GEOMETRY OF NUMBERS E

Tapani Matala-aho, Aalto University, 2023

References

Lenny Fukshansky, Link: Geometric Number Theory, Lecture notes.

W. M. Schmidt, Diophantine approximation. Lecture Notes in Mathematics, 785. Springer, Berlin, 1980.

See, pages 3–9.

Notations

Let $\overline{a} \in \mathbb{R}^n$ and $R \in \mathbb{R}_{\geq 0}$. For an $\overline{a}$-centered Euclidean n-ball of radius R we use notation

$$\mathcal{B}^n(R, \overline{a}) := \{\overline{x} \in \mathbb{R}^n | \ \|\overline{x} - \overline{a}\|_2 \leq R\}.$$

and a shorthand notation

$$\mathcal{B}^n(R) := \mathcal{B}^n(R, \overline{0})$$

for an origin-centered ball.

Successive minima

Definition 1

Let $n \in \mathbb{Z}^+$. Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice and let $\mathcal{C}$ be a non-empty subset of $\mathbb{R}^n$. The successive minima $\lambda_1, ..., \lambda_n$ of $\mathcal{C}$ with respect to Λ are given by

$$\lambda_j = \lambda_j(\mathcal{C}, \Lambda) = \inf \left\{ \lambda > 0 \,|\, \operatorname{rank} \left\langle (\lambda \mathcal{C}) \cap \Lambda \right\rangle_{\mathbb{Z}} \geq j \right\}. \tag{1}$$

Note, that $\lambda_j = \lambda_j(\mathcal{C}, \Lambda)$ depends on the set $\mathcal{C}$ and the lattice Λ.

Lemma 2

$$0 < \lambda_1 \leq \cdots \leq \lambda_n < \infty.$$

The first Minkowski's convex body theorem revised

Theorem 3

Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is a central symmetric convex body. Then

$$\mathrm{vol}(\lambda_1 \cdot \mathcal{C}) \leq 2^n \det \Lambda. \tag{2}$$

Note that

$$\mathrm{vol}(\lambda_1 \cdot \mathcal{C}) = \lambda_1^n \mathrm{vol}(\mathcal{C}). \tag{3}$$

The first Minkowski's convex body theorem revised

Proof. If not (2), then $\mathrm{vol}\,(\lambda_1 \cdot \mathcal{C}) > 2^n \det \Lambda$ which means that there exists a $\lambda < \lambda_1$ such that $\mathrm{vol}\,(\lambda \cdot \mathcal{C}) > 2^n \det \Lambda$. By the first Minkowski's convex body theorem there exists a non-zero point in $(\lambda \cdot \mathcal{C}) \cap \Lambda$. Thus

$$\mathrm{rank}\,\big\langle (\lambda \cdot \mathcal{C}) \cap \Lambda \big\rangle_{\mathbb{Z}} \geq 1 \tag{4}$$

which contradicts the definition of

$$\lambda_1 = \inf\{\lambda > 0 \,|\; \mathrm{rank}\,\langle (\lambda \mathcal{C}) \cap \Lambda \rangle_{\mathbb{Z}} \geq 1\}. \quad \square \tag{5}$$

Successive minima

Example 4

Let $k < l \in \mathbb{Z}^+$ and define an orthotope or cuboid

$$\mathcal{T} := \left\{ \overline{x} \in \mathbb{R}^3 \,\middle|\, |x_1| \leq \frac{1}{k},\ |x_2| \leq \frac{1}{l},\ |x_3| \leq kl \right\}.$$

Then $\lambda_1 = \frac{1}{kl} < \lambda_2 = k < \lambda_3 = l$ are the successive minima of $\mathcal{T}$ with respect to a lattice $\mathbb{Z}^3$.

Proof.

$$\lambda\mathcal{T} := \left\{ (\lambda x_1, \lambda x_1, \lambda x_1) \,\middle|\, |\lambda x_1| \leq \frac{\lambda}{k},\ |\lambda x_2| \leq \frac{\lambda}{l},\ |\lambda x_3| \leq \lambda kl \right\}. \tag{6}$$

Successive minima

0. If $\lambda < \frac{1}{kl}$, then there are no non-zero lattice points in $\lambda\mathcal{T}$ because

$$|\lambda x_1| \leq \frac{\lambda}{k} < 1,\ |\lambda x_2| \leq \frac{\lambda}{l} < 1,\ 0 \leq |\lambda x_3| \leq \lambda kl < 1\}. \tag{7}$$

1. If $\lambda = \frac{1}{kl}$, then

$$|\lambda x_1| \leq \frac{\lambda}{k} = \frac{1}{k^2 l} < 1,\ |\lambda x_2| \leq \frac{\lambda}{l} = \frac{1}{kl^2} < 1,\ |\lambda x_3| \leq \lambda kl = 1\}. \tag{8}$$

