Math. Ann. 296, 625–635 (1993)

Mathematische Annalen

New bounds in some transference theorems in the geometry of numbers

W. Banaszczyk
Institute of Mathematics, Łódź University, Banacha 22, PL-90-238 Łódź, Poland

Received July 4, 1992

Mathematics Subject Classification (1991): 11H06, 11H60, 52C07

Introduction

The aim of this paper is to give new bounds in certain inequalities concerning mutually reciprocal lattices in $\mathbb{R}^n$. To formulate the problem, we have to introduce some notation and terminology.

We shall treat $\mathbb{R}^n$ as an n-dimensional euclidean space with the norm $\| \ \|$ and metric d. The inner product of vectors u, v will be denoted by uv; we shall usually write u^2 instead of uu. The closed and open unit balls in $\mathbb{R}^n$ will be denoted by B_n and B_n', respectively. If $A \subset \mathbb{R}^n$, then span A and $A^\perp$ denote the linear subspace spanned over A and the orthogonal complement of A in $\mathbb{R}^n$.

A lattice in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors. The family of all lattices in $\mathbb{R}^n$ will be denoted by Λ_n.

Given a lattice $L \in \Lambda_n$, we define the polar (dual, reciprocal) lattice L^* in the usual way:

$$L^* = \{u \in \mathbb{R}^n : uv \in \mathbb{Z} \text{ for each } v \in L\} .$$

One has $L^{**} = L$. By $d(L)$ we shall denote the determinant of L, i.e. the n-dimensional volume of a fundamental domain of L. Naturally, $d(L^*) = d(L)^{-1}$.

A convex body in $\mathbb{R}^n$ is a compact convex subset of $\mathbb{R}^n$ containing interior points. The family of all o-symmetric convex bodies in $\mathbb{R}^n$ will be denoted by $\mathscr{C}_n$. Given a convex body $U \in \mathscr{C}_n$, we define the polar body U^0 in the usual way:

$$U^0 = \{u \in \mathbb{R}^n : uv \leqq 1 \text{ for each } v \in U\} .$$

By $\| \ \|_U$ we shall denote the norm on $\mathbb{R}^n$ induced by U (the Minkowski functional of U). By d_U we shall denote the metric induced by $\| \ \|_U$. Thus $\| \ \| = \| \ \|_{B_n}$ and $d = d_{B_n}$.

Given a lattice $L \in \Lambda_n$ and a convex body $U \in \mathscr{C}_n$, we denote

$$\begin{aligned} \mu(L, U) &= \max\{d_U(u, L) : u \in \mathbb{R}^n\} \\ &= \min\{r > 0 : L + rU = \mathbb{R}^n\} , \\ \lambda_i(L, U) &= \min\{r > 0 : \dim \operatorname{span}(L \cap rU) \geqq i\} \quad (i = 1, \ldots, n) . \end{aligned}$$

The quantity $\mu(L, U)$ is called the covering radius of L with respect to U. The quantities $\lambda_i(L, U)$ are called the successive minima of L with respect to U. To simplify the notation, we shall write $\mu(L)$ and $\lambda_i(L)$ instead of $\mu(L, B_n)$ and $\lambda_i(L, B_n)$, respectively.

Given a convex body $U \in \mathscr{C}_n$, we define

$$\xi(U) = \sup_{L \in \Lambda_n} \max_{1 \leqq i \leqq n} \lambda_i(L, U)\, \lambda_{n-i+1}(L^*, U^0)\,,$$

$$\eta(U) = \sup_{L \in \Lambda_n} \mu(L, U)\, \lambda_1(L^*, U^0)\,,$$

$$\zeta(U) = \sup_{L \in \Lambda_n} \sup_{u \in \mathbb{R}^n \setminus L} \inf_{\substack{v \in L^* \\ uv \notin \mathbb{Z}}} d(uv, \mathbb{Z})^{-1}\, d_U(u, L)\, \|v\|_{U^0}\,.$$

It is clear that the quantities $\xi(U)$, $\eta(U)$ and $\zeta(U)$ are affine invariants of U. The obvious inequality $\mu(L, U) \leqq \frac{1}{2} n\, \lambda_n(L, U)$ implies that $\eta(U) \leqq \frac{1}{2} n\xi(U)$. It is also clear that $\eta(U) \leqq \frac{1}{2}\zeta(U)$.

