Bull. Aust. Math. Soc. **88** (2013), 390–406
doi:10.1017/S0004972713000257

SLIDE REDUCTION, SUCCESSIVE MINIMA AND SEVERAL APPLICATIONS

JIANWEI LI[✉] **and WEI WEI**

(Received 21 September 2012; accepted 6 February 2012; first published online 30 April 2013)

Abstract

Gama and Nguyen ['Finding short lattice vectors within Mordell's inequality', in: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, New York, 2008, 257–278] have presented *slide reduction* which is currently the best SVP approximation algorithm in theory. In this paper, we prove the upper and lower bounds for the ratios $\|\mathbf{b}_i^*\|/\lambda_i(\mathbf{L})$ and $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$, where $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a slide reduced basis and $\lambda_1(\mathbf{L}), \ldots, \lambda_n(\mathbf{L})$ denote the successive minima of the lattice $\mathbf{L}$. We define generalised slide reduction and use slide reduction to approximate i-SIVP, SMP and CVP. We also present a critical slide reduced basis for blocksize 2.

2010 *Mathematics subject classification*: primary 11H06; secondary 11P21.
Keywords and phrases: slide reduction, successive minima, SIVP, SMP, CVP.

1. Introduction

Let $\mathbb{R}^m$ be m-dimensional Euclidean space. A lattice $\mathbf{L}$ in $\mathbb{R}^m$ is the set $\mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^n x_i\mathbf{b}_i : x_i \in \mathbb{Z}\}$ of all integer linear combinations of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathbb{R}^m$ ($m \geq n$). The integers n and m are called the rank and dimension of the lattice, respectively. There are many computational problems on lattices, which play an important role in many areas of computer science, mathematics and engineering, including cryptography, cryptanalysis, combinatorial optimisation, communication theory and algebraic number theory.

The most famous problem on lattices is the shortest vector problem (SVP), which asks for the shortest nonzero vector in an input lattice. Slide reduction, presented by Gama and Nguyen [8], is currently the best SVP approximation algorithm in theory, although preliminary experiments suggest that it might not be the best algorithm in practice. Several generalisations and variants of SVP naturally arise both in the theoretical study of lattices and in their applications. The most common generalisation of SVP encountered in computer science is the i-shortest independent vectors problem (i-SIVP): given a lattice, find i linearly independent lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_i$ such

The work of Jianwei Li (corresponding author) was supported by 973 program (No. 2013CB834205) and the National Natural Science Foundation of China (No. 61133013).

that the maximum length $\max\{\|\mathbf{v}_j\| : 1 \le j \le i\}$ is minimised. SVP is recovered as a special case of i-SIVP by setting $i = 1$. At the other end of the spectrum, for $i = n$, this is the classic SIVP problem arising in the construction of cryptographic functions with worst-case/average-case connection [1, 16, 18]. For arbitrary i, i-SIVP is the computational problem naturally associated with the successive minima $\lambda_1, \ldots, \lambda_n$, which are defined as follows: the ith successive minimum λ_i is the radius of the smallest sphere centred in the origin containing i linearly independent lattice vectors,

$$\lambda_i = \lambda_i(\mathbf{L}) := \inf\{r : \dim(\operatorname{span}(\mathbf{L} \cap \mathcal{B}(\mathbf{0}, r))) \ge i\},$$

where $\mathcal{B}(\mathbf{0}, r) = \{\mathbf{x} \in \mathbf{R}^m : \|\mathbf{x}\| \le r\}$ is the m-dimensional ball of radius r centred in $\mathbf{0}$. Clearly, $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$.

Closely related to the successive minima problem is the (γ-approximate) successive minima problem (SMP): given a lattice, find linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of length at most $\|\mathbf{v}_j\| \le \gamma\lambda_j$ for all $j = 1, \ldots, n$. This is also a classic mathematical problem in the study of lattices that subsumes both SVP and SIVP as special cases. Another important generalisation of SVP is the closest vector problem (CVP): given a lattice basis $\mathbf{B} \in \mathbb{R}^{m\times n}$ and a target vector $\mathbf{x} \in \mathbb{R}^m$, find a lattice vector $\mathbf{By}$ closest to the target $\mathbf{x}$, that is, find an integer vector $\mathbf{y} \in \mathbb{Z}^n$ such that $\|\mathbf{By} - \mathbf{x}\| \le \|\mathbf{Bz} - \mathbf{x}\|$ for any other $\mathbf{z} \in \mathbb{Z}^n$. The special case $\mathbf{x} = \mathbf{0}$ of CVP is SVP. Importantly, SVP, i-SIVP, SMP and CVP are all NP-hard problems. That is, they cannot be solved in subexponential time under standard complexity assumptions. The hardness of solving the above problems has led computer scientists to consider approximation versions of these problems.

In this paper, we prove the upper and lower bounds for the ratios $\|\mathbf{b}_i^*\|/\lambda_i(\mathbf{L})$ and $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$, where $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a slide reduced basis of a lattice $\mathbf{L}$. We define generalised slide reduction and use slide reduction to solve i-SIVP, SMP and CVP approximately. We also present a critical slide reduced basis for blocksize 2.

2. Preliminaries

Let $\|\cdot\|$ be the Euclidean norm of $\mathbb{R}^m$. We denote the field of real numbers by $\mathbb{R}$ and the integer ring by $\mathbb{Z}$. We use bold letters to denote vectors, in column notation. The notation $[x]$ denotes the largest integer which is less than or equal to x, $\lceil x \rceil$ denotes the smallest integer which is not less than x, and $\lceil x \rfloor$ denotes the integer nearest to x.

2.1. Lattice

Hermite's constant. The Hermite invariant of a lattice is defined by $\gamma(\mathbf{L}) = (\lambda_1(\mathbf{L})/\operatorname{vol}(\mathbf{L})^{1/n})^2$. Hermite's constant γ_n is the maximal value of $\gamma(\mathbf{L})$ over all n-dimensional lattices. The exact value of Hermite's constant γ_n is known for $1 \le n \le 8$ and $n = 24$, where $\gamma_2 = \sqrt{4/3}$ is frequently used. For other values of γ_n, it is known that $\gamma_n \le 1 + n/4$ (see [14]) and the best numerical upper bounds known are those given in [4]. The best asymptotic bounds are (see [5, 17])

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

Thus, γ_n is essentially linear in n, but it is unknown if $(\gamma_n)_{n\ge1}$ is an increasing sequence.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

Orthogonalisation. Given an ordered lattice basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$, we associate the Gram–Schmidt orthogonalisation $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^* \in \mathbb{R}^m$, which can be computed together with the Gram-Schmidt coefficients $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / \langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle$ by the recursion $\mathbf{b}_1^* = \mathbf{b}_1$, $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$, for $i = 2, \ldots, n$. We have $\mu_{i,i} = 1$ and $\mu_{i,j} = 0$ for $i < j$. From the above equations we have the unique Gram–Schmidt decomposition $\mathbf{B} = \mathbf{Q}\mathbf{D}\mu$, where $\mathbf{Q} = (\mathbf{b}_1^*/\|\mathbf{b}_1^*\|, \ldots, \mathbf{b}_n^*/\|\mathbf{b}_n^*\|)$ is an orthogonal matrix, $\mathbf{D} = \mathrm{diag}(\|\mathbf{b}_1^*\|, \ldots, \|\mathbf{b}_n^*\|)$, $\mu = (\mu_{i,j})_{1 \le i,j \le n}^t$. Obviously, $\mathbf{B}^* = \mathbf{Q}\mathbf{D} = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$.

Orthogonal projections. Given an ordered lattice basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$, we associate the orthogonal projections:

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

where $\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ denotes the linear space generated by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Let $\mathbf{L}_i$ denote the lattice $\mathbf{L}_i = \pi_i(\mathbf{L})$. The lattice $\mathbf{L}_i$ has rank $n - i + 1$ and basis $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_n))$. We have $\pi_i(\mathbf{b}_i) = \mathbf{b}_i^*$ and $\pi_i(\mathbf{b}_j) = \sum_{k=i}^{j} \mu_{j,k} \mathbf{b}_k^*$. We will use the notation $\mathbf{B}_{[i,j]}$ for the projected block $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_j))$. If $\mathbf{B}$ has integer coefficients, then $\mathbf{B}_{[i,j]}$ has rational coefficients for $i > 1$, and integer coefficients for $i = 1$.

