COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 10 (4) (1990) 333–348

KORKIN-ZOLOTAREV BASES AND SUCCESSIVE MINIMA OF A LATTICE AND ITS RECIPROCAL LATTICE

J. C. LAGARIAS, H. W. LENSTRA, JR. and C. P. SCHNORR*

Received June 9, 1986
Revised March 17, 1989

Let $\lambda_i(L)$, $\lambda_i(L^*)$ denote the successive minima of a lattice L and its reciprocal lattice L^*, and let $[\mathbf{b}_1, .\ ., \mathbf{b}_n]$ be a basis of L that is reduced in the sense of Korkin and Zolotarev. We prove that $[4/(i+3)]\lambda_i(L)^2 \leq |\mathbf{b}_i|^2 \leq [(i+3)/4]\lambda_i(L)^2$ and $|\mathbf{b}_i|^2\lambda_{n-i+1}(L^*)^2 \leq [(i+3)/4][(n-i+4)/4]\gamma_n^{*2}$, where $\gamma_n^* = \min\{\gamma_j : 1 \leq j \leq n\}$ and γ_j denotes Hermite's constant. As a consequence the inequalities $1 \leq \lambda_i(L)\lambda_{n-i+1}(L^*) \leq n^2/6$ are obtained for $n \geq 7$. Given a basis B of a lattice L in $\mathbf{R}^m$ of rank n and $\mathbf{x} \in \mathbf{R}^m$, we define polynomial time computable quantities $\lambda(B)$ and $\mu(\mathbf{x}, B)$ that are lower bounds for $\lambda_1(L)$ and $\mu(\mathbf{x}, L)$, where $\mu(\mathbf{x}, L)$ is the Euclidean distance from $\mathbf{x}$ to the closest vector in L. If in addition B is reciprocal to a Korkin-Zolotarev basis of L^*, then $\lambda_1(L) \leq \gamma_n^*\lambda(B)$ and $\mu(\mathbf{x}, L)^2 \leq \left(\sum_{i=1}^n \gamma_i^{*2}\right)\mu(\mathbf{x}, B)^2$.

1. Introduction

The problem of selecting from all bases for a lattice a canonical basis with desirable properties is called *reduction theory.* The classical question motivating the invention of reduction theory is the determination of the minima of positive definite integral quadratic forms. Lagrange [10] developed a reduction theory for binary quadratic forms, and the general study of the higher dimensional case was initiated by Hermite [6] in 1850 and Korkin and Zolotarev [9] in 1873. Several distinct notions of reduction have been studied, including those associated to the names Hermite, Korkin-Zolotarev, Minkowski and Venkov; see [19, 20, 22, 23].

Recently there has been renewed interest in reduction theory arising from the problem of designing computationally efficient algorithms for finding a short vector in a lattice. This was stimulated by a new method in integer programming [12] and by Lovász' lattice basis reduction algorithm, presented in [11], which has had quite a few applications, see [4, 8, 11, 13]. From this computational perspective the most natural of the classical reduction theories to consider is that of Korkin and Zolotarev, because the computational problem of finding a basis of a general lattice reduced in the sense of Korkin and Zolotarev is polynomial time equivalent to the computational problem of finding a shortest non-zero vector in a lattice.

Our object in this paper is to prove inequalities bounding vectors in a Korkin-Zolotarev reduced basis of a lattice L in terms of the successive minima of L and

AMS subject classification (1980): 11 H 06, 11 H 50

*The research of the second author was supported by NSF contract DMS 87-06176. The research of the third author was performed at the University of California, Berkeley, with support from NSF grant 21823, and at AT&T Bell Laboratories.

its reciprocal lattice L^*. Our results can be viewed as giving various senses in which a Korkin-Zolotarev basis of a lattice is nearly orthogonal. Roughly speaking, our bounds improve on classically known bounds by replacing certain constants exponential in the rank n of the lattice involved by constants polynomial in n. In particular we obtain for a lattice L of rank n the inequalities

$$1 \leq \lambda_i(L)\lambda_{n-i+1}(L^*) \leq \frac{1}{6}n^2 \qquad \text{for } 1 \leq i \leq n,$$

valid for $n \geq 7$.

We also study certain quantities $\lambda(B)$ and $\mu(\mathbf{x}, B)$ that are computable in polynomial time given a basis B of a lattice L in $\mathbf{R}^n$ and a vector $\mathbf{x}$ in $\mathbf{R}^n$, which have the properties that $\lambda(B)$ is a lower bound for the length of a shortest non-zero vector in L and $\mu(\mathbf{x}, B)$ is a lower bound for the distance of $\mathbf{x}$ to any vector in L. We show that these lower bounds are quite good when the basis B of L is reciprocal to a Korkin-Zolotarev basis of the reciprocal lattice L^*. These results give some information concerning the computational complexity of recognizing short vectors in a lattice.

2. Statement of results

Let m be a positive integer. We denote by $\langle\ ,\ \rangle$ the Euclidean inner product on $\mathbf{R}^m$ and by $|\ |$ the Euclidean norm, so $|\mathbf{v}|^2 = \sum_{i=1}^m v_i^2$ for $v = (v_1, \ldots, v_m) \in \mathbf{R}^m$. A *lattice* is a discrete additive subgroup L of $\mathbf{R}^m$. Its *rank* is the dimension of the $\mathbf{R}$-subspace $V(L)$ that it spans. Each lattice L of rank n has a *basis*, i.e. a sequence $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of n elements of L that generate L as an abelian group. We define the *determinant* $d(L)$ of L by choosing any basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of L and setting

$$d(L) = \det[\langle \mathbf{b}_i, \mathbf{b}_j\rangle]_{1\leq i,j\leq n}^{1/2}.$$

This does not depend on the choice of the basis. The *i-th successive minimum* $\lambda_i(L)$ of a lattice L (with respect to the Euclidean norm) is the smallest real number r such that there are i vectors in L of length at most r that are $\mathbf{R}$-linearly independent.

The lattice L^* *reciprocal* to L (also called the lattice *polar* or *dual* to L) is defined as

$$L^* = \{\mathbf{w} \in V(L) : \langle \mathbf{w}, \mathbf{v}\rangle \in \mathbf{Z} \text{ for all } \mathbf{v} \in L\}.$$

We have $L^{**} = L$ and $d(L^*) = d(L)^{-1}$. For each basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a lattice L there is a unique basis $B^* = [\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ of L^* such that

$$\langle \mathbf{b}_i, \mathbf{b}_j^*\rangle = \begin{cases} 1 & \text{if } i + j = n + 1, \\ 0 & \text{otherwise.} \end{cases}$$

We call this the *basis of L^* reciprocal to B*. Note that we numbered the elements of B^* in reverse order to what is customary.

