Algorithmische Geometrie der Zahlen

prelude

Martin Henk

Otto-von-Guericke-Universität Magdeburg

Contents

0 Some basic and convex facts

0.1 Notation. *Let* $\mathbb{R}^n = \{x = (x_1, \dots, x_n)^\intercal : x_i \in \mathbb{R}\}$ *be the* n*-dimensional Euclidean space, equipped with the inner product* $\langle x, y\rangle = \sum_{i=1}^n x_i \cdot y_i$, $x, y \in \mathbb{R}^n$, *and Euclidean norm* $|x| = (\sum_{i=1}^n x_i^2)^{(1/2)}$.

0.2 Definition [Convex sets/bodies].

i) *A set* $X \subset \mathbb{R}^n$ *is called* convex, *iff for all* $x, y \in X$ *and* $\lambda \in [0, 1]$ *holds* $\lambda\, x + (1 - \lambda)\, y \in X$.

ii) *A convex compact (bounded and closed) subset* $K \subset \mathbb{R}^n$ *is called a* convex body. *The family of all convex bodies in* $\mathbb{R}^n$ *is denoted by* $\mathcal{K}^n$. $K \in \mathcal{K}^n$ *is called o-symmetric if* $K = -K = \{-x : x \in K\}$, *and the family of all o-symmetric convex bodies is denoted by* $\mathcal{K}_0^n$.

iii) *Let* $x_1, \dots, x_m \in \mathbb{R}^n$ *and let* $\lambda_i \geq 0$, $1 \leq i \leq m$, *such that* $\sum_{i=1}^m \lambda_i = 1$. *Then* $x = \sum_{i=1}^m \lambda_i\, x_i$ *is called a* convex combination *of* $x_1, \dots, x_m$.

0.3 Notation.

i) $\mathrm{vol}\,(X)$ *denotes for* $X \subset \mathbb{R}^n$ *the volume of* X, *i.e.,* $\mathrm{vol}\,(X) = \int_{\mathbb{R}^n} 1_X \,\mathrm{d}x$ *provided the Riemann integral of the characteristic function* 1_X *of* X *exists. A set* X *having a volume will be called* Jordan-measurable *or just measurable for short.*

ii) $B_n = \{x \in \mathbb{R}^n : |x| \leq 1\} \in \mathcal{K}_o^n$ *denotes the* n-dimensional unit ball *centered at* 0 *with radius 1. Its volume* $\mathrm{vol}\,(B^n)$ *is denoted by* κ_n *and it is given by*

$$\kappa_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2} + 1)}.$$

In particular we have $\kappa_1 = 2$, $\kappa_2 = \pi$, $\kappa_3 = \frac{4}{3}\pi$, $\kappa_4 = \frac{\pi^2}{2}$, *etc.*

iii) *For* $\mu \leq \lambda \in \mathbb{R}$ *the set* $[\mu, \lambda]^n = \{x \in \mathbb{R}^n : \mu \leq x_i \leq \lambda\} \in \mathcal{K}^n$ *describes the* n-dimensional rectangular box *of edge length* $\lambda - \mu$ *with* $\mathrm{vol}\,([\mu, \lambda]^n) = (\lambda - \mu)^n$. *The associated open or half open box is denoted by* $(\mu, \lambda)^n$ *or* $[\mu, \lambda)^n$, *etc.*

iv) *For a matrix* $A \in \mathbb{R}^{n \times n}$ *and a set* $X \subset \mathbb{R}^n$ *we denote by* $A\,X = \{Ax : x \in X\}$ *the image of* X *under the linear map induced by* A. *If* A *is non-singular and if* X *is "measurable" (it has a volume), then we have*

$$\mathrm{vol}\,(A\,X) = |\det(A)| \mathrm{vol}\,(X).$$

v) *For* $\lambda, \mu \in \mathbb{R}$ *and* $X, Y \subset \mathbb{R}^n$ *we write*

$$\lambda \cdot X + \mu \cdot Y = \{\lambda x + \mu y : x \in X,\, y \in Y\}.$$

0.4 Lemma. *Let $X \subset \mathbb{R}^n$ be a Jordan-measurable set. Then*

$$\operatorname{vol}(X) = \lim_{m\to\infty} \frac{\#(X \cap \frac{1}{m}\mathbb{Z}^n)}{m^n}.$$