Duality. If $\mathbf{L}$ is a lattice, the dual lattice of $\mathbf{L}$ is $\mathbf{L}^{\times} = \{y \in \mathrm{span}(\mathbf{B}) : \langle x, y \rangle \in \mathbb{Z}, \ \forall x \in \mathbf{L}\}$. For any basis $\mathbf{B}$ of $\mathbf{L}$, $\mathbf{B}^{-t} \triangleq \mathbf{B}(\mathbf{B}^t\mathbf{B})^{-1}$ is a basis of $\mathbf{L}^{\times}$. However, in lattice reduction, it is more convenient to consider the reversed dual basis [7] defined as $\mathbf{B}^{-s} = \mathbf{R}_m \mathbf{B}^{-t} \mathbf{R}_n$, where $\mathbf{R}_n$ is the reversed identity matrix: $\mathbf{R}_n(i, j) = \delta_{i,n-j+1}$, where $\delta_{i,j}$ denotes Kronecker's symbol. The lattice generated by the reversed dual basis is isometric to the standard dual lattice, and has therefore the same mathematical properties. 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, because $(\mathbf{Q}\mathbf{D}\mu)^{-s} = \mathbf{Q}^{-s}\mathbf{D}^{-s}\mu^{-s}$.

2.2. Lattice reduction

Size reduction. We call a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ size-reduced, if $|\mu_{i,j}| \le \frac{1}{2}$, for all $1 \le j < i \le n$. The basis vector $\mathbf{b}_i$ is size-reduced, if $|\mu_{i,j}| \le \frac{1}{2}$, for $1 \le j < i$. After size reduction, a basis will be almost orthogonal and appropriately shortened.

LLL reduction. A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$ is LLL-reduced [12] with factor $\varepsilon \ge 0$ if it is size-reduced and every 2×2 block $\mathbf{B}_{[i,i+1]}$ satisfies Lovász's condition: $\|\mathbf{b}_i^*\|^2 \le (1 + \varepsilon)(\|\mathbf{b}_{i+1}^*\|^2 + \mu_{i+1,i}^2 \|\mathbf{b}_i^*\|^2)$. Lovász's condition combined with size reduction implies Siegel's condition: $\|\mathbf{b}_i^*\|^2 \le (4/3)(1 + \varepsilon)^2 \|\mathbf{b}_{i+1}^*\|^2$. The LLL algorithm [12] outputs an LLL-reduced basis in polynomial time in $1/\varepsilon$ and size($\mathbf{B}$).

HKZ reduction. A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$ is HKZ-reduced [10] if it is size-reduced, and $\mathbf{b}_i^*$ is a shortest vector of $\mathbf{L}(\mathbf{B}_{[i,n]})$ for all $i \in [1, n - 1]$.

k-BKZ reduction. A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{m \times n}$ is k-BKZ reduced [19], that is, it is a block Korkin-Zolotarev basis with blocksize k, if it is size-reduced, and $\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_{i+k-1})$ are HKZ-reduced for $i = 1, \ldots, n - k + 1$.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

In HKZ reduction or k-BKZ reduction there is a basic subroutine, namely, SVP reduction.

SVP reduction. A basis $\mathbf{B}$ is SVP-reduced if the first basis vector $\mathbf{b}_1$ reaches the first minimum, that is, $\|\mathbf{b}_1\| = \lambda_1(\mathbf{L}(\mathbf{B}))$. There is a natural relaxation: a basis $\mathbf{B}$ is $(1+\varepsilon)$-SVP-reduced for $\varepsilon \geq 0$ if the first basis vector satisfies $\|\mathbf{b}_1\| \leq \sqrt{1+\varepsilon} \cdot \lambda_1(\mathbf{L}(\mathbf{B}))$. If the basis is a projected block $\mathbf{B}_{[i,j]}$, this implies that

$$\|\mathbf{b}_i^*\|^{j-i+1} \leq ((1+\varepsilon) \cdot \gamma_{j-i+1})^{(j-i+1)/2} \operatorname{vol}(\mathbf{B}_{[i,j]}).$$

DSVP reduction. For $\varepsilon \geq 0$, a basis $\mathbf{B}$ is $(1+\varepsilon)$-DSVP-reduced (where D stands for dual) if the reversed dual basis $\mathbf{B}^{-s}$ is $(1+\varepsilon)$-SVP-reduced. If the basis is a projected block $\mathbf{B}_{[i,j]}$, this implies that:

$$\operatorname{vol}(\mathbf{B}_{[i,j]}) \leq ((1+\varepsilon) \cdot \gamma_{j-i+1})^{(j-i+1)/2} \|\mathbf{b}_j^*\|^{j-i+1}.$$

By simplifying the combination of k-BKZ reduction and $(1+\varepsilon)$-DSVP reduction, Gama and Nguyen [8] introduced the following new blocksize reduction notion based on duality for lattices of rank n, where n is an exact multiple of the blocksize k.

Slide reduction. A basis $\mathbf{B}$ of an n-rank lattice $\mathbf{L}$, where $n = pk$, is slide reduced with a factor $\varepsilon \geq 0$ if it is size-reduced and satisfies the following two sets of conditions:

(1) primal conditions: for all $i \in [0, p-1]$, the block $\mathbf{B}_{[ik+1,ik+k]}$ is HKZ-reduced;
(2) dual conditions: for all $i \in [0, p-2]$, the block $\mathbf{B}_{[ik+2,ik+k+1]}$ is $(1+\varepsilon)$-DSVP-reduced.

3. Slide reduced basis and successive minima

3.1. Previous work and remark. The successive minima are some of the most fundamental mathematical parameters describing the geometry of a lattice, and yield a measure of the reducedness of a lattice basis. A basis is 'reduced', when the values $\|\mathbf{b}_i\|/\lambda_i$ for $i = 1, 2, \ldots, n$ are 'small'.

THEOREM 3.1 (Lenstra *et al.* [12]). *Every basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *of a lattice* $\mathbf{L}$ *which is LLL-reduced with* $\varepsilon \in [0, 3)$ *satisfies*

$$\alpha^{1-i} \leq \frac{\|\mathbf{b}_i^*\|^2}{\lambda_i(\mathbf{L})^2} \leq \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \leq \alpha^{n-1},$$

with $\alpha = 4(1+\varepsilon)/(3-\varepsilon)$ *for* $i = 1, \ldots, n$. *In particular, for* $\varepsilon = 0$,

$$\left(\frac{3}{4}\right)^{i-1} \leq \frac{\|\mathbf{b}_i^*\|^2}{\lambda_i(\mathbf{L})^2} \leq \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \leq \left(\frac{4}{3}\right)^{n-1}, \quad i = 1, \ldots, n. \tag{3.1}$$

THEOREM 3.2 (Mahler [13] and Lagarias *et al.* [11]). *Every HKZ-reduced basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *of a lattice* $\mathbf{L}$ *satisfies*

$$\frac{4}{i+3} \leq \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \leq \frac{i+3}{4},$$

for $i = 1, \ldots, n$.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

THEOREM 3.3 (Schnorr [20]). *Every k-BKZ basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *of a lattice* $\mathbf{L}$ *satisfies*

$$\frac{\|\mathbf{b}_i^*\|^2}{\lambda_i(\mathbf{L})^2} \le \gamma_k^{2(n-i)/(k-1)} \quad \text{for } i = 1, \ldots, n,$$
$$\frac{4}{i+3}\gamma_k^{-2(i-1)/(k-1)} \le \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \le \gamma_k^{2(n-i)/(k-1)}\frac{i+3}{4} \quad \text{for } i = 1, \ldots, n.$$

In particular, for $k = 2$, this implies that

$$\frac{\|\mathbf{b}_i^*\|^2}{\lambda_i(\mathbf{L})^2} \le \left(\frac{4}{3}\right)^{n-i}, \quad i = 1, \ldots, n,$$
$$\frac{4}{i+3}\left(\frac{3}{4}\right)^{i-1} \le \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \le \left(\frac{4}{3}\right)^{n-1}\frac{i+3}{4}, \quad i = 1, \ldots, n, \tag{3.2}$$

which is almost the upper bound of (3.1).

THEOREM 3.4 (Gama and Nguyen [8]). *A slide reduced basis* $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^m$ *of a lattice* $\mathbf{L}$ *with blocksize* k *dividing* n *and factor* $\varepsilon \ge 0$ *satisfies the following two inequalities:*

$$\|\mathbf{b}_1\| \le (\gamma_k\sqrt{1+\varepsilon})^{(n-1)/2(k-1)}\,\mathrm{vol}(\mathbf{L})^{1/n},$$
$$\|\mathbf{b}_1\| \le (\gamma_k\sqrt{1+\varepsilon})^{(n-k)/(k-1)}\lambda_1(\mathbf{L}).$$

Clearly slide reduction achieves Mordell's inequality: $\gamma_n \le \gamma_k^{(n-1)/(k-1)}$. Further, the process of proving Theorem 3.4 in [8] indicates that it is enough that the blocks $\mathbf{B}_{[ik+1,ik+k]}$ for $i \in [0, p-1]$ are SVP-reduced. Thus, if we only search for the approximate solution of $\lambda_1(\mathbf{L})$, the complexity of the slide reduction algorithm can be greatly reduced.

