} + \alpha \mathbf{y}\|$ for any $\alpha > 1$.

C. Hermite Normal Form

The Hermite Normal Form (HNF) of a matrix is a canonical form used in linear algebra and number theory for integer matrices.

Definition 6 ([7]). (*Hermite Normal Form*). A nonsingular matrix $\mathbf{H} \in \mathbb{Z}^{d \times d}$ is said to be in HNF if (1) $h_{i,i} > 0$ for $1 \leq i \leq d$. (2) $h_{j,i} = 0$ for $i < j \leq d$. (3) $0 \leq h_{j,i} < h_{i,i}$ for $1 \leq j < i$.

For any nonsingular integer matrix \mathbf{A} , there exists a unique matrix \mathbf{H} in Hermite Normal Form (HNF) and a unique unimodular matrix \mathbf{U} such that $\mathbf{H} = \mathbf{U}\mathbf{A}$ [7]. Specifically, for any two-dimensional lattice, the basis matrix can be efficiently converted into its HNF using the following lemma.

Lemma 4 ([4]). *Given a matrix $\mathbf{B} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$, let $c = \gcd(a_2, b_2) = xa_2 + yb_2$ be the greatest common divisor of a_2 and b_2 , then*

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} b_2/\gcd(a_2, b_2) & x \\ -a_2/\gcd(a_2, b_2) & y \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$$

with $a = (a_1b_2 - a_2b_1)/\gcd(a_2, b_2)$ and $b = a_1x + b_1y$. By applying elementary vector transformations, we can ensure that the matrix satisfy the HNF conditions.

III. OUR NEW REDUCED BASIS AND ITS PROPERTIES

In this section, we first introduce a new reduced basis and then present its properties. Throughout this section and the rest of the paper, unless otherwise specified, the notations $\|\mathbf{x}\|$ and $\|\mathbf{x}\|_2$ are used to represent the Minkowski measure (ℓ_∞ norm) of \mathbf{x} and the Euclidean measure (ℓ_2 norm), respectively.

Definition 7. *Given a lattice $\mathcal{L} = L(\mathbf{B})$ with a basis*

$$\mathbf{B} = [\mathbf{a} \ \mathbf{b}] = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in \mathbb{R}^{2 \times 2}, \quad (1)$$

we call \mathbf{B} is reduced if

$$a_1a_2b_1b_2 \leq 0 \wedge (|a_1| - |a_2|)(|b_1| - |b_2|) \leq 0 \quad (2)$$

It should be remarked that the equation (2) also can be equivalently reformulated as $a_1a_2b_1b_2 \leq 0 \wedge |a_1b_1 - a_2b_2| \leq |\det(\mathbf{B})|$. Now we present two important properties of the new defined reduced basis. The first theorem establishes the minimality of the reduced basis under the Minkowski (ℓ_∞) norm, while the second theorem demonstrates a similar property under the Euclidean (ℓ_2) norm.

Theorem 1. *Let $\mathcal{L} = L(\mathbf{B})$ be a lattice with basis \mathbf{B} defined in equation (1), and let $\lambda_1(\mathcal{L})$ and $\lambda_2(\mathcal{L})$ denote the successive minima under ℓ_∞ norm. If \mathbf{B} is reduced, then $\lambda_1(\mathcal{L}) = \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$. Further, let $\mathbf{c} = (c_1 \ c_2) \in \mathcal{L}$ be a vector achieving $\lambda_2(\mathcal{L})$. Then $\mathbf{c} = \operatorname{argmax}\{\|\mathbf{a}\|, \|\mathbf{b}\|\} - z \cdot \operatorname{argmin}\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$, where z is determined as follows:*

(1) *If $a_1b_1 \geq 0, a_2b_2 \leq 0$, then*

$$z = \begin{cases} \left\lfloor \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rfloor & \text{or } \left\lceil \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rceil, & \|\mathbf{a}\| \leq \|\mathbf{b}\| \\ \left\lfloor \frac{|a_1| - |a_2|}{|b_1| + |b_2|} \right\rfloor & \text{or } \left\lceil \frac{|a_1| - |a_2|}{|b_1| + |b_2|} \right\rceil, & \|\mathbf{a}\| > \|\mathbf{b}\| \end{cases}$$

(2) *If $a_1b_1 < 0, a_2b_2 \geq 0$, then*

$$z = \begin{cases} \left\lfloor \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \right\rfloor & \text{or } \left\lceil \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \right\rceil, & \|\mathbf{a}\| \leq \|\mathbf{b}\| \\ \left\lfloor \frac{|a_2| - |a_1|}{|b_1| + |b_2|} \right\rfloor & \text{or } \left\lceil \frac{|a_2| - |a_1|}{|b_1| + |b_2|} \right\rceil, & \|\mathbf{a}\| > \|\mathbf{b}\| \end{cases}$$

Specially, if $a_1a_2b_1b_2 = 0$ and none of the above cases apply, negate \mathbf{a} or \mathbf{b} as necessary to fit into one of the above cases.

Proof. Without loss of generality, we only consider the case $a_1b_1 \geq 0$ and $a_2b_2 \leq 0$. We aim to prove that for any non-zero lattice vector $\mathbf{v} = z_1\mathbf{a} + z_2\mathbf{b} = (z_1a_1 + z_2b_1 \ z_1a_2 + z_2b_2)^T$, the following inequality holds:

$$\min\{\|\mathbf{a}\|, \|\mathbf{b}\|\} \leq \|\mathbf{v}\|. \quad (3)$$

Clearly, in case that $z_1 = 0, z_2 \neq 0$,

$$\|\mathbf{v}\| = \max\{|z_1a_1 + z_2b_1|, |z_1a_2 + z_2b_2|\} = \max\{|z_2b_1|, |z_2b_2|\} \geq \max\{|b_1|, |b_2|\} = \|\mathbf{b}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}.$$

and, in case that $z_1 \neq 0, z_2 = 0$,

$$\|\mathbf{v}\| = \max\{|z_1a_1 + z_2b_1|, |z_1a_2 + z_2b_2|\} = \max\{|z_1a_1|, |z_1a_2|\} \geq \max\{|a_1|, |a_2|\} = \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}.$$

We now analyze the case $z_1z_2 \neq 0$ based on the properties of the reduced basis (i.e., $(|a_1| - |a_2|)(|b_1| - |b_2|) \leq 0$).

1) $|a_1| = |a_2|$. Here, $\|\mathbf{a}\| = \max\{|a_1|, |a_2|\} = |a_1| = |a_2|$. Then, if $z_1z_2 > 0$, we have $\|\mathbf{v}\| = \max\{|z_1a_1 + z_2b_1|, |z_1a_2 + z_2b_2|\} \geq |z_1a_1 + z_2b_1| \geq \max\{|a_1|, |b_1|\} \geq |a_1| = \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$ and, if $z_1z_2 < 0$, we have $\|\mathbf{v}\| = \max\{|z_1a_1 + z_2b_1|, |z_1a_2 + z_2b_2|\} \geq |z_1a_2 + z_2b_2| \geq |a_2| = \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$.

- 2) $|b_1| = |b_2|$. Here, $\|\mathbf{b}\| = \max\{|b_1|, |b_2|\} = |b_1| = |b_2|$. Then, if $z_1 z_2 > 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_1 + z_2 b_1| \geq \max\{|a_1|, |b_1|\} \geq |b_1| = \|\mathbf{b}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$ and, if $z_1 z_2 < 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_2 + z_2 b_2| \geq |b_2| = \|\mathbf{b}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$.
- 3) $|a_1| < |a_2|$ and $|b_1| > |b_2|$. Here, $\|\mathbf{a}\| = \max\{|a_1|, |a_2|\} = |a_2|$ and $\|\mathbf{b}\| = \max\{|b_1|, |b_2|\} = |b_1|$. Then, if $z_1 z_2 > 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_1 + z_2 b_1| \geq \max\{|a_1|, |b_1|\} = |b_1| = \|\mathbf{b}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$ and, if $z_1 z_2 < 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_2 + z_2 b_2| \geq |a_2| = \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$.
- 4) $|a_1| > |a_2|$ and $|b_1| < |b_2|$. Here, $\|\mathbf{a}\| = \max\{|a_1|, |a_2|\} = |a_1|$ and $\|\mathbf{b}\| = \max\{|b_1|, |b_2|\} = |b_2|$. Then, if $z_1 z_2 > 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_1 + z_2 b_1| \geq \max\{|a_1|, |b_1|\} \geq |a_1| = \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$, and, if $z_1 z_2 < 0$, we have $\|\mathbf{v}\| = \max\{|z_1 a_1 + z_2 b_1|, |z_1 a_2 + z_2 b_2|\} \geq |z_1 a_2 + z_2 b_2| \geq |b_2| = \|\mathbf{b}\| \geq \|\mathbf{a}\| \geq \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$.

Overall, the equation (3) holds, confirming that $\lambda_1(\mathcal{L}) = \min\{\|\mathbf{a}\|, \|\mathbf{b}\|\}$. Next, we will analyze the vector that achieves the second successive minimum $\lambda_2(\mathcal{L})$, by considering two distinct cases.

Case 1: $\min\{\|\mathbf{a}\|, \|\mathbf{b}\|\} = \|\mathbf{a}\| = \lambda_1(\mathcal{L})$, i.e., $\max\{|a_1|, |a_2|\} \leq \max\{|b_1|, |b_2|\}$. Define the function

$$f(x) = \|\mathbf{b} - x\mathbf{a}\| = \max\{|b_1 - xa_1|, |b_2 - xa_2|\} \triangleq \max\{f_1(x), f_2(x)\}.$$

Let $f(z) = \min_{z \in \mathbb{Z}} f(x)$. Then, $\|\mathbf{a}\| \leq f(z) = \|\mathbf{b} - z\mathbf{a}\| \leq f(z+1) = \|\mathbf{b} - (z+1)\mathbf{a}\| = \|\mathbf{a} - (\mathbf{b} - z\mathbf{a})\|$ and $f(z-1) = \|\mathbf{b} - (z-1)\mathbf{a}\| = \|\mathbf{a} + (\mathbf{b} - z\mathbf{a})\|$. By **Lemma 2**, it follows that $\lambda_2(\mathcal{L}) = f(z)$. Thus, we only need to estimate z . We now consider the case where $a_1 a_2 \neq 0$. The argument is essentially the same for cases where $a_1 = 0$ or $a_2 = 0$. From the definitions of $f_1(x)$ and $f_2(x)$, we have

$$f_1(x) = \begin{cases} |a_1|x - |b_1|, & x \geq \frac{b_1}{a_1} \\ -|a_1|x + |b_1|, & x < \frac{b_1}{a_1} \end{cases}, \quad f_2(x) = \begin{cases} |a_2|x + |b_2|, & x \geq \frac{b_2}{a_2} \\ -|a_2|x - |b_2|, & x < \frac{b_2}{a_2} \end{cases}.$$

The minimum $f(z)$ is achieved at the integer closest to the point of intersection where $-|a_1|x + |b_1| = |a_2|x + |b_2|$ (i.e., $x = \frac{|b_1| - |b_2|}{|a_1| + |a_2|}$). Therefore,

$$z = \left\lfloor \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rfloor \quad \text{or} \quad \left\lceil \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rceil.$$

Case 2: $\min\{\|\mathbf{a}\|, \|\mathbf{b}\|\} = \|\mathbf{b}\|$, i.e., $\max\{|a_1|, |a_2|\} \geq \max\{|b_1|, |b_2|\}$. Define the function

$$g(y) = \|\mathbf{a} - y\mathbf{b}\| = \max\{|a_1 - yb_1|, |a_2 - yb_2|\} \triangleq \max\{g_1(y), g_2(y)\}.$$

Let $g(z) = \min_{z \in \mathbb{Z}} g(y)$. Then $\|\mathbf{b}\| \leq g(z) = \|\mathbf{a} - z\mathbf{b}\| \leq g(z+1) = \|\mathbf{a} - (z+1)\mathbf{b}\| = \|\mathbf{b} - (\mathbf{a} - z\mathbf{b})\|$ and $g(z-1) = \|\mathbf{b} - (z-1)\mathbf{b}\| = \|\mathbf{b} + (\mathbf{a} - z\mathbf{b})\|$. By **Lemma 2**, it follows that $\lambda_2(\mathcal{L}) = g(z)$. Thus, we only need to estimate z . We now consider the case where $b_1 b_2 \neq 0$. The argument is essentially the same for cases where $b_1 = 0$ or $b_2 = 0$. From the definitions of $g_1(y)$ and $g_2(y)$, we have

$$g_1(y) = \begin{cases} |b_1|y - |a_1|, & y \geq \frac{a_1}{b_1} \\ -|b_1|y + |a_1|, & y < \frac{a_1}{b_1} \end{cases}, \quad g_2(y) = \begin{cases} |b_2|y + |a_2|, & y \geq \frac{a_2}{b_2} \\ -|b_2|y - |a_2|, & y < \frac{a_2}{b_2} \end{cases}.$$