Proof. Follows by the definition of a Riemann integrability. □

1 Some basic facts about lattices

1.1 Definition [Lattice]. *Let $b_1, \dots, b_n \in \mathbb{R}^n$ be linearly independent. The set*

$$\Lambda = \{z_1 b_1 + z_2 b_2 + \cdots + z_n b_n : z_i \in \mathbb{Z},\, 1 \le i \le n\}$$

is called lattice. *The set of generating vectors $\{b_1, \dots, b_n\}$ or the matrix $B = (b_1, \dots, b_n)$ with columns b_i is called* basis *of Λ. An element $b \in \Lambda$ is called* lattice point *of Λ. The set of all lattices in $\mathbb{R}^n$ is denoted by $\mathcal{L}^n$.*

1.2 Remark.

i) *The unit vectors $e_1, \dots, e_n \in \mathbb{R}^n$ form a basis of the* integral lattice *(*standard lattice*)* $\mathbb{Z}^n = \{z \in \mathbb{R}^n : z_i \in \mathbb{Z}\}$.

ii) *Let $B = (b_1, \dots, b_n)$ be a basis of Λ. Then $\Lambda = B\mathbb{Z}^n$ and, in particular, Λ is a subgroup of $\mathbb{R}^n$, i.e., $b - \bar{b} \in \Lambda$ for all $b, \bar{b} \in \Lambda$.*

iii) $\Lambda = \begin{pmatrix} 25 & 64 \\ 16 & 41 \end{pmatrix} \mathbb{Z}^2 = \mathbb{Z}^2$.

1.3 Definition [Unimodular matrix]. *An integral matrix $U \in \mathbb{Z}^{n\times n}$ is called* unimodular *iff $|\det U| = 1$. The group of all unimodular matrices is denoted by* $\mathrm{GL}(n, \mathbb{Z})$.

Oberserve that a matrix is unimodular if and only the matrix and its inverse are integral matrices.

1.4 Proposition. $\mathrm{GL}(n, \mathbb{Z}) = \{U \in \mathbb{R}^{n\times n} : U\mathbb{Z}^n = \mathbb{Z}^n\}$.

Proof. $U \in \mathrm{GL}(n, \mathbb{Z})$ if and only if $U, U^{-1} \in \mathbb{Z}^{n\times n}$ wich is equivalent to $U\,\mathbb{Z}^n \subseteq \mathbb{Z}^n$ and $U^{-1}\,\mathbb{Z}^n \subseteq \mathbb{Z}^n$. Since the last inclusion is equivalent to $\mathbb{Z}^n \subseteq U\,\mathbb{Z}^n$ we are done. □

1.5 Lemma. *Let $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. $A = (a_1, \dots, a_n)$ is a basis of Λ iff there exists a $U \in \mathrm{GL}(n, \mathbb{Z})$ such that $A = B\,U$.*

Proof. A is a basis of Λ if and only if $A\,\mathbb{Z}^n = \Lambda = B\,\mathbb{Z}^n$ which is equivalent to $B^{-1}A \in \mathrm{GL}(n, \mathbb{Z})$ by Proposition 1.4. □

1.6 Definition [Determinant, fundamental cell]. *Let $\Lambda \in \mathcal{L}^n$ with basis $B = (b_1, \dots, b_n)$.*

i) $\det \Lambda = |\det B|$ *is called* determinant *of Λ.*

ii) $P_B = \{\rho_1 b_1 + \cdots + \rho_n b_n : 0 \le \rho_i < 1,\, 1 \le i \le n\} = B\,[0,1)^n$ *is called* fundamental cell *or* fundamental parallelepiped *of Λ (w.r.t. the basis B).*

1.7 Remark.

i) $\det \Lambda$ *is independent of the choice of the basis (cf. Lemma 1.5).*

ii) $\det \Lambda = \mathrm{vol}\,(P_B)$ *and* $\det(\mu\Lambda) = |\mu|^n \det \Lambda$, $\mu \in \mathbb{R}$.

iii) $\det \Lambda \leq |b_1|\,|b_2| \cdot \ldots \cdot |b_n|$, *with equality if and only if the vectors* b_i *are pairwise orthogonal (Hadamard inequality).*

iv) $P_B \cap \Lambda = \{0\}$. *Since* $(P_B - P_B) = B\,(-1,1)^n$ *we even have* $(P_B - P_B) \cap \Lambda = \{0\}$.