Hence $\lambda x_1 = \lambda x_2 = 0$ but $\lambda x_3 = 1$, if we choose $x_3 = kl$. Therefore $(0, 0, 1) \in (\frac{1}{kl} \cdot \mathcal{T}) \cap \Lambda$ and thus

$$\lambda_1 = \inf\{\lambda > 0 \mid \operatorname{rank} \langle(\lambda\mathcal{T}) \cap \Lambda\rangle_{\mathbb{Z}} \geq 1\} = \frac{1}{kl}. \tag{9}$$

Successive minima

2. If $\lambda = k$, then

$$|\lambda x_1| \leq \frac{\lambda}{k} = 1,\ |\lambda x_2| \leq \frac{\lambda}{l} = \frac{k}{l} < 1,\ |\lambda x_3| \leq \lambda k l = k^2 l > 1\}. \qquad (10)$$

Hence $\lambda x_2 = 0$ but $\lambda x_1 = \lambda x_3 = 1$, if we choose $x_1 = 1/k$ and $x_3 = kl$.

Therefore $(0,0,1),(1,0,1) \in (k\mathcal{T}) \cap \Lambda$ but $(1,0,1) \notin (\lambda\mathcal{T}) \cap \Lambda$ if $\lambda < k$.

Thus

$$\lambda_2 = \inf\{\lambda > 0 \mid \text{ rank } \langle(\lambda\mathcal{T}) \cap \Lambda\rangle_{\mathbb{Z}} \geq 2\} = k. \qquad (11)$$

Successive minima

3. If $\lambda = l$, then

$$|\lambda x_1| \leq \frac{l}{k} > 1, \ |\lambda x_2| \leq \frac{\lambda}{l} = 1, \ |\lambda x_3| \leq \lambda k l = k l^2 > 1\}. \tag{12}$$

Therefore $(0,0,1), (1,0,1), (0,1,0) \in (l \cdot \mathcal{T}) \cap \Lambda$ but $(0,1,0) \notin (\lambda \mathcal{T}) \cap \Lambda$ if $\lambda < l$. Thus

$$\lambda_3 = \inf\{\lambda > 0 \,|\, \text{ rank}\,\langle(\lambda\mathcal{T}) \cap \Lambda\rangle_{\mathbb{Z}} \geq 3\} = l. \tag{13}$$

Successive minima

Furthermore, in this example holds

$$\operatorname{rank} \langle (\lambda_j \mathcal{T}) \cap \Lambda \rangle_{\mathbb{Z}} = j, \quad j = 1, 2, 3. \tag{14}$$

Successive minima

Example 5

Define a triangle or hexagonal lattice

$$\Lambda_2 := \langle \overline{\ell}_1, \overline{\ell}_2 \rangle_{\mathbb{Z}}, \quad \overline{\ell}_1 := \frac{1}{2}\overline{e}_1, \ \overline{\ell}_2 := \frac{1}{4}\overline{e}_1 + \frac{\sqrt{3}}{4}\overline{e}_2.$$

Now $\|\overline{\ell}_1\|_2 = \|\overline{\ell}_2\|_2 = \frac{1}{2}$, so that $\overline{\ell}_1$ and $\overline{\ell}_2$ stay at the boundary of the 2-ball

$$\mathcal{B}^2(1/2) := \{\overline{x} \in \mathbb{R}^2 | \ \|\overline{x}\|_2 \leq 1/2\}$$

of radius $\frac{1}{2}$. Thus $\lambda_1 = \lambda_2 = 1$ are the successive minima of $\mathcal{B}^2(1/2)$ with respect to the lattice Λ_2.

Successive minima

Example 6

If we choose a different 2-ball, $\mathcal{B}^2(1)$. Then $\beta_1 = \beta_2 = 1/2$ are the successive minima of $\mathcal{B}^2(1)$ with respect to a lattice Λ_2. Namely,

$$\operatorname{rank} \left\langle \left(\frac{1}{2} \cdot \mathcal{B}^2(1) \right) \cap \Lambda_2 \right\rangle_{\mathbb{Z}} = 2$$

because $\overline{\ell}_1, \overline{\ell}_2 \in \left(\frac{1}{2} \cdot \mathcal{B}^2(1)\right) \cap \Lambda_2$ but $\left(\lambda \cdot \mathcal{B}^2(1)\right) \cap \Lambda_2 = \{\overline{0}\}$ for all $0 < \lambda < \frac{1}{2}$.