Hermite's constant γ_n is defined by

$$\gamma_n = \sup\{\lambda_1(L)^2 d(L)^{-2/n} : L \text{ is a lattice of rank } n\}.$$

Its value is known exactly for $n \leq 8$, see [2, Appendix]. Minkowski's convex body theorem implies that $\gamma_n \leq 4\pi^{-1}\Gamma(1 + n/2)^{2/n}$ (see [2, IX.7]), which yields $\gamma_n \leq 2n/3$ for all $n \geq 2$. It is known that

$$\frac{n}{2\pi e}(1 + o(1)) \leq \gamma_n \leq \frac{n}{\pi e}(1 + o(1)) \qquad \text{as } n \to \infty,$$

see [18], and the upper bound has been further improved to $(1+o(1)) \cdot 0.872n/(\pi e)$ by Kabatyanskiĭ and Levenshteĭn, see [3, Ch. 9]. It has never been proved that γ_n is an increasing function of n, though this is very likely true. For convenience we define

$$\gamma_n^* = \max\{\gamma_i : 1 \leq i \leq n\} \tag{1}$$

to obtain a non-decreasing function of n. We have $\gamma_n^* \leq 2n/3$ for all $n \geq 2$.

Given a basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a lattice L in $\mathbf{R}^m$, we define the *Gram-Schmidt orthogonalization* $B^\dagger = [\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$ of B by the Gram-Schmidt orthogonalization process: let $\mathbf{b}_1^\dagger = \mathbf{b}_1$, and define $\mathbf{b}_i^\dagger$ recursively for $2 \leq i \leq n$ by

$$\mathbf{b}_i^\dagger = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^\dagger,$$

where

$$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^\dagger \rangle}{\langle \mathbf{b}_j^\dagger, \mathbf{b}_j^\dagger \rangle} \qquad \text{for } 1 \leq j < i \leq n.$$

Thus we have the Gram-Schmidt decomposition

$$\mathbf{b}_i = \mathbf{b}_i^\dagger + \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^\dagger \qquad \text{for } 1 \leq i \leq n. \tag{2}$$

It follows that $d(L) = \prod_{i=1}^n |\mathbf{b}_i^\dagger|$. It is not difficult to prove that the Gram-Schmidt orthogonalization $B^{*\dagger} = [\mathbf{b}_1^{*\dagger}, \ldots, \mathbf{b}_n^{*\dagger}]$ of the reciprocal basis B^* of L^* is expressed in $B^\dagger$ by

$$\mathbf{b}_{n-i+1}^{*\dagger} = \mathbf{b}_i^\dagger / |\mathbf{b}_i^\dagger|^2 \qquad \text{for } 1 \leq i \leq n. \tag{3}$$

We say that a basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is *reduced in the sense of Korkin and Zolotarev*, or that it is a *Korkin-Zolotarev basis*, if it satisfies the following recursive set of conditions:

(4) $\mathbf{b}_1$ is a shortest non-zero vector of L in the Euclidean norm;

(5) $|\mu_{i,1}| \leq 1/2$ for $2 \leq i \leq n$;

(6) if $L^{(n-1)}$ denotes the orthogonal projection of L on the orthogonal complement $(\mathbf{R}\mathbf{b}_1)^\perp$ of $\mathbf{R}\mathbf{b}_1$. then the projections $\mathbf{b}_i - \mu_{i,1}\mathbf{b}_1$ of $\mathbf{b}_2, \ldots, \mathbf{b}_n$ yield a Korkin-Zolotarev basis $[\mathbf{b}_2 - \mu_{2,1}\mathbf{b}_1, \ldots, \mathbf{b}_n - \mu_{n,1}\mathbf{b}_1]$ of $L^{(n-1)}$.

The above definition is equivalent to the definition of Korkin and Zolotarev [9]. An equivalent non-recursive definition can be given as follows.

Let $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a basis for a lattice L in $\mathbf{R}^m$. For $i \in \{1, \ldots, n\}$, denote by $\pi_i \colon \mathbf{R}^m \to (\mathbf{R}\mathbf{b}_1 + \ldots + \mathbf{R}\mathbf{b}_{i-1})^\perp$ the orthogonal projection on the orthogonal complement of $\mathbf{R}\mathbf{b}_1 + \ldots + \mathbf{R}\mathbf{b}_{i-1}$. Write $L^{(n-i+1)} = \pi_i(L)$; this is a lattice of rank $n-i+1$ with basis $[\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]$. In terms of the Gram-Schmidt decomposition we have $\pi_i(\mathbf{b}_j) = \mathbf{b}_j^\dagger + \sum_{k=i}^{j-1} \mu_{j,k}\mathbf{b}_k^\dagger$, in particular $\pi_i(\mathbf{b}_i) = \mathbf{b}_i^\dagger$. Unwinding the definition just given, we see that B is a Korkin-Zolotarev basis if and only if the following two conditions are satisfied:

(7) $\mathbf{b}_i^\dagger$ is a shortest non-zero vector of $L^{(n-i+1)}$ in the Euclidean norm, for $1 \le i \le n$;

(8) $|\mu_{i,j}| \le 1/2$ for $1 \le j < i \le n$.

It is known that the domain of all Korkin-Zolotarev bases of lattices of rank n in the space of all bases of lattices of rank n in $\mathbf{R}^n$ can be specified by a finite set of inequalities that are quadratic in the entries b_{ij} of the $n \times n$ basis matrix $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$. These inequalities have been determined explicitly for $n \le 8$, see [17].

We call a basis B of a lattice L a *reciprocal Korkin-Zolotarev basis* if its reciprocal basis B^* is a Korkin-Zolotarev basis of L^*.

In Section 3 of this paper we prove the following two theorems, which relate the length of vectors in any Korkin-Zolotarev basis of L to the successive minima of L and L^*.

Theorem 2.1. *If $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is a Korkin-Zolotarev basis of a lattice L, then*

$$\frac{4}{i+3}\lambda_i(L)^2 \le |\mathbf{b}_i|^2 \le \frac{i+3}{4}\lambda_i(L)^2 \qquad \textit{for } 1 \le i \le n.$$

The upper bound in this theorem is essentially due to Mahler [14], cf. [2, V.4] We will give examples to show that the inequalities in Theorem 2.1 cannot be much improved.

Theorem 2.2. *If $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is a Korkin-Zolotarev basis of a lattice L, then*

$$|\mathbf{b}_i|^2\lambda_{n-i+1}(L^*)^2 \le \frac{i+3}{4} \cdot \frac{n-i+4}{4} \cdot \gamma_n^{*2} \qquad \textit{for } 1 \le i \le n,$$

where γ_n^* is as in (1).

Note that the upper bound is $O(n^4)$.

As consequences of these results we obtain the following two theorems, which are also proved in Section 3.

Theorem 2.3. *If $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is a Korkin-Zolotarev basis of a lattice L, then*

$$\prod_{i=1}^{n} |\mathbf{b}_i|^2 \le \Big(\gamma_n^n \prod_{i=1}^{n} \frac{i+3}{4}\Big) d(L)^2.$$

Note that $\gamma_n^n \prod_{i=1}^n (i+3)/4 \le n^{2n}/(4\pi e^2 + o(1))^n$ for $n \to \infty$. This theorem provides an upper bound for the *orthogonality defect* $(\prod_{i=1}^n |\mathbf{b}_i|)/d(L)$ of a Korkin-Zolotarev basis. Hermite's inequality asserts that any basis has orthogonality defect at least 1, with equality if and only if the basis is orthogonal.