REMARK 3.1. LLL reduction [12] is the first polynomial time lattice reduction algorithm, but the upper bounds of the ratios $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$ are rather large. (This assertion follows from Hermite's inequality $\gamma_k \le (\sqrt{4/3})^{k-1}$). From the computational point of view, HKZ reduction is the most natural one. However, HKZ-reduced bases are not easy to find for lattices of higher dimensions (see Kannan [9] and Schnorr [19] for algorithms). No polynomial time algorithm is known for k-BKZ reduction. Then, Schnorr and Euchner [21] presented a practical 'approximate' algorithm performing k-BKZ reduction: transform an arbitrary lattice basis into a $(1+\varepsilon)$-approximate k-BKZ basis with factor $\varepsilon > 0$, which by definition satisfies, for $i = 1, \ldots, n$,

$$\|\mathbf{b}_i^*\|^2 \le (1+\varepsilon)\lambda_1(\pi_i(\mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{\min(i+k-1,n)})))^2.$$

However, the Schnorr and Euchner algorithm is not proven to be polynomial time.

Fortunately, slide reduction [8] is a polynomial-time blocksize reduction algorithm, which is currently the best SVP approximation algorithm in theory. Hence, it is very important to present the values $\|\mathbf{b}_i\|/\lambda_i$ for a slide reduced basis of a lattice.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

3.2. Our result on successive minima. We are going to extend Theorems 3.1–3.4 to the following main theorem for slide reduced bases. It will be proved in Section 3.3.

THEOREM 3.5. *Every slide reduced basis* $\mathbf{b}_1, \dots, \mathbf{b}_n$ *of a lattice* $\mathbf{L}$ *with blocksize* k *and factor* $\varepsilon = 0$*, where* $n = pk$*, satisfies:*

(1) *the upper bounds for the ratios* $\|\mathbf{b}_i^*\|/\lambda_i(\mathbf{L})$*:*

$$\frac{\|\mathbf{b}_{lk+j}^*\|}{\lambda_{lk+j}(\mathbf{L})} \le \gamma_{k-j+1}^{(k-j+1)/(k-j)} \gamma_k^{(p-l-2)k/(k-1)}, \quad l = 0, \dots, p-2, \quad j = 1, \dots, k-1,$$

$$\frac{\|\mathbf{b}_{lk+k}^*\|}{\lambda_{lk+k}(\mathbf{L})} \le \gamma_2 \gamma_k^{(p-l-2)k/(k-1)}, \quad l = 0, \dots, p-2,$$

$$\frac{\|\mathbf{b}_{(p-1)k+j}^*\|}{\lambda_{(p-1)k+j}(\mathbf{L})} \le 1, \quad j = 1, \dots, k;$$

(2) *the upper and lower bounds for the ratios* $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$*:*

$$\sqrt{\frac{3}{i+3}}\gamma^{-1}\gamma_k^{(k-[i]_k)/(k-1)} \le \frac{\|\mathbf{b}_i\|}{\lambda_i(\mathbf{L})} \le \sqrt{\frac{i+3}{3} - \frac{1}{12}\left[\frac{i}{k}\right]}\gamma\gamma_k^{(n-2k)/(k-1)}, \quad 1 \le i \le n,$$

where $[i]_k = [i/k]k$ *and* $\gamma = \max\{\gamma_i : 2 \le i \le k\}$.

Clearly, our upper bound for $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$ is better than that in Theorem 3.3 for $1 \le i \le k$ in general. In particular, for $k = 2$, $\varepsilon = 0$, it implies that

$$\frac{\|\mathbf{b}_i^*\|^2}{\lambda_i(\mathbf{L})^2} \le \left(\frac{4}{3}\right)^{n-i}, \quad i = 1, \dots, n-r,$$

$$\frac{4}{i+3}\left(\frac{3}{4}\right)^{i-1} \le \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathbf{L})^2} \le \left(\frac{4}{3}\right)^{n-1}\left(\frac{i+3}{4} - \frac{1}{16}\left[\frac{i}{2}\right]\right), \quad i = 1, \dots, n. \tag{3.3}$$

The upper bound of (3.3) is better than that of (3.2). This is enough, because a slide reduced basis can be obtained in polynomial time while the k-BKZ basis cannot! It is remarkable that if the blocksize k is a fixed fraction of the rank, that is, if p is fixed, then the upper bounds of Theorem 3.5 are polynomial in k.

3.3. Proof of Theorem 3.5.

LEMMA 3.6 (Schnorr [20]). *We have* $\lambda_1(\mathbf{L_i}) \le \lambda_i(\mathbf{L})$ *for* $i = 1, \dots, n$.

This is because there are i linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_i$ of length at most $\lambda_i(\mathbf{L})$ in $\mathbf{L}$ and at least one of these vectors $\mathbf{v}_t$ satisfies $\pi_i(\mathbf{v}_t) \ne 0$; otherwise $\mathbf{v}_1, \dots, \mathbf{v}_i \in \mathrm{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})$, which is impossible. Hence, $\lambda_1(\mathbf{L_i}) \le \|\pi_i(\mathbf{v}_t)\| \le \lambda_i(\mathbf{L})$.

LEMMA 3.7. (1) *If* $\mathbf{b}_1, \dots, \mathbf{b}_n$ *is a slide reduced basis, then so is* $\pi_{lk+1}(\mathbf{b}_{lk+1}), \dots, \pi_{lk+1}(\mathbf{b}_{qk})$ *for* $0 \le l < q \le p$.

(2) *If* $\mathbf{b}_1, \dots, \mathbf{b}_k$ *is an HKZ-reduced basis, then so is* $\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_j)$ *for* $1 \le i \le j \le k$.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

This follows easily from $(\pi_i(\mathbf{b}_l))^* = \mathbf{b}_l^*$, $\langle \pi_i(\mathbf{b}_q), (\pi_i(\mathbf{b}_l))^* \rangle / \langle (\pi_i(\mathbf{b}_l))^*, (\pi_i(\mathbf{b}_l))^* \rangle = \langle \mathbf{b}_q, \mathbf{b}_l^* \rangle / \langle \mathbf{b}_l^*, \mathbf{b}_l^* \rangle$ for $1 \le i \le l \le q$, where $(\pi_i(\mathbf{b}_l))^*$ denotes the component of $\pi_i(\mathbf{b}_l)$ which is orthogonal to $\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}), \ldots, \pi_i(\mathbf{b}_{l-1})$. This is a property of forward (backward) shrinkage. The same properties hold for an LLL-reduced basis [12], a k-BKZ-reduced basis [19], a semi block $2k$-reduced basis [19], a semi k-reduced basis [19] and a $2k$-Block-Rankin-reduced basis [6]. Furthermore, the reversed dual basis has the aforesaid property.

LEMMA 3.8. *If the block $\mathbf{B}_{[ik+2,ik+k+1]}$ is $(1+\varepsilon)$-DSVP-reduced, that is, $\mathbf{B}^{-s}_{[ik+2,ik+k+1]}$ is $(1+\varepsilon)$-SVP-reduced, then $\mathbf{B}_{[ik+l,ik+k+1]}$ is also $(1+\varepsilon)$-DSVP-reduced for $2 \le l \le k$. Hence,*

$$\mathrm{vol}(\mathbf{B}_{[ik+l,ik+k+1]}) \le ((1+\varepsilon)\cdot\gamma_{k-l+2})^{(k-l+2)/2} \|\mathbf{b}^*_{ik+k+1}\|^{k-l+2}. \tag{3.4}$$

PROOF. Given a vector $\mathbf{b} = (b_1, b_2, \ldots, b_m)^t$, we denote $\overline{\mathbf{b}} = (b_m, b_{m-1}, \ldots, b_1)^t$. Let $\mathbf{B}_{[ik+2,ik+k+1]} = (\mathbf{d}_2, \ldots, \mathbf{d}_{k+1})$ and

$$\mathbf{B}^{-t}_{[ik+2,ik+k+1]} \triangleq \mathbf{B}_{[ik+2,ik+k+1]}(\mathbf{B}^t_{[ik+2,ik+k+1]}\mathbf{B}_{[ik+2,ik+k+1]})^{-1} = (\mathbf{c}_2, \ldots, \mathbf{c}_{k+1}),$$

where $\mathbf{d}_l, \mathbf{c}_l \in \mathbb{R}^m$. Then

$$\mathbf{d}_l^t \cdot \mathbf{c}_j = \delta_{l,j}, \quad 2 \le l, \quad j \le k+1, \tag{3.5}$$