Successive minima

Therefore

$$\begin{aligned} \beta_1 &= \inf \left\{ \lambda > 0 \,\middle|\, \operatorname{rank} \left\langle (\lambda \mathcal{B}^2(1)) \cap \Lambda_2 \right\rangle_{\mathbb{Z}} \geq 1 \right\} = \frac{1}{2}, \\ \beta_2 &= \inf \left\{ \lambda > 0 \,\middle|\, \operatorname{rank} \left\langle (\lambda \mathcal{B}^2(1)) \cap \Lambda_2 \right\rangle_{\mathbb{Z}} \geq 2 \right\} = \frac{1}{2}. \end{aligned} \tag{15}$$

Now we have found linearly independent lattice points $\overline{y}_1 := \overline{\ell}_1, \overline{y}_2 := \overline{\ell}_2$ such that

$$\begin{aligned} \|\overline{y}_1\|_2 &= \beta_1, \\ \|\overline{y}_2\|_2 &= \beta_2. \end{aligned} \tag{16}$$

Successive minima

More generally, let

$$\beta_k := \beta_k(\mathcal{B}^n(1), \Lambda), \quad k = 1, \ldots, n, \tag{17}$$

be the successive minima of $\mathcal{B}^n(1)$ with respect to a full lattice $\Lambda \subseteq \mathbb{R}^n$.

Are there linearly independent lattice points $\overline{y}_1, \ldots, \overline{y}_n \in \Lambda$ such that

$$\|\overline{y}_k\|_2 = \beta_k \quad \forall\ k = 1, \ldots, n? \tag{18}$$

Lemma 7

There are linearly independent lattice points $\overline{y}_1, \ldots, \overline{y}_n \in \Lambda$ such that

$$\|\overline{y}_k\|_2 = \beta_k \quad \forall\ k = 1, \ldots, n. \tag{19}$$

Successive minima

Proof. Note that

$$\overline{y} \in \beta \cdot \mathcal{B}^n(1) \quad \Leftrightarrow \quad \|\overline{y}\|_2 \leq \beta. \tag{20}$$

By the definition

$$\beta_k = \inf \left\{ \lambda > 0 \middle| \text{ rank} \left\langle (\lambda \cdot \mathcal{B}^n(1)) \cap \Lambda \right\rangle_{\mathbb{Z}} \geq k \right\}. \tag{21}$$

Thus there exist k linearly independent vectors $\overline{y}_1, \ldots, \overline{y}_k$ such that

$$\overline{y}_1, \ldots, \overline{y}_k \in (\beta_k \cdot \mathcal{B}^n(1)) \cap \Lambda. \tag{22}$$

Hence we may write

$$\|\overline{y}_1\|_2 \leq \ldots \leq \|\overline{y}_k\|_2 \leq \beta_k. \tag{23}$$

Successive minima

If we now suppose

$$\beta := \|\overline{y}_k\|_2 < \beta_k, \tag{24}$$

then

$$\overline{y}_1, \ldots, \overline{y}_k \in (\beta \cdot \mathcal{B}^n(1)) \cap \Lambda. \tag{25}$$

Thus, by (21) we have

$$\beta_k \leq \beta. \tag{26}$$

A contradiction. □

Shortest vector in a lattice

A non-zero vector $\overline{s} \in \Lambda$ is called a minimal vector or a shortest vector in the lattice $\Lambda \subseteq \mathbb{R}^n$, if

$$\sigma = \sigma_\Lambda := \|\overline{s}\|_2 \leq \|\overline{h}\|_2, \quad \forall\ \overline{h} \in \Lambda \setminus \{\overline{0}\}. \tag{27}$$

It can be proved that minimal vectors exist.

Let

$$\beta_1 = \inf \left\{ \lambda > 0 \middle|\ \text{rank} \left\langle (\lambda \cdot \mathcal{B}^n(1)) \cap \Lambda \right\rangle_{\mathbb{Z}} \geq 1 \right\}. \tag{28}$$

be the first minimum of $\mathcal{B}^n(1)$ with respect to a lattice $\Lambda \subseteq \mathbb{R}^n$.

Shortest vector in a lattice

Lemma 8

Let $\overline{s}$ be a minimal vector of the full lattice Λ. Then

$$\sigma = \beta_1, \tag{29}$$

where β_1 is given in (17).