Theorem 2.4. *The successive minima of a lattice L of rank n and its reciprocal lattice L^* satisfy*

$$1 \le \lambda_i(L)^2\lambda_{n-i+1}(L^*)^2 \le \frac{i+3}{4} \cdot \frac{n-i+4}{4} \cdot \gamma_n^{*2}$$

for $1 \le i \le n$, *with* γ_n^* *as in* (1).

The lower bound is classical, see [2, VIII.5, Theorem VI]. From Theorem 2.4 we see that

$$1 \le \lambda_i(L)\lambda_{n-i+1}(L^*) \le \frac{1}{6}n^2 \qquad \text{for } n \ge 7,\ 1 \le i \le n.$$

Previously known upper bounds were exponential in n, see [2, VIII.5, Theorem VI].

A limit on the amount of improvement possible in Theorems 2.2 and 2.4 is imposed by a result of Conway and Thompson, see [16, Ch. II, Theorem 9.5], which asserts that there exist lattices L_n of rank n with $L_n = L_n^*$ for which

$$\lambda_1(L_n)^2\lambda_1(L_n^*)^2 \ge \left(\frac{n}{2\pi e}\right)^2(1+o(1)) \qquad \text{as } n \to \infty. \tag{9}$$

In Section 4 we prove lower bounds for the Gram-Schmidt orthogonalizations of Korkin-Zolotarev bases and reciprocal Korkin-Zolotarev bases. These include

$$|\mathbf{b}_n^\dagger| \ge \gamma_n^{-1}\lambda_1(L)$$

for a reciprocal Korkin-Zolotarev basis and

$$|\mathbf{b}_n^\dagger| \ge n^{-(1+\log n)/2} \cdot \lambda_1(L)$$

for a Korkin-Zolotarev basis, see Proposition 4.1 and 4.2. It is an interesting open problem whether or not a bound of the form $|\mathbf{b}_n^\dagger| \ge n^{O(1)}\lambda_1(L)$ holds for all Korkin-Zolotarev bases.

The *covering radius* $\mu(L)$ is the smallest number r such that all vectors $\mathbf{x} \in V(L)$ are at distance at most r from a lattice vector. In Section 5 we prove the following bounds for the covering radius.

Theorem 2.5. *The covering radius* $\mu(L)$ *of a lattice* L *of rank* n *satisfies*

$$\frac{1}{4} \le \mu(L)^2\lambda_1(L^*)^2 \le \frac{1}{4}\sum_{i=1}^{n}\gamma_i^{*2},$$

with γ_i^* *as in* (1).

The lower bound is well known [2, XI.3]. From the upper bound it follows that

$$\mu(L)\lambda_1(L^*) \le \frac{1}{2}n^{3/2}$$

for all $n \ge 1$. The Conway-Thompson result (9) together with the obvious bound $\mu(L) \ge \lambda_1(L)/2$ imply that there exist lattices L_n of rank n with $L_n = L_n^*$ and

$$\mu(L_n)\lambda_1(L_n^*) \ge \frac{n}{4\pi e}(1+o(1)) \qquad \text{as } n \to \infty.$$

In Section 6 we obtain bounds for $\lambda_1(L)$ and for the quantity $\mu(\mathbf{x}, L)$ that measures the distance from a vector $\mathbf{x}$ to the closest vector in the lattice L. Given a basis B of a lattice L, with Gram-Schmidt orthogonalization $[\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$, we define

$$\lambda(B) = \min\{|\mathbf{b}_i^\dagger| : 1 \le i \le n\}.$$

This quantity gives rise to the following bounds for $\lambda_1(L)$.

Theorem 2.6. *For any basis B of a lattice L we have*

$$\lambda_1(L) \geq \lambda(B).$$

If B is a reciprocal Korkin-Zolotarev basis of a lattice L of rank n, then we have

$$\lambda_1(L) \leq \gamma_n^* \lambda(B),$$

where γ_n^* is as in (1).

Next we consider $\mu(\mathbf{x}, L)$. Let B be a basis of a lattice L, with Gram-Schmidt orthogonalization $[\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$. Let $\mathbf{x} \in \mathbb{R}^m$, and write $\mathbf{x} = \mathbf{x}' + \mathbf{x}''$ with $\mathbf{x}' \in V(L)$ and $\mathbf{x}'' \in V(L)^\perp$. It is not difficult to see that there exists a unique $\mathbf{b} \in L$ such that $\mathbf{x}' - \mathbf{b} = \sum_{j=1}^n v_j \mathbf{b}_j^\dagger$ for certain real numbers v_j with $-1/2 \leq v_j < 1/2$. Using this representation, we define

$$\mathbf{w}_0 = \mathbf{x}' - \mathbf{b}, \qquad \mathbf{w}_i = \frac{1}{2}\mathbf{b}_i^\dagger + \sum_{j=i+1}^{n} v_j \mathbf{b}_j^\dagger \qquad \text{for } 1 \leq i \leq n,$$

$$\mu(\mathbf{x}', B) = \min\{|\mathbf{w}_i| : 0 \leq i \leq n\}, \qquad \mu(\mathbf{x}, B) = \left(\mu(\mathbf{x}', B)^2 + |\mathbf{x}''|^2\right)^{1/2}.$$

This quantity gives rise to the following bounds for $\mu(\mathbf{x}, L)$.

Theorem 2.7. *For any basis B of a lattice L in $\mathbb{R}^m$ of rank n and any $\mathbf{x} \in \mathbb{R}^m$ we have*

$$\mu(\mathbf{x}, L) \geq \mu(\mathbf{x}, B).$$

If in addition B is a reciprocal Korkin-Zolotarev basis of L, then we have

$$\mu(\mathbf{x}, L)^2 \leq \left(\sum_{j=1}^{n} \gamma_j^{*2}\right) \cdot \mu(\mathbf{x}, B)^2,$$

with γ_j^* as in (1).

In Section 7 we use Theorems 2.6 and 2.7 to bound the non-deterministic computational complexity of finding a provably short, or provably close, vector in a lattice.

In Section 8 we extend the bounds from Sections 3 and 5 to arbitrary symmetric convex distance functions, i. e. functions $F: \mathbb{R}^n \to \mathbb{R}$ satisfying

$$F(\mathbf{x}) \geq 0, \quad \text{with equality if and only if } \mathbf{x} = 0,$$
$$F(\alpha\mathbf{x}) = |\alpha| F(\mathbf{x}), \qquad F(\mathbf{x} + \mathbf{y}) \leq F(\mathbf{x}) + F(\mathbf{y})$$

for all $\mathbf{x}$, $\mathbf{y} \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$. Such a function is determined by its *unit ball* $\Omega = \{\mathbf{x} \cdot F(\mathbf{x}) \leq 1\}$, which is a compact symmetric convex set containing 0 in its interior The *reciprocal distance function* F^* is defined by

$$F^*(\mathbf{x}) = \sup\{\langle \mathbf{x}, \mathbf{y}\rangle / F(\mathbf{y}) : \mathbf{y} \in \mathbb{R}^n, \mathbf{y} \neq 0\}.$$

The unit ball Ω^* of F^* is given by

$$\Omega^* = \{\mathbf{x} : |\langle \mathbf{x}, \mathbf{y}\rangle| \leq 1 \text{ for all } \mathbf{y} \in \Omega\}.$$

For a lattice $L \subset \mathbb{R}^n$ we define the *i-th successive minimum $\lambda_i(L; \Omega)$ of L with respect to Ω to be the smallest real number r such that $r\Omega$ contains i points of L* that are $\mathbb{R}$-linearly independent. For background on the above notions we refer to [2, 5].