1.8 Notation. *Let* $a_1, \ldots, a_n \in \mathbb{R}^n$ *be linearly independent and let* $A = (a_1, \ldots, a_n)$. *Let* $x \in \mathbb{R}^n$ *with* $x = \sum_{i=1}^n \rho_i a_i$, $\rho_i \in \mathbb{R}$. *Then we write* $\lfloor x \rfloor_A = \sum_i \lfloor \rho_i \rfloor a_i$. *In particular,* $\lfloor x \rfloor_A \in A\mathbb{Z}^n$ *and* $x - \lfloor x \rfloor_A \in P_A$.

1.9 Proposition. *Let* $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. *Then*

$$\mathbb{R}^n = \bigcup_{b \in \Lambda} (b + P_B)\,,$$

i.e., $\mathbb{R}^n$ *is the pairwise disjunct union of the lattice translates* $b + P_B$.

Proof. Each $x \in \mathbb{R}^n$ can be decomposed as $x = (x - \lfloor x \rfloor_B) + \lfloor x \rfloor_B$. The first summand is in P_B and second is a lattice point of Λ. To show that the union is disjunct we observe that the intersection of two lattice translates $b + P_B, \overline{b} + P_B$ of P_B, $b, \overline{b} \in \Lambda$, is non-empty, if and only if $b - \overline{b} \in (P_B - P_B) \cap \Lambda$. By Remark 1.7 iv) this is equivalent to $b = \overline{b}$. □

1.10 Definition [Discrete set]. *A set* $S \subset \mathbb{R}^n$ *is called* discrete *iff there exists an* $\epsilon > 0$ *such that* $|s_1 - s_2| \geq \epsilon$ *for all* $s_1, s_2 \in S$, $s_1 \neq s_2$.

1.11 Theorem. *$S \subset \mathbb{R}^n$ is a lattice if and only if S a discrete subgroup of $\mathbb{R}^n$ and it contains n linearly independent points.*

1.12 Definition [Index of a sublattice]. *Let* $\Lambda \in \mathcal{L}^n$ *and let* $a_1, \ldots, a_n \in \Lambda$ *be linearly independent.*

$$\Lambda_0 = \{z_1 a_1 + \cdots + z_n a_n : z_i \in \mathbb{Z}\}$$

is called a sublattice *with basis* $A = (a_1, \ldots, a_n)$. *The number of cosets of the subgroup* Λ_0 *in* Λ, *i.e., the* index of Λ_0 in Λ *is denoted by* $|\Lambda : \Lambda_0|$.

1.13 Lemma. *Let* $\Lambda_0 \subseteq \Lambda \in \mathcal{L}^n$ *be a sublattice of* Λ. *Then*

i) $|\Lambda : \Lambda_0| = \#(P_A \cap \Lambda)$ *for any basis* A *of* Λ_0.

ii) $|\Lambda : \Lambda_0| = \det \Lambda_0 / \det \Lambda$.

1.14 Corollary. *Let $z_1, \dots, z_n \in \mathbb{Z}^n$ be linearly independent. Then*

$$|\det(z_1, \dots, z_n)| = \#\big(\{\rho_1 z_1 + \cdots + \rho_n z_n : 0 \le \rho_i < 1\} \cap \mathbb{Z}^n\big).$$

Proof. We just apply Lemma 1.13 i), ii) with $\Lambda = \mathbb{Z}^n$ and Λ_0 being the lattice generated by $z_1, \dots, z_n$. □

1.15 Remark. *Let $\Lambda_0 = A\mathbb{Z}^n \subseteq \Lambda \in \mathcal{L}^n$ be a sublattice of Λ. Then*

$$\begin{aligned} &A \text{ is basis of } \Lambda \Leftrightarrow |\Lambda : \Lambda_0| = 1 \Leftrightarrow \Lambda \cap P_A = \{0\} \\ &\quad \Leftrightarrow \Lambda \cap \{\rho_1 a_1 + \cdots + \rho_n a_n : 0 \le \rho_i \le 1\} = \{\epsilon_1 a_1 + \cdots + \epsilon_n a_n : \epsilon_i \in \{0,1\}\}. \end{aligned}$$

1.16 Proposition. *Let $\Lambda \in \mathcal{L}^2$ and let $a_1, a_2 \in \Lambda$ be linearly independent. Then*

$$a_1, a_2 \text{ basis of } \Lambda \Leftrightarrow \operatorname{conv}\{0, a_1, a_2\} \cap \Lambda = \{0, a_1, a_2\}.$$