Proof. By Lemma 7 we know there exists a lattice vector $\overline{y}_1$ such that

$$\|\overline{y}_1\|_2 = \beta_1. \tag{30}$$

Thus

$$\sigma \leq \beta_1. \tag{31}$$

Shortest vector in a lattice

If we assume

$$\sigma < \beta_1, \tag{32}$$

then

$$\overline{s} \in (\sigma \cdot \mathcal{B}^n(1)) \cap \Lambda. \tag{33}$$

But

$$(\lambda \cdot \mathcal{B}^n(1)) \cap \Lambda = \{\overline{0}\} \tag{34}$$

for all $0 < \lambda < \beta_1$ by the definition

$$\beta_1 = \inf \left\{ \lambda > 0 \,\middle|\, \text{rank} \left\langle (\lambda \cdot \mathcal{B}^n(1)) \cap \Lambda \right\rangle_{\mathbb{Z}} \geq 1 \right\}. \quad \square \tag{35}$$

An estimate for the first minimum

By Theorem 3 we have

$$\mathrm{vol}\,(\beta_1 \cdot \mathcal{B}^n(1)) \leq 2^n \det \Lambda. \tag{36}$$

Using $\mathcal{B}^n(\beta_1) = \beta_1^n \cdot \mathcal{B}^n(1)$ and (36) we get

$$\mathrm{vol}\,(\beta_1 \cdot \mathcal{B}^n(1)) = \frac{\pi^{n/2}\beta_1^n}{\Gamma(1+n/2)} \leq 2^n \det \Lambda. \tag{37}$$

Hence we get an estimate

$$\beta_1 \leq \frac{2}{\sqrt{\pi}}\Gamma(1+n/2)^{1/n}\,(\det \Lambda)^{1/n} \tag{38}$$

for the first minimum of $\mathcal{B}^n(1)$ with respect to a lattice $\Lambda \subseteq \mathbb{R}^n$.

An estimate for shortest vectors

Let $\overline{s}$ be a minimal vector of the lattice Λ. Then

$$\|\overline{s}\|_2 = \beta_1. \tag{39}$$

Thus by (38) we have an estimate for shortest vectors.

Lemma 9

Let $\overline{s}$ be a minimal vector of the full lattice $\Lambda \subseteq \mathbb{R}^n$. Then

$$\sigma_\Lambda = \|\overline{s}\|_2 \leq \frac{2}{\sqrt{\pi}}\Gamma(1+n/2)^{1/n}\left(\det\Lambda\right)^{1/n}. \tag{40}$$

Examples

Example 10

$n = 2$.

$$\sigma_\Lambda = \|\bar{s}\|_2 \leq \frac{2}{\sqrt{\pi}} (\det \Lambda)^{1/2} \leq 1.1284 \, (\det \Lambda)^{1/2} . \qquad (41)$$

Example 11

$\Lambda = \mathbb{Z}^2$.

$$\sigma(\mathbb{Z}^2) \leq \frac{2}{\sqrt{\pi}} \leq 1.1284, \qquad (42)$$

while the true value of the shortest vectors is $\sigma(\mathbb{Z}^2) = 1$.

Examples

Example 12

Define a triangular (hexagonal) lattice

$$\Lambda_{t2} := \left\langle \bar{\ell}_1, \bar{\ell}_2 \right\rangle_{\mathbb{Z}}, \quad \bar{\ell}_1 = \bar{e}_1,\ \bar{\ell}_2 = \frac{1}{2}\bar{e}_1 + \frac{\sqrt{3}}{2}\bar{e}_2. \tag{43}$$

By (41) we get an estimate

$$\sigma_{\Lambda_{t2}} \le \frac{2}{\sqrt{\pi}}\sqrt{\frac{\sqrt{3}}{2}} = \sqrt{\frac{2\sqrt{3}}{\pi}} \le 1.051, \tag{44}$$

while the true value of the shortest vectors in the lattice Λ_{t2} is $\sigma_{\Lambda_{t2}} = 1$.

Lattice packing

Definition 13

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice and let $\mathcal{P} \subseteq \mathbb{R}^n$ be a compact set with $\mathrm{vol}\,\mathcal{P} \leq \det \Lambda$. The sets $\overline{h} + \mathcal{P}$ form a lattice packing

$$\Lambda + \mathcal{P} = \bigcup_{\overline{h} \in \Lambda} (\overline{h} + \mathcal{P}) \tag{45}$$

of $\mathcal{P}$, if

$$\mathrm{int}\,(\overline{h}_i + \mathcal{P}) \cap \mathrm{int}\,(\overline{h}_j + \mathcal{P}) = \emptyset \quad \forall i \neq j. \tag{46}$$

NOTE: The interiors of different sets $\overline{h}_i + \mathcal{P}$ are disjoint but there are different sets whose boundaries may intersect.

