On the Smallest Ratio Problem of Lattice Bases

Jianwei Li*

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 ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ for $i = 1, \ldots, n$ do arise in the analysis of many lattice algorithms and are somehow related to their performances. In this paper, we study the problem of minimizing the ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-rank lattice. We first prove that there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice L such that $\|\mathbf{b}_1\| = \min_{\mathbf{v}\in L\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\| \le i$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\| \le i^{1.5}$ for $1 \le i \le n$. This leads us to introduce a new NP-hard computational problem, namely the *smallest ratio problem* (SRP): given an n-rank 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 a new 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 a new lattice constant $\mu_n = \max \mu_n(L)$ over all n-rank lattices L: both the minimum and maximum are justified. Some properties of $\mu_n(L)$ and μ_n are investigated. We also present an exact algorithm and an approximation algorithm for SRP.

This is the first sound study of SRP. Our work is a tiny step towards solving an open problem proposed by Dadush-Regev-Stephens-Davidowitz (CCC '14) for tackling the closest vector problem with preprocessing, that is, whether there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice such that $\max_{1\le i\le j\le n} \|\mathbf{b}_i^*\|/\mathbf{b}_j^*\| \le \mathrm{poly}(n)$.

1 Introduction

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 $\mathbb{R}^m$ ($m \ge n$): $L = \{\sum_{i=1}^n x_i\mathbf{b}_i : x_i \in \mathbb{Z}\}$. Such a set $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ forms a *basis* of L, which has a unique Gram-Schmidt orthogonalization $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$: for each i, $\mathbf{b}_i^*$ is the component of $\mathbf{b}_i$ orthogonal to $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$. The integer n is the *rank* of L. All the bases of L have the same n-dimensional volume, called the *co-volume* $\mathrm{vol}(L)$ of L. As usual, $L(B)$ or $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ denotes the lattice generated by the n columns of a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Two of the most important lattice problems are the *shortest vector problem* (SVP) and the *closest vector problem* (CVP). Given a basis of a lattice L endowed with the Euclidean norm, SVP is to find a shortest nonzero vector in L, and CVP asks for a closest vector in L to a target vector $\mathbf{t}$. SVP is NP-hard under randomized reductions [Ajt98] and CVP is NP-complete [vEB81]: further, both problems are NP-hard to approximate to within any factor less than $n^{c/\log\log n}$ for some constant $c > 0$ under reasonable complexity-theoretic assumptions [CN98, Mic00, Kho05, HR12, ABSS93, DKRS03]. Algorithms for solving SVP and CVP either exactly or approximately have proved invaluable in many fields of mathematics and computer science, notably in cryptology (see, *e.g.*, [Ajt96, MG02, JS98, NV10]).

The most basic approach for solving both SVP and CVP exactly is *enumeration*, which requires $n^{O(n)}$-time and polynomial space (see, *e.g.*, [Kan87, SE94, HS07, GNR10, MW15]). The classical approach for approximating SVP is known as *lattice reduction*, which is to find good reduced bases consisting of reasonably short and almost orthogonal vectors: it was revived with the celebrated LLL algorithm [LLL82] and continued with blockwise algorithms [Sch87, SE94, GN08, MW16]. Both enumeration and lattice reduction are still very active in recent years (see, *e.g.*, [MW15, MW16, ANSS18, ABF+20, ALNS20, ABLR20, LN20]).

The most famous approximation algorithm for CVP is perhaps the Babai nearest plane algorithm [Bab86]. Given a basis $B = (\mathbf{b}_1, \cdots, \mathbf{b}_n)$ of a lattice L and a target vector $\mathbf{t} \in \mathbb{R}^m$, Babai's algorithm size-reduces $\mathbf{t}$ with respect to B into a new vector $\mathbf{t} - \mathbf{x}$ with $\mathbf{x} \in L$ such that

$$\|\mathbf{t} - \mathbf{x}\| \le \left(\max_{1\le i\le n} \frac{\sqrt{\sum_{j=1}^i \|\mathbf{b}_j^*\|^2}}{\|\mathbf{b}_i^*\|} \right) \times \min_{\mathbf{y}\in L} \|\mathbf{t} - \mathbf{y}\|.$$

In other words, Babai's algorithm approximates the *closest vector problem with preprocessing* (CVPP) to within $\max_{1\le i\le n} \frac{\sqrt{\sum_{j=1}^i \|\mathbf{b}_j^*\|^2}}{\|\mathbf{b}_i^*\|}$ factor, when using the basis B as preprocessing. CVPP has applications in coding theory and cryptography [MG02, DRS14]. Dadush-Regev-Stephens-Davidowitz (DRS) [DRS14] proposed an open problem whether every lattice has a basis that one can use to obtain a polynomial approximation for CVPP. Once specialized to Babai's algorithm, DRS's open problem is equivalent to Seysen's open problem [Sey93] whether there exists

*Information Security Group, Royal Holloway, University of London. Email: Jianwei.Li@rhul.ac.uk

a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice such that the Gram-Schmidt decay $\max_{1\le i\le j\le n} \|\mathbf{b}_i^*\|/\|\mathbf{b}_j^*\| \le \mathrm{poly}(n)$. The best known upper bound is $n^{(1+\ln n)/2}$ [Sch87, LLS90, Ajt08, HS08] using a HKZ-reduced basis introduced by Hermite [Her50] and Korkine and Zolotareff [KZ73].

We fail to solve DRS/Seysen's open problem. Recall that any HKZ-reduced basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an n-rank lattice L satisfies [LLS90]: $\|\mathbf{b}_1\| = \lambda_1(L)$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\| \le i^{(1+\ln i)/2}$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\| \le i^{1+\frac{1}{2}\ln i}$ for $i = 1, \ldots, n$, where $\lambda_1(L)$ denotes the (Euclidean) length of the shortest nonzero vector in L. This inspires us to consider an interesting relaxation of the above open problem whether there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice L such that all of the ratios $\|\mathbf{b}_1\|/\lambda_1(L)$, $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|$ simultaneously have upper bounds polynomial in i for $i = 1, \ldots, n$. The motivation comes from the fact that the ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ and $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|$ do come up in the analysis of many lattice algorithms and are somehow related to their performances:

- The cost of enumeration is somehow related to the ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$: the smaller the heuristic estimation $\max_{1\le k\le n}\left(\prod_{i=n-k+1}^{n} \frac{\|\mathbf{b}_1\|}{\sqrt{k}\|\mathbf{b}_i^*\|}\right)$, the faster the enumeration (see, *e.g.*, [GNR10, HS07]).
- Since $\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n} = \prod_{i=1}^{n}(\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|)^{1/n}$ and $\|\mathbf{b}_1\|/\lambda_1(L) \le \max_{1\le i\le n}\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$, the ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ are related 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 assess the quality of a reduced basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ (see, *e.g.*, [LLL82, Sch87, GHGKN06, GN08, HPS11, MW16, ALNS20]). More precisely, some classical lattice reduction algorithms follow the paradigm below (see Appendix A for the proof).

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

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

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

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

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

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

  Here, $B_{[i,j]}$ denotes the projected block of the vectors $\mathbf{b}_i, \ldots, \mathbf{b}_j$ over $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$.

  It can be checked that the LLL-reduction [LLL82], BKZ-reduction [Sch87, SE94], semi k-reduction [Sch87] and slide reduction (achieving the best time/quality trade-off among known lattice reduction algorithms) [GN08, ALNS20] follow the paradigm. This means that at least in theory, the local ratios $\|\mathbf{b}_{ik+1}^*\|/\|\mathbf{b}_{ik+k+1}^*\|$ might play a more important role on the output quality of lattice reduction than the local Hermite factors $\|\mathbf{b}_{ik+1}^*\|/\mathrm{vol}(B_{[ik+1,ik+k]})^{1/k}$.
- The ratios $\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|$ are natively related to the *orthogonality defect* $\prod_{i=1}^{n}(\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|)$, which measures the orthogonality of a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ [Len82, LLS90].

In order to study the minimality of multiple ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ for $i = 1, \ldots, n$, a natural way is to resolve it into a more basic problem of minimizing the single ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-rank lattice. A natural question is whether there is a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ is minimal. If yes, one may be interested to further investigate the hardness and algorithmic aspects of the computational problem of finding such a basis.

In mathematics, SVP is tightly related to the study of Hermite's constant γ_n, namely $\gamma_n = \max \lambda_1(L)^2$ over all n-rank lattices L of unit co-volume. This fundamental parameter in the geometry of numbers is typically used in the study of both enumeration algorithms and lattice reduction algorithms, *e.g.*, to measure the running time [Hel85, HS07] and output quality [GN08, HPS11, MW16, ALNS20] respectively. By analogy with this case, one may wonder what should be the lattice parameters related to the problem of minimizing the ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$.

This paper first formalizes and answers the aforementioned questions, excluding DRS/Seysen's open problem. Our work is a tiny step towards solving DRS/Seysen's open problem and might be useful in the design and analysis of better lattice algorithms for SVP and CVP.

Our results. Our first main result of this paper is as follows:

Theorem 1.2. *For any n-rank lattice L in $\mathbb{R}^m$, there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that the following inequalities simultaneously hold:*

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

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

This means that there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice L such that $\max_{1\le i\le n}(\|\mathbf{b}_i\|/\|\mathbf{b}_i^*\|) \le n^{1.5}$. It indeed solves a weaker version of the so-called well-conditioned basis problem [HL90, Sey93] minimizing the quantity $S(B) = \max_{1\le i\le n}(\|\mathbf{b}_i\| \cdot \|\mathbf{d}_i\|)$ over all bases $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given lattice L, where $(\mathbf{d}_1, \ldots, \mathbf{d}_n)$ is the dual basis of B: it is known that there exists a basis B for any n-rank lattice L such that $S(B) \le n^{O(\log n)}$ [Sey93].

Our second main result is to study the so-called *smallest ratio problem* (SRP): given an n-rank 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. It allows to construct a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ for any n-rank lattice L such that $\max_{1\le i\le n/2} \frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{n-i+1}^*\|} \le n$: yet, it is just a tiny step towards solving DRS/Seysen's open problem

SRP can also be equivalently defined as finding a pair of orthogonal nonzero vectors $\mathbf{v}$ and $\mathbf{w}$ in L and its dual lattice such that $\|\mathbf{v}\| \cdot \|\mathbf{w}\|$ is minimal. Assume that $\mathbf{w}$ is already found, finding $\mathbf{v}$ is equivalent to solving SVP on the sublattice $L \cap \mathrm{span}(\mathbf{w})^\perp$ of rank $n-1$. This intuitively suggests that SRP is related to SVP.

We show that for both the search problem and the promise problem, approximating SRP with any factor $\gamma \ge 1$ is at least as hard as approximating SVP with the same factor γ. This means that it is NP-hard to approximate SRP with any factor less than $n^{c/\log\log n}$ for some constant $c > 0$ under reasonable complexity-theoretic assumptions.

We define the 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 lattice constant $\mu_n = \max \mu_n(L)$ over all n-rank lattices L: the maximum is also justified. We then investigate some properties of $\mu_n(L)$ and μ_n. Interestingly, the new constant μ_n has close relations with classical Hermite's constant γ_n, Bergé-Martinet's constant γ'_n [BM89] and Korkine-Zolotareff's constant γ''_n [KZ73, Sch87, BM89, Ajt08]: 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 is to consider the algorithmic aspects of SRP. We provide a deterministic enumeration-based algorithm for solving SRP on any n-rank integer lattice with $n^{\frac{n}{e}}2^{O(n)}$ time and polynomial space.

Notice that Kannan's CVP (resp. SVP) enumeration algorithm [Kan87] solves CVP (resp. SVP) on any n-rank integer lattice with $n^{\frac{n}{2}}2^{O(n)}$ (resp. $n^{\frac{n}{2e}}2^{O(n)}$) time and polynomial space [HS07]. We hence conjecture that SRP is not harder than CVP. SRP might be useful in understanding the gap between the NP-hardnesses of SVP and CVP.

