On the smallest ratio problem of lattice bases

Jianwei Li

KLMM, Academy of Mathematics and Systems Science,
The Chinese Academy of Sciences, Beijing 100190, China
lijianwei2015@amss.ac.cn

Abstract

Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a lattice basis with Gram-Schmidt orthogonalization $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$, the quantities $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ for $i = 1, \ldots, n$ play important roles in analyzing lattice reduction algorithms and lattice enumeration algorithms. In this paper, we study the problem of minimizing the quantity $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-dimensional lattice. We first prove that there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any lattice L of dimension n such that $\|\mathbf{b}_1\| = \min_{\mathbf{v}\in L\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\| \leq i$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\| \leq i^{1.5}$ for $1 \leq i \leq n$. This leads us to introduce a new NP-hard computational problem, that is, the smallest ratio problem (SRP): given an n-dimensional lattice L, find a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal. The problem inspires the new lattice invariant $\mu_n(L) = \min\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \text{ is a basis of } L\}$ and new lattice constant $\mu_n = \max \mu_n(L)$ over all n-dimensional lattices L: both the minimum and maximum are justified. The properties of $\mu_n(L)$ and μ_n are discussed. We also present an exact algorithm and an approximation algorithm for SRP.

To the best of our knowledge, this is the first sound study of SRP. Our work provides a new perspective on both the quality limits of lattice reduction algorithms and complexity estimates of enumeration algorithms.

Keywords. lattice reduction, lattice enumeration algorithms, smallest ratio problem

AMS subject classifications. 11H06, 11Y16, 68W25

1 Introduction

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space. A *lattice* L in $\mathbb{R}^m$ is a discrete and additive subgroup of $\mathbb{R}^m$, or equivalently, the set of all integer linear combinations of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$ ($m \geq n$): $L = \{\sum_{i=1}^n x_i\mathbf{b}_i, x_i \in \mathbb{Z}\}$. Such a set $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ forms a *basis* of L, which has a unique Gram-Schmidt orthogonalization $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$. All the bases of L have the same number n of elements, called the *dimension* of L, and they all have the same n-dimensional volume, called the *volume* $\mathrm{vol}(L)$ or *determinant* of L. As usual, $L(B)$ or $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ denotes the lattice spanned by the n columns of a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

The most famous computational problem involving lattices is the *shortest vector problem* (SVP), which asks to find a nonzero lattice vector of smallest norm, given a lattice basis as input. Algorithms for solving SVP either exactly or approximately have proved invaluable in many fields of mathematics and computer science, notably in cryptology (see [2, 3, 8, 32, 36, 23, 44, 45, 43]).

There are two main algorithmic techniques for SVP (and hence for other related lattice problems). The first and basic approach is the *enumeration technique*, which dates back to the early work by Pohst [47], Kannan [25], and Fincke-Pohst [11], and is still actively investigated (see [53, 56, 1, 18, 48, 16, 37, 59, 10, 60, 38, 39]). Intuitively, enumeration algorithms perform an exhaustive search of all extremely short lattice vectors within exponential time or worse. This is unavoidable because of NP-hardness: SVP is known to be NP-hard under randomized reductions [3, 20].

The hardness of SVP has led mathematicians and computer scientists to usually find a short vector instead of the shortest one. It is equivalent to finding good reduced bases consisting of reasonably short and almost orthogonal vectors: this is the second technique, known as *lattice reduction*. Lattice reduction was revived with the celebrated LLL algorithm [29], continued with blockwise algorithms [53, 56, 12, 14], and is still very active in recent years (see, *e.g.*, [7, 17, 46, 51, 30, 39]).

From the computational perspective, the most natural reduction is HKZ-reduction introduced by Hermite [22] and Korkine and Zolotareff [26]. HKZ-reduced bases have very strong quality, but are expensive to compute. Contrarily, LLL-reduction is weak but fairly cheap.

HKZ-reduced bases have a classicial property [27, Proposition 4.2]: if a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an n-dimensional lattice L is HKZ-reduced, then $\|\mathbf{b}_1\| = \lambda_1(L)$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\| \leq i^{(1+\ln i)/2}$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\| \leq i^{1+\frac{1}{2}\ln i}$ for $i = 1, \ldots, n$, where $\lambda_1(L)$ is the length of the shortest nonzero vector of L. The similar result on LLL-reduced bases is the following [29]: if a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L is LLL-reduced (with factor 1/3), then $\|\mathbf{b}_1\| \leq 2^{(n-1)/2}\lambda_1(L)$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\| \leq 2^{(i-1)/2}$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\| \leq 2^{(i-1)/2}$ for $i = 1, \ldots, n$.

Since $\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n} = \prod_{i=1}^{n}(\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|)^{1/n}$ and $\|\mathbf{b}_1\|/\lambda_1(L) \leq \max_{1\leq i\leq n}\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$, the ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ are crucial to the *Hermite factor* $\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n}$ and *approximation factor* $\|\mathbf{b}_1\|/\lambda_1(L)$, both of which are typically used to measure the quality of a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$; see [29, 53, 54, 12, 15, 14, 17]. Since $(\prod_{i=1}^{n}\|\mathbf{b}_i\|)/\mathrm{vol}(L) = \prod_{i=1}^{n}(\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|)$, the ratios $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|$ are natively related to the *orthogonality defect* $(\prod_{i=1}^{n}\|\mathbf{b}_i\|)/\mathrm{vol}(L)$, which gives a measure of the orthogonality of a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ [28, 27].

It is natural to ask whether there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any lattice L of dimension n such that the ratios $\|\mathbf{b}_1\|/\lambda_1(L)$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|$ have bounds polynomial in i for $i = 1, \ldots, n$.

The quantities $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ are of significant interest to enumeration algorithms and lattice reduction algorithms in both theory and practice:

- In enumeration algorithms, the cost of enumeration depends on the quality of the basis with respect to the ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$; the smaller the quantities $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$, the faster the enumeration; see, *e.g.*, [25, 21, 53, 56, 16, 18]).

  As an example in practice, the preprocessing of local blocks in BKZ 2.0 [7] speeds up enumeration on the projected lattices $L(B_{[i,j]})$ by decreasing the quantity $\max_{i\leq k\leq j}\|\mathbf{b}_i^*\|/\|\mathbf{b}_k^*\|$, where $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ denotes the input basis and $B_{[i,j]}$ denotes the projected block of the vectors $\mathbf{b}_i, \ldots, \mathbf{b}_j$ over $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$.

- Some classical lattice reduction algorithms follow the paradigm below (see Appendix A for the proof).

  Proposition 1.1 (Paradigm of lattice reduction)**.** *Let L be an n-dimensional lattice where $n = pk$ with $p, k \geq 1$. If a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L satisfies the following two sets of conditions:*

  1. *Hermite conditions: $\|\mathbf{b}_{ik+1}^*\| \leq g(k) \times \mathrm{vol}(B_{[ik+1,ik+k]})^{1/k}$ for $i = 0, \ldots, p-1$;*
  2. *Linked conditions: $\|\mathbf{b}_{ik+1}^*\| \leq h(k+1) \times \|\mathbf{b}_{ik+k+1}^*\|$ for $i = 0, \ldots, p-2$,*

  where both $g(k)$ and $h(k)$ are functions on k. Then

  $$\|\mathbf{b}_1\| \leq g(k) \cdot h(k+1)^{(n-k)/2k} \times \mathrm{vol}(L)^{1/n}.$$

  Furthermore, if $\|\mathbf{b}_{ik+1}^*\| \leq \sqrt{1+\varepsilon}\lambda_1(L(B_{[ik+1,ik+k]}))$ for $i = 0, \ldots, p-1$ with factor $\varepsilon \geq 0$, then

  $$\|\mathbf{b}_1\| \leq \sqrt{1+\varepsilon} \cdot h(k+1)^{(n-k)/k} \times \lambda_1(L).$$

  It can be checked that the LLL-reduction [29], BKZ-reduction [53, 56], Schnorr's semi k-reduction [53] and Gama-Nguyen's slide reduction [14] follow the paradigm. Interestingly, slide reduction provides the best polynomial-time blockwise algorithm known, which provably approximates SVP within a factor corresponding to the classical Mordell's inequality [41].

  This means that at least in theory, the local ratios $\|\mathbf{b}_{ik+1}^*\|/\|\mathbf{b}_{ik+k+1}^*\|$ may play a more important role on the quality of lattice reduction than the local Hermite factors $\|\mathbf{b}_{ik+1}^*\|/\mathrm{vol}(B_{[ik+1,ik+k]})^{1/k}$.

  In the implementation of lattice reduction algorithms, the extensive experiments provided in [55, 15, 7] obtain good reduced bases by decreasing the quantity $\max_{1\leq i\leq n}\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$.

The ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ are also useful in analyzing *simultaneous reduction* [19, 57]. Specifically, given an n-dimensional lattice L, let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of L and $D = (\mathbf{d}_1, \ldots, \mathbf{d}_n)$ be the dual basis of B, simultaneous reduction is to minimize the quantity $S(B) = \max_{1\leq i\leq n}(\|\mathbf{b}_i\| \cdot \|\mathbf{d}_i\|)$ when B is taken over all bases of L: $S(B)$ is locally dominated by the value $\max_{1\leq i\leq j\leq n}\|\mathbf{b}_i^*\|/\mathbf{b}_j^*\|$ (see [57, p. 369]).

Hence, it is interesting and useful to study the minimality of the ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ (including in the worst-case) for $i = n, \ldots, 1$. These essentially refer to the problem of minimizing the quantity $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-dimensional lattice. A natural question is whether there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any given n-dimensional lattice such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal. If yes, it becomes interesting to further discuss the hardness and algorithmic aspects of the computational problem of finding such a basis.

In mathematics, SVP with respect to the Euclidian norm is tightly related to the study of Hermite's constants γ_n, which are defined as $\gamma_n = \max(\lambda_1(L)/\mathrm{vol}(L)^{1/n})^2$ over all n-dimensional lattices L. These fundamental parameters in the geometry of numbers are typically used in the study of both enumeration algorithms and lattice reduction algorithms, *e.g.*, to measure the running time [21, 18] and output quality [14, 17] respectively. By analogy with this case, one may wonder what should be the lattice parameters related to the problem of minimizing the quantity $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$

This paper first formalizes and answers the aforementioned questions. Our work is a step towards a clearer understanding of both enumeration algorithms and lattice reduction algorithms, which could inspire faster or improved lattice algorithms.

Our results. Our first main result of this paper is the following:

Theorem 1.2. *For any n-dimensional lattice $L \subseteq \mathbb{R}^m$, there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that*

$$\begin{aligned} &\|\mathbf{b}_1\| = \lambda_1(L), \\ &\|\mathbf{b}_1\| \le i\|\mathbf{b}_i^*\| \quad \textit{for } \ i = 1, \ldots, n, \\ &\|\mathbf{b}_i\| \le i^{1.5}\|\mathbf{b}_i^*\| \quad \textit{for } \ i = 1, \ldots, n. \end{aligned}$$

Furthermore, finding such a basis is polynomial-time equivalent to solving SVP.

Our second main result of this paper is to study the so-called *smallest ratio problem* (SRP): given an n-dimensional lattice L, find a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal. The existence of such a basis is proved. We further show that SRP is at least as hard as SVP and hence NP-hard under randomized reductions.

We define the lattice invariant $\mu_n(L) = \min\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a basis of $L\}$ and lattice constant $\mu_n = \max \mu_n(L)$ over all n-dimensional lattices L: the maximum is also justified. We then discuss the properties of $\mu_n(L)$ and μ_n. Interestingly, the new constants μ_n have close relation with the classical Hermite's constants γ_n, Bergé-Martinet's constants γ_n' [4] and Korkine-Zolotareff's constants γ_n'' [26, 4]: for instance, $\gamma_n' \le \mu_n \le \gamma_n''$ and $\mu_n \le \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)}$ for $n \ge 2$. This implies the following asymptotical bounds on μ_n:

$$\frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} + o(1) \le \mu_n \le \frac{1.744n}{2\pi e} + o(n).$$

Our third main result of this paper is to consider the algorithmic aspects of SRP. We first provide an algorithm for solving SRP exactly within $\mathrm{poly}(\log\|B\|, m) \cdot n^{\frac{n}{2e}+o(n)}$ bit operations and space, given an n-dimensional basis $B \in \mathbb{Z}^{m\times n}$ as input. This algorithm uses Kannan's enumeration algorithm (see [25, 18]) as a subroutine.

We then present a new reduction notion, together with a polynomial-time blockwise reduction algorithm, called block-ratio reduction. We show that block-ratio reduction is an algorithmic version of the new inequality $\mu_n \le \mu_k^{(n-1)/(k-1)}$ where $k-1$ divides $n-1$ with $k \ge 2$. More precisely, given a basis B_0 of an n-dimensional lattice $L \subseteq \mathbb{Z}^m$, a blocksize k satisfying $n = p(k-1)+1$ for some $p \ge 1$, a reduction factor $\varepsilon > 0$, and an exact SRP-subroutine for any lattice of dimension k, block-ratio reduction outputs a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L within $\mathrm{poly}(\log\|B_0\|, m, 1/\varepsilon)$ bit operations such that

$$\|\mathbf{b}_1\| \le (\sqrt{1+\varepsilon}\mu_k)^{(n-1)/(k-1)}\|\mathbf{b}_n^*\|,$$

where the number of calls to the SRP-subroutine is $O(np^2(\log\|B_0\|)/\varepsilon)$, and the input to the subroutine always has entries of size $O(n(n+\log\|B_0\|))$.

Roadmap. In Section 2, we provide preliminaries on lattices and basic lemmas. In Section 3, we prove Theorem 1.2. In Section 4, we study SRP and its related lattice parameters. Section 5 is devoted to the algorithmic aspects of SRP. In Appendices A-E, we provide missing details.

2 Background

Let $\|\cdot\|$ and $\langle\cdot,\cdot\rangle$ be the Euclidean norm and inner product of $\mathbb{R}^m$. We use bold lower case letters to denote column vectors, and use column-representation for matrices which are written in capital letters. The ring of $m \times n$ matrices with coefficients in the ring $\mathbb{A}$ is denoted by $\mathbb{A}^{m\times n}$, and we identify $\mathbb{A}^m$ with $\mathbb{A}^{m\times 1}$. The $n \times n$ identity matrix is denoted by I_n, and $\widetilde{M} = \det(M)M^{-1}$ denotes the adjunct matrix of a nonsingular matrix M. For any integers a and b, we define $[a,b]_{\mathbb{Z}} = [a,b] \bigcap \mathbb{Z}$.