The minimum $g(z)$ will achieve at the integer around the point of intersection $-|b_1|y + |a_1| = |b_2|y + |a_2|$ (i.e., $y = \frac{|a_1| - |a_2|}{|b_1| + |b_2|}$). Therefore,

$$z = \left\lfloor \frac{|a_1| - |a_2|}{|b_1| + |b_2|} \right\rfloor \quad \text{or} \quad \left\lceil \frac{|a_1| - |a_2|}{|b_1| + |b_2|} \right\rceil.$$

□

Theorem 2. Let $\mathcal{L} = L(\mathbf{B})$ be a lattice with basis \mathbf{B} defined in equation (1), and let $\lambda_1(\mathcal{L})$ and $\lambda_2(\mathcal{L})$ denote the successive minima under ℓ_2 norm. If \mathbf{B} is reduced, then $\mathbf{u} = \operatorname{argmin}\{\|\mathbf{a}\|_2, \|\mathbf{b}\|_2, \|\mathbf{a} + \mathbf{b}\|_2, \|\mathbf{a} - \mathbf{b}\|_2\}$ is a shortest non-zero lattice vector under the ℓ_2 norm. That is, $\lambda_1(\mathcal{L}) = \|\mathbf{u}\|_2$. Further, for any vector $\mathbf{x} \in \{\mathbf{a}, \mathbf{b}, \mathbf{a} + \mathbf{b}, \mathbf{a} - \mathbf{b}\} \setminus \{\mathbf{u}\}$, $\mathbf{v} = \mathbf{x} - q\mathbf{u}$ with $q = \left\lfloor \frac{\langle \mathbf{x}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} \right\rfloor$ is a lattice vector achieving $\lambda_2(\mathcal{L})$. That is, $\lambda_2(\mathcal{L}) = \|\mathbf{v}\|_2$.

Proof. First, we prove $\lambda_1(\mathcal{L}) = \|\mathbf{u}\|_2$. Namely, we need to prove $\forall (z_1, z_2) \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}, \|\mathbf{v}\|_2 = \|z_1 \mathbf{a} + z_2 \mathbf{b}\|_2 \geq \|\mathbf{u}\|_2$. Clearly, if $z_1 z_2 = 0$ or $z_1 = z_2$, we can easily deduce that $\|\mathbf{v}\|_2 \geq \min\{\|\mathbf{a}\|_2, \|\mathbf{b}\|_2, \|\mathbf{a} + \mathbf{b}\|_2\} \geq \|\mathbf{u}\|_2$; Without loss of generality, we now assume $\|\mathbf{a}\|_2 \leq \|\mathbf{b}\|_2$, $a_1 b_1 \geq 0$, $a_2 b_2 \leq 0$ and $z_1 z_2 \neq 0 \wedge z_1 \neq z_2$.

(1) $\mathbf{u} = \mathbf{a}$. In this case, we need to prove

$$\|z_1 \mathbf{a} + z_2 \mathbf{b}\|_2 \geq \|\mathbf{a}\|_2 \iff (z_1^2 - 1)(a_1^2 + a_2^2) + z_2^2(b_1^2 + b_2^2) + 2z_1 z_2(a_1 b_1 + a_2 b_2) \geq 0. \quad (4)$$

If $(z_1 z_2)(a_1 b_1 + a_2 b_2) \geq 0$, the above inequality clearly holds. Meanwhile, from $\|\mathbf{a}\|_2 \leq \|\mathbf{b}\|_2$ and $\|\mathbf{a}\|_2 \leq \|\mathbf{a} + \mathbf{b}\|_2, \|\mathbf{a} - \mathbf{b}\|_2$, we have

$$a_1^2 + a_2^2 \leq b_1^2 + b_2^2 \quad \wedge \quad -(b_1^2 + b_2^2) \leq 2(a_1 b_1 + a_2 b_2) \leq b_1^2 + b_2^2. \quad (5)$$

Applying these bounds, we conclude that inequality (4) follows from

$$\begin{aligned} & (z_1^2 - 1)(a_1^2 + a_2^2) + z_2^2(b_1^2 + b_2^2) + 2z_1z_2(a_1b_1 + a_2b_2) \\ & \geq (z_1^2 - 1)(a_1^2 + a_2^2) + z_2^2(b_1^2 + b_2^2) - z_1z_2(b_1^2 + b_2^2) \\ & \geq (z_1^2 - 1)(a_1^2 + a_2^2) + (z_2^2 - z_1z_2)(b_1^2 + b_2^2) \geq 0 \end{aligned}$$

Thus, it remains to consider the case where $(z_1z_2)(a_1b_1 + a_2b_2) < 0$ and $|z_1| > |z_2| \geq 1$. We proceed by analyzing this scenario in detail.

- $z_1z_2 > 0$ and $a_1b_1 + a_2b_2 < 0$, we have

$$\begin{aligned} & (z_1^2 - 1)(a_1^2 + a_2^2) + z_2^2(b_1^2 + b_2^2) + 2z_1z_2(a_1b_1 + a_2b_2) \\ & = (z_1^2 - 1)a_1^2 + (z_1^2 - 1)a_2^2 + z_2^2b_1^2 + z_2^2b_2^2 - 2|z_1||z_2|(a_2b_2 + a_1b_1) \\ & = (z_1^2 - 1)a_1^2 + (z_1^2 - 1)a_2^2 + z_2^2b_1^2 + z_2^2b_2^2 - 2|z_1||z_2|(|a_2||b_2| - a_1b_1) \\ & = z_1^2a_2^2 + z_2^2b_2^2 - 2|z_1||z_2||a_2||b_2| + (z_1^2 - 1)a_1^2 + z_2^2b_1^2 + 2z_1z_2a_1b_1 - a_2^2 \end{aligned} \quad (6)$$

Clearly, if $|a_1| \geq |a_2|$, then the equation (6) $\geq (z_1^2 - 1)a_1^2 - a_2^2 \geq 3a_1^2 - a_2^2 \geq 0$, and, if $|b_1| \geq |a_2|$, then the equation (6) $\geq z_2^2b_1^2 - a_2^2 \geq b_1^2 - a_2^2 \geq 0$. Consequently, the remaining case to consider is $|a_1| < |a_2| \wedge |b_1| < |a_2|$. From $|a_1| < |a_2|$ and the definition of the reduced base, we know $|b_1| \geq |b_2|$. Combining this with $|b_1| < |a_2|$ and the bound $a_1^2 + a_2^2 \leq b_1^2 + b_2^2$ (equation (5)), we deduce $|a_1| < |b_2|$. Thus, the remaining case is

$$|a_1| < |b_2| \leq |b_1| < |a_2|.$$

In this case, if $|z_2| \geq 2$, then the equation (6) $\geq z_2^2b_1^2 - a_2^2 \geq 4b_1^2 - a_2^2 \geq 2b_1^2 + 2b_2^2 - a_2^2 \geq 2(a_1^2 + a_2^2) - a_2^2 \geq 0$. If $|z_2| = 1$, the equation (6) is

$$\begin{aligned} & (b_1^2 + b_2^2) - (a_1^2 + a_2^2) + 2|z_1|a_1b_1 + z_1^2(a_1^2 + a_2^2) - 2|z_1||a_2||b_2| \\ & \geq z_1^2a_2^2 - 2|z_1||a_2||b_2| \geq z_1^2|a_2||b_2| - 2|z_1||a_2||b_2| = (z_1^2 - 2|z_1|)|a_2||b_2| \geq 0. \end{aligned}$$

- $z_1z_2 < 0$ and $a_1b_1 + a_2b_2 > 0$, we have

$$\begin{aligned} & (z_1^2 - 1)(a_1^2 + a_2^2) + z_2^2(b_1^2 + b_2^2) + 2z_1z_2(a_1b_1 + a_2b_2) \\ & = (z_1^2 - 1)a_1^2 + (z_1^2 - 1)a_2^2 + z_2^2b_1^2 + z_2^2b_2^2 - 2|z_1||z_2|(a_1b_1 - |a_2b_2|) \\ & = z_1^2a_1^2 + z_2^2b_1^2 - 2|z_1||z_2|a_1b_1 + (z_1^2 - 1)a_2^2 + z_2^2b_2^2 + 2|z_1||z_2||a_2||b_2| - a_1^2. \end{aligned} \quad (7)$$

Clearly, if $|a_2| \geq |a_1|$, then the equation (7) $\geq (z_1^2 - 1)a_2^2 - a_1^2 \geq 3a_2^2 - a_1^2 \geq 0$, and, if $|b_2| \geq |a_1|$, then the equation (7) $\geq z_2^2b_2^2 - a_1^2 \geq b_2^2 - a_1^2 \geq 0$. Consequently, the left case is $|a_1| > |a_2| \wedge |a_1| > |b_2|$. From $|a_1| > |a_2|$ and the definition of the reduced base, we know $|b_1| \leq |b_2|$, and, $|a_1| > |b_2|$ and $a_1^2 + a_2^2 \leq b_1^2 + b_2^2$ (equation (5)) implies $|a_2| < |b_1|$. That is, the left case is

$$|a_2| < |b_1| \leq |b_2| < |a_1|.$$

In this case, if $|z_2| \geq 2$, then the equation (7) $\geq z_2^2b_2^2 - a_1^2 \geq 4b_2^2 - a_1^2 \geq 2b_1^2 + 2b_2^2 - a_1^2 \geq 2(a_1^2 + a_2^2) - a_1^2 \geq 0$. If $|z_2| = 1$, the equation (7) is

$$\begin{aligned} & z_1^2(a_1^2 + a_2^2) + (b_1^2 + b_2^2) - (a_1^2 + a_2^2) - 2|z_1|a_1b_1 + 2|z_1||a_2||b_2| \\ & \geq z_1^2a_1^2 - 2|z_1|a_1b_1 \geq z_1^2|a_1||b_1| - 2|z_1|a_1b_1 = (z_1^2 - 2|z_1|)a_1b_1 \geq 0. \end{aligned}$$

- (2) $\mathbf{u} = \mathbf{a} + \mathbf{b}$. In this case, we need to prove

$$\|z_1\mathbf{a} + z_2\mathbf{b}\| \geq \|\mathbf{a} + \mathbf{b}\| \iff (z_1^2 - 1)(a_1^2 + a_2^2) + (z_2^2 - 1)(b_1^2 + b_2^2) + 2(z_1z_2 - 1)(a_1b_1 + a_2b_2) \geq 0. \quad (8)$$

From $\|\mathbf{a} + \mathbf{b}\|_2 \leq \|\mathbf{a}\|_2 \leq \|\mathbf{b}\|_2$, we have

$$a_1b_1 + a_2b_2 < 0 \wedge a_1^2 + a_2^2 \leq b_1^2 + b_2^2 \leq -2(a_1b_1 + a_2b_2) = 2(|a_2||b_2| - |a_1||b_1|) \leq (a_1^2 + a_2^2) + (b_1^2 + b_2^2). \quad (9)$$

Since $a_1b_1 + a_2b_2 < 0$, the target inequality (8) clearly holds if $z_1z_2 - 1 \leq 0$. We only need to consider the case that $z_1z_2 > 1$.

In fact, by equation (9),

$$\begin{aligned} & (z_1^2 - 1)(a_1^2 + a_2^2) + (z_2^2 - 1)(b_1^2 + b_2^2) + 2(z_1z_2 - 1)(a_1b_1 + a_2b_2) \\ & = (z_1^2 - 1)(a_1^2 + a_2^2) + (z_2^2 - 1)(b_1^2 + b_2^2) + 2z_1z_2(a_1b_1 + a_2b_2) - 2(a_1b_1 + a_2b_2) \\ & = z_1^2a_1^2 + z_1^2a_2^2 - (a_1^2 + a_2^2) + z_2^2b_1^2 + z_2^2b_2^2 - (b_1^2 + b_2^2) - 2z_1z_2|a_2||b_2| + 2z_1z_2|a_1||b_1| - 2(a_1b_1 + a_2b_2) \\ & = (z_1^2a_2^2 - 2z_1z_2|a_2||b_2| + z_2^2b_2^2) + 2z_1z_2|a_1||b_1| + (z_1^2 - 1)a_1^2 + z_2^2b_1^2 + (-2(a_1b_1 + a_2b_2) - (b_1^2 + b_2^2)) - a_2^2 \end{aligned} \quad (10)$$

$$= (z_1^2a_2^2 - 2z_1z_2|a_2||b_2| + z_2^2b_2^2) + 2z_1z_2|a_1||b_1| + z_1^2a_1^2 + (z_2^2 - 1)b_1^2 + (-2(a_1b_1 + a_2b_2) - (a_1^2 + a_2^2)) - b_2^2 \quad (11)$$

If $|b_1| \geq |a_2|$, then the equation (10) $\geq z_2^2 b_1^2 - a_2^2 \geq b_1^2 - a_2^2 \geq 0$. Hence, we only argue the case that $|b_1| < |a_2|$. Here, since $a_1^2 + a_2^2 \leq b_1^2 + b_2^2$, we have $|b_2| > |a_1|$. Also, $(|a_1| - |a_2|)(|b_1| - |b_2|) \leq 0$ implies that (1) $|b_1| < |a_2| \leq |a_1| < |b_2|$ or (2) $|a_1| < |b_2| \leq |b_1| < |a_2|$. Now, we argue each case as follows.