Proof. If a_1 and a_2 are basis then every point of Λ has an unique representation as an integral linear combination of a_1 and a_2. Hence $\operatorname{conv}\{0, a_1, a_2\} \cap \Lambda = \{0, a_1, a_2\}$. In order to show the reverse implication we set $T_A = \operatorname{conv}\{0, a_1, a_2\}$ and $\overline{P_A} = \{\rho_1 a_1 + \rho_2 a_2 : 0 \le \rho_1, \rho_2 \le 1\}$. By Remark 1.15 it suffices to verify that $\overline{P_A} \cap \Lambda = \{0, a_1, a_2, a_1 + a_2\}$. Let $b \in \overline{P_A} \cap \Lambda$. If $b \in T_A \cap \Lambda$ then we have $b \in \{0, a_1, a_2\}$. Hence we may assume $b \notin T_A$ and thus $b = \rho_1 a_1 + \rho_2 a_2$ with $0 \le \rho_1, \rho_2 \le 1$, but $\rho_1 + \rho_2 > 1$. So we have $(1 - \rho_1) + (1 - \rho_2) \le 1$ and thus

$$(a_1 + a_2) - b = (1 - \rho_1)a_1 + (1 - \rho_2)a_2 \in T_A,$$

which shows $b \in \{a_1, a_2, a_1 + a_2\}$. □

1.17 Remark. *An analogous statement to Lemma 1.16 does not exist in dimension ≥ 3. For $n \ge 3$ and $m \in \mathbb{N}$ let $b(m) = (1, \dots, 1, m)^\intercal \in \mathbb{R}^n$ and $T^n(m) = \operatorname{conv}\{0, e_1, \dots, e_{n-1}, b(m)\}$. Then*

$$T^n(m) \cap \mathbb{Z}^n = \{0, e_1, \dots, e_{n-1}, b(m)\},$$

but the determinant of the lattice with basis $\{e_1, \dots, e_{n-1}, b(m)\}$ is m. $T^n(m)$ are called Reeve simplices.

1.18 Definition [Lattice planes, k-dimensional (sub)lattices]. *Let $\Lambda \in \mathcal{L}^n$.*

i) *A k-dimensional linear subspace L_k is called a* k-dimensional lattice plane *of Λ if $\dim(L_k \cap \Lambda) = k$. The set of all k-dimensional lattice planes of Λ is denoted by $\mathcal{L}(k, \Lambda)$.*

ii) *Let $L_k \in \mathcal{L}(k, \Lambda)$. Then $\Lambda_k = L_k \cap \Lambda$ will be called a* k-dimensional (sub)lattice of Λ.

1.19 Remark. *Let $L_k \in \mathcal{L}(k, \Lambda)$. Then $\Lambda_k = L_k \cap \Lambda$ is a k-dimensional lattice (in the Euclidean space L_k) and if $b_1, \dots, b_k \in \Lambda_k$ is a basis of Λ_k then*

$$\det \Lambda_k = \sqrt{\det \left((b_1, \dots, b_k)^\intercal (b_1, \dots, b_k) \right)}.$$

1.20 Definition [Polar lattice]. *Let $\Lambda \in \mathcal{L}^n$ with basis $b_1, \dots, b_n$. Let $b_i^\star \in \mathbb{R}^n$, $1 \le i \le n$ be given by*

$$\langle b_j, b_i^\star \rangle = \delta_{i\,j} = \begin{cases} 0, & i \neq j \\ 1, & i = j, \end{cases}, \quad 1 \le j \le n.$$

The lattice $\Lambda^\star$ with basis $b_1^\star, \dots, b_n^\star$ is called the polar lattice *of Λ.*

1.21 Remark.

i) *If $B = (b_1, \dots, b_n)$ is a basis of Λ then $(b_1^\star, \dots, b_n^\star) = B^{-\intercal}$. In particular, the definition of the polar lattice is independent of the basis B of Λ.*

ii) $\det \Lambda^\star = \det(\Lambda)^{-1}$.