For each $n = 1, 2, \ldots$, we define

$$\xi_n = \sup_{U \in \mathscr{C}_n} \xi(U)\,, \quad \eta_n = \sup_{U \in \mathscr{C}_n} \eta(U)\,, \quad \zeta_n = \sup_{U \in \mathscr{C}_n} \zeta(U)\,.$$

Then $\eta_n \leqq \frac{1}{2} n\xi_n$ and $\eta_n \leqq \frac{1}{2}\zeta_n$. Mahler [11] proved that $\xi_n \leqq (n!)^2$ for $n \geqq 1$. See also [6], VIII, Sect. 5, Theorem VI, where $(n!)^2$ is replaced by $n!$. Recently, Lagarias et al. [10] proved that $\xi(B_n) \leqq \frac{1}{6} n^2$ for $n \geqq 7$. Similar bounds were obtained independently in [4], Theorem (2.1).

The inequalities $\eta(B_n) \leqq \frac{3}{2} n^{3/2}$ for $n \geqq 5$ follow from Lemma 1.4 of [3] (see also [4], Lemma (1.4) and the subsequent remarks). Lagarias et al. [10] proved that $\eta_n \leqq \frac{1}{2} n^{3/2}$ for every n.

That $\zeta_n < \infty$ was proved by Khinchin [9]. Cassels [6], XI, Sect. 3, Theorem VI gave the bound $\zeta_n \leqq 2^{1-n}(n!)^2$. Babai [1] proved that $\zeta_n \leqq C^n$ for some universal constant C. The inequalities $\zeta(B_n) \leqq 12n(n+1)$ can be derived from Lemma 7 of [2]; see also [4], Lemma (1.1) and the subsequent remarks. Hastad [7] proved that $\zeta(B_n) \leqq 6n^2 + 1$.

In the present paper we show that there exists an universal constant C such that $\xi(B_n)$, $\eta(B_n)$, $\zeta(B_n) \leqq Cn$ for every n. Examples show that $\xi(B_n)$, $\eta(B_n)$, $\zeta(B_n) \geqq cn$ where c is some other universal constant. For the numerical values of C and c, see the final remarks in Sect. 2. The corresponding inequalities for convex bodies other than B_n are discussed in Sect. 3.

The determination of the quantities $\xi(U)$, $\eta(U)$ and $\zeta(U)$ is a classical problem in the geometry of numbers. The corresponding results belong to the so-called transference theorems; a detailed description is given in Cassels' book [6]. Recently, these questions became a subject of intensive investigations in integer programming; we refer the reader to the introductions in [1, 7, 10]. Another source of motivation is commutative harmonic analysis, more precisely, the theory of characters of additive subgroups and quotient groups of topological vector spaces. This point of view is presented exhaustively in monograph [5], especially, in Section 3. See also the survey article [4].

Papers [2–4, 7, 10] all found on the idea of Korkin-Zolotarev bases. The method used in the present paper is entirely different. Taken from commutative harmonic analysis, it consists in investigating certain probability measures on lattices and Fourier transforms of such measures. The proofs are non-constructive.

1 Gaussian-like measures on lattices

Let μ be a finite Borel measure on $\mathbb{R}^n$. For the purpose of the present paper, it is convenient to define the Fourier transform $\mu^\wedge$ of μ by the formula

$$\mu^\wedge(x) = \int_{\mathbb{R}^n} e^{2\pi ixy}\, d\mu(y) \quad (x \in \mathbb{R}^n)\,.$$

Similarly, given an integrable complex-valued function f on $\mathbb{R}^n$, by the Fourier transform $f^\wedge$ of f we shall mean the function

$$f^\wedge(x) = \int_{\mathbb{R}^n} e^{2\pi ixy} f(y)\, dy \quad (x \in \mathbb{R}^n)\,.$$

The symbol dy denotes integration with respect to the n-dimensional Lebesgue measure on $\mathbb{R}^n$. Under such a definition, the function $e^{-\pi x^2}$ is equal to its Fourier transform.

Let L be a lattice in $\mathbb{R}^n$. By σ_L we shall denote the probability measure on L given by the formula

$$\sigma_L(A) = \sum_{x\in A} e^{-\pi x^2} \Big/ \sum_{x \in L} e^{-\pi x^2} \quad (A \subset L)\,.$$

By φ_L we shall denote the function on $\mathbb{R}^n$ defined by the formula

$$\varphi_L(u) = \sum_{x\in L+u} e^{-\pi x^2} \Big/ \sum_{x \in L} e^{-\pi x^2} \quad (u \in \mathbb{R}^n)\,.$$

To simplify the notation, we shall write

$$\rho(A) = \sum_{x\in A} e^{-\pi x^2} \quad (A \subset \mathbb{R}^n)\,.$$

Then $\sigma_L(A) = \rho(A)/\rho(L)$ for $A \subset L$, and $\varphi_L(u) = \rho(L+u)/\rho(L)$ for $u \in \mathbb{R}^n$.