and $\mathbf{B}^{-s}_{[ik+2,ik+k+1]} = \mathbf{R}_m\mathbf{B}^{-t}_{[ik+2,ik+k+1]}\mathbf{R}_k = (\overline{\mathbf{c}}_{k+1}, \ldots, \overline{\mathbf{c}}_2)$. Since $\mathbf{B}^{-s}_{[ik+2,ik+k+1]}$ is $(1+\varepsilon)$-SVP-reduced, we have $\|\overline{\mathbf{c}}_{k+1}\| \le \sqrt{1+\varepsilon}\lambda_1(\mathbf{L}(\overline{\mathbf{c}}_{k+1}, \ldots, \overline{\mathbf{c}}_2))$. From (3.5), we easily get the right inverse of $\mathbf{B}^t_{[ik+l,ik+k+1]}$: $\mathbf{B}^{-t}_{[ik+l,ik+k+1]} = (\mathbf{c}_l, \ldots, \mathbf{c}_{k+1})$ for $2 \le l \le k$. Then $\mathbf{B}^{-s}_{[ik+l,ik+k+1]} = \mathbf{R}_m\mathbf{B}^{-t}_{[ik+l,ik+k+1]}\mathbf{R}_{k-l+2} = (\overline{\mathbf{c}}_{k+1}, \ldots, \overline{\mathbf{c}}_l)$. Consequently, $\|\overline{\mathbf{c}}_{k+1}\| \le \sqrt{1+\varepsilon}\lambda_1(\mathbf{L}(\overline{\mathbf{c}}_{k+1}, \ldots, \overline{\mathbf{c}}_2)) \le \sqrt{1+\varepsilon}\lambda_1(\mathbf{L}(\overline{\mathbf{c}}_{k+1}, \ldots, \overline{\mathbf{c}}_l))$, that is $\mathbf{B}_{[ik+l,ik+k+1]}$ is $(1+\varepsilon)$-DSVP-reduced for $2 \le l \le k$. □

PROPOSITION 3.9. *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a slide reduced basis of a lattice $\mathbf{L}$ with blocksize k and factor $\varepsilon \ge 0$, where $n = pk$. Then, for $l = 0, \ldots, p-2$ and $l+1 \le q \le p-1$,*

$$\|\mathbf{b}^*_{lk+j}\| \le (\gamma_{k-j+1}\sqrt{1+\varepsilon})^{(k-j+1)/(k-j)}(\gamma_k\sqrt{1+\varepsilon})^{(q-l-1)k/(k-1)}\|\mathbf{b}^*_{qk+1}\|, \quad j = 1, \ldots, k-1, \tag{3.6}$$

$$\|\mathbf{b}^*_{lk+k}\| \le \gamma_2(1+\varepsilon)(\gamma_k\sqrt{1+\varepsilon})^{(q-l-1)k/(k-1)}\|\mathbf{b}^*_{qk+1}\|. \tag{3.7}$$

In particular, $\|\mathbf{b}^*_{lk+1}\| \le (\gamma_k\sqrt{1+\varepsilon})^{(q-l)k/(k-1)}\|\mathbf{b}^*_{qk+1}\|$, for $0 \le l \le q \le p-1$.

PROOF. Since $\mathbf{B}_{[lk+1,lk+k]}$ is HKZ-reduced, $\mathbf{B}_{[lk+j,lk+k]}$ is SVP-reduced for $j \in [1, k-1]$. This implies $\|\mathbf{b}^*_{lk+j}\| \le \gamma^{1/2}_{k-j+1}\,\mathrm{vol}(\mathbf{B}_{[lk+j,lk+k]})^{1/(k-j+1)}$, which is equivalent to

$$\|\mathbf{b}^*_{lk+j}\|^{k-j} \le \gamma^{(k-j+1)/2}_{k-j+1}\,\mathrm{vol}(\mathbf{B}_{[lk+j+1,lk+k]}). \tag{3.8}$$

From Lemma 3.8, by eliminating $\|\mathbf{b}^*_{lk+k+1}\|$ on the left-hand side of (3.4), this yields

$$\mathrm{vol}(\mathbf{B}_{[lk+j+1,lk+k]}) \le ((1+\varepsilon)\cdot\gamma_{k-j+1})^{(k-j+1)/2}\|\mathbf{b}^*_{lk+k+1}\|^{k-j}. \tag{3.9}$$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

Combining (3.8) with (3.9), we obtain $\|\mathbf{b}^*_{lk+j}\| \le (\gamma_{k-j+1}\sqrt{1+\varepsilon})^{(k-j+1)/(k-j)}\|\mathbf{b}^*_{lk+k+1}\|$. In particular, this yields $\|\mathbf{b}^*_{lk+k+1}\| \le (\gamma_k\sqrt{1+\varepsilon})^{(q-l-1)k/(k-1)}\|\mathbf{b}^*_{qk+1}\|$. Putting the above two formulas together, we obtain (3.6). Setting $j = k-1$ in (3.9), we get $\|\mathbf{b}^*_{lk+k}\| \le \gamma_2(1+\varepsilon)\|\mathbf{b}^*_{lk+k+1}\|$, which implies (3.7). □

THEOREM 3.10. *Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a slide reduced basis of a lattice $\mathbf{L}$ with blocksize k and factor $\varepsilon \ge 0$, where $n = pk$.*

(1) *For $l = 0, \dots, p-2$,*

$$\|\mathbf{b}^*_{lk+j}\| \le (\gamma_{k-j+1}\sqrt{1+\varepsilon})^{(k-j+1)/(k-j)}(\gamma_k\sqrt{1+\varepsilon})^{(p-l-2)k/(k-1)}\lambda_{lk+j}(\mathbf{L}),\ 1 \le j \le k-1,$$
$$\|\mathbf{b}^*_{lk+k}\| \le \gamma_2(1+\varepsilon)(\gamma_k\sqrt{1+\varepsilon})^{(p-l-2)k/(k-1)}\lambda_{lk+k}(\mathbf{L}).$$

(2) $\|\mathbf{b}^*_{(p-1)k+j}\|/\lambda_{(p-1)k+j}(\mathbf{L}) \le 1,\ 1 \le j \le k-1.$

PROOF. (1) Let u be the shortest vector of $\mathbf{L}_{lk+j}$. Then u can be written as $u = \sum_{i=lk+j}^{\kappa} \alpha_i \pi_{lk+j}(\mathbf{b}_i)$, where $\alpha_\kappa \ne 0$. If $\kappa \le (l+1)k$, then $\|\mathbf{b}^*_{lk+j}\| = \|u\| = \lambda_1(\mathbf{L}_{lk+j})$. If $\kappa > (l+1)k$, then $\pi_{qk+1}(u)$ is a nonzero vector of $\mathbf{L}(\mathbf{B}_{[qk+1,qk+k]})$, where $q = \lfloor(\kappa-1)/k\rfloor$. Since $\mathbf{B}_{[qk+1,qk+k]}$ is HKZ-reduced, $\|\mathbf{b}^*_{qk+1}\| \le \|\pi_{qk+1}(u)\| \le \|u\| = \lambda_1(\mathbf{L}_{lk+j})$. Therefore, $\|\mathbf{b}^*_{lk+j}\|/\lambda_{lk+j}(\mathbf{L}) \le \|\mathbf{b}^*_{lk+j}\|/\|\mathbf{b}^*_{qk+1}\|$, which completes the proof by Proposition 3.9 since $q \le p-1$.

(2) Since $\mathbf{B}_{[(p-1)k+1,n]}$ is HKZ-reduced, the claim holds by Lemma 3.6. □

THEOREM 3.11. *Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a slide reduced basis of a lattice $\mathbf{L}$ with blocksize k and factor ε, where $n = pk$, and $\gamma = \max\{\gamma_i : 2 \le i \le k\}$. Then for $1 \le j \le k$*

$$\frac{\|\mathbf{b}_{lk+j}\|^2}{\lambda_{lk+j}(\mathbf{L})^2} \le \left(\frac{lk+j+3}{3} - \frac{l}{12}\right)(1+\varepsilon)^{(n-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}, \quad 0 \le l \le p-2,$$
$$\frac{\|\mathbf{b}_{(p-1)k+j}\|^2}{\lambda_{(p-1)k+j}(\mathbf{L})^2} \le \frac{j+3}{4} + \left(\frac{(p-1)k}{3} - \frac{p-1}{12}\right)(1+\varepsilon)^{(n-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}.$$

PROOF. For simplicity, we denote $\lambda_i(\mathbf{L})$ by λ_i. By Mordell's inequality $\gamma_n \le \gamma_k^{(n-1)/(k-1)}$ for $2 \le k \le n$, so the sequence $(\gamma_i^{1/(i-1)})_{i\ge 2}$ decreases. Consequently,

$$(\gamma_{k-j+1}\sqrt{1+\varepsilon})^{2(k-j+1)/(k-j)} \le (1+\varepsilon)^2\gamma_2^2\gamma^2, \quad j = 1, \dots, k-1. \tag{3.10}$$

By Theorem 3.10, together with the facts $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n$ and $\mu_{i,j}^2 \le \frac{1}{4}$, we have the following.