1.22 Proposition. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then*

$$\Lambda^\star = \{ y \in \mathbb{R}^n : \langle b, y \rangle \in \mathbb{Z} \text{ for all } b \in \Lambda \}.$$

Proof. Let B be a basis of Λ and let $y = B^{-\intercal} x \in \mathbb{R}^n$ with $x \in \mathbb{R}^n$. Then

$$\begin{aligned} y \in \Lambda^\star &\Leftrightarrow x \in \mathbb{Z}^n \Leftrightarrow x^\intercal z \in \mathbb{Z} \text{ for all } z \in \mathbb{Z}^n \\ &\Leftrightarrow (B^{-\intercal} x)^\intercal B z \in \mathbb{Z} \text{ for all } z \in \mathbb{Z}^n \Leftrightarrow (y)^\intercal B z \in \mathbb{Z} \text{ for all } z \in \mathbb{Z}^n. \end{aligned}$$

□

2 Minkowski's theorems on successive minima

2.1 Lemma. *Let $X \subset \mathbb{R}^n$ be a bounded Jordan-measurable set.*

i) *If $(z_1 + X) \cap (z_2 + X) = \emptyset$, for all $z_1, z_2 \in \mathbb{Z}^n$, $z_1 \neq z_2$, then* $\mathrm{vol}\,(X) \leq 1$.

ii) *If $\mathbb{Z}^n + X = \mathbb{R}^n$ then* $\mathrm{vol}\,(X) \geq 1$.

Proof. Let $P = [0,1)^n$ be the fundamental cell of $\mathbb{Z}^n$ Since $\mathbb{Z}^n + P$ is a tiling of $\mathbb{R}^n$ (cf. Proposition 1.9) and the volume is a translation invariant functional we may write

$$\mathrm{vol}\,(X) = \mathrm{vol}\,((\mathbb{Z}^n + P) \cap X) = \sum_{z \in \mathbb{Z}^n} \mathrm{vol}\,((z + P) \cap X) = \sum_{z \in \mathbb{Z}^n} \mathrm{vol}\,(P \cap (X - z))\,.$$

In the first case we have $[P \cap (X - z_1)] \cap [P \cap (X - z_2)] = \emptyset$ for $z_1 \neq z_2 \in \mathbb{Z}^n$, and thus

$$\sum_{z \in \mathbb{Z}^n} \mathrm{vol}\,(P \cap (X - z)) = \mathrm{vol}\,(\cup_{z \in \mathbb{Z}^n} (P \cap (X - z))) \leq \mathrm{vol}\,(P) = 1.$$

In the second case we find

$$\sum_{z \in \mathbb{Z}^n} \mathrm{vol}\,(P \cap (X - z)) \geq \mathrm{vol}\,(\cup_{z \in \mathbb{Z}^n} (P \cap (X - z))) = \mathrm{vol}\,(P) = 1.$$

□

2.2 Corollary. *Let $X \subset \mathbb{R}^n$ with* $\mathrm{vol}\,(X) > 1$. *Then $(X - X) \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$.*

Proof. By Lemma 2.1 i) there exist $z_1, z_2 \in \mathbb{Z}^n$, $z_1 \neq z_2$, and a $x \in \mathbb{R}^n$ such that $x \in (z_1 + X) \cap (z_2 + X)$. Thus $x - z_1$, $x - z_2 \in X$ and $(x - z_1) - (x - z_2) \in \mathbb{Z}^n$. □

2.3 Theorem [Minkowski, 1896]. *Let $K \in \mathcal{K}_0^n$ with* $\mathrm{vol}\,(K) \geq 2^n$. *Then*

$$K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset,$$

i.e., a o-symmetric convex body of volume at least 2^n contains a non-trivial lattice point.

Proof. First we assume $\mathrm{vol}\,(K) > 2^n$. Then we have $\mathrm{vol}\,(\frac{1}{2}K) > 1$ and by Corollary 2.2 there exists $z \in \mathbb{Z}^n \setminus \{0\}$ with $z \in \frac{1}{2}K - \frac{1}{2}K = K$.

Now let $\mathrm{vol}\,(K) = 2^n$ and suppose $K \cap \mathbb{Z}^n = \{0\}$. Since K is compact there exists a $\lambda > 1$ with $\lambda K \cap \mathbb{Z}^n = \{0\}$. However $\mathrm{vol}\,(\lambda K) > 2^n$ and thus we get a contradiction to the previous case.