In the remaining part of this section, n is a fixed positive integer, and L is an arbitrary, but fixed lattice in $\mathbb{R}^n$.

(1.1) Lemma. *Let a, b be positive numbers such that $ab = \pi$. Let μ be the measure on L given by the formula $\mu(\{x\}) = e^{-ax^2}$. Then*

(i) $$\sum_{x\in L+u} e^{2\pi ixy} e^{-ax^2} = b^{n/2} d(L)^{-1} \sum_{z\in L^*} e^{-2\pi iuz} e^{-\pi b(y+z)^2} \quad (u, y \in \mathbb{R}^n)\,;$$

(ii) $$\mu^\wedge(y) = b^{n/2} d(L)^{-1} \sum_{z\in L^*} e^{-\pi b(y+z)^2} \quad (y \in \mathbb{R}^n)\,.$$

Proof. Point (i) follows from the Poisson summation formula; see e.g. [8, (31.46) (c)]. Point (ii) is a direct consequence of (i). □

(1.2) Corollary. *One has $\sigma_L^\wedge = \varphi_{L^*}$ and $\sigma_{L^*}^\wedge = \varphi_L$.*

Proof. It is enough to prove that $\sigma_L^\wedge = \varphi_{L^*}$. Let μ be the measure on L given by the formula $\mu(\{x\}) = e^{-\pi x^2}$. Then $\sigma_L = \mu/\mu(L)$, so that $\sigma_L^\wedge = \mu^\wedge/\mu^\wedge(0)$, and the result follows from (1.1) (ii). $\square$

Let $k = 1, \ldots, n$ and let $x \in \mathbb{R}^n$. By x_k we shall denote the kth coordinate of x. If f is a function on $\mathbb{R}^n$, we shall write $f_{kk} = \dfrac{\partial^2}{\partial x_k^2} f$.

(1.3) Lemma. *Given arbitrary $u \in \mathbb{R}^n$, $a > 0$ and $k = 1, \ldots, n$, one has*

$$\kappa := \sum_{x \in L+u} x_k^2 \, e^{-ax^2} \Big/ \sum_{x \in L} e^{-ax^2} \leqq \frac{1}{a} \, .$$

If $u = 0$, then $\kappa \leqq \dfrac{1}{2a}$.

Proof. Let μ be the measure on $L + u$ given by the formula $\mu(\{x\}) = e^{-ax^2}$. Then

$$\mu^\wedge(y) = \sum_{x \in L+u} e^{2\pi i x y} \, e^{-ax^2} \quad (y \in \mathbb{R}^n) \, ,$$

$$\mu_{kk}^\wedge(y) = -4\pi^2 \sum_{x \in L+u} x_k^2 \, e^{2\pi i x y} \, e^{-ax^2} \quad (y \in \mathbb{R}^n) \, .$$

Setting here $y = 0$, we get

$$\sum_{x \in L+u} x_k^2 \, e^{-ax^2} = -(4\pi^2)^{-1} \, \mu_{kk}^\wedge(0) \, . \tag{1}$$

Let us denote $b = \dfrac{\pi}{a}$. It follows from (1.1) (ii) that

$$\mu_{kk}^\wedge(y) = b^{n/2} \, d(L)^{-1} \sum_{z \in L^*} e^{-2\pi i u z} \left[-2\pi b + 4\pi^2 b^2 (y_k + z_k)^2 \right] e^{-\pi b (y+z)^2}$$

for $y \in \mathbb{R}^n$. Setting $y = 0$, we get

$$\mu_{kk}^\wedge(0) = b^{n/2} \, d(L)^{-1} \sum_{z \in L^*} e^{-2\pi i u z} \left[-2\pi b + 4\pi^2 b^2 z_k^2 \right] e^{-\pi b z^2} \, . \tag{2}$$

Let ν be the measure on L^* given by the formula $\nu(\{z\}) = e^{-\pi b z^2}$. Then

$$\sum_{z \in L^*} e^{-2\pi i u z} \, e^{-\pi b z^2} = \nu^\wedge(-u) \, , \tag{3}$$

$$\sum_{z \in L^*} z_k^2 \, e^{-2\pi i u z} \, e^{-\pi b z^2} = -(4\pi^2)^{-1} \, \nu_{kk}^\wedge(-u) \, . \tag{4}$$