We use the bit complexity model without fast integer arithmetic, and the size of an object is the length of its binary representation. For a matrix $B = (b_{i,j}) = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of n columns, we denote $\|B\| = \max\{\|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\|\}$, $\|B\|_\infty = \max_{i,j} |b_{i,j}|$, and $\|\cdot\|_F$ is the Frobenius norm: $\|B\|_F = \sqrt{\sum_{i=1}^n \|\mathbf{b}_i\|^2}$. The notation $\log(\cdot)$ stands for the base 2, and $\mathrm{poly}(x_1, \ldots, x_i)$ means $\prod_{j=1}^i x_j^{c_j}$ for some constants $c_j > 0$.

2.1 Lattices

Orthogonalization. Given a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m\times n}$, consider the *orthogonal projections*:

$$\pi_i : \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \mapsto \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp \quad \text{for} \quad i = 1, \ldots, n,$$

where $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ denotes the space spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Define the *projection matrices*:

$$P_i = I_m - M_i(M_i^t M_i)^{-1} M_i^t \quad \text{with} \quad M_i = (\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}) \quad \text{for} \quad i = 1, \ldots, n.$$

It is classical that $\pi_i(\mathbf{b}) = P_i\mathbf{b}$ for $\forall \mathbf{b} \in \mathbb{R}^m$ (see [61, Chapter 2]). We will use the notation $B_{[i,j]}$ for the projected block $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_j))$, then $B_{[i,j]} = P_i(\mathbf{b}_i, \ldots, \mathbf{b}_j)$. If B is integral, then so is $\det(M_i^t M_i)B_{[i,j]}$: this is because $\det(M_i^t M_i)P_i = \det(M_i^t M_i)I_m - M_i(\widetilde{M_i^t M_i})M_i^t$ is integral.

The vectors $\mathbf{b}_i^* = \pi_i(\mathbf{b}_i)$ for $i = 1, \ldots, n$ are the *Gram-Schmidt vectors* of B, and the family $B^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ is the *Gram-Schmidt orthogonalization* of B. The *Gram-Schmidt coefficients* are $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$ for $1 \le i, j \le n$: we have $\mu_{i,i} = 1$ and $\mu_{i,j} = 0$ for $i < j$. Let μ denote the unit upper triangular matrix $(\mu_{i,j})_{1\le i,j\le n}^t$. Then B has a classical decomposition $B = B^*\mu$.

For any integer basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{Z}^{m\times n}$, the GSO matrices B^* and μ are rational, both of which can be computed within $O(mn^4 \log^2 \|B\|)$ bit operations [29] by the recursion: $\mathbf{b}_1^* = \mathbf{b}_1$ and $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$ with $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$ for $i = 2, \ldots, n$.

Isometry. Two bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and $(\mathbf{c}_1, \ldots, \mathbf{c}_n)$ are *isometric* if $\langle \mathbf{b}_i, \mathbf{b}_j \rangle = \langle \mathbf{c}_i, \mathbf{c}_j \rangle$ for $1 \le i, j \le n$. Two lattices of the same dimension are *isometric* if and only if they have isometric bases. Two isometric lattices have the same mathematical properties.

Duality. For any n-dimensional lattice L with basis $B \in \mathbb{R}^{m\times n}$, the *dual lattice* of L is defined as $L^\times = \{\mathbf{y} \in \mathrm{span}(B) : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}, \forall \mathbf{x} \in L\}$. $L^\times$ has basis $B^{-t} \triangleq B(B^tB)^{-1}$, which is called the *dual basis* of B. The *reversed dual basis* of B is defined as $B^{-s} = R_m B^{-t} R_n$ [13], where $R_n = (r_{i,j})_{1\le i,j\le n}$ is the reversed identity matrix: $r_{i,j} = \delta_{i,n-j+1}$ where $\delta_{i,j}$ denotes Kronecker's symbol. Write $\widehat{\mathbf{b}} := R_m\mathbf{b} = (b_m, b_{m-1}, \ldots, b_1)^t$ where $\mathbf{b} = (b_1, b_2, \ldots, b_m)^t$, and let $\widehat{L} := \{\widehat{\mathbf{x}} : \mathbf{x} \in L\}$. Then $\widehat{L}^\times := \widehat{(L^\times)} = (\widehat{L})^\times$ is the *reversed dual lattice* of L, which has basis B^{-s}. Clearly, $\widehat{L}^\times$ is isometric to $L^\times$ and hence $\mathrm{vol}(L) \cdot \mathrm{vol}(\widehat{L}^\times) = \mathrm{vol}(L) \cdot \mathrm{vol}(L^\times) = 1$. In lattice reduction, it is more convenient to consider B^{-s} than to consider B^{-t} [14, 30].

Hermite′s constant. The *Hermite invariant* of an n-dimensional lattice L is defined by $\gamma_n(L) = (\lambda_1(L)/\mathrm{vol}(L)^{1/n})^2$, where $\lambda_1(L) = \min_{\mathbf{v}\in L\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$ is the first minimum of L. *Hermite's constant* is the maximum $\gamma_n = \max \gamma_n(L)$ over all n-dimensional lattices L. Its exact value is known for $1 \le n \le 8$ and $n = 24$, and we have $\gamma_n < 1 + n/4$ for $n \ge 1$; see [35, p. 43 and p. 53].

Rankin's constant. Let L be an n-dimensional lattice and $1 \le r \le n$. We will use the notation:

$$m_r(L) := \min_{\substack{\mathbf{x}_1,\ldots,\mathbf{x}_r \in L \\ \mathrm{vol}(\mathbf{x}_1,\ldots,\mathbf{x}_r)\neq 0}} \mathrm{vol}(\mathbf{x}_1, \ldots, \mathbf{x}_r).$$

Rankin [49] introduced the *Rankin invariant* $\gamma_{n,r}(L)$ defined as $\gamma_{n,r}(L) = (m_r(L)/\mathrm{vol}(L)^{r/n})^2$. *Rankin's constant* is the maximum $\gamma_{n,r} = \max \gamma_{n,r}(L)$ over all n-dimensional lattices L. Clearly, $m_1(L) = \lambda_1(L), \gamma_{n,1}(L) = \gamma_n(L)$ and $\gamma_{n,1} = \gamma_n$.

Berge – Martinet′s constant ([4, Definition 2.1]). The *Bergé-Martinet invariant* of an n-dimensional lattice L is defined by $\gamma'_n(L) = \lambda_1(L)\lambda_1(L^\times)$. *Bergé-Martinet's constant* is the maximum $\gamma'_n = \max \gamma'_n(L)$ over all n-dimensional lattices L.
Korkine – Zolotareff′s constant ([4, Definition 1.3]). The *Korkine-Zolotareff invariant* of an n-dimensional lattice L is defined by $\gamma''_n(L) = \max \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_n^*\|}$ over all HKZ-reduced bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L. *Korkine-Zolotareff's constant* is the maximum $\gamma''_n = \max \gamma''_n(L)$ over all n-dimensional lattices L.
Primitive vector. A vector $\mathbf{b}$ in a lattice L is *primitive* for L if and only if it can be extended to a basis of L. In particular, a vector $\mathbf{x} = (x_1, \ldots, x_n)^t \in \mathbb{Z}^n$ is *primitive* for $\mathbb{Z}^n$ if and only if it can be extended to a unimodular matrix, or equivalently, $\gcd(x_1, \ldots, x_n) = 1$ [58, Theorem 32].

2.2 Lattice reduction

Size reduction. A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is *size-reduced* if its GSO satisfies: $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$. The single vector $\mathbf{b}_i$ is *size-reduced* if $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i$.
LLL reduction. A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is *LLL-reduced* [29] with factor $\varepsilon \in [0, 3)$ if it is size-reduced and every 2×2 block $B_{[i,i+1]}$ satisfies Lovász's condition: $\|\mathbf{b}_i^*\|^2 \leq (1+\varepsilon)(\|\mathbf{b}_{i+1}^*\|^2 + \mu_{i+1,i}^2\|\mathbf{b}_i^*\|^2)$. This implies Siegel's condition: $\|\mathbf{b}_i^*\|^2 \leq \frac{4(1+\varepsilon)}{3-\varepsilon}\|\mathbf{b}_{i+1}^*\|^2$. Given as inputs a basis $B \in \mathbb{Z}^{m\times n}$ and $\varepsilon > 0$, the LLL algorithm [29] outputs an LLL-reduced basis within $O(\frac{mn^5 \log^3 \|B\|}{\log(1+\varepsilon)})$ bit operations.
SVP reduction. A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is *SVP-reduced* if the first basis vector $\mathbf{b}_1$ satisfies $\|\mathbf{b}_1\| = \lambda_1(L(B))$. Then, $\|\mathbf{b}_1\| \leq \sqrt{\gamma_n}\text{vol}(B)^{1/n}$.
DSVP reduction. A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is *DSVP-reduced* [14] (where D stands for dual) if its reversed dual basis B^{-s} is SVP-reduced. Such a reduced basis satisfies $\text{vol}(B) \leq \gamma_n^{n/2}\|\mathbf{b}_n^*\|^n$ [14].
HKZ reduction. A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is *HKZ-reduced* [22, 26] if it is size-reduced and $B_{[i,n]}$ is SVP-reduced for $i = 1, \ldots, n$.
Rankin reduction. A basis B of a lattice L is *r-Rankin-reduced* [12] if its first r basis vectors reach $m_r(L)$. There exist r-Rankin reduced bases for any given lattice. By duality, an n-dimensional lattice basis B is $(n-1)$-Rankin-reduced if and only if it is DSVP-reduced.

2.3 Basic lemmas

We here present some basic lemmas.

Lemma 2.1. *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of a lattice L and $B^{-s} = (\mathbf{d}_1, \ldots, \mathbf{d}_n)$ with the Gram-Schmidt orthogonalization $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ and $(\mathbf{d}_1^*, \ldots, \mathbf{d}_n^*)$ respectively. Then the identity holds:*

$$\frac{\|\mathbf{b}_1^*\|}{\|\mathbf{b}_n^*\|} = \frac{\|\mathbf{b}_1^*\| \cdot \text{vol}(B_{[1,n-1]})}{\text{vol}(L)} = \frac{\|\mathbf{b}_1^*\|^2 \cdot \text{vol}(B_{[2,n-1]})}{\text{vol}(L)} = \|\mathbf{b}_1^*\| \cdot \|\mathbf{d}_1^*\| = \frac{\|\mathbf{d}_1^*\|}{\|\mathbf{d}_n^*\|}. \tag{2.1}$$

Proof. It is classical that $\|\mathbf{b}_1^*\|\cdot\|\mathbf{d}_n^*\| = \|\mathbf{d}_1^*\|\cdot\|\mathbf{b}_n^*\| = 1$ (see, *e.g.*, [50, Claim 7]). Therefore, $\|\mathbf{b}_1^*\|/\|\mathbf{b}_n^*\| = \|\mathbf{b}_1^*\|\cdot\|\mathbf{d}_1^*\| = \|\mathbf{d}_1^*\|/\|\mathbf{d}_n^*\|$. This proves the identity since the other equalities are trivial. □

Lemma 2.2 ([31, Lemma 3.8])**.** *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an n-dimensional lattice basis. If the projected block $B_{[i,j]}$ is DSVP-reduced for $1 \leq i < j \leq n$, then $B_{[k,j]}$ is DSVP-reduced for $i \leq k < j$.*

Lemma 2.3 ([9, Lemma 3.2])**.** *Let B be a r-Rankin-reduced basis of a lattice L. Then $\lambda_1(L(B_{[1,r]})) \leq \gamma_r\lambda_1(L)$.*

The dual strategy used in the classical proof of Mordell's inequality (see [41] or [14, Section 3.1]) inspires the following lemma:

Lemma 2.4. *If a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of dimension $n \geq 2$ is in either of the two cases below:*

1. *B is SVP-reduced and $B_{[2,n]}$ is DSVP-reduced;*

2. *B is DSVP-reduced and $B_{[1,n-1]}$ is SVP-reduced,*

then $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| < \frac{3}{5}n$.

Proof. Cases 1 and 2 have similar proofs, we verify Case 2. Since $B_{[1,n-1]}$ is SVP-reduced, then

$$\|\mathbf{b}_1\|^{n-1} \leq \gamma_{n-1}^{(n-1)/2}\mathrm{vol}(B_{[1,n-1]}). \tag{2.2}$$

Since B is DSVP-reduced, we have $\mathrm{vol}(B) \leq \gamma_n^{n/2}\|\mathbf{b}_n^*\|^n$ and therefore

$$\mathrm{vol}(B_{[1,n-1]}) \leq \gamma_n^{n/2}\|\mathbf{b}_n^*\|^{n-1}. \tag{2.3}$$

Combining (2.2) and (2.3), we obtain

$$\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)}. \tag{2.4}$$

Now, it suffices to show that $\sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n$, which is done by distinguishing two cases:

- For $n = 2, 3$, it can be trivially checked that $\sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n$ using the exact value of γ_n.
- For $n \geq 4$, we can deduce that $(1 + \frac{n-1}{4})(1 + \frac{n}{4})^{n/(n-1)} < (\frac{3}{5}n)^2$, by considering the derivative of the function $f(n) = 2\log(\frac{3}{5}n) - \log(1 + \frac{n-1}{4}) - \log(1 + \frac{n}{4})^{n/(n-1)}$. Thus, $\gamma_{n-1}\gamma_n^{n/(n-1)} < (1 + \frac{n-1}{4})(1 + \frac{n}{4})^{n/(n-1)} < (\frac{3}{5}n)^2$.

This proved $\sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n$ for $n \geq 2$, which completes the proof. □

3 A new type of reduced basis

In this section, we prove Theorem 1.2 and formalize its related lattice problem and lattice parameters.