(1) For $l = 0, \dots, p-2$, $j = 1, \dots, k-1$,

$$\|\mathbf{b}_{lk+j}\|^2 = \|\mathbf{b}^*_{lk+j}\|^2 + \sum_{h=1}^{lk+j-1} \mu_{lk+j,h}^2\|\mathbf{b}^*_h\|^2$$
$$= \|\mathbf{b}^*_{lk+j}\|^2 + \sum_{t=0}^{l-1}\sum_{q=1}^{k-1} \mu_{lk+j,tk+q}^2\|\mathbf{b}^*_{tk+q}\|^2 + \sum_{t=1}^{l} \mu_{lk+j,tk}^2\|\mathbf{b}^*_{tk}\|^2 + \sum_{q=1}^{j-1} \mu_{lk+j,lk+q}^2\|\mathbf{b}^*_{lk+q}\|^2$$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

$$\begin{aligned}
&\le (\gamma_{k-j+1}\sqrt{1+\varepsilon})^{2(k-j+1)/(k-j)}(\gamma_k\sqrt{1+\varepsilon})^{2(p-l-2)k/(k-1)}\lambda_{lk+j}^2\\
&\quad+\frac{1}{4}\sum_{t=0}^{l-1}\sum_{q=1}^{k-1}(\gamma_{k-q+1}\sqrt{1+\varepsilon})^{2(k-q+1)/(k-q)}(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-2)k/(k-1)}\lambda_{tk+q}^2\\
&\quad+\frac{1}{4}\sum_{t=1}^{l}\gamma_2^2(1+\varepsilon)^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-1)k/(k-1)}\lambda_{tk}^2\\
&\quad+\frac{1}{4}\sum_{q=1}^{j-1}(\gamma_{k-q+1}\sqrt{1+\varepsilon})^{2(k-q+1)/(k-q)}(\gamma_k\sqrt{1+\varepsilon})^{2(p-l-2)k/(k-1)}\lambda_{lk+q}^2\\
&\le\Big((1+\varepsilon)^2\gamma_2^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-l-2)k/(k-1)}\\
&\quad+\frac{1}{4}\sum_{t=0}^{l-1}\sum_{q=1}^{k-1}(1+\varepsilon)^2\gamma_2^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-2)k/(k-1)}\\
&\quad+\frac{1}{4}\sum_{t=1}^{l}\gamma_2^2(1+\varepsilon)^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-1)k/(k-1)}\\
&\quad+\frac{1}{4}\sum_{q=1}^{j-1}(1+\varepsilon)^2\gamma_2^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-l-2)k/(k-1)}\Big)\lambda_{lk+j}^2\\
&\le(1+\varepsilon)^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-2)k/(k-1)}\Big(\gamma_2^2+\frac{l(k-1)}{4}\gamma_2^2+\frac{l}{4}+\frac{j-1}{4}\gamma_2^2\Big)\lambda_{lk+j}^2\\
&=\Big(\frac{lk+j+3}{3}-\frac{l}{12}\Big)(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}\lambda_{lk+j}^2.
\end{aligned}$$

(2) Similarly, for $l=0,\dots,p-2$, $j=k$,

$$\begin{aligned}
\|\mathbf{b}_{lk+k}\|^2&\le(1+\varepsilon)^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-2)k/(k-1)}\Big(1+\frac{(l+1)(k-1)}{4}\gamma_2^2+\frac{l}{4}\Big)\lambda_{lk+k}^2\\
&=\Big(\frac{lk+k+2}{3}-\frac{l}{12}\Big)(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}\lambda_{lk+k}^2.
\end{aligned}$$

For $l=p-1$, $j=1,\dots,k$,

$$\begin{aligned}
\|\mathbf{b}_{(p-1)k+j}\|^2&\le\frac{j+3}{4}\lambda_{(p-1)k+j}^2+\frac{p-1}{4}(1+\varepsilon)^2\\
&\quad\times\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-2)k/(k-1)}((k-1)\gamma_2^2+1)\lambda_{(p-1)k+j}^2\\
&=\Big(\frac{j+3}{4}+\Big(\frac{(p-1)k}{3}-\frac{p-1}{12}\Big)\\
&\quad\times(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}\Big)\lambda_{(p-1)k+j}^2.
\end{aligned}$$

This completes the proof. □

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

THEOREM 3.12. *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a slide reduced basis of a lattice $\mathbf{L}$ with blocksize k and factor ε, where $n = pk$. Then*

$$\frac{\lambda_{lk+j}^2}{\|\mathbf{b}_{lk+j}\|^2} \le \frac{lk+j+3}{3}(1+\varepsilon)^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(l-1)k/(k-1)}, \quad 1 \le lk+j \le n.$$

PROOF. By definition of $\lambda_i = \lambda_i(\mathbf{L})$,

$$\lambda_{lk+j}^2 \le \max\{\|\mathbf{b}_w\|^2 : w = 1, \ldots, lk+j\}.$$

It follows from $\|\mathbf{b}_{lk+j}\|^2 = \|\mathbf{b}_{lk+j}^*\|^2 + \sum_{h=1}^{lk+j-1} \mu_{lk+j,h}^2\|\mathbf{b}_h^*\|^2$ that

$$\lambda_{lk+j}^2 \le \frac{lk+j+3}{4}\max\{\|\mathbf{b}_w^*\|^2 : w = 1, \ldots, lk+j\}. \tag{3.11}$$

Since $\mathbf{B}_{[lk+1,lk+j]}$ is HKZ-reduced,

$$\|\mathbf{b}_{lk+q}^*\| \le \|\pi_{lk+q}(\mathbf{b}_{lk+j})\| \le \|\mathbf{b}_{lk+j}\|, \quad \text{for } q = 1, \ldots, j. \tag{3.12}$$

For $t = 0, \ldots, l-1$, by Proposition 3.9 and (3.12),

$$\|\mathbf{b}_{tk+q}^*\| \le (\gamma_{k-q+1}\sqrt{1+\varepsilon})^{(k-q+1)/(k-q)}(\gamma_k\sqrt{1+\varepsilon})^{(l-t-1)k/(k-1)}\|\mathbf{b}_{lk+j}\|, \quad 1 \le q \le k-1, \tag{3.13}$$

$$\|\mathbf{b}_{tk+k}^*\| \le \gamma_2(1+\varepsilon)(\gamma_k\sqrt{1+\varepsilon})^{(l-t-1)k/(k-1)}\|\mathbf{b}_{lk+j}\|. \tag{3.14}$$

From (3.12)–(3.14), together with (3.10), we obtain

$$\|\mathbf{b}_w^*\| \le (1+\varepsilon)\gamma_2\gamma(\gamma_k\sqrt{1+\varepsilon})^{(l-1)k/(k-1)}\|\mathbf{b}_{lk+j}\|, \quad \text{for } w = 1, \ldots, lk+j.$$

Hence, together with (3.11), we complete the proof of Theorem 3.12. □

From the perspective of the proof of Theorem 3.11, the upper bounds for the ratios $\|\mathbf{b}_i\|/\lambda_i(\mathbf{L})$ are somewhat loose. Hence, it may be better to use Theorem 3.11 to estimate the lower bound of $\lambda_i(\mathbf{L})$. The main Theorem 3.5 consists of Theorems 3.10–3.12.

4. Generalised slide reduction and several applications

4.1. Generalised slide reduction. The original slide reduction proposed by Gama and Nguyen [8] claims that the rank of lattices is an exact multiple of the blocksize. We extend the notion to lattices of any rank as follows.

DEFINITION 4.1 (Forward generalised slide reduction). A basis $\mathbf{B}$ of an n-rank lattice $\mathbf{L}$, where $n = (p-1)k + r$ for $1 \le r \le k$, is forward generalised slide reduced with blocksize k and factor $\varepsilon \ge 0$ if it is size-reduced and satisfies the following two sets of conditions:

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

(1) primal conditions: the blocks $\mathbf{B}_{[1,r]}$ and $\mathbf{B}_{[ik+r+1,ik+k+r]}$ for $i \in [0, p-2]$ are HKZ-reduced;
(2) dual conditions: the blocks $\mathbf{B}_{[2,r+1]}$ and $\mathbf{B}_{[ik+r+2,ik+k+r+1]}$ for $i \in [0, p-3]$ are $(1+\varepsilon)$-DSVP-reduced.

Definition 4.2 (Backward generalised slide reduction). A basis $\mathbf{B}$ of an n-rank lattice $\mathbf{L}$, where $n = (p-1)k + r$ for $1 \le r \le k$, is backward generalised slide reduced with blocksize k and factor $\varepsilon \ge 0$ if it is size-reduced and satisfies the following two sets of conditions:

(1) primal conditions: the blocks $\mathbf{B}_{[ik+1,ik+k]}$ for $i \in [0, p-2]$ and $\mathbf{B}_{[(p-1)k+1,n]}$ are HKZ-reduced;
(2) dual conditions: the blocks $\mathbf{B}_{[ik+2,ik+k+1]}$ for $i \in [0, p-2]$ are $(1+\varepsilon)$-DSVP-reduced.