Lattice packing

Lemma 14

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice. Suppose $\mathcal{K} \subseteq \mathbb{R}^n$ is a central symmetric convex body containing no non-zero lattice Λ points. Then

$$\left(\overline{h}_i + \frac{1}{2}\mathcal{K}\right) \cap \left(\overline{h}_j + \frac{1}{2}\mathcal{K}\right) = \emptyset \quad \forall i \neq j. \tag{47}$$

Proof. Assume there exist $\overline{h}_i \neq \overline{h}_j \in \Lambda$ such that

$$\overline{h}_i + \frac{1}{2}\overline{k}_i = \overline{h}_j + \frac{1}{2}\overline{k}_j \tag{48}$$

for some $\overline{k}_i, \overline{k}_j \in \mathcal{K}$.

Lattice packing

As in the proof of the first Minkowski's theorem we get

$$\overline{h}_i - \overline{h}_j = \frac{1}{2}\overline{k}_j - \frac{1}{2}\overline{k}_i \in \mathcal{K}. \tag{49}$$

Hence $\overline{h}_i = \overline{h}_j$ because $\mathcal{K}$ does not contain non-zero lattice points.

Further, $\overline{k}_i = \overline{k}_j$. Therefore

$$\left(\overline{h}_i + \frac{1}{2}\mathcal{K}\right) \cap \left(\overline{h}_j + \frac{1}{2}\mathcal{K}\right) = \emptyset \quad \forall i \neq j. \quad \square \tag{50}$$

Lattice packing

Corollary 15

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice. Suppose $\mathcal{K} \subseteq \mathbb{R}^n$ is a central symmetric compact convex body containing no non-zero lattice Λ points satisfying

$$\operatorname{vol} \frac{1}{2}\mathcal{K} \leq \det \Lambda. \tag{51}$$

Then

$$\Lambda + \frac{1}{2}\mathcal{K} \tag{52}$$

is a lattice packing.

Lattice packing densities

Definition 16

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice and let $\mathcal{P} \subseteq \mathbb{R}^n$ be a compact set with $\operatorname{vol}\mathcal{P} \leq \det\Lambda$. A lattice packing density is given by

$$\Delta_n(\mathcal{P},\Lambda) := \frac{\operatorname{vol}\mathcal{P}}{\det\Lambda}. \tag{53}$$

The supremum over all lattices packing lattices Λ of $\mathcal{P}$ is denoted by

$$\Delta_n(\mathcal{P}) := \sup_{\Lambda} \Delta_n(\mathcal{P},\Lambda). \tag{54}$$

Lattice packing density

Lemma 17

Let $L: \mathbb{R}^n \to \mathbb{R}^n$ be a one to one linear transformation. Then

$$\Delta_n(L\mathcal{P}) = \Delta_n(\mathcal{P}). \tag{55}$$

Proof. First we note

$$\Delta_n(L\mathcal{P}, L\Lambda) = \frac{\mathrm{vol}(L\mathcal{P})}{\det(L\Lambda)} = \frac{\det L \cdot \mathrm{vol}\,\mathcal{P}}{\det L \cdot \det \Lambda} = \Delta_n(\mathcal{P}, \Lambda). \tag{56}$$

From the injectivity of L follows that Λ is a lattice packing lattice of $\mathcal{P}$ exactly when $L\Lambda$ is a lattices packing lattice of $L\mathcal{P}$.

Lattice packing density

Therefore

$$\begin{aligned}\Delta_n(\mathcal{P}) &= \sup_{\Lambda} \Delta_n(\mathcal{P}, \Lambda) \\ &= \sup_{L\Lambda} \Delta_n(L\mathcal{P}, L\Lambda) \\ &= \sup_{\Lambda'=L\Lambda} \Delta_n(L\mathcal{P}, \Lambda') \\ &= \Delta_n(L\mathcal{P}),\end{aligned} \tag{57}$$

where the last supremum is determined over all lattices packing lattices Λ' of $L\mathcal{P}$. □

The second revision of the first Minkowski's theorem

Theorem 18

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice and let $\mathcal{C} \subseteq \mathbb{R}^n$ be central symmetric compact convex body. Assume

$$\operatorname{vol}\mathcal{C} > 2^n \cdot \det\Lambda \cdot \Delta_n(\mathcal{C}). \tag{58}$$

Then there exists a non-zero lattice point in $\mathcal{C}$.