Setting $u = y = 0$ in (1.1) (i), we see that

$$\nu^\wedge(0) := \sum_{z \in L^*} e^{-\pi b z^2} = d(L) \, b^{-n/2} \sum_{x \in L} e^{-ax^2} \, . \tag{5}$$

Now, from (1)–(5) we derive

$$\kappa = \frac{1}{2a}\frac{v^\wedge(-u)}{v^\wedge(0)} + \frac{1}{4a^2}\frac{v^\wedge_{kk}(-u)}{v^\wedge(0)}. \tag{6}$$

Take an arbitrary $v \in \mathbb{R}^n$. By (1.1) (i), we have

$$\begin{aligned} d(L)^{-1} b^{n/2} v^\wedge(v) &= d(L)^{-1} b^{n/2} \sum_{z \in L^*} e^{2\pi i v z} e^{-\pi b z^2} \\ &= \sum_{x \in L+v} e^{-ax^2} = \frac{1}{2}\sum_{x \in L} [e^{-a(x+v)^2} + e^{-a(x-v)^2}] \\ &= e^{-av^2} \sum_{x \in L} e^{-ax^2} \cosh 2axv \geqq e^{-av^2} \sum_{x \in L} e^{-ax^2}. \end{aligned}$$

Hence, by (5),

$$v^\wedge(v)/v^\wedge(0) \geqq e^{-av^2} \quad (v \in \mathbb{R}^n). \tag{7}$$

The functions $v^\wedge$ and $-v^\wedge_{kk}$ are positive-definite, being the Fourier transforms of the positive measures $e^{-\pi b z^2}$ and $4\pi^2 z_k^2 e^{-\pi b z^2}$, respectively. Therefore $v^\wedge(-u) \leqq v^\wedge(0)$ and $v^\wedge_{kk}(-u) \leqq -v^\wedge_{kk}(0)$. It follows directly from (7) that $-v^\wedge_{kk}(0)/v^\wedge(0) \leqq 2a$. Now, (6) implies that $\kappa \leqq \frac{1}{2a} + \frac{1}{2a} = \frac{1}{a}$. If $u = 0$, then (6) yields $\kappa < \frac{1}{2a}$, because $v^\wedge_{kk}(0) < 0$. □

(1.4) Lemma. *For each $a \geqq 1$, one has*

(i) $\sum_{x \in L} e^{-\pi a^{-1} x^2} \leqq a^{n/2} \sum_{x \in L} e^{-\pi x^2}$;

(ii) $\sum_{x \in L+u} e^{-\pi a^{-1} x^2} \leqq 2a^{n/2} \sum_{x \in L} e^{-\pi x^2} \quad (u \in \mathbb{R}^n)$.

Proof. Let us consider the function

$$f(a) = \sum_{x \in L} e^{-\pi a^{-1} x^2} \quad (a \geqq 1).$$

From (1.3) we obtain

$$\begin{aligned} f'(a) &= \frac{\pi}{a^2} \sum_{x \in L} x^2 e^{-\pi a^{-1} x^2} = \frac{\pi}{a^2} \sum_{k=1}^{n} \sum_{x \in L} x_k^2 e^{-\pi a^{-1} x^2} \\ &\leqq \frac{n\pi}{a^2} \frac{a}{2\pi} \sum_{x \in L} e^{-\pi a^{-1} x^2} = \frac{n}{2a} f(a) \quad (a \geqq 1). \end{aligned}$$

Hence $[\log f(a)]' \leqq \frac{n}{2a}$ etc., which yields $f(a) \leqq a^{n/2} f(1)$ for $a \geqq 1$. This proves (i). To prove (ii), take an arbitrary $u \in \mathbb{R}^n$ and consider the function

$$g(a) = \sum_{x \in L+u} e^{-\pi a^{-1} x^2} \quad (a \geqq 1).$$

Applying (1.3) and then (i), we may write

$$g'(a) = \frac{\pi}{a^2} \sum_{x \in L+u} x^2 e^{-\pi a^{-1} x^2} = \frac{\pi}{a^2} \sum_{k=1}^{n} \sum_{x \in L+u} x_k^2 e^{-\pi a^{-1} x^2}$$

$$\leqq \frac{n\pi}{a^2} \frac{a}{\pi} \sum_{x \in L} e^{-\pi a^{-1} x^2} \leqq n a^{-1+n/2} f(1) \quad (a \geqq 1)\,.$$