□

2.4 Corollary. *Let $\Lambda \in \mathcal{L}^n$ and $K \in \mathcal{K}_0^n$ with* $\mathrm{vol}\,(K) \geq 2^n \det \Lambda$. *Then*

$$K \cap \Lambda \setminus \{0\} \neq \emptyset.$$

Proof. Let B be a basis of Λ. Then we observe that

$$K \cap \Lambda = B\left(B^{-1}K \cap \mathbb{Z}^n\right) \quad \text{and} \quad \operatorname{vol}(B^{-1}K) = \frac{\operatorname{vol}(K)}{\det \Lambda} \geq 2^n.$$

Thus the corollary is an immediate consequence of Theorem 2.3. □

2.5 Definition [Successive minima]. *Let $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. For $1 \leq i \leq n$,*

$$\lambda_i(K, \Lambda) = \min\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geq i\}$$

is called the i-th successive minimum *(of K w.r.t. Λ).*

2.6 Remark.

i) $\lambda_i(K, \Lambda) \geq \lambda_{i-1}(K, \Lambda)$, $2 \leq i \leq n$.

ii) $\lambda_i(K, \Lambda) = \lambda_i(AK, A\Lambda)$, $A \in \mathrm{GL}(n, \mathbb{R})$, *i.e.*, $A \in \mathbb{R}^{n\times n}$ *with* $\det A \neq 0$.

iii) $\lambda_i(\mu\, K, \Lambda) = \frac{1}{\mu}\lambda_i(K, \Lambda) = \lambda_i(K, \frac{1}{\mu}\Lambda)$, $\mu \in \mathbb{R}$, $\mu \neq 0$.

iv) $\operatorname{int} K \cap \Lambda \setminus \{0\} = \emptyset \Leftrightarrow \lambda_1(K, \Lambda) \geq 1$.

v) $\lambda_1(B^n, \Lambda) = \min\big\{|b| : b \in \Lambda \setminus \{0\}\big\}$.

2.7 Proposition. *Let $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Let $a_1, \ldots, a_n \in \Lambda$ be linearly independent such that $a_i \in \lambda_i(K, \Lambda)\, K$, $1 \leq i \leq n$. Then*

$$\operatorname{int}\,(\lambda_i(K, \Lambda)\, K) \cap \Lambda \subset \operatorname{lin}\{a_1, \ldots, a_{i-1}\},\ 1 \leq i \leq n,$$

where we set $\operatorname{lin} \emptyset = \{0\}$.

Proof. Immediate consequence of the facts that $\dim\Big(\operatorname{int}\big(\lambda_i(K, \Lambda)\, K\big) \cap \Lambda\Big) \leq i - 1$, $1 \leq i \leq n$, and that the $\lambda_i(K, \Lambda)$ are an increasing sequence. □

2.8 Theorem [Minkowski's first theorem on successive minima]. *Let $K \in \mathcal{K}_0^n$ and $\Lambda \in \mathcal{L}^n$. Then*

$$\lambda_1(K, \Lambda)^n \operatorname{vol}(K) \leq 2^n \det \Lambda.$$

Proof. By the definition of $\lambda_1(K, \Lambda)$ it is $\operatorname{int}(\lambda_1(K, \Lambda)\, K) \cap \Lambda \setminus \{0\} = \emptyset$ and so by Corollary 2.4 we get $\operatorname{vol}(\lambda_1(K, \Lambda)\, K) \leq 2^n \det \Lambda$. □

textcolormproof

2.9 Theorem [Minkowski's second theorem on successive minima]. *Let $K \in \mathcal{K}_0^n$ and $\Lambda \in \mathcal{L}^n$. Then*

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1(K, \Lambda)\, \lambda_2(K, \Lambda) \cdot \ldots \cdot \lambda_n(K, \Lambda) \operatorname{vol}(K) \leq 2^n \det \Lambda.$$

Obviously, both bounds of Minkowski's second theorem are best possible. For instance, the lower bound is attained by the regular cross-polytope $C_n^\star$ and the upper bound by any o-symmetric box with edges parallel to the coordinate edges.

3 Transference theorems

3.1 Notation. *For $K \in \mathcal{K}_o^n$ let $|x|_K = \min\{\rho \geq 0 : x \in \rho K\}$ be the norm induced by K.*

3.2 Definition [Polar body]. *Let $K \in \mathcal{K}_o^n$. Then*

$$K^\star = \{y \in \mathbb{R}^n : \langle x, y\rangle \leq 1 \quad \text{for all } x \in K\}$$

is called the polar body of K.