The second revision of the first Minkowski's theorem

Proof. Assume, on the contrary, that $\mathcal{C} \cap \Lambda = \{\overline{0}\}$. By the first Minkowski's theorem we have $\mathrm{vol}(\mathcal{C}) \leq 2^n \det \Lambda$ which implies $\mathrm{vol}(\frac{1}{2} \cdot \mathcal{C}) \leq \det \Lambda$. Thus $\Lambda + \frac{1}{2}\mathcal{C}$ is a lattice packing by Corollary 15. By Lemma 17 and the definition of density

$$\Delta_n(\mathcal{C}) = \Delta_n\left(\frac{1}{2}\mathcal{C}\right) \geq \Delta_n\left(\frac{1}{2}\mathcal{C}, \Lambda\right) = \frac{\mathrm{vol}\left(\frac{1}{2}\mathcal{C}\right)}{\det \Lambda} = \left(\frac{1}{2}\right)^n \frac{\mathrm{vol}(\mathcal{C})}{\det \Lambda}. \quad \square \tag{59}$$

Lattice sphere packing

The spheres (balls) $\mathcal{B}^n(R,\overline{h})$ centered at lattice points $\overline{h}$ form a lattice packing

$$\mathcal{B}^n(R)+\Lambda=\bigcup_{\overline{h}\in\Lambda}\mathcal{B}^n(R,\overline{h}), \tag{60}$$

if

$$\operatorname{int}\mathcal{B}^n(R,\overline{h_i})\cap\operatorname{int}\mathcal{B}^n(R,\overline{h_j})=\emptyset\quad\forall i\neq j. \tag{61}$$

The interiors of different spheres are disjoint but there are different spheres whose boundaries may intersect.

Lattice sphere packing densities

Obviously the maximum radius of any lattice sphere packing is $R = \sigma_\Lambda/2 = \beta_1/2$, half of the length $\sigma = \sigma_\Lambda := \|\overline{s}_1\|_2$ of a shortest vector $\overline{s}_1$ in Λ. Therefore we define

Definition 19

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice. A sphere lattice packing density is given by

$$\Delta_n(\mathcal{B}^n(\sigma_\Lambda/2), \Lambda) := \frac{\operatorname{vol} \mathcal{B}^n(\sigma_\Lambda/2)}{\det \Lambda}. \tag{62}$$

The maximal sphere packing density, the supremum over all lattices Λ, is denoted by

$$\Delta_{\mathcal{B},n} := \sup_{\Lambda} \Delta_n(\mathcal{B}^n(\sigma_\Lambda/2), \Lambda). \tag{63}$$

Lattice sphere packing densities

Hereby

$$\Delta_n(\mathcal{B}^n(\sigma_\Lambda/2),\Lambda)=\frac{\pi^{n/2}\sigma_\Lambda^n}{2^n\Gamma(1+n/2)\det\Lambda}\leq\Delta_{\mathcal{B},n}. \tag{64}$$

Hence, we may refine estimate (40) as follows

Lemma 20

Let $\overline{s}$ be a minimal vector of the full lattice $\Lambda\subseteq\mathbb{R}^n$. Then

$$\sigma_\Lambda=\|\overline{s}\|_2\leq\frac{2}{\sqrt{\pi}}\Gamma(1+n/2)^{1/n}\left(\det\Lambda\right)^{1/n}\left(\Delta_{\mathcal{B},n}\right)^{1/n}. \tag{65}$$

Triangular (hexagonal) lattice

Example 21

Let Λ_{t2} be the triangular (hexagonal) lattice

$$\Lambda_{t2} := \langle \overline{\ell}_1, \overline{\ell}_2 \rangle_{\mathbb{Z}}, \quad \overline{\ell}_1 = \overline{e}_1, \ \overline{\ell}_2 = \frac{1}{2}\overline{e}_1 + \frac{\sqrt{3}}{2}\overline{e}_2. \tag{66}$$

The sphere lattice packing density with respect to the triangular lattice Λ_{t2} is given by

$$\begin{aligned} \Delta_2(\mathcal{B}^2(\sigma_{\Lambda_{t2}}/2), \Lambda_{t2}) &= \frac{\operatorname{vol} \mathcal{B}^2(1/2)}{\det \Lambda_{t2}} \\ &= \frac{\pi(1/2)^2}{\sqrt{3}/2} = \frac{\pi}{2\sqrt{3}} = 0.906899\ldots. \end{aligned} \tag{67}$$

The sphere lattice packing density in dimension 2

In 1831? C.F. Gauss proved that the sphere lattice packing density given in (67) is the best among all lattices in $\mathbb{R}^2$:

Theorem 22

$$\Delta_{\mathcal{B},2} = \sup_{\Lambda} \Delta_2(\mathcal{B}^2(\sigma_\Lambda/2), \Lambda) = \frac{\pi}{2\sqrt{3}} = 0.906899\ldots, \qquad (68)$$

where the supremum is determined over all lattices $\Lambda \subseteq \mathbb{R}^2$.

In 1910 Thue proved that (68) actually gives the best sphere packing density in dimension 2.