We also present a polynomial-time blockwise reduction algorithm for approximating SRP, which is an efficient 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 of an n-rank integer lattice L, a blocksize k satisfying $n = p(k-1)+1$ for some $p \ge 1$, a reduction factor $\varepsilon > 0$, and an exact SRP-oracle for any lattice of rank k, the algorithm outputs a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that

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

and the number of oracle quires is $O(p^2n^2/\varepsilon)$ (independent of the input basis).

Roadmap. Section 2 recalls background on lattices. Section 3 proves Theorem 1.2. Section 4 studies SRP and related lattice parameters. Section 5 is devoted to the algorithmic aspects of SRP. Appendices A-D provide missing details.

2 Background

Notation. This paper uses bold lower case letters to denote column vectors, and uses column-representation for matrices which are written in capital letters. The set 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 $\mathbb{A}^{m\times 1}$. Let $\|\cdot\|$ and $\langle\cdot,\cdot\rangle$ denote respectively the Euclidean norm and inner product over $\mathbb{R}^m$. For a matrix $B = (b_{i,j}) = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of n columns, we denote $\|B\| = \max\{\|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\|\}$ and $\|B\|_\infty = \max_{i,j}|b_{i,j}|$. The size of an object is the length of its binary representation. 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 $c_j > 0$. For any integers $a \le b$, we define $[a,b]_{\mathbb{Z}} = [a,b] \bigcap \mathbb{Z}$.

2.1 Lattices

GSO. Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m\times n}$ be a basis of a lattice. It is usual for lattice algorithms to consider the orthogonal projections $\pi_i : \mathbb{R}^m \to \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$ for $i = 1, \ldots, n$. The vectors $\mathbf{b}_i^* = \pi_i(\mathbf{b}_i)$ for $i = 1, \ldots, n$ are the *Gram-Schmidt vectors* of B. The *Gram-Schmidt orthogonalization* (GSO) of B is $B^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$. Then $\mathbf{b}_1^* = \mathbf{b}_1$ and $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1}\mu_{i,j}\mathbf{b}_j^*$ for $i = 2, \ldots, n$, where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^*\rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^*\rangle}$. For completeness, let $\mu_{i,i} = 1$ 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 $B = B^*\mu$.

If B is integral, then B^* and μ are rational, both of which can be computed in polynomial time [LLL82].

We will use the notation $B_{[i,j]}$ for the projected block $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_j))$. In particular, $B_{[1,j]} = (\mathbf{b}_1, \ldots, \mathbf{b}_j)$.

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 all $1 \le i, j \le n$. Two lattices of the same rank are *isometric* iff they have isometric bases.

Duality. For any n-rank lattice L in $\mathbb{R}^m$, its *dual lattice* is $L^\times = \{\mathbf{y} \in \mathrm{span}(L) : \langle \mathbf{x}, \mathbf{y}\rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in L\}$. If L has basis B, then $L^\times$ has basis $B^\times \triangleq B(B^T B)^{-1}$, which is called the *dual basis* of B. The *reversed dual basis* of B is $B^{-s} = R_m B^\times R_n$ [GHGN06], where $R_n = (r_{i,j})_{1\le i,j\le n}$ is the reversed identity matrix: $r_{i,j} = 1$ if $i + j = n + 1$ and $r_{i,j} = 0$ otherwise. In lattice reduction, it is more convenient to consider B^{-s} than to consider $B^\times$ [GN08, LN14]. The main advantage is that the reversed duality preserves upper triangular, lower triangular, diagonal and orthogonal matrices; it is fully compatible with the matrix product, for instance, $(M \cdot N)^{-s} = M^{-s} \cdot N^{-s}$ for any matrices $M, N \in \mathbb{R}^{n\times n}$; the lattice generated by B^{-s} is isometric to the standard dual lattice $L^\times$. For instance, we will use the properties below:

Lemma 2.1. *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m\times n}$ be a basis of a lattice L, $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ be $B^\times$ with its columns in reversed order, and $B^{-s} = (\mathbf{d}_1, \ldots, \mathbf{d}_n)$. Let $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$, $(\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*)$ and $(\mathbf{d}_1^*, \ldots, \mathbf{d}_n^*)$ be their GSO, respectively. Then*

$$\mathbf{b}_i^* = \frac{\mathbf{c}_{n-i+1}^*}{\|\mathbf{c}_{n-i+1}^*\|^2} \text{ for } i = 1, \ldots, n, \qquad \text{(See, e.g., [Reg04, Claim 7])} \tag{2.1}$$

$$\|\mathbf{c}_i^*\| = \|\mathbf{d}_i^*\| \text{ for } i = 1, \ldots, n, \tag{2.2}$$

$$\frac{\|\mathbf{b}_1^*\|}{\|\mathbf{b}_n^*\|} = \frac{\|\mathbf{b}_1^*\| \cdot \mathrm{vol}(B_{[1,n-1]})}{\mathrm{vol}(L)} = \frac{\|\mathbf{b}_1^*\|^2 \cdot \mathrm{vol}(B_{[2,n-1]})}{\mathrm{vol}(L)} = \|\mathbf{b}_1^*\| \cdot \|\mathbf{d}_1^*\| = \frac{\|\mathbf{d}_1^*\|}{\|\mathbf{d}_n^*\|}. \tag{2.3}$$

Proof. Since B^{-s} is simply C with its rows in reversed order (*i.e.*, $B^{-s} = R_m C$), it follows that for $i = 1, \ldots, n$, $\mathbf{c}_i = R_m \mathbf{d}_i$ implies $\mathbf{c}_i^* = R_m \mathbf{d}_i^*$ and hence Eq. (2.2) holds.

By Eq. (2.1), we have $\|\mathbf{b}_1^*\| = \frac{1}{\|\mathbf{c}_n^*\|}$. Then Eq. (2.2) implies $\|\mathbf{b}_1^*\| \cdot \|\mathbf{d}_n^*\| = 1$. Similarly, $\|\mathbf{d}_1^*\| \cdot \|\mathbf{b}_n^*\| = 1$. Therefore, $\|\mathbf{b}_1^*\|/\|\mathbf{b}_n^*\| = \|\mathbf{b}_1^*\| \cdot \|\mathbf{d}_1^*\| = \|\mathbf{d}_1^*\|/\|\mathbf{d}_n^*\|$. This proves Eq. (2.3) since the other equalities are trivial. □

Hermite's constant. The *Hermite invariant* of an n-rank lattice L is $\gamma_n(L) = \lambda_1(L)^2/\mathrm{vol}(L)^{2/n}$, where $\lambda_1(L) = \min_{\mathbf{v}\in L\setminus\{\mathbf{0}\}} \|\mathbf{v}\|$ is the first minimum of L. *Hermite's constant* of dimension n is the maximum $\gamma_n = \max \gamma_n(L)$ over all n-rank lattices L. Its exact value is known for $1 \le n \le 8$ and $n = 24$, and we have $\gamma_n \le \frac{n+6}{7}$ for $n \ge 3$ (see [Neu17]).
Bergé-Martinet's constant ([BM89, Def. 2.1]). The *Bergé-Martinet invariant* of an n-rank lattice L is $\gamma'_n(L) = \lambda_1(L)\lambda_1(L^\times)$. *Bergé-Martinet's constant* of dimension n is the maximum $\gamma'_n = \max \gamma'_n(L)$ over all n-rank lattices L.
Korkine-Zolotareff's constant ([BM89, Def. 1.3]). The *Korkine-Zolotareff invariant* of an n-rank lattice L is $\gamma''_n(L) = \max \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_n^*\|}$ over all HKZ-reduced bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L. *Korkine-Zolotareff's constant* of dimension n is the maximum $\gamma''_n = \max \gamma''_n(L)$ over all n-rank lattices L.
Primitive vector. Let L be a lattice with basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. A vector $\mathbf{b} = \sum_{i=1}^n x_i \mathbf{b}_i \in L$ with $x_i \in \mathbb{Z}$ is *primitive* for L iff it can be extended to a basis of L, or equivalently, $\gcd(x_1, \ldots, x_n) = 1$ [Sie89, Th. 32].

2.2 Lattice reduction

Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of a lattice L.
Size reduction and LLL reduction. B is *size-reduced* if $|\mu_{i,j}| \le \frac{1}{2}$ for all $1 \le j < i \le n$. The single vector $\mathbf{b}_i$ is *size-reduced* (w.r.t. B) if $|\mu_{i,j}| \le \frac{1}{2}$ for all $1 \le j < i$. For $\varepsilon \in [0, 3)$, B is *ε-LLL-reduced* [LLL82] if it is size-reduced and every 2-rank projected block $B_{[i,i+1]}$ satisfies Lovász's condition: $\|\mathbf{b}_i^*\|^2 \le (1 + \varepsilon)(\|\mathbf{b}_{i+1}^*\|^2 + \mu_{i+1,i}^2 \|\mathbf{b}_i^*\|^2)$. This implies Siegel's condition: $\|\mathbf{b}_i^*\|^2 \le \frac{4(1+\varepsilon)}{3-\varepsilon}\|\mathbf{b}_{i+1}^*\|^2$. Given as input a basis $B \in \mathbb{Z}^{m\times n}$ and $\varepsilon > 0$, the LLL algorithm [LLL82] outputs an LLL-reduced basis in time polynomial in $(\log \|B\|, m, 1/\varepsilon)$.
SVP reduction and its extensions. B is *SVP-reduced* if $\|\mathbf{b}_1\| = \lambda_1(L)$. Then $\|\mathbf{b}_1\| \le \sqrt{\gamma_n}\mathrm{vol}(B)^{1/n}$.

B is *DSVP-reduced* [GN08] (where D stands for dual) if its reversed dual basis B^{-s} is SVP-reduced.

B is *HKZ-reduced* [Her50, KZ73] if it is size-reduced and $B_{[i,n]}$ is SVP-reduced for $i = 1, \ldots, n$.
Rankin reduction. For $1 \le r \le n$, we will use the notation:

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

The Rankin invariant $\gamma_{n,r}(L) = m_r(L)^2/\mathrm{vol}(L)^{2r/n}$ [Ran53] suggests to define: B is *r-Rankin-reduced* [GHGKN06] if $\mathrm{vol}(B_{[1,r]}) = m_r(L)$. There exist r-Rankin reduced bases for any given lattice. By duality, any n-rank lattice basis is $(n-1)$-Rankin-reduced iff it is DSVP-reduced.

2.3 Basic lemmas

Besides Lemma 2.1, this paper will use the following basic lemmas.

Lemma 2.2 ([LW13, Lemma 3.8])**.** *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an n-rank lattice basis. If the projected block $B_{[i,j]}$ is DSVP-reduced for some indices $1 \le i < j \le n$, then $B_{[k,j]}$ is DSVP-reduced for all $k = i, i+1, \ldots, j-1$.*

Lemma 2.3 ([DM13, Lemma 3.2])**.** *Let B be a r-Rankin-reduced basis of a lattice L. Then $\lambda_1(L(B_{[1,r]})) \le \gamma_r \lambda_1(L)$.*

The dual strategy used in the classical proof of Mordell's inequality (see [Mor44] or [GN08, §3.1]) implies the assertion below:

Lemma 2.4. *If a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of rank $n \geq 2$ 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

$$\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n. \tag{2.4}$$

Proof. Since Case 1 and Case 2 have similar proofs, we only verify Case 2.

Since $B_{[1,n-1]}$ is SVP-reduced, we have $\|\mathbf{b}_1\|^{n-1} \leq \gamma_{n-1}^{(n-1)/2}\mathrm{vol}(B_{[1,n-1]})$. Since B is DSVP-reduced, we have $\mathrm{vol}(B) \leq \gamma_n^{n/2}\|\mathbf{b}_n^*\|^n$ (see [GN08]), or equivalently, $\mathrm{vol}(B_{[1,n-1]}) \leq \gamma_n^{n/2}\|\mathbf{b}_n^*\|^{n-1}$. This implies $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)}$.