3.1 Proof of Theorem 1.2

We recall the classical property on HKZ-reduced bases proved in [27]: let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a HKZ-reduced basis of a lattice L, then

$$\begin{aligned}
&\|\mathbf{b}_1\| = \lambda_1(L),\\
&\|\mathbf{b}_1\| \leq i^{(1+\ln i)/2}\|\mathbf{b}_i^*\| \quad \text{for } i = 1, \ldots, n,\\
&\|\mathbf{b}_i\| \leq i^{(2+\ln i)/2}\|\mathbf{b}_i^*\| \quad \text{for } i = 1, \ldots, n.
\end{aligned}$$

This follows from the facts: B is size-reduced and $B_{[i,n]}$ is SVP-reduced for $i = 1, \ldots, n$.

Proof of Theorem 1.2. Our goal is to show that there exists a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-dimensional lattice L such that

$$\begin{aligned}
&\|\mathbf{b}_1\| = \lambda_1(L),\\
&\|\mathbf{b}_1\| \leq i\|\mathbf{b}_i^*\| \quad \text{for } i = 1, \ldots, n,\\
&\|\mathbf{b}_i\| \leq i^{1.5}\|\mathbf{b}_i^*\| \quad \text{for } i = 1, \ldots, n.
\end{aligned}$$

Our approach is to inductively combine SVP-reduction and DSVP-reduction.

We prove the existence of the desired basis by induction on n. For the initial cases $n = 1, 2$, any HKZ-reduced basis of the lattice is as desired. Assume that the existence holds for $n = k \geq 2$.

Let L be a lattice of dimension $n = k + 1$. There exists a size-reduced basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ of L such that C is SVP-reduced, $C_{[2,n]}$ is DSVP-reduced and $C_{[1,n-1]}$ is HKZ-reduced. Let $(\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*)$ be the Gram-Schmidt orthogonalization of C. We have $\|\mathbf{c}_1\| = \lambda_1(L)$ and $\|\mathbf{c}_1^*\|/\|\mathbf{c}_n^*\| < \frac{3}{5}n$ by Lemma 2.4.

Let $i \in [2, n-1]_{\mathbb{Z}}$. Since $C_{[2,n]}$ is DSVP-reduced, by Lemma 2.2, $C_{[i,n]}$ is DSVP-reduced. $C_{[i,n-1]}$ is SVP-reduced since $C_{[1,n-1]}$ is HKZ-reduced. Applying Lemma 2.4 to the projected block $C_{[i,n]}$, we have

$$\|\mathbf{c}_i^*\|/\|\mathbf{c}_n^*\| < \frac{3}{5}(n - i + 1) \ \text{ for } i = 2, \ldots, n - 1.$$

Since C is size-reduced, this implies

$$\|\mathbf{c}_n\|^2 \leq \|\mathbf{c}_n^*\|^2 + \frac{1}{4}\sum_{i=1}^{n-1}\|\mathbf{c}_i^*\|^2 < (1 + \frac{1}{4}\sum_{i=1}^{n-1}\frac{9}{25}(n-i+1)^2)\|\mathbf{c}_n^*\|^2 < \frac{1}{5}n^3\|\mathbf{c}_n^*\|^2.$$

Thus, $\|\mathbf{c}_n\|/\|\mathbf{c}_n^*\| < n^{1.5}$.

By the induction hypothesis, there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ for the lattice $L(C_{[1,n-1]})$ such that

$$\|\mathbf{b}_1\| = \lambda_1(L(C_{[1,n-1]})) = \|\mathbf{c}_1\| = \lambda_1(L),$$

$\|\mathbf{b}_1\| \leq i\|\mathbf{b}_i^*\|$ and $\|\mathbf{b}_i\| \leq i^{1.5}\|\mathbf{b}_i^*\|$ for $i = 1, \ldots, n-1$. Hence, the set $B = (\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}, \mathbf{c}_n)$ forms the desired basis of L, since the Gram-Schmidt vector of $\mathbf{c}_n$ in the set B is still $\mathbf{c}_n^*$. This proved the existence of the desired basis for a lattice of any dimension.

The above proof can be easily converted into a recursive algorithm. Specifically, the algorithm finds the basis vectors $\mathbf{b}_1, \mathbf{b}_n, \mathbf{b}_{n-1}, \ldots, \mathbf{b}_2$ in turn by calling $\frac{n(n-1)}{2}$ SVP-solvers in dimensions $\leq n$. This completes the proof. □

3.2 Lattice problem and lattice parameters related to Theorem 1.2

Theorem 1.2 can be essentially formulated and divided into the subproblems of minimizing the ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ of the sublattice $L(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ in turn for $i = n, \ldots, 1$.

This is reminiscent of HKZ-reduction, that is, any HKZ-reduced basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice minimizes the ratio $\|\mathbf{b}_i^*\|/\mathrm{vol}(B_{[i,n]})^{1/(n-i+1)}$ with respect to the projected lattice $L(B_{[i,n]})$ in turn for $i = 1, \ldots, n$. The minimization problem related to HKZ-reduction is the well-known SVP problem.

As mentioned in Section 1, the quantities $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ are of significant interest to both enumeration algorithms and lattice reduction algorithms. By analogy with SVP, these suggest to formalize the problem of minimizing the quantity $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-dimensional lattice.

Definition 3.1 (Smallest Ratio Problem, abbreviated SRP)**.** *Given an n-dimensional lattice L, find a basis* $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *of L such that* $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ *is minimal.*

The justification of SRP is guaranteed by Theorem 4.1. It is natural and interesting to discuss the hardness and algorithmic aspects of SRP, which will be done in the sections below.

We then define the lattice parameters related to SRP.

Definition 3.2. *For any n-dimensional lattice L, the lattice invariant $\mu_n(L)$ is defined as*

$$\mu_n(L) = \inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \textit{ is a basis of } L\}.$$

The lattice constant μ_n is defined as $\mu_n = \sup \mu_n(L)$ over all n-dimensional lattices L.

Both the infimum and supremum are well-defined, because any basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L satisfies $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \geq \sqrt{\gamma_n(L)\gamma_{n,n-1}(L)}$ by the identity (2.1) and $\mu_n(L) \leq n$ by Theorem 1.2.

Further, both $\mu_n(L)$ and μ_n are reached, which we will show in the next section.

The new invariants $\mu_n(L)$ are different from the classical Hermite invariants $\gamma_n(L)$, Bergé-Martinet invariants $\gamma_n'(L)$ and Korkine-Zolotareff invariants $\gamma_n''(L)$. This is illustrated in the two examples below.

Example 1. *Consider the following matrices B and B^{-s} where the columns of B span a lattice L:*

$$B = \begin{pmatrix} 1+\epsilon & \frac{1+\epsilon}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2}(1+\epsilon) & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \textit{and} \quad B^{-s} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{2}{\sqrt{3}(1+\epsilon)} & -\frac{1}{\sqrt{3}(1+\epsilon)} \\ 0 & 0 & \frac{1}{1+\epsilon} \end{pmatrix},$$

where $0 < \epsilon < (4/3)^{1/7} - 1$. It isnot hard to deduce that $\lambda_1(L) = \lambda_1(\widehat{L^*}) = 1, \gamma_3(L) = (\frac{4}{3(1+\epsilon)^4})^{1/3}, \gamma_3'(L) = 1$ and $\mu_3(L) = 1 + \epsilon$. We have $\gamma_3'(L) < \mu_3(L) < \gamma_3(L)$.

Example 2. *Consider a 3-dimensional lattice L with HKZ-reduced basis B:*

$$B = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+\epsilon & \frac{1+\epsilon}{2} \\ 0 & 0 & \frac{\sqrt{3}}{2}(1+\epsilon) \end{pmatrix},$$

where $0 < \epsilon < (4/3)^{1/4} - 1$. *We have* $\mu_3(L) = 1 + \epsilon < \frac{2}{\sqrt{3}(1+\epsilon)} = \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_3^*\|} \leq \gamma_3''(L)$.

4 The smallest ratio problem and its related lattice parameters

In this section, we first prove that SRP is solvable and a new NP-hard lattice problem: in particular, the infimum $\mu_n(L)$ is reached at some basis of any given n-dimensional lattice L. Secondly, we show that the supremum μ_n is reached at some n-dimensional lattice. Thirdly, we discuss the properties of lattice parameters $\mu_n(L)$ and μ_n: for instance, we prove $\mu_n \leq \mu_k^{(n-1)/(k-1)}$ if $k-1$ divides $n-1$, which has an efficient algorithmic version; see the next section.

For simplicity, the set of all bases of a lattice L is denoted by $\mathcal{B}(L)$ in what follows.

4.1 Solvability and hardness of SRP

The theorem below shows that SRP is solvable and $\mu_n(L) = \min\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L)\}$.

Theorem 4.1. *For any n-dimensional lattice L, there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal, that is, $\mu_n(L) = \|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$.*

Proof. Recall that $\mu_n(L) = \inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L)\}$ and any lattice of dimension ≥ 2 has infinitely many bases. To prove the theorem, our approach is to express $\mu_n(L)$ as the infimum of some finite set so that the infimum can be replaced by minimum.

Our proof is algorithmic and has four steps. First, there exists a basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ of L such that C is $(n-1)$-Rankin-reduced and $C_{[1,n-1]}$ is SVP-reduced. Let $(\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*)$ be the Gram-Schmidt orthogonalization of C. We have $\mathrm{vol}(C_{[1,n-1]}) = m_{n-1}(L)$ and

$$\mu_n(L) \leq \frac{\|\mathbf{c}_1\|}{\|\mathbf{c}_n^*\|} = \frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,n-1]})}{\mathrm{vol}(C)} = \frac{\|\mathbf{c}_1\| \cdot m_{n-1}(L)}{\mathrm{vol}(L)}. \tag{4.1}$$

Let $\mathcal{S}_1 = \{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L) : \|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \|\mathbf{c}_1\|/\|\mathbf{c}_n^*\|\}$. (4.1) implies

$$\mu_n(L) = \inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{S}_1\}. \tag{4.2}$$

Secondly, for any $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{S}_1$, it follows from $m_{n-1}(L) \leq \mathrm{vol}(B_{[1,n-1]})$ and (4.1) that

$$\|\mathbf{b}_1\| \leq \frac{\|\mathbf{c}_1\| \cdot m_{n-1}(L) \cdot \|\mathbf{b}_n^*\|}{\mathrm{vol}(L)} = \frac{\|\mathbf{c}_1\| \cdot m_{n-1}(L) \cdot \|\mathbf{b}_n^*\|}{\mathrm{vol}(B)} = \frac{\|\mathbf{c}_1\| \cdot m_{n-1}(L)}{\mathrm{vol}(B_{[1,n-1]})} \leq \|\mathbf{c}_1\|.$$

Let $\mathcal{S}_2 = \{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L) : \|\mathbf{b}_1\| \leq \|\mathbf{c}_1\|\}$. Then $\mathcal{S}_1 \subseteq \mathcal{S}_2 \subseteq \mathcal{B}(L)$. By the definition and (4.2), we have

$$\mu_n(L) = \inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{S}_2\}. \tag{4.3}$$

Until now, the set $\mathcal{S}_2$ is still not finite if $n \geq 3$.

Thirdly, consider the set $\mathcal{S}_3 = \{\mathbf{b} \in L : \mathbf{b} \text{ is primitive for } L \text{ such that } \|\mathbf{b}\| \leq \|\mathbf{c}_1\|\}$. Since a lattice is discrete and $\|\mathbf{c}_1\| \leq \gamma_{n-1}\lambda_1(L)$ by Lemma 2.3, the set $\{\mathbf{b} \in L : \|\mathbf{b}\| \leq \|\mathbf{c}_1\|\}$ is finite and so is its subset $\mathcal{S}_3$. For any $\mathbf{b} \in \mathcal{S}_3$, define the set

$$\mathcal{B}_{\mathbf{b}}(L) = \{B \in \mathcal{B}(L) : \mathbf{b} \text{ is the first column of } B\}.$$

Then, $\mathcal{S}_2$ can be expressed as a union of finitely many subsets:

$$\mathcal{S}_2 = \bigcup_{\mathbf{b} \in \mathcal{S}_3} \mathcal{B}_{\mathbf{b}}(L). \tag{4.4}$$

Fourthly, for each $\mathbf{b} \in \mathcal{S}_3$, there is a basis $G = (\mathbf{b}, \mathbf{g}_2, \ldots, \mathbf{g}_n) \in \mathcal{B}_{\mathbf{b}}(L)$ with Gram-Schmidt orthogonalization $(\mathbf{b}, \mathbf{g}_2^*, \ldots, \mathbf{g}_n^*)$ such that $G_{[2,n]}$ is $(n-2)$-Rankin-reduced. Thus, $\mathrm{vol}(G_{[2,n-1]}) = m_{n-2}(L(G_{[2,n]}))$. For any $H = (\mathbf{b}, \mathbf{h}_2, \ldots, \mathbf{h}_n) \in \mathcal{B}_{\mathbf{b}}(L)$, we have $L(H_{[2,n]}) = L(G_{[2,n]})$ and therefore $\mathrm{vol}(G_{[2,n-1]}) \leq \mathrm{vol}(H_{[2,n-1]})$. Applying the identity (2.1), we obtain

$$\frac{\|\mathbf{b}\|}{\|\mathbf{h}_n^*\|} = \frac{\|\mathbf{b}\|^2 \cdot \mathrm{vol}(H_{[2,n-1]})}{\mathrm{vol}(L)} \geq \frac{\|\mathbf{b}\|^2 \cdot \mathrm{vol}(G_{[2,n-1]})}{\mathrm{vol}(L)} = \frac{\|\mathbf{b}\|}{\|\mathbf{g}_n^*\|} \triangleq \sigma(\mathbf{b}).$$

Thus, the set $\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}_{\mathbf{b}}(L)\}$ has minimum $\sigma(\mathbf{b})$. By (4.3) and (4.4), this implies

$$\mu_n(L) = \inf_{\mathbf{b} \in \mathcal{S}_3} (\inf \{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}_{\mathbf{b}}(L)\}) = \inf\{\sigma(\mathbf{b}) : \mathbf{b} \in \mathcal{S}_3\}.$$

Since the set $\mathcal{S}_3$ is finite, we obtain $\mu_n(L)$ as the minimum of finite set $\{\sigma(\mathbf{b}) : \mathbf{b} \in \mathcal{S}_3\}$. That is,

$$\mu_n(L) = \min\{\sigma(\mathbf{b}) : \mathbf{b} \in \mathcal{S}_3\}. \tag{4.5}$$

Hence, $\mu_n(L) = \sigma(\mathbf{b})$ for some $\mathbf{b} \in \mathcal{S}_3$. Since the real value $\sigma(\mathbf{b})$ is reached at some basis in the set $\mathcal{B}_{\mathbf{b}}(L)$, $\mu_n(L)$ is reached at such a basis. This completes the proof. □

Theorem 4.1 allows us to define SRP-reduced bases, which will be useful in the sequel.