Hence

$$g(a) - g(1) = \int_1^a g'(t)\,dt \leqq nf(1) \int_1^a t^{-1+n/2}\,dt$$

$$= 2f(1)\,[a^{n/2} - 1] \quad (a \geqq 1)\,. \tag{8}$$

By (1.2), the function φ_L is positive-definite, being the Fourier transform of the positive measure σ_{L^*}. Thus

$$\frac{g(1)}{f(1)} = \frac{\rho(L+u)}{\rho(L)} = \varphi_L(u) \leqq \varphi_L(0) = 1\,,$$

i.e. $g(1) \leqq f(1)$. Now (8) yields

$$g(a) = 2f(1)\,[a^{n/2} - 1] + g(1) \leqq 2a^{n/2} f(1) - f(1) < 2a^{n/2} f(1). \quad \square$$

(1.5) Lemma. *For each* $c \geqq (2\pi)^{-1/2}$, *one has*

(i) $\rho(L \backslash c\sqrt{n}\, B'_n) < [c\sqrt{2\pi e}\, e^{-\pi c^2}]^n \rho(L)$,

(ii) $\rho((L+u) \backslash c\sqrt{n}\, B'_n) < 2[c\sqrt{2\pi e}\, e^{-\pi c^2}]^n \rho(L) \quad (u \in \mathbb{R}^n)$.

Proof. For each $t \in (0, 1)$, we have

$$\sum_{x \in L} e^{-\pi t x^2} = \sum_{x \in L} e^{\pi(1-t)x^2} e^{-\pi x^2}$$

$$> \sum_{\substack{x \in L \\ x^2 \geqq c^2 n}} e^{\pi(1-t)x^2} e^{-\pi x^2} > e^{\pi(1-t)c^2 n} \sum_{\substack{x \in L \\ x^2 \geqq c^2 n}} e^{-\pi x^2}\,.$$

On the other hand, (1.4) (i) says that

$$\sum_{x \in L} e^{-\pi t x^2} < t^{-n/2} \sum_{x \in L} e^{-\pi x^2}\,.$$

Thus

$$\sum_{\substack{x \in L \\ x^2 \geqq c^2 n}} e^{-\pi x^2} < t^{-n/2} e^{-\pi(1-t)c^2 n} \sum_{x \in L} e^{-\pi x^2}\,.$$

which can be written as

$$\rho(L \backslash c\sqrt{n}\, B'_n) < [t^{-1/2} e^{-\pi c^2 (1-t)}]^n \rho(L)\,.$$

Setting here $t = (2\pi c^2)^{-1}$, we obtain (i). To prove (ii), it is enough to apply (1.4) (ii) instead of (1.4) (i). $\square$

2 Transference theorems

(2.1) Theorem. *Let L be an arbitrary lattice in $\mathbb{R}^n$, $n \geqq 1$. Then*

$$\lambda_i(L)\,\lambda_{n-i+1}(L^*) \leqq n \quad (i = 1, \dots, n)\,.$$

Proof. If $n = 1$, then $\lambda_1(L)\lambda_1(L^*) = 1$. If $n = 2$, then it is not hard to verify that $\lambda_1(L)\lambda_2(L^*) \leqq 2 \cdot 3^{-1/2}$. So, we may assume that $n \geqq 3$.

Let us suppose the contrary, that there is an index $i = 1, \dots, n$ with $\lambda_i(L)\lambda_{n-i+1}(L^*) > n$. Replacing L by sL for a suitably chosen coefficient s, we may assume that

$$\lambda_i(L) > \frac{3}{4}\sqrt{n}\,, \tag{9}$$

$$\lambda_{n-i+1}(L^*) > \frac{4}{3}\sqrt{n}\,. \tag{10}$$

Let K be the subgroup of $\mathbb{R}^n$ generated by $L \cap \frac{3}{4}\sqrt{n}\,B_n'$, and let H be the subgroup generated by $L^* \cap \frac{4}{3}\sqrt{n}\,B_n'$. Denote $M = \operatorname{span} K$ and $N = \operatorname{span} H$. From (9) and (10) we get $\dim M \leqq i-1$ and $\dim N \leqq n-i$. Hence $\dim M^\perp + \dim N^\perp \geqq n+1$, and we can find a vector $u \in M^\perp \cap N^\perp$ with $\|u\| = 3^{-1/2}$.