3.3 Remark. *Let $K \in \mathcal{K}_o^n$.*

i) *$K^\star \in \mathcal{K}_o^n$ and*

$$|y|_{K^\star} = \max\{\langle x, y\rangle : x \in K\} = \max\left\{\frac{\langle x, y\rangle}{|x|_K} : x \in \mathbb{R}^n \setminus \{0\}\right\}.$$

ii) $(B_n)^\star = B_n$.

iii) *$K_1, K_2 \in \mathcal{K}_o^n$ with $K_1 \subseteq K_2$. Then ${K_2}^\star \subseteq {K_1}^\star$.*

iv) *Let $A \in \mathbb{R}^{n\times n}$, $\det A \neq 0$. Then $(AK)^\star = A^{-\intercal}K^\star$.*

3.4 Theorem [Bourgain&Milman and Blaschke&Santaló]. *Let $K \in \mathcal{K}_o^n$. Then*

$$\frac{\mathrm{c}^n}{n!} \leq \mathrm{vol}\,(K)\,\mathrm{vol}\,(K^\star) \leq \mathrm{vol}\,(B_n)^2,$$

where c *is an universal constant.*

3.5 Lemma. *Let $K \in \mathcal{K}_o^n$ and $\Lambda \in \mathcal{L}^n$. Then*

$$\lambda_1(K, \Lambda)\,\lambda_1(K^\star, \Lambda^\star) \leq \mathrm{c}\,n,$$

where c *is a universal constant.*

Proof. By Minkowski's Theorem 2.8 we have

$$\lambda_1(K, \Lambda) \leq \frac{2\det\Lambda^{1/n}}{\mathrm{vol}\,(K)^{1/n}} \quad \text{and} \quad \lambda_1(K^\star, \Lambda^\star) \leq \frac{2\det\Lambda^{\star 1/n}}{\mathrm{vol}\,(K^\star)^{1/n}}.$$

Multiplying both inequalities and applying the lower bound of Theorem 3.4 to the product $\mathrm{vol}\,(K)\,\mathrm{vol}\,(K^\star)$ gives the desired bound. □

3.6 Theorem [Conway&Thompson]. *For any n there exist lattices $\Lambda \in \mathcal{L}^n$ with $\Lambda = \Lambda^\star$ and*

$$\lambda_1(B_n, \Lambda)\,\lambda_1(B_n, \Lambda^\star) \geq \mathrm{c}\,n,$$

where c *is an universal constant.*

3.7 Definition [Inhomogeneous minimum or Covering radius]. *Let $K \in \mathcal{K}^n$ and $\Lambda \in \mathcal{L}^n$. The number*

$$\mu(K, \Lambda) = \min\{\mu > 0 : \Lambda + \mu\, K = \mathbb{R}^n\}$$

is called the inhomogeneous minimum *or* covering radius *of K w.r.t. Λ.*

3.8 Remark.

i) *By Lemma 2.1 ii) we have $\mu(K, \Lambda) \geq (\det \Lambda / \mathrm{vol}\,(K))^{1/n}$.*

ii) *For $K \in \mathcal{K}^n_o$ we can also write $\mu(K, \Lambda) = \max_{x \in \mathbb{R}^n} \min_{b \in \Lambda} |x - b|_K$.*

3.9 Definition [Lattice width]. *Let $K \in \mathcal{K}^n$ and $\Lambda \in \mathcal{L}^n$.*

$$\mathrm{w}_\Lambda(K) = \min_{b \in \Lambda^\star \setminus \{0\}} \left(\max_{x \in K} \langle b, x \rangle - \min_{y \in K} \langle b, y \rangle \right)$$

is called the lattice width *of K with respect to Λ.*

3.10 Proposition. *Let $K \in \mathcal{K}^n$ and $\Lambda \in \mathcal{L}^n$.*

i) $\mathrm{w}_\Lambda(K) = \lambda_1((K - K)^\star, \Lambda^\star)$.

.

Proof. For i) we observe that (cf. Remark 3.3 i))

$$\mathrm{w}_\Lambda(K) = \min_{b \in \Lambda^\star \setminus \{0\}} \max_{z \in K - K} \langle b, z \rangle = \min_{b \in \Lambda^\star \setminus \{0\}} |b|_{(K-K)^\star} = \lambda_1((K - K)^\star, \Lambda^\star).$$

□

3.11 Corollary [Flatness Theorem]. *Let $K \in \mathcal{K}^n$ and $\Lambda \in \mathcal{L}^n$ with $K \cap \Lambda = \emptyset$. Then $\mathrm{w}_\Lambda(K) \leq \mathrm{c}\, n^{7/2}$, where c is an universal constant.*

Proof. Since $K \cap \Lambda = \emptyset$ we have $\mu(K, \Lambda) \geq 1$ and with Proposition 3.10 ii) we are done. □

4 Packing

4.1 Definition [Packing sets]. *A subset $D \subset \mathbb{R}^n$ is called a* packing set *of $K \in \mathcal{K}^n$ if for all $x, y \in D$, $x \neq y$,*

$$(x + \operatorname{int} K) \cap (y + \operatorname{int} K) = \emptyset.$$

The family of all packing sets of K is denoted by $\mathcal{P}(K)$.