Minimal vectors in dimension 2

Corollary 23

Let $\Lambda \subseteq \mathbb{R}^2$ be a full lattice. Then

$$\sigma_\Lambda \le \left(\frac{2}{\sqrt{3}}\right)^{1/2} (\det\Lambda)^{1/2} \le 1.07457\,(\det\Lambda)^{1/2}\,. \tag{69}$$

Proof. Estimate (65) with $n = 2$ and (68) give

$$\begin{aligned}\sigma_\Lambda &\le \frac{2}{\sqrt{\pi}}\Gamma(2)^{1/2}(\det\Lambda)^{1/2}(\Delta_{\mathcal{B},2})^{1/2}\\ &= \frac{2}{\sqrt{\pi}}\left(\frac{\pi}{2\sqrt{3}}\right)^{1/2}(\det\Lambda)^{1/2} = \left(\frac{2}{\sqrt{3}}\right)^{1/2}(\det\Lambda)^{1/2}\,. \quad \square\end{aligned} \tag{70}$$

Examples

Example 24

In the triangular (hexagonal) lattice Λ_{t2} we get an estimate

$$\sigma_{\Lambda_{t2}} \leq 1, \tag{71}$$

while the true value of the shortest vectors in the lattice Λ_{t2} is $\sigma_{\Lambda_{t2}} = 1$.

Examples

Example 25

Problem 24. Consider the lattice

$$\Lambda_\pi = \left\langle (\pi, 1/7)^t, (1, 1/22)^t \right\rangle_{\mathbb{Z}}. \tag{72}$$

By (69) we have an estimate

$$\sigma_{\Lambda_\pi} \leq \left(\frac{2}{\sqrt{3}} \det \Lambda \right)^{1/2} = \left| \frac{2}{\sqrt{3}} \left(\frac{\pi}{22} - \frac{1}{7} \right) \right|^{1/2} = 0.0081466\ldots. \tag{73}$$

For example

$$\|22(1, 1/22)^t - 7(\pi, 1/7)^t\|_2 = 0.0088514\ldots. \tag{74}$$

Thus $22(1, 1/22)^t - 7(\pi, 1/7)^t$ can not be a minimal vector.

Examples

We will show that

$$\sigma_{\Lambda_\pi} = \|355(1, 1/22)^t - 113(\pi, 1/7)^t\|_2 = 0.00649357\ldots. \tag{75}$$

Proof. Take an arbitrary vector

$$v(a, b) := a(\pi, 1/7)^t - b(1, 1/22)^t \in \Lambda_\pi, \ \ a, b \in \mathbb{Z}, \tag{76}$$

and estimate its length

$$\|v(a, b)\| = \sqrt{(a\pi + b)^2 + \left(\frac{22a - 7b}{7 \cdot 22}\right)^2} \tag{77}$$

from below.

Examples

1. If

$$22a - 7b = 0, \tag{78}$$

then

$$a = k7, \;\; b = k22, \quad k \in \mathbb{Z} \setminus \{0\}. \tag{79}$$

Now

$$\begin{aligned} \|v(a,b)\| &= \sqrt{(a\pi - b)^2 + \left(\frac{22a - 7b}{7 \cdot 22}\right)^2} \\ &= \sqrt{k^2(7\pi - 22)^2} = |k||7\pi - 22| \geq 0.0088514\ldots. \end{aligned} \tag{80}$$

Examples

2. If

$$|22a - 7b| \geq 2, \tag{81}$$

then

$$\begin{aligned} \|v(a,b)\| &= \sqrt{(a\pi - b)^2 + \left(\frac{22a - 7b}{7 \cdot 22}\right)^2} \\ &> \sqrt{0 + \left(\frac{2}{7 \cdot 22}\right)^2} = \frac{1}{7 \cdot 11} = 0.012987\ldots. \end{aligned} \tag{82}$$

Examples

3. Let

$$|22a - 7b| = 1, \tag{83}$$

then

$$a = 1 + k7, \;\; b = 3 + k22, \quad k \in \mathbb{Z}, \tag{84}$$

see Basic Number Theory course. Now

$$\begin{aligned} \|v(a,b)\|_2 &= \sqrt{(a\pi - b)^2 + \left(\frac{22a - 7b}{7 \cdot 22}\right)^2} \\ &= \sqrt{(a\pi - b)^2 + \left(\frac{1}{7 \cdot 22}\right)^2}. \end{aligned} \tag{85}$$

Examples

3. So, it is up to find the minimum of

$$|a\pi - b| = |(1+7k)\pi - (3+22k)|, \quad k \in \mathbb{Z}. \tag{86}$$

We have

$$|(1+7k)\pi - (3+22k)| = \begin{cases} (22-7\pi)k - (\pi - 3), & k \geq \frac{\pi-3}{22-7\pi}; \\ \pi - 3 - (22-7\pi)k, & k < \frac{\pi-3}{22-7\pi}. \end{cases} \tag{87}$$

Because $\frac{\pi-3}{22-7\pi} = 15.9966\ldots$, then the minima of the above function pieces are attained at $k = 16$ and $k = 15$, respectively, where the minimum $(22-7\pi)16 - (\pi - 3)$ is smaller.