As $u \in M^\perp$, we have $uv = 0$ for each $v \in K$. Hence

$$\begin{aligned}\hat{\sigma_L}(u) &= \sum_{v\in L} \sigma_L(\{v\})\cos 2\pi uv = \sum_{v\in K} + \sum_{v\in L\setminus K} \sigma_L(\{v\})\cos 2\pi uv \\ &\geqq \sum_{v\in K} \sigma_L(\{v\}) - \sum_{v\in L\setminus K} \sigma_L(\{v\}) = 1 - 2\sigma_L(L\setminus K)\,.\end{aligned}$$

Now, (1.5) (i) implies that

$$\sigma_L(L\setminus K) \leqq \sigma_L\left(L \setminus \frac{3}{4}\sqrt{n}\,B_n'\right) < \left[\frac{3}{4}\sqrt{2\pi e}\,e^{-9\pi/16}\right]^3 < 0.15\,,$$

so that

$$\hat{\sigma_L}(u) > 0.7\,. \tag{11}$$

Since $\|u\| = 3^{-1/2}$ and $n \geqq 3$, we have $\sqrt{n}\,B_n' - u \subset \frac{4}{3}\sqrt{n}\,B_n'$, which means that

$$\left(L^* \setminus \frac{4}{3}\sqrt{n}\,B_n'\right) + u \subset (L^* + u)\setminus\sqrt{n}\,B_n'\,.$$

Hence, by (1.5) (ii),

$$\begin{aligned}\rho((L^*\setminus H) + u) &\leqq \rho\left(\left(L^*\setminus\frac{4}{3}\sqrt{n}\,B_n'\right) + u\right) \leqq \rho((L^* + u)\setminus\sqrt{n}\,B_n') \\ &< 2[\sqrt{2\pi e}\,e^{-\pi}]^3\,\rho(L^*)\,.\end{aligned} \tag{12}$$

Next, as $u \in N^\perp$, we have

$$\rho(H + u) = e^{-\pi u^2}\rho(H) \leqq e^{-\pi/3}\rho(L^*)\,. \tag{13}$$

From (12) and (13) we derive

$$\rho(L^* + u) = \rho((L^* \backslash H) + u) + \rho(H + u) < 0.4\,\rho(L^*)\,,$$

i.e. $\varphi_{L^*}(u) < 0.4$. In view of (1.2), this means that $\sigma_L^\wedge(u) < 0.4$, which contradicts (11). □

(2.2) Theorem. *Let L be an arbitrary lattice in $\mathbb{R}^n$, $n \geqq 1$. Then $\lambda_1(L)\,\mu(L^*) \leqq \frac{1}{2}\,n$.*

Proof. If $n = 1$, then $\lambda_1(L)\,\mu(L^*) = \frac{1}{2}$. If $n = 2$, then it is not hard to verify that $\lambda_1(L)\,\mu(L^*) \leqq 2^{-1/2}$. Therefore we may assume that $n \geqq 3$.

Suppose the contrary, that $\lambda_1(L)\,\mu(L^*) > \frac{1}{2}\,n$. Replacing L by sL for a suitably chosen coefficient s, we may assume that

$$\lambda_1(L) > 2^{-1/2}\sqrt{n}\,, \tag{14}$$

$$\lambda_1(L^*) > 2^{-1/2}\sqrt{n}\,. \tag{15}$$

Condition (15) means that there is some $u \in \mathbb{R}^n$ such that $(L^* + u) \cap 2^{-1/2}\sqrt{n}\,B_n = \varnothing$. Then, by (1.5) (ii),

$$\rho(L^* + u) = \rho((L^* + u) \backslash 2^{-1/2}\sqrt{n}\,B_n) < 2[2^{-1/2}\sqrt{2\pi e}\,e^{-\pi/2}]^3\,\rho(L^*)\,,$$

whence

$$\varphi_{L^*}(u) < \frac{1}{2}\,. \tag{16}$$

On the other hand, (14) means that $L \cap 2^{-1/2}\sqrt{n}\,B_n = \{0\}$, and then

$$\begin{aligned}\sigma_L^\wedge(u) &= \sum_{\substack{v \in L\\ v^2 < n/2}} + \sum_{\substack{v \in L\\ v^2 \geqq n/2}} \sigma_L(\{v\}) \cos 2\pi uv \\ &\geqq \sum_{\substack{v \in L\\ v^2 < n/2}} - \sum_{\substack{v \in L\\ v^2 \geqq n/2}} \sigma_L(\{v\}) = 1 - 2\,\sigma_L(L \backslash 2^{-1/2}\sqrt{n}\,B'_n)\,.\end{aligned}$$