Definition 4.2 (SRP-reduction)**.** *A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L is* SRP-reduced *if $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal, that is, B reaches $\mu_n(L)$.*

SRP is a new NP-hard lattice problem, as shown below.

Theorem 4.3. *SRP is at least as hard as SVP. Further, SRP is NP-hard under randomized reductions.*

Proof. We construct a deterministic reduction from SVP to SRP. Let L_1 be an $(n-1)$-dimensional lattice with basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$. Define an n-dimensional lattice L_2 with basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n) := \mathrm{Diag}(B, t)$ where t is a sufficiently large positive constant. Let $(\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*)$ be the Gram-Schmidt orthogonalization of C. Since $\|\mathbf{c}_1\|/\|\mathbf{c}_n^*\| = \|\mathbf{b}_1\|/t$, finding a SRP-reduced basis for L_2 is equivalent to finding a SVP-reduced basis for L_1. Thus, we can reduce any SVP instance in dimension $(n-1)$ to some SRP instance in dimension n. Since SVP is NP-hard under randomized reductions [3], so is SRP. This completes the proof. □

4.2 Reachability of μ_n

Our main result of this subsection is as follows:

Theorem 4.4. *There exists an n-dimensional lattice L such that $\mu_n = \mu_n(L)$.*

By the theorem, $\mu_n = \max \mu_n(L)$ over all n-dimensional lattices L.
Our proof of Theorem 4.4 uses Lemmas 4.5-4.7 below.

Lemma 4.5. *Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an n-dimensional lattice basis such that $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_n\|$ and $1 \leq \|\mathbf{b}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{b}_i\| \leq \prod_{i=1}^{n} \|\mathbf{b}_i\| \leq (n!)^2$. Then $1/(n!)^{2n} \leq \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \leq (n!)^4$.*

Proof. Since $\|\mathbf{b}_1\|^n \leq \prod_{i=1}^{n} \|\mathbf{b}_i\|$, we have $\|\mathbf{b}_1\| \leq (n!)^{2/n}$. Note that $1 \leq \|\mathbf{b}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{b}_i\| \leq \frac{\|\mathbf{b}_1\|(n!)^2}{\|\mathbf{b}_n\|}$, then $\|\mathbf{b}_n\| \leq (n!)^2\|\mathbf{b}_1\| \leq (n!)^{2+2/n}$. It follows from $1 \leq \|\mathbf{b}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{b}_i\| \leq \|\mathbf{b}_1\| \cdot \|\mathbf{b}_n\|^{n-1}$ that $\|\mathbf{b}_1\| \geq 1/\|\mathbf{b}_n\|^{(n-1)} \geq 1/(n!)^{2n}$. This implies $1/(n!)^{2n} \leq \|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_n\| \leq (n!)^{2+2/n}$, as desired. □

Lemma 4.6. *The set $\mathcal{S} = \left\{B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n} : 1/(n!)^n \leq \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \leq (n!)^4 \text{ and } \det(B) = 1\right\}$ is bounded and closed.*

Proof. Let $\mathcal{S}_1 = \left\{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n} : 1/(n!)^n \leq \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \leq (n!)^4\right\}$ and $\mathcal{S}_2 = \{B \in \mathbb{R}^{n \times n} : \det(B) = 1\}$. Clearly, $\mathcal{S}_1$ is a bounded closed set in $\mathbb{R}^{n \times n}$. Since $\det(\cdot)$ is a continuous mapping from $\mathbb{R}^{n \times n}$ to $\mathbb{R}$ and $\{1\}$ is a closed set in $\mathbb{R}$, $\mathcal{S}_2$ is closed in $\mathbb{R}^{n \times n}$. Hence, $\mathcal{S} = \mathcal{S}_1 \bigcap \mathcal{S}_2$ is a bounded closed set. □

Lemma 4.7. *Let $\mathcal{S}$ be the set defined in Lemma 4.6 and $f(B) = \mu_n(L(B))$ for every $B \in \mathcal{S}$. Then f is continuous on $\mathcal{S}$.*

Proof. For each $B \in \mathcal{S}$, since $\mathrm{vol}(L(B)) = \det(B) = 1$, by Theorem 4.1 and Lemma 2.1, we have

$$f(B) = \mu_n(L(B)) = \min\{\|B\mathbf{u}_1\| \cdot \mathrm{vol}(BU_{[1,n-1]}) : U = (\mathbf{u}_1, \ldots, \mathbf{u}_n) \text{ is an } n \times n \text{ unimodular matrix}\}.$$

For any $B, C \in \mathcal{S}$, we may assume without loss of generality that $f(C) \geq f(B)$ and $f(B) = \|B\mathbf{u}_1\| \cdot \mathrm{vol}(BU_{[1,n-1]})$ for some unimodular matrix $U = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$. Then,

$$|f(C) - f(B)| = f(C) - f(B) \leq \|C\mathbf{u}_1\| \cdot \mathrm{vol}(CU_{[1,n-1]}) - \|B\mathbf{u}_1\| \cdot \mathrm{vol}(BU_{[1,n-1]}).$$

For $\forall\ \varepsilon > 0$, since $g(B) := \|B\mathbf{u}_1\| \cdot \mathrm{vol}(BU_{[1,n-1]})$ is continuous at B, there exists $\delta > 0$ such that $|g(C) - g(B)| < \varepsilon$ if $\|C - B\|_F < \delta$. This implies

$$|f(C) - f(B)| < \varepsilon \quad \text{if} \quad \|C - B\|_F < \delta.$$

Thus, f is continuous at B. By the arbitrariness of B, f is continuous on $\mathcal{S}$. □

Proof of Theorem 4.4. Recall that $\mu_n = \sup \mu_n(L)$ over all n-dimensional lattices L. Our approach is to express μ_n as the supremum of a continuous mapping defined on some bounded closed set, so that the maximum principle immediately implies the conclusion.

Define the set $\mathcal{L}_n = \{L \subseteq \mathbb{R}^n : L \text{ is a lattice of dimension } n \text{ such that } \mathrm{vol}(L) = 1 \text{ and } \mu_n(L) \geq 1\}$. It is classical that any n-dimensional lattice in $\mathbb{R}^m$ is isometric to some n-dimensional lattice in $\mathbb{R}^n$ (see, *e.g.*, [6, p. 57]). Together with homogeneity and $\mu_n(\mathbb{Z}^n) = 1$, we have

$$\mu_n = \sup\{\mu_n(L) : L \in \mathcal{L}_n\}. \tag{4.6}$$

For any $L \in \mathcal{L}_n$, by Theorem 1.2, there exists a basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ of L such that

$$\|\mathbf{c}_1\| \leq \|\mathbf{c}_2\| \leq \cdots \leq \|\mathbf{c}_n\| \quad \text{and} \quad 1 \leq \|\mathbf{c}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{c}_i\| \leq \prod_{i=1}^{n} \|\mathbf{c}_i\| \leq (n!)^{1.5}$$

where we used the facts that $\det(C) = \mathrm{vol}(L) = 1$ and by Lemma 2.1, $\|\mathbf{c}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{c}_i\| \geq \|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,n-1]}) \geq \mathrm{vol}(L)\mu_n(L) \geq 1$.

By Lemma 4.5, $C \in \mathcal{S} \triangleq \left\{B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n} : 1/(n!)^{2n} \leq \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \leq (n!)^4 \text{ and } \det(B) = 1\right\}$. Thus, $L = L(C) \in \{L(B) : B \in \mathcal{S}\}$ and hence $\mathcal{L}_n \subseteq \{L(B) : B \in \mathcal{S}\}$. Together with (4.6), this implies $\mu_n \leq \sup\{\mu_n(L(B)) : B \in \mathcal{S}\} \leq \mu_n$. That is,

$$\mu_n = \sup\{\mu_n(L(B)) : B \in \mathcal{S}\} \tag{4.7}$$

By Lemmas 4.6 and 4.7, the mapping $B \mapsto \mu_n(L(B))$ is continuous on the bounded closed set $\mathcal{S}$. Applying the maximum principle, there is a basis $B_0 \in \mathcal{S}$ such that

$$\mu_n(L(B)) \leq \mu_n(L(B_0)) \quad \text{for } \forall\ B \in \mathcal{S}.$$

By (4.7), this implies $\mu_n = \mu_n(L(B_0))$ and the conclusion follows. □

4.3 Properties of $\mu_n(L)$ and μ_n

In this subsection, we discuss the properties of lattice parameters $\mu_n(L)$ and μ_n including the relations with other classical lattice parameters.

Proposition 4.8. *Let L be an n-dimensional lattice.*

1. $\mu_n(L) = \mu_n(\widehat{L^*}) = \mu_n(L^*)$.

2. $\gamma'_n(L) \leq \mu_n(L) \leq \gamma''_n(L)$.

3. $\mu_n(L) = \mu_n(c \cdot L)$ *for* $\forall c \in \mathbb{R}\backslash\{0\}$.

Proof. By the definition and identity (2.1), the proof is trivial. □

The new constants μ_n have close relation with Hermite's constants γ_n , Bergé-Martinet's constants γ'_n and Korkine-Zolotareff's constants γ''_n, as shown below.

Theorem 4.9. *For $n \geq 2$, we have:*

1. $\gamma'_n \leq \mu_n \leq \gamma''_n$*;*
2. $\mu_n \leq \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)}$*;*
3. $\frac{1}{2}(\gamma_n - 1) \leq \mu_n \leq \sqrt{\frac{4}{3}}\gamma_n$*;*
4. $\gamma'_n \leq \mu_n \leq \frac{4}{\sqrt{3}}(\gamma'_n + \frac{1}{2})$*;*
5. $\frac{3}{8}\mu_{n+1} - \frac{1}{2} \leq \mu_n \leq \frac{8}{3}(\mu_{n+1} + \frac{1}{2})$*;*
6. μ_n *has the following asymptotical bounds:*

$$\frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} + o(1) \leq \mu_n \leq \frac{1.744n}{2\pi e} + o(n).$$

Proof. Proposition 4.8.2 and the inequality (2.4) imply Properties 1 and 2, respectively.

Since $\gamma_n \leq (\sqrt{4/3})^{n-1} = \gamma_2^{n-1}$ [22] and $\gamma_{n-1} \leq \gamma_n^{n/(n-1)}$ [42], Property 2 implies

$$\mu_n \leq \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} \leq \gamma_n^{n/(n-1)} \leq \sqrt{\frac{4}{3}}\gamma_n. \tag{4.8}$$

Let ω_n be the volume of the unit Euclidean ball in dimension n and $\vartheta(n)$ be the closest integer to $(\frac{5}{3}\omega_n^{-1})^{2/n}$. Then $\vartheta(n) = \frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} + o(1)$ [40, p. 31]. By Conway-Thomson's Theorem (see [40, Theorem 9.5]), there is an n-dimensional lattice L with $L = L^\times$ such that $\lambda_1(L)\lambda_1(L^\times) \geq \vartheta(n)$. Thus, $\mu_n \geq \gamma'_n \geq \gamma'_n(L) \geq \vartheta(n)$. Since $\vartheta(n) \geq (\frac{5}{3}\omega_n^{-1})^{2/n} - \frac{1}{2}$ and $2\omega_n^{-2/n} \geq \gamma_n$ [5], we have

$$\frac{1}{2}(\gamma_n - 1) \leq \frac{1}{2}(\frac{5}{3})^{2/n}\gamma_n - \frac{1}{2} \leq \vartheta(n) \leq \mu_n,$$
$$\gamma'_n \leq \mu_n \leq \sqrt{\frac{4}{3}}\gamma_n \leq \frac{4}{\sqrt{3}}\omega_n^{-2/n} \leq \frac{4}{\sqrt{3}}(\vartheta(n) + \frac{1}{2}) \leq \frac{4}{\sqrt{3}}(\gamma'_n + \frac{1}{2}).$$

Together with (4.8), these imply Properties 3 and 4.

Applying the relations $\gamma_n \leq \gamma_{n+1}^{(n+1)/n}$ and $\gamma_n \leq \gamma_2^{n-1}$ again, together with Mordell's inequality $\gamma_{n+1} \leq \gamma_n^{n/(n-1)}$ [41], we deduce that

$$\mu_n \leq \gamma_n^{\frac{n}{n-1}} \leq \gamma_n^{\frac{2}{n-1}(1-\frac{1}{n+1})}\gamma_{n+1} \leq \gamma_2^2 2\omega_{n+1}^{-2/(n+1)} \leq \frac{8}{3}(\vartheta(n+1) + \frac{1}{2}) \leq \frac{8}{3}(\mu_{n+1} + \frac{1}{2}),$$
$$\mu_n \geq \frac{1}{2}\gamma_n - \frac{1}{2} \geq \gamma_{n+1}(2\gamma_n^{1/(n-1)})^{-1} - \frac{1}{2} \geq \frac{\sqrt{3}}{4}\gamma_{n+1} - \frac{1}{2} \geq \frac{3}{8}\mu_{n+1} - \frac{1}{2},$$

which yield Property 5.

Since $\gamma_n \leq \frac{1.744n}{2\pi e} + o(n)$ [24] and $\gamma_n^{1/(n-1)} = 1 + o(1)$, the relation $\vartheta(n) \leq \mu_n \leq \gamma_n^{n/(n-1)}$ immediately implies Property 6. This completes the proof. □

The following theorem upper bounds the constant μ_n in high dimension using μ_k in low dimension.

Theorem 4.10. *For $n \geq k \geq 2$, if $k - 1$ divides $n - 1$, then $\mu_n \leq \mu_k^{(n-1)/(k-1)}$.*

Proof. It suffices to show that $\mu_{p(k-1)+1} \leq \mu_k^p$ for $p \geq 1$, which is done by induction over p.