Theorem 2.8. *Let Ω be the unit ball of a symmetric convex distance function in $\mathbb{R}^n$ and Ω^* the unit ball of its reciprocal distance function. Let L be a lattice of rank n in $\mathbb{R}^n$, and let $\lambda_i(L;\Omega)$ denote the i-th successive minimum of L with respect to Ω. Then we have*

$$\lambda_i(L;\Omega)^2\lambda_1(L^*;\Omega^*)^2 \le n\cdot\frac{i+3}{4}\cdot\gamma_n^{*2}$$

and

$$1 \le \lambda_i(L;\Omega)^2\lambda_{n-i+1}(L^*,\Omega^*)^2 \le n\cdot\frac{i+3}{4}\,\frac{n-i+4}{4}\,\gamma_n^{*2}$$

for $1 \le i \le n$, with γ_n^* as in (1).

The last upper bound is a sharpening of the M. Riesz-K. Mahler theorem [15, 5, Ch. 2, sec. 14.2, Theorem 5, cf. 2, VIII.5], which gives $n!^4$ as the upper bound.

If Ω and L are as in the previous theorem, we write $\mu(L;\Omega)$ for the covering radius of L with respect to Ω. Our final result is the following.

Theorem 2.9. *With Ω and L as in Theorem 2.8 we have*

$$\mu(L;\Omega)^2\lambda_1(L^*;\Omega^*)^2 \le \frac{1}{4}n\sum_{i=1}^{n}\gamma_i^{*2},$$

where γ_i^* is as in (1).

3. Korkin-Zolotarev bases and successive minima

Proof of Theorem 2.1. There are i linearly independent vectors of length at most $\lambda_i(L)$ in L, and under the projection $L \to L^{(n-i+1)}$ at least one of them maps to a non-zero vector. Therefore we have $\lambda_1(L^{(n-i+1)}) \le \lambda_i(L)$. Combining this with (7) we find that $|\mathbf{b}_i^\dagger| \le \lambda_i(L)$. Using (2) and (8) we obtain

$$|\mathbf{b}_i|^2 \le |\mathbf{b}_i^\dagger|^2 + \frac{1}{4}\sum_{j=1}^{i-1}|\mathbf{b}_j^\dagger|^2 \le \lambda_i(L)^2 + \frac{1}{4}\sum_{j=1}^{i-1}\lambda_j(L)^2 \le \frac{i+3}{4}\lambda_i(L)^2.$$

This proves the right side of the inequality in Theorem 2.1. To prove the left side, we first note that for $j \le i$ we have

$$|\mathbf{b}_j^\dagger|^2 = \lambda_1(L^{(n-j+1)})^2 \le |\pi_j(\mathbf{b}_i)|^2 \le |\mathbf{b}_i|^2,$$

since $\pi_j(\mathbf{b}_i)$ is a non-zero element of $L^{(n-j+1)}$. Hence for $j \le i$ we have

$$|\mathbf{b}_j|^2 \le |\mathbf{b}_j^\dagger|^2 + \frac{1}{4}\sum_{k=1}^{j-1}|\mathbf{b}_k^\dagger|^2 \le \frac{j+3}{4}|\mathbf{b}_i|^2.$$

Therefore we have

$$\lambda_i(L)^2 \le \max\{|\mathbf{b}_j|^2 : 1 \le j \le i\} \le \frac{i+3}{4}|\mathbf{b}_i|^2.$$

This proves Theorem 2.1. ∎

Remark 3.1. We give a few examples to show that the bounds in Theorem 2.1 cannot be improved by more than a constant factor. By $\mathbf{e}_1, \ldots, \mathbf{e}_n$ we denote the standard orthonormal basis of $\mathbb{R}^n$.

First let $1 \le i < n$. Let L be the lattice in $\mathbb{R}^n$ that is spanned by $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, where $\mathbf{b}_j = \mathbf{e}_j$ for $j \neq i$ and $\mathbf{b}_i = \mathbf{e}_i + \sum_{j=1}^{i-1} \mathbf{e}_j/2$. We have $\mathbf{b}_j^\dagger = \mathbf{e}_j$ for all j, and using the first inequality in Theorem 2.6 one easily deduces that $\lambda_j(L) = 1$ for $1 \le j \le n-1$, and that B is a Korkin-Zolotarev basis for L. From $|\mathbf{b}_i|^2 = (i+3)/4 = (i+3)\lambda_i(L)^2/4$ we see that the upper bound in Theorem 2.1 is sharp whenever $i < n$.

One can show that for $i = n > 1$ the upper bound in Theorem 2.1 is not sharp. We show that it is sharp up to a factor $3 + o(1)$, for $n \to \infty$. Let $n > 1$, and let L be the lattice in $\mathbb{R}^n$ that is spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_n$, where $\mathbf{b}_j = \mathbf{e}_j$ for $j < n$ and $\mathbf{b}_n = \sqrt{3}\mathbf{e}_n/2 + \sum_{j=1}^{n-1} \mathbf{e}_j/2$. It is easy to check that $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is a Korkin-Zolotarev basis for L, and that $\lambda_n(L)^2 = \min\{3, (n+2)/4\} \le 3$. Therefore $|\mathbf{b}_n|^2 = (n+2)/4 \ge (n+2)\lambda_n(L)^2/12$, which establishes our claim. A more complicated example can be constructed in which $|\mathbf{b}_n|^2 = (n + O(1))\lambda_n(L)^2/4$.

Next we consider the lower bound in Theorem 2.1. For $i = 1$ we clearly have equality. Let $1 < i \le n$, and let L be the lattice in $\mathbb{R}^n$ that is spanned by $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, where $\mathbf{b}_j = \mathbf{e}_j$ for $j < i - 1$, $\mathbf{b}_{i-1} = \mathbf{e}_{i-1} + \sum_{j=1}^{i-2} \langle\!\langle j/(i-1) \rangle\!\rangle \mathbf{e}_j$, $\mathbf{b}_i = \mathbf{e}_i$ and $\mathbf{b}_j = n\mathbf{e}_j$ for $j > i$, where $\langle\!\langle\ \rangle\!\rangle$ denotes the distance to the nearest integer. One easily proves that B is a Korkin-Zolotarev basis for L, that $\lambda_j(L) = 1$ for $j < i$ and $\lambda_j(L) = n$ for $j > i$, and that

$$\lambda_i(L)^2 = \min\{m^2 + \sum_{j=0}^{i-2} \left\langle\!\!\left\langle \frac{jm}{i-1} \right\rangle\!\!\right\rangle^2 : m \in \mathbb{Z},\ m \neq 0\}.$$

The inside sum depends only on $\gcd(m, i-1)$, so the minimum is assumed when m is a divisor of $i - 1$. By means of a straightforward computation this leads to $\lambda_i(L)^2 \ge (i+10)/12 = (i+10)|\mathbf{b}_i|^2/12$. This proves that the lower bound in Theorem 2.1 cannot be improved by more than a factor of 3.