Now, it remains to show $\sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n$. To do so, we distinguish two cases:

- For $n = 2, 3$, it can be 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 have $\frac{n+5}{7}\left(\frac{n+6}{7}\right)^{n/(n-1)} < \left(\frac{3}{5}n\right)^2$, because the function $f(n) = 2\log\left(\frac{3}{5}n\right) - \log\frac{n+5}{7} - \log\left(\frac{n+6}{7}\right)^{n/(n-1)}$ increases over $n \geq 4$ by considering its derivative. Then $\gamma_{n-1}\gamma_n^{n/(n-1)} \leq \frac{n+5}{7}\left(\frac{n+6}{7}\right)^{n/(n-1)} < \left(\frac{3}{5}n\right)^2$.

This proved $\sqrt{\gamma_{n-1}}\,\sqrt{\gamma_n}^{n/(n-1)} < \frac{3}{5}n$ for $n \geq 2$. Thus, Eq. (2.4) holds for Case 2. This 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 first recall the definition of HKZ-reduction and its classical property proved in [LLS90]: A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is HKZ-reduced if it is size-reduced and $B_{[i,n]}$ is SVP-reduced for $i = 1, \ldots, n$; then

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

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-rank lattice L such that

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

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

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

Let L be a lattice of rank n. There exists a size-reduced basis $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ of L with GSO $(\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*)$ such that C is SVP-reduced, $C_{[2,n]}$ is DSVP-reduced and $C_{[1,n-1]}$ is HKZ-reduced.[1] 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 $C_{[i,n]}$ is DSVP-reduced (by Lemma 2.2) and $C_{[i,n-1]}$ is SVP-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, the inequality $\|\mathbf{c}_n\|/\|\mathbf{c}_n^*\| < n^{1.5}$ follows from the calculation:

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

[1] We here explain the existence of C. Firstly, let $P = (\mathbf{p}_1, \ldots, \mathbf{p}_n)$ be an arbitrary SVP-reduced basis of L. Secondly, there is a unimodular matrix $U \in \mathbb{Z}^{(n-1)\times(n-1)}$ s.t. $P_{[2,n]}U$ is a DSVP-reduced basis of the projected lattice $L(P_{[2,n]})$. Let $Q = (\mathbf{p}_1, \mathbf{q}_2, \ldots, \mathbf{q}_n) = (\mathbf{p}_1, (\mathbf{p}_2, \ldots, \mathbf{p}_n)U)$ with GSO $(\mathbf{p}_1, \mathbf{q}_2^*, \ldots, \mathbf{q}_n^*)$. Then Q is also an SVP-reduced basis of L s.t. $Q_{[2,n]} = P_{[2,n]}U$ is DSVP-reduced, namely $1/\|\mathbf{q}_n^*\| = \lambda_1(L(Q_{[2,n]})^\times)$. Thirdly, there is a unimodular matrix $V \in \mathbb{Z}^{(n-2)\times(n-2)}$ s.t. $Q_{[2,n-1]}V$ is HKZ-reduced. Let $S = (\mathbf{p}_1, (\mathbf{q}_2, \ldots, \mathbf{q}_{n-1})V, \mathbf{q}_n)$. Then S is an SVP-reduced basis of L satisfying the following properties:

- $S_{[2,n]}$ is DSVP-reduced. Indeed, $L(S_{[2,n]}) = L(Q_{[2,n]})$ and the last Gram-Schmidt vector of S is still $\mathbf{q}_n^*$, so that the DSVP-reducedness $1/\|\mathbf{q}_n^*\| = \lambda_1(L(S_{[2,n]})^\times)$ still holds.
- $S_{[2,n-1]} = Q_{[2,n-1]}V$ is HKZ-reduced, so is $S_{[1,n-1]}$.

Finally, S can be size-reduced into the desired basis.

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

$$\|\mathbf{b}_1\| = \lambda_1(L(C_{[1,n-1]})), \ \ \|\mathbf{b}_1\| \le i\|\mathbf{b}_i^*\| \ \text{ and } \ \|\mathbf{b}_i\| \le i^{1.5}\|\mathbf{b}_i^*\| \ \text{ for } \ i = 1, \ldots, n-1.$$

Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}, \mathbf{c}_n)$. Since $\|\mathbf{b}_1\| = \|\mathbf{c}_1\| = \lambda_1(L)$ and the Gram-Schmidt vector of $\mathbf{c}_n$ in the set B is still $\mathbf{c}_n^*$, it follows that B is a desired basis of L. This proved the existence of a desired basis for any lattice of any rank.

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 totally calling $\frac{n(n-1)}{2}$ SVP-solvers in ranks $\le n$. This completes the proof. □

3.2 Lattice problem and lattice parameters related to Theorem 1.2

Theorem 1.2 can be essentially formulated and resolved 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 an n-rank 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 ratios $\|\mathbf{b}_1\|/\|\mathbf{b}_i^*\|$ do come up in the analysis of many lattice algorithms and are somehow related to their performances. By analogy with SVP, this suggests to formalize a more basic problem of minimizing the single ratio $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ over all bases $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a given n-rank lattice.

Definition 3.1 (Smallest Ratio Problem (SRP))**.** *Given an n-rank 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. We then define the lattice parameters related to SRP.

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

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

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

Both the infimum and supremum are well-defined, because any basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L satisfies $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \ge \sqrt{\gamma_n(L)\gamma_{n,n-1}(L)}$ (by Identity (2.3)) and $\mu_n(L) \le n$ (by Theorem 1.2).

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

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

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

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

where $0 < \epsilon < (4/3)^{1/7} - 1$. It is not hard to deduce that $\lambda_1(L) = \lambda_1(L^\times) = 1, \gamma_3(L) = \left(\frac{4}{3(1+\epsilon)^4}\right)^{1/3}, \gamma'_3(L) = 1$ and $\mu_3(L) = 1 + \epsilon$. We have $\gamma'_3(L) < \mu_3(L) < \gamma_3(L)$.

Example 2. *Consider a 3-rank 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 $\mu_3(L) = 1 + \epsilon < \frac{2}{\sqrt{3}(1+\epsilon)} = \frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_3^*\|} \le \gamma''_3(L)$.

4 The smallest ratio problem and related lattice parameters

In this section, we first prove that SRP is solvable, i.e., the infimum $\mu_n(L)$ is reached at some basis of any given n-rank lattice L. Secondly, we argue that SRP is at least as hard as SVP, including in the approximate sense. Thirdly, we show that the supremum μ_n is reached at some n-rank lattice. Fourthly, we investigate some properties of lattice parameters $\mu_n(L)$ and μ_n: for instance, we prove $\mu_n \le \mu_k^{(n-1)/(k-1)}$ if $k-1$ divides $n-1$, which has an efficient algorithmic version (see Section 5.2).

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

4.1 Solvability 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-rank 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 rank ≥ 2 has infinitely many bases. Our approach is to express $\mu_n(L)$ as the infimum of some finite set so that the infimum can be replaced by minimum.

First, there exists a basis $A = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ of L with GSO $(\mathbf{a}_1^*, \ldots, \mathbf{a}_n^*)$ such that A is DSVP-reduced (or equivalently, $(n-1)$-Rankin-reduced) and $A_{[1,n-1]}$ is SVP-reduced.

Let $\mathcal{S}_1 = \{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L) : \|\mathbf{b}_1\| \leq \|\mathbf{a}_1\|\}$. We have $\|\mathbf{a}_1\| \leq \gamma_{n-1}\lambda_1(L)$ (by Lemma 2.3) and claim that

$$\mu_n(L) = \inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{S}_1\}. \tag{4.1}$$

Indeed, for any $(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L)$ such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \|\mathbf{a}_1\|/\|\mathbf{a}_n^*\|$, we have

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

Then $\{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L) : \|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| \leq \|\mathbf{a}_1\|/\|\mathbf{a}_n^*\|\} \subseteq \mathcal{S}_1 \subseteq \mathcal{B}(L)$ implies Eq. (4.1).

Next, consider the finite set $\mathcal{S}_2 = \{\mathbf{b} \in L : \mathbf{b} \text{ is primitive for } L \text{ such that } \|\mathbf{b}\| \leq \|\mathbf{a}_1\|\} \subseteq \{\mathbf{x} \in L : \|\mathbf{x}\| \leq \gamma_{n-1}\lambda_1(L)\}$. For any $\mathbf{b} \in \mathcal{S}_2$, define the set $\mathcal{B}_\mathbf{b}(L) = \{B \in \mathcal{B}(L) : \mathbf{b} \text{ is the first column of } B\}$. Then $\mathcal{S}_1$ can be expressed as a union of finitely many subsets:

$$\mathcal{S}_1 = \bigcup_{\mathbf{b} \in \mathcal{S}_2} \mathcal{B}_\mathbf{b}(L). \tag{4.2}$$

For each $\mathbf{b} \in \mathcal{S}_2$, there is a basis $C = (\mathbf{b}, \mathbf{c}_2, \ldots, \mathbf{c}_n) \in \mathcal{B}_\mathbf{b}(L)$ with GSO $(\mathbf{b}, \mathbf{c}_2^*, \ldots, \mathbf{c}_n^*)$ such that $C_{[2,n]}$ is DSVP-reduced. Consider the $(n-1)$-rank projected lattice $\pi_\mathbf{b}(L)$, where $\pi_\mathbf{b}$ denotes the projection over $\mathrm{span}(\mathbf{b})^\perp$. Since

$$\frac{\|\mathbf{b}\|}{\|\mathbf{c}_n^*\|} = \frac{\|\mathbf{b}\|^2 \cdot m_{n-2}(\pi_\mathbf{b}(L))}{\mathrm{vol}(L)} \triangleq \sigma(\mathbf{b}),$$

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 Eq. (4.1) and Eq. (4.2), this implies

$$\mu_n(L) = \inf_{\mathbf{b} \in \mathcal{S}_2} \left(\inf\{\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| : (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}_\mathbf{b}(L)\}\right) = \inf\{\sigma(\mathbf{b}) : \mathbf{b} \in \mathcal{S}_2\}.$$

Thus, we obtain $\mu_n(L)$ as the minimum of a finite set: $\mu_n(L) = \min\{\sigma(\mathbf{b}) : \mathbf{b} \in \mathcal{S}_2\}$. That is, $\mu_n(L) = \sigma(\mathbf{b})$ for some $\mathbf{b} \in \mathcal{S}_2$. 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. □

In summary, this algorithmic proof implies the following identity, which can be turned into an enumeration-based algorithm for solving SRP exactly (see Section 5.1):

$$\mu_n(L) = \min\left\{\|\mathbf{b}_1^*\|/\|\mathbf{b}_n^*\| : B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathcal{B}(L), \|\mathbf{b}_1\| \leq \|\mathbf{a}_1\| \text{ and } B_{[2,n]} \text{ is DSVP-reduced}\right\}. \tag{4.3}$$

Geometrically, SRP or $\mu_n(L)$ can also be defined using orthogonality and duality:[2]

Proposition 4.2. *Let L be a lattice of rank n. Then*

$$\mu_n(L) = \min\left\{\|\mathbf{v}\| \cdot \|\mathbf{w}\| : \mathbf{v} \in L\backslash\{\mathbf{0}\} \textit{ is orthogonal to } \mathbf{w} \in L^\times\backslash\{\mathbf{0}\}\right\}.$$

Proof. For any primitive vector $\mathbf{v} \in L$ and any primitive vector $\mathbf{w} \in L^\times$ such that $\langle \mathbf{v}, \mathbf{w} \rangle = 0$, we claim that

$$\|\mathbf{v}\| \cdot \|\mathbf{w}\| \geq \mu_n(L).$$

Indeed, $\mathbf{w}$ can be extended into a basis $(\mathbf{w}, \mathbf{w}_{n-1}, \ldots, \mathbf{w}_1)$ of $L^\times$. Let $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ be the dual basis of $(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}, \mathbf{w})$. Then $\mathbf{v} \in L \cap \mathrm{span}(\mathbf{w})^\perp = L(\mathbf{a}_1, \ldots, \mathbf{a}_{n-1})$ and hence $\mathbf{v}$ can be extended into a basis $(\mathbf{v}, \mathbf{v}_2, \ldots, \mathbf{v}_{n-1})$ of $L(\mathbf{a}_1, \ldots, \mathbf{a}_{n-1})$. Thus, $(\mathbf{v}, \mathbf{v}_2, \ldots, \mathbf{v}_{n-1}, \mathbf{a}_n)$ is a basis of L: its GSO $(\mathbf{v}, \mathbf{v}_2^*, \ldots, \mathbf{v}_{n-1}^*, \mathbf{a}_n^*)$ satisfies $\mathbf{a}_n^* = \frac{\mathbf{w}}{\|\mathbf{w}\|^2}$ (by Eq. (2.1)), which implies $\|\mathbf{v}\| \cdot \|\mathbf{w}\| = \|\mathbf{v}\|/\|\mathbf{a}_n^*\| \geq \mu_n(L)$.

Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of L satisfying $\mu_n(L) = \|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ and with dual basis $(\mathbf{c}_n, \ldots, \mathbf{c}_1)$. By Eq. (2.1), we have $\mathbf{b}_n^* = \frac{\mathbf{c}_1}{\|\mathbf{c}_1\|^2}$. Then $\mu_n(L) = \|\mathbf{b}_1\| \cdot \|\mathbf{c}_1\|$ and $\langle \mathbf{b}_1, \mathbf{b}_n^* \rangle = 0$ ensures $\langle \mathbf{b}_1, \mathbf{c}_1 \rangle = 0$. The proposition follows. □

[2] This observation came from an anonymous reviewer for previous submission of this paper.

If one leaves aside the orthogonality requirement, the problem is equivalent to two independent SVP computations (on the primal lattice and its dual lattice, respectively), and the optimal value $\mu_n(L)$ becomes the Bergé-Martinet invariant $\gamma'_n(L)$. Thus, $\gamma'_n(L) = \lambda_1(L)\lambda_1(L^\times) \le \mu_n(L)$ for any lattice L of rank n.

This intuitively suggests that SRP is an NP-hard lattice problem related to SVP, as shown in the next subsection.

Theorem 4.1 allows us to define SRP-reduced bases, which will be convenient in what follows.

Definition 4.3 (SRP-reduction)**.** *A basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice L is* SRP-reduced *if $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| = \mu_n(L)$.*

With the existence of SRP-reduced bases, we can solve a weaker version of DRS/Seysen's open problem:

Corollary 4.4. *For any n-rank lattice L, there exists a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that $\max_{1\le i\le n/2} \frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{n-i+1}^*\|} \le n$.*

Proof. First, there exists an SRP-reduced basis $B^{(1)} = (\mathbf{b}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{n-1}, \mathbf{b}_n)$ of L. Next, there exists a unimodular matrix $U \in \mathbb{Z}^{(n-2)\times(n-2)}$ such that $B^{(1)}_{[2,n-1]}U$ is an SRP-reduced basis of the projected lattice $L(B^{(1)}_{[2,n-1]})$. Let $B^{(2)} = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{q}_3, \ldots, \mathbf{q}_{n-2}, \mathbf{b}_{n-1}, \mathbf{b}_n) := (\mathbf{b}_1, (\mathbf{p}_2, \ldots, \mathbf{p}_{n-1})U, \mathbf{b}_n)$. Since the last Gram-Schmidt vectors of both $B^{(1)}$ and $B^{(2)}$ are the same, $B^{(2)}$ is still an SRP-reduced basis of L. Further, $B^{(2)}_{[2,n-1]} = B^{(1)}_{[2,n-1]}U$ is also SRP-reduced.

By recursively using the existence of SRP-reduced bases for (projected) lattices of rank k over $k = n, n-2, n-4, \ldots$, we eventually find a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L with GSO $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ such that $B_{[i,n-i+1]}$ is SRP-reduced and hence $\frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{n-i+1}^*\|} = \mu_{n-2i+2}(L(B_{[i,n-i+1]})) \le n - 2i + 2$ over $i = 1, 2, \ldots, \lfloor n/2 \rfloor$. Then $\max_{1\le i\le n/2} \frac{\|\mathbf{b}_i^*\|}{\|\mathbf{b}_{n-i+1}^*\|} \le n$, as desired. □

4.2 Hardness of SRP

We first recall the search variant and the promise variant of the well-known SVP-approximation problem ($\gamma \ge 1$):

- The search problem SVP_γ: Given a basis of a lattice L, find a nonzero vector $\mathbf{v} \in L$ such that $\|\mathbf{v}\| \le \gamma \cdot \lambda_1(L)$.
- The promise problem GapSVP_γ: Given a basis of a lattice L and a parameter $d > 0$, distinguish between a YES instance where $\lambda_1(L) \le d$ and a NO instance where $\lambda_1(L) > \gamma \cdot d$.

Similarly, Th. 4.1 allows us to define the SRP-approximation problem as follows:

Definition 4.5. *Let L be an n-rank lattice endowed with the Euclidean norm and $\gamma \ge 1$ be an approximation factor.*

- *The search problem SRP_γ: Given a basis of L, find a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that $\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_n^*\|} \le \gamma \cdot \mu_n(L)$.*
- *The promise problem GapSRP_γ: Given a basis of L and a parameter $d > 0$, distinguish between a YES instance where $\mu_n(L) \le d$ and a NO instance where $\mu_n(L) > \gamma \cdot d$.*

The hardness argument of $(\mathrm{Gap})\mathrm{SRP}_\gamma$ relies on the following sufficient condition for being SRP-reduced:

Claim 4.6 (Sufficient Condition)**.** *Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of an n-rank lattice L. If B is both SVP-reduced and DSVP-reduced, then B is SRP-reduced. Conversely, it may not be true.*

Proof. Let $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n)$ be an SRP-reduced basis of L. Since B is SVP-reduced and DSVP-reduced (or equivalently, $(n-1)$-Rankin-reduced), we have $\|\mathbf{b}_1\| \le \|\mathbf{c}_1\|$ and $\mathrm{vol}(B_{[1,n-1]}) \le \mathrm{vol}(C_{[1,n-1]})$. Thus, Identity (2.3) implies

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

Then $\frac{\|\mathbf{b}_1\|}{\|\mathbf{b}_n^*\|} = \mu_n(L)$. This proves the first assertion.

The second assertion follows from Example 1: the basis B in Example 1 is SRP-reduced and not SVP-reduced. This completes the proof of the claim. □

$(\mathrm{Gap})\mathrm{SRP}_\gamma$ on lattices of rank n is at least as hard as $(\mathrm{Gap})\mathrm{SVP}_\gamma$ on lattices of rank $(n-1)$:

Theorem 4.7. *Let $\gamma \ge 1$ be an arbitrary approximation factor.*

1. *There is a deterministic polynomial time Cook-reduction from SVP_γ on any lattice of rank $(n-1)$ to SRP_γ on a lattice of rank n.*
2. *There is a deterministic polynomial time Karp-reduction from GapSVP_γ on any lattice of rank $(n-1)$ to GapSRP_γ on a lattice of rank n.*

Proof. Let L be an $(n-1)$-rank lattice with basis B. We define an n-rank lattice Λ with basis $\mathrm{Diag}(B, t) := \begin{pmatrix} B & \\ & t \end{pmatrix}$, where t is an arbitrary rational number satisfying $t > \gamma \cdot \|B\|$.

We first show $\mu_n(\Lambda) = \lambda_1(L)\lambda_1(\Lambda^\times)$. Let $C = (\mathbf{c}_1, \ldots, \mathbf{c}_{n-1})$ be an SVP-reduced basis of L. Then $D = \mathrm{Diag}(C, t)$ is also a basis of Λ with the following properties:

- D is SVP-reduced. Indeed, since $\|\mathbf{c}_1\| = \lambda_1(L) \le \|B\| < t$, we have

$$\|\mathbf{c}_1\| \le \left\| \begin{pmatrix} B\mathbf{w} \\ tx \end{pmatrix} \right\| = \left\| \mathrm{Diag}(B, t) \begin{pmatrix} \mathbf{w} \\ x \end{pmatrix} \right\|$$

  for any non-zero integer vector $\begin{pmatrix} \mathbf{w} \\ x \end{pmatrix} \in \mathbb{Z}^n$ where $\mathbf{w} \in \mathbb{Z}^{n-1}$ and $x \in \mathbb{Z}$. Then $\|\mathbf{c}_1\| = \lambda_1(\Lambda)$ implies the SVP-reducedness of D.

- D is DSVP-reduced. Indeed, it can be checked by the definition that $D^{-s} = \mathrm{Diag}(t^{-1}, C^{-s})$. Using the transference theorem $\lambda_1(L^\times)\lambda_{n-1}(L) \ge 1$ [Ban93] and the fact $\lambda_{n-1}(L) \le \|B\| < t$, we have $t^{-1} < \lambda_{n-1}(L)^{-1} \le \lambda_1(L^\times)$. Since $L(C^{-s})$ is isometric to $L^\times$, we have $\lambda_1(L^\times) = \lambda_1(L(C^{-s}))$. Then $t^{-1} < \lambda_1(L(C^{-s}))$ implies

$$t^{-1} \le \left\| \begin{pmatrix} t^{-1}y \\ C^{-s}\mathbf{z} \end{pmatrix} \right\| = \left\| D^{-s} \begin{pmatrix} y \\ \mathbf{z} \end{pmatrix} \right\|$$

  for any non-zero integer vector $\begin{pmatrix} y \\ \mathbf{z} \end{pmatrix} \in \mathbb{Z}^n$ where $y \in \mathbb{Z}$ and $\mathbf{z} \in \mathbb{Z}^{n-1}$. Thus, $t^{-1} = \lambda_1(L(D^{-s})) = \lambda_1(\Lambda^\times)$ and hence D^{-s} is SVP-reduced. This implies the DSVP-reducedness of D.

By Claim 4.6, D is an SRP-reduced basis of Λ such that $\mu_n(\Lambda) = \frac{\|\mathbf{c}_1\|}{t} = \lambda_1(L)\lambda_1(\Lambda^\times)$, as desired.

We show Item 1. One calls the SRP_γ oracle on the input instance $\mathrm{Diag}(B, t)$ to find a basis $G = (\mathbf{g}_1, \ldots, \mathbf{g}_n)$ of Λ s.t. its GSO satisfies $\frac{\|\mathbf{g}_1\|}{\|\mathbf{g}_n^*\|} \le \gamma \cdot \mu_n(\Lambda)$. Then $\mathbf{g}_1 = \begin{pmatrix} \mathbf{v} \\ t\xi \end{pmatrix}$ for some vector $\mathbf{v}$ in L and some integer ξ satisfying $\|\mathbf{v}\| + |\xi| \ne 0$.

We claim that $\mathbf{v}$ is a solution to SVP_γ on L, namely $\mathbf{v} \in L$ with $0 < \|\mathbf{v}\| \le \gamma \cdot \lambda_1(L)$. Indeed, by Eq. (2.1), the dual basis $(\mathbf{h}_1, \ldots, \mathbf{h}_n)$ of G satisfies $\frac{1}{\|\mathbf{g}_n^*\|} = \|\mathbf{h}_n\| \ge \lambda_1(\Lambda^\times)$. Then $\frac{\|\mathbf{g}_1\|}{\|\mathbf{g}_n^*\|} \le \gamma \cdot \mu_n(\Lambda) = \gamma \cdot \lambda_1(L)\lambda_1(\Lambda^\times)$ implies:

$$0 < \|\mathbf{g}_1\| = \sqrt{\|\mathbf{v}\|^2 + \xi^2 t^2} \le \gamma \cdot \lambda_1(L) \le \gamma \cdot \|B\| < t.$$

It follows that $\xi = 0$ and $0 < \|\mathbf{v}\| \le \gamma \cdot \lambda_1(L)$, as desired. This proves Item 1.

It remains to show Item 2. Given as input a GapSVP_γ instance (B, d) with parameter $d > 0$, the output of the reduction is the tuple $\left(\mathrm{Diag}(B, t), \frac{d}{t}\right)$:

- If (B, d) is a YES GapSVP_γ instance, then $\lambda_1(L) \le d$. Since $\mu_n(\Lambda) = \frac{\lambda_1(L)}{t}$, this implies $\mu_n(\Lambda) \le \frac{d}{t}$. Thus, $\left(\mathrm{Diag}(B, t), \frac{d}{t}\right)$ is a YES GapSRP_γ instance.
- If (B, d) is a NO GapSVP_γ instance, then $\lambda_1(L) > \gamma \cdot d$. Since $\mu_n(\Lambda) = \frac{\lambda_1(L)}{t}$, this implies $\mu_n(\Lambda) > \gamma \cdot \frac{d}{t}$. Thus, $\left(\mathrm{Diag}(B, t), \frac{d}{t}\right)$ is a NO GapSRP_γ instance.