- $|b_1| < |a_2| \leq |a_1| < |b_2|$. If $|z_1| \neq 1$, then the equation (10) $\geq (z_1^2 - 1)a_1^2 - a_2^2 \geq 3a_1^2 - a_2^2 \geq 0$. If $|z_1| = 1$, then $|z_2| \geq 2$ and the equation (10) is

$$\begin{aligned} & z_2^2 b_1^2 + z_2^2 b_2^2 - 2|z_2||a_2||b_2| + 2|z_2||a_1||b_1| + (2(|a_2||b_2| - |a_1||b_1|) - (b_1^2 + b_2^2)) \\ & \geq z_2^2 b_2^2 - 2|z_2||a_2||b_2| \geq z_2^2 |a_2||b_2| - 2|z_2||a_2||b_2| = (z_2^2 - 2|z_2|)|a_2||b_2| \geq 0. \end{aligned}$$

- $|a_1| < |b_2| \leq |b_1| < |a_2|$. If $|z_2| \neq 1$, then the equation (11) $\geq (z_2^2 - 1)b_1^2 - b_2^2 \geq 3b_1^2 - b_2^2 \geq 0$. If $|z_2| = 1$, then $|z_1| \geq 2$ and the equation (11) is

$$\begin{aligned} & z_1^2 a_2^2 - 2|z_1||a_2||b_2| + 2|z_1||a_1||b_1| + z_1^2 a_1^2 + (-2(a_1 b_1 + a_2 b_2) - (a_1^2 + a_2^2)) \\ & \geq z_1^2 a_2^2 - 2|z_1||a_2||b_2| \geq z_1^2 |a_2||b_2| - 2|z_1||a_2||b_2| \geq (z_1^2 - 2|z_1|)|a_2||b_2| \geq 0. \end{aligned}$$

(3) $\mathbf{u} = \mathbf{a} - \mathbf{b}$. The proof for this case follows the same logic as case $\mathbf{u} = \mathbf{a} + \mathbf{b}$, and thus we omit the details.

Combining the three cases (1)-(3) above, we complete the proof of $\lambda_1(\mathcal{L})$. To prove $\lambda_2(\mathcal{L}) = \|\mathbf{v}\|_2$, by **Lemma 2**, it suffices to show that the pair $[\mathbf{u}, \mathbf{v}]$ is Lagrange-reduced, i.e.,

$$\|\mathbf{u}\|_2 \leq \|\mathbf{v}\|_2 \leq \min \{ \|\mathbf{u} + \mathbf{v}\|_2, \|\mathbf{u} - \mathbf{v}\|_2 \}.$$

In fact, by the choice of q , we have:

$$\begin{aligned} \|\mathbf{v}\|_2 &= \|\mathbf{x} - q\mathbf{u}\|_2 \leq \|\mathbf{x} - (q+1)\mathbf{u}\|_2 = \|\mathbf{v} - \mathbf{u}\|_2, \\ \|\mathbf{v}\|_2 &= \|\mathbf{x} - q\mathbf{u}\|_2 \leq \|\mathbf{x} - (q-1)\mathbf{u}\|_2 = \|\mathbf{v} + \mathbf{u}\|_2. \end{aligned}$$

Thus, the inequalities $\|\mathbf{v}\|_2 \leq \|\mathbf{u} \pm \mathbf{v}\|_2$ hold, completing the proof. \square

IV. OUR NEW REDUCED ALGORITHM AND ITS ANALYSIS

Building upon our new defined reduced basis (**Definition 7**) and its properties (**Theorem 1**), we introduce an algorithm that directly transforms any given two-dimensional lattice basis into a reduced basis. This approach eliminates the necessity for an initial conversion to HNF as employed by Eisenbrand [4].

A. Design Idea

For any input lattice basis $[\mathbf{a} \ \mathbf{b}]$ with $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$ and $\|\mathbf{a}\| \geq \|\mathbf{b}\|$, if it is not reduced, then we have two possible cases: (1) $a_1 a_2 b_1 b_2 > 0$ or (2) $a_1 a_2 b_1 b_2 \leq 0$ and $(|a_1| - |a_2|)(|b_1| - |b_2|) > 0$.

We first consider the case (2), without loss of generality, assume $a_1 \geq b_1 \geq 0$ and $a_2 b_2 \leq 0$. If these conditions are not met, we can adjust the basis vectors using negation or swapping operations to achieve them.

If $|a_1| > |a_2|$ and $|b_1| > |b_2|$, inspired by prior work [3, 4], we can compute a new basis $[\mathbf{b} \ \mathbf{c}]$ with $\mathbf{c} = \mathbf{a} - q\mathbf{b}$, where $q = \lfloor \frac{a_1}{b_1} \rfloor_o > 0$. Then

$$a_1 > b_1 > c_1 \geq 0, \quad b_2 c_2 \leq 0, \quad |c_2| = |a_2 - qb_2| = |a_2| + q|b_2| > |b_2|.$$

As a result, $b_1 b_2 c_1 c_2 \leq 0$. If $|c_1| - |c_2| \leq 0$, the new basis $[\mathbf{b} \ \mathbf{c}]$ is reduced. Otherwise, we have $|b_1| - |b_2| > |c_1| - |c_2| > 0$. Repeating this process iteratively reduces the difference between the absolute values of the first and second coordinates of the new vector until the terminal condition (the equation (2)) is satisfied.

If $|a_1| < |a_2|$ and $|b_1| < |b_2|$, in this case, we focus on the second coordinate. Using a similar process, we compute a new basis $[\mathbf{b} \ \mathbf{c}]$, where $\mathbf{c} = \mathbf{a} - q\mathbf{b}$ and $q = \lfloor \frac{a_2}{b_2} \rfloor_o \leq 0$. Then

$$c_1 > a_1 > b_1 \geq 0, \quad b_2 c_2 \leq 0, \quad |c_2| = |a_2 - qb_2| = |a_2| - |q||b_2| < |b_2|.$$

Thus, $b_1 b_2 c_1 c_2 \leq 0$. If $|c_1| - |c_2| \geq 0$, the new basis $[\mathbf{b} \ \mathbf{c}]$ is reduced. Otherwise, we have $|b_1| - |b_2| < |c_1| - |c_2| < 0$. Repeating this process iteratively reduces the difference between the absolute values of the coordinates until the terminal condition (the equation (2)) is satisfied.

For the case (1). When $a_1 a_2 b_1 b_2 > 0$, the key is to transform the basis such that $a_1 a_2 b_1 b_2 \leq 0$. Since \mathbf{a} and \mathbf{b} are linearly independent, it holds that $\frac{a_1}{b_1} \neq \frac{a_2}{b_2}$. Let $q_1 \triangleq \lfloor \frac{a_1}{b_1} \rfloor_o, q_2 \triangleq \lfloor \frac{a_2}{b_2} \rfloor_o$. If $q_1 \neq q_2$, we choose

$$q = \begin{cases} q_1, & \text{if } |a_1| \geq |a_2| \wedge q_1 \geq q_2, \\ q_1 + 1, & \text{if } |a_1| \geq |a_2| \wedge q_1 < q_2, \\ q_2, & \text{if } |a_1| < |a_2| \wedge q_2 \geq q_1, \\ q_2 + 1, & \text{if } |a_1| < |a_2| \wedge q_2 < q_1. \end{cases}$$

Then the new basis $[\mathbf{b} \ \mathbf{c}]$ with $\mathbf{c} = \mathbf{a} - q\mathbf{b}$ ensures $b_1 b_2 c_1 c_2 \leq 0$, achieving the goal. Otherwise $q = q_1 = q_2$, iteratively reduce the basis $[\mathbf{b} \ \mathbf{c}]$ with the same method until $q_1 \neq q_2$.

B. Algorithm Description and Analysis

Based on the proposed design concept, the detailed steps of our algorithm are provided in **Algorithm 3**. It should be noted that the **Algorithm 3** invokes two sub-algorithms: **UMTrans1*** and **UMTrans2***, which are variants of **UMTrans1** (**Algorithm 1**) and **UMTrans2** (**Algorithm 2**), respectively. The only difference is whether the returned result includes the integer q .

Before discussing the correctness and complexity of **Algorithm 3**, we first present two lemmas to analyze the properties of **Algorithm 1** and **Algorithm 2**.

Algorithm 1 UMTrans1(a, b)

Input: A basis $[\mathbf{a} \ \mathbf{b}]$ where $\mathbf{a} = (a_1 \ a_2)^T$ and $\mathbf{b} = (b_1 \ b_2)^T$, satisfying $a_1 a_2 b_1 b_2 > 0$

Output: A new base $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$ and an integer q

- 1: **if** ($|a_1| \geq |a_2|$)
 - 2: $q := \lfloor \frac{a_1}{b_1} \rfloor_o$
 - 3: **if** ($|a_2 - qb_2| \geq |b_2| \wedge \text{sgn}(a_2) = \text{sgn}(a_2 - qb_2)$), $q := q + 1$
 - 4: **else**
 - 5: $q := \lfloor \frac{a_2}{b_2} \rfloor_o$
 - 6: **if** ($|a_1 - qb_1| \geq |b_1| \wedge \text{sgn}(a_1) = \text{sgn}(a_1 - qb_1)$), $q := q + 1$
 - 7: $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a} - q\mathbf{b})$
 - 8: **return** $\mathbf{a}, \mathbf{b}, q$
-

Algorithm 2 UMTrans2(a, b)

Input: A basis $[\mathbf{a} \ \mathbf{b}]$ where $\mathbf{a} = (a_1 \ a_2)^T$ and $\mathbf{b} = (b_1 \ b_2)^T$, satisfying $a_1 a_2 b_1 b_2 \leq 0$ and $(|a_1| - |a_2|)(|b_1| - |b_2|) > 0$

Output: A new basis $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$ and an integer q

- 1: **if** ($|a_1| > |a_2|$)
 - 2: $q := \lfloor \frac{a_1}{b_1} \rfloor_o$
 - 3: **else**
 - 4: $q := \lfloor \frac{a_2}{b_2} \rfloor_o$
 - 5: $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a} - q\mathbf{b})$
 - 6: **return** $\mathbf{a}, \mathbf{b}, q$
-

Algorithm 3 CrossEuc(a, b)

Input: A basis $[\mathbf{a} \ \mathbf{b}] \in \mathbb{Z}^{2 \times 2}$ with $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$

Output: A new basis $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$ satisfy $a_1 a_2 b_1 b_2 \leq 0 \wedge (|a_1| - |a_2|)(|b_1| - |b_2|) \leq 0$

- 1: **While** ($a_1 a_2 b_1 b_2 > 0$), **do**
 - 2: $(\mathbf{a}, \mathbf{b}) \leftarrow \text{UMTrans1}^*(\mathbf{a}, \mathbf{b})$
 - 3: **Endwhile**
 - 4: **While** ($(|a_1| - |a_2|)(|b_1| - |b_2|) > 0$), **do**
 - 5: $(\mathbf{a}, \mathbf{b}) \leftarrow \text{UMTrans2}^*(\mathbf{a}, \mathbf{b})$
 - 6: **Endwhile**
 - 7: **If** ($(a_1 b_1 = 0 \wedge \text{sgn}(a_2) \neq \text{sgn}(b_2))$ or $(a_2 b_2 = 0 \wedge \text{sgn}(a_1) \neq \text{sgn}(b_1))$), $\mathbf{b} := -\mathbf{b}$.
 - 8: **If** $\|\mathbf{a}\| > \|\mathbf{b}\|$, **Swap**(\mathbf{a}, \mathbf{b})
 - 9: **If** $\mathbf{a} = [0, 0]$, **Return**[\mathbf{a}, \mathbf{b}]
 - 10: **Else**
 - 11: **if** ($a_2 b_2 \leq 0$)
 - 12: $\mathbf{b} := \min \left\{ \mathbf{b} - \lfloor \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \rfloor \mathbf{a}, \mathbf{b} - \lceil \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \rceil \mathbf{a} \right\}$
 - 13: **else**
 - 14: $\mathbf{b} := \min \left\{ \mathbf{b} - \lfloor \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \rfloor \mathbf{a}, \mathbf{b} - \lceil \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \rceil \mathbf{a} \right\}$
 - 15: **Return** [$\mathbf{a} \ \mathbf{b}$].
-