It holds trivially when $p = 1$. Assume that it holds for some p. Let L be a lattice of dimension $n = (p+1)(k-1)+1$ and $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an m-Rankin-reduced basis of L with $m = p(k-1)+1$. Let $(\mathbf{c}_1, \ldots, \mathbf{c}_m)$ be a SRP-reduced basis of the lattice $L(B_{[1,m]})$ and $C = (\mathbf{c}_1, \ldots, \mathbf{c}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_n)$ with Gram-Schmidt orthogonalization $(\mathbf{c}_1^*, \ldots, \mathbf{c}_m^*, \mathbf{b}_{m+1}^*, \ldots, \mathbf{b}_n^*)$. Then C is a basis of L such that

$$\frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,m-1]})}{\mathrm{vol}(C_{[1,m]})} = \mu_m(L(B_{[1,m]})) \leq \mu_m. \tag{4.9}$$

There is a $k \times k$ unimodular matrix U such that $C_{[m,n]}U$ is a SRP-reduced basis of the lattice $L(C_{[m,n]})$ since $k = n - m + 1$. Let $(\mathbf{d}_m, \ldots, \mathbf{d}_n) = (\mathbf{c}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_n)U$ and $D = (\mathbf{c}_1, \ldots, \mathbf{c}_{m-1}, \mathbf{d}_m, \ldots, \mathbf{d}_n)$ with Gram-Schmidt orthogonalization $(\mathbf{c}_1^*, \ldots, \mathbf{c}_{m-1}^*, \mathbf{d}_m^*, \ldots, \mathbf{d}_n^*)$. Then D is also a basis of L such that $D_{[m,n]} = C_{[m,n]}U$ is SRP-reduced and $\mathrm{vol}(C_{[m,n]}) = \mathrm{vol}(D_{[m,n]})$. Therefore,

$$\frac{\|\mathbf{d}_m^*\| \cdot \mathrm{vol}(D_{[m,n-1]})}{\mathrm{vol}(C_{[m,n]})} = \mu_k(L(C_{[m,n]})) \leq \mu_k. \tag{4.10}$$

We claim that $\|\mathbf{c}_m^*\|/\|\mathbf{d}_m^*\| \leq 1$. Indeed, $\mathrm{vol}(C_{[1,m]}) = \mathrm{vol}(B_{[1,m]}) \leq \mathrm{vol}(D_{[1,m]})$ since B is m-Rankin-reduced. Note that $\mathrm{vol}(C_{[1,m]}) = \mathrm{vol}(C_{[1,m-1]}) \cdot \|\mathbf{c}_m^*\|$ and $\mathrm{vol}(D_{[1,m]}) = \mathrm{vol}(C_{[1,m-1]}) \cdot \|\mathbf{d}_m^*\|$, this implies $\|\mathbf{c}_m^*\| \leq \|\mathbf{d}_m^*\|$.

Then it follows from (4.9) and (4.10) that

$$\begin{aligned}
\mu_n(L) &\leq \frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(D_{[1,n-1]})}{\mathrm{vol}(D)} = \frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,m-1]})}{\mathrm{vol}(C_{[1,m]})} \cdot \frac{\mathrm{vol}(D_{[m,n-1]})}{\mathrm{vol}(C_{[m+1,n]})} \\
&\leq \mu_m \cdot \frac{\mathrm{vol}(D_{[m,n-1]})}{\mathrm{vol}(C_{[m+1,n]})} = \mu_m \cdot \frac{\|\mathbf{d}_m^*\| \cdot \mathrm{vol}(D_{[m,n-1]})}{\mathrm{vol}(C_{[m,n]})} \cdot \frac{\|\mathbf{c}_m^*\|}{\|\mathbf{d}_m^*\|} \\
&\leq \mu_m \cdot \mu_k.
\end{aligned}$$

By the inductive hypothesis, $\mu_m \leq \mu_k^p$. Therefore, $\mu_n(L) \leq \mu_k^{p+1}$. By the arbitrariness of L, $\mu_n \leq \mu_k^{p+1}$. Thus, we proved $\mu_{p(k-1)+1} \leq \mu_k^p$ by induction over $p \geq 1$, which completes the proof. □

Theorem 4.11 below yields $\mu_4 > \mu_3^{3/2}$, and hence $\mu_n \leq \mu_k^{(n-1)/(k-1)}$ doesn't always hold for $n \geq k \geq 2$.

Similarly to the classical lattice constants γ_n, γ_n' and γ_n'', it is hard to determine the exact value of μ_n. The following theorem summarizes the explicit values of some μ_n in low dimensions.

Theorem 4.11. *$\mu_2 = \frac{2}{\sqrt{3}}$, $\mu_3 = \sqrt{\frac{3}{2}}$, $\mu_4 = \sqrt{2}$, $\sqrt{2} \leq \mu_5 < \frac{3}{2}$, $\sqrt{\frac{8}{3}} \leq \mu_6 \leq \frac{2^{9/10}}{3^{1/10}}$, $\sqrt{3} \leq \mu_7 \leq \frac{2}{3^{1/12}}$ and $\mu_8 = 2$.*

Proof. By [4, Proposition 2.13], we have $\gamma_2'' = \gamma_2' = \gamma_2 = 2/\sqrt{3}$, $\gamma_3'' = \gamma_3' = \sqrt{\frac{3}{2}} < \sqrt[3]{2} = \gamma_2$ and $\gamma_4'' = \gamma_4' = \gamma_4 = \sqrt{2}$. This implies the exact values of μ_2, μ_3 and μ_4 by Theorem 4.9.1. Since the exact values of γ_n and γ_n' are known for $1 \leq n \leq 8$ (see [4, 52]), together with $\gamma_5'' < \frac{3}{2}$ [26], the inequalities $\gamma_n' \leq \mu_n \leq \min\{\gamma_n'', \sqrt{\gamma_{n-1}}\sqrt{\gamma_n}^{n/(n-1)}\}$ imply the remainder assertions. □

We provide the critical lattices for μ_2, μ_3, μ_4 and μ_8 in Appendix B.

5 Algorithmic aspects of the smallest ratio problem

In this section, we present an exact algorithm and an approximation algorithm for SRP in Subsections 5.1 and 5.2 respectively.

Our main result on the exact SRP algorithm is the following: given as input a basis B_0 of an n-dimensional lattice $L \subseteq \mathbb{Z}^m$, the algorithm outputs a SRP-reduced basis B of L and an $n \times n$ unimodular matrix U within $\mathrm{poly}(\log\|B_0\|, m) \cdot n^{\frac{n}{2e}+o(n)}$ bit operations and space such that $B = B_0U$, $\|B\| \leq 2^{(n-1)/2}\|B_0\|$ and $\|U\| \leq 2^{(n-1)/2}n^{n+1}\|B_0\|^{2n}$.

Our main result on the SRP-approximation algorithm is as follows: given as inputs a basis B_0 of an n-dimensional lattice $L \subseteq \mathbb{Z}^m$, a blocksize k such that $k-1$ divides $n-1$, a reduction factor $\varepsilon > 0$, and a SRP-subroutine computing SRP-reduced bases in any lattice of dimension k, the algorithm outputs (in time polynomial in $(\log\|B_0\|, m, 1/\varepsilon)$) a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that

$$\|\mathbf{b}_1\| \leq (\sqrt{1+\varepsilon\mu_k})^{(n-1)/(k-1)}\|\mathbf{b}_n^*\|$$

where the number of calls to the SRP-subroutine and the size of the input are polynomial, and apart from the running time of the subroutine, the algorithm runs in polynomial time. If $k \leq \frac{\log n}{\log \log n}$ and we use the exact SRP algorithm given in Subsection 5.1 as the SRP-subroutine, then the whole algorithm runs in polynomial time.

5.1 An exact SRP algorithm

Our exact SRP algorithm is Algorithm 1, which computes a SRP-reduced basis of a given integer lattice. The main idea stems from the proof of Theorem 4.1, more precisely, is based on the equality (4.5). Algorithm 1 uses four local algorithms related to SVP:

- Magliveras *et al.*'s extending algorithm [34, Algorithm A], which extends a primitive vector for $\mathbb{Z}^n$ to a unimodular matrix. Given as input an integer vector $\mathbf{a} = (a_1, \ldots, a_n)^t$, the algorithm outputs the gcd $g = \gcd(a_1, \ldots, a_n)$ and an $n \times n$ unimodular matrix U within $O(n^2 \log^2 \|\mathbf{a}\|_\infty)$ bit operations such that $\mathbf{a}/g$ is the first column of U and $\|U\|_\infty \leq \|\mathbf{a}\|_\infty$.
- An SVP-algorithm, which finds the shortest vector of a given lattice. Given as input a basis $B \in \mathbb{Z}^{m\times n}$, an SVP algorithm outputs a primitive vector $\mathbf{x}$ for $\mathbb{Z}^n$ such that $B\mathbf{x}$ is the shortest vector of $L(B)$. If we take the Micciancio-Voulgaris algorithm [37] as an SVP algorithm, then it requires poly$(\log \|B\|, m) \cdot 2^{2n}$ bit operations and poly$(\log \|B\|, m) \cdot 2^n$ space. Combining this with Magliveras *et al.*'s extending algorithm, one can HKZ-reduce the basis B within poly$(\log \|B\|, m) \cdot 2^{2n}$ bit operations.
- A DSVP-algorithm (see Algorithm 4 in Appendix D), which performs a DSVP-reduction of a given block. Given as inputs a basis $B \in \mathbb{Z}^{m\times n}$ and an index $i \in [1, n-1]_{\mathbb{Z}}$, Algorithm 4 outputs a basis C of $L(B)$ such that $C_{[1,i-1]} = B_{[1,i-1]}$ and $C_{[i,n]}$ is DSVP-reduced.
- An enumeration algorithm (see, *e.g.*, [18, Fig.1]), which given a basis of a lattice $L \subseteq \mathbb{Z}^m$ and a bound R, finds the set $\mathcal{S} = \{\mathbf{y} \in L : \|\mathbf{y}\| \leq R\}$; see [18] for the optimal complexity analysis.

In order to avoid "intermediate entries explosion", each Step 17 performs a LLL-reduction. In fact, if we apply the LLL algorithm on a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, the quantity $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ can never increase. Therefore, there exists a basis for any lattice which is both LLL-reduced and SRP-reduced.

The main result on Algorithm 1 is the following:

Theorem 5.1. *Given as input a basis B_0 of an n-dimensional lattice $L \subseteq \mathbb{Z}^m$, Algorithm 1 outputs a SRP-reduced basis B and an $n \times n$ unimodular matrix U such that*

$$B = B_0 U, \quad \|B\| \leq 2^{(n-1)/2}\|B_0\| \quad \textit{and} \quad \|U\| \leq 2^{(n-1)/2} n^{n+1} \|B_0\|^{2n}.$$

The algorithm requires poly$(\log \|B_0\|, m) \cdot n^{\frac{n}{2e}+o(n)}$ bit operations and space.

Proof. We first show correctness. If Steps 6-7 occur, the output basis B reaches $\mu_n(L)$ by Lemma B.2. Assume that Step 8 occurs. From the proof of Theorem 4.1 (mainly (4.5)), we have

$$\mu_n(L)^2 = \min\left\{ \frac{\|\mathbf{c}_1\|^2 \cdot \mathrm{vol}(C_{[1,n-1]})^2}{\mathrm{vol}(L)^2} : C = (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in \mathcal{B}(L), \mathbf{c}_1 \in \mathcal{S} \text{ and } C_{[2,n]} \text{ is DSVP-reduced} \right\}.$$

Thus, Steps 12-19 output a SRP-reduced basis B, which proves the correctness by Lemma C.1.

Next, we analyze the complexity. The main issue is to upper bound the magnitudes of intermediate bases occurring during the algorithm. We have

$$\|B\| \leq \begin{cases} n^{n^3}\|B_0\|^{2n^3} & \text{at the end of Step 2,} \\ 2^{(n-1)/2}\|B_0\| & \text{at the end of Step 4,} \\ 2^{(n-1)/2}\|B_0\| & \text{at the end of Step 20,} \end{cases} \tag{5.1}$$

$$\|C\| \leq \begin{cases} n^2\|B_0\|^{n+1} & \text{at the end of Step 15,} \\ n^{5n^3}\|B_0\|^{2n^3(n+1)} & \text{at the end of Step 16,} \\ 2^{(n-1)/2}\|B_0\| & \text{at the end of Step 17.} \end{cases} \tag{5.2}$$

Algorithm 1 Computing a SRP-reduced basis of an integer lattice

```
Input: A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice $L$ in $\mathbb{Z}^m$.
Output: A SRP-reduced basis of $L$ and the corresponding unimodular transformation.
 1: Store $A \leftarrow B$ and compute the first minimum $\lambda_1(L)$ by calling the MV SVP-algorithm [37] on $B$
 2: DSVP-reduce $B$ using Algorithm 4 and passingly store $A^{-s}$    //$\det(A^tA)A^{-s} = R_mA\widetilde{(A^tA)}R_n \in \mathbb{Z}^{m\times n}$
 3: Compute $T \leftarrow R_n(A^{-s})^tR_m$    //For matrices $M$ and $N$, $AM = N$ iff $M = (A^tA)^{-1}A^tN = TN$.
 4: HKZ-reduce $B_{[1,n-1]}$ and then size-reduce $\mathbf{b}_n$
 5:   //The current basis $B$ is LLL-reduced with factor 0 since $B_{[n-1,n]}$ is SVP-reduced by Lemma 2.2.
 6: if $\|\mathbf{b}_1\| = \lambda_1(L)$ then
 7:   Go to Line 21    //The current basis $B$ is SRP-reduced by Lemma B.2.
 8: else
 9:   Compute $\phi(B) \leftarrow \|\mathbf{b}_1\|^2 \cdot \mathrm{vol}(B_{[1,n-1]})^2$
10:     //Note that $\|\mathbf{b}_1\|^2 \cdot \mathrm{vol}(B_{[1,n-1]})^2$ is integral but $\frac{\|\mathbf{b}_1\|\cdot\mathrm{vol}(B_{[1,n-1]})}{\mathrm{vol}(B)}$ may be real.
11:   Compute $\mathcal{S} \leftarrow \{\mathbf{y} \in L\backslash\{\mathbf{0}\} : \|\mathbf{y}\| \leq \|\mathbf{b}_1\|\}$ by calling the enumeration algorithm [18, Fig.1] on $B$
12:   for $\mathbf{y} \in \mathcal{S}$ do
13:     Compute $\mathbf{x} = (x_1, \ldots, x_n)^t \leftarrow T\mathbf{y}$    //Step 3 implies $A\mathbf{x} = \mathbf{y}$ and hence $\mathbf{x} \in \mathbb{Z}^n$.
14:     Call Magliveras et al.'s extending algorithm [34, Algorithm A] to compute $g = \gcd(x_1, \ldots, x_n)$ and an
        $n \times n$ unimodular matrix $V$ such that $\mathbf{x}/g$ is the first column of $V$
15:     Compute $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n) \leftarrow AV$ and remove $\{i \cdot \frac{\mathbf{y}}{g} : -g \leq i \leq g\}$ from $\mathcal{S}$
16:     DSVP-reduce $C_{[2,n]}$ using Algorithm 4
17:     LLL-reduce $C$ with factor $1/3$ and then compute $\phi(C) \leftarrow \|\mathbf{c}_1\|^2 \cdot \mathrm{vol}(C_{[1,n-1]})^2$
18:     if $\phi(C) < \phi(B)$ then $B \leftarrow C, \phi(B) \leftarrow \phi(C)$; else continue Step 12
19:   end for
20: end if
21: Compute $U \leftarrow TB$    //Step 3 implies $B = AU$ and hence $U$ is unimodular.
22: return $B$ and $U$
```

Indeed, since the current basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ at Step 11 is $(n-1)$-Rankin-reduced and $B_{[1,n-1]}$ is HKZ-reduced, Lemma 2.3 implies $\|\mathbf{b}_1\| \leq \gamma_{n-1}\lambda_1(L) \leq n\|B_0\|$. By Lemma C.2, the matrix V and vector $\mathbf{x}$ appearing at Steps 13-15 satisfy $\|V\|_\infty \leq \|\mathbf{x}\|_\infty \leq n\|B_0\|^n$. Applying Lemma C.1 and Theorem D.1, It is easy to deduce (5.1) and (5.2).