Now, (1.5) (i) implies that

$$\sigma_L(L \backslash 2^{-1/2}\sqrt{n}\,B_n) < [2^{-1/2}\sqrt{2\pi e}\,e^{-\pi/2}]^3 < \frac{1}{4}\,,$$

and therefore $\sigma_L^\wedge(u) > \frac{1}{2}$. In view of (1.2), this contradicts (16). □

(2.3) Theorem. *Let L be an arbitrary lattice in $\mathbb{R}^n$, $n \geqq 1$, and let $u \in \mathbb{R}^n \backslash L$. Then there exists some $v \in L^*$ with* $\cos 2\pi uv \leqq 0.1$ *and* $\|v\|\,d(u, L) \leqq n$.

Proof. Let us suppose that $n \geqq 2$, the case $n = 1$ being trivial. Replacing L by sL and u by su for a suitably chosen coefficient s, we may assume that $d(u, L) = \sqrt{n}$. Then (1.5) (ii) yields

$$\rho(L + u) = \rho((L + u) \backslash \sqrt{n}\,B'_n) < 2\,[\sqrt{2\pi e}\,e^{-\pi}]^2\,\rho(L)\,.$$

Hence, by (1.2),

$$\sigma_{L^*}^\wedge(u) = \varphi_L(u) < 2[\sqrt{2\pi e}\,e^{-\pi}]^2\,. \tag{17}$$

On the other hand, (1.5) (i) implies that

$$\kappa := \sigma_{L^*}(L^* \setminus \sqrt{n}\, B_n') < [\sqrt{2\pi e}\, e^{-\pi}]^2 . \tag{18}$$

Let us denote

$$\vartheta = \sum_{\substack{v \in L^* \\ v^2 < n}} e^{-\pi v^2} \cos 2\pi uv \Bigg/ \sum_{\substack{v \in L^* \\ v^2 < n}} e^{-\pi v^2} .$$

Then we may write

$$\begin{aligned} \hat{\sigma}_{L^*}(u) &= \sum_{\substack{v \in L^* \\ v^2 < n}} + \sum_{\substack{v \in L^* \\ v^2 \geqq n}} \sigma_{L^*}(\{v\}) \cos 2\pi uv \\ &> \vartheta \sigma_{L^*}(L^* \cap \sqrt{n}\, B_n') - \sigma_{L^*}(L^* \setminus \sqrt{n}\, B_n') \\ &= \vartheta(1 - \kappa) - \kappa . \end{aligned} \tag{19}$$

Now, (17)–(19) imply that $\vartheta < 0.1$. Consequently, there must exist a vector $v \in L^* \cap \sqrt{n}\, B_n'$ with $\cos 2\pi uv < 0.1$. $\square$

Theorem (2.1) says that $\xi(B_n) \leqq n$ for every n. Its proof, based on (1.5), allows one to deduce that

$$\xi(B_n) \leqq \frac{n}{2\pi}(1 + O(n^{-1/2})) \quad \text{as } n \to \infty .$$

On the other hand, there is a result of Conway and Thompson (see [12], Ch. II, Theorem 9.5) which asserts that one can construct a sequence of lattices $L_n \in \Lambda_n$ such that $L_n^* = L_n$ for every n, and

$$\lambda_1^2(L_n) \geqq \frac{n}{2\pi e}(1 + o(1)) \quad \text{as } n \to \infty . \tag{20}$$

Consequently, one has

$$\xi(B_n) \geqq \frac{n}{2\pi e}(1 + o(1)) \quad \text{as } n \to \infty .$$

As $L_n^* = L_n$, we have $d(L_n) = 1$ for every n, which implies that $\mu(L_n)^n \operatorname{vol}(B_n) > 1$. Thus

$$\mu(L_n) \geqq \left(\frac{n}{2\pi e}\right)^{1/2} (1 + o(1)) \quad \text{as } n \to \infty . \tag{21}$$

Theorem (2.2) says that $\eta(B_n) \leqq \frac{1}{2} n$ for every n. The proof shows that

$$\eta(B_n) \leqq \frac{n}{2\pi}(1 + O(n^{-1/2})) \quad \text{as } n \to \infty .$$

On the other hand, (20) and (21) imply that

$$\eta(B_n) \geqq \frac{n}{2\pi e}(1 + o(1)) \quad \text{as } n \to \infty .$$

Let L be an arbitrary lattice in $\mathbb{R}^n$, $n \geqq 2$. Choose any $u \in L$ with $\|u\| = \lambda_1(L)$. It is not hard to see that there exists a vector $v \in L^*$ with $uv = 1$ and $v^2 \leqq 1 + \frac{4}{3}[\eta(B_{n-1})]^2$ (cf. the proof of Theorem (3.3) in [4]). As $\eta(B_{n-1}) \leqq \frac{1}{2}(n-1)$, it follows that $\|v\| \leqq 3^{-1/2}\, n$.