Proof of Theorem 2.3. This follows immediately from Theorem 2.1 and Minkowski's theorem that $\prod_{i=1}^n \lambda_i(L) \le \gamma_n^{n/2} d(L)$, see [2, VIII.2]. ∎

Proposition 3.2. *Let $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a Korkin-Zolotarev basis of a lattice L, and let L^* be its reciprocal lattice. Then we have*

$$|\mathbf{b}_i|^2 \lambda_1(L^*)^2 \le \frac{i+3}{4}\gamma_n^{*2}$$

for $1 \le i \le n$, where γ_n^* is as in (1).

Proof. It is easy to see that $L^{(n-j+1)*}$ is a sublattice of L^*, so we have $\lambda_1(L^*) \le \lambda_1(L^{(n-j+1)*})$ for each j. Combining this with

$$|\mathbf{b}_i|^2 \le |\mathbf{b}_i^\dagger|^2 + \frac{1}{4}\sum_{j=1}^{i-1} |\mathbf{b}_j^\dagger|^2 = \lambda_1(L^{(n-i+1)})^2 + \frac{1}{4}\sum_{j=1}^{i-1} \lambda_1(L^{(n-j+1)})^2 \tag{10}$$

we obtain

$$|\mathbf{b}_i|^2\lambda_1(L^*)^2 \le \lambda_1(L^{(n-i+1)})^2\lambda_1(L^{(n-i+1)*})^2 + \frac{1}{4}\sum_{j=1}^{i-1}\lambda_1(L^{(n-j+1)})^2\lambda_1(L^{(n-j+1)*})^2.$$

For any lattice M of rank k we have by definition of Hermite's constant

$$\lambda_1(M)^2\lambda_1(M^*)^2 \le \gamma_k \cdot d(M)^{2/k} \cdot \gamma_k \cdot d(M^*)^{2/k} = \gamma_k^2,$$

where we use that $d(M^*) = d(M)^{-1}$. So we find that

$$|\mathbf{b}_i|^2\lambda_1(L^*)^2 \le \gamma_{n-i+1}^2 + \frac{1}{4}\sum_{j=1}^{i-1}\gamma_{n-j+1}^2 \le \frac{i+3}{4}\gamma_n^{*2}.$$

This proves Proposition 3.2. ∎

Proposition 3.3. *For any lattice L of rank n with reciprocal lattice L^* we have*

$$\lambda_i(L)^2\lambda_1(L^*)^2 \le \frac{i+3}{4}\gamma_n^{*2}$$

for $1 \le i \le n$, where γ_n^* is as in (1).

Proof. This follows from Proposition 3.2, since $\lambda_i(L)^2 \le \max\{|\mathbf{b}_j|^2 : 1 \le j \le i\}$.

For $i = 1$ the bound in Proposition 3.3 is sharp up to a multiplicative constant, by (9).

Proof of Theorem 2.2. We have $\lambda_{n-i+1}(L^*) \le \lambda_{n-i+1}(L^{(n-j+1)*})$ whenever $j \le i$, since $L^{(n-j+1)*}$ is a sublattice of L^*. Combining this with (10) we obtain

$$\begin{aligned}|\mathbf{b}_i|^2\lambda_{n-i+1}(L^*)^2 &\le \lambda_1(L^{(n-i+1)})^2\lambda_{n-i+1}(L^{(n-i+1)*})^2 \\ &\quad + \frac{1}{4}\sum_{j=1}^{i-1}\lambda_1(L^{(n-j+1)})^2\lambda_{n-i+1}(L^{(n-j+1)*})^2.\end{aligned}$$

Applying Proposition 3.3 to each $L^{(n-j+1)}$ we find that

$$\begin{aligned}|\mathbf{b}_i|^2\lambda_{n-i+1}(L^*)^2 &\le \frac{n-i+4}{4}\cdot\gamma_{n-i+1}^{*2} + \frac{1}{4}\sum_{j=1}^{i-1}\frac{n-i+4}{4}\gamma_{n-j+1}^{*2} \\ &\le \frac{n-i+4}{4}\cdot\frac{i+3}{4}\cdot\gamma_n^{*2}.\end{aligned}$$

This proves Theorem 2.2. ∎

Proof of Theorem 2.4. The lower bound is well known, see [2, VIII.5, Theorem VI]. We prove the upper bound. Interchanging L and L^*, if necessary, we may assume that $i \le (n+1)/2$. Choosing a Korkin-Zolotarev basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of L and applying Theorem 2.2 we obtain

$$\begin{aligned}\lambda_i(L)^2\lambda_{n-i+1}(L^*)^2 &\le \max\{|\mathbf{b}_j|^2 : 1 \le j \le i\}\cdot\lambda_{n-i+1}(L^*)^2 \\ &\le \max\{|\mathbf{b}_j|^2\lambda_{n-j+1}(L^*)^2 : 1 \le j \le i\} \\ &\le \max\left\{\frac{j+3}{4}\cdot\frac{n-j+4}{4}\gamma_n^{*2} : 1 \le j \le i\right\} \\ &= \frac{i+3}{4}\cdot\frac{n-i+4}{4}\cdot\gamma_n^{*2}.\end{aligned}$$

This proves Theorem 2.4. ∎

4. Bounds for Gram-Schmidt orthogonalizations

Proposition 4.1. *Let B be a reciprocal Korkin-Zolotarev basis of a lattice L, with Gram-Schmidt orthogonalization $B^\dagger = [\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$. Then we have*

$$\gamma_i |\mathbf{b}_i^\dagger| \geq \lambda_1(L)$$

for $1 \leq i \leq n$.

Proof. By (3) and (4) we have

$$|\mathbf{b}_n^\dagger|^{-1} = |\mathbf{b}_1^{*\dagger}| = |\mathbf{b}_1^*| = \lambda_1(L^*) \leq \gamma_n^{1/2} d(L^*)^{1/n} = \gamma_n^{1/2} d(L)^{-1/n}.$$

Multiplying this by $\lambda_1(L) \leq \gamma_n^{1/2} d(L)^{1/n}$ we obtain the desired inequality for $i = n$. For general i we consider the sublattice L_i with basis $B_i = [\mathbf{b}_1, \ldots, \mathbf{b}_i]$. It is easy to see that B_i is a reciprocal Korkin-Zolotarev basis for L_i. Hence the result just proved implies that $\gamma_i |\mathbf{b}_i^\dagger| \geq \lambda_1(L_i)$. This is at least $\lambda_1(L)$ because $L_i \subset L$. This proves Proposition 4.1. ∎

Proposition 4.2. *Let $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a Korkin-Zolotarev basis of a lattice L, with Gram-Schmidt orthogonalization $[\mathbf{b}_1^\dagger, \ldots, \mathbf{b}_n^\dagger]$. Then we have*

$$i^{1+\log i} |\mathbf{b}_i^\dagger|^2 \geq \lambda_1(L)^2$$
$$i^{2+\log i} |\mathbf{b}_i^\dagger|^2 \geq |\mathbf{b}_i|^2$$

for $1 \leq i \leq n$.