Lemma 5. For any lattice basis \mathbf{B} defined in equation (1) satisfying $\|\mathbf{a}\| \geq \|\mathbf{b}\|$ and $a_1 a_2 b_1 b_2 > 0$, let $q_i = \lfloor \frac{a_i}{b_i} \rfloor_o$ for $i = 1, 2$. If $|a_1| \geq |a_2|$, define

$$q := \begin{cases} q_1, & \text{if } q_1 \geq q_2, \\ q_1 + 1, & \text{if } q_1 < q_2. \end{cases}$$

If $|a_1| < |a_2|$, define

$$q := \begin{cases} q_2, & \text{if } q_2 \geq q_1, \\ q_2 + 1, & \text{if } q_2 < q_1. \end{cases}$$

Then the new matrix

$$\mathbf{B}' = [\mathbf{a}' \ \mathbf{b}'] = \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := [\mathbf{b} \ \mathbf{a} - q\mathbf{b}] = \mathbf{B} \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \in \mathbb{R}^{2 \times 2}$$

forms a valid basis, satisfying one of the following conditions:

- 1) $a'_1 a'_2 b'_1 b'_2 \leq 0$, with $(\|\mathbf{a}'\| = \|\mathbf{b}'\|) \wedge (\|\mathbf{b}'\| < \max\{\|\mathbf{a}\| \cdot \|\mathbf{b}\|, \|\mathbf{a}\|, \|\mathbf{b}\|\})$ or
- 2) $a'_1 a'_2 b'_1 b'_2 > 0$, with $(\|\mathbf{b}'\| \leq \min\{\|\mathbf{a} - \mathbf{b}\|, \|\mathbf{a} + \mathbf{b}\|\}) \wedge (\|\mathbf{b}'\| < \|\mathbf{a}'\|) \wedge (\|\mathbf{b}'\| < \frac{1}{2}\|\mathbf{a}\|)$.

Proof. Due to the property of the unimodular matrix transformation, it is evident that \mathbf{B}' forms a basis. Without loss of generality, we assume $a_1 b_1 > 0$ and $a_2 b_2 > 0$, focusing on the case where $|a_1| \geq |a_2|$; the argument for $|a_1| < |a_2|$ follows analogously.

Let $a_1 = q_1 b_1 + r_1$ and $a_2 = q_2 b_2 + r_2$. Then $\text{sgn}(r_1) = \text{sgn}(a_1) = \text{sgn}(b_1)$, $\text{sgn}(r_2) = \text{sgn}(a_2) = \text{sgn}(b_2)$, and $0 \leq |r_1| < |b_1|, 0 \leq |r_2| < |b_2|$.

(1) $q_1 > q_2$. In this case,

$$\begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := \begin{pmatrix} b_1 & a_1 - q_1 b_1 \\ b_2 & a_2 - q_1 b_2 \end{pmatrix}.$$

Clearly, $\text{sgn}(a'_1) = \text{sgn}(b_1) = \text{sgn}(a_1 - q_1 b_1) = \text{sgn}(b'_1)$. Assuming $q_1 = q_2 + k$ with $1 \leq k \leq q_1 = \lfloor \frac{a_1}{b_1} \rfloor_o \leq \frac{a_1}{b_1}$, we have

$$\begin{aligned} 0 &\leq |a_2 - q_2 b_2| = |r_2| < |b_2| \\ \implies (k-1)|b_2| &< |a_2 - q_1 b_2| = |r_2 - k b_2| = k|b_2| - |r_2| \leq k|b_2| \leq \frac{a_1}{b_1} |b_2| \leq |a_1| |b_2| \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \\ \implies \|\mathbf{b}'\| &= \max\{|a_1 - q_1 b_1|, |a_2 - q_1 b_2|\} = \max\{|r_1|, |r_2 - k b_2|\} \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \end{aligned}$$

and $\text{sgn}(a'_2) = \text{sgn}(b_2) \neq \text{sgn}(a_2 - q_1 b_2) = \text{sgn}(b'_2)$, which implies $a'_1 a'_2 b'_1 b'_2 \leq 0$.

(2) $q_1 < q_2$. In this case,

$$\begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := \begin{pmatrix} b_1 & a_1 - (q_1 + 1)b_1 \\ b_2 & a_2 - (q_1 + 1)b_2 \end{pmatrix}.$$

Clearly, $|b'_1| = |a_1 - (q_1 + 1)b_1| = |r_1 - b_1| \leq |b_1| = |a'_1|$, and $\text{sgn}(a'_1) = \text{sgn}(b_1) \neq \text{sgn}(a_1 - (q_1 + 1)b_1) = \text{sgn}(b'_1)$. Assuming $q_2 = q_1 + k$ with $k \geq 1$, we have

$$\begin{aligned} |a_2 - (q_1 + 1)b_2| &= |a_2 - (q_2 - k + 1)b_2| = |r_2 + (k-1)b_2| < k|b_2| < q_2 |b_2| < |a_2| \leq \|\mathbf{a}\| \\ \implies \|\mathbf{b}'\| &= \max\{|b'_1|, |b'_2|\} = \max\{|r_1 - b_1|, |r_2 + (k-1)b_2|\} \leq \max\{|b_1|, |a_2|\} \leq \max\{\|\mathbf{a}\|, \|\mathbf{b}\|\}, \end{aligned}$$

and $\text{sgn}(a'_2) = \text{sgn}(b_2) = \text{sgn}(a_2 - (q_1 + 1)b_2) = \text{sgn}(b'_2)$, leading to $a'_1 a'_2 b'_1 b'_2 \leq 0$.

(3) $q_1 = q_2$. In this case,

$$\begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := \begin{pmatrix} b_1 & a_1 - q_1 b_1 \\ b_2 & a_2 - q_1 b_2 \end{pmatrix} = \begin{pmatrix} b_1 & r_1 \\ b_2 & r_2 \end{pmatrix}.$$

If $r_1 = 0$ or $r_2 = 0$, then $a'_1 a'_2 b'_1 b'_2 \leq 0$ and $\max\{|a'_1|, |a'_2|, |b'_1|, |b'_2|\} = \max\{|b_1|, |b_2|\}$. Otherwise, $a'_1 a'_2 b'_1 b'_2 > 0$ and

$$\begin{aligned} &\left. \begin{aligned} (|b'_1| = |r_1| = |a_1 - q_1 b_1| \leq \min\{|a_1 - b_1|, |a_1 + b_1|\}) \wedge (|b'_1| = |r_1| < |b_1| = |a'_1|) \wedge (|b'_1| = |r_1| < \frac{|a_1|}{2}), \\ (|b'_2| = |r_2| = |a_2 - q_2 b_2| \leq \min\{|a_2 - b_2|, |a_2 + b_2|\}) \wedge (|b'_2| = |r_2| < |b_2| = |a'_2|) \wedge (|b'_2| = |r_2| < \frac{|a_2|}{2}). \end{aligned} \right\} \\ \implies (\|\mathbf{b}'\| \leq \min\{\|\mathbf{a} - \mathbf{b}\|, \|\mathbf{a} + \mathbf{b}\|\}) \wedge (\|\mathbf{b}'\| < \|\mathbf{a}'\|) \wedge (\|\mathbf{b}'\| < \frac{1}{2}\|\mathbf{a}\|). \end{aligned}$$

□

Lemma 6. Let \mathbf{B} be a lattice basis as defined in equation (1) satisfying $\|\mathbf{a}\| \geq \|\mathbf{b}\|$, $a_1 a_2 b_1 b_2 \leq 0$ and $(|a_1| - |a_2|)(|b_1| - |b_2|) > 0$.

If $|a_1| > |a_2|$, define $q_1 = \lfloor \frac{a_1}{b_1} \rfloor_o$ and

$$\mathbf{B}' = [\mathbf{a}' \ \mathbf{b}'] = \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := \begin{pmatrix} b_1 & a_1 - q_1 b_1 \\ b_2 & a_2 - q_1 b_2 \end{pmatrix} = [\mathbf{b} \ \mathbf{a} - q_1 \mathbf{b}] = \mathbf{B} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

If $|a_1| < |a_2|$, define $q_2 = \lfloor \frac{a_2}{b_2} \rfloor_o$ and

$$\mathbf{B}' = [\mathbf{a}' \ \mathbf{b}'] = \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} := \begin{pmatrix} b_1 & a_1 - q_2 b_1 \\ b_2 & a_2 - q_2 b_2 \end{pmatrix} = [\mathbf{b} \ \mathbf{a} - q_2 \mathbf{b}] = \mathbf{B} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}$$

Then the new matrix \mathbf{B}' forms a valid basis, satisfying one of the following conditions:

1) \mathbf{B}' is reduced, or

2) $a'_1 a'_2 b'_1 b'_2 \leq 0$, with $(\|\mathbf{b}'\| \leq \min\{\|\mathbf{a} - \mathbf{b}\|, \|\mathbf{a} + \mathbf{b}\|\}) \wedge (\|\mathbf{b}'\| < \|\mathbf{a}'\|) \wedge (\|\mathbf{b}'\| < \frac{1}{2}\|\mathbf{a}\|) \wedge (|b'_1| - |b'_2| < \frac{\|a_1| - |a_2||}{2})$.

Proof. Clearly, \mathbf{B}' forms a basis as a direct consequence of the properties of unimodular matrix transformations. Without loss of generality, we focus on the case where $|a_1| > |a_2|$; the argument for $|a_1| < |a_2|$ follows analogously.

In case that $|a_1| > |a_2|$, since $a_1 a_2 b_1 b_2 \leq 0$ and $(|a_1| - |a_2|)(|b_1| - |b_2|) > 0$, we have $|a_1| > |a_2| \geq 0$, $|b_1| > |b_2| \geq 0$ and, without loss of generality, we assume $a_1 b_1 > 0$ and $a_2 b_2 \leq 0$. Let $a_1 = q_1 b_1 + r_1$. Then $q_1 > 0$, $\text{sgn}(r_1) = \text{sgn}(a_1) = \text{sgn}(b_1)$, and

$$0 \leq |r_1| < |b_1| \implies 0 \leq |r_1| < \frac{|a_1|}{2}.$$

Additionally, $\text{sgn}(a'_1) = \text{sgn}(b_1) = \text{sgn}(a_1 - q_1 b_1) = \text{sgn}(b'_1)$ and $\text{sgn}(a'_2) = \text{sgn}(b_2) \neq \text{sgn}(a_2 - q_1 b_2) = \text{sgn}(b'_2)$, which implies $a'_1 a'_2 b'_1 b'_2 \leq 0$. Furthermore, if $|b'_1| - |b'_2| \leq 0$, then $(|a'_1| - |a'_2|)(|b'_1| - |b'_2|) \leq 0$ and thus \mathbf{B}' is reduced. Otherwise, $|b'_2| < |b'_1| = |r_1|$, which implies

$$\|\mathbf{b}'\| = \max\{|b'_1|, |b'_2|\} = |b'_1| = |r_1| = |a_1 - q_1 b_1| \leq \min\{|a_1 - b_1|, |a_1 + b_1|\} \leq \min\{\|\mathbf{a} - \mathbf{b}\|, \|\mathbf{a} + \mathbf{b}\|\},$$

$$\|\mathbf{b}'\| = \max\{|b'_1|, |b'_2|\} = |b'_1| = |r_1| < |b_1| \leq \max\{|b_1|, |b_2|\} = \|\mathbf{b}\| = \|\mathbf{a}'\|,$$

$$\|\mathbf{b}'\| = \max\{|b'_1|, |b'_2|\} = |b'_1| = |r_1| < \frac{|a_1|}{2} = \frac{1}{2} \max\{|a_1|, |a_2|\} = \frac{1}{2} \|\mathbf{a}\|,$$

$$|b'_1| - |b'_2| = |r_1| - |a_2 - q_1 b_2| = |r_1| - (|a_2| + q_1 |b_2|) \leq |r_1| - |a_2| < \frac{|a_1| - |a_2|}{2}.$$

□

Based on **Lemma 5** and **Lemma 6**, we can establish the correctness and complexity of **Algorithm 3**. Specifically, the following theorem holds

Theorem 3. Given a lattice basis $\mathbf{B} = [\mathbf{a} \ \mathbf{b}] \in \mathbb{Z}^{2 \times 2}$ with $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$, and $\#(\mathbf{a}, \mathbf{b}) = n$, **Algorithm 3** outputs a basis $\mathbf{B}' = [\mathbf{a}' \ \mathbf{b}']$ satisfying $\|\mathbf{a}'\| = \lambda_1(L(\mathbf{B}))$ and $\|\mathbf{b}'\| = \lambda_2(L(\mathbf{B}))$ with a time complexity of $O(n^2)$.