This proves Item 2 and completes the proof of Th. 4.7. □

Combining with the best known hardness result for $(\mathrm{Gap})\mathrm{SVP}_\gamma$ [HR12, Th. 1.1] (building on work of [Ajt98, CN98, Mic00, Kho05]), Th. 4.7 immediately implies the following hardness result for $(\mathrm{Gap})\mathrm{SRP}_\gamma$:

Corollary 4.8. *1. For any constant $\gamma \ge 1$, both SRP_γ and GapSRP_γ are NP-hard under randomized polynomial-time reductions. I.e., there is no randomized polynomial-time algorithm for $(\mathrm{Gap})\mathrm{SRP}_\gamma$ unless NP $\subseteq$ RP.*

2. For $1 \le \gamma \le 2^{(\log n)^{1-\varepsilon}}$ with any constant $\varepsilon > 0$, both SRP_γ and GapSRP_γ on n-rank lattices are NP-hard under randomized quasipolynomial-time reductions. I.e., there is no randomized polynomial-time algorithm for $(\mathrm{Gap})\mathrm{SRP}_\gamma$ unless NP $\subseteq$ RTIME$(2^{\mathrm{poly}(\log n)})$.

3. For $1 \le \gamma \le n^{c/\log\log n}$ with some universal constant $c > 0$, both SRP_γ and GapSRP_γ on n-rank lattices are NP-hard under randomized subexponential-time reductions. I.e., there is no randomized polynomial-time algorithm for $(\mathrm{Gap})\mathrm{SRP}_\gamma$ unless NP $\subseteq$ RSUBEXP $:= \bigcap_{\delta>0}$ RTIME(2^{n^δ}).

4.3 Reachability of μ_n

Our main result of this subsection is as follows, which implies $\mu_n = \max \mu_n(L)$ over all n-rank lattices L.

Theorem 4.9. *There exists an n-rank lattice L such that $\mu_n = \mu_n(L)$.*

Our proof of Theorem 4.9 uses Lemmas 4.10 and 4.11 below.

Lemma 4.10. *Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an n-rank lattice basis such that $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\| \le \cdots \le \|\mathbf{b}_n\|$ and $1 \le \|\mathbf{b}_1\| \cdot \prod_{i=1}^{n-1} \|\mathbf{b}_i\| \le \prod_{i=1}^{n} \|\mathbf{b}_i\| \le (n!)^2$. Then $1/(n!)^{2n} \le \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \le (n!)^4$.*

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

Lemma 4.11. *Let* $\mathcal{S} = \left\{B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times n} : 1/(n!)^{2n} \le \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \le (n!)^4 \text{ and } \det(B) = 1\right\}$ *and* $f(B) = \mu_n(L(B))$ *for every* $B \in \mathcal{S}$. *Then* f *is continuous on the bounded closed set* $\mathcal{S}$.

Proof. We first show compactness of $\mathcal{S}$. Let $\mathcal{S}_1 = \left\{(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times n} : 1/(n!)^{2n} \le \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \le (n!)^4\right\}$ 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.

We next show continuity of f. For each $B \in \mathcal{S}$, since $\mathrm{vol}(L(B)) = \det(B) = 1$, Theorem 4.1 and Lemma 2.1 imply

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

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

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

For $\forall\ \varepsilon > 0$, since $g(B) := \|B\mathbf{u}_1\| \cdot \mathrm{vol}(B(U_{[1,n-1]}))$ is continuous at B, there exists $\delta > 0$ such that $|g(C) - g(B)| < \varepsilon$ if $\|C - B\|_F < \delta$, where $\|\cdot\|_F$ denotes the Frobenius norm. 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 $\mathcal{S}$. This completes the proof. □

We now show Theorem 4.9 as follows:

Proof of Theorem 4.9. Recall that $\mu_n = \sup \mu_n(L)$ over all n-rank lattices L. Our approach is to express μ_n as the supremum of a continuous mapping on some bounded closed set, so that the extreme value theorem in calculus implies the conclusion.

Define the set $\mathcal{L}_n = \{L \subset \mathbb{R}^n : L \text{ is a lattice of rank } n \text{ such that } \mathrm{vol}(L) = 1 \text{ and } \mu_n(L) \ge 1\}$. It is classical that any n-rank lattice in $\mathbb{R}^m$ is isometric to some n-rank lattice in $\mathbb{R}^n$ (see, *e.g.*, [BP87, p. 57]) and two isometric lattices have the same value on $\mu_n(\cdot)$. Together with homogeneity and $\mu_n(\mathbb{Z}^n) = 1$, we have

$$\mu_n = \sup\{\mu_n(L) : L \in \mathcal{L}_n\}. \tag{4.4}$$

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

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

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

By Lemma 4.10, $C \in \mathcal{S} \triangleq \left\{B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n\times n} : 1/(n!)^{2n} \le \|\mathbf{b}_1\|, \ldots, \|\mathbf{b}_n\| \le (n!)^4 \text{ and } \det(B) = 1\right\}$. Thus, $L = L(C) \in \{L(B) : B \in \mathcal{S}\}$ and hence $\mathcal{L}_n \subseteq \{L(B) : B \in \mathcal{S}\}$. Combining with Eq. (4.4), this implies

$$\mu_n = \sup\{\mu_n(L(B)) : B \in \mathcal{S}\} \tag{4.5}$$

By Lemma 4.11, the mapping $B \mapsto \mu_n(L(B))$ is continuous on the bounded closed set $\mathcal{S}$. By the extreme value theorem in calculus, there exists a basis $B_0 \in \mathcal{S}$ such that $\mu_n(L(B)) \le \mu_n(L(B_0))$ for $\forall\ B \in \mathcal{S}$. By Eq. (4.5), this implies $\mu_n = \mu_n(L(B_0))$ and the conclusion follows. □

4.4 Properties of $\mu_n(L)$ and μ_n

In this subsection, we investigate some elementary properties of lattice parameters $\mu_n(L)$ and μ_n including relations with other classical lattice parameters. The characterization in Proposition 4.2 and bounds in Proposition 4.12 and Theorem 4.13 show that it is natural for $\mu_n(L)$ and μ_n to arise.

Proposition 4.12. *Let* L *be an* n*-rank lattice.*

1. $\mu_n(L) = \mu_n(L^\times)$.
2. $\gamma_n'(L) \le \mu_n(L) \le \gamma_n''(L)$.
3. $\mu_n(L) = \mu_n(\rho \cdot L)$ *for any real* $\rho \ne 0$.

Proof. By Identity (2.3) and the definitions of $\mu_n(L), \gamma'_n(L)$ and $\gamma''_n(L)$, the proof is trivial. □

The new constant μ_n has close relations with classical Hermite's constant γ_n, Bergé-Martinet's constant γ'_n and Korkine-Zolotareff's constant γ''_n, as shown below.

Theorem 4.13. *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. $\gamma'_n \leq \mu_n \leq \frac{4}{\sqrt{3}}\left(\gamma'_n + \frac{1}{2}\right)$;
5. $\frac{3}{8}\mu_{n+1} - \frac{1}{2} \leq \mu_n \leq \frac{8}{3}\left(\mu_{n+1} + \frac{1}{2}\right)$;
6. *μ_n has the 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 4.12.2 and Eq. (2.4) imply Items 1 and 2, respectively.

Since $\gamma_n \leq (\sqrt{4/3})^{n-1} = \gamma_2^{n-1}$ [Her50] and $\gamma_{n-1} \leq \gamma_n^{n/(n-1)}$ [New63], Item 2 implies

$$\mu_n \leq \sqrt{\gamma_{n-1}}\sqrt{\gamma_n}^{n/(n-1)} \leq \gamma_n^{n/(n-1)} \leq \sqrt{\frac{4}{3}}\gamma_n. \tag{4.6}$$

Let ω_n denote the volume of the n-dimensional unit Euclidean ball and $\vartheta(n)$ be the closest integer to $\left(\frac{5}{3}\omega_n^{-1}\right)^{2/n}$. Then $\vartheta(n) = \frac{n}{2\pi e} + \frac{\log(\pi n)}{2\pi e} + o(1)$ [MH73, p. 31]. By Conway-Thomson's Theorem (see [MH73, Th. 9.5]), there is an n-rank 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 $\vartheta(n) \geq \left(\frac{5}{3}\omega_n^{-1}\right)^{2/n} - \frac{1}{2}$ and $2\omega_n^{-2/n} \geq \gamma_n$ [Bli14], we have

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

Together with Eq. (4.6), these inequalities imply Items 3 and 4.

Applying the inequalities $\gamma_n \leq \gamma_{n+1}^{(n+1)/n}$ and $\gamma_n \leq \gamma_2^{n-1}$ again, together with Mordell's inequality $\gamma_{n+1} \leq \gamma_n^{n/(n-1)}$ [Mor44], Item 5 follows from the calculations below:

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

Since $\gamma_n \leq \frac{1.744n}{2\pi e} + o(n)$ [KL78] and $\gamma_n^{1/(n-1)} = 1 + o(1)$, the inequalities $\vartheta(n) \leq \mu_n \leq \gamma_n^{n/(n-1)}$ implies Item 6. This completes the proof. □

We mention in passing that Schnorr [Sch87] used the notation α_k for Korkine-Zolotareff's constant γ''_k to assess the quality of BKZ-reduced bases with blocksize k: it is known that $\gamma''_k = k^{\frac{\ln k}{2} + O(1)} \leq k^{\frac{\ln k}{2} + \frac{1}{2}}$ for any $k \geq 2$ [HS08, LLS90]; our Theorem 4.13 suggests that the term $O(1)$ should be great than $\log_k \mu_k - \frac{\ln k}{2}$ (*e.g.*, we have $\log_k \mu_k - \frac{\ln k}{2} \in (-2.51, -1.85)$ for feasible blocksize $k = 150$ [SG]).

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

Theorem 4.14. *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 rank $n = (p+1)(k-1)+1$ 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 an SRP-reduced basis of the sublattice $L(B_{[1,m]})$ with GSO $(\mathbf{c}_1^*, \ldots, \mathbf{c}_m^*)$. Then $C = (\mathbf{c}_1, \ldots, \mathbf{c}_m, \mathbf{b}_{m+1}, \ldots, \mathbf{b}_n)$ is a basis of L such that

$$\frac{\|\mathbf{c}_1\| \cdot \mathrm{vol}(C_{[1,m-1]})}{\mathrm{vol}(C_{[1,m]})} = \mu_m(L(B_{[1,m]})) \leq \mu_m. \tag{4.7}$$

Since $k = n - m + 1$, there is a $k \times k$ unimodular matrix U such that $C_{[m,n]}U$ is an SRP-reduced basis of the projected lattice $L(C_{[m,n]})$. 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 GSO

$(\mathbf{c}_1^*, \ldots, \mathbf{c}_{m-1}^*, \mathbf{d}_m^*, \ldots, \mathbf{d}_n^*)$. 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,

$$\frac{\|\mathbf{d}_m^*\| \cdot \mathrm{vol}(D_{[m,n-1]})}{\mathrm{vol}(C_{[m,n]})} = \mu_k(L(C_{[m,n]})) \le \mu_k. \tag{4.8}$$

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

As a result, it follows from Eq. (4.7) and Eq. (4.8) that

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

Then the inductive hypothesis $\mu_m \le \mu_k^p$ implies $\mu_n(L) \le \mu_k^{p+1}$. By the arbitrariness of L, this implies $\mu_n \le \mu_k^{p+1}$. Thus, we proved $\mu_{p(k-1)+1} \le \mu_k^p$ by induction over $p \ge 1$. This completes the proof. □

Theorem 4.15 below implies $\mu_4 > \mu_3^{3/2}$: hence, $\mu_n \le \mu_k^{(n-1)/(k-1)}$ does not always hold for $n \ge k \ge 2$.