From (5.1) and (5.2), all intermediate bases during the execution have size $\mathrm{poly}(\log\|B_0\|, m)$. Thus, both Steps 1-7 and a single execution of Steps 13-18 require $\mathrm{poly}(\log\|B_0\|, m) \cdot 2^{2n}$ bit operations and $\mathrm{poly}(\log\|B_0\|, m) \cdot 2^n$ space.

It remains to bound the number of elements in the set $\mathcal{S}$ and cost of Step 11. Consider again the current basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ at Step 11. Since B is DSVP-reduced and $B_{[1,n-1]}$ is HKZ-reduced, then

$$\begin{aligned}
\max_{I\subseteq[1,n]_{\mathbb{Z}}} \left(\frac{\|\mathbf{b}_1\|^{|I|}}{(\sqrt{n})^{|I|} \prod_{i\in I} \|\mathbf{b}_i^*\|} \right) &\leq \frac{n}{\sqrt{n}} \cdot \max_{I\subseteq[1,n-1]_{\mathbb{Z}}} \left(\frac{\|\mathbf{b}_1\|^{|I|}}{(\sqrt{n-1})^{|I|} \prod_{i\in I} \|\mathbf{b}_i^*\|} \right) && \text{by Lemma 2.4} \\
&\leq \sqrt{n} \cdot (\sqrt{n-1})^{\frac{n-1}{e}} && \text{by [18, Theorem 3]} \\
&\leq n^{\frac{n}{2e}+\frac{1}{2}}.
\end{aligned}$$

By the Hanrot-Stehlé's analysis [18, Section 4.1], the cost of the enumeration occurring at Step 11 is bounded by $\mathrm{poly}(\log\|B\|, m) \cdot |\mathcal{S}|$ with

$$|\mathcal{S}| \leq 3n \cdot (e(1 + 2\sqrt{\pi}))^n \cdot \max_{I\subseteq[1,n]_{\mathbb{Z}}} \left(\frac{\|\mathbf{b}_1\|^{|I|}}{(\sqrt{n})^{|I|} \prod_{i\in I} \|\mathbf{b}_i^*\|} \right) \leq 3n^2 \cdot 2^{3.63n} \cdot n^{\frac{n}{2e}}.$$

Since Steps 13-18 occur at most $|\mathcal{S}|/2$ times, we conclude that Algorithm 1 totally requires $\mathrm{poly}(\log\|B_0\|, m) \cdot 2^{5.63n} \cdot n^{\frac{n}{2e}}$ bit operations and $\mathrm{poly}(\log\|B_0\|, m) \cdot 2^{3.63n} \cdot n^{\frac{n}{2e}}$ space. This completes the proof. □

Algorithm 1 is unavoidably expensive because of NP-hardness. So, it becomes interesting to find polynomial-time algorithms for approximating SRP, which is done in the next subsection.

5.2 An approximation algorithm for SRP

Recall that blockwise approximation algorithms for SVP rely on an exact algorithm in low dimension. By analogy, the exact SRP algorithm suggests finding an approximation algorithm for SRP using an exact algorithm in low dimension.

We define an SRP-oracle as any algorithm which, given a basis $B \in \mathbb{Z}^{m \times k}$, outputs a $k \times k$ unimodular matrix U such that BU is both SRP-reduced and LLL-reduced with factor $\varepsilon \geq 0$. Forcing the output to be LLL-reduced allows us to bound the coefficients of U using Lemma C.1. Obviously, Algorithm 1 is an SRP-oracle.

In what follows, we first introduce a new reduction notion called block-ratio reduction. Then we present a deterministic polynomial-time reduction algorithm to output block-ratio reduced bases. The algorithm approximates SRP in dimension n within a factor essentially $\mu_k^{(n-1)/(k-1)}$, using polynomially many calls to the SRP-oracle in dimension k, provided that $k-1$ divides $n-1$. Hence, block-ratio reduction can be viewed as an algorithmic version of Theorem 4.10.

5.2.1 Definition and property

We will use a natural relaxation of SRP-reduction: a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an n-dimensional lattice L is $(1+\varepsilon)$-*SRP-reduced* for $\varepsilon \geq 0$ if $\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_n^*\|} \leq \sqrt{1+\varepsilon}\mu_n(L)$.

Definition 5.2 (Block-ratio reduction). *A basis B of an n-dimensional lattice L where $n = p(k-1)+1$ with $p \geq 1$ is* block-ratio reduced *with blocksize k and factor $\varepsilon \geq 0$ if it is size-reduced and the block $B_{[i(k-1)+1, i(k-1)+k]}$ is $(1+\varepsilon)$-SRP-reduced for $i = 0, \ldots, p-1$.*

Block-ratio reduction achieves the new inequality $\mu_n \leq \mu_k^{(n-1)/(k-1)}$ where $k-1$ divides $n-1$, like slide reduction achieved Mordell's inequality $\gamma_n \leq \gamma_k^{(n-1)/(k-1)}$ for $n \geq k \geq 2$ (see [14]):

Theorem 5.3. *If a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an n-dimensional lattice L is block-ratio reduced with blocksize k and factor ε where $n = p(k-1)+1$ with $p \geq 1$ and $\varepsilon \geq 0$, then*

$$\|\mathbf{b}_1\| \leq (\sqrt{1+\varepsilon}\mu_k)^{(n-1)/(k-1)} \|\mathbf{b}_n^*\|.$$

Proof. By the definition, the block $B_{[i(k-1)+1, i(k-1)+k]}$ satisfies:

$$\|\mathbf{b}_{i(k-1)+1}^*\| \leq \sqrt{1+\varepsilon}\mu_k \|\mathbf{b}_{i(k-1)+k}^*\| \quad \text{for } i = 0, \ldots, p-1.$$

This immediately implies the conclusion. □

Moreover, this approximation factor is essentially tight in the worst-case, see Appendix E.

5.2.2 A reduction algorithm

Our block-ratio reduction algorithm is Algorithm 2, which uses one local algorithm based on an SRP-oracle: Algorithm 3 performs a $(1+\varepsilon)$-SRP-reduction of a given block.

Algorithm 2 Block-ratio reduction of an integer lattice

Input: An integer k, a factor $\varepsilon > 0$, and a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{Z}^{m \times n}$ in dimension $n = p(k-1)+1$.

Output: A block-ratio reduced basis of $L(B)$ with blocksize k and factor ε.

```
while $B$ is modified by the loop do
    // ⇔ While $B$ is not block-ratio reduced
    for $i = 0$ to $p-1$ do
        $(1+\varepsilon)$-SRP-reduce $B_{[i(k-1)+1, i(k-1)+k]}$ using Algorithm 3
        LLL-reduce $B$ with factor $\varepsilon$ and update the GSO matrices $B^*$ and $\mu$
    end for
end while
return $B$.
```

Algorithm 3 SRP-reduction of the block $B_{[i(k-1)+1,i(k-1)+k]}$

```
Input: A blocksize $k$, a factor $\varepsilon$, and a basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{Z}^{m\times n}$ with its GSO matrices $B^*$ and $\mu$.
Output: The block $B_{[i(k-1)+1,i(k-1)+k]}$ becomes $(1+\varepsilon)$-SRP-reduced, but none of the basis vectors outside the block are modified.
Let $j = i(k-1)$
if $i = 0$ then $C \leftarrow B_{[1,k]}$
else
    Compute $B_{[j+1,j+k]} \leftarrow (\mathbf{b}^*_{j+1}, \dots, \mathbf{b}^*_{j+k})(\mu_{\iota,j})^t_{j+1\leq\iota,j\leq j+k}$
    Compute $C \leftarrow \det((B_{[1,j]})^t B_{[1,j]}) B_{[j+1,j+k]}$
end if
    //Note that $C \in \mathbb{Z}^{m\times k}$ and $\mu_k(L(C))^2 = \mu_k(L(B_{[j+1,j+k]}))^2 \in \mathbb{Q}$.
Call the SRP-oracle on $C$ to output a $k \times k$ unimodular matrix $\mathbf{U}$ such that $CU$ is both SRP-reduced and LLL-reduced with factor $\varepsilon$, and then compute $\mu_k(L(C))^2$
if $(1+\varepsilon)\mu_k(L(C))^2 < \frac{\|\mathbf{b}^*_{j+1}\|^2}{\|\mathbf{b}^*_{j+k}\|^2}$ then
    Compute $(\mathbf{b}_{j+1}, \dots, \mathbf{b}_{j+k}) \leftarrow (\mathbf{b}_{j+1}, \dots, \mathbf{b}_{j+k})U$
end if
return $B$.
```

We first show correctness of Algorithm 2:

Theorem 5.4. *For all $\varepsilon \geq 0$, Algorithm 2 terminates, and outputs a block-ratio reduced basis with blocksize k and factor ε.*

Proof. Let B_0 denote the input integer lattice basis and B denote the current basis during the execution. Following the standard analysis of LLL [29], we consider the following integral potential

$$P(B) = \prod_{i=0}^{p-1} \mathrm{vol}(B_{[1,i(k-1)+1]})^2 \mathrm{vol}(B_{[1,(i+1)(k-1)]})^2 \in \mathbb{Z}. \tag{5.3}$$

Then, the initial potential satisfies $\log P(B_0) \leq 2np \log \|B_0\|$ and every operation in Algorithm 2 either preserves or strictly decreases $P(B)$. More precisely, if each $(1+\varepsilon)$-SRP-reduction modifies the block $B_{[i(k-1)+1,i(k-1)+k]}$ for some $i \in [0; p-1]$, or each special swap of LLL (in line 5) between two indices $(i(k-1)+1, i(k-1)+2)$ or $((i+1)(k-1), i(k-1)+k)$ occurs, then the integer $P(B)$ is reduced by a multiplicative factor $< \frac{1}{1+\varepsilon}$. Therefore, there is a bounded number of such $(1+\varepsilon)$-SRP-reductions and special swaps even if $\varepsilon = 0$. The operations which preserve $P(B)$ cannot modify the basis indefinitely. Hence, Algorithm 2 terminates for all $\varepsilon \geq 0$.

It is easy to see that Algorithm 2 finally outputs a block-ratio reduced basis with blocksize k and factor ε. Indeed, the output basis is size-reduced due to the LLL-reduction; each block $B_{[i(k-1)+1,i(k-1)+k]}$ is $(1+\varepsilon)$-SRP-reduced due to the use of Algorithm 3. This completes the proof. □

5.2.3 Complexity analysis

The following theorem shows that Algorithm 2 is in fact polynomial, in the same sense as blockwise reduction algorithms [53, 12, 14] to approximate SVP.

Theorem 5.5. *Given as inputs a blocksize k, a reduction factor $\varepsilon \in (0,1] \bigcap \mathbb{Q}$, and a basis $B_0 \in \mathbb{Z}^{m\times n}$ of dimension $n = p(k-1)+1$ with $p \geq 1$, then any execution of Algorithm 2 satisfies:*

1. *The number of calls to the SRP-oracle is $O(np^2(\log\|B_0\|)/\varepsilon)$;*
2. *The coefficients passed to the SRP-oracle have size $O(n(n+\log\|B_0\|))$;*
3. *Apart from the calls to the SRP-oracle, the algorithm only performs arithmetic operations on rational numbers such that the number of arithmetic operations is polynomial in $(\log\|B_0\|, m, 1/\varepsilon)$, and the size of the rational numbers remains polynomial in $(\log\|B_0\|, n)$.*

We consider again the integral potential $P(B)$ defined in (5.3). Since $\varepsilon > 0$, the number of calls to $(1+\varepsilon)$-SRP-reduction subroutine and special swap is at most $\frac{\log P(B_0)}{\log(1+\varepsilon)}$. That is, Algorithm 2 terminates after at most $\frac{\log P(B_0)}{\log(1+\varepsilon)}$ loops. Since every loop has p SRP-reductions, the total number of calls to the SRP-oracle is at most $\frac{2np^2 \log \|B_0\|}{\log(1+\varepsilon)}$.