Proof. If the input lattice basis satisfies $a_1 a_2 b_1 b_2 > 0$, we assume that the reduced lattice basis sequence in the first **While** loop of **Algorithm 3** is as follows:

$$\begin{aligned} \mathbf{B}^{(0)} = [\mathbf{a}^{(0)} \ \mathbf{b}^{(0)}] &= \begin{pmatrix} a_1^{(0)} & b_1^{(0)} \\ a_2^{(0)} & b_2^{(0)} \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \rightarrow \mathbf{B}^{(1)} = [\mathbf{a}^{(1)} \ \mathbf{b}^{(1)}] = \begin{pmatrix} a_1^{(1)} & b_1^{(1)} \\ a_2^{(1)} & b_2^{(1)} \end{pmatrix} \rightarrow \dots \\ \rightarrow \mathbf{B}^{(k-1)} = [\mathbf{a}^{(k-1)} \ \mathbf{b}^{(k-1)}] &= \begin{pmatrix} a_1^{(k-1)} & b_1^{(k-1)} \\ a_2^{(k-1)} & b_2^{(k-1)} \end{pmatrix} \rightarrow \mathbf{B}^{(k)} = [\mathbf{a}^{(k)} \ \mathbf{b}^{(k)}] = \begin{pmatrix} a_1^{(k)} & b_1^{(k)} \\ a_2^{(k)} & b_2^{(k)} \end{pmatrix}, \end{aligned} \quad (12)$$

where $\mathbf{a}^{(i)} = \mathbf{b}^{(i-1)}$ for $i = 1, \dots, k$, and, with loss of generality, we assume k is even. By **Lemma 5**, we have $a_1^{(k)} a_2^{(k)} b_1^{(k)} b_2^{(k)} \leq 0$ and

$$\begin{aligned} \|\mathbf{a}^{(k)}\| &= \|\mathbf{b}^{(k-1)}\| < \frac{1}{2} \|\mathbf{a}^{(k-2)}\| < \dots < \frac{1}{2^{k/2}} \|\mathbf{a}\|, \\ \|\mathbf{a}^{(k-1)}\| &< \frac{1}{2} \|\mathbf{a}^{(k-3)}\| < \dots < \frac{1}{2^{(k-2)/2}} \|\mathbf{a}^{(1)}\| = \frac{1}{2^{(k-2)/2}} \|\mathbf{b}\| \\ \|\mathbf{b}^{(k)}\| &< \|\mathbf{a}^{(k-1)}\| \cdot \|\mathbf{b}^{(k-1)}\| < \frac{1}{2^{k/2}} \|\mathbf{a}\| \cdot \frac{1}{2^{(k-2)/2}} \|\mathbf{b}\| = \frac{1}{2^{k-1}} \|\mathbf{a}\| \cdot \|\mathbf{b}\|. \end{aligned}$$

Since $1 \leq \min\{\|\mathbf{a}^{(k)}\|, \|\mathbf{b}^{(k)}\|\} < \frac{1}{2^{k-1}} \|\mathbf{a}\| \cdot \|\mathbf{b}\|$, it follows that $k < \log \|\mathbf{a}\| + \log \|\mathbf{b}\| + 1$ is finite.

Further, if $(|a_1^{(k)}| - |a_2^{(k)}|)(|b_1^{(k)}| - |b_2^{(k)}|) > 0$, then during the second **While** loop, we assume the reduced lattice basis sequence is

$$\begin{aligned} \mathbf{B}^{(k)} = [\mathbf{a}^{(k)} \ \mathbf{b}^{(k)}] &= \begin{pmatrix} a_1^{(k)} & b_1^{(k)} \\ a_2^{(k)} & b_2^{(k)} \end{pmatrix} \rightarrow \mathbf{B}^{(k+1)} = [\mathbf{a}^{(k+1)} \ \mathbf{b}^{(k+1)}] = \begin{pmatrix} a_1^{(k+1)} & b_1^{(k+1)} \\ a_2^{(k+1)} & b_2^{(k+1)} \end{pmatrix} \rightarrow \dots \\ \rightarrow \mathbf{B}^{(k+s-1)} = [\mathbf{a}^{(k+s-1)} \ \mathbf{b}^{(k+s-1)}] &= \begin{pmatrix} a_1^{(k+s-1)} & b_1^{(k+s-1)} \\ a_2^{(k+s-1)} & b_2^{(k+s-1)} \end{pmatrix} \rightarrow \mathbf{B}^{(k+s)} = [\mathbf{a}^{(k+s)} \ \mathbf{b}^{(k+s)}] = \begin{pmatrix} a_1^{(k+s)} & b_1^{(k+s)} \\ a_2^{(k+s)} & b_2^{(k+s)} \end{pmatrix}, \end{aligned} \quad (13)$$

where $\mathbf{a}^{(k+i)} = \mathbf{b}^{(k+i-1)}$ for $i = 1, \dots, s$, and, without loss of generality, we assume s is even. Then, by **Lemma 6**, we have $a_1^{(k+i)} a_2^{(k+i)} b_1^{(k+i)} b_2^{(k+i)} \leq 0$ for $i = 0, \dots, s$,

$$1 \leq |a_1^{(k+s)}| - |a_2^{(k+s)}| = |b_1^{(k+(s-1))}| - |b_2^{(k+(s-1))}| < \frac{|a_1^{(k+(s-2))}| - |a_2^{(k+(s-2))}|}{2} < \dots < \frac{|a_1^{(k)}| - |a_2^{(k)}|}{2^{s/2}},$$

and $|b_1^{(k+s)}| - |b_2^{(k+s)}| \leq 0$. Consequently, after the second **While** loop, we have

$$a_1^{(k+s)} a_2^{(k+s)} b_1^{(k+s)} b_2^{(k+s)} \leq 0 \wedge (|a_1^{(k+s)}| - |a_2^{(k+s)}|)(|b_1^{(k+s)}| - |b_2^{(k+s)}|) \leq 0,$$

and thus, the lattice basis $\mathbf{B}^{(k+s)} = [\mathbf{a}^{(k+s)} \ \mathbf{b}^{(k+s)}]$ is reduced. Finally, by **Theorem 1**, the returned basis $\mathbf{B}' = [\mathbf{a}' \ \mathbf{b}']$ of **Algorithm 3** satisfies $\|\mathbf{a}'\| = \lambda_1(L(\mathbf{B}))$ and $\|\mathbf{b}'\| = \lambda_2(L(\mathbf{B}))$

Now, we estimate the time complexity. Without loss of generality, we assume $\|\mathbf{a}^{(0)}\| \geq \|\mathbf{b}^{(0)}\|$, $\#\mathbf{a}^{(i)} = n_i$ and $\#q^{(i)} = \ell_i$ for $i = 1, \dots, k, k+1, \dots, k+s$. For the first **While** loop, since $\mathbf{a}^{(i-1)} = q^{(i)}\mathbf{b}^{(i-1)} + \mathbf{b}^{(i)} = q^{(i)}\mathbf{a}^{(i)} + \mathbf{a}^{(i+1)}$, where

$$q^{(i)} \in \left\{ \left\lfloor \frac{a_1^{(i-1)}}{b_1^{(i-1)}} \right\rfloor_0 = \left\lfloor \frac{a_1^{(i-1)}}{a_1^{(i)}} \right\rfloor_0, \left\lfloor \frac{a_1^{(i-1)}}{b_1^{(i-1)}} \right\rfloor_0 + 1 = \left\lfloor \frac{a_1^{(i-1)}}{a_1^{(i)}} \right\rfloor_0 + 1, \right. \\ \left. \left\lfloor \frac{a_2^{(i-1)}}{b_2^{(i-1)}} \right\rfloor_0 = \left\lfloor \frac{a_2^{(i-1)}}{a_2^{(i)}} \right\rfloor_0, \left\lfloor \frac{a_2^{(i-1)}}{b_2^{(i-1)}} \right\rfloor_0 + 1 = \left\lfloor \frac{a_2^{(i-1)}}{a_2^{(i)}} \right\rfloor_0 + 1 \right\}, \quad (14)$$

we have $n_{i-1} = n_i + \ell_i$. Therefore, in each loop, the time complexity of division is bounded by $O(n_{i-1}\ell_i)$ and the time complexity of multiplication is bounded by $O(n_i\ell_i)$. Consequently, the total complexity of the first **While** loop is $T_1 = O(\sum_{i=1}^k (n_{i-1}\ell_i + n_i\ell_i)) = O(\sum_{i=1}^k (n_i + n_{i-1})(n_{i-1} - n_i)) = O(\sum_{i=1}^k (n_{i-1}^2 - n_i^2)) = O(n_0^2 - n_k^2)$. Similarly, for the second **While** loop, the total complexity is $T_2 = O(\sum_{i=k+1}^{k+s} (n_{i-1}\ell_i + n_i\ell_i)) = O(\sum_{i=k+1}^{k+s} (n_i + n_{i-1})(n_{i-1} - n_i)) = O(\sum_{i=k+1}^{k+s} (n_{i-1}^2 - n_i^2)) = O(n_k^2 - n_{k+s}^2)$. Therefore, the total complexity of **Algorithm 3** is $T = O(T_1 + T_2) = O(n_0^2) = O(n^2)$. \square

V. OPTIMIZED ALGORITHM AND ITS ANALYSIS

For two integers with bit lengths of n , the well-known Half-GCD algorithm [9, 10] can efficiently find two integers of approximately $n/2$ -bit length that share the same common divisor. Inspired by the Half-GCD algorithm, this section first explores the **HVec** algorithm, which rapidly reduces a lattice basis to a new basis with bit lengths approximately halved from the original, along with a complexity analysis. Furthermore, we leverage this algorithm to optimize and accelerate the **CrossEuc-SBP** algorithm presented in the previous section.

A. HVec algorithm and its analysis

Analogous to the case of two integers, our design for the input of two vectors is based on the following key observation:

Assume $[\mathbf{a}' \ \mathbf{b}']$ and $[\mathbf{c}' \ \mathbf{d}']$ are two different bases for the same lattice, *i.e.*,

$$[\mathbf{a}' \ \mathbf{b}'] = \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} = \begin{pmatrix} c'_1 & d'_1 \\ c'_2 & d'_2 \end{pmatrix} \mathbf{M}' = [\mathbf{c}' \ \mathbf{d}'] \mathbf{M}' \quad (15)$$

for some unimodular matrix \mathbf{M}' . The two new vectors

$$[\mathbf{a} \ \mathbf{b}] = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = 2^{n_\ell} \begin{pmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{pmatrix} + \begin{pmatrix} a''_1 & b''_1 \\ a''_2 & b''_2 \end{pmatrix} = 2^{n_\ell} [\mathbf{a}' \ \mathbf{b}'] + [\mathbf{a}'' \ \mathbf{b}''], \quad (16)$$

where $[\mathbf{a}'' \ \mathbf{b}'']$ represents the n_ℓ least significant bits, and $[\mathbf{a}' \ \mathbf{b}']$ refers to the $n_h = \#(\mathbf{a}, \mathbf{b}) - n_\ell$ most significant bits of $[\mathbf{a} \ \mathbf{b}]$. Additionally, the vectors $[\mathbf{c} \ \mathbf{d}]$ satisfy

$$[\mathbf{a} \ \mathbf{b}] = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = \begin{pmatrix} c_1 & d_1 \\ c_2 & d_2 \end{pmatrix} \mathbf{M}' = [\mathbf{c} \ \mathbf{d}] \mathbf{M}' \quad (17)$$

for the same unimodular matrix \mathbf{M}' . Then, we have

$$[\mathbf{c} \ \mathbf{d}] = [\mathbf{a} \ \mathbf{b}] (\mathbf{M}')^{-1} = 2^{n_\ell} [\mathbf{c}' \ \mathbf{d}'] + [\mathbf{a}'' \ \mathbf{b}''] (\mathbf{M}')^{-1} \quad (18)$$

Building on the above fact, we can halve the bit-length of $[\mathbf{a} \ \mathbf{b}]$ by adopting a recursive reduction strategy. **Algorithm 4** provides the details of our design. We now provide a rigorous theoretical analysis to establish the correctness and complexity of **Algorithm 4**. That is, we argue the following result:

Theorem 4. *For any input basis $\mathbf{B} = [\mathbf{a} \ \mathbf{b}] \in \mathbb{Z}^{2 \times 2}$ with $\#(\mathbf{a}, \mathbf{b}) = n$, **Algorithm 4** will output a new basis $\mathbf{B}' = [\mathbf{c} \ \mathbf{d}]$ and an unimodular matrix \mathbf{M} such that $[\mathbf{a} \ \mathbf{b}] = [\mathbf{c} \ \mathbf{d}] \mathbf{M}$ in time $T(n) = O(M(n) \log n)$, where $M(n)$ refers to the time complexity of multiplying two n -bit integers. Additionally, the basis $[\mathbf{c} \ \mathbf{d}]$ satisfies one of the following two conditions:*

- 1) $[\mathbf{c}, \mathbf{d}]$ is reduced, or
- 2) $\underline{\#}(\mathbf{c}, \mathbf{d}) > \lfloor \frac{n}{2} \rfloor + 1$, and $\underline{\#}(\mathbf{c} - \mathbf{d}, \mathbf{c} + \mathbf{d}) \leq \lfloor \frac{n}{2} \rfloor + 1$.