Examples

Hence $113(\pi, 1/7)^t - 355(1, 1/22)^t$ will be a minimal vector and

$$\begin{aligned} \|v(a,b)\|_2 &\geq \|v(113,355)\|_2 = \|113(\pi,1/7)^t - 355(1,1/22)^t\|_2 \\ &= \sqrt{(113\pi - 355)^2 + \left(\frac{1}{7\cdot 22}\right)^2} \\ &= 0.00649357\ldots. \quad \square \end{aligned} \tag{88}$$

The SVP-problem

Example 25 and other exercise problems show that finding a shortest vector may be quite challenging even in dimension 2 and 3.

The SVP-problem: Create a polynomial time algorithm that finds a shortest vector in an arbitrary dimension n.

It is generally not known whether such an algorithm exists. Thereby, people are investigating quantum-safe or post-quantum cryptosystems based e.g. on the hardness of the SVP-problem.

The sphere packing density in dimension 3/The Kepler problem

The Kepler conjecture 1611: In dimension 3 the best sphere packing density is $\frac{\pi}{3\sqrt{2}} = 0.74048\ldots$.

In 1831 C.F. Gauss proved the Kepler bound for lattice sphere packings:

Theorem 26

$$\Delta_{\mathcal{B},3} = \frac{\pi}{3\sqrt{2}} = 0.74048\ldots, \tag{89}$$

The sphere packing density in dimension 3/The Kepler problem

Density (89) may be received by the face-centered cubic lattice

$$\Lambda_{fcc} = \left\langle (1,1,0)^t, (1,-1,0)^t, (0,1,-1)^t \right\rangle_{\mathbb{Z}}, \tag{90}$$

Finally in 1998 T.C. Hales proved the full Kepler conjecture, namely, that (89) indeed is the best sphere packing in dimension 3.

Minimal vectors in dimension 3

Corollary 27

Let $\Lambda \subseteq \mathbb{R}^3$ *be a full lattice. Then*

$$\sigma_\Lambda \leq 2^{1/6} (\det \Lambda)^{1/3} . \tag{91}$$

The Kepler problem in dimension n

In dimension $n \geq 4$ the sphere packing problem is open. However, the optimal lattice packing is known in dimension $n \in \{2, 3, 4, 5, 6, 7, 8, 24\}$.

See more at Lenny Fukshansky's web-page

Link: Talk 32. Sphere packing, lattices, and Epstein zeta function.

The third revision of the first Minkowski's theorem

Theorem 28

Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice and let $\mathcal{C} \subseteq \mathbb{R}^n$ be central symmetric compact convex body. Then

$$\mathrm{vol}(\lambda_1 \mathcal{C}) \leq 2^n \cdot \det \Lambda \cdot \Delta_n(\mathcal{C})\,. \tag{92}$$

The third revision of the first Minkowski's theorem

Proof. Assume, on the contrary, that $\operatorname{vol}(\lambda_1 \cdot \mathcal{C}) > 2^n \cdot \det \Lambda \cdot \Delta_n(\mathcal{C})$. Then there exists a $\lambda < \lambda_1$ such that

$$\operatorname{vol}(\lambda \cdot \mathcal{C}) > 2^n \cdot \det \Lambda \cdot \Delta_n(\mathcal{C}) = 2^n \cdot \det \Lambda \cdot \Delta_n(\lambda \cdot \mathcal{C}). \tag{93}$$

By Theorem 18 there exists a non-zero point in $(\lambda \cdot \mathcal{C}) \cap \Lambda$. Thus

$$\operatorname{rank} \left\langle (\lambda \cdot \mathcal{C}) \cap \Lambda \right\rangle_{\mathbb{Z}} \geq 1 \tag{94}$$

which contradicts the definition of

$$\lambda_1 = \inf\{\lambda > 0 \mid \operatorname{rank} \langle (\lambda\mathcal{C}) \cap \Lambda \rangle_{\mathbb{Z}} \geq 1\}. \quad \square \tag{95}$$

The second Minkowski's convex body theorem

Theorem 29

Let $n \in \mathbb{Z}^+$. Assume that $\Lambda \subseteq \mathbb{R}^n$ is a lattice with rank $\Lambda = n$ and $\mathcal{C} \subseteq \mathbb{R}^n$ is a central symmetric convex body. Then

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 \cdots \lambda_n V(\mathcal{C}) \leq 2^n \det \Lambda.$$