Thus, the blocksize of slide reduction is not limited to the divisors of the rank. Similar to the original slide reduction, we have the following theorem.

Theorem 4.3. (1) *A forward generalised slide reduced basis* $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^m$ *of a lattice* $\mathbf{L}$ *with blocksize* k *and factor* $\varepsilon \ge 0$, *where* $n = (p-1)k + r$ *for* $1 \le r \le k$, *satisfies*

$$\|\mathbf{b}_1\| \le (\gamma_r \sqrt{1+\varepsilon})^{r(2n-r-1)/2n(r-1)} (\gamma_k \sqrt{1+\varepsilon})^{(n-r)(n-r-1)/2n(k-1)} \operatorname{vol}(\mathbf{L})^{1/n},$$
$$\|\mathbf{b}_1\| \le (\gamma_r \sqrt{1+\varepsilon})^{r/(r-1)} (\gamma_k (1+\varepsilon))^{(p-2)k/(k-1)} \lambda_1(\mathbf{L}).$$

(2) *A backward generalised slide reduced basis* $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^m$ *of a lattice* $\mathbf{L}$ *with blocksize* k *and factor* $\varepsilon \ge 0$, *where* $n = (p-1)k + r$ *for* $1 \le r \le k$, *satisfies*

$$\|\mathbf{b}_1\| \le (\gamma_k (1+\varepsilon))^{(pk-1)/2(k-1)} \left(\frac{\gamma_r}{\gamma_k}\right)^{r/2n} \operatorname{vol}(\mathbf{L})^{1/n},$$
$$\|\mathbf{b}_1\| \le (\gamma_k (1+\varepsilon))^{(p-1)k/(k-1)} \lambda_1(\mathbf{L}).$$

In particular, the case $r = k$ of Theorem 4.3 is consistent with Theorem 3.4.

Corollary 4.4. *Given* $n = (p-1)k + r > k$ *for* $1 \le r \le k$, *Hermite's constant* γ_n *satisfies*

$$\gamma_n \le \min\left\{ \gamma_r^{r(2n-r-1)/n(r-1)} \gamma_k^{(n-r)(n-r-1)/n(k-1)}, \gamma_k^{(pk-1)/(k-1)} \left(\frac{\gamma_r}{\gamma_k}\right)^{r/n} \right\}.$$

Clearly, the slide reduction algorithm [8] also applies to generalised slide reduction. Furthermore, all properties of slide reduction can be generalised to generalised slide reduction.

4.2. Approximate *i*-SIVP and SMP. Theorems 3.4 and 3.5 suggest that slide reduction can not only approximate SVP in polynomial time, but also approximate i-SIVP and SMP well. Specifically, we obtain the following theorem.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

THEOREM 4.5. *Given $k = O(\log n/\log\log n)$, $n = pk$, and a factor $\varepsilon > 0$, there exists a polynomial time algorithm that on input a basis of a lattice $\mathbf{L}$, outputs a basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ satisfying*

$$\max_{1\le j\le i} \|\mathbf{b}_j\| \le \sqrt{\frac{i+3}{3} - \frac{1}{12}\left\lceil \frac{i}{k}\right\rceil}(1+\varepsilon)^{(pk-2)/2(k-1)}\gamma\gamma_k^{(n-2k)/(k-1)}\lambda_i(\mathbf{L}), \quad 1 \le i \le n,$$

$$\|\mathbf{b}_j\| \le \sqrt{\frac{n+3}{3} - n/(12k)}(1+\varepsilon)^{(pk-2)/2(k-1)}\gamma\gamma_k^{(n-2k)/(k-1)}\lambda_j(\mathbf{L}), \quad j = 1, \dots, n.$$

PROOF. Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be a slide reduced basis with blocksize k and factor ε. It follows from Theorem 3.11 that the assertion holds. □

REMARK 4.1. Our new result is currently the best in approximating i-SIVP and SMP with polynomial complexity.

4.3. Approximate CVP. Babai [2] showed that, given a lattice $\mathbf{L}$ and a point $\mathbf{x} \in \mathrm{span}(\mathbf{L})$, one can use LLL reduction to find a point $\mathbf{v} \in \mathbf{L}$ satisfying $\|\mathbf{x}-\mathbf{v}\|^2 \le 2^{n/2}\min_{\mathbf{u}\in\mathbf{L}}\|\mathbf{x}-\mathbf{u}\|^2$. Schnorr [20] showed that a k-BKZ basis can be used to find a point $\mathbf{v} \in \mathbf{L}$ satisfying $\|\mathbf{x}-\mathbf{v}\|^2 \le n\gamma_k^{2(n-1)/(k-1)}\min_{\mathbf{u}\in\mathbf{L}}\|\mathbf{x}-\mathbf{u}\|^2$. Note that the LLL reduction algorithm is polynomial, but the factor $2^{n/2}$ is exponential in n; Schnorr [20] obtained an improved factor $n\gamma_k^{2(n-1)/(k-1)}$, but no polynomial time algorithm is known for k-BKZ reduction. In this section, we use slide reduction, which is polynomial, to improve the approximate factor.

THEOREM 4.6. *Given an integer lattice $\mathbf{L}$ of rank n, a point $\mathbf{x} \in \mathrm{span}(\mathbf{L})$, $k = O(\log n/\log\log n)$ and a factor $\varepsilon > 0$, there exists a polynomial time algorithm that on input of a basis of the lattice $\mathbf{L}$, outputs a lattice vector $\mathbf{v}$ satisfying*

$$\|\mathbf{x}-\mathbf{v}\|^2 \le C_{n,k,\varepsilon}\min_{\mathbf{u}\in\mathbf{L}}\|\mathbf{x}-\mathbf{u}\|^2,$$

where $C_{n,k,\varepsilon} = ((4n+3k)/3)(1+\varepsilon)^{(\lceil n/k\rceil k-2)/(k-1)}\gamma^2\gamma_k^{2(\lceil n/k\rceil-2)k/(k-1)}$.

PROOF. Set $n = (p-1)k + r$, where $1 \le r \le k$. Clearly, $C_{n,k,\varepsilon}$ is monotonously increasing in n and $C_{n,k,\varepsilon} \ge 1$ for $n > k \ge 1$. Let $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{Z}^m$ be a backward generalised slide reduced basis of $\mathbf{L}$ with blocksize k and factor $\varepsilon \ge 0$, whose Gram-Schmidt orthogonalisation is $\mathbf{b}_1^* = \mathbf{b}_1$, $\mathbf{b}_i^* = \mathbf{b}_i^* - \sum_{j=1}^{i-1}\mu_{i,j}\mathbf{b}_j^*$, for $i = 2, \dots, n$. Then let $\mathbf{x} = \sum_{i=1}^n x_i\mathbf{b}_i^*$. Suppose that $\|\mathbf{b}_\beta^*\| = \max(\|\mathbf{b}_{(p-1)k+1}^*\|, \dots, \|\mathbf{b}_n^*\|)$, $(p-1)k+1 \le \beta \le n$. Let $\mathbf{v} = \sum_{j=1}^n v_j\mathbf{b}_j$ be a lattice point such that $\sum_{j=\beta}^n |x_j - \sum_{i=j}^n v_i\mu_{i,j}|^2\|\mathbf{b}_j^*\|^2$ is minimal for all $v_\beta, \dots, v_n \in \mathbb{Z}$ and $v_j = \lceil x_j - \sum_{i=j+1}^n v_i\mu_{i,j}\rfloor$ for $j = \beta-1, \dots, 1$. Clearly, $\mathbf{v} = \sum_{j=1}^n(\sum_{i=j}^n v_i\mu_{i,j})\mathbf{b}_j^*$. By the construction of $\mathbf{v}$,

$$\|\mathbf{x}-\mathbf{v}\|^2 = \sum_{j=1}^n\left|x_j - \sum_{i=j}^n v_i\mu_{i,j}\right|^2\|\mathbf{b}_j^*\|^2 \le \frac{1}{4}\sum_{j=1}^n\|\mathbf{b}_j^*\|^2.$$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