Similarly to 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 4.15. $\mu_2 = \frac{2}{\sqrt{3}}$, $\mu_3 = \sqrt{\frac{3}{2}}$, $\mu_4 = \sqrt{2}$, $\sqrt{2} \le \mu_5 < \frac{3}{2}$, $\sqrt{\frac{8}{3}} \le \mu_6 \le \frac{2^{9/10}}{3^{1/10}}$, $\sqrt{3} \le \mu_7 \le \frac{2}{3^{1/12}}$ *and* $\mu_8 = 2$.

Proof. By [BM89, Prop. 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 4.13.1. Since the exact values of γ_n and γ'_n are known for $1 \le n \le 8$ (see [BM89, SWO10]), together with $\gamma''_5 < \frac{3}{2}$ [KZ73], the inequalities $\gamma'_n \le \mu_n \le \min\{\gamma''_n, \sqrt{\gamma_{n-1}}\sqrt{\gamma_n}^{n/(n-1)}\}$ imply the remainder assertions. □

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

5 Algorithms for the smallest ratio problem

We present an exact algorithm and an approximation algorithm for SRP in Sections 5.1 and 5.2 respectively.

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

Our main result on the SRP-approximation algorithm is the following: given as input a basis of an n-rank integer lattice L, a blocksize k such that $k-1$ divides $n-1$, a reduction factor $\varepsilon > 0$, and an SRP-subroutine computing SRP-reduced bases for any lattice of rank k, the algorithm outputs a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L such that

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

and has running time upper bounded by a polynomial factor in the input size times the cost of the SRP-subroutine.

All the proofs of this section are relegated to Appendix D.

5.1 An exact SRP algorithm

Our exact SRP algorithm is Alg. 1, which is a deterministic enumeration-based algorithm for computing an SRP-reduced basis of a given integer lattice. The main idea stems from the algorithmic proof of Theorem 4.1, more precisely, is based on Identity (4.3): if $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is an SRP-reduced basis of an integer lattice L, then $\|\mathbf{b}_1\| \le R$ for some computable radius $R \in [\lambda_1(L), \gamma_{n-1}\lambda_1(L)]$ and $B_{[2,n]}$ is DSVP-reduced. One can simply enumerate all primitive vectors $\mathbf{b} \in \{\mathbf{x} \in L : \|\mathbf{x}\| \le R\}$ and then extend every $\mathbf{b}$ into a basis C of L such that $C_{[2,n]}$ is DSVP-reduced: by comparing all their quantities $\|\mathbf{b}\| \cdot \mathrm{vol}(C_{[1,n-1]})$, one extracts an SRP-reduced basis of L.

Alg. 1 uses three local algorithms, two out of which are related to SVP:

- An enumeration algorithm (see, *e.g.*, [HS07, Fig.1]) which, given a basis of an n-rank integer lattice L in $\mathbb{Z}^m$ and a radius $R \in \mathbb{R}^+$, outputs all vectors in the set $\{\mathbf{x} \in L : \|\mathbf{x}\| \le R\}$. In particular, Kannan's SVP enumeration algorithm [Kan87] finds a shortest nonzero vector for L within $\mathrm{poly}(\log \|B_{\mathrm{input}}\|, m) \cdot n^{\frac{n}{2e}} 2^{O(n)}$ bit operations and polynomial space [HS07].

- A DSVP-algorithm (see [GN08, Alg. 3][3]), which performs a DSVP-reduction of a given block. Given as input a basis $B \in \mathbb{Z}^{m\times n}$ and an index $i \in [1, n-1]_{\mathbb{Z}}$ such that $B_{[i,n]}$ is LLL-reduced, the algorithm (dominated by an SVP computation in rank $n-i+1$) outputs a basis C of $L(B)$ such that $C_{[1,i-1]} = B_{[1,i-1]}$, $C_{[i,n]}$ is DSVP-reduced and $\|C\| \leq 2^{O(n^2)} \times \|B\|$.
- A basis extension algorithm, which extends a primitive vector for a lattice L into a basis of L. Given as input $(\mathbf{b}, B)$ where $\mathbf{b}$ is a primitive vector for L with basis $B \in \mathbb{Z}^{m\times n}$, the Li-Nguyen XGCD-based basis algorithm [LN19, Alg. 7] outputs a basis C of L in $O(mn^4 \log^2 \beta)$ bit operations (without fast integer arithmetic) such that $\mathbf{b}$ is the first column of C, $\|C^*\| \leq \beta$ and $\|C\| \leq \sqrt{n} \times \beta$, where $\beta = \max\{\|\mathbf{b}\|, \|B\|\}$.

In order to avoid "intermediate entries explosion", Alg. 1 performs LLL-reductions at Step 11 and Step 16. In fact, if LLL-reducing a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, then both $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\|$ and $\max_{1\leq i\leq n} \|\mathbf{b}_i^*\|$ can never increase. Therefore, there exists a basis for any lattice which is both LLL-reduced and SRP-reduced.

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

Input: A $\frac{1}{3}$-LLL-reduced basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an integer lattice L.
Output: An SRP-reduced basis of L and the corresponding unimodular transformation.

1: Store $B_0 \leftarrow B$
2: DSVP-reduce B using [GN08, Alg. 3] and then HKZ-reduce $B_{[1,n-1]}$
3: Size-reduce $\mathbf{b}_n$ w.r.t. B and store $A = (\mathbf{a}_1, \ldots, \mathbf{a}_n) \leftarrow B$
4: **if** $\|\mathbf{a}_1\| = \lambda_1(L)$ **then**
5: Go to Step 18 //The current basis B is already SRP-reduced (by Claim 4.6) and $\frac{1}{3}$-LLL-reduced.
6: **else**
7: **for** each $\mathbf{b} \in \mathcal{S} \triangleq \{\mathbf{x} \in L : \|\mathbf{x}\| \leq \|\mathbf{a}_1\|\}$ **do**
8: //In order to reduce memory space, one extracts every element from $\mathcal{S}$ (for Steps 9-14) one by one via running the enumeration algorithm [HS07, Fig.1] on the strongly reduced basis A
9: **if** $\mathbf{b}$ is primitive for L **then**
10: Extend $\mathbf{b}$ into a basis C of L by calling the XGCD-based basis algorithm on $(\mathbf{b}, B_0)$
11: $\frac{1}{3}$-LLL-reduce $C_{[2,n]}$ and then size-reduce C
12: DSVP-reduce $C_{[2,n]}$ using [GN08, Alg. 3]
13: **if** $\|\mathbf{b}\| \cdot \mathrm{vol}(C_{[1,n-1]}) < \|\mathbf{b}_1\| \cdot \mathrm{vol}(B_{[1,n-1]})$ **then** $B \leftarrow C$
14: **end if**
15: **end for**
16: $\frac{1}{3}$-LLL-reduce B
17: **end if**
18: Compute the unimodular transformation U such that $B = B_0 U$
19: **return** B and U

Our main result on Alg. 1 is the following:

Theorem 5.1. *Given as input a $\frac{1}{3}$-LLL-reduced basis B_0 of an n-rank lattice $L \subseteq \mathbb{Z}^m$, Alg. 1 outputs an SRP-reduced basis B of L and an $n \times n$ unimodular matrix U such that*

$$B = B_0 U, \quad \|B\| \leq 2^{(n-1)/2} \times \|B_0\| \quad \text{and} \quad \|U\|_\infty \leq 2^{(n-1)/2} \times \|B_0\|^n.$$

Moreover, if Alg. 1 performs its (D)SVP computations at Step 2, Step 4 and each Step 12 using Kannan's SVP enumeration algorithm, then it requires poly$(\log \|B_0\|, m) \cdot n^{\frac{n}{e}} 2^{O(n)}$ bit operations and polynomial space.

We mention that if Alg. 1 performs its (D)SVP computations using the Micciancio-Voulgaris SVP algorithm [MV10] (instead of Kannan's SVP enumeration algorithm), then it requires poly$(\log \|B_0\|, m) \cdot n^{\frac{n}{2e}} 2^{O(n)}$ bit operations and poly$(\log \|B_0\|, m) \cdot 2^n$ space.

Alg. 1 is unavoidably expensive because of the NP-hardness of SRP. Naturally, 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 rank. By analogy, the exact SRP algorithm suggests finding an approximation algorithm for SRP using an exact algorithm in low rank.

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. Forcing the output to be LLL-reduced allows us to bound the coefficients of U (see Cor. C.2). Obviously, Alg. 1 is an SRP-oracle.

[3] [GN08, Alg. 3] performs a DSVP-reduction up to a relaxation factor of $(1+\varepsilon)$ for any $\varepsilon \geq 0$. By setting $\varepsilon = 0$, [GN08, Alg. 3] actually does an exact DSVP-reduction.

In what follows, we first introduce a new reduction notion called block-ratio reduction. Then we present a deterministic polynomial-time reduction algorithm to compute block-ratio reduced bases. The algorithm approximates SRP in rank n within a factor essentially $\mu_k^{(n-1)/(k-1)}$, using polynomially many calls to an SRP-oracle in rank k, provided that $k-1$ divides $n-1$. Hence, block-ratio reduction can be viewed as an algorithmic version of Theorem 4.14.

5.2.1 Definition and properties

We will use a natural relaxation of SRP-reduction: a basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of an n-rank 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-rank lattice L where $n = p(k-1)+1$ with $p \geq 1$ is* (ε, k)-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 [GN08, MW16, ALNS20]):

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

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

This approximation factor is essentially tight in the worst-case. More precisely, the upper-bound in Theorem 5.3 can be matched in the worst-case if $\varepsilon = 0$, as shown below.

Proposition 5.4. *For $n = p(k-1)+1$ and any $\varepsilon \geq 0$, there exists a (ε, k)-block-ratio reduced basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of rank n such that $\|\mathbf{b}_1\| = \mu_k^{(n-1)/(k-1)} \|\mathbf{b}_n^*\|$.*

5.2.2 A reduction algorithm

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

Algorithm 2 Block-ratio reduction of an integer lattice

Input: A blocksize $k \geq 2$, a reduction factor $\varepsilon > 0$, and a $\frac{1}{3}$-LLL-reduced basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{Z}^{m \times n}$ of rank $n = p(k-1)+1$.
Output: A (ε, k)-block-ratio reduced basis of $L(B)$.

while B is modified by the loop **do**
  // $\Leftrightarrow$ 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 Alg. 3
    ε-LLL-reduce B and update the GSO matrices B^* and μ
  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 ε, and a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{Z}^{m \times n}$ with GSO matrices B^* and μ.
Output: The block $B_{[i(k-1)+1, i(k-1)+k]}$ becomes $(1+\varepsilon)$-SRP-reduced and the basis vectors outside the block remain unchanged.

Let $j = i(k-1)$
if $i = 0$ **then** $C \leftarrow B_{[1,k]}$
else
  Compute $B_{[j+1, j+k]} \leftarrow (\mathbf{b}_{j+1}^*, \ldots, \mathbf{b}_{j+k}^*)(\mu_{t,j})_{j+1 \leq t, j \leq j+k}^T$
  Compute $C \leftarrow \det((B_{[1,j]})^T B_{[1,j]}) \times B_{[j+1, j+k]} \in \mathbb{Z}^{m \times k}$ //Note that $\mu_k(L(C))^2 = \mu_k(L(B_{[j+1, j+k]}))^2 \in \mathbb{Q}$.
end if
Call the SRP-oracle on C to output a $k \times k$ unimodular matrix $\mathbf{U}$ such that CU is both SRP-reduced and ε-LLL-reduced, 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 $(\mathbf{b}_{j+1}, \ldots, \mathbf{b}_{j+k}) \leftarrow (\mathbf{b}_{j+1}, \ldots, \mathbf{b}_{j+k})U$
end if
return B.