Proof. First, we argue that the algorithm will inevitably terminate. Assume

$$(\mathbf{c}^{new}, \mathbf{d}^{new}, q) \leftarrow \mathbf{UMTrans1}(\mathbf{c} \ \mathbf{d}) (\text{resp. } \mathbf{UMTrans2}(\mathbf{c} \ \mathbf{d})).$$

Algorithm 4 HVec(a b)

Input: Two vectors $\mathbf{a} = (a_1, a_2)^T$, $\mathbf{b} = (b_1, b_2)^T$ and $\#(\mathbf{a}, \mathbf{b}) = n$, $\#(\mathbf{a}, \mathbf{b}) > \lfloor \frac{n}{2} \rfloor + 1$, $\#(\mathbf{a} + \mathbf{b}, \mathbf{a} - \mathbf{b}) > \lfloor \frac{n}{2} \rfloor + 1$

Output: Two vectors $\mathbf{c} = (c_1, c_2)^T$, $\mathbf{d} = (d_1, d_2)^T$ and an unimodular matrix \mathbf{M} such that $[\mathbf{a} \ \mathbf{b}] = [\mathbf{c} \ \mathbf{d}]\mathbf{M}$. Meanwhile, either $(\#(\mathbf{c}, \mathbf{d}) \leq n) \wedge (\#(\mathbf{c}, \mathbf{d}) > \lfloor \frac{n}{2} \rfloor + 1) \wedge (\#(\mathbf{c} + \mathbf{d}, \mathbf{c} - \mathbf{d}) \leq \lfloor \frac{n}{2} \rfloor + 1)$, or $[\mathbf{c} \ \mathbf{d}]$ is reduced.

```

1:  $\mathbf{c} := \mathbf{a}, \mathbf{d} := \mathbf{b}, \mathbf{M} := \mathbf{I}$ 
2: if  $c_1 c_2 d_1 d_2 \leq 0 \wedge (|c_1| - |c_2|)(|d_1| - |d_2|) \leq 0$  then
3:   return  $\mathbf{c}, \mathbf{d}, \mathbf{M}$ 
4: end if
5:  $n := \#(\mathbf{c}, \mathbf{d})$ 
6:  $s := \lfloor \frac{n}{2} \rfloor + 1$ 
7: if  $\#(\mathbf{c}, \mathbf{d}) \geq \lfloor \frac{3}{4}n \rfloor + 2$ , then
8:    $n_{\ell 1} := \lfloor n/2 \rfloor$ 
9:    $a'_1 := \lfloor c_1/2^{n_{\ell 1}} \rfloor, a''_1 := c_1 - 2^{n_{\ell 1}} a'_1, a'_2 := \lfloor c_2/2^{n_{\ell 1}} \rfloor, a''_2 := c_2 - 2^{n_{\ell 1}} a'_2$ 
10:   $b'_1 := \lfloor d_1/2^{n_{\ell 1}} \rfloor, b''_1 := d_1 - 2^{n_{\ell 1}} b'_1, b'_2 := \lfloor d_2/2^{n_{\ell 1}} \rfloor, b''_2 := d_2 - 2^{n_{\ell 1}} b'_2$ 
11:   $\mathbf{a}' := (a'_1, a'_2)^T, \mathbf{b}' := (b'_1, b'_2)^T, \mathbf{a}'' := (a''_1, a''_2)^T, \mathbf{b}'' := (b''_1, b''_2)^T$ 
12:   $(\mathbf{c}', \mathbf{d}', \mathbf{M}'_1) \leftarrow \mathbf{HVec}(\mathbf{a}', \mathbf{b}')$ 
13:   $[\mathbf{c} \ \mathbf{d}] := 2^{n_{\ell 1}} [\mathbf{c}' \ \mathbf{d}'] + [\mathbf{a}'' \ \mathbf{b}''] (\mathbf{M}'_1)^{-1}$ 
14:   $\mathbf{M} := \mathbf{M}'_1 \mathbf{M}$ 
15: end if
16: while  $\#(\mathbf{c}, \mathbf{d}) > \lfloor 3n/4 \rfloor + 1$  and  $\#(\mathbf{c} - \mathbf{d}, \mathbf{c} + \mathbf{d}) > s$  do
17:   if  $(c_1 c_2 d_1 d_2 \leq 0 \wedge (|c_1| - |c_2|)(|d_1| - |d_2|) \leq 0)$ , return  $\mathbf{c}, \mathbf{d}, \mathbf{M}$ 
18:   if  $(c_1 c_2 d_1 d_2 > 0)$ ,
19:      $(\mathbf{c}, \mathbf{d}, q) \leftarrow \mathbf{UMTrans1}(\mathbf{c}, \mathbf{d})$ 
20:   else
21:      $(\mathbf{c}, \mathbf{d}, q) \leftarrow \mathbf{UMTrans2}(\mathbf{c}, \mathbf{d})$ 
22:   if  $(\# \mathbf{d} \leq s)$ ,  $q := q - 1, \mathbf{d} := \mathbf{c} + \mathbf{d}$ 
23:    $\mathbf{M} := \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \mathbf{M}$ 
24: end while
25: if  $\#(\mathbf{c}, \mathbf{d}) > s + 2$ , then
26:    $n' := \#(\mathbf{c}, \mathbf{d}), n_{\ell 2} := 2s - n' + 1$ 
27:    $a'_1 := \lfloor c_1/2^{n_{\ell 2}} \rfloor, a''_1 := c_1 - 2^{n_{\ell 2}} a'_1, a'_2 := \lfloor c_2/2^{n_{\ell 2}} \rfloor, a''_2 := c_2 - 2^{n_{\ell 2}} a'_2$ 
28:    $b'_1 := \lfloor d_1/2^{n_{\ell 2}} \rfloor, b''_1 := d_1 - 2^{n_{\ell 2}} b'_1, b'_2 := \lfloor d_2/2^{n_{\ell 2}} \rfloor, b''_2 := d_2 - 2^{n_{\ell 2}} b'_2$ 
29:    $\mathbf{a}' := (a'_1, a'_2)^T, \mathbf{b}' := (b'_1, b'_2)^T, \mathbf{a}'' := (a''_1, a''_2)^T, \mathbf{b}'' := (b''_1, b''_2)^T$ 
30:    $(\mathbf{c}', \mathbf{d}', \mathbf{M}'_2) \leftarrow \mathbf{HVec}(\mathbf{a}', \mathbf{b}')$ 
31:    $[\mathbf{c} \ \mathbf{d}] := 2^{n_{\ell 2}} [\mathbf{c}' \ \mathbf{d}'] + [\mathbf{a}'' \ \mathbf{b}''] (\mathbf{M}'_2)^{-1}$ 
32:    $\mathbf{M} := \mathbf{M}'_2 \mathbf{M}$ 
33: end if
34: while  $\#(\mathbf{c} - \mathbf{d}, \mathbf{c} + \mathbf{d}) > s$  do
35:   if  $(c_1 c_2 d_1 d_2 \leq 0 \wedge (|c_1| - |c_2|)(|d_1| - |d_2|) \leq 0)$ , return  $\mathbf{a}, \mathbf{b}, \mathbf{M}$ 
36:   if  $(c_1 c_2 d_1 d_2 > 0)$ ,
37:      $(\mathbf{c}, \mathbf{d}, q) \leftarrow \mathbf{UMTrans1}(\mathbf{c}, \mathbf{d})$ 
38:   else
39:      $(\mathbf{c}, \mathbf{d}, q) \leftarrow \mathbf{UMTrans2}(\mathbf{c}, \mathbf{d})$ 
40:   if  $(\# \mathbf{d} \leq s)$ ,  $q := q - 1, \mathbf{d} := \mathbf{c} + \mathbf{d}$ 
41:    $\mathbf{M} := \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \mathbf{M}$ 
42: end while
43: return  $\mathbf{c}, \mathbf{d}, \mathbf{M}$ 

```

Then, by **Lemma 5** and **Lemma 6**, if $[\mathbf{c}^{new}, \mathbf{d}^{new}]$ is not reduced, the following inequalities hold except for a special case where $c_1 c_2 d_1 d_2 > 0$ and $c_1^{new} c_2^{new} d_1^{new} d_2^{new} \leq 0$, which occurs only once during execution and can be ignored:

$$(\mathbf{c}^{new} = \mathbf{d}) \wedge (\|\mathbf{d}^{new}\| \leq \min\{\|\mathbf{c} - \mathbf{d}\|, \|\mathbf{c} + \mathbf{d}\|\}) \wedge (\|\mathbf{d}^{new}\| < \|\mathbf{c}^{new}\|) \wedge (\|\mathbf{d}^{new}\| < \frac{1}{2}\|\mathbf{c}\|),$$

which implies that

$$\#(\mathbf{c}^{(new)}, \mathbf{d}^{(new)}) < \#(\mathbf{c}, \mathbf{d}), \quad \#\mathbf{d}^{(new)} \leq \underline{\#}(\mathbf{c} + \mathbf{d}, \mathbf{c} - \mathbf{d}), \quad \#\mathbf{d}^{(new)} < \#\mathbf{c} - 1. \quad (19)$$

Meanwhile, steps 22 and 40 ensure that $\underline{\#}(\mathbf{c}^{(new)}, \mathbf{d}^{(new)}) > s = \lfloor \frac{n}{2} \rfloor + 1$. Consequently, the **While** conditions in Step 16 and Step 34 will eventually be violated. That is, **Algorithm 4** will terminate. Additionally, by equations (15)-(18) and the properties of the unimodular transformations **UMTrans1** and **UMTrans2**, the output $(\mathbf{c}, \mathbf{d}, \mathbf{M})$ satisfies $[\mathbf{a} \ \mathbf{b}] = [\mathbf{c} \ \mathbf{d}]\mathbf{M}$ and one of the following conditions holds:

- (1) $[\mathbf{c} \ \mathbf{d}]$ is reduced, or
- (2) $\underline{\#}(\mathbf{c}, \mathbf{d}) > \lfloor \frac{n}{2} \rfloor + 1$ and $\underline{\#}(\mathbf{c} - \mathbf{d}, \mathbf{c} + \mathbf{d}) \leq \lfloor \frac{n}{2} \rfloor + 1$.