From Proposition 3.9 and (3.10),

$$\begin{aligned}
\sum_{j=1}^{n}\|\mathbf{b}_j^*\|^2 &= \sum_{t=0}^{p-2}\sum_{q=1}^{k-1}\|\mathbf{b}_{tk+q}^*\|^2 + \sum_{t=1}^{p-1}\|\mathbf{b}_{tk}^*\|^2 + \sum_{q=1}^{r}\|\mathbf{b}_{(p-1)k+q}^*\|^2\\
&\le \sum_{t=0}^{p-2}\sum_{q=1}^{k-1}(\gamma_{k-q+1}\sqrt{1+\varepsilon})^{2(k-q+1)/(k-q)}(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-2)k/(k-1)}\|\mathbf{b}_{(p-1)k+1}^*\|^2\\
&\quad + \sum_{t=1}^{p-1}\gamma_2^2(1+\varepsilon)^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-1)k/(k-1)}\|\mathbf{b}_{(p-1)k+1}^*\|^2 + \sum_{q=1}^{r}\|\mathbf{b}_{(p-1)k+q}^*\|^2\\
&\le \Bigg(\sum_{t=0}^{p-2}\sum_{q=1}^{k-1}(1+\varepsilon)^2\gamma_2^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-2)k/(k-1)}\\
&\quad + \sum_{t=1}^{p-1}\gamma_2^2(1+\varepsilon)^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-t-1)k/(k-1)} + r\Bigg)\|\mathbf{b}_\beta^*\|^2\\
&\le \Bigg((p-1)\Bigg((k-1)(1+\varepsilon)^2\gamma_2^2\gamma^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-2)k/(k-1)}\\
&\quad + \gamma_2^2(1+\varepsilon)^2(\gamma_k\sqrt{1+\varepsilon})^{2(p-2)k/(k-1)}\Bigg) + r\Bigg)\|\mathbf{b}_\beta^*\|^2\\
&\le ((p-1)(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}((k-1)\gamma_2^2+1)+r)\|\mathbf{b}_\beta^*\|^2\\
&\le \frac{4pk-k-p+1}{3}(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}\|\mathbf{b}_\beta^*\|^2.
\end{aligned}$$

This yields

$$\|\mathbf{x}-\mathbf{v}\|^2 \le \frac{4pk-(k+p)+1}{3}(1+\varepsilon)^{(pk-2)/(k-1)}\gamma^2\gamma_k^{2(p-2)k/(k-1)}\frac{\|\mathbf{b}_\beta^*\|^2}{4}. \tag{4.1}$$

Then, we define the hyperplane $\mathbf{H}_c = c\mathbf{b}_n^* + \operatorname{span}(\mathbf{b}_1,\dots,\mathbf{b}_{n-1})$. Thus, $\mathbf{L}\subset\bigcup_{c\in\mathbb{Z}}\mathbf{H}_c$, $\mathbf{v}\in\mathbf{H}_{v_n}$ and the distance of $\mathbf{H}_c$ and $\mathbf{H}_{c+1}$ is $\|\mathbf{b}_n^*\|$. Let $\mathbf{u}\in\mathbf{L}$ be the lattice point that is nearest to $\mathbf{x}$. Following Babai, we consider two cases:

• *Case 1.* $\mathbf{u}\in\mathbf{H}_{v_n}$, that is, $\mathbf{u}-\mathbf{v}\in\mathbf{L}(\mathbf{b}_1,\dots,\mathbf{b}_{n-1})$. Then $\mathbf{u}-v_n\mathbf{b}_n$ is a nearest lattice point to $\mathbf{x}'-v_n\mathbf{b}_n$ in $\mathbf{L}(\mathbf{b}_1,\dots,\mathbf{b}_{n-1})$, where $\mathbf{x}'=\sum_{i=1}^{n-1}x_i\mathbf{b}_i^*+v_n\mathbf{b}_n^*\in\mathbf{H}_{v_n}$. Consequently, by induction on n,

$$\begin{aligned}
\|\mathbf{x}'-\mathbf{v}\|^2 &= \|(\mathbf{x}'-v_n\mathbf{b}_n)-(\mathbf{v}-v_n\mathbf{b}_n)\|^2 \le C_{n-1,k,\varepsilon}\|(\mathbf{x}'-v_n\mathbf{b}_n)-(\mathbf{u}-v_n\mathbf{b}_n)\|^2\\
&= C_{n-1,k,\varepsilon}\|\mathbf{x}'-\mathbf{u}\|^2 = C_{n-1,k,\varepsilon}(\|\mathbf{x}-\mathbf{u}\|^2-\|\mathbf{x}-\mathbf{x}'\|^2).
\end{aligned}$$

This implies that

$$\begin{aligned}
\|\mathbf{x}-\mathbf{v}\|^2 &= \|\mathbf{x}-\mathbf{x}'\|^2+\|\mathbf{x}'-\mathbf{v}\|^2\\
&\le C_{n-1,k,\varepsilon}\|\mathbf{x}-\mathbf{u}\|^2+(1-C_{n-1,k,\varepsilon})\|\mathbf{x}-\mathbf{x}'\|^2\\
&\le C_{n,k,\varepsilon}\|\mathbf{x}-\mathbf{u}\|^2.
\end{aligned}$$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

• *Case 2.* $\mathbf{u} \notin \mathbf{H}_{v_n}$, that is, $\mathbf{u} - \mathbf{v} \notin \mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$. It follows from the construction of $\mathbf{v}$ that $\pi_\beta(\mathbf{v})$ is the nearest lattice point to $\pi_\beta(\mathbf{x})$ in $\mathbf{L}_\beta$. Note that $\pi_\beta(\mathbf{v}) \neq \pi_\beta(\mathbf{u})$ and they are all in $\mathbf{L}_\beta$, which implies that

$$\|\pi_\beta(\mathbf{x}) - \pi_\beta(\mathbf{u})\| \geq \frac{\lambda_1(\mathbf{L}_\beta)}{2}.$$

Since $\pi_\beta(\mathbf{b}_\beta), \ldots, \pi_\beta(\mathbf{b}_n)$ is HKZ-reduced, we obtain

$$\|\mathbf{x} - \mathbf{u}\|^2 \geq \|\pi_\beta(\mathbf{x}) - \pi_\beta(\mathbf{u})\|^2 \geq \frac{\lambda_1(\mathbf{L}_\beta)^2}{4} = \frac{\|\mathbf{b}_\beta^*\|^2}{4}.$$

Hence, it follows from (4.1) that

$$\|\mathbf{x} - \mathbf{v}\|^2 \leq \frac{4pk - k - p + 1}{3}(1+\varepsilon)^{(pk-2)/(k-1)}\gamma_2^2\gamma_k^{2(p-2)k/(k-1)}\|\mathbf{x} - \mathbf{u}\|^2 \leq C_{n,k,\varepsilon}\|\mathbf{x} - \mathbf{u}\|^2.$$

Algorithm and complexity. A backward generalised slide reduced basis with blocksize k and factor $\varepsilon > 0$ can be computed in polynomial time from an arbitrary basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$ by the slide reduction algorithm (see [8, Algorithm 1]). Then, we enumerate at most $k^{O(k)}$ lattice vectors close to $\mathbf{x}$ and find integers $v_\beta, \ldots, v_n$ that minimise $\sum_{j=\beta}^n |x_j - \sum_{i=j}^n v_i\mu_{i,j}|^2\|\mathbf{b}_j^*\|^2$. Finally, we compute $v_j = \lceil x_j - \sum_{i=j+1}^n v_i\mu_{i,j}\rfloor$ for $j = \beta - 1, \ldots, 1$ (this is the nearest plane algorithm of Babai [2]). If $k = O(\log n/\log\log n)$, we obtain the lattice vector $\mathbf{v} = \sum_{j=1}^n v_j\mathbf{b}_j$ with polynomial arithmetic operations. □

Note that $C_{n,k,\varepsilon} \approx (4/3)n\gamma_k^{2(n-k-1)/(k-1)} \leq (4/3)^{(n-k)/2}n$, so our new result is better than the previous results.

4.4. The number of slide reduced bases. Clearly, a slide reduced basis with blocksize k and factor $\sqrt{3/2} - 1$ is an LLL-reduced basis with factor $1/3$. Micciancio [15] showed that the number of LLL-reduced bases with factor $1/3$ is at most $2^{n^3/6+n^2/2+n/3}$, so we have the following theorem.

THEOREM 4.7. *Any given n-dimensional lattice has at most $2^{n^3/6+n^2/2+n/3}$ slide reduced bases with blocksize k and factor $\sqrt{3/2} - 1$.*

This suggests that the smallest volume problem (see [6] for its definition and further information) can be solved by enumerating all slide reduced bases of the lattice. The details of this, and further consequences for the smallest volume problem, will be given in the full paper.