We first show correctness of Alg. 2:

Theorem 5.5. *For all $\varepsilon \geq 0$, Alg. 2 terminates, and outputs a (ε, k)-block-ratio reduced basis.*

We next show that the running time of Alg. 2 is dominated by $\mathrm{poly}(n, 1/\varepsilon)$ times the cost of an SRP-oracle in rank k. Hence, Alg. 2 is polynomial in the same sense as blockwise reduction algorithms for approximating SVP [Sch87, GHGKN06, GN08, MW16, ALNS20]. In particular, if $k \leq \frac{\log n}{\log\log n}$ and we select Alg. 1 as the SRP-oracle, then Alg. 2 runs in polynomial time.

Theorem 5.6. *Given as input a blocksize $k \geq 2$, a reduction factor $\varepsilon \in (0, 1] \bigcap \mathbb{Q}$, and a $\frac{1}{3}$-LLL-reduced basis $B_0 \in \mathbb{Z}^{m \times n}$ of rank $n = p(k-1)+1$ with $p \geq 1$, then any execution of Alg. 2 satisfies:*

1. *The number of calls to the SRP-oracle is $O(p^2 n^2/\varepsilon)$;*
2. *Each coefficient passed to the SRP-oracle has 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 $(\log \|B_0\|, n)$.*

Technically, our complexity analysis uses a ratio potential $r(B) = \prod_{i=0}^{p-1} \left(\frac{\mathrm{vol}(B_{[1,i(k-1)+1]})}{m_{i(k-1)+1}(L(B_0))} \cdot \frac{\mathrm{vol}(B_{[1,(i+1)(k-1)]})}{m_{(i+1)(k-1)}(L(B_0))} \right) \geq 1$, rather than the standard integral potential $P(B) = \prod_{i=0}^{p-1} \mathrm{vol}(B_{[1,i(k-1)+1]})^2 \mathrm{vol}(B_{[1,(i+1)(k-1)]})^2 \in \mathbb{Z}^+$ as used in [LLL82, GN08, LN14, ALNS20]: with the LLL-reduced input, it makes the number of oracle quires in Item 1 independent of the input basis; see Appendix D for details.

This strategy also works well for analyzing blockwise reduction algorithms presented in [GN08, LN14, ALNS20]: for instance, under the notation of [ALNS20, Alg. 2] and with the ratio potential $r(B) = \frac{\mathrm{vol}(B_{[1,q]})}{m_q(L(B))} \geq 1$ (instead of their integral potential $P(B) = \mathrm{vol}(B_{[1,q]})^2 \in \mathbb{Z}^+$), if the input basis B_0 is $\frac{1}{3}$-LLL-reduced, then [ALNS20, Alg. 2] makes at most $\left(\frac{qk}{\log(1+\varepsilon)} + k - q\right)$ calls to the SVP-oracle (rather than their claimed number $\frac{qk \log \|B_0\|}{\log(1+\varepsilon)}$).

References

[ABF+20] M. Albrecht, S. Bai, P.-A. Fouque, P. Kirchner, D. Stehlé, and W. Wen. Faster enumeration-based lattice reduction: Root Hermite factor $k^{1/(2k)}$ in time $k^{k/8+o(k)}$. In *CRYPTO*, pages 186–212, 2020.

[ABLR20] M. R. Albrecht, S. Bai, J. Li, and J. Rowell. Lattice reduction with approximate enumeration oracles: Practical algorithms and concrete performance. Available at https://eprint.iacr.org/2020/1260, 2020.

[ABSS93] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optimia in lattices, codes, and systems of linear equations. In *FOCS*, pages 724–733, 1993.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *STOC*, pages 99–108, 1996.

[Ajt98] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In *STOC*, pages 10–19, 1998.

[Ajt08] M. Ajtai. Optimal lower bounds for the Korkine-Zolotareff parameters of a lattice and for Schnorr's algorithm for the shortest vector problem. *Theory of Computing*, 4(1):21–51, 2008. Preliminary version in *STOC 2003* with title "The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice".

[ALNS20] D. Aggarwal, J. Li, P. Q. Nguyen, and N. Stephens-Davidowitz. Slide reduction, revisited — filling the gaps in SVP approximation. In *CRYPTO*, pages 274–295, 2020.

[ANSS18] Y. Aono, P. Q. Nguyen, T. Seito, and J. Shikata. Lower bounds on lattice enumeration with extreme pruning. In *CRYPTO*, pages 608–637, 2018.

[Bab86] L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

[Bli14] H. F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 16:227–235, 1914.

[BM89] 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.

[BP87] J. Buchmann and M. Pohst. Computing a lattice basis from a system of generating vectors. In *EUROCAL*, pages 54–63, 1987.

[CN98] J.-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor $(1 + 1/\dim^{\varepsilon})$ is NP-hard under randomized reductions. In *CCC*, page 46, 1998.

[DKRS03] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003. Preliminary version in *FOCS 1998*.

[DM13] D. Dadush and D. Micciancio. Algorithms for the densest sub-lattice problem. In *SODA*, pages 1103–1122, 2013.

[DRS14] D. Dadush, O. Regev, and N. Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *CCC*, pages 98–109, 2014. Full version at https://arxiv.org/pdf/1409.8063.pdf.

[GHGKN06] N. Gama, N. Howgrave-Graham, H. Koy, and P. Nguyen. Rankin's constant and blockwise lattice reduction. In *CRYPTO*, pages 112–130, 2006.

[GHGN06] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen. Symplectic lattice reduction and NTRU. In *EUROCRYPT*, pages 233–253, 2006.

[GN08] N. Gama and P. Q. Nguyen. Finding short lattice vectors within Mordell's inequality. In *STOC*, pages 207–216, 2008.

[GNR10] N. Gama, P. Q. Nguyen, and O. Regev. Lattice enumeration using extreme pruning. In *EUROCRYPT*, pages 257–278, 2010.

[Hel85] B. Helfrich. Algorithms to construct Minkowski reduced an Hermite reduced lattice bases. *Theoretical Computer Science*, 41:125–139, 1985.

[Her50] 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.

[HL90] J. Håstad and J. C. Lagarias. Simultaneously good bases of a lattice and its reciprocal lattice. *Mathematische Annalen*, 287(1):163–174, 1990.

[HPS11] G. Hanrot, X. Pujol, and D. Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *CRYPTO*, pages 447–464, 2011.

[HR12] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *Theory of Computing*, 8(1):513–531, 2012. Preliminary version in *STOC 2007*.

[HS07] G. Hanrot and D. Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm. In *CRYPTO*, pages 170–186, 2007.

[HS08] G. Hanrot and D. Stehlé. Worst-case Hermite-Korkine-Zolotarev reduced lattice bases. Available at http://arxiv.org/abs/0801.3331, 2008.

[JS98] A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. *Journal of Cryptology*, 11(3):161–185, 1998.

[Kan87] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987. Preliminary version in *STOC 1983* with title "Improved Algorithms for Integer Programming and Related Lattice Problems".

[Kho05] S. Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, 2005. Preliminary version in *FOCS 2004*.

[KL78] 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.

[KZ73] A. Korkine and G. Zolotareff. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873.

[Len82] A. K. Lenstra. Lattices and factorization of polynomials over algebraic number fields. In *EUROCAL*, pages 32–39, 1982.

[LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:366–389, 1982.

[LLS90] J. C. Lagarias, H. W. Lenstra Jr., and C. P. Schnorr. Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal. *Combinatorica*, 10:333–348, 1990.

[LN14] 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 ANTS-XI, 2014.

[LN19] J. Li and P. Q. Nguyen. Computing a lattice basis revisited. In *ISSAC*, pages 275–282, 2019.

[LN20] J. Li and P. Q. Nguyen. A complete analysis of the BKZ lattice reduction algorithm. Available at https://eprint.iacr.org/2020/1237.pdf, 2020.

[Lut96] H. Lutkepohl. *Handbook of matrices*. John Wiley & Sons, 1996.

[LW13] J. Li and W. Wei. Slide reduction, successive minima and several applications. *Bulletin of the Australian Mathematical Society*, 88:390–406, 2013.

[Mar02] J. Martinet. *Perfect lattices in Euclidean spaces*. Springer, 2002.

[MG02] 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, 2002.

[MH73] J. Milnor and D. Husemoller. *Symmetric bilinear forms*. Springer, 1973.

[Mic00] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2000. Preliminary version in *FOCS 1998*.

[Mor44] 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.

[MV10] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *STOC*, pages 351–358, 2010.

[MW15] D. Micciancio and M. Walter. Fast lattice point enumeration with minimal overhead. In *SODA*, pages 276–294, 2015.

[MW16] D. Micciancio and M. Walter. Practical, predictable lattice basis reduction. In *EUROCRYPT*, pages 820–849, 2016.

[Neu17] A. Neumaier. Bounding basis reduction properties. *Designs, Codes and Cryptography*, 84:237–259, 2017.

[New63] M. Newman. Bounds for cofactors and arithmetic minima of quadratic forms. *Journal of the London Mathematical Society*, 38:215–217, 1963.

[NV10] P. Q. Nguyen and B. Vallée, editors. *The LLL algorithm: survey and applications*. Information Security and Cryptography. Springer, 2010.

[PT08] G. Pataki and M. Tural. On sublattice determinants in reduced bases. 2008. Aailable at https://arxiv.org/pdf/0804.4014.pdf.

[Ran53] R. A. Rankin. On positive definite quadratic forms. *Journal of the London Mathematical Society*, 28:309–314, 1953.

[Reg04] O. Regev. Lecture 8: Dual lattices. 2004. Aailable at http://www.cims.nyu.edu/regev/teaching/lattices-fall-2004/index.html.

[Sch87] C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[SE94] C. P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66:181–199, 1994.

[Sey93] M. Seysen. Simultaneous reduction of a lattice basis its reciprocal basis. *Combinatorica*, 13(3):363–376, 1993.

[SG] M. Schneider and N. Gama. TU Darmstadt SVP challenge. Aailable at http://www.latticechallenge.org/svp-challenge/index.php.

[Sie89] C. L. Siegel. *Lectures on the geometry of numbers*. Springer, 1989.

[SWO10] 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.

[vEB81] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Tecnical Report 81-04, Department of Mathmatics, University of Amsterdam, 1981.

A Proof of Claim 1.1

Proof of Claim 1.1. We first bound $\|\mathbf{b}_1\|/\mathrm{vol}(L)^{1/n}$. The gluing 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 $i = 0, \ldots, p-1$ gives rise to: $\|\mathbf{b}_1\| \leq g(k)h(k+1)^{(n-k)/2k}\mathrm{vol}(L)^{1/n}$.

It remains to bound $\|\mathbf{b}_1\|/\lambda_1(L)$ under the assumption. Let $\mathbf{u}$ be a shortest nonzero 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 $L(B_{[qk+1,qk+k]})$, we have $\|\pi_{qk+1}(\mathbf{u})\| \geq \lambda_1(L(B_{[qk+1,qk+k]}))$. Therefore,

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

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

B Critical lattices for μ_n

An n-rank lattice L is *critical* for μ_n if $\mu_n(L) = \mu_n$. Consider the following 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 [Mar02, Chapter 4] for details);
2. B is i-Rankin reduced for $1 \le i \le 7$ (see [SWO10, Prop. 1]).

Our main result of this appendix is as follows:

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

Proof. For each $i \in [2, 8]_z$, by Property 2, $B^{(i)}$ is SVP-reduced and $(i-1)$-Rankin reduced. Then $B^{(i)}$ reaches $\mu_i(L(B^{(i)}))$ by Claim 4.6. The conclusion follows easily from Theorem 4.15. □

C Bounding the size of transformation

Both Lemma C.1 and Cor. C.2 can be used to efficiently bound the size of transformation.

Lemma C.1. *Let $B \in \mathbb{Z}^{m \times n}$ have rank n and $\mathbf{x} \in \mathbb{Z}^{j-i+1}$ for $1 \le i < j \le n$. If $B_{[i,j]}\mathbf{x} = \mathbf{b}$, then $\|\mathbf{x}\|_\infty \le \|B\|^{n-1}\|\mathbf{b}\|$.*

Proof. Let $k = j - i + 1$, $A = B_{[i,j]} = (\mathbf{a}_1, \ldots, \mathbf{a}_k)$ and $A_s = (\mathbf{a}_1, \ldots, \mathbf{a}_{s-1}, \mathbf{b}, \mathbf{a}_{s+1}, \ldots, \mathbf{a}_k)$ for $s = 1, \ldots, k$. Define:

$$y = \det(A^T A) \quad \text{and} \quad z_s = \det(A^T A_s) \quad \text{for} \quad s = 1, \ldots, k.$$

Since $A\mathbf{x} = \mathbf{b}$ is equivalent to $A^T A\mathbf{x} = A^T\mathbf{b}$ and $A^T A$ is a nonsingular square matrix, Cramer's rule implies $\mathbf{x} = (\frac{z_1}{y}, \ldots, \frac{z_k}{y})^T$. To complete the proof, it suffices to upper bound the $\left|\frac{z_s}{y}\right|$'s.