Now, we estimate the time complexity. We need to estimate the bit size of the numbers and the time complexity of each **while** loop during execution. According to our recursive design, the underlying operations are the unimodular transformations **UMTrans1** and **UMTrans2**. For each recursive invocation $(\mathbf{c}', \mathbf{d}', \mathbf{M}') \leftarrow \mathbf{HVec}(\mathbf{a}' \ \mathbf{b}')$, we adopt the same notations as in the proof of **Theorem 3** for brevity. Assume that $\|\mathbf{a}'\| \geq \|\mathbf{b}'\|$ and the lattice basis sequence is given by

$$\mathbf{B}^{(0)} = [\mathbf{a}^{(0)} \ \mathbf{b}^{(0)}] = [\mathbf{a}' \ \mathbf{b}'] \rightarrow \mathbf{B}^{(1)} = [\mathbf{a}^{(1)} \ \mathbf{b}^{(1)}] \rightarrow \dots \rightarrow \mathbf{B}^{(m)} = [\mathbf{a}^{(m)} \ \mathbf{b}^{(m)}] = [\mathbf{c}' \ \mathbf{d}'],$$

where, for $i = 1, \dots, m$,

$$\mathbf{a}^{(i)} = \mathbf{b}^{(i-1)}, \quad \mathbf{a}^{(i-1)} = q^{(i)}\mathbf{b}^{(i-1)} + \mathbf{b}^{(i)} = q^{(i)}\mathbf{a}^{(i)} + \mathbf{a}^{(i+1)} \quad (20)$$

and $q^{(i)}$ is defined in equation (14). Then $[\mathbf{a}' \ \mathbf{b}'] = [\mathbf{c}' \ \mathbf{d}']\mathbf{M}'$ with

$$\mathbf{M}' = \begin{pmatrix} q^{(m)} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q^{(m-1)} & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} q^{(1)} & 1 \\ 1 & 0 \end{pmatrix}. \quad (21)$$

Furthermore, by **Lemma 5** and **Lemma 6**, the following inequalities hold for almost all $i \in \{1, \dots, m\}$, with at most one exception, which does not affect the proof and can be ignored:

$$\|\mathbf{a}^{(i+1)}\| = \|\mathbf{b}^{(i)}\| < \frac{1}{2}\|\mathbf{a}^{(i-1)}\| \quad \text{and} \quad \|\mathbf{b}^{(i)}\| < \|\mathbf{a}^{(i)}\|.$$

Then, the equation (20) indicate that $\#\mathbf{a}^{(i-1)} = \#q^{(i)} + \#\mathbf{a}^{(i)}$. While, the equation (21) implies that $\#\mathbf{M}' < \sum_{i=1}^m \#q^{(i)} + 1$. Hence,

$$\begin{aligned} \#\mathbf{a}^{(0)} &= \#q^{(1)} + \#\mathbf{a}^{(1)} = \sum_{i=1}^m \#q^{(i)} + \#\mathbf{a}^{(i)} > \#\mathbf{M}' - 1 + \#\mathbf{c}' \\ \implies \#\mathbf{M}' &< \#\mathbf{a}^{(0)} - \#\mathbf{c}' + 1 \leq \#(\mathbf{a}', \mathbf{b}') - \underline{\#}(\mathbf{c}', \mathbf{d}') + 1. \end{aligned} \quad (22)$$

Based on the above observation, in step 7-step 15, we have

$$\begin{aligned} \#(\mathbf{c}', \mathbf{d}') &\leq n - n_{\ell 1} \wedge \underline{\#}(\mathbf{c}', \mathbf{d}') > \lfloor \frac{n - n_{\ell 1}}{2} \rfloor + 1 \wedge \underline{\#}(\mathbf{c}' + \mathbf{d}', \mathbf{c}' - \mathbf{d}') \leq \lfloor \frac{n - n_{\ell 1}}{2} \rfloor + 1 \wedge \\ \#\mathbf{M}'_1 &\leq \#(\mathbf{a}', \mathbf{b}') - \underline{\#}(\mathbf{c}', \mathbf{d}') + 1 < n - n_{\ell 1} - (\lfloor \frac{n - n_{\ell 1}}{2} \rfloor + 1) + 1. \end{aligned}$$

Thus, the equation $[\mathbf{c} \ \mathbf{d}] = 2^{n_{\ell 1}}[\mathbf{c}' \ \mathbf{d}'] + [\mathbf{a}'' \ \mathbf{b}''](\mathbf{M}'_1)^{-1}$ in step 13 implies that

$$\begin{aligned} \#(\mathbf{c}, \mathbf{d}) &\leq \max\{n_{\ell 1} + \#(\mathbf{c}', \mathbf{d}'), n_{\ell 1} + \#\mathbf{M}'_1\} + 1 = n + 1, \\ \underline{\#}(\mathbf{c} \pm \mathbf{d}) &= \underline{\#}(2^{n_{\ell 1}}(\mathbf{c}' + \mathbf{d}') + (\mathbf{a}'' + \mathbf{b}'')(\mathbf{M}'_1)^{-1}, 2^{n_{\ell 1}}(\mathbf{c}' - \mathbf{d}') + (\mathbf{a}'' - \mathbf{b}'')(\mathbf{M}'_1)^{-1}) \\ &= \min\{\#(2^{n_{\ell 1}}(\mathbf{c}' + \mathbf{d}') + (\mathbf{a}'' + \mathbf{b}'')(\mathbf{M}'_1)^{-1}), \#(2^{n_{\ell 1}}(\mathbf{c}' - \mathbf{d}') + (\mathbf{a}'' - \mathbf{b}'')(\mathbf{M}'_1)^{-1})\} \\ &= \min\{\max\{n_{\ell 1} + \#(\mathbf{c}' + \mathbf{d}'), \#(\mathbf{a}'' + \mathbf{b}'') + \#\mathbf{M}'_1\} + 1, \max\{n_{\ell 1} + \#(\mathbf{c}' - \mathbf{d}'), \#(\mathbf{a}'' - \mathbf{b}'') + \#\mathbf{M}'_1\} + 1\} \\ &\leq \max\{n_{\ell 1} + \underline{\#}(\mathbf{c}' \pm \mathbf{d}'), \max\{\#\mathbf{a}'', \#\mathbf{b}''\} + 1 + \#\mathbf{M}'_1\} + 1 \\ &\leq \max\{n_{\ell 1} + \lfloor \frac{n - n_{\ell 1}}{2} \rfloor + 1, n_{\ell 1} + 1 + n - n_{\ell 1} - (\lfloor \frac{n - n_{\ell 1}}{2} \rfloor + 1) + 1\} \\ &= \max\{n_{\ell 1} + \lfloor \frac{n_{\ell 1}}{2} \rfloor + 1, n - \lfloor \frac{n_{\ell 1}}{2} \rfloor + 1\} < \frac{3n}{4} + 3 < \lfloor \frac{3n}{4} \rfloor + 4. \end{aligned}$$

By the equation (19), the bit length of the new vector generated by the unimodular matrix transformation **UMTrans1** (resp. **UMTrans2**) is less than $\min\{\#\underline{\mathbf{c}} + \mathbf{d}, \#\mathbf{c} - \mathbf{d}\}$. Therefore, the **while** loop in step 16 will terminate after at most 8 iterations and thus the time complexity is $O(M(n))$. Similarly, in step 25-step 33, we have

$$\begin{aligned} \#\mathbf{M}'_2 &\leq \#(\mathbf{a}', \mathbf{b}') - \#\underline{\mathbf{c}}(\mathbf{c}', \mathbf{d}') + 1 < n' - n_{\ell 2} - (\lfloor \frac{n' - n_{\ell 2}}{2} \rfloor + 1) + 1 = n' - s, \\ \#(\mathbf{c}, \mathbf{d}) &\leq \max\{n_{\ell 2} + \#\underline{\mathbf{c}}(\mathbf{c}', \mathbf{d}'), n_{\ell 2} + \#\mathbf{M}'_2\} + 1 = n' + 1, \\ \#\underline{\mathbf{c}}(\mathbf{c} \pm \mathbf{d}) &= \#\underline{\mathbf{c}}(2^{n_{\ell 2}}(\mathbf{c}' + \mathbf{d}') + (\mathbf{a}'' + \mathbf{b}'')(\mathbf{M}'_2)^{-1}, 2^{n_{\ell 2}}(\mathbf{c}' - \mathbf{d}') + (\mathbf{a}'' - \mathbf{b}'')(\mathbf{M}'_2)^{-1}) < s + 2. \end{aligned}$$

By the equation (19), the bit length of the new vector generated by the unimodular matrix transformation **UMTrans1** (resp. **UMTrans2**) is less than $\min\{\#\underline{\mathbf{c}} + \mathbf{d}, \#\mathbf{c} - \mathbf{d}\}$. Therefore, the **while** loop in step 34 will terminate after at most 4 iterations and thus the time complexity is $O(M(n))$. Overall, the total time complexity is

$$T(n) = 2T\left(\frac{n}{2}\right) + O(M(n)) = \left(2^2T\left(\frac{n}{2^2}\right) + O\left(2 \cdot M\left(\frac{n}{2}\right)\right)\right) + O(M(n)) = O\left(\sum_{i=0}^{\log n} 2^i M\left(\frac{n}{2^i}\right)\right).$$

Since $M\left(\frac{n}{2^i}\right) \leq \frac{1}{2^i}M(n)$ for $i = 0, \dots, \log n$,

$$T(n) = O\left(\sum_{i=0}^{\log n} 2^i M\left(\frac{n}{2^i}\right)\right) = O\left(M(n) \sum_{i=0}^{\log n} 1\right) = O(M(n) \log n).$$

□

B. HVecSBP algorithm and its analysis

By cyclically invoking the proposed **HVec** algorithm, the reduced basis can ultimately be obtained. This design, referred to as **HVecSBP**, is detailed in **Algorithm 5**. Clearly, by **Theorem 4**, the **HVecSBP** algorithm will output a reduced basis with a worst-case time complexity of

$$\begin{aligned} O\left(T(n) + T\left(\frac{n}{2}\right) + \dots + T\left(\frac{n}{2^{\log n}}\right)\right) &= O\left(M(n) \log n + M\left(\frac{n}{2}\right) \log \frac{n}{2} + \dots + M\left(\frac{n}{2^{\log n}}\right) \log \frac{n}{2^{\log n}}\right) \\ &= O\left(M(n) \log n + \frac{1}{2}M(n) \log n + \dots + \frac{1}{2^{\log n}}M(n) \log n\right) = O(M(n) \log n) \end{aligned}$$

VI. PRACTICAL PERFORMANCE EVALUATION

A. Experimental Methodology

It is evident that the practical performance of existing algorithms is closely related to the form of the input lattice basis. Therefore, we separately compare the performance for lattice bases in the special HNF and those in general form.

(1) Input lattice basis in HNF: Consider the input lattice basis $\mathbf{B} = [\mathbf{a} \ \mathbf{b}] = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, where $a > b > |c| > 0$. Note that in this case, our algorithm **CrossEuc** is identical to the continued fraction-based algorithm (**ParEuc**) [3, 4]. Thus, we only compare three algorithms: the optimized Lagrange algorithm under the ℓ_∞ metric (**GoLEuc**) [3, 5], the continued fraction-based algorithm (**ParEuc**) [3, 4], and our optimized algorithm (**HVec-SBP**).

(2) Input lattice basis in general form: For the input lattice basis $\mathbf{B} = [\mathbf{a} \ \mathbf{b}] = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$, we evaluate the practical performance of each algorithm based on the linear dependency between vectors \mathbf{a} and \mathbf{b} . We define the linear dependency measure $\Delta(\mathbf{a}, \mathbf{b})$ as:

$$\Delta(\mathbf{a}, \mathbf{b}) = \left| \frac{a_1}{b_1} - \frac{a_2}{b_2} \right|.$$

It is clear that a smaller Δ value indicates a higher degree of linear dependency between vectors \mathbf{a} and \mathbf{b} . In this case, we assessed the practical performance of the following six algorithms across different Δ values:

- **GoLEuc**: The optimized Lagrange algorithm under the ℓ_∞ metric presented in [3].
- **EEA-HNF-ParEuc**: An algorithm that first transforms the basis into Hermite Normal Form (HNF) using the extended Euclidean algorithm (EEA) and then reduces it with the continued fraction-based algorithm (**ParEuc**). Visually

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \xrightarrow{\text{EEA}} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \xrightarrow{\text{ParEuc}} \text{reduced basis}$$

- **CrossEuc**: Our proposed reduced algorithm without using **Hvec**.