5. Critical slide reduced basis for blocksize 2

A k-BKZ basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of a lattice $\mathbf{L}$ is *critical* for (k, n) if the value $\|\mathbf{b}_1\|/\lambda_1(\mathbf{L})$ is maximal for all k-BKZ bases of n-rank lattices. Similarly, we call a slide reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ with blocksize k of a lattice $\mathbf{L}$ *critical* for (k, n) if the value $\|\mathbf{b}_1\|/\lambda_1(\mathbf{L})$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

is maximal for all slide reduced bases of n-rank lattices with blocksize k and $\varepsilon = 0$ (denoted by k-slide reduced bases). Bachem and Kannan [3] presented the *critical* 2-BKZ basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Afterwards, Schnorr [20] described a slight variant of the *critical* 2-BKZ basis of Bachem and Kannan [3], which is also a *critical* 2-BKZ basis. We find that Schnorr's variant in [20] forms a *critical* 2-slide reduced basis, whose expression is as follows:

$$\mathbf{A}_n = (\mathbf{b}_1, \ldots, \mathbf{b}_n) = \begin{pmatrix} 1 & \frac{1}{2} & & & & \\ & \rho & \rho/2 & & \mathbf{0} & \\ & & \rho^2 & \rho^2/2 & & \\ & & & \ddots & \ddots & \\ & & & & \ddots & \ddots \\ & & \mathbf{0} & & & \rho^{n-2} \quad \rho^{n-2}/2 \\ & & & & & \rho^{n-1} \end{pmatrix}$$

where $\rho = \sqrt{3/4}$ and $n > 2$. The matrices $\mathbf{A}_n$ satisfy the recursion

$$\mathbf{A}_n = \begin{pmatrix} 1 & \frac{1}{2} & 0 & \cdots & 0 \\ & \cdots & \cdots & \cdots & \cdots \\ 0 & \vdots & & & \\ \vdots & \vdots & & \rho \cdot \mathbf{A}_{n-1} & \\ 0 & \vdots & & & \end{pmatrix}.$$

THEOREM 5.1 (Bachem and Kannan [3]). *The column vectors of the matrix $\mathbf{A}_n$ form a critical 2-BKZ basis.*

LEMMA 5.2. *The column vectors of the matrix $\mathbf{A}_n$ forms a 2-slide reduced basis, where $n > 2$.*

PROOF. Given the matrix $\mathbf{A}_n$, we denote its column vector group by $\mathbf{B}$. Clearly, for $i = 0, \ldots, [(n-3)/2]$

$$\mathbf{B}^t_{[2i+2,2i+3]} = \begin{pmatrix} 0 & \cdots & 0 & \rho^{2i+1} & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \rho^{2i+1}/2 & \rho^{2i+2} & 0 & \cdots & 0 \end{pmatrix},$$

where there are $2i+1$ zeros in front of ρ^{2i+1}. It is easy to get

$$\begin{aligned} \mathbf{B}^{-s}_{[2i+2,2i+3]} &= \mathbf{R}_n \mathbf{B}^{-t}_{[2i+2,2i+3]} \mathbf{R}_2 \\ &= \begin{pmatrix} 0 & \cdots & 0 & \dfrac{1}{\rho^{2i+2}} & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -\dfrac{1}{2\rho^{2i+2}} & \dfrac{1}{\rho^{2i+1}} & 0 & \cdots & 0 \end{pmatrix}^t \triangleq (\mathbf{c}_1, \mathbf{c}_2), \end{aligned}$$

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

where there are $n-2i-3$ zeros before $1/\rho^{2i+2}$. Then, for any $x, y \in \mathbb{Z}$, $x^2+y^2 \neq 0$,

$$\|x\mathbf{c}_1 + y\mathbf{c}_2\| = \frac{1}{\rho^{2i+2}}\sqrt{\left(x-\frac{y}{2}\right)^2 + \frac{3y^2}{4}} \geq \frac{1}{\rho^{2i+2}} = \|\mathbf{c}_1\|.$$

This shows that $\mathbf{B}^{-s}_{[2i+2,2i+3]}$ is SVP-reduced, that is, $\mathbf{B}_{[2i+2,2i+3]}$ is DSVP-reduced. Together with Theorem 5.1, this implies that $\mathbf{B}$ forms a 2-slide reduced basis. □

THEOREM 5.3. *The column vectors of the matrix $\mathbf{A}_n$ form a critical 2-slide reduced basis if n is an even number bigger than 2.*

PROOF. It is easy to see that the vector $\mathbf{b}_n$ is a shortest vector in $\mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) - \mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$, where $\|\mathbf{b}_n\|^2 = \rho^{2n-4}(\rho^2 + 1/4) = (3/4)^{n-2}$. It follows that $\mathbf{b}_n$ is the shortest vector in the lattice $\mathbf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Therefore, $\lambda_1(\mathbf{L})$ satisfies $\|\mathbf{b}_1\|/\lambda_1(\mathbf{L}) = \gamma_2^{n-2}$ and $\|\mathbf{b}_1\|/\operatorname{vol}(\mathbf{L})^{1/n} = \rho^{(1-n)/2} = \gamma_2^{(n-1)/2}$. It follows from Theorem 3.4 and Lemma 5.2 that the claim holds. □

The proof of Theorem 5.3 indicates that the upper bounds of Theorem 3.4 with blocksize 2 are tight, provided that n is an even number bigger than 2 and $\varepsilon = 0$.

Acknowledgements

We are grateful to the anonymous referee for his careful reading and useful comments. We also thank Professor Phong Q. Nguyen for his comments.

References

[1] M. Ajtai, 'Generating hard instances of lattice problems', in: *Complexity of Computations and Proofs*, Vol. 13 of Quaderni di Matematica (ed. J. Krajicek), Seconda Universita di Napoli, 2004, 1–32.
[2] L. Babai, 'On Lovász' lattice reduction and the nearest lattice point problem', *Combinatorica* **6** (1986), 1–13.
[3] A. Bachem and R. Kannan, *Lattices and the Basis Reduction Algorithm, TR* (Carnegie Mellon University, 1984), 22–25.
[4] H. Cohn and N. Elkies, 'New upper bounds on sphere packings I', *Ann. of Math. (2)* **157**(2) (2003), 689–714.
[5] J. Conway and N. Sloane, *Sphere Packings, Lattices and Groups*, 3rd edn (Springer, New York, 1998).
[6] N. Gama, N. Howgrave-Graham, H. Koy and P. Nguyen, 'Rankin's constant and blockwise lattice reduction', in: *Advances in Cryptology-Proceedings of CRYPTO'06*, Lecture Notes in Computer Science, 4117 (Springer, New York, 2006), 112–130.
[7] N. Gama, N. Howgrave-Graham and P. Q. Nguyen, 'Symplectic lattice reduction and NTRU', in: *Proceedings of EUROCRYPT'06*, LNCS, 4004 (Springer, New York, 2006), 233–253.
[8] N. Gama and P. Q. Nguyen, 'Finding short lattice vectors within Mordell's inequality', *Proc. 40th Annual ACM Symposium on Theory of Computing*, New York (2008), 207–216.
[9] R. Kannan, 'Minkowski's convex body theorem and integer programming', *Math. Oper. Res.* **12** (1987), 415–440.
[10] A. Korkine and G. Zolotareff, 'Sur les formes quadratiques', *Math. Ann.* **6** (1873), 366–389.
[11] J. C. Lagarias, H. W. Lenstra Jr and C. P. Schnorr, 'Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice', *Combinatorica* **10** (1990), 333–348.

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press

[12] A. K. Lenstra, H. W. Lenstra Jr and L. Lovász, 'Factoring polynomials with rational coeffcients', *Math. Ann.* **261** (1982), 515–534.
[13] K. Mahler, 'A theorem on inhomogeneous diophantine inequalities', *Nederl. Akad. Wetensch.* **41** (1938), 634–637.
[14] J. Martinet, *Les réseaux parfaits des espaces euclidiens* (Masson, Paris, 1996).
[15] D. Micciancio, 'How many LLL reduced bases are there? Answer 1', http://mathoverflow.net/questions/57021 (7 June 2011).
[16] D. Micciancio and O. Regev, 'Worst-case to average-case reductions based on Gaussian measures', *SIAM J. Comput.* **37**(1) (2007), 267–302.
[17] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms* (Springer, New York, 1973).
[18] O. Regev, 'On lattices, learning with errors, random linear codes, and cryptography', *Proc. 37th Annual ACM Symposium on Theory of Computing*, Baltimore, MD (2005), 84–93.
[19] C. P. Schnorr, 'A hierarchy of polynomial time lattice basis reduction algorithms', *Theoret. Comput. Sci.* **53** (1987), 201–224.
[20] C. P. Schnorr, 'Block Korkin-Zolotarev bases and successive minima', *Combin. Probab. Comput.* **3** (1994), 507–522.
[21] C. P. Schnorr and M. Euchner, 'Lattice basis reduction: improved algorithms and solving subset sum problems', in: *Proceedings of Fundamentals of Computation Theory*, FCT'91 (ed. L. Budach) (Springer LNCS 529, 1991), 68–85.

JIANWEI LI, Institute for Advanced Study, Tsinghua University,
Beijing 100084, PR China
e-mail: lijianwei10@mails.tsinghua.edu.cn

WEI WEI, Institute for Advanced Study, Tsinghua University,
Beijing 100084, PR China
e-mail: wei-wei08@mails.tsinghua.edu.cn

https://doi.org/10.1017/S0004972713000257 Published online by Cambridge University Press