Proof. By (7) we have

$$|\mathbf{b}_{n-j+1}^\dagger|^2 = \lambda_1(L^{(j)})^2 \leq \gamma_j d(L^{(j)})^{2/j} = \gamma_j \cdot \Big(\prod_{k=1}^{j} |\mathbf{b}_{n-k+1}^\dagger|^2\Big)^{1/j}$$

and therefore

$$|\mathbf{b}_{n-j+1}^\dagger|^2 \leq \gamma_j^{j/(j-1)} \Big(\prod_{k=1}^{j-1} |\mathbf{b}_{n-k+1}^\dagger|^2\Big)^{1/(j-1)}$$

for $1 < j \leq n$. By a straightforward induction on i this yields

$$|\mathbf{b}_{n-i+1}^\dagger|^2 \leq \gamma_i \Big(\prod_{k=2}^{i} \gamma_k^{1/(k-1)}\Big) |\mathbf{b}_n^\dagger|^2$$

for $1 \leq i \leq n$. Using that $\gamma_k \leq 2k/3$ for $k \geq 2$ one readily derives that

$$|\mathbf{b}_{n-i+1}^\dagger|^2 \leq i^{1+\log i} |\mathbf{b}_n^\dagger|^2.$$

With $i = n$ we obtain the case $i = n$ of the first inequality of Proposition 4.2. For general i one applies the same result to L_i and uses that $\lambda_1(L_i) \geq \lambda_1(L)$. Further we have

$$|\mathbf{b}_n|^2 \leq |\mathbf{b}_n^\dagger|^2 + \frac{1}{4}\sum_{i=2}^{n} |\mathbf{b}_{n-i+1}^\dagger|^2 \leq \Big(1 + \frac{1}{4}\sum_{i=2}^{n} i^{1+\log i}\Big)|\mathbf{b}_n^\dagger|^2 \leq n^{2+\log n}|\mathbf{b}_n^\dagger|^2,$$

which is the case $i = n$ of the last inequality of Proposition 4.2. For general i one argues as before. This proves Proposition 4.2. ▮

5. Bounds for the covering radius

Proof of Theorem 2.5. The easy lower bound $\mu(L) \geq \lambda_n(L)/2$ (see [2, XI.3]) combined with $\lambda_n(L)\lambda_1(L^*) \geq 1$ implies that $\mu(L)\lambda_1(L^*) \geq 1/2$, which proves the left inequality in Theorem 2.5.

We prove the right inequality in Theorem 2.5 by induction on n, the case $n = 1$ being obvious. Let $n > 1$, let $\mathbf{b}_1 \in L$ satisfy $|\mathbf{b}_1| = \lambda_1(L)$, and denote by L' the projection of L on $(\mathbb{R}\mathbf{b}_1)^\perp$. We first prove that

$$\mu(L)^2 \leq \frac{1}{4}\lambda_1(L)^2 + \mu(L')^2. \tag{11}$$

Let $\mathbf{x} \in V(L)$. By definition of $\mu(L')$, there exists $\mathbf{b}' \in L$ such that the projection $\mathbf{x}'$ of $\mathbf{x} - \mathbf{b}'$ on $(\mathbb{R}\mathbf{b}_1)^\perp$ has length at most $\mu(L')$. If we write $\mathbf{x} - \mathbf{b}' = \mathbf{x}' + \mathbf{x}''$, then $\mathbf{x}'' \in \mathbb{R}\mathbf{b}_1$, so we can find $\mathbf{b}'' \in \mathbb{Z}\mathbf{b}_1$ such that $|\mathbf{x}'' - \mathbf{b}''| \leq |\mathbf{b}_1|/2 = \lambda_1(L)/2$. Then $\mathbf{b} = \mathbf{b}' + \mathbf{b}''$ is an element of L satisfying

$$|\mathbf{x} - \mathbf{b}|^2 = |\mathbf{x}' + \mathbf{x}'' - \mathbf{b}''|^2 = |\mathbf{x}'|^2 + |\mathbf{x}'' - \mathbf{b}''|^2 \leq \mu(L')^2 + \frac{1}{4}\lambda_1(L)^2,$$

which proves (11).

Since L'^* is a sublattice of L^* we have $\lambda_1(L^*) \leq \lambda_1(L'^*)$. Hence (11), Proposition 3.3 and the induction hypothesis imply that

$$\begin{aligned}\mu(L)^2\lambda_1(L^*)^2 &\leq \frac{1}{4}\lambda_1(L)^2\lambda_1(L^*)^2 + \mu(L')^2\lambda_1(L^*)^2 \\ &\leq \frac{1}{4}\gamma_n^{*2} + \mu(L')^2\lambda_1(L'^*)^2 \leq \frac{1}{4}\sum_{i=1}^{n}\gamma_i^{*2},\end{aligned}$$

as required. This proves Theorem 2.5. ▮

6. Lower bounds for shortest vector problems and closest vector problems

Proof of Theorem 2.6. Let $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, and let $\mathbf{b} = \sum_{j=1}^{n} m_j\mathbf{b}_j$ be a non-zero element of L, with $m_j \in \mathbb{Z}$. Let i be maximal with $m_i \neq 0$. Then $\mathbf{b} - m_i\mathbf{b}_i^\dagger$ lies in the subspace $\sum_{j=1}^{i-1}\mathbb{R}\mathbf{b}_j$. Since this subspace is orthogonal to $\mathbf{b}_i^\dagger$, we find that

$$|\mathbf{b}| \geq |m_i\mathbf{b}_i^\dagger| \geq |\mathbf{b}_i^\dagger| \geq \lambda(B).$$

This proves the first assertion of Theorem 2.6.

Next assume that B is a reciprocal Korkin-Zolotarev basis. Then by 4.1 we have

$$\lambda_1(L) \le \min\{\gamma_i |\mathbf{b}_i^\dagger| : 1 \le i \le n\} \le \gamma_n^* \lambda(B),$$

as required. This proves Theorem 2.6.

Proof of Theorem 2.7. Let $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, and let $\mathbf{x} \in \mathbf{R}^m$. As in Section 2, we consider the unique representation

$$\mathbf{x} = \mathbf{x}' + \mathbf{x}'' = \mathbf{b} + \Big(\sum_{j=1}^{n} v_j \mathbf{b}_j^\dagger\Big) + \mathbf{x}''$$

with $\mathbf{x}' \in V(L)$, $\mathbf{b} \in L$, $v_j \in \mathbf{R}$, $-1/2 \le v_j < 1/2$, $\mathbf{x}'' \in V(L)^\perp$. Let $\mathbf{v} \in L$. To prove the first inequality in Theorem 2.7 it suffices to show that $|\mathbf{x}' - \mathbf{v}| \ge |\mathbf{w}_i|$ for some i, $0 \le i \le n$, where the $\mathbf{w}_i$ are as in Section 2.