It remains to bound the size of intermediate numbers and the cost of operations (apart from oracle queries) used by Algorithm 2. The key is to upper bound $\|B\|$ during the execution with respect to $\|B_0\|$. We have

$$\|B\| \leq \begin{cases} 2^{4kn^2}\|B_0\|^{4kn} & \text{at the end of Step 4,} \\ 2^{n-1}\|B_0\| & \text{at the end of Step 5.} \end{cases}$$

Indeed, since the current basis B right after Step 5 is LLL-reduced with factor $\varepsilon \in (0,1]$, Lemma C.1 implies $\|B\| \leq 2^{n-1}\|B_0\|$. Consider Step 4, where Algorithm 3 is called: for index $i \in [0, p-1]_{\mathbb{Z}}$, the integer matrix C appearing in Algorithm 3 satisfies $\|C\| \leq (2^n\|B_0\|)^{2i(k-1)+k} \leq (2^n\|B_0\|)^{2n-k}$ and the SRP-oracle outputs a unimodular transformation U such that $\|U\| \leq 2^{k-1}k^{k+1}\|C\|^{2k}$ by Lemma C.1; then the current basis B right after Step 4 has magnitude: $\|B\| \leq \sqrt{k}\|U\|(2^n\|B_0\|) \leq 2^{4kn^2}\|B_0\|^{4kn}$.

Therefore, we always have $\log\|B\| \leq 4kn(n + \log\|B_0\|)$ throughout Algorithm 2: by the classical analysis of the LLL algorithm [29, Proposition 1.26], a single execution of Steps 4-5 (except the oracle) runs in time polynomial in $(\log\|B_0\|, m, 1/\varepsilon)$ and works on rational numbers which have size polynomial in $(\log\|B_0\|, n)$ during the computation.

This completes the proof of Theorem 5.5. We conclude that the running time of Algorithm 2 can be upper bounded by a polynomial factor times the cost of the SRP-oracle. Hence, Algorithm 2 is polynomial in the same sense as blockwise reduction algorithms [53, 12, 14, 30]. In particular, if $k \leq \frac{\log n}{\log\log n}$ and we select Algorithm 1 as the SRP-oracle, then Algorithm 2 runs in polynomial time.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger. Closest point search in lattices. *IEEE Transactions on Information Theory*, 48(8):2201–2214, 2002.

[2] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of STOC '96*, pages 99–108. ACM, 1996.

[3] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of STOC '98*, pages 10–19. ACM, 1998.

[4] A. M. Bergé and J. Martinet. Sur un problème de dualite lié aux sphères en géométrie des nombres. *Journal of Number Theory*, 32:14–42, 1989.

[5] H. F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 16:227–235, 1914.

[6] J. Buchmann and M. Pohst. Computing a lattice basis from a system of generating vectors. In *Proceedings of the 1987 European Conference on Computer Algebra (EUROCAL '87)*, volume 378 of *LNCS*, pages 54–63. Springer-Verlag, 1987.

[7] Y. Chen and P. Q. Nguyen. BKZ 2.0: better lattice security estimates. In *Proceedings of ASIACRYPT '11*, volume 7073 of *LNCS*, pages 1–20. Springer-Verlag, 2011.

[8] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, New York, second edition, 1995.

[9] D. Dadush and D. Micciancio. Algorithms for the densest sub-lattice problem. In *Proceedings of SODA '13*, pages 1103–1122. SIAM, 2013.

[10] D. Dadush, C. Peikert, and S. Vempala. Enumerative lattice algorithms in any norm via M-ellipsoid coverings. In *Proceedings of FOCS '11*, pages 580–589. IEEE, 2011.

[11] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, 1985.

[12] N. Gama, N. Howgrave-Graham, H. Koy, and P. Nguyen. Rankin's constant and blockwise lattice reduction. In *Proceedings of CRYPTO '06*, volume 4117 of *LNCS*, pages 112–130. Springer-Verlag, 2006.

[13] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen. Symplectic lattice reduction and NTRU. In *Proceedings of EUROCRYPT '06*, volume 4004 of *LNCS*, pages 233–253. Springer-Verlag, 2006.

[14] N. Gama and P. Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In *Proceedings of STOC '08*, pages 207–216. ACM, 2008.

[15] N. Gama and P. Q. Nguyen. Predicting lattice reduction. In *Proceedings of EUROCRYPT '08*, volume 4965 of *LNCS*, pages 31–51. Springer-Verlag, 2008.

[16] N. Gama, P. Q. Nguyen, and O. Regev. Lattice enumeration using extreme pruning. In *Proceedings of EUROCRYPT '10*, volume 6110 of *LNCS*, pages 257–278. Springer-Verlag, 2010.

[17] G. Hanrot, X. Pujol, and D. Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *Proceedings of CRYPTO '11*, volume 6841 of *LNCS*, pages 447–464. Springer-Verlag, 2011.

[18] G. Hanrot and D. Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm. In *Proceedings of CRYPTO '07*, volume 4622 of *LNCS*, pages 170–186. Springer-Verlag, 2007.

[19] J. Håstad and J. C. Lagarias. Simultaneously good bases of a lattice and its reciprocal lattice. *Mathematische Annalen*, 287:163–174, 1990.

[20] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *Proceedings of STOC '07*, pages 469–477. ACM, 2007.

[21] B. Helfrich. Algorithms to construct Minkowski reduced an Hermite reduced lattice bases. *Theoretical Computer Science*, 41:125–139, 1985.

[22] C. Hermite. Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre. *J. Reine Angew. Math.*, 40:279–290, 1850. Also available in the first volume of Hermite's complete works, published by Gauthier-Villars.

[23] A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. *Journal of Cryptology*, 11(3):161–185, 1998.

[24] G. A. Kabatiansky and V. I. Levenshtein. On bounds for packings on a sphere and in space. *Problemy Peredachi Informatsii*, 14(1):3–25, 1978.

[25] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of STOC '83*, pages 193–206. ACM, 1983.

[26] A. Korkine and G. Zolotareff. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873.

[27] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[28] A. K. Lenstra. Lattices and factorization of polynomials over algebraic number fields. In *Proceedings of the 1982 European Conference on Computer Algebra (EUROCAL '82)*, volume 144 of *LNCS*, pages 32–39. Springer-Verlag, 1982.

[29] A. K. Lenstra, H. W. Lenstra. JR., and L. Lovász. Factoring polynomials with rational coeffcients. *Mathematische Annalen*, 261:366–389, 1982.

[30] J. Li and P. Q. Nguyen. Approximating the densest sublattice from Rankin's inequality. *LMS Journal of Computation and Mathematics*, 17(Special Issue A):92–111, 2014. Contributed to the 11th Algorithmic Number Theory Symposium (ANTS-XI), GyeongJu, Korea, 6-11 August 2014.

[31] J. Li and W. Wei. Slide reduction, successive minima and several applications. *Bulletin of the Australian Mathematical Society*, 88:390–406, 12 2013.

[32] L. Lovász. *An algorithmic theory of numbers, graphs and convexity. CBMSNSF Regional Conference Series in Applied Mathematics.* SIAM, 1986.

[33] H. Lütkepohl. *Handbook of matrices*. John Wiley & Sons, New York, 1996.

[34] S. S. Magliveras, T. van Trung, and W. Wei. Primitive sets in a lattice. *Australasian Journal of Combinatorics*, 40:173–186, 2008.

[35] J. Martinet. *Perfect lattices in Euclidean spaces*. Springer-Verlag, New York, 2002.

[36] 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, 2002.

[37] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *Proceedings of STOC '10*, pages 351–358. ACM, 2010.

[38] D. Micciancio and M. Walter. Fast lattice point enumeration with minimal overhead. In *Proceedings of SODA '15*, pages 276–294. SIAM, 2015.

[39] D. Micciancio and M. Walter. Practical, predictable lattice basis reduction. *IACR Cryptology ePrint Archive*, 2015:1123, 2015.

[40] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York, 1973.

[41] L. J. Mordell. Observation on the minimum of a positive quadratic form in eight variables. *Journal of the London Mathematical Society*, 19:3–6, 1944.

[42] M. Newman. Bounds for cofactors and arithmetic minima of quadratic forms. *Journal of the London Mathematical Society*, 38:215–217, 1963.

[43] P. Q. Nguyen. Lattice reduction algorithms: theory and practice. In *Proceedings of EUROCRYPT '11*, volume 6632 of *LNCS*, pages 2–6. Springer-Verlag, 2011.

[44] P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Proceedings of the 2001 Cryptography and Lattices Conference (CALC '01)*, volume 2146 of *LNCS*, pages 146–180. Springer-Verlag, 2001.

[45] P. Q. Nguyen and B. Vallée, editors. *The LLL algorithm: survey and applications*. Information Security and Cryptography. Springer-Verlag, New York, 2010.

[46] A. Novocin, D. Stehlé, and G. Villard. An LLL-reduction algorithm with quasi-linear time complexity. In *Proceedings of STOC '11*, pages 403–412. ACM, 2011.

[47] M. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *ACM Sigsam Bulletin*, 15:37–44, 1981.

[48] X. Pujol and D. Stehlé. Rigorous and efficient short lattice vectors enumeration. In *Proceedings of ASIACRYPT '08*, volume 5350 of *LNCS*, pages 390–405. Springer-Verlag, 2008.

[49] R. A. Rankin. On positive definite quadratic forms. *Journal of the London Mathematical Society*, 28:309–314, 1953.

[50] O. Regev. Lecture 8: Dual lattices. *http://www.cims.nyu.edu/regev/teaching/lattices-fall-2004/index.html*, 2004.

[51] Saruchi, I. Morel, D. Stehlé, and G. Villard. LLL reducing with the most significant bits. In *Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation (ISSAC '14)*, pages 367–374. ACM, 2014.

[52] K. Sawatani, T. Watanabe, and K. Okuda. A note on the Hermite-Rankin constant. *Journal de Théorie des Nombres de Bordeaux*, 22:209–217, 2010.

[53] C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[54] C. P. Schnorr. Block Korkin-Zolotarev bases and successive minima. *Combinatorics, Probability and Computing*, 3:507–522, 1994.

[55] C. P. Schnorr. Lattice reduction by random sampling and birthday methods. In *Proceedings of STACS '03*, volume 2607 of *LNCS*, pages 145–156. Springer-Verlag, 2003.

[56] C. P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–199, 1994.

[57] M. Seysen. Simultaneous reduction of a lattice basis and its reciprocal basis. *Combinatorica*, 13(3):363–376, 1993.

[58] C. L. Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, New York, 1989.

[59] D. Stehlé and M. Watkins. On the extremality of an 80-dimensional lattice. In *Proceedings of the 9th Algorithmic Number Theory Symposium (ANTS-IX)*, volume 6197 of *LNCS*, pages 340–356. Springer-Verlag, 2010.

[60] M. Walter. Lattice point enumeration on block reduced bases. In *Proceedings of the 8th International Conference on Information Theoretic Security (ICITS '15)*, volume 9063 of *LNCS*, pages 269–282. Springer-Verlag, 2015.

[61] H. Yanai, K. Takeuchi, and Y. Takane. *Projection matrices, generalized inverse matrices, and singular value decomposition*. Springer-Verlag, New York, 2011.

A Proof of Proposition 1.1

Proof. We first bound $\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n}$. The linked conditions imply:

$$\|\mathbf{b}_1\| \leq h(k+1)^i \|\mathbf{b}^*_{ik+1}\| \text{ for } i = 0, \ldots, p-1. \tag{A.1}$$

Together with the Hermite conditions, we have

$$\|\mathbf{b}_1\| \leq g(k)h(k+1)^i \mathrm{vol}(B_{[ik+1,ik+k]})^{1/k} \text{ for } i = 0, \ldots, p-1.$$

The product of the above p inequalities for $i \in [0, p-1]_{\mathbb{Z}}$ gives rise to:

$$\|\mathbf{b}_1\| \leq g(k)h(k+1)^{(n-k)/2k} \mathrm{vol}(L)^{1/n}.$$

We now bound $\|\mathbf{b}_1\|/\lambda_1(L)$ under the assumption. Let $\mathbf{u}$ be a shortest vector of L. Then $\mathbf{u}$ can be written as $\mathbf{u} = \sum_{i=1}^t \alpha_i \mathbf{b}_i$ where $\alpha_t \neq 0$. Thus, $qk+1 \leq t \leq qk+k$ for some $q \in [0, p-1]_{\mathbb{Z}}$. Since $\pi_{qk+1}(\mathbf{u})$ is a nonzero vector of $L(B_{[qk+1,qk+k]})$, $\|\pi_{qk+1}(\mathbf{u})\| \geq \lambda_1(L(B_{[qk+1,qk+k]}))$. Therefore,

$$\|\mathbf{b}^*_{qk+1}\| \leq \sqrt{1+\varepsilon}\lambda_1(L(B_{[qk+1,qk+k]})) \leq \sqrt{1+\varepsilon}\|\pi_{qk+1}(\mathbf{u})\| \leq \sqrt{1+\varepsilon}\|\mathbf{u}\| = \sqrt{1+\varepsilon}\lambda_1(L).$$

By (A.1), this implies $\|\mathbf{b}_1\|/\lambda_1(L) \leq \sqrt{1+\varepsilon}\|\mathbf{b}_1\|/\|\mathbf{b}^*_{qk+1}\| \leq \sqrt{1+\varepsilon}h(k+1)^{(n-k)/k}$ since $qk+k \leq n$. This completes the proof. □

B Critical lattices for μ_n

An n-dimensional lattice L is *critical* for μ_n if $\mu_n(L) = \mu_n$. Consider the upper triangular matrix:

$$B = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{3}{4}} & \frac{1}{\sqrt{12}} & \frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} & \sqrt{\frac{3}{8}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{8}} & \frac{1}{\sqrt{6}} & \sqrt{\frac{2}{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{12}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Let $B^{(i)}$ denote the upper left $i \times i$ block of B for $i = 1, \ldots, 8$. The following properties hold:

1. $\mathbb{A}_2 = L(B^{(2)}), \mathbb{A}_3 = L(B^{(3)}), \mathbb{D}_4 = L(B^{(4)}), \mathbb{D}_5 = L(B^{(5)}), \mathbb{E}_6 = L(B^{(6)}), \mathbb{E}_7 = L(B^{(7)})$ and $\mathbb{E}_8 = L(B^{(8)})$ (see [35, Chapter 4] for details);
2. B is i-Rankin reduced for $1 \leq i \leq 7$ (see [52, Proposition 1]).