4.2 Definition [Density of a Packing]. *Let $K \in \mathcal{K}^n$ and $D \in \mathcal{P}(K)$.*

$$\delta(K, D) = \limsup_{\lambda \to \infty} \frac{\operatorname{vol}(K) \#\big\{x \in D : x + K \subset \lambda\, C_n\big\}}{\operatorname{vol}\big(\lambda\, C_n\big)}$$

is called the density of the packing $D + K$ *(with respect to the gauge body $C_n = [-1, 1]^n$).*

4.3 Theorem. *Let $K \in \mathcal{K}^n$. The supremum $\sup\big\{\delta(K, D) : D \in \mathcal{P}(K)\big\}$ is independent of the chosen gauge body, and there exists a packing set $D_K \in \mathcal{P}(K)$ such that*

$$\sup\big\{\delta(K, D) : D \in \mathcal{P}(K)\big\} = \delta(K, D_K).$$

4.4 Definition [Density of a Densest Packing]. *Let $K \in \mathcal{K}^n$.*

$$\delta(K) = \sup\big\{\delta(K, D) : D \in \mathcal{P}(K)\big\}$$

is called the density of a densest packing of K *and a set $D_K \in \mathcal{P}(K)$ with $\delta(K) = \delta(K, D_K)$ is called a* densest packing set of K.

4.5 Lemma. *Let $S \subset \mathbb{R}^n$ be a bounded and measurable set with $\operatorname{vol}(S) > 0$ and let $D \in \mathcal{P}(K)$. Then there exist $v, w \in \mathbb{R}^n$ such that*

$$\frac{\operatorname{vol}(K)\, \#\big\{(w + S) \cap D\big\}}{\operatorname{vol}(S)} \leq \delta(K, D) \leq \frac{\operatorname{vol}(K)\, \#\big\{(v + S) \cap D\big\}}{\operatorname{vol}(S)}.$$

4.6 Corollary. *Let $K \in \mathcal{K}^n$ and $\Lambda \in \mathcal{L}^n \cap \mathcal{P}(K)$. Then*

$$\delta(K, \Lambda) = \frac{\operatorname{vol}(K)}{\det \Lambda}.$$

Proof. Let P_B be a fundamental cell of Λ. By Proposition 1.9, $\mathbb{R}^n$ is the pairwise disjoint union of the translates $b+P_B$, $b \in \Lambda$. Hence $\#\{(x+P_B)\cap\Lambda\} \leq 1$ for all $x \in \mathbb{R}^n$, whereas the property that $\mathbb{R}^n$ is covered by all translates is equivalent to the lower bound $\#\{(x + P_B) \cap \Lambda\} \geq 1$ for all $x \in \mathbb{R}^n$. Hence $\#\{(x + P_B) \cap \Lambda\} = 1$ for all $x \in \mathbb{R}^n$. Together with $\mathrm{vol}\,(P_B) = \det \Lambda$ the identity follows from Lemma 4.5.

□

4.7 Definition [Density of a densest Lattice Packing]. *For $K \in \mathcal{K}^n$ the set $\mathcal{P}_\mathcal{L}(K) = \mathcal{L}^n \cap \mathcal{P}(K)$ is called the family of all* packing lattices *of K. For $\Lambda \in \mathcal{P}_\mathcal{L}(K)$ the arrangement $\Lambda + K$ is called a* lattice packing *of K and*

$$\delta_\mathcal{L}(K) = \sup\big\{\delta(K, \Lambda) : \Lambda \in \mathcal{P}_\mathcal{L}(K)\big\}$$

is called the density of a densest lattice packing of K.

4.8 Theorem [K. Ball, 1992]. $\delta(B_n) \geq (n-1)2^{-(n-1)}\zeta(n)$.

4.9 Theorem [Fejes Tóth, 1950; Rogers, 1951]. *Let $K \in \mathcal{K}^2$. Then*

$$\delta(K) = \delta_\mathcal{L}(K).$$

4.10 Theorem [Hales, 1998/2005].

$$\delta(B_3) = \delta_\mathcal{L}(B_3) = \frac{\pi}{3\sqrt{2}}.$$

Index