If $\mathbf{v} = \mathbf{b}$ then $\mathbf{x}' - \mathbf{v} = \mathbf{w}_0$, and we can take $i = 0$. Suppose that $\mathbf{v} \ne \mathbf{b}$, and write $\mathbf{b} - \mathbf{v} = \sum_{j=1}^{i} m_j \mathbf{b}_j$ with $m_j \in \mathbf{Z}$, $m_i \ne 0$. Then

$$\mathbf{x}' - \mathbf{v} = \sum_{j=1}^{i} m_j \mathbf{b}_j + \sum_{j=1}^{n} v_j \mathbf{b}_j^\dagger = \mathbf{y} + (m_i + v_i)\mathbf{b}_i^\dagger + \sum_{j=i+1}^{n} v_j \mathbf{b}_j^\dagger$$

for some $\mathbf{y}$ in the subspace spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$. This subspace is orthogonal to each of $\mathbf{b}_i^\dagger, \ldots, \mathbf{b}_n^\dagger$, so

$$|\mathbf{x}' - \mathbf{v}|^2 \ge (m_i + v_i)^2 |\mathbf{b}_i^\dagger|^2 + \sum_{j=i+1}^{n} |v_j \mathbf{b}_j^\dagger|^2 \ge |\mathbf{w}_i|^2,$$

where we use that $|m_i + v_i| \ge 1/2$. This proves the first inequality of Theorem 2.7.

Next suppose that B is a reciprocal Korkin-Zolotarev basis, let $\mathbf{x} \in \mathbf{R}^m$, and let the notation be as above. To prove the second inequality of Theorem 2.7, it suffices to prove that for each $i \in \{0, 1, \ldots, n\}$ there exists $\mathbf{v} \in L$ such that

$$|\mathbf{x}' - \mathbf{v}|^2 \le \Big(\sum_{j=1}^{n} \gamma_j^{*2}\Big) |\mathbf{w}_i|^2.$$

For $i=0$ one can take $\mathbf{v}=\mathbf{b}$, so let $i>0$. Let L_i be the lattice spanned by $\mathbf{b}_1, \ldots, \mathbf{b}_i$, and let $\mathbf{z}$ be the element of $V(L_i)$ defined by

$$\mathbf{z} = \sum_{j=1}^{i} v_j \mathbf{b}_j^\dagger = \mathbf{x}' - \mathbf{b} - \sum_{j=i+1}^{n} v_j \mathbf{b}_j^\dagger.$$

Let $\mathbf{v}' \in L_i$ be such that $|\mathbf{z} - \mathbf{v}'| \le \mu(L_i)$. Then the element $\mathbf{v} = \mathbf{b} + \mathbf{v}'$ of L satisfies

$$\mathbf{x}' - \mathbf{v} = (\mathbf{z} - \mathbf{v}') + \sum_{j=i+1}^{n} v_j \mathbf{b}_j^\dagger$$

and therefore

$$|\mathbf{x}' - \mathbf{v}|^2 \leq \mu(L_i)^2 + \sum_{j=i+1}^{n} |v_j \mathbf{b}_j^{\dagger}|^2.$$

By Theorem 2.5 we have

$$\mu(L_i)^2 \leq \frac{1}{4}\Big(\sum_{j=1}^{i} \gamma_j^{*2}\Big)\lambda_1((L_i)^*)^{-2}.$$

From the fact that B^* is a Korkin-Zolotarev basis for L^* it follows easily that a Korkin-Zolotarev basis for $(L_i)^*$ is given by the orthogonal projections of $\mathbf{b}_{n-i+1}^*$, $\ldots$, $\mathbf{b}_n^*$ on $V(L_i)$. The first of these projections is $\mathbf{b}_{n-i+1}^{*\dagger}$, and its length is $\lambda_1((L_i)^*)$. By (3) this implies that $\lambda_1((L_i)^*) = |\mathbf{b}_i^{\dagger}|^{-1}$. Putting everything together we obtain

$$\begin{aligned} |\mathbf{x}' - \mathbf{v}|^2 &\leq \frac{1}{4}\Big(\sum_{j=1}^{i} \gamma_j^{*2}\Big)|\mathbf{b}_i^{\dagger}|^2 + \sum_{j=i+1}^{n} |v_j \mathbf{b}_j^{\dagger}|^2 \\ &\leq \Big(\sum_{j=1}^{n} \gamma_j^{*2}\Big)\Big(\frac{1}{4}|\mathbf{b}_i^{\dagger}|^2 + \sum_{j=i+1}^{n} |v_j \mathbf{b}_j^{\dagger}|^2\Big) = \Big(\sum_{j=1}^{n} \gamma_j^{*2}\Big)|\mathbf{w}_i|^2, \end{aligned}$$

as required. This proves Theorem 2.7. ■

7. Computational complexity of lattice problems

The following are two basic computational problems concerning lattices.

Finding shortest vector: given n and a basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a sublattice L of $\mathbb{Z}^n$, find a shortest non-zero vector in L.

Finding closest vector: given n, a basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of a sublattice L of $\mathbb{Z}^n$, and $x \in \mathbb{Z}^n$, find a vector $\mathbf{b} \in L$ that minimizes $|\mathbf{x} - \mathbf{b}|^2$.

It is not difficult to see that the first problem is polynomial time equivalent to the problem of finding a Korkin-Zolotarev basis of an arbitrary integer lattice L. It is suspected to be NP-hard, but this has never been proved. Van Emde Boas [24] showed that the second problem is NP-hard.

The fastest algorithms known for the above two problems are due to R. Kannan [8], and require the exponential time $O(n^{9n}H^6)$, where H is the length of the input of the problem with the usual encoding in binary.

Several polynomial time algorithms are known for solving weaker versions of these problems. Lovász' lattice basis reduction algorithm [11] runs in time $O(n^6H^3)$ and is guaranteed to find a short non-zero lattice vector $\mathbf{b}$ satisfying

$$|\mathbf{b}|^2 \leq 2^{n-1}\lambda_1(L)^2.$$

Babai [1] observed that this algorithm can also be used to find, for given $\mathbf{x}$, a close lattice vector $\mathbf{b}$ satisfying

$$|\mathbf{x} - \mathbf{b}|^2 \leq 2^n \mu(\mathbf{x}, L)^2.$$

Schnorr [21] has given a hierarchy of polynomial time lattice basis reduction algorithms, showing that for any positive ε there exists a polynomial time algorithm that produces a non-zero lattice vector $\mathbf{b}$ satisfying

$$|\mathbf{b}|^2 \leq (1+\varepsilon)^n \lambda_1(L)^2.$$

It is of great interest to find practical polynomial time algorithms that determine a non-zero vector $\mathbf{b} \in L$ that is certified to satisfy

$$|\mathbf{b}|^2 \leq f(n)\lambda_1(L)^2$$

with $f(n)$ as small as possible.

Even if a shortest, or closest, lattice vector $\mathbf{b} \in L$ has been found, it is not clear how to prove that it is indeed the shortest, or closest, lattice vector. No polynomial length proofs ("certificates") are known to exist for statements of the form "$\mathbf{b}$ is a shortest non-zero vector in L" or "$\mathbf{b}$ is a closest vector in L to $\mathbf{x}$". In this context the results of Section 6 imply that there is at least a polynomial length proof that $\mathbf{b}$ is quite short, or quite close to $\mathbf{x}$, respectively.