Our main result of this appendix is as follows:

Proposition B.1. *$\mu_2 = \mu_2(\mathbb{A}_2) = \frac{2}{\sqrt{3}}$, $\mu_3 = \mu_3(\mathbb{A}_3) = \sqrt{\frac{3}{2}}$, $\mu_4 = \mu_4(\mathbb{D}_4) = \sqrt{2}$, $\mu_5 \geq \mu_5(\mathbb{D}_5) = \sqrt{2}$, $\mu_6 \geq \mu_6(\mathbb{E}_6) = \sqrt{\frac{8}{3}}$, $\mu_7 \geq \mu_7(\mathbb{E}_7) = \sqrt{3}$ and $\mu_8 = \mu_8(\mathbb{E}_8) = 2$.*

Our proof of Proposition B.1 uses the lemma below.

Lemma B.2 (Sufficient Condition)**.** *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of an n-dimensional lattice L. If B is SVP-reduced and $(n-1)$-Rankin-reduced, then B reaches $\mu_n(L)$. Conversely, it may not be true.*

Proof. Let $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ be a SRP-reduced basis of L. The identity (2.1) implies

$$\mu_n(L) = \frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,n-1]})}{\mathrm{vol}(L)} \geq \frac{\|\mathbf{b}_1\| \cdot \mathrm{vol}(B_{[1,n-1]})}{\mathrm{vol}(L)} \geq \mu_n(L).$$

Thus, B reaches $\mu_n(L)$. The second assertion follows from Example 1. □

Proof of Proposition B.1. For each $i \in [2, 8]_{\mathbb{Z}}$, by Property 2, $B^{(i)}$ is SVP-reduced and $(i-1)$-Rankin reduced. Then $B^{(i)}$ reaches $\mu_i(L(B^{(i)}))$ by Lemma B.2. The claim follows easily from Theorem 4.11. □

C Bounding the size of transformation

Lemma C.1 (Adapted from [30, Lemma C.2])**.** *Let $B \in \mathbb{Z}^{m \times n}$ be an n-dimensional lattice basis and $U \in \mathbb{Z}^{n \times n}$ be a unimodular matrix. If $C = BU$ is LLL-reduced with factor $\varepsilon \geq 0$, then*

$$\|C\| \leq \alpha^{(n-1)/2} \|B\| \quad \text{and} \quad \|U\| \leq \alpha^{(n-1)/2} n^{n+1} \|B\|^{2n}$$

where $\alpha = 4(1+\varepsilon)/(3-\varepsilon)$.

Proof. The conclusion is slightly different from [30, Lemma C.2], in which B is also LLL-reduced. The proof essentially follows the same principle as the one of [30, Lemma C.2].

The classical property on LLL-reduced bases [29, Proposition 1.12] implies $\|C\|^2 \leq \alpha^{n-1} \|B\|^2$.

We use the Frobenius norm $\| \cdot \|_F$ to bound $\|U\|$. Since $U = (B^t B)^{-1} B^t C$, we have

$$\|U\|_F = \|(B^t B)^{-1} B^t C\|_F \leq \|(B^t B)^{-1}\|_F \|B^t\|_F \|C\|_F. \tag{C.1}$$

Note that $\|\widetilde{A}\|_F \leq n\|A\|_F^{n-1}$ for $A \in \mathbb{R}^{n\times n}$ (see [30, Lemma C.1.(iv)]), $\det(B^tB)$ is a positive integer, and $\|B^tB\|_F \leq \|B^t\|_F\|B\|_F = \|B\|_F^2$, we obtain

$$\|(B^tB)^{-1}\|_F = \|\det(B^tB)^{-1}\widetilde{B^tB}\|_F \leq \|\widetilde{B^tB}\|_F \leq n\|B^tB\|_F^{n-1} \leq n\|B\|_F^{2(n-1)}. \tag{C.2}$$

Since $\|B\| \leq \|B\|_F \leq \sqrt{n}\|B\|$, by (C.1), this implies $\|U\| \leq \|U\|_F \leq n\|B\|_F^{2n-1}\|C\|_F \leq \alpha^{(n-1)/2}n^{n+1}\|B\|^{2n}$. This completes the proof. □

Lemma C.2. *Let $B \in \mathbb{Z}^{m\times n}$ be column independent and $\mathbf{x} \in \mathbb{Z}^n$. If $B\mathbf{x} = \mathbf{b}$, then $\|\mathbf{x}\|_\infty \leq \|B\|^{n-1}\|\mathbf{b}\|$.*

Proof. Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and $B_i = (\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n)$ for $i = 1, \ldots, n$, define integers:

$$y = \det(B^tB) \quad \text{and} \quad z_i = \det(B^tB_i) \quad \text{for} \quad i = 1, \ldots, n.$$

Since $B\mathbf{x} = \mathbf{b}$ is equivalent to $B^tB\mathbf{x} = B^t\mathbf{b}$ and B^tB is a nonsingular square matrix, Cramer's rule implies $\mathbf{x} = (\frac{z_1}{y}, \ldots, \frac{z_n}{y})^t$. To complete the proof, it suffices to upper bound the $|\frac{z_i}{y}|$'s.

For each i, by Cauchy-Schwartz's inequality on determinants (see, *e.g.*, [33, p. 54]), we have

$$|\det(B^tB_i)|^2 \leq \det(B^tB)\det(B_i^tB_i).$$

It is calssical that $0 < \det(B_i^tB_i) \leq (\prod_{j\neq i}\|\mathbf{b}_j\|^2)\|\mathbf{b}\|^2$ if B_i is column independent and $\det(B_i^tB_i) = 0$ otherwise. Thus, $0 \leq \det(B_i^tB_i) \leq \|B\|^{2n-2}\|\mathbf{b}\|^2$. Since $\det(B^tB)$ is a positive integer, this implies

$$|\frac{z_i}{y}| = |\frac{\det(B^tB_i)}{\det(B^tB)}| \leq \frac{\sqrt{\det(B^tB)\det(B_i^tB_i)}}{\det(B^tB)} \leq \sqrt{\det(B_i^tB_i)} \leq \|B\|^{n-1}\|\mathbf{b}\| \quad \text{for} \quad i = 1, \ldots, n.$$

Therefore, $\|\mathbf{x}\|_\infty \leq \|B\|^{n-1}\|\mathbf{b}\|$, which completes the proof. □

D DSVP-reduction of the projected block

Algorithm 4 performs a DSVP-reduction of a given block. The algorithm differs in the usage of local procedures (*i.e.*, Steps 2-7) from the DSVP-algorithm presented in [14, Algorithm 3]. The advantage of Algorithm 4 is that it can compute the reversed dual basis of input basis (see Steps 2-5); the unimodular matrix and the occurring integers at Step 7 have small magnitudes (see [34] for details).

Algorithm 4 DSVP-reduction of the block $B_{[i,n]}$

```
Input: A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{Z}^{m\times n}$ and an index $i \in [1, n-1]_{\mathbb{Z}}$.
Output: The block $B_{[i,n]}$ becomes DSVP-reduced, but the lattice $L(B)$ and the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$ remain unchanged.
 1: Let $k = n - i + 1$ denote the size of the block
 2: Compute the GSO matrices $B^*$ and $\mu$ of $B$.
 3: Compute $(B^*)^{-s} \leftarrow R_m(\frac{\mathbf{b}_n^*}{\|\mathbf{b}_n^*\|^2}, \ldots, \frac{\mathbf{b}_1^*}{\|\mathbf{b}_1^*\|^2})$ and $\mu^{-s} \leftarrow \sum_{j=0}^{n-1} N^j$ where $N = I_n - \mu^s$
 4:     //Note that $B = B^*\mu$ implies $B^{-s} = (B^*)^{-s}\mu^{-s}$
 5: Compute $B^{-s} \leftarrow (B^*)^{-s}\mu^{-s}$    //Note that $\det(B^tB)B^{-s} = R_mB(\widetilde{B^tB})R_n$ is integral
 6: Call the MV SVP-algorithm [37] on $\det(B^tB)(B^{-s})_{[1,k]}$ to output a primitive vector $\mathbf{x} = (x_1, \ldots, x_k)^t$ for $\mathbb{Z}^k$ such that $(B^{-s})_{[1,k]}\mathbf{x}$ is the shortest vector of lattice $L((B^{-s})_{[1,k]})$
 7: Call Magliveras et al.'s algorithm [34, Algorithm A] to extend $\mathbf{x}$ into a unimodular matrix $U \in \mathbb{Z}^{k\times k}$
 8:     //Note that $\mathbf{x}$ is the first column of $U$ and hence $(B_{[i,n]})^{-s}U = (B^{-s})_{[1,k]}U$ is SVP-reduced.
 9: Compute $U^{-s} \leftarrow R_kU^{-t}R_k$
10: Compute $(\mathbf{b}_i, \ldots, \mathbf{b}_n) \leftarrow (\mathbf{b}_i, \ldots, \mathbf{b}_n)U^{-s}$
11: return $B$.
```

The main result on Algorithm 4 is the following:

Theorem D.1. *Given as inputs a basis $B \in \mathbb{Z}^{m\times n}$ and an index $i \in [1, n-1]_{\mathbb{Z}}$, Algorithm 4 outputs a basis C of $L(B)$ such that $B_{[1,i-1]} = C_{[1,i-1]}$, $C_{[i,n]}$ is DSVP-reduced and $\|C\| \leq n^{n^2(n-i+1)}\|B\|^{2n^2(n-i+1)}$. The algorithm requires $poly(\log\|B\|, m)\cdot 2^{2(n-i+1)}$ bit operations and $poly(\log\|B\|, m)\cdot 2^{n-i+1}$ space.*

Proof. We first show correctness. Since U is unimodular, so is U^{-s} and hence $L(B) = L(C)$. Note that $(B_{[i,n]})^{-s}U$ is SVP-reduced, then $C_{[i,n]} = B_{[i,n]}U^{-s} = ((B_{[i,n]})^{-s}U)^{-s}$ is DSVP-reduced.

Next, we upper bound $\|C\|$ with respect to $\|B\|$. Using (C.2), we can deduce that

$$\|\det(B^tB)B^{-s}\|_{\mathbb{F}} = \|B\widetilde{(B^tB)}\|_F \leq \|B\|_F\|\widetilde{B^tB}\|_F \leq n\|B\|_F^{2n-1} \leq n^{n+1/2}\|B\|^{2n-1}. \tag{D.1}$$

Since $\|\det(B^tB)(B^{-s})_{[1,k]}\| \leq \|\det(B^tB)B^{-s}\|_{\mathbb{F}}$ where $k = n-i+1$, Lemma C.2 implies

$$\|\mathbf{x}\|_\infty \leq \|\det(B^tB)(B^{-s})_{[1,k]}\|^n \leq n^{n^2+n/2}\|B\|^{2n^2-n}. \tag{D.2}$$

Note that $\|U\|_\infty \leq \|\mathbf{x}\|_\infty$, we have

$$\|U^{-s}\|_{\mathbb{F}} = \|U^{-1}\|_F = \|\widetilde{U}\|_F \leq k\|U\|_F^{k-1} \leq k(k\|U\|_\infty)^{k-1} \leq k^k\|\mathbf{x}\|_\infty^{k-1}. \tag{D.3}$$

Let G and H denote the matrices formed by the last k columns of B and C, respectively. Step 10 implies $H = GU^{-s}$. Since $\|G\|_{\mathbb{F}} \leq \sqrt{k}\|B\|$, it follows from (D.2) and (D.3) that

$$\|H\| \leq \|H\|_{\mathbb{F}} \leq \|G\|_{\mathbb{F}}\|U^{-s}\|_{\mathbb{F}} \leq n^{n^2k}\|B\|^{2n^2k}.$$

Therefore, $\|C\| \leq n^{n^2k}\|B\|^{2n^2k}$ since $B_{[1,i-1]} = C_{[1,i-1]}$.

It remains to analyze the complexity. Step 6 requires $\mathrm{poly}(n\log(n\|B\|), m)\cdot 2^{2(n-i+1)}$ bit operations and $\mathrm{poly}(n\log(n\|B\|), m)\cdot 2^{n-i+1}$ space by (D.1), and the other steps run in time polynomial in $(\log\|B\|, m)$. This proves the conclusion. □

E The worst-case behaviour of block-ratio reduction

The upper-bound in Theorem 5.3 can be matched in the worst-case if $\varepsilon = 0$, as shown below.

Theorem E.1. *For $n = p(k-1)+1$ and all $\varepsilon \geq 0$, there exists an n-dimensional block-ratio reduced basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ with blocksize k and factor ε such that $\|\mathbf{b}_1\| = \mu_k^{(n-1)/(k-1)}\|\mathbf{b}_n^*\|$.*

Proof. The technical idea stems from the worst-case analysis of slide reduction [14, Section 4]. By Theorems 4.1 and 4.4, there exists a k-dimensional lattice L with SRP-reduced basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_k)$ such that $\mu_k = \mu_k(L) = \|\mathbf{c}_1\|/\|\mathbf{c}_k^*\|$, where $(\mathbf{c}_1^*, \ldots, \mathbf{c}_k^*)$ is the Gram-Schmidt orthogonalization of C. It is classical that C has a unique Gram-Schmidt decomposition $C = QD\mu$, where $Q = (\frac{\mathbf{c}_1^*}{\|\mathbf{c}_1^*\|}, \ldots, \frac{\mathbf{c}_k^*}{\|\mathbf{c}_k^*\|})$ is an orthonomal set, $D = \mathrm{Diag}(\|\mathbf{c}_1^*\|, \ldots, \|\mathbf{c}_k^*\|)$, and $\mu = (\mu_{i,j})_{1\leq i,j\leq k}^t$ is upper triangular. Then the block $T = D\mu$ is upper triangular with diagonal entries $\|\mathbf{c}_i^*\|$. Further, T is also SRP-reduced and reaches μ_k, since T is isometric to C. This elementary "brick" T can be duplicated and rescaled p times to form a big n-dimensional upper-triangular matrix $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ as follows: one will match the bottom right coefficient with the top left coefficient of the next block, in such a way that $B_{[i(k-1)+1, i(k-1)+k]} = \alpha^i \cdot T$ where $\alpha = \|\mathbf{c}_k^*\|/\|\mathbf{c}_1\| = \mu_k^{-1} < 1$. Then B is block-ratio reduced with blocksize k and factor 0 such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| = \|\mathbf{c}_1\|/(\alpha^{p-1}\|\mathbf{c}_k^*\|) = \mu_k^p$. This completes the proof. □