Let $d_0 = 1$ and $d_\ell = \det((B_{[1,\ell]})^T B_{[1,\ell]})$ for $\ell = 1, \ldots, n$. Then $d_\ell \in \mathbb{Z}^+$ and $d_\ell \le \|B^*\|^{2\ell}$ for $\ell = 1, \ldots, n$. In particular, we have $\det(A^T A) = \mathrm{vol}(L(A))^2 = \mathrm{vol}(L(B_{[1,j]})^2/\mathrm{vol}(L(B_{[1,i-1]})^2 = d_j/d_{i-1}$.

Note that $|\det(A^T A_s)|^2 \le \det(A^T A)\det(A_s^T A_s)$ (see [Lut96, p. 54]) with $0 \le \det(A_s^T A_s) \le \|A\|^{2k-2}\|\mathbf{b}\|^2$, this implies

$$\left|\frac{z_s}{y}\right| = \left|\frac{\det(A^T A_s)}{\det(A^T A)}\right| \le \sqrt{\frac{\det(A_s^T A_s)}{\det(A^T A)}} \le \sqrt{\frac{d_{i-1}}{d_j}}\|A\|^{k-1}\|\mathbf{b}\| \le \|B\|^{j-i}\|B^*\|^{i-1}\|\mathbf{b}\| \quad \text{for} \quad s = 1, \ldots, k.$$

Thus, $\|\mathbf{x}\|_\infty \le \|B\|^{j-i}\|B^*\|^{i-1}\|\mathbf{b}\| \le \|B\|^{n-1}\|\mathbf{b}\|$. This completes the proof. □

Corollary C.2. *Let $B \in \mathbb{Z}^{m \times n}$ be an n-rank lattice basis. Let $1 \le i < j \le n$ be indices such that $j - i + 1 = k$ and let $U \in \mathbb{Z}^{k \times k}$ be a unimodular matrix. If $C = B_{[i,j]}U$ is ε-LLL-reduced for $\varepsilon \ge 0$, then*

$$\|C\| \le \alpha^{(k-1)/2} \times \|B\| \quad \text{and} \quad \|U\|_\infty \le \alpha^{(k-1)/2} \times \|B\|^n$$

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

Proof. The classical property of LLL-reduced bases [LLL82, Prop. 1.12] implies $\|C\|^2 \le \alpha^{k-1}\|B_{[i,j]}\|^2$. Applying Lemma C.1 to the equality $C = B_{[i,j]}U$, we have $\|U\|_\infty \le \|B\|^{n-1}\|C\| \le \alpha^{(k-1)/2}\|B\|^n$. This completes the proof. □

D Proofs of Section 5

Proof of Theorem 5.1. We first show correctness. If Steps 4-5 occur, then the output basis B is already SRP-reduced (by Claim 4.6). Assume that Step 6 occurs. Recall Identity (4.3), we have

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

where $\mathcal{S} = \{\mathbf{x} \in L : \|\mathbf{x}\| \leq \|\mathbf{a}_1\|\}$ is defined by Step 7. Steps 7-15 execute this equality exactly: hence, the resulting basis B at Step 15 is indeed SRP-reduced. The LLL requirement (at Step 16 or see Step 5) ensures good magnitudes for both the output SRP-reduced basis and the corresponding unimodular transformation (by Cor. C.2). This proves the correctness.

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

$$\|B\| \leq \begin{cases} 2^{O(n^2)} \times \|B_0\| & \text{right after Step 2,} \\ 2^{(n-1)/2} \times \|B_0\| & \text{right after Step 3 or Step 16,} \end{cases} \tag{D.1}$$

$$\|C\| \leq \begin{cases} n^{1.5} \times \|B_0\| & \text{right after Step 10 or Step 11,} \\ 2^{O(n^2)} \times \|B_0\| & \text{right after Step 12.} \end{cases} \tag{D.2}$$

Indeed, since the basis $A = (\mathbf{a}_1, \ldots, \mathbf{a}_n)$ at Step 3 is $(n-1)$-Rankin-reduced and $A_{[1,n-1]}$ is HKZ-reduced, Lemma 2.3 implies $\|\mathbf{a}_1\| \leq \gamma_{n-1}\lambda_1(L) \leq n\|B_0\|$. Then the current basis C during Steps 10-11 always has short Gram-Schmidt vectors: $\|C^*\| \leq \max\{\|\mathbf{a}_1\|, \|B_0\|\}$. It follows that $\|C\| \leq n^{1.5} \times \|B_0\|$ right after Step 10/Step 11. Then the properties of both the DSVP-reduction performed by [GN08, Alg. 3] and the LLL-reduction (see Cor. C.2) imply Eq. (D.1) and Eq. (D.2).

From Eq. (D.1) and Eq. (D.2), all intermediate bases during execution have size $O(n^2 + \log\|B_0\|)$. Then both Steps 1-5 and every single execution of Steps 9 -14 require $\mathrm{poly}(\log\|B_0\|, m) \cdot n^{\frac{n}{2e}} 2^{O(n)}$ bit operations and polynomial space.

It remains to count the cardinality of the set $\mathcal{S} = \{\mathbf{x} \in L : \|\mathbf{x}\| \leq \|\mathbf{a}_1\|\}$ defined by Step 7. Again, since A is DSVP-reduced and $A_{[1,n-1]}$ is HKZ-reduced, we have

$$\begin{aligned} \max_{I \subseteq [1,n]_{\mathbb{Z}}} \left(\frac{\|\mathbf{a}_1\|^{|I|}}{(\sqrt{n})^{|I|}\prod_{i\in I}\|\mathbf{a}_i^*\|}\right) &\leq \frac{n}{\sqrt{n}} \cdot \max_{I \subseteq [1,n-1]_{\mathbb{Z}}} \left(\frac{\|\mathbf{a}_1\|^{|I|}}{(\sqrt{n-1})^{|I|}\prod_{i\in I}\|\mathbf{a}_i^*\|}\right) && \text{(by Lemma 2.4)} \\ &\leq \sqrt{n} \cdot (\sqrt{n-1})^{\frac{n-1}{e}} && \text{(by [HS07, Th. 3])} \\ &\leq n^{\frac{n}{2e}+\frac{1}{2}}. \end{aligned}$$

By Hanrot-Stehlé's analysis of Kannan's SVP enumeration algorithm [HS07, §4.1], $\mathcal{S}$ has cardinality:

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

Since Steps 9-14 occur at most $|\mathcal{S}|$ times, we conclude that Alg. 1 totally requires $\mathrm{poly}(\log\|B_0\|, m) \cdot n^{\frac{n}{e}} 2^{O(n)}$ bit operations and polynomial space. This completes the proof. □

Proof of Theorem 5.3. By the definition, the block $B_{[i(k-1)+1,i(k-1)+k]}$ satisfies: $\|\mathbf{b}^*_{i(k-1)+1}\| \leq \sqrt{1+\varepsilon}\mu_k\|\mathbf{b}^*_{i(k-1)+k}\|$ for $i = 0, \ldots, p-1$. This implies the conclusion. □

Proof of Proposition 5.4. The technical idea stems from the worst-case analysis of slide reduction [GN08, §4]. By Theorems 4.1 and 4.9, there exists a k-rank 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 GSO 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 orthonormal set, $D = \mathrm{Diag}(\|\mathbf{c}_1^*\|, \ldots, \|\mathbf{c}_k^*\|)$, and $\mu = (\mu_{i,j})^T_{1\leq i,j\leq k}$ 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, because T is isometric to C. This elementary "brick" T can be duplicated and rescaled p times to form a big n-rank 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 (ε, k)-block-ratio reduced such that $\|\mathbf{b}_1\|/\|\mathbf{b}_n^*\| = \|\mathbf{c}_1\|/(\alpha^{p-1}\|\mathbf{c}_k^*\|) = \mu_k^p$. This completes the proof. □

Proof of Theorem 5.5. Let B_0 denote the input $\frac{1}{3}$-LLL-reduced basis and B denote the current basis during execution. Consider the following ratio potential

$$r(B) = \prod_{i=0}^{p-1}\left(\frac{\mathrm{vol}(B_{[1,i(k-1)+1]})}{m_{i(k-1)+1}(L(B_0))} \cdot \frac{\mathrm{vol}(B_{[1,(i+1)(k-1)]})}{m_{(i+1)(k-1)}(L(B_0))}\right) \geq 1. \tag{D.3}$$

Initially, $\log r(B_0) \leq O(pn^2)$ (by the classical property of LLL-reduced bases [PT08, Eq. (2)]). Every operation in Alg. 2 either preserves or strictly decreases $r(B)$. More precisely, if each $(1+\varepsilon)$-SRP-reduction modifies the block

$B_{[i(k-1)+1,i(k-1)+k]}$ for some $i \in [0, p-1]_{\mathbb{Z}}$, or each special swap of LLL (at Step 5) between two indices $(i(k-1)+1, i(k-1)+2)$ or $((i+1)(k-1), i(k-1)+k)$ occurs, then $r(B)$ is reduced by a multiplicative factor $< \frac{1}{\sqrt{1+\varepsilon}}$. Therefore, there is a bounded number of such $(1+\varepsilon)$-SRP-reductions and special swaps even if $\varepsilon = 0$. The operations which preserve $r(B)$ cannot modify the basis indefinitely. Hence, Alg. 2 terminates for all $\varepsilon \geq 0$.

It is easy to see that Alg. 2 finally outputs a (ε, k)-block-ratio reduced basis. 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 Alg. 3. This completes the proof. □

Proof of Theorem 5.6. We consider again the rato potential $r(B)$ defined by Eq. (D.3). Since $\varepsilon > 0$, the number of calls to the $(1+\varepsilon)$-SRP-reduction subroutine and special swaps of LLL is at most $\frac{\log r(B_0)}{\log \sqrt{1+\varepsilon}}$. Thus, Alg. 2 terminates after at most $\frac{\log r(B_0)}{\log \sqrt{1+\varepsilon}}$ loops. Since every loop has p SRP-reductions, the total number of calls to the SRP-oracle is at most $O(\frac{p^2 n^2}{\log(1+\varepsilon)})$.

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

$$\|B\| \leq \begin{cases} 2^{n^2+2k} \times \|B_0\|^{n+1} & \text{right after Step 4,} \\ 2^{n-1} \times \|B_0\| & \text{right after Step 5.} \end{cases}$$

Indeed, since the current basis B right after Step 5 is ε-LLL-reduced for $\varepsilon \in (0, 1]$, Cor. C.2 implies $\|B\| \leq 2^{n-1}\|B_0\|$. Consider Step 4, where Alg. 3 is called: for index $i \in [0, p-1]_{\mathbb{Z}}$, the integer matrix C appearing in Alg. 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 $\|U\|_\infty \leq 2^{k-1}(2^{n-1}\|B_0\|)^n$ (by Cor. C.2); then the current basis B right after Step 4 has magnitude: $\|B\| \leq k\|U\|_\infty(2^{n-1}\|B_0\|) \leq k2^{n^2+k}\|B_0\|^{n+1}$.

Therefore, we always have $\log\|B\| \leq 2n(n + \log\|B_0\|)$ throughout Alg. 2: by the classical analysis of the LLL algorithm [LLL82, Prop. 1.26], every single execution of Steps 4-5 (except the oracle) runs in time polynomial in $(\log\|B_0\|, m, 1/\varepsilon)$ and runs on rational numbers which have size polynomial in $(\log\|B_0\|, n)$ during execution. This completes the proof of Theorem 5.6. □