From (2.3) we get $\zeta(B_n) \leqq 5n$ for every n. The constant 5 may be replaced by a smaller one, perhaps even just by 1. From the proof of (2.3) one can deduce that

$$\zeta(B_n) \leqq \frac{2n}{\pi}(1 + O(n^{-1/2})) \quad \text{as } n \to \infty .$$

On the other hand, from (20) and (21) we obtain

$$\zeta(B_n) \geqq \frac{n}{\pi e}(1 + o(1)) \quad \text{as } n \to \infty .$$

3 Other convex bodies

Let U be a symmetric convex body in $\mathbb{R}^n$. According to the John theorem, there exists an n-dimensional ellipsoid D such that $D \subset U \subset \sqrt{n}\, D$. Thus, from (2.1)–(2.3) it follows that $\xi(U)$, $\eta(U)$, $\zeta(U) \leqq Cn^{3/2}$ for some universal constant C. The technique used in Sections 2 and 3 allows one to show that if U is symmetric through each of the coordinate hyperplanes, then $\xi(U)$, $\eta(U)$, $\zeta(U) \leqq C_1\, n \log n$ for some other constant C_1. Moreover, if U is the unit ball in l_p^n, $1 \leqq p \leqq \infty$, then $\xi(U)$, $\eta(U)$, $\zeta(U) \leqq C_2\, n\sqrt{\log n}$. The proofs will be given in a separate paper. On the other hand, the following fact is true:

(3.1) Theorem. *There exists an universal constant c such that, given an arbitrary convex body $U \in \mathscr{C}_n$, one can find a lattice $L \in \Lambda_n$ with $\lambda_1(L, U)\,\lambda_1(L^*, U^0) \geqq cn$.*

This implies that $\xi(U)$, $\eta(U)$, $\zeta(U) \geqq c_1 n$ for each $U \in \mathscr{C}_n$. Theorem (3.1) follows easily from Siegel's mean value theorem; the details of the proof will be given elsewhere.

Let us close with the following remark: it follows easily from the Bourgain-Milman theorem on the product of volumes of polar bodies and from the Minkowski convex body theorem that

$$\lambda_1(L, U)\,\lambda_1(L^*, U^0) \leqq Cn \quad (L \in \Lambda_n,\ U \in \mathscr{C}_n,\ n = 1, 2, \ldots)$$

for some universal constant C.

References

1. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**, 1–13 (1986)
2. Banaszczyk, W.: Closed subgroups of nuclear spaces are weakly closed. Studia Math. **80**, 119–128 (1984)
3. Banaszczyk, W.: Pontryagin duality for subgroups and quotients of nuclear spaces. Math. Ann. **273**, 653–664 (1986)
4. Banaszczyk, W.: Polar lattices from the point of view of nuclear spaces. Rev. Mat. Univ. Complutense Madr. **2** (special issue), 35–46 (1989)

5. Banaszczyk, W.: Additive subgroups of topological vector spaces. (Lect. Notes Math., vol 1466) Berlin Heidelberg New York: Springer 1991
6. Cassels, J.W.S.: An introduction to the geometry of numbers. Berlin Göttingen Heidelberg: Springer 1959
7. Hastad, J.: Dual vectors and lower bounds for the nearest lattice point problem. Combinatorica **8**, 75–81 (1988)
8. Hewitt, E., Ross, K.A.: Abstract harmonic analysis, vol. II. Berlin Heidelberg New York: Springer 1970
9. Khinchin, A.I.: A quantitative formulation of Kronecker's theory of approximation. Izv. Akad. Nauk SSSR, Ser. Mat. **12**, 113–122 (1948)
10. Lagarias, J.C., Lenstra, H.W., Schnorr, C.P.: Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica **10**, 333–348 (1990)
11. Mahler, K.: Ein Übertragungsprinzip für konvexe Körper. Čas. Péstováni Mat. Fys. **68**, 93–102 (1939)
12. Milnor, J., Husemoller, D.: Symmetric bilinear forms. Berlin Heidelberg New York: Springer 1973