Algorithm 5 HVecSBP(\mathbf{a}, \mathbf{b})

Input: A base $[\mathbf{a} \ \mathbf{b}]$ with $\mathbf{a} = (a_1 \ a_2)^T$, $\mathbf{b} = (b_1 \ b_2)^T$
Output: A reduced base $[\mathbf{a} \ \mathbf{b}]$

```

1:  $\mathbf{M} = \mathbf{I}$ 
2: While(1)
3:   if  $(a_1 a_2 b_1 b_2 \leq 0 \wedge (|a_1| - |a_2|)(|b_1| - |b_2|) \leq 0)$  break
4:   if  $\|\mathbf{a}\| < \|\mathbf{b}\|$ , Swap( $\mathbf{a}, \mathbf{b}$ )
5:    $n := \#\mathbf{a}$ 
6:   if  $\#\mathbf{b} \leq \lfloor \frac{n}{2} \rfloor + 1$ 
7:     if  $(|a_1| \geq |a_2| \wedge b_1 \neq 0)$ ,  $q := \lfloor \frac{a_1}{b_1} \rfloor$ 
8:     else  $q := \lfloor \frac{a_2}{b_2} \rfloor$ 
9:      $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a} - q\mathbf{b})$ 
10:    continue
11:    $(\mathbf{a}, \mathbf{b}, \mathbf{M}) \leftarrow \mathbf{HVec}(\mathbf{a}, \mathbf{b})$ 
12:   if  $\#(\mathbf{a} + \mathbf{b}) \leq \lfloor \frac{n}{2} \rfloor + 1$ ,  $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a} + \mathbf{b})$ 
13:   else if  $\#(\mathbf{a} - \mathbf{b}) \leq \lfloor \frac{n}{2} \rfloor + 1$ ,  $(\mathbf{a}, \mathbf{b}) := (\mathbf{b}, \mathbf{a} - \mathbf{b})$ 
14:   If  $((a_1 b_1 = 0 \wedge \text{sgn}(a_2) \neq \text{sgn}(b_2))$  or  $(a_2 b_2 = 0 \wedge \text{sgn}(a_1) \neq \text{sgn}(b_1)))$ ,  $\mathbf{b} := -\mathbf{b}$ 
15:   If  $\|\mathbf{a}\| > \|\mathbf{b}\|$ , Swap( $\mathbf{a}, \mathbf{b}$ )
16:   If  $\mathbf{a} = [0, 0]$ , Return $[\mathbf{a}, \mathbf{b}]$ 
17:   Else
18:     if  $(a_2 b_2 \leq 0)$ 
19:        $\mathbf{b} := \min \left\{ \mathbf{b} - \left\lfloor \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rfloor \mathbf{a}, \mathbf{b} - \left\lfloor \frac{|b_1| - |b_2|}{|a_1| + |a_2|} \right\rfloor \mathbf{a} \right\}$ 
20:     else
21:        $\mathbf{b} := \min \left\{ \mathbf{b} - \left\lfloor \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \right\rfloor \mathbf{a}, \mathbf{b} - \left\lfloor \frac{|b_2| - |b_1|}{|a_1| + |a_2|} \right\rfloor \mathbf{a} \right\}$ 
22:     Return  $[\mathbf{a} \ \mathbf{b}]$ 

```

- **HGCD-HNF-ParEuc:** Similar to **EEA-HNF-ParEuc**, but the basis is transformed into HNF using the HGCD-based extended Euclidean algorithm. Visually

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \xrightarrow{\text{HGCD}} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \xrightarrow{\text{ParEuc}} \text{reduced basis}$$

- **HGCD-HNF-HVecSBP:** Similar to **HGCD-HNF-ParEuc**, but the HNF is reduced using our proposed **HVecSBP** algorithm. Visually

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \xrightarrow{\text{HGCD}} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \xrightarrow{\text{HVecSBP}} \text{reduced basis}$$

- **HVecSBP:** Our proposed algorithm applied directly to the input basis without prior transformation to HNF.

B. Experimental Environment and Result Analysis

Our experiment are performed on a Ubuntu 22.04 machine with Intel Core i7-9750H, 2.6 GHz CPU and 16 GB RAM and implement the algorithm with C language. The detailed experimental results and their analysis are presented as follows.

(1) For the input lattice basis in HNF, let $\#a = \#b = n_1, \#c = n_2$, TABLE I compares the time cost of each algorithms as the variance of n_2 . These results highlight **HVecSBP**'s superior performance in handling HNF-structured bases, particularly in scenarios with highly imbalanced parameter lengths ($n_2 \ll n_1$). Such scenarios are common in cryptographic applications, such as lattice-based attacks, where **HVecSBP** achieves at least $13.5\times$ efficiency improvement over previous approaches.

(2) For the input lattice basis in general form, Table II compares the time cost of each algorithm as the difference $\Delta = |a_1/b_1 - a_2/b_2| \approx 10^{-\delta}$ varies. The last column, κ , represents the proportion of differing terms in the continued fraction expansions of a_1/b_1 and a_2/b_2 , counted from right to left, relative to the total number of terms in the expansions. Specially, the first $\kappa = 1$ indicates that only the last term of the continued fraction expansions of a_1/b_1 and a_2/b_2 differs. Notably, as Δ decreases, κ increases, indicating that a_1/b_1 and a_2/b_2 become closer to being equal. This further implies that the lattice basis vectors $\mathbf{a} = (a_1 \ a_2)^T$ and $\mathbf{b} = (b_1 \ b_2)^T$ approach linear dependence. From the experimental results, the following observations can be made:

- For the three algorithms without HGCD optimization—**CrossEuc**, **EEA-HNF-ParEuc**, and **GoEuc**: In general, the closer the two input lattice basis vectors are to being linearly dependent, the higher the time cost for these three algorithms. However, our proposed algorithm, **CrossEuc**, significantly outperforms the other two. Specifically, the time cost of

TABLE I: Time cost of different algorithms as n_2 varies (in seconds)

length (dec) n_1	length (dec) n_2	HVecSBP	CrossEuc/ParEuc	GolEuc
1000000	1000000	0.006217	0.002445	0.002459
1000000	800000	0.426119	10.279363	49.977750
1000000	600000	0.832923	18.195970	90.955213
1000000	400000	1.162091	26.268203	121.361453
1000000	200000	1.607177	27.132104	141.404999
1000000	100000	1.947272	28.337137	146.895788
1000000	80000	1.919498	28.082500	147.245142
1000000	60000	1.951394	28.259035	148.577950
1000000	40000	1.976183	28.483309	148.651564
1000000	20000	2.039936	28.457997	148.667026
1000000	10000	2.061487	29.026893	150.630187
1000000	5000	2.114340	29.114340	150.116029
1000000	1000	2.153284	29.424312	150.084888
1000000	100	2.164948	29.353622	150.895833
1000000	1	2.168530	29.583845	150.976715

CrossEuc is approximately 20% of that of **GolEuc**, representing a $5\times$ efficiency improvement. Compared to **EEA-HNF-ParEuc**, **CrossEuc** achieves a time cost of 22% – 5% as Δ increases, corresponding to an efficiency improvement of $4.6\times$ to $19\times$.

- For the HGCD-optimized algorithms—**HGCD-HNF-ParEuc**, **HGCD-HNF-HVecSBP**, and our algorithm **HVecSBP**, we can observe the following two experimental phenomena:
 - 1) When the continued fraction expansions of a_1/b_1 and a_2/b_2 differ only in the last term, **HGCD-HNF-ParEuc** achieves the highest efficiency, followed by **HGCD-HNF-HVecSBP**. The time cost of **HVecSBP** is approximately $2\times$ that of the other two algorithms, making it the least efficient. This is intuitive, as the input lattice basis vectors nearly degenerate into two integers, making integer-based HGCD processing more efficient. The vectorized **HVec** algorithm, which handles two dimensions, naturally incurs double the time cost.
 - 2) As the linear dependency between the two lattice basis vectors weakens—specifically, when the continued fraction expansions of a_1/b_1 and a_2/b_2 differ in approximately the last 27.5% of terms—our algorithm **HVecSBP** begins to outperform the other two. As this proportion increases, the efficiency advantage of **HVecSBP** grows progressively.

TABLE II: Time cost of different algorithms as δ varies (in seconds): $\#\{a_1, a_2, b_1, b_2\} = 10^6, \Delta \approx 10^{-\delta}$

δ	HVecSBP	HGCD-HNF-HVecSBP	HGCD-HNF-ParEuc	CrossEuc	EEA-HNF-ParEuc	GolEuc	κ
2000000	4.634715	2.474747	2.335431	54.612207	250.625570	269.501145	1
1750000	3.759720	2.881473	3.509663	53.949515	231.295727	262.973879	12.5%
1500000	3.281029	3.130119	7.128568	53.507613	229.640975	249.979270	25%
1450000	3.177414	3.165364	8.725851	51.548659	210.162490	249.096180	27.5%
1400000	3.092249	3.232044	9.014794	50.038115	208.529073	248.094480	30%
1250000	2.765591	3.551487	14.045340	45.819027	204.894112	231.718764	37.5%
1000000	2.412870	4.063529	21.208691	40.766721	200.351373	206.916571	50%
750000	1.855896	4.274508	31.767607	35.590796	198.790794	173.002045	62.5%
500000	1.417675	4.729311	44.924310	29.244469	197.095717	139.971889	75%
250000	0.917597	5.205109	59.637123	19.667034	196.227950	97.178470	87.5%
100000	0.685130	5.302298	70.196164	14.644298	196.028048	71.587244	95%
50000	0.568257	5.336118	74.210315	13.054622	196.026205	62.898395	97.5%
10000	0.467744	5.331523	75.565236	11.143312	195.498931	54.231681	99.5%
5000	0.459721	5.425184	76.523376	10.757789	195.399899	53.463294	99.75%
1000	0.448851	5.505665	76.635827	10.684234	195.360483	52.133793	99.95%
500	0.447047	5.662536	76.843067	10.612306	195.329952	51.892477	99.975%
100	0.439681	5.689787	77.879209	10.525084	194.966942	51.416951	99.995%
0	0.437364	5.701985	78.296140	10.396514	194.718627	51.037448	100%

VII. CONCLUSION

This paper introduces a newly defined reduced basis for two-dimensional lattices and develops a fast reduction algorithm, **CrossEuc**, which effectively solves the SVP and SBP in two-dimensional lattices. Furthermore, we extend the integer version of the HGCD algorithm and propose a vector-based **HVec** algorithm, providing detailed implementation and analysis. This leads to an optimized version, **HVecSBP**, which further accelerates the performance of **CrossEuc**. Finally, we conduct extensive experiments to evaluate the practical performance of our newly designed algorithms.

REFERENCES

- [1] F. Arnault and T. P. Berger. Correction to “feedback with carry shift registers synthesis with the euclidean algorithm”[may 04 910-917]. *IEEE Transactions on Information Theory*, 54(1):502–502, 2008.
- [2] F. Arnault, T. P. Berger, and A. Necer. Feedback with carry shift registers synthesis with the euclidean algorithm. *IEEE Transactions on Information Theory*, 50(5):910–917, 2004.
- [3] J. Che, C. Tian, Y. Jiang, and G. Xu. Algorithms for the minimal rational fraction representation of sequences revisited. *IEEE Transactions on Information Theory*, 68(2):1316–1328, 2022.
- [4] F. Eisenbrand. Short vectors of planar lattices via continued fractions. *Information Processing Letters*, 79(3):121–126, 2001.
- [5] J. Lagrange. Recherches d’arithmétique. *Nouv. Mém. Acad. Roy. Sc. Belles Lett. Berlin*, pages 265–312, 1773.
- [6] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261:515–534, 1982.
- [7] R. Liu and Y. Pan. Computing hermite normal form faster via solving system of linear equations. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, pages 283–290, 2019.
- [8] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.
- [9] N. Möller. Robust hgcd with no backup steps. In *International Congress on Mathematical Software*, pages 194–204. Springer, 2006.
- [10] N. Möller. On schönhage’s algorithm and subquadratic integer gcd computation. *Mathematics of Computation*, 77(261):589–607, 2008.
- [11] F. Morain. Implementing the thull-yap algorithm for computing euclidean remainder sequences. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation, ISSAC’22*, page 197–205, New York, NY, USA, 2022. Association for Computing Machinery.
- [12] G. Rote. Finding a shortest vector in a two-dimensional lattice modulo m . *Theoretical Computer Science*, 172(1-2):303–308, 1997.
- [13] H. Wu and G. Xu. Qin’s algorithm, continued fractions and 2-dimensional lattices. *arXiv preprint arXiv:2310.09103*, 2023.
- [14] C.-K. Yap. Fast unimodular reduction: Planar integer lattices. In *Proceedings., 33rd Annual Symposium on Foundations of Computer Science*, pages 437–446. IEEE Computer Society, 1992.

Lihao Zhao received the B.E. degree in information security from Qingdao University in 2023. He is currently pursuing the M.S. degree in the School of Computer Science and Technology of Qingdao University. His research interests include lattice algorithms and privacy computing.

Chengliang Tian received the B.S. and M.S. degrees in mathematics from Northwest University, Xi'an, China, in 2006 and 2009, respectively, and the Ph.D. degree in information security from Shandong University, Ji'nan, China, in 2013. He held a post-doctoral position with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing. He is currently with the College of Computer Science and Technology, Qingdao University, as an Associate Professor. His research interests include lattice-based cryptography and cloud computing security.

Jingguo Bi received the B.Sc. and Ph.D. degrees in information security from Shandong University, Jinan, China, in 2007 and 2012, respectively. He is currently an Associate Researcher with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. His research interests are public key cryptography, cloud computing, and post-quantum cryptography.

Guangwu Xu (Senior Member) received his Ph.D. in mathematics from SUNY Buffalo. He is now with the School of Cyber Science and Technology, Shandong University, China. His research interests include cryptography, arithmetic number theory, compressed sensing, algorithms, and functional analysis.

Jia Yu (Member, IEEE) received the B.S. and M.S. degrees from the School of Computer Science and Technology, Shandong University, Jinan, China, in 2003 and 2000, respectively, and the Ph.D. degree from the Institute of Network Security, Shandong University in 2006. He is a Professor with the College of Computer Science and Technology, Qingdao University, Qingdao, China. He was a Visiting Professor with the Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY, USA, from November 2013 to November 2014. His research interests include cloud computing security, key evolving cryptography, digital signature, and network security