Theorem 7.1. *There exists a non-deterministic polynomial time algorithm that given a basis B of an integer lattice $L \subset \mathbb{Z}^n$ of rank n produces a vector $\mathbf{b}$ in L and a proof that*

$$|\mathbf{b}| \leq n^2 \lambda_1(L)^2.$$

Furthermore, there exists a non-deterministic polynomial time algorithm that when given in addition an element $\mathbf{x} \in \mathbb{Z}^n$ produces a vector $\mathbf{b}$ in L and a proof that

$$|\mathbf{x}-\mathbf{b}|^2 \leq n^3 \mu(\mathbf{x}, L)^2.$$

Proof. We give only a sketch of the proof, leaving the details to the reader.

The first algorithm consists of non-deterministically guessing an element $\mathbf{b} \in L$ satisfying $|\mathbf{b}|^2 = \lambda_1(L)^2$ as well as a Korkin-Zolotarev basis $B^* = [\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ of L^*. If we guess right, then by the second inequality of Theorem 2.6 we have

$$|\mathbf{b}|^2 \leq n^2 \lambda(B)^2,$$

where B is the basis of L reciprocal to B^*. We can now verify this inequality directly, since $\lambda(B)^2$ is easy to compute. If in addition we check that B is indeed a basis of L, then the first inequality of Theorem 2.6 implies that $|\mathbf{b}|^2 \leq n^2\lambda_1(L)^2$, as required.

For the second algorithm one proceeds in a similar manner, replacing Theorem 2.6 by 2.7.

This proves Theorem 7.1. ▮

8. Symmetric convex distance functions

Proof of Theorem 2.8. For the last lower bound, see [2, VIII.5, Theorem 6]. If Ω is the standard unit sphere in $\mathbb{R}^n$, then the upper bounds in Proposition 3.3 and Theorem 2.4 are sharper by a factor of n than the upper bounds in Theorem 2.8. Applying a linear transformation we see that these sharper bounds are also valid if Ω is an ellipsoid. In the general case we use the theorem of John [7, 5, Ch. 1, sec. 1.6], which asserts that for any Ω there exists an ellipsoid E centered at 0 such that $E \subset \Omega \subset \sqrt{n}E$. Then $\lambda_i(L;\Omega) \leq \lambda_i(L;E)$ for all i and L, by the definition of successive minima. Also $(\sqrt{n})^{-1}E^* = (\sqrt{n}E)^* \subset \Omega^* \subset E^*$, so $\lambda_i(L;\Omega^*) \leq \sqrt{n}{\cdot}\lambda_i(L;E^*)$. Hence the upper bounds in Theorem 2.8 are implied by the sharper bounds that are valid for ellipsoids. This proves Theorem 2.8. ∎

Proof of Theorem 2.9. This follows from Theorem 2.5 by the same argument as in the previous proof. ∎

Acknowledgements. The authors would like to thank L. Lovász and G. Miller for helpful suggestions. The research of the first author was supported in part by NSF grant 8120790.

References

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

[2] J. W. S. Cassels: *An introduction to the geometry of numbers,* Springer-Verlag, Berlin, **1971**.

[3] J. H. Conway, and N. J. A. Sloane: *Sphere packings, lattices and groups*, Springer-Verlag, New York, **1988**.

[4] M. Grötschel, L. Lovász, and A. Schrijver: *Geometric algorithms and combinatorial optimization*, Springer-Verlag, Berlin, **1988**.

[5] P. M. Gruber, and C. G. Lekkerkerker: *Geometry of numbers*, North-Holland, Amsterdam, **1987**.

[6] C. Hermite: Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres, Deuxième lettre, *J. Reine Angew. Math.* **40** (1850), 279–290.

[7] F. John: Extremum problems with inequalities as subsidiary conditions, K. O. Friedrichs, O. E. Neugebauer, J. J. Stoker (eds), *Studies and essays presented to R. Courant on his 60th birthday*, 187–204, Interscience Publishers, New York, **1948**.

[8] R. Kannan: Minkowski's convex body theorem and integer programming, *Math. Oper. Res.* **12** (1987), 415–440.

[9] A. Korkine, and G. Zolotareff: Sur les formes quadratiques, *Math. Ann.* **6** (1873), 366–389.

[10] J. L. Lagrange: Recherches d'arithmétique, *Nouv. Mém. Acad. Berlin* (1773), 265–312; Œuvres, vol. VIII, 693–753.

[11] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász: Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

[12] H. W. LENSTRA, JR.: Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (1983), 538–548.

[13] L. LOVÁSZ: An algorithmic theory of numbers, graphs and convexity, *CBMS-NSF Regıonal Conference Serıes ın Applıed Mathematıcs* **50**, SIAM, Philadelphia, Pennsylvania, **1986**.

[14] K. MAHLER: A theorem on inhomogeneous diophantine inequalities, *Nederl. Akad. Wetensch., Proc.* **41** (1938), 634–637.

[15] K. MAHLER: *The geometry of numbers*, duplicated lectures, Boulder, Colorado, **1950**.

[16] J. MILNOR, and D. HUSEMOLLER: *Symmetrıc bılınear forms*, Springer-Verlag, Berlin, **1973**.

[17] N. V. NOVIKOVA: Korkin-Zolotarev reduction domains of positive quadratic forms in $n \leq 8$ variables and a reduction algorithm for these domains, *Dokl. Akad. Nauk SSSR* **270** (1983), 48–51; English translation: *Sovıet Math. Dokl.* **27** (1983), 557–560.

[18] C. A. ROGERS: *Packıng and coverıng*, Cambridge University Press, Cambridge, **1964**.

[19] S. S. RYSHKOV: Geometry of positive quadratic forms (Russian), *Proceedıngs of the Internatıonal Congress of Mathematıcıans (Vancouver, B. C.*, 1974), **1**, 501-506, *Canad. Math. Congress, Montreal, Que.*, 1975.

[20] S. S. RYSHKOV, and E. P. BARANOVSKIĬ: Classical methods in the theory of lattice packings, *Uspekhı Mat. Nauk* **34**, 4 (208) (1979), 3–63; English translation: *Russıan Math. Surveys* **34** (4) (1979), 1–68.

[21] C. P. SCHNORR: A hierarchy of polynomial time lattice basis reduction algorithms, *Theoret. Comput. Scı.* **53** (1987), 201–224.

[22] B. L. VAN DER WAERDEN: Die Reduktionstheorie der positiven quadratischen Formen, *Acta Math.* **96** (1956), 265–309.

[23] B. L. VAN DER WAERDEN: H. Gross (eds), *Studıen zur Theorıe der quadratıschen Formen*, Birkhäuser-Verlag, Basel, **1968**.

[24] P. VAN EMDE BOAS: Another *NP*-complete partition problem and the complexity of computing short vectors in a lattice, *Report 81-04, Department of Mathematıcs, Unıversıty of Amsterdam, Amsterdam,* **1981**.

J. C. Lagarias

AT&T Bell Laboratorıes
Murray Hıll, New Jersey
U.S.A.

H. W. Lenstra, Jr.

Department of Mathematıcs
Unıversıty of Calıfornıa
Berkeley, CalıfornıaU.S.A.

C. P. Schnorr

Unıversıtät Frankfurt
Frankfurt,
